FROM CONTAGION TO STABILITY: INSIGHTS INTO NETWORK DYNAMICS, RESILIENCE AND STABILITY

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Marios Papachristou

August 2025

Dissertation Committee

Jon M. Kleinberg (Thesis Advisor)

Department of Computer Science

Cornell University

Siddhartha Banerjee

Department of Operations Research and Information Engineering

Cornell University

Emma Pierson

Department of Electrical Engineering and Computer Science

University of California, Berkeley

M. Amin Rahimian

Department of Industrial Engineering

University of Pittsburgh

FROM CONTAGION TO STABILITY:

INSIGHTS INTO NETWORK DYNAMICS, RESILIENCE AND STABILITY

Marios Papachristou, Ph.D.

Cornell University 2025

The resilience of interconnected systems, such as financial networks, supply chains, software systems, and social networks, is a critical concern in today's highly connected world. While interconnectedness enables efficient economic transactions, rapid social learning, and adaptability to shocks, it also increases vulnerability to systemic risks, where localized disruptions can propagate and cause widespread failures.

This thesis addresses this fundamental challenge by examining how to reason about and reinforce the resilience of complex networks through theoretical and applied tools, including probability, statistics, algorithms, and network science, whereas we rely on centralized and decentralized decision-making to design interventions that mitigate cascading failures and bolster network stability. First, the thesis focuses on optimizing resource allocation in networks undergoing contagion, developing novel resilience metrics for supply chains, and creating efficient algorithms to prevent cascading failures. Secondly, this thesis studies models of contagion and gives a formalized definition of resilience. Then, this thesis explores decentralized privacy-aware decision-making to reconcile privacy with efficient social learning in risk-prone environments to ensure resilience. Finally, the thesis studies models of network formation and also suggest modern ways to view complex interconnected systems through the lens of LLMs.

BIOGRAPHICAL SKETCH

Marios Papachristou is a computer scientist who studies the resilience of complex systems. Marios was born in Athens, Greece, and obtained his Electrical and Computer Engineering undergraduate degree from the National Technical University of Athens. Since September 2020, Marios has pursued his PhD at Cornell University, advised by Jon Kleinberg. His research has been funded by LinkedIn, Cornell, the Onassis Foundation, the A.G. Leventis Foundation, and the Gerondelis Foundation. Marios enjoys cycling, cooking, going to the gym, and dancing in his free time. Marios will join the Department of Information Systems at the W.P. Carey School of Business at Arizona State University as a tenure-track Assistant Professor starting in Fall 2025.

Dedicated to all of those around me who have supported me in my journey and dreams.

This thesis is a testimony to all of you!

ACKNOWLEDGEMENTS

Earning a Ph.D. is a long and challenging journey, marked by many ups and downs and unexpected turns. I am deeply grateful to those who have supported and guided me throughout my Ph.D. journey.

First and foremost, I extend my deepest gratitude to my advisor, Jon Kleinberg, whose exceptional mentorship, brilliant insights, and unwavering support have profoundly shaped my academic journey. Your guidance has not only sharpened my research skills but also fostered my personal growth in ways I could never have anticipated. Jon, your tactful sense of humor and genuine encouragement made even the toughest moments manageable, and I feel incredibly fortunate to have had you as a mentor and role model. Thank you for everything!

I would also like to thank Sid Banerjee wholeheartedly for his mentorship and advice throughout my Ph.D. Sid, I will always remember our long meetings in your office before the paper submission deadlines!

I am truly grateful to Emma Pierson for her invaluable support and advice on career matters. Emma, I appreciate your constant (and instant) availability to discuss any thoughts that arise!

I would like to express my heartfelt gratitude to my longtime coauthor and thesis committee member, Amin Rahimian, for the many network papers we coauthored, for introducing me to new research topics, for sharing our common interests on probability and networks, and for his mentorship and kind advice!

Moreover, I want to thank my collaborator, Yuan Yuan, for giving me invaluable knowledge about empirical research and for helping me do fun projects with LLMs.

I am also indebted to my great collaborators from the Volesti open-source

project, which I contributed to and helped grow and maintain during the first part of my Ph.D.: Apostolos Chalkis, Vissarion Fisikopoulos, and Elias Tsigaridas.

I want to thank Yong-Yeol (YY) Ahn for the great collaboration opportunities and his continued support!

I would also want to thank my other collaborators, Rachith Aiyappa, Junsol Kim, Byungkyu Lee (BK), Akhil Jalan, Anirudh Rayas, Jasmine Li, Ioannis Iakovidis, Negin Raoof, Alkis Kalavasis, Alex Dimakis, and Costis Daskalakis. Thanks for doing great research every day!

Thanks to my industry collaborators, specifically my internship mentor, Chin-Chia Hsu, for introducing me to the world of LLMs for the first time and for coauthoring a really cool paper that gave new directions to my future research! I also want to thank Longqi Yang and the rest of Microsoft's Office of Applied Research for their support during my time there.

Also, thanks to my mentor, Rishab Goel, for introducing me to real-world billion-scale industry problems, as well as Matt Miller, Frank Portman, Rong Jin, and Rani Nelken at the User Modeling Research Group from Twitter.

Additionally, I want to thank Kate Donahue, Vasilis Charisopoulos, Manish Raghavan, Serina Chang, Nikhil Garg, and Emma Pierson for their advice during my Ph.D. and during the job market.

My time in the Ph.D. program has greatly benefited from my interaction with the Cornell/Ithaca community and my friends. Thanks, Kate Donahue, Kiran Tomlinson, Michela Meister, Yanbang Wang, Katie van Koevering, Katy Blumer, Caz Comrie, Ben Laufer, Emily Ryu, Sophie Greenwood, Yoav Kolumbus, Gali Noti, Giannis Fikioris, Sloan Nietert, Makis Arsenis, Dan Bateyko, Spencer Peters, Princewill Okoroafor, Abhishek Vijaya Kumar, Farhana Shahid,

Mohit Gurumukhani, Lehka Revankar, Matt Einchorn, Sean Sinclair, Abhay Singh, Connor Lawless, Arjun Devraj, Jason Gaitonde, Raunak Kumar, Makis Arsenis, Jesse Goodman, Nitika Saran, Erald Sinanaj, Richa Rastogi, Ayush Sekhari, Vasilis Charisopoulos, Giannis Ntekas, Renia Kotsinonou, Colin Bundschu, Rafael Panagiotopoulos, Andreas Stephanou, Tilemachos Bolioudakis, Thea Nikolaou, Theo Koutserimpas, Jason Milionis, Giannis Pyrovolakis, Alex Polyzois, Aias Asteris, Anna Koshcheeva, Alexandra Khlyustova, Ece Erlat, Kostas Ameranis, Polina Alexeenko, the AIPP community, the Coal Yard Café, and many others!

I am grateful to Johan Ugander, Deepay Chakrabarti, Georgios Gousios, and my attorneys at Chen Immigration for their support of my green card petition.

I would like to thank the department staff and specifically Becky Stewart, Kim Budd, Randy Hess, Coralia Torres, and Kelsey Whiting for their invaluable help!

The work presented in this thesis would not have been possible without financial support from LinkedIn, the Cornell Graduate School, the Alexander S. Onassis Public Benefit Foundation, the A.G. Leventis Foundation, and the Gerondelis Foundation for their support through scholarships and fellowships. Additionally, I would like to thank the National Science Foundation, the Simons Foundation, the MacArthur Foundation, the US Department of Defense, and the US Air Force Office of Scientific Research for supporting the research presented in this thesis.

I am fortunate to have had the unwavering friendship of Stavros, Giannis, Harry, and Victor, whose encouragement and camaraderie have made this journey all the more meaningful.

I extend my deepest gratitude to my parents, Apostolos and Panagiota; my

sisters, Anastasia and Angelina; and my beloved aunt Rena. Your unwavering support, encouragement, and love have been my constant source of strength throughout this journey. Lastly, Ezgi — your love, patience, and unwavering belief in me have meant more than words can express. Through every challenge, your presence has been my anchor and my greatest comfort. Thank you for your endless support and for walking this path with me! I am forever grateful. This thesis is dedicated to all of you!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION AND THESIS OVERVIEW

The global financial system, supply chain, software systems, and modern gigantic social networks are highly interconnected. Being interconnected is beneficial for the function of the global economy and society since it enables efficient economic transactions, fast social learning, and more flexibility in response to exogenous shocks. Interconnectedness has many benefits, but it also brings new challenges, such as increased vulnerability to systemic risks, since small localized shocks and disruptions have an unexpected effect and may wreak havoc on the global system, such as price volatility, disruption in the production system, and disruption to the diffusion of information.

Several recent events include the economic impacts of the global trade war, the global supply chain failures, and the recent CrowdStrike software failure.

Understanding how failures spread in interconnected networks is a topic of cardinal importance given the well-connected structure of our modern world. For instance, the supply chain disruptions and the economic crisis caused by the recent pandemic show how localized incidents can spread rapidly. Our overarching research question is:

How do we reason about and ensure the resilience of complex networks?

Through our research, we study the resilience of networks and the broader societal impacts of complex networks through modeling, decision-making, and intervention design. We use a mix of theoretical and applied tools, particularly probability, statistics, algorithms, and network science techniques, providing a

unified and interdisciplinary approach to study contagion, risk, and decision-making for several problem domains. The work presented in this thesis can be partitioned into two main themes, *centralized* and *decentralized* inference and decision-making, and more broadly addresses the following interrelated questions:

1. *How does a central planner **measure** and **reinforce** the resilience of networks?* In Chapter 2 (see also [320, 322, 321, 324]), we study how limited resources can be (optimally) allocated in a network that undergoes contagion. We give a polynomial-time algorithm to solve the underlying Markov Decision Process, provide algorithms with provable approximation guarantees (optimal under reasonable assumptions) for the case of discrete controls, and test the algorithms with real-world data.

2. *What are **metrics** to characterize the resilience of a network?* In Chapter 3, we propose a novel topological measure of resilience. We develop efficient algorithms to calculate the resilience in large-scale networks by leveraging LP duality and establishing novel connections with widely used models of financial contagion and systemic risk. Besides, we also develop algorithms to allocate resources to avert cascading failures and devise mathematically motivated and "rules-of-thumb".

3. *How can **decentralized privacy-aware decisions** reinforce the resilience of networks?* Agents operating in risky environments, such as banks deciding whom to lend to, operate under uncertainty and face privacy considerations, such as regulations regarding disclosing their clients' financial data. Preserving individual privacy and enabling efficient social learning is crucial to making these complex systems robust to failures; however, privacy

and efficiency seem fundamentally at odds with each other and are hard to reconcile. In our research, we rely on the framework of differential privacy (DP) to control information leakage.

In Chapter 4, we provide algorithms for parameter estimation and online learning in discrete and continuous parameter spaces under uncertainty and offer noise-optimal algorithms for learning under uncertainty subject to DP (cf. [325, 326]). Our results flesh out important trade-offs between privacy, accuracy, and communication complexity.

4. *How can we build **stylized models** to promote or stop contagion?* Many complex networks are characterized by the so-called core-periphery structure, where a small number of well-connected nodes "dominate" the whole network, and have been shown to be able to make networks more resilient or allow rampant failures. In Chapter 5, we axiomatize core-periphery graphs and hypergraphs, provide scalable algorithms for inference and sampling in large-scale real-world data (cf. [318, 323]).

5. *Can we make network models and contagion processes "richer" via using **LLM agents?*** Furthermore, the recent emergence of Large Language Models (LLMs) has brought a lot of interest in studying interactions of multi-agent systems comprised of LLM agents. Our work in Chapter 6 analyzes *LLMs' network formation behavior* to examine whether the dynamics of multiple LLMs are similar to or different from human social dynamics. We find that LLMs exhibit key social network principles, including preferential attachment, triadic closure, homophily, community structure, and the small-world phenomenon when asked about their preferences in network formation. In real-world networks, LLMs exhibit a stronger tendency towards triadic closure and homophily compared to preferential

attachment.

1.1 Optimal Interventions to Remediate Contagion

An exciting class of problems involves optimal interventions in dynamic networks that experience exogenous shocks. It is well-documented that the recent pandemic has spread uncertainty among financial entities that experience income shocks. A policy framework is stimulus checks, i.e., cash injections into the financial system so that consumption is stimulated and contagion is averted. A cardinal question policymakers face is [338, 389]: *Who gets the interventions?* A typical pattern in these scenarios is that when somebody's income is below a certain threshold or satisfies some criterion, the household is entitled to a fixed-value check, depending on the entity's features. However, such rules are limited by ignoring contagion effects through the financial network. If a business defaults, that may translate to job loss for the employees, who may not be able to pay their debts, potentially creating a sequence of defaults.

A planner who aims to avert contagion faces two main design questions: The first question corresponds to how the agents ration their assets upon defaults, which corresponds to solving a high-dimensional intractable problem (cf. [40, 44]), and the second question corresponds on how to allocate resources to resuscitate the network which can have significant impact on the economy and society.

In Chapter 2 (cf. [322, 320, 321]), we address this issue by designing algorithms to remediate contagion in dynamic networks undergoing shocks. The corresponding high-dimensional optimization problem, modeled by a Markov

Decision Process (MDP), is, in general, a hard problem that requires solving an exponential number of optimization problems in the time horizon T, even when the interventions are fractional.

We prove that the optimal policy for fractional interventions can be efficiently calculated by solving only a polynomial number of optimization problems in the time horizon T. Moreover, when the interventions are assumed to be discrete, we prove that this problem is hard to solve efficiently (NP-Hard). In some cases, it cannot even be solved efficiently in an approximate way, i.e., by giving solutions that are "close enough" to the best possible solution. In cases where the problem can be approximately solved, we develop efficient and principled approximation algorithms that approximate the optimal solutions. We also introduce fairness constraints regarding the intervention and study how fairly allocating stimuli affects social welfare, using fairness measures that resemble and generalize the Gini coefficient. Imposing such fairness measures can distribute resources fairly while negatively impacting social welfare.

We test our methods with real-world and semi-artificial data and compare them to heuristics that may represent simple policies that model existing government policies, such as bailing individuals and businesses earning less than a threshold income. Moreover, our framework is vastly valuable for various supply and demand networks, where if the nodes cannot meet their demand, they must split it proportionally, and the planner's goal is to remediate contagion. Examples include supply chains [324], ridesharing, high-performance computing, and influence maximization.

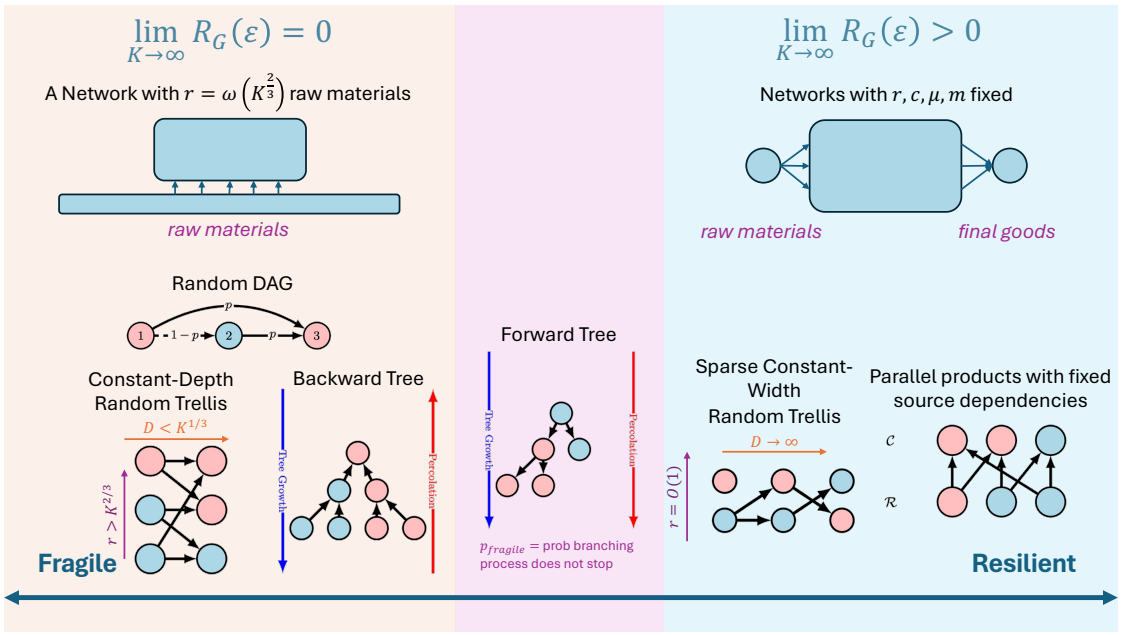


Figure 1.1: Resilience of common supply chain architectures

Cascading Failures, Resilience and Interventions in Supply Chains. A first insight into the extensions of our research above to other systems is the study of cascading failures in production networks. In Chapter 3 (cf. [324]), we develop a framework for studying how contagion spreads in production networks, which production networks are resilient, and how to design optimal interventions to avert contagion. A production network corresponds to products (e.g., computers) that a variety of suppliers can produce (e.g., HP, Lenovo, Apple, etc.) and have sourcing dependencies (e.g., graphics card, motherboard, etc.) (cf. [142]). The suppliers are hit by exogenous shocks, which result in cascading failures.

In Chapter 3 (cf. [324]), we first show that the distribution of failures in even a simple family of realistic supply chain graphs is a power law, indicating the need for formalizing a topological measure of resilience.

For this reason, we introduce the resilience metric, which is the maximum

shock that a system can withstand such that it is highly likely that a large fraction of products (e.g., 90%) will survive. We show that networks can be partitioned into two categories: fragile networks, which cannot withstand any systemic shock, and resilient networks, which can withstand nontrivial shocks even as the network size goes to infinity. Both from theoretical findings and via simulations of real-world supply-chain data, we conclude that more interconnected networks – i.e., with increased interdependencies among products – are less resilient, in agreement with prior works (cf. [142]).

For general graphs, identifying lower bounds for the resilience requires upper bounding the expected number of failures, which is generally a hard counting problem (#P-hard), and provides sample complexity bounds for estimating the cascade size. To circumvent the high complexity of sampling, we leverage LPs and prove that the number of failures can be bounded by solving a linear program in polynomial time. Furthermore, the LP for the number of failures is directly connected with the financial contagion literature [139], establishing the first connection between financial contagion and cascade models such as the independent cascade model [236]. Since financial contagion models have elegant LP structures and can accommodate additional constraints while sharing several properties with independent cascade models (hardness, inapproximability, submodularity), this opens a new realm of possibilities to perform tasks such as influence maximization, risk estimation, and network inference (see, e.g., [136]).

The rich LP structure of this upper bound can be used to design targeted intervention algorithms so that the worst-case upper bound on the size of the cascade is the smallest possible. We show that under certain assumptions, it is optimal to intervene in the products with the maximum potential impact,

which measures the dependence of other products on them. We show that the appropriate measure corresponds to the Katz centrality of the edge-reversed (or export) network. This is in agreement with our natural intuition and has been empirically observed, namely, when the big electronic chip suppliers failed during the pandemic, this resulted in a large shock to the hardware industry. Moreover, we show that the "most complex/vulnerable" products correspond to the products with many paths leading to them, corresponding to the Katz centrality of the nodes in the network. Finally, we establish connections between our proposed resilience measure and the commonly used Risk Exposure Index, as well as systemic risk measures. [371, 96].

1.2 Privacy-preserving Group Decision-making

Highly connected environments can also offer informational benefits, but to take advantage of this, we need to think about the underlying privacy issues that affect this information. Individual agents usually operate in privacy-critical environments where protecting their information and simultaneously learning from each other to assert resilience is critical. For example, consider a set of financial institutions trying to learn what stocks they should invest in while at the same time protecting their clients' portfolios. Similarly, a group of hospitals wants to learn whether a new treatment is effective; however, their clients' data are governed by privacy regulations such as HIPAA and GDPR.

Efficient information aggregation and preserving individual privacy are both crucial desiderata but seem fundamentally at odds and hard to reconcile; therefore, an important question to ask is how high is the overhead of main-

taining privacy while learning simultaneously. In Chapter 4 (cf. [326, 325]), we control information leakage using rigorous statistical guarantees based on DP. Adding DP randomization noise gives communicating agents plausible deniability concerning their private information and network neighborhoods. We consider two learning environments: linear updates for learning best estimates from a continuous state space and log-linear updates for choosing from a discrete state space.

The main technical contribution, compared to the non-private benchmarks [343], is that in privacy-preserving regimes, the addition of DP noise may change the most likely state with non-trivial probability, and, therefore, multiple runs of the algorithm need to be carefully combined to produce high-probability guarantees. To address this, we introduce two algorithms, an averaging and a thresholding algorithm where each of these algorithms produces two estimators; the former one with low Type-I error, and the latter one with low Type-II error. We compare the algorithms using the notion of communication complexity, which corresponds to the total number of belief exchanges across all instantiations of each algorithm to achieve a certain level of error and DP guarantee, and provide asymptotic analysis and finite-time convergence bounds. This way of comparing our proposed algorithms emphasizes the trade-offs between learning accuracy, communication cost, and the level and type of privacy protection the agents are afforded. Finally, we prove that the optimal noise distribution that minimizes the communication complexity is the Laplace noise with appropriately chosen parameters.

1.3 Structural Insights of Core-periphery Networks

Besides understanding the spread of failures in networks, in Chapter 5, we build stylized models to understand contagion (cf. [318, 323]). It is a frequent observation (cf. [7, 141]) that lots of financial networks and production networks obey the so-called "core-periphery" structure, where the "big players" of an economy correspond to the "core", i.e., a well-connected set that almost every other entity in the network has a connection to, and the "small players" which correspond to the "periphery" of the network which is sparsely connected, but well-connected to the core. It has been shown that depending on the magnitude of the shocks, these well-connected nodes can either amplify or repress contagion [141, 7]. In Chapter 5, we axiomatize and develop random core-periphery models for graphs and hypergraphs. We also develop efficient algorithms for sampling and inference that can run in (nearly)-linear time instead of exponential time, which naïve inference and sampling take.

Moreover, in [91, 92], we develop open-source software for high-dimensional truncated sampling, which can be used for such models.

1.4 Emergence of Complex Behavior with LLM Agents

Social networks shape opinions, behaviors, and information dissemination in human societies. As large language models (LLMs) increasingly integrate into social and professional environments, understanding their behavior within the context of social interactions and networks becomes essential.

In Chapter 6 (cf. [328]), we examine LLMs' network formation behavior to

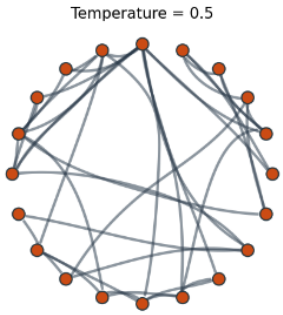


Figure 1.2: LLM generated small world network.

examine whether the dynamics of multiple LLMs are similar to or different from human social dynamics. We find that networks created by LLM agents exhibit properties similar to the ones found in real-world human networks. Firstly, we find that these networks exhibit micro-scale properties, such as preferential attachment, triadic closure, and homophily. Moreover, these networks exhibit macro-scale properties such as small-world phenomena and community structure. We also investigate LLMs' decision-making based on real-world networks, revealing that triadic closure and homophily have a more substantial influence than preferential attachment.

These behaviors align closely with human behaviors, illuminating their potential to replicate complex network dynamics. This insight broadens our understanding of LLMs' capabilities, paving the way for applications in network science and social sciences and practical applications such as chatbot development, personal assistant technologies, and synthetic dataset generation, where emulating human-like network behaviors is paramount.

1.5 Thesis Conclusions

This Ph.D. thesis synthesizes my research on dynamic network systems, encompassing resource allocation, network resilience, privacy-preserving decision-making, core-periphery structures, and network formation in LLM agents. In resource allocation, I develop scalable algorithms for dynamic contagion problems, leveraging linear programming to approximate interventions in large networks and exploring potential extensions to dynamic influence maximization. Future work could involve refining approximation guarantees for dynamic contagion by extending classic influence maximization techniques to multi-period settings, potentially integrating reinforcement learning for adaptive interventions. The resilience chapter characterizes supply chain networks as resilient or fragile through graph percolation theory, proposing deterministic LP approaches for influence spread estimation. Promising research directions include decentralized models where entities act strategically and exploring connections between supply chain disruptions and financial contagion. The privacy-preserving decision-making chapter addresses decentralized estimation under privacy constraints, identifying avenues for black-box hypothesis testing and optimal consensus algorithms. Further work could investigate Bayesian analogs of these algorithms and scalable methods for distributed differential privacy in large networks. In core-periphery analysis, I introduce frameworks and efficient inference algorithms for identifying core structures in real-world networks, with potential extensions in influence maximization, node ranking, and hypergraph analysis. Lastly, the network formation chapter demonstrates that LLM agents exhibit classical network properties like homophily and triadic closure, opening avenues for developing heterogeneous

agent simulations that model diverse human decision-making processes. This line of work could extend to prototyping market dynamics, information spread, and strategic interactions in AI-driven networks. Across these projects, I underscore the importance of systemic risk analysis, privacy-accuracy trade-offs, and foundational model security, proposing future research on algorithmic interventions, multi-agent simulations, and resilience metrics to safeguard complex networked systems[1].

[1] A detailed discussion of the results and future directions can be found in Chapter 7.

Part I

Decision-making for Reinforcing Network Resilience

CHAPTER 2

CONTAGION AND RESOURCE ALLOCATION

The contents of this chapter constitute joint work with Jon Kleinberg and Sid Banerjee.

The world consists of interconnected entities that interact with one another through networks. Networks experience shocks due to adverse scenarios, such as (partial) failures of nodes and edges. When exogenous shocks hit networks, such shocks propagate through the edges of the network, causing cascades that may affect a significant population of nodes in the network. This phenomenon is often referred to as *network contagion*, and is of particular interest in the context of *financial networks* [139, 180]. In these networks, financial entities, such as individuals, businesses, and banks, have *liabilities* and *assets*, which result in negative/positive cash flows. Assets and liabilities can be either *internal*, i.e., between nodes in the financial network in question, or *external*, i.e., originating outside the network. While these cash flows are balanced under normal operating conditions, from time to time, shocks may lead to entities within the network being unable to pay off their financial obligations (i.e., *defaulting* on their liabilities). In such cases, these entities may only be able to *clear* a fraction of their debts, which then impacts other entities, thereby setting off a chain of defaults.

The above description captures the basic model of a *contagion* in an uncontrolled network. In many settings, however, the network regulator may be able to intervene to help mitigate the effects of this contagion. The regulator thus acts as an external controller responsible for (optimally) allocating intervention resources (or interventions), subject to certain budget constraints, to avert de-

faults. These interventions can sometimes take the form of continuous interventions or sometimes require discrete interventions [12, 122].

While the contagion process described above is specialized to the context of financial networks, with small modifications, a similar model can be applied to many other settings – to model unavailability and delays in ridesharing and/or computer networks, viral marketing, failures in power grids, and shortages in food bank networks, to name a few. Moreover, the network controller faces similar resource rationing problems in each of these contexts. For example, in ridesharing, nodes correspond to neighborhoods of a city, flows correspond to the movement of cars between neighborhoods, defaults correspond to increasing delays and vehicle unavailability in some neighborhoods, and the regulator's interventions correspond to dispatching additional vehicles to mitigate these defaults [37].

At a high level, the framework we study in this Chapter considers the problem of allocating resources to mitigate contagions in any generic supply/demand network, subject to defaults, and where the demand is proportionally split between neighbors of a node upon default.

In this Chapter, we develop a framework for budget-constrained interventions in dynamic networks spanning a time horizon T based on the well-studied Eisenberg-Noe (EN) model [139] where interventions affect its future states due to the accumulation of liabilities at the nodes. Specifically, our work makes several algorithmic contributions and offers useful managerial insights:

- We motivate the use of the EN model, as we initially show that finding *the optimal rationing scheme to minimize defaults is a computationally intractable*

problem (Theorem 2.3.1).

- When interventions are *fractional*, we show that solving the corresponding Markov Decision Process (MDP) requires solving a *only* polynomial number of LPs as a function of the time horizon T (Theorem 2.4.1). In contrast, naïvely solving the problem would require solving an *exponential* (in the time horizon T) number of LPs.

  We also show that under some conservation assumptions, a special case of our problem corresponds to solving one LP per sample path at the terminal time T (Corollary 2.4.2).

- Next, we turn our attention to *discrete* interventions, which correspond to intervention problems similar to intervention problems governments faced during the pandemic, such as the case of Greece, New Zealand, and the United States.

  In detail, when discrete interventions are considered, we show that the problem is intractable (Theorem 2.5.1) and that objectives that correspond to minimizing the number of defaults are inapproximable (Theorem 2.5.2). For the approximable objectives, we design LP-based approximation algorithms for objectives that correspond to linear functions of the clearing payments. Our algorithms obtain an instance-dependent guarantee, which depends on how much the network is endogenously exposed in the worst case (Theorem 2.5.3), which we call the *endogenous exposure index* (Section 2.3.5). Our LP-based approximation scheme is flexible and can be extended to accommodate more general contagion models, such as the model with bankruptcy costs studied in [356] (Theorem 2.5.5).

- Subsequently, if the static variant ($T = 1$) of the problem is considered, we show that optimizing linear functions of the flows correspond to maxi-

mizing a monotone submodular function, and, hence, we obtain an $1 - 1/e$ approximation guarantee which is *optimal* unless $P = NP$ (Theorem 2.5.4).

- Our LP-based framework is versatile and is also able to *accommodate fairness considerations*. In particular, we optimize the same objectives as above subject to a family of fairness constraints inspired by the Gini Coefficient [178] and network fairness measures [257, 256]. We show that the Price of Fairness (PoF) can be unbounded in the discrete case and bounded in the fractional case (Theorem 2.6.2).

2.1 Managerial Insights and Policy Implications

To demonstrate our framework's wide applicability, we experiment with a variety of networks, such as synthetic networks, banking networks, online financial transaction networks, and ridesharing networks. We compare the results of the proposed approximation algorithms with other network-based heuristics on these datasets. We empirically study the incorporation of the fairness constraint in multiple datasets. By combining theoretical and empirical results, we are able to obtain a variety of managerial insights and policy implications:

Fine-Grained Efficiently-Computable Intervention Decisions. Financial crises profoundly impacted the study of how failures propagate within financial networks. It prompted extensive research into understanding the dynamics of financial contagion and the interconnectedness of financial institutions. The literature primarily aimed to answer the question of which nodes, if they fail or experience significant losses, could potentially harm the financial network the most. This concern often examines what happens when a node fails, ef-

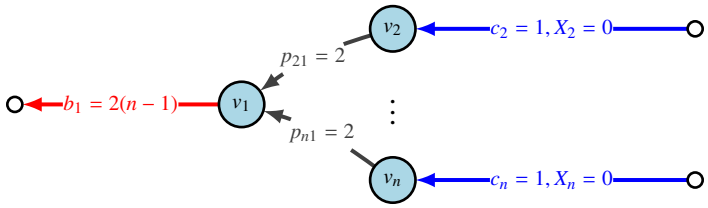


Figure 2.1: Example network to demonstrate the capability of the intervention framework. The network consists of n nodes partitioned into one "sink node" (v_1) and $n-1$ "source nodes" ($v_2, \ldots, v_n$). The regulator has a budget of $B = n$. We compare two intervention policies of the regulator: Policy A (failure-based) and Policy B (resuscitation-based; ours). The regulator chooses the most vulnerable node for Policy A and bails it out with the entire budget B. For Policy B, we allow the regulator to decide to bail out each node with an amount of at most 1, $j \in [n]$. In Policy A, the regulator decides to save the node whose failure is the most detrimental to the network, i.e., the regulator chooses one of $v_2, \ldots, v_n$. Thus, Policy A in equilibrium would yield a total payment flow of $2n-1$. On the other hand, Policy B distributes the budget to $v_2, \ldots, v_n$, yielding a total payment flow of $4(n-1) > 2n-1$ in equilibrium.

fectively reducing its assets to zero. Several key works in this domain, such as [141, 81, 179, 180, 122, 62, 8], focused on the interplay between network structure and the spread of financial contagion, such as the degree distribution, the edge density [48], and centrality [211]. These works emphasized that understanding the network's connectivity patterns is crucial in determining the potential for a financial epidemic to propagate easily and, therefore, highlighted that resuscitating highly interconnected entities would be the most impactful.

To this end, our work provides the following important real-world insights:

- Our work provides ***a new perspective and efficient algorithms*** *to combat this matter by devising intervention strategies* for the entire financial network (while most of the works of the last decade have focused on the impact of an entity failing), and essentially asks the question of *which subset of*

the network needs to be resuscitated to avert contagion subject to a budget. Designing an intervention algorithm is much more sophisticated than determining the individual network effects of a node failing since it depends on additional constraints such as the interventions themselves, the budget, and the underlying contagion mechanism, as illustrated in Figure 2.1, which shows that an intervention strategy focused on nodes whose failure causes the most harm may produce fundamentally different (and less effective) solutions than our proposed strategy, which focuses directly on sets of nodes with the most potential to resuscitate the network.

- Our work contributes to the growing literature on systemic risk measures (cf. [250, 96, 154, 54]) with novel insights (e.g., regarding dynamic and discrete controls). Compared with the existing work on systemic risk measures which focus on static network instances and identifying the minimum amount of intervention to bring the system to solvency, our framework allows for the dynamic distribution of the interventions where the regulator is not required to spend their budget all at once but instead the regulator can allocate it dynamically according to the exogeneities. Thus, our framework extends the existing literature and allows for extensions of the systemic risk measures beyond the existing ones.
- *Our experiments indicate that* ***the network structure*** *affects the regulator's policy* (Section 2.7). We show that:
  - In many real-world datasets, the nodes responsible for clearing more payments generally receive higher interventions (Section 2.7.1). How the interventions are distributed varies according to the network. For instance, for a *core-periphery* network their values are concentrated in two main "bands" (core and periphery). For datasets that correspond

to *scale-free* networks, the interventions are non-uniformly spread, with most interventions having a low value and corresponding to most of the less central nodes and few interventions having a high value. Moreover, for most experiments, there is a positive correlation between the financial connectivity of a node – which determines how exposed the node is within the network – and the intervention it received, highlighting that in most real-world data, interventions are mostly allocated due to *endogenous contagion*.

  - However, the regulator's strategy for allocating interventions *should not always be focused on the most central nodes in the network*. We show that in core-periphery networks the best approach depends heavily on how densely connected the core of the network is (Section 2.7.2). These networks experience a ***phase transition*** complementary to phase transitions found in other related works such as [8]. Focusing interventions on these central nodes helps maximize network resilience when core nodes have sparse connections. However, as the core becomes more densely interconnected, a point is reached where shifting support to the peripheral nodes becomes the most effective strategy. This nuanced approach to interventions underscores the need to evaluate the network's structural characteristics before implementing strategies. Specifically, regulators should monitor the connectivity ratio between the core and the periphery and adjust their focus accordingly to improve the overall stability of the network.

- Our algorithm is efficient and can run ***for several real-world datasets*** ($n \sim 10^2, T \sim 10^1$) ***within a few seconds/minutes*** (Section 2.7.5).

Furthermore, the recent global pandemic heightened the necessity of formulating intervention strategies to rescue individuals, businesses, and financial institutions from impending economic collapse. Countries worldwide, including the United States CARES Act, New Zealand, and Greece, implemented intervention programs to alleviate the economic crisis. These initiatives were designed based on various criteria, such as income [120], the number of dependents, and whether employment was disrupted due to the pandemic (e.g., inability to work remotely).

We want to emphasize that such policies are *inherently discrete* and can be seen as fundamentally rooted in fairness, ensuring that entities receive fixed interventions based on their circumstances, as opposed to a scenario where only a select few large banks or businesses are eligible for financial assistance, which is a scenario mostly suited for a model of continuous interventions (see, e.g., [12]). Our model captures this policy since each financial entity is entitled to a fixed intervention – which the entity either received or not – that depends on the entity's characteristics.

Specifically, when discrete interventions are considered, our work provides the following insights:

- *Our experiments demonstrate that when considering network effects,* ***thersholding-based heuristics fail*** *(Section 2.7.4). Such heuristics include thresholding based on income or other attributes – which have been used worldwide to design discrete intervention decisions (e.g., CARES Act, Greece, and New Zealand's case).* For instance, the rationale behind ordering nodes according to their wealth is straightforward: nodes with very low wealth may have fewer connections, making it challenging for the positive effects of an intervention to

propagate. Conversely, nodes with considerably high wealth may already be on the brink of solvency, minimizing the discrete intervention's impact on the network.

- *In addition,* ***several other network-based heuristics (degrees, centralities, PageRank), proxies for a node's influence produce inferior results*** *(Section 2.7.4).* The reason behind this is the non-linear nature of the model and the fact that most centrality measures can be considered as equilibria to contagion problems, where there are no inputs provided (cf. Figure 2.1). While the equilibria of the EN model without solvent nodes resemble the calculation of the Katz centrality (cf. [369]), the non-linear nature of the solvency constraint can cause inconsistencies, which makes using classical centrality measures an underperforming heuristic. Therefore, our method can be perceived as *a new measure of financial centrality*, which can be provably and efficiently computed at scale through linear programming as demonstrated through extensive experiments, contrary to other recent works examining financial centrality for interventions [211, 214].
- On the other hand, the LP-based randomized rounding algorithm we propose performs significantly better compared to the heuristics and better, in fact, than its worst-case guarantee. In the static case, we also show that the greedy algorithm (for which we provide a constant approximation) performs similarly to the LP-based algorithm (Section 2.7.4).

Fairness in Interventions and its Effects. Our model offers significant flexibility and can accommodate a variety of fairness considerations, as demonstrated by our experiments on several real-world datasets. Specifically:

- Our model offers the ability to *integrate both fine and coarse-grained fairness*

constraints, a capability not present in other related works (Section 2.6). Our experiments demonstrate that we can efficiently address the associated intervention problem while minimizing the impact on the Price of Fairness in practice. This is achieved by extending the Gini Coefficient and incorporating it as an additional constraint within our linear programming relaxation.

- Our computational experiments show that *fairness is in alignment with optimality* (Section 2.7.3). Specifically, we show that for instances for which spatial fairness constraints are considered (i.e., the interventions between neighboring nodes should not vary much on average), the impact of inducing fairness is minimal both in macroscopic terms – i.e., the Price of Fairness (PoF) – and microscopically regarding the interventions themselves. This behavior is coherent in all the network structures we empirically study.

Recognizing Fundamental Supply-Demand Patterns in Other Domains. Our proposed model has applications in a variety of domains of particular interest to the management science community in which there are *dynamic supply-demand imbalances*. Real-world applications include designing interventions for supply-chain networks (cf. [324]), ridesharing (cf. [159]), and can have further applications on influence maximization (cf. [291, 236]), allocation of compute resources, and many more. Fundamentally, any network that corresponds to a supply-demand network where there are demand requests between pairs of nodes, resources are allocated proportionally to demand on equilibrium, shocks can introduce scarcity of supply and initiate networked contagions, and the goal of a regulator is to allocate discrete resources – such as vehicles, capital, and other resources – are natural candidates for our model.

Our model can be used to study network seeding problems and design seeding algorithms to maximize influence – corresponding to maximizing flows – in large-scale real-world networks. The work of [324] motivates the use of our model to study a problem that is conceptually similar to the influence maximization problem (cf. [236]). Therefore, a very interesting application to our model is to design such algorithms via modeling the probabilities of a node's influence at equilibrium by the equilibrium payments, the seeds as external assets, and the cascade process as the proportional payment rule.

2.2 Related Work

Static Financial Networks. The EN model introduced in [139] models a financial network where each node has assets and liabilities concerning the internal network, namely the other nodes of the network and the external sector. According to the EN model, when a node *defaults*, namely is not able to pay out its creditors (internal and external), it rescales its obligations proportionally and pays the rescaled responsibilities in full. The EN model calculates these payments, usually called *clearing payments*, by computing a solution to a fixed-point problem or, equivalently, an optimal solution to a mathematical program with a strictly increasing objective. The general problem has multiple equilibria; however, this Chapter, for simplicity, examines the cases where the equilibrium payments are unique.

In the presence of shocks [179], the nodes similarly can become default due to external shocks that disrupt their assets. Moreover, the works of [238, 272, 153] perform sensitivity analyses on the EN model and [18, 407] study

network compression as a means of reducing the systemic risk. Moreover, [213, 12, 137], investigate *optimal interventions* in the cases of defaulting. More specifically, [213] investigates scenarios for multiple equilibria and provides necessary and sufficient conditions for solvency under any equilibrium. Besides this, their paper investigates optimal interventions that bring the system into solvency and provides computational intractability results for the minimum intervention problem by a reduction from the partition problem. The subsequent work of [137] considers the structure of optimal discrete interventions under the RV model (a model with bankruptcy costs) of [356] and proves hardness results for objectives that are similar to ours using different approaches where there are non-zero bankruptcy costs. Their paper does not consider stochastic shocks but rather a fixed state of the network and a fixed non-zero percentage regarding default costs. Additionally, their work does not include approximation algorithms, fairness-constrained optimization, and empirical work. They prove that for *non-zero* bankruptcy costs, maximizing the number of solvent nodes cannot be approximated within a factor of $n^{1/(\log\log n)^C}$ for some universal constant $C > 0$ that agrees with our improved inapproximability result for the EN model.

Several works have also focused on mechanisms for remediating contagion with mechanisms different than interventions, such as credit default swaps, claims trading, and purchasing illiquid assets. Specifically, several works have studied credit default swaps, that is, triads of entities enter contracts with one another, whereas the default of a third entity in the network forces a bilateral transaction between the other two. Computing a clearing vector in such models was shown to be PPAD-Complete by [362, 363]. [329] investigates the problem of *sequential defaulting* in networks with debt contracts and credit default swaps and shows hardness results regarding identifying the number of default

banks on the best-possible and worst-possible orders at which banks announce their defaults. Moreover, the work of [39] studies a different policy framework than ours based on purchasing illiquid assets rather than interventions. Such a framework has been utilized as a major policy approach during the 2008 financial crisis, called the Troubled Asset Relief Program (TARP). Finally, the work of [201] discusses algorithmic claim trading as a means of remediating contagion and provides hardness results.

The work of [12] considers optimal intervention methods under budget constraints under the extended model of [179] and formulate optimization problems that minimize the systemic losses as well as reducing the number of defaulting institutions and apply their methods on publicly available data on the Korean financial system. Their work considers *fractional intervention* policies, which differentiate it from ours. More specifically, we consider *discrete interventions* for the static and the dynamic regime in which case the model of [12] can be seen as the fractional relaxation of the optimization objectives we study. Secondly, we experiment with high-granularity financial institutions (banks) and view the problem from a societal lens, namely modeling the system's entities as "societal nodes" (businesses, households, individuals). Moreover, the work of [117] focuses on providing the optimal bailout policies for networks arising from the Stochastic Block Model using the Elliot-Golub-Jackson model.

From an experimental viewpoint, the work of [165] introduces a Bayesian framework based on Gibbs sampling to recover the liability network when only the aggregate assets and liabilities of nodes are known.

Finally, the work of [152] generalizes the classical EN model to a multi-layered one, where the interconnected entities of the financial network have

traded in multiple assets, develop a financial contagion model with fire sales that allow institutions to both buy and sell assets subject to some utility and study its equilibria. While the exact contributions of [152] are tangential to ours, generalizing our model in their framework provides an excellent pathway for extending the current work.

Dynamic Financial Networks. The work of [43] investigates multi-period liability clearing mechanisms by formulating convex optimal control problems on a different model from the EN we study in this Chapter. In their model, an initial liability matrix L_0 is (perhaps partially) cleared at a finite horizon T. The entities have some cash held each time t, and they try to clear as many liabilities as possible. The work of [43] waives the obligation of each node to repay its debts in a *pro-rata* fashion. We believe that in a resource allocation setting, equitably splitting the debts is fairer on first principles. Moreover, their work does not extend to discrete interventions and fairness constraints, as we consider in our work.

In a similar flavor, the work of [155] considers a continuous-time version of the EN model and studies the default risk. The paper investigates defaults that can result from insolvency or illiquidity and identifies the default times of nodes. The authors, however, do not study network interventions. In a similar spirit, [378] study a dynamic clearing and show that under the assumption that the liability matrix is constant through time, the clearing problem corresponds to solving a static problem at the terminal time. We want to emphasize that the work of [378] differs significantly from our work for two main reasons. The first differentiating point is that in our case, the liabilities arrive one at a time and thus, the relative liabilities change over time, which makes the problem signif-

icantly more complicated from a computational standpoint. The second differentiating point corresponds to the fact that the work of [378] does not consider interventions.

Another work closely tied to ours is the result of [86], where the authors study a multi-period clearing framework where the level of systemic risk is mitigated through assistance. The network is stochastic, and defaulted entities are sold through a first-price sealed-bid auction. The authors also empirically find that in core-periphery network architectures, targeting the systemically important entities is more effective, and in random topologies, targeting entities that maximize the total liquidity is more effective. While being close to our work, [86] differs from us in that while they mainly consider heuristic policies, we derive optimal policies for continuous interventions and approximately optimal policies for discrete interventions.

Additionally, the work of [253] considers multi-maturity contracts, which are different compared to single-maturity models such as [38, 86]. Our work mostly resembles the latter works since the liabilities are revealed one at a time.

Finally, we mention the contemporary work of [83], which is closely related to ours. The authors study a dynamic extension of the EN model and design optimal intervention policies, assuming that the relative liability matrix remains *constant* during the dynamic process. We note here that our framework is more general than [83] since we consider the more general case where the relative liability matrix (see Section 2.3) varies with time, which makes the resulting dynamics non-convex (see also Appendix A.4).

When the temporal dimension is introduced, the model's dynamics change

significantly since accumulated liabilities from round $t-1$ affect the future states of the model; in a sense, the behavior is closer to the dynamics in queuing network models (see [235, 37]). On the other hand, this also suggests that insights from the financial contagion model can be used to study interventions in more general network allocation problems, such as in ridesharing [37].

Systemic Risk Measures. The theory of *systemic risk* has a long history of financial mathematics. One of the papers that is most closely connected to our work is the work of [179], where financial contagion in the presence of shocks is investigated, and results are provided regarding the probability of contagion of a subset of nodes due to a shock on a specific node.

Moreover, our work has connections to *convex and coherent risk measures* (cf. [99, 250, 54, 154]). The work of [99], and the follow-up works of [250, 154], study axiomatic frameworks for systemic risk over interconnected entities which has the property to be decomposable over each agent. The aggregation functions defined in their work are related to the social welfare functions we study in this Chapter. Moreover, the interventions could be associated with measures of susceptibility of each entity to systemic risk (see also Section 2.1), in accordance with the "shadow prices" – which capture the systemic risk externality of the decision-making of individual firms – studied in these works. In a similar spirit, [54] defines the systemic risk measure as the minimum (random) cash injection to that is required for each entity to bring the system to solvency. Although directly related to the works of [99, 250, 154, 54], our models and algorithms, such as the discrete interventions and the associated guarantees as well as the dynamic contagion model, are complementary to the aforementioned works.

Contagion Mitigation. In their recent work, [239] explore optimal interventions within the Elliot-Golub-Jackson contagion model and present a $(1 - 1/e)$-approximation algorithm for an intervention problem. this Chapter, under certain conditions, also proves that our objective is submodular and establishes a similar $(1 - 1/e)$-approximation algorithm. However, our focus diverges as we use the EN model instead. Additionally, we address interventions in dynamic networks and fairness in interventions. We also demonstrate a stronger inapproximability result when maximizing the number of solvent nodes, compared to [239].

All these works, including ours, relate to epidemics and epidemic contagion mitigation, as seen in studies by [99, 72, 131, 132, 203]. However, the mathematical questions differ significantly. Epidemiological control problems often pose #P-hardness challenges, whereas our behavioral assumptions in the EN model allow for polynomial-time solutions for fractional interventions.

2.3 Model

We use $[n]$ to denote the set $\{1, \ldots, n\}$. For vectors (resp. matrices), we use $\|x\|_p$ for the p-norm of x (resp. for the induced p-norm); for the Euclidean norm (i.e., $p = 2$), we omit the subscript. 0 (resp. $\mathbb{1}$) denotes the all zeros (resp. all ones) column vector, and $\mathbb{1}_S$ represents the indicator column vector of the set S. We use $x \wedge y$ (resp. $x \vee y$) as shorthand for the coordinate-wise minimum (resp. maximum) of vectors x and y. For a given vector x, we use the array notation $x(i : j)$ to denote a sub-vector of x from x_i to x_j (inclusive range). We use $x \odot y$ to denote the Hadamard product between vectors x and y, and $\geq, \leq, >, <$ to denote

coordinate-wise ordering. In a network context, we use the notation $j \sim i$ to denote a directed edge from a node j to a node i.

Throughout the paper, we use the tildes (e.g., $\widetilde{p}(t), \widetilde{z}(t)$, etc.) to denote the decision variables for fractional controls and bars (e.g., $\bar{p}(t), \bar{z}(t)$, etc.) to denote the decision variable for discrete controls.

2.3.1 Liability Network and Control Problem

The system consists of a dynamic network $\{G(t)\}_{t\in[T]}$ spanning a finite time horizon T with n entities (denoted by $[n]$), where each *directed* edge (j, i) denotes that entity j owes a total internal liability $p_{ji}(t) > 0$ to entity i at round t. Agents have external liabilities $b_j(t) \geq 0$, generated at the start of each round t. Each agent owes in total $p_j(t) = b_j(t) + \sum_{j\sim i} p_{ji}(t)$.

Each agent possesses assets $c_j(t) \geq 0$ to clear their liabilities. Moreover, each agent experiences shocks $x_j(t) \in [0, c_j(t)]$, and is able to clear a total of $\widetilde{p}_j(t) \in [0, p_j(t)]$.

The regulator has a budget $B(t) \geq 0$ at each time and aims to infuse it to the agents through interventions. Each agent j receives an intervention $\widetilde{z}_j(t) \in [0, L_j(t)]$ which increases their total assets from $c_j(t)$ to $c_j(t) + \widetilde{z}_j(t)$. The sum of all interventions is at most $B(t)$, i.e. $\sum_{j\in[n]} \widetilde{z}_j(t) \leq B(t)$. The set of feasible intervention policies is denoted by $\mathcal{Z}$.

Definition 2.3.1. We say that node j undergoes *default* at time t if $\widetilde{p}_j(t) < p_j(t)$; else, when $\widetilde{p}_j(t) = p_j(t)$, we say that j is *solvent*. For brevity, in the static regime (i.e., $T = 1$), we ignore the time index.

2.3.2 Liability and Asset Accumulation

At the start of each (discrete) round t, new *internal* liabilities $\ell_{ji}(t) \geq 0$ get generated in the system. The total liability $p_{ji}(t)$ is calculated as the sum of the instantaneous internal liabilities $\ell_{ji}(t) \geq 0$ and the accumulated liabilities. At equilibrium in round $t-1$, each agent is able to clear a total amount of $\widetilde{p}_j(t-1) \in [0, p_j(t-1)]$.

So at each round a fraction $\left(1 - \frac{\widetilde{p}_j(t-1)}{p_j(t-1)}\right)$ of each of agent j's liabilities are cleared. Thus, the total liability between $j, i \in [n]$ *at the start of round* t (i.e., before clearing) is given by

$$p_{ji}(t) = \ell_{ji}(t) + p_{ji}(t-1) \cdot \left(1 - \frac{\widetilde{p}_i(t-1)}{p_i(t-1)}\right),$$

If we define $\ell_j(t) = \sum_{j \in [n]} \ell_{ji}(t)$; then the total liabilities owed by j at the start of round t become

$$p_j(t) = b_j(t) + \ell_j(t) + (p_j(t-1) - \widetilde{p}_j(t-1)).$$

Similarly, at the start of each round t, new external endowments $\xi_j(t) \geq 0$ arrive, and an agent's assets constitute of the new endowments and the surplus assets from round $t-1$, i.e.

$$c_j(t) = \xi_j(t) + c_j(t-1) - x_j(t-1) + \widetilde{z}_j(t-1) + \sum_{i:i\sim j} a_{ij}(t-1)\widetilde{p}_i(t-1) - p_j(t) \geq 0. \quad (2.1)$$

whereas $a_{ij}(t-1) \in [0,1]$ correspond to the ratio of the total liabilities of i that i has decided to give to j. In Section 2.3.3, we elaborate on the values of the fractions $a_{ij}(t)$.

Finally, we assume that the surplus budget carries forward to the next round and that a new non-negative budget $W(t) \geq 0$ is added at each time, namely

$$B(t) = W(t) + B(t-1) - \sum_{j \in [n]} \widetilde{z}_j(t).$$

At time $t = 0$ (before the contagion starts), the values of all variables are assumed to be zero.

2.3.3 Rationing

One of the important problems faced by the regulator and the agents is the nature of the model assumed regarding the rationing of the clearing payments, cf. [139, 356, 43, 15, 8]. In simple words, choosing how to split a node's obligations is a non-trivial task which poses some intractability challenges (see, e.g., [330, 53] and the references therein). Below, we give computational arguments regarding these challenges and propose the model of [139] as a computationally tractable solution.

As we briefly elaborated in Equation (2.1), the quantity $a_{ji}(t)\widetilde{p}_j(t)$ corresponds to the total payment from node j to node i at equilibrium, and $a_{ji}(t) \in [0, 1]$ corresponds to the fraction that j gives to i compared to its other obligations, and $\sum_{j \sim i} a_{ji}(t) \leq 1$ (as the node can also be obliged to the externally). We call the row (sub)-stochastic matrix $A(t)$ with entries $a_{ji}(t)$ the *rationing scheme*.

The first question regarding the rationing scheme is whether there is an *optimal* rationing scheme, in the sense that it minimizes the total number of defaults defaults. Our answer to this problem is negative form a computational

standpoint by showing that finding the optimal rationing scheme is NP-Hard. Specifically, we define the OPTIMAL-RATIONING decision problem as:

Definition 2.3.2 (OPTIMAL-RATIONING)**.** Given an integer D, aggregate liabilities $p(t)$, aggregate assets $c(t)$, a subset S of the nodes, and a rationing scheme $A_{S^c}(t)$ of the nodes that belong to $S^c = [n] \setminus S$, does there exist a rationing scheme $A_S(t)$ for the nodes of S such that the total number of defaults is at most D?

We prove that OPTIMAL-RATIONING is NP-Hard by a reduction from the 3-SET-COVER problem [230]:

Theorem 2.3.1. OPTIMAL-RATIONING *is NP-Hard.*

Given that finding the optimal rationing is an NP-Hard problem, an alternative way to ration the payments is to use the computationally tractable (and suboptimal) rationing scheme proposed in [139]. In the sequel, we state this modeling assumption:

Assumption 1 (Proportional Rationing [139])**.** *The relative liabilities are set as follows:*

$$a_{ji}(t) = \begin{cases} \frac{p_{ji}(t)}{p_j(t)}, & \text{if } p_j(t) > 0 \\ 0, & \text{otherwise} \end{cases}.$$

Conceptually, the EN model has an engraved notion of "fairness" since each node j must return to i the actual fraction of its total liabilities.

2.3.4 Financial Environment

We let $(\Omega, \mathcal{F}, \mathbb{P})$ denote the probability space, let $(\mathfrak{I}, \leq)$ be a totally ordered index set; let $(\mathfrak{S}, \Sigma)$ be a measurable space, and $\mathfrak{X} : \mathfrak{I} \times \Omega \to \mathfrak{S}$ be a stochastic process. For an event $E \subseteq \Omega$, we write $\mathbb{P}[E|\mathfrak{X}(1 : t)]$ to denote the probability of E conditioned on the natural filtration of $\mathfrak{X}$ up to t.

Till now, we have been agnostic in our model description as to the exact nature of the exogenous shocks to the system, i.e., the per-round internal and external liabilities and external asset payouts. We assume that the environment is *stochastic*, i.e., the instantaneous assets and (internal and external) liabilities induce uncertainty in the system in the forms of a *disturbance*. We denote the *financial environment* at round t as $U(t) = (b(t), \xi(t), x(t), \{\ell_{ji}(t)\}_{j,i\in[n]}, W(t))$ and assume that it is a Markov Chain evolving in a state space $\mathcal{U} \subseteq \mathbb{R}_{\geq 0}^{3n+\binom{n}{2}+1}$. We will use the letter Δ to denote the maximum ℓ_1 norm of a component of u, for instance, $\Delta_u = \sup_{u\in\mathcal{U}} \|u\|_1$, and $\Delta_b = \sup_{u=(b,\xi,x,\ell,W)\in\mathcal{U}} \|b\|_1$, etc.

Assumption 2 (Markovian Exogenous Shocks)**.** *The financial environment $U(t)$ is a Markov Chain, i.e.* $\mathbb{P}[U(t) = u(t)|U(t-1) = u(t-1), \ldots, U(1) = u(1)] = \mathbb{P}[U(t) = u(t)|U(t-1) = u(t-1)]$.

Moreover, we assume that the interventions $\widetilde{z}(t)$ are Markovian.

Assumption 2 is a reasonable assumption for a financial system since we are studying a model of accumulated debt and equity, and furthermore, it offers mathematical tractability. A realistic scenario where Assumption 2 fails in the case of contracts with maturity dates, namely at time t, we are considering random bilateral contracts of the form $\ell_{ji}(t, \tau)$ signed at time $0 \leq \tau \leq t$ which matures at time t. In this case, the total liability between nodes j and i

is given as $p_{ji}(t) = \sum_{\tau \leq t} \ell_{ji}(t, \tau) + p_{ji}(t-1)\left(1 - \frac{\widetilde{p}_i(t-1)}{p_i(t-1)}\right)$ which makes the state $s(t)$ non-Markovian. Another interesting case where the Markovian assumption is violated is credit default swaps (CDS; cf. [329, 330]), where the seller entity of the CDS insures the buyer entity against some third-party defaulting. The above extensions of our framework constitute interesting avenues for future work.

2.3.5 The Endogenous Exposure Index

We define $\beta_j(t) = \sum_{j \in [n]} a_{ji}(t)$ denote the *financial connectivity* of j at time t (cf. [179]) and $\beta(t)$ to be the vector of the financial connectivity. Throughout the rest of the paper, the following *instance-dependent quantity*, which we define as the *endogenous exposure index* would be useful:

$$\beta_{\max}(\mathcal{I}) = \sup_{u(1:T) \in \mathcal{U}^T} \max_{t \in [T]} \|\beta(t)\|_\infty.$$

Similarly to related works (cf. [38, 253]) in order to establish the uniqueness of the solution, we make the following assumption about $\beta_{\max}$, which is equivalent to requiring $b_j(t) > 0$ for all $t \in [T]$:

Assumption 3 (Non-vanishing External Liabilities)**.** $\beta_{\max} < 1$.

From a societal context, this assumption is reasonable since it can be interpreted as a "tax" (see, for example, similar points made in [40]). When fractional (resp. discrete) interventions are assumed we will use the notation $\widetilde{\beta}_{\max}(\mathcal{I})$ (resp. $\bar{\beta}_{\max}(\mathcal{I})$) to denote the Endogenous Exposure Index.

2.3.6 Control Problem and Markov Decision Process

Now, as in the EN model, the clearing vectors $\widetilde{p}(t) \geq 0$ must satisfy the following constraints for $t \in [T]$,

$$\widetilde{p}(t) \leq p(t) = b(t) + \ell(t) + p(t-1) - \widetilde{p}(t-1) \tag{2.2a}$$

$$\widetilde{p}(t) \leq A^T(t)\widetilde{p}(t) + c(t) - x(t) + \widetilde{z}(t) \tag{2.2b}$$

$$\widetilde{z}(t) \in \mathcal{Z}$$

We refer to the first constraint (Equation (2.2a)) as the *solvency constraint*, since if for some node j it holds with equality, it means that this node can repay its debts in full. We refer to the second constraint (Equation (2.2b)) as the *default constraint*, since when it holds with equality for some node $j \in [n]$, this means that j partially repays its debts proportionally to its creditors. Finally, clearing vectors are always non-negative. Note by definition the bounds in Equations (2.2a) and (2.2b) are non-negative; we can thus compress these constraints as $\widetilde{p}(t) \in [0, p(t) \wedge (A^T(t)\widetilde{p}(t) + c(t) - x(t) + \widetilde{z}(t))]$. Note that in the above equations, $A(t)$ is implicitly a function of $p(t)$, which makes the constraints non-linear.

Next, given the current state $p(t)$, exogenous input $c(t)$, shock $x(t)$, and action $\widetilde{z}(t)$, a natural "maximal" choice of the clearing vector $\widetilde{p}(t)$ is for it to be the *fixed point* of the system

$$s(t) = \begin{pmatrix} p(t) \\ \widetilde{p}(t) \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} p(t) \\ p(t) \wedge \left(A^T(t)\widetilde{p}(t) + c(t) - x(t) + \widetilde{z}(t)\right) \end{pmatrix}}_{=\Phi(s(t),\widetilde{z}(t);s(t-1),U(t))}. \tag{2.3}$$

When the round is evident from the context, we use the abbreviation $\Phi_t(s, z)$ to denote the mapping with information up to time t acting on the state action pair

(s, z), i.e., for all z we have that $s(z) = \Phi_t(s(z), z)$. Note that, under Assumption 3, the *second component* (i.e., $\widetilde{p}(t)$) of Φ_t is a contraction. We also make the following assumption based on the agents' responses:

Assumption 4 (Maximal instantaneous clearing)**.** *In each round t, each agent maximally clears her current liabilities, i.e., with clearing vector $\widetilde{p}(t)$ as the (unique) fixed point of*

$$\widetilde{p}(t) = p(t) \wedge \left(A^T(t)\widetilde{p}(t) + c(t) - X(t) + \widetilde{z}(t)\right).$$

The above condition, taken from the EN model, is standard in the finance literature – it imposes a natural requirement that agents try and explicit liabilities as soon as possible, subject to the proportional clearing rule. If one wants to maximize flows (or minimize defaults), one may be tempted to think this is without loss of generality. However, this is not the case in dynamic external interventions; one can create examples where dropping this assumption leads to higher overall rewards. These settings, however, are somewhat extreme, and it may be possible to eliminate them via other assumptions.

We want to emphasize that this is a subtle issue and is not without loss of generality since we are specifying a particular form of clearing payments via maximal clearing. In our context, this provides a natural and interesting way that a behavioral assumption in the finance literature – simply that agents clear liabilities as they arise to the extent possible (see the works cited in Section 2.2) – leads to tractable instances of dynamic optimization over multiple stages, as we show in Theorem 2.4.1.

It is easy to observe that under Assumption 2 and Assumption 4, the sequence $s(t) = (p(t), \widetilde{p}(t))$ is a *Markov Chain* (MC). More specifically, at time t, the only information needed to determine $p_{ij}(t)$ is the instantaneous liabilities

(which is an MC), the action $\widetilde{z}(t-1)$ and the remaining liabilities from times $t-1$, therefore extra information from round 0 up to $t-2$ is redundant. Since the external liabilities are also an MC and the sum of $p_{ji}(t)$ only depends on the state of the system at $t-1$, then $s(t)$ is an MC based wrt to $s(t-1)$ and $\widetilde{z}(t-1)$. Also Equation (2.2) depends only on the state of the system at time $t-1$ and the calculated maximum liabilities at the start of round t; therefore, the optimal clearing vector that occurs on the element-wise minimum of the RHS of the inequalities of Equation (2.2) is dependent on the previous state $s(t-1)$ and the action $\widetilde{z}(t-1)$. Similarly, the control $\widetilde{z}(t)$ depends on instantaneous liabilities $\ell(t)$ and $b(t)$, the external endowments $\xi(t)$ and shocks $x(t)$, which are Markovian by Assumption 2 and Assumption 4. Furthermore, $\widetilde{z}(t)$ depends on $p(t)$ and $A(t)$, which depend on the liabilities at time t and the uncleared liabilities from time $t-1$. These define a transition kernel $\mathcal{T}$, $\mathcal{T}((s,z)\to s') = \mathcal{T}(s'|s,z) = \mathbb{P}[s(t)=s'|s(t-1)=s,\widetilde{z}(t-1)=z]$. We also denote the projection on (s,z) of the kernel (which is a distribution itself) as $\mathcal{T}(\cdot|s,z) = \mathcal{T}_{s,z}(\cdot)$. The MC is associated with an initial distribution over the state space $s(0)\sim\pi_0$. The state space of the MC is denoted by $\mathcal{S}$.

Given the above setting of networked interactions over time with stochastic shocks, we can now formulate the problem of optimal dynamic interventions for maximizing various objectives as a Markov Decision Process (MDP). In this section, we formalize this and show that when interventions are continuous, the MDP can be solved optimally for a wide range of objectives.

Rewards & Objective. We consider two classes of reward function. The former type of reward is a *linear reward function* parametrized by a vector $v>0$,

$$R_v(t) = v^T \widetilde{p}(t) = \sum_{j \in [n]} v_j \widetilde{p}_j(t). \tag{Lin-OBJ}$$

When not clear from context, we assume that $v = \mathbb{1}$, and we denote the function simply by $R(t)$. We note that due to the properties of the EN model [139] all objectives of the above form would yield the same policy, which we call the optimal policy. Thus, our framework allows for the maximization of a large family of reward functions.

This reward measures the *total flows* of payments in the network. Another reward function we are interested in is counting solvent nodes, which we call the *absolute solvency* reward, i.e.

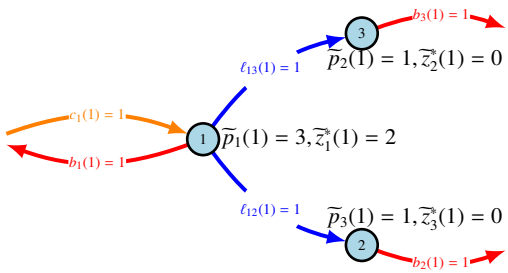
$$R_{\mathrm{AS}}(t) = \sum_{j \in [n]} \mathbb{1}\left\{\widetilde{p}_j(t) = p_j(t)\right\}. \tag{AS}$$

The stochastic reward incurred by a state-action pair at time t is $R(t)$. Note that here we can use *any function of* $\widetilde{p}(t)$ *that is coordinate-wise strictly increasing* due to [139, Lemma 4] and get the *same solution*.

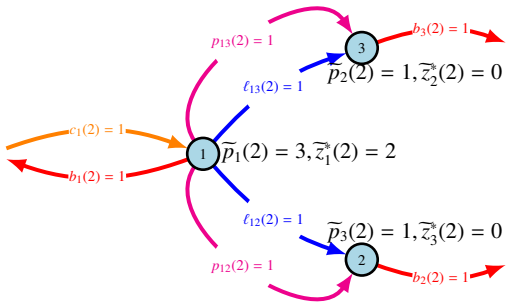
The overall objective that is to be maximized is the sum of rewards over a finite horizon $[T]$,

$$\begin{aligned} \max_{\widetilde{z}(1:T) \in \mathcal{Z}} \quad & \mathbb{E}_{s(0) \sim \pi_0}\left[\sum_{t=0}^{T-1} R(s(t), \widetilde{z}(t) = \Pi(t, s(t)), U(t))\right] \\ \text{s.t.} \quad & \textit{Equation (2.2)} \quad \forall t \in [T] \end{aligned} \tag{2.4}$$

We also assume no accumulated debts and interventions from time $t \leq 0$. We let $r(s, z) = \mathbb{E}_{U(t)}\left[R(s(t) = s, \widetilde{z}(t) = z, U(t))\right]$.



(a) $t = 1$: $p(1) = (3, 1, 1)^T, r(1) = 5$



(b) $t = 2$: $p(2) = (3, 1, 1)^T, r(2) = 5$

Figure 2.2: A contagion network over $T = 2$, with instantaneous internal liabilities ℓ, external liabilities b, and external assets c that are identical over the two rounds. The total budget infusion is $W(t) = 2$ at each round. The optimal intervention for $t = 1$ is $\widetilde{z}^*(1) = (2, 0, 0)^T$, in which all nodes can cover their debts, and no liabilities are carried over from $t = 1$ to $t = 2$. Similarly, in $t = 2$ the optimal intervention vector is $\widetilde{z}^*(2) = (2, 0, 0)^T$ and all liabilities are cleared. The value function equals $r(1) + r(2) = 10$.

Value Function. We define the value function $V^{\widetilde{z}}(t, s)$ as the optimal reward we can collect from time t onward, starting from state s and applying policy $\widetilde{z}(1 : T)$. The value function obeys the HJB equations for actions chosen from the action set, i.e., $V(t, s) = \max_{z \in \mathcal{Z}(t)} \left\{ r(s, z) + \mathbb{E}_{s' \sim \mathcal{T}_{s,z}} [V(t + 1, s')] \right\}$. In Figure 2.2, we present an example of an intervention scenario under our model for a toy dynamic network with $T = 2$ periods.

2.4 Efficient Computation of the Optimal Policy

The above MDP has a very high-dimensional state and action space ($\mathbb{R}^{2nT}$ and $\mathbb{R}^{nT}$ respectively), so a priori it is unclear if it can be solved efficiently. Surprisingly, we show below that we can exploit the structure of the problem – in particular, the fact that the random shocks are exogenous (Assumption 2), and the maximal clearing assumption (Assumption 4) – to give a *closed-form expression* for the value function as an expectation over the exogenous shock vector $U(1:T)$; moreover, this also allows us to compute it efficiently (and thus find near-optimal policies) via Monte Carlo estimation.

We now proceed to show how to calculate the value function $V(t,s)$ and the optimal policy $\widetilde{z}^*(t)$. First, it is easy to check that *given* a realization of the random shocks $u(t:T)$, the optimal reward (and policy) can be written as a sequence of *nested linear programs*. More surprisingly, we prove that, due to the structure of our model, we can exchange the maximum and expectation operators in the value function. Consequently, when the shocks are generated randomly, we get that the value function (Theorem 2.4.1) can be approximated by sampling N sample paths and then, for each sample path $u(t:T)$ solving a sequence of $T-t+1$ linear programs.

Our algorithm (Algorithm 1) is comprised of two routines: first, **Pathwise-V** takes as an input a sample-path $u(t:T)$ of exogenous shocks, a starting state s, and budget constraints $L(1:T)$ and $W(1:T)$ and solves a deterministic dynamic program for each sample paths.

The second routine (**Aggregate**) inputs a natural number N, the budget constraints $L(1:T)$ and $W(1:T)$, a financial environment $\mathcal{U}$, and the starting state

Algorithm 1 Approximate $V(t, s)$

Pathwise-V$(L(t:T), W(t:T), u(t:T), s)$

1. Given the initial state at round $t-1$ calculate $A(t)$ and $p(t)$
2. For each $t' \in [t, T]$
   (a) Let $u(t') = \left(b(t'), c(t'), \mathsf{vec}(\{\ell_{ji}(t')\}_{j,i\in[n]})\right)$ be the financial environment.
   (b) Let $\widetilde{p}^*(t'), z^*(t')$ be the optimal solution to $\max_{\widetilde{p}(t'),z(t')} \mathbb{1}^T\widetilde{p}(t')$ subject to the dynamics of Equation (2.2) and the random shocks $b(t'), c(t'), \{\ell_{ij}(t')\}_{i,j\in[n]}$.
   (c) If $t' < T$, use $\widetilde{p}^*(t')$ to calculate $A(t'+1)$, $p(t'+1)$, $c(t'+1)$ and $B(t'+1)$.
3. Return $V_{u(t:T)} = \sum_{t'\in[t,T]} \mathbb{1}^T\widetilde{p}^*(t')$.

Aggregate$(N, L(t:T), W(t:T), \mathcal{U}, s)$

1. Sample N i.i.d. sample paths $\{u_i(t:T)\}_{i\in[N]} \sim \mathcal{U}$ where a sample path consists of a realization of the environment on $T-t+1$ periods.
2. For every $i \in [N]$ compute
$$V_{u_i(t:T)} = \textbf{Pathwise-V}(L(1:T), W(t:T), u_i(t:T), s)$$
3. Return $\bar{V}(t, s) = \frac{1}{N}\sum_{i=1}^{N} V_{u_i(t:T)}$.

---

s. The algorithm then samples N exogenous shock realizations from $\mathcal{U}$. Conditioned on any of the sample paths $u_i(t:T)$ with $i \in [N]$, it calls the first routine to compute the sample value function $\bar{V}_{u_i(t:T)}$. Finally, it aggregates all solutions and outputs an estimate $\bar{V}(t, s)$.

Theorem 2.4.1. *Under Assumption 3, Assumption 4, and Assumption 2, the following are true*

1. *The value function $V(t, s)$ satisfies*
$$V(t,s) = \mathbb{E}_{U(t:T)}\left[\max_{\widetilde{z}_t,\widetilde{p}_t}\{\mathbb{1}^T\widetilde{p}_t + \max_{\widetilde{z}_{t+1},\widetilde{p}_{t+1}}\{\mathbb{1}^T\widetilde{p}_{t+1} + \max_{\widetilde{z}_{t+2},\widetilde{p}_{t+2}}\{\mathbb{1}^T\widetilde{p}_{t+2} + \dots\}\}\}\right]$$
and corresponds to solving a sequence of linear programs.

2. *For* $N = \frac{\log(2/\delta)(T-t+1)^2\Delta_u^2}{2\varepsilon^2}$ *samples, Algorithm 1 returns an* ε*-approximate solution* $\bar{V}(t,s)$ *such that* $|\bar{V}(t,s) - V(t,s)| \leq \varepsilon$ *with probability at least* $1-\delta$.

In general, it is known that solving a general MDP has exponential complexity (see, e.g., [374]) and it would naïvely require to solve $O\left(\left(\frac{\log(1/\delta)\Delta_u^2}{\varepsilon^2}\right)^T\right)$ LPs on $2n$ variables each to approximate $V(1,s)$. Theorem 2.4.1 reduces the complexity with respect to T to polynomial; namely to approximate $V(1,s)$ we now *only* require solving $O\left(\frac{\log(1/\delta)\Delta_u^2 T^3}{\varepsilon^2}\right)$ LPs on $2n$ variables each which is *polynomial* in the time horizon T. Also, in practical scenarios, the matrices $\{A(t)\}_{t\in[T]}$ are typically sparse, so the sequence of nested LPs can be solved efficiently.

Finally, as a special case of Theorem 2.5.3, we can show that if certain conservation conditions regarding the state space $\mathcal{U}$ of the financial environment hold, then $A(t)$ is a constant matrix, Equation (2.2) become linear, and, therefore, resolving the dynamic clearing problem requires solving $O\left(\frac{\log(1/\delta)\Delta_u^2 T^2}{\varepsilon^2}\right)$ LPs at the terminal time with $2nT$ variables each.

Corollary 2.4.2. *The dynamics of Equation* (2.2) *are convex (and, specifically, linear) if and only if* $\frac{\ell_{ji}(t)}{b_j(t)+\sum_{k\in[n]}\ell_{jk}(t)}$ *are constant for every* $j,i \in [n]$ *and* $t \in [T]$. *If this condition holds, then approximating the value function within accuracy* $\varepsilon > 0$ *with probability* $1-\delta$ *requires taking* $N = \frac{\log(2/\delta)\Delta_u^2 T^2}{2\varepsilon^2}$ *sample-paths, and solving a single terminal LP on each path.*

This recovers the results of [378, 83].

2.5 Network Control with Discrete Interventions

We next focus on the problem of allocating discrete interventions. For the discrete interventions problem, each node can be allocated discrete resources up to some value $L_j \in \mathbb{N}$. We allow controls to belong to either $\mathcal{Z}_d^{\text{BIN}} = \left\{\bar{z}(1:T) \in \prod_{t=1}^{T}[L(t)] : \bar{z}(1:T) \geq 0, \mathbb{1}^T\bar{z}(t) \leq B(t)\ \forall t \in [T]\right\}$ or $\mathcal{Z}_d^{\text{AON}} = \left\{\bar{z}(1:T) \in \prod_{t=1}^{T}\{0, L(t)\} : \bar{z}(1:T) \geq 0, \mathbb{1}^T\bar{z}(t) \leq B(t)\ \forall t \in [T]\right\}$. We seek to find the optimal policy that maximizes the value function at round $t = 0$, subject to the dynamics

$$s(t) = \begin{pmatrix} p(t) \\ \bar{p}(t) \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} p(t) \\ p(t) \wedge \left(A^T(t)\bar{p}(t) + c(t) - x(t) + \bar{z}(t)\right) \end{pmatrix}}_{=\Psi(s(t),\bar{z}(t);s(t-1),U(t))}. \tag{2.5}$$

Again, when the round is clear from context, we use the abbreviation $\Psi_t(s, z)$ to denote the mapping with information up to time t acting on the state action pair (s, z), i.e., for all z we have that $s(z) = \Psi_t(s(z), z)$.

2.5.1 Intractability Results and Failure of Threshold-based Policies

In the sequel, we define the decision version of the optimal intervention problem:

Definition 2.5.1 (OPTIMAL-DISCRETE-INTERVENTIONS)**.** Given a financial environment $u(1:T) \sim \mathcal{U}$ and a non-negative number V^*, does there exist a discrete

intervention rule $\widetilde{z}(1:T) \in \mathcal{Z}_d^{\text{BIN}}$ (or $\mathcal{Z}_d^{\text{AON}}$) such that the value function under reward Equation (Lin-OBJ) (or Equation (AS)) is at least V^*?

To give intuition on the reduction and its construction, we proceed by giving a polynomial-time reduction from a variant of the Set-Cover problem to the decision version for the maximization of the Equation (Lin-OBJ) objective, and similarly for the Equation (AS) objective. Our reduction resembles the reduction presented in [236] for the Influence Maximization problem.

Theorem 2.5.1. OPTIMAL-DISCRETE-INTERVENTIONS *is NP-Hard.*

At first glance, it would seem that Equation (Lin-OBJ) and Equation (AS) would need similar algorithms to be solved approximately. However, surprisingly, while there is an approximation algorithm for Equation (Lin-OBJ), the answer regarding Equation (AS) is negative, and, specifically, it is NP-hard to approximate a solution for Equation (AS) within any polynomial factor in the instance size.

We first state the inapproximability result for Equation (AS):

Theorem 2.5.2. *It is NP-Hard to approximate the Equation* (AS) *within a factor of* $\frac{k+a(|\mathcal{I}|)n}{k+n} = \Omega(a(|\mathcal{I}|))$ *for any function* $a(|\mathcal{I}|) = \text{poly}(|\mathcal{I}|)$ *of the input instance size* $|\mathcal{I}|$*, unless* $P = NP$*.*

We then turn our attention to Equation (Lin-OBJ). Initially, a natural policy for interventions would be a *threshold policy*, regarding one's existing equity, that is if the initial equity w_j of a node is below a threshold θ, then this node is bailed out with a stimulus check of value L_j. Thus, the designer should order nodes by their equities in ascending (or descending) order and intervene as many nodes

as possible, in this order, subject to the budget, breaking ties consistently. Such a policy can perform arbitrarily badly. To observe this, consider the static regime ($T = 1$), a network G on n nodes, which is built as follows: It consists of an initial node with $c_1 = \xi_1 = b_1 = 1$ and a directed path $2 \to n$ where $b_j = \varepsilon/2$ for $2 \leq j \leq n-1$, $b_n = 1 - (n-1)\varepsilon + \varepsilon/2$ and $c_2 = 1$. We let $x = c, L = \mathbb{1}$ and $B = 1$. The optimal policy bails out v_2 and achieves a total flow of $O(n)$, whereas the naive policy bails out node v_1 and achieves an objective of 1. The gap grows unbounded as $n \to \infty$. The same (bad) example can be altered to fool the policy, which bails out nodes in descending order of their equity.

From a policymaker's perspective, this policy is reasonable since the entities are sorted according to their wealth, and someone would argue that the interventions are "fair". However, as we show, this is not the case and such policies may not serve the policymaker's eventual goal of maximizing welfare. In Section 2.7.4, we give more examples of this policy failing in real-world datasets. Finally, the failure of the aforementioned policy motivates the development of more sophisticated approximation algorithms, which we will discuss in the next section.

2.5.2 Approximation Algorithms for Linear Rewards

In this Section, we prove approximation guarantees based on randomized rounding. In brief, we solve the relaxation problem where the fractional solutions belong to $\mathcal{Z}$ and round accordingly.

First, note that a rounding regime that iteratively rounds the fractional optimal solutions in a backward fashion does *not* yield correct results. The reason is

Algorithm 2 Randomized Rounding for Dynamic Interventions

Sample-Interventions$(L(t:T), W(t:T), u(t:T), s)$

1. Until constraints are satisfied and the approximation guarantee is not violated
   (a) For every agent $j \in [n]$ sample (independent) interventions

$$\bar{z}_j(t:T) \sim \text{Bin}\left(\frac{\widetilde{z}^*_j(t:T)}{L_j(t:T)}, L_j(t:T)\right)$$

   or $\bar{z}_j(t:T) \sim L_j(t:T)\text{Be}\left(\frac{\widetilde{z}^*_j(t:T)}{L_j(t:T)}\right)$ (for AON).

2. Return the value function $V^{SOL}_{u(t:T)} = \sum_{t' \in [t,T]} \mathbb{1}^T \bar{p}(t)$ given the calculated approximate (SOL) policy after calculating the clearing payments $\bar{p}(t:T)$.

Aggregate-Discrete$(N, L(t:T), W(t:T), \mathcal{U}, s)$

1. Sample N exogenous shocks $\{u_j(t:T)\}_{j \in [N]} \sim \mathcal{U}$
2. For $i \in [N]$
   (a) Call **Pathwise-V**$(L(t:T), W(t:T), u_i(t:T), s)$ and get the optimal fractional policy $\widetilde{z}^*(t:T)$.
   (b) Calculate

$$V^{SOL}_{u_i(t:T)} = \textbf{Sample-Interventions}(L(t:T), W(t:T), u_i(t:T), s)$$

3. Return $\bar{V}^{SOL} = \frac{1}{N}\sum_{i=1}^{N} V^{SOL}_{u_i(t:T)}$

that a suboptimal action at round $t+1$ can affect the optimal fractional action at round t.

To combat this, we rely on the following algorithm: More specifically, let t be a fixed round and $s(t)$ be a fixed state at round t and let $u(t:T)$ be a sample path for the random sequence $U(t:T)$ from time t onward. Conditioned on the realization of $u(t:T)$, the regulator seeks to solve the following deterministic

problem

$$\begin{aligned} \max_{\bar{z}(t:T)} \quad & V_{u(t:T)}(t, s(t)) = \sum_{t'=t}^{T} R(s(t'), \bar{z}(t'), u(t')) \\ \text{s.t.} \quad & s(t') = \Psi_{t'}(s(t'), \bar{z}(t'), u(t')), \bar{z}(t') \in \mathcal{Z}_d^{\text{BIN}} \quad \forall t' \in [t, T]. \end{aligned}$$

We also consider the fractional relaxation where the decision variables lie in $\mathcal{Z}$. Let $V^{SOL}_{u(t:T)}(t, s(t))$ be the value that the approximation algorithm produces, let $V^{REL}_{u(t:T)}(t, s(t))$ be the optimal solution of the relaxation (i.e., when the interventions belong to $\mathcal{Z}$) and let $V^{OPT}_{u(t:T)}(t, s(t))$ be the optimal solution. From optimality we know that $V^{REL}_{u(t:T)}(t, s(t)) \geq V^{OPT}_{u(t:T)}(t, s(t))$. Note that since $u(t : T)$ is given, the optimal policy for the relaxed program consists of solving $T - t + 1$ LPs sequentially and finding the pair of the clearing vector and optimal policy. We produce a rounded policy SOL that corresponds to an intervention vector $\bar{z}(t : T)$ randomly by rounding the matrix $\widetilde{z}^*(t : T)$ of the optimal relaxed policy by rounding all random variables $\bar{z}_j(t')$ as Binomial i.i.d. vectors on L_j trials with biases $\widetilde{z}^*_j(t')/L_j$ for all $t' \in [t, T]$.

Theorem 2.5.3. *Algorithm 2 yields the following approximation guarantee (on expectation):*

$$\mathbb{E}_{u(t:T),\bar{z}(t:T)}\left[V^{SOL}(t, s(t))\right] \geq \left(1 - \widetilde{\beta}_{\max}\right) \cdot \mathbb{E}_{u(t:T)}\left[V^{OPT}(t, s(t))\right]$$

for the reward function $R(t) = \mathbb{1}^T \bar{p}(t)$.

Similarly, if we want to extend it to other linear objectives, the approximation ratio is going to be downscaled by a factor of $\zeta = \max_{j\in[n]} v_j / \min_{j\in[n]} v_j$. Note that in the proof of Theorem 2.5.3, there is no dependence on the states created by the rounded outcomes. Therefore, we can compare and lower bound by the fractionally relaxed policy's reward value at each round t.

Note here that the approximation guarantee of Theorem 2.5.3 depends on the *endogenous exposure index* $\beta_{\max}$, which depends on the domain of the sample path and the fractional interventions. While, to the best of our knowledge, this is the first approximation guarantee for this problem, we should note that the approximation guarantee can be simplified under specific cases: Firstly, if the system can clear all the liabilities, then the approximation factor simplifies to $\Delta_b/(\Delta_b + \Delta_\ell$ where Δ_b is the maximum magnitude of an external liability. This is similar to the static case, has no dependency on the time horizon, and is only instance-dependent (i.e., it depends on $\mathcal{U}$). Otherwise, the approximation factor lower bound loses an $\Omega(T^{-1})$ factor.

As the approximation factor of Theorem 2.5.3 is instance-dependent, one may ask whether obtaining a better approximation guarantee for the problem is possible. We give a positive answer to this question in the case of $T = 1$ (i.e., the static regime). In [226], the authors show that a greedy policy that orders nodes based on their financial connectivity achieves an approximation ratio of at most 3/4 for the case when $T = 1$. In this Chapter, we improve upon this result. Specifically, for interventions in $\mathcal{Z}_d^{\text{AON}}$ and $T = 1$, we can show that the corresponding optimization problem corresponds to maximizing a *monotone submodular function*, which yields an approximation algorithm achieving a constant approximation factor of $1 - 1/e$ which is optimal unless $P = NP$ [151, 302]. The detailed description of the greedy algorithm and its proof are provided in Appendix A.3.6.

Theorem 2.5.4. *For $T = 1$ and $\bar{z}(1 : T) \in \mathcal{Z}_d^{AON}$, there is a greedy algorithm that satisfies*

$$\mathbb{E}_{u,\bar{z}}\left[V^{SOL}(s)\right] \geq \left(1 - \frac{1}{e}\right) \cdot \mathbb{E}_u\left[V^{OPT}(s)\right]$$

for linear rewards $R_v = v^T \bar{p}$. Moreover, the approximation guarantee is optimal unless

$P = NP$.

2.5.3 Generalization of the LP-based algorithm for Bankruptcy Costs

A natural extension of our model would consider incorporating bankruptcy costs as it is captured by the Rogers-Veraart (RV) model introduced in [356]. According to [356, Definition 2.6], the clearing payments must satisfy:

$$\widetilde{p}_j(t) = \begin{cases} p_j(t), & \widetilde{p}_j(t) \leq \sum_{i\in[n]} a_{ij}(t)\widetilde{p}_i(t) + c_j(t) - x_j(t) + \widetilde{z}_j(t) \\ \kappa_A \sum_{i\in[n]} a_{ij}(t)\widetilde{p}_i(t) + \kappa_c(c_j(t) - x_j(t) + \widetilde{z}_j(t)), & \text{otherwise} \end{cases},$$

(RV-model)

where $\kappa_A, \kappa_c \in (0, 1]$ are scalar constants such that (see [356, Definition 2.5]), κ_A is the fraction of the face value of net external assets realized on liquidation, and κ_c is the fraction of the face value of inter-entity assets realized on liquidation. The EN model (and subsequently our model that includes interventions) is a special case of the RV model for $\kappa_A = \kappa_c = 1$.

Thus, all of our hardness and inapproximability results (Theorems 2 and 3) hold naturally in the more general RV model as well, since our model can be obtained by plugging $\kappa_A = \kappa_c = 1$ to Equation (RV-model). Moreover, based on the mixed integer linear programming formulation of [22], the dynamics correspond to

$$\bar{y}(t) \odot p(t) \leq A^T(t)\bar{p}(t) + c(t) - x(t) + \bar{z}(t) \tag{2.6}$$

$$\bar{p}(t) \leq \kappa_A A^T(t)\bar{p}(t) + \kappa_c(c(t) - x(t) + \bar{z}(t)) + \bar{y}(t) \odot p(t) \tag{2.7}$$

$$\bar{p}(t) \leq p(t)$$

$$0 \leq p(t)$$

$$\bar{z}(1:T) \in \mathcal{Z}_d^{\text{BIN}} \text{or } \mathcal{Z}_d^{\text{AON}}$$

$$\bar{y}(1:T) \in \{0,1\}^{nT},$$

where $\bar{y}(1:T)$ are auxiliary variables that we optimize together with the clearing payments $\bar{p}(1:T)$ and the controls $\bar{z}(1:T)$, the fractional relaxation corresponds to relaxing the controls to belong to $\mathcal{Z}$, and the auxiliary variables to belong to $[0,1]^{nT}$. It is straightforward to extend the proof of Theorem 2.4.1 to the fractional relaxation of the RV model. We can similarly show that the value function of the fractional relaxation of the RV model can be solved similarly to the EN model and corresponds to a sequence of nested LPs, with the only change that now we also optimize over the fractional relaxation $\widetilde{y}(1:T)$ of $\bar{y}(1:T)$.

In the sequel, we turn our attention to applying the same LP-based framework as in the case of the EN model, where we solve the fractional relaxation and then sample the interventions similarly to Algorithm 2. The following theorem provides an approximation guarantee (under certain values of κ_A) for the randomized rounding algorithm when bankruptcy costs are considered:

Theorem 2.5.5. *For the RV model and all* $\kappa_c \in (0,1], \kappa_A \in \left[0, \min\left\{1, 1/\widetilde{\beta}_{\max} - 1\right\}\right)$, *the randomized rounding algorithm yields the following approximation guarantee (on*

expectation):

$$\mathbb{E}_{u(t:T),\bar{z}(t:T)}\left[V^{SOL}(t,s(t))\right] \geq \frac{\kappa_c}{1+\kappa_c}\left(1-(1+\kappa_A)\widetilde{\beta}_{\max}\right)\cdot \mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right]$$

for the reward function $R(t) = \mathbb{1}^T \bar{p}(t)$.

Note that this algorithm does not yield the optimal approximation guarantee as choosing $\kappa_A = \kappa_c = 1$ yields a guarantee of $1/2 - \beta_{\max}$ which we already know is worse than the $1 - \beta_{\max}$ guarantee of Theorem 2.5.3.

2.6 Incorporating Fairness Constraints in Network Interventions

We say that an intervention is fair across the nodes if the intervention each node gets "does not differ a lot from its neighbors", whereas the "neighborhood" of a node can be expressed in terms of the existing financial network or can be expressed in terms of an auxiliary network. In this way, we can measure fairness in interventions in various settings. For instance, we can compare the interventions between a node and all other nodes in the network, interventions between a node and its neighbors on the financial network, and interventions between nodes belonging to different population groups (such as minority groups). We require the fairness metrics to be invariant towards scaling the entire control vector, namely, do not change when the control changes from $z(t)$ to $\alpha z(t)$ for some $\alpha > 0$, similarly to [178, 257, 256].

Proposition 2.6.1. *Our model allows for incorporating any convex fairness constraint* $\phi(\widetilde{p}(t), \widetilde{z}(t)) \leq 0$ *through augmenting the constraints of Equation* (2.2).

Driven by the above desiderata, we call an intervention rule[1] $z(t)$ in the model *fair* if the interventions of a node do not *"differ much"* from its neighbors. As a starting point, we consider the Gini Coefficient [178] and generalize it accordingly to our model. In detail, we measure the deviation between a node and its neighbors on a dynamic graph $H(t)$ with weights $w_{ji}(t) \geq 0$ ($w_{jj}(t) = 0$ for all $j \in [n]$), with the following two measures:

1. *Asymetric Fairness.*

$$\mathrm{GC}^{\mathrm{asym}}(z(t); H(t)) = \frac{\sum_{(i,j)\in E(H(t))} w_{ij}(t)|z_j(t) - z_i(t)|}{2\sum_{i\in[n]} z_i(t)\left(\sum_{j\in[n]} w_{ij}(t)\right)}. \tag{2.8}$$

   This measure, though asymmetric, is inspired by the initial definition of the Gini Coefficient [178], which equals 0 if all resources are equitably distributed and $1 - 1/n$ if one node gets all the resources. However, such measure varies from 0 to $\frac{\sum_{i\in[n]}(w_{i,j_0}(t)+w_{j0,i}(t))}{2\sum_{i\in[n]} w_{i,j0}(t)}$ (if a node $j_0 \in [n]$ gets all the interventions) for an arbitrary measurement graph $H(t)$. In contrast, a more natural fairness measure is expected to lie in $[0, 1]$. This technical issue is mitigated subsequently by the subsequent definition of symmetric fairness.

2. *Symmetric Fairness.*

$$\mathrm{GC}^{\mathrm{sym}}(z(t); H(t)) = \frac{\sum_{(i,j)\in E(H(t))} w_{ij}(t)|z_j(t) - z_i(t)|}{\sum_{i\in[n]} z_i(t)\left(\sum_{j\in[n]}(w_{ij}(t) + w_{ji}(t))\right)}. \tag{2.9}$$

   Note that the above measure of inequality is well defined: when all nodes get the same interventions, it equals zero, and when one node gets all the interventions, it equals one.

[1] Here, $z(t)$ can correspond to discrete or fractional interventions. When the context is specified, we use the corresponding notation, i.e., $\bar{z}(t)$ for the discrete interventions and $\overline{z}(t)$ for the fractional interventions, respectively.

Appendix A.2 provides some potential fairness measures.

To incorporate these fairness measures, we formulate the following relaxations to the optimization problems involving the aforementioned fairness metrics for a target fairness metric upper bound $g(t) \geq 0$ for any choice of non-negative weights. First, we consider the following optimization problem that extends the formulation without fairness by adding the GC-dependent constraints for asymmetric fairness. We introduce auxiliary variables $\varpi_{ji}(t)$ for all (j,i) such that:

$$\begin{aligned} \varpi_{ji}(t) &\geq 0 && \forall (j,i) \\ -\varpi_{ji}(t) \leq z_j(t) - z_i(t) &\leq \varpi_{ji}(t) && \forall (j,i) \\ \sum_{(j,i)\in E(H(t))} w_{ji}(t)\varpi_{ji}(t) &\leq 2g(t) \sum_{j,i\in[n]} w_{ji}(t) z_j(t). \end{aligned} \tag{2.10}$$

Similarly, by replacing the right-hand side of the last inequality, i.e., $2g \sum_{j,i\in[n]} w_{ji}(t)z_j(t)$, with $g(t) \sum_{j,i\in[n]} (w_{ij}(t) + w_{ji}(t))z_j(t)$, then we get the optimization formulation for the case of symmetric fairness. Then, a natural question we might ask is, *"What is the maximum effect of these fairness constraints on the welfare objective function?"*. We define the *Price of Fairness* (PoF) to be

$$\text{PoF}(z(1:T)) = \frac{\text{Value function without Fairness Constraints}}{\text{Value function with Fairness Constraints}}.$$

We prove the following about the PoF:

Theorem 2.6.2. *The following are true:*

1. *For any $M = M(n, T, \Delta_u) > 0$, there exist instances with non-trivial fairness*

constraints (i.e., $g(1:t) > 0$) such that discrete interventions yield PoF $> M$.

2. *For any non-negative increasing reward function R such that R is bounded by a function $f(n, T, \Delta_u) < \infty$ and fairness constraints $g(1:t) \geq 0$, there exists $M = M(n, T, \Delta_u, g(1:T)) > 0$ such that fractional interventions yield* PoF $< M$.

2.7 Effect of Network Structure on Intervention Policies

We assess how the network structure affects interventions in real-world and semi-synthetic data. We run experiments with various datasets, including synthetic networks and financial networks from various online and physical settings, and an application to a non-financial networked resource intervention problem arising in ridesharing.

2.7.1 Distribution of Interventions

We construct the following datasets[2]:

Synthetic Core-periphery Network (Stochastic blockmodel) ($T = 10, n = 50$). We generate a network of $n = 50$ nodes and $T = 10$ rounds. In contrast, the structural graphs G_t are drawn i.i.d. from an SBM with a Core-periphery structure with two blocks of size $n_{\text{core}} = 10$ and $n_{\text{periphery}} = 40$ and edge probability matrix $\begin{pmatrix} p_{cc} = 0.45 & p_{cp} = 0.1 \\ p_{pc} = 0.1 & p_{pp} = 0.1 \end{pmatrix}$. The internal liabilities and the external liabilities are drawn i.i.d. from Exp(1), where the internal liability between (i, j) at round

[2]More information can be found at Appendix A.6.

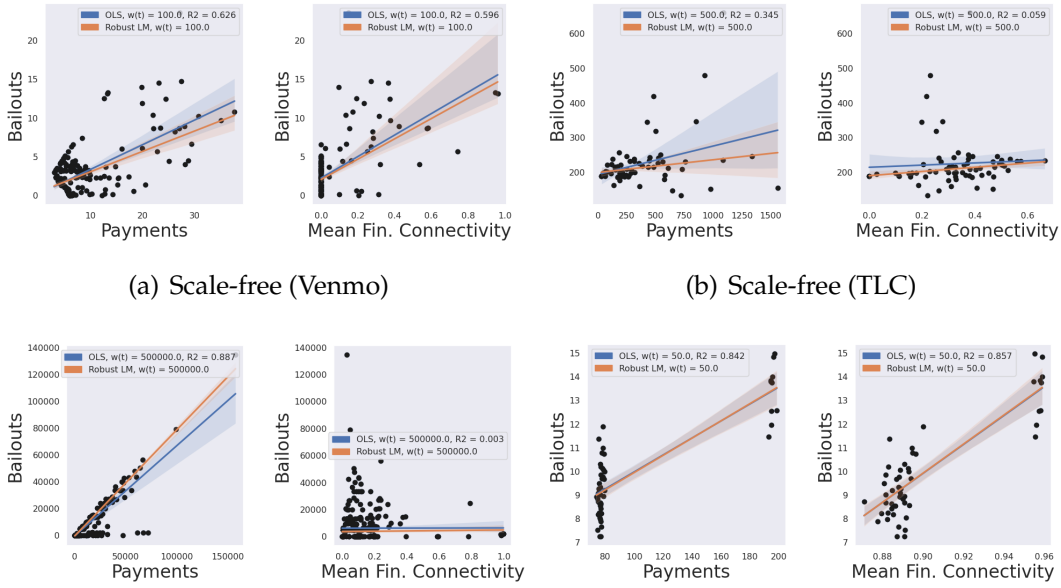
t is realized conditioned on the edge (i, j) existing on G_t. The asset and shock vector are set to 0 every time.

Online Financial Network (Scale-free) (Venmo transaction data) ($T = 6, n = 200$). We use publicly available data[3] from public Venmo transactions to form a dynamic transaction network. The dynamic financial network corresponds to Venmo transactions between July 2018 to September 2018 (3.8M transactions). Data is grouped weekly, and we identified two sets of nodes: V_1 (top 100 by incoming transactions) and V_2 (top 100 by outgoing transactions), combined as $V = V_1 \cup V_2$. We counted transactions within V and between V and the external system, adding one transaction for nodes with zero outgoing transactions. Random liabilities were generated using a Gamma distribution based on transaction counts, ensuring $b(t) > 0$. The details of the dataset construction have been deferred to Appendix A.5.

Non-financial Allocation Network (Scale-free) (Extra dispatches in ridesharing) ($T = 31, n = 69$). To demonstrate our framework's applicability beyond financial networks, our final experiment looks at the problem of creating extra dispatches (for example, using autonomous vehicles) in ridesharing networks to mitigate instantaneous demand-supply imbalances. We use publicly available trip data from the NYC Taxi and Limousine Commission (TLC). We describe the process of creating the dynamic network in detail in Appendix A.5.

Physical Financial Network (Bipartite) (Cellphone Mobility Data) ($T = 5, n = 152$). Data generated based on mobility data from the SafeGraph platform dur-

[3] https://github.com/sa7mon/venmo-data



(a) Scale-free (Venmo)

(b) Scale-free (TLC)

(c) Bipartite (SafeGraph)

(d) Core-periphery (SBM)

Figure 2.3: Relation of topology and interventions for the three types of networks. We use $L(t) = W(t) \cdot \mathbb{1}$.

ing April 2020. The nodes in the financial network represent *(i)* Points of Interest nodes (POI nodes) that represent various businesses categorized by their *NAICS codes* to categories (i.e., grocery stores, banks, gas stations, etc.) and the Census Block Group[4] (CBG) they are located at *(ii)* CBG nodes that represent a set of households in a certain location. We focus on a period of $T = 5$ months spanning from December 2020 to April 2021. The detailed creation of the financial network has been deferred to Appendix A.6.

We study the distribution of interventions for the various topologies. In Figure 2.3, we report the relationship between the clearing payments and the interventions and the relation between the mean financial connectivity and the interventions. We fit an ordinary least squares model (OLS) to the points and

[4]A CBG is a unit used by the US Census. It is the smallest geographical unit for which the bureau publishes sample data, i.e., data that is only collected from a fraction of all households and contains 600-3K people.

a robust linear model via iteratively reweighted least squares with Huber's T criterion.

Regarding the scale-free networks, we observe a positive correlation between the clearing payments and the interventions, which are mostly concentrated in a non-uniform way, meaning that the regulator focuses more on nodes that clear more payments. Lower values have more observations, and higher values have fewer observations due to the scale-free nature of the liabilities. Additionally, there is a positive correlation between the financial connectivities and the interventions.

For the bipartite graph, we observe a positive correlation between the clearing payments and the interventions ($R^2 = 0.887$), with several nodes getting small interventions regardless of their payments. However, the mean financial connectivity is uncorrelated ($R^2 \approx 0$) with the interventions. A potential explanation for this could be that most nodes (which correspond to households) have external obligations that are significantly larger than the internal ones, making the financial connectivity small in general while at the same time, these nodes receive high enough interventions.

Finally, we observe that in the case of the core-periphery network, the interventions are separated into two main "bands", which correspond to the core and the periphery nodes, respectively, and are positively correlated with $R^2 \approx 0.85$, meaning that the optimal interventions are focused more towards the core nodes.

In all of the experiments of Figure 2.3, a common pattern emerges: nodes that clear more payments get higher interventions. These nodes are also cen-

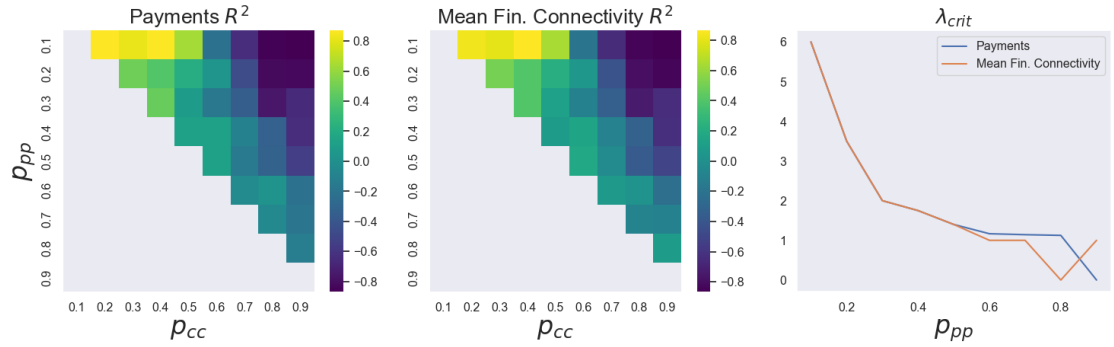


Figure 2.4: We analyze the R^2 values that relate clearing payments and financial connectivity to interventions across varying values of p_{cc} and $p_{pp} = p_{pc} = p_{cp}$. Our observations reveal a distinct pattern: when the core is sufficiently sparse (i.e., p_{cc} is small), the optimal policy allocates more bailouts to more central nodes (reflected by $R^2 > 0$). Conversely, when p_{cc} is high, the budget is optimally allocated to the most peripheral nodes (indicated by $R^2 < 0$). Therefore, interventions in a sparse core enhance the network's resilience, while a dense core can facilitate the spread of shocks.

tral in the network regarding their exposure. One may be urged to think that more central nodes would generally get higher bailouts. As we show in the following Section when the more central nodes are sparsely connected, this is the case; however, as the connections between the central nodes become denser, the regulator should focus on the less central nodes to remediate contagion.

2.7.2 The Role of Centrality and a Phase Transition

Previously, we showed that more central nodes generally get higher interventions. In the core-periphery network, we observed a "banding" phenomenon, where the interventions were concentrated around the core and the periphery nodes, with higher interventions corresponding to the core nodes. The first question that comes up is whether this is a general trend. As we show below, our answer is negative. Namely, we can construct networks where this does

not hold. Specifically, we show that as long as the core nodes are sufficiently sparsely connected, then intervening in the core nodes incurs the maximum benefit for the network; however, when the core connections become dense enough, it is optimal to intervene in the periphery nodes.

To show this, we consider a family of core-periphery networks constructed via a stochastic blockmodel with $n_{\text{core}} = 10$ nodes and $n_{\text{periphery}} = 40$ nodes, and edge probability matrix $\begin{pmatrix} p_{cc} & p_{pc} \\ p_{cp} & p_{pp} \end{pmatrix}$ with $p_{cc} \geq \max\left\{p_{pp}, p_{pc}, p_{cp}\right\}$. For simplicity we have taken $p_{pp} = p_{cp} = p_{pc}$, and sample liabilities from Exp(1) for the realized edges. In Figure 2.4, we vary p_{cc} from 0.1 to 0.9, and p_{pp} from 0.1 to p_{cc} and report the correlation coefficient R^2 between the clearing payments and the interventions as well as the mean financial connectivity and the interventions.

We observe the following interesting phase transition: When the ratio $\lambda = p_{cc}/p_{pp}$ is close to 1, i.e., the core is relatively sparsely connected compared to the periphery, then $R^2 > 0$ and the core nodes (which have higher financial connectivity) are the ones which get the interventions. On the other hand, as λ increases and the core becomes dense enough, it reaches a critical value λ_{crit} (see the rightmost subfigure in Figure 2.4), at which the regulator allocates to the periphery nodes (which corresponds to $R^2 < 0$).

The regulator's interventions are not universally centered on the most central nodes in a financial network. Instead, the optimal intervention strategy depends critically on the density of connections within the network's core. When core nodes are sparsely connected, interventions should be concentrated on these central nodes to maximize network resilience. Conversely, as the core becomes densely interconnected, a critical threshold is reached beyond which the

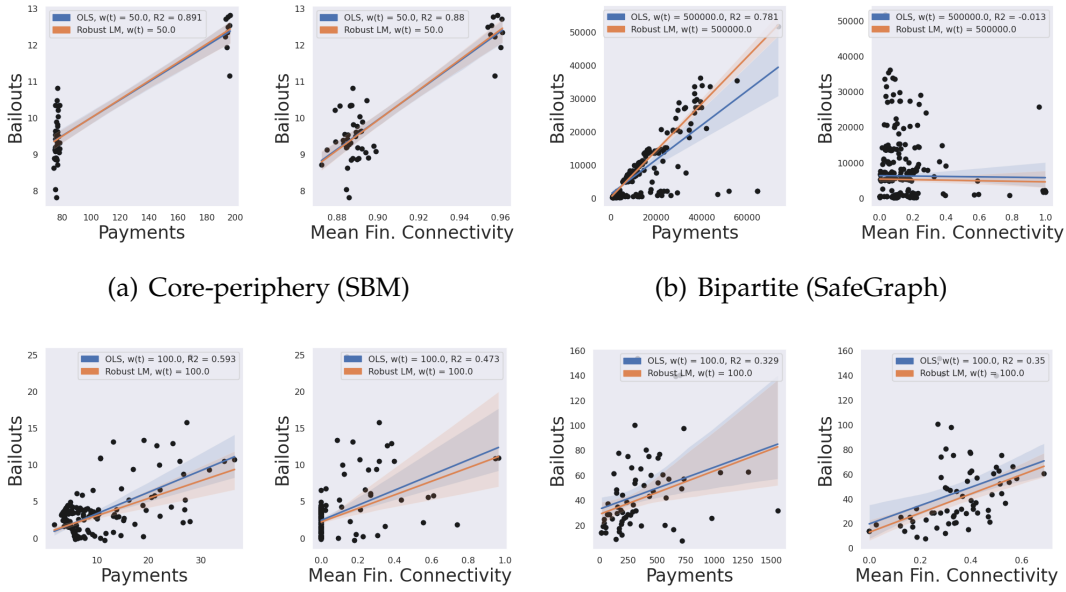
most effective intervention strategy shifts towards supporting the peripheral nodes. This nuanced understanding of interventions highlights the importance of assessing the network's structural properties before deciding on intervention strategies.

A related but complementary to our phase transition has also been observed in [8] from the point of network shocks. Specifically, the authors find that when network shocks are sufficiently small, denser connections enhance financial stability; however, dense connections become a mechanism to propagate shocks beyond a certain shock magnitude. Our phase transition complements this finding and provides additional insights regarding optimal interventions. Under the assumption that the magnitude of shocks is homogeneous but the network structure is heterogeneous, intervention at the core nodes remediates contagion the sparser their connections are.

2.7.3 Experiments with Fairness

In Section 2.6 and Appendix A.2, we proposed various fairness measures, which we examine here. Specifically, to induce fair interventions (in the fractional case), we run Algorithm 1 with the constraints of Section 2.6. In Table 2.1, we run experiments with the fairness constraints where we constrain the symmetric Spatial GC (Figure 2.5) and the Standard GC (Figure 2.6) to be at most $g(t) = 0.5$ at all times for different values of the budget infusion $W(t)$ (per dataset).

We observe that constraining according to the Spatial Gini Coefficient affects the relation of payments and interventions slightly (see Figure 2.5); however, constraining according to the Standard Gini Coefficient (see Figure 2.6) affects



(a) Core-periphery (SBM)

(b) Bipartite (SafeGraph)

(c) Scale-free (Venmo)

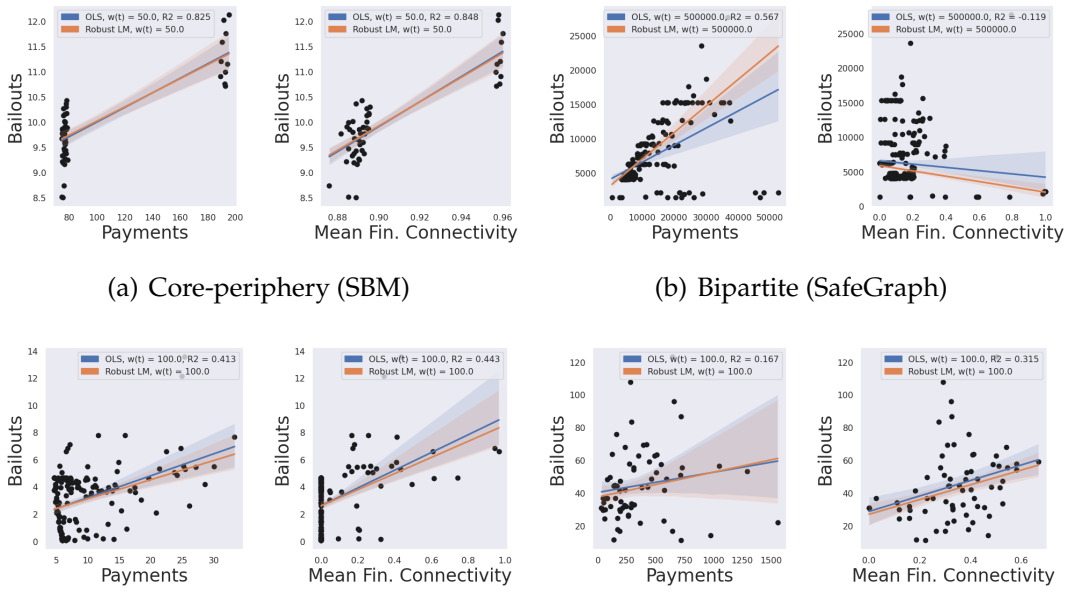
(d) Scale-free (TLC)

Figure 2.5: Relation of topology and interventions for the three types of networks and fairness constraints according to the Spatial Gini Coefficient. We use $L(t) = W(t) \cdot \mathbb{1}$ and $g(t) = 0.5$.

the results non-trivially, with the most important changes occurring at the scale-free networks. This is because the Standard Gini Coefficient treats the intervention graph as a complete graph and treats the nodes on an equal basis. This can greatly affect scale-free networks since very few nodes are the most exposed ones, and most nodes have small exposure in terms of their liabilities.

Next, in Table 2.1, we report the PoF for the corresponding experiments of Figures 2.5 and 2.6. We take the average of over 50 independent runs for the datasets that involve randomness. Table 2.1 indicates that all fairness measures achieve a PoF close to 1 in all datasets. This indicates that, generally, our intervention algorithm can respect algorithmic fairness constraints with a very small cost on the total welfare.

Secondly, we perform experiments imposing asymmetric fairness con-



(a) Core-periphery (SBM)

(b) Bipartite (SafeGraph)

(c) Scale-free (Venmo)

(d) Scale-free (TLC)

Figure 2.6: Relation of topology and interventions for the three types of networks and fairness constraints according to the Standard Gini Coefficient. We use $L = W(t) \cdot \mathbb{1}$ and $g(t) = 0.5$.

Fairness Constraint	Synthetic	TLC	Venmo	Safegraph
Budget Increase $W(t)$	50	100	50	500K
Spatial GC ($w_{ij}(t) = a_{ij}(t)$)	1.013	1.008	1.020	1.020
Standard GC ($w_{ij}(t) = \mathbb{1}\{i \neq j\}$)	1.005	1.009	1.013	1.102

Table 2.1: Price of Fairness. The payments and interventions are at Figures 2.5 and 2.6. We set $g(t) = 0.5$.

straints. In Figures 2.7(a) to 2.7(c), we study the total flow objective where we run the unconstrained optimization problem (i.e., with a large upper bound), and second, we restrict the Equation (Standard-GC-Asym) to be at most 0.1. After the optimization, we report the relaxation optimum, the rounded solutions to the problem, and the realized Equation (Standard-GC-Asym). We study the behavior concerning the Equation (Standard-GC-Asym) and Equation (Prop-GC-Asym) constraints. For the SafeGraph and the German Banks data, we use the fuzzy version of the Equation (Prop-GC-Asym) where the weights repre-

sent the probability that a node is a minority node. In other words, we want to impose constraints between *minority* and *non-minority* groups. For the former dataset, the weights q are the minority scores for each CBG and business where we impute missing data with the MLEs of the existing data. For the latter dataset, the values of q are sampled i.i.d. from Beta$(2, 5)$. We use a budget increase rate of 10^4 for SafeGraph, similar to the one reported in Figure 2.8, and an intervention $L = 10^6 \cdot \mathbb{1}$ for German Banks. Lastly (Figure 2.7(d)), we plot the relation between the upper bound on the Equation (Sp-GC-Asym) coefficient and the PoF for the German Banks Data for $L = 10^5 \cdot \mathbb{1}$.

The German banks dataset Equation (Standard-GC-Asym) case (Figures 2.7(a) and 2.7(c)) has predictable behavior. To be more specific, as the number of interventions k is small, the instance for which $g = 0.1$ has a lower relaxation optimum as well as rounded value for $k \leq 6$ and later approaches the unconstrained optimum (i.e., where $g = 1$). In the constrained case, the Gini coefficient rises to its upper bound of 0.1 until $k = 6$ and then starts to drop, which coincides with the objective value plots. The explanation for this phenomenon is rather simple: at first, when resources are scarce, selecting certain nodes on the network subject to these resources creates inequality, which is mitigated by the constraint at the expense of the quality of the solution, creating a worse PoF of about 1.2. When k is large enough, i.e., $k \geq 6$, the available resources allow the constrained version to create a solution close to the unconstrained version (by "rebalancing" some $\vec{z}_i^*$ values), which is reflected on both objective values, and eventually the PoF reaches 1 when the two solutions eventually meet. Similarly, when we constrain the Equation (Prop-GC-Asym) (Figure 2.7(c)) the PoF is approximately 1.16 in the worst case ($k = 2$) and approaches 1 at $k = 6$.

The PoF for the SafeGraph subject to the Equation (Prop-GC-Asym) constraint data is approximately 1, meaning all the resources have been equitably allocated between minority/non-minority groups subject to the respective constraint(s). Lastly, in Figure 2.7(d) we observe that the PoF drops quickly to 1 in most cases and a decent trade-off between fairness and optimality can be achieved when $g = 0.4$.

2.7.4 Failure of Threshold-based and Structure-based Heuristics for Discrete Interventions

The next set of experiments evaluates the randomized and greedy algorithms against network-based heuristics. For this reason, we focus on the case where $T = 1$. We use the following heuristic methods to allocate stimulus, where for each step, we augment each set (based on the criteria below) maximally subject to the budget constraint:

- *Wealth Policy.* We sort the nodes in increasing order of initial wealth $b_j + \sum_{i\sim j} p_{ij} - \sum_{j\sim i} p_{ji}$, nodes with the lowest wealth each time. Note that we performed the same experiments with decreasing order of wealth, and the results were similar and thus omitted.
- *Out-degree Policy.* We take the nodes with the highest out-degrees.
- *PageRank [316].* We take the k-top nodes in decreasing PageRank values. The calculation of PageRank takes into account the directionality of the graph.
- *Eigenvector Centrality [158].* We take the nodes in decreasing value of their

eigenvector centrality (i.e., values of the principal eigenvector of the corresponding random walk transition matrix). The computation of the eigenvector centrality measure ignores directionality.

- *Random Permutation.* Baseline criterion that considers a random permutation of the nodes.

Such policies are well-known benchmarks and have been used on similar tasks such as Influence Maximization [236]. We also report the relaxation optimum for all experiments, which is an upper bound to the true optimum (assuming discrete interventions). We are considering an additional dataset of German banks. ($T = 1, n = 22$) from the work of [97] where the internal and external assets and liabilities of German Banks are reported.

Firstly, for various values of L, either fixed or varying, we report the corresponding objective values averaged over multiple draws of shocks from the corresponding shock distribution, where we report both the empirical mean and standard deviation (std). We parameterize the available budget with a pair of parameters. The former parameter ℓ parameterized the budget increase rate, and the latter parameter k parameterized the multiplicity of resources. We make assumptions about the interventions that fall into two main categories: *(i)* fixed interventions, where $L = \ell \cdot \mathbb{1}$ and $B_k = \ell \cdot k$ and the number of interventions k varies along the x-axis of the plots. This is equivalent to bailing out at most k nodes on the network, where every node gets a stimulus value of ℓ. *(ii)* variable interventions: in the SafeGraph experiments, we determine the interventions as discussed in Appendix A.6. We assume that for each step k, the budget increases by some amount ℓ, so, again, the available budget is $B_k = \ell \cdot k$. In the experiments, we focus on the following linear objectives: the total flows/sum of

payments, which corresponds to choosing $v = \mathbb{1}$, the sum of internal flows/payments which corresponds to choosing $v = \beta$, and the sum of external flows/sum of taxes which corresponds to choosing $v = \mathbb{1} - \beta$.

On the German Banks dataset, in the worst case, the greedy algorithm outperforms the LP-based one by $\approx 15\%$. In contrast, the PageRank and centrality-based heuristics are outperformed by greedy by $\approx 58\%$ in the worst case. Finally, we note that the random permutation, wealth, and outdegree heuristics perform poorly in both objectives. The significantly decreased performance of the wealth heuristic is justified by the fact that nodes that are important for the intervention process and have priority (i.e., lower wealth) are not well-connected.

Similarly, one can argue about the other heuristics. In the case of the outdegree heuristic, nodes with low equity may be well connected to the other nodes; thus, giving them priority does not contribute substantially to the overall objective. The uneven form of such curves suggests that these simple heuristics are not good candidates for this optimization problem.

For the SafeGraph data, the randomized rounding algorithm outperforms all benchmarks and is also very close to the greedy algorithm with a worst-case difference of about 7.1% and being as far as approximately 40% from the other heuristics in the worst case in the $v = \mathbb{1} - \beta$ plot. In Figure 2.8(d), the differences are about 18% in the worst case, however the greedy algorithm quickly approaches the randomized rounding algorithm. Figure 2.8 suggests that interventions and {financial connectivity, centrality, wealth} may have some correlation; but not very high. We believe such naïve policies have pitfalls, i.e., including bailing out big corporations that may not need interventions or bailing out individuals who are not *"important"* to the network.

2.7.5 Additional Computational Experiments

Dynamic Fractional Interventions. For the fractional intervention setting, we report the payments, cumulative rewards, and interventions for the datasets in question; since we solve the problem optimally, we do not report competing methods. In Figure 2.9, we plot the average clearing payments, the average cumulative reward, and the average *fractional* interventions for the Synthetic Core-periphery data and the Venmo data together with confidence intervals by averaging over 50 samples of the random networks. We plot the clearing payments of the five most *important* nodes (in terms of total payments). The runtime required to solve these problems varies from a few seconds to a few minutes.

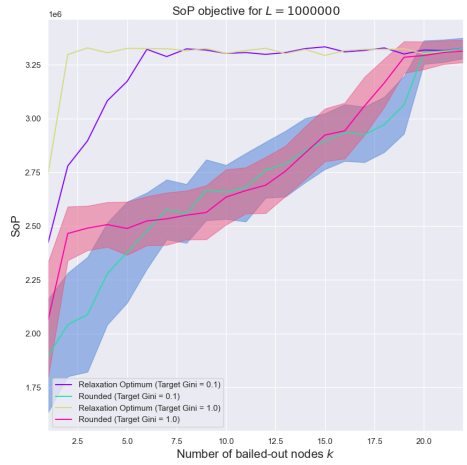
Dynamic Discrete Interventions and Randomized Rounding. For the discrete intervention setting, we report the results from running the randomized rounding algorithm which performs well in practice (see next Section), and has been shown to outperform several network-based heuristics. Similarly, in Figure 2.10, we plot the average clearing payments, the average cumulative reward, and the average *discrete* interventions for the TLC data and the SafeGraph data. Again, the runtime required to solve these problems varies from a few seconds to a few minutes.

2.8 Discussion

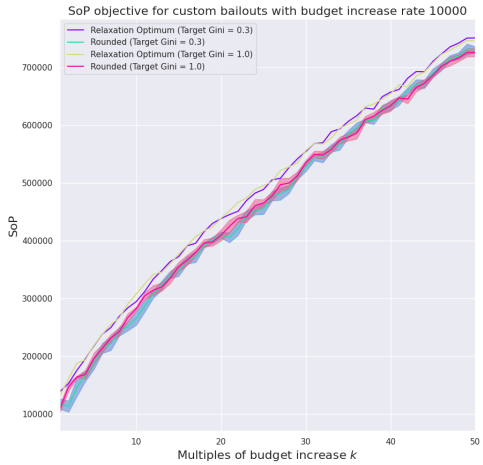
In this paper, we have studied a dynamic resource allocation problem through the lens of financial contagion, which can incorporate a variety of resource allocation problems. We formulate an intervention problem in a network that

obeys the EN contagion model. We study the problem of allocating fractional and discrete resources so that contagion is averted, and we design algorithms to calculate the optimal interventions. We prove that the problem of discrete interventions is intractable and that there is no hope of finding an approximation algorithm for some specific objectives. For the other objectives, we develop approximation algorithms that rely on randomized rounding and provide a greedy algorithm that works for a particular intervention setting. In the sequel, we introduce various fairness measures in both regimes and study the Price of Fairness. Then, we test our developed algorithms on real-world and semi-artificial data and develop decision-making insights.

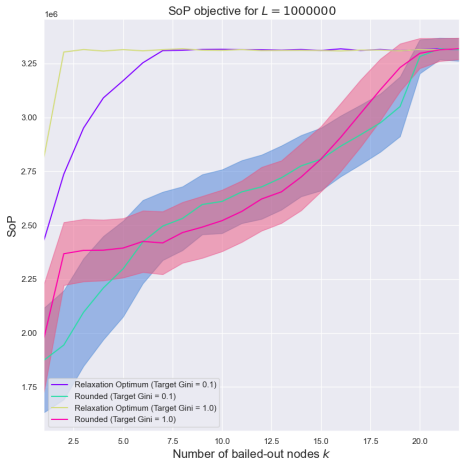
There are several potential future road maps for our work. Firstly, whether the approximation ratio for discrete interventions can be improved (and by how much) is currently unknown beyond the case of $T = 1$. Moreover, another interesting question in the dynamic setting relaxing is the assumption that the system responds optimally at each step and how it compares with the globally optimal policy. Lastly, rounding the clearing variables is interesting to achieve a provable solution within some factor from the optimal policy.



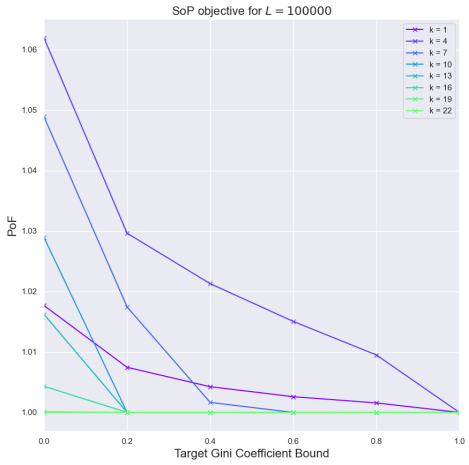
(a) German Banks, Equation (Standard-GC-Asym), $L = 10^6 \cdot \mathbb{1}$



(b) SafeGraph, Equation (Prop-GC-Asym), L custom

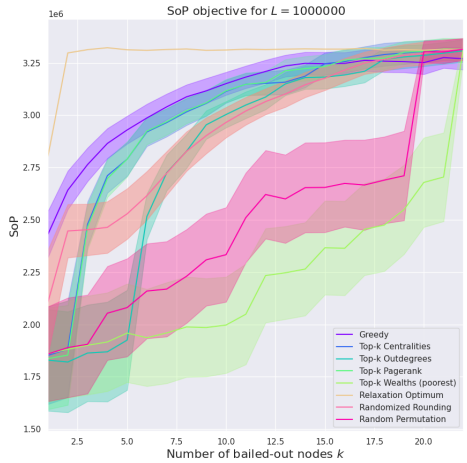


(c) German Banks, Equation (Prop-GC-Asym), $L = 10^6 \cdot \mathbb{1}$

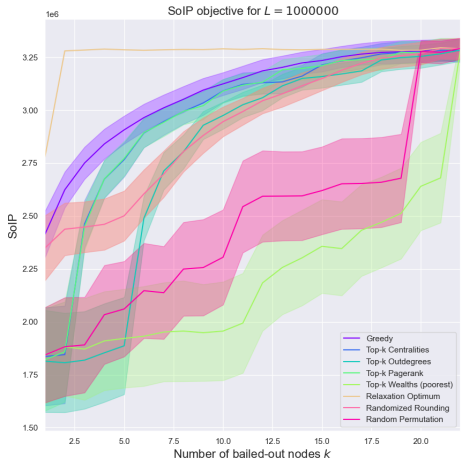


(d) German Banks Data, Equation (Sp-GC-Asym), $L = 10^5 \cdot \mathbb{1}$

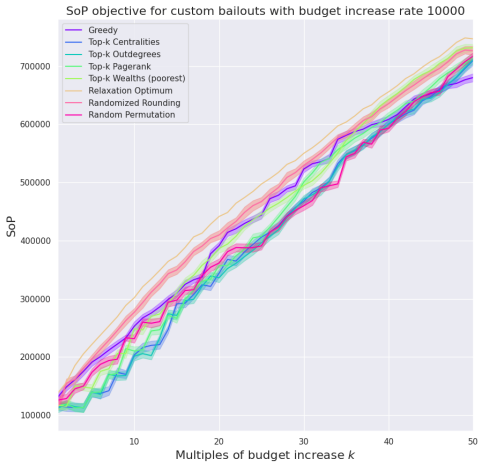
Figure 2.7: Figures 2.7(a) to 2.7(c): Relaxation Optima and Rounded Values for (i) unconstrained fairness, (ii) constrained fairness (given by the `TargetGini` variable, which gives the upper bound g on the fairness). For Equation (Prop-GC-Asym), we use minority demographic characteristics for SafeGraph, and artificial data drawn i.i.d. from Beta(2, 5) for German Banks. Number of simulations as in Figure 2.8. Figure 2.7(d): Relation between fractional PoF and the upper bound g on the Equation (Sp-GC-Asym) for varying resources for the German Banks dataset.



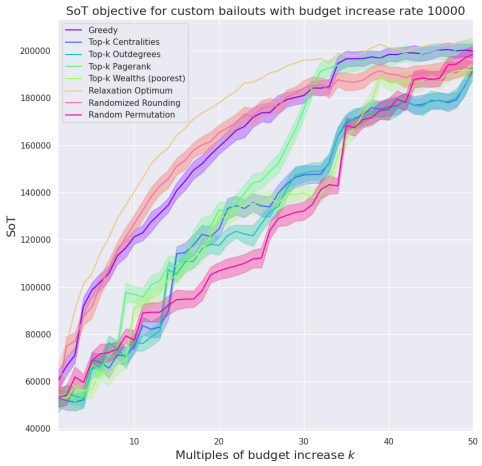
(a) German Banks,$v = \mathbb{1}$, $L = 10^6 \cdot \mathbb{1}$



(b) German Banks, $v = \beta$, $L = 10^6 \cdot \mathbb{1}$

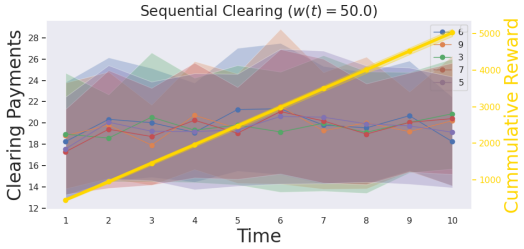


(c) SafeGraph,$v = \mathbb{1}$, L estimated from real-world data with a budget given by $B_k = 10^4 \cdot k$

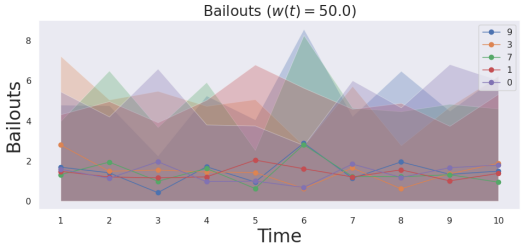


(d) SafeGraph, $v = \mathbb{1} - \beta$, L estimated from real-world data with a budget given by $B_k = 10^4 \cdot k$

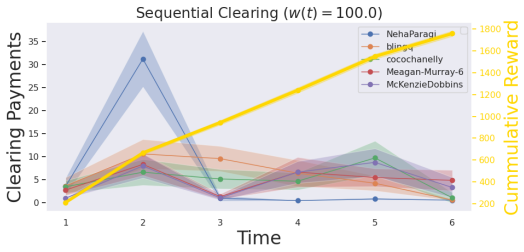
Figure 2.8: Comparison of randomized rounding, greedy, and network heuristics on the data. We ran 1K simulations for German Banks and 50 simulations for SafeGraph. Error areas represent 1 std.



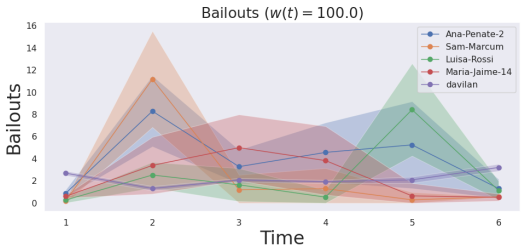
(a) Clearing Payments ($L_i(t) = W(t) = 50$)



(b) Interventions ($L_i(t) = W(t) = 50$)

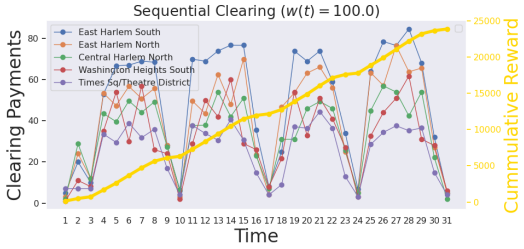


(c) Clearing Payments ($L_i(t) = W(t) = 100$)

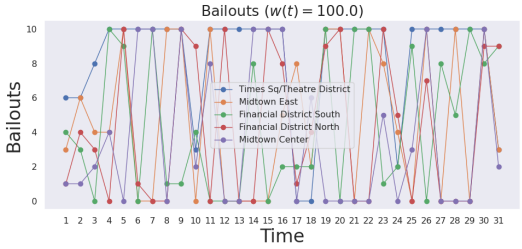


(d) Interventions ($L_i(t) = W(t) = 100$)

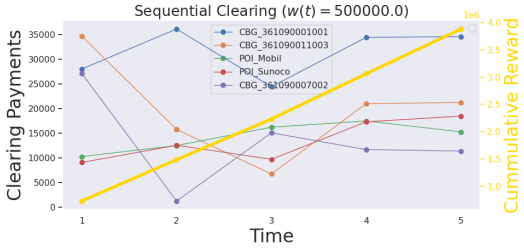
Figure 2.9: Fractional interventions in financial networks based on the stochastic block model (a-b) and Venmo data (c-d).



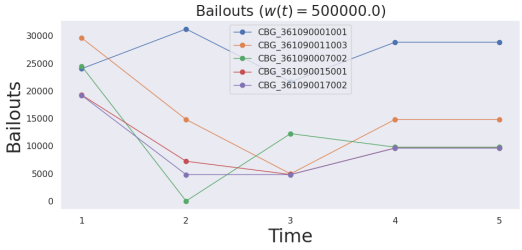
(a) Vehicle flows ($W(t) = 100, L_i = 10$)



(b) Extra dispatches ($W(t) = 100, L_i = 10$)



(c) Payments ($W(t) = 500K, L$ custom)



(d) Interventions ($W(t) = 500K, L$ custom)

Figure 2.10: Figs (a-b): Interventions (extra dispatches) in ridesharing (January 2021 NYC data; we report 5 busiest neighborhoods).Figs (c-d): Discrete interventions in a financial network (based on SafeGraph Data, December 2020-April 2021).

CHAPTER 3

TOPOLOGICAL MEASURES OF SYSTEMIC RESILIENCE: A NETWORK PERCOLATION APPROACH

The contents of this chapter constitute joint work with Amin Rahimian.

The global economy consists of many interconnected entities that are responsible for the supply and sourcing of products [88]. These *production networks* consist of *products*, each of which has some required *inputs* that can be obtained from a group of *suppliers* and play a critical role in the day-to-day operations of the world economy [274]. This interdependence between products leads to *cascading failures* once parts of the supply chain are disrupted [206, 88, 275, 164, 4, 193]. For example, the recent COVID-19 pandemic and the war in Ukraine disrupted parts of global supply, whose failures then spread to other parts of the supply chain network, causing *bottlenecks* and *choke points* [145, 142, 189, 413, 372]. In light of such problems, there is an ever-emerging need to study the resilience of supply chain networks to identify vulnerabilities, such as bottlenecks and choke points, and take steps to mitigate their effects [242, 191, 370, 58, 371]. A motivating example is a tree production network in which various raw materials lead to the production of more specialized products in several layers. There, it is easy to observe that the failure to produce any of the raw materials, because all the suppliers that make them have failed, has a devastating effect on the network and almost nothing can be produced.

Various methods and approaches can be used to study the resilience of supply chain networks [334, 24, 143]. One direction is to use network analysis tools to identify critical components of the network and assess their vulnerability to

disruption. This can include identifying key suppliers, products, and transportation routes and evaluating their importance to the overall network. Another approach is to use simulation modeling to analyze the impact of different disruptions on the network and evaluate the network's ability to recover from these disruptions [371]. This can include analyzing the effect of different disturbances (e.g., natural disasters, supply chain failures, etc.) and scenarios where disruptions occur (e.g., simultaneous disruptions, sequential disruptions, etc.). In addition to these technical approaches, it is important to consider organizational and strategic approaches to building resilience in supply chain networks [77, 373]. This can include implementing contingency plans, developing relationships with alternative suppliers, and diversifying the network to reduce the impact of a single point of failure. Building resilience in supply chain networks requires a multifaceted approach that includes technical analysis, strategic planning, and organizational preparedness. By understanding the structure and dynamics of these networks, it is possible to build foundational resilience into systems that can evolve to withstand disruptions and recover more quickly when they occur.

3.1 Overview of the Results

We model the product requirements as a digraph, including raw material with no incoming edges and only outgoing edges, and more complex products whose sets of incoming edges indicate requirements for their productions. We refer to this digraph as the production network and also assume that each product has a number of suppliers that operate and can fail with probability x. According to our model, a product can be produced when all its requirements are

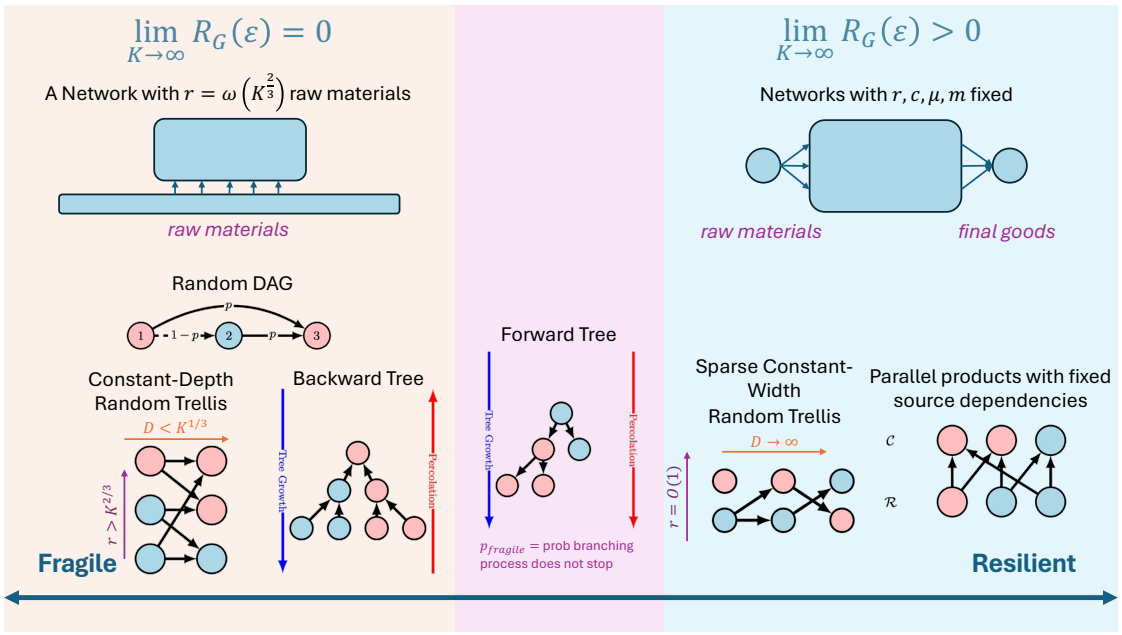


Figure 3.1: High-level graphical overview of our main results. Exact bounds are located in Table 3.1.

met and its suppliers do not all fail. We consider two models for percolation: *(i)* a ***homogeneous model*** according to which each product has n suppliers and suppliers fail i.i.d., and *(ii)* a ***heterogeneous model*** according to which each sector has a varying size (modeled by a heterogeneous number of suppliers) and supplier failures can be correlated.

For a high-level summary of managerial insights, see Section 3.6.

Emergence of Power Laws due to Cascading Failures (Section 3.3). To start with, we state that the size of cascading failures in a production network follows a power law when the underlying production network is a random directed acyclic graph (DAG) – representing a simple topological hierarchy among K ordered products whereby the production of more complex products is contingent on the supply of simpler products and raw materials. Our first result follows:

Informal Theorem 1. *Consider the production network of K products that is realized according to a random DAG model with edge probability p, and consider the node percolation model with failure probability x for each of the n suppliers of each product. Let F be the total number of products that cannot be produced due to the unavailability of their suppliers or other required products. Then F follows a power law distribution and admits a lower tail bound of $\mathbb{P}[F \geq f] \geq C/f$ for some constant $C > 0$ which depends on K, p, and x.*

Random DAGs provide a simple and clear representation of our resilience measure. These and other stylized models of production networks allow us to gain a foundational understanding before analyzing the resilience of real-world production networks (see, e.g., [422, 57]).

The Resilience Metric (Section 3.4). We study the drivers of resilience in several stylized models of production networks and identify resilient and non-resilient architectures. Recall that we use x to denote the probability of suppliers failing randomly. Consider a production network $\mathcal{G}$ with K products. Our notion of resilience, denoted by $R_{\mathcal{G}}(\varepsilon)$, determines the maximum value of x such that at least $(1-\varepsilon)$ fraction of the products in the production network $\mathcal{G}$ are produced with probability at least $1 - 1/K$. In particular, we are interested in the behavior of $R_{\mathcal{G}}(\varepsilon)$ for fixed ε as $K \to \infty$. For resilient production networks, this limit is bounded away from zero. We show that this asymptotic notion of resilience is non-trivial, as resilient and fragile families of networks both exist. In the sequel, we provide a non-asymptotic characterization of resilience, i.e., for a production network of finite size with a finite number of suppliers, suitable for analyzing real-world network architectures.

Topology	Is the Network Resilient?	Main Result	Resilience
Random DAG	No	Theorem 3.4.2	$O_\varepsilon\left(\left(\frac{1}{K}\right)^{1/n}\right)$
Parallel Products	Yes	Theorem 3.4.3	$\Omega_\varepsilon\left(\left(\frac{1}{\mu m}\right)^{1/n}\right)$
Backward network	No	Theorem 3.4.4 and Equation (3.4)	$O_\varepsilon\left(\left(\frac{m\log K}{K}\right)^{1/n}\right)$ for $m \geq 2$
	No		$O_\varepsilon\left(\left(\frac{1}{K}\right)^{1/n}\right)$ for $m = 1$
Forward network	Yes, with probability η^*	Theorem 3.4.5	See Theorem 3.4.5
Random Trellis	Yes, when $r = m = \mu = O(1)$	Informal Theorem 4	$\Omega_\varepsilon\left(\left(\frac{1}{r(1+p)}\right)^{2/n}\right)$
	No, when $K/r = o(K^{1/3})$		$O_\varepsilon\left(\left(\frac{1}{\sqrt{K}}\right)^{1/n}\right)$
Any Network $\mathcal{G}$	No if $r = \omega(K^{2/3})$	Theorem 3.4.7	$O_\varepsilon\left(\left(\frac{K}{r^{3/2}}\right)^{1/n}\right)$
	Yes, for μ, r, and c fixed		$\Omega_\varepsilon\left(\left(\frac{1}{(m+r)(\mu+c)}\right)^{1/n}\right)$

Table 3.1: Summary of Results for the Homogeneous Cascade Model (see Section 3.1 for the definition of parameters for each network). The notation $\Omega_\varepsilon(\cdot), O_\varepsilon(\cdot)$ suppresses the dependence on ε.

Characteristics of Fragile and Resilient Networks (Section 3.4). We characterize the resilience of networks based on their structural characteristics. We find that there are ***four unifying characteristics/global graph features that determine resilience***: *(i)* r: the number of raw products, which corresponds to the size of the primary sector; *(ii)* c: the number of final goods; *(iii)* m: the sourcing dependency, which is the maximum number of inputs a product sources from; and *(iv)* μ: the supply dependency, which is the maximum number of outputs a specific product supplies.

In the warm-up results, we study the resilience of stylized production networks that help demonstrate the interplay between these parameters. These structures and their parameterization are as follows.

1. *Random DAGs:* K products ordered as $1, 2, \ldots, K$ and connected with directed edge probability p that respects their ordering; see Section 3.3.2 and Figure 3.3(a).
2. *Parallel products with dependencies:* A set of r raw materials that are used to

produce $K - r$ final goods, each complex product requires m raw inputs (source dependencies), and each raw material is sourced by μ final goods (supply dependency); see Section 3.4.1 and Figure 3.3(b).

3. *Hierarchical production networks: (i) Backward hierarchical production network:* A tree production network with depth D and fanout $m \geq 1$, i.e., each product has m inputs independently of the other products. In this supply chain, the failures start from the raw materials we position at the tree's leaves, and the cascades grow from the leaves to the root (see Section 3.4.2 and Figure 3.4(a)), and *(ii) Forward hierarchical production network:* A tree production network generated by a branching process (also known as the Galton-Watson process) with branching distribution $\mathcal{D}$ with mean μ, which has (random) extinction time τ, and extinction probability $\eta^*(\mathcal{D}) = \mathbb{P}[\tau < \infty]$. In this regime, the percolation starts from the root node (raw material), and proceeds to the leaves (see Section 3.4.2 and Figure 3.4(b)).

Table 3.1 and Figure 3.1 summarize our results for the resilience of the above architectures and the corresponding theorems where the results are proved. Namely, we show:

Informal Theorem 2. *Random DAG, backward production network, and random trellis with $m \geq 1$ and constant width are always fragile with $R_{\mathcal{G}}(\varepsilon) \to 0$ as $K \to \infty$ for all ε. In contrast, parallel products with dependencies are resilient. The forward production network satisfies $\mathbb{P}[R_{\mathcal{G}}(\varepsilon) = 0] > 0$.*

In addition to identifying fragile architectures, our non-asymptotic analysis of $R_{\mathcal{G}}(\varepsilon)$ reveals how various factors such as the number of raw materials r,

the number of final goods c, and the sourcing dependency μ affect resilience. These nuances are fleshed out in Section 3.4, as we present our results for each architecture in Table 3.1. Specifically, we show:

Informal Theorem 3. *For any network $\mathcal{G}$, even $r > K^{2/3}$ raw products cause it to be fragile. In contrast, a network that has a fixed number of raw products r, source dependency m, supply dependency μ, and number of final goods c is always resilient.*

Intuitively, fragile networks look like "cowboy hats", and resilient networks look like "rolling pins" (cf. Figure 3.1). As a corollary of the previous result, we see that a trellis network with width r and $D = K/r$ tiers with random edges generated independently with probability p between tiers d and $d+1$ satisfies the following:

Informal Theorem 4. *If the trellis has $D = o(K^{1/3})$ tiers, then it is fragile with resilience that goes to zero at the rate $O_\varepsilon\left(\left(\frac{1}{\sqrt{K}}\right)^{1/n}\right)$ as $K \to \infty$. On the other hand, if the number of raw products and the edge probability for the trellis are fixed (r and p are both $O(1)$), then the trellis is resilient and its resilience can be lower bounded by $\Omega_\varepsilon\left(\left(\frac{1}{r(1+p)}\right)^{2/n}\right)$ as $K \to \infty$.*

Homogeneous Model with Inventory. In the sequel, we consider the capability of suppliers to hold inventories. In the simple case of the homogeneous model, if the suppliers of product i have enough stock of product j, then they drop the dependency of i to j with probability $1 - y$ where $y \in (0, 1)$ is a quantity related to the available inventory. The question comes to evaluating the cascade size when inventories are available. As a first remark, this is equivalent to decreasing the sourcing dependency from m to my.

However, if done with Monte Carlo methods, calculating the cascade size F_y in a network is #P-hard to compute [99, 71]. A way to efficiently estimate the size of the cascade $\mathbb{E}\left[F_y\right]$ is through linear programming (LP). Using the union bound, we bound the cascade size $\mathbb{E}\left[F_y\right]$ by a linear program that takes into account the failure probabilities x, the number of suppliers, the network structure, and the inventory (cf. Theorem 3.4.10). We show that if y is sufficiently small, then the cascade size is well approximated by a linear program:

Informal Theorem 5. *If $y = \varrho/m$ for some $\varrho \in (0, 1)$, then there exists an LP, whose optimal value $p^*_{\mathcal{G}}$ satisfies $\mathbb{E}\left[F_y\right] \leq p^*_{\mathcal{G}} \leq \left(1 + \varrho + O(\varrho^2)\right) \cdot \mathbb{E}\left[F_y\right]$.*

The linear program we give can be used to give an $(1 + \varrho + O(\varrho^2))$ approximation to the cascade size ($\mathbb{E}\left[F_y\right]$) which can be computed in almost linear time $\tilde{O}(K + M)$ for small infection probabilities $y = \varrho/m$ for $\varrho \in (0, 1)$. This matches the lower bound $\Omega(K + M)$ in runtime for maximum influence (up to logarithmic factors); see [71]. This constitutes a novel result and connection to the independent cascade literature, perhaps of independent interest, to the best of our knowledge.

Our LP resembles those used in the literature on systemic risk and financial contagion (see, e.g., [139, 179]), and it is also related to the literature on influence maximization [71, 236]. With the LP framework, we establish a promising connection between cascading failures in supply chains and financial contagion, as well as the independent cascade model. On the other hand, we show that if the inventory is small ($y > 1/m$), there exist instances where the LP can be as far away as an $\Omega(K)$ additive factor from $\mathbb{E}[F]$ (Appendix B.7). Moreover, the dual LP of $p^*_{\mathcal{G}}$ corresponds to a systemic risk measure, as axiomatized in [96] and subsequent works.

Finally, the LP formulation can be used to identify "vulnerable" products – i.e., products that are more likely to fail than others, and subsequently design interventions in supply chains (see Section 3.4.5) based on Katz centrality. We show that under certain assumptions, the probability that each node fails is related to its Katz centrality [231], which is consistent with the existing literature on financial networks [368, 45]. Furthermore, we establish a generic lower bound on $R_{\mathcal{G}}(\varepsilon)$ and an optimal intervention policy (under assumptions) as follows:

Informal Theorem 6. *1. For $y < 1/m$, $R_{\mathcal{G}}(\varepsilon) \geq \left(\frac{\varepsilon}{\mathbb{1}^T \beta_{\mathcal{G}}^{\text{Katz}}(y)}\right)^{1/n}$, where $\beta_{\mathcal{G}}^{\text{Katz}}(y) = (I - yA^T)^{-1}\mathbb{1}$ is the Katz centrality of $\mathcal{G}$.*

2. If a planner can protect up to T products, then the optimal intervention of the planner is to protect the T products in decreasing order of Katz centrality in $\mathcal{G}^R$, i.e., $\gamma_{\mathcal{G}}^{\text{Katz}}(y) = (I - yA)^{-1}\mathbb{1}$ for $0 < x < (1-\mu y)^{1/n}$. If $x \geq (1-\mu y)^{1/n}$ the optimization problem can be solved in poly-time via leveraging the Lovasz extension of $p_{\mathcal{G}}^*$ subject to the intervention constraints.

Therefore, with sufficiently large inventories ($y < 1/m$) and sufficiently small shocks ($x \geq (1 - \mu y)^{1/n}$), the Katz centrality of each node in the production network can inform the social planner's effort to design contagion mitigation strategies to improve supply chain resilience. In the latter case, our approximation algorithm leverages the LP's submodularity and cascade size approximation.

Connections to Risk Exposure Index (Section 3.4.6). To establish connections with existing measures of supply chain risk in the literature, we adopt the definition of Risk Exposure Index (REI) by [372] to our model. Accordingly, REI

for a product i is defined as the maximum potential impact of a given product (node), measured by the change (derivative) of the cascade size subject to a shock at node i. We show that

Informal Theorem 7. *Under reasonable assumptions, a network's REI is proportional to its nodes' highest Katz centrality.*

Empirical Results (Section 3.4.7). We experiment with real-world supply chain networks from [422] and the World Input-Output database from [390]. In the former case, the production networks are DAGs, whereas in the latter case, the networks correspond to countries' economies and can have cycles. We use Monte Carlo simulations to numerically determine the average resilience ($\widehat{R}_{\mathcal{G}}^{\text{avg}} = \int_0^1 \widehat{R}_{\mathcal{G}}(\varepsilon)d\varepsilon$) in the multi-echelon networks of [422], and show that the average resilience agrees with the derived upper bound of Theorem 3.4.7:

Observation 1. $\widehat{R}_{\mathcal{G}}^{\text{avg}} \propto \frac{K^{\alpha_1}}{r^{\beta_1}}$ *for some* $\alpha_1, \beta_1 > 0$ *empirically determined (p-values* < 0.01*) by regressing* $\widehat{R}_{\mathcal{G}}^{\text{avg}}$ *calculated from the supply chain data set of [422].*

We also relate the average REI, that is, $\text{REI}_{\mathcal{G}}^{\text{avg}} = \int_0^1 \text{REI}_{\mathcal{G}}(x)dx$, to $R_{\mathcal{G}}^{\text{avg}}$, m, and K using regression. We show:

Observation 2. *In the large inventory regime of Informal Theorems 5 and 6,* $\text{REI}_{\mathcal{G}}^{\text{avg}} \propto \frac{K^{\alpha_2} m^{\beta_2}}{(R_{\mathcal{G}}^{\text{avg}})^{\gamma_2}}$ *where* α_2, β_2, *and* $\gamma_2 > 0$ *are empirically determined (p-values* < 0.01*) using regression from values calculated in the supply chain data set of [422].*

Heterogeneous Model (Section 3.5). We generalize our analysis to a heterogeneous model, where each product has a different number of suppliers and supplier failures may be correlated. We generalize the definition of $R_{\mathcal{G}}(\varepsilon)$ as the

largest value x such that under the worst-case joint distribution of failures, ν, with the average number of failures upper bounded by x, at least $(1-\varepsilon)$ fraction of the products survive with probability at least $1/K$ over the supplier failures sampled from their joint distribution ν.

We give lower bounds by extending the aforementioned LP technique and, moreover, show how to have low-dimensional representations of the marginals of ν by leveraging the Bahadur representation [33], according to which we express the probability of failure of a product i as a function of higher-order correlations. This allows us to establish upper and lower bounds for resilience with correlations (Proposition 3.5.1). Finally, we empirically show how resilience is affected by correlations in real-world data sets of [422].

3.2 Related Work

We model the production network as a graph that undergoes a percolation process on its nodes, representing products. Each product has some suppliers, who, if they all fail, then the product cannot be produced. Subsequently, a cascade is caused by such a failure. Our modeling decision to study the supply network as a graph that undergoes percolation has its roots in previous work (see the referenced works in Appendix B.4); the most closely related is the work of [142].

Comparison with the results of [142]. [142] consider a *hierarchical production network* that undergoes a *link percolation process*. Specifically, firms are operational if all their inputs have operating links to at least one firm producing the specific inputs. [142] study the *reliability of the supply network* as the probability

that the root product is produced. They show that three important factors affect reliability: *(i)* the depth/size of the supply chain, *(ii)* the number of inputs that each product requires, and *(iii)* the number of suppliers (which corresponds to the ability of firms to multisource their required inputs). We investigate the effect of similar structural factors – i.e., topology, number of inputs, and number of suppliers – under a fundamentally expanded setup by *(i)* considering production shocks at the level of individual suppliers rather than links; *(ii)* considering more general architectures than the hierarchical production networks of [142], and *(iii)* studying a novel theory-informed resilience metric that guarantees that almost all products can be produced in the event of a supply chain shock. One of our main results shows that production networks are either resilient or fragile. [142] show that when the magnitude of the systemic shock is greater than some critical value, the reliability goes to zero, corresponding to *fragile* networks. When the magnitude of the shocks is below this critical value, the reliability attains a strictly positive value corresponding to the *resilient* networks. They observe that reliability increases with multisourcing (having many suppliers) and decreases with interdependency (requiring a multitude of inputs). Our analysis differs from [142]. It focuses on determining the largest possible shock that a network can withstand so that a significant fraction of products are produced (survive) in the event of such a shock as the size of the network increases. Our networks are similarly parametrized by size, multi-sourcing, and interdependency parameters. In agreement with [142], we show that networks become more resilient when multi-sourcing increases, and when interdependencies among products increase, networks become less resilient.

Our model and resilience metric complement the results of [142] as our metric, model, and results provide tools for studying any production network (in

contrast to the tree model presented in [142]). Moreover, we show two stronger premises for determining the resilience of supply chain networks with global features: Our first result says that *even a sublinear number of raw materials on any graph (not necessarily tree-like) can cause fragility*, which agrees and generalizes the observations on the tree model of [142]. Moreover, *spare networks with a few raw and final goods are resilient*, as our theory suggests, complementing their theory. In addition, we model the scenario where suppliers have inventories and show that under sufficient inventory capacity, the cascade size is closely connected to financial contagion models and experiences a phase transition. Specifically, we show that there is a critical value y_{crit} where for large enough inventories, which correspond to $y < y_{\text{crit}}$), the cascade can be well approximated by solving a linear program; however, above this critical threshold (i.e., $y > y_{\text{crit}}$), there are instances where approximating the cascade size becomes impossible. Conceptually, this phase transition is complementary to the phase transition of [142], as y would be related to their notion of the strength of the relationship between suppliers. In contrast, our results focus on characterizing the maximum shock probability (resilience) by approximating the cascade size via an LP.

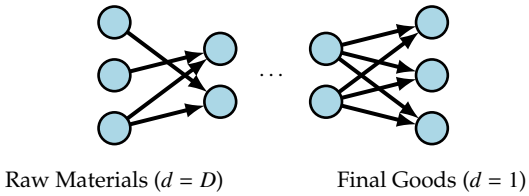
We observe that certain types of networks are resilient, i.e., they can withstand sufficiently large shocks without experiencing catastrophic cascading failures, and others are fragile, i.e., non-trivial shocks are enough to render a significant proportion of their products unproducible. We provide additional evidence in the form of the emergence of power laws for the size of cascading failures, which further motivates the study of resilience in complex production networks. Compared to existing indices that combine many temporal, financial, and economic risk factors [167], our resilience metric identifies topological risk factors and focuses on cascading failures to identify fragile and resilient sup-

ply chain architectures. [334] systematically reviews the literature on modeling the topology and robustness of production networks with applications to real-world data. Their first observation is that many real-world production networks follow a power-law degree distribution with an exponent of around two.

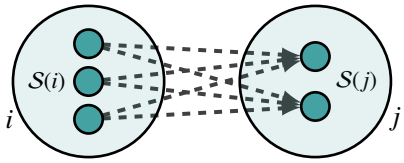
Moreover, the resilience (called "robustness" in their work) of such networks is defined as the size of the largest connected component or the average/max path length in the presence of random failures. In contrast, we propose a novel, theory-informed resilience metric that complements the existing measures in [334] and references therein and supplement their empirical work with novel theories about how topological attributes contribute to the increased risk of cascading failures in production networks. We also test our proposed metric on real-world data and provide empirical insights comparable to [334]. Finally, we propose interventions to improve resilience with theoretical guarantees similar to optimal allocations in the presence of shocks and financial risk contagion [139, 322, 62, 149, 57], and complementary to other supply chain interventions that, for example, increase visibility and traceability [59], or design optimal investments [98]. Appendix B.4 provides an extensive review of the literature.

3.3 The Production Network

We start by describing the production network (see Figure 3.2(a) for an example production network). We consider the production of a set of products $\mathcal{K}$ with cardinality $|\mathcal{K}| = K$ where each product $i \in \mathcal{K}$ can be produced by a number of suppliers and also requires certain inputs to be produced. Specifically, each product $i \in \mathcal{K}$ has a set of requirements (inputs), denoted by $\mathcal{N}(i)$ that it needs



(a) Production Network



(b) Supply Chain Network Between Two Products

Figure 3.2: Supply Chain Instance. Each node in the production network of Figure 3.2(a) has a supplier set. The supply chain network between two products is shown in Figure 3.2(b).

in order to be made. The products and the set of requirements for each product define *production network* $\mathcal{G}(\mathcal{K}, \mathcal{E})$. The production network is also associated with the adjacency matrix A and the cardinality of the edges is $M = |\mathcal{E}|$.

The production network $\mathcal{G}$ starts with *raw materials* (or sources), which are materials that do not require any input, that is, they have $|\mathcal{N}(i)| = 0$ and are the "initial products" that are used in the production of others. We denote the set of raw materials (or primary sector), which corresponds to products that do not have input, by $\mathcal{R}$ and its cardinality by $|\mathcal{R}| = r$. We use $\mathcal{C}$ to denote the set of final goods (or final sector), which corresponds to products that do not have output, and use $c = |\mathcal{C}|$ to denote their cardinality. Each product $i \in \mathcal{K}$ can be sourced from a set of suppliers $\mathcal{S}(i)$. We assume that a supplier of a product can source from any of the suppliers of the products on which it depends.

We define the sourcing dependency m of $\mathcal{G}$ as the maximum in-degree of any product, and the supply dependency μ of $\mathcal{G}$ as the maximum out-degree of any product. If $\mathcal{G}$ is random, m and μ are defined to be the corresponding expected

in/out-degrees.

Associated with the production network $\mathcal{G}$, we can also define a supply chain network by focusing on the supply relations between the suppliers of different products (cf. Figure 3.2(b)). The supply chain network $\mathcal{H}$ is defined as a graph with vertex set $\mathcal{V}(\mathcal{H}) = \bigcup_{i\in\mathcal{K}} \mathcal{S}(i)$ and edge set $\mathcal{E}(\mathcal{H}) = \bigcup_{i\in\mathcal{K}} \bigcup_{j\in\mathcal{N}(i)} \mathcal{B}(\mathcal{S}(i), \mathcal{S}(j))$, where $\mathcal{B}(\mathcal{S}(i), \mathcal{S}(j))$ is the complete bipartite graph between $\mathcal{S}(i)$ and $\mathcal{S}(j)$.

Example. Assume a simple network that produces

$$\mathcal{K} = \{\text{engines}, \text{bolts}, \text{screws}\}.$$

We have, e.g.,

$$\mathcal{N}(\text{engines}) = \{\text{bolts}, \text{screws}\}$$

and

$$\mathcal{S}(\text{engines}) = \{\text{BMW}, \text{General Motors}\},$$

and suppliers for the screws and bolts.

We use $[K]$ to denote the set $\{1, \ldots, K\}$. For vectors (resp. matrices), we use $\|v\|_p$ (resp. $\|V\|_p$) for the p-norm of v (resp. for the induced p-norm); for the Euclidean norm (i.e., $p = 2$), we omit the subscript. 0 (resp. $\mathbb{1}$) denotes the column vector of all zeros (resp. all ones) and $\mathbb{1}_S$ represents the column vector indicator of the set S. We use $x \wedge y$ (resp. $x \vee y$) as shorthand for the coordinate-wise minimum (resp. maximum) of the vectors x and y. Finally, order relations $\geq$, $\leq$, $>$, $<$ denote coordinate-wise ordering. We use $\mathcal{G}^R$ to denote the edge-reversed graph of $\mathcal{G}$, i.e., the graph which has the same vertex set as $\mathcal{G}$ and reversed edges. In our context, $\mathcal{G}$ corresponds to the graph of supply relations and $\mathcal{G}^R$

corresponds to the graph of source relations. The notation $x_n \asymp y_n$ means that $\lim_{n\to\infty} \frac{x_n}{y_n} = 1$.

3.3.1 Node Percolation in the Homogeneous Model

For most of the theoretical results of this Chapter, we focus on the homogeneous failure model for simplicity of exposition. The **homogeneous** model assumes that all nodes have the *same number of suppliers* and all products *fail independently* of each other with the same probability. Later in the paper (see Section 3.5), we introduce the **heterogeneous** model, which assumes that failures *can be correlated with each other*, as well as each product, can have a different number of suppliers.

According to the homogeneous model, each product i has a *constant* number of suppliers that is equal to n. The supply chain graph $\mathcal{G}$ undergoes a node percolation process in which each supplier fails independently at random with probability $x \in (0, 1)$. Each product can be produced if, and only if, *(i)* all of its requirements $j \in \mathcal{N}(i)$ can be produced, and, *(ii)* at least one of the suppliers $s \in \mathcal{S}(i)$ is operational. Upon completion of the percolation process, a random number F of products fails, and the remaining $S = K - F$ products survive. The number of surviving products can be expressed as $S = \sum_{i\in\mathcal{K}} Z_i$ where $\{Z_i\}_{i\in\mathcal{K}}$ are the indicator variables that equal to one if, and only if, product i is produced and are zero otherwise. The sequence of variables $\{Z_i\}_{i\in\mathcal{K}}$ obeys the following random system of equations (or dynamics) for every $i \in \mathcal{K}$:

$$Z_i = \prod_{j\in\mathcal{N}(i)} Z_j \left(1 - \prod_{s\in\mathcal{S}(i)} X_{is}\right), \tag{3.1}$$

where $X_{is} \overset{\text{i.i.d.}}{\sim} \text{Be}(x)$ correspond to the indicator variables that equal to 1 if supplier $s \in \mathcal{S}(i)$ of product $i \in \mathcal{K}$ has spontaneously failed. Our paper aims to study the random behavior of F (resp. S). A planner is interested in finding the maximum probability value x such that the number of failures is at most εK (e.g., sublinear) with high probability. We show that some very simple production networks can experience power-law cascades to motivate such a resilience metric.

3.3.2 Motivation for a resilience metric: cascading failures and the emergence of power laws in random DAG structures

We start by motivating the need for the definition of a resilience measure for supply chain graphs. More specifically, similar to large social networks [265, 420] and power networks [128, 129, 304], we show that a randomly generated supply chain with random DAG structure exhibits cascade sizes that obey a power law, namely the average cascade size is dominated by a few very large cascades rather than the many smaller ones. Our motivation comes from the literature on network science and social networks literature in accordance with the literature that uses network science ideas to introduce and study supply chain concepts (see, e.g., [70, 24, 334]).

In a supply chain, we can assume that there is a "natural order" among the products being produced; namely, producing more complex products is contingent on the supply of simpler products. In a supply chain, raw materials and component parts are typically transformed into intermediate products and finished products through a series of production processes. The production of

more complex products often depends on the availability of simpler products, as the simpler products are used as inputs in the production of the more complex products. For example, in the production of a car, the production of the car's engine may depend on the availability of simpler components, such as computer chips. In its simplest form, this behavior can be captured by a random DAG model, where a DAG is created by independently sampling edges via coin tosses. We also want to emphasize that the random DAG model has a significantly different structure from the Erdös-Rényi random graph, which allows the study of cascading behavior.

To observe this, we start with the random DAG model $\mathsf{rdag}(K, p)$ described in the work of [420]. More specifically, we consider a supply chain with K products $1, \ldots, K$ connected as follows: for every $k \in [K]$ and for every $1 \leq l \leq k-1$ we add a directed edge (l, k) independently, with probability $p \in (0, 1)$. Figure 3.3(a) shows the creation of a $\mathsf{rdag}(K, p)$ with probability p and $K = 3$ vertices.

The percolation process occurs as described in Section 3.3.1. The following theorem determines the distribution of the failure cascade size F and shows that it grows at least as a power law with exponent one. Our proof in Appendix B.2.1 follows arguments similar to those made by [420].

Theorem 3.3.1. *Let $\mathcal{G} \sim \mathsf{rdag}(K, p)$ be the production network of K products that is realized according to a random DAG model, and consider the node percolation model with failure probability x on the supplier graph associated with the production network $\mathcal{G}$. Then $\mathbb{P}[F = f] \asymp \frac{x^n}{K(1-(1-x^n)(1-p)^f)} \geq \frac{C(K,p,x,n)}{f}$ where $C(K, p, x, n) > 0$ is a constant dependent on K, p, and x for large enough K.*

The above result implies that F has a tail lower bound, i.e., $\mathbb{P}[F \geq f] \geq C/f$. Having proven Theorem 3.3.1, the next question is: *How can we calculate the*

probability that a fractional cascade emerges? Conceptually, if the probability of a fractional cascade emerging is $O(1/K)$ for some choice of the percolation probability x, then, with a high probability, we will have the majority of products survive. To quantify this phenomenon, we can first calculate $\mathbb{P}[F \geq \varepsilon K]$ for a fixed fraction $\varepsilon \in (0, 1)$. A simple calculation shows that, for large enough K,

$$\mathbb{P}[F \geq \varepsilon K] \asymp x^n \left[1 - \varepsilon + \frac{1}{K \log\left(\frac{1}{1-p}\right)} \log\left(\frac{1 - (1 - x^n)(1-p)^K}{1 - (1-x^n)(1-p)^{\varepsilon K}} \right) \right] = g(x, K, p, \varepsilon, n). \tag{3.2}$$

We want to find values of x such that for every $\varepsilon \in (0, 1)$, the probability that a cascade of size at least εK emerges goes to zero as $K \to \infty$. Note that as $K \to \infty$ we have $\frac{1}{K \log\left(\frac{1}{1-p}\right)} \log\left(\frac{1-(1-x^n)(1-p)^K}{1-(1-x^n)(1-p)^{\varepsilon K}} \right) \to 0$ and therefore $\mathbb{P}[F \geq \varepsilon K] \to x^n(1 - \varepsilon)$. In order to make this zero for every $\varepsilon \in (0, 1)$, we should set $x \to 0$. In Appendix B.1, we give an analytical bound on x to ensure $\mathbb{P}[F \geq \varepsilon K] = O(1/K)$.

The above calculation shows that for a large random DAG, it is impossible to have a $(1 - \varepsilon)$-fraction of the products that survive for any non-zero percolation probability x. Therefore, we could, on a high level, characterize the random DAG as a *"fragile"* architecture, because even the tiniest shock can be devastating for the production network.

Identifying fragile supply chains is important, as it allows companies and organizations to identify potential vulnerabilities and risks in their supply chain operations. This can then be used to design more robust supply chains through targeted interventions. Thus, once fragile supply chains are identified, companies can take a number of steps to make them more robust, such as diversifying their supplier base, increasing inventory levels, and implementing contingency plans.

3.4 Resilience in the Homogeneous Model

The emergence of power laws for cascading failures in supply chain graphs, as we show in Theorem 3.3.1, indicates the need to define a resilience metric. It is important to have a suitable resilience metric to understand the behavior of complex systems and identify potential vulnerabilities. There are many different ways to define and measure resilience, and which metric is most appropriate will depend on the specific system being studied and the goals of the analysis. Some common approaches to defining resilience include looking at the system's ability to recover from disturbances, absorb or adapt to change, and maintain function in the face of stress or disruption.

In our percolation model, ideally, a "more resilient" network is a network that can withstand larger shocks, which are associated with larger percolation probabilities x. Therefore, it is natural to assume that in a resilient network, we want to find the maximum value that the percolation probability x can get in order for a "large" fraction of the items to survive almost surely. Formally, for $\varepsilon \in (0,1)$, the *resilience* of a product graph (possibly random) $\mathcal{G}$ is defined as follows.

$$R_{\mathcal{G}}(\varepsilon) = \sup\left\{x \in (0,1) : \mathbb{P}_{\mathcal{G},x}[S \geq (1-\varepsilon)K] \geq 1 - \frac{1}{K}\right\}, \tag{3.3}$$

$R_{\mathcal{G}}(\varepsilon)$ corresponds to the maximum percolation probability for which, at most εK products fail with a probability at least $1 - 1/K$ that increases to one as $K \to \infty$. The expectation $\mathbb{E}_{\mathcal{G}}[\cdot]$ corresponds to the randomness of the graph generation process and the probability $\mathbb{P}_{\mathcal{G},x}[\cdot]$ corresponds to the joint randomness of the percolation and the edges of the graph. In the case of $\mathsf{rdag}(K,p)$, our

lower bound on x in Appendix B.1 to ensure $\mathbb{P}[F \geq \varepsilon K] = O(1/K)$ is also a lower bound on the resilience for this particular architecture.

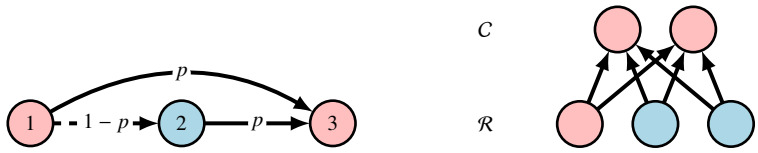
We make a distinction between the following two classes of networks:

Definition 3.4.1. A family of production networks $\mathcal{G}$ indexed by their number of products K, is **resilient** iff $\lim_{K\to\infty} R_{\mathcal{G}}(\varepsilon) > 0$ for any fixed $\varepsilon \in (0,1)$, and it is **fragile** iff $\lim_{K\to\infty} R_{\mathcal{G}}(\varepsilon) = 0$ for any fixed $\varepsilon \in (0,1)$.

That is, the former type of architecture can be characterized as *fragile architecture* since even the smallest failure can devastate the network. The latter can be characterized as *resilient architecture* since it can withstand non-trivial shocks in the limit of $K \to \infty$.

Similarly to existing approaches in random graph theory (cf. [64]), we consider the case where the number of products is large as a means to represent an arbitrarily complex economy. However, we want to note that our results are non-asymptotic, which makes them suitable for real-world supply chains.

In the sequel, we study a variety of network architectures and derive lower bounds for the resilience of such supply chain architectures. Table 3.1 summarizes our results. Briefly, to prove that a supply chain $\mathcal{G}$ is resilient, it suffices to choose some lower bound percolation probability $\underline{R}_{\mathcal{G}}(\varepsilon) \in (0,1)$ such that $\mathbb{P}_{x=\underline{R}_{\mathcal{G}}(\varepsilon)}[F \geq \varepsilon K] = O(1/K)$ and prove that, which implies that $\lim_{K\to\infty} R_{\mathcal{G}}(\varepsilon) > 0$ since $R_{\mathcal{G}}(\varepsilon) \geq \underline{R}_{\mathcal{G}}(\varepsilon)$. Moreover, to prove that architecture is fragile, we prove an upper bound $\overline{R}_{\mathcal{G}}(\varepsilon) \in (0,1)$ on the resilience that goes to 0 as $K \to \infty$. To derive upper bounds, we can use the following lemma, whose proof is deferred to Appendix B.2.2. The constant 1/2 in the following lemma is arbitrary and the proof works for any constant $\theta \in (0,1)$.



(a) rdag($K = 3, p$) (b) Parallel Products ($\mu = 2, m = 3$).

Figure 3.3: Production networks of Section 3.3.2 and Section 3.4.1. Failures are drawn in pink color.

Lemma 3.4.1. *Let $\varepsilon \in (0,1)$ and let $\overline{R}_{\mathcal{G}}(\varepsilon) \in (0,1)$ be a percolation probability such that $\mathbb{P}_{x=\overline{R}_{\mathcal{G}}(\varepsilon)}[S \geq (1-\varepsilon)K] \leq \frac{1}{2}$. Then, for $K \geq 3$, we have $R_{\mathcal{G}}(\varepsilon) < \overline{R}_{\mathcal{G}}(\varepsilon)$.*

As a warm-up, the analysis of Section 3.3.2 shows that rdag(K, p) is a fragile architecture, and therefore we get our first theorem.

Theorem 3.4.2. *Let $\mathcal{G} \sim$ rdag(K, p). Then, as $K \to \infty$, we have $R_{\mathcal{G}}(\varepsilon) \to 0$.*

In the next sections, we study various architectures and derive upper and lower bounds of $R_{\mathcal{G}}(\varepsilon)$.

3.4.1 Parallel Products with Dependencies

The first architecture we study is parallel products (cf. [57, 422] for related works that motivate this architecture). Here, our objective is to produce a set C of final goods and each requires m inputs (raw materials; source dependencies). We also introduce supply dependencies among raw materials, assuming that each raw material can supply μ products. Figure 3.3(b) shows an example of this supply chain together with an instance of the percolation process (the affected nodes are drawn in pink). Here, it is interesting to study both the resilience of the whole graph, i.e., the graph with vertex set $C \cup \mathcal{R}$, as well as the resilience of the

final goods C alone. We show that if the source dependency m and the supply dependency μ between the products are independent of K, then the production network is resilient. The resilience metric is lower bounded by $\left(\frac{\varepsilon}{2(\mu+1)m}\right)^{1/n}$ in both cases (final goods alone or together with raw materials), as the number of products goes to infinity. Moreover, if the number of inputs m goes to infinity, the resilience goes to 0 at rate $O\left(e^{-\frac{1}{mn}}\right)$, Formally, we prove the following for the resilience of the parallel products (proved in Appendix 3.4.3):

Theorem 3.4.3. *Let $\mathcal{G}$ consist of parallel products with c final goods and assume that r raw materials can produce these products, and each raw material supplies at most μ final goods, and each final good requires at most m raw products. Then, the resilience of the final goods C (which corresponds to the highest probability that at least $(1-\varepsilon)c$ final products survive) satisfies: $\left(\frac{\varepsilon}{\mu m}+\sqrt{\frac{\log K}{2mK}}\right)^{1/n} \leq R_C(\varepsilon) \leq \left(1-\left(\frac{1-\varepsilon}{2}\right)^{1/m}\right)^{1/n}$. In addition, the resilience of all products (final and raw) satisfies $\left(\frac{\varepsilon}{2(\mu+1)m}+\sqrt{\frac{\log(K/2)}{2mK}}\right)^{1/n} \leq R_{\mathcal{G}}(\varepsilon) \leq \left(1-\frac{1-\varepsilon}{2(m+1)}\right)^{1/n}$. Subsequently, if ε, μ and m are independent of K, then the resilience is $\Omega\left(\left(\frac{\varepsilon}{\mu m}\right)^{1/n}\right)$ and the network is resilient.*

3.4.2 Hierarchical Production Networks

A supply chain can be organized hierarchically, with different levels representing different stages of the production process. The raw materials or components that go into the production of a product are at the bottom of the hierarchy, and the finished product is at the top. Each level of the hierarchy represents a stage of production in which materials or components are transformed into a more advanced or finished product [142]. This hierarchical structure helps visualize the flow of materials and information throughout the supply chain and identify potential bottlenecks or inefficiencies. Moreover, another possible hierarchy is

to produce final goods from a source of raw products. In this section, we study these two hierarchies, which we call *backward* and *forward* (referring to the directions of percolation with respect to network growth), production networks visualized in Figure 3.4. More specifically, we consider:

- The *backward production network* (Figure 3.4(a)) at which the tree grows from the root, and then the percolation starts from the leaves and proceeds to the root. For the scope of this Chapter, we study backward percolation in deterministic m-ary trees. In Section 3.4.2 we prove that, as expected, such supply chains are, in fact, fragile and give lower bounds on resilience.
- The *forward production network* (Figure 3.4(b)) at which the tree grows from the root, and then the percolation starts from the root and proceeds to the leaves. Here, the production network is generated by a stochastic *branching process*; the Galton-Watson (GW) process. In Section 3.4.2, we prove that, under specific conditions, such supply chains are fragile with a non-negative probability and are otherwise resilient.

Backward Production Network

In the case of the backward production network, we consider an m-ary tree with height D and fanout $m \geq 1$. The levels of the tree correspond to the "tiers" with raw materials placed in the tier D and more complicated products placed in higher tiers. Each product has n potential suppliers, and each product in the tier $d \in [D-1]$ has exactly $|\mathcal{N}(i)| = m$ inputs from the tier $d+1$. Tier $d = D$, which corresponds to the raw products, has no inputs. Figure 3.4(a) shows how the percolation process evolves in a tree with $m = 2$ and $D = 3$, where failures

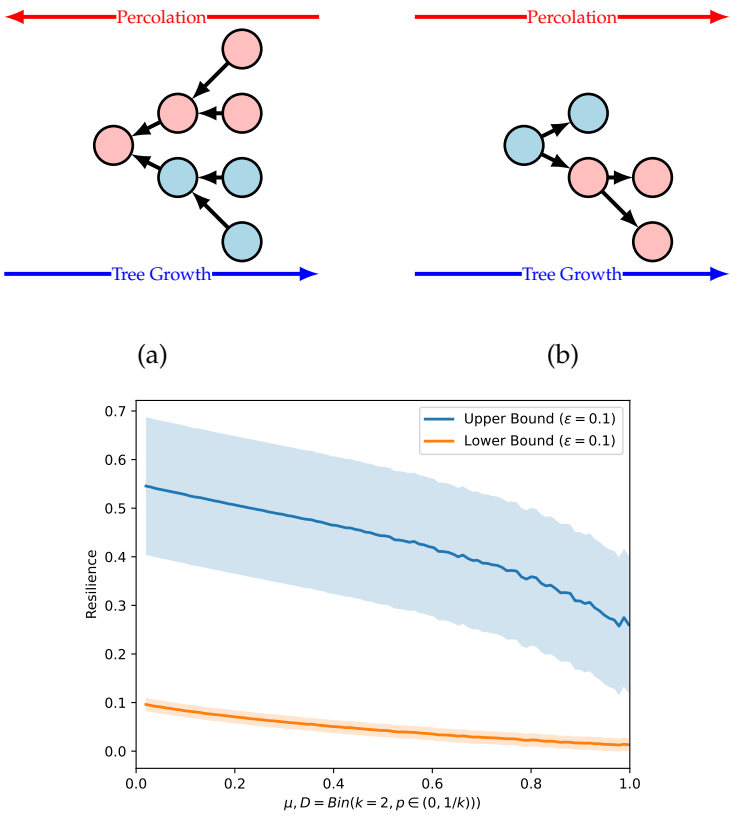


Figure 3.4: (a, b): Backward and Forward Networks. Node failures are drawn in pink. (c): Resilience bounds for a subcritical GW process with branching distribution as a function of μ; note the decreasing trends in both upper and lower bounds, $\mathbb{E}_{\mathcal{G}}\left[\overline{R}_{\mathcal{G}}(\varepsilon)\right]$ and $\mathbb{E}_{\mathcal{G}}\left[\underline{R}_{\mathcal{G}}(\varepsilon)\right]$, with increasing μ.

(drawn in pink) propagate from the two faulty raw materials to the root.

In addition to the power law result (Theorem 3.3.1), the case of the m-ary tree is another example that motivates the resiliency measure $R_{\mathcal{G}}(\varepsilon)$. Specifically, let us think about the probability of a catastrophic failure in a tree, that is, one that affects a substantial proportion of the suppliers in the production network. A raw material failing to be produced can cause its parent product not to be produced and inductively create a cascade up to the root. The complete cascade will start from the failed product in tier $D-1$ since some products in tier $D-1$

may be made if their corresponding raw materials are produced. However, no product can be produced from tier $D-2$ onward. As a result, only $o(K)$ products survive. The probability of such an event equals:

$$\mathbb{P}[S = o(K)] \geq \mathbb{P}[\geq 1 \text{ raw material malfunctions}] = 1 - (1 - x^n)^{m^{D-1}} \geq 1 - e^{-x^n m^{D-1}}. \tag{3.4}$$

It is easy to see that if $x = \Omega\left((m \log K/K)^{1/n}\right)$, then a catastrophe occurs with a high probability in the tree structure, meaning that failure probabilities as small as $(m \log K/K)^{1/n} + o(1)$ can cause catastrophes with probability approaching one (and therefore the backward hierarchical production network is a fragile architecture). Therefore, it is interesting to study cases where such a scenario does not happen; on the contrary, we have many products that survive. The following theorem formalizes the lower bounds and provides an additional upper bound for the resilience of the backward production network (proved in Appendix B.2.4).

Theorem 3.4.4. *Let $\mathcal{G}$ be a backward production network with fanout m and depth D. Then,*

$$\left[1 - \left(1 - \frac{1}{K}\right)^{\frac{1}{(1-\varepsilon)K}}\right]^{1/n} \leq R_{\mathcal{G}}(\varepsilon) \leq \begin{cases} \left(\frac{2}{K(1-\varepsilon)}\right)^{1/n} = \left(\frac{2}{D(1-\varepsilon)}\right)^{1/n}, & m = 1 \\ \left(\frac{(1-\varepsilon)\log m}{\log K}\right)^{1/n} \asymp \left(\frac{(1-\varepsilon)}{D}\right)^{1/n}, & m \geq 2 \end{cases}. \tag{3.5}$$

Therefore, the network is fragile.

Upper Bound Comparison. Since $\varepsilon \in (0,1)$ the above quantity behaves asymptotically as $O\left(\left(\frac{\log m}{\log K}\right)^{1/n}\right)$ for all values of ε. Therefore, the resilience goes to 0 with rate $\log K$. However, note that in Equation (3.4), we showed a better rate of $O\left(\left(\frac{m \log K}{K}\right)^{1/n}\right)$, and therefore we state that the resilience goes to 0 with a rate of $O\left(\left(\frac{m \log K}{K}\right)^{1/n}\right)$ (for $m \geq 2$).

Forward Production Network

We consider a random hierarchical network in which the products at each level D are denoted by $\mathcal{K}_d$. Starting from one raw material, we branch out through a Galton-Watson (GW) process such that every product $i \in \mathcal{K}_d$ at the level $d \geq 1$ creates $\xi_i^{(d)}$ supply dependencies, where $\{\xi_i^{(d)}\}_{i\in\mathcal{K}_d, d\geq 0}$ are generated i.i.d. from a distribution $\mathcal{D}$, with mean $\mathbb{E}_{\mathcal{D}}\left[\xi_i^{(d)}\right] = \mu > 0$. Subsequently, the number of products at each level obeys

$$|\mathcal{K}_{d+1}| = \begin{cases} \sum_{i\in\mathcal{K}_d} \xi_i^{(d)}, & d \geq 2 \\ 1 & d = 1 \end{cases}. \tag{3.6}$$

Adding the node percolation process, we start a percolation of the children of the root node r and subsequently proceed to their children, etc. The number of the surviving products S in this case can be expressed as $S = \sum_{d:|\mathcal{K}_d|\geq 1} \sigma_d$, where $\{\sigma_d\}_{d\geq 0}$ follow another branching process, namely

$$\sigma_{d+1} = \begin{cases} \sum_{1\leq i\leq \sigma_d} \xi_i^{(d)} \left(1 - \prod_{s\in\mathcal{S}(i)} X_{is}\right), & d \geq 2 \\ 1 - \prod_{s\in\mathcal{S}(r)} X_{rs} & d = 1 \end{cases}. \tag{3.7}$$

In Figure 3.4(b), we show such an example in which failures propagate from the raw product to products of increasing complexity. In the case of the GW process, the network has a random number of nodes K. For this reason, to characterize resilience and fragility, instead, we focus on quantities $\mathbb{P}_K[R_{\mathcal{G}}(\varepsilon) = 0]$. We generalize the definition of resilience as follows.

Definition 3.4.2. A network $\mathcal{G}$ is q-resilient for some $q \in (0, 1)$ if and only if $\mathbb{P}_K[R_{\mathcal{G}}(\varepsilon) = 0] \leq 1 - q$.

Theorem 3.4.5. *Let $\mathcal{G}$ be generated by a GW process in which the number of children of each node is generated by a distribution $\mathcal{D}$ with mean $\mu > 0$ and extinction time τ. Let $G_{\mathcal{D}}(\eta) = \mathbb{E}_{\xi\sim\mathcal{D}}\left[e^{s\xi}\right]$ be the moment generating function of $\mathcal{D}$, and let $\mathbb{P}[\tau < \infty] = \eta^* = \inf\{\eta \in [0,1] : G_{\mathcal{D}}(\eta) = \eta\}$ be the extinction probability of the GW process. Then the following are true:* (i) *If $\mu < 1$, then $\mathcal{G}$ is 1-resilient,* (ii) *If $\mu(1-x^n) > 1$, then $\mathcal{G}$ is η^*-resilient.*

Moreover, the expected upper bound on the resilience is, for $\mu \in (0,1) \cup (e^2, \infty)$, given by $\mathbb{E}_{\mathcal{G}}\left[\overline{R}_{\mathcal{G}}(\varepsilon)\right] = \sum_{1\le k<\infty} \mathbb{P}[\tau = k]\overline{x}(\mu,\tau,\varepsilon)$ with

$$\overline{x}(\mu,\tau,\varepsilon) = \inf\left\{x \in \left[0, \mathbb{1}\{\mu<1\} + \left(1-\frac{1}{\mu}\right)^{1/n}\mathbb{1}\{\mu>1\}\right] : (1-x^n)\frac{\mu^\tau(1-x^n)^\tau - 1}{\mu(1-x^n)-1} \le \frac{1-\varepsilon}{2}\frac{\mu^\tau - 1}{\mu - 1}\right\}. \tag{3.8}$$

The expected lower bound on the resilience is, for $\mu \in (0,1) \cup (e, \infty)$, given by $\mathbb{E}_{\mathcal{G}}\left[\underline{R}_{\mathcal{G}}(\varepsilon)\right] = \sum_{1\le k<\infty} \mathbb{P}[\tau = k]\underline{x}(\mu,\tau,\varepsilon)$ with

$$\underline{x}(\mu,\tau,\varepsilon) = \sup\left\{x \in \left[0, \mathbb{1}\{\mu<1\} + \left(1-\frac{1}{\mu}\right)^{1/n}\mathbb{1}\{\mu>1\}\right] : \frac{\mu^\tau - 1}{\mu - 1} - (1-x^n)\frac{\mu^\tau(1-x^n)^\tau - 1}{\mu(1-x^n)-1} \le \varepsilon\right\}. \tag{3.9}$$

Applying Theorem 3.4.5 for the case where $\mathcal{D}$ is a point-mass function that equals μ with probability 1, yields the following corollary for deterministic structures.

Corollary 3.4.6. *Let $\mathcal{D}$ have $\mathbb{P}_{\xi\sim\mathcal{D}}[\xi = \mu] = 1$ for $\mu > 1$. Then $\mathcal{G}$ is 0-resilient.*

For the subcritical regime, we plot the expected resilience bounds in Figure 3.4(c) for a subcritical GW process with branching distribution $\mathcal{D} = \mathsf{Bin}(k, p \in (0, 1/k))$, as a function of $\mu = kp$.

We want to remark here that the work of [142] considers a hierarchical supply network similar to the one presented in Section 3.4.2 – though by assuming a

different percolation process. In Section II of their paper, they observe that their reliability metric decreases as the interdependency increases, and the reliability increases as the number of suppliers increases. This is in agreement with the lower bound presented in Theorem 3.4.4 for the backward production network, which increases as n increases and decreases as m increases, the probability that there is at least a raw material failure (Equation (3.4)) increases. Moreover, in their paper, if the shocks are below a value, then for large depths, the reliability goes to zero, which is conceptually in agreement with the upper bounds presented in Theorem 3.4.4, which go to zero as D grows. Finally, for the forward production network – which is not studied by [142] – we again get a result that is in agreement with their results, since as the average interdependency μ increases, we observe that the upper and lower bounds in the resilience decrease, as empirically shown in Figure 3.4(c).

3.4.3 Bounding the Resilience with Global Graph Features

The next series of results focuses on deriving bounds for any network $\mathcal{G}$ using global graph features. Specifically, the global graph features governing the bounds are the source dependency (m), the supply dependency (μ), the number of raw products (r) and the number of final goods (c). We present the bound (proved in Appendix B.2.7):

Theorem 3.4.7. *For any network $\mathcal{G}$, the resilience satisfies*

$$\left(\frac{\varepsilon}{2(m+r)(\mu+c)} + \sqrt{\frac{\log K}{rK}}\right)^{1/n} \leq R_{\mathcal{G}}(\varepsilon) \leq \left[\frac{(1-\varepsilon)K}{\sqrt{2}r^{3/2} + \sqrt{r\log K}}\right]^{1/n}.$$

Thus, if $r = \omega(K^{2/3})$, then the network is fragile. Moreover, if r, c, μ are fixed, the network is resilient.

On the one hand, the consequence of Theorem 3.4.7, which characterizes the upper bound of resilience, is that, in general, production networks with a lot of raw products are fragile. For example, the tree model of Section 3.4.2 satisfies the above condition and is indeed fragile, as we analytically show in Theorem 3.4.4. The inverse dependence of resilience on the number of raw products is also empirically verified by regression with empirical resilience values calculated on real-world supply chain data sets in Table 3.2. Theorem 3.4.7 gives a slower decay rate of $O_\varepsilon\left(m^{-\ln n/2}\right)$. As a corollary of Theorem 3.4.7, we see that a trellis network with width r and $D = K/r$ tiers with random edges generated independently with probability p between tiers d and $d+1$ satisfies the following:

Corollary 3.4.8. *If the trellis has $D = o(K^{1/3})$ tiers, then $R_{\mathcal{G}}(\varepsilon) = O_\varepsilon\left(\left(\frac{1}{\sqrt{K}}\right)^{1/n}\right)$. Moreover, if a trellis has $r = p = O(1)$, then $R_{\mathcal{G}}(\varepsilon) = \Omega_\varepsilon\left(\left(\frac{1}{r(1+p)}\right)^{2/n}\right)$.*

3.4.4 Techniques for General Production Networks

So far, we have focused our attention on simple structures where we can find analytical expressions for $\mathbb{E}[F]$, and, subsequently, by bounding $\mathbb{E}[F]$ we can determine the upper and / or lower bounds for $R_{\mathcal{G}}(\varepsilon)$. However, in more general cases, $\mathcal{G}$ may have a more complicated structure for which we want to calculate the resilience, and in general, $\mathbb{E}[F]$ is #P-hard to compute; cf. [99].Moreover, it is certainly possible for a production network to have cycles, e.g., when complex products are used in the production of simpler products. It is also possible that production networks have cycles that represent recycling or other forms

of circular flows of materials or resources in modern economies; cf. circular economies [172]. In this section, we offer techniques to address the following questions for general network topologies:

1. *How do we efficiently calculate the cascade size F?*
2. *How do we identify network vulnerabilities in the failure of their most critical nodes?*
3. *How can we design interventions to minimize the (expected) size of failure cascades?*

As expected, production networks are most vulnerable to failure of their most "central" nodes, to which many of their products have (potentially higher order) connections. In fact, we can identify such nodes using their Katz centrality [231], which arises naturally under certain assumptions in our model. Moreover, efficient network protection can be achieved to minimize the size of cascading failures (in part) by protecting the most central nodes, which we formulate in Section 3.4.5.

A surprising way to identify such nodes involves extending the percolation process to allow link failures, creating a noisy version of the node percolation process introduced in Section 3.3.1. More specifically, for each edge $(i, j) \in \mathcal{E}(\mathcal{G})$ of the production network, we flip a coin of bias $y \in (0, 1]$, independently of the other edges and suppliers, and decide to keep the edge with probability y. Model-wise, this corresponds to firms holding inventories and, therefore, if a product i has enough inventory from its input product j, then it is likely to discard its network dependencies with probability $1 - y$.

This creates a subsampled graph $\mathcal{G}_y \subseteq \mathcal{G}$, which, under reasonable assump-

tions for x and y, can be used to identify vulnerabilities of the network to products whose failure is likely to cause the largest cascading failures. The above process can also be viewed as a *joint percolation* on both nodes and edges or a node percolation on the noisy subnetwork $\mathcal{G}_y$, where in order for a product to function, on average it only needs a y-fraction of its inputs to operate. We define $R_{\mathcal{G}}(\varepsilon; y)$ as resilience assuming randomness in the sampling $\mathcal{G}_y$, such that $R_{\mathcal{G}}(\varepsilon) = R_{\mathcal{G}}(\varepsilon; y = 1)$. Moreover, we define F_y as the size of the cascade in $\mathcal{G}_y$ and F as the size of the cascade when $y = 1$. A simple coupling argument similar to Lemma 3.4.1 for $0 < y_1 \leq y_2 < 1$ shows that survivals in $\mathcal{G}_{y_1}$ are greater than in $\mathcal{G}_{y_2}$:

Proposition 3.4.9. *For any $0 < y_1 \leq y_2 \leq 1$, we have $R_{\mathcal{G}}(\varepsilon; y_1) \geq R_{\mathcal{G}}(\varepsilon; y_2)$. Subsequently, $R_{\mathcal{G}}(\varepsilon; y) \geq R_{\mathcal{G}}(\varepsilon)$ for all $y \in (0, 1]$.*

In the following, we answer the above questions and provide a systematic way to treat general graphs that undergo a joint percolation process. More specifically, we systematically bound the expected number of failures and subsequently derive bounds for the resilience metric. Finally, we show that our analysis has deep connections to financial networks. To put our analysis into a mathematical framework, Markov's inequality states $\mathbb{P}[F_y \geq \varepsilon K] \leq \mathbb{E}\left[F_y\right]/\varepsilon K$. This together with Proposition 3.4.9 allows us to have an upper bound on resilience by limiting the failure of at least εK products which requires an upper bound on $\mathbb{E}\left[F_y\right] = \sum_{i \in \mathcal{K}} \mathbb{P}[Z_i = 0]$ following Markov's inequality; recalling notation of Equation (3.1), Z_i is an indicator variable for the failure of product i.

To connect the approximation of $\mathbb{E}\left[F_y\right]$ with linear programming, we define the following optimization problem and its dual, with optimal solutions $\beta^*_{\mathcal{G}}(u; y)$ and $\gamma^*_{\mathcal{G}}(u; y)$, which are parametrized by a shock vector $u \in [0, \mathbb{1}] := [0, 1]^K$:

$$p^*_{\mathcal{G}}(u;y) = \max_{\beta\in[0,\mathbb{1}]} \mathbb{1}^T\beta \qquad \text{s.t.} \quad \beta \le yA^T\beta + u, \tag{3.10}$$

$$d^*_{\mathcal{G}}(u;y) = \min_{\gamma,\theta\ge 0} u^T\gamma + \mathbb{1}^T\theta \qquad \text{s.t.} \quad (I - yA)\gamma + \theta \ge \mathbb{1}.$$

When the context is evident, we skip the arguments and simply write p^*, d^*, β^* and γ^*. The following theorem gives a way to characterize an upper bound on $\mathbb{E}\left[F_y\right]$ as the solution to a linear program (proof in Appendix B.2.8).

Theorem 3.4.10. *Let $\mathcal{G}$ be a production network that undergoes a joint percolation process with the probability of supplier failure x and the probability of survival of edges y. If p^* is the optimal value of the primal problem in Equation (3.10) for $u = \mathbb{1}x^n$, then, for $y = \varrho/m$ and $\varrho \in (0,1)$, we have $\mathbb{E}\left[F_y\right] \le p^* \le \left(1 + \varrho + O((\varrho)^2)\right)\mathbb{E}\left[F_y\right]$. The solution to LP can be found as the unique fixed point β^* of the contraction $\Phi(\beta) = \mathbb{1} \wedge (yA^T\beta + x^n\mathbb{1})$.*

The above theorem provides an algorithm to find β^* by solving the fixed point problem, i.e., if $\beta^{(t)}$ corresponds to the failure probabilities in iteration t, then β^* can be found using the following iteration which corresponds to a contraction map (since $y < 1/m$):

$$\beta^{(t)} = \mathbb{1} \wedge \left(yA^T\beta^{(t-1)} + x^n\mathbb{1}\right). \tag{3.11}$$

To obtain a solution with precision η, we need to iterate Equation (3.11) $\log(2K/\eta)/\log(1/\varrho)$ times, where $\varrho < 1$ is the Lipschitz constant for the contraction map and $2K$ bounds the L_1 norm of the initial condition. This algorithm has a runtime of $O\left(\frac{(K+M)\log(K/\eta)}{\log(1/\varrho)}\right) = \tilde{O}(K+M)$ to yield a solution that is close to β^* by some accuracy η, and subsequently is a $1 + \eta + \varrho + O(\varrho^2)$ approximation of the cascade size. The runtime matches the lower bound (up to logarithmic factors) $\Omega(K+M)$ of the influence maximization problem as shown in [71]. We also

show that the following approximation bounds hold for F_y and also that $\mathbb{E}\left[F_y\right]$ can never give a better approximation than $3/4 + o(1)$ – the proof is in Appendix B.2.9.

Theorem 3.4.11. *For $y < 1/m$, we have $\mathbb{E}\left[F_y\right] \geq \frac{\mathbb{E}[F]-Kq}{1-q}$ where $q = (1-(1-x^n(1-y))^m$. Moreover, $\mathbb{E}\left[F_y\right] \leq \left(\frac{3}{4} + o(1)\right)\mathbb{E}[F]$.*

Theorem 3.4.10 shows that there is a systematic way of bounding $\mathbb{E}[F]$ and $\mathbb{E}\left[F_y\right]$ via the solution of a linear program or a fixed-point equation (if the edge survival probability is less than $1/m$). It is surprising to note that an elegant upper bound on the expected number of failures becomes possible by introducing sampling at the edge level which reduces network dependencies. Moreover, if we want to maximize a weighted cascade, namely the objective function is $\pi^T\beta$ for some vector $\pi \geq 0$ instead of $\mathbb{1}^T\beta$, then the corresponding dual program, corresponds to the systemic risk measure [96, Example 7]:

$$\Lambda_{\mathcal{G}}(\pi; x) = \min_{\gamma,\theta\geq 0} x^n \mathbb{1}^T\gamma + \mathbb{1}^T\theta \quad \text{s.t.} \quad (I - yA)\gamma + \theta \geq \pi.$$

After defining $p^*_{\mathcal{G}}$ and its dual $d^*_{\mathcal{G}}$, the next question is how they are related to resilience. In the following (proved in Appendix B.2.10), we show that we can bound the resilience using the sum of the Katz centralities $\beta^{\text{Katz}}_{\mathcal{G}}(y) = (I - yA^T)^{-1}\mathbb{1}$ in $\mathcal{G}$.

Theorem 3.4.12. *If $y < 1/m$, the resilience $R_{\mathcal{G}}(\varepsilon; y)$ satisfies $R_{\mathcal{G}}(\varepsilon; y) \geq \left(\frac{\varepsilon}{\mathbb{1}^T\beta^{\text{Katz}}_{\mathcal{G}}(y)}\right)^{1/n}$.*

So far, we have focused on the regimes where $y < 1/m$. A reasonable question to ask here is whether the LP bounds are a good approximation of $\mathbb{E}\left[F_y\right]$ for $y > 1/m$. Unfortunately, the answer is negative as we show in Appendix B.7 as we can find families of graphs such that the gap between the LP and $\mathbb{E}\left[F_y\right]$ is at least $K/8$.

3.4.5 Intervention Design

In our model, we build intuition behind designing interventions to protect the supply chain. Our problem involves a global planner that can treat a maximum of B products in the network. Regulators aim to minimize failures, which can be achieved in many ways, such as diversifying the supplier base, building inventory buffers, and implementing robust risk management and monitoring systems. In mathematical terms, since each product can be produced if it has at least one functional supplier, this is equivalent to selecting a maximum of B products in which to intervene. The decision variables are set to $t_i \in \{0, 1\}, i \in \mathcal{K}$, corresponding to the subset $T \subseteq \mathcal{K}$ of treated products). The probability of failure of every product is then given by $(x(1-t_i))^n = x^n(1-t_i)$. Abusing notation, we define $p^*_{\mathcal{G}}(T; y)$ (resp. $d^*_{\mathcal{G}}(T; y)$) as the value of $p^*_{\mathcal{G}}(u; y)$ (resp. $d^*_{\mathcal{G}}(u; y)$) where $u_i = 0$ for every $i \in T$ and with $F(T)$ (resp. $F_y(T)$) to be the cascade size (resp. cascade size on the subsampled graph) after treating the products in T. A candidate problem for the planner in this case is

$$\min_{T \subseteq \mathcal{K}:|T|=B} p^*_{\mathcal{G}}(T; y) = \min_{T \subseteq \mathcal{K}:|T|=B} d^*_{\mathcal{G}}(T; y) \tag{3.12}$$

The function $p^*_{\mathcal{G}}(T; y)$ is increasing and submodular as a direct consequence of [40, Online Appendix, Proposition A.7]. Therefore, the intervention problem focuses on minimizing a monotone, increasing sub-modular function. This problem can be solved in polynomial time by relying on the Lovász extension of $p^*_{\mathcal{G}}(T; y)$. For small shocks, we can solve the intervention problem analytically. Specifically, if $0 < y < \frac{1}{\max\{m,\mu\}}$ and $0 < x < (1 - y \max\{m, \mu\})^{1/n}$, then the optimal solution of the maximization LP in Equation (3.12) (since the constraint

that corresponds to the network and individual effects holds with equality) is $\widehat{\beta}(T) = x^n(I - yA^T)^{-1}\mathbb{1}_{\mathcal{K}\setminus T}$ where $\mathbb{1}_{\mathcal{K}\setminus T}$ is the indicator vector of $\mathcal{K} \setminus T$. This yields the following proposition (proved in Appendix B.2.11).

Proposition 3.4.13. *Let* $0 < y < \frac{1}{\max\{m,\mu\}}$, $0 < x < (1 - y\max\{m,\mu\})^{1/n}$. *Let* $\mathcal{G}^R$ *be the graph where the direction of the edges in* $\mathcal{G}$ *is reversed, and consider* $\gamma_{\mathcal{G}}^{\text{Katz}}(y) = (I - yA)^{-1}\mathbb{1}$, *the Katz centrality of* $\mathcal{G}^R$. *Let* $\pi : \mathcal{K} \to \mathcal{K}$ *be a decreasing order on the entries of* $\gamma_{\mathcal{G}}^{\text{Katz}}(y)$. *Then, the optimal policy* $\widehat{t}$ *sets* $\widehat{t}_{\pi(i)} = 1$ *for* $i \in [B]$ *and sets it to zero otherwise.*

So, we can think of the "riskiest" products to be the ones with a high Katz centrality in $\mathcal{G}^R$ — the reversed graph representing the sourcing relationships between products. This agrees with our intuition about DAGs, which says to intervene starting from the raw materials and progressing in the topological order of the DAG until the budget is exhausted.

3.4.6 The Risk Exposure Index

Our metric has connections to important metrics already present in the supply chain literature [372, 370, 194], such as the Risk Exposure Index (REI). To define REI, suppose that a product in the production network is disrupted by an infinitesimal shock, assuming the same responses from the other nodes. In our case, this corresponds to a change in the probability of shock of the product i from x to $x + \delta$ and its impact on the size of cascading failures, which corresponds to the potential impact $\text{PI}(i)$. Since it is difficult to quantify an exact formula for the change of $\mathbb{E}[F]$, we will instead focus on the change in $\mathbb{E}\left[F_y\right]$ given by Equation (3.10). Specifically, the potential impact for a node is defined

as

$$\mathrm{PI}_i(x;y) = \lim_{\delta\to 0} \frac{p^*_{\mathcal{G}}\left((x^n,\ldots,(x+\delta)^n,\ldots,x^n)^T;y\right) - p^*_{\mathcal{G}}\left((x^n,\ldots,x^n,\ldots,x^n)^T;y\right)}{\delta} \tag{3.13}$$

$$= \left(nx^{n-1}\right)\cdot \left.\frac{\partial \beta^*_i(u;y)}{\partial u_i}\right|_{u_i=x^n}. \tag{3.14}$$

Subsequently, the Risk Exposure Index of $\mathcal{G}$ (REI, [372]) is given as the worst possible magnitude of $\mathrm{PI}_i(x;y)$, i.e.,

$$\mathrm{REI}_{\mathcal{G}}(x;y) = \max_{i\in\mathcal{K}} |\mathrm{PI}_i(x;y)| = nx^{n-1}\left\|\left.\frac{\partial \beta^*}{\partial u}\right|_{u=\mathbb{1}x^n}\right\|_\infty. \tag{3.15}$$

We give the following Theorem to characterize the REI:

Theorem 3.4.14. *Consider an optimal solution $\beta^\star$ of Equation (3.10). Let $\mathcal{K}^+ = \left\{i\in[K]:\beta^*_i=1,\beta^*_i\le y\sum_{j\sim i}\beta^*_j+x^n\right\}, \mathcal{K}^- = \left\{i\in[K]:\beta^*_i<1,\beta^*_i=y\sum_{j\sim i}\beta^*_j+x^n\right\}, \mathcal{K}^0 = \left\{i\in[K]:\beta^*_i=1=y\sum_{j\sim i}\beta^*_j+x^n\right\}$ be a partition of the products $\mathcal{K}$. Let $\mathcal{B}^+ = \mathcal{K}^-\cup\left\{K+j:j\in\mathcal{V}^+\cup\mathcal{V}^0\right\}, \mathcal{B}^- = \mathcal{K}^+\cup\left\{K+j:j\in\mathcal{V}^-\cup\mathcal{V}^0\right\}$ be the bases of the equivalent LP with variable s, that is, $\max_{\beta,s\ge 0}\ \mathbb{1}^T\beta$ subject to $(I-yA^T)\beta+s=\mathbb{1}x^n$ and $\beta\le\mathbb{1}$. If B^+ and B^- are the matrices formed by the columns of $\left(I-yA^T \quad I\right)$ corresponding to $\mathcal{B}^+$ and $\mathcal{B}^-$, and*

$$\mathrm{PI}^+_i(x;y) = \left(nx^{n-1}\right)\cdot\left.\frac{\partial^+\beta^*_i(u;y)}{\partial u_i}\right|_{u_i=x^n}, \mathrm{REI}^+_{\mathcal{G}}(x) = \max_{i\in[K]}|\mathrm{PI}^+_i(x;y)|,$$
$$\mathrm{PI}^-_i(x;y) = \left(nx^{n-1}\right)\cdot\left.\frac{\partial^-\beta^*_i(u;y)}{\partial u_i}\right|_{u_i=x^n}, \mathrm{REI}^-_{\mathcal{G}}(x;y) = \max_{i\in[K]}|\mathrm{PI}^-_i(x;y)|,$$

then $\mathrm{REI}^+_{\mathcal{G}}(x;y) = nx^{n-1}\left\|\left(I \quad O\right)_{\cdot,\mathcal{B}^+}(B^+)^{-1}\right\|_\infty$ *and* $\mathrm{REI}^-_{\mathcal{G}}(x;y) = nx^{n-1}\left\|\left(I \quad O\right)_{\cdot,\mathcal{B}^-}(B^-)^{-1}\right\|_\infty$.

Moreover, if there are no borderline nodes (i.e., $\mathcal{K}^0 = \emptyset$), then $\mathcal{B}^+ = \mathcal{B}^- = \mathcal{B}$, $B^+ = B^- = B$, and subsequently $\text{REI}_{\mathcal{G}}(x;y) = nx^{n-1} \left\| \begin{pmatrix} I & O \end{pmatrix}_{\cdot,\mathcal{B}} (B)^{-1} \right\|_\infty$.

Theorem 3.4.14 is a direct consequence of applying Proposition 1 of [272]. We can also show that when firms hold large enough inventory ($y < 1/m$) and the shocks are sufficiently small the REI is proportional to the node with the highest Katz centrality in $\mathcal{G}^R$.

Corollary 3.4.15. *If $y < 1/m$, and $x < (1 - my)^{1/n}$, then* $\text{REI}_{\mathcal{G}}(x;y) = nx^{n-1} \|\gamma_{\mathcal{G}}^{\text{Katz}}(y)\|_\infty$.

Finally, systematizing the analysis above for other supply chain graphs already yields the definition of the resiliency metric, which we formalize in the next Section.

3.4.7 Resilience of Empirical Production Networks

With the definition of resilience and the theoretical results developed in the previous sections, we study the resilience of production networks in practice. We examine the resilience of networks contained in the following two data sets of production networks (Tables 3.4 and B.1):

1. *Multi-echelon Supply-chain Networks* from [422]. The dataset contains 38 different multi-echelon (see also Figure 3.2) supply chain networks, from which we select three networks to run simulations on. Similar supply chain networks have been used in prior literature, see, e.g., [59] and [334].
2. *Country Economy Production Networks* derived from *World Input-Output Tables* taken from the World Input-Output Database [390]. We focus on the

economies of six countries in 2014: the USA, Japan, China, Great Britain, Indonesia, and India. We consider any non-zero amount cell at the input-output tables as an edge between two industries in a country. For space considerations, the results have been deferred to Appendix B.5.

	Dependent variable: log-$R_{\mathcal{G}}^{\text{avg}}(y)$
const	-1.757*** (0.045)
log-K	0.146*** (0.012)
log-r	-0.029*** (0.010)
Observations	34
R^2	0.871
Adjusted R^2	0.862
Residual Std. Error	0.067 ($df = 31$)
F Statistic	104.385*** ($df = 2; 31$)
Note:	$^{*}p < 0.1;^{**}p < 0.05;^{***}p < 0.01$

Table 3.2: Relation between the $R_{\mathcal{G}}^{\text{avg}}(y)$, K and r for the multi-echelon networks of [422]. For each network, we set $y = 1/(m + 10^{-5})$.

Resilience metrics. First, we study the resilience of the above networks as a function of ε for ε ranging from 0 to 1 numerically. To achieve this, we run 1000 Monte Carlo (MC) simulations where we sample the (spontaneous) state of n suppliers and then propagate the state of each product to the adjacent ones, based on Equation (3.1). To calculate resilience, we estimate the probability $\mathbb{P}[S \geq (1-\varepsilon)K]$ for various values of $x \in (0,1)$ with MC simulation and find the maximum value of x for which the estimate is at least $1 - 1/K$. We plot the estimated resilience $\widehat{R}_{\mathcal{G}}(\varepsilon)$ as a function of ε. and present the results in Figures 3.5(a) and B.1(a). As an additional resilience metric that's independent of ε, we also report the average resilience $\widehat{R}_{\mathcal{G}}^{\text{avg}}(y) = \int_0^1 \widehat{R}_{\mathcal{G}}(\varepsilon; y)d\varepsilon$.

Furthermore, we perform a regression to relate $\widehat{R}_{\mathcal{G}}^{\text{avg}}(y)$ with the number of raw products (r) and the size of the network (K), and report the results in Ta-

ble 3.2. We find that $\widehat{R}^{\text{avg}}_{\mathcal{G}}(y)$ increases in K ($p < 0.01$) and decreases with r ($p < 0.01$). This agrees with our theoretical results (e.g., Theorem 3.4.7) which highlight that networks with more raw products have lower resilience.

Optimal interventions. To study the effect of targeted interventions in real-world supply chain networks, we apply the results of Proposition 3.4.13 for the networks from the two datasets. More specifically, for a value of $y = \frac{1}{10^{-5}+\mu}$, and $\varepsilon = 0.2$, we plot the lower bound for the resilience devised by Proposition 3.4.13 as a function of the total intervention budget T. This involves calculating the Katz centralities for the reverse graph $\mathcal{G}^R$, sorting them in decreasing order, and plotting the cumulative sum for the first T entries, for T ranging from 0 to K. In Figures 3.5(b) and B.1(b), we report the lower bound on the resilience as a function of the normalized intervention budget T/K.

Empirical relation between REI and our resilience metric. In Table 3.3, we show the relationship between $\text{REI}^{\text{avg}}_{\mathcal{G}}(y) = \int_0^1 \text{REI}_{\mathcal{G}}(x;y)dx \approx \left\|\gamma^{\text{Katz}}_{\mathcal{G}}(y)\right\|_\infty)$ and $R^{\text{avg}}_{\mathcal{G}}(y)$ and the maximum degree m of the network. We observe that $\text{REI}^{\text{avg}}_{\mathcal{G}}(y)$ is inversely proportional to $R^{\text{avg}}_{\mathcal{G}}(y)$ ($p < 0.01$) showing that less resilient networks (on average) are "riskier" (on average) and proportional to m ($p < 0.01$) and K ($p < 0.01$), showing that bigger and denser networks are "riskier" (on average).

[t]

	Dependent variable: log-$\text{REI}_{\mathcal{G}}^{\text{avg}}(y)$
const	-14.782*** (2.817)
log-m	0.540*** (0.167)
log-K	0.932*** (0.259)
log-$R_{\mathcal{G}}^{\text{avg}}(y)$	-8.828*** (1.589)
Observations	34
R^2	0.678
Adjusted R^2	0.646
Residual Std. Error	0.629 ($df = 30$)
F Statistic	21.089*** ($df = 3; 30$)
Note:	$^{*}p < 0.1;^{**}p < 0.05;^{***}p < 0.01$

Table 3.3: Relation between $\log \text{REI}_{\mathcal{G}}^{\text{avg}}(y)$ and $\log m$, $\log K$ and $\log R_{\mathcal{G}}^{\text{avg}}(y)$ for the multi-echelon networks of [422]. For each network, we set $y = 1/(m + 10^{-5})$.

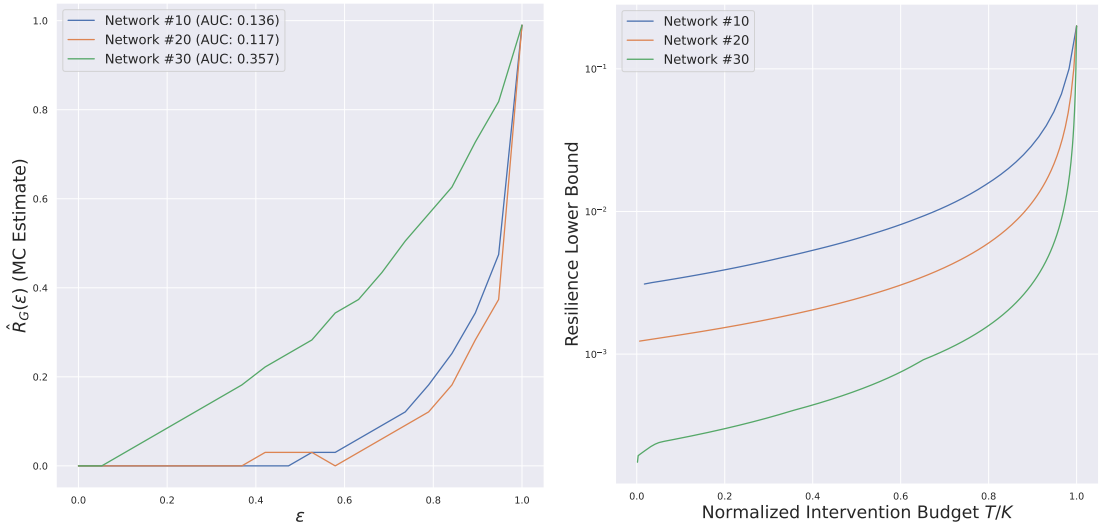
Network ID	Size (K)	Avg. Degree	Density ($\frac{\lvert\mathcal{E}(\mathcal{G})\rvert}{K^2-K}$)	μ	m	$\widehat{R}_{\mathcal{G}}^{\text{avg}}$
#10	58	3.03	0.053	27	13	0.136
#20	156	1.08	0.006	29	3	0.117
#30	626	1.00	0.001	2	48	0.357

Table 3.4: Network Statistics and $\widehat{R}_{\mathcal{G}}^{\text{avg}}(y)$ from [422].

3.5 The Heterogeneous Model

So far, for simplicity of exposition and to be able to derive meaningful bounds, we have assumed that each product has n suppliers and that each supplier fails i.i.d. with probability x. In this section, we extend our proposed model and the resilience metric to account for heterogeneities, such as a different number of suppliers and different failure probabilities.

In our heterogeneous model, each product has $n_i = |\mathcal{S}(i)| = O(1)$ suppliers. We define the universe of suppliers as $\mathcal{U} = \bigcup_{i \in \mathcal{K}} \mathcal{S}(i)$ and $N = |\mathcal{U}|$, and each supplier $s \in \mathcal{U}$ fails with probability $x_s = \mathbb{P}[X_s = 1]$. Note that here suppliers' failures are not assumed to be i.i.d. but are correlated according to a joint



(a) Estimating $\widehat{R}_{\mathcal{G}}(\varepsilon)$ and $\widehat{R}^{\text{avg}}_{\mathcal{G}}(\varepsilon)$ (b) Optimal Interventions

Figure 3.5: Resilience estimation and optimal interventions for three networks from [422]. We set the number of suppliers for each product to $n = 1$.

distribution ν with marginals $\{x_s\}_{s\in\mathcal{U}}$.

The resilience metric for a joint distribution ν is defined as the maximum shock $x \in (0,1)$ such that: *(i)* there are on average $\sum_{s\in\mathcal{U}} x_s = xN$ failures, *(ii)* at least $1-\varepsilon$ of the products survive with high probability assuming that the failures of the suppliers ($F_{\mathcal{S}}$) are distributed according to ν (i.e., $F_{\mathcal{S}} \sim \nu$). The resilience of the graph is taken to be the resilience over the worst possible such joint distribution, i.e.:

$$R_{\mathcal{G}}(\varepsilon) = \inf_{\nu} \sup_{x} x \quad \text{s.t.} \quad \sum_{s\in\mathcal{U}} x_s \le xN \text{ and } \mathbb{P}_{F_{\mathcal{S}}\sim\nu}[F \ge \varepsilon K] \le \frac{1}{K}. \tag{3.16}$$

First, we can show that if $x_s \in \{0,1\}$, i.e., the marginals are deterministic, then calculating $R_{\mathcal{G}}(\varepsilon)$ is NP-Hard and is also hard to approximate (see Appendix B.6). Even when the marginals are fractional, numerically evaluating resilience is computationally intractable, as one has to search for all possible

joint distributions and calculate the resilience for each joint distribution. Therefore, we are interested in efficiently computable upper and lower bounds.

3.5.1 The Bahadur Representation

Regarding the upper bound, since the definition of resilience according to Equation (3.16) considers the worst possible joint distribution, the generalized resilience value is upper bounded by resilience in the case of i.i.d. failures, and the upper bound of Theorem 3.4.7 holds for the general definition of resilience.

To devise a lower bound, since Markov's inequality depends on $\mathbb{E}[F]$, maximizing this quantity implies a lower bound on the resilience. However, such an optimization program has $O(K)$ variables and $O(2^N)$ constraints, making it impractical to solve.

In the sequel, we focus on low-dimensional representations of ν. Our analysis is based on the Bahadur decomposition [33, 432], which gives a way to calculate the joint probability distribution of failures as a sum of multi-way correlations. According to the Bahadur representation, the joint distribution ν of active suppliers can be written.

$$\nu(T) = \prod_{s \in T} x_s \prod_{s \notin T} (1 - x_s) \left\{ \sum_{j=1}^{N} \sum_{\{s_1, \ldots, s_j\} \in \binom{\mathcal{U}}{j}} \rho_{s_1, \ldots, s_j}(T) \prod_{j'=1}^{j} \widehat{x}_{s'_j}(T) \right\} \tag{3.17}$$

where $\widehat{x}_{s_j} = \frac{\mathbb{1}\{s_j \in T\} - x_{s_j}}{\sqrt{x_{s_j}(1-x_{s_j})}}$, $\rho_{s_1, \ldots, s_j}(T)$ denotes the j-th order correlation between $s_1, \ldots, s_j$, and $T \subseteq \mathcal{U}$ denotes the set of active suppliers. From this we can obtain the marginal for each product $i \in \mathcal{K}$ as $u_i = \sum_{T \subseteq \mathcal{U} \setminus \mathcal{S}(i)} \nu(\mathcal{S}(i) \cup T)$.

To obtain a low-dimensional representation of ν, we can make some assumptions that simplify our calculations and provide meaningful ways to calculate resilience. In the following, we give some simplified models that account for correlations between suppliers within each product, across products, and across all suppliers.

Homogeneous failures, uncorrelated products, and correlated suppliers. The first simplification of Equation (3.17) considers the case of homogeneous failures and correlated suppliers within a product (but not across products), which requires $O(N)$ parameters. This model accounts for failures within a product or a sector in the economy; for instance, a failure of a supplier of a specific scarce raw material would harm the failure of other suppliers of the same raw product since the failure of a supplier can increase the demand of the material from another supplier, and, thus, increase its failure probability.

Thus, if $x_s = x$ for all suppliers $s \in \mathcal{U}$, and the j-th order correlation coefficient for product i is $\rho_{ij} \in [0, 1]$ for all j-tuples, we can write the joint probability of failure of a product as

$$u_i = x^{n_i} + \sum_{j=2}^{n_i} \binom{n_i}{j} \rho_{ij} (1-x)^{j/2} x^{n_i - j/2} \tag{3.18}$$

As we expect, increasing ρ_{ij} to +1 increases the probability of failure of one product and therefore decreases the resilience. Similarly, bringing ρ_{ij} equal to 0 makes the failure probability equal to x^{n_i}, which reduces to the previously studied case of independent failures. When $\rho_{ij} = 1$, the problem is equivalent to each product having one supplier instead of n_i suppliers and thus retains

its resilience properties; that is, for network classes that are indexed by their number of products K their asymptotic in $K \to \infty$ classification as resilient or fragile (i.e., their resilience taxonomy) remains the same with the introduction correlations between suppliers of the same product (recall Definition 3.4.1). This is no longer the same when correlations are introduced between products; then all networks are, in general, fragile.

Homogeneous failures, correlated products, and uncorrelated suppliers. The second simplification considers the case of homogeneous failures and correlated products but uncorrelated suppliers within a product, which requires $O(K)$ parameters. This case models a scenario where a natural disaster can affect multiple sectors, even if they are not dependent on each other by import/export relations.

Thus, if we assume that all suppliers $s \in \mathcal{U}$ fail with probability $x_s = x$ independently within each product, but products are correlated with each other, with the j-th order correlation coefficient being $\rho_j \in [0,1]$. Then, we can show that the marginal probability of one product's failure is

$$u_i = \sum_{b=0}^{K-1} \binom{K-1}{b} (x^{n_i})^{b+1} (1-x^{n_i})^{K-1-b} \left\{ 1 + \sum_{j=2}^{K} \sum_{r=0}^{\min\{j,b+1\}} \binom{j}{r} \binom{K-j}{j-r} \rho_j (1-x^{n_i})^{r-j/2} (x^{n_i})^{j/2-r} \right\} \tag{3.19}$$

When $\rho_j = 1$, the failure of a single product is enough to have $F \geq \varepsilon K$ for $\varepsilon \in (0, 1-1/K)$. By the union bound, this happens with probability at most $\sum_{i=1}^{K} x^{n_i} \leq Kx$, and setting the probability of this event to be at most $1/K$, yields the result that the average resilience is dropping at an $O_\varepsilon\left(1/K^2\right)$ rate, and therefore the network becomes fragile.

Homogeneous failures, correlated suppliers and products. The final simplification considers the case of homogeneous failures and correlations among all suppliers, which requires $O(N)$ parameters. This case models the scenario where a firm produces more than one product; for example, an automotive manufacturer produces engines (which can be exported to others) and chips using the same manufacturing facilities. Then a disaster in the manufacturing facility (e.g., a fire) would damage both products.

By extending Equation (3.19), we can state a similar result for the case where all suppliers are correlated, and the j-th order correlation coefficient is $\rho_j \in [0, 1]$. Similarly to Equation (3.19), we can show that the marginal probability of failure of one product is

$$u_i = \sum_{b=0}^{N-n_i} \binom{N-n_i}{b} x^{b+n_i} (1-x)^{N-n_i-b} \left\{ 1 + \sum_{j=2}^{N} \sum_{r=0}^{\min\{j,b+n_i\}} \binom{j}{r} \binom{N-j}{j-r} \rho_j (1-x)^{r-j/2} x^{j/2-r} \right\} \quad (3.20)$$

We can verify that setting $n_i = 1$ (which implies $N = K$) yields Equation (3.19), and setting $K = 1$ yields Equation (3.18). Furthermore, in the extreme case where $\rho_j = 1$, the failure of a single supplier is enough to make $F \geq (1-\varepsilon)K$. By the union bound, this happens with probability at most Nx, and setting this to be at most $1/K$, shows that the average resilience is dropping as $O_\varepsilon\left(1/K^2\right)$. Therefore, the network becomes fragile.

Bounds based on the Bahadur representation. To obtain bounds on the resilience assuming the simplified marginals (e.g. Equations (3.18) to (3.20)) we can directly apply the results of Theorem 3.4.7 and Theorem 3.4.12 and invert the corresponding marginals (cf. Figure 3.7):

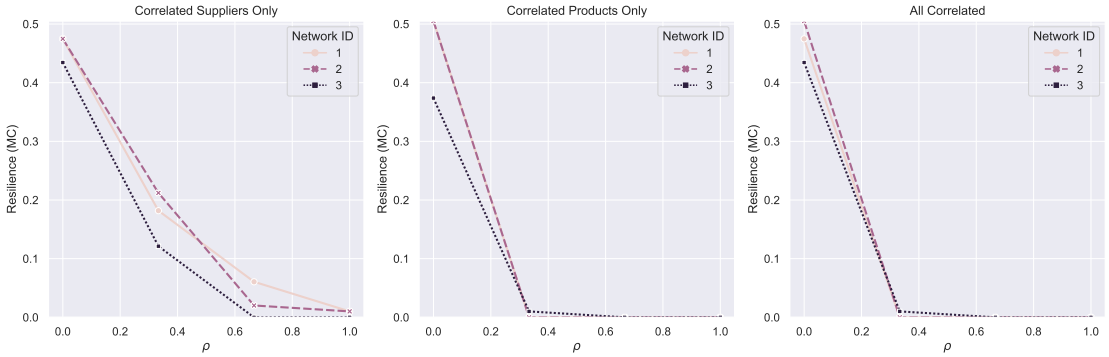


Figure 3.6: Effect of correlation on $R_{\mathcal{G}}(\varepsilon)$ for three networks from [422]. We consider the cases studied in Equations (3.18) to (3.20). The 2n-th order correlation coefficient has been set to $\rho_2 = \rho \in \{0, 0.25, 0.5, 0.75, 1\}$. The higher-order correlations have been set to zero.

Proposition 3.5.1. *Let $\mathcal{G}$ be a network where suppliers fail with a correlation vector ρ, which corresponds to the marginal failure probabilities $u_i = u(x;\rho)$ which are monotone, increasing in x, let $y < 1/m$, and $n_i = n$. Then, the resilience $R_{\mathcal{G}}(\varepsilon; y, \rho)$ satisfies $R_{\mathcal{G}}(\varepsilon; y, \rho) \geq u^{-1}\left(\frac{\varepsilon}{\mathbb{1}^T \beta_{\mathcal{G}}^{\mathrm{Katz}}(y)}; \rho\right)^{1/n}$ and $R_{\mathcal{G}}(\varepsilon; y, \rho) \leq u^{-1}\left(\frac{(1-\varepsilon)K}{2r^{3/2} + \sqrt{r \log K}}; \rho\right)^{1/n}$.*

An example from empirical networks. Figure 3.6 shows the impact of introducing correlations to the resilience. Specifically, we see that introducing correlations decreases resilience, with the biggest impact in the case where correlations is assumed among all pairs of suppliers (correlated products and suppliers).

3.6 Managerial Insights

Increased risk from raw products. Our results show that ***production networks with even a sublinear number of raw products are fragile***. Theorem 3.4.7 implies that $\Omega(K^{2/3})$ raw products suffice for the network to be fragile. Two di-

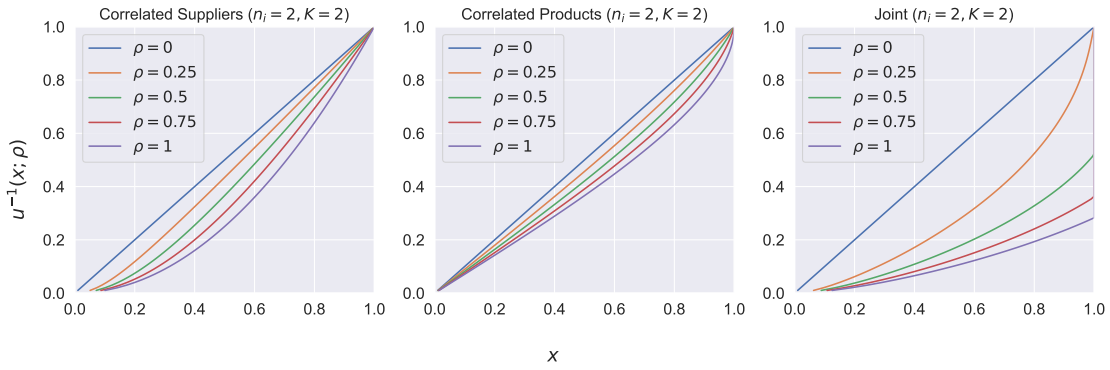


Figure 3.7: Value of inverted marginal $u^{-1}(x;\rho)$ for the cases studied in Equations (3.18) to (3.20). All correlations have been set equal to $\rho \in \{0.25, 0.5, 0.75, 1\}$. The network is assumed to have $K = 2$ products and each product has $n_i = n = 2$ suppliers.

rect corollaries of this are the tree network, where the number of raw products is m^D, for m-ary tree with D layer and a complex product at the root, and the trellis network with width at least $K^{2/3}$ and depth at most $K^{1/3}$, which both constitute fragile families of structures. This increased risk from raw products is also verified empirically, and we show that the average resilience decreases as the number of raw products increases using Monte Carlo estimates of resilience on real-world supply chain networks (Table 3.2). This agrees with our theoretical results and prior works that state networks with higher interdependence in the tree model (which correspond to a higher number of raw products) are less resilient [142]. Qualitatively, these graphs look like "cowboy hats" (see Figure 3.8), with a large number of raw products on the base.

Increased resilience from lower dependencies, fewer raw products, and fewer final goods. Our lower bounds on the resilience of the complex products (Theorem 3.4.3), and general networks (Theorem 3.4.7) show that ***networks with low dependencies*** (μ, m) ***and few raw products (small*** r***) and few final goods (small*** c***) are resilient***. For example, the sparse random trellis network (Informal The-

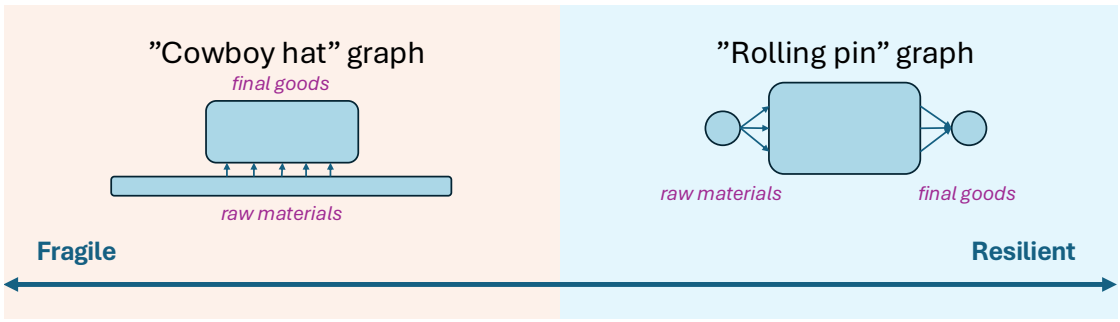


Figure 3.8: Qualitative representation of fragile and resilient networks

orem 4) with constant width is resilient. Qualitatively, such graphs look like "rolling pins" (see Figure 3.8), while there are small primary and final sectors and sparse connections in the layers between them.

Connections to Risk Exposure Index (REI). We adopt the definition of REI in [372] to our setup by considering the product that has the maximum potential impact on the size of the cascading failures and we show that under reasonable assumptions the ***Risk Exposure Index of a network is determined by the node with the highest Katz centrality in the edge-reversed graph***. Our empirical results verify the inverse relationship between REI and our resilience metric.

Optimal interventions. We show that ***targeting nodes with highest Katz centrality in the edge-reversed graph is optimal*** under regularity assumptions — these nodes represent less complex products. This argument agrees with our intuition and recent observations from the COVID-19 pandemic, where the failure of chip manufacturing industries (which are relatively close to the raw materials, compared e.g., to more complicated electronic devices) caused very large global cascades.

Role of heterogeneity and correlations. We extend our resilience metric to capture supply heterogeneities and correlations among suppliers and products. Our results show that while restricting correlations to suppliers of the same product has limited effect, ***correlation across suppliers of different products can significantly impact resilience, rendering all network structures fragile***. Low dimensional representations based on lower-order moments of the joint distribution open a way to efficiently estimate expected cascade size using measurable failure statistics on historical supply chain data. Our empirical results on a real-world data set of multi-echelon supply chain networks [422] also verify that higher supplier correlation reduces resilience.

3.7 Discussion

Through this chapter, we aim to devise a systematic way to test which supply chain networks are *resilient*, i.e., can withstand "large enough" shocks while sourcing almost all their productions. Through this metric of resilience, we classify some common supply chain architectures as resilient or fragile and identify structural factors that affect resiliency. We then generalize our analysis and provide tools for studying the resilience of general supply networks, as well as motivating methods that can be used for the design of optimal interventions.

There are various ways that our model can be extended. The first interesting direction is to fit our model of the production network to economic and financial networks that are encountered in practice and real-world settings. Our model can be extended to contain costs, quantities, and link capacities, and the desired objective would be to optimize the network total profits subject to production

shocks, extending, thus, a long-standing line of work on economic networks [193, 3, 4]. Another promising avenue is to give theoretical bounds on networks with varying interdependency and multi-sourcing. So far, we have assumed that products have the same number n of suppliers. However, this can be extended to cases where each industry has random size $n_i \sim \mathcal{D}_{\text{industry}}$, where $\mathcal{D}_{\text{industry}}$ is a distribution (e.g., power law, as in [164]). It would be interesting to study this heterogeneity in the size of different industries and how it affects $R_{\mathcal{G}}(\varepsilon)$; see also [164]. Moreover, as we saw in Section 3.4.4, there is a direct connection between cascading failures in supply chains and systemic risk in financial networks. Therefore, we can readily adapt tools from the study of financial risk to supply chain resiliency and risk.

CHAPTER 4

PRIVACY-PRESERVING DECISION-MAKING FOR RESILIENCE: DIFFERENTIALLY PRIVATE DISTRIBUTED INFERENCE IN CONTINUOUS AND DISCRETE HYPOTHESIS SPACES

The contents of this chapter constitute joint work with Amin Rahimian.

Sociotechnical systems' resilience depends on their ability to integrate information from distributed agents while preserving privacy and ensuring accurate decision-making. In modern networked environments, agents—whether individuals, institutions, or automated systems—continuously interact to estimate unknown quantities, form beliefs, and make decisions.

In the previous two Chapters, we studied two phenomena regarding resilience. First, we studied how allocation mechanisms can be used to measure and reinforce dynamic network resilience, and, second, we studied what types of networks are resilient and which are not. Both of the previous Chapters adopted a centralized viewpoint in decision-making; however, it is natural to think about cases where the agents in a network act completely autonomously and make utility-maximizing decisions. For instance, when banks decide to invest or lend they face and cause counterparty risk due to their individual decisions. Similar are the cases of health centers who wish to test a new drug treatment to improve the standard of care for a disease such as AIDS, or agents in a social network who express public opinions on the Web.

Most of these interactions introduce privacy risks and potential vulnerabilities, particularly when sensitive data is involved. The work presented in this Chapter addresses these challenges by developing novel distributed estimation

and learning algorithms that balance privacy, accuracy, and efficiency in networked decision-making processes.

In this Chapter, we study distributed estimation problems where agents seek to learn the statistical properties of random variables from their private observations while sharing information over a network. Our proposed methods extend existing distributed estimation and learning frameworks by incorporating differential privacy (DP) mechanisms that introduce controlled noise into shared estimates.

The contributions presented in this Chapter consider two types of regimes: Firstly, we study the distributed inference tasks in continuous hypothesis spaces where agents have access to signals from an exponential family distribution. Secondly, we study distributed inference tasks in discrete hypothesis spaces, where we do not make any assumption regarding the underlying models that produce the agents' signals. In both cases, we demonstrate how privacy-preserving information aggregation influences the trade-offs between learning accuracy, statistical power, and computational efficiency.

Through tailored linear and log-linear aggregation schemes, agents can collaboratively estimate complete sufficient statistics (in the first part) and perform maximum likelihood estimation or hypothesis testing (in the second part) while preserving privacy. Theoretical analysis establishes tight finite-time convergence bounds, showing that Laplace noise optimally balances privacy and convergence speed based on each agent's sensitivity to their signals and network topology. Additionally, empirical validation on real-world datasets, such as power grid networks and household energy consumption, and data from multi-center clinical trials demonstrates superior performance compared to ex-

isting privacy-aware distributed optimization methods and privacy-preserving methods, which are based on encryption.

4.1 Privacy-Preserving Estimation and Learning in Continuous Hypothesis Spaces

Differential privacy (DP) is a gold standard in privacy-preserving algorithm design that limits what an adversary (or any observer) can learn about the inputs to an algorithm by observing its outputs [133, 135], according to a privacy budget that is usually denoted by ε. It requires that given the output, the probability that any pair of adjacent inputs generate the observed output should be virtually the same. Adding noise to the input data helps enforce this standard in different settings — e.g., for distributed learning — but the added noise can also degrade our performance, e.g., lowering the quality of distributed estimation and collective learning for which agents exchange information.

This Chapter provides aggregation algorithms that facilitate distributed estimate and learning among networked agents while accommodating their privacy needs (e.g., protecting their private or private signals and network neighborhoods). Each algorithm implies a different tradeoff between its quality of collective learning and how much privacy protection it affords the participating agents (i.e., their privacy budgets). Our performance metrics reflect how distributional features of the private signals and the nature of privacy needs for individual agents determine the learning quality and requisite noise.

Decentralized decision-making and distributed learning problems arise nat-

urally in a variety of applications ranging from sensor and robotic networks in precision agriculture, digital health, and military operations to the Internet of things and social networks [79, 209]; see Section 4.1.2 for a detailed literature review. We are particularly interested in distributed estimation problems that arise in smart grids with distributed generation and energy resources. Notably, a recent report from [296, 297] suggests that net metering practices should be revised to reflect the value of distributed electricity generation, such as rooftop solar panels. Net metering compensates customers for the electricity they provide to the grid through distributed generation. The report notes that net metering has facilitated the embrace of distributed generation in states where it has been put into effect, resulting in levels surpassing 10% in a few states and projected to rise in both these and other states. Additionally, the report emphasizes the need to revisit and evolve net metering policies to support the deployment of distributed generation that adds value in reducing fossil fuel use, enhancing resilience, and improving equity. In this context, each customer faces an individual privacy risk in sharing their estimates since revealing exact measurements can pose security risks that can be leveraged by an adversary (e.g., understanding when someone is at their home, daily habits, family illness, etc.), and, therefore, developing privacy-preserving methods that support decentralized decision making in such setups is critical.

This Chapter introduces novel algorithms designed for the distributed estimation of the expected value of sufficient statistics in an exponential family distribution. The proposed methods leverage signals received by individual agents, who maintain and update estimates based on both these signals and information from their local neighborhood. Our contributions to the existing literature on distributed optimization include new privacy-aware distributed

estimation algorithms that exhibit faster convergence rates compared to established first-order methods (cf. [354]). Notably, our algorithms safeguard the information in agents' signals and local neighborhood estimates, ensuring optimal convergence times to true estimates. Furthermore, in contrast to existing approaches, our algorithms can support privacy-aware estimation within an online learning framework, accommodate dynamic topologies, and balance privacy and accuracy by distributing the privacy budget among agents. Finally, we verify our proposed algorithms on real-world datasets and show that they outperform existing first-order methods.

4.1.1 Main Results

We consider a network of n agents indexed by $[n] = \{1, \ldots, n\}$ whose interconnections are characterized by a symmetric, doubly-stochastic, adjacency matrix A. This adjacency structure, encoded by graph neighborhoods, $\mathcal{N}_i = \{j : a_{ij} \neq 0\}, i \in [n]$, may be a consequence of geospatial constraints such as sensing and communication range or geographic proximity; it can also be a reflection of how the network has evolved and other engineering considerations, e.g., which nodes belong to which countries or companies in a multi-party network. The adjacency weights may also result from geoeconomic constraints such as access to local trade and business intelligence (contracts, sales, and filled orders). In the case of social networks, they can also represent the presence of influence and mutual interactions among individuals.

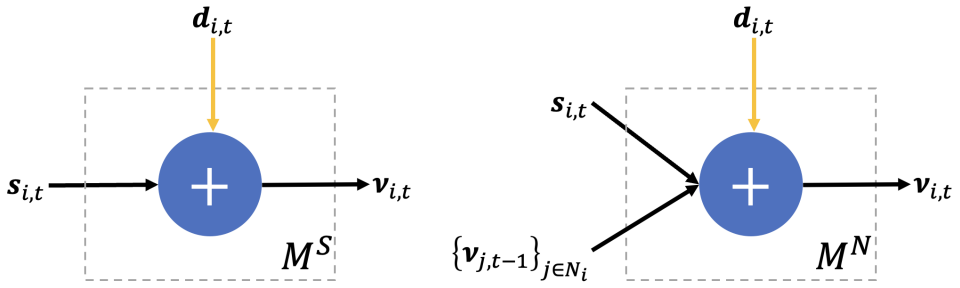
Given the adjacency structure A, at every round $t \in \{1, 2, 3, \ldots\}$, each agent i receives a private signal $s_{i,t}$ that is sampled from an exponential family dis-

tribution with the natural sufficient statistic $\xi(\cdot) \in \mathbb{R}$ and a common, unknown parameter θ belonging to a measurable set Θ. The goal of the agents is to collectively estimate the common value of $\mathbb{E}_\theta[\xi(s)]$ by combining their samples. This is achieved through a consensus algorithm by forming an estimate $\nu_{i,t}$ and exchanging it with their network neighbors in a distributed manner respecting the adjacency structure of A. The agents also want to control the information that is leaked about their signals and the estimates of their neighbors $\{\nu_{j,t-1}\}_{j\in\mathcal{N}_i}$. They add noise $d_{i,t}$ to their updates. The noise level should be high enough not to violate an ε differential privacy budget. Briefly, we say that a mechanism $\mathcal{M}$ is ε-DP when for any pair of "adjacent" inputs (i.e., private signals or private signals and neighboring estimates), the logarithm of the probability ratio of any output in the range space of $\mathcal{M}$ being resulted from either of the adjacent inputs is bounded by ε: $|\log(\mathbb{P}[\mathcal{M}(s) \in R]/\mathbb{P}[\mathcal{M}(s') \in R])| \leq \varepsilon$, for all adjacent pairs (s and s') in the input domain and any subset R of the output range space. Our specific notion of adjacency between the input pairs will be determined by the nature of information leaks, i.e., private signals or private signals and network neighborhoods, against which the exchanged estimates ($\nu_{i,t}$) are being protected (Figure 4.1).

We provide bounds for the convergence of the DP estimates $\nu_t = (\nu_{i,t})_{i\in[n]}$ to the desired value $m_\theta := \mathbb{1}m_\theta$, where $m_\theta = \mathbb{E}_\theta[\xi(s)]$. We decompose the total error as follows:

$$\underbrace{\mathbb{E}\left[\|\nu_t - m_\theta\|_2\right]}_{\text{Total Error (TE)}} \leq \underbrace{\mathbb{E}\left[\|\nu_t - \mu_t\|_2\right]}_{\text{Cost of Privacy (CoP)}} + \underbrace{\mathbb{E}\left[\|\mu_t - m_\theta\|_2\right]}_{\text{Cost of Decentralization (CoD)}}$$

Here, $\mu_t = (\mu_{i,t})_{i\in[n]}$ corresponds to the vector of non-private estimates. The first term corresponds to the "Cost of Privacy" (CoP), the estimation cost incurred by the ε-DP noising. The second term corresponds to the expected error from run-



(a) Signal DP (b) Network DP

Figure 4.1: Two types of DP protections considered in this Chapter are signal DP, $\mathcal{M}^S$, and network DP, $\mathcal{M}^N$. The private signal of agent i at round t is denoted by $s_{i,t}$, $d_{i,t}$ corresponds to the noise added from agent i at round t, and $v_{i,t}$ corresponds to the estimate of agent i at round t. Our theoretical guarantees delineate the relationship between communication resources (t rounds), privacy budget (ε-DP), and total error (TE). Signal and network DP imply different performance tradeoffs as detailed in Table 4.1.

ning the non-private distributed learning algorithm and, therefore, measures the "Cost of Decentralization" (CoD). In Algorithm 5, when we consider "offline" estimation of m_θ from a fixed collection of initial signals available at the beginning ($t = 0$), we replace m_θ by the best possible estimate — the minimum variance unbiased estimate (MVUE) — of an omniscient observer who has *centralized* access to all the private signals.

Our goal is to find differentially private aggregation mechanisms $\mathcal{M}$ with fast convergence guarantees that minimize CoP parametrized by noise distributions $\{\mathcal{D}_{i,t}\}_{i\in[n],t\geq 1}$ of the agents and subject to their ε differential privacy budget constraints, i.e., "s.t. ε-DP":

$$\mathrm{CoP}(\mathcal{M}) = \inf_{\{\mathcal{D}_{i,\tau}\}_{i\in[n],\tau\in[t]} \text{ s.t. } \varepsilon\text{-DP}} \mathbb{E}_{\{(v_\tau,s_\tau)\}_{\tau\in[t]}} \left[\|v_t - \mu_t\|_2\right]. \tag{4.1}$$

From now on, we will refer to this optimal value as the cost of privacy. In our analysis, the CoP and CoD are proportional to the signal and noise variance. The convergence rate also depends on the number of nodes n and the *SLEM* $b_n^\star$

of the doubly-stochastic adjacency matrix A, which dictates the convergence rate of A^t to its limiting matrix $(\mathbb{1}\mathbb{1}^T)/n$, as $t \to \infty$.

Subsequently, the noise distribution can be optimized by minimizing the weighted variances of the noise terms in the upper bounds subject to DP constraints. Our main results are summarized in Table 4.1. These consist of minimum variance unbiased estimation and online learning of expected values under *(i)* protection of the private signals (Signal DP), and *(ii)* protection of the private signals and the local neighborhoods (Network DP). Table 4.1 summarizes our main contributions.

Moreover, whenever the global sensitivity $\Delta_{n,\Theta}$ is unbounded, something that happens to a variety of sufficient statistics ξ, we rely on the smooth sensitivity introduced by [310] and derive the same algorithms (but with parameters depending on the smooth sensitivity instead of $\Delta_{n,\Theta}$), which achieve (ε, δ)-DP, namely using the smooth sensitivity introduces a compromise in the ε-DP guarantee by a small information leakage probability δ, relaxing the DP constraint for a mechanism $\mathcal{M}$ as follows: $\mathbb{P}[\mathcal{M}(s) \in R] \leq e^{\varepsilon}\mathbb{P}[\mathcal{M}(s') \in R] + \delta$, for all adjacent input pairs (s and s') and all subsets R of the output range space.

Table 4.1: Total Error Bounds. $\Delta_{n,\Theta}$ is the maximum signal sensitivity (absolute value of the derivative of $\xi(\cdot)$), $M_n = \max_{i\in[n]} |\xi(s_i)|$, $a = \max_{i\neq j} a_{ij}$ is the maximum non-diagonal entry of the adjacency matrix A, and $b_n^\star = \max\{\lambda_2(A), |\lambda_n(A)|\}$ is the SLEM of A. The blue terms are due to privacy constraints (CoP), and the red terms are due to decentralization (CoD).

	Minimum Variance Unbiased Estimation	Online Learning of Expected Values
Signal DP	Theorem 4.1.1 $O\left(n(b_n^\star)^t\left(\frac{\Delta_{n,\Theta}}{\varepsilon} + \Gamma_{n,\Theta}\right) + \frac{\Delta_{n,\Theta}}{\varepsilon}\right)$	Theorem 4.1.3 $O\left(\frac{n}{\sqrt{t}}\left(\frac{\Delta_{n,\Theta}}{\varepsilon} + \sqrt{\mathbb{V}\left[\xi(s)\right]}\right)\right)$
Network DP	Corollary 4.1.2 $O\left(n(b_n^\star)^t\left(\frac{\max\{a,\Delta_{n,\Theta}\}}{\varepsilon} + \Gamma_{n,\Theta}\right) + \frac{\max\{a,\Delta_{n,\Theta}\}}{\varepsilon}\right)$	Theorem 4.1.4 $O\left(\frac{n}{\sqrt{t}}\left(\frac{\max\{a,\Delta_{n,\Theta}\}}{\varepsilon} + \sqrt{\mathbb{V}\left[\xi(s)\right]}\right)\right)$

We conduct experiments with two real-world datasets motivated by decentralized decision problems in power grids (see Section 4.1). The first dataset considers the daily consumption of several German Households over three years [286], and the second one considers the US Power Grid network from [419]. Our experiments show that we can achieve (ε, δ)-DP while not significantly sacrificing convergence compared to the non-private baselines. The results also indicate the increased challenges in ensuring network DP compared to Signal DP and the importance of distributional features of the signals, in particular, having sufficient statistics with bounded derivatives.

4.1.2 Related Work

Our results relate to different bodies of literature across the engineering, statistics, and economics disciplines, and in what follows, we shall expand upon these relations.

Decentralized Decision Making and Distributed Learning. Decentralized Decision Making and Distributed Learning have attracted a large body of literature over the years, with notable examples of [73, 398, 399, 326]. Recently, there has been a renewed interest in this topic due to its applications to sensor and robotic networks [93, 311, 229, 27, 26] and emergence of a new literature considering networks of sensor and computational units [365, 300, 299]. Other relevant results investigate the formation and evolution of estimates in social networks and subsequent shaping of the individual and mass behavior through social learning [249, 415, 254, 342, 344]. Obtaining a global consensus by combining noisy and unreliable locally sensed data is a crucial step in many wire-

less sensor network applications; subsequently, many sensor fusion schemes offer good recipes to address this requirement [426, 427]. In many such applications, each sensor estimates the field using its local measurements, and then, the sensors initiate distributed optimization to fuse their local forecast. If all the data from every sensor in the network can be collected in a fusion center, then a jointly optimal decision is readily available by solving the global optimization problem given all the data [14]. However, many practical considerations limit the applicability of such a centralized solution. This gives rise to the distributed sensing problems that include distributed network consensus or agreement [28, 171, 73], and distributed averaging [127]; with close relations to the consensus and coordination problems that are studied in the distributed control theory [216, 285, 79]. Our work contributes to this body of work by providing a privacy-aware method for distributed estimation over a network.

The work most importantly connected to our work is the work of [354], which introduces a first-order DP method for distributed optimization over a network of agents. While their work presents a general first-order method for DP distributed optimization, which is suitable for a larger family of optimization problems that include MVUE, adapting their method to our task comes with important trade-offs in the quality of the estimation, as running their method results in significantly higher error (up to 1000× more; see Figure 4.7) for the MVUE task due to the repeated inclusion of the signal in the belief updates. Moreover, contrary to ours, their method does not support the online learning regime. Finally, the concept of "graph-homomorphic noise" proposed in their paper is equivalent to the Network DP regime of this chapter.

Differential privacy. Differential privacy is a modern definition of data privacy encompassing many previous definitions, such as K-anonymity. A mechanism is differentially private if it maps similar records to the same value with equal probability. One consequence of the definition is that it guarantees that the outcome of a statistical analysis will be identical whether the individual chooses to participate in the social learning process. Many previously proposed mechanisms can be shown to be differentially private, such as randomized response [416], the Laplace mechanism, and the Gaussian mechanism. The randomized response algorithm originally proposed by [416] consists of randomly perturbing binary responses, and it allows the population means to be recovered while giving individual respondents plausible deniability – an instance of adding noise to data.

Statistical disclosure control of donated data, e.g., submitting recommendations to a public policy agency or submitting online product reviews to an e-commerce platform, requires safeguarding donors' privacy against adversarial attacks where standard anonymization techniques are shown to be vulnerable to various kinds of identification [42], linkage and cross-referencing [383, 295, 382], and statistical difference and re-identification attacks [252]. Here, we propose to analyze the efficiency of distributed estimation where agents learn from each other's actions protected by the gold standard of differential piracy [133] to optimize statistical precision against the privacy risks to data donors who engage in social learning.

DP can be implemented using central or local schemes. In centralized DP implementations, individual data are collected, and privacy noise is added to data aggregates, used, e.g., in the U.S. Census Bureau's Disclosure Avoidance

system [405]. In local implementations, DP noising is done as data is being collected. Local methods forego the need for any trusted parties and typically provide more fundamental protection that can withstand a broader range future infiltration, e.g., even a government subpoena for data cannot violate the privacy protection when collected data is itself subject to privacy noising — e.g., Google, LinkedIn, and Apple's DP noising of their user data [21, 147, 87, 357], cf. [423, 190].

Regarding privacy and networks, [248] present a privacy-preserving mechanism to enable private data to diffuse over social networks, where a user wants to access another user's data and provide privacy guarantees on the privacy leak, which depends on the shortest path between two users in the network. [13] study the problem of private weighted sum aggregation with secret weights, where a central authority wants to compute the weighted sum of the local data of some agents under multiple privacy regimes. [345, 346] study influence maximization using samples of network nodes that are collected in a DP manner.

Our work contributes to the above line of work by introducing a novel DP mechanism for distributed estimation and learning of exponential family distributions. Particularly, to the best of our knowledge, in the online learning regime, our algorithm introduces a novel weighting scheme that can protect both the individual signals and the neighboring beliefs, which can efficiently learn the expected value of the sufficient statistic. Moreover, we also provably derive the optimal distributions that minimize the convergence time of the algorithm and show that they are the Laplace distributions with appropriately chosen parameters.

Cyber-Physical Systems. Cyber-Physical Systems (e.g., energy, transportation systems, healthcare systems, etc.) correspond to the building blocks of modern information and communication technologies, whose privacy and security are crucial for the function of such technologies. There have been multiple methods, such as encryption and K-anonymity, to achieve privacy and security in cyber-physical systems [196, 434, 244]. By incorporating differential privacy techniques, such as noise injection or data aggregation, into the design and operation of cyber-physical systems, privacy risks can be mitigated while preserving the utility of the collected data. This ensures that individual privacy is protected, as the data released from these systems cannot be used to infer sensitive information about specific individuals. Moreover, the application of differential privacy to cyber-physical systems enables the collection and analysis of data at scale, allowing for improved system performance, anomaly detection, and predictive maintenance while maintaining the trust of individuals and protecting their privacy in an increasingly connected world [268, 186, 428]. Our method's efficiency, e.g., compared to [354]; see Section 4.1.9 and Appendix C.2, makes it suitable for several large-scale data applications.

Federated Learning (FL). Federated Learning (FL) is a collaborative learning paradigm for decentralized optimization without the need to collect all data points in a central server for gradient calculations [282, 244], with many applications in mind: distributed training of ML models [67, 367, 433], healthcare [225], wireless communications [308], etc. While more general than the setup we consider here, it suffers from issues in terms of communication and privacy. Existing privacy-preserving FL methods (cf. [354]) usually adopt the instance-level differential privacy (DP), which provides a rigorous privacy guarantee but with

several bottlenecks [396]. [395] proposed a privacy-aware FL system that combines DP with secure multiparty computation, which utilizes less noise without sacrificing privacy as the number of federating parties increases and produces models with high accuracy. Other FL methods, such as [436], accommodate differentially private updates via incorporating gradient clipping before adding privacy noise to achieve good performance subject to privacy constraints.

Contrary to most of these methods, which are first-order optimization methods that are suitable to a large variety of losses compared to our method, our zero-order belief updates for the MVUE are simple, more efficient, and have significantly lower error than first-order methods (see Figure 4.7 for comparison with [354]). Moreover, our method can learn from data that arrive in an online way, whereas methods such as [354, 436] are offline. Finally, most of these approaches rely on SGD. In contrast, our method focuses more on the decision-theoretic and statistical problem of estimating the expected value of the sufficient statistics of signals generated by an exponential family distribution.

4.1.3 The Distributed Information Aggregation Problem

Let Θ be any measurable set, and in particular, not necessarily finite. Consider a network of n agents and suppose that each agent $i \in [n]$ observes an i.i.d. samples s_i from a common distribution $\ell(\cdot|\theta)$ over a measurable sample space $\mathcal{S}$ (For simplicity in our proofs, we consider the simple case of 1D signals, i.e., $\mathcal{S} \subseteq \mathbb{R}$. Extending to multi-dimensional signals (i.e., $\mathcal{S} \subseteq \mathbb{R}^s$) is straightforward and considers the ℓ_∞ norm of the partial derivatives.). We assume that $\ell(\cdot|\theta)$

belongs to a one-parameter exponential family so that it admits a probability density or mass function that can be expressed as

$$\ell(s|\theta) = \tau(s)e^{\alpha(\theta)^T \xi(s) - \varkappa(\alpha(\theta))}, \tag{4.2}$$

where $\xi(s) \in \mathbb{R}$ is a measurable function acting as a complete sufficient statistic for the i.i.d. random samples s_i, and $\alpha : \Theta \to \mathbb{R}$ is a mapping from the parameter space Θ to the real line $\mathbb{R}$, $\tau(s) > 0$ is a positive weighting function, and $\varkappa(\alpha) := \ln \int_{s \in \mathcal{S}} \tau(s)e^{\alpha\xi(s)}ds$ is a normalization factor known as the log-partition function. In Equation (4.2), $\xi(\cdot)$ is a complete sufficient statistic for θ. It is further true that $\sum_{i=1}^n \xi(s_i)$ is a complete sufficient statistic given the n i.i.d. signals that the agents have received [56, Section 1.6.1]. In particular, any inferences that involve the unknown parameter θ based on the observed signals $s = (s_i)_{i \in [n]}$ can be equivalently performed given $\sum_{i=1}^n \xi(s_i)$. The agents aim to estimate the expected value of $\xi(\cdot)$: $m_\theta = \mathbb{E}[\xi(s_i)]$, with as little variance as possible. The Lehmann-Scheffé theory — cf. [89, Theorem 7.5.1] — implies that any function of the complete sufficient statistic that is unbiased for m_θ is the almost surely unique minimum variance unbiased estimator of m_θ. In particular, the minimum variance unbiased estimator of m_θ given the initial data sets of all nodes in the network is given by: $\widehat{m_\theta} = (1/n) \sum_{i=1}^n \xi(s_i)$.

For concreteness, we can consider a group of n suppliers whose private signals consist of their contracts, sales orders, and fulfillment data. These suppliers would benefit from aggregating their private information to better estimate market conditions captured by the unknown parameter θ, e.g., to predict future demand. However, sharing their private signals would violate the privacy of their customers and clients. In Section 4.1.4, we explain how the agents can

compute the best (minimum variance) unbiased estimator of m_θ using average consensus algorithms [312] that guarantee convergence to the average of the initial values without direct access to each other's private signals.

4.1.4 The Information Exchange Model

We consider an undirected network graph and let the undirected network $\mathcal{G}(\mathcal{V} = [n], \mathcal{E})$ which corresponds to a Markov chain with a doubly-stochastic symmetric adjacency/transition matrix $A = [a_{ij}]_{i,j=1}^n$ with the uniform stationary distribution. For instance, such an adjacency matrix $A = [a_{ij}]_{i,j=1}^n$ can defined according to the Metropolis-Hastings weights [75]: $a_{ij} = 1/\max\{\deg(i), \deg(j)\}$ if $(j,i) \in \mathcal{E}$, and $[A]_{ij} = 0$ otherwise for $i \neq j$; furthermore, $a_{ii} = 1 - \sum_{j \neq i} a_{ij}$. This choice of weights leads to a Markov chain where the stationary distribution is the uniform distribution [75], and the agents can set these weights locally based on their own and neighboring degrees without the global knowledge of the network structure. For choices of A that yield the fastest mixing Markov chain (but may not be locally adjustable), see [75].

Algorithm 3 Non-Private Minimum Variance Unbiased Estimation Algorithm

The agents initialize with: $\mu_{i,0} = \xi(s_i)$, and in any future time period, the agents communicate their values and update them according to the following rule:

$$\mu_{i,t} = a_{ii}\,\mu_{i,t-1} + \sum_{j \in \mathcal{N}_i} a_{ij}\mu_{j,t-1}. \tag{4.3}$$

The mechanisms for convergence, in this case, rely on the product of stochastic matrices, similar to the mixing of Markov chains (cf. [266, 365]); hence, many available results on mixing rates of Markov chains can be employed to provide finite time grantees after T iteration of the average consensus algorithm for fixed

T. Such results often rely on the eigenstructure (eigenvalues/eigenvectors) of the communication matrix A, and the facts that it is a primitive matrix and its ordered eigenvalues satisfy $-1 < \lambda_n(A) \leq \lambda_{n-1}(A) \leq \ldots \leq \lambda_1(A) = 1$, as a consequence of the Perron-Frobenius theory [364, Theorems 1.5 and 1.7].

Moreover, another mechanism considers learning the expected values online. In this method, agents receive signals at every round and then update their estimates by averaging the estimates of their neighbors, their own estimates, and the new signals.

Algorithm 4 Non-Private Online Learning of Expected Values

Initializing $\mu_{i,0}$ arbitrarily, in any future time period $t \geq 1$ the agents observe a signal $s_{i,t}$, communicate their current values $\mu_{i,t-1}$, and update their beliefs to $\mu_{i,t}$, according to the following rule:

$$\mu_{i,t} = \frac{t-1}{t}\left(a_{ii}\,\mu_{i,t-1} + \sum_{j \in \mathcal{N}_i} a_{ij}\mu_{j,t-1}\right) + \frac{1}{t}\xi(s_{i,t}). \tag{4.4}$$

The $1/t$ discounting provided in the above algorithm enables learning the expected values $m_\theta = \mathbb{E}_\theta[\xi(s)]$ asymptotically almost surely with a variance that scales as $O(1/t)$; i.e., linearly in time. As shown in [343], the variance upper bound comprises two terms. The former term considers the rate at which the Markov chain with transition matrix A is mixing and is governed by the spectral gap, i.e., the second largest magnitude of the eigenvalues of A. The latter term captures the diminishing variance of the estimates with the increasing number of samples gathered by all the agents in the network.

Now that we have the necessary background in distributed estimation, we present the two DP protection mechanisms that this chapter considers: the Signal DP and the Network DP.

4.1.5 Differential Privacy Protections

In this Chapter, we consider two methods for differential privacy and refer to them as *Signal Differential Privacy (Signal DP)* and *Network Differential Privacy (Network DP)*. Both algorithms are local in principle; the agents simply add noise to their estimates to achieve a desired privacy guarantee. Roughly, Signal DP adds noise to protect the signal $s_{i,t}$ of each agent, and Network DP adds noise to protect the signal $s_{i,t}$ of each agent, as well as the estimates $\{\nu_{j,t-1}\}_{j\in\mathcal{N}_i}$ of her neighbors from round $t-1$. We assume that the non-private network dynamics evolve as

$$\mu_{i,t} = F_{i,t}(\mu_{i,t-1}) + G_{i,t}\left(\left\{\mu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) + H_{i,t}(s_{i,t}), \tag{4.5}$$

for each agent $i \in [n]$, and $t \geq 1$, where $F_{i,t} : \mathbb{R} \to \mathbb{R}$, $G_{i,t} : \mathbb{R}^{d_i} \to \mathbb{R}$, and $H_{i,t} : \Theta \to \mathbb{R}$ are functions determined by the learning algorithm, and correspond to the information from the agent's own estimate, the information from the neighboring estimates, and the information from the agent's private signal respectively. To achieve differential privacy, each agent adds some amount of noise $d_{i,t}$ drawn from a distribution $\mathcal{D}_{i,t}$ to their estimate and reports the noisy estimate to their neighbors. The agent can either aim to protect only their private signal – which we call Signal DP and denote by $\mathcal{M}^S$ –, or protect their network connections and their private signal – which we call Network DP and denote by $\mathcal{M}^N$. The noisy dynamics are:

$$\nu_{i,t} = F_{i,t}(\nu_{i,t-1}) + \underbrace{G_{i,t}\left(\left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) + \overbrace{H_{i,t}(s_{i,t})}^{\text{Signal DP } \mathcal{M}^S_{i,t}}}_{\text{Network DP } \mathcal{M}^N_{i,t}} + d_{i,t} \tag{4.6}$$

In Equation (4.6) and Figure 4.1, we have outlined the dynamics of the two types of privacy protections. Formally, the two types of mechanisms can also be written as

$$\psi_{\mathcal{M}_{i,t}^S}(s_{i,t}) = H_{i,t}(s_{i,t}) + d_{i,t}, \tag{$\mathcal{M}_{i,t}^S$}$$

$$\psi_{\mathcal{M}_{i,t}^N}\left(s_{i,t}, \left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) = H_{i,t}(s_{i,t}) + G_{i,t}\left(\left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) + d_{i,t}, \tag{$\mathcal{M}_{i,t}^N$}$$

and the ε-DP requirement is denoted as

$$\left|\log\left(\frac{\mathbb{P}\left[\psi_{\mathcal{M}_{i,t}^S}(s_{i,t}) = x\right]}{\mathbb{P}\left[\psi_{\mathcal{M}_{i,t}^S}(s'_{i,t}) = x\right]}\right)\right| \leq \varepsilon \text{ for all } s_{i,t}, s'_{i,t} \in \mathcal{S} \text{ s.t. } \left\|s_{i,t} - s'_{i,t}\right\|_1 \leq 1$$

$$\left|\log\left(\frac{\mathbb{P}\left[\psi_{\mathcal{M}_{i,t}^N}\left(s_{i,t}, \left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) = x\right]}{\mathbb{P}\left[\psi_{\mathcal{M}_{i,t}^N}\left(s'_{i,t}, \left\{\nu'_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) = x\right]}\right)\right| \leq \varepsilon \text{ for all } \left(s_{i,t}, \left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right), \left(s'_{i,t}, \left\{\nu'_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) \in \mathcal{S}\times\mathbb{R}^{\deg(i)}$$

$$\text{s.t. } \left\|\left(s_{i,t}, \left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right) - \left(s'_{i,t}, \left\{\nu'_{j,t-1}\right\}_{j\in\mathcal{N}_i}\right)\right\|_1 \leq 1$$

for all $x \in \mathbb{R}$.

In a local privacy scheme, the DP noise of the measurements can occur at the agent level by adding noise to the collected signals. Noise may be added to the signals after measurement to protect them against the revelations of belief exchange. The central scheme assumes a trusted environment where signal measurements can be collected without privacy concerns, but to the extent that protecting signals from the revelations of beliefs exchange is concerned, these methods would be equivalent.

4.1.6 Minimum Variance Unbiased Estimation with Signal DP

We present our first algorithm, which considers Minimum Variance Unbiased Estimation (MVUE). In this task, we aim to learn the MVUE of m_θ, i.e., to construct the estimate $\widehat{m_\theta} = (1/n)\sum_{i=1}^n \xi(s_i)$ through local information exchange. In the non-private version of the algorithm, the agents start with some private signals $\{s_i\}_{i\in[n]}$, calculate the sufficient statistics $\{\xi(s_i)\}_{i\in[n]}$ and then exchange these

initial estimates with their local neighbors. The non-private algorithm converges to $\widehat{m_\theta}$ in $t = O\left(\frac{\log(n\Gamma_{n,\Theta}/\rho)}{\log(1/b_n^\star)}\right)$ steps to ρ-accuracy, which depends on the number of nodes n, the maximum absolute value $\Gamma_{n,\Theta}$ of the sufficient statistics, and the SLEM $b_n^\star$ of the transition matrix A.

In its DP version, the algorithm proceeds similarly to the non-DP case, except each agent i adds noise d_i to their sufficient statistic $\xi(s_i)$. As we show later, to respect ε-DP, the noise d_i depends on the agent's realized signal s_i, the sufficient statistics $\xi(\cdot)$, and the privacy budget ε. We provide the algorithm for the differentially private in Algorithm 5:

Algorithm 5 Minimum Variance Unbiased Estimation with Signal/Network DP

The agents initialize with $\nu_{i,0} = \xi(s_i) + d_i$ where $d_i \sim \mathcal{D}_i$ ($\mathcal{D}_i$ is an appropriately chosen noise distribution), and in any future time period the agents communicate their values and update them according to the following rule:

$$\nu_{i,t} = a_{ii}\,\nu_{i,t-1} + \sum_{j\in\mathcal{N}_i} a_{ij}\nu_{j,t-1}. \tag{4.7}$$

Regarding convergence, in Theorem 4.1.1, we prove that the convergence error is incurred due to two sources. The first source of error is the error due to the omniscient observer, which is the same as in the non-DP case, and the second source of error is incurred due to the privacy noise. Briefly, the latter term can be roughly decomposed to correspond to two terms: the former term is due to estimating the minimum variance unbiased estimator due to the noise, i.e. $(1/n)\sum_{i=1}^n d_i$ and is vanishing with a rate proportional to $\log\left(\sum_{i=1}^n \mathbb{V}\left[d_i\right]\right)/\log(1/b_n^\star)$, and an additional non-vanishing term which is due to the mean squared error of $(1/n)\sum_{i=1}^n d_i$ which corresponds to the sum of the variances of the signals.

To minimize the convergence error, it suffices to minimize each variance

$\mathbb{V}[d_i]$ subject to ε-DP constraints. By following recent results on the DP literature (cf. [247]) we deduce that the variance minimizing distribution under ε-DP constraints are the Laplace distributions with parameters $\Delta_{n,\Theta}/\varepsilon$, where $\Delta_{n,\Theta}$ corresponds to the signal sensitivity (see below) and ε is the privacy budget. We present our Theorem (proved in Appendix C.1.1):

Theorem 4.1.1 (Minimum Variance Unbiased Estimation with Signal DP)**.** *The following hold for Algorithm 5:*

1. *For all t and any zero-mean zero-mean distributions*

$$\mathbb{E}\left[\|\nu_t - \mathbb{1}\widehat{m_\theta}\|_2\right] \leq (1 + \sqrt{(n-1)}(b_n^\star)^t)\sqrt{\sum_{j=1}^{n}\mathbb{V}\left[d_j\right]} + \sqrt{n(n-1)}(b_n^\star)^t\Gamma_{n,\Theta}, \quad (4.8)$$

   where $\Gamma_{n,\Theta} = \max_{i\in[n]}|\xi(s_i)|$ and $b_n^\star = \max\{\lambda_2(A), |\lambda_n(A)|\}$.

2. *The optimal distributions $\{\mathcal{D}_i^\star\}_{i\in[n]}$ that minimize the MSE for each agent are the Laplace distribution with parameters $\Delta_{n,\Theta}/\varepsilon$ where $\Delta_{n,\Theta}$ is the global sensitivity of ξ Subsequently,* $\mathrm{TE}(\mathcal{M}^S) = O\left(n(b_n^\star)^t\left(\Gamma_{n,\Theta} + \frac{\Delta_{n,\Theta}}{\varepsilon}\right) + \frac{\Delta_{n,\Theta}}{\varepsilon}\right)$.

Finally, we note that similarly, in the multi-dimensional case, the sensitivity would be $\Delta_{n,\Theta} = \max_{s\in\Theta}\|\nabla_s\xi(s)\|_\infty$.

In the above Theorem, it is tempting to think that the local sensitivity of each agent, i.e., $\Delta_{n,\Theta}\xi_i = |d\xi(s_i)/ds_i|$ can be used to calibrate the noise distribution that preserves differential privacy and has the minimum variance. However, as it has been shown in [310], releasing noise that depends on the local sensitivity can compromise the signal. However, there are cases where global sensitivity is unsuitable for the learning task. For instance, in many distributions, such as the log-normal distribution, the global sensitivity may be unbounded (e.g.,

$\xi(s) = \log s$ for the log-normal and the sensitivity is $+\infty$ in this case). A possible solution for this situation and many exponential family distributions is to use another sensitivity instead of the global sensitivity. [310, Definition 2.2] proposes the use of the γ-smooth sensitivity. The way of constructing the γ-smooth sensitivity is to calculate

$$S^*_{\xi,\gamma}(s) = \max_{k>0} \left\{ e^{-\gamma k} \max_{s':\|s'-s\|_1=k} |\xi(s') - \xi(s)| \right\}.$$

Using the Laplace mechanism with parameters $2S^\star_{\xi,\gamma}(s)/\varepsilon$ for $\gamma = \varepsilon/(2\log(2/\delta))$ would guarantee (ε, δ)-DP; see [310, Corollary 2.4].

For example, we will consider the case of mean estimation in a log-normal distribution with known variance, a common task in many sensor networks, as we argue in Section 4.1.9. The sufficient statistic in this case is $\xi(s) = \log s$, and the local sensitivity at distance k can be computed to be k/s. Therefore, the smooth sensitivity is (note the global sensitivity in this case is unbounded):

$$S^*_{\xi,\gamma}(s) = \max_{k>0} \left\{ e^{-\beta k} \frac{k}{s} \right\} = \frac{1}{e\gamma s} = \frac{2\log(2/\delta)}{e\varepsilon s}, \quad \text{for } s > 0. \tag{4.9}$$

If agents have access to several signals, and the exact formula of ξ is not known, the sensitivity can still be approximated via samples as shown in [424].

Note that to achieve Network DP, one natural algorithm is to add noise $d_{i,t}$ at each round of Algorithm 5 at a high enough level to protect both the network neighborhoods and the private signals. The issue with this algorithm is that it is divergent, i.e., $\mathbb{E}\left[\|\nu_t\|_2^2\right] \to \infty$, because the estimate at time t is $\nu_t = A^t\xi + \sum_{\tau=0}^{t-1} A^\tau d_{t-\tau}$, and its mean squared error, i.e., $\mathbb{E}\left[\left\|\sum_{\tau=0}^{t-1} A^\tau d_{t-\tau}\right\|_2^2\right]$, grows linearly with n and t. To avoid the accumulation of the DP noise, we should limit the DP noising to the initial step, which will achieve a bounded error because the mixing matrix, A, is doubly stochastic. To this end, we choose the noise level

to satisfy ε-DP with the aim of protecting both signals and network connections — and run Algorithm 5 at the new noise level. The error of this algorithm will be identical to the error bound of Theorem 4.1.1. However, the sensitivity of the noise should be set to accommodate both network and signal dependencies as follows: $\Delta_{n,\Theta} v_i^{\mathcal{M}^N} = \max\left\{\Delta_{n,\Theta}, \max_{j\in\mathcal{N}_i} a_{ij}\right\}$, and the optimal distributions will be $\mathcal{D}_i^\star = \text{Lap}\left(\max\left\{\Delta_{n,\Theta}, \max_{j\in\mathcal{N}_i} a_{ij}\right\}/\varepsilon\right)$; see Corollary 4.1.2. In the case that $\Delta_{n,\Theta}$ is unbounded, we can replace $\Delta_{n,\Theta}$ with the smooth sensitivity accounting for the network effects, i.e., $\max\left\{\max_{j\neq i} a_{ij}, S^*_{\xi,\gamma}(s_i)\right\}$ for each signal s_i and get an (ε,δ)-DP algorithm. Note that private signals will remain DP-protected by the post-processing immunity of the Laplace mechanism. In Appendix C.1.2, we use induction to show that Network DP is preserved at the ε level for all times t when the mixing matrix A is non-singular. The following corollary summarizes our results:

Corollary 4.1.2 (Total Error of Minimum Variance Unbiased Estimation with Network DP)**.** *Assume the mixing matrix A is non-singular, let $\Delta_{n,\Theta}$ be the global sensitivity of ξ, and $a = \max_{i\neq j} a_{ij}$. The Total Error of Algorithm 5 with Network DP satisfies*

$$\text{TE}(\mathcal{M}^N) = O\left(n(b_n^\star)^t\left(\Gamma_{n,\Theta} + \frac{\max\{a,\Delta_{n,\Theta}\}}{\varepsilon}\right) + \frac{\max\{a,\Delta_{n,\Theta}\}}{\varepsilon}\right).$$

We note that the above analysis is tight because there exists an instance for which the upper bound is precisely achieved (for any noise distribution). To show this, consider the complete graph K_n, which corresponds to weights $a_{ij} = 1/n$ for all $i,j \in [n]$ with a spectral gap of zero, and $s_i \sim \mathcal{N}(0,1)$. The network dynamics on the complete graph converge in one iteration, and it is straightforward to show that the total error (TE) converges to $1/\varepsilon$ as $n \to \infty$ for any noise distributions subject to ε-DP constraints (by the central limit theorem), i.e., Equation (C.1) in the Supplementary Materials holds with equality.

4.1.7 Online Learning of Expected Values

We consider the online learning framework where the agents aim to learn the common expected value $m_\theta = \mathbb{E}_\theta[\xi(s)]$ of the sufficient statistics of their signal distributions. In this regime, the agents observe signals $s_{i,t}$ at every time $t \geq 1$ and update their estimates $\nu_{i,t}$ by weighing the information content of their most recent private signals, $\xi(s_{i,t})$, their previous estimates, $\nu_{i,t-1}$, and the estimates of their neighbors, $\{\nu_{j,t-1}\}_{j\in\mathcal{N}_i}$. The mechanisms that we analyze in this section will accommodate two types of privacy needs with convergence and ε-DP guarantees for the agents:

$\mathcal{M}^S$: *Signal DP (Algorithm 6).* Here the agent adds noise to privatize their belief $\nu_{i,t}$ with respect to their signal. To assert the consistency of the estimator, the agent averages her previous estimate and the estimates of her neighbors with weight $(t-1)/t$ and her signal with weight $1/t$, similarly to Algorithm 4. Therefore, the local sensitivity of this mechanism is the sensitivity of the sufficient statistic weighted by $1/t$ and equals $\Delta_{n,\Theta}\nu_{i,t}^{\mathcal{M}^S} = \frac{\Delta_{n,\Theta}}{t}$.

$\mathcal{M}^N$: *Network DP (Algorithm 7).* Here we consider the protection of the agent's signals $s_{i,t}$ together with their local neighborhood, namely the neighboring beliefs $\left\{\nu_{j,t-1}\right\}_{j\in\mathcal{N}_i}$. We note that when deciding the noise level at time t, we do not need to include the agent's own belief from time $t-1$ in the DP protection; $\nu_{i,t-1}$ including all the private signals up to and including at time $t-1$ remain protected by the property of the post-processing immunity. If we were to use Algorithm 6 for Network DP the sensitivity of the mechanism would be $\max\left\{\frac{\Delta_{n,\Theta}}{t}, \frac{t-1}{t}\max_{j\in\mathcal{N}_i} a_{ij}\right\}$ which approaches 1 as $t \to \infty$ and violates the consistency of the estimator $\nu_{i,t}$. For this reason, we need to adapt the weighting scheme of Algorithm 6 to be consistent and respect

Network DP. We give more details of the altered algorithm (Algorithm 7) in Section 4.1.8.

Algorithm 6 Online Learning of Expected Values with Signal DP

In any time period $t \geq 1$ the agents observe a signal $s_{i,t}$, and update their estimates according to the following rule:

$$\nu_{i,t} = \frac{t-1}{t}\left(a_{ii}\,\nu_{i,t-1} + \sum_{j\in\mathcal{N}_i} a_{ij}\nu_{j,t-1}\right) + \frac{1}{t}\left(\xi(s_{i,t}) + d_{i,t}\right), \tag{4.10}$$

where $d_{i,t} \sim \mathcal{D}_{i,t}$ is appropriately chosen noise.

Here we will analyze the performance of Algorithm 6 where agents only protect their signals and present the corresponding error analysis. The error of the estimates $\nu_{i,t}$ compared to the expected value $m_\theta = \mathbb{E}_\theta[\xi(s)]$, again consists of two terms; one due to decentralization and the statistics of the signals themselves (CoD), and another due to the variances of the added DP noise variables (CoP). Each of these two terms decays at a rate of $1/\sqrt{t}$. They, in turn, can be bounded by the sum of two terms: a constant that is due to the principal eigenvalue of A and represents the convergence of the sample average to m_θ, and $n-1$ terms due to $|\lambda_i(A)|$ for $2 \leq i \leq n$ which dictate the convergence of the estimates $\nu_{i,t}$ to their sample average. The latter depends on the number of nodes n and the SLEM $b_n^\star$ of matrix A. We formalize our results as follows (proved in Appendix C.1.3):

Theorem 4.1.3 (Online Learning of Expected Values with Signal DP)**.** *The following hold for Algorithm 6 and mechanism $\mathcal{M}^S$:*

1. *For every time t, and all distributions $\{\mathcal{D}_{i,t}\}_{i\in[n],t\geq 1}$ we have that*

$$\mathbb{E}\left[\|\nu_t - \mathbb{1}m_\theta\|_2\right] \leq \frac{1}{t}\left(\sqrt{nt\mathbb{V}\left[\xi(s)\right]} + \sqrt{\sum_{j=1}^{n}\sum_{\tau=0}^{t-1}\mathbb{V}\left[d_{j,t-\tau}\right]}\right)\left(1 + \sqrt{\frac{n-1}{1-(b_n^\star)^2}}\right).$$

2. *The optimal distributions $\{\mathcal{D}_{i,t}^\star\}_{i\in[n],t\geq 1}$ are $\mathcal{D}_{i,t}^\star = \mathrm{Lap}\left(\Delta_{n,\Theta}/\varepsilon\right)$, where $\Delta_{n,\Theta}$ is the global sensitivity. Moreover, we have:* $\mathrm{TE}(\mathcal{M}^S) = O\left(\frac{n}{\sqrt{t}}\left(\sqrt{\mathbb{V}\left[\xi(s)\right]} + \frac{\Delta_{n,\Theta}}{\varepsilon}\right)\right)$.

4.1.8 Online Learning of Expected Values with Network DP

Above, we briefly discussed why a learning algorithm that puts weights $\frac{t-1}{t}$ on the network predictions and $\frac{1}{t}$ on the private signal would not work (and in fact, the dynamics become divergent in that case). In Algorithm 7, we present a different learning scheme that uses weights $\frac{1}{t}$ for the private signals and neighboring observations and $1 - \frac{1}{t}(2 - a_{ii})$ for the previous beliefs of the agent. The motivation behind this learning scheme is that the sensitivity is now going to be $\Delta_{n,\Theta}\nu_{i,t}^{\mathcal{M}^N} = \frac{1}{t}\max\left\{\max_{j\in\mathcal{N}_i} a_{ij}, \Delta_{n,\Theta}\right\}$ which goes to zero, instead of $\max\left\{\frac{t-1}{t}\max_{j\in\mathcal{N}_i} a_{ij}, \frac{1}{t}\Delta_{n,\Theta}\right\}$ which approaches 1. The drawback is that the added self-weight on one's own beliefs at every time step will slow down the mixing time and convergence. In the sequel, we present Algorithm 7 and analyze its performance.

Algorithm 7 Online Learning of Expected Values with Network DP

In any time period $t \geq 1$ the agents observe a signal $s_{i,t}$ and update their estimates according to the following rule:

$$\nu_{i,t} = \left(1 - \frac{1}{t}(2 - a_{ii})\right)\nu_{i,t-1} + \frac{1}{t}\left(\sum_{j\in\mathcal{N}_i} a_{ij}\nu_{j,t-1} + \xi(s_{i,t})\right) + \frac{1}{t}d_{i,t}, \tag{4.11}$$

where $d_{i,t} \sim \mathcal{D}_{i,t}$ is appropriately chosen noise.

We can write the above system in matrix notation as $\nu_t = \left(B(t) - \frac{1}{t}I\right)\nu_{t-1} + \frac{1}{t}\xi_t + \frac{1}{t}d_t$ where $b_{ii}(t) = 1 - \frac{1}{t}(1 - a_{ii})$ and $b_{ij}(t) = \frac{1}{t}a_{ij}$ for all $j \neq i$. First, we study the convergence of Algorithm 7 when no noise is added, i.e., $d_t = 0$. Note that similarly to Algorithm 6, the error term is comprised of two terms, one owing to the principal eigenvalues of $C(t) = B(t) - \frac{1}{t}I$, i.e., $\lambda_1(C(t)) = 1 - 1/t$ which controls the convergence of the sample average of the estimates to m_θ, and $n - 1$ terms due to $|\lambda_i(C(t))|$ which control the convergence of the estimates $\nu_{i,t}$ to their sample average.

Theorem 4.1.4 (Online Learning of Expected Values with Network DP)**.** *For Algorithm 7, the following hold:*

1. *For all $t \geq 1$ and all distributions $\{\mathcal{D}_{i,t}\}_{i\in[n],t\geq 1}$, we have that*

$$\mathbb{E}\left[\|\nu_t - \mathbb{1}m_\theta\|_2\right] \leq \frac{1}{t}\left(\sqrt{nt\mathbb{V}\left[\xi(s)\right]} + \sqrt{\sum_{i=1}^{n}\sum_{\tau=0}^{t-1}\mathbb{V}\left[d_{i,t-\tau}\right]}\right)\left(1 + \sqrt{\frac{n-1}{3-2b_n^\star}}\right).$$

2. *The optimal distributions $\{\mathcal{D}_{i,t}^\star\}_{i\in[n],t\geq 1}$ that minimize the MSE bound subject to ε-DP are the Laplace Distributions with parameters $\max\left\{\max_{j\in\mathcal{N}_i} a_{ij}, \Delta_{n,\Theta}\right\}/\varepsilon$. Moreover, if $\Delta_{n,\Theta}$ is the global sensitivity and $a = \max_{i\neq j} a_{ij}$, then*

$$\mathrm{TE}(\mathcal{M}^N) = O\left(\frac{n}{\sqrt{t}}\left(\frac{\max\{a, \Delta_{n,\Theta}\}}{\varepsilon} + \sqrt{\mathbb{V}\left[\xi(s)\right]}\right)\right).$$

We note that the analysis is tight, and the tight example is precisely the same as the example we provided for MVUE.

4.1.9 Real-World Experiments with Household Energy Consumption Data and Data from the US Power Grid

To showcase the effectiveness of our algorithms, i.e., convergence to the actual estimates subject to (ε, δ)-DP, we conduct two experiments that correspond to the estimation of power consumption in the electric grid.

The first case considers estimating power consumption via electricity measurements of individual households. Consumption behavior is considered highly sensitive. It can reveal compromising information about daily habits and family illnesses or pose a security threat if exploited by an adversary, e.g.,

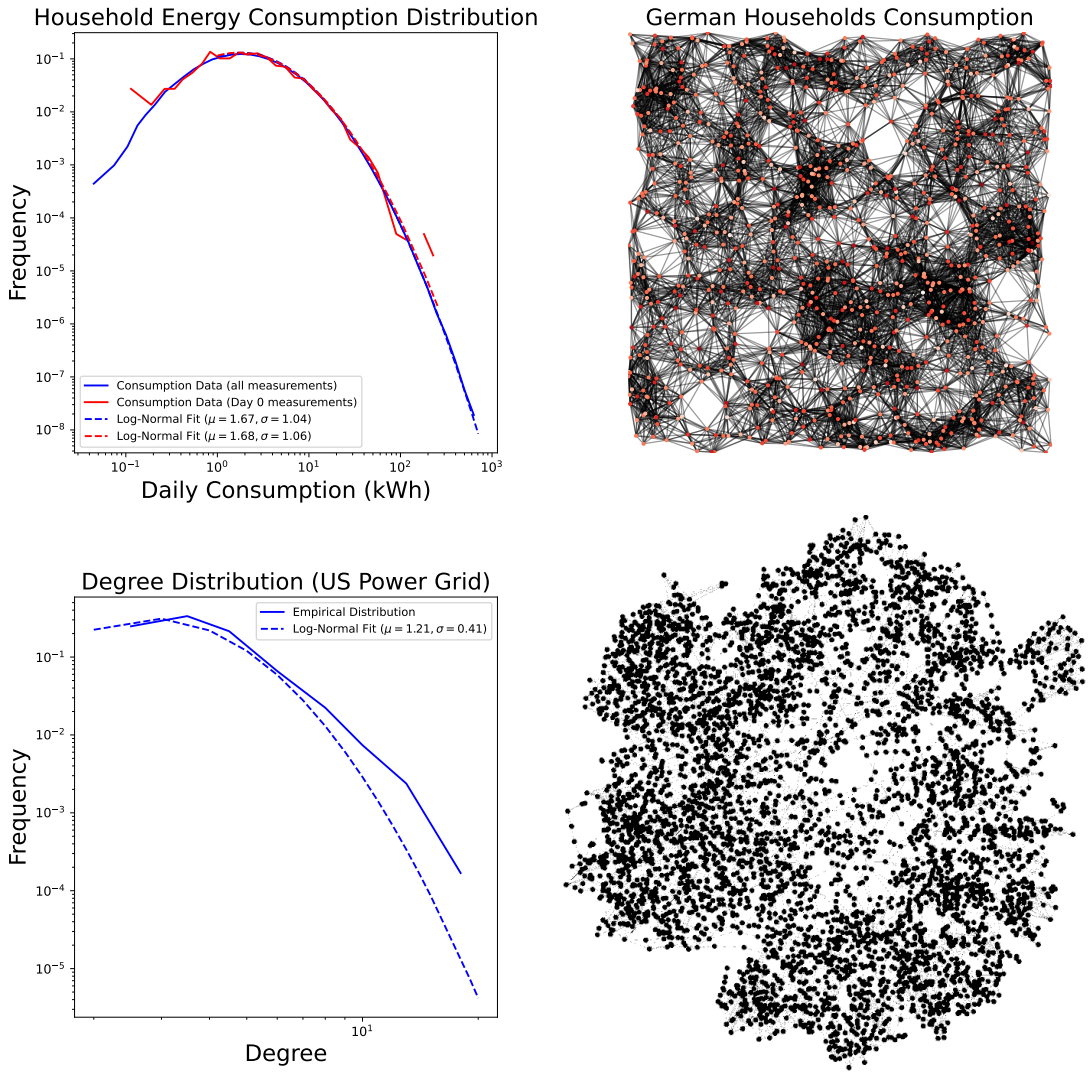


Figure 4.2: Distribution of Daily Consumption (in kWh) for the GEM House openData with log-normal fits is shown on the left (for all measurements and Day 0 measurements), followed by a visualization of the generated random geometric network with $\rho = 0.1$. The next two figures show the US Power Network degree distribution with log-normal fit, followed by its visualization.

to coordinate attack time. Here, we assume that each household faces a privacy risk in sharing their measurements, and they may decide to mitigate the privacy risks by adding noise to their estimates. The ability to estimate average consumption in a distributed manner is useful for distributed load balancing and deciding generation plans.

For this scenario, we consider the GEM House openData dataset [286], which contains power consumption measurements of $n = 969$ individual households over $T = 1096$ days (i.e., three years). The dataset contains cumulative power consumption measurements $c_{i,t}$ for each particular day. To extract the actual measurements (in kWh) $s_{i,t}$ we take the differences between consecutive days and divide by 10^{10} (see Section 3.2.1 of [286]), i.e., $s_{i,t} = \frac{c_{i,t} - c_{i,t-1}}{10^{10}}$. We observe that $s_{i,t}$ follows a log-normal distribution with mean $\mu = 1.67$ and standard deviation $\sigma = 1.04$, as shown in Figure 4.2. Moreover, in this dataset, the network structure is absent. For this reason, we generate a random geometric graph, i.e., we generate $n = 969$ nodes randomly distributed in $[0, 1]^2$ and connect nodes with a distance at most $\rho = 0.1$. Random geometric graphs have been used to model sensor networks [237] and correspond to a straightforward criterion for determining links since they connect nearby households. For a fixed random seed (seed = 0), the network contains $m = 13,236$ edges and is visualized in Figure 4.2.

The second dataset examines estimating power consumption in the US Power Grid Network from [419]. In this case, we hypothesize that each power station faces a privacy risk – for example, vulnerability to a cyber attack – in sharing their measurements and decides to reduce its privacy risk by adding noise. The network contains $n = 4,941$ nodes and $m = 6,594$ edges. Figure 4.2 shows the power network and its degree distribution. Here we artificially generate i.i.d. signals for $T = 100$ as $s_{i,t} \sim \text{LogNormal}(\mu = 10, \sigma = 1)$.

In both cases, the task is to estimate each log-normal distribution's mean μ in two scenarios. In the first scenario, we estimate the mean only from the initial measurements, i.e., estimate $\widehat{\mu}_{\text{MVUE}} = \frac{\sum_{i=1}^{n} \log s_{i,1}}{n}$. Figure 4.3 presents some sample

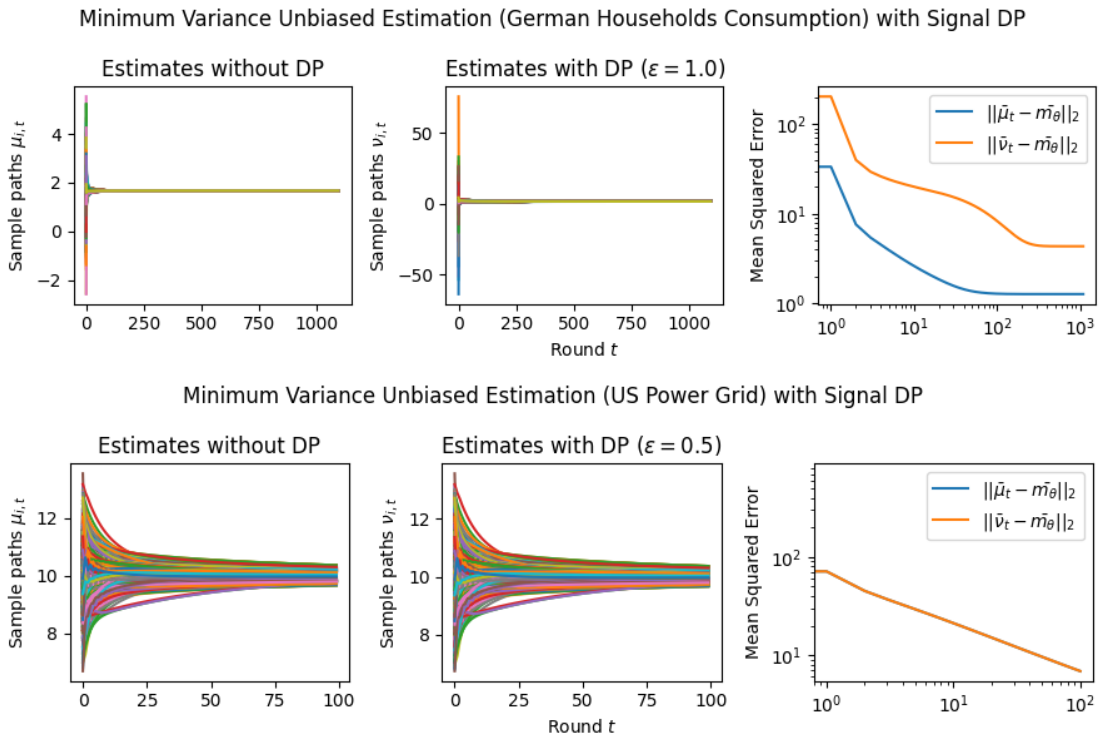


Figure 4.3: Sample Paths for MVUE with Signal DP. Note the large error in the case of the German household dataset is because protecting households with low (near zero) consumption rates even at a relatively high privacy budget ($\varepsilon = 10$) comes at a huge cost to accuracy.

paths for this task as the horizon t varies, and Figure 4.7 presents the final MSE after T for various values of the privacy budget ε. In the second scenario, we estimate the mean with online learning (OL) to estimate $\widehat{\mu}_{\text{OL}} = \frac{\sum_{i=1}^{n}\sum_{t=1}^{T}\log s_{i,t}}{nT} \to \mathbb{E}[\log s] = \mu_{\text{OL}}$. We run simulations in both regimes where we want to protect the signal and the network connections. Because in this case the global sensitivity is unbounded, we use the smooth signal sensitivities $S^*_{\xi,\gamma}(s_{i,t}) = \frac{2\log(2/\delta)}{e\varepsilon s_{i,t}}$ for each signal $s_{i,t}$ with $\delta = 0.01$. The resulting algorithms are (ε, δ)-DP (see Section 4.1.6).

Finally, in Appendix C.2 we explain the adaptation of [354] first-order DP consensus algorithm to both MVUE and OL tasks. Figure 4.7 shows the comparison of MSE performances between our algorithms and [354] given the same privacy budget per agent. Compared to [354], our method is able to achieve

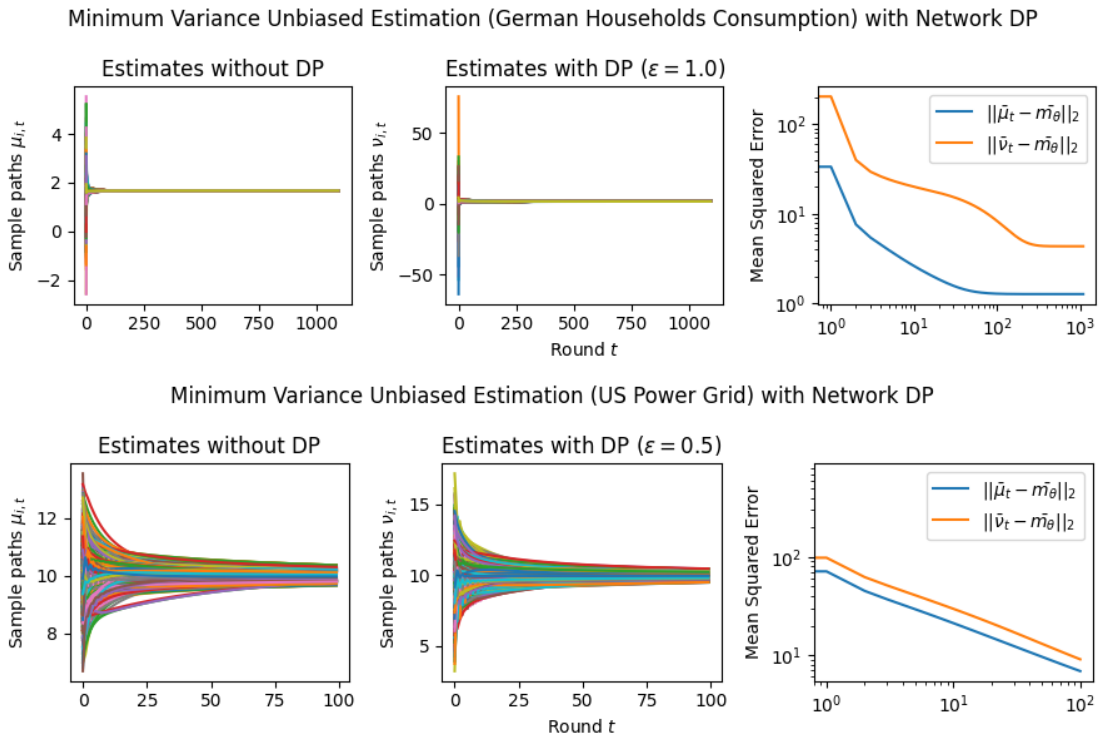


Figure 4.4: Sample Paths for MVUE with Network DP. Note that even requiring a moderate accuracy in the case of the German household dataset comes at a high cost to privacy ($\varepsilon = 1$), pointing to the challenges of maintaining privacy when sensitivities cannot be locally bounded (some household consumption values are close to zero).

significantly smaller MSE under the same total privacy budget; $\approx 1000\times$ smaller for both datasets. While [354]'s algorithm are applicable to a broader set of tasks than the MVUE and OL estimation setups presented here, their inclusion of private signals at every iteration entails DP noising at every step of the iteration and comes at a higher cost to accuracy.

In all cases of signal DP with the US power grid network, the DP noise did not affect the convergence rate in practice for this choice of signals, privacy budget ε, and information leakage probability δ. Also, we observe that the Signal DP algorithm converges faster than the online learning algorithm with Network DP (even in the absence of DP noise) because of the underlying mixing matri-

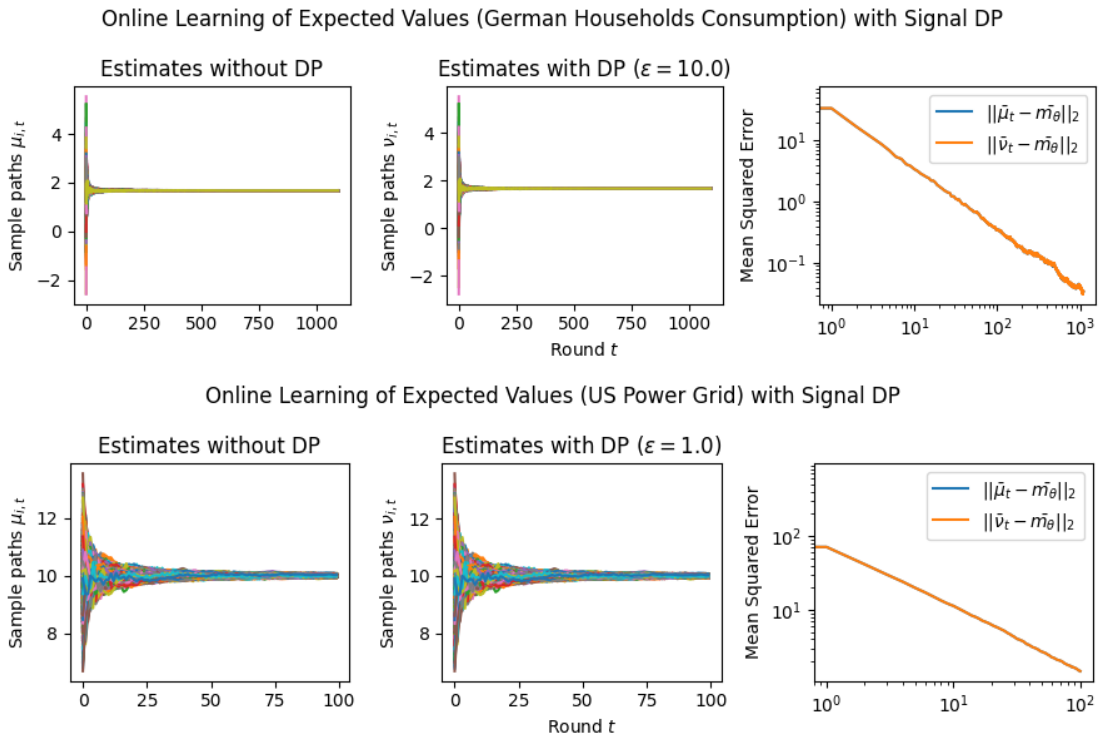


Figure 4.5: Sample Paths for Online Learning of Expected Values with Signal DP. Choosing ε large enough leads to a convergent behavior for the German household dataset, but no meaningful privacy protection can be afforded in that case ($\varepsilon = 10$).

ces, which are $\frac{t-1}{t}A$, and $C(t) = \frac{t-2}{t}I + \frac{1}{t}A$ respectively. Moreover, both of these algorithms converge faster (with and without DP noise) than the MVUE. This is expected since the MVUE has access to n samples in total, while the online algorithms have access to nt signals and can bring the estimation error down by a $1/t$ factor. Comparison of Signal DP (Figures 4.3 and 4.5) with Network DP (Figures 4.4 and 4.6) for MVUE and online learning tasks points to the increased difficulty of ensuring network DP: network privacy protections are harder to achieve and they imply signal protections automatically. On the other hand, when the local sensitivities can grow large — as with the German household dataset — maintaining privacy for households with low consumption comes at a huge cost to accuracy (see, e.g., Figure 4.5). This is because for the log-normal

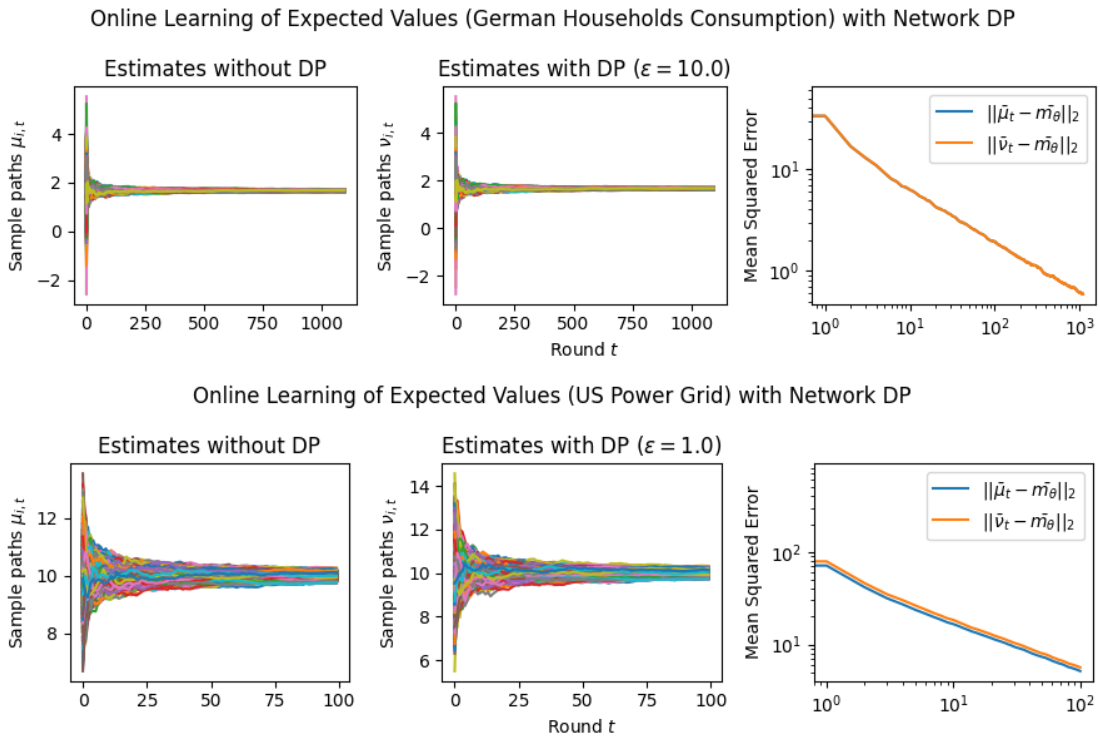


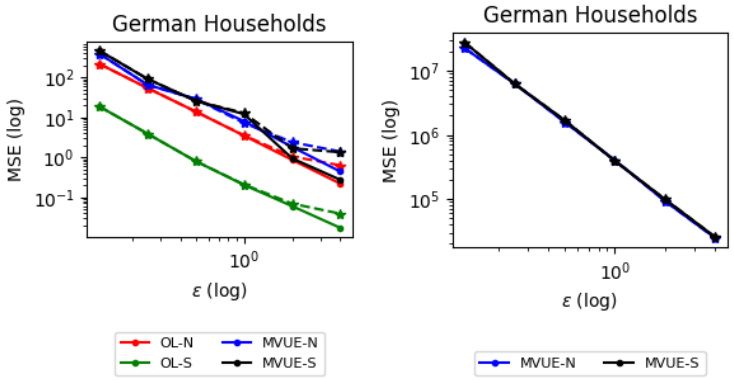
Figure 4.6: Sample Paths for the Online Learning of Expected Values with Network DP. Protecting network neighborhoods is a harder task than protecting private signals. While almost perfect signal DP can be achieved with reasonable accuracy for the US power grid network ($\varepsilon = 1$ in Figure 4.5), even moderate protection of network neighborhoods ($\varepsilon = 1$) come at a noticeable cost to accuracy. Privacy protection for network neighborhoods in the case of German households is further complicated by the existence of almost zero signals with locally unbounded sensitivity and no meaningful protections is accomplished ($\varepsilon = 10$). Privacy and accuracy, in this case, become conflicting criteria that cannot be reconciled.

distribution, $d\xi(s)/ds$ grows unbounded as $s \to 0$.

We extend our algorithms to address additional forms of heterogeneity. Specifically, in Appendix C.3, we show how our algorithms can provably converge under minimal assumptions when the network topology is changing dynamically (Appendix C.3.1) and when the corresponding topology is directed (Appendix C.3.2). These scenarios are pertinent to real-world sensor networks since sensors and communications can fail, corresponding to dynam-

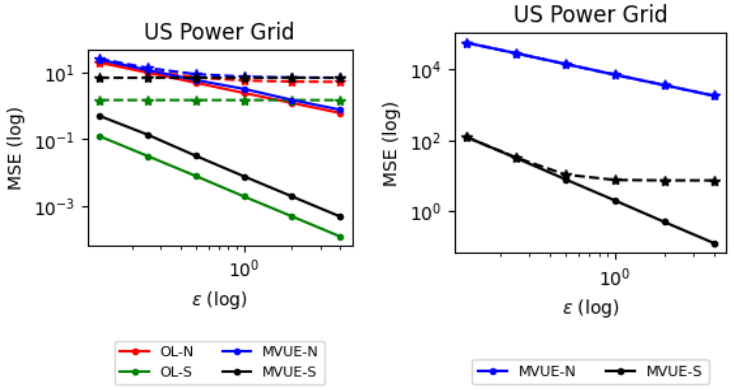
ically changing networks with asymmetries (cf. [391]). Moreover, to balance the trade-offs between accuracy and privacy, the agents can resort to heterogeneous privacy budgets $\{\varepsilon_i\}_{i\in[n]}$ and improve their collective estimation performance while maintaining minimum privacy protection (capping the individual privacy budgets at $\varepsilon_{i,\max}$). The possibility to accommodate heterogeneous budgets in the local DP setting leads to interesting design choices for improving the collective learning performance, e.g., using personalized DP methods [9, 223]. In Appendix C.3.3, we provide both centralized and decentralized schemes to allocate privacy budgets to optimize their collective accuracy subject to individual privacy budget caps and test their performance on the German Households dataset (cf. Supplementary Figure C.3).

This Section focuses on distributed estimation and learning in a networked environment subject to privacy constraints. The aim is to estimate the statistical properties of unknown random variables based on observed data. Our aggregation methods aim to combine the observed data efficiently without requiring explicit coordination beyond the local neighborhood of each agent. This allows for estimating a complete sufficient statistic using either offline or online signals provided to the agents. To preserve privacy, agents add noise to their estimates, adhering to a differential privacy budget (ε-DP) to safeguard the privacy of either their signals (signal DP) or their signals and network neighborhoods (Network DP). Our algorithms employ linear aggregation schemes that combine the observations of all agents while incorporating the added noise, either online or offline. We prove that the estimation error bounds depend on two terms: the first term corresponds to the error incurred due to the aggregation scheme (which we call Cost of Decentralization) and can be controlled by the mixing rate of the doubly-stochastic adjacency weights, and the second term



(a) Ours

(b) [354]



(c) Ours

(d) [354]

Figure 4.7: MSE plots vs. varying privacy budget ε for the German Households dataset and the US Power Grid Dataset. We compare with the first-order method of [354] with a learning rate of $\eta = 0.001$ (see Appendix C.2). The solid lines represent the CoP, and the dashed lines represent the Total Error.

corresponds to the error due to the DP noising (which we call Cost of Privacy). We prove that under all cases (see also Section 4.1.1), the noise distributions that minimize the convergence rate correspond to the Laplace distributions with parameters that depend on the (local or global) signal sensitivities, the network structure, and the differential privacy budget ε. Finally, we test our algorithms and validate our theory in numerical experiments.

When sensitivities are locally bounded, signal DP can be achieved efficiently with a graceful accuracy loss over a decreasing privacy budget. This is facil-

itated by the post-processing immunity of DP [135, Proposition 2.1] that no future leaks are possible after adequate noising of the private signals and indicates the resilience of linear aggregation schemes to DP noising. However, achieving network DP with noising of estimates is significantly more challenging, and while individual noisy estimates are protected against a one-time attack, network information can still leak over time across multiple estimates. The composition property [135, Chapter 3] implies that we can protect the network neighborhoods at ε-DP level against an adversary who eavesdrops k times by protecting individual estimates at ε/k-DP level. Such protection can be challenging if an adversary can eavesdrop on the estimates for a long time or has simultaneous access to estimates of multiple agents. In such cases, a fast convergence rate (using the fastest mixing weights) can limit communications and help agents maintain privacy without completely sacrificing the accuracy of their estimates.

4.2 Privacy-Preserving Estimation and Learning in Discrete Hypothesis Spaces

In many information environments, participating agents have privacy and security needs that prevent them from engaging in information exchange at their socially optimal levels (for optimum collective decision-making and social learning), e.g., when bound by client confidentiality, obligated by user privacy laws, or needing to safeguard their information sources. In other social and business settings, participants may be reluctant to express unpopular opinions or openly deliberate on controversial or contentious issues. Even in the absence of such privacy, legal, security, or safety concerns, strategic and competitive considerations can lead to suboptimal information sharing at equilibrium. Differential privacy (DP) is a versatile framework for the design of privacy-preserving algorithms and statistical disclosure control. DP has been applied in large-scale and high-profile cases such as the 2020 US decennial census [169] and the tech industry [146, 21]. Earlier work also points to the potential of DP in alleviating misaligned incentives and reducing competitive inefficiencies in game-theoretic equilibria [234, 61]. Our statistical disclosure control guarantees are based on DP and allow agents to communicate belief statistics to collectively infer a common known state without compromising their private information.

For example, sharing protected health information (PHI) in multicenter clinical trials requires complex data use agreements (DUAs) to protect confidentiality and manage patient authorizations between centers. Clinical trials are the gold standard for establishing medical evidence; however, when testing treatments for emerging diseases, recruiting patients for clinical trials is challenging,

especially if the disease is rare and/or severe and there are not many available treatments [359, 163]. One solution is to establish a centralized network of clinical trials that collectively recruit patients into a study. For example, in the case of AIDS, this was achieved through the AIDS Clinical Trials Group (ACTG) network, which required substantial prior investment and central coordination [195, 84]. Generally, multicenter clinical trials require the execution of extensive DUAs that slow (or sometimes prevent) collaborations. The sharing of clinical trial data remains a significant challenge due to institutional and regulatory barriers, such as the Federal Policy for the Protection of Human Subjects of 1981 (Common Rule), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Genetic Information Nondiscrimination Act of 2008 (GINA) in the United States, and the General Data Protection Regulation (GDPR) in the European Union that restrict the sharing of data in healthcare settings and beyond. The privacy-preserving distributed inference framework in this Section can alleviate the need for complex DUAs and allow centers to communicate privacy-preserving statistics while complying with patient confidentiality and privacy regulations. In 2024, the US Department of Health & Human Services launched the Advancing Clinical Trial Readiness (ACTR) initiative through the ARPA-H Resilient Systems Office [23]. ACTR emphasizes the development of a decentralized and on-demand clinical trial infrastructure, aiming to make clinical trials accessible to 90% of eligible participants within 30 minutes of their home. A critical aspect of this transformation is automating data extraction and synchronization between electronic health records (EHRs) and case report forms (CRFs), as well as standardizing data collection across diverse centers. Using data from real-world clinical trials, we demonstrate the utility of our privacy-preserving distributed inference framework for multicen-

ter studies.

This paper provides new methodologies for distributed privacy-preserving inference to improve the quality of information aggregation for collective decision-making in environments where entities harbor privacy concerns that may otherwise deter their efficient participation. These privacy concerns can arise from community retaliation for leaking individual data or the need to comply with regulations that protect the privacy of individual and patient/client data. Similarly to the healthcare sector, in finance, education, and development, organizations, while legally obligated to protect client data, can improve service quality and operational efficiency through responsible information sharing (e.g., to improve loan and financial aid screening systems or college admission outcomes). Our proposed framework can facilitate these goals by allowing multiple entities, such as healthcare care providers, banks, or universities, to perform distributed inference on their private data collectively, without centralizing access to sensitive information, to achieve greater inclusivity, representativeness, and cost efficiency.

In this Section, we propose a differentially private distributed inference model for information aggregation among a group of agents endowed with private signals and exchanging beliefs to agree on a set of best alternatives, test a hypothesis, or learn a true state of the world. Our agents are wary of revealing their private signals to each other. The private signals are generated according to the true state of the world, which is unknown but common to all agents. We propose non-Bayesian belief exchange models that protect private signals while achieving collective inference and asymptotic learning.

We characterize the quality of learning subject to DP budget constraints and

quantify the trade-off between learning rate and privacy: learning in privacy-critical environments can be sustained at a reasonable cost to communication complexity and accuracy. We show that log-linear belief updates, while common as a means of iterative opinion pooling to reach consensus [177, 358, 1, 340], can be modified to accommodate strict privacy protections for the participating agents at a reasonable cost to social learners and their quality of group decision making.

DP constraints in our algorithms are satisfied by adding noise to belief updates at an appropriate level that protects individual signals according to a privacy budget: the less the privacy budget, the more noise is needed to satisfy the DP requirement. In the online learning setting, where agents have access to an infinite, intermittent stream of signals, the effect of noise vanishes asymptotically. Still, DP noising slows down the belief dynamics, requiring more communication rounds than the non-private baseline to achieve the same accuracy level. Our nonasymptotic (finite-time) analysis allows us to delineate the trade-offs between privacy budget, communication complexity, and error probability in the online setting. When agents have access to only finitely many private signals, they aim to agree on a set of alternatives that best explains their collective observations using a distributed, maximum-likelihood estimation (distributed MLE). In this case, the crux of our analysis is that DP noising makes our distributed MLE algorithm non-deterministic. Hence, we need to repeat the distributed MLE algorithm in K rounds to achieve the desired accuracy level. Our approach for DP-distributed MLE opens up a new design dimension to decide how best to aggregate the outcome of different rounds for a reliable MLE output. We propose two methods for aggregating distributed MLE rounds, each of which offers distinct advantages in terms of communication complexity and

flexibility to control error probabilities. Our MLE methods have a natural application in binary hypothesis testing, which we formalize as a differentially private, distributed hypothesis test at a given significance level.

Belief aggregation to detect the best alternatives or test a hypothesis. Our first method is based on *arithmetic* and *geometric* averaging of beliefs across rounds. Specifically, it uses arithmetic averaging as a way to ensure that all good alternatives make their way to the identified set (no Type II errors) and with a control on the false positive rate (Type I errors). Geometric averaging offers a way to control missed detection rate (Type II errors) while ensuring that no bad alternatives are admitted in the output (no Type I errors).

For example, consider evaluating different alternatives to determine the best course of treatment for a critically ill patient. When different alternatives come with severe side effects, it is important to avoid Type I errors (false positives) because a Type I error would admit a less effective treatment while subjecting the patient to unnecessary risks. Geometric averaging is the suitable choice in this case. Similarly, when conducting a clinical trial to test the efficacy of a new drug, controlling the Type I error rate (false positives) is critical because a Type I error would mean approving ineffective drugs that incur unnecessary costs and harmful side effects. We will show that geometric averaging has a natural extension for distributed hypothesis testing and can be applied in clinical trials to test the efficacy of new drugs. However, when screening patients for early detection of cancer, minimizing the Type II error rate (false negatives) is more important because Type II errors, in this case, reduce the chance of early detection, which delays treatment and leads to worse outcomes for patients. In cases such as cancer screening, we prefer to identify as many true cases as possible, even if it

means admitting some false positives (Type I errors), which are resolved at the cost of additional diagnostic tests; therefore, arithmetic aggregation of beliefs is preferred because it precludes Type II errors and allows us to control the Type I error rate.

Our second aggregation method is based on a *thresholding* technique that tracks the frequencies with which beliefs on different states across rounds exceed two thresholds and uses them in two stages to select MLE states. This algorithm works analogously to the averaging algorithms and relies on the concentration of frequencies to control Type I and Type II errors simultaneously using the two thresholds. The advantage of the thresholding method over the geometric and arithmetic averaging algorithms is that it offers more flexibility to control Type I and Type II error rates individually (rather than precluding one and controlling the other); however, this comes at a cost to runtime and communication complexity (an increased number of exchanges of beliefs between the agents) that we characterize in our theoretical performance bounds.

We test our algorithms on two data sets from clinical trials. Our first experiment considers distributed hypothesis testing for clinical trial data from an AIDS Clinical Trial Group (ACTG) study [84] to determine the effect of different treatments on the survival of AIDS patients using the proportional hazards model [115]. In a second experiment, we work with clinical trial data from advanced cancer patients [359] and study the effect of a cancer index – called the Tumor Mutational Burden – on patient survival. Both of our experiments show that our method can efficiently balance distributed learning and privacy while also being easy to implement with significantly faster runtime than existing encryption-based privacy-enhancing technologies (PETs) and federated

analytics for multicenter studies [163].

4.2.1 The Dilemma of Privacy-Preserving Data Sharing

We begin with a toy example that helps flesh out a problem at the heart of privacy-preserving data sharing for collective inference: whether to delegate decisions to a central authority with access to shared privatized/noisy data of all agents or to act alone based on clean, individual data? We consider a collection of n agents who want to perform a hypothesis test of a simple null ($\theta = 0$) against a simple alternative ($\theta = 1$) at the significance level α; for example, $\alpha = 0.05$. Agents receive binary signals $s_i \in \{0, 1\}$ such that $\mathbb{P}[s_i = 1|\theta = 1] = \mathbb{P}[s_i = 0|\theta = 0] = p$ for some $1/2 < p < 1$; i.e., $\mathbb{P}[s_i = 0|\theta = 1] = \mathbb{P}[s_i = 1|\theta = 0] = 1 - p$. The most powerful individual test at the significance level α varies with p as follows:

1. If $1 - p < \alpha$, then the most powerful test at the significance level α will always reject $\theta = 0$ if $s_i = 1$; and if $s_i = 0$, then it will reject $\theta = 0$ with probability $(\alpha - 1 + p)/p$, giving a total statistical power of $\beta_{\text{IND}} = p + (1 - p)(\alpha - 1 + p)/p$.
2. If $1 - p = \alpha$, then the most powerful test at the significance level α would be to reject $\theta = 0$ if $s_i = 1$ and accept otherwise. The statistical power in this case is given by $\beta_{\text{IND}} = \mathbb{P}[s_i = 1|\theta = 1] = p = 1 - \alpha$.
3. If $1 - p > \alpha$, then the most powerful test at the significance level α will reject $\theta = 0$ with probability $\alpha/(1 - p)$ when $s_i = 1$ and never when $s_i = 0$, giving a statistical power of $\beta_{\text{IND}} = p\alpha/(1 - p)$.

Alternatively, agents can choose to send their private signals to a central au-

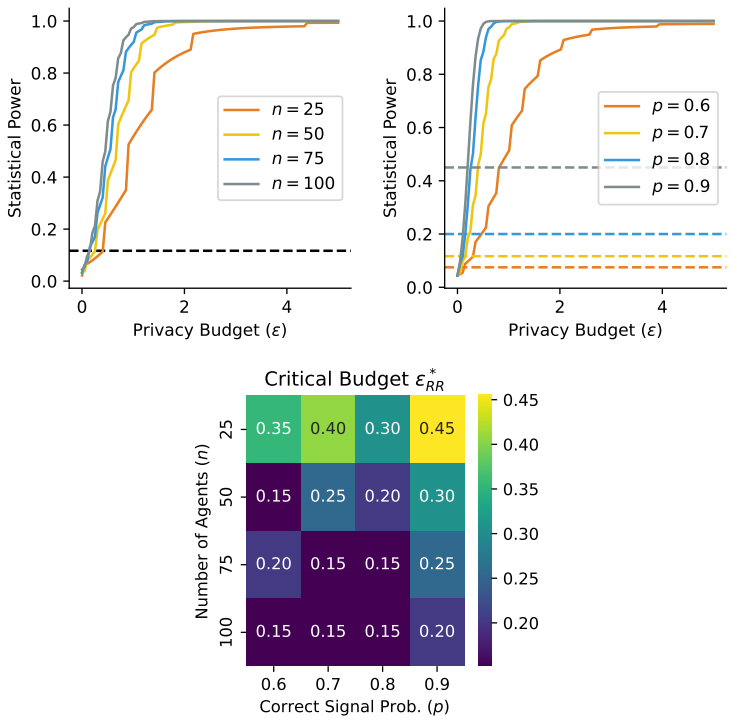


Figure 4.8: *When inferring a binary state from a binary signal that agrees with the state with probability p, there is a critical privacy budget, $\varepsilon^*_{\text{RR}}$, above which sharing noisy (DP-protected) data becomes beneficial.* **Top Left:** Statistical power (β_{RR}) as a function of privacy budget ε for different number of agents (n) with $p = 0.7$. The critical budget $\varepsilon^*_{\text{RR}}$ corresponds to the intersection of each curve with the dotted line (β_{IND}) showing the statical power for a single agent. The intersection points show $\varepsilon^*_{\text{RR}}$ decreases with increasing number of agents. **Top Right:** Statistical power (β_{RR}) as a function of privacy budget ε for different values of p with $n = 100$ agents. The critical budget ($\varepsilon^*_{\text{RR}}$) corresponds to the intersection points of the power curve for collective hypothesis testing (β_{RR}) with the dotted lines showing statistical power without data sharing for single agents (β_{IND}). Increasing p increases the statical power for both individual agents and collectively when agents share their data; therefore, variation of $\varepsilon^*_{\text{RR}}$ may not be much or monotone. However for very high values pf p where individuals can perform highly accurate tests on their own, the value of $\varepsilon^*_{\text{RR}}$ increases. **Bottom:** The critical budget ($\varepsilon^*_{\text{RR}}$) values for varying n and p. We use $\alpha = 0.05$ for all tests.

thority, who performs the hypothesis test on the collective data on their behalf, in which case they need protection against the privacy ramifications of sharing their signals. Differential privacy with a privacy budget ε limits what can be inferred about private signals from the output of an algorithm $\mathcal{A}$ that is ε-

DP because any subset R in the range space of $\mathcal{A}$ must satisfy $\mathbb{P}[\mathcal{A}(s_i = 1) \in R]/\mathbb{P}[\mathcal{A}(s_i = 0) \in R] \leq e^{\varepsilon}$. The randomized response (RR) is a simple mechanism that achieves DP with a privacy budget ε to release private binary signals [416]. According to the randomized response, each agent transmits a signal y_i, which is equal to $1 - s_i$ with probability $p_\varepsilon = 1/(1 + e^{\varepsilon})$ where $\varepsilon > 0$ is the privacy budget. By applying the randomized response mechanism before sharing their private signals, agents will have plausible deniability as to what their true private signals were. As $\varepsilon \to 0$, agents randomize their signals with probability $1/2$, providing no information to the receiver; on the other hand, as $\varepsilon \to \infty$, agents tend to share their true private signals without randomization noise ($p_\varepsilon \to 0$). To construct the most powerful α level test, agents construct the sum statistic $\sum_{i=1}^{n} y_i$ and choose a threshold τ_{RR} to reject $\theta = 0$ whenever $\sum_{i=1}^{n} y_i \geq \tau_{\text{RR}}$. Under the null ($\theta = 0$), the sum statistic is distributed as a binomial random variable with size n and success probability p' where $p' = pp_\varepsilon + (1 - p)(1 - p_\varepsilon)$. Therefore, agents choose the threshold τ_{RR} to be $\tau_{\text{RR}} = Q_{\text{Bin}(n,p')}(1-\alpha)$, where $Q_{\text{Bin}(n,p')}(1-\alpha)$ is the $(1-\alpha)$-quantile of the $\text{Bin}(n, p')$ distribution. The statistical power of the test, denoted as β_{RR}, is given by (Here we ignore the possibility of randomizing the test outcome if $\mathbb{P}\left[\sum_{i=1}^{n} y_i \geq \tau_{\text{RR}} + 1 \middle| \theta = 0\right] < \alpha$ and $\mathbb{P}\left[\sum_{i=1}^{n} y_i \geq \tau_{\text{RR}} \middle| \theta = 0\right] > \alpha$, for some positive integer $\tau_{\text{RR}} \leq n$. This case does not arise for the values of $n \geq 25$, p, and $\alpha = 0.05$ that we consider. In general, for $n \geq 25$ the binomial distribution is well approximated by a Gaussian, and such cases, even if they arise, will have minimal effect on the power):

$$\beta_{\text{RR}} = \mathbb{P}\left[\sum_{i=1}^{n} y_i \geq \tau_{\text{RR}} \middle| \theta = 1\right] = 1 - F_{\text{Bin}(n,1-p')}(\tau_{\text{RR}}) = 1 - F_{\text{Bin}(n,1-p')}\left(Q_{\text{Bin}(n,p')}(1-\alpha)\right). \tag{4.12}$$

Thus, agents are motivated to share information whenever $\beta_{\text{RR}} \geq \beta_{\text{IND}}$. The *critical privacy budget*, $\varepsilon^*_{\text{RR}}$, above which agents prefer collective hypothesis test-

ing using shared noisy data to individual decision making using their private signals, is given by:

$$\varepsilon^*_{\mathrm{RR}} = \inf_{\varepsilon>0} \left\{ Q_{\mathrm{Bin}(n,p')}(1-\alpha) \leq Q_{\mathrm{Bin}(n,1-p')}(1-\beta_{\mathrm{IND}}),\ \text{where } p' = pp_\varepsilon + (1-p)(1-p_\varepsilon) \right\}. \tag{4.13}$$

Figure 4.8 shows the critical budgets $\varepsilon^*_{\mathrm{RR}}$ as a function of n and p: $\varepsilon^*_{\mathrm{RR}}$ decreases with increasing n because the benefit of collective hypothesis testing is greater in larger groups. Our simulations further suggest that $\varepsilon^*_{\mathrm{RR}}$ increases as private signals become more informative with increasing p; with such highly informative private signals, individuals can make accurate inferences without data sharing. Note that in most cases, $\varepsilon^*_{\mathrm{RR}}$ is relatively small ($\varepsilon^*_{\mathrm{RR}} < 1$ in all the cases we have tested), and information sharing is beneficial even for moderate values of n.

Our exploration of the statistical power of the randomized response mechanism gives rise to the following question: Does the randomized response mechanism give a sufficiently powerful statistical test among the class of all DP mechanisms for random binary signals? [30] give a negative answer and provide the mechanism with the maximum statistical power for binary signals. The mechanism of [30] works only in the case of binary signals and cannot be applied to general signal distributions. To address this, [233] extend the construction of differentially private hypothesis tests for general distributions by splitting the data sets and applying the mechanism of [30] on the random variable that counts the rejection of the null hypothesis in subsets of the data. In general, agents may have different sample sizes, denoted by n_i for each agent i, and can have general distributions. One possibility is for each agent to run the algorithm of [233] and share the outcome of their privatized hypothesis tests. The results of the pri-

vatized hypothesis tests, weighted as a function of the individual sample sizes and signal likelihoods, can then be combined into an aggregate that is protected by post-processing immunity of DP. However, this prevents consensus on the results of the hypothesis test. In applications such as multicenter clinical trials discussed in Section 4.2.2, agents need to merge their statistics to test a hypothesis collectively. Our methods allow agents to exchange their statistics and learn from each other towards a consensus on the best alternative, not only for binary hypothesis tests but generally in finite, discrete spaces with more than two alternatives.

In this Section, we devise decentralized algorithms for agents to exchange their log-likelihood ratio statistics and use the Laplace mechanism to privatize the signal log-likelihoods. The Laplace mechanism has several advantages, such as being simple to calculate and implement; it can accommodate DP constraints for general signal distributions and is the mechanism that minimizes the mean squared error bound and convergence time for distributed estimation [325, 247], and has similar optimality properties for convergence time in our case as well (Theorems 4.2.2 and 4.2.8 in Section 4.2.7). It is also the noise distribution that minimizes the sample complexity of differentially private simple hypothesis tests using noisy clamped log-likelihood ratios [85].

For example, in the case of binary signals, when the agents decide to share data with each other, they calculate their private statistics that correspond to the likelihood ratios and add appropriately chosen Laplace noise, i.e. $\log\left(\frac{\ell(s_i|\theta=1)}{\ell(s_i|\theta=0)}\right) + d_i$, where $d_i \sim \text{Lap}(\Delta/\varepsilon)$ with $\Delta = 2|\log(p) - \log(1-p)|$ being the sensitivity of the log-likelihood ratios to the binary private signals. Then, each agent forms $\sum_{i=1}^{n}\left(\log\left(\frac{\ell(s_i|\theta=1)}{\ell(s_i|\theta=0)}\right) + d_i\right)$ and determines a threshold to reject the null hypothesis at

the significance level α. The rejection criteria and the corresponding statistical power β_{Laplace} can be found numerically by simulating the distribution of the test statistics under the null and alternative. Figure 4.9 shows the statistical power of the test as a function of n and p as well as the critical budgets $\varepsilon^*_{\text{Laplace}}$ above which a collective test based on noisy shared data is more powerful than individual tests based on clean private data. Here we also find $\varepsilon^*_{\text{Laplace}} < 1$ in all our simulations.

4.2.2 Survival Analysis for Multicenter Clinical Trials

Survival analysis is widely used to examine how patients' survival outcomes (i.e., timing of events such as death, relapse, remission, recovery, etc.) vary in response to specific treatments or other health factors. Importantly, survival analysis accounts for censoring, which refers to the existence of data points where events of interest, such as death, have not occurred by the end of the study period, and yet these data points are informative about the effect of treatments. Survival models account for censoring to give more accurate and unbiased estimates. This approach typically involves key metrics such as survival functions, hazard rates, and median survival times, allowing researchers to compare the effectiveness of different treatments or identify prognostic factors. Standard nonparametric and semiparametric models, such as the Kaplan-Meier curve [228] and the Cox proportional hazards model [115], allow us to analyze patient survival data with great flexibility in various clinical and experimental settings. By modeling time-to-event data, survival analysis plays a crucial role in clinical trials, epidemiological studies, and personalized medicine, helping clinicians and researchers make informed decisions about treatment strategies and

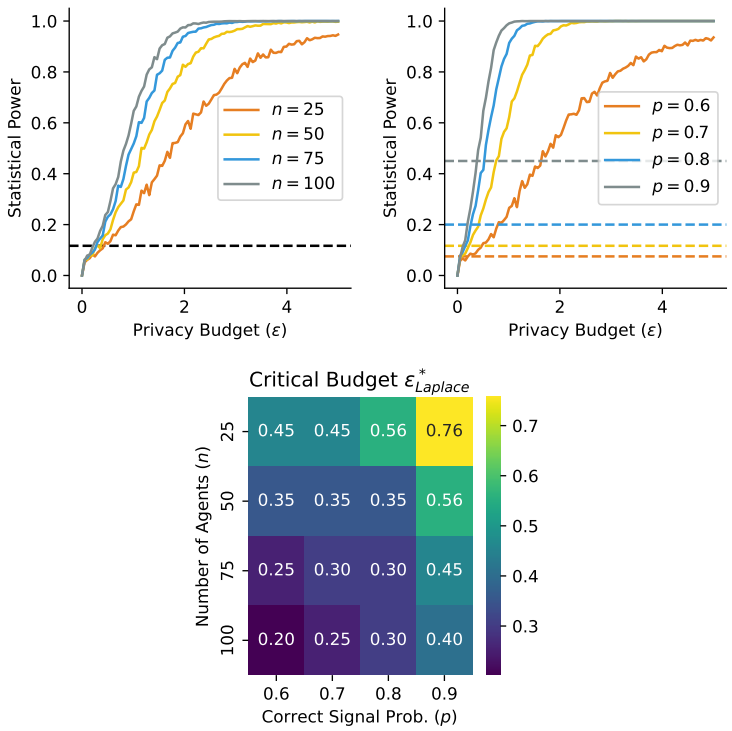


Figure 4.9: Statistical power versus privacy budget for testing the probability of private Bernoulli random variables. The intersections of the dotted lines (β_{IND}) and the curves (β_{Laplace}) give the critical privacy budget, $\varepsilon^*_{\text{Laplace}}$, above which collective testing using noisy shared data is more powerful than individual tests using private signals. All tests are performed at significance level $\alpha = 0.05$. **Top Left:** Statistical power with different number of agents (n) and $p = 0.7$. The critical privacy budget $\varepsilon^*_{\text{Laplace}}$ decreases with the increasing number of agents n. **Top Right:** Statistical power with different values of p and $n = 100$ agents. $\varepsilon^*_{\text{Laplace}}$ as a function of p. The statistical power for both individual and collective tests increase with p, and therefore the intersection points does not vary monotonically with increasing p; however, $\varepsilon^*_{\text{Laplace}}$ is highest at high values of p where individuals alone can perform highly accurate tests. **Bottom:** The critical privacy budget $\varepsilon^*_{\text{Laplace}}$ for different values of n and p. The rejection criteria and statistical power are numerically determined by drawing 10,000 samples under the null and alternative ($\theta = 0, 1$).

patient care. Our simulation study in Section 4.2.11 consists of survival analysis on a data set from the AIDS Clinical Trials Group (ACTG) network [298], which has conducted several studies of HIV-infected and AIDS patients since the late 1980s [195, 84].

Healthcare centers vary in the demographics of the patients that they serve, and they may even have different target groups (e.g., children's or women's hospitals). Although different centers can conduct clinical trials and hypothesis tests on their own, potential data limitations can yield false conclusions, for example, due to small sample sizes or higher prevalence of specific health conditions among some demographics that are under- or overrepresented in their patient population. For this reason, multiple healthcare centers can join multicenter trials to perform hypothesis tests with more accuracy, using larger and more diverse patient samples. To model multicenter trials, we divide patient data from the ACTG study 175 [298] equally at random between five centers and use the proportional hazards model [115] for survival analysis. For ease of exposition, we consider a simple hypothesis testing scenario to determine the efficacy and safety of a new treatment (ddI) against standard care (ZDV), which are antiretroviral HIV / AIDS medications in the ACTG study 175. For each center $i \in [n]$, we denote their data set of patients by $cref S_i$ with cardinality n_i. The patient j in the center i has the treatment variable $x_{ij} \in \{0, 1\}$ which indicates if they have received the new treatment (ddI), $x_{ij} = 1$, or standard care (ZDV), $x_{ij} = 0$. The effect of the treatment is parametrized by θ. The survival event for each patient is denoted by $\delta_{ij} \in \{0, 1\}$ with $\delta_{ij} = 1$ corresponding to death (survival time is observed) and $\delta_{ij} = 0$ corresponding to survival (survival time is censored). The survival or censoring time is measured in days and is indicated by $t_{ij} \in \mathbb{N}$. Following the Cox proportional hazards model, the partial log-likelihood of the patient survival data for center i is given by:

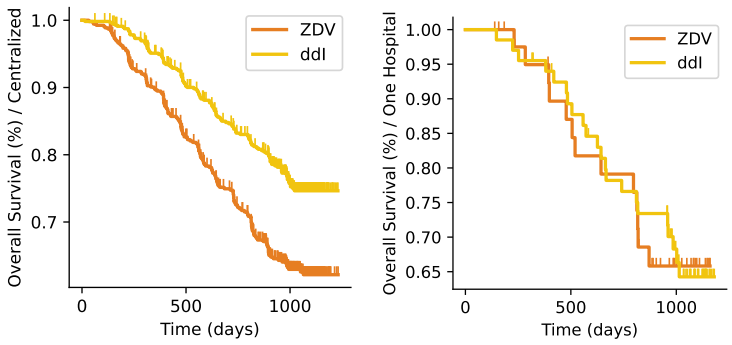
$$\log \ell_i(S_i|\theta) = \sum_{j:\delta_{ij}=1} \left(x_{ij}\theta - \log \sum_{j':t_{ij'} \geq t_{ij}} e^{x_{ij'}\theta} \right). \tag{4.14}$$

Note that using ℓ_i in (4.14) is with some abuse of notation because it does not represent the full likelihood of the observed data; however, under Cox's propor-

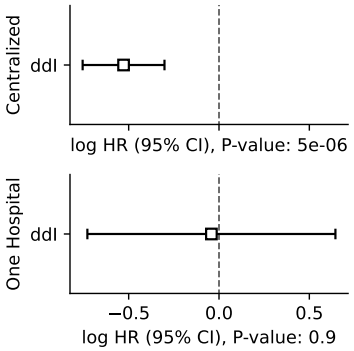
tional hazards model we can reliably infer the effect of the new treatment and other risk factors that can be included as covariates along with the treatment variable in Equation (4.14), from the partial likelihoods without specifying the full likelihoods or the functional form of the baseline hazard rate corresponding to $x_{ij} = 0$. We are interested in rejecting the simple null hypothesis that $\theta = 0$, i.e., that the two survival curves are the same, which in the absence of other covariates is equivalent to a nonparametric log-rank test of survival times between the treatment and control groups. For concreteness, we use $\theta_1 = -\log(2)$ as the simple alternative, which corresponds to patients being twice as likely to survive under the new treatment than in standard care (e^θ is the relative risk for the new treatment under the proportional hazards model).

Figure 4.10(b) shows that the sample size of Kaplan-Meier survival curves calculated by one of the hospitals is not large enough to detect a difference between the two treatments, and, in fact, fitting the proportional hazards model using data from one hospital yields a p-value of 0.9 in Figure 4.10(c). However, if centers were to pool their data (ignoring privacy concerns) through a centralized authority, then the centralized authority could perform the test at a larger sample size. Figure 4.10(a) shows the Kaplan-Meier survival curves are easily distinguishable in the centralized case. In Figure 4.11(c), when all data are pooled together, the difference between log-hazard ratios (log HR) from fitting proportional hazards models for the two treatments is statistically significant at $p < 0.001$.

In a distributed setting where privacy concerns limit data sharing and preclude data pooling for centralized access, centers can exchange noisy information locally to achieve distributed hypothesis testing with privacy guarantees.



(a) Centralized curves (b) Curves for one hospital



(c) Log hazard ratios

Figure 4.10: **Top Left:** Kaplan-Meier survival curves for ACTG study 175 [298] for the ZDV and ddI treatments. ZDV stands for Zidovudine, and ddI stands for Didanosine. **Top Right:** Survival curves for one hospital (the data is split equally among five hospitals) for the same study. **Bottom:** Log hazard ratios with 95% confidence intervals from the fitted proportional hazards model using all the data (centralized) and one hospital.

In the private regime, inspired by the likelihood ratio test, we propose that each center calculate its local (partial) log-likelihood ratio statistic $\log\left(\frac{\ell_i(S_i|\theta=\theta_1)}{\ell_i(S_i|\theta=0)}\right)$, add appropriately chosen Laplace noise d_i, and then exchange the noisy statistic with its neighbors; see the simulation study in Section 4.2.11. The methods we devise in Sections 4.2.3 and 4.2.7 allow agents to form belief statistics locally, in a privacy-preserving manner, and use them for collective hypothesis testing with guarantees of false positive and false negative rates.

4.2.3 Belief Prorogation for Differentially Private Distributed Inference

More generally, each agent can have access to private observations with different likelihoods (for example, representing different populations of patients in different centers), which are parametrized by a common, finite set of alternatives. The goal of the agents is to exchange information to calculate the likelihoods of their collective observations and to choose a common set of maximum likelihood estimates (MLEs). To this end, agents exchange (non-Bayesian) belief statistics and decide on a common set of best alternatives (collective likelihood maximizers) based on their convergent beliefs. This MLE setup has natural extensions to hypothesis testing and online learning that we explore in Section 4.2.7. Before focusing on the theoretical performance and privacy guarantees of our distributed belief exchange algorithms in Section 4.2.7, we introduce our information environment and the setup of distributed inference in Section 4.2.4. Our belief exchange rules have a log-linear format, which have normative foundations in decision analysis and can also be justified on the basis of their convergence properties. We discuss these normative foundations and convergence properties in Section 4.2.5, followed by an explanation of our performance analysis framework and associated metrics in Section 4.2.6.

4.2.4 Problem Formulation: Distributed Inference & Learning in Discrete Spaces

A collection of n agents, denoted by the set $[n] = \{1, \dots, n\}$, wants to select an alternative from a finite set Θ. Each agent i has its own data, which are fixed at the beginning or arrive in an online stream over time. The data follow a parametric model given by its likelihood function $\ell_i(\cdot|\theta), \theta \in \Theta$. The goal of the agents is to exchange information to select a set of alternatives that best describes their data collectively, in a maximum likelihood sense. Information exchange between agents (e.g., collaborating hospitals) is constrained by organizational and legal barriers, as well as *privacy regulations* (e.g., HIPAA or GDPR) that limit who can exchange what information with whom. In our framework, organizational and legal barriers are captured by the structure of the communication network that limits information exchange to permissible local neighborhoods, and protection of private data (e.g., protected health information at each hospital) is achieved through differential privacy.

Agents are connected according to an undirected graph $\mathcal{G}([n], \mathcal{E})$ without self-loops. The neighborhood of agent i in $\mathcal{G}$ is denoted by $\mathcal{N}_i$ and corresponds to all agents with whom agent i can exchange information locally. The graph is associated with an irreducible doubly stochastic adjacency matrix $A = \left[a_{ij}\right]_{i,j\in[n]}$ with weights $a_{ij} = 0$ whenever $(i, j) \notin \mathcal{E}$ and weight $a_{ij} > 0$ for all $(i, j) \in \mathcal{E}$, and, moreover, $\sum_{i\in[n]} a_{ij} = \sum_{j\in[n]} a_{ij} = 1$. The n eigenvalues of the adjacency matrix A are ordered by their modulus and denoted by $0 < |\lambda_n(A)| \leq \cdots \leq b_n^\star = |\lambda_2(A)| < |\lambda_1(A)| = 1$, with their associated set of bi-orthonormal eigenvectors, $\{l_i, r_i\}_{i\in[n]}$, satisfying $\|l_i\|_2 = \|r_i\|_2 = l_i^T r_i = 1$ for all $i \in [n]$ and $l_i^T r_j = 0$ for all $i \neq j$. Differential privacy restrictions dictate the protection of individual data, that

is, ensuring that information exchange mechanisms between agents satisfy the following criteria for ε-DP.

Definition 4.2.1. A mechanism $\mathcal{M}_i : \mathcal{S} \to \mathcal{R}$, acting on private signals, is said to be ε-DP with respect to the signal $s \in \mathcal{S}$ if and only if for all $X \subseteq \mathcal{R}$ we have that

$$\mathbb{P}[\mathcal{M}_i(s) \in X] \leq e^{\varepsilon}\mathbb{P}[\mathcal{M}_i(s') \in X], \text{ for all } s, s' \in \mathcal{S}, \text{ s.t. } \|s - s'\|_1 \leq 1.$$

The ε-DP constraint on $\mathcal{M}_i$ ensures that as $\varepsilon \to 0$, no information can be inferred about whether s or any of its adjacent points (i.e., $s' \in \mathcal{S}$ such that $\|s-s'\|_1 \leq 1$) are the input that generates the observed output $\mathcal{M}_i(s)$. Our primary interest in this Section is in belief exchange mechanisms for which the range space $\mathcal{R}$ is the probability simplex of all distributions over the state space Θ, denoted by SimplexΘ. Defining the appropriate notion of adjacency allows us to control sensitive information leaks. When working with clinical trial data, we declare two observations s and s' adjacent if, and only if, they differ in the data of one patient.

We consider two distributed learning environments: In the first, we estimate the best alternative or perform hypothesis testing in a distributed manner based on a set of initial observations; in the second, we learn the true alternative online by repeatedly observing data streams over time. In the sequel, we present the two settings with the corresponding nonprivate algorithms in Appendix C.5, which serve as benchmarks for the DP regime.

Distributed MLE. In the distributed maximum likelihood estimation task (MLE), there is a set of likelihood maximizers $\Theta^\star \subset \Theta$, and agents aim to determine $\Theta^\star$ collectively by combining their private signals while communicating within their local neighborhoods. Specifically, each agent has access to a dataset

of n_i i.i.d. observations, $S_i = (s_1, \ldots, s_{n_i})$, where $s_1, \ldots, s_{n_i} \in \mathcal{S}$ obey a statistical model determined by the likelihood function $\ell_i(S_i|\widehat{\theta}) = \prod_{j=1}^{n_i} \ell_i(s_j|\widehat{\theta}), \quad \widehat{\theta} \in \Theta$. The agents' task is, given signals S_i for each agent $i \in [n]$, to find the set of likelihood maximizers, i.e.,

$$\Theta^\star = \operatorname*{argmax}_{\widehat{\theta} \in \Theta} \Lambda(\widehat{\theta}), \text{ where } \Lambda(\widehat{\theta}) = \sum_{i=1}^{n} \log\left(\ell_i(S_i|\widehat{\theta})\right). \tag{4.15}$$

We define $\bar{\Theta} = \Theta \setminus \Theta^\star$ as the set of non-optimal states. We let $f^\star$ represent the proportion of MLE states, i.e., $f^\star = |\Theta^\star|/|\Theta|$. [343] give a non-private algorithm for belief exchange, described in Appendix C.5.1, that is able to recover $\Theta^\star$ asymptotically.

In the multicenter clinical trial example of Section 4.2.2, the hypothesis space is $\Theta = \{0, \theta_1\}$ where $\theta = 0$ corresponds to the hypothesis that the two treatments are statistically indistinguishable and $\theta = \theta_1 < 0$ corresponds to the hypothesis that ddI improves patient survival compared to ZDV as is the case based on Figure 4.10; hence, $\Theta^\star = \{\theta_1\}$. The goal of the agents is to collectively infer that $\theta = \theta_1$ is the best state (MLE) given the data of the patients because $\Lambda(\theta_1) > \Lambda(0)$. In Section 4.2.9, we show how distributed MLE algorithms can be modified for distributed hypothesis testing with statistical significance guarantees.

Online Learning from Intermittent Streams. In the online setting, we consider a network of agents making streams of observations intermittently over time. At each time step t, agent i makes $n_{i,t}$ i.i.d. observations $s_{i,t}^1, \ldots, s_{i,t}^{n_{i,t}}$ that are distributed according to a parametric model $\ell_i(\cdot|\widehat{\theta}), \widehat{\theta} \in \Theta$; and the number of observations at time t for each agent $i \in [n]$ is independently and identically distributed, $\{n_{i,t}\} \overset{\text{i.i.d.}}{\sim} \mathcal{P}_i$, with mean $\mathbb{E}[n_{i,t}] = \xi_i$ and variance $\mathbb{V}[n_{i,t}] = \chi_i$. In the online setting, we assume that the data are generated according to a true parameter $\theta^\circ \in \Theta$, which is uniquely identifiable from the collective observa-

tions of the agents. The collective identifiability condition can be expressed as $\sum_{i=1}^{n} \xi_i D_{KL}\left(\ell_i(\cdot|\bar{\theta})|\ell_i(\cdot|\theta^\circ)\right) > 0, \forall \bar{\theta} \neq \theta^\circ$. Note that, unlike the MLE setting, where agents can increase the power of their inferences by exchanging belief statistics, in the online setting, each agent alone has access to an infinite signal stream. An informational advantage of collective inference in the online setting is apparent where agents individually face identification problems; for example, for an agent $i \in [n]$, a pair of states ($\widehat{\theta}_1$ and $\widehat{\theta}_2$) may induce the same distribution of observations, making them undistinguishable from the perspective of agent i. In such cases, by exchanging beliefs, agents can benefit from each other's observational abilities to collectively identify the truth even though they may face an identification problem individually. [343] give a non-private algorithm for belief exchange that is able to asymptotically recover the true state θ° from a stream of observations (cf. Appendix C.5.2).

In multicenter clinical trials, the online learning setup corresponds to centers recruiting patients over time. The centers can rely on each other's observational capabilities to recruit a diverse patient demographic, which they may otherwise lack access to and can compromise their ability to detect effects in certain populations.

4.2.5 Log-Linear Belief Updates and Opinion Pools

The fastest way to (asymptotically) compute the joint log-likelihood would be for the agents to run a linear consensus algorithm [121, 313] in the (privatized) log-likelihood space for each $\theta \in \Theta$. This rule is equivalent to performing log-linear updates (i.e., geometric means) in a (non-Bayesian) belief space [343]. On

the other hand, simple DeGroot (linear) averaging of beliefs converges to the average of initial likelihoods (rather than log-likelihoods) and can give biased estimates if used for maximum likelihood estimation. [232] and [255, Corollary 2] point out that log-linear learning converges faster than linear learning in the belief space. [278] provide guarantees on the percentage of time that the action profile will be a potential maximizer in potential games using log-linear best-response dynamics.

The log-linear updates that we use to exchange belief statistics among neighboring agents also have parallels as opinion pools to combine probability distributions from multiple experts in the decision and risk analysis literature [110]. [1], in particular, proposes scoring rules based on the KL divergence between the expert distributions and aggregate beliefs that yield linear and log-linear aggregates as the solution to the expert aggregation problem: If KL divergence is computed from the aggregate belief to the expert beliefs then we obtain log-linear updates, otherwise (i.e., if the KL divergence is computed from the expert beliefs to the aggregate belief) we obtain linear updates. Denoting expert beliefs by ν_j with weights $a_{ij}, j \neq i$, the log-linear belief aggregate $\nu^\star$ sets the belief in every state $\nu(\theta)$ proportionally to $\prod_{j\in[n]} \nu_j^{a_{ij}}(\theta)$ and is the solution to $\arg\min \sum_{j\neq i} a_{ij} D_{KL}\left(\nu_i|\nu_j\right)$. Such rules are especially sensitive to experts who put zero or small beliefs on some states and can be useful for rejecting non-MLE states or null hypotheses. In this section, we use the framework of [1] with explicitly modeled privacy costs to justify our update rules beyond the algorithmic performance framework of Section 4.2.6 and our theoretical guarantees in Section 4.2.7.

Following [1], consider a decision maker (i) who is interested in choosing

the best option among a set of alternatives (Θ), given access to their own private information (S_i) and other opinions from n experts. The decision maker forms a time-varying public belief $\nu_{i,t} \in \text{Simplex}(\Theta)$ over Θ for treatments that capture all expert distributions and its own data. Initially (at $t = 0$), the agent forms an intrinsic belief $\gamma_i \in \text{Simplex}(\Theta)$ based on its own data, i.e., $\gamma_i(\widehat{\theta}) = \frac{\ell_i(S_i|\widehat{\theta})}{\sum_{\tilde{\theta}\in\Theta} \ell_i(S_i|\tilde{\theta})}$ for all $\widehat{\theta} \in \Theta$. In subsequent steps ($t \geq 1$), the decision maker chooses an expert at random with probability a_{ij} corresponding to the strength of the connection in the communication matrix A and pays C_i to consult with them and C_i to consult its own data and incurs a revenue R_i regardless of its decision. Since the decision maker consults its own data and communicates its beliefs with others, it must protect its own signals due to privacy risks.

The ε-DP mechanism $\mathcal{M}_i$, satisfying Definition 4.2.1, applied to γ_i produces $\mathcal{M}_i(\gamma_i)$ which is privatized belief over the hypothesis space $|\Theta|$. Putting everything together, the expected payoff of agent i at time t is given as (see Eq. (9) in [1]):

$$U_{i,t}(\nu_{i,t}, \nu_{t-1}) = \begin{cases} R_i - C_i \sum_{j=1}^{n} a_{ij} D_{KL}\left(\nu_{i,t}|\nu_{j,t-1}\right) - C_i D_{KL}\left(\nu_{i,t}|\nu_{i,t-1}\right), & t \geq 1 \\ R_i - C_i D_{KL}\left(\nu_{i,0}|\mathcal{M}_i(\gamma_i)\right), & t = 0. \end{cases} \tag{4.16}$$

To implement the mechanism $\mathcal{M}_i$, the decision maker draws appropriately chosen zero-mean (w.l.o.g.) noise variables $d_i(\widehat{\theta})$ for each state $\widehat{\theta} \in \Theta$ and adds them to the corresponding log-likelihoods $\log \gamma_i(\widehat{\theta})$. Thus, $\mathcal{M}_i(\gamma_i)$ can be written as the product of the two distributions γ_i and $\mathfrak{D}_i$, where $\mathfrak{D}_i(\widehat{\theta}) = \frac{e^{d_i(\widehat{\theta})}}{\sum_{\tilde{\theta}\in\Theta} e^{d_i(\tilde{\theta})}}$. If we write $\nu_{i,0}$ as the product of $\nu_{i,0}$ together with the uniform measure $\mathcal{U}_\Theta$ on Θ and using the properties of the KL-divergence, we get $D_{KL}\left(\nu_{i,0}|\mathcal{M}_i(\gamma_i)\right) = D_{KL}\left(\nu_{i,0}|\gamma_i\right) + D_{KL}\left(\mathcal{U}_\Theta|\mathfrak{D}_i\right)$. The term $D_{KL}\left(\mathcal{U}_\Theta|\mathfrak{D}_i\right)$ corresponds to the privacy loss and equals

$$D_{KL}\left(\mathcal{U}_\Theta|\mathfrak{D}_i\right) = \sum_{\widehat{\theta}\in\Theta} \frac{1}{|\Theta|} \log\left(\frac{\sum_{\bar{\theta}\in\Theta} e^{d_i(\bar{\theta})}}{|\Theta| e^{d_i(\widehat{\theta})}}\right) = \log\left(\sum_{\bar{\theta}\in\Theta} e^{d_i(\bar{\theta})}\right) - \log|\Theta| - \sum_{\widehat{\theta}\in\Theta} d_i(\widehat{\theta}).$$

Taking the expectation over $\mathcal{M}_i$ we get $\mathbb{E}_{\mathcal{M}_i}\left[D_{KL}\left(\mathcal{U}_\Theta|\mathfrak{D}_i\right)\right] = \mathbb{E}_{\mathcal{M}_i}\left[\log\left(\sum_{\bar{\theta}\in\Theta} e^{d_i(\bar{\theta})}\right)\right] - \log|\Theta|$. Since the KL divergence is nonnegative, the expected privacy loss with respect to $\mathcal{M}_i$ is minimized whenever the noise variables $d_i(\widehat{\theta})$ are independent of each other, and their distribution does not depend on $\widehat{\theta}$.

To achieve the aforementioned property, $d_i(\widehat{\theta})$ can be distributed according to the Laplace noise mechanism, and, in addition, the distribution of the noise should be independent of the state $\widehat{\theta} \in \Theta$, i.e. $d_i(\widehat{\theta}) \sim \mathcal{D}$. The Laplace mechanism possesses further benefits since it minimizes the convergence time of the belief exchange algorithms (cf. Section 4.2.7 and prior results by [325] and [247]). The global ℓ_1-sensitivity is computed as

$$\Delta_{n,\Theta} = \max_{i\in[n],\widehat{\theta}\in\Theta} n_i g_i(\widehat{\theta}), \quad \text{where} \quad g_i(\widehat{\theta}) = \max_{s,s'\in\mathcal{S}:\|s-s'\|\leq 1} \left\| \log \ell_i(s|\widehat{\theta}) - \log \ell_i(s'|\widehat{\theta}) \right\|_1. \tag{4.17}$$

In Appendix C.9, we compute (4.17) for the proportional hazards model. More generally, the signal structure may be such that the sensitivity is unbounded when computed globally over the signal space. In such cases, an additive relaxation of the privacy constraints in Definition 4.2.1 can be used with a smoothed notion that looks at sensitivity locally at the realized signal values [310].

The best update rule that optimizes the time-varying utility of Equation (4.16) yields the log-linear update rules [1, Proposition 4]. The above can be extended to the online setting where data $S_{i,t}$ with $n_{i,t} \geq 0$ data points for each agent i are intermittently arriving at each iteration t, by introducing a time-varying utility and measuring the likelihood at each iteration t. In that regime,

first, the agents form the probability measure $\gamma_{i,t}$ such that $\gamma_{i,t}(\widehat{\theta}) = \frac{\ell_i(S_{i,t}|\widehat{\theta})}{\sum_{\bar{\theta}\in\Theta}\ell_i(S_{i,t}|\bar{\theta})}$ for all $\widehat{\theta} \in \Theta$ (when $n_{i,t} = 0$ we set $\ell_i(S_{i,t}|\widehat{\theta}) = 1$ for all $\widehat{\theta} \in \Theta$). Then the agents have the time-varying utility:

$$U_{i,t}(\nu_{i,t}, \nu_{t-1}) = R_i - C_i \sum_{j=1}^{n} a_{ij} D_{KL}\left(\nu_{i,t}|\nu_{j,t-1}\right) - C_i D_{KL}\left(\nu_{i,t}|\mathcal{M}_i(\gamma_{i,t})\right). \tag{4.18}$$

Optimizing this utility yields log-linear learning, which we leverage in our OL Algorithm 10.

4.2.6 Performance Analysis Framework

Our proposed log-linear update rules in Section 4.2.5 rely on adding zero-mean Laplace noise to the likelihood functions drawn from distributions that are independent of the states. For example, in the MLE problem, in expectation, log-linear updates can identify MLE states $\Theta^\star$. However, the added noise makes the algorithm output random, so the algorithm needs to be repeated to achieve the desired accuracy level. Therefore, we need a systematic way to control the error of the output of any algorithm $\mathcal{A}$. Providing high-probability guarantees for an algorithm $\mathcal{A}$ comes at a cost: The algorithm needs to be repeated in sufficiently many rounds and its outputs combined across the rounds.

Type I and Type II error rates. To control the output uncertainty resulting from privacy-preserving randomization noise, our distributed MLE algorithms, in addition to respecting a set DP budget $\varepsilon > 0$, also admit two types of error guarantees, which we refer to as Type I and Type II error probabilities and denote by α and $1 - \beta$, following the hypothesis testing nomenclature. In fact, in Appendix C.7 we show that our distributed MLE algorithms and guarantees can be transformed to conduct a distributed hypothesis test at the significance level

α. For a distributed MLE algorithm $\mathcal{A}$ that returns a set of maximum likelihood estimators $\widehat{\Theta}^{\mathcal{A}} \subseteq \Theta$, we define the *Type I* error rate α as the probability that $\left\{\Theta^\star \not\supseteq \widehat{\Theta}^{\mathcal{A}}\right\}$, which can be controlled by bounding $\mathbb{P}\left[\Theta^\star \supseteq \widehat{\Theta}^{\mathcal{A}}\right] \geq 1 - \alpha$. Similarly, we define the *Type II* error rate $1 - \beta$ as the probability of the event $\left\{\Theta^\star \not\subseteq \widehat{\Theta}^{\mathcal{A}}\right\}$, which can be controlled by ensuring that $\mathbb{P}\left[\Theta^\star \subseteq \widehat{\Theta}^{\mathcal{A}}\right] \geq \beta$. A Type I error occurs when the algorithm detects a superset of the MLE set $\Theta^\star$. A Type II error occurs when the algorithm filters too many states, missing some MLE states in its output, thus generating a subset of the MLE set $\Theta^\star$.

Returning to our examples from before, when selecting among treatments with severe side effects, we want to limit the possibility of selecting ineffective treatments by ensuring a small Type I error rate α so that $\mathbb{P}\left[\Theta^\star \supseteq \widehat{\Theta}^{\mathcal{A}}\right] \geq 1 - \alpha$. Similarly, when conducting a clinical trial, we need to ensure efficacy at a desired level of statistical significance (e.g., $\alpha = 0.05$). On the other hand, when developing a new cancer screening tool, we want MLE states to be included in the algorithm output ($\{\Theta^\star \subseteq \widehat{\Theta}^{\mathcal{A}}\}$) with high probability, that is, for β to be high (e.g., $\beta = 0.8$). This will ensure that we can detect all patients who are at high risk of cancer ($\Theta^\star$). In this case, it is important to control the Type II error rate so that $\mathbb{P}\left[\Theta^\star \not\subseteq \widehat{\Theta}^{\mathcal{A}}\right] \leq 1 - \alpha$ for a large enough β, but it may be acceptable to misidentify some patients as high risk (i.e., for $\Theta^{\mathcal{A}}$ to include some non-MLE states). In Section 4.2.8, we show that arithmetic or geometric averaging of beliefs across the rounds may each be suitable, depending on the type of error that one needs to preclude or control.

Communication complexity. To achieve guarantees on the DP budget and the two error probabilities, we must run our algorithms in $K\left(\varepsilon, \eta, \Theta, \mathcal{G}, \{\ell_i(\cdot|\cdot)\}_{i\in[n]}\right)$ rounds and with $T\left(\varepsilon, \eta, \Theta, \mathcal{G}, \{\ell_i(\cdot|\cdot)\}_{i\in[n]}\right)$ iterations in each round, where η here

corresponds to either α or $1-\beta$, or the maximum of the two (depending on the algorithm). We define Communication Complexity $= K\left(\varepsilon, \eta, \Theta, \mathcal{G}, \{\ell_i(\cdot|\cdot)\}_{i\in[n]}\right) \cdot T\left(\varepsilon, \eta, \Theta, \mathcal{G}, \{\ell_i(\cdot|\cdot)\}_{i\in[n]}\right)$ as the total number of belief updates. We summarize our communication complexity bounds for MLE and online learning in Table 4.2 at the beginning of Section 4.2.7 before explaining them in detail. Beyond the privacy budget ε, the error probability η, and the number of agents n, the results of Table 4.2 also depend on the statistical properties of the information environment and the network structure, as described below:

- Regarding the *private signal strcutures*, the bounds depend on the largest log-likelihood magnitude

$$\Gamma_{n,\Theta} = \max_{i\in[n],\widehat{\theta}\in\Theta} |\log \gamma_{i,t}(\widehat{\theta})|,$$

  the minimum divergence between any non-MLE state and an MLE state

$$l_{n,\Theta} = \min_{\bar{\theta}\in\bar{\Theta},\theta^\star\in\Theta^\star} \left|\sum_{i=1}^{n} \xi_i D_{KL}\left(\ell_i(\cdot|\bar{\theta})|\ell_i(\cdot|\theta^\star)\right)\right|,$$

  the global sensitivity $\Delta_{n,\Theta} = \max_{i\in[n],t\in\mathbb{N}} \Delta_{i,t}$, the sum of variances of the number of signals $\Xi_n = \sum_{i=1}^{n} \chi_i$, and the maximum deviation of the KL divergence

$$Q_{n,\Theta} = \max_{i\in[n],\bar{\theta}\in\bar{\Theta},\theta^\star\in\Theta^\star} \sqrt{\mathbb{V}\left[\log\left(\frac{\ell_i(\cdot|\bar{\theta})}{\ell_i(\cdot|\theta^\star)}\right)\right]}.$$

- Regarding the *graph structure*, our bounds depend on the second-largest eigenvalue modulus (SLEM) of A, $b_n^\star = b_n^\star$, and the SLEM of $(A+I)/2$, $a_n^\star = |\lambda_2(A+I)|/2$.

Setting	With DP (ours)	Without DP [343]
	Communication Complexity with respect to ε, η	
MLE (AM/GM)	$O_{\lvert\Theta\rvert,n}\left(\log(1/\eta)(\log(1/\eta)+\log(1/\varepsilon)+\log(1/\varrho)\right)$	$O_{\lvert\Theta\rvert,n}\left(1\right)$
MLE (Threshold)	$O_{\lvert\Theta\rvert,n}\left(\frac{\log(1/\eta)}{\pi^2}(\log(1/\eta)+\log(1/\varepsilon)+\log(1/q))\right)$	$O_{\lvert\Theta\rvert,n}\left(1\right)$
Online Learning	$O_{\lvert\Theta\rvert,n}\left(\frac{1}{\eta^{3/2}}\frac{1}{\varepsilon}\right)$	$O_{\lvert\Theta\rvert,n}\left(1\right)$
	Communication Complexity with respect to n	
MLE (AM/GM)	$O_{\lvert\Theta\rvert,\varepsilon,\eta}\left(\max\left\{\log\left(\frac{n}{l_{n,\Theta}}\right), \frac{\log\left(\frac{n(\Gamma_{n,\Theta}+\Delta_{n,\Theta})}{\varrho}\right)}{\log(1/a_n^\star)}\right\}\right)$	$O_{\lvert\Theta\rvert}\left(\max\left\{\log\left(\frac{n}{l_{n,\Theta}}\right), \frac{\log(n\Gamma_{n,\Theta})}{\log(1/a_n^\star)}\right\}\right)$
MLE (Threshold)	$O_{\lvert\Theta\rvert,\varepsilon,\eta}\left(\frac{1}{\pi^2}\max\left\{\log\left(\frac{n}{l_{n,\Theta}}\right), \frac{\log\left(\frac{n(\Gamma_{n,\Theta}+\Delta_{n,\Theta})}{q}\right)}{\log(1/a_n^\star)}\right\}\right)$	$O_{\lvert\Theta\rvert}\left(\max\left\{\log\left(\frac{n}{l_{n,\Theta}}\right), \frac{\log(n\Gamma_{n,\Theta})}{\log(1/a_n^\star)}\right\}\right)$
Online Learning	$O_{\lvert\Theta\rvert,\varepsilon,\eta}\left(\frac{n(Q_{n,\Theta}+\Delta_{n,\Theta})(\max_{i\in[n]}\xi_i+\sqrt{\Xi_n})}{l_{n,\Theta}(1-b_n^\star)}\right)$	$O_{\lvert\Theta\rvert}\left(\frac{nQ_{n,\Theta}(\max_{i\in[n]}\xi_i+\sqrt{\Xi_n})}{l_{n,\Theta}(1-b_n^\star)}\right)$
	Communication Complexity with respect to $\lvert\Theta\rvert$	
MLE (AM/GM)	$O_{n,\varepsilon,\eta}\left(\lvert\Theta\rvert\log\lvert\Theta\rvert\left(\log\lvert\Theta\rvert+\log\left(\frac{\Gamma_{n,\Theta}+\lvert\Theta\rvert\log\lvert\Theta\rvert\Delta_{n,\Theta}}{\varrho}\right)\right)\right)$	$O_n\left(\log\Gamma_{n,\Theta}\right)$
MLE (Threshold)	$O_{n,\varepsilon,\eta}\left(\frac{\log\lvert\Theta\rvert}{\pi^2}\left(\log\lvert\Theta\rvert+\log\left(\frac{\Gamma_{n,\Theta}+\lvert\Theta\rvert\log\lvert\Theta\rvert\Delta_{n,\Theta}}{q}\right)\right)\right)$	$O_n\left(\log\Gamma_{n,\Theta}\right)$
Online Learning	$O_{n,\varepsilon,\eta}\left(\frac{\lvert\Theta\rvert(Q_{n,\Theta}+\lvert\Theta\rvert\Delta_{n,\Theta})}{l_{n,\Theta}}\right)$	$O_n\left(\frac{\lvert\Theta\rvert Q_{n,\Theta}}{l_{n,\Theta}}\right)$

Table 4.2: Communication complexity of distributed inference algorithms for a fixed privacy budget $\varepsilon > 0$ and target maximum Type I/Type II error $\eta \in (0,1)$. We use $O_{a_1,\ldots,a_N}(\cdot)$ to denote the big-O notation where the constants are allowed to depend on $a_1,\ldots,a_N$. The overhead of introducing privacy is outlined in blue. For compactness in notation, η refers to $\max\{\alpha, 1-\beta\}$, ϱ refers to $\min\{\varrho^{\mathrm{AM}}, \varrho^{\mathrm{GM}}\}$, π refers to $\min\{\pi_2, \pi_1\}$, and q refers to $\min\{1-q_2, q_1\}$ (see Theorems 4.2.2 and 4.2.5). The AM/GM algorithms have matching communication complexities whenever $q = O(1)$ and $\pi = O\left(1/\sqrt{\lvert\Theta\rvert}\right)$. The non-DP results are due to [343].

4.2.7 Performance and Privacy Guarantees

We study distributed belief exchange algorithms to find MLEs with theoretical guarantees of privacy and performance (error probability and communication complexity) in Section 4.2.8. These non-Bayesian belief statistics have a natural application for distributed hypothesis testing, for which we give statistical significance guarantees in Section 4.2.9. They can also be used for the online learning of the true alternative based on streaming data, which we analyze in Section 4.2.10.

Maximum Likelihood Estimation and Hypothesis Testing. Our first set of re-

sults considers the recovery of MLEs $\Theta^\star \subset \Theta$ by using two main types of algorithms: The first set of algorithms averages the beliefs of the K independent rounds resulting from log-linear updates both arithmetically and geometrically. As noted earlier in the paper, arithmetic averaging can recover a superset of $\Theta^\star$ – controlling Type I errors – while geometric averaging can recover a subset of $\Theta^\star$ – controlling Type II errors. The formal description of the algorithm is given in Algorithm 8.

Our second algorithm, instead of averaging beliefs, uses two thresholds to select the states for which the average number of times their belief exceeds a (third) threshold is larger than the two initial thresholds. The advantage of this algorithm is that it gives more flexibility in controlling Type I and Type II errors, and it can even recover the exact MLE set but at a high cost to runtime. The formal description of the algorithm is given in Algorithm 9. Our main result for the MLE follows: Given Type I and Type II errors α and $1-\beta$, respectively, and $\eta = \max\{\alpha, 1-\beta\}$, the following hold:

- For thresholds $\varrho^{\mathrm{AM}}, \varrho^{\mathrm{GM}} > 0$, $\varrho = \min\{\varrho^{\mathrm{AM}}, \varrho^{\mathrm{GM}}\}$, there is an algorithm that requires

$$K \cdot T = O\left(|\Theta| \log\left(\frac{|\Theta|}{\eta}\right) \max\left\{\log\left(\frac{n}{l_{n,\Theta}}\right), \frac{\log\left(|\Theta| n(\Gamma_{n,\Theta} + \Delta_{n,\Theta}/\varepsilon)/\varrho\right)}{\log(1/a_n^\star)}\right\}\right)$$

  exchanges of the beliefs of an agent and constructs two estimators $\widehat{\Theta}_{i,T}^{\mathrm{GM}}$ and $\Theta_{i,T}^{\mathrm{AM}}$ such that $\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star \subseteq \Theta_{i,T}^{\mathrm{AM}}$ with probability at least $1 - 2\eta$.

- For thresholds $q_1, q_2 \in (0,1)$, accuracy parameters $\pi_1, \pi_2 \in (0,1)$, $q = \min\{1 - q_1, q_2\}$, and $\pi = \min\{\pi_1, \pi_2\}$ there is an algorithm that requires

$$K \cdot T = O\left(\frac{1}{\pi^2} \log\left(\frac{|\Theta|}{\eta}\right) \max\left\{\log\left(\frac{n}{l_{n,\Theta}}\right), \frac{\log\left(|\Theta| n(\Gamma_{n,\Theta} + \Delta_{n,\Theta}/\varepsilon)/q\right)}{\log(1/a_n^\star)}\right\}\right)$$

exchanges of the beliefs of an agent, and constructs two estimators $\widehat{\Theta}_{i,T}^{\text{thres},1}$ and $\widehat{\Theta}_{i,T}^{\text{thres},2}$ such that $\widehat{\Theta}_{i,T}^{\text{thres},1} \subseteq \Theta^\star \subseteq \widehat{\Theta}_{i,T}^{\text{thres},2}$ with probability at least $1 - 2\eta$.

- The noise distributions that optimize the number of belief exchanges of an agent are the Laplace distributions with parameters $\Delta_{n,\Theta}|\Theta|^2 \log(|\Theta|/\eta)/\varepsilon$ (up to constant multiplicative factors).
- The resulting estimates are ε-DP with respect to private signals.
- Theorems 4.2.2 and 4.2.5 give formal statements of these results.
- The results of the GM algorithm can be extended to design hypothesis tests at significance level α (see Proposition 4.2.6).

Online Learning. In the sequel, we provide an algorithm that can learn from intermittent streams of data in an online manner, assuming an identifiable joint model $\Lambda(\cdot)$ and data generated from a distribution with (true) parameter $\theta^\circ \in \Theta$. The algorithm is simple and returns the state with the highest belief value. Our main result for the online learning algorithm follows: Given an accuracy parameter $\eta \in (0, 1)$ and the identifiability condition $\sum_{i=1}^{n} \xi_i D_{KL}\left(\ell_i(\cdot|\bar{\theta})|\ell_i(\cdot|\theta^\circ)\right) > 0, \forall \bar{\theta} \neq \theta^\circ$:

- There exists an algorithm that requires $K = 1$ round and

$$T = O\left(\frac{n|\Theta|(Q_{n,\Theta} + \Delta_{n,\Theta}|\Theta|/\varepsilon)\left(\max_{i\in[n]} \xi_i + \sqrt{\frac{\Xi_n}{\eta}}\right)}{l_{n,\Theta}\eta(1 - b_n^\star)}\right)$$

exchanges of the beliefs of an agent, and returns an estimator $\widehat{\theta}_{i,T}^{\text{OL}}$ such that $\widehat{\theta}_{i,T}^{\text{OL}} = \theta^\circ$ with probability at least $1-\eta$. The noise distributions that optimize the number of belief exchanges of an agent are the Laplace distributions with parameters $\Delta_{n,\Theta}|\Theta|/\varepsilon$.

- The resulting estimates are ε-DP with respect to private signals.
- Theorem 4.2.8 gives a formal version. Table 4.2 compares the DP algorithms with their non-DP counterparts and presents the overhead of introducing privacy in each case.

In this section, we present the algorithms used to perform distributed MLE and OL. As noted earlier in the paper, the algorithms are based on log-linear belief exchanges between the agents. Our results are non-asymptotic and determine upper and lower bounds in the communication complexity $K \cdot T$ for a given privacy budget ε, Type I error α, and Type II error $1 - \beta$.

4.2.8 Distributed MLE

The first idea behind the MLE algorithm is to introduce multiplicative noise subject to DP to the likelihood functions $\gamma_i(\widehat{\theta})$. Adding multiplicative noise – which corresponds to additive noise in the log domain – ensures privacy. The agents then communicate their beliefs about the states with their local neighbors and form estimates of the true MLE over time. However, introducing noise makes the algorithm randomized, and therefore, the agents may misidentify the MLE with a non-trivial probability. To overcome this problem and guarantee Type I (resp. Type II) error at most α (resp. $1 - \beta$), we run the algorithm for K independent rounds and combine these K estimates to produce the final beliefs. By setting K accordingly, we can reduce the algorithm's errors, which we show in Theorem 4.2.1.

To produce the final estimates, we rely on two ways of aggregating the K rounds of the algorithm: The first approach is to take the arithmetic mean of

the K rounds to produce the final belief, which we call the AM estimator. The benefit of the AM estimator is that it can accurately w.h.p. identify all the MLE states, i.e., we can control its Type II error probability: $\mathbb{P}\left[\Theta^\star \not\subseteq \widehat{\Theta}_{i,T}^{\mathrm{AM}}\right] \leq 1-\beta$. This estimator has high recall but low precision because it can recover a superset of $\Theta^\star$. The second way to combine the K rounds is to take the geometric mean, which we call the GM estimator. For the GM estimator, we can control the Type I error probability, $\mathbb{P}\left[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \not\subseteq \Theta^\star\right] \leq \alpha$, to ensure that it recovers a subset of $\Theta^\star$ with high probability. We first start with a result on the asymptotic behavior of Algorithm 8. Specifically, we show that we can recover the MLE with high probability by repeating the algorithm K times for appropriately chosen K:

Theorem 4.2.1. *For Algorithm 8, with state-independent noise distributions $\mathcal{D}_i(\widehat{\theta};\varepsilon) = \mathcal{D}_i(\varepsilon)$ that satisfy ε-DP and do not depend on the state $\widehat{\theta}$; as $\varrho^{\mathrm{AM}} \to \infty$ and $\varrho^{\mathrm{GM}} \to \infty$,*

- *for $K \geq |\bar{\Theta}| \log\left(|\Theta^\star|/(1-\beta)\right)$, we have $\lim_{T\to\infty} \mathbb{P}\left[\Theta^\star \subseteq \widehat{\Theta}_{i,T}^{\mathrm{AM}}\right] \geq \beta$ for all $i \in [n]$.*
- *for $K \geq |\Theta^\star| \log\left(|\bar{\Theta}|/\alpha\right)$, we have $\lim_{T\to\infty} \mathbb{P}\left[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star\right] \geq 1-\alpha$ for all $i \in [n]$.*
- *The beliefs exchanged and the resulting estimates are ε-DP with respect to private signals.*

Repeating Algorithm 8 for $K \geq |\Theta| \log(|\Theta|/\min\{\alpha, 1-\beta\})$ iterations, one can assert $\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star \subseteq \widehat{\Theta}_{i,T}^{\mathrm{AM}}$ as $T \to \infty$ with probability $\beta - \alpha$ without knowing $f^\star$. Also, it is interesting to point out that the above theorem holds regardless of the noise, as long as the noise distribution does not depend on the state for a given agent and the noise is ε-DP.

The distributed MLE algorithm is repeated K times for each of the $|\Theta|$ states, and an attacker would have more observations of the same signals; therefore, we need to rescale the privacy guarantee for each run and each state by

Algorithm 8 Private Distributed MLE (AM/GM)

Inputs: Privacy budget ε, Error probabilities $\alpha, 1-\beta$, Log-belief Thresholds $\varrho^{\mathrm{AM}}, \varrho^{\mathrm{GM}} > 0$.
Initialization: Set the number of iterations T and the number of rounds K as indicated by Theorem 4.2.1 (for the asymptotic case) or Theorem 4.2.2 (for the non-asymptotic case), and $\tau^{\mathrm{AM}} = 1/(1+e^{\varrho^{\mathrm{AM}}})$ (resp. for τ^{GM}). The DP noise distribution for protecting beliefs is $\mathcal{D}_i(\widehat{\theta};\varepsilon)$ which can be set optimally according to Theorem 4.2.2.
Procedure: The following is repeated in K rounds indexed by $k \in [K]$. In each round k, agents begin by forming noisy likelihoods $\sigma_{i,k}(\widehat{\theta}) = e^{d_{i,k}(\widehat{\theta})}\gamma_i(\widehat{\theta})$, where $\gamma_i(\widehat{\theta}) = \prod_{j=1}^{n_i} \ell_i(s_i^j|\widehat{\theta})$ and $d_{i,k}(\widehat{\theta}) \sim \mathcal{D}_i(\widehat{\theta};\varepsilon)$ independently across agents $i \in [n]$ and states $\widehat{\theta} \in \Theta$. The agents initialize their beliefs to $\nu_{i,k,0}(\widehat{\theta}) = \sigma_{i,k}(\widehat{\theta})/\sum_{\tilde{\theta}\in\Theta}\sigma_{i,k}(\tilde{\theta})$, and over the next T time steps, they communicate with their neighbors and update their beliefs accordingly:

$$\nu_{i,k,t}(\widehat{\theta}) = \frac{\nu_{i,k,t-1}^{1+a_{ii}}(\widehat{\theta}) \prod_{j\in\mathcal{N}_i} \nu_{j,k,t-1}^{a_{ij}}(\widehat{\theta})}{\sum_{\tilde{\theta}\in\Theta} \nu_{i,k,t-1}^{1+a_{ii}}(\tilde{\theta}) \prod_{j\in\mathcal{N}_i} \nu_{j,k,t-1}^{a_{ij}}(\tilde{\theta})} \quad \text{for every } \widehat{\theta}\in\Theta, k\in[K] \text{ and } t\in[T]. \tag{4.19}$$

After the T iterations, the agents aggregate the outcome of the K rounds:

$$\nu_{i,T}^{\mathrm{AM}}(\widehat{\theta}) = \frac{\sum_{k\in[K]}\nu_{i,k,T}(\widehat{\theta})}{K}, \quad \nu_{i,T}^{\mathrm{GM}}(\widehat{\theta}) = \frac{\prod_{k\in[K]}\nu_{i,k,T}(\widehat{\theta})^{1/K}}{\sum_{\tilde{\theta}\in\Theta}\prod_{k\in[K]}\nu_{i,k,T}(\tilde{\theta})^{1/K}} \quad \text{for every } \widehat{\theta}\in\Theta. \tag{4.20}$$

Outputs: Return

$$\widehat{\Theta}_{i,T}^{\mathrm{AM}} = \left\{\widehat{\theta}\in\Theta : \nu_{i,T}^{\mathrm{AM}}(\widehat{\theta}) \geq \tau^{\mathrm{AM}}\right\}, \quad \widehat{\Theta}_{i,T}^{\mathrm{GM}} = \left\{\widehat{\theta}\in\Theta : \nu_{i,T}^{\mathrm{GM}}(\widehat{\theta}) \geq \tau^{\mathrm{GM}}\right\}.$$

$K|\Theta|$. Thus, choosing $\mathcal{D}_i(\varepsilon) = \mathrm{Lap}\left(\frac{K|\Theta|\Delta_{n,\Theta}}{\varepsilon}\right)$ satisfies ε-DP and the assumptions of Theorem 4.2.1. Our nonasymptotic analysis (presented next) shows that $\mathcal{D}_i(\varepsilon) = \mathrm{Lap}\left(\frac{K|\Theta|\Delta_{n,\Theta}}{\varepsilon}\right)$ is indeed optimal to minimize the required number of iterations per round.

The previous analysis focused on the regime where $T \to \infty$. The next question that arises is to study the behavior of Algorithm 8 for finite t. As expected,

the speed of convergence depends on the sum of standard deviations of the noise, that is, $V_{n,\Theta} = \sum_{i=1}^{n} \sqrt{\mathbb{V}_{d_i \sim \mathcal{D}_i(\varepsilon)}[d_i]}$. Our result follows:

Theorem 4.2.2. *The following holds for Algorithm 8, and any $\varrho^{\mathrm{AM}}, \varrho^{\mathrm{GM}} > 0$:*

- *For* $T \geq \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2\alpha\varrho^{\mathrm{GM}}\sqrt{K}}\right)}{\log(1/a_n^\star)}\right\}$ *and* $K \geq |\Theta^\star|\log(|\bar{\Theta}|/\alpha)$, *we have* $\mathbb{P}[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star] \geq 1 - 2\alpha$.
- *For* $T \geq \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)K(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2\log(1/1-\beta)\varrho^{\mathrm{AM}}}\right)}{\log(1/a_n^\star)}\right\}$ *and* $K \geq |\bar{\Theta}|\log(|\Theta^\star|/(1-\beta))$, *we have* $\mathbb{P}[\Theta^\star \subseteq \widehat{\Theta}_{i,T}^{\mathrm{AM}}] \geq 2\beta - 1$.
- *The optimal distributions that minimize the convergence time T, are* $\mathcal{D}_i^\star(\varepsilon) = \mathrm{Lap}\left(\frac{\Delta_{n,\Theta}K|\Theta|}{\varepsilon}\right)$.
- *The beliefs exchanged and the resulting estimates are ε-DP with respect to private signals.*

To minimize communication complexity, it suffices to pick the optimal threshold that makes the terms inside the maximum equal – and, hence, the maximum is minimized – which corresponds to $\varrho_\star^{\mathrm{AM}} = \left(\frac{|\Theta|^2(n-1)K(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2\log(1/(1-\beta))}\right)^{\frac{\log 2}{\log(2/a_n^\star)}}\left(\frac{l_{n,\Theta}}{2n}\right)^{\frac{-\log a_n^\star}{\log(2/a_n^\star)}}$, for AM and $\varrho_\star^{\mathrm{GM}} = \left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2\alpha\sqrt{K}}\right)^{\frac{\log 2}{\log(2/a_n^\star)}}\left(\frac{l_{n,\Theta}}{2n}\right)^{\frac{-\log a_n^\star}{\log(2/a_n^\star)}}$ for GM.

A Two Threshold Algorithm for Recovering the MLE. In Algorithm 9, we provide a two threshold algorithm to simultaneously control both Type I and Type II error probabilities, with more design flexibility that comes at an increased cost of communication complexity.

The analysis of Theorem 4.2.1 shows that in a given round k, the probability an MLE state $\theta^\star \in \Theta$ ends up positive as $T \to \infty$ is at least $1/|\bar{\Theta}|$, so in expectation

Algorithm 9 Private Distributed MLE (Two Threshold Algorithm)

Inputs: Privacy budget ε, Error probabilities $\alpha, 1-\beta$, Log-belief Thresholds $\varrho^{\text{thres},1}, \varrho^{\text{thres},2} > 0$.
Initialization: Set the number of iterations T and the number of rounds K, and the thresholds $\tau^{\text{thres},2}, \tau^{\text{thres},1}$ as indicated by Theorem 4.2.3 (for the asymptotic case) or Theorem 4.2.5 (for the non-asymptotic case), and $\widehat{\tau}^{\text{thres},1} = \frac{1}{1+e^{\varrho^{\text{thres},1}}}$ (resp. $\widehat{\tau}^{\text{thres},2}$). The DP noise distribution for protecting beliefs is $\mathcal{D}_i(\widehat{\theta}; \varepsilon)$ which can be set optimally according to Theorem 4.2.5.
Procedure: The following is repeated in K rounds indexed by $k \in [K]$. In each round k, the agents begin by forming the noisy likelihoods $\sigma_{i,k}(\widehat{\theta}) = e^{d_{i,k}(\widehat{\theta})}\gamma_i(\widehat{\theta})$, where $\gamma_i(\widehat{\theta}) = \prod_{j=1}^{n_i} \ell_i(s_i^j|\widehat{\theta})$ and $d_{i,k}(\widehat{\theta}) \sim \mathcal{D}_i(\widehat{\theta}; \varepsilon)$ independently across agents $i \in [n]$ and states $\widehat{\theta} \in \Theta$. The agents initialize their beliefs to $\nu_{i,k,0}(\widehat{\theta}) = \sigma_{i,k}(\widehat{\theta}) / \sum_{\tilde{\theta}\in\Theta} \sigma_{i,k}(\tilde{\theta})$. Over the next T time steps, the agents update their belief after communicating with their neighbors, and according to the following update rule:

$$\nu_{i,k,t}(\widehat{\theta}) = \frac{\nu_{i,k,t-1}^{1+a_{ii}}(\widehat{\theta}) \prod_{j\in\mathcal{N}_i} \nu_{j,k,t-1}^{a_{ij}}(\widehat{\theta})}{\sum_{\tilde{\theta}\in\Theta} \nu_{i,k,t-1}^{1+a_{ii}}(\tilde{\theta}) \prod_{j\in\mathcal{N}_i} \nu_{j,k,t-1}^{a_{ij}}(\tilde{\theta})} \quad \text{for every } \widehat{\theta} \in \Theta, k \in [K] \text{ and } t \in [T]. \tag{4.21}$$

After T iterations, each agent aggregates the results of the K rounds as:

$$N_{i,T}^{\text{thres},1}(\widehat{\theta}) = \frac{1}{K}\sum_{k\in[K]} \mathbb{1}\left\{\nu_{i,k,T}(\widehat{\theta}) > \widehat{\tau}^{\text{thres},1}\right\}, \quad N_{i,T}^{\text{thres},2}(\widehat{\theta}) = \frac{1}{K}\sum_{k\in[K]} \mathbb{1}\left\{\nu_{i,k,T}(\widehat{\theta}) > \widehat{\tau}^{\text{thres},2}\right\} \quad \text{for every } \widehat{\theta} \in \Theta. \tag{4.22}$$

Outputs: Return

$$\widehat{\Theta}_{i,T}^{\text{thres},1} = \left\{\widehat{\theta} \in \Theta : N_{i,T}^{\text{thres},1}(\widehat{\theta}) \geq \tau^{\text{thres},1}\right\}, \quad \widehat{\Theta}_{i,T}^{\text{thres},2} = \left\{\widehat{\theta} \in \Theta : N_{i,T}^{\text{thres},2}(\widehat{\theta}) \geq \tau^{\text{thres},2}\right\}.$$

at least $K/|\bar{\Theta}|$ rounds will yield a positive belief. On the other hand, we know that for a non-MLE state $\bar{\theta}$, in expectation, at most $(1 - 1/|\Theta^\star|)K$ trials will come up heads. For brevity, we define $p_1 = 1 - 1/|\Theta^\star|$ and $p_2 = 1/|\bar{\Theta}|$. Moreover, we define $N_{i,T}^{\text{thres},1}(\widehat{\theta})$ (resp. $N_{i,T}^{\text{thres},2}(\widehat{\theta})$) as the (average) number of times the belief $\nu_{i,k,t}(\widehat{\theta})$ exceeds a threshold $\widehat{\tau}^{\text{thres},1}$ (resp. $\widehat{\tau}^{\text{thres},2}$) for $k \in [K]$.

Because $N_{i,T}^{\text{thres},1}(\widehat{\theta})$ (resp. $N_{i,T}^{\text{thres},2}(\widehat{\theta})$) is an average of independent indicator

variables for all $\widehat{\theta} \in \Theta$, the Chernoff bound indicates that it concentrates around its mean $\mathbb{E}\left[N_{i,T}^{\text{thres},1}(\widehat{\theta})\right]$ (resp. $\mathbb{E}\left[N_{i,T}^{\text{thres},2}(\widehat{\theta})\right]$). This prompts the development of the following simple algorithm, which resembles boosting algorithms such as AdaBoost [160]. The algorithm uses two thresholds $\tau^{\text{thres},1}$ and $\tau^{\text{thres},2}$ to estimate the MLE states as those whose beliefs exceed $\hat{\tau}^{\text{thres},1}$ and $\hat{\tau}^{\text{thres},2}$ at least $\tau^{\text{thres},1}$ and $\tau^{\text{thres},2}$ times, leading to output sets $\widehat{\Theta}_{i,T}^{\text{thres},1}$ and $\widehat{\Theta}_{i,T}^{\text{thres},2}$ respectively.

We first present an asymptotic result:

Theorem 4.2.3. *For Algorithm 9, with $p_1 = 1 - 1/|\Theta^\star|$ and $p_2 = 1/|\bar{\Theta}|$, noise distributions $\mathcal{D}_i(\widehat{\theta}; \varepsilon) = \mathcal{D}_i(\varepsilon)$ that are ε-DP and do not depend on the state $\widehat{\theta}$, we have that as $\varrho^{\text{thres},1} \to \infty$ and $\varrho^{\text{thres},2} \to \infty$,*

- *for any $\pi_1 > 0$, $\tau^{\text{thres},1} = (1 + \pi_1)p_1$, and $K \geq \frac{\log(|\bar{\Theta}|/\alpha)}{2\pi_1^2}$, we have that $\lim_{T\to\infty} \mathbb{P}\left[\widehat{\Theta}_{i,T}^{\text{thres},1} \subseteq \Theta^\star\right] \geq 1 - \alpha$, for all $i \in [n]$.*
- *for any $\pi_2 > 0$, $\tau^{\text{thres},2} = (1 - \pi_2)p_2$, and $K \geq \frac{\log(|\Theta^\star|/(1-\beta))}{2\pi_2^2}$, we have that $\lim_{T\to\infty} \mathbb{P}\left[\Theta^\star \subseteq \widehat{\Theta}_{i,T}^{\text{thres},2}\right] \geq \beta$, for all $i \in [n]$.*

Similarly to Theorem 4.2.1, the estimator $\widehat{\Theta}_{i,T}^{1,\text{thres}}$ has a low Type I error and the estimator $\widehat{\Theta}_{i,T}^{2,\text{thres}}$ has a low Type II error. If the agents do not have knowledge of $|\Theta^\star|$, as long as they choose thresholds $\tau^{\text{thres},1\prime} \geq (1+\pi_1)p_1 = \tau^{\text{thres},1}$ and $\tau^{\text{thres},2\prime} \leq (1 - \pi_2)p_2 = \tau^{\text{thres},2}$, they can obtain the same guarantees. For example, one can choose the following upper and lower bounds to set the thresholds: $\tau^{\text{thres},1\prime} = (1 + \pi_1)(1 - 1/|\Theta|) \geq (1 + \pi_1)p_1$ and $\tau^{\text{thres},2\prime} = (1 - \pi_2)(1/|\Theta|) \leq (1 - \pi_2)p_2$. Also, running the algorithm for $K \geq \max\left\{\frac{\log(|\Theta|/\alpha)}{2\pi_1^2}, \frac{\log(|\Theta|/(1-\beta))}{2\pi_2^2}\right\}$ we can guarantee that as $T \to \infty$, we have $\Theta_{i,T}^{\text{thres},2} \subseteq \Theta^\star \subseteq \Theta_{i,T}^{\text{thres},1}$ with probability at least $\beta - \alpha$.

Observe that when $\pi_1 \to \infty$ (which yields $K \to 0$), the result is trivial since the estimator recovered is the empty set which trivially satisfies the error guarantee

with probability 1. Similarly, when $\pi_2 \to \infty$ (which, again, yields $K \to 0$), the guarantee is satisfied with probability one since the whole state set is recovered.

Because $N_{i,T}^{\text{thres},1}(\theta^\star)$ (resp. $N_{i,T}^{\text{thres},2}(\theta^\star)$) for the MLE states are concentrated around a distribution with a mean that is at least $1/|\bar{\Theta}|$ and, similarly, $N_{i,T}^{\text{thres},1}(\bar{\theta})$ (resp. $N_{i,T}^{\text{thres},2}(\bar{\theta})$) for the non-MLE states are concentrated around their expectation which is at most $1 - 1/|\Theta^\star|$, one may rightly question whether it is possible to achieve perfect detection of $\Theta^\star$ assuming the two modes are "sufficiently" well-separated. The answer to this is affirmative as long as $p_2 > p_1$ and is given by the following corollary:

Corollary 4.2.4 (Exact Recovery with a Single Threshold)**.** *If the density of MLE states $f^\star$ satisfies*

$$\begin{cases} 0 \le f^\star \le 1, & \text{if } 1 \le |\Theta| \le 4 \\ 0 \le f^\star < \frac{1}{2} - \frac{1}{2}\sqrt{\frac{|\Theta|-4}{|\Theta|}} \quad \vee \quad \frac{1}{2} + \frac{1}{2}\sqrt{\frac{|\Theta|-4}{|\Theta|}} < f^\star \le 1, & \text{otherwise} \end{cases}, \tag{4.23}$$

the thresholds are set equal, i.e., $\tau^{\text{thres},2} = \tau^{\text{thres},1}$ and $\hat{\tau}^{\text{thres},1} = \hat{\tau}^{\text{thres},2}$ which corresponds to $\widehat{\Theta}_{i,T}^{\text{thres},2} = \widehat{\Theta}_{i,T}^{\text{thres},1}$ and $\pi_1 = (1-\pi_2)\frac{p_2}{p_1} - 1$ for some $\pi_2 > 0$, and $K \ge \max\left\{\frac{\log(|\Theta|/\alpha)}{2\pi_1^2}, \frac{\log(|\Theta|/(1-\beta))}{2\pi_2^2}\right\}$ we have that $\lim_{T\to\infty} \mathbb{P}\left[\widehat{\Theta}_{i,T}^{\text{thres},2} = \Theta^\star\right] \ge \beta - \alpha$.

By performing an analysis similar to Theorem 4.2.2, we derive a non-asymptotic result:

Theorem 4.2.5. *Let $q_1, q_2 \in (0,1)$, and $\varrho^{\text{thres},1}, \varrho^{\text{thres},2} > 0$. Then for Algorithm 9 the following hold:*

- *For any $\pi_1 > 0$, $\tau^{\text{thres},1} = (1+\pi_1)q_1$, $T \ge \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2q_1\varrho^{\text{thres},1}}\right)}{\log(1/a_n^\star)}\right\}$, and $K \ge \frac{\log(|\bar{\Theta}|/\alpha)}{2\pi_1^2}$, we have $\mathbb{P}\left[\widehat{\Theta}_{i,T}^{\text{thres},1} \subseteq \Theta^\star\right] \ge 1 - \alpha$.*

- *For any* $\pi_2 > 0$, $\tau^{\text{thres},2} = (1-\pi_2)q_2$, $T \geq \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2(1-q_2)\varrho^{\text{thres},2}}\right)}{\log(1/a_n^\star)}\right\}$, *and* $K \geq \frac{\log(|\Theta^\star|/(1-\beta))}{2\pi_2^2}$, *we have* $\mathbb{P}\left[\Theta^\star \subseteq \widehat{\Theta}_{i,T}^{\text{thres},2}\right] \geq \beta$.
- *The optimal distributions that minimize the convergence time* T *for both estimators are* $\mathcal{D}_i^\star(\varepsilon) = \text{Lap}\left(\Delta_{n,\Theta} K|\Theta|/\varepsilon\right)$.

To minimize the number of iterations, we can pick the thresholds as

$$\varrho_\star^{\text{thres},1} = \left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2q_1\sqrt{K}}\right)^{\frac{\log 2}{\log(2/a_n^\star)}}\left(\frac{l_{n,\Theta}}{2n}\right)^{\frac{\log(1/a_n^\star)}{\log(2/a_n^\star)}},$$
$$\varrho_\star^{\text{thres},2} = \left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2(1-q_2)\sqrt{K}}\right)^{\frac{\log 2}{\log(2/a_n^\star)}}\left(\frac{l_{n,\Theta}}{2n}\right)^{\frac{\log(1/a_n^\star)}{\log(2/a_n^\star)}}.$$

In addition, we can show that we can achieve perfect recovery with a single threshold as long as $q_2 > q_1$ and $\pi_1 = (1-\pi_2)\frac{q_2}{q_1} - 1$; similarly to Corollary 4.2.4.

Moreover, the above shows that communication complexity can be minimized by setting $1-q_2$ as close as possible to q_1. However, achieving perfect recovery of MLE comes at a cost to communication complexity, which is poly-logarithmic and depends on the inverse of $|1-q_2-q_1|$.

To complement our upper bounds for communication complexity, in Appendix C.10, we give information-theoretic lower bounds on the minimum number of belief exchanges required by any algorithm that achieves the same Type I and Type II error rates as ours. In the next section, we show that the GM estimator can be applied naturally to conduct distributed hypothesis tests at significance level α.

4.2.9 Application to Hypothesis Testing

The results we devised above for the MLE have a natural application in the case of hypothesis testing with simple or composite hypotheses. Specifically, the decentralized hypothesis testing algorithm at the significance level α is designed as follows: We run the GM algorithm for T iterations and K rounds and set a threshold ϱ_d to reject the null ($\theta = 0$) if the log-belief ratio exceeds it: $(n/2^{T-1}) \log(\nu_{i,T}^{\mathrm{GM}}(1)/\nu_{i,T}^{\mathrm{GM}}(0)) > \varrho_d$. For the case of a simple null and a simple alternative, the threshold ϱ_d can be derived from the threshold ϱ_c of the corresponding uniformly most powerful (UMP) centralized log-likelihood ratio test (LRT) at level $\alpha/2$. For sufficiently large T and K we can show that

Proposition 4.2.6 (Simple Hypothesis Testing)**.** *Let $\alpha \in (0,1)$ be a significance level. Let ϱ_c be the threshold of the UMP centralized log-likelihood ratio test at level $\alpha/2$, such that $\mathbb{P}[2(\Lambda(1) - \Lambda(0)) \geq \varrho_c | \theta = 0] = \alpha/2$. Then by running the GM algorithm (Algorithm 8) with Type I error rate guarantee $\alpha/2$ for T and K given in Theorem 4.2.2, and $\varrho_d = \varrho_c - 1$ we get the following: The decentralized test has Type I error at most α, that is, $\mathbb{P}\left[(n/2^{T-1}) \log(\nu_{i,T}^{\mathrm{GM}}(1)/\nu_{i,T}^{\mathrm{GM}}(0)) > \varrho_d \middle| \theta = 0\right] \leq \alpha$. The resulting hypothesis test is ε-DP.*

The idea behind the result is that, in practice, for sufficiently large T and K, $(n/2^{T-1}) \log(\nu_{i,T}^{\mathrm{GM}}(1)/\nu_{i,T}^{\mathrm{GM}}(0)) \sim 2\Lambda(1,0)$ with high probability – i.e., at least $1 - \alpha/2$ – due to Chebyshev's inequality.

However, in general, when the distribution of the centralized statistic under the null is not available, we cannot choose ϱ_c based on the UMP centralized LRT. In that case, the agents can perform a generalized likelihood ratio test locally and propagate the statistic. This sacrifices the optimality of the UMP test;

however, it is more practical in real-world scenarios where the distribution of the sum of the statistics is known under the null hypothesis. Specifically, the generalized likelihood ratio test can be used to test a composite null hypothesis ($\theta \in \tilde{\Theta}_0$) against a composite alternative ($\theta \in \tilde{\Theta}_1$, $\tilde{\Theta}_0 \cap \tilde{\Theta}_1 = \emptyset$), and requires a log-likelihood function which is twice differentiable defined in a continuous parameter space $\tilde{\Theta} = \tilde{\Theta}_0 \cup \tilde{\Theta}_1$. Specifically, in that case, each agent initialize their belief using $\gamma_i(\tilde{\Theta}_0) = \sup_{\tilde{\theta}_0 \in \tilde{\Theta}_0} \prod_{j=1}^{n_i} \ell_i(s_i^j | \tilde{\theta}_0)$ and $\gamma_i(\tilde{\Theta}) = \sup_{\tilde{\theta} \in \tilde{\Theta}} \prod_{j=1}^{n_i} \ell_i(s_i^j | \tilde{\theta})$, and runs the GM algorithm with the binary state space $\Theta = \{\tilde{\Theta}_0, \tilde{\Theta}\}$. By Wilks' theorem, for large sample sizes n_i, each local log-likelihood ratio statistic is asymptotically distributed according to the χ_1^2 distribution, and thus the sum of the independent local statistics of the n agents follows a χ_n^2 distribution. We can use the asymptotic distribution of the sum of the local log-likelihood ratio statistics to set the rejection threshold for a distributed level α test to be $\varrho_d = F^{-1}_{\chi_n^2}(1-\alpha/2) - 1$. In contrast, the centralized test has a threshold of $\varrho_c = F^{-1}_{\chi_1^2}(1-\alpha)$. We provide additional details for the extension to composite hypothesis tests in Appendix C.7.2.

4.2.10 Online Learning from Intermittent Streams

In Algorithm 10, we introduce the online learning setting, where agents receive $n_{i,t} \geq 1$ signals at every time step t, calculate the likelihood and the noisy version of it (in order to preserve DP), and then aggregate it with their self- and neighboring beliefs from iteration $t-1$.

The asymptotic analysis of the belief dynamics centers around the fact that the log-belief ratio between θ° and any other state $\bar{\theta} \neq \theta^\circ$ converges to

Algorithm 10 Private Online Learning

Inputs: Privacy budget ε, Error probabilities η.
Initialization: Set the number of iterations T as in Theorem 4.2.8. The DP noise distribution for protecting beliefs is $\mathcal{D}_i(\widehat{\theta};\varepsilon)$ which can be set optimally according to Theorem 4.2.8.
Procedure: Every time $t \in \mathbb{N}_0$, each agent forms the likelihood product of the signals that it has received at that time period: $\gamma_{i,t}(\widehat{\theta}) = \prod_{j=1}^{n_{i,t}} \ell_i(s_{i,t}^j|\widehat{\theta})$, if $n_{i,t} \geq 1$, and $\gamma_{i,t}(\widehat{\theta}) = 1$ if $n_{i,t} = 0$. The agent then draws a noise variable $d_{i,t}(\widehat{\theta}) \sim \mathcal{D}_{i,t}(\widehat{\theta};\varepsilon)$ for all $i \in [n]$, $\widehat{\theta} \in \Theta$ independently and forms $\sigma_{i,t}(\widehat{\theta}) = e^{d_{i,t}(\widehat{\theta})}\gamma_{i,t}(\widehat{\theta})$ for all $\widehat{\theta} \in \Theta$. The agent then updates its belief as:

$$\nu_{i,t}(\widehat{\theta}) = \frac{\sigma_{i,t}(\widehat{\theta})\nu_{i,t-1}^{a_{ii}}(\widehat{\theta}) \prod_{j\in\mathcal{N}_i} \nu_{j,t-1}^{a_{ij}}(\widehat{\theta})}{\sum\limits_{\tilde{\theta}\in\Theta} \sigma_{i,t}(\tilde{\theta})\nu_{i,t-1}^{a_{ii}}(\tilde{\theta}) \prod_{j\in\mathcal{N}_i} \nu_{j,t-1}^{a_{ij}}(\tilde{\theta})} \quad \text{for every } \widehat{\theta} \in \Theta \text{ and } t \in [T], \tag{4.24}$$

initialized by: $\nu_{i,0}(\widehat{\theta}) = \sigma_{i,0}(\widehat{\theta}) / \sum_{\tilde{\theta}\in\Theta} \sigma_{i,0}(\tilde{\theta})$.
Outputs: After T iterations, return $\widehat{\theta}_{i,T}^{\mathrm{OL}} = \operatorname{argmax}_{\widehat{\theta}\in\Theta} \nu_{i,T}(\widehat{\theta})$.

$(-1/n)\sum_{i=1}^n \xi_i D_{KL}\left(\ell_i(\cdot|\bar{\theta})|\ell_i(\cdot|\theta^\circ)\right)$ as $t \to \infty$ and the effect of DP noise disappears as a consequence of the Césaro mean and the weak law of large numbers. Therefore, agents learn the true states θ° exponentially fast, asymptotically. Unlike the MLE setup, for online learning, we do not need to repeat the algorithm in multiple rounds because DP noise cancels out as $T \to \infty$. For completeness, we state the asymptotic result and provide a proof sketch.

Theorem 4.2.7. *As $T \to \infty$ and $K = 1$ in Algorithm 10, for any distribution $\mathcal{D}_{i,t}(\widehat{\theta};\varepsilon) = \mathcal{D}_{i,t}(\varepsilon)$ that satisfies ε-DP and does not depend on the state $\widehat{\theta}$, we have the following: If $\sum_{i=1}^n \xi_i D_{KL}\left(\ell_i(\cdot|\bar{\theta})|\ell_i(\cdot|\theta^\circ)\right) > 0$ for all $\bar{\theta} \neq \theta^\circ$, then $\lim_{t\to\infty} \nu_{i,t}(\theta^\circ) = 1$ and the agents learn θ° asymptotically, exponentially fast with rate $-l_{n,\Theta}/n$. The resulting estimates are ε-DP with respect to private signals.*

The next theorem characterizes the non-asymptotic behavior of Algorithm 10:

Theorem 4.2.8. *Running Algorithm 10, for*

$$T = O\left(\frac{n|\Theta|(Q_{n,\Theta} + \Delta_{n,\Theta}|\Theta|/\varepsilon)\left(\max_{i\in[n]}\xi_i + \sqrt{\frac{\Xi_n}{\eta}}\right)}{l_{n,\Theta}\eta(1-b_n^\star)}\right)$$

iterations, yields $\mathbb{P}\left[\theta^\circ = \widehat{\theta}_{i,T}^{\mathrm{OL}}\right] \geq 1-\eta$ *as long as* $\sum_{i=1}^n \xi_i D_{KL}\left(\ell_i(\cdot|\bar{\theta})|\ell_i(\cdot|\theta^\circ)\right) > 0$ *for all* $\bar{\theta} \neq \theta^\circ$. *Subsequently, the noise distributions that optimize runtime are* $\mathcal{D}_{i,t}^\star = \mathrm{Lap}\left(\Delta_{n,\Theta}|\Theta|/\varepsilon\right)$. *The resulting estimates are* ε*-DP with respect to the private signals.*

Also, similarly to distributed MLE algorithms, the algorithm adds noise to each of the $|\Theta|$ states, and an attacker would have more observations of the same signals; therefore, we need to rescale the privacy guarantee of each run and each state by $|\Theta|$.

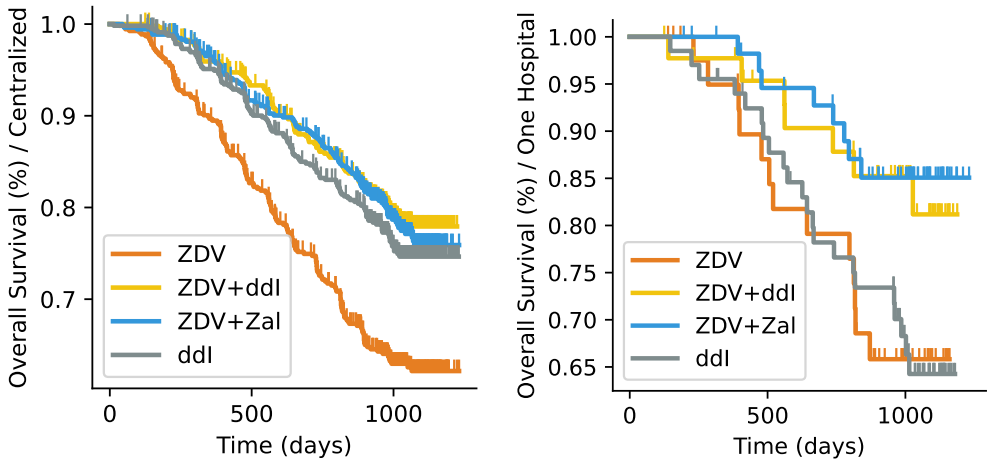
4.2.11 Simulation Study

In the ACTG dataset, the control is zidovudine (ZDV), and the three possible treatments are didanosine (ddI), zidovudine plus didanosine (ZDV + ddI), and zidovudine plus zalcitabine (ZDV + Zal). The survival curves and log hazard ratios from the fitted proportional hazards model are shown in Figure 4.11.

Hypothesis testing with a single treatment. Initially, we are interested in whether a single treatment improves patient survival. Recall from Section 4.2.2, that the treatment variable is modeled as a covariate $x_{ij} \in \{0,1\}$. We are interested in the following hypothesis test with a simple null and a composite alternative where we have used ddI as a treatment and ZDV as the control:

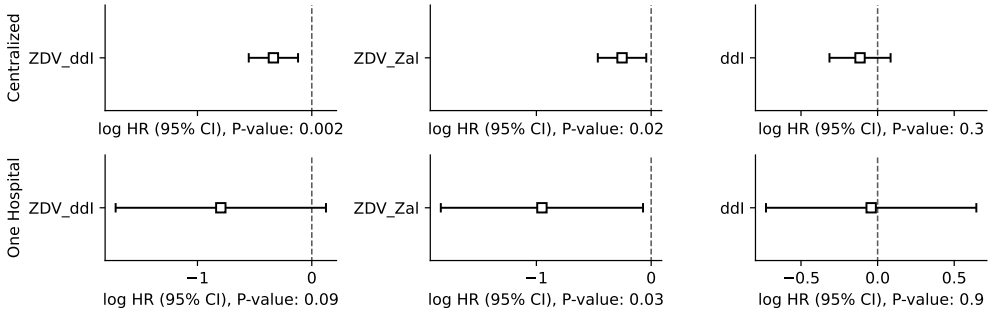
$\tilde{\Theta}_0$ $(\theta = 0)$:*The treatment has no effect on patient survival.*

$\tilde{\Theta}_1$ $(\theta < 0)$:*The treatment has a positive effect on patient survival.*



(a) Centralized

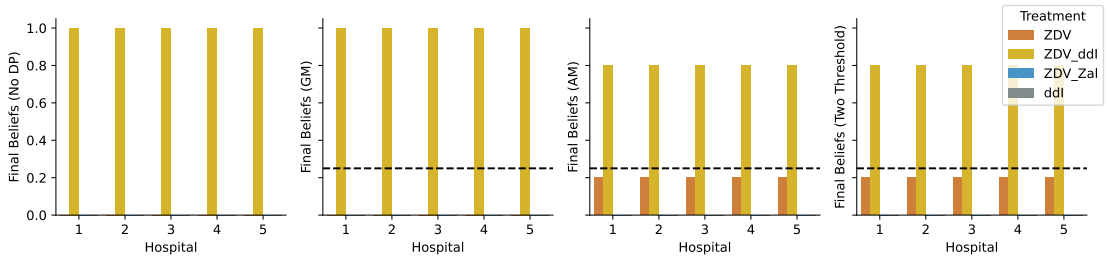
(b) One hospital



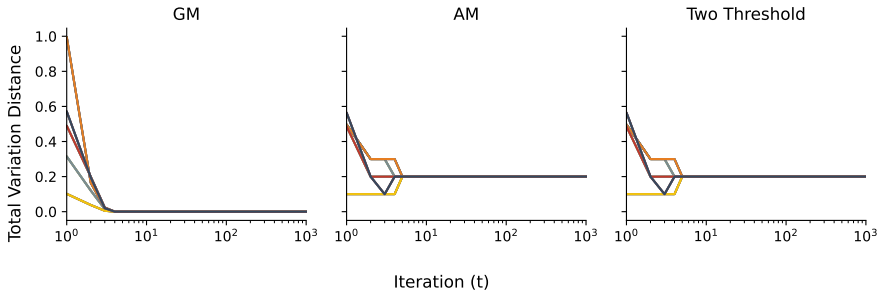
(c) Log Hazard Ratios

Figure 4.11: **Top Left:** Centralized curves. **Top Right:** Curves for one hospital. Data is split evenly among $n = 5$ hospitals. **Bottom:** Log Hazard Ratios for each of the treatments for centralized and for one hospital fitted on the data. 95% confidence intervals are reported. The data is split uniformly across centers.

We consider a network of $n = 5$ fully connected hospitals and a significance level of $\alpha = 0.05$, which is usually used in cases of clinical trials, run the algorithm presented in Appendix C.7 and compare against the centralized hypothesis testing algorithm. We evenly split the data between hospitals and between the control and treatment groups (that is, hospitals with the same amount of control or treated patients). In Appendix C.9 we calculate the global sensitivity $\Delta_{n,\Theta}$ of the proportional hazards model and show that it is $\Delta_{n,\Theta} = 2B_\theta$ where B_θ is an upper bound on the parameter value. We use a privacy budget of $\varepsilon = 1$.



(a) Final Beliefs



(b) Total Variation Distance

Figure 4.12: **Top:** Resulting beliefs (at terminal time T) for distributed MLE for AM, GM, and the Two-Threshold algorithm (recovery is performed with one threshold). **Bottom:** Total variation distance between the results of each algorithm and the non-DP baseline. The privacy budget is set to be $\varepsilon = 1$, and the errors to be $\alpha = 1 - \beta = 0.05$. The thresholds are set to 0.25 (in the belief space). The network corresponds to a network of $n = 5$ fully connected centers. All algorithms recover the best treatment (ZDV+ddI; see also Figure 4.11).

Generalized likelihood ratio statistics have been calculated with the `lifelines` package implemented in Python, which offers methods to fit the proportional hazards model. To improve the stability of estimates and controls for high correlation between covariates, we have used an L_2 regularization term $\lambda_{\text{reg}}|\theta|^2$ with $\lambda_{\text{reg}} = 0.05$. The centralized test yields a p-value of $P < 10^{-4}$. Similarly, the distributed hypothesis test produces a p-value of $P < 10^{-5}$, showing that treatment (ddI) positively affects survival.

Next, we leverage our framework to identify the best of the three treatments. To achieve that in practice with a numerically stable algorithm, we propagate the generalized likelihood ratios over each of the treatments and then convert

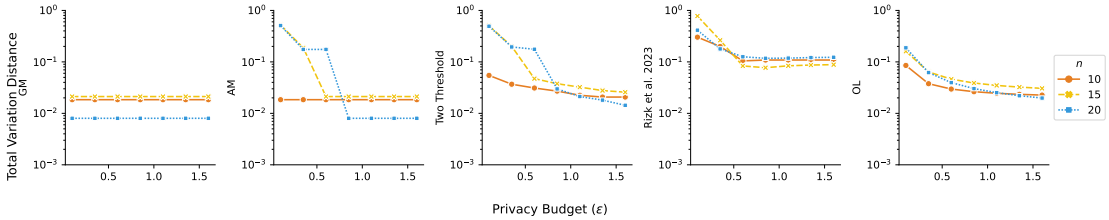


Figure 4.13: Average total variation distance between the algorithm outputs and the ground truth for the MLE algorithms (AM/GM/Two-threshold), the OL algorithm, and the first-order method introduced in [354] for a range of values for the privacy budget ε and $n \in \{10, 15, 20\}$ centers. Our MLE algorithms exhibit a smaller average total variation distance compared to the algorithm of [354].

them to beliefs. We use the same topology as above (a complete network of $n = 5$ centers), set $\varepsilon = 1$, and the errors to be $\alpha = 1 - \beta = 0.05$. Figure 4.12 shows the resulting beliefs as well as the total variation distance between each of the inference algorithms and the non-DP baseline. All algorithms are able to identify the best treatment that corresponds to ZDV + ddI and is in agreement with the ground truth (cf. Figure 4.11).

In Appendix C.11, we perform a runtime study on our proposed algorithms and show that our algorithm can run between $\sim 10^{-2}$ and 10 seconds for values of n ranging from $n = 3$ up to $n = 96$, which is significantly faster (up to 1000x) than existing methods relying on homomorphic encryption [163]. Also, in Appendix C.11, we provide experiments with data from clinical trials in advanced cancer patients, where the task is to determine whether certain biometric indices affect patient survival.

Θ	Algorithm	ε	η	n	$\lvert\Theta\rvert$
Continuous	MVUE (Algorithm 5)	polylog $(1/\varepsilon)$	polylog $(1/\eta)$	polylog (n)	—
Discrete	MLE (Algorithm 8)	polylog $(1/\varepsilon)$	polylog $(1/\eta)$	polylog (n)	poly $(\lvert\Theta\rvert)$
Continuous	OL (Algorithm 6)	poly $(1/\varepsilon)$	poly $(1/\eta)$	poly (n)	—-
Discrete	OL (Algorithm 10)	poly $(1/\varepsilon)$	poly $(1/\eta)$	poly (n)	poly $(\lvert\Theta\rvert)$

Table 4.3: Runtime overhead due to privacy. For the continuous hypothesis space, the runtime has been obtained by applying Markov's inequality to the expected value analysis by setting the error probability to be η. We have ignored quantities referring to the signal structure or the graph structure.

4.3 Discussion

Table 4.3 summarizes the results of the runtime overhead due to privacy in all algorithms. In theory, introducing privacy in the estimation task incurs a polylog $(1/\varepsilon, 1/\eta)$ cost in the runtime with respect to the privacy budget ε and the error η (which is either the estimation accuracy in the MVUE task in continuous hypothesis spaces or the Type I/Type II error in the MLE task for discrete hypothesis spaces compared to the non-DP benchmark and a polylog (n) overhead with respect to n. Moreover, the MLE task incurs a runtime overhead of poly $(|\Theta|)$ with respect to the cardinality of Θ. Moreover, in the online learning regime, we end up having a poly $(1/\varepsilon, 1/\eta)$ dependency compared to the non-private benchmark with respect to ε and η, a poly (n) dependency with respect to n, and a poly $(|\Theta|)$ dependency with respect to $|\Theta|$ (for the discrete hypothesis spaces). This shows that achieving the same privacy and accuracy levels in the online case requires many more communication rounds than in the (offline) estimation case.

In summary, in this Chapter, we study distributed estimation and learning in network environments where agents face privacy risks with respect to their own data and the beliefs expressed by their neighbors. The signals of the agents

can come from either a continuous or a discrete hypothesis space. For the continuous hypothesis spaces, we propose algorithms to calculate the MVUE and the expected value of the sufficient statistic of signals coming from an exponential family distribution, while in the discrete case, we propose two algorithms for distributed MLE for which we give guarantees to control Type I and Type II errors. Our updated rules are based on the decision-analysis literature and possess certain optimality guarantees. The agents add noise to their own signals and neighboring beliefs (depending on the nature of the protections) and exchange their beliefs with each other. To control the estimation errors, we devise upper bounds on the number of iterations and the number of times the algorithms should be applied, which can be thought of as their communication complexity. Introducing privacy-preserving computations incurs trade-offs in communication complexity and shows that the mechanism that optimizes the privacy overhead is the Laplace mechanism with appropriately chosen parameters. Finally, we test our algorithms and validate our theory in various experiments with real-world data from sensor networks and multicenter clinical trials.

Part II

Models of Contagion and New Insights into Network Modeling

CHAPTER 5

STYLIZED NETWORK MODELS FOR RESILIENCE: CORE-PERIPHERY NETWORKS

The contents of this chapter constitute joint work with Jon Kleinberg.

In the three previous Chapters, we discussed how centralized and decentralized decision-making can be important for reinforcing the resilience of sociotechnical systems. Beyond that, it is a widely known observation that the network structure plays a crucial role in the network's resilience. In particular, there are specific types of network structures that are cardinal to assessing systemic risk and stability in a system [141, 4, 29] such as the core-periphery structure. The core-periphery structure of networks considers a network that is comprised of a *core* and a *periphery*. The core of the network is a small subset of the node-set, which are *tightly connected* with one another, and the periphery "lies around" the core, and nodes within the periphery are *sparsely connected* with one another. In the context of a social network, the core of the network refers to the individuals that possess a *celebrity status* in society, such as famous politicians, actors, and athletes, and the rest of the users constitute the periphery of the network.

The resilience of core-periphery networks stems from the ability of the core to absorb and redistribute shocks due to its high density of connections. In financial networks, as studied by [141], the core can reinforce systemic risk and contagion when the failures occur in the core and the core is densely connected, but when failures happen to the periphery, systemic risk increases as core exposure increases and then decreases, at which case the core has both amplifying

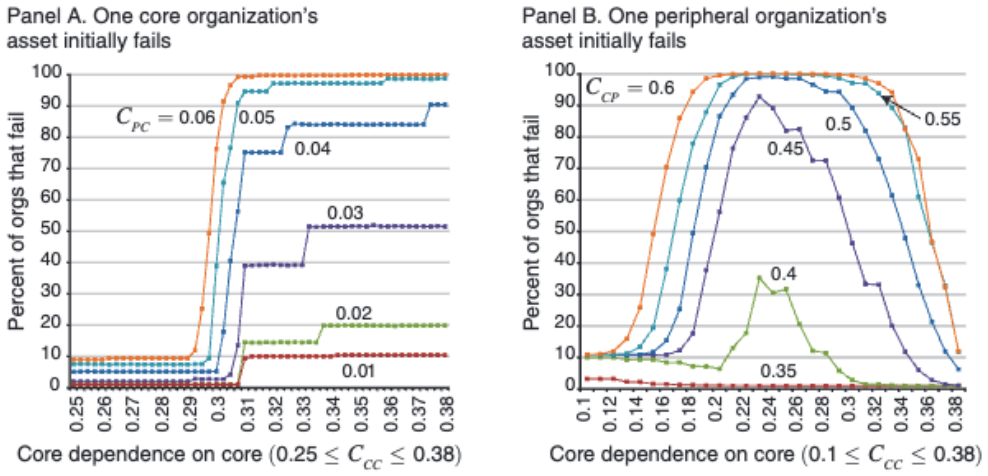


Figure 5.1: The consequences of failure in core-periphery networks for the contagion model of [141]. The figure is taken verbatim from [141]. Panel A shows that When a core organization's assets fail and the core organization's connectedness to the core is above a threshold, then that has, as a result, the whole network fails. Also, Panel B shows that when an asset of a peripheral organization fails, the percentage of organizations that fail increases as the exposure to the core increases up to a maximum point (core enables contagion), after which they decrease (core absorbs contagion).

and mitigating properties (see Figure 5.1). Similarly, [4] shows that the architecture of core-periphery networks influences the propagation of shocks, with highly centralized cores being more robust to small perturbations but vulnerable to large systemic shocks. This duality highlights the trade-off between efficiency and fragility in such networks: while the core enhances information flow, resource allocation, and coordination, it also creates potential failure points that can destabilize the entire system in most circumstances. Understanding the role of core-periphery structures in resilience is crucial for designing interventions in financial, social, and infrastructure networks to prevent large-scale breakdowns. This Chapter provides an axiomatized way to model core-periphery networks as networks that possess a sublinearly-sized dominating set and gives algorithms to infer the core-periphery structure of large-scale (potentially higher-order) networks.

Core-periphery networks have existed for a while in the literature and in multiple domains such as economics, biology, and social networks [301, 412, 435, 377, 435]. The intuition behind core-periphery networks has its roots in political economy. Wallerstein, in his seminal work *"World-systems theory"* [412] theorized that the globe can be divided into core nations, which focus on "highly-skilled labor" and "capital-intensive" production, whereas peripheral countries focused on "low-skilled labor" and "labor-intensive" production. Moreover, trade and diplomatic ties between countries seem to follow this structure, backed by Krugman's theory [251], which argues that core-periphery structures emerge due to the core regions' low centralized production costs and the supply-oriented peripheral regions. Avin et al. present an axiomatic approach towards core-periphery networks and draw strong conclusions [29]. Generative models for core-periphery networks have also been studied at [69, 435, 222, 140]. The closest model to ours is the stochastic blockmodel of [435] which assumes that *core-core* nodes are connected with probability p_{CC}, *periphery-periphery* nodes are connected with probability p_{PP} and *core-periphery* nodes are connected with probability p_{CP}, with $p_{CC} > p_{CP} > p_{PP}$, and its recent extension to directed graphs in [140].

The *dominating set* is a well-studied component of networks. More specifically, a subset of the nodes of an undirected network is a dominating set if and only if every node in the network has at least one neighbor belonging to the dominating set. The interesting question from an algorithmic perspective is finding the *minimum dominating set*, which is shown to be an *NP-Hard* problem [168]. Multiple previous works have investigated dominating sets in the context of social and biological networks [66, 288, 113, 294]. The work of [65] shows that the *geometric protean* model exhibits a sublinear dominating set, both

in theory and in practice.

However, this previous modeling work used a generative framework that was quite complex and lacked a connection with the core-periphery structure. Here, we present much simpler generative models for networks whose minimum dominating set is sub-linear in size. We *associate* the resulting minimum dominating sets with the core of the network and its neighborhood (without including nodes of itself) to the periphery of the network. The main concept behind exploiting the core-periphery structure of networks to speed up computational tasks is based on the general idea that intense computational tasks can be performed within the *sublinear core*, and then the results can be aggregated to the periphery with relatively low query complexity. So, leveraging the connection between dominating sets and the core-periphery structure from an algorithmic viewpoint can be used in many problems, such as all-pairs-shortest-paths computation, community detection, embedding generation, and many more.

The first model we present is called the *Discrete Influencer-Guided Attachment Model* (DIGAM). The DIGAM model is built onto a *hierarchical substructure*, also known as a *communities-within-communities* (fractal-like) model [263, 241], that is a tree of *fanout* b and height H. Based on the tree skeleton, nodes are associated with *prestige* (equivalently "coreness") values, and between any two nodes, the log probability of connection depends on the most prestigious node. The *novelty* of DIGAM concentrates on the existence of a *sublinear minimum dominating set*, which can be seen as defining the core of the network, with the rest of the nodes being the periphery of the network. We validate our hypothesis by efficiently fitting the DIGAM model to real-world data and show an almost perfect correlation between the construction of an almost dominating set based on the DIGAM

model and the construction of an almost dominating set via the maximum coverage greedy algorithm of [303]. DIGAM follows a *power law* distribution and exhibits *small-world* phenomena, which are evident in social networks. We compare the DIGAM model with the logistic models of [222, 401] and conclude that DIGAM is able to produce *smaller* almost dominating sets than the logistic models of [222, 401].

In the sequel, we extend the DIGAM model continuously, which we call the CIGAM model. CIGAM is a random hypergraph model for core-periphery structures. By leveraging our model's sufficient statistics, we develop a novel statistical inference algorithm that is able to scale to large hypergraphs with a runtime that is practically linear with respect to the number of nodes in the graph after a preprocessing step that is almost linear in the number of hyperedges, as well as a scalable sampling algorithm. Our inference algorithm is capable of learning embeddings that correspond to the reputation (rank) of a node within the hypergraph. We also give theoretical bounds on the size of the core of hypergraphs generated by our model. We experiment with hypergraph data that range to $\sim 10^5$ hyperedges mined from the Microsoft Academic Graph, Stack Exchange, and GitHub and show that our model outperforms baselines wrt. producing good fits.

5.1 The Discrete Influencer-Guided Attachment Model

Real-world networks usually exhibit *power laws* together with *self-similar artifacts*. Self-similar structures are similar to a part of themselves and are common properties of *fractals* [361, 263]. Self-similar structures have been long ob-

served in networks such as computer networks, patent networks, and social networks [418, 284, 262]. A model that is able to describe the communities-within-communities structure can be a tree structure. Moreover, we want a way to quantify that nodes have a higher affinity to be connected with more *prestigious* nodes that are located higher in the tree rather than other nodes below their level, which refers to a common property of core-periphery networks [435, 69, 412]. This property is given by something which we call, similarly to [263], a *difficulty function*. We want the graph to follow a power law degree distribution as well as experience small-world phenomena [241].

We are ready to describe the generative model formally: The model starts with a hierarchical structure of a perfect b-ary tree T of height H and fanout $b \geq 2$ where b is a constant. Every node v of the tree is associated with a height $0 \leq h(v) \leq H$ which is defined to be the *inverse prestige* of the corresponding node. The root has a higher prestige, and as we go down on the tree, the nodes have lower prestige up to the leaves. Two nodes u and v are linked with a probability equal to $f(u, v)$. We want $f(u, v)$ to depend on the node with the higher inverse prestige and be scale-free. For the former property, we can assume that $f(u, v)$ depends on $\min\{h(u), h(v)\}$. For f to be scale-free, we need f to be level-independent (or translation-invariant). Namely, for two nodes u, v at levels $h(u), h(v)$ and for two nodes u', v' with $h(u') = h(u) - 1$ and $h(v') = h(v) - 1$ we must have that $f(u, v)$ and $f(u', v')$ to be level-independent and, thus, a constant multiplicative factor apart. Formally, if we let $\tilde{h} = \min\{h(u), h(v)\}$ then $\min\{h(u'), h(v')\} = \tilde{h} - 1$ that means $f(\tilde{h})/f(\tilde{h} - 1) = c$, and subsequently, $f(\tilde{h}) \propto c^{-h}$ for some constant $c > 1$. This analysis yields a law of the form

$$f(u,v) = c^{-1-\min\{h(u),h(v)\}}, \tag{DIGAM}$$

where $c \in (1,b)$ is a constant. The requirement that $c \in (1,b)$ will become evident as we go through this Chapter. After the generation of the random edges according to the law $f(u,v)$, we delete the auxiliary tree edges of T. For instance, if $b = 3$ and $c = 2$ then the root is connected with every leaf with probability $1/2$, the first level is connected with every leaf with probability $1/4$, and so on. The network has $n = \Theta(b^H)$ nodes.

We say that a subset S of the vertex set of a graph is a κ almost dominating set (κ-ADS) if the set S dominates at least κn of the nodes present in the graph. In other words, at least κn of the nodes of the graph have a neighbor in S.

We say that an event $E(n)$ holds *with high probability* (w.h.p.) if $\mathbb{P}[E(n)] = 1-O(1/n)$, *with extreme probability* (w.e.p.) if $\mathbb{P}[E(n)] = 1-O(e^{-n})$, and *asymptotically almost surely* (a.a.s.) if $\mathbb{P}[E(n)] \to 1$ as $n \to \infty$.

5.1.1 Core size for the DIGAM Model

We show that the *core* of the network consists, as one should expect, of a *sub-linear* number of nodes located at the top levels of the tree. To observe this phenomenon, we calculate the probability $q_{h\tau}$ of a node at height h not being dominated by any node between levels 0 and τ where $\tau \le h$, which equals

$$q_{h\tau} = \prod_{r=0}^{\tau} \left(1 - c^{-r-1}\right)^{b^r} \le e^{-\frac{1}{c}\sum_{r=0}^{\tau}(b/c)^r} \lesssim e^{-\frac{1}{c}\left(\frac{b}{c}\right)^{\tau+1}} = e^{-\Theta\left(\left(\frac{b}{c}\right)^{\tau}\right)},$$

where $a \lesssim b$ denotes that there exists a constant $C > 0$ independent of b such that $a \leq C \cdot b$ (i.e. inequality up to a constant factor), and the first inequality holds since $1 - t \leq e^{-t}$ for all $t \in \mathbb{R}$. Note that $q_{h\tau}$ does not depend on the height of the node in question, as long as $\tau \leq h$. Now the probability that there is at least one node uncovered below level $\tau + 1$ is given by the Union bound and is at most

$$\sum_{h=\tau+1}^{H} b^h q_{h\tau} = q_{h\tau} \sum_{h=\tau+1}^{H} b^h \lesssim q_{h\tau} b^H \lesssim e^{H \log b - \Theta((\frac{b}{c})^\tau)}.$$

To assert an w.h.p. guarantee we force the above probability to be $\Theta(b^{-H})$, therefore, solving for τ we arrive at a dominating set of size

$$n_0 = b^{O(\log(2cH \log b)/\log(b/c))} = b^{o(H)} = o(n)$$

with probability at least $1 - \Theta(b^{-H})$. Consequently, a *sublinear* fraction of nodes $C = \{v : h(v) \leq \tau\}$ located on a *logarithmic height* τ from the root of the skeleton tree T dominate the whole periphery $P = \{v : h(v) \geq \tau + 1\}$ with $\tau = \Omega(\log H)$.

5.1.2 Degree Distribution for the DIGAM Model

To fit the model to real-world data, we infer the degree distribution of DIGAM. The average degree of a node u at level h is

$$\begin{aligned}\bar{d}_h &\approx \sum_{r=0}^{H} b^r c^{-\min\{h,r\}-1} \\ &= \frac{1}{c}\left[\left(\frac{b}{c}\right)^{h+1} - 1 + \frac{b^{H+1} - b^{h+1}}{c^h}\right] = \Theta\left(\frac{b^{H+1}}{c^{h+1}}\right).\end{aligned}$$

and the total expected number of edges at level h is $\bar{m}_h = b^h \bar{d}_h = \Theta(b^{h+H+1}/c^{h+1})$. The asymptotics of the previous Equation yield a power law with exponent

$$\frac{\mathrm{d}\log \bar{d}_h}{\mathrm{d}h} = \log\left(\frac{1}{c}\right).$$

If the rank of u, with $h(u) = h$ is given as $r_h = c^h$, which is an increasing function of h, then the expected degree depends on the inverse rank $1/r_h$, yielding a *Zipfian* power law. The trials for connecting every node are independent Bernoulli variables, and therefore by the multiplicative Chernoff bound with probability at least $1 - \Theta(b^{-H})$ we have that the average degree at height h, $\widehat{d}_h$ is $\Theta(1/r_h) \pm O(\sqrt{H \log b/(2b^h)})$.

By a union bound, we have that

$$\mathbb{P}\left[\exists h \in \{0,\ldots,H\} : \left|\widehat{d}_h - \Theta\left(\frac{1}{r_h}\right)\right| = \Omega\left(\sqrt{\frac{H\log b}{2b^h}}\right)\right] \leq \sum_{h=0}^{H} \mathbb{P}\left[\left|\widehat{d}_h - \Theta\left(\frac{1}{r_h}\right)\right| = \Omega\left(\sqrt{\frac{H\log b}{2b^h}}\right)\right].$$

The above quantity is $O(H/b^H)$. Thus, with probability $1 - O(Hb^{-H})$ (i.e. w.h.p.) the degree histogram follows Zipf's Law.

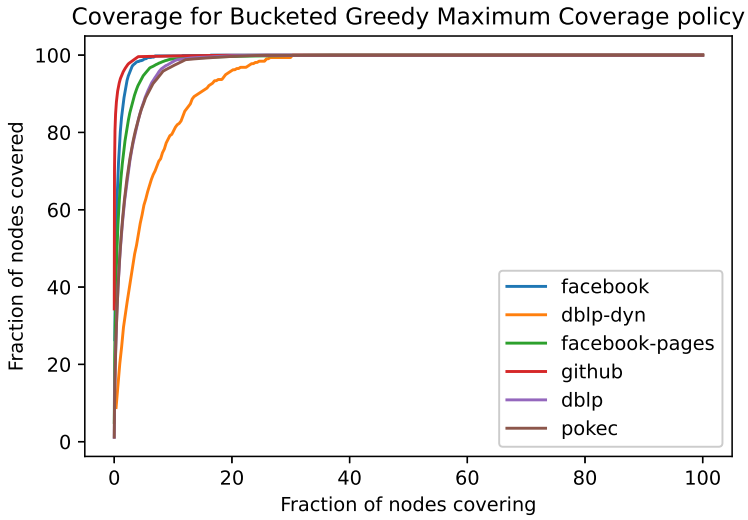


Figure 5.2: Results of fitting an IGAM model to the world-trade, cs-faculty, history-faculty, business-faculty, and airports datasets examined in [140, 119, 107, 111, 10]. The Figure displays the predicted values of b and c for the IGAM model, and the total degree at each level h of the skeleton tree of fanout b. A linear fit is presented for each dataset to showcase the power law behavior. Moreover, values of the log-likelihood and Pearson's Correlation Coefficient R^2 are reported. Nodes with degree ≤ 4 have been filtered out as outliers except for the london-underground network.

The exponent of the degree distribution can be altered, if the same model is generated with parameters $b' = b^\alpha, c' = c^\alpha$ for some $\alpha \geq 0$. The expected number of edges $\bar{m}$ is given as

$$\bar{m} = \frac{1}{2}\sum_{h=0}^{H} b^h \bar{d}_h = \Theta\left(\frac{b^{2H}}{c^H}\right),$$

and is *superlinear* with respect to the number of nodes.

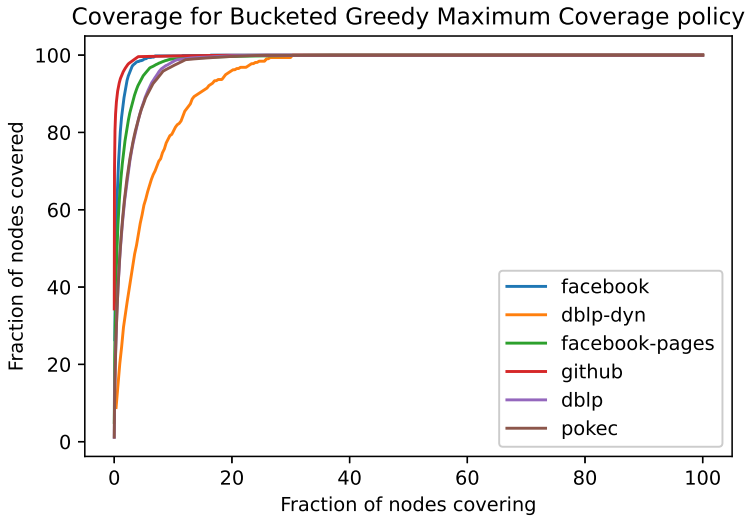


Figure 5.3: Log-log plot between the percentages of dominated nodes when running the greedy $(1 - 1/e)$-maximum coverage algorithm of [303] (x-axis) and selecting nodes according to their hierarchy, i.e., in order of descending initial degree (y-axis). The slope γ and R^2 of linear fits are reported. The rule that selects nodes based on their prestige h yields very close results to the greedy maximum coverage algorithm. In general instances, these two algorithms are expected to have different results since the former algorithm may select prestigious nodes whose neighborhoods have large overlaps, which may not yield good coverage in general. However, specifically in core-periphery networks, high-prestige nodes seem to have small overlaps, which justifies the good performance of the prestige-based algorithm.

5.1.3 Fitting the DIGAM Model to Real-World Data

We describe a fitting algorithm for the DIGAM model (Algorithm 13). The fitting process considers of being given a sample of m edges $\mathcal{D} = \{e_i\}_{1 \le i \le m}$ on a network of n nodes where n is known. Our goal is to find the optimal fanout $b^\star$, the optimal height function $h^\star$ and the optimal scale factor $c^\star$ that maximizes the log-likelihood of the model, that is

$$\max_{b,\, h,\, c} \ell(b, h, c|\mathcal{D}) = \max_{b,\, h,\, c} \log \mathbb{P}[\mathcal{D}|b, h, c].$$

where the likelihood equals

$$\begin{aligned}\ell(b,h,c|\mathcal{D}) &= \sum_{(u,v)\in E} \log f(u,v) + \sum_{(u,v)\notin E} \log(1-f(u,v)) \\ &= \sum_{(u,v)\in E} \log\left(\frac{f(u,v)}{1-f(u,v)}\right) + \sum_{u,v\in V\times V} \log(1-f(u,v)).\end{aligned}$$

Directly optimizing the likelihood is very hard since there are $O(n)$ possible fanouts, each fanout can generate an exponential number of possible trees, and thus height functions, and given the fanout and the height function the remaining problem consists of finding the optimal c that explains $\ell(c|\mathcal{D}, b, h)$.

To optimize the log-likelihood of DIGAM efficiently, we first calculate the sample degrees of each node, that is $\bar{y}_u = \sum_{i=1}^{m} \mathbf{1}\{u \in e_i\}$, and then order the nodes on decreasing order of their sample degrees. After that, we fix a fanout b from the interval $\{2, \ldots, n-1\}$, and according to that fanout we start by attributing heights of a hypothetical b-ary tree on the nodes according to their descending order. For example, for $b = 2$ the first node gets a height of 0, the next two a height of 1, and so on. Then, for each height $0 \le h \le \lceil \log n / \log b \rceil$, we form the log-degrees $\bar{z}_h = \log\left(\sum_{u:h(u)=h} \bar{y}_u\right)$, and fit linear-least-squares with x-values being the range of heights and y-values being the log-degrees $\bar{z}_h$. The optimal slope a yields c to be $c = b \cdot e^{-a}$. If $c \ge b$ then the current fit is rejected. We can then calculate the likelihood function ℓ and keep the best parameters $(b^\star, h^\star, c^\star)$.

Each step is dominated by the calculation of the likelihood that costs $O(n^2)$ time, since *exactly* computing the log-likelihood requires summing over all pairs of nodes (regardless of whether an edge exists or not), and thus the total complexity is $O(n^3)$. Note that since the values of $f(u,v)$ are small (i.e. close to

0) and real-world networks are sparse (i.e. m is of the order of n or $n \log n$) the log-likelihood can be *approximated* in time $O(m)$ by ignoring the network-independent term, i.e. the term that sums on $V \times V$, which yields an algorithm with runtime $O(nm)$ instead of $O(n^3)$. If a full b-ary tree does not cover the network, we allow the last level to be incomplete.

We fit the DIGAM model to networks examined in [140]. More specifically, we examine the world-trade network from [119] ($n = 76$, $m = 845$), the faculty datasets from [107] (cs-faculty: $n = 205$, $m = 2,861$; history-faculty: $n = 145$, $m = 2,334$; business-faculty: $n = 113$, $m = 3,027$), the polblogs dataset from [10] ($n = 852$, $m = 15,956$), the airports dataset from [111] ($n = 210$, $m = 2,429$), the c-elegans dataset from [224] ($n = 279$, $m = 1.9$K), the open-airlines dataset from [222] ($n = 7.2$K, $m = 18.6$K), and the london-underground dataset from [222] ($n = 315$, $m = 270$); treating the networks as undirected. Figure 5.2 presents the (total) degree distribution fits for the DIGAM model, where the parameters b, c and the height function have been determined. Observe that the total degree at each constructed level is linearly correlated ($R^2 \geq 0.93$ except for the airport's dataset) with the coreness value of each group of nodes (per level). Moreover, in Figure 5.3 we do a log-log plot between the construction of the dominating set as in Section 5.1.1 and the construction of the dominating set using the maximum coverage greedy algorithm. The former algorithm treats the nodes as DIGAM would do in the construction of the dominating set, i.e. by traversing the levels of the hierarchy from top to bottom. The latter algorithm picks the node with the largest *active degree* at each step, adds it to the set, and removes itself and all the nodes connected to it from the network up to a certain number of steps or if there are no more nodes left.

Markers on the plot represent subsequent iterations of both algorithms. We observe an almost perfect correlation between the two algorithms and slightly superlinear relations of the form $y \propto x^{\gamma}$ for $\gamma \in [1, 1.21]$, which is a phenomenon that we should not expect in more general networks since choosing the nodes with the highest degrees shall not yield good coverage in general. Moreover, note that a sublinear number of iterations, denoted by the number of x markers outside the $[1.9, 2.0]^2$ box (the mapping is increasing), suffices to dominate $10^{1.9}\% \approx 80\%$ of the nodes. A visualization of the DIGAM fitting process can be found in Figure 5.5 for the small datasets, whereas the various levels h of the DIGAM model are color-coded.

5.1.4 Qualitative Insights from Fitting DIGAM

In this Section, we highlight the following structures that emerge from fitting the DIGAM model to real-world data. We examine the first three levels of the hierarchy, devised by the height function h, for the datasets that contain labeled nodes. The analytical form of the core nodes can be found in the Methods Section.

1. *Faculty Networks.* In the faculty networks of each one of the three disciplines (computer science, history, and business) the core consisted of nodes referring to highly ranked universities in the United States (in each discipline), as well as an (aggregate) node referring to faculty coming from all non-US academic institutions. To elaborate, the cs-faculty network contains MIT, CMU, Stanford, UT Austin, Purdue, and UIUC in its core, together with the aggregate node. The history-faculty core consists, for in-

stance, of Harvard, Yale, University of Chicago, Columbia, Stanford, Johns Hopkins, and Cornell. Finally, the business-faculty network has, for instance, the University of Michigan, UT Austin, Penn State, and the University of Pennsylvania at its core. These findings are consistent with the body of research on faculty hiring networks[107, 258] where it is stated that, for the computer science discipline, a very small percentage (9%) of departments is responsible for 50% of academic hires in faculty position.

2. *Open-airlines.* The open-airlines network has a core that consists of very large and central international airports such as AMS, FRA, CDG, IST, MUC, ATL, and PEK.
3. *World-trade.* The world-trade dataset contains data about the trade of metals among 80 countries in 1994. The nodes represent countries that have available entries in the Commodity Trade Statistics released by the United Nations. In this network, the core consists of, for instance, Finland, Hungary, Slovenia, Singapore, Chile, and so on.
4. *London-underground.* In the london-underground dataset, we recover a core that consists of busy train stations such as Bank, Baker Street, Canning Town, and so on, all of which are cardinal to the British underground system.

5.1.5 Relation to Logistic Core-periphery Models

We compare the DIGAM model with two logistic models introduced by Jia and Benson[222] and Tudisco and Higham[401]. In detail, we fit both models and give empirical answers to the following question: *Are the logistic core-periphery models able to explain the domination structure of core-periphery networks?*

The model of Jia and Benson assigns a *coreness score* $\theta_v \in \mathbb{R}$ for every node v in the vertex set V. The simple version of the model produces edges (u, v) randomly and independently with probability

$$\rho(u, v) = \frac{1}{1 + e^{-\theta_u - \theta_v}}. \tag{Logistic-CP}$$

Intuitively what this model describes is that a node with $\theta_v \geq 0$ is considered to be a core node and a node with $\theta_v < 0$ to be a peripheral node. That is, for a pair (u, v) if both nodes are peripheral, i.e. have $\theta_u < 0$ and $\theta_v < 0$, then the link probability $\rho(u, v)$ is less than the case when one of θ_u, θ_v is non-negative that represents a core-periphery link. Similarly, when both $\theta_u \geq 0$ and $\theta_v \geq 0$, which corresponds to a core-core node, then the edge creation law attributes a larger connection probability. When spatial features $x : V \to \mathbb{R}^d$ are provided, as well as a kernel function $K(u, v)$ (for example, $K(u, v) = \|x_u - x_v\|_2$), and a hyperparameter ε, then Equation (Logistic-JB) is generalized to an edge law

$$\mu(u, v) = \frac{e^{\theta_u + \theta_v}}{K^{\varepsilon}(u, v) + e^{\theta_u + \theta_v}}. \tag{Logistic-JB}$$

The model of Tudisco and Higham[401] is based on a logistic probability law determined by a ranking π of the nodes. The more prestigious a node v is the higher the value π_v is. The edge creation law is given by

$$\varphi(u, v) = \sigma_{s,t}\left(\frac{\max\{\pi_u, \pi_v\}}{n}\right), \tag{Logistic-TH}$$

where $\sigma_{s,t} = 1/(1 + e^{-s(x-t)})$ is the smooth approximation of the Heaviside step function $H_t(x)$ that is 1 if $x \geq t$ and 0 otherwise. We use $s = 10$, and $t =$

1/2. Again, the model intuitively says that nodes tend to be associated with more prestigious nodes rather than less prestigious nodes. Finally, the authors propose an iterative method to infer the ranking π which has an $O(m)$ per-step cost.

We evaluate how well Logistic-CP, Logistic-JB, and Logistic-TH capture the domination properties of the core-periphery structure compared to DIGAM. For the logistic models of Jia and Benson, we fit the Logistic-CP model when there are no spatial data available and the Logistic-JB when spatial data are available (i.e., in the c-elegans, open-airlines, and London-underground datasets). We use the optimal parameters θ_v^* of the logistic models to build a ranking for the nodes by sorting them in decreasing order of the scores θ_v^*. For the Logistic-TH model, we use the iterative method provided in their paper to infer the ranking by sorting the entries of the fixed point that their algorithm produces. Then, for all models, we report the domination curves in Figures 5.3, 5.7 and 5.8. To give better visual insights on how the models perform, we visualize the outcome of fitting the models for the c-elegans dataset on Figure 5.4 for a core set of size $\lfloor n^{0.7} \rfloor$. For each dataset and figure we report the exponent $p \in [0, 1]$ of a set that dominates 80% of the network (i.e. and 0.8-ADS). Namely, if a fraction $\varpi \in [0, 1]$ suffices to cover at least 80% of the network, then $p = \log(\varpi \cdot n)/\log n$.

The DIGAM model can better explain the sublinear domination phenomenon in core-periphery networks than Logistic-JB, Logistic-CP, and Logistic-TH. Also Logistic-CP and Logistic-JB achieve better coverage compared to Logistic-TH. Perhaps the most characteristic are the faculty (cs-faculty, history-faculty, business-faculty) and the world-trade datasets where DIGAM produces an almost dominating set with an exponent $p \leq 0.16$ whereas Logistic-

TH finds a similar set with $p \geq 0.54$, and Logistic-CP finds an 0.8-ADS with $p = 0.15$ in the case of business-faculty and with $p \geq 0.32$ in the rest of the datasets. In the polblogs dataset, DIGAM is able to find an 0.8-ADS with $p = 0.27$ whereas Logistic-CP finds one with $p = 0.64$ and Logistic-TH finds a much larger one with $p = 0.81$. In the open-airlines dataset the 0.8-ADS corresponds to $p = 0.61$ for DIGAM and to $p \geq 0.82$ for the logistic methods. Finally, the smallest variation between the methods exhibits the london-underground dataset where p ranges from $p = 0.75$ (DIGAM) to $p = 0.85$ (Logistic-TH). In conclusion, the ADS constructed by DIGAM are consistently smaller than the ones produced by Logistic-CP and Logistic-JB which are smaller than the ones produced with Logistic-TH, which suggests that DIGAM is able to *explain* the sublinear domination phenomenon where other logistic models *fail* to do so.

5.1.6 Miscellaneous Properties

Small-world Behaviour. To determine the diameter (the diameter of a disconnected network is taken to be the diameter of its giant connected component) of the network, we build an Erdös-Renyi (ER) network W with n nodes and edge probability $f^* = \min_{u,v} f(u,v) = c^{-H-1}$. It follows from a standard coupling argument, i.e., a "toss-by-toss" comparison that we can relate the two networks as one being a subgraph of the other, in our case, the ER network W being a subgraph of the DIGAM network, say G. The coupling is constructed as follows: $\mathbb{P}\left[(u,v) \in E(G) \mid (u,v) \in E(W)\right] = 1$, $\mathbb{P}\left[(u,v) \in E(G) \mid (u,v) \notin E(W)\right] = \frac{f(u,v)-f^*}{1-f^*}$, so that $\mathbb{P}\left[(u,v) \in E(G)\right] = f(u,v)$, and $\mathbb{P}[(u,v) \in E(W)] = f^*$. Then it follows that the diameter of the DIGAM network is at most the diameter of W. Using a result from [63, 105], we have that since the average degree of W is $\Theta((b/c)^H) \to \infty$ as

$H \to \infty$, the diameter of W is close to $\log n / \log(nf^*) = \Theta(\log b / \log(b/c)) = O(1)$ a.a.s. From that we can deduce that G has a diameter close to $O(\log b / \log(b/c)) = O(1)$ a.a.s. This result can follow from intuition also, since all the nodes at a logarithmic height of the root dominate the periphery, and a worst-case path should roughly be between two peripheral nodes which are connected via a node at the core, with this node being a common dominator of them.

Global Clustering Coefficient (GCC). The probability of uvw being a triangle given that $h(u) \leq h(v) \leq h(w)$ is $\beta_{uvw} = f(u,v)f(u,w)f(v,w) = c^{-3-2h(u)-h(v)}$, thus the expected total number of closed triangles T_C is

$$\mathbb{E}[T_C] = \sum_{(u,v,w):h(u)<h(v)<h(w)} b^{h(u)+h(v)+h(w)}\beta_{uvw} = \Theta\left(\frac{b^{3H}}{c^{3H+3}}\right).$$

The calculation has been deferred to the Methods Section (Equation (D.1)). The probability γ_{uvw} of uvw being a triplet (open or closed) is given as $\gamma_{uvw} = f(u,v)f(u,w) + f(u,v)f(v,w) + f(u,w)f(v,w)$. Conditioned on the event that $h(u) \leq h(v) \leq h(w)$ we can deduce that $3c^{-2-2h(v)} \leq \gamma_{uvw} \leq 3c^{-2-2h(u)}$. Similarly to T_C, the expected number of open triplets T_R is $\Theta\left(\frac{b^{3H}}{c^{2H+2}}\right)$ (see Equation (D.2) in the Methods Section). By McDiarmid's Inequality [130], since T_C and T_R are $\Theta(b^H)$-Lipschitz we have that $\mathbb{P}\left[|T_C - \mathbb{E}[T_C]| = \Omega(b^H)\right] = O\left(e^{-b^H}\right)$, and $\mathbb{P}\left[|T_R - \mathbb{E}[T_R]| = \Omega(b^H)\right] = O\left(e^{-b^H}\right)$ and therefore we can deduce that the GCC T_C/T_R is $O(c^{-H} + b^{-H}) = O(c^{-H})$ with probability $1 - O\left(e^{-b^H}\right)$ by combining the two concentration bounds. Therefore, w.e.p. clustering coefficient is $O(c^{-H})$.

Core-periphery Conductance. The expected conductance of a set $\emptyset \subset S \subset [n]$ is given as $\bar{\phi}(S) = \mathbb{E}\left[e(S,\bar{S})\right] / \min\{|S|, |\bar{S}|\}$, where $\bar{S} = [n] \setminus S$. Letting S_τ to be the

nodes at the first $\tau < H$ levels where $|S_\tau| \leq |\bar{S}_\tau|$ yields $\min\{|S_\tau|, |\bar{S}_\tau|\} = b^{\tau+1} - 1$, and

$$\mathbb{E}\left[e(S_\tau, \bar{S}_\tau)\right] = \sum_{s=\tau+1}^{H} \sum_{r=0}^{\tau} b^r b^s c^{-1-\min\{r,s\}} = \frac{1}{c} \sum_{s=\tau+1}^{H} b^s \sum_{r=0}^{\tau} \left(\frac{b}{c}\right)^r = \frac{1}{c} \sum_{s=\tau+1}^{H} b^s \Theta\left(\left(\frac{b}{c}\right)^\tau\right) = \Theta\left(|\bar{S}_\tau|\left(\frac{b}{c}\right)^\tau\right).$$

$\bar{\phi}(S_\tau) = \Theta(b^H/c^\tau)$. Letting $\tau = \log(2cH \log b)/\log(b/c)$ be the core's height we deduce that $\bar{\phi}(C) = \Theta(b^H/H)$.

5.2 Multilayer Extension of IGAM

We fully align with the stochastic blockmodel definition of core-periphery networks presented in [435] by defining the following generalization of IGAM, which we call IGAM2, parametrized by $b > c_2 > c_1 > 1$. In this context, we start with the same skeleton tree of fanout b and then the law $g(u, v)$ for generating the edges is

$$g(u,v) = \begin{cases} c_2^{-1-\min\{h(u),h(v)\}} & \max\{h(u), h(v)\} > H_0 \\ c_1^{-1-\min\{h(u),h(v)\}} & \max\{h(u), h(v)\} \leq H_0 \end{cases}, \qquad \text{(IGAM2)}$$

where $0 < H_0 < H$ is the core's threshold. The probability $g(u, v)$ of an edge between two nodes with $\max\{h(u), h(v)\} \leq H_0$ (i.e. core-core edges) is greater than the probability between two nodes whose heights satisfy $\min\{h(u), h(v)\} \leq H_0$ and $\max\{h(u), h(v)\} > H_0$ (core-periphery edges), which is greater than the probability of the case that $\min\{h(u), h(v)\} > H_0$ (periphery-periphery edges).

We analyze the mathematical properties of IGAM2, which are similar to the properties of IGAM, in the Methods Section. Most of our proofs are based on

a construction of a coupling of an IGAM2 network with two (simple) IGAM networks with parameters (b, c_1, H) and (b, c_2, H). The coupling is constructed such that the three graphs form an ordering based on the subgraph relation.

5.3 The Continuous Influencer-Guided Attachment Model (CIGAM)

In the previous section, the IGAM and IGAM2 models assumed that the height $h(v)$ of a node is a discrete variable. In this section, we relax the assumption of $h(v)$ being discrete, to having the "prestige of a node" being a continuous variable. Moreover, we extend the IGAM to accommodate higher order structures (hypergraphs) and show that sampling and inference can be efficiently achieved.

As we noted, such models have been extensively and successfully used to model *graphs*, yet the generation of *hypergraphs* from such hierarchical models is a completely new task. Although hypergraphs are the obvious generalization of graphs, tasks regarding random hypergraph models pose new challenges, primarily from a computational standpoint, which correspond to the tractability of computing the respective log-likelihood function (see Section 5.3.1). Furthermore, the *hybrid* nature of the existing models (i.e. involving both discrete and continuous structures) poses challenges wrt. the corresponding optimization problems of fitting the data. Here existing models such IGAM use *heuristic* methods to recover the model parameters given data, which in general do *not* correspond to the maximum likelihood estimates.

The continuous model (CIGAM) starts with a hypergraph $G(V = [n], E)$ on n nodes where each node $i \in [n]$ is associated with a (probably learnable) *prestige* value $r_i \in [0, 1]$ which we call the *rank of node i* and is generated (i.i.d.) from a *truncated exponential distribution*[1], i.e.

$$p(r_i) \propto \lambda e^{-\lambda r_i} \mathbf{1}\{r_i \in [0, 1]\} \text{ for } \lambda > 0. \tag{5.1}$$

We define $b = e^{\lambda} > 1$. For simplicity of exposition, we start with presenting the *single-layer* CIGAM model. The model generates hyperedges of any order $2 \leq k \leq n$. Conceptually, we want the hyperedge creation probabilities to exhibit attachment towards more prestigious nodes; in agreement with existing generative core-periphery models [222, 401, 380]. Subsequently, we want the edge creation law $f(e)$ to depend on r_i for $i \in e$ and be scale-free, such as IGAM.

For the former property, we assume that $f(e)$ depends on $r_e = (r_i)_{i \in e}$, and specifically on $\|r_e\|_\infty = \max_{i \in e} r_i$. For the latter property, we want that for two edges e, e' with $r_{e'} = r_e + \delta$ and for any appropriately chosen δ to obey $\frac{f(e')}{f(e)} = c^{\delta}$. This functional equation has a solution of the form $f(e) \propto c^{\|r(e)\|_\infty}$, and, thus, we generate each hyperedge e independently with probability

$$f(e) = c^{-\zeta + \|r_e\|_\infty} \tag{SL-CIGAM}$$

for $c, \zeta > 1$. We define $|e|$ to be the size of $e \in E$, $k_{\min} = \min_{e \in E} |e|$, and $k_{\max} = \max_{e \in E} |e|$ (also known as the *hypergraph rank*).

From Equation (5.1), we observe that CIGAM overcomes the design chal-

[1]It has been shown that many creative rank-based measures follow power-laws [109]. The log-transforms of such quantities are exponentially-tailed.

lenge of a hybrid model since learning the parameters of CIGAM corresponds to solving a continuous optimization problem (see also Section 5.3.3), and that the hyperedge creation probabilities of Equation (SL-CIGAM) are determined by the node with the highest prestige. Thus, the highest-prestige nodes serve as *sufficient statistics* to *simplify* the log-likelihood of the model.

The previous definition can be extended to a multi-layer model parametrized by $\lambda > 0$, and $1 < c_2 \leq c_3 \leq \cdots \leq c_L$, $H_0 = 0 \leq H_1 \leq H_2 \cdots \leq H_L = 1$ as follows: We define a function $\phi : E \to [L]$ such that $\phi(e) = \inf\{i \in [L] : 1 - \|r_e\|_{-\infty} \geq H_i\}$, where $\|r_e\|_{-\infty} = \min_{u \in e} r_u$, and draw each edge e independently with probability

$$f(e) = c_{\phi(e)}^{-\zeta + \|r_e\|_\infty}. \tag{ML-CIGAM}$$

The value of $\zeta = 2$ works well empirically, so we set $\zeta = 2$ from now on. We will refer to $c = (c_i)_{i \in [L]}$ as the *density parameters* (or *core profile*) and to $H = (H_i)_{i \in [L]}$ as the *breakpoints*. The models agree with the stochastic block model of [435], namely for nodes that are closer to the core, their probability of jointly participating as a hyperedge is higher than a subset of nodes that are further from it. The density parameters c give us a way to tweak the density between different levels of the graph, thus giving us the flexibility to encode more complex structures with a constant overhead in terms of complexity when the number of layers is constant (in our experiments $L \in \{1, 2\}$). Figure 5.9 shows instances generated from CIGAM.

5.3.1 Fast Algorithms for Sampling and Inference

Note that the naïve exact computation of the log-likelihood (LL), i.e. without taking into account the sufficient statistics of each hyperedge, requires flipping $\sum_{k=k_{\min}}^{k_{\max}} \binom{n}{k}$ coins in total which is highly prohibitive even for hypergraphs with very small $k_{\max}$ even if n is moderate ($n > 100$)[2]. In the same way, sampling hypergraphs from CIGAM also needs flipping $\sum_{k=k_{\min}}^{k_{\max}} \binom{n}{k}$ coins which make sample generation inefficient as well. We also note that in the simple case of graphs with spatial features, the work of [222], the authors approximate the likelihood and sampling of their model, where, in our case, we take advantage of the *sufficient statistics* of each hyperedge to do *exact inference in linear time*. Our approach follows the methodology used to sample Kronecker hypergraphs [138]. However, the partitioning of the graph is *significantly* different in both cases and requires careful calculation.

More specifically, we observe that a graph generated by the CIGAM model can be broken down into multiple Erdös-Rényi graphs, whose block sizes and parameters we devise in Section 5.3.2, and such partitions have efficient representations in terms of the LL as well as can be sampled by standard methods for sampling Erdös-Rényi graphs [350].

5.3.2 Hyperedge Set Partitioning

From the definition of the model, we deduce that the hyperedge set can be efficiently partitioned, both for sampling and inference, namely each edge in the

[2]In our experiments k typically ranges between 2 and 25. Moreover, in the worst case, when $k \in [2, n]$ naïvely computing the likelihood costs $O(2^n)$.

multi-layer model is determined by $\max_{u\in e} r_u$ and $\min_{u\in e} r_u$. The edge set E of a hypergraph that contains simplices of order $k \in [k_{\min}, k_{\max}]$ is partitioned as

$$E = \bigsqcup_{k\in[k_{\min},k_{\max}],\ i\in[n],\ l\in[L]} E(k,i,l),$$

where $E(k,i,l) = \{e \in E : |e| = k, i = \text{argmax}_{u\in e} r_u, \phi(e) = l\}$. To sample the multi-layer model, we first assign a layer to each node i, assuming again that $r_1 \succ r_2 \succ \cdots \succ r_n$, that is the layer that the current node belongs if its the node with the smallest rank in a given hyperedge. We call this matrix, which has increasing entries, `layers[n]`. We then form $N(i,l) = \{i < j \leq n | \texttt{layers[}j\texttt{]} = l\}$. Now, a hyperedge e needs two components: the *largest* rank, which determines the exponent of $f(e)$ and the *smallest* rank in e that determines the layer that the hyperedge is in. We start by iterating on the ranks array and while fixing i as the dominant node: we first select j from $N(i,l)$ and then, we sample $k-2$ nodes from $[i+1, j-1]$, for $j-i-1 \geq k-2$ for every $k \in [k_{\min}, k_{\max}]$. Therefore, a total of $\sum_{j\in N(i,l)} \binom{j-i-1}{k-2}$ k-simplices can belong to the partition where i is the dominant rank node. We construct a $(k_{\max} - k_{\min} - 1) \times n \times L$ matrix which contains $|E(k,i,l)|$ for all $k \in [k_{\min}, k_{\max}]$, $i \in [n]$ and $l \in [L]$. We iterate over all $e \in E$ and increment the $(|e|, \text{argmax}_{u\in e}\{r_u\}, \texttt{layers[}\text{argmin}_{u\in e}\{r_u\}\texttt{]})$-th entry of the matrix. The complement sets have sizes

$$|\bar{E}(k,i,l)| = \sum_{j\in N(i,l)} \binom{j-i-1}{k-2} - |E(k,i,l)| \quad \forall k,i,l.$$

To simplify the summation, note that by the binomial identity $\binom{j-i-1}{k-2} = \binom{j-i}{k-1} - \binom{j-i-1}{k-1}$, we calculate the sum $\sum_{j\in N(i,l)} \binom{j-i-1}{k-2}$ as

$$\sum_{j \in N(i,l)} \binom{j-i-1}{k-2} = \binom{j_{\max}(i,l)-i}{k-1} - \binom{j_{\min}(i,l)-i-1}{k-1}, \tag{5.2}$$

with $j_{\max}(i,l) = \max_{j \in N(i,l)} j$, and $j_{\min}(i,l) = \min_{j \in N(i,l)} j$ and using the fact that $N(i,l)$ is a contiguous array. We can further validate that for the simple case that $k_{\min} = k_{\max} = k$, $L = 1$ we have that $j_{\min}(i,1) = i+1$ and $j_{\max}(i,1) = n$ yielding $|\bar{E}(i,1)| = \binom{n-i}{k-1} - |E(i,1)|$ as expected. As a generative model, each block requires throwing $E|(k,i,l)|$ balls where $|E(k,i,l)|$ follows a binomial r.v. with $\binom{j_{\max}(i,l)-i}{k-1} - \binom{j_{\min}(i,l)-i-1}{k-1}$ trials of bias $c_l^{-2+r_i}$ for a hyperedge of order k. We further simplify the number of trials by noting that $j_{\max}(i,l) = j_{\min}(i,l) + |N(i,l)| - 1$ since $N(i,l)$ is a contiguous array. We need $O(k_{\max}(m+n) + n \log n)$ to build the $|E(k,i,l)|$ and time $O(n(k_{\max} + L))$ to build $|\bar{E}(k,i,l)|$ giving a total preprocessing time of $T_{PRE} = O(n(k_{\max} + L) + k_{\max} m + n \log n)$. Usually (see Section 5.4.1), $k_{\max}$ and L are constant which brings T_{PRE} to $O(n \log n + m)$.

5.3.3 Exact Inference for CIGAM

Based on the hyperedge set partitioning of Section 5.3.2 we can compute the LL function $\log p(G, r|\lambda, c)$ as follows, assuming the elements of r are *sorted in decreasing order*:

$$\begin{aligned} \log p(G, r|\lambda, c) = &- \lambda \sum_{i \in [n]} r_i + n \log \lambda - n \log(1 - e^{-\lambda}) \\ &+ \sum_{i,l} \left[\left(\sum_k |E(k,i,l)| \right) \log \left(c_l^{-2+r_i} \right) \right. \\ &\left. + \left(\sum_k |\bar{E}(k,i,l)| \right) \log \left(1 - c_l^{-2+r_i} \right) \right]. \end{aligned} \tag{5.3}$$

Then, the likelihood can be computed in $T_{LL} = O(nL)$ time by precomputing $\sum_k |E(k,i,l)|$ and $\sum_k |\bar{E}(k,i,l)|$. The total memory required is $O(nL)$ to store $\sum_k |E(k,i,l)|$ (resp. $\sum_k |\bar{E}(k,i,l)|$), $O(m)$ to store the edges, and $O(nk_{\max})$ to store the binomial coefficients. Therefore, the total memory cost is $O(n(k_{\max}+L)+m)$. Since the number of layers L is constant compared to n, the time needed to compute the likelihood is $O(n)$.

The breakpoints H_i are *hyperparameters* of the model. We impose constraints on the density of the edges, i.e., we want the graph to "sparsify" towards the periphery, which can be encoded with the following domain $\mathcal{K} = \{(\lambda, c) : 1 < c_1 < c_2 \cdots < c_L\}$. We encode the domain $\mathcal{K}$ on the LL by considering the log-barrier function $\varphi(\lambda, c) = \log(c_1 - 1) + \sum_{i=1}^{L-1} \log(c_{i+1} - c_i)$ which equals $-\infty$ for every $(\lambda, c) \notin \mathcal{K}$. Thus, we solve the following inference problem to get the optimal parameters of the model

$$\max_{(\lambda,c)\in\mathcal{K}} \log p(G, r|\lambda, c) \Leftrightarrow \max_{(\lambda,c)\in\mathbb{R}^{L+1}} \log p(G, r|\lambda, c) + \varphi(\lambda, c).$$

5.3.4 Learning the Endogenous Ranks

When the rank vector r is not provided we learn the endogenous (or *latent*) ranks given a feature matrix $X \in \mathbb{R}^{n\times d}$ by using a learnable model $h(\cdot|\theta)$ to get $r_i = h(x_i|\theta)$, which we replace on the LL as follows:

$$\log p(G, X|\lambda, c, \theta) = -\lambda \sum_{i\in[n]} h(x_i|\theta) + n\log\lambda - n\log(1-e^{-\lambda}) + \sum_{i,l}\Bigg[\Bigg(\sum_{k}|E(k,i,l)|\Bigg)\log\left(c_l^{-2+h(x_i|\theta)}\right) + \Bigg(\sum_{k}|\bar{E}(k,i,l)|\Bigg)\log\left(1-c_l^{-2+h(x_i|\theta))}\right)\Bigg].$$

In Section 5.4.1, we use a simple logistic model for determining the ranks, i.e. $r_i = h(x_i|w,b) = \sigma(w^T x_i + b)$ where $\sigma(\cdot)$ is the sigmoid function. After training, we can use the learned parameters θ^* to extract embeddings that capture the *endogenous ranks* of nodes in the graph. Besides, we can use centrality measures (degree centrality, [hypergraph] eigenvector centrality for k-uniform hypergraphs [50]), PageRank, etc.) to enrich the feature vectors. Here, the ranks r_i need to be re-sorted after each forward call to h which makes the total per-step cost for evaluating the LL equal to $T_{PRE} + T_{LL} + O(dn)$.

5.3.5 Choosing Hyperparameters

A question that arises when we fit a multi-layer CIGAM model is the following: *How to choose the number of layers L and the breakpoints H?* We observe that samples generated from CIGAM have roughly a piecewise linear form when the observed degree is plotted versus the degree ordering of a node in the degree ordering in a log-log plot (Figure 5.10). This observation motivates the following heuristic for hyperparameter selection: given a hypergraph G we calculate the degrees of all nodes, sort them in decreasing order and fit a piecewise linear function on the log-log scale. We then apply the *elbow* criterion [388] and choose the number of layers to be

$$L_{\text{pw}} = \underset{l \in [2, L_{\max}-1]}{\text{argmax}} \left\{ \frac{\log \text{pwerr}^*(l) - \log \text{pwerr}^*(l-1)}{\log \text{pwerr}^*(l+1) - \log \text{pwerr}r^*(l)} \right\}$$

where $\text{pwerr}^*(l)$ is the minimum piecewise linear fit error when fitting a function that is a piecewise combination of l lines. Roughly the rule says to pick the number of layers around which the ratio of the subsequent gradients is maximized. Then to identify the breakpoints we run grid search (i.e. likelihood ratio test/AIC[3]/BIC) on all feasible L_{pw} breakpoints.

5.3.6 Exact Sampling for CIGAM

Given the parameters λ, c of a single-layer model, a reasonable question to ask is: How can we efficiently generate k-uniform - and subsequently general hypergraphs - samples from the model with parameters λ, c? Identically to computing the LL a naïve coin flipping approach is computationally intractable and can be exponential in the worst case. To mitigate this issue we use the *ball-dropping* technique to generate edges as follows:

Step 1. Generate the n ranks $r \sim \text{TruncatedExp}(\lambda, [0, 1])$ with inverse transform sampling in $O(n)$ time (assuming access to a uniform $[0, 1]$-variable in $O(1)$ time). Sort wrt. $\succ$.

Step 2. For each $i \in [n]$ in the order draw a random binomial variable $M_i \sim \text{Bin}\left(\binom{n-i}{k-1}, c^{-2+r_i}\right)$. Drop M_i balls, where each ball represents a hyperedge e with $i \in e$ (see App. D.2.2 for how hyperedges are sampled).

[3]The difference between LR and the AIC between two models with layers L and L' is $L - L'$, so the two measures differ by at most 1, i.e. they are very close.

We repeat the same process for various values of k to create a graph with multiple orders. This technique runs much faster than $\binom{n}{k}$ (see [350]). The same logic can be extended to the multi-layer model where instead of dropping $M_i \sim \text{Bin}(\binom{n-i}{k-1}, c^{-2+r_i})$ balls for each i on the corresponding spots, we (more generally) throw $M_{i,l} \sim \text{Bin}\left(\binom{j_{\max}(i,l)-i}{k-1} - \binom{j_{\min}(i,l)-i-1}{k-1}, c_l^{-2+r_i}\right)$ for every $i \in [n]$ and $l \in [L]$ where each ball spot is chosen by throwing the first ball between $j_{\min}(i,l)$ and $j_{\max}(i,l)$ and the rest $k-2$ balls between i and $j_{\max}(i,l)$. We again use a rejection sampling mechanism to sample from this space. Finally, to sample a hypergraph with a simplex order range between $k_{\min}$ and $k_{\max}$ we repeat the above process for every $k \in [k_{\min}, k_{\max}]$ and take the union of the produced edge sets. Our implementation contains ball-dropping techniques for the general case of multiple layers, however here we present the single layer case for clarity of exposition.

5.4 "Small-core" Property

The model we are using serves as a generalization of hierarchical random graph models to random hypergraphs. In those models (cf. IGAM), it is often a straightforward calculation to bound the size of the core. Nevertheless, trivially carrying out the same analysis on hypergraphs does not work since the combinatorial structure of the problem changes cardinally, which highlights the need for new analysis tools in order to be proven.

In detail, in order to characterize the properties of the core of networks generated with CIGAM, we ask the following question: Given a randomly generated k-uniform hypergraph G generated by CIGAM, *what is the size of its core*? In our regime, the core is a subset C of the vertices with the following properties:

1. Nodes within the core set C are "tightly" connected with respect to the rest of the graph.
2. Nodes within the core set C form a dominating set for G *with high probability* (i.e. w.p. $1 - O(1/n)$).

For the former requirement, it is easy to observe that the induced subhypergraph that contains nodes with $r_i \geq t$ for some appropriately chosen t would form the most densely connected set wrt. the rest of the network. For the latter requirement, we use a probabilistic argument to characterize the core.

Clearly, members of the core are responsible for covering the periphery of the graph, i.e. each peripheral node has at least one hyperedge in the core. Thus the size of the core is the number of nodes that are needed to cover the periphery with high probability. We analyze the core size of the multi-layer model by constructing coupling with a single layer model that generates k-uniform hypergraphs with density c_L (that corresponds to the "sparsest" density). Then, we start with a threshold $t \in [0, 1]$ and we let $N_k(t)$ be the number of $(k-1)$-combinations that have at least one rank value $\geq t$. Then, we need to determine the value of t such that *(i)* $N_k(t)$ exceeds some quantity N_0 with high probability; *(ii)* the nodes with $r_j \geq t$ form an almost dominating set (serving as the core of the graph) with probability $1 - O(1/n)$ conditioned on $N_k(t) \geq N_0$. Proving *(ii)* proceeds by calculating the (random) probability that a node is not dominated by a *core hyperedge*, i.e. a hyperedge that has at least one node with $r_j \geq t$, and then taking a union bound over the nodes and setting the resulting probability to be at most $1/n$, yielding the desired lower bound N_0. Now, given that we know N_0 we want to set it in a value such that $N_k(t) \geq N_0$ with probability at least $1 - 1/n$. Observing that $N_k(t)$ obeys a combinatorial identity involving $N_2(t)$

which is a binomial r.v. and by using the Chernoff bound on $N_2(t)$ we can get a high probability guarantee for $N_k(t) \geq N_0$ by setting N_0 appropriately. Finally, we set the threshold t such that the probability of having a core at threshold t is at least $1 - O(1/n)$. We present the Theorem (proof in App. D.2.1)

Theorem 5.4.1. *Let G be a k-uniform hypergraph on $n \geq 2$ nodes with $k < n$ generated by a CIGAM model with L layers and parameters $1 < c_1 \leq c_2 \cdots \leq c_L < e^{\lambda}$ for $\lambda < \frac{\ln(n/72)}{4}$. Then, with probability at least $1 - 2/n$ the graph has a core at a threshold t such that $\frac{2\log n}{c_L^{-2+t}} = \binom{n}{k-1} - \binom{nF(t) + \sqrt{n\log n/2}}{k-1}$ with size $\tilde{O}(\sqrt{n})$. $\binom{x}{y}$ is the generalized binomial coefficient.*

Figure 5.11 depicts the (theoretical) threshold t for a 3-uniform and a 4-uniform hypergraph on 10 nodes. In App. D.2.1 we also plot the empirical thresholds of CIGAM-generated hypergraphs with $n = 200$. As k increases, the threshold t moves to the right, and therefore, the core becomes smaller.

5.4.1 Experiments with CIGAM

We first validate our model's ability to recover the correct parameters on synthetically generated data, as well as the efficiency of the proposed sampling method. We then perform experiments on small-scale graphs and show that the recovered latent ranks (and their subsequent ordering) can accurately represent the degree structure of the network. Finally, we do experiments with large-scale hypergraph data where we evaluate and compare our model with (generalized) baselines with respect to their abilities to fit the data.

We implement *Point Estimation (MLE/MAP)* and *Bayesian Inference (BI)* algorithms as part of the evaluation process, which are available in the code supple-

Table 5.1: Time complexity of fitting CIGAM for preprocessing (PP) and log-likelihood (LL). Here $r_i = \sigma(w^T x_i + b)$.

Ranks	Method	# Params	PP	LL
Known	All	$L+1$	T_{PRE}	T_{LL}
Exogenous	BI	$L+1+n$	-	$T_{PRE} + T_{LL}$
Endogenous	MLE, MAP	$L+d+2$	-	$T_{PRE} + T_{LL} + O(dn)$

ment. App. D.2.3 describes the specifics of each implementation and the design choices, and Tab. 5.1 shows the costs of fitting CIGAM on various occasions.

Sampling. Figure 5.12 shows the performance of the ball-dropping method on 2-order and 3-order hypergraphs for graphs with 50-500 nodes with a step of 50 nodes where for each step we sample 10 graphs and present the aggregate statistics (mean and 1 standard deviation).

Inference. In Figure 5.12, we generate a 2-Layer graph with $n = 100$ nodes, $k \in \{2, 3\}$, $\lambda = 2.5$, $c = [1.5, 2.5]$, $H = [0.5, 1]$, and use non-informative priors for recovery. Our algorithm can successfully recover the synthetic data.

Recovering the Degree Structure of small-scale graphs. We perform BI on world-trade, c-elegans, history-faculty, and business-faculty using $L = 1$ layer, a Gamma$(2, 2)$ prior for λ, and a Pareto$(1, 2)$ prior for c. In Figure 5.13, we order the actual degrees of the graphs in decreasing order and for every draw of the vector r from the posterior (using MCMC with $N = 1$K samples) as follows: (i) We sort the entries of r in decreasing order. Let $\{\pi\}_{i\in[N]}$ be the corresponding permutations of the nodes. For each $i \in [n]$ we calculate the mean and the

Table 5.2: Dataset Statistics. n_{LCC}, m_{LCC} refer to the size of the LCCs, n_{dt}, m_{dt} refers to the size of the LCCs after removing nodes with degree ≤ 4, n_{kc}, m_{kc} refers to the size of the 2-core of the LCC.

Dataset	$k_{\max}$	n_{LCC}	m_{LCC}	n_{dt}	m_{dt}	n_{kc}	m_{kc}
c-MAG-KDD	22	2.7K	1.4K	47	40	-	-
t-ask-ubuntu	6	6.2K	7.8K	664	1.7K	50	33
t-math-sx	7	26.4K	66.1K	5.4K	39.2K	100	58
t-stack-overflow	10	164.9K	306.4K	34.3K	140.4K	7.0K	6.0K
ghtorrent-p	7	78.4K	74.8K	10.8K	14.8K	3.4K	2.7K

standard deviation of $\left(\texttt{degrees}[\pi_{1,i}], \ldots, \texttt{degrees}[\pi_{N,i}]\right)^T$[4]. The scales of Figure 5.13 are log-log. We observe that the degrees, as they are determined by the ranks, are consistent with the actual degree sequence. This suggests that core-periphery organizations agree with the degree centralities, as in IGAM.

5.4.2 Experiments with large-scale data

Datasets. We perform experiments with publicly available datasets.

1. *coauth-MAG-KDD.* Contains all papers published at the KDD conference and are included in the *Microsoft Academic Graph v2* [386, 375]. We also include data for each of the authors' number of citations, h-index, number of publications and use the R package `amelia` [204] to impute missing data at rows where at least one of the columns exists after applying a log-transformation.

2. *ghtorrent-projects.* We mined timestamped data from the `ghtorrent` project [185, 184] and created the ghtorrent-projects dataset where each hyperedge corresponds to the users that have push access to a repository.

[4]I.e. the degree of the node which is first in the i-th ranking is added to the 1st position of the x-axis etc.

Table 5.3: Hypergraph Experiments. We use SGD with step-size 0.001 for CIGAM, and SGD with stepsize of 1e-6 for Logistic-CP, for 10 epochs. For HyperNSM we use $a = 10$, $p = 20$, and $\xi(e) = 1/|e|$. For evaluating the log-likelihood of Logistic-CP and HyperNSM we use $|\mathcal{B}| = 0.2\bar{m}$ negative samples. Best likelihood is in bold. † = LL cannot be computed.

Dataset	CIGAM	c^*	λ^*	Logistic-CP	HyperNSM	CIGAM	c^*	λ^*	Logistic-CP	HyperNSM
	Degree Threshold + LCC					LCC + 2-core				
	Exogenous ranks									
coauth-MAG-KDD	**-1334**	[3.0e+4]	1.4	-2025	-2.5e+6	-	-	-	-	-
threads-ask-ubuntu	**-1.3e+5**	[9.5e+9]	3.5	†	†	**-166**	[11.94]	1.5	-1510	-1073
threads-math-sx	**-4.2e+6**	[2.3e+20]	8.7	†	†	-1736	[5.2, 31.1]	1.8	**-1478**	-1.4e+5
threads-stack-overflow	**-2.0e+7**	[1.8e+20, 8.3e+27]	4.8	†	†	**-1.2e+5**	[2.1e+5]	5.1	-1.0+e7	†
ghtorrent-projects	**-1.2e+6**	[7.8e+15, 5.9e+20]	4.4	†	†	**-2.6e+5**	[9.4e+18]	3.6	†	†
	Endogenous (Learnable) ranks									
coauth-MAG-KDD	-1.8e+5	[32.4]	1.1	**-2024**	-2.5e+6	-	-	-	-	-
threads-ask-ubuntu	**-1.6e+5**	[9.6e+6]	1.1	†	†	-2079	[1.1]	1.1	**-1659**	-1075
threads-math-sx	-4.2e+6	[2.3e+20]	11.3	†	†	**-3.8e+4**	[2.8]	1.1	-5.8e+4	-1.4e+5
threads-stack-overflow	**-1.9e+7**	[4.1e+29]	26.8	†	†	**-4.0e+5**	[8.6e+8]	1.1	†	†
ghtorrent-projects	**-1.2e+6**	[2.9e+22]	2.8	†	†	**-2.1e+5**	[9.4e+20]	1.1	†	†

We used features regarding: number of followers on GitHub, number of commits, number of issues opened, number of repositories created, and the number of organizations the user participates at.

3. *threads-{ask-ubuntu, math-sx, stack-overflow} [51].* Nodes are users on `askubuntu.com`, `math.stackexchange.com`, and `stackoverflow.com`. A simplex describes users participating in a thread that lasts ≤ 24 hours. We observe that there is a high concentration of (non-engaged) users with reputation 1 and then the next peak in the reputation distrubution is at reputation 101. This bimodality is explained since Stack Exchange gives users an engagement bonus of 100 for staying on the platform. Therefore, we filter out all the threads at which non-engaged users (i.e. users with reputation less than 101) participate. We keep the (platform-given) reputation (as the ranks), the up-votes, and the down-votes of each user as her features.

Table 5.4: Projected Graph Experiments. We use SGD with step-size 0.001 for CIGAM, and SGD with stepsize of 1e-6 for Logistic-CP, for 10 epochs. For evaluating the log-likelihood of Logistic-CP, and Logistic-TH ($\alpha = 10, p = 20$) we use $|\mathcal{B}| = 0.2\bar{m}$ negative samples. Best likelihood in bold. † = LL cannot be computed.

Dataset	CIGAM	c^*	λ^*	Logistic-CP	Logistic-TH	CIGAM	c^*	λ^*	Logistic-CP	Logistic-TH
	Degree Threshold + LCC					LCC + 2-core				
	Exogenous ranks									
coauth-MAG-KDD	**-532**	[12.2]	1.4	-1532	-1419	-	-	-	-	-
threads-ask-ubuntu	-2.8e+4	[1.9e+3]	3.5	**-1.3e+4**	-2.4e+5	**-166**	[11.94]	1.5	-1510	-1329
threads-math-sx	**-8.5e+5**	[116.1, 2.0e+3]	8.7	-6.1e+6	-1.6e+7	**-564**	[2.7, 4.9]	1.8	-1376	-5471
threads-stack-overflow	**-4.0e+6**	[5.1e+6]	4.8	†	†	**-1.2e+5**	[2.1e+5]	5.1	†	-2.7e+7
ghrtorrent-projects	**-4.9e+6**	[1.7e+6]	4.4	†	†	**-7.4e+5**	[359.3, 951.3]	3.6	†	-1.8e+6
	Endogenous (Learnable) ranks									
coauth-MAG-KDD	-2171	[1.1]	1.1	-1680	**-1458**	-	-	-	-	-
threads-ask-ubuntu	-5.0e+4	[3.2]	1.1	-3.4e+4	-2.8e+5	**-185**	[12.1]	1.3	-1666	-1329
threads-math-sx	-1.3e+6	[1.2e+5]	10.7	†	†	**-402**	[45.2]	1.7	-1926	-5471
threads-stack-overflow	**-3.8e+6**	[5.2e+6]	20.7	†	†	**-1.2e+5**	[2.1e+5]	1.9	-1.0e+7	-2.7e+7
ghtorrent-projects	**-7.1e+5**	[5.1e+5]	4.4	†	†	**-5.7e+4**	[1.4e+4]	4.5	-1.9e+5	-1.8e+6

Deduplication. We keep each appearing hyperedge exactly once.

Outlier Removal & Feature Pre-processing. We filter *outliers* from the data in two ways. This is done in order to guarantee the numerical stability of the fitting algorithms. In the former filtering (Degree Threshold + LCC), we remove all nodes with degree < 4 and then find the Largest Connected Component (LCC) of the resulting data. In the latter filtering (LCC + 2-core) we first find the LCC of the hypergraph and then keep the 2-core[5] within it. The statistics of the post-processed datasets can be found in Tab. 5.2.

In the experiments considering exogenous ranks only, we take logarithms (plus one) of the exogenous ranks and min-max normalize the results to lie in $[0, 1]$. For the learning task (i.e., endogenous ranks), we perform standard Z-normalization (i.e., subtract column means and divide by the column stds.) in lieu of min-max normalization.

[5]The δ-core of G is a subgraph G' such that all nodes in G' have degree $\geq \delta$.

Hypergraph Experiments. We compare CIGAM with the *baseline* (without spatial dependencies) logistic model of [222]. This model is also known as the β-model [380, 411] and has been already generalized to hypergraphs (see [380]). However, the inference algorithm of [380] suffers from combinatorial explosion since for every node, the fixed-point equations require a summation over $\binom{n-1}{k-1}$ terms for a k-uniform hypergraph which makes the inference task infeasible for the datasets we study.

Logistic-CP generates independent hyperedges based on the sum of core scores $\sum_{i\in e} z_i$ for a hyperedge e, i.e. e is generated with probability $\rho(e) = \sigma\left(\sum_{i\in e} z_i\right)$ where $\sigma(z) = \frac{1}{1+e^{-z}}$. That corresponds to a LL $\log p(G|z) = \sum_{e\in E} \log \rho(e) + \sum_{\bar{e}\notin E} \log(1-\rho(e))$. In contrast to our model, computing the likelihood of Logistic-CP and its gradient exactly is - contrary to the case of CIGAM - intractable since it requires exhaustively summing over $\bar{e} \notin E$, which can be very large. To approximate the log-likelihood we use negative sampling by selecting a batch $\mathcal{B}$ as follows: We sample a hyperedge order $K \in [k_{\min}, k_{\max}]$ with probability $\mathbb{P}[K = k] = \frac{\bar{m}_k}{\bar{m}}$ where $\bar{m}_k = \binom{n}{k} - m_k$ denotes the number of negative hyperedges of order k and then given the sampled order K we sample a negative hyperedge $\bar{e}$ uniformly from the set of non-edges of order k. That uniform sampling scheme has a probability of selecting a hyperedge $\bar{e}$ equal to $\frac{|\mathcal{B}|}{\bar{m}}$ (App. D.2.2 describes the sampling algorithm). We use the following unbiased estimator of the LL based on this sampling scheme,

$$\widehat{\ell}(G|z) = \sum_{e\in E} \log \rho(e) + \frac{\bar{m}}{|\mathcal{B}|} \sum_{\bar{e}\sim\mathcal{B}} \log(1-\rho(\bar{e})), \tag{5.4}$$

where its easy to confirm that $\mathbb{E}\left[\widehat{\ell}\right] = \log p(G|\theta)$, and that $\mathrm{Var}[\widehat{\ell}] = \frac{\bar{m}-|\mathcal{B}|}{|\mathcal{B}|} \sum_{\bar{e}\in\bar{E}} \log^2(1-\rho(\bar{e}))$, which is at most $\frac{(\bar{m}-|\mathcal{B}|)\bar{m}}{|\mathcal{B}|}$ for $\rho(\bar{e}) \in [0, 0.51]$ (true for real-

world datasets). Letting $|\mathcal{B}| = \alpha\bar{m}$ for some $\alpha \in (0,1)$ we get a variance upper bound that equals $\frac{1-\alpha}{\alpha}\bar{m}$ for small values of $\rho(\bar{e})$. The per-step complexity of approximately computing the likelihood and its gradient in this case is both higher than computing the LL for CIGAM[6]. Logistic-CP can also be augmented with the use of features and a learnable map ψ with parameters ν such that $z_i = \psi(x_i|\nu)$. In this model, the core nodes are nodes with $z_i \geq 0$ and the periphery nodes are nodes with $z_i < 0$ respectively.

We also use the concurrent and independently developed method of [402] - HyperNSM - where a permutation π of the nodes is generated and then hyperedges are independently generated with probability $\sigma(\xi(e)M_a(\{a_u\}_{u\in e}))$, where M_a denotes the generalized (Hölder) a-mean. $\xi(e)$ is a weight function (e.g. $\xi(e) = 1/|e|$) and $a_u = 1 - \frac{\pi_u}{n}$. The goal of HyperNSM is to recover the optimal permutation π^* of the nodes through a fixed-point iteration scheme. To calculate the LL of HyperNSM, we use negative sampling, such as in the case of Logistic-CP.

Tab. 5.3 shows the results of comparing CIGAM with Logistic-CP and HyperNSM. As in Section 4.2 of [222], we compare the optimized LL values of both CIGAM, Logistic-CP, and HyperNSM. We run experiments both using *exogenous* ranks (directly from the features), as well as *endogenous* (learnable) ranks via the mined features. We also report the learned core profile c^* and the learned λ^* for all datasets. The breakpoints are taken with step 0.5. In almost all of the experiments, CIGAM has a *substantially better* optimal LL than its competitors, which in many cases cannot scale (because GPUs run out of memory) to even moderate dataset sizes (denoted by †). In terms of learned parameters, we ob-

[6]Briefly, for a k-uniform hypergraph, computing the positive part of the LL cost $O(km)$, and the negative part of the LL costs (on expectation over the draws) $O\left(k\binom{n}{k}\log(\bar{m}/(\bar{m}-|\mathcal{B}|)\right)$.

serve that most of the datasets are very sparse (very high values of c^*) in both the exogenous and the endogenous case. In App. D.3, we show how to add regularization (or priors) to the model.

Projected Hypergraph Experiments.. We run the same experiments as in Tab. 5.3 but instead of the hypergraph data, we use the *projected* graphs that result from replacing each hyperedge with a clique. We also use the model of [401], together with Logistic-CP and CIGAM. More specifically, the model of [401], which we call Logistic-TH, is a logistic-based model (the graph analog of HyperNSM) that depends on finding a permutation π of the nodes. In this model, and edge (u, v) is generated independently with probability $\sigma(M_a(a_u, a_v))$ where $a_u = 1 - \frac{\pi_u}{n}$ (resp. a_v). The authors devise an iterative method to optimize the LL of the corresponding generative model. The iterative method converges to a fixed point vector x^*, and the ordering of the elements of x^* implies the optimal permutation π^*. Again, to calculate the LL after finding π^* we use negative sampling.

We report the experimental results in Tab. 5.4. Again, we observe that CIGAM is able to find better fits than both Logistic-CP and Logistic-TH, while it is also able to scale more smoothly to the largest datasets. Furthermore, we observe that the values of c^* that CIGAM finds compared to the hypergraph case are *substantially smaller*. This can be attributed to the fact that the projected hypergraphs have a smaller possible number of edges (i.e. $\binom{n}{2}$), and, thus, they are *"denser"* than the hypergraph instances since hyperedges are projected on the same order.

5.5 Discussion

The present Chapters observe a connection between the core-periphery structure of networks and dominating sets and devise two models - DIGAM and CIGAM - to optimize these metrics, and both are fitted in real-world data as the core-periphery structure is present in several real-world networks. As potential for future works, it is important to emphasize the main concept behind exploiting the core-periphery structure of networks to speed up hard computational tasks. In general, small computations can be performed in the core - which has size $o(n)$ - and then the results can be used to perform approximate computations for the whole network, which is significantly larger than the core. Examples correspond to as all-pairs-shortest-paths computation, betweenness centrality (see, e.g., the recent work in [400]), community detection, embedding generation, and many more.

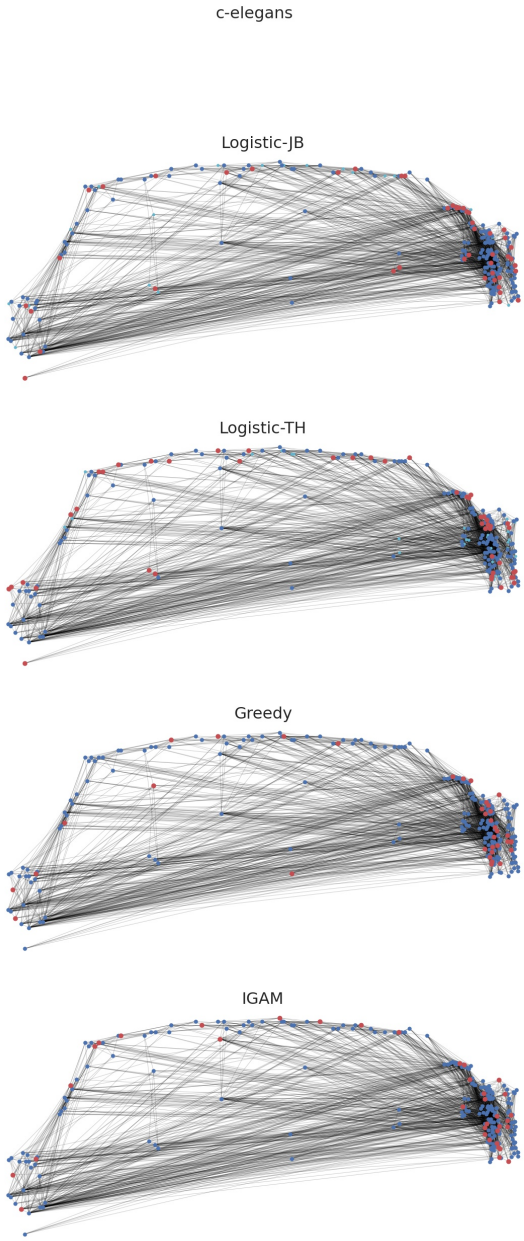


Figure 5.4: Visualization of a core set of size $n^{0.7}$ for the Logistic-JB, Logistic-TH, Greedy, and IGAM strategies. The red nodes represent members of the core set, the blue nodes are dominated nodes, and the cyan nodes are non-dominated nodes.

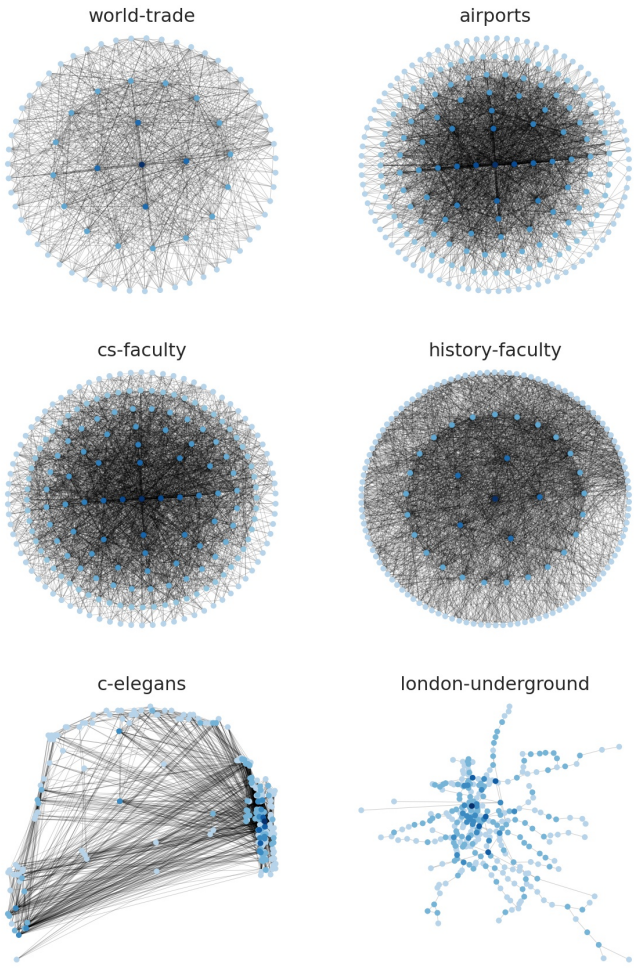


Figure 5.5: IGAM model fitted on small datasets (world-trade, airports, cs-faculty, history-faculty, c-elegans, london-underground). The darker colors refer to nodes with higher prestige, and the lighter colors refer to nodes with lower prestige.

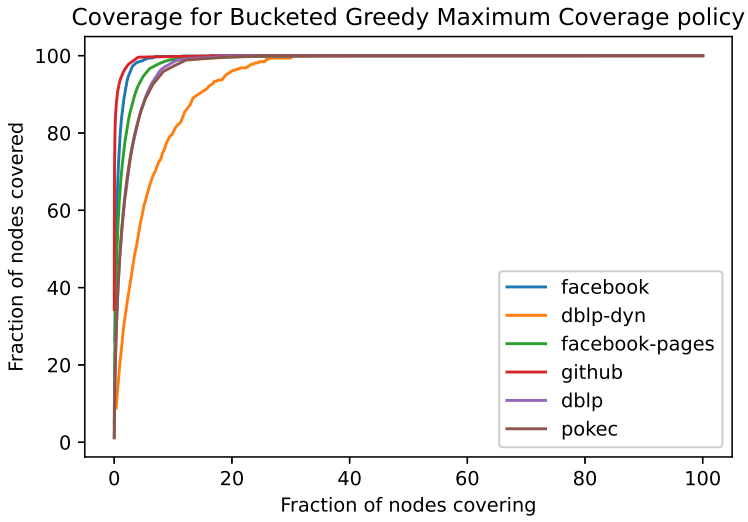


Figure 5.6: Adjacency matrix of IGAM2 model with $c_1 = 1.5, c_2 = 2.5, b = 3$, $H_0 = 2$ and $H = 6$.

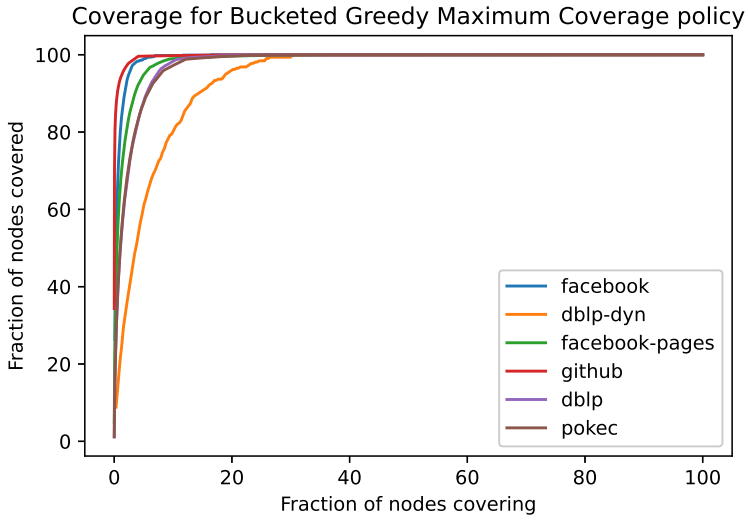


Figure 5.7: Domination Curve by running the method of Tudisco and Higham [401].

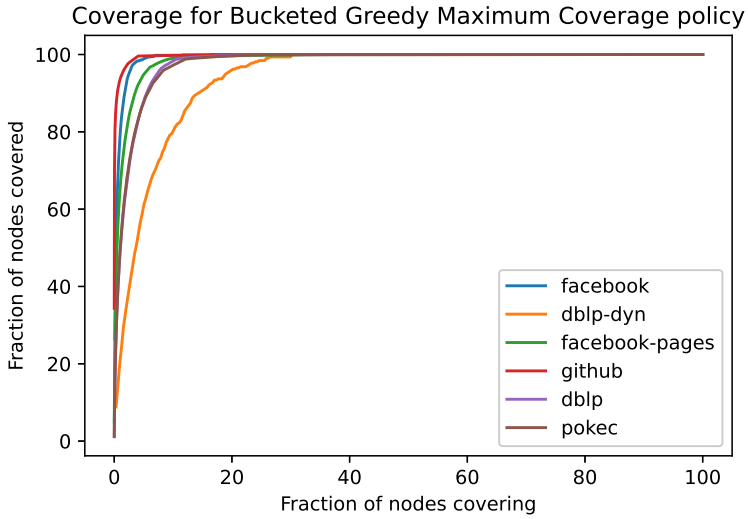


Figure 5.8: Domination Curve by fitting the model of Jia and Benson [222] on spatial data and the logistic CP model otherwise.

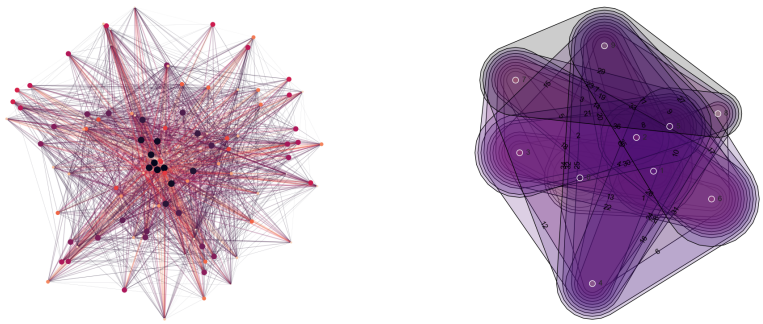


Figure 5.9: Generated Instances of a 2-layer model with $c = [1.5, 2.5], H = [0.25, 1], \lambda = \log 3$. Left: $k = 2$, Right: $k = 3$.

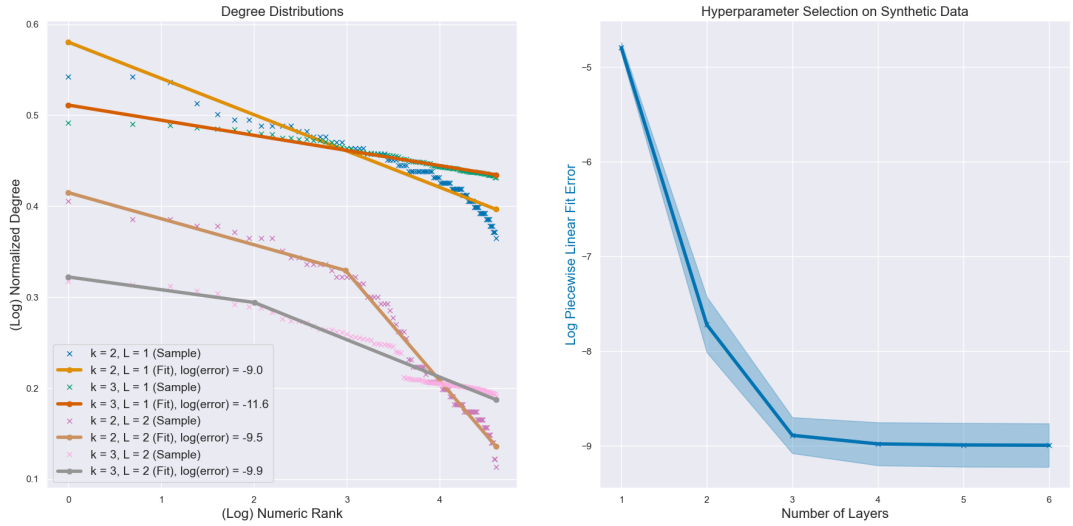


Figure 5.10: (Left) Degree Plot for an instance with $k \in \{2,3\}, L \in \{1,2\}$ layer, $b = 3$, $H = 1$, H split as powers of $1/2$ in $[0,1]$ and c split uniformly on $[1.5, 2.9]$ with p/w fits. (Right) Elbow plot for 10 3-layer simulated graphs.

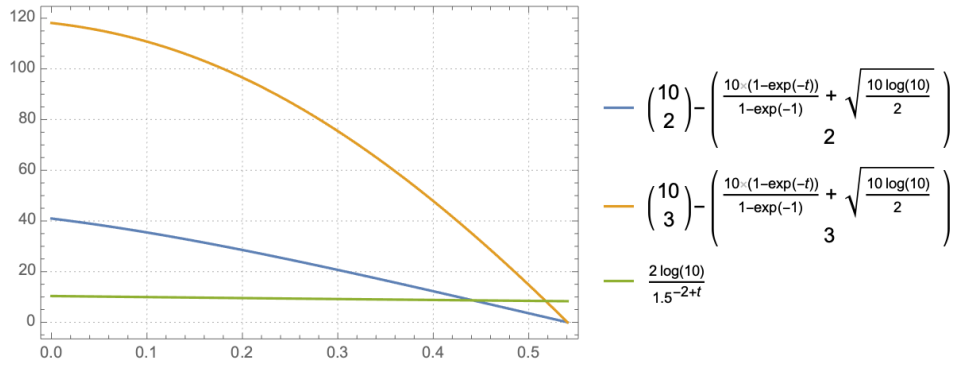


Figure 5.11: Core threshold functions from Thm. 5.4.1 for $c_L = 1.5, \lambda = 1, k \in \{3,4\}$, and $t \in [0, F^{-1}(1 - \sqrt{\log n/(2n)})]$ (x-axis).

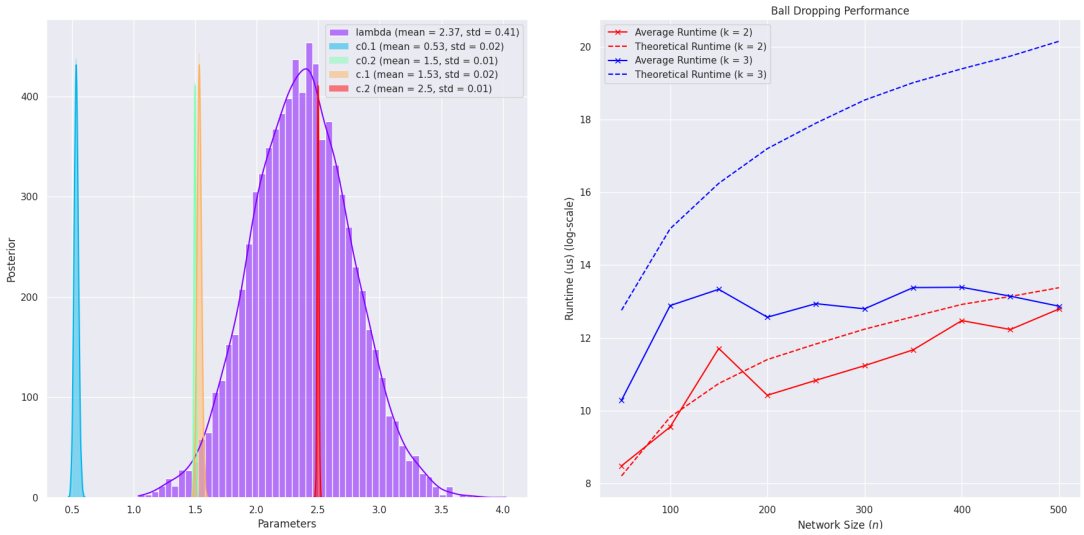
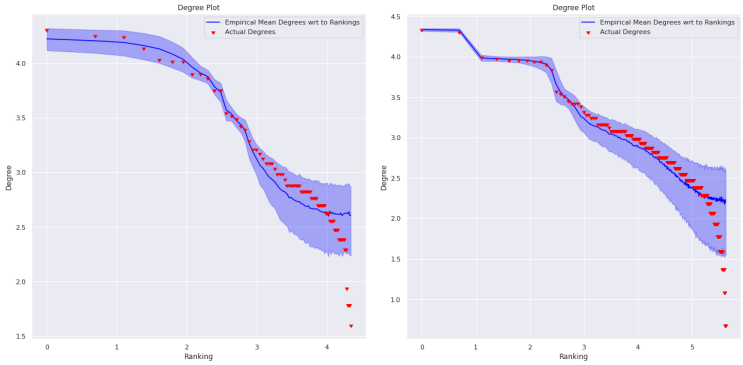
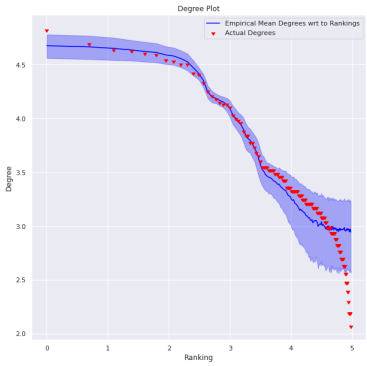


Figure 5.12: **Left:** Parameter recovery for $n = 100, k \in \{2, 3\}, c = [1.5, 2.5], \lambda = 2.5$. Legend: `c0` corresponds to off-by-one parameters and `c` corresponds to the actual parameters. **Right:** Average Runtime of Sampling Using the Ball Dropping Method for hypergraphs of orders $k \in \{2, 3\}$ and $50 - 500$ nodes with a step of 50 nodes for a 1-layer instance with $b = 3, c = 1.5$. The dashed line is the function that is the expected number of edges of a k-uniform CIGAM hypergraph.

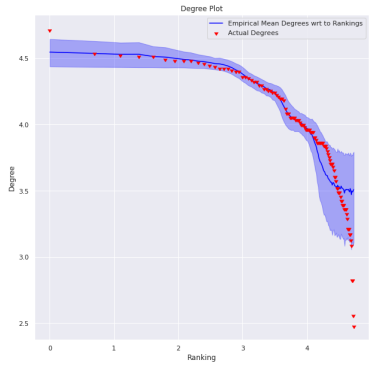


(a) world-trade [119] ($n = 76, m = 845$)

(b) c-elegans [224] ($n = 279, m = 1.9$K)



(c) history [107] ($n = 145, m = 2$K)



(d) business [107] ($n = 113, m = 3$K)

Figure 5.13: Recovery of the Degree Structure for world-trade, c-elegans, history-faculty, and business-faculty datasets.

CHAPTER 6

AN EMERGING RESEARCH DIRECTION: MODELING NETWORKS WITH LARGE LANGUAGE MODELS

The contents of this chapter constitute joint work with Yuan Yuan.

Social networks fundamentally shape human opinions, behaviors, and the dissemination of information, affecting sociotechnical networks and their resilience. As large language models (LLMs) like GPT, Claude, and Llama increasingly integrate into social and professional settings, understanding their behavior in the context of social interactions and network formation becomes essential. In this Chapter, we attempt to ask the following question:

> *Do network formation behaviors of multiple LLMs approximate certain aspects of human network dynamics?*

By simulating interactions among LLM agents across various model families, we observe that these models consistently exhibit key patterns associated with social network principles—including preferential attachment, triadic closure, homophily, community structure, and the small-world phenomenon—when forming networks. Moreover, LLMs adapt their network formation strategies based on each network's characteristics, reflecting the context-dependent nature of human behavior: In Facebook networks, they prioritize triadic closure and homophily, mirroring close-knit friendships; in phone networks, homophily, and preferential attachment dominate, capturing personal and professional connections; and in employment networks, LLMs favor heterophily and high-degree connections, aligning with career advancement dynamics. These results open new avenues for using LLMs in network science

research, with potential applications in agent-based modeling and synthetic network generation.

6.1 Modeling Networks with Large Language Models

Recent progress in large language models (LLMs), such as GPT [314], Claude [20], and Llama [392], has shown promising developments in AI techniques and their integration into real-life applications. It is thus crucial to comprehend AI actions to ensure they align with human expectations, mitigate potential risks, and maximize their benefits. Misaligned AI actions may lead to unintended consequences, such as biased decision-making, fairness issues, and the miscoordinative or non-cooperative behavior [348]. Recently, researchers have started to apply social science methodologies, such as methods analogous to laboratory experiments [205, 11, 408, 277], agent-based modeling [332, 166, 199, 118, 150, 335], and qualitative methods [102], to study LLMs. These methods not only reveal the capabilities and interpretability of LLMs but also suggest their potential for applications in social science [205, 331, 101, 260].

In human societies, social networks play a crucial role in shaping individual behaviors, preferences, and connections, as well as influencing the diffusion of information and norms across communities [355, 34, 157, 36, 431]. LLMs have shown great potential in social contexts, notably as intelligent personal assistants that facilitate social and prosocial interactions (see, e.g., [327, 104, 408]). However, less is known about how LLMs' behaviors and preferences align with human network formation principles [210, 437, 331]. This is particularly crucial, as it sheds light on the potential of these models to shape and be shaped by

the networks of human relationships, which is a fundamental aspect of social systems.

This Chapter explores LLMs' behaviors and preferences in the context of network formation with both synthetic and real-world social networks. By analyzing interactions between multiple LLMs (or multi-LLMs), we aim to understand the implications of LLMs representing humans in social and professional settings. Specifically, we examine micro-level social network properties including preferential attachment [41], triadic closure [188], and homophily [283], as well as macro-level properties including community structure [307], and the small-world phenomenon [240, 419].

In synthetic network simulations, LLMs displayed preferential attachment, homophily, and triadic closure, resulting in the formation of community structures and small-world dynamics. More notably, in real-world social network simulations, we find that LLMs prioritized triadic closure and homophily over preferential attachment when forming new links, indicating a strong preference for connecting with similar nodes or shared acquaintances. Additionally, in a telecommunication network, LLMs tended to prioritize homophily and preferential attachment over triadic closure, and in a company network, the agents who corresponded to employees formed links frequently with managers, which showcases behavior that is consistent with human social mobility principles.

Generally, LLMs not only exhibit fundamental social network formation principles in synthetic simulations but also adapt their strategies based on the context of real-world networks, mirroring human social behaviors specific to each setting.

As LLM technology continues to evolve, this Chapter serves as an early exploration of their potential in social network studies, with several significant implications for future studies. First, this Chapter demonstrates the potential of LLMs for agent-based modeling. By simulating decision-making processes that approximate human-like behavior across various network settings, LLMs can provide valuable insights into the emergence of social phenomena. Although these models are still in early stages of development, they offer an intriguing framework for studying and designing systems that can mimic key aspects of real-world dynamics. This opens up possibilities for applying LLMs to explore and understand complex behaviors in social, professional, and collaborative environments. Second, our work highlights the potential of LLMs for synthetic dataset generation, a critical area in network science. Although the accuracy of LLM-based predictions is not yet perfect like all other link prediction models, this approach is particularly valuable in scenarios where privacy concerns limit access to real-world data. By simulating realistic datasets that capture important network properties, LLMs can facilitate research and experimentation without compromising sensitive information.

We investigated whether LLMs exhibit fundamental principles of network formation observed in human social networks. By simulating multiple LLM agents acting independently within separate conversational threads, we examined their behaviors in decision-making scenarios involving network connections. We focused on three micro-level network principles—preferential attachment, triadic closure, and homophily—and two macro-level phenomena: community structure and the small-world effect. To assess the robustness of our findings, we varied the temperature settings of different LLM models, including GPT-3.5-turbo, GPT-4o Mini, Llama 3 (70b-instruct), and Claude 3.5 Sonnet.

We also experimented with different environmental prompts (e.g., friendship, collaboration, and community) to test prompt sensitivity. Additionally, we employed an interview-like method to probe the LLMs' decision-making rationale and conducted experiments using Chain-of-Thought (CoT) reasoning [421] (the experiments are deferred to Appendix E.8). Finally, we extended our analysis to real-world networks, including a social media friendship network, a telecommunication network, and a company collaboration network, to compare the network formation preferences between LLMs and humans.

6.1.1 Micro-Level Properties

Principle 1: Preferential Attachment. Preferential attachment is a fundamental concept in network science, illustrating how nodes in a network gain connections over time, leading to a scale-free degree distribution characterized by a few highly connected nodes [41, 55].

To test if LLM agents exhibit preferential attachment, we simulated network growth by sequentially adding nodes to an initially empty network. Each new node was prompted with information about existing nodes, and the person to connect with was decided. We generated networks with $n = 200$ nodes to observe meaningful degree distributions[1].

On a micro-scale, Figure 6.1(a) illustrates the probability of connecting to a top-k node as a function of its degree percentile (k/n). To demonstrate the tendency toward preferential attachment, we compare these probabilities to a null model assuming random connections (represented by dashed lines), where

[1]Note that we provide the full network structure in the prompt, so models are not inherently biased toward forming links with the highest-degree nodes.

the likelihood of connecting to a top-k node is simply k/n. Our findings reveal that all models prefer connecting to higher-degree nodes. Notably, GPT-3.5 exhibits a weaker preference, while other, arguably more capable models, show an even stronger inclination toward preferential attachment. Using GPT-3.5 as an example, we examine the effect of temperature – a parameter controlling the variability of model output – on this tendency. At lower temperatures, the model makes fewer stochastic choices and, as a result, is more likely to connect to high-degree nodes. We also vary the prompt to explore the influence of "environment"-contextual settings such as school, work, or community. The results show slight variations compared to the baseline (GPT-3.5 with temperature = 1.5), yet the tendency for preferential attachment persists across environments. In all cases, the observed curves lie above the null model, underscoring the presence of preferential attachment.

Next, we investigate the degree distribution of the resulting graphs. As shown in Figure 6.1(c), the resulting networks display a pattern where a few nodes have many connections while most have few, indicative of a scale-free distribution, with form:

$$\pi(d) \propto d^{-\gamma}, \quad \text{where} \quad \gamma > 1. \tag{6.1}$$

We estimated the exponent γ for different models and temperatures. Our analysis reveals several notable patterns in the networks generated by LLM agents under different conditions. First, models newer than GPT-3.5 exhibit a slightly larger $\widehat{\gamma}$ than GPT-3.5. This implies that these models display a stronger tendency toward preferential attachment and the formation of hubs. Second, as the temperature increases the power-law exponent $\widehat{\gamma}$ generally becomes larger. This indicates that higher temperatures introduce more variance in node connectivity, leading to degree distributions with heavier tails. Third, the environmental

context significantly affects the value of $\hat{\gamma}$. For example, when the network is framed within a "school" environment, the exponent increases, suggesting a more uniform distribution of connections and fewer highly central nodes.

Finally, while the prompts we have utilized thus far have provided the model with the complete existing network structure, we also explore an alternative scenario: what happens if agents are supplied solely with the degree of other alternatives, without access to the network's full structure? As detailed in Appendix E.7, our findings reveal that limiting agents to degree information alone also leads to notable structural differences in the networks that emerge (cf Figure E.2). Thus, degree information alone yields more restrictive structures than providing the agents with the full topological information (i.e. the neighbors).

The findings highlight the practical potential of LLMs in modeling complex networks, such as social, economic, or biological systems, by leveraging their ability to simulate preferential attachment and scale-free distributions. These models can be used to study real-world phenomena like information diffusion, hub formation, or connectivity patterns under varying conditions. Additionally, the sensitivity of network structures to parameters like temperature and context underscores the importance of prompt design in steering outcomes, making LLMs versatile tools for tailored simulations.

Principle 2: Triadic Closure. The second micro-level principle we examine is triadic closure, which posits that individuals are more likely to form connections with friends of friends, thus creating closed triads in the network. This process strengthens network structure and cohesion, grounded in the idea that

two nodes are more likely to connect if they share a common neighbor [188, 290].

To investigate triadic closure, we employ an assortative stochastic block model (SBM) [305] to create an initial network G_1 with n nodes divided into two equal-sized clusters A and B. Connections within each cluster are formed with a probability of 0.5, while inter-cluster connections occur with a probability of 0.1. This setup mirrors our assumption that nodes within the same cluster are more inclined to connect due to a higher number of shared neighbors. In subsequent time steps, we then examine each node i, considering the intersection of neighborhoods of i's non-neighbors[2].

We conducted ten simulations with $n = 50$ nodes to facilitate clear visualization and ensure statistical significance[3].

On a micro-scale, Figure 6.2(a) illustrates the probability of connecting to a top-k-percentile node as a function of the number of common neighbors. The dashed lines represent the results of null models, where connections are chosen randomly; which corresponds to the probability of connecting to a top-k percentile node in terms of the common neighbors being k/n. Our findings reveal that, across all models, there is a consistently higher probability of forming links with nodes that share more common neighbors. Unlike the behavior observed in preferential attachment, temperature does not appear to severely impact this probability. This tendency to form links with nodes that have more common neighbors is consistent across various contexts, including school, work, and community environments. These results suggest that the triadic closure tendency is a robust phenomenon, persisting across different model families, con-

[2]Similar outcomes arise when providing neighbors instead of common neighbors.

[3]Choosing $n = 50$ instead of a larger number like $n = 200$ aids in visualization and maintains statistical significance.

figurations, and environments.

Then, for evaluating triadic closure on the network (macroscopic) level, we utilize two metrics: *marginal transitivity* and *probability of edge formation within the same community*. Marginal transitivity (D) represents the change in the ratio of closed triangles to all triads, transitioning from the initial network G_T to the SBM-generated G_1:

$$D = 3 \times \frac{\#\text{ triangles}(G_T)}{\#\text{ triads}(G_T)} - 3 \times \frac{\#\text{ triangles}(G_1)}{\#\text{ triads}(G_1)}.$$

where a large positive D indicates a strong triadic closure tendency. The probability of forming an edge within the same community ($\widehat{p}$) is calculated by the ratio of edges in $G_T \setminus G_1$ (newly formed edges) connecting nodes within the same cluster:

$$\widehat{p} = \frac{\left|\left\{\{i,j\} \in E(G_T) \setminus E(G_1) : y_i = y_j\right\}\right|}{|E(G_T) \setminus E(G_1)|},$$

where $y_i, y_j \in A, B$ denote the community memberships of nodes i and j, respectively. A value of $\widehat{p}$ exceeding 0.5 suggests a triadic closure tendency. As we investigate under SBM, same community membership indicates more open triads being closed.

Marginal transitivity (D), presented in Figure 6.2(b), demonstrates a statistically significant increase across all models, temperatures, and environments, underscoring the robust nature of triadic closure. Similarly, the probability of within-community edge formation ($\widehat{p}$), shown in Figure 6.2(b), consistently exceeds 0.5, reaffirming the tendency of nodes to form new connections within their respective clusters.

In Figure 6.3(a), sample networks from GPT-3.5 are displayed, with the upper panel showing networks where the entire structure is provided and the

lower panel showing those with only common neighbor numbers provided. Nodes are color-coded to indicate their cluster memberships in the SBM, with red and blue edges within clusters and orange edges between clusters. Newly formed edges are highlighted with thicker lines.

In summary, these findings show that most LLMs exhibit a consistent tendency for triadic closure across various configurations, temperatures, and environments. This behavior mirrors human network dynamics, highlighting the models' ability to simulate realistic social and structural networks and reinforcing their alignment with social principles observed in real-world communities.

Principle 3: Homophily. Homophily reflects the tendency for nodes with similar characteristics or attributes to form connections and associate with each other. This phenomenon is based on the principle that individuals in a network are more likely to connect with others who share similar traits, interests, or demographics [283].

To test whether LLM agents exhibit homophily, we perform the following experiment: We generate nodes with randomly generated attributes regarding a hobby (randomly chosen among three hobbies), a favorite color (randomly chosen among three colors), and a location within the US (randomly chosen among three US locations) and provide the attributes of the other nodes and the node's own attributes, and each node is tasked to form up to $\delta = 5$ links with others. For each node i, we provide it with the features x_j of all non-neighbors j of i. The seed network is taken to be the empty graph. We run ten simulations for networks with $n = 50$ nodes and $\delta = 5$.

To evaluate homophily, we calculate the attribute assortativity coefficient for

each of the features. For each property P which takes K distinct values $P_1, \ldots, P_K$ (indexed by k or l), its *assortativity coefficient* R is defined as

$$R = \frac{\sum_{k=1}^{K} M_{kk} - \sum_{k=1}^{K} a_k b_k}{1 - \sum_{k=1}^{K} a_k b_k}.$$

Here M represents the mixing matrix. Its elements M_{kl} reflect the proportion of edges connecting two nodes with values P_k and P_l, respectively. We define $a_k = \sum_{l=1}^{K} M_{kl}$ and $b_k = \sum_{l=1}^{K} M_{lk}$. Assortativity ranges from -1 to $+1$. A positive assortativity indicates nodes preferentially connect to similar ones, forming a homophilous network. Conversely, a negative assortativity suggests connections primarily occur between dissimilar nodes, indicating heterophily.

From Figure 6.4(a), we observe that different attributes exhibit varying levels of assortativity. First, homophily is present across all LLMs—regardless of the specific model or configuration (e.g., temperature settings), all show positive assortativity for all four attributes. This aligns with human societies, where homophily is a primary driver of network formation [283][4].

Moreover, to test the effect of the features on homophily as indicated by the assortativity coefficient for each attribute, we introduce a *distractor feature*, which corresponds to a lucky number that is randomly chosen between 0 and 9. We repeat the simulations for all models and measure the effect of each feature on Figure 6.5. We show that lucky numbers consistently show lower assortativity coefficients, indicating they are less considered when forming homophilous connections. This is consistent with our prior expectation that humans typically do not prioritize shared lucky numbers when establishing relationships.

[4] As an additional robustness check, we also tested mutual agreement connections. In that setting, after a node j is chosen by node i, j has to confirm the creation of the link from itself to i ($j \to i$). We ran several experiments with different models and temperatures and we found the results not to be affected, namely, the proposed connections were always bilateral.

Surprisingly, even though the lucky number does not seem to impact homophily much, the favorite color exhibits a similar level of homophily as hobbies. One might expect that hobbies, being substantive interests, would have a stronger influence on social connections than favorite colors, which are more arbitrary preferences. However, this finding aligns with the social identity theory and the minimal group paradigm [384]. According to this paradigm, even minimal and arbitrary group distinctions – such as a preference for certain colors – can lead to in-group favoritism and influence social connections. This suggests that LLM agents, akin to humans, may form connections based on even trivial shared attributes, reflecting inherent tendencies toward group formation based on minimal commonalities.

All in all, LLMs can capture and reproduce subtle human social behaviors, not just linguistic patterns. This underscores their potential as powerful tools for social simulation. However, these findings may also raise important considerations regarding bias, fairness, and the ethical design of AI systems (cf. Discussion Section).

6.1.2 Macro-Level Principles

Principle 4: Community Structure. The community structure of networks refers to the organization of nodes or individuals within a network into distinct and densely interconnected groups or clusters [307, 306, 60, 108]. Identifying community structures is crucial for understanding the overall dynamics of a network, as it reveals patterns of relationships and interactions that might not

be apparent at the global level.[5]

Both triadic closure and homophily contribute to the formation of community structures. By examining how these two factors contribute to network formation, we aim to gain insights into the underlying mechanisms driving community dynamics in LLM-generated networks. We employ the simulation results presented in the synthetic networks to determine whether community structure in networks generated by LLMs emerges from triadic closure or homophily.

First, we consider the networks generated in Figure 6.2. We examine how LLM agents' choices strengthen the network's community structure. Specifically, we leverage the fact that the SBM graph has a preexisting community structure and measure how the newly formed links reinforce such a structure. Visual inspection shows that the newly added links, represented by the bold edges, happen mostly within each cluster, reinforcing the community structure. This is further quantitatively verified by the fraction $\hat{p}$ newly created inter-community edges. We find that $\hat{p}$ is significantly higher than 0.5 ($P < 0.001$, t-test comparing with 0.5). This indicates that most edges are within the same community, strengthening the community structure.

Next, we investigate the community structure resulting from homophily using modularity maximization [60] (Figure 6.4). Modularity quantifies the discrepancy between the actual number of edges within communities and the expected number in a random network with identical node count and degree distribution, following the Chung-Lu model [106]. This model presumes that nodes maintain their weighted degree, with edges randomly distributed. The

[5] As an example, we present only the results from GPT-3.5 for Principle 4 (Community Structure) and Principle 5 (Small-World).

weighted modularity Q [108] for a graph with edge weights w_{ij} and C communities is defined as

$$Q = \sum_{c=1}^{C} \left[\frac{L_c}{W} - r\left(\frac{k_c}{2W} \right)^2 \right].$$

Here W represents the total edge weights, L_c the intra-community link weights for community c, k_c the total weighted degree within community c, and r the resolution parameter, set to 1 for our analysis. High modularity values (e.g., greater than 0.5) indicate significant community structuring, diverging from the random model.[6] For the network's weights, we use the number of common attributes shared between each pair of nodes: $w_{ij} = \left| \left\{ k : x_i^{(k)} = x_j^{(k)} \right\} \right|$ for each link (i, j) in the final network. Here, $x_i^{(k)}$ and $x_j^{(k)}$ correspond to the k-th features of x_i and x_j, respectively.

In Figure 6.4(b), various colors represent the communities identified by the Louvain algorithm at different temperatures for GPT-3.5. Notably, communities appear more distinct at lower temperatures, likely due to reduced randomness in decision-making at these temperatures. Figure 6.4(a) presents the distribution of Louvain modularity values across simulations accross different LLM models and different environments, indicating consistent community structure with positive modularity at all temperatures, confirmed by a t-test against a modularity of $Q = 0$ for a random graph ($P < 0.001$).

Our results demonstrate that community structures manifest in networks generated by LLMs, driven by both triadic closure and homophily.

[6] Given the NP-Hard nature of maximizing Q, we employ the Louvain algorithm [60] to approximate the highest possible modularity.

Principle 5: Small-World. The small-world phenomenon is characterized by networks where nodes are interconnected in tight clusters, yet the average distance between any two nodes remains relatively short, typically scaling logarithmically with the network size [419, 240]. This balance between high clustering and short path lengths characterizes small-world networks. A small-world network is defined by its *average shortest path length* L, which grows logarithmically with the size of the network n,[7] expressed as

$$L \sim \log(n).$$

Our analysis utilizes the Watts-Strogatz model [419] as a benchmark to investigate whether LLMs can generate networks exhibiting small-world characteristics. This model has a delicate balance between local clustering and short average path lengths: Nodes tend to form clusters or groups (triadic closure), exhibiting a high level of interconnectedness within these local neighborhoods, whereas at the same time, the existence of a few long-range connections ensures that the entire network is reachable with relatively few steps [332, 276, 218].

We employ a modified version of the model, where edge rewiring is informed by LLM queries, based on the current network structure. The generation process is parametrized by the number of nodes (n), average degree (k), and the rewiring probability (β). See details in *Methods and Materials*.

We generated networks of various sizes, ranging from $n = 10$ to $n = 100$, to explore the relationship between the network size (n) and two key metrics: the average shortest path length (L) and the average clustering coefficient (C). For this analysis, we considered values of β set at 0.25, 0.5, and 0.75, with a fixed

[7] As per the definition in [215].

$k = 5$ to serve as a consistent parameter. Visual representations and average clustering coefficients are presented in Figures 6.6(a) to 6.6(c).

However, when directly compared with the Watts-Strogatz model, the networks generated by the LLMs do not precisely replicate the characteristics of Watts-Strogatz networks for the corresponding the rewiring probabilities (β). As illustrated in right panels of Figures 6.6(a) to 6.6(c), we find weak evidence that the LLM-generated networks share the same average shortest path length as the Watts-Strogatz model for the rewiring probabilities (β) of 0.25, 0.5, and 0.75, with $P < 0.1$ from a t-test comparing the average shortest path lengths. Additionally, LLM-generated networks exhibit a larger average clustering coefficient than those of the Watts-Strogatz model for the same rewiring probabilities β, also with a significance level of $P < 0.1$ in the t-test comparisons. This discrepancy suggests the differences in the network structure and connectivity patterns between the LLM-generated networks and the classical Watts-Strogatz model.

We also provide regressions analysis by examining the correlation between the average shortest path length and average clustering coefficient versus $\log(n)$ (refer to Figure 6.7(a), Figure 6.7(b), and Figure 6.7(c)). We found that across all tested temperatures, the relationships were statistically significant, with most regressions yielding $P < 0.001$. This indicates that the average shortest path length increases proportionally with $\log(n)$. Similarly, for the average clustering coefficient, we demonstrated that it inversely scales with $1/\log(n)$, with the majority of regression analyses also showing $P < 0.001$. These findings align with the small-world properties of organizational networks as documented in the study by [215], suggesting that these characteristics are not only prevalent

but also predictable across different network sizes.

To quantify how LLM-generated networks resemble Watts-Strogatz networks, we fit the estimated $\widehat{\beta}$ values for each LLM-generated network.[8] In Figures 6.7(d) to 6.7(f), we plot the estimated values for $\widehat{\beta}$ for each value of β and each temperature. Here P-values result from a t-test comparing with the average shortest path length of Watts-Strogatz with rewiring probability $\widehat{\beta}$. These results show that while the average shortest path lengths are not identical, they are sufficiently close, with the differences not being statistically significant at the 0.1 level for most temperature settings. Finally, as Figure 6.7(g) shows, the relation $L \sim \log(n)$ holds for different LLM models and environments.

In conclusion, our analysis demonstrates that LLM-generated networks exhibit key small-world properties, with logarithmic scaling of average shortest path lengths and inverse logarithmic scaling of average clustering coefficients. While these networks do not perfectly align with the Watts-Strogatz model, they exhibit similar structural characteristics.

6.1.3 Real-World Networks with Heterogeneous Agents

We investigate the behavior of LLMs in real-world network formation contexts with four datasets in two differing real-world domains. Despite the significant advancements in social network analysis over recent years, the availability of fully complete and comprehensive network datasets remains exceptionally rare [431]. We employ three datasets from the *Facebook100* collection [394] and the telecommunication (*Andorra*) and the employment (*MobileD*) datasets

[8] We conducted a binary search to identify the $\widehat{\beta}$ values for which the Watts-Strogatz networks' average clustering coefficients match those of the LLM-generated networks.

from [431]. The Facebook100 data correspond to "friendship" networks from one hundred American colleges and universities, captured at a specific moment from Facebook's online social network. The Andorra dataset contains nationwide call records in Andorra from July 2015 to June 2016, where calls correspond to mutual calls between Andorran residents containing information about the caller's and the callee's location, phone type, and usage. Finally, the MobileD dataset corresponds to a company network where relations correspond to call or text communication, and each employee is either a manager or a subordinate.

For all network datasets, the agents have *heterogeneous* profiles (i.e., profiles with different features) whose statistics (degree distribution, clustering coefficient distribution, assortativity) we report in Figure 6.8.

To infer the models' tendencies, we employ a discrete choice modeling framework [315, 279]. Specifically, we model the network formation process as a discrete choice process, wherein nodes are sequentially prompted to form connections from a set of available alternatives (see *Methods and Materials*).

Number of Samples and Alternatives. For the three datasets from Facebook100 are Caltech36 ($n = 769$) Swarthmore42 ($n = 1,659$), and UChicago30 ($n = 6,591$), we set the number of alternatives to be $A = 15$ and randomly sampled from the existing network. For the UChicago30 dataset, we consider a randomly sampled subset of $N = 2,000$ nodes because of the limited context window of the LLM models. For Andorra ($n = 32,812$) and MobileD ($n = 1,982$), we set the number of alternatives to $A = 5$ and consider a randomly sampled subset of $N = 1,000$ nodes.

Model	Preferential Attachment ($\widehat{\theta}_{\text{PA}}$)	Homophily ($\widehat{\theta}_{\text{H}}$)	Triadic Closure ($\widehat{\theta}_{\text{TC}}$)	Log Likelihood	AIC
Caltech36 (n = 769 nodes, m = 33,312 edges, N = 769 samples, A = 15 alternatives each)					
GPT-3.5	0.20*** (0.002)	0.65*** (0.005)	-0.06 (0.006)	-2,088.21	4,184.41
GPT-4o Mini	0.34*** (0.006)	2.13*** (0.03)	0.44*** (0.02)	-1,201.27	2,410.55
GPT-4 (gpt-4-1106-preview)	0.41*** (0.01)	1.95*** (0.02)	0.59*** (0.01)	-1,377.47	2,762.94
Claude 3.5 Sonnet	0.46*** (0.005)	0.55*** (0.01)	0.55*** (0.007)	-1,748.19	3,504.38
Llama 3 70b Instruct	0.28*** (0.006)	2.43*** (0.02)	0.84*** (0.01)	-809.57	1,627.15
Swarthmore42 (n = 1,659 nodes, m = 122,100 edges, N = 1,659 samples, A = 15 alternatives each)					
GPT-3.5	0.19*** (0.008)	0.47*** (0.01)	0.00 (0.009)	-4,484.45	8,976.90
GPT-4o Mini	0.27*** (0.21)	2.22*** (0.78)	0.57*** (0.43)	-1,899.09	3,806.19
GPT-4 (gpt-4-1106-preview)	0.18*** (0.003)	1.62*** (0.006)	0.65*** (0.002)	-2,838.33	5,684.66
Claude 3.5 Sonnet	0.36*** (0.002)	0.75*** (0.006)	0.55*** (0.004)	-3,563.02	7,134.03
Llama 3 70b Instruct	0.39*** (0.003)	2.31*** (0.005)	0.62*** (0.004)	-1,820.26	3,648.52
UChicago30 (n = 6,951 nodes, m = 416,206 edges, N = 2,000 samples, A = 15 alternatives each)					
GPT-3.5	0.22*** (0.001)	0.48*** (0.004)	-0.02 (0.0005)	-8,157.38	16,322.77
GPT-4o Mini	0.27*** (0.005)	2.22*** (0.019)	0.57*** (0.011)	-1,899.09	3,806.19
GPT-4 (gpt-4-1106-preview)	0.23*** (0.001)	2.00*** (0.005)	0.41*** (0.002)	-3,444.33	6,896.67
Claude 3.5 Sonnet	0.43*** (0.003)	0.78*** (0.005)	0.39*** (0.002)	-6,604.77	13,217.54
Llama 3 70b Instruct	0.43*** (0.007)	2.57*** (0.014)	0.32*** (0.005)	-3,689.00	7,386.00
Andorra (n = 32,812 nodes, m = 513,931 edges, N = 1,000 samples, A = 5 alternatives each)					
GPT-3.5	0.53*** (0.001)	0.21* (0.01)	-0.24*** (0.002)	-1,712.91	3,433.83
GPT-4o Mini	0.54*** (0.004)	3.47*** (0.06)	-0.09* (0.01)	-1,002.11	2,012.22
GPT-4 (gpt-4-1106-preview)	0.21 (0.20)	3.45*** (1.16)	-0.22 (0.25)	-1271.20	2622.30
Claude 3.5 Sonnet	0.54*** (0.003)	1.94*** (0.009)	-0.15*** (0.003)	-1,541.77	3,091.55
Llama 3 70b Instruct	0.38*** (0.003)	3.92*** (0.02)	-0.04 (0.01)	-985.95	1,979.91
MobileD (n = 1,982 nodes, m = 25,470 edges, N = 1,000 samples, A = 5 alternatives each)					
GPT-3.5	1.06*** (0.003)	-0.94*** (0.009)	-0.02 (0.001)	-1,663.42	3,334.84
GPT-4o Mini	1.38*** (0.02)	-0.85*** (0.02)	0.87*** (0.01)	-880.39	1,768.78
GPT-4 (gpt-4-1106-preview)	0.42*** (0.01)	-1.84*** (0.009)	0.94*** (0.003)	-1,321.01	2,650.02
Claude 3.5 Sonnet	0.71*** (0.009)	-2.44*** (0.02)	1.13*** (0.005)	-1,197.92	2,403.83
Llama 3 70b Instruct	1.04*** (0.005)	-0.36** (0.01)	0.71*** (0.002)	-1,269.42	2,546.83

*Note: *: $P < 0.05$, **: $P < 0.01$, ***: $P < 0.001$*

Table 6.1: Effect sizes for real-world networks from Facebook100 [394] and Andorra dataset [431] for several LLMs for temperature set to 0.5.

Regression Coefficients. We regress network formation decisions on standardized scores reflecting the three micro-level principles. We present the regression results in Table 6.1.[9] First, we observe a dominant effect of homophily across all datasets and models. The coefficients for homophily ($\widehat{\theta}_{\text{H}}$) are consistently the largest and highly significant ($P < 0.05$) in almost all cases. For instance, in the Caltech36 dataset, the homophily coefficients for GPT-3.5, GPT-4, and Llama 3 70b Instruct are 0.65, 1.95, and 2.43, respectively ($P < 0.001$). The emphasis on homophily suggests that LLMs, much like humans, prioritize forming connections based on shared characteristics.

[9] More detailed results can be found in Table E.1 in Appendix E.6.

Second, we find that preferential attachment plays a secondary role in the network formation decisions of LLMs. While the coefficients for preferential attachment ($\widehat{\theta}_{\text{PA}}$) are generally positive and statistically significant across most models and datasets, they are notably smaller than those for homophily. For example, in the Swarthmore42 dataset, GPT-3.5 and Llama 3 70b Instruct have preferential attachment coefficients of 0.19 and 0.39, respectively ($P < 0.001$). This suggests that while LLMs do consider the degree of potential connection nodes—favoring connections to well-connected nodes—the influence of this factor is less evident compared to homophily.

Finally, the influence of triadic closure appears to vary across different datasets and models. In most cases, the coefficients for triadic closure ($\widehat{\theta}_{\text{TC}}$) are positive and significant, indicating that LLMs consider the number of mutual connections when forming new links. However, in some instances, such as with GPT-3.5 on the Andorra dataset, the triadic closure coefficient is negative (-0.24) and significant, suggesting a structure-dependent role of this principle as shown by the low clustering coefficient of the network, which is dominated by preferential attachment, as also shown in Figure 6.8. This variability implies that while triadic closure is a factor in LLMs' decision-making, its impact may be influenced by the specific characteristics of the dataset or the model used.

In summary, our analysis demonstrates that while homophily, triadic closure, and preferential attachment are integral to the network formation behaviors of LLMs, homophily is the dominant factor.

6.2 Discussion

In this Chapter, we conducted a comprehensive evaluation of LLMs' network formation preferences, examining both micro-level network principles—such as preferential attachment, triadic closure, and homophily—and macro-level network properties like community structure and the small-world phenomenon. Our findings indicate that networks generated by multiple LLMs exhibit these properties, particularly when the models are primed with network statistics like the number of mutual friends or the degrees of potential connections. Furthermore, using discrete choice modeling, we explored the emergence of these properties in simulations based on real-world networks. Our results reveal that the LLM agents' selections are predominantly driven by homophily, followed by triadic closure and preferential attachment.

On the one hand, this Chapter enhances our understanding of how multiple LLMs behave in networked settings. Specifically, our findings reveal varying strengths in network formation properties among LLMs, suggesting that when these models are employed to coordinate social networks in social or work environments, they may exhibit human-like behaviors. This has important implications for applications like agent-based modeling, where realistic simulation of human behavior is crucial. Traditionally, agent-based models rely on simplified rules or heuristics to represent individual behaviors, which may not capture the complexity of human decision-making. By incorporating LLMs as agents, we can simulate more nuanced and context-aware interactions that closely resemble human social behavior, without the need to rigidly specify decision rules or heuristics.

On the other hand, our results suggest that we should exercise caution when leveraging LLMs in networking scenarios. The model family, configuration, and prompts can subtly affect the models' behavior, resulting in qualitatively similar but quantitatively different outcomes.

For example, newer models such as GPT-4 and Claude 3.5 exhibit stronger biases compared to prior models such as GPT-3.5. For instance, in the preferential attachment principle, newer models such as GPT-4 and Claude 3.5 have stronger biases – i.e., connect to *highest*-degree-nodes yielding star-like networks – compared to GPT-3.5 and LLama 3, which had weaker biases – i.e., connect to *high*-degree-nodes. Similar results can be found in homophily, as larger biases towards homophily, and triadic closure. Thus, even though LLMs exhibit these principles, we should be cautious of such biases when designing simulations.

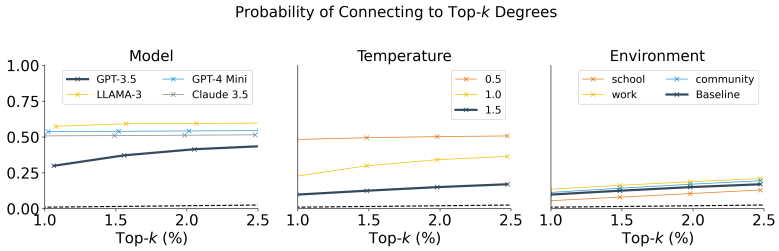
Similarly, in our experiments with real-world data, we find an interesting phase transition from homophily to heterophily: In the Facebook100 data, the LLMs generally exhibited positive biases toward homophily ($\widehat{\theta}_H > 0$). However, in employment networks, agents were either managers or subordinates, and we discovered that LLM agents were heterophilous in such a case ($\widehat{\theta}_H < 0$), which aligns with career advancement dynamics (i.e. employees want to form links with managers because of better career prospects).

The above underscores the need for researchers to provide oversight and ensure that LLM behaviors align with human expectations when employing them in scientific research methods, such as agent-based modeling and even prototypical human subject research with LLMs.

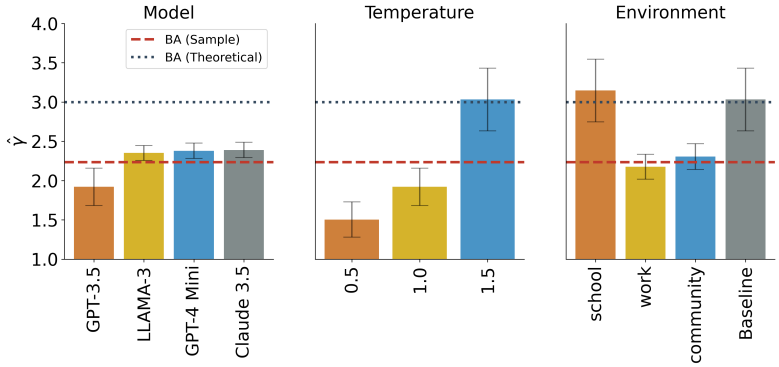
Thus, although we find that LLMs resemble human network formation be-

haviors, we should consider whether these models should exhibit such behaviors when serving as assistants to humans in work and social lives. Biases like homophily, triadic closure, or preferential attachment may lead to network structures that overemphasize certain individuals or fragment information flow. Humans form networks with communities and central nodes partly due to limited social capacities; however, LLMs do not share these limitations.

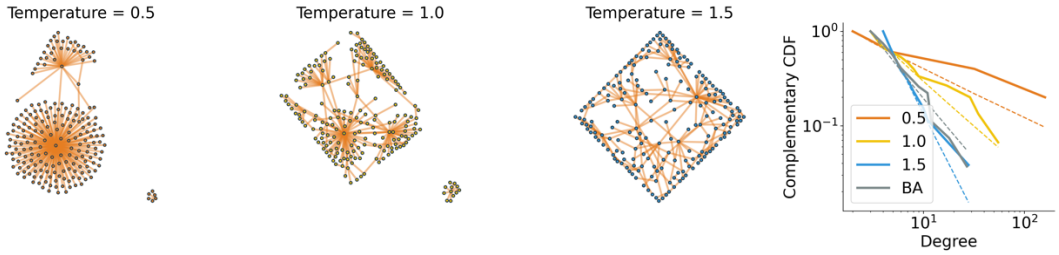
Therefore, when used as social assistants, LLMs may not necessarily need to mirror human networking behaviors and could be personalized to promote more equitable and efficient information dissemination.



(a) Probability of connecting to top-k nodes for different models, temperatures, and environments

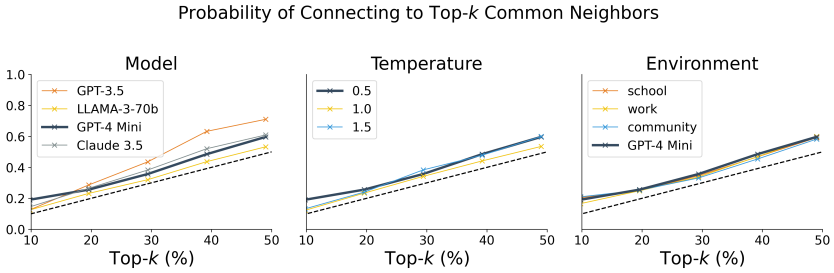


(b) Power law fits ($\hat{\gamma}$) and standard errors for different models, temperatures, and environments

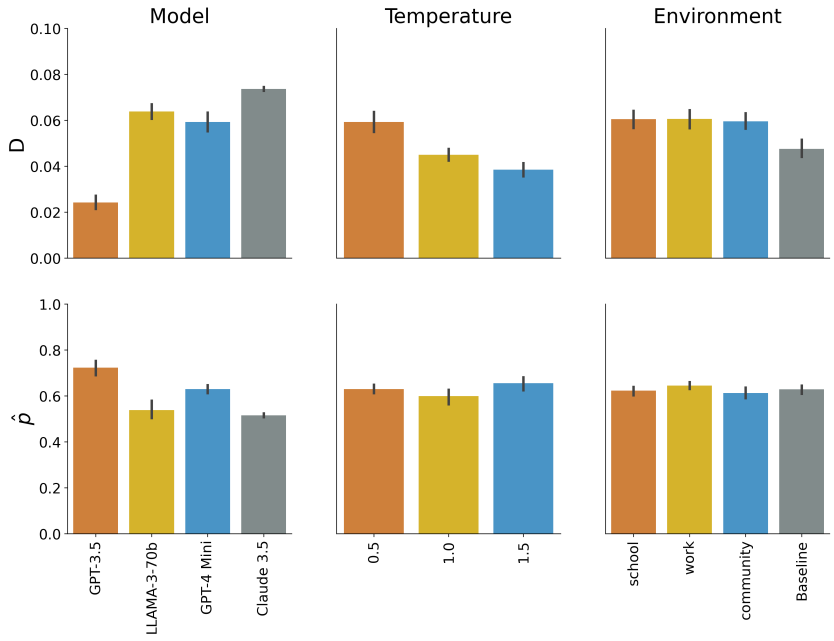


(c) Network instances generated by GPT-3.5 agents

Figure 6.1: **Results for Principle 1 (preferential attachment)** The multi-LLM setup was given neighborhood information $\{N_{j,t} : j \in V_t\}$. **Top Left:** Probability of connecting to top-k-degree nodes for varying model (temperature is fixed to 1.0 and environment to baseline), temperature (model fixed to GPT-3.5 and environment to baseline) and environment (model fixed to GPT-3.5 and environment temperature to 1.5) for networks generated according to Principle 1 with $n = 200$ nodes. **Top Right:** Power Law exponents and standard errors for varying model, temperature, and environment. **Bottom:** Simulated networks. Power-law degree distributions are evident ($P > 0.5$, K-S test), with the networks at a temperature of 1.5 closely resembling the Barabási-Albert model ($P > 0.1$, K-S test) for GPT-3.5 agents.

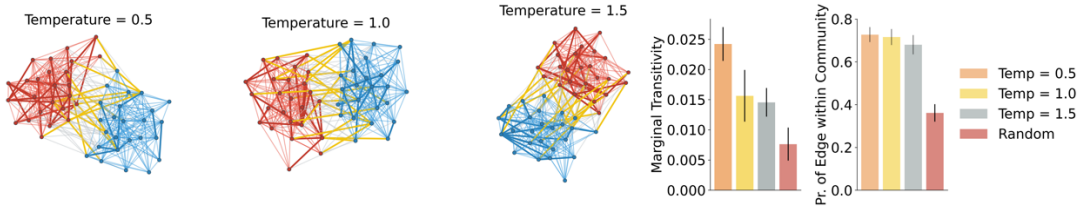


(a) Probability of connecting to top-k for different models, temperatures, and environments



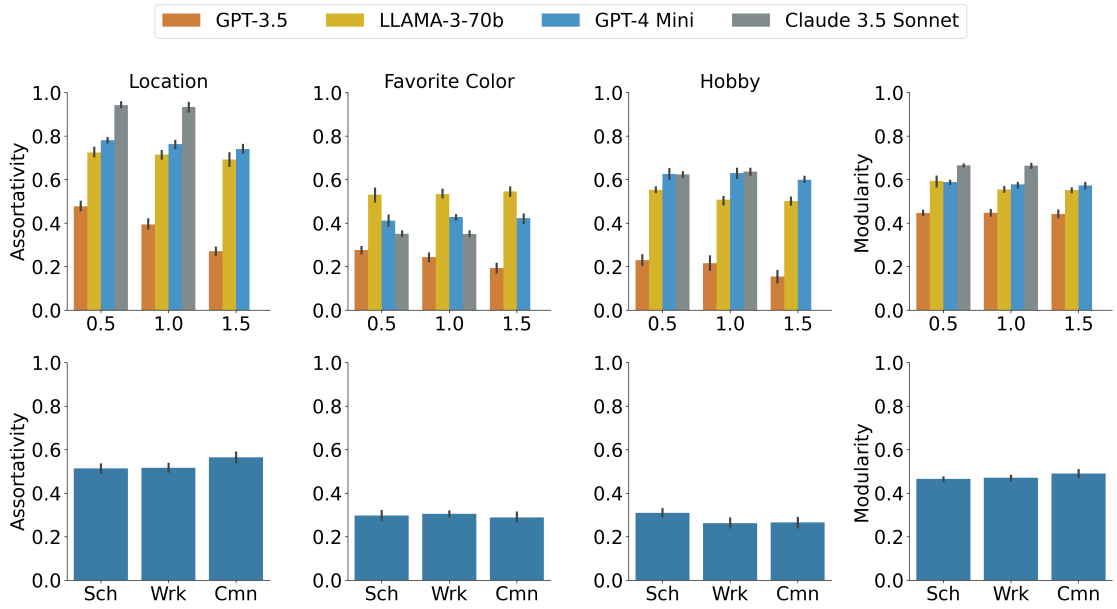
(b) Marginal transitivity (D) and probability of an edge within a community ($\hat{p}$) for different models, temperatures, and environments

Figure 6.2: **Results for Principle 2 (triadic closure). Top:** Probability of connecting to top-k nodes (in terms of common neighbors) for varying model (temperature is fixed to 1.0 and environment to baseline), temperature (model fixed to GPT-4 Mini and environment to baseline) and environment (model fixed to GPT-4 Mini and environment temperature to 0.5) for networks generated according to Principle 2 ($n = 50$, 10 simulations for each model, environment and temperature). **Middle:** Marginal transitivity (D) and probability of an edge within a community ($\hat{p}$) for networks generated according to Principle 2 in different models, temperatures, and environments.

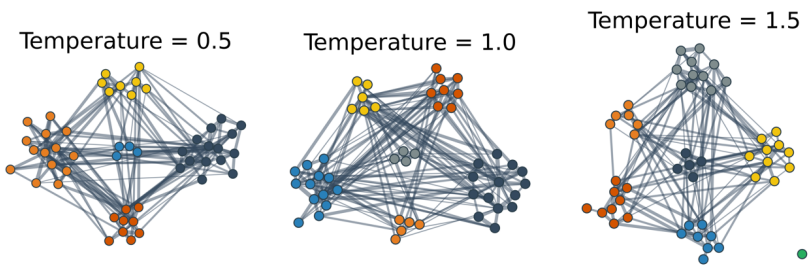


(a) Network instances by GPT-3.5 agents

Figure 6.3: The figure shows the resulting networks created by GPT-4 Mini, according to Principle 2 when the intersection of the neighborhoods of the query node and each alternative is provided. The node colors correspond to the groups to which each node belongs. The bold edges (red or blue) correspond to the newly created inter-cluster edges, and the orange edges correspond to the new intra-cluster edges.



(a) Assortativity and Louvain Modularity with different LLM models and environments



(b) Network instances generated by GPT-3.5 agents

Figure 6.4: **Results for Principle 3 (Homophily) and Principle 4 (Community structure due to homophily). Top:** Assortativities and Louvain modularity according to Principle 3 ($n = 50$, 5 simulations for each row) in different environments (school, work, community) using different models. The statistical significance is $P < 0.001$ for all t-tests (comparing with 0). **Bottom:** Network instances and community structure.

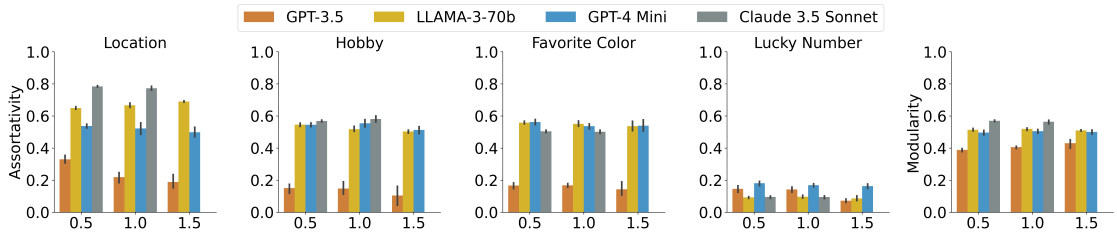
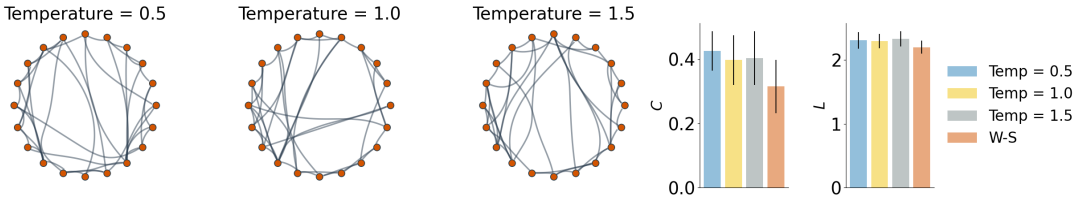
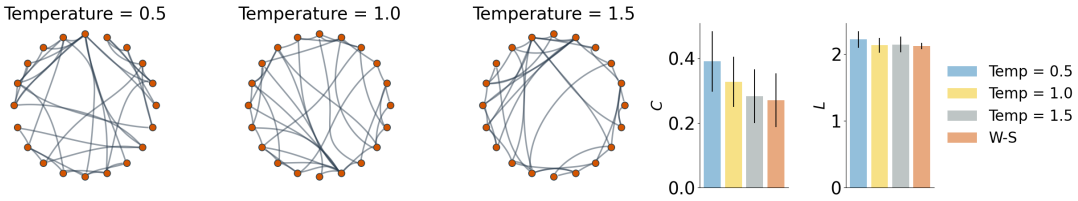


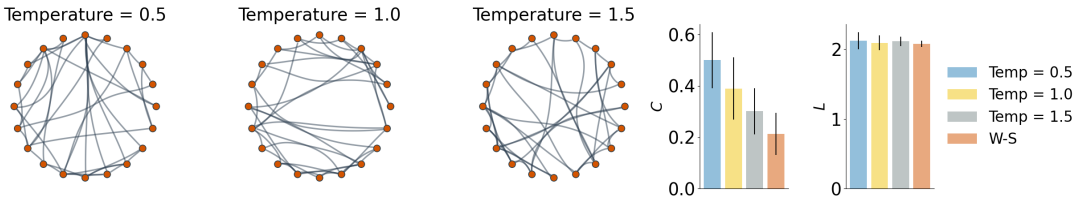
Figure 6.5: Effect of distractor features (favorite color and lucky number) on homophily.



(a) Network Instances for $\beta = 0.25$

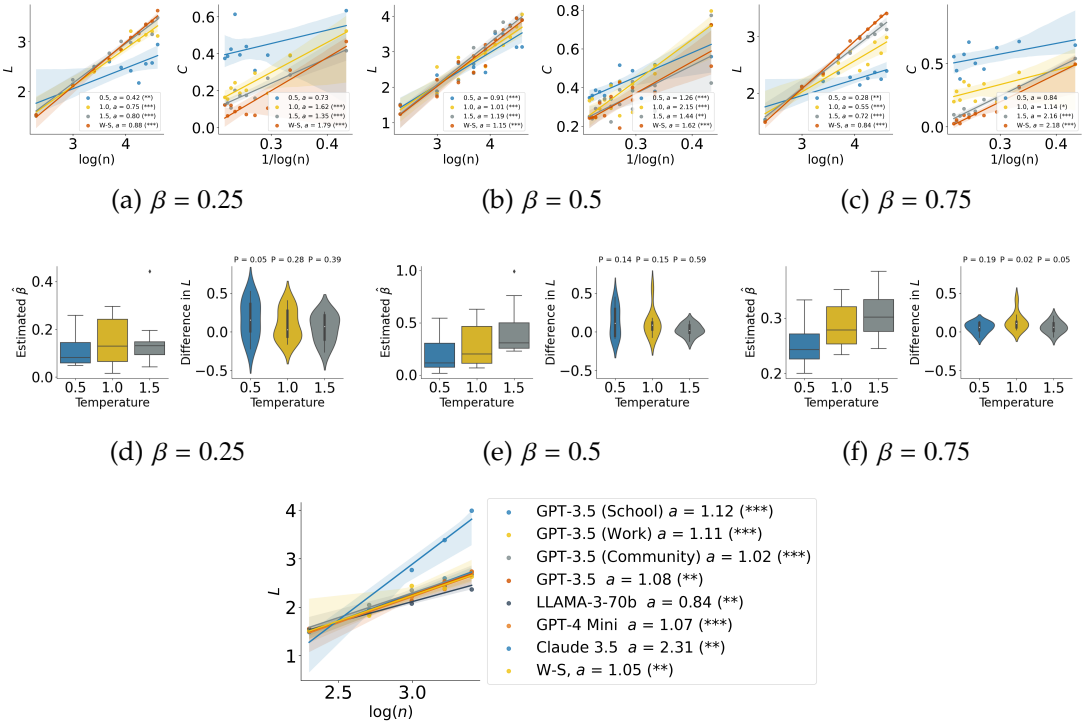


(b) Network Instances for $\beta = 0.5$



(c) Network Instances for $\beta = 0.75$

Figure 6.6: **Simulation results for Principle 5 (small world).** Network instances for the networks created according to Principle 5 using the altered Watts-Strogatz Model for node count $n = 50$, average degree $k = 5$, rewriting probability $\beta \in \{0.25, 0.5, 0.75\}$, together with plots of the **average clustering coefficient** C and the **average shortest path length** L. The comparison is made with respect to a Watts-Strogatz graph with $n = 50, k = 5, \beta \in \{0.25, 0.5, 0.75\}$. The error bars correspond to 95% confidence intervals.



(a) $\beta = 0.25$ (b) $\beta = 0.5$ (c) $\beta = 0.75$

(d) $\beta = 0.25$ (e) $\beta = 0.5$ (f) $\beta = 0.75$

(g) Regression plot for different models and environments for $\beta = 0.25$ and $k = 5$.

Figure 6.7: **Fitted results for Principle 5 (small world). Top (a-c):** Regression plots relating **average shortest path length** (L) and **average clustering coefficient** (C) with n for $\beta \in \{0.25, 0.5, 0.75\}$ and $k = 5$ for GPT-3.5. The value a in legends represents the effect size (slope of the regression lines). **Middle (d-f):** Estimated values $\widehat{\beta}$ of $\beta \in \{0.25, 0.5, 0.75\}$ for LLM-generated networks based on matching the average clustering coefficient and difference in the average shortest path between LLM-generated networks and Watts-Strogatz with the **estimated rewiring probability** $\widehat{\beta}$ for GPT-3.5 agents. We report the P-values of the t-test comparing the average shortest path length of the LLM-generated networks and the average shortest path length of the Watts-Strogatz graphs with rewiring probability $\widehat{\beta}$. **Bottom (g):** Regression plot for the relation $L \sim \log(n)$ for different LLM models and environments (school, work, community) for $\beta = 0.25$ and $k = 5$. The legend shows the effect size (a) and the P-value. (*: $P < 0.05$; **: $P < 0.01$, and ***: $P < 0.001$.)

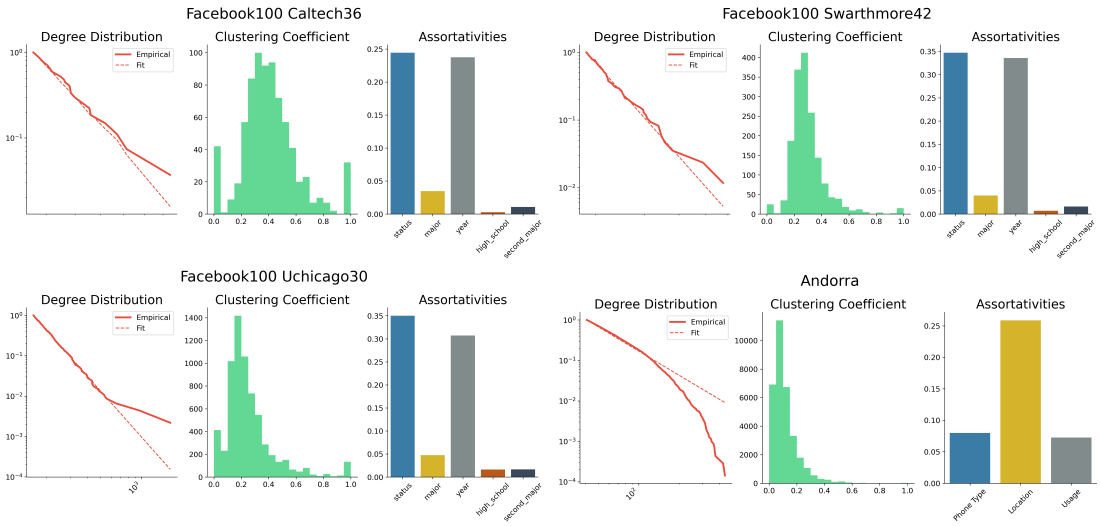


Figure 6.8: Distributions of real-world datasets analyzed in this Chapter, including degree, clustering coefficients, and the assortativities of the attributes included in the datasets.

CHAPTER 7

CONCLUSION AND FUTURE WORK

In this Ph.D. thesis, we have elaborated on the projects that span the majority of my graduate career at Cornell.

First, in Chapter 2, we have talked about how a planner can allocate resources in a dynamic networked system that undergoes exogenous shocks and contagion, and we have developed algorithms that can solve the dynamic contagion problem at scale – namely when the network has a large number of nodes (n) and the time horizon (T) is large – providing an algorithm that solves $O(\text{poly}(T))$ LPs to approximate the value function for fractional interventions. This contagion model can be used to solve problems that are much more general than traditional influence maximization [236] or financial contagion [139]. The algorithm leverages the fact that contagion problems arising from the Eisenberg-Noe problem have an elegant representation as linear programs, allowing us to solve the Hamilton-Jacobi-Bellman equations efficiently. Additionally, we leverage this LP relaxation to solve the problem when the interventions are discrete and give an instance-dependent approximation that depends on the Endogenous Exposure Index $\widetilde{\beta}_{\max}$, as well as give the best possible approximation guarantee $(1 - 1/e)$ when the horizon is trivial ($T = 1$) showing that in this case the corresponding objective is submodular. One potential promising direction is to attempt to devise a better approximation guarantee for the dynamic contagion problem by leveraging recent results that extend classic influence maximization results to the dynamic setting [333]. We anticipate that this extension would require the development of several algorithmic techniques given the generality of our model.

Subsequently, in Chapter 3, we have explored how network structure affects the susceptibility of supply chain networks to cascading failures by studying the resilience metrics $R_{\mathcal{G}}(\varepsilon)$ from the perspective of graph percolation theory. We characterize networks into two categories – resilient and fragile – based on how large systemic shocks they can withstand and identify key indicators of resilience or fragility in networks. Additionally, we give systematic ways to calculate bounds on the resilience and show that, in fact, the underlying graph percolation problem has several important connections to the financial contagion and influence maximization literature. One of the results we believe is interesting for future work constitutes a deterministic linear programming formulation that can approximate (up to some error) the influence spread of the classical independent cascade model of Kempe, Kleinberg, and Tardos [236] when the transmission probability is sufficiently low. We believe that this observation can be used to design *approximate* influence maximization algorithms that do not rely on sampling cascades. Also, extending the model to a decentralized one where each entity/supplier acts strategically also constitutes an interesting research direction (see, e.g., related results in opinion dynamics [221, 243, 219]).

In Chapter 4, we study decentralized estimation and learning in the presence of privacy risks, develop algorithms for both continuous and discrete hypothesis spaces, quantify the cost of privacy in both cases, and apply them in real-world applications involving distributed measurements in sensor networks and distributed survival analysis. The algorithms presented in Chapter 4 are non-Bayesian in nature, and an interesting research direction would be to study the Bayesian analogs of these algorithms. So far, recent work has studied the problem of sequential learning [273], and it remains an open question whether similar results hold in the case of general networks, whereas the corresponding

decision-making problems may face computational complexity challenges (for instance, see earlier work in [198]). Another promising research direction would be to consider designing distributed black-box DP hypothesis tests. To this end, the black-box mechanism presented in [30] together with the optimal (in terms of convergence time) linear consensus algorithm given by [313] could constitute an interesting research direction in distributed DP hypothesis testing.

Then, in Chapter 5, we develop an axiomatic approach for core-periphery (higher-order) networks as well as inference algorithms to identify core-periphery structure in real-world large-scale networks such as networks taken from the Stack Exchange website [51], and the Microsoft Academic Graph. The general idea is that the core nodes in a network correspond to an almost dominating set of the network and that this core has a sublinear size, which is both proven theoretically and verified empirically. The statistical graph models we propose leverage sufficient statistics among collections of nodes to yield both realistic fits to real-world data as well as algorithms that run in $\widetilde{O}(n+m)$ time in realistic cases. The potential extensions of this work are multi-fold: First, on the algorithmic front, the core-periphery structure can be used to speed up several conventional network analysis tasks. For example, existing approaches such as [400, 49] have leveraged this algorithmic idea to perform betweenness centrality computation as well as uniform node sampling in very large networks. This idea has the potential to be adapted to several other tasks, such as influence maximization, ranking, and all-pairs shortest-path computation. On the modeling front, devising graph and hypergraph formation models that are both motivated from a theoretical network science standpoint and possess computational tractability are also interesting research directions (see, for example, the HyperKron model of [138]).

Finally, in Chapter 6, we study the network formation behavior of collectives of LLM agents, showing that several classical properties of network formation – such as preferential attachment, homophily, triadic closure, community structure, and small-world phenomenon – exist in such networks. We believe that this line of work offers several interesting future research avenues that could transform our understanding of complex systems by creating heterogeneous agents that mimic diverse human decision-making processes [327, 328]. This approach allows us to explore phenomena such as market dynamics, social network behavior, and information spread (see, e.g., [90]) and develop prototyping tools with LLMs that can have several applications for businesses and society.

Finally, using tools from the systemic risk and contagion literature, as my research has extensively done [322, 320, 324, 321], we can get a better understanding of how complex systems work. Modern AI systems are vastly interconnected as fine-tuned specialist models depend on general-purpose foundation models. This creates a complex AI supply chain, posing similar risks to physical and software supply chains. Foundation models are inherently different from foundational technologies such as 3D printing [245], open-source software systems [317], or physical chips, as these are human-built, whereas foundational AI models are trained. Just as disruptions can lead to cascading failures (e.g., modeled as errors due to fine-tuning), vulnerabilities in foundational AI models can propagate through the entire network of dependent applications. Ensuring these foundational models' security, robustness, and ethical integrity is crucial, as any flaws or biases can be magnified in the specialized models that rely on them. This interconnectedness underscores the need for developing new methods to analyze systemic risk and intervention strategies. Additionally, such collectives of foundation models are trained on sheer amounts of data, often col-

lectively via federated learning methods. Ensuring the privacy and accuracy trade-offs of these systems is crucial (cf. [325, 326]), and constitutes an interesting avenue for research.

All in all, complex networks are ubiquitous in our technological infrastructure, and modeling and reinforcing their resilience requires obtaining insights into their dynamics, structure, and the incentives of the autonomous agents participating in them, which requires the development of methods, scalable algorithms, and models.

APPENDIX A

CONTAGION AND RESOURCE ALLOCATION

A.1 Extended Related Work

Influence Maximization. While not directly related to financial networks, the allocation problem we study in this paper has very close ties to *Influence Maximization (IM)*. The work of [236] introduced the influence maximization problem as follows: given a network in which each edge can transmit information (e.g., disease, marketing information, etc.) with probability p independently of the other edges, the IM problem asks whether there exists a set S with $|S| = k$ such as the number of influenced nodes is maximized. Based on the submodularity properties of the influence function, the authors devise an $(1 - 1/e - o(1))$-approximation algorithm for approximating the optimal influence set. This work has been greatly extended by a series of works that optimize its algorithm (e.g., see [71, 187] and the references therein) and adapt it to different contexts (see, e.g., [264, 261, 100]). Another recent interesting work related to ours is the concept of *Fair Influence Maximization* studied in [397, 347], which discusses the maximization of influence subject of fairness constraints.

Income Shocks. The work of [2] studies subsidy allocations in the presence of income shocks where there is only temporal but no spatial information about the nodes. The analysis in their paper is based on *ruin processes*. It considers two main objectives: one is minimizing the expected number of nodes that are economically ruined (min-sum objective), and the other objective considers minimizing the worst ruin probability of a node in the network (min-max ob-

jective). As they mention in their paper, a crucial point that highlights income shocks at a societal level is that households have different abilities to withstand income shocks. The phenomenon disproportionately affects low-income families and can bring them into long-lasting poverty [124, 25, 366]. This Chapter can be seen as a part and extension of this work direction, which uses optimization methods for decision-making, and a possible combination of the model of both [2] and ours presents an interesting research pathway.

Financial Datasets & Network Reconstruction Algorithms. Another important component of the problem of financial contagion is the existence of financial datasets. It is well documented; see, e.g., [165, 144, 19, 404] (and the references therein), that financial network datasets are released in terms of aggregate liabilities (balance sheets). Namely, the form of the liability matrix is unknown, and only the column and row sums of the liability matrix are provided. To address this, mechanisms have been developed to generate synthetic liability networks out of balance sheet data [165, 103, 18, 349, 19, 403] by sampling and optimization methods.

A.2 Fairness Measures

Gini Coefficient. The Gini Coefficient [178] measures the fairness of the interventions between all pairs of nodes defined as

$$\text{Standard} - \text{GC}^{\text{asym}}(z(t)) = \frac{\sum_{i,j\in[n]} |z_j(t) - z_i(t)|}{2n \sum_{j\in[n]} z_j(t)} \qquad \text{(Standard-GC-Asym)}$$

$$\text{Standard} - \text{GC}^{\text{sym}}(z(t)) = \frac{\sum_{i,j\in[n]} |z_j(t) - z_i(t)|}{2(n-1) \sum_{j\in[n]} z_j(t)} \qquad \text{(Standard-GC-Sym)}$$

We note that a possible disadvantage of this metric is that it does not consider each node's debts, i.e., it treats all nodes on an equalized basis. This issue is mitigated by the Equation (Sp-GC-Asym) and Equation (Sp-GC-Sym) metrics, which are presented below.

Property Gini Coefficient. The collection of real-world data from SafeGraph and the US Census we present in Section 2.7.3 comprises the nodes' attributes. One of the key attributes in these datasets is the *minority status* of the owner of a business, if such business participates in the network as a node, or the demographic characteristics of a group of people, for instance, the fraction of people belonging to a minority group within a Census Block Group under which we want to impose fairness constraints. (That is, to measure the relative assistance between different groups, approximately).

This type of data motivates the following metric: We introduce the Property Gini Coefficient Equation (Prop-GC-Asym) in which nodes may have a *property* of interest (such as the demographic group in the SafeGraph or Census data) along which we want to apply an equity analysis. We model this by a *property vector* $q \in [0,1]^n$, where each element q_j corresponds to the probability that node $j \in [n]$ has this property. We can now construct the graph H with weights $w_{ji}(t) = q_j(1 - q_i)$, which yields the following two measures

$$\mathrm{PGC}^{\mathrm{asym}}(z(t); q) = \frac{\sum_{j,i\in[n]} q_j(1-q_i)|z_j(t) - z_i(t)|}{2\left(n - n_q\right) \cdot \sum_{j\in[n]} q_j z_j(t)} \tag{Prop-GC-Asym}$$

$$\mathrm{PGC}^{\mathrm{sym}}(z(t); q) = \frac{\sum_{j,i\in[n]} q_j(1-q_i)|z_j(t) - z_i(t)|}{\sum_{j\in[n]} z_j(t)(n_{\neg q} q_j + n_q(1-q_j))}. \tag{Prop-GC-Sym}$$

where $n_q = \sum_{j\in[n]} q_j$ and $n_{\neg q} = n - n_q$ are the total weights of the (soft) bipartition. Taking $q = \frac{1}{2}\cdot\mathbb{1}$ reduces Equation (Prop-GC-Asym) to the conventional GC. Moreover, for $L = \ell \cdot \mathbb{1}$ and $q^T z = 0$, we observe that Equation (Prop-GC-Asym) becomes unbounded since the denominator goes to zero. One case where this happens and further justifies the correctness of the criterion is when q and z are a $0/1$ vector and where the entries of q are 1, the entries of z are 0, and vice-versa, where the entries of q are 0 the entries of z are 1, which corresponds to giving all the interventions to the majority group. Other measures of disparity can be encoded as different notions of difference between groups, e.g. $w_{ji}(t) = |q_j - q_i|$, or $w_{ji}(t) = |q_j - q_i|\mathbb{1}\{a_{ji}(t) > 0\}$.

Spatial Gini Coefficient. To make the GC take into account network effects, we define its spatial analog, the Equation (Sp-GC-Asym), to be

$$\mathrm{SGC}^{\mathrm{asym}}(z(t); A(t)) = \frac{\sum_{(j,i)\in E} a_{ji}(t)|z_j(t) - z_i(t)|}{2\sum_{j\in[n]} \beta_j(t) z_j(t)}. \tag{Sp-GC-Asym}$$

The aforementioned definition also appears in [292], where the graph is assumed to have unit weights. In our case, the role of the unweighted graph plays the relative liability matrix A. Since A is substochastic, the total weight of each row is $\beta_{\max} < 1$, and the contribution of edge (i, j) is a_{ij}. Normalizing by the sum $\sum_{j\in[n]} \beta_j(t) z_j(t)$ allows for comparing different population groups and

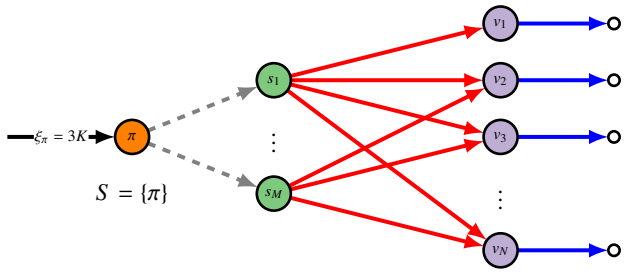


Figure A.1: NP-Hardness reduction. The green nodes correspond to the M set nodes; the purple nodes correspond to the N element nodes. The blue edges correspond to an external liability of 1, and the red edges correspond to the rationing amount of 1/3.

intervention magnitudes. When the interventions are distributed equally, the Equation (Sp-GC-Asym) is 0. If $A(t) = A^T(t)$ for all $t \in [T]$ and one node gets all the interventions, then the Equation (Sp-GC-Asym) is bounded by 1 in the asymmetric case. We note here that unlike Equation (Standard-GC-Asym), the Equation (Sp-GC-Asym) metric takes into account each node's debt, that is a node j with a significant (compared to its neighbors) liability to node i, i.e. it has $a_{ji}(t) \approx \beta_j(t)$. This deviation gets a higher weight in the coefficient calculation compared to j's deviation from the rest of its neighbors. The symmetric extension of Equation (Sp-GC-Asym) is given by

$$\text{SGC}^{\text{sym}}(z(t); A(t)) = \frac{\sum_{(j,i)\in E} a_{ji}(t)|z_i(t) - z_j(t)|}{\sum_{j\in[n]} \left(\sum_i (a_{ij}(t) + a_{ji}(t))\right) z_j(t)} \qquad \text{(Sp-GC-Sym)}$$

A.3 Proofs

A.3.1 Proof of Theorem 2.3.1

Proof. We construct a reduction (see Figure A.1) from the set cover with M sets, N elements, and set cover size K as follows

- We set $T = 1$.
- We create a bipartite graph with partitions X and Y.
- For each of the M sets we create vertices $s_1, \ldots, s_M$ in X.
- For each of the N elements we create vertices $v_1, \ldots, v_N$ in Y.
- For each element v belonging to a set s we create a directed edge (s, v) between the corresponding vertices in the graph.
- We create a source node π and create directed edges (π, s) for all $s \in X$, and set $S = \{\pi\}$.
- For all $s \in X$ and for all $v \in Y$ the element v belongs to the set s in the set cover problem, we set the entries of the liability matrix to $a_{sv} = \frac{1}{3}$.
- We set $\xi_\pi = 3K$, and set the assets to 0 elsewhere.
- We set $b_v = 1$ for all $v \in Y$, and set it to zero elsewhere.
- Finally, we set $D = K + N$, and $n = N + M + 1$.

The reduction runs in poly-time, creating a graph with $O(N + M)$ nodes and $O(N + M)$ edges.

($\Longrightarrow$) Assume that there's a set cover $\mathcal{J}$ of size K. Then we pick the set nodes $J \subseteq X$ corresponding to $\mathcal{J}$ and set $a_{\pi s} = \frac{1}{k}$. The source, K of the set nodes, are solvent, and all N elements are solvent. Therefore, the number of disagreements is now $K + N$.

($\Longleftarrow$) Assume that there exists a rationing scheme X such that there are at least $K + N$ disagreements. Then, if there exists any set J of K solvent nodes activated by the source for which, if its payments are proportionally rationed,

the number of disagreements is at least $K + N$, the 3-SET-COVER problem must be solvable.

□

A.3.2 Proof of Theorem 2.4.1

Proof. Base Case $t' = T$. Let f_T be the PDF of $U(T)$. We have that

$$
\begin{aligned}
V(T, s) &= \max_{\widetilde{z}\in\mathcal{Z}, \widetilde{p} \text{ fixed point given } \widetilde{z}} \langle f_T, \mathbb{1}^T \widetilde{p} \rangle \\
&= \max_{\widetilde{z}\in\mathcal{Z}} \int_{\mathcal{U}} f_T(u) \max_{\widetilde{p} \text{ fixed point given } \widetilde{z}} \mathbb{1}^T \widetilde{p}(u) du \\
&= \max_{\widetilde{z}\in\mathcal{Z}} \lim_{N\to\infty} \sum_{i=1}^{N} f(u_i)\Delta u_i \max_{\widetilde{p}(u_i) \text{ fixed point given } \widetilde{z}} \mathbb{1}^T \widetilde{p}(u_i) \\
&= \max_{\widetilde{z}\in\mathcal{Z}} \lim_{N\to\infty} \max_{(p(u_1)^T,\ldots,p(u_N)^T)^T \text{ fixed point given } (\widetilde{z}^T,\ldots,\widetilde{z}^T)^T} \sum_{i=1}^{N} f(u_i)\Delta u_i \sum_{j\in[n]} \widetilde{p}_j(u_i) \\
&= \lim_{N\to\infty} \max_{(p(u_1)^T,\ldots,p(u_N)^T)^T \text{ fixed point given } (\widetilde{z}^T,\ldots,\widetilde{z}^T)^T} \sum_{i=1}^{N} f(u_i)\Delta u_i \sum_{j\in[n]} \widetilde{p}_j(u_i) \\
&= \int_{\mathcal{U}} f_T(u) \max_{\widetilde{z}, \widetilde{p}(u)} \mathbb{1}^T \widetilde{p}(u) du \\
&= \mathbb{E}_{U(T)} \left[\max_{\widetilde{z}, \widetilde{p}} \mathbb{1}^T \widetilde{p} \right]
\end{aligned}
$$

The equalities follow from: (i) definition of expectation, (ii) pushing the maximization wrt s inside since z is fixed, (iii) definition of Riemannian integral, (iv) the N optimization problems being decoupled since z is fixed and thinking of the optimization as a large problem with a state vector of dimension $2 \times N \times n$, (v) pushing the optimization inside the limit (rewards are bounded regardless of the value of N and the corresponding mappings are continuous), (vi) definition

of integration, and (vii) definition of the expected value.

Inductive Hypothesis. Assume that for $t' = t + 1$ we have that

$$V(t+1, s_t) = \mathbb{E}_{U(t+1:T)}\left[\max_{\widetilde{z}_{t+1}, \widetilde{p}_{t+1}}\left\{\mathbb{1}^T\widetilde{p}_{t+1} + \max_{\widetilde{z}_{t+2}, \widetilde{p}_{t+2}}\left\{\mathbb{1}^T\widetilde{p}_{t+2} + \max_{\widetilde{z}_{t+3}, \widetilde{p}_{t+3}}\left\{\mathbb{1}^T\widetilde{p}_{t+3} + \dots\right\}\right\}\right\}\right]$$

Inductive Step. For $t' = t$ we have that

$$\begin{aligned}
V(t, s_t) &= \max_{z_t}\left\{r(s_t, z_t) + \mathbb{E}_{s_{t+1}\sim\mathcal{T}(s_t, z_t)}\left[V(t+1, s_{t+1})\right]\right\} \\
&= \max_{z_t}\mathbb{E}_{U(t)}\Bigg[\max_{\widetilde{p}_t}\mathbb{1}^T\widetilde{p}_t + \mathbb{E}_{U(t+1:T)}\left[\max_{\widetilde{z}_{t+1}, \widetilde{p}_{t+1}}\left\{\mathbb{1}^T\widetilde{p}_{t+1} + \max_{\widetilde{z}_{t+2}, \widetilde{p}_{t+2}}\left\{\mathbb{1}^T\widetilde{p}_{t+2} + \max_{\widetilde{z}_{t+3}, \widetilde{p}_{t+3}}\left\{\mathbb{1}^T\widetilde{p}_{t+3} + \dots\right\}\right\}\right\}\right]\Bigg] \\
&= \max_{z_t}\mathbb{E}_{U(t:T)}\Bigg[\max_{\widetilde{p}_t}\left\{\mathbb{1}^T\widetilde{p}_t + \max_{\widetilde{z}_{t+1}, \widetilde{p}_{t+1}}\left\{\mathbb{1}^T\widetilde{p}_{t+1} + \max_{\widetilde{z}_{t+2}, \widetilde{p}_{t+2}}\left\{\mathbb{1}^T\widetilde{p}_{t+2} + \max_{\widetilde{z}_{t+3}, \widetilde{p}_{t+3}}\left\{\mathbb{1}^T\widetilde{p}_{t+3} + \dots\right\}\right\}\right\}\right\}\Bigg] \\
&= \mathbb{E}_{U(t:T)}\left[\max_{\widetilde{z}_t, \widetilde{p}_t}\left\{\mathbb{1}^T\widetilde{p}_t + \max_{\widetilde{z}_{t+1}, \widetilde{p}_{t+1}}\left\{\mathbb{1}^T\widetilde{p}_{1+2} + \max_{\widetilde{z}_{t+2}, \widetilde{p}_{t+2}}\left\{\mathbb{1}^T\widetilde{p}_{t+2} + \dots\right\}\right\}\right\}\right]
\end{aligned}$$

The equalities follow from: (i) the HJB equations, (ii) the inductive hypothesis, (iii) the fact that the maximization over $\widetilde{p}_t$ is independent of the sample paths from round $t + 1$ onwards and thus we can reorganize the expectations into one expectation over sample paths $U(t : T) \sim \mathcal{U}$, (iv) identically to the base case argument.

Sample Complexity. At any point, with probability 1, the value functions $V_{u_i(t:T)}$ are between 0 and $\sum_t \mathbb{1}^T(b(t) + \ell(t)) \leq (T - t + 1) \cdot \Delta$, where $\Delta = \sup_{\mathcal{U}}(\|b\|_1 + \|\ell\|_1)$ since the maximum reward can be achieved when all debts are paid and all nodes are solvent. Thus, by standard Chernoff bounds, one

needs to choose $N = \frac{\log(2/\delta)(T-t+1)^2\Delta_u^2}{2\varepsilon^2}$ samples to get an ε-accurate estimation of the actual value function with probability at least $1-\delta$. □

Remarks on the Proof of Theorem 2.4.1.

First, note that the pair $(\tilde{p}(t), z(t))$ are sufficient for the state/action description of the MDP, and $p(t)$, which corresponds to the total accumulated liabilities is an auxiliary variable that one can compute from these using the definition of $p(t)$ (Equation (2.2)). This formulation has come up in past work; for example, Eq. 31 of [83].

Another important point of the above proof is how the structure of our problem allows us to interchange maximization and expectation operators and take expectation over the entire trajectory. This interchange is, of course, not true in general MDPs. What is critical in our formulation is the *maximal clearing* assumption Assumption 4), which effectively reduces the action space to only choosing interventions $z(t)$ since the clearing payments $\tilde{p}(t)$ are now completely specified, given $z(t)$ and all previous clearing payments, via the fixed-point equation of Assumption 4. The fixed-point formulation has an equivalent LP formulation where there is an optimization over *only* $z(t)$ and $\tilde{p}(t)$. The same approach is followed in prior works, e.g., on page 3 of [12], and Lemma 4 of [139], and can be applied here due to Assumption 4. Next, for a two-stage problem, we can interchange expectation and maximization and write the value function as nested LPs. We extend this to multiple stages via induction.

This is a subtle issue and is not without loss of generality since we are specifying a particular form of clearing payments via maximal clearing. In our con-

text, this provides a natural and interesting way that a behavioral assumption in the finance literature (simply that agents will clear liabilities as they arise to the extent possible) leads to tractable instances of dynamic optimization over multiple stages.

Proof of Corollary 2.4.2.

Corollary 2.4.2 is a direct consequence of the theorems discussed in Appendix A.4.

A.3.3 Proof of Theorem 2.5.1

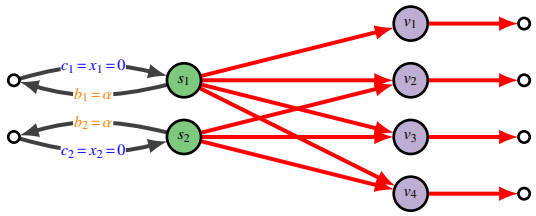


Figure A.2: Reduction Construction of Theorem 2.5.1 from 3-SET-COVER for two sets $s_1 = \{v_1, v_2, v_3\}$, $s_2 = \{v_2, v_3, v_4\}$, and four items $\{v_1, v_2, v_3, v_4\}$. Here $\alpha \in (0, 3)$. Red edges represent a liability of $1 - \alpha/3$.

Proof. We first start by designing a polynomial-time reduction from a 3-SET-COVER instance with n elements and m sets to an instance of the decision version of the Equation (AS) objective.

We set $T = 1$ and fix a constant $\alpha \in (0, 3)$. We create a bipartite network with a node set partitioned into X and Y where $X = \{s_1, \ldots, s_m\}$ is the node set that represents all the "set nodes" and $Y = \{v_1, \ldots, v_n\}$ is the node set that represents all the "item nodes" of the corresponding 3-SET-COVER instance. For each set

node s_j and each item v_i we add an edge (s_j, v_i) if and only if $v_i \in s_j$. We set the parameters of the EN model as follows. First, for each "set node", there is an external influx of $\xi_j = x_j = 0$, and an external outflux of $b_j = \alpha$. For each edge (s_j, v_i) created there is an obligation of $p_{ji} = 1 - \alpha/3$ from the set to the corresponding item. Thus $\beta_{\max} = 1 - \alpha/3 < 1$. Each item node has no external influx, i.e. $\xi_i = 0$, and has external liabilities of $b_i = 1 - \alpha/3$. We also take $L_j = 3$ for all $j \in [n]$, $B = 3k$ and $V^* = k + n$. After the shock, the influx of cash is disrupted, and all nodes default to having $\bar{p}_i = 0$; no one can meet its obligations. The reduction creates a network with $n + m$ nodes and $n + 4m$ edges and runs in polynomial time.

($\implies$) Suppose that $\mathcal{J}$ is a set cover with $|\mathcal{J}| = k$. Giving aid L to set nodes s_i such that $i \in \mathcal{J}$ we have that every "set node" in $\mathcal{J}$ becomes solvent since it can pay the obligations of $p_j = 3$ to the "item nodes", and the corresponding items that it covers become solvent themselves. Since $\mathcal{J}$ is a set cover, every item becomes solvent, and all the set nodes s_i for $i \notin \mathcal{J}$ remain the default. Hence we have a total of $k + n$ solvent nodes.

($\impliedby$) Suppose there are at least $V^* = k+n$ solvent nodes. Therefore, there are at most $d = m - k$ default nodes. Let $\mathcal{J} \subseteq X \cup Y$ be the set with $|\mathcal{J}| = k$ elements such that every element $j \in \mathcal{J}$ gets an aid of L. We will show that $\mathcal{J}$ is a subject of X. Suppose that $\mathcal{J}$ has ℓ elements on Y and $k - \ell$ elements on X. Then, the number of solvent nodes is at most $\ell + k - \ell + k - \ell = 2k - \ell$, and the number of default nodes is therefore at least $(n - k + \ell) + (m - k)$. For this to hold we must have that $n - k + \ell \leq 0$, which implies that $\ell = 0$. Therefore $\mathcal{J} \subseteq X$. Therefore, every item node is solvent; thus, $\mathcal{J}$ must be a set cover for the original problem. The budget constraint is also satisfied.

Equation (Lin-OBJ) *objective.* The reduction construction for the Equation (Lin-OBJ) problem is very similar: instead of letting $V^* = k + n$ we let $V^* = 3k + n$. Moreover, we let $v = \mathbb{1}$. □

A.3.4 Proof of Theorem 2.5.2

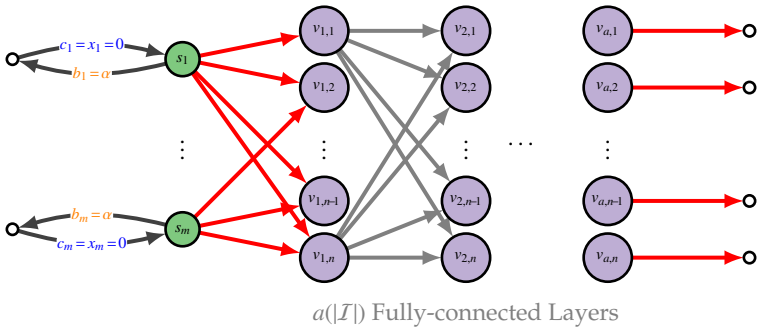


Figure A.3: Proof of Theorem 2.5.2 (see Appendix A.3 for the full proof). Here $\alpha \in (0, 3)$ and $a(|\mathcal{I}|) \in \mathbb{N}^*$ is a poly-time computable function of the input instance size $|\mathcal{I}|$. The red edges represent liabilities of value $1-\alpha/3$. Gray edges represent liabilities of value $\frac{1-\alpha/3}{n}$. The maximum financial connectivity is $\beta_{\max} = 1 - \alpha/3 < 1$. A YES answer to the 3-SET-COVER problem implies at least $k+a(|\mathcal{I}|)\cdot n$ solvent nodes, whereas a NO answer implies at most $k + n$ solvent nodes.

Proof. Let $a(|\mathcal{I}|) = \text{poly}(|\mathcal{I}|)$ be a poly-time computable function on the input size $|\mathcal{I}|$, and $\alpha \in (0, 3)$. We construct the same proof as the hardness reduction of Theorem 2.5.1 with the only change that instead of adding one copy of "element nodes" we add $a(|\mathcal{I}|)$ copies of "element nodes" resulting in a network with a polynomial number, i.e., $m + a(|\mathcal{I}|) \cdot n$, of nodes. We connect, with direction from left to right, the element nodes with liabilities $\frac{1-\alpha/3}{n}$ (i.e., a fully-connected network) and we set the external liabilities of the $a(|\mathcal{I}|)$-th level to be $1 - \alpha/3$. We distinguish the following cases: If the answer to the 3-SET-COVER problem is YES then there are at least $k + a(|\mathcal{I}|) \cdot n$ solvent nodes. Else, if the answer to the 3-SET-COVER problem is NO then there are at most $k + n$ solvent nodes.

That is, if we were able to distinguish between the Equation (AS) being between $k + n$ and $k + a(|\mathcal{I}|) \cdot n$ in polynomial time we will be able to solve the 3-SET-COVER in polynomial time, which is a contradiction assuming that P $\neq$ NP. The approximation gap is $\frac{k+n\cdot a(|\mathcal{I}|)}{k+n} \geq \frac{a(|\mathcal{I}|)\cdot n}{2n} = \frac{a(|\mathcal{I}|)}{2} = \Omega\left(a(|\mathcal{I}|)\right)$.

□

A.3.5 Proof of Theorem 2.5.3

Proof. We fix a sample path $u(t : T)$. We let $\bar{D}(t')$ and $\bar{R}(t')$ be the default and solvent nodes' sets under discrete interventions at round t'. We have that

1. If $j \in \bar{D}(t')$ we have that $\mathbb{E}_{\bar{z}(t:T)}\left[\bar{p}_j(t')|j \in \bar{D}(t'), u(1:T)\right] \geq c_j(t') - x_j(t') + \widetilde{z}^*_j(t')$.
2. If $j \in \bar{R}(t')$ we have that

$$
\begin{aligned}
\mathbb{E}_{\bar{z}(t:T)}\left[\bar{p}_j(t')|j \in \bar{R}(t'), u(t:T)\right] &= \mathbb{E}_{Z(t:T)}\left[p_{d,j}(t')|j \in \bar{R}(t'), u(1:T)\right] \\
&= \mathbb{E}_{\bar{z}(t:T)}\left[\sum_{t''<t'}(b_j(t'') + \ell_j(t'')) - \sum_{t''<t'}\bar{p}_j(t'')|u(1:T)\right] \\
&\geq \mathbb{E}_{\bar{z}(t:T)}\left[\sum_{t''<t'}(b_j(t'') + \ell_j(t'')) - \sum_{t''<t'}\widetilde{p}_j(t'')|u(t:T)\right] \\
&= \mathbb{E}_{\bar{z}(t:T)}\left[p_{r,j}(t')|u(t:T)\right] \\
&\geq \widetilde{p}^*_j(t') \\
&\geq (1 - \max_{i\in[n]}\widetilde{\beta}_i(t'))\widetilde{p}^*_j(t').
\end{aligned}
$$

The statement follows from: (i) definition of a solvent node in the rounded solution, (ii) recursively using the definition of $p_{d,i}(t'')$ for all $1 \leq t'' < t'$, (iii) point-wise optimality of the fractional clearing vector, (iv) definition

of the solvency constraint for the fractional relaxation, (v) feasibility of the fractional solution, (vi) $\max_{i\in[n]} \widetilde{\beta}_i(t') > 0$ by Assumption 3.

Moreover, we have that for every $S \subseteq [n]$, from Equation (2.2b) that

$$\left(1 - \max_{i\in S} \widetilde{\beta}_i(t')\right) \sum_{j\in S} \widetilde{p}^*_j(t') \leq \sum_{j\in S} \left(1 - \widetilde{\beta}_j(t')\right) \widetilde{p}^*_j(t) \leq \sum_{j\in S} \left[c_j(t') - x_j(t') + \widetilde{z}^*_j(t')\right]. \quad \text{(A.1)}$$

By letting $S = \bar{D}(t')$ on Equation (A.1) and since $\max_{i\in\bar{D}(t')} \widetilde{\beta}_i(t') \leq \max_{i\in[n]} \widetilde{\beta}_i(t')$ we have that

$$\left(1 - \max_{i\in[n]} \widetilde{\beta}_i(t')\right) \sum_{j\in D_d(t')} \widetilde{p}^*_j(t') \leq \sum_{j\in D_d(t')} \left[c_j(t') - x_j(t') + \widetilde{z}^*_j(t')\right].$$

Moreover,

$$p_{r,j}(t') \geq \widetilde{p}^*_j(t') \geq \left(1 - \max_{i\in[n]} \widetilde{\beta}_i(t')\right) \widetilde{p}^*_j(t')$$

the second inequality is due to feasibility, and the last inequality is because we multiply with a quantity strictly in $(0, 1)$. Therefore, we have that the expected reward of the rounded solution at time t' is at least $\left(1 - \max_{i\in[n]} \widetilde{\beta}_i(t')\right)$ the optimal reward, i.e

$$\mathbb{E}_{Z(t:T)}\left[R(s(t'), \bar{z}(t') = SOL)\right] \geq \left(1 - \max_{i\in[n]} \widetilde{\beta}_i(t')\right) \cdot R(s(t'), \bar{z}(t') = OPT) \quad \forall t' \in [t, T]$$

We sum over $t' \in [t, T]$ and have that

$$\begin{aligned}
\mathbb{E}_{\bar{z}(t:T)}\left[V^{SOL}_{u(t:T)}(t,s(t))\right] &= \sum_{t'\in[t,T]} \mathbb{E}_{\bar{z}(t:T)}\left[R(s(t'),\bar{z}(t')=SOL)\right] \\
&\geq \sum_{t'\in[t,T]} (1-\max_{i\in[n]}\widetilde{\beta}_i(t'))\cdot R(s(t'),\bar{z}(t')=OPT) \\
&\geq \min_{t\in[t,T]}(1-\max_{i\in[n]}\widetilde{\beta}_i(t'))\cdot \sum_{t'\in[t,T]} R(s(t'),\bar{z}(t')=OPT) \\
&= \left(1-\max_{t'\in[t,T],i\in[n]}\widetilde{\beta}_i(t')\right)\cdot V^{OPT}_{u(t:T)}(t,s(t)).
\end{aligned}$$

Taking expectation with respect to $u(t:T)$ and arrive to

$$\begin{aligned}
\mathbb{E}_{\bar{z}(t:T),u(t:T)}\left[V^{SOL}(t,s(t))\right] &\geq \mathbb{E}_{u(t:T)}\left[\left(1-\max_{t'\in[t,T]}\max_{i\in[n]}\widetilde{\beta}_i(t')\right)V^{OPT}_{u(t:T)}(t,s(t))\right] \\
&= \mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right] - \mathbb{E}_{u(t:T)}\left[\left|V^{OPT}_{u(t:T)}(t,s(t))\max_{t'\in[t,T]}\max_{i\in[n]}\widetilde{\beta}_i(t')\right|\right] \\
&\overset{\text{Hölder}}{\geq} \mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right] \\
&\quad - \mathbb{E}_{u(t:T)}\left[\left\|V^{OPT}_{u(t:T)}(t,s(t))\right\|_1\right]\sup_{u(t:T)}\max_{t'\in[t,T]}\max_{i\in[n]}\widetilde{\beta}_i(t') \\
&\overset{V^{OPT}\geq 0}{=} \mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right] \\
&\quad - \mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right]\sup_{u(t:T)}\max_{t'\in[t,T]}\max_{i\in[n]}\widetilde{\beta}_i(t') \\
&= \left(1-\sup_{u(t:T)}\left\{\max_{t'\in[t,T]}\max_{i\in[n]}\widetilde{\beta}_i(t')\right\}\right)\cdot\mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right] \\
&= \left(1-\widetilde{\beta}_{\max}\right)\cdot\mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right].
\end{aligned}$$

□

Simplification of approximation guarantee.

Having $B > \Delta_u$ implies that at each round all liabilities can be covered and therefore $p_i(t') = b_i(t') + \ell_i(t') \leq \Delta_u$, thus

$$\widetilde{\beta}_i(t') = 1 - \frac{b_i(t')}{p_i(t')} \leq 1 - \frac{\Delta_b}{\Delta_u} \implies \max_{t' \in [t,T], i \in [n]} \widetilde{\beta}_i(t') \leq 1 - \frac{\Delta_b}{\Delta_u},$$

Otherwise, it always holds that

$$\widetilde{\beta}_i(t') = 1 - \frac{b_i(t')}{p_i(t')} \leq 1 - \frac{\Delta_b}{(t' - t + 1)\Delta_u} \implies \max_{t' \in [t,T], i \in [n]} \widetilde{\beta}_i(t') \leq 1 - \frac{\Delta_b}{(T - t + 1)\Delta_u},$$

since $p_i(t')$ (generally) is maximized when no liabilities are cleared for every $t'' \in [t, t']$.

A.3.6 Proof of Theorem 2.5.4

Algorithm Description.

We consider a family of *greedy hill-climbing algorithms* for the AON bailouts in the static case to find an approximate bailout set for a linear objective $R_v = v^T \bar{p}$, where $v > 0$. The greedy algorithm selects the node with the maximum marginal gain and bails it out until the budget is exhausted. As we mention in the main text, the greedy algorithm achieves an optimal approximation guarantee of $1 - 1/e$ (see Theorem 2.5.4), whose proof we give below:

Proof of Approximation Guarantee

Proof. For convenience, let $\bar{p}^*(w)$ be the EN solution to a system with assets $w \geq 0$. We fix a sample path u and define the set function $h_u : 2^{[n]} \to \mathbb{R}_{\geq 0}$ to be the

value function if the set S is bailed out, i.e. $h_u(S) = v^T \bar{p}^*(c - x + L \odot \mathbb{1}_S)$. A direct consequence of [139] is that a system with pointwise higher assets has a larger clearing payment vector (point-wise); thus, h_u is monotonically increasing. In the sequel, we prove that h_u is submodular, i.e., for any two sets $S, T \subseteq [n]$, we have that $h_u(S \cup T) + h_u(S \cap T) \geq h_u(S) + h_u(T)$. We have that

$$
\begin{aligned}
h_u(S \cup T) + h_u(S \cap T) &= \sum_{j=1}^{n} v_j \bar{p}_j^*(c - x + L \odot \mathbb{1}_{S \cup T}) \\
&+ \sum_{j=1}^{n} v_j \bar{p}_j^*(c - x + L \odot \mathbb{1}_{S \cap T}) \\
&= \sum_{j=1}^{n} v_j \bar{p}_j^*(c - x + (L \odot \mathbb{1}_S) \vee (L \odot \mathbb{1}_T)) \\
&+ \sum_{j=1}^{n} v_j \bar{p}_j^*(c - x + (L \odot \mathbb{1}_S) \wedge (L \odot \mathbb{1}_T)) \\
&= \sum_{j=1}^{n} v_j \bar{p}_j^*((c - x + L \odot \mathbb{1}_S) \vee (c - x + L \odot \mathbb{1}_T)) \\
&+ \sum_{j=1}^{n} v_j \bar{p}_j^*((c - x + L \odot \mathbb{1}_S) \wedge (c - x + L \odot \mathbb{1}_T)) \\
&\overset{(*)}{\geq} \sum_{j=1}^{n} v_j \bar{p}_j^*(c - x + L \odot \mathbb{1}_S) + \sum_{j=1}^{n} v_j \bar{p}_j^*(c - x + L \odot \mathbb{1}_T) \\
&= h_u(S) + h_u(T).
\end{aligned}
$$

whereas the (*) step is due to Proposition A.7 of [40]. Taking expectations over sample paths $u \sim \mathcal{U}$ in the above expression shows that the value function $\mathbb{E}_u[h_u(\cdot)]$ is monotone and submodular. Therefore the results of [302] yield an $\left(1 - \frac{1}{e}\right)$-approximation guarantee. Moreover, the guarantee is optimal unless $P = NP$ [151].

□

Expectation via Samples. The evaluation of $\mathbb{E}_u[h_u(\cdot)]$ is done via independently sampling a number of sample paths $u_1, \ldots, u_N$, apply the approximation algorithm N times and then calculate the empirical mean. The approximation guarantee becomes $1 - 1/e - o(1)$.

A.3.7 Extension to Include Bankruptcy Costs (Theorem 2.5.5)

Value Function.

Similarly to Theorem 2.4.1, we can show that if the agents respond maximally with the RV clearing vector of Equation (RV-model), then the value function for the RV model can be calculated as

$$V^{RV}(t,s) = \mathbb{E}_{U(t:T)}\left[\max_{\widetilde{z}_t,\widetilde{p}_t,\bar{y}_t}\{\mathbb{1}^T\widetilde{p}_t + \max_{\widetilde{z}_{t+1},\widetilde{p}_{t+1},\bar{y}_{t+1}}\{\mathbb{1}^T\widetilde{p}_{t+1} + \max_{\widetilde{z}_{t+2},\widetilde{p}_{t+2},\bar{y}_{t+2}}\{\mathbb{1}^T\widetilde{p}_{t+2} + \ldots\}\}\}\right]$$

whereas the constraints obey Equation (RV-model), $\widetilde{p}(t:T)$ and $\widetilde{z}(t:T)$ are fractional, and $\bar{y}(t:T)$ is discrete (cf. [22]). Relaxing the value of $\bar{y}(t:T)$ to be fractional we obtain the relaxation

$$V^{REL}(t,s) = \mathbb{E}_{U(t:T)}\left[\max_{\widetilde{z}_t,\widetilde{p}_t,\widetilde{y}_t}\{\mathbb{1}^T\widetilde{p}_t + \max_{\widetilde{z}_{t+1},\widetilde{p}_{t+1},\widetilde{y}_{t+1}}\{\mathbb{1}^T\widetilde{p}_{t+1} + \max_{\widetilde{z}_{t+2},\widetilde{p}_{t+2},\widetilde{y}_{t+2}}\{\mathbb{1}^T\widetilde{p}_{t+2} + \ldots\}\}\}\right]$$

whereas $V^{REL}(t,s) \geq V^{RV}(t,s)$ for all t and s.

A.3.8 Proof of Theorem 2.5.5.

Proof. The proof proceeds similarly to Theorem 2.5.3: Specifically, we fix a sample path $u(t:T)$, and let $\bar{D}(t'), \bar{R}(t')$ be the sets of default and solvent nodes under the discrete interventions.

If $j \in \bar{D}(t')$ we have that $\mathbb{E}_{\tilde{z}(t:T)}\left[\bar{p}_j(t') | j \in \bar{D}(t'), u(t:T)\right] \geq \kappa_c[c_j(t') - x_j(t') + \widetilde{z}_j^*(t')]$. Moreover, for the relaxation solution we have, due to Equation (RV-model), that

$$\begin{aligned}\widetilde{p}_j^*(t') &\leq \kappa_A \sum_{i\in[n]} a_{ij}(t')\widetilde{p}_i^*(t') + \kappa_c(c_j(t') - x_j(t') + \widetilde{z}_j^*(t')) + p_j(t)\widetilde{y}_i(t') \\ &\leq (1+\kappa_A)\sum_{i\in[n]} a_{ij}\widetilde{p}_i^*(t') + (1+\kappa_c)(c_j(t') - x_j(t') + \widetilde{z}_j^*(t')).\end{aligned}$$

Summing over $\bar{D}(t')$ we get that

$$\begin{aligned}\frac{\kappa_c}{1+\kappa_c}\left[1 - (1+\kappa_A)\max_{i\in\bar{D}(t')}\widetilde{\beta}_i(t')\right]\sum_{j\in\bar{D}(t')}\widetilde{p}_j^*(t') &\leq \kappa_c \sum_{j\in\bar{D}(t')}(c_j(t') - x_j(t') + \widetilde{z}_j^*(t')) \\ &\leq \sum_{j\in\bar{D}(t')}\bar{p}_j^*(t')\end{aligned}$$

If $j \in \bar{R}(t')$, similarly to Theorem 2.5.3, we can show that

$$\mathbb{E}_{\tilde{z}(t:T)}\left[\bar{p}_j(t') | j \in \bar{R}(t'), u(t:T)\right] \geq \widetilde{p}_j^*(t') \geq \frac{\kappa_c}{1+\kappa_c}\left[1 - (1+\kappa_A)\max_{i\in[n]}\widetilde{\beta}_i(t')\right]\widetilde{p}_j^*(t').$$

We then proceed exactly as in Theorem 2.5.3, and arrive at the guarantee

$$\mathbb{E}_{\tilde{z}(t:T),u(t:T)}\left[V^{SOL}(t,s(t))\right] \geq \frac{\kappa_c}{1+\kappa_c}\left[1 - (1+\kappa_A)\widetilde{\beta}_{\max}\right]\mathbb{E}_{u(t:T)}\left[V^{OPT}(t,s(t))\right].$$

Note that the approximation guarantee is valid for all $\kappa_c \in [0,1)$ and $\kappa_A \in \left[0, \min\{1/\widetilde{\beta}_{\max} - 1\}\right)$.

□

A.3.9 Proof of Theorem 2.6.2

Proof. Let $\widetilde{z}^*(1:T)$ (resp. $\bar{z}^*(1:T)$ be the optimal fractional (resp. discrete) policy without fairness and let $\widetilde{z}'(1:T)$ (resp. $\bar{z}'(1:T)$) be the optimal fractional (resp. discrete) policy with imposing a fairness constraint $g(1:T)$. Let $V(1,s)$ and $V'(1,s)$ be the corresponding value functions. The PoF is defined as PoF = $V(1,s)/V'(1,s)$.

Discrete Bailouts. We start by proving that there exist instances where the discrete PoF is unbounded. We will give the proof of the symmetric fairness case (the same holds for the asymmetric fairness case). Consider any financial network G with $x(t) = \xi(t) = 0$, $b(t) = \mathbb{1}$, $B = 1$, $L(t) = \mathbb{1}$. Pick any measurement network $H(t)$ with weights $w_{ij}(t)$ and any fairness constraint $g(t)$ such that $0 < g(t) < 1$ (notice the strict inequality).

For each step, if no fairness is considered, the planner bailouts one node in the optimal solution, which has a liability of 1 to the external sector, and, therefore $V(1,s) \geq T$.

When fairness is considered, the planner has two options:

- Bailout exactly one node, where the Gini coefficient will be $1 > g(t)$.
- Do not bailout any node, at which case the fairness constraint yields $0 \leq g(t) \times 0$ that is always true. This solution yields $V'(1,s) = 0$ which implies that $V(1,s)/V'(1,s)$ is unbounded.

Fractional Bailouts. For simplicity, we will give the proof when $T = 1$ as the proof for a general horizon can be easily proven with induction. We will

assume, without loss of generality, that the reward function R equals 0 when $\widetilde{p}(t) = 0$, as we can always translate the reward function to have value 0 at $\widetilde{p}(t) = 0$. We will prove the claim's correctness for the symmetric and asymmetric fairness measures.

Fix some $g(t) \geq 0$. We use the notation $\widetilde{p}'(t)$ to denote the value of the clearing payments, assuming a bound $g(t)$ on fairness.

Assume, for contradiction, that the PoF is unbounded. The following can happen:

- $V'(1, s) \neq 0$ and $V(1, s)$ grows such that $V(1, s)/V'(1, s) \to \infty$. This is a contradiction since the reward function is bounded by $f(n, T, \Delta)$, and therefore, the value function is bounded by $T f(n, T, \Delta) < \infty$ for finite T.
- $V'(1, s) = 0$. Since the rewards are non-negative, this happens if and only if $R(t) = 0$ for all $t \in [T]$. Since R is strictly increasing with $R(p'(t) = 0) = 0$ then $\widetilde{p}'(t) = 0$. We will show that $\widetilde{p}'(t) = 0$ if and only if $c(t) - x(t) = 0$ and $\widetilde{z}'(t) = 0$. We remind here that there are no isolated nodes (to the internal or the external sector) and hence $p'(t) > 0$. The ($\implies$) direction is trivial since the fairness constraint is always satisfied (hence it does not affect the feasible region) and the fixed point operator is $\Phi_t(\widetilde{p}'(t)) = p'(t) \wedge (A'^T(t)\widetilde{p}'(t))$, so $\Phi_t(0) = p'(t) \wedge 0 = 0$, i.e. $\widetilde{p}'(t) = 0$. For the ($\impliedby$) direction, since $p'(t) > 0$ the only way for $\widetilde{p}'(t)$ to be 0 is (i) $g(t) = B(t) = 0$ which is impossible since (i) if $B(t) > 0$ since $W(t) > 0$, and (ii) the relative liability non-homogeneous part is zero, i.e., $(c(t) - x(t)) + \widetilde{z}'(t) = 0$ (the fairness constraint is trivially satisfied). Since $c(t) - x(t) \geq 0$, $L(t) > 0$ and $\widetilde{z}'(t) \geq 0$, the only way for the equation to hold is $c(t) - x(t) = 0$ with probability 1 and $\widetilde{z}'(t) = 0$, yielding a contradiction. Therefore, $R(\widetilde{p}'(t)) > 0$ and subsequently $V'(1, s) < \infty$,

therefore the PoF is bounded by a function $M(n, T, \Delta)$.

□

A.4 General Response Dynamics

In this Section, we study the dynamic model's dynamics when agents can respond with any feasible vector (not necessarily a fixed point as Assumption 4 implies) satisfying Equation (2.2). We restate the optimization problem again, for simplicity, for a given sample path $u(1:T)$.

$$\max_{\widetilde{p}(1:T),\widetilde{z}(1:T)} \quad \sum_{t\in[T]} \mathbb{1}^T \widetilde{p}(t) \tag{A.2a}$$

$$\text{s.t.} \quad 0 \le \widetilde{p}(t) \le p(t) \quad \forall t \in [T] \tag{A.2b}$$

$$\widetilde{p}(t) \le A^T(t)\widetilde{p}(t) + c(t) + -x(t) + \widetilde{z}(t) \quad \forall t \in [T] \tag{A.2c}$$

$$c(t) = \xi(t) + c(t-1) - x(t-1) + \widetilde{z}(t-1) + A^T(t-1)\widetilde{p}(t-1) - \widetilde{p}(t-1) \forall t \in [T] \tag{A.2d}$$

$$0 \le \widetilde{z}(t) \le L(t) \quad \forall t \in [T] \tag{A.2e}$$

$$\mathbb{1}^T \widetilde{z}(t) \le B(t) \quad \forall t \in [T] \tag{A.2f}$$

$$B(t) = W(t) + B(t-1) - \mathbb{1}^T \widetilde{z}(t-1) \quad \forall t \in [T] \tag{A.2g}$$

$$p(t) = b(t) + \ell(t) + p(t-1) - \widetilde{p}(t-1) \quad \forall t \in [T] \tag{A.2h}$$

$$p_{ji}(t) = \ell_{ji}(t) + p_{ji}(t-1)\left(1 - \frac{\widetilde{p}_j(t-1)}{p_j(t-1)}\right) \quad \forall j, i \in [n] \forall t \in [T] \tag{A.2i}$$

$$a_{ji}(t) = p_{ji}(t)/p_j(t) \quad \forall j, i \in [n], \forall t \in [T] \tag{A.2j}$$

A.4.1 Convexity

We investigate conditions under which Equation (A.2) corresponds to a convex program. Firstly, all the constraints and the objective are convex concerning $\widetilde{z}(1:T)$. The objective is also convex in $\widetilde{p}(1:T)$. The solvency constraints (Equation (A.2b)) are convex with respect to $\widetilde{p}(1:T), \widetilde{z}(1:T)$. For the default constraints (Equations (A.2c) and (A.2d)), we let $\varphi_{ij}(t) = a_{ij}(t)\widetilde{p}_i(t)$ and $g_j(t) = \widetilde{p}_j(t) - \sum_{i\in[n]} \varphi_{ij}(t) - c(t) + x(t) - \widetilde{z}(t)$. Note that if $-\varphi_{ij}(t)$ are convex for all $j, i \in [n]$ and $t \in [T]$, then Equations (A.2c) and (A.2d) are also convex, and vice versa. All other second derivatives are zero since $\varphi_{i_1 j}(t)$ is independent from $\varphi_{i_2 j}(t)$ for all $i_1 \neq i_2$. The Hessian of $-\varphi_{ij}(t)$ equals:

$$\nabla^2 \varphi_{ij}(t) = \begin{pmatrix} -\frac{\partial \varphi_{ij}^2(t)}{\partial \widetilde{p}_i(t)^2} & -\frac{\partial \varphi_{ij}^2(t)}{\partial \widetilde{p}_i(t)\partial \widetilde{p}_i(t-1)} \\ -\frac{\partial \varphi_{ij}^2(t)}{\partial \widetilde{p}_i(t-1)\partial \widetilde{p}_i(t)} & -\frac{\partial \varphi_{ij}^2(t)}{\partial \widetilde{p}_i(t-1)^2} \end{pmatrix} = \begin{pmatrix} 0 & -\frac{a_{ij}(t)-a_{ij}(t-1)}{p_i(t)} \\ -\frac{a_{ij}(t)-a_{ij}(t-1)}{p_i(t)} & -\frac{2\widetilde{p}_j(t)(a_{ij}(t)-a_{ij}(t))}{\widetilde{p}_i(t)^2} \end{pmatrix} \tag{A.3}$$

The leading principal minors are $\Delta_1 = 0$, and $\Delta_2 = -\frac{(a_{ij}(t)-a_{ij}(t-1))^2}{p_i^2(t)} \leq 0$. In order to make $-\nabla^2 \varphi_{ij}(t) \geq 0$ we should make the leading principal minors of $-\nabla^2 \varphi_{ij}(t)$ non-negative. For this to happen, we should set $\Delta_2 = 0$ (since we require it to be ≥ 0 for positive semi-definiteness and $\Delta_2 \leq 0$ by Equation (A.3)). This requires setting $a_{ij}(t)$ to be some constant $\zeta_{ij} \in [0, 1)$ for all $t \in [T]$. Therefore the necessary and sufficient condition for convexity of the dynamics is that for every $j \in [n], t \in [T]$

$$a_{ij}(t) = \zeta_{ij}\ \forall i \in [n] \iff -\nabla^2 \varphi_{ij} \geq 0 \iff \nabla^2 g_j(t) \geq 0 \iff g_j(t) \text{ is convex.}$$

A.4.2 A Necessary and Sufficient Condition for Convexity

We restrict $A(t)$ to be some constant row sub-stochastic matrix $\Im$ with entries $\zeta_{ji} \in [0, 1)$ for all $t \in [T]$. This yields the following assumption and the following Condition and Theorem:

Assumption 5. *The financial environment* $U(t) = (b(t), c(t), \{\ell_j i(t)\}_{i,j\in[n]})$ *is a Markov Chain subject to the constraint that* $\frac{\ell_{ji}(t)}{b_j(t)+\sum_{k\in[n]}\ell_{jk}(t)}$ *is constant for all* $j, i \in [n]$ *and* $t \in [T]$. *Equivalently the internal and external instantaneous liabilities are samples from the polytope* $\mathcal{K} = \{(b, \{\ell_{ji}\}_{j,i\in[n]}) \in \mathbb{R}^{3n} : \zeta_{ji} + \sum_{k\in[n]}(\zeta_{ji} - \mathbb{1}\{k = j\})\ell_{ji} = 0, \forall j, i \in [n]\}$

Which yields Theorem A.4.1,

Theorem A.4.1 (Necessary and Sufficient Condition for Convexity)**.** *If for every* $j, i \in [n]$ *the quantity* $\frac{\ell_{ji}(t)}{b_j(t)+\sum_{k\in[n]}\ell_{jk}(t)}$ *is constant and equal to* $0 \leq \zeta_{ji} < 1$ *for a (row)-substochastic matrix* $\Im = \{\zeta_{ij}\}_{j,i\in[n]}$*, if and only if Equation* (A.2) *corresponds to a convex program. Moreover, under Theorem A.4.1, calculating the value function corresponds to solving an one-shot LP at the terminal time.*

Proof. For all $j, i \in [n]$ and $t \in [T]$ we have that

$$
\begin{aligned}
p_{ji}(t) &= \zeta_{ji} p_j(t) && \iff \\
\ell_{ji}(t) + p_{ji}(t-1)\left(1 - \frac{\widetilde{p}_j(t-1)}{p_j(t-1)}\right) &= \zeta_{ji}\left(b_j(t) + \ell_j(t) + p_j(t-1) - \widetilde{p}_j(t-1)\right) && \iff \\
\ell_{ji}(t) + \zeta_{ji} p_i(t-1)\left(1 - \frac{\widetilde{p}_j(t-1)}{p_j(t-1)}\right) &= \zeta_{ji}\left(b_j(t) + \ell_j(t) + p_j(t-1) - \widetilde{p}_j(t-1)\right) && \iff \\
\ell_{ji}(t) + \zeta_{ji} p_j(t-1) - \zeta_{ji}\widetilde{p}_j(t-1) &= \zeta_{ji}\left(b_j(t) + \ell_j(t) + p_j(t-1) - \widetilde{p}_j(t-1)\right) && \iff \\
\ell_{ji}(t) &= \zeta_{ji}\left(b_j(t) + \ell_j(t)\right) && \iff \\
\frac{\ell_{ji}(t)}{b_j(t) + \sum_{k\in[n]} \ell_{jk}(t)} &= \zeta_{ji}.
\end{aligned}
$$

The LP to calculate the value function for a fixed sample path $u(1:T)$ that corresponds to Equation (A.2) is:

$$
\begin{aligned}
V_{u(1:T)}(1, s) = \max_{\widetilde{p}(1:T), \widetilde{z}(1:T)} \quad & \sum_{t\in[T]} \mathbb{1}^T \widetilde{p}(t) && \text{(A.4a)} \\
\text{s.t.} \quad & \sum_{t'\le t} \widetilde{p}(t') \le \sum_{t'\le t} (b(t) + \ell(t)) && \forall t \in [T] \\
& && \text{(A.4b)} \\
& 0 \le \widetilde{p}(t) \le \mathcal{J}^T \widetilde{p}(t) + c(t) - x(t) + \widetilde{z}(t) && \forall t \in [T] \\
& && \text{(A.4c)} \\
& c(t) = \xi(t) + c(t-1) - x(t-1) + \widetilde{z}(t-1) + \mathcal{J}^T \widetilde{p}(t-1) - \widetilde{p}(t-1) && \forall t \in [T] \\
& && \text{(A.4d)} \\
& 0 \le \widetilde{z}(t) \le L(t) && \forall t \in [T] \\
& && \text{(A.4e)} \\
& \mathbb{1}^T \widetilde{z}(t) \le B(t) && \forall t \in [T] \\
& && \text{(A.4f)} \\
& B(t) = W(t) + B(t-1) - \mathbb{1}^T \widetilde{z}(t-1) && \forall t \in [T] \\
& && \text{(A.4g)}
\end{aligned}
$$

By defining the prefix variables $\widetilde{p}_c(t), \widetilde{z}_c(t), p_c(t), \xi_c(t), x_c(t), W_c(t), L_c(t)$ (i.e.

$\widetilde{p}_c(t) = \sum_{t' \le t} \widetilde{p}(t')$, etc.) we can rewrite the above problem as

$$V_{u(1:T)}(1, s) = \max_{\widetilde{p}_c(1:T), \widetilde{z}_c(1:T)} \quad \mathbb{1}^T \widetilde{p}_c(T) \tag{A.5a}$$

$$\text{s.t.} \quad \widetilde{p}_c(t) \le p_c(t) \qquad \forall t \in [T] \tag{A.5b}$$

$$0 \le \widetilde{p}_c(t) \le \mathcal{Z}^T \widetilde{p}_c(t) + \xi_c(t) - x_c(t) + \widetilde{z}_c(t) \qquad \forall t \in [T] \tag{A.5c}$$

$$0 \le \widetilde{z}_c(t) \le L_c(t) \qquad \forall t \in [T] \tag{A.5d}$$

$$\mathbb{1}^T \widetilde{z}_c(t) \le W_c(t) - \mathbb{1}^T z_c(t-1) \qquad \forall t \in [T] \tag{A.5e}$$

The above problem is equivalent to solving a one-step allocation problem at the terminal time T in a graph with Tn vertices. To approximate $V(1, s)$ with accuracy ε with probability at least $1 - \delta$ we need to average $N = \frac{\log(2/\delta)\Delta_u^2 T^2}{2\varepsilon^2}$ such sample paths.

□

A.4.3 Optimality of the Myopic (Sequential) Policy under Assumption 5

The sequential/myopic policy solves the contagion problem at each round t and then supplies the solution to round $t + 1$, and so on. Below we prove that under Assumption 5 and Theorem A.4.1 the myopic policy is in fact the globally

optimal one

Theorem A.4.2. *Under Assumption 5 the myopic policy is globally optimal for Equation (A.4), i.e. for all $t \in [T]$ the reward accumulated from time t onwards (for the myopic policy) for every $\widetilde{p}(1:t-1), \widetilde{z}(1:T-1)$ equals*

$$\max_{\widetilde{p}(t:T), \widetilde{z}(t:T)} \quad \sum_{t' \geq t} \mathbb{1}^T \widetilde{p}(t')$$
$$\text{s.t.} \quad \textit{Equation (A.4) constraints}$$

Subsequently, for $t = 1$ we get that the optimal policy can be found by solving Equation (A.4).

Proof. Fix some sample path $u(1 : T)$ obeying Assumption 5. Then define the value function at which the environment responds myopically, i.e. in a way that maximizes its reward from round t onwards, that is $V^{\flat}(t) = \max_{\widetilde{p} \text{ feasible clearing vector}} \max_{z \in \mathcal{Z}} \left\{ \mathbb{1}^T \widetilde{p} + V^{\flat}(t+1) \right\}$. In our case, for $t' \geq T$ we have that $V^{\flat}(t') = 0$. For $t' = T$ we have that for all $\widetilde{p}(1 : T-1), \widetilde{z}(1 : T-1)$

$$V^{\flat}(T) = \max_{\widetilde{p}(T)} \max_{\widetilde{z}(T)} \mathbb{1}^T \widetilde{p}(T) \overset{\text{LP}}{=} \max_{\widetilde{p}(T), \widetilde{z}(T)} \mathbb{1}^T \widetilde{p}(T)$$
$$\text{s.t.} \quad \text{Equation (A.4) constraints}$$

Now assume that for $t' = t + 1$ and for all $\widetilde{p}(1 : t), \widetilde{z}(1 : T)$ that

$$V^{\flat}(t+1) = \max_{\widetilde{p}(t+1:T),\widetilde{z}(t+1:T)} \sum_{t' \geq t+1} \mathbb{1}^T \widetilde{p}(t')$$

s.t. Equation (A.4) constraints

For $t' = t$ and for all $\widetilde{p}(1:t-1), \widetilde{z}(1:t-1)$ the value function of the myopic equals

$$\begin{aligned}
V^{\flat}(t) &= \max_{\widetilde{p}(t)} \left\{ \max_{\widetilde{z}(t)} \mathbb{1}^T \widetilde{p}(t) + V^{\flat}(t+1) \right\} \\
&\overset{\text{Inductive Hypothesis}}{=} \max_{\widetilde{p}(t)} \left\{ \max_{\widetilde{z}(t)} \mathbb{1}^T \widetilde{p}(t) + \max_{\widetilde{p}(t+1:T),\widetilde{z}(t+1:T)} \sum_{t' \geq t+1} \mathbb{1}^T \widetilde{p}(t') \right\} \\
&\overset{\text{LP}}{=} \max_{\widetilde{p}(t)} \max_{\widetilde{z}(t:T),\widetilde{p}(t+1:T)} \sum_{t' \geq t} \mathbb{1}^T \widetilde{p}(t) \\
&\overset{\text{LP}}{=} \max_{\widetilde{p}(t:T),\widetilde{z}(t:T)} \sum_{t' \geq t} \mathbb{1}^T \widetilde{p}(t)
\end{aligned}$$

s.t. Equation (A.4) constraints

We have merged the maximizations because the objective functions and constraints are linear (and separable). Recursing to $t = 1$ we get that $V^{\flat}(1) \equiv$ Equation (A.4). □

A.5 Dataset Information

Online Financial Network (Venmo transaction data). The dataset is split into three distinct periods: (i) July 2018 to September 2018 (3.8M transactions), October 2018 (3.2M transactions) January 2019 to February 2019 (167K transactions).

For our experiments, we used the first period (July 2018 to September 2018) as it was the period with the most transactions. We generate the random instances as follows:

- The timestamps are grouped every week according to which year and week of the year they correspond to.
- For the whole dataset (corresponding to the July-September 2018 period), we create two sets: V_1 and V_2. V_1 corresponds to the top 100 nodes in the number of incoming transactions, and V_2 corresponds to the top 100 nodes in the number of outgoing transactions. We use $V = V_1 \cup V_2$ as the vertex set.
- We count the transactions between nodes of V and the transactions from V to the outside system and from V to the inside system for each round (week of the year 2018). For nodes with zero outgoing transactions, we add one transaction.
- We create random liabilities as follows

$$\begin{aligned}
\ell_{ji}(t) &= \mathbb{1}\{\#\text{ of transactions } j \to i \text{ at round } t \text{ is } > 0\} \\
&\quad \times \text{Gamma}(\#\text{ of transactions } j \to i \text{ at round } t, 1) && \forall j, i \in [n], t \in [T], \\
b_j(t) &= \max\{1, \text{Gamma}(\#\text{ of transactions from } j \text{ to outside}, 1)\} && \forall j \in [n], t \in [T], \\
\xi_j(t) &= \mathbb{1}\{\#\text{ of transactions from outside to } j \text{ is } > 0\} \\
&\quad \times \text{Gamma}(\#\text{ of transactions from outside to } i, 1) && \forall i \in [n], t \in [T] \\
X_i(t) &= 0 && \forall i \in [n], t \in [T].
\end{aligned}$$

Note that for $b_i(t)$, we assert a *positive* value for Assumption 3 to hold.

Non-financial Allocation Network (Extra dispatches in ridesharing). The TLC data[1] are split into periods, with each entry containing the start time of a ride and its source and destination location IDs (corresponding to *zones*, e.g., Washington Heights, East Harlem, etc.). We build a temporal network for Manhattan: nodes in the graph are rides between zones, and the rest of the rides (to and from other boroughs) belong to the external network. We set the shocks to zero. The period is January 2021, and the $T = 31$ rounds correspond to different days. The edge weights (instantaneous liabilities) are determined by the number of rides requested from one zone to another (or to and from the external network). The statistics of the dynamic network are shown in Figure A.4

Physical Financial Network (see Figure A.5) ($T = 6$). Data generated based on mobility data from the SafeGraph platform during April 2020. The nodes in the financial network represent *(i)* Points of Interest nodes (POI nodes) that represent various businesses categorized by their *NAICS codes*[2] to categories (i.e., grocery stores, banks, gas stations, etc.) and the Census Block Group[3] (CBG) they are located at *(ii)* CBG nodes that represent a set of households in a certain location. The dataset is constructed by access to an initial pair of geographical coordinates (i.e., latitude and longitude) and a number k_{kNN} of neighboring CBGs. The POI nodes are determined to be the businesses located in the k_{kNN}-nearest neighboring CBGs based on the Haversine distance metric. Each POI provides data about the CBGs of its unique visitors[4] and the dwell times. For

[1] We obtained the data here: https://www1.nyc.gov/site/tlc/about/tlc-trip-record-data.page

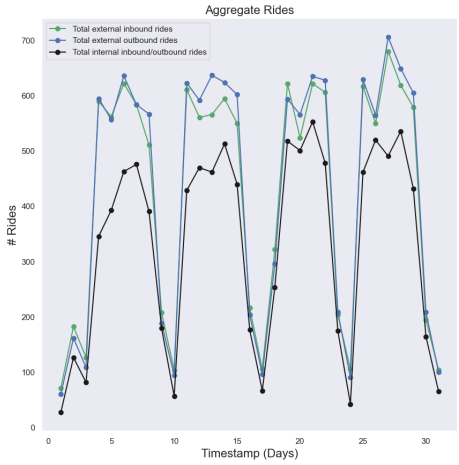
[2] https://www.naics.com/search

[3] A CBG is a unit used by the US Census. It is the smallest geographical unit for which the bureau publishes sample data, i.e., data which is only collected from a fraction of all households and contains 600-3K people.

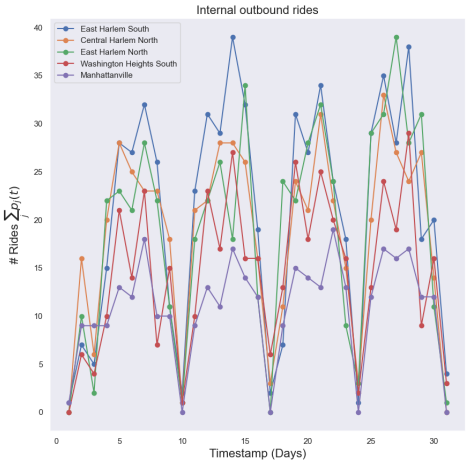
[4] A unique visitor is a unique mobile device, i.e., each device is only counted once. We assume that each device represents a distinct person.

the source of its visitors, we estimate the number of people who come from each CBG. From the *dwell times* of available devices, we determine the percentage of people who work on the POIs and the ones who visit the POIs. For the former category, we create a financial liability edge from the POI to the CBG node to indicate the payment of liability (i.e., a wage). For the latter category, we create a liability edge from the CBG node to the POI representing some form of expense (e.g., groceries). The weights are multiplied accordingly to represent the people interacting with each POI. The aforementioned process creates a bipartite network. Each CBG node is associated with multiple data from the US Census, and every POI node is associated with data from the US Economic Census. For each CBG node, we estimate the average size of households per CBG, the average income level and the percentage of people that belong to a minority group.

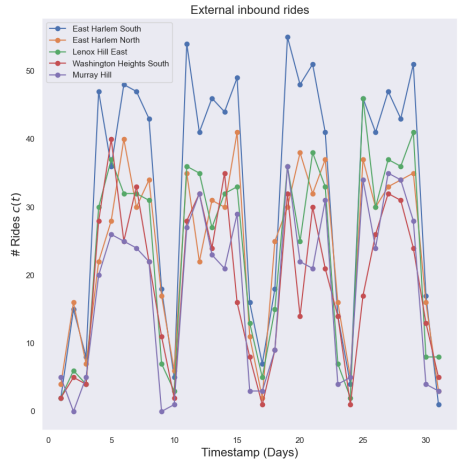
We use the above data to estimate the external assets and liabilities of the CBG nodes. For the bailouts of CBG nodes, we calculate a bailout devised by the CARES act that considers as income the average income of the CBG and as the size of household, the average size of the household multiplied by an estimate for the number of people in that CBG who interact with the POI nodes. Similarly, for the POI nodes, we use data from the US Economic Census and NAICS to determine average wages, income, and expenses. For the bailouts of the POI nodes, we use loan data regarding loans that were given during April 2020 as part of the SBA Paycheck Protection Program (PPP) provided by SafeGraph, adjusted to the number of workers being present in the network and the span of one month. Moreover, the loan data included demographic characteristics about the businesses in question so we were able to determine (or estimate in the case of missing data) the minority status of a business, i.e. the probability of a certain business being a business with a minority owner. A complete



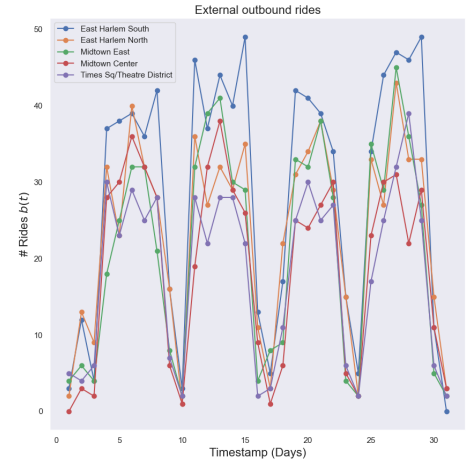
(a) Aggregate statistics



(b) Top-5 Zones



(c) Top-5 Zones



(d) Top-5 Zones

Figure A.4: Non-financial network dataset statistics during January 2021 for Manhattan.

description of the data generation process is presented in Appendix A.6.

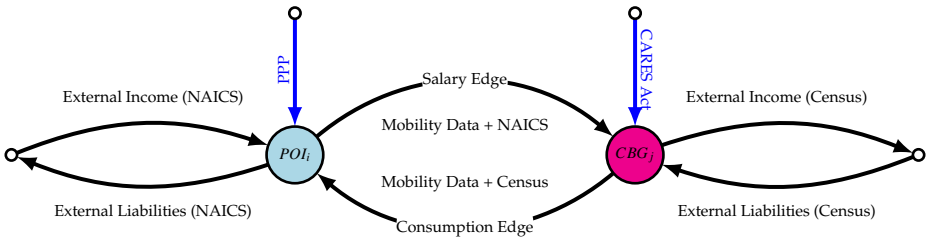


Figure A.5: Physical Financial Network Construction for an example POI and CBG. The complete network is a bipartite graph with POIs on the one side and CBGs on the other side.

A.6 Data Addendum for Physical Financial Network

We present the creation of the dynamic (resp. static) SafeGraph dataset. The dynamic network is created with a monthly granularity for the period of December 2020 to April 2021. For the static allocation experiments of Section 2.7.4, we have taken a snapshot of the network on April 2021. The network topology and the corresponding data sources can be presented in Figure A.5.

A.6.1 Network Topology

The network is bipartite and consists of two types of nodes: POI nodes that correspond to businesses (such as restaurants, gyms, grocery stores, etc.) and CBG nodes (which represent unidentifiable groups of households of people). The data period spans the period of December 2020 to April 2021 with monthly granularity. The POI nodes are constructed as follows: we start from some geographical coordinates (in our case a small rural US city center) and then we find the POIs that belong to the k-closest CBGs (in terms of their Haversine distance). In our experiment, we have chosen k to be 3. Then, for each POI and each period

of interaction, we find out devices from which CBGs visited the specific POI by using the `visitor_home_cbg` column to find the number of visitors for each POI from each CBG, assuming that each device represents a different person. For each CBG j we find the average household size $\bar{h}_j$, the average number of dependents $\bar{d}_j$, the average income $\bar{\iota}_j$ and the probability of someone being unemployed $q_j^{\text{employment}}$ using data from the 2020 US Census.

A.6.2 Internal Liabilities

For each POI-CBG interaction, there are two types of edges: consumption edges and salary edges. The former kind of edge is from a CBG to a POI whereas the latter is from a POI to a CBG. The weights on the edges are calculated following a two-step approach: Firstly, we use the *bucketed dwelling times* to find the percentage of people that are *employed* on these businesses (which we denote by $q_j^{\text{worker}}(t)$), where we consider someone to be employed if they spend more than 4 hours in the POI, and we consider the rest to be consumers (i.e. the ones that spend less than 4 hours in the POI). Between a POI i and a CBG j whereas $n_{ij}(t)$ people have commuted from the CBG to the POI we add the two edges: An edge (j, i) for the worker nodes that we estimate to be $n_{ij}^{\text{workers}}(t) = \lfloor n_{ij}(t) \times q_j^{\text{worker}}(t) \rfloor$ workers, and an edge (i, j) for the non-workers with $n_{ij}^{\text{non-workers}}(t) = n_{ij}(t) - \lfloor n_{ij}(t) \times q_j^{\text{workers}}(t) \rfloor$. For each type of POI i we find the average salary $\bar{s}_i$, and the average consumption $\bar{o}_i$ using data from the NAICS and the US Economic Census (Consumer Expenditure Survey) and calculate the final internal liabilities between POI i and CBG j to be

$$\ell_{ij}(t) = n_{ij}^{\text{workers}}(t) \times \bar{s}_i,\ \ell_{ji}(t) = n_{ij}^{\text{non-workers}}(t) \times \bar{o}_i$$

The total number of workers (resp. non-workers) for each POI j and each CBG i is estimated to be

$$n_j^{\text{workers}}(t) = \sum_{i \text{ is CBG}} n_{ij}^{\text{workers}}(t),\ n_j^{\text{non-workers}}(t) = \sum_{i \text{ is CBG}} n_{ij}^{\text{non-workers}}(t)$$

$$n_i^{\text{workers}}(t) = \sum_{j \text{ is POI}} n_{ij}^{\text{workers}}(t),\ n_i^{\text{non-workers}}(t) = \sum_{j \text{ is POI}} n_{ij}^{\text{non-workers}}(t)$$

The estimated total number of households in the CBG j that are related to interaction with the corresponding POIs is

$$n_j^{\text{households}}(t) = \left\lceil \frac{\frac{n_j^{\text{workers}}(t)}{q_j^{\text{employment}}} + n_j^{\text{non-workers}}(t)}{\bar{h}_j} \right\rceil.$$

A.6.3 Interventions

For each CBG j we use the US CARES Act rule to calculate the interventions as follows:

$$L_j(t) = n_j^{\text{households}(t)} \times \begin{cases} 1200 & \bar{h}_j < 2, \bar{\iota}_j \leq 75000 \\ \left(1200 \times \frac{150000 - \bar{\iota}_j}{75000}\right) \vee 0 & \bar{h}_j < 2, \bar{\iota}_j > 75000 \\ 2400 + 500(\bar{h}_j - 2) & \bar{h}_j \geq 2, \bar{\iota}_j \leq 150000 \\ \left((2400 + 500(\bar{h}_j - 2) \times \frac{300000 - \bar{\iota}_j}{150000}\right) \vee 0 & \bar{h}_j \geq 2, \bar{\iota}_j > 150000 \end{cases}.$$

For each POI i the Safegraph data provides annual business loans from the Paycheck Protection Program (PPP), whereas each loan has value ψ_i. Also the businesses report the number of employees $n_i^{\text{PPP-employees}}$, which we use to calculate the intervention as

$$L_i(t) = \frac{1}{12} \times \frac{\psi_i}{n_i^{\text{PPP-employees}}} \times n_i^{\text{workers}}(t).$$

In our data, there are nodes that, after processing, have missing interventions or interventions that equal 0. For these nodes, we proceed with the following *imputation scheme:* For each POI node (resp. CBG node), we replace the missing interventions with the average intervention of the POI node (resp. CBG node) across rounds where the interventions are well defined. If a POI node (resp. CBG node) has no interventions across all rounds, we set the intervention of the node (for all rounds) to equal the average POI intervention (resp. average CBG intervention).

A.6.4 External Assets and Liabilities

For each POI i we use the total assets earned annually from all establishments, normalized them by month, divide by the total number of workers for the spe-

cific NAICS code that the POI belongs, and multiply $n_i^{\text{workers}}(t)$. Finally, from this amount we subtract the revenue due to nodes within the network $\sum_{j \text{ is CBG}} \ell_{ji}(t)$ (i.e., inbound edges) and take the positive part in case the result is negative to deduce $\xi_i(t)$. $b_i(t)$ is determined in a similar way, with the only change being that the total weight of the outbound edges is subtracted in the end. To ensure that Assumption 3 holds throughout the experiments we assert a minimum of \$100 for the external liabilities. Such a number is smaller than the order of most quantities and thus does not significantly affect the results.

For each CBG j the process is similar where for determining $\xi_j(t)$ we use $\bar{\iota}_j$, following a similar procedure as in the POI case, but now normalized concerning $n_j^{\text{households}}(t)$. For $b_j(t)$, we assume each household spends the national US average of $\sim \$63,000$.

APPENDIX B

TOPOLOGICAL MEASURES OF SYSTEMIC RESILIENCE: A NETWORK PERCOLATION APPROACH

B.1 Analytical Bound on x to ensure $\mathbb{P}[F \geq \varepsilon K] = O(1/K)$ for rdag(K, p)

We can convert the statement of Section 3.3.2 to a statement of high probability if we require $\mathbb{P}[F \geq \varepsilon K]$ to be $O(1/K)$. Because $g(x, K, p, \varepsilon)$ is an increasing function of x, we are asking to find the largest possible x such that $g(x, K, p, \varepsilon) \leq \frac{C}{K}$. In order to get an analytically tractable expression for x, we use the fact that $\log t \leq t$ for all $t > 0$ and get that Equation (3.2) becomes

$$\begin{aligned} g(x, K, p, \varepsilon) &\leq x^n \left[1 - \varepsilon + \frac{1}{K \log\left(\frac{1}{1-p}\right)} \left(\frac{1 - (1 - x^n)(1-p)^K}{1 - (1 - x^n)(1-p)^{\varepsilon K}} \right) \right] \\ &\leq x^n \left[1 - \varepsilon + \frac{1}{K \log\left(\frac{1}{1-p}\right)} \left(\frac{1}{1 - (1 - x^n)(1-p)^0} \right) \right] \\ &= x^n (1 - \varepsilon) + \frac{1}{K \log\left(\frac{1}{1-p}\right)} = \overline{g}(x, K, p, \varepsilon) \end{aligned}$$

If p is constant, then choosing $x = \left(\frac{1}{K \log\left(\frac{1}{1-p}\right)(1-\varepsilon)} \right)^{1/n}$, makes $\overline{g}(x, K, p, \varepsilon) \leq \frac{2}{\log\left(\frac{1}{1-p}\right) K} = O\left(\frac{1}{K}\right)$.

B.2 Omitted Proofs

B.2.1 Proof of Theorem 3.3.1

Let $\mathcal{G} \sim \text{rdag}(K, p)$, with nodes $1, 2, \ldots, K$ (in this order). Let $P_{k,f}$ be the probability of having f distinct failures in the random DAG with k nodes conditioned on a failure on node 1. We have $P_{1,1} = 1$ and $P_{k,f} = 0$ for $f > i$ and $f < 1$. To devise a recurrence formula for $P_{i,f}$, note that for the i-th node we have the following:

1. i is affected by the cascade. That happens if at least one connection to $f-1$ infected nodes upto node $i-1$, or if i fails due to percolation. This happens with probability $\{[1-(1-p)^{f-1}] + x^n - [1-(1-p)^{f-1}]x^n\}P_{k-1,f-1} = [1-(1-p)^{f-1}(1-x^n)]P_{k-1,f-1}$.
2. i is not affected by the cascade. That means that i has ≥ 1 functional supplier, and no connection exists from the f infected nodes. That happens with probability $(1-p)^f(1-x^n)P_{k-1,f}$.

This produces the following recurrence,

$$P_{k,f} = \left[1-(1-p)^{f-1}(1-x^n)\right]P_{k-1,f-1} + (1-p)^f(1-x^n)P_{k-1,f}. \tag{B.1}$$

To determine the distribution of F in $\text{rdag}(K, p)$, we assume that the cascade can start at any node with equal probability $1/K$ and that the probability of failure for any given node is x^n. Also, since a cascade in $\text{rdag}(K, p)$ starting from node 1 is the same as starting from node i in $\text{rdag}(K+i-1, p)$, the distribution obeys the following,

$$\mathbb{P}[F = f] = \frac{x^n}{K}\sum_{k\in[K]} P_{k,f} \tag{B.2}$$

We let $Q_{K,f} = \sum_{k\in[K]} P_{k,f}$, so that $\mathbb{P}[F = f] = \frac{x^n}{K} Q_{K,f}$. Summing Equation (B.1) for $k \in [K]$ and using the definition of $Q_{K,f}$ yields a recurrence relation for $Q_{K,f}$, that is, $Q_{K,f} = (1-p)^f(1-x^n)Q_{K-1,f} + [1-(1-p)^{f-1}](1-x^n)Q_{K-1,f-1}$. We take the limit for K large, we let $q_f = \lim_{K\to\infty} Q_{K,f}$, and solve the recurrence $q_f = (1-p)^f(1-x^n)q_f + [1-(1-p)^{f-1}](1-x^n)q_{f-1}$ to get $q_f = \frac{1}{1-(1-x^n)(1-p)^f}$. Since $e^x \geq x$, we have $(1-p)^f \leq \log(1-p)f$ and subsequently $1-(1-x^n)(1-p)^f \leq f\left(1+(1-x^n)\log\left(\frac{1}{1-p}\right)\right)$. Therefore, for sufficiently large K,

$$\mathbb{P}[F = f] \asymp \frac{x^n q_f}{K} \asymp \frac{x^n}{K(1-(1-x^n)(1-p)^f)} \geq \underbrace{\frac{x^n}{K\left(1+(1-x^n)\log\left(\frac{1}{1-p}\right)\right)}}_{C(K,p,x,n)>0} \frac{1}{f}.$$

B.2.2 Proof of Lemma 3.4.1

If $S(x)$ is the number of products that survive at a given probability of percolation x, and $x_1 \leq x_2$ are two percolation probabilities, then a straightforward coupling argument shows that $S(x_1) \geq S(x_2)$, and subsequently, for every $s \in [0, K]$ we have $\mathbb{P}_{x=x_1}[S \geq s] \geq \mathbb{P}_{x=x_2}[S \geq s]$. Now, in order to arrive at a contradiction, let $\overline{R}_{\mathcal{G}}(\varepsilon) \leq R_{\mathcal{G}}$, and $s = (1-\varepsilon)K$. Then $1 - 1/K \leq \mathbb{P}_{x=R_{\mathcal{G}}(\varepsilon)}[S \geq (1-\varepsilon)K] \leq \mathbb{P}_{x=\overline{R}_{\mathcal{G}}(\varepsilon)}[S \geq (1-\varepsilon)K] \leq 1/2$ which yields a contradiction.

B.2.3 Proof of Theorem 3.4.3

Lower Bound. For C, let $\varepsilon \in (0,1)$. If $F_{\mathcal{R}}$ (resp. F_C) is the number of failed raw materials (resp. complex products), we have that $\{F_C \geq \varepsilon K\} \implies \{F_{\mathcal{R}} \geq \varepsilon K/\mu\}$. Let $\delta = \frac{1}{x^n}\sqrt{\frac{\log K}{2r}}$ and let $\frac{\varepsilon K}{\mu} = (1+\delta)\mathbb{E}[F_R] = (1+\delta)rx^n$. We apply the one-sided Chernoff bound and get $\mathbb{P}[F_C \geq \varepsilon K] \leq \mathbb{P}\left[F_{\mathcal{R}} \geq \frac{\varepsilon K}{\mu}\right] = \mathbb{P}[F_{\mathcal{R}} \geq (1+\delta)\mathbb{E}[F_{\mathcal{R}}]] \leq e^{-2\delta^2\mathbb{E}[F_{\mathcal{R}}]^2/r} = \frac{1}{K}$. Finally, by resolving the last equation $(1+\delta)rx^n = \frac{\varepsilon K}{\mu}$, we get

that $x = \left(\frac{\varepsilon K}{r\mu} + \sqrt{\frac{\log K}{2\mu}}\right)^{1/n}$. Also, we have that $r \leq mK$ and therefore $R_C(\varepsilon) \geq \left(\frac{\varepsilon}{\mu m} + \sqrt{\frac{\log K}{2mK}}\right)^{1/n}$. If ε, m and μ are independent of K then for $K \to \infty$ we have that $R_C(\varepsilon) \geq \left(\frac{\varepsilon}{m\mu}\right)^{1/n} > 0$.

For $\mathcal{G}$, the analysis is similar to the above. For brevity, we give the analysis in expectation (it is easy to extend it to a high-probability analysis). If in expectation $\mathbb{E}[F_{\mathcal{R}}] = rx^n$ raw materials fail, that implies that at most $\mathbb{E}[F] = \mathbb{E}[F_{\mathcal{R}}] + \mathbb{E}[F_C] \leq rx^n + \mu rx^n = (\mu+1)rx^n \leq mKx^n(\mu+1)$ total products fail in expectation. We want the fraction of failed products to be at least $\varepsilon(K+r) \geq \varepsilon K/2$. Therefore, by solving the inequality, we find that the resilience is lower bounded by $\left(\frac{K}{2m(\mu+1)}\right)^{1/n}$. The high-probability analysis would be similar to the above case with an extra additive factor of $\sqrt{\frac{\log(K/2)}{2mK}}$.

Upper Bound. For C, to derive the upper bound, we first bound $\mathbb{E}[S_C]$. It is easy to see that due to the linearity of expectation $\mathbb{E}[S_C] = K(1-x^n)^m$. Thus by Markov's inequality we have that $\mathbb{P}[S_C \geq (1-\varepsilon)K] \leq \frac{\mathbb{E}[S]}{(1-\varepsilon)K} \leq \frac{(1-x^n)^m}{1-\varepsilon}$. To make this probability $1/2$ it suffices to set $x = \left(1 - \left(\frac{1-\varepsilon}{2}\right)^{1/m}\right)^{1/n}$, thus from Lemma 3.4.1 this establishes an upper bound on $R_C(\varepsilon)$.

For $\mathcal{G}$, we proceed similarly by showing that the number of expected products is $\mathbb{E}[S] = r(1-x^n) + K(1-x^n)^m \leq mK(1-x^n) + K(1-x^n)^m \leq K(m+1)(1-x^n)$. Similarly to the above, from Lemma 3.4.1 we see that the upper bound on $R_{\mathcal{G}}$ is $\left(1 - \frac{1-\varepsilon}{2(m+1)}\right)^{1/n}$.

B.2.4 Proof of Theorem 3.4.4

Lower Bound. Depending on the range of m we have two choices

- **Case where $m = 1$.** For every $\tau \in [D]$ we have that $\mathbb{P}[S \geq D - \tau] = \mathbb{P}\left[\bigcap_{d>\tau}\{Z_i = 1\}\right] = \mathbb{P}[Z_1 = 1]\mathbb{P}[Z_2 = 1|Z_1 = 1]\cdots = \prod_{d>\tau}(1 - x^n) = (1 - x^n)^{D-\tau}$. We let $\tau = \varepsilon D$ for some $\varepsilon \in (0, 1)$ and thus $\mathbb{P}[S \geq (1-\varepsilon)D] = (1 - x^n)^{(1-\varepsilon)D}$. We want to make this probability at least $1 - 1/D$, and therefore, the resilience of the path graph is $R_{\mathcal{G}}(\varepsilon) \geq \left(1 - \left(1 - \frac{1}{D}\right)^{\frac{1}{(1-\varepsilon)D)}}\right)^{1/n}$. Since $K = D$ we get the desired result.

- **Case where $m \geq 2$.** Let $\mathcal{K}_d$ be the products of tier d. We let $\tau = \sup\{d \in [D] : \exists i \in \mathcal{K}_d : Z_i = 0\}$ be the bottom-most tier for which a product failure occurs. If at level τ a failure occurs, then all levels above τ are deactivated. The probability that all products up to tier τ operate is given by

$$\begin{aligned}
\mathbb{P}[\text{all products up to tier } \tau \text{ operate}] &= \mathbb{P}\left[\bigcap_{d>\tau}\bigcap_{i\in\mathcal{K}_d}\{Z_i = 1\}\right] \\
&= \prod_{d=D}^{\tau+1}\mathbb{P}\left[\bigcap_{i\in\mathcal{K}_d}\{Z_i = 1\}\middle|\bigcap_{d'>d}\bigcap_{i\in\mathcal{K}_{d'}}\{Z_i = 1\}\right] \\
&= \prod_{d=D}^{\tau+1}(1 - x^n)^{m^d} \\
&= (1 - x^n)^{\sum_{d=D}^{\tau+1} m^d} \\
&= (1 - x^n)^{\frac{m^D - m^\tau}{m-1}}
\end{aligned}$$

  Also, $\{\text{all products up to tier } \tau \text{ operate}\} \implies \{S \geq \frac{m^D - m^\tau}{m-1}\}$. Therefore, the tail probability of S for $\tau \in [D]$ is given by $\mathbb{P}\left[S \geq \frac{m^D - m^\tau}{m-1}\right] = \mathbb{P}\left[S \geq \underbrace{\left(1 - \frac{m^\tau}{m^D}\right)}_{:=1-\varepsilon}\frac{m^D}{m-1}\right] \geq (1 - x^n)^{(1-\varepsilon)\frac{m^D}{m-1}}$. For large enough D we approach the continuous distribution and thus $\mathbb{P}[S \geq (1 - \varepsilon)K] \geq (1 - x^n)^{(1-\varepsilon)K}$. Letting the above be at least $1 - 1/K$, we get $R_{\mathcal{G}}(\varepsilon) \geq \left[1 - \left(1 - \frac{1}{K}\right)^{\frac{1}{(1-\varepsilon)K}}\right]^{1/n}$.

Upper Bound. To derive an upper bound, we have the following cases, depending on the value of m

- **Case** $m = 1$**.** We follow the same logic as the $m \geq 2$ case, and upper bound $\mathbb{E}[S] \leq \sum_{d\geq 0}(1-x^n)^d = \frac{1}{x^n}$ which yields an upper bound $R_{\mathcal{G}}(\varepsilon) < \left(\frac{2}{D(1-\varepsilon)}\right)^{1/n} \to 0$ as $D \to \infty$.

- **Case** $m \geq 2$**.** By Markov's Inequality we get that $\mathbb{P}[S \geq (1-\varepsilon)K] \leq \frac{\mathbb{E}[S]}{(1-\varepsilon)K}$. Lemma B.3.2 (proved in Appendix B.3), implies that $\mathbb{E}[S] \leq \frac{KDx^n}{2}$, thus $\mathbb{P}[S \geq (1-\varepsilon)K] \leq \frac{KDx^n}{2(1-\varepsilon)K}$. To make the RHS equal to $1/2$, it suffices to pick $x = \left(\frac{1-\varepsilon}{D}\right)^{1/n}$. By Lemma 3.4.1 we get that $R_{\mathcal{G}}(\varepsilon) < \left(\frac{1-\varepsilon}{D}\right)^{1/n} \to 0$ as $D \to \infty$.

B.2.5 Proof of Theorem 3.4.5

In order to prove Theorem 3.4.5, we first prove this auxiliary lemma:

Lemma B.2.1. *For τ finite, $\frac{\mathbb{1}\{\mu>1\}}{\log\mu} < \alpha < \frac{1}{2}$, and $0 < \beta < \mathbb{1}\{\mu<1\} + \mathbb{1}\{\mu>1\}\frac{\log\mu - 1}{\mu}$, let*

$$\phi(z) = z\frac{\mu^\tau z^\tau - 1}{\mu z - 1} - \alpha\frac{\mu^\tau - 1}{\mu - 1}, \text{ for } z \neq \frac{1}{\mu}, \quad \psi(z) = \frac{\mu^\tau - 1}{\mu - 1} - z\frac{\mu^\tau z^\tau - 1}{\mu z - 1} - \beta, \text{ for } z \neq \frac{1}{\mu}.$$

Then

1. *If $\mu < 1$, then there exist $z_1, z_2 \in (0,1)$ such that $\phi(z_1) = \psi(z_2) = 0$.*
2. *If $\mu > e^2$, then there exists $z_1 \in (1/\mu, 1)$ such that $\phi(z_1) = 0$.*
3. *If $\mu > e$, then there exists $z_2 \in (1/\mu, 1)$ such that $\phi(z_2) = 0$.*

Proof. **Analysis for $\phi(z)$.** We do case analysis:

- If $\mu < 1$ then ϕ is defined everywhere in $[0,1]$ and is also continuous. It is also easy to prove that ϕ is increasing in $[0,1]$ since its the product of two non-negative increasing functions, z and $\frac{(\mu z)^\tau - 1}{\mu z - 1} = \sum_{i=0}^{\tau-1}(\mu z)^i$. Moreover,

note that $\phi(0) < 0$ and $\phi(1) > 0$. Therefore, there exists a unique solution $z_1 \in (0, 1)$ such that $\phi(z_1) = 0$.

- If $\mu > e^2$, we study ϕ in $(1/\mu, 1]$. Again, ϕ is increasing (for the same reason as above), continuous in $(1/\mu, 1]$, and has $\phi(1) > 0$. We also have that, by using L'Hôspital's rule,

$$\lim_{z\to 1/\mu} \frac{\mu^\tau z^\tau - 1}{\mu z - 1} = \lim_{z\to 1/\mu} \frac{(\mu^\tau z^\tau - 1)'}{(\mu z - 1)'} = \lim_{z\to 1/\mu} \frac{\mu^\tau \tau z^{\tau-1}}{\mu} = \tau \implies$$
$$\lim_{z\to 1/\mu} \phi(z) = \frac{\tau}{\mu} - \alpha\frac{\mu^\tau - 1}{\mu - 1} < \frac{\tau(1 - \alpha\log\mu)}{\mu} < 0 \text{ for } \alpha > \frac{1}{\log\mu}.$$

  Therefore, for $\alpha \in (1/\log\mu, 1/2)$, there exists a unique solution $z_1 \in (1/\mu, 1]$ such that $\phi(z_1) = 0$.

Analysis for $\psi(z)$. Note that ψ is a decreasing function of z. We do case analysis:

- If $\mu < 1$, then ψ is defined everywhere in $[0, 1]$ and is continuous in $[0, 1]$. We have that $\psi(0) > 0$ and $\psi(1) < 0$ therefore there exists a unique solution z_2 such that $\psi(z_2) = 0$.
- If $\mu > e$, then ψ is decreasing and contunuous in $(1/\mu, 1]$, with $\psi(1) < 0$. We also have that $\lim_{z\to 1/\mu} \psi(z) = \frac{\mu^\tau - 1}{\mu - 1} - \frac{\tau}{\mu} - \beta > \frac{\tau(\log\mu - 1 - \mu\beta)}{\mu} > 0$ for $\beta < \frac{\log\mu - 1}{\mu}$.

□

Subsequently, we prove Theorem 3.4.5:

B.2.6 Proof of Theorem 3.4.5

Upper Bound. Let $\tau = \inf\{d \geq 1 : |\mathcal{K}_d| = 0\}$ be the extinction time of the GW process. In order to establish an upper bound on the resilience, it suffices to set the expected number of surviving products to be at most $\frac{1-\varepsilon}{2}\mathbb{E}_{\mathcal{G}}[K]$, since by Markov's inequality the probability of a fraction of at least $(1-\varepsilon)$-fraction of products surviving would be at most $1/2$ and by Lemma 3.4.1 we would get an upper bound on the resilience $R_{\mathcal{G}}(\varepsilon)$; that is, $\mathbb{P}_{\mathcal{G},x}[S \geq (1-\varepsilon)\mathbb{E}_{\mathcal{G}}[K]] \leq \frac{\mathbb{E}_{\mathcal{G},x}[S]}{(1-\varepsilon)\mathbb{E}_{\mathcal{G}}[K]} \leq \frac{1}{2}$. Conditioned on $Z_1 = 1$, which occurs with probability $1-x^n$, the surviving products grow as a GW process with mean $\mu_x = (1-x^n)\mu$. Therefore, the condition $\mathbb{E}_{\mathcal{G},x}[S] = \frac{1-\varepsilon}{2}\mathbb{E}_{\mathcal{G}}[K]$, conditioned on the extinction time being τ, is equivalent to

$$(1-x^n)\frac{\mu_x^\tau - 1}{\mu_x - 1} \leq \frac{1-\varepsilon}{2}\frac{\mu^\tau - 1}{\mu - 1} \iff (1-x^n)\frac{\mu^\tau(1-x^n)^\tau - 1}{\mu(1-x^n) - 1} \leq \frac{1-\varepsilon}{2}\frac{\mu^\tau - 1}{\mu - 1} \tag{B.3}$$

We have the following cases.

1. If $\mu < 1$ then $\mathbb{P}[\tau < \infty] = 1$ (i.e., the process goes extinct after a finite number of steps), then the upper bound on the resilience is always finite due to Lemma B.2.1 which can be found by numerically solving Equation (B.3).
2. If $\mu(1-x^n) > 1$, then $\mathbb{P}[\tau = \infty] > 0$ and in this case Equation (B.3) is only feasible if and only iff $x = 0$, at which case the upper bound on the resilience is 0, and the GW process is not resilient. If $\tau < \infty$, which happens with non-zero probability, the upper bound on the resilience is finite when $\mu > e^2$ due to Lemma B.2.1.

For a specific triplet (μ, τ, ε), let $\bar{x}(\mu, \tau, \varepsilon)$ be the smallest possible solution to Equation (B.3), which exists for $\mu \in (0,1) \cup (e^2, \infty)$ due to Lemma B.2.1. Then the

expected upper bound on resilience $\mathbb{E}_{\mathcal{G}}\left[\overline{\mathcal{R}}_{\mathcal{G}}(\varepsilon)\right]$, can be expressed as $\mathbb{E}_{\mathcal{G}}\left[\overline{\mathcal{R}}_{\mathcal{G}}(\varepsilon)\right] = \mathbb{E}_{\tau}\left[\overline{\mathcal{R}}_{\mathcal{G}}(\varepsilon)\right] = \sum_{1\leq k<\infty}\mathbb{P}[\tau = k]\overline{x}(\mu,\tau,\varepsilon) > 0$.

Lower Bound. Similarly to the upper bound, in order to devise a lower bound, it suffices to set $\mathbb{E}_{\mathcal{G}}[K] - \mathbb{E}_{\mathcal{G}}[S]$ to be at most ε, since, again, by Markov's inequality, we are going to get that the probability that at least a ε-fraction of products fails is at most $\frac{1}{\mathbb{E}_{\mathcal{G}}[K]}$; namely, $\mathbb{P}_{\mathcal{G},x}[F \geq \varepsilon\mathbb{E}_{\mathcal{G}}[K]] \leq \frac{\mathbb{E}_{\mathcal{G},x}[F]}{\varepsilon\mathbb{E}_{\mathcal{G}}[K]} \leq \frac{1}{\mathbb{E}_{\mathcal{G}}[K]}$. This yields

$$\frac{\mu^{\tau}-1}{\mu-1} - (1-x^n)\frac{\mu_x^{\tau}-1}{\mu_x-1} \leq \varepsilon \iff \frac{\mu^{\tau}-1}{\mu-1} - (1-x^n)\frac{\mu^{\tau}(1-x^n)^{\tau}-1}{\mu(1-x^n)-1} \leq \varepsilon \tag{B.4}$$

Similarly to the upper bound, we have the following cases.

1. In the subcritical regime $\mu < 1$, we can again prove that the lower bound is always finite due to Lemma B.2.1.
2. In the supercritical regime $\mu(1-x^n) > 1$, we have that when $\tau < \infty$, which happens with positive probability then for $\mu > e$ from Lemma B.2.1 we get the existence of the resilience. When $\tau = \infty$, we have again that the only way Equation (B.4) can hold is iff $x = 0$.

For a specific triplet (μ,τ,ε), let $\underline{x}(\mu,\tau,\varepsilon)$ be the largest possible solution to Equation (B.4), which exists for $\mu \in (0,1)\cup(e,\infty)$ due to Lemma B.2.1. Then the expected lower bound on the resilience $\mathbb{E}_{\mathcal{G}}\left[\underline{\mathcal{R}}_{\mathcal{G}}(\varepsilon)\right]$, can be expressed as $\mathbb{E}_{\mathcal{G}}\left[\underline{\mathcal{R}}_{\mathcal{G}}(\varepsilon)\right] = \mathbb{E}_{\tau}\left[\underline{\mathcal{R}}_{\mathcal{G}}(\varepsilon)\right] = \sum_{1\leq k<\infty}\mathbb{P}[\tau = k]\underline{x}(\mu,\tau,\varepsilon) > 0$.

Determining $\mathbb{P}[\tau < \infty]$ when $\mu(1-x^n) > 1$. It is known from the analysis of GW processes (see, e.g., [379]) that the extinction probability $\mathbb{P}[\tau < \infty]$ can be found as the smallest solution $\eta \in [0,1]$ to the fixed-point equation $\eta = G_{\mathcal{D}}(\eta)$ where $G_{\mathcal{D}}(s) = \mathbb{E}_{\xi\sim\mathcal{D}}\left[e^{s\xi}\right]$ is the moment generating function of the branching distribution $\mathcal{D}$.

B.2.7 Proof of Theorem 3.4.7

Upper Bound. Let $F_{\mathcal{R}}$ correspond to the number of failures of the raw products. Let $x_{\mathcal{R}} = \sup\{x \in (0,1) : \mathbb{P}[F_{\mathcal{R}} \leq (1-\varepsilon)K] \geq 1 - 1/K\}$. $x_{\mathcal{R}}$ is an upper bound to $R_{\mathcal{G}}(\varepsilon)$ since the event $\{F \leq (1-\varepsilon)K\}$ implies $\{F_{\mathcal{R}} \leq (1-\varepsilon)K\}$. Moreover, by the Chernoff bound, we have that for any $\varepsilon' > 0$:

$$\mathbb{P}\left[\frac{F_{\mathcal{R}}}{r} \leq (1+\varepsilon')x^n\right] \geq 1 - e^{-2r(\varepsilon')^2}.$$

Letting $(1+\varepsilon')x^n = (1-\varepsilon)K/r$, $e^{-2r(\varepsilon')^2} = 1/K$ and solving for x would produce an upper bound to $x_{\mathcal{R}}$ and subsequently an upper bound to $R_{\mathcal{G}}(\varepsilon)$. Solving the system yields the following result.

$$\varepsilon' = \sqrt{\frac{\log(K)}{2r}} \qquad \text{and} \qquad x = \left[\frac{(1-\varepsilon)K}{\sqrt{2}r^{3/2} + \sqrt{r\log K}}\right]^{1/n}.$$

To determine conditions where the resilience goes to zero as $K \to \infty$ we focus on the denominator of the upper bound: First, the term $\sqrt{r\log K}$ is at most $\sqrt{K\log K} < K$ and cannot grow faster than K. Second, the term $\sqrt{2}r^{3/2}$ grows faster than K as long as $r = \omega\left(K^{3/2}\right)$.

Lower Bound. We construct $\mathcal{G}'$ as follows: We start by $\mathcal{G}$, and additionally, for each final good $j \in C$ in $\mathcal{G}$ and each raw product i we add an edge from i to j in $\mathcal{G}'$ if there is a path from i to j in $\mathcal{G}$. By construction $\mathcal{G} \subseteq \mathcal{G}'$ and thus $R_{\mathcal{G}}(\varepsilon) \geq R_{\mathcal{G}'}(\varepsilon)$. In $\mathcal{G}'$ we have that the sourcing dependency m' satisfies $m' \leq m + r$ and the supply dependency satisfies $\mu' \leq \mu + c$. The result follows by applying Theorem 3.4.3 to $\mathcal{G}'$.

B.2.8 Proof of Theorem 3.4.10

Let u_i be the probability that the product i fails spontaneously (in the simple case, we have $u_i = x^n$ but for more general cases, we can assume that $u_i \in [0, 1]$).

For $i \in \mathcal{K}$ let $\beta_i = \mathbb{P}[Z_i = 0] \in [0, 1]$. By the union bound, we have that

$$\begin{aligned}\beta_i &= \mathbb{P}[(\exists j \in \mathcal{N}(i) : (i, j) \text{ is operational } \wedge Z_j = 0) \vee (\forall s \in \mathcal{S}(i) X_{is} = 0)] \\ &\leq \mathbb{P}[\exists j \in \mathcal{N}(i) : (i, j) \text{ is operational } \wedge Z_j = 0] + \mathbb{P}[\forall s \in \mathcal{S}(i) X_{is} = 0] \\ &\leq y \sum_{j \in N(i)} \beta_j + u_i.\end{aligned}$$

The number of failed products equals $\mathbb{E}[F] = \sum_{i \in \mathcal{K}} \beta_i$. Thus, finding the upper bound on $\mathbb{E}[F]$ corresponds to solving the following LP,

$$p^*_{\mathcal{G}}(u; y) = \max_{\beta \in [0, \mathbb{1}]} \sum_{i \in \mathcal{K}} \beta_i \qquad \text{s.t.} \qquad \beta \leq y A^T \beta + u.$$

When $y \|A^T\|_1 < 1$, which is equivalent to $y < \frac{1}{m}$, this problem is the financial clearing problem of [139], and from Lemma 4 of [139], we know that we can also compute β by solving the fixed point equation $\beta = \mathbb{1} \wedge (y A^T \beta + u) = \Phi(\beta)$. Since $y < 1/m$, the mapping is a contraction and has a unique fixed-point theorem due to Banach's theorem.

To obtain the upper bound, note that if β^* is an optimal solution, then the union-bound constraint implies that $(1 - my) \sum_{i=1}^{K} \beta_i^* \leq K x^n \leq \mathbb{E}\left[F_y\right]$. Using the fact that $\frac{1}{1-my} = 1 + my + O((my)^2)$ we get the right-hand side with $\varrho = my$.

B.2.9 Proof of Theorem 3.4.11

Upper bound. Given the subsampled graph $\mathcal{G}_y$, if a product i survives in $\mathcal{G}$, then it survives in $\mathcal{G}_y$; and if a product fails in $\mathcal{G}$, then it survives in $\mathcal{G}_y$ with probability at least $q = (1-y)^m(1-x^n)$, which is the probability that the product does not fail on its own and none of its inputs are selected in $\mathcal{G}_y$. Taking expectations we get that $\mathbb{E}\left[F_y\right] \leq (1-q)\mathbb{E}\left[F\right]$. The quantity q is minimized for $y = 1/m$ and satisfies $q \geq (1-1/m)^m(1-x^n) \geq 1/4(1-x^n)$. This implies the $3/4 + x^n/4$ upper bound.

Lower Bound. If Z_i' are the indicator variables for failures in G_y then we have $\mathbb{P}[Z_i = 0] = \mathbb{P}[Z_i = 0|Z_i' = 0]\mathbb{P}[Z_i' = 0] + \mathbb{P}[Z_i = 0|Z_i' = 1]\mathbb{P}[Z_i = 1] \leq q'(1 - \mathbb{P}[Z_i' = 0]) + \mathbb{P}[Z_i' = 0]$ where q' is an upper bound on the probability that a node fails in $\mathcal{G}$ conditioned on its survival in $\mathcal{G}_y$. By linearity of expectation, this gives $\mathbb{E}\left[F_y\right] \geq \frac{\mathbb{E}[F]-Kq'}{1-q'}$. The value of q' corresponds to the probability that for each node, at least $f \geq 1$ neighbors have failed but none of them is sampled in G_y and it is given by:

$$q' = 1 - (1 - x^n(1-y))^m .$$

yielding the final result.

B.2.10 Proof of Theorem 3.4.12

If p^* is the optimal value of the primal given in Equation (3.10), and $(\tilde{\gamma}, \tilde{\theta})$ is a feasible dual solution with the objective value $\tilde{d}$, then from weak duality we

have $\mathbb{E}[F] \le p^* \le \tilde{d}$. If we let $\tilde{d} \le \varepsilon$, then $\mathbb{P}[F \ge \varepsilon K] \le \frac{\mathbb{E}[F]}{\epsilon K} \le \frac{\tilde{d}}{\varepsilon K} \le \frac{1}{K}$. Therefore any x such that $\tilde{d} \le \varepsilon$ will be a lower bound on $R_{\mathcal{G}}(\varepsilon)$. This is equivalent to

$$R_{\mathcal{G}}(\varepsilon) \ge x \ge \left(\frac{\varepsilon - \mathbb{1}^T\tilde{\theta}}{\mathbb{1}^T\tilde{\gamma}}\right)^{1/n}, \qquad \text{for all} \qquad \tilde{\theta}, \tilde{\gamma} \ge 0 \text{ s.t. } (I - yA)\tilde{\gamma} + \tilde{\theta} \ge \mathbb{1}. \tag{B.5}$$

We are interested in the values of $(\tilde{\gamma}, \tilde{\theta})$ that maximize this lower bound, and therefore the best lower bound is given by

$$\underline{R}_{\mathcal{G}}(\varepsilon) = \max_{\gamma,\theta \ge 0} \left(\frac{\varepsilon - \mathbb{1}^T\theta}{\mathbb{1}^T\gamma}\right)^{1/n}, \qquad \text{s.t.} \qquad (I - yA)\gamma + \theta \ge \mathbb{1}. \tag{B.6}$$

Observe that increasing any θ_i from $\theta_i = 0$ would decrease the lower bound; therefore, the optimal θ is $\theta^* = 0$. Moreover, due to monotonicity,

$$\underline{R}_{\mathcal{G}}(\varepsilon) = \left(\frac{\varepsilon}{\min_{\gamma \ge 0, \gamma \ne 0} \mathbb{1}^T\gamma}\right)^{1/n}, \qquad \text{s.t.} \qquad (I - yA)\gamma \ge \mathbb{1}. \tag{B.7}$$

yielding our final result. We take the dual of the denominator, which corresponds to $\max_{\beta \ge 0} \mathbb{1}^T\beta$ subject to $\beta \le yA^T\beta + \mathbb{1}$. If $y < 1/m$, from the main result of [139] (or the KKT conditions) we get that the optimal solution is $\beta_{\mathcal{G}}^{\text{Katz}}(y)$. Similarly for its dual, the optimal solution is $\gamma_{\mathcal{G}}^{\text{Katz}}(y)$.

B.2.11 Proof of Proposition 3.4.13

Recall $\min_{T \subseteq \mathcal{K}: |T| = B} p^*_{\mathcal{G}}(T; y)$, where $p^*_{\mathcal{G}}(T; y)$ is the solution to LP maximization (Equation (3.10)). Since $0 < y < \frac{1}{m}$ and $0 < x < (1 - ym)^{1/n}$, the optimal solu-

tion of the internal maximization equals $\widehat{\beta}(t) = x(I - yA^T)^{-1}(\mathbb{1} - t)$. Substituting that in the objective function of Equation (3.10), we get that

$$\widehat{t} = \arg\min_{t\in\{0,1\}^n} \mathbb{1}^T\widehat{\beta}(t) = \arg\min_{t\in\{0,1\}^n} \mathbb{1}^T(I - yA^T)^{-1}(\mathbb{1} - t) = \arg\min_{t\in\{0,1\}^n} (\mathbb{1} - t)^T((I - yA^T)^{-1})^T\mathbb{1}$$
$$= \arg\min_{t\in\{0,1\}^n} (\mathbb{1} - t)^T(I - yA)^{-1}\mathbb{1} = \arg\min_{t\in\{0,1\}^n} \gamma^T_{\text{Katz}}(\mathcal{G}^R, y)(\mathbb{1} - t),$$

where, we remind that $\gamma_{\text{Katz}}(\mathcal{G}^R, y) = (I - yA)^{-1}\mathbb{1}$ is the vector of Katz centralities for the *reverse graph* $\mathcal{G}^R$. The third equality is true because $(I - yA^T)^{-T} = \left(\sum_{k\geq 0}(yA^T)^k\right)^T = \sum_{k\geq 0}(yA)^k \overset{y<\frac{1}{\mu}}{=} (I - yA)^{-1}$. It is easy to observe that, by the rearrangement inequality, the optimal solution would be to intervene in the top-T nodes in terms of Katz centrality in $\mathcal{G}^R$.

B.3 Upper and Lower Bounds on $\mathbb{E}[S]$ for the m-ary tree

Lemma B.3.1. *Let q_d be the probability that a product in tier d can be produced. Then*

$$q_d = \begin{cases} (1 - x^n)^{\frac{m^{D-d+1}-1}{m-1}}, & m \geq 2 \\ (1 - x^n)^{D-d+1}, & m = 1 \end{cases} \tag{B.8}$$

Proof. Let$q_d = \mathbb{P}$[a product in tier d can be produced] = $\mathbb{P}[\exists$a functional supplier at tier d]. To calculate q_d, note that all the inputs for a product node at tier d succeed with probability q^m_{d+1}, and then the probability that at least one supplier is functionally conditioned on all the inputs working is $1 - x^n$. This yields the following recurrence relation $q_d = q^m_{d+1}(1 - x^n)$ with $q_{D+1} = 1$. Solving this recurrence relation, we get $q_{D-d} = (1 - x^n)^{\sum_{l=0}^{d} m^l}$ for $d \in [D]$. This yields $q_d = \begin{cases} (1 - x^n)^{\frac{m^{D-d+1}-1}{m-1}}, & m \geq 2 \\ (1 - x^n)^{D-d+1}, & m = 1 \end{cases}$. □

Lemma B.3.2 (Upper Bound when $m \geq 2$)**.** *Under the tree structure and $m \geq 2$ the expected size obeys $\mathbb{E}[S] \leq \frac{Kx^n(D-1)}{2} = U(x)$.*

Proof. From Lemma B.3.1 we have $q_d = (1-x^n)^{\frac{m^{D-d+1}-1}{m-1}}$. Using the inequality $(1-t)^a \leq \frac{1}{1+ta}$ for $a > 0$ and $t \in (0,1)$ we get that

$$\mathbb{E}[S] = \sum_{d=1}^{D} m^{d-1} q_d \leq \sum_{d=1}^{D} m^{d-1} \frac{1}{1 + x^n \frac{m^{D-d+1}}{2(m-1)}} \asymp \int_{t=1}^{D} \frac{m^{t-1}}{1 + x^n \frac{m^{D-t+1}}{2(m-1)}}.$$

By letting $u = \frac{x^n m^{D-t+1}}{2(m-1)}$ we get that the above integral equals

$$\frac{m^D x^n}{2 \log m(m-1)} \log\left(\frac{(1-x^n)(1-p)^{\varepsilon K}(1+(1-x^n)(1-p)^K)}{(1-x^n)(1-p)^K(1+(1-x^n)(1-p)^{\varepsilon K})}\right)\Bigg|_{u_2 = x^n m^D/2(m-1)}^{u_1 = x^n m/2(m-1)}$$
$$\leq \frac{m^D x^n}{2 \log m(m-1)} \log\left(m^{D-1}\right) \leq \frac{Kx^n(D-1)}{2} = U(x).$$

□

Lemma B.3.3 (Lower bound when $m \geq 2$)**.** *Under the tree structure and $m \geq 2$ the expected cascade size obeys $\mathbb{E}[S] \geq K(1 - x^n(D-1)) = L(x)$ where $K = m^D - 1$ is the number of products.*

Proof. From Lemma B.3.1 we have $q_d = (1-x^n)^{\frac{m^{D-d+1}-1}{m-1}}$. By Bernoulli's inequality $q_d \geq 1 - x^n\left(\frac{m^{D-d+1}-1}{m-1}\right)$.

Since every level has m^{d-1} nodes we have that

$$\mathbb{E}[S] = \sum_{d=1}^{D} m^{d-1} q_d \geq \sum_{d=1}^{D} m^{d-1}\left[1 - x^n\left(\frac{m^{D-d+1}-1}{m-1}\right)\right] = K(1+x^n) - x^n \frac{1}{m-1}\sum_{d=1}^{D} m^{d-1} m^{D-d+1}$$
$$= K(1+x^n) - x^n \frac{1}{m-1}\sum_{d=1}^{D} m^D = K(1+x^n) - x^n D(K-1) \geq K(1-x^n(D-1)).$$

□

B.4 Extended Related Work

Supply Chain Contagion. There have been multiple works on production networks in macroeconomics and how shocks in production networks propagate through the production network's input-output relations, see a comprehensive survey by [88]. One of the earliest works dates back to [206] introduces a multi-sector model that extends the earlier Long-Plosser model [274] and argues that sector-specific shocks are, in fact, affected by the graph topology between producing sectors. Such arguments contrast the previous arguments of [275], which argue that small microeconomic shocks would significantly affect the economy. In the 2008 financial crisis, the ex-CEO of Ford, Alan Mulally, argued that the collapse of GM or Chrysler would significantly impact Ford's production capabilities for nontrivial amounts of time. The works of [4, 164] build on the above observation and show that even small shocks lead to cascades that can have devastating effects on the economy. Specifically, [164] argues that firm-level idiosyncratic shocks can translate into large fluctuations in the production network when the firm sizes are heavy-tailed, and, in the sequel, [4] replaced [164]'s analysis on the firm size with the intersectoral network, building on the Long-Plosser model. [193] introduces a supply chain model in which, when a firm cannot satisfy its orders, it rations its production to the firms that depend on it via the Input-Output matrix. The model of [193] has been used to study supply chain effects of the COVID-19 pandemic [189, 413, 208, 336]. Finally, recent work by [142] studies the propagation of shocks in a network. Our work is related to the above works and attempts to study the propagation of individual shocks at the supplier level to the (aggregate) production network through the definition of a resilience metric.

Seeding Problems in Supply Chains. In a different flavor from the literature we discussed above, the work of [59] study how to find the least costly set of firms to target as early adopters of traceability technology in a supply chain network, where hyperedges model individual supply chains. The connections to our paper involve the spread of information in a networked environment through interventions. However, in this paper, we do not focus on building algorithms for interventions; instead, we provide metrics to assess the vulnerability of nodes in a supply chain network, which can be informative for interventions.

Node Percolation. [181, 430] study node percolation processes, wherein graph nodes fail independently with probability p. Their goal is to find the graphs – among graphs with a fixed number of nodes and edges – such that the probability that the induced subgraph (after percolation) is connected is maximized.

Resilience and Risk Contagion in Financial Networks. In a different context, similar models have been used to study financial networks, and optimal allocations in the presence of shocks [139, 179, 322, 320, 330, 161, 122, 12] and financial network formation and risk, see, e.g., [62, 220, 212, 31, 32, 148, 149, 16, 385, 57]. Our work is related to the above works and attempts to study the propagation of individual shocks at the supplier level to the (aggregate) production network through the definition of a resilience metric. [8] study financial networks and state that contagion in financial networks has a phase transition: for small enough shocks, a densely connected financial network is more stable, and, on the contrary, for large enough shocks, a densely connected system is a more fragile financial system. In a similar spirit, [17] and [46] characterize the size of

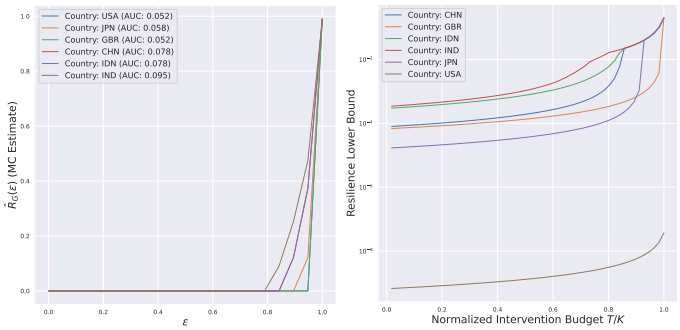
defaults under financial contagion in random graphs. They show that firms that contribute the most to network instability are highly connected and have highly contagious links. Moreover, it has also been shown – see, e.g., [368, 47, 45], and the references therein – that risky nodes in financial networks are connected to centrality measures.

Cascading Failures and Emergence of Power Laws. There has been a large body of literature on cascading failures in networks and how the cascade distributions behave as power laws in social networks [265, 420], and power grids, see e.g., [128, 304]). We bring the perspective of supply chains and production networks to this literature and offer new insights on how complexity of products and their interdependence affect production network resilience.

B.5 Experiments Addendum: World I-O Tables

Country	Size (K)	Avg. Degree	Density	Min/Max In-degree	Min/Max Out-degree	AUC
USA	55	54.00	1.000	54	54	0.052
Japan	56	45.33	0.824	0 – 50	0 – 50	0.058
G. Britain	56	52.05	0.946	0 – 54	0 – 54	0.052
China	56	37.89	0.688	0 – 46	0 – 46	0.078
Indonesia	56	35.75	0.65	0 – 46	0 – 46	0.078
India	56	29.57	0.537	0 – 41	0 – 43	0.095

Table B.1: Network Statistics and AUC for the world economies. The edge density is computed as $\frac{|\mathcal{E}(\mathcal{G})|}{K^2-K}$.



(a) Estimating $R_{\mathcal{G}}(\varepsilon)$ (b) Optimal Interventions

Figure B.1: World Economy Input-Output Networks. We set the number of suppliers for each product to $n = 1$.

B.6 Generalizing Resilience

B.6.1 Hardness with deterministic marginals

If supplier failures are deterministic, the hardness follows from the following decision problem, which is equivalent to calculating the resilience.

Definition B.6.1 (RESILIENCE-DETERMINISTIC)**.** Given a production network $\mathcal{G}$, an average number of supplier failures x, and a non-negative integer f, does there exist a deterministic distribution ν such that the number of failures is f?

Theorem B.6.1. RESILIENCE-DETERMINISTIC *is NP-hard.*

The proof relies on a reduction from the 3-SET-COVER problem, where the input consists of c elements $V = \{v_1, \ldots, v_c\}$ and r sets $S = \{s_1, \ldots, s_r\}$ where each set has cardinality 3, and a number B. The question is whether there is a collection of B subsets that cover all the elements.

To construct the reduction, we consider a bipartite production network with raw products $\mathcal{R}$, labeled by $\{s_1, \ldots, s_r\}$, and final goods C, labeled by $\{v_1, \ldots, v_c\}$, with $K = c + r$ products, where the left partition (raw products $\mathcal{R}$) corresponds to the sets in 3-SET-COVER and the right partition (consumer goods C) corresponds to the elements in 3-SET-COVER. Each product/node has a single supplier ($n_i = 1$). Each raw product $s_i \in \mathcal{R}$ is used to make three complex products such that for each complex product $v_j \in C$ we have $v_j \in s_i$ in the 3-SET-COVER instance. We set $f = B + c$ and $x = B/K$. The reduction runs in polynomial time, creating a graph with $O(K)$ nodes and $O(K)$ edges.

($\Longrightarrow$) Assume that there is a set cover $\mathcal{J} \subset S$ of size $B = |\mathcal{J}|$. Then we choose the raw products $J \subseteq \mathcal{R}$ corresponding to $\mathcal{J}$ and the set $x_i = 1$ for the unique supplier of the product i (so that it fails deterministically with probability 1). B of the raw products and all c consumer goods fail. Therefore, the number of failures is now $B + c$.

($\Longleftarrow$) Take any supplier failure assignment with at least $B + c$ supplier failures. Then, if there exists a scenario with $B + c$ failed products, then it should necessarily include all c consumer goods and B of the raw products, whose corresponding subsets in S constitute a solution to the 3-SET-COVER problem.

B.6.2 Distribution Constraints

For brevity, we let $N = \sum_{i \in \mathcal{K}} n_i$. The definition of Equation (3.16) requires defining a distribution ν over the union of the suppliers. We let $\mathcal{U} = \bigcup_{i \in \mathcal{K}} \mathcal{S}(i)$ be the universe of suppliers. We let $\nu : 2^{\mathcal{U}} \to [0, 1]$ be the distribution, where $\nu(U)$ corresponds to the probability that at subset $U \subseteq \mathcal{U}$ of the suppliers is active.

We require the coupling to be non-negative and normalized:

$$\nu(U) \geq 0, \qquad \forall U \in 2^{\mathcal{U}} \tag{B.9}$$

$$\sum_{U \subseteq \mathcal{U}} \nu(U) = 1, \tag{B.10}$$

and respect the corresponding marginals, i.e.

$$\sum_{T \subseteq \mathcal{U}: s \notin T} \nu(T \cup \{s\}) \leq x_s. \tag{B.11}$$

Finally, we impose the budget constraint, i.e.

$$0 \leq x_s \leq 1 \qquad \forall s \in \mathcal{U} \tag{B.12}$$

$$\sum_{s \in \mathcal{U}} x_s \leq xN. \tag{B.13}$$

In matrix notation, if $\bar{x}$ is the vector of marginals,

$$\nu \geq 0, \bar{x} \geq 0 \tag{B.14}$$

$$\bar{x} - \mathbb{1} \leq 0, \Phi\nu - \bar{x} \leq 0, \mathbb{1}^T \bar{x} \leq xN, \mathbb{1}^T \nu \leq 1 \tag{B.15}$$

where Φ is a matrix such that $\phi_{T,s} = 1$ if and only if $s \notin T$. The number of variables needed to define ν is $O\left(2^N\right)$.

B.6.3 Upper bound on $\mathbb{E}[F]$

We extend Equation (3.10) to account for ν. Specifically, we are interested in the upper bound on the number of failures for the worst possible joint distribution ν. The primal problem corresponding to this upper bound is as follows:

$$p^* = \max_{\beta,q,\nu \geq 0} \quad \mathbb{1}^T \beta \tag{B.16}$$

$$\text{s.t.} \quad \beta \leq 1, (I - yA^T)\beta - \Psi\nu \leq 0 \tag{B.17}$$

$$\text{Equation (B.14)} \tag{B.18}$$

We define Ψ as the $K \times 2^N$ matrix with elements $\psi_{i,T} = 1$ iff $T \subseteq \mathcal{U} \setminus \mathcal{S}(i)$ and 0 otherwise. Taking the dual yields,

$$d^* = \min_{\gamma,\theta,\zeta,\kappa,\eta,\xi \geq 0} \mathbb{1}^T\theta + \mathbb{1}^T\zeta + \eta + \xi x N \tag{B.19}$$

$$\text{s.t.} \quad (I - yA)\gamma + \theta \geq \mathbb{1}$$

$$\zeta - \kappa + \mathbb{1}\xi \geq 0$$

$$-\Psi^T\gamma + \Phi^T\kappa + \mathbb{1}\eta \geq 0.$$

B.6.4 Lower Bound

Similarly to Theorem 3.4.12, if we take a feasible dual solution $(\tilde{\gamma}, \tilde{\theta}, \tilde{\zeta}, \tilde{\kappa}, \tilde{\eta}, \tilde{\xi})$ to Equation (B.19) with objective value $\tilde{d}$, we can show from weak duality that it suffices to set $\tilde{d} \leq 1 - \varepsilon$ to get a lower bound on $R_{\mathcal{G}}(\varepsilon)$. This implies that

$$R_{\mathcal{G}}(\varepsilon) \geq \frac{\varepsilon - \mathbb{1}^T\tilde{\theta} - \mathbb{1}^T\tilde{\zeta} - \tilde{\eta}}{\tilde{\xi}N} \tag{B.20}$$

Therefore, a lower bound can be devised by taking the maximum possible value of the RHS, i.e.

$$\begin{aligned} \underline{R}_{\mathcal{G}}(\varepsilon) = \max_{\gamma,\theta,\zeta,\kappa\eta,\xi} \quad & \frac{\varepsilon - \mathbb{1}^T\theta - \mathbb{1}^T\zeta - \eta}{\xi N} \\ \text{s.t.} \quad & \text{Equation (B.19) constraints} \end{aligned} \tag{B.21}$$

It is easy to show that in optimality $\eta = 0$, $\theta = 0$ and $\zeta = 0$, we therefore have the following.

$$\begin{aligned} \underline{R}_{\mathcal{G}}(\varepsilon) = \max_{\gamma,\kappa,\xi} \quad & \frac{\varepsilon}{\xi N} \\ \text{s.t.} \quad & (I - yA)\gamma \geq \mathbb{1},\ -\kappa + \mathbb{1}\xi \geq 0,\ -\Psi^T\gamma + \Phi^T\kappa \geq 0. \end{aligned} \tag{B.22}$$

B.6.5 Resulting Lower Bound for the Resilience

The results yield the following theorem.

Theorem B.6.2. *If resilience is defined as in Equation (3.16), then a lower bound on resilience can be found by solving the following optimization problem with $O(K)$ variables and $O(2^N)$ constraints:*

$$\underline{R}_{\mathcal{G}}(\varepsilon; y) = \max_{\gamma,\kappa,\xi \geq 0} \quad \frac{\varepsilon}{\xi N}$$
$$s.t. \quad (I - yA)\gamma \geq \mathbb{1},\ -\kappa + \mathbb{1}\xi \geq 0,\ -\Psi^T\gamma + \Phi^T\kappa \geq 0,$$

where Ψ, Φ *are matrices given in Appendix B.6.*

B.7 Limitations of the LP-based bound

Theorem B.7.1. *There exist non-negative integers* $m \geq 2$ *and* $h \geq 1$ *such that there exists a family of graphs* $\{\mathcal{G}_{m,h}\}_{m\geq 2,h\geq 1}$ *with* $K = \Theta(m^h)$ *nodes,* $n = 1$ *suppliers and subsampling probabilities* $y_m > 1/m$*, such that* $p^*_{m,h} - \mathbb{E}[F_{m,h}] \geq K/8$*, where* $p^*_{m,h}$ *is the value of Equation (3.10) for* $\mathcal{G}_{m,h}$ *and* $\mathbb{E}[F_{m,h}]$ *is the expected number of failures in* $\mathcal{G}_{m,h}$*.*

The tree graphs with height h and fanout m are the family of graphs that achieve this gap. Throughout the analysis, we will set $m' = my_m$ for brevity, as the percolation process on this (random) tree graph is equivalent to percolation in a deterministic tree graph of height h and fanout m'. We set $n = 1$, and let $g_{m,h} = p^*_{m,h} - \mathbb{E}[F_{m,h}]$ be the additive gap between the LP approximation $p^*_{m,h}$ and the true value $\mathbb{E}[F_{m,h}]$ for the graph $\mathcal{G}_{m,h}$.

We start the proof with the case of $h = 1$, corresponding to a star graph graph with m raw goods and a final product in the center. To find $p^*_{m,1}$, note that each of the leaf nodes fails with probability x and for the root we have $\beta^*_{root} \leq m'x + x = (m' + 1)x$. If $x \geq 1/(1 + m')$ we have $\beta^*_{root} = 1$, because the union bound is loose and the box constraint on the range of β becomes active. Therefore, $p^*_{m,1} = mx + 1$. In contrast, the size of the cascade is given by $\mathbb{E}[F_{m,1}] =$

$mx + x + 1 - (1-x)^m - x(1-(1-x))^m = mx + 1 - (1-x)^{m+1}$. The gap $g_{m,1}$ equals $g_{m,1} = (1-x)^{m+1}$ and for $x = 1/(1+m')$ we have $g_{m,1} \geq \left(\frac{1}{4}\right)^{(m+1)/(m'+1)} \geq \frac{1}{4}$. Moreover, for any $h \geq 2$ we can inductively show that $g_{m,h} = g_{m,1} + mg_{m,h-1}$, and therefore solving the recurrence yields $g_{m,h} \geq m^h/4 \geq K/8$ (since $m^h \geq K/2$) which grows unbounded as $h, m \to \infty$.

APPENDIX C

PRIVACY-PRESERVING DECISION-MAKING FOR RESILIENCE: DIFFERENTIALLY PRIVATE DISTRIBUTED INFERENCE IN CONTINUOUS AND DISCRETE HYPOTHESIS SPACES

Part 1: Learning and Inference in Continuous Hypothesis Spaces

C.1 Proofs

C.1.1 Proof of Theorem 4.1.1

Proof. Since A is real and symmetric, we can do an eigen decomposition of A as $A = Q\Lambda Q^T$ where Q is an orthonormal eigenvector matrix, and Λ is the diagonal eigenvalue matrix. We have that $\|\nu_t - \mu_t\|_2^2 = \|Q\Lambda^t Q^T d\|_2^2 = \sum_{i=1}^n \lambda_i^{2t}(A)(q_i^T d)^2$. Note that $\mathbb{E}\left[(q_i^T d)^2\right] = \mathbb{E}\left[\sum_{j=1}^n q_{ij}^2 d_j^2 + \sum_{1\le j<k\le n} q_{ij}q_{ik}d_j d_k\right] = \mathbb{E}\left[\sum_{j=1}^n q_{ij}^2 d_j^2\right] = \sum_{i=1}^n q_{ij}^2 \mathbb{V}[d_i]$. Therefore $\mathbb{E}\left[\|\nu_t - \mu_t\|_2^2\right] = \sum_{j=1}^n \mathbb{V}\left[d_j\right] \sum_{i=1}^n \lambda_i^{2t}(A) q_{ij}^2$. Since for all $2 \le i \le n$ we have that $|\lambda_i(A)| \le b_n^\star$, and by using Jensen's inequality we get that

$$
\begin{aligned}
\mathbb{E}\left[\|\nu_t - \mu_t\|_2\right] &\le \sqrt{\sum_{i,j=1}^n \mathbb{V}\left[d_j\right] \lambda_i^{2t}(A) q_{ij}^2} \le \sum_{i,j=1}^n \sqrt{\mathbb{V}\left[d_j\right]} |\lambda_i^t(A)| |q_{ij}| \\
&\le \sum_{j=1}^n \sqrt{\mathbb{V}\left[d_j\right]} |q_{1j}| + (b_n^\star)^t \sum_{i,j=1}^n \sqrt{\mathbb{V}\left[d_j\right]} |q_{ij}| \\
&\le \sqrt{\sum_{j=1}^n \mathbb{V}\left[d_j\right]} \left(1 + \sqrt{n-1}(b_n^\star)^t\right).
\end{aligned}
$$

To minimize the upper bound on the MSE for each agent j, it suffices to minimize the variance of $d_j \sim \mathcal{D}_j$, subject to differential privacy constraints. We assume that the PDF of $\mathcal{D}_j$ – denoted by $p_{d_j}(\cdot) \in \Delta_{n,\Theta}(\mathbb{R})$ – is differentiable everywhere in $\mathbb{R}$. The differential privacy constraint is equivalent to

$$\begin{aligned}\left|\frac{d}{ds_j}\log \mathbb{P}[\psi_{\mathcal{M}_j^s}(s_j)=t]\right| \le \varepsilon \iff \\ \left|\frac{d}{ds_j}\log p_{d_j}(t-\xi(s_j))\right| \le \varepsilon \iff \\ \left|\frac{d}{ds_j}p_{d_j}(t-\xi(s))\right| \le \varepsilon p_{d_j}(t-\xi(s_j)),\end{aligned}$$

for all $t \in \mathbb{R}$ and $s_j \in \Theta$. Letting $u = t - \xi(s_j)$ we get that, in order to satisfy ε-DP,

$$\left|\frac{dp_{d_j}(u)}{du}\right| \le \frac{\varepsilon}{\Delta_{n,\Theta}}p_{d_j}(u),$$

where $\Delta_{n,\Theta} = \max_{s\in\Theta}\left|\frac{d\xi(s_j)}{ds_j}\right|$ is the global sensitivity of ξ. We have that

$$\begin{aligned}\min_{p_{d_j}(\cdot)\in\Delta_{n,\Theta}(\mathbb{R})} \quad & \mathbb{E}_{d_j\sim\mathcal{D}_j}\left[d_j^2\right] = \int_{\mathbb{R}} t^2 p_{d_j}(t)dt \\ \text{s.t.} \quad & \int_{\mathbb{R}} p_{d_j}(t)dt = 1, \\ & |p'_{d_j}(t)| \le \frac{\varepsilon}{\Delta_{n,\Theta}}p_{d_j}(t), \qquad \forall t \in \mathbb{R}.\end{aligned}$$

From Theorem 6 of [247] we get that the optimal solution to the above problem is the Laplace distribution with scale $\lambda_j = \Delta_{n,\Theta}/\varepsilon$,

$$p_{d_j}(t) = \frac{\varepsilon}{2\Delta_{n,\Theta}}\exp\left(-\frac{\varepsilon}{\Delta_{n,\Theta}}|t|\right), \quad \forall t \in \mathbb{R}.$$

To derive the upper bound on the error note that by Theorem 3 of [343] we have that $\mathbb{E}\left[\|\mu_t - \mathbb{1}\widehat{m}_\theta\|_2\right] \le \sqrt{n(n-1)}(b_n^\star)^t\Gamma_{n,\Theta}$, and also $\mathbb{E}\left[\|\mu_t - \nu_t\|_2\right] \le \sqrt{\sum_{j=1}^n \mathbb{V}\left[d_j\right]}(1 + \sqrt{n-1}(b_n^\star)^t)$. Applying the triangle inequality yields the final result, i.e.,

$$\mathbb{E}\left[\|\nu_t - \mathbb{1}\widehat{m}_\theta\|_2\right] \le \sqrt{n(n-1)}(b_n^\star)^t\Gamma_{n,\Theta} + \sqrt{\sum_{j=1}^n \mathbb{V}\left[d_j\right]}(1 + \sqrt{n-1}(b_n^\star)^t). \tag{C.1}$$

Using the optimal distributions $\mathcal{D}_i^\star = \mathrm{Lap}(\Delta_{n,\Theta}/\varepsilon)$ in (4.8) gives the claimed upper bound on $\mathrm{TE}(\mathcal{M}^S)$. □

C.1.2 Proof of Corollary 4.1.2 (DP preservation across time)

To derive the DP guarantee for the MVUE for round t, we will do an induction. Specifically, we want to prove that for all $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ we have for all $i \in [n]$,

$$\left|\log\left(\frac{\mathbb{P}[\nu_{i,t} = x_i]}{\mathbb{P}[\nu'_{i,t} = x_i]}\right)\right| \leq \varepsilon,$$

for all adjacent pairs of signals and beliefs, i.e., $\left\|(s_i, \{\nu_{j,t-1}\}_{j\in\mathcal{N}_i}) - (s'_i, \{\nu'_{j,t-1}\}_{j\in\mathcal{N}_i})\right\|_1 \leq 1$. We proceed with the induction as follows:

- For $t = 1$, the result is held by the construction of the noise and the definition of DP.
- For time $t \in \mathbb{N}$, we assume that $\left|\log\left(\frac{\mathbb{P}[\nu_{i,t}=x_i]}{\mathbb{P}[\nu'_{i,t}=x_i]}\right)\right| \leq \varepsilon$ for all $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$.
- For time $t + 1$, we have that for all $i \in [n]$,

$$\left|\log\left(\frac{\mathbb{P}[\nu_{i,t+1} = x_i]}{\mathbb{P}[\nu'_{i,t+1} = x_i]}\right)\right| = \left|\log\left(\frac{\mathbb{P}[\nu_{i,t} = (A^{-1}x)_i]}{\mathbb{P}[\nu'_{i,t} = (A^{-1}x)_i]}\right)\right| \leq \varepsilon.$$

  which holds by applying the definition of the MVUE update, the fact that A is non-singular, and the inductive hypothesis for t.

C.1.3 Proof of Theorem 4.1.3

Proof. Similarly to Theorem 4.1.1, we decompose A as $A = Q\Lambda Q^T$ and get that

$$\begin{aligned}\|\nu_t - \mu_t\|_2^2 &= \left\|\frac{1}{t} Q \sum_{\tau=0}^{t-1} \Lambda^\tau d_{t-\tau} Q^T\right\|_2^2 \\ &= \frac{1}{t^2} \sum_{i=1}^{n} \sum_{\tau=0}^{t-1} \lambda_i^{2\tau}(A)(q_i^T d_{t-\tau})^2.\end{aligned}$$

We take expectations and apply Cauchy-Schwarz to get

$$\begin{aligned}\mathbb{E}\left[\|\nu_t - \mu_t\|_2^2\right] &\le \frac{1}{t^2} \sum_{i=1}^{n} \sum_{\tau=0}^{t-1} \lambda_i^{2\tau}(A)\mathbb{E}\left[\|d_{t-\tau}\|_2^2\right] \\ &\le \frac{1}{t^2}\left(1 + \sum_{i=2}^{n} \sum_{\tau=0}^{t-1} \lambda_i^{2\tau}(A)\right)\left(\sum_{j=1}^{n} \sum_{\tau=0}^{t-1} \mathbb{V}\left[d_{j,t-\tau}\right]\right) \\ &\le \frac{1}{t^2}\left(1 + (n-1)\sum_{\tau=0}^{t-1} (b_n^\star)^{2\tau}\right)\left(\sum_{j=1}^{n} \sum_{\tau=0}^{t-1} \mathbb{V}\left[d_{j,t-\tau}\right]\right) \\ &\le \frac{1}{t^2}\left(1 + \frac{n-1}{1-(b_n^\star)^2}\right)\left(\sum_{j=1}^{n} \sum_{\tau=0}^{t-1} \mathbb{V}\left[d_{j,t-\tau}\right]\right).\end{aligned} \tag{C.2}$$

By Jensen's inequality, we get that

$$\mathbb{E}\left[\|\nu_t - \mu_t\|_2\right] \le \frac{1}{t}\left(1 + \sqrt{\frac{n-1}{1-(b_n^\star)^2}}\right)\sqrt{\sum_{j=1}^{n} \sum_{\tau=0}^{t-1} \mathbb{V}\left[d_{j,t-\tau}\right]}.$$

Also note that the dynamics of $q_t = \mu_t - \mathbb{1} m_\theta$ obey

$$q_t = \frac{t-1}{t} A q_{t-1} + \frac{1}{t}\left(\xi_t - \mathbb{1} m_\theta\right).$$

By following the same analysis as Equation (C.2) we get that

$$\mathbb{E}\left[\|\nu_t - \mu_t\|_2\right] \leq \sqrt{\frac{n}{t}}\left(1 + \sqrt{\frac{n-1}{1-(b_n^\star)^2}}\right)\sqrt{\mathbb{V}\left[\xi(s)\right]},$$

and then, the triangle inequality yields

$$\mathbb{E}\left[\|\nu_t - \mathbb{1}m_\theta\|_2\right] \leq \frac{1}{t}\left(1 + \sqrt{\frac{n-1}{1-(b_n^\star)^2}}\right)\left(\sqrt{nt\mathbb{V}\left[\xi(s)\right]} + \sqrt{\sum_{j=1}^{n}\sum_{\tau=0}^{t-1}\mathbb{V}\left[d_{j,t-\tau}\right]}\right).$$

To optimize the upper bound of Equation (C.2), for every index $0 \leq \tau \leq t-1$ and agent $j \in [n]$ we need to find the zero mean distribution $\mathcal{D}_{j,\tau+1}$ with minimum variance subject to differential privacy constraints. We follow the same methodology as Theorem 4.1.1 and arrive at the optimization problem

$$\begin{aligned}
\min_{p_{d_{j,\tau+1}}(\cdot)\in\Delta_{n,\Theta}(\mathbb{R})} \quad & \mathbb{E}_{d_{j,\tau+1}\sim\mathcal{D}_j}\left[d_{j,\tau+1}^2\right] = \int_{\mathbb{R}} u^2 p_{d_{j,\tau+1}}(u)du \\
\text{s.t.} \quad & \int_{\mathbb{R}} p_{d_{j,\tau+1}}(u)du = 1, \\
& |p'_{d_{j,\tau+1}}(u)| \leq \frac{\varepsilon}{\Delta_{n,\Theta}} p_{d_{j,\tau+1}}(u), \qquad \forall u \in \mathbb{R}.
\end{aligned}$$

The optimal distribution is derived identically to Theorem 4.1.1, and equals $\mathcal{D}^\star_{j,\tau+1} = \text{Lap}\left(\frac{\Delta_{n,\Theta}}{\varepsilon}\right)$ for all $j \in [n]$ and $0 \leq \tau \leq t-1$.

□

C.1.4 Proof of Theorem 4.1.4

Proof. Let $C(t) = B(t) - \frac{1}{t}I$, and let $\Phi(t) = \prod_{\tau=0}^{t-1} C(\tau)$. Note that $C(t)$ can be written as $tC(t) = (t-2)I + A$, and we can infer that the eigenvalues of $C(t)$ satisfy $\lambda_i(C(t)) =$

$1 + \frac{\lambda_i(A)-2}{t}$, and that $\{C(\tau)\}_{\tau\in[t]}$ and A have the same eigenvectors. Therefore,

$$\lambda_i(\Phi(t)) = \prod_{\tau=0}^{t-1} \lambda_i(C(\tau)) \leq \exp\left(\sum_{\tau=1}^{t} \frac{\lambda_i(A)-2}{\tau}\right) \leq t^{\lambda_i(A)-2}.$$

Similarly to Theorem 4.1.3, we have the following.

$$\begin{aligned}
\mathbb{E}\left[\|\nu_t - \mu_t\|_2^2\right] &= \frac{1}{t^2}\sum_{i=1}^{n}\sum_{\tau=0}^{t-1} \lambda_i(\Phi(\tau))^2 \mathbb{E}\left[\left(q_i^T d_{t-\tau}\right)^2\right] \\
&\leq \frac{1}{t^2}\left(\sum_{i=1}^{n}\sum_{\tau=0}^{t-1} \lambda_i(\Phi(\tau))^2\right)\left(\sum_{\tau=0}^{t-1}\mathbb{E}\left[\|d_{t-\tau}\|_2^2\right]\right) \\
&\leq \frac{1}{t^2}\left(\sum_{i=1}^{n}\int_1^t \tau^{2\lambda_i(A)-4} d\tau\right)\sum_{\tau=0}^{t-1}\mathbb{E}\left[\|d_{t-\tau}\|_2^2\right] \\
&\leq \frac{1}{t^2}\left(\sum_{i=1}^{n}\int_1^t \tau^{2\lambda_i(A)-4} d\tau\right)\left(\sum_{\tau=0}^{t-1}\mathbb{E}\left[\|d_{t-\tau}\|_2^2\right]\right) \\
&\leq \frac{1}{t^2}\left(\sum_{i=1}^{n}\frac{1}{3-2\lambda_i(A)}\right)\sum_{\tau=0}^{t-1}\mathbb{E}\left[\|d_{t-\tau}\|_2^2\right] \\
&\leq \frac{1}{t^2}\left(1+\frac{n-1}{3-2b_n^\star}\right)\sum_{\tau=0}^{t-1}\mathbb{E}\left[\|d_{t-\tau}\|_2^2\right] \\
&\leq \frac{1}{t^2}\left(1+\frac{n-1}{3-2b_n^\star}\right)\left(\sum_{i=1}^{n}\sum_{\tau=0}^{t-1}\mathbb{V}\left[d_{i,t-\tau}\right]\right).
\end{aligned}$$

Applying Jensen's inequality, we get that

$$\mathbb{E}\left[\|\nu_t - \mu_t\|_2\right] \leq \frac{1}{t}\sqrt{\sum_{i=1}^{n}\sum_{\tau=0}^{t-1}\mathbb{V}\left[d_{i,t-\tau}\right]}\left(1+\sqrt{\frac{n-1}{3-2b_n^\star}}\right).$$

Similarly, by considering the dynamics of $q_t = \mu_t - \mathbb{1}m_\theta$ we get that

$$\mathbb{E}\left[\|\mu_t - \mathbb{1}m_\theta\|_2\right] \leq \sqrt{\frac{n}{t}}\sqrt{\mathbb{V}\left[\xi(s)\right]}\left(1+\sqrt{\frac{n-1}{3-2b_n^\star}}\right).$$

The triangle inequality yields the final error bound.

To derive the optimal distributions, note that at each round t, the optimal action for agent i is to minimize $\mathbb{V}[d_{i,t}]$ subject to DP constraints. By following the analysis similar to Theorem 4.1.1, we deduce that the optimal noise to add is Laplace with parameter $\max\{\max_{j\in\mathcal{N}_i} a_{ij}, \Delta_{n,\Theta}\}/\varepsilon$.

□

C.2 Algorithm of Rizk et al. (2023)

We adapt the framework of [354] to our problem, for which the identification of the MVUE $\widehat{m_\theta}$ can be formulated as

$$\widehat{m_\theta} = \operatorname*{argmin}_{m\in\mathbb{R}} \frac{1}{2n} \sum_{i=1}^{n} \underbrace{(m - \xi(s_i))^2}_{J_i(m)}.$$

The private dynamics for updating the beliefs ν_t can be found by simplifying the consensus algorithm given in Equations (24)-(26) of [354]:

$$\nu_{i,t} = a_{ii}(\nu_{i,t-1} + g_{ii,t}) + \sum_{j\in\mathcal{N}_i} a_{ij}\left(\nu_{j,t-1} + g_{ij,t}\right) + d_{i,t} - \eta(\nu_{i,t-1} - \xi(s_i)).$$

Here, η is the learning rate, $d_{i,t}$ is noise used to protect the private signal, and $g_{ij,t}$, $\left\{g_{ij,t}\right\}_{j\in\mathcal{N}_i}$ are noise terms used to protect own and the neighboring beliefs. As a first difference, we observe that [354] uses $(n+m)T$ noise variables, whereas our method uses just n noise variables, which makes our method easier to implement for the MVUE task. It is easy to observe that these dynamics converge

slower than our dynamics for two reasons: (i) the privacy protections are added separately for the signal and each neighboring belief, and (ii) the beliefs are always using information from the signals since the method is first-order, thus requiring noise to be added at each iteration.

For this reason, the authors consider graph-homomorphic noise, i.e., noise of the form $g_{ij,t} = q_{i,t}$ for all $j \neq i$ and $g_{ii,t} = -\frac{1-a_{ii}}{a_{ii}} q_{i,t}$ where $q_{i,t}$ are noise variables. Rewriting the dynamics in this form, we get the following update:

$$\nu_{i,t} = (a_{ii} - \eta)\nu_{i,t-1} + \sum_{j \in \mathcal{N}_i} a_{ij}\nu_{j,t-1} + \eta\xi(s_i) + d_{i,t}.$$

Given a privacy budget ε, in order to make a fair comparison with our algorithm, the noise variable should be chosen as $d_{i,t} \sim \text{Lap}\left(\frac{\eta T S^{\star}_{\xi,\gamma}(s_i)}{\varepsilon}\right)$ for Signal DP, and $d_{i,t} \sim \text{Lap}\left(\frac{T \max\{\max_{j \neq i} a_{ij}, \eta S^{\star}_{\xi,\gamma}(s_i)\}}{\varepsilon}\right)$ for Network DP. Here, since the per-agent privacy budget is ε, and the noise is added T times at each iteration, the initial budget needs to be divided by T.

We run the same experiments as in Section 4.1.9 with the method of [354] and compare with our method using the same values of the privacy budget ε and a learning rate $\eta = 0.001$ to get the results in Figure 4.7.

C.3 Extensions to Dynamic and Directed Networks and Heterogeneous Privacy Budgets

C.3.1 Dynamic Networks

In this problem, the agents observe a sequence of dynamic networks $\{G(t)\}_{t\in\mathbb{N}}$, for example, due to corrupted links, noisy communications, other agents choosing not to share their measurements, power failures etc. These dynamic networks correspond to a sequence of doubly stochastic matrices $\{A(t)\}_{t\in\mathbb{N}}$. A choice for the weights are the modified Metropolis-Hastings (MH) weights:

$$a_{ij}(t) = \begin{cases} \frac{1}{2\max\{\deg_t(i),\deg_t(j)\}}, & j \neq i \\ 1 - \sum_{j\in\mathcal{N}_i} a_{ij}(t), & j = i \end{cases}. \tag{C.3}$$

This is a natural choice of weights since they can be easily and efficiently computed by the agents in a distributed manner (e.g., in a sensor network) from the knowledge of own and neighboring degrees, thus requiring minimal memory to be stored for each agent. Below we will show that the MVUE and the OL algorithms converge under minimal assumptions for the time-varying MH weights.

MVUE.. We can prove that if G_t contain no isolated nodes, the beliefs would converge to $\widehat{m_\theta}$ as a direct consequence of [95, Theorem 1.4], i.e.

Proposition C.3.1. *If G_t contains no isolated nodes for all $t \in \mathbb{N}$, for accuracy $0 < \rho < 1/2$, the dynamics with the modified MH weights of Equation (C.3) will converge to the*

MVUE, $\widehat{m_\theta}$, in

$$t = \min\left\{\frac{2^{O(n)}(\Gamma_{n,\Theta} + \Delta_{n,\Theta}/\varepsilon)}{\rho}, \left(\log\frac{\Gamma_{n,\Theta} + \Delta_{n,\Theta}/\varepsilon}{\rho}\right)^{n-1} 2^{n^2-O(n)}\right\}$$

steps.

Proof. The proof follows from applying Theorem 1.4 of [95], since $\max_{j\neq i} a_{ij} \leq 1/2$, the graph is undirected, and the diameter of the points is at most $2(\Gamma_{n,\Theta} + \Delta_{n,\Theta}/\varepsilon)$. □

Note that the above convergence rate is exponentially worse than the

$$t = O\left(\frac{\log\left(n(\Gamma_{n,\Theta} + \Delta_{n,\Theta}/\varepsilon)/\rho\right)}{\log(1/b_n^\star)}\right)$$

convergence time that we obtain for static networks.

Online Learning.. For the online learning regime, we can follow the approach presented in [391]. For this, we consider the following update rule:

$$\nu_t = \frac{t-1}{t}\nu_{t-1} + \frac{1}{t}A(t)\nu_{t-1} + \frac{1}{t}\left(\xi_t + d_t\right). \tag{C.4}$$

We show that under reasonable assumptions on the graph sequence, the above algorithm converges to $\mathbb{1}m_\theta$ almost surely.

Proposition C.3.2. *If G_t contains no isolated nodes for all $t \in \mathbb{N}$, and there exists an integer B such that $\bigcup_{\tau=tB}^{t(B+1)-1} G_\tau$ is strongly connected for every $t \in \mathbb{N}$, then the dynamics of Equation (C.4) with the modified MH weights of Equation (C.3) converge to $\mathbb{1}m_\theta$ almost surely.*

Proof. The dynamics have the form of the dynamics of [391]. We will show the result by showing that the assumptions of [391] hold. Specifically, all non-zero elements of $A(t)$ have value at least $1/(2n)$, $a_{ii}(t) \geq 1/2$ for all $i \in [n], t \in \mathbb{N}$ by our hypothesis, there exists an integer B such that $\bigcup_{\tau=tB}^{t(B+1)-1} G_\tau$ is strongly connected for every $t \in \mathbb{N}$ by our hypothesis, $\sum_{t=1}^{\infty} 1/t = \infty$, and $\sum_{t=1}^{\infty} 1/t^2 < \infty$. Thus, by Proposition 2 of [391], the beliefs converge almost surely to $\mathbb{1}m_\theta$ as $t \to \infty$. Furthermore, we can show that the dependence on t becomes slower, i.e., from $t^{-1/2}$ when the network is static to t^{-1/n^3} when the network is dynamic.

□

C.3.2 Directed Networks

We can also consider extensions of our results to directed graphs, i.e., when $a_{ij} \neq a_{ji}$ in general. Such asymmetries can arise due to systemic heterogeneities, e.g., varying accuracy and reliability of sensors in a sensor network or imbalances caused by influence dynamics in a social network. The adjacency weights in such cases are no longer doubly stochastic, making the MVUE dynamics in Equations (4.3) and (4.7) to converge to $\widehat{m_\theta} = q_1^T \xi$ where q_1 is the stationary distribution of the Markov chain with transition matrix A, satisfying $Aq_1 = q_1$ and $q_1^T \mathbb{1} = 1$. Unlike the doubly stochastic case, the stationary distribution is not necessarily uniform, in which case the aggregate converges to a weighted average of $\xi(s_i)$ that is no longer minimum variance. To analyze the convergence rate of the algorithms with asymmetric adjacency weights, we cannot use tools from the theory of doubly-stochastic matrices anymore, and we need to rely on different tools from the analysis of convergence of non-reversible Markov chains.

The results of [94] extend the notion of spectral gap and can make this analysis possible. However, these results come with significant technicalities, using substantially different analytical steps that are beyond the scope of our present work. More limited conclusions about the asymptotic rates and finite-time convergence can be asserted in special cases by applying existing results such as [391].

C.3.3 Heterogeneous Privacy Budgets

Our algorithms extend easily to the case where each agent has their own privacy budget ε_i, e.g., due to their differing energy consumption levels. In this case, it is easy to show that all of the results can be updated to accommodate heterogeneous ε_i and the smooth sensitivities $\Delta_{n,\Theta,i}$, as shown in Table C.1 below.

Table C.1: Total Error Bounds for heterogeneous privacy budgets $\{\varepsilon_i\}_{i\in[n]}$. The blue terms are due to privacy constraints (CoP), and the red terms are due to decentralization (CoD). Here $\Gamma_{n,\Theta}$ and $b_n^\star$ are the same as in Table 4.1, and $\{\Delta_{n,\Theta,i}\}_{i\in[n]}$ are the smooth sensitivities for each agent which can be set as $\Delta_{n,\Theta,i} = S^*_{\xi,\gamma}(s_i)$ for the case of Signal DP and $\Delta_{n,\Theta,i} = \max\left\{\max_{j\neq i} a_{ij}, S^*_{\xi,\gamma}(s_i)\right\}$ for the case of Network DP.

Minimum Variance Unbiased Estimation	Online Learning of Expected Values
$O\left((b_n^\star)^t\Gamma_{n,\Theta} + (1+(b_n^\star)^t)\sum_{i=1}^n \frac{\Delta_{n,\Theta,i}}{\varepsilon_i}\right)$	$O\left(\frac{n}{\sqrt{t}}\sqrt{\mathbb{V}\left[\xi(s)\right]} + \frac{1}{\sqrt{t}}\sum_{i=1}^n \frac{\Delta_{n,\Theta,i}}{\varepsilon_i}\right)$

The possibility of heterogeneous privacy budgets opens new avenues to explore the allocation of an overall privacy budget ($n\varepsilon$) while respecting individual budgets $\{\varepsilon_{i,\max}\}_{i\in[n]}$. Such a situation may arise, e.g., to limit overall information leakage against an adversary that can eavesdrop on some or all of the communications. Suppose that each agent wants to maintain ε_i-DP and suppose that there is an adversary that eavesdrops on all of the beliefs (this also covers the

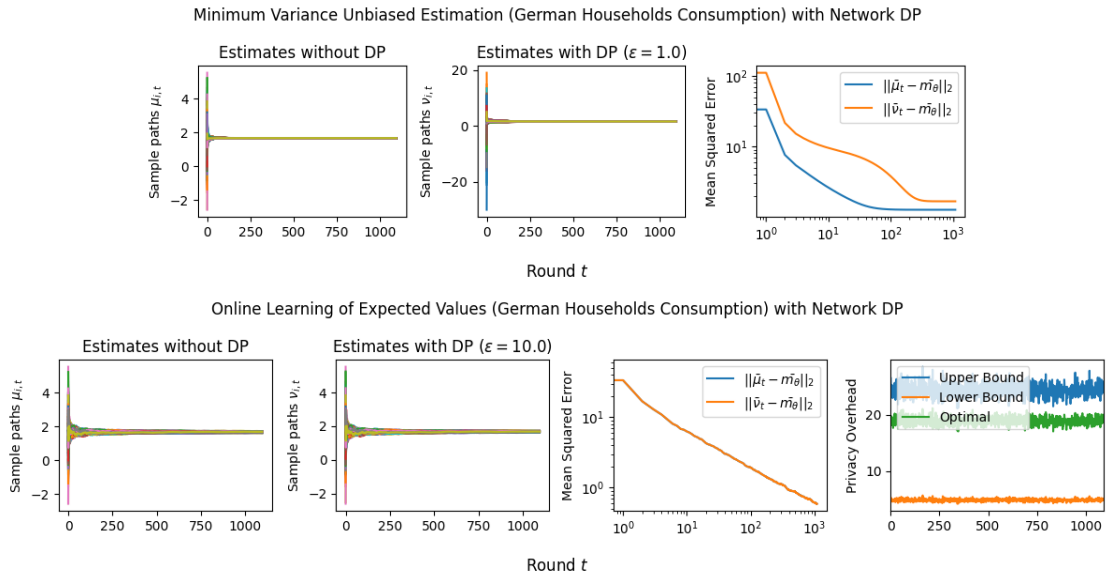


Figure C.1: Sample Paths for MVUE and OL for the German Households Dataset with heterogeneous budgets (centralized solution). For the OL case, we plot the optimal privacy overhead $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon_i^\star}$ which we compare with the lower bound $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon}$, and the upper bound $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon_{i,\max}}$.

cases where the adversary has access to a subset W of the $[n]$, such as in the case of a targeted attack to a large part of the network). Note that all of the results presented so far protect against information leakage about a single agent's signals (or their network neighborhoods) when their reports $\nu_{i,t}$ are compromised. However, if the goal is to protect the private signals against an adversary that can eavesdrop simultaneously on all or a subset of agents, then each individual agent's report can be regarded as a data release about the vector of all signals that needs to be protected at the $n\varepsilon$-DP level, in addition to the individual-level $\varepsilon_{i,\max}$-DP protections required by each agent. If the adversary can eavesdrop on all of the signals, then the resulting mechanism that protects the joint distribution of the signals can be thought of as a mechanism $\Psi^{\mathcal{M}^S}$ which adds n-dimensional noise d to the sufficient statistics and each dimension $i \in [n]$ of the

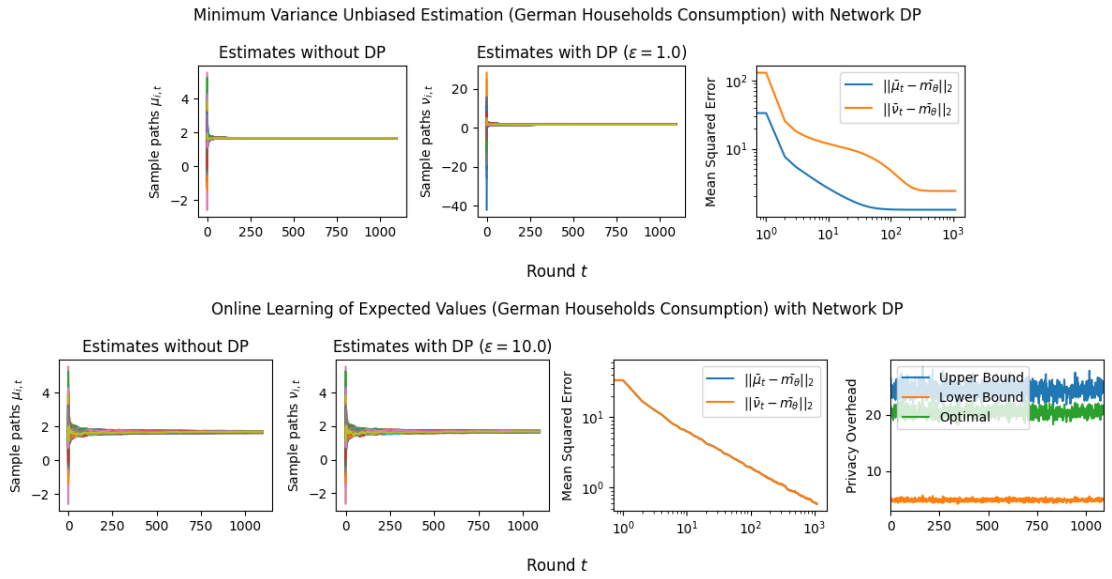
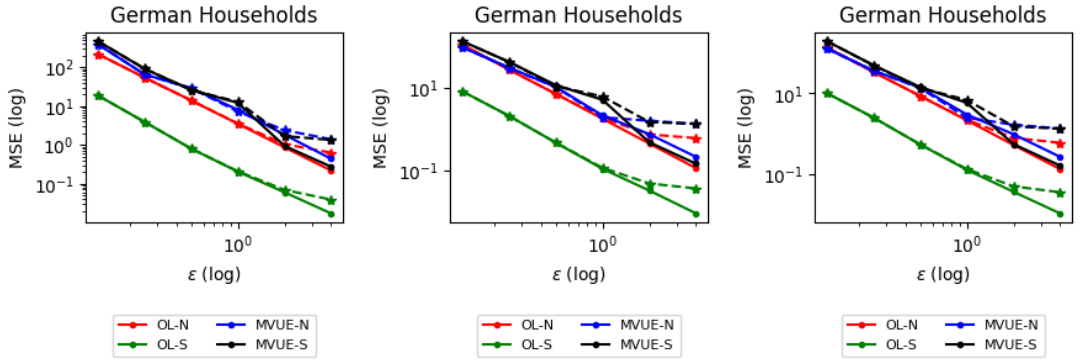


Figure C.2: Sample Paths for MVUE and OL for the German Households Dataset with heterogeneous budgets (decentralized solution). For the OL case, we plot the optimal privacy overhead $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon_i^\star}$ which we compare with the lower bound $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon}$, and the upper bound $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon_{i,\max}}$.



(a) Homogeneous (b) Problem (C.6) (c) Problem (C.7)

Figure C.3: MSE Plots for the German Households Dataset with heterogeneous privacy budgets. We note that compared to the homogeneous case, using heterogeneous budgets reduces the MSE.

noise corresponds to $d_{i,t}$, i.e.,

$$\Psi^{\mathcal{M}^S}(s_{1,t}, \ldots, s_{n,t}) = \xi_t + d_t$$

Then, if $\Delta_{n,\Theta,i}$ is the sensitivity for each agent i, the noise has PDF:

$$p_{d_t}(u_1, \ldots, u_n) = \prod_{i=1}^{n} \frac{\varepsilon_i}{2\Delta_{n,\Theta,i}} \exp\left(-\frac{\varepsilon_i}{\Delta_{n,\Theta,i}}|u_i|\right) \propto \exp\left(-\sum_{i=1}^{n} \frac{\varepsilon_i}{\Delta_{n,\Theta,i}}|u_i|\right)$$

Now, consider a pair $(s_{1,t}, \ldots, s_{n,t}), (s'_{1,t}, \ldots, s'_{n,t})$ of sets of signals such that

$$\left\|(s_{1,t}, \ldots, s_{n,t}) - (s'_{1,t}, \ldots, s'_{n,t})\right\|_1 \leq 1.$$

Then, we have that for all $x \in \mathbb{R}^n$:

$$\begin{aligned}
\left|\log\left(\frac{\mathbb{P}[\Psi^{\mathcal{M}^S_{i,t}}(s_{1,t}, \ldots s_{n,t}) = x]}{\mathbb{P}[\Psi^{\mathcal{M}^S_{i,t}}(s'_{1,t}, \ldots s'_{n,t}) = x]}\right)\right| &= \left|\log\left(\frac{p_{d_t}(\xi_t - x)}{p_{d_t}(\xi'_t - x)}\right)\right| \\
&= \left|\sum_{i=1}^{n} \frac{\varepsilon_i}{\Delta_{n,\Theta,i}}(|\xi(s'_{i,t}) - x| - |\xi(s_{i,t}) - x|)\right| \\
&\leq \sum_{i=1}^{n} \frac{\varepsilon_i}{\Delta_{n,\Theta,i}}|\xi(s_{i,t}) - \xi(s'_{i,t})| \\
&\leq \sum_{i=1}^{n} \varepsilon_i \left\|s_{i,t} - s'_{i,t}\right\|_1 \\
&\leq \left(\sum_{i=1}^{n} \varepsilon_i\right) \max_{i\in[n]} \left\|s_{i,t} - s'_{i,t}\right\|_1 \\
&\leq \sum_{i=1}^{n} \varepsilon_i. \qquad \text{(C.5)}
\end{aligned}$$

Now suppose we want to protect the vector of all beliefs against the eavesdropper at the $n\varepsilon$-DP level (assuming an average privacy budget of ε per agent for the overall protection of the vector of all private signals). The noise that is added to individual estimates also works to protect the entire vector of all estimates against the eavesdropper and to achieve the latter at the $n\varepsilon$ level, Equation (C.5) indicates that it is sufficient to ensure that $\sum \varepsilon_i \leq n\varepsilon$. On the other hand, given ε_i privacy level at every agent i, we also want to minimize the accuracy loss by reducing $\sum_{i=1}^{n} \Delta_{n,\Theta,i}/\varepsilon_i$ while ensuring that individual privacy

budgets do not exceed a preset maximum: $vec\varepsilon_i \leq \varepsilon_{i,\max}$ for all i. The subsequent optimization problem to allocate individual privacy budgets can be formulated as follows:

$$\begin{aligned} \min_{\varepsilon_1,\ldots,\varepsilon_n>0} \quad & \sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon_i} \\ \text{s.t.} \quad & \sum_{i=1}^{n} \varepsilon_i \leq n\varepsilon. \\ & \varepsilon_i \leq \varepsilon_{i,\max} \quad \forall i \in [n] \end{aligned} \tag{C.6}$$

Following KKT conditions [74], Equation (C.6) admits a closed-form solution. The solution indicates that by allowing heterogeneous privacy budgets and taking into account individual smooth sensitivities in the optimal allocation, we can improve the total error. These observations are summarized below:

Proposition C.3.3. *The following hold:*

1. *If* $\sum_{i=1}^{n} \varepsilon_{i,\max} \geq n\varepsilon$, *then the optimal solution to Equation* (C.6) *is*

$$\varepsilon_i^\star = \min\left\{\varepsilon_{i,\max}, \frac{n\varepsilon\sqrt{\Delta_{n,\Theta,i}}}{\sum_{j\in[n]}\sqrt{\Delta_{n,\Theta,j}}}\right\}$$

   for all $i \in [n]$. *Moreover, the improvement over* $\sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon}$ *satisfies* $\frac{\min_{i\in[n]}\Delta_{n,\Theta,i}}{\max_{i\in[n]}\Delta_{n,\Theta,i}} \leq \frac{\sum_{i=1}^{n}\frac{\Delta_{n,\Theta,i}}{\varepsilon_i}}{\sum_{i=1}^{n}\frac{\Delta_{n,\Theta,i}}{\varepsilon}} \leq 1$.

2. *If* $\sum_{i=1}^{n} \varepsilon_{i,\max} < n\varepsilon$ *then the optimal solution is* $\varepsilon_i^\star = \varepsilon_{i,\max}$ *for all* $i \in [n]$.

In a large network making individual nodes aware of their allocated budgets based on their smooth sensitivities is difficult to achieve in a central manner. The

following formulation of the allocation problem arrives at a sub-optimal solution that satisfies the $n\varepsilon$ global privacy budget constraint by imposing n additional constraints in the local neighborhoods: $a_{ii}\varepsilon_i + \sum_{j\in\mathcal{N}_i} a_{ij}\varepsilon_j \leq \varepsilon, \quad \forall i \in [n]$. The advantage of these constraints is that they can be verified locally, and satisfying them implies the $n\varepsilon$ global budget constraint in Equation (C.6). The subsequent optimization problem is given in Equation (C.7). It allows individuals to learn their allocated budgets in a distributed manner by running distributed gradient descent, which is guaranteed to converge since the problem is convex [360, Chapter 7].

$$\begin{aligned} \min_{\varepsilon_1,\ldots,\varepsilon_n>0} \quad & \sum_{i=1}^{n} \frac{\Delta_{n,\Theta,i}}{\varepsilon_i} \\ \text{s.t.} \quad & a_{ii}\varepsilon_i + \sum_{j\in\mathcal{N}_i} a_{ij}\varepsilon_j \leq \varepsilon, \quad \forall i \in [n] \\ & \varepsilon_i \leq \varepsilon_{i,\max}, \quad \forall i \in [n]. \end{aligned} \tag{C.7}$$

Numerical Experiment.. We test our method with the German Households dataset. Specifically, we set a per-agent average budget of $\varepsilon = 1$ for MVUE and $\varepsilon = 10$ for OL. We put a maximum individual budget cap of $\varepsilon_{i,\max} = 10\varepsilon$ in both cases. We report the sample paths in Supplementary Figures C.1 and C.2, and observe that the dynamics converge faster compared to the homogeneous case (cf. Figure 4.4). In Supplementary Figure C.3, we present an MSE plot where the MSE is plotted as a function of ε, and observe that the algorithm with the heterogeneous thresholds has smaller MSE compared to the homogeneous thresholds. These results confirm our theoretical observations in Proposition C.3.3.

Part 2: Learning and Inference in Discrete Hypothesis Spaces

C.4 Additional Related Work

In this section, we review the following collections of literature on privacy and group decision-making: *(i)* differential privacy, *(ii)* works at the intersection of group decision-making and social learning, *(iii)* privacy protections in social network contexts, *(iv)* literature in distributed learning and estimation, and *(v)* existing advances in the literature of privacy in healthcare contexts.

Differential privacy. Data privacy has evolved to incorporate various concepts, including K-anonymity. In modern definition, a mechanism is considered differentially private if it assigns similar records to the same value with equal likelihood. This definition has a significant implication. It ensures that the outcome of a statistical analysis remains consistent regardless of an individual's participation in the social learning process. Numerous existing mechanisms, such as the randomized response [416], the Laplace mechanism, and the Gaussian mechanism, can be demonstrated to adhere to differential privacy principles. The randomized response, for example, introduces random perturbations in binary responses, allowing the retrieval of population means while allowing individual respondents to maintain plausible deniability. It serves as an example of adding noise to the data.

When it comes to handling donated data for purposes such as providing recommendations to public policy agencies or submitting online product reviews

on e-commerce platforms, it is crucial to protect the privacy of data donors. This is because common anonymization techniques used in such scenarios are susceptible to different types of attacks, including identification risks [42], linkage and cross-referencing vulnerabilities [382, 383], as well as statistical difference and reidentification attacks [252]. Therefore, protecting the privacy of data donors becomes an essential aspect of statistical disclosure control in these contexts with important trade-offs between privacy and utility [438]. Our work contributes to the literature on DP by utilizing DP techniques to enable group decision making in distributed environments.

Group decision-making and social learning. The problem of aggregating the opinions and observations of different individuals into a coherent collective option arises naturally in jury deliberations, expert committees, medical diagnoses, or board meetings where several stakeholders must agree on a factual basis despite heterogeneity and uncertainty of their opinions and private information. A common way to resolve disagreements in such contexts is to engage in repeated peer interactions. Subsequently, a long line of literature goes back to seminal works of [28, 171, 121] that investigate the formation and evolution of Bayesian and non-Bayesian beliefs towards consensus agreement. This problem has close parallels in distributed estimation [73, 398], data fusion [281], as well as consensus and coordination in distributed control [216, 285]. The formation, evolution and aggregation of beliefs in distributed environments have attracted a lot of interest in statistics [174, 175, 170, 425, 337], engineering [232, 289, 197, 76, 426, 352, 114, 339, 387, 73, 398, 365], philosophy [259, 270, 126, 112], sociology [200, 162], machine learning [381], and economics [182, 123, 183, 217, 35, 125, 116], among others.

Of particular interest to us in this paper is the growing literature on non-Bayesian information aggregation and opinion pooling, going back to the classical work of DeGroot [121], who proposes linear opinion pools by averaging the latest beliefs of each agent with those of their neighbors. Several asymptotic properties and extensions of this model, including streams of private signals over time, are studied in the literature [217, 182, 123]. To combine beliefs on a finite set of alternatives, we use geometric averaging and logarithmic opinion pools, which also have a long history in Bayesian analysis and behavioral decision models [177, 358] and can be justified under specific axioms [287] or derived as a no-recall behavioral update rule [340, 341, 342]. In this paper, we ask how one should limit the information requirement of a non-Bayesian update to guarantee differential privacy and ensure consensus agreement and asymptotic learning for the agents.

Privacy-preserving methods in healthcare contexts. Data privacy and security are critical in healthcare contexts [23]. An example is multicenter clinical trials, which are often difficult to coordinate and conduct; see, for example, the AIDS Clinical Trials Group [84, 195]. In the literature, a variety of methods and protocols have been proposed for privacy-preserving data sharing between collaborating healthcare centers and data providers; see, for example, [414, 351, 163, 293]. Most of these methods are based on holomorphic encryption schemes and rely on centralized processing authority; see, e.g., [163, 293, 176]). In contrast, our method allows for fully distributed computation and does not require a centralized party to coordinate communication or computations between the centers. Furthermore, our method is based on statistical disclosure control following the differential privacy framework, which offers significant advantages in runtime and flexibility to accommodate a variety of statistical

models, including survival analysis [176, 163], logistic regression [176], and linear regression [163].

Differentially private hypothesis testing. There have recently been several works on differentially private hypothesis testing [85, 82, 310]. A work related to ours is the work of [30], which devises the most powerful differentially private hypothesis test for binary variables, which introduces a new type of DP noise: the TULAP noise. Our work differs from the work of [30] in two main axes: first, [30] can be viewed as a centralized test, while ours is decentralized and can only handle binary signals, where our work can support arbitrary distributions. The work of [233] utilizes and adapts the mechanism [30] to general distributions; however, the new mechanism is not distributed and does not have optimal statistical power. Moreover, the work of [85] shows that one of the noise distributions that optimize the sample complexity in nondistributed differentially private hypothesis testing is the Laplace noise. Similarly, in our work, we leverage the Laplace noise mechanism, which also has the added advantage of minimizing the convergence time of our distributed estimators.

Privacy in social network contexts. With our DP formulation for distributed learning environments, we can focus on privacy leaks through the information flow on the network rather than the underlying network structure. More broadly, the fundamental relationship between information flow and privacy is well noted, cf., contextual integrity [309, 52] or how social network contexts affect link formation and information sharing behaviors [5, 6]. Notwithstanding, the privacy implications of information diffusion and algorithmic intervention on social networks are largely unexplored, except in a few studies [346, 269, 345]. The existing work looks at this issue in specific, highly stylized scenarios. One

study shows that it is extremely hard to hide the existence of a giant connected component of infected nodes under an independent cascade model, and a simple inference attack can reveal the status of a good fraction of nodes [353]. In another study, the authors propose a decaying pseudo-noise added locally to mask the influence structure against an external observer with access to the entire information flow under the Friedkin-Johnsen influence propagation model [269].

Literature on Distributed Learning and Estimation. Our work builds upon the distributed learning algorithms presented in [343], by incorporating DP. Even though the belief updates posited in [343] are similar to the ones presented in this paper, the incorporation of noise makes the algorithms' behavior significantly different, which requires novel tools to analyze that the current paper provides. Moreover, the work of [343] provides asymptotic results for online learning and estimation, whereas, in our paper, we provide non-asymptotic results which flesh out the trade-offs between the privacy budget, the number of agents, the network, the errors, as well as the statistical models of the agents.

Moreover, an essential distinction between estimating a continuous quantity in [325, 267, 227, 354, 429] and choosing from a discrete set in this work is in the fact that DP randomization in the latter case induces a non-trivial failure probability that is bounded away from zero with increasing number of iterations. Hence, in our work, to satisfactorily control the quality of the group decision outcome, we need the agents to repeat their deliberations in multiple rounds and then aggregate the outcome of several rounds towards a collective belief. Different aggregation schemes are possible (e.g., based on arithmetic or geometric averaging of the beliefs and using different threshold rules to identify

the selected alternatives), which lead to different false-positive and missed detection rates and come with their own privacy guarantee and communication complexity requirements.

C.5 Non-Private Belief Propagation Algorithms

C.5.1 Non-private Distributed MLE

In the non-private regime, agents form beliefs $\mu_{i,t}(\widehat{\theta})$ over the states $\widehat{\theta} \in \Theta$ at every iteration t and exchange their beliefs with their neighbors until they can detect the MLE. [343] give Algorithm 11 for belief exchange and prove that beliefs converge to a uniform distribution over the MLE set (see Theorem 1 in their paper).

Algorithm 11 Non-Private Distributed MLE

The agents begin by forming: $\gamma_i(\widehat{\theta}) = \prod_{j=1}^{n_i} \ell_i(s_j|\widehat{\theta})$, and initializing their beliefs to $\mu_{i,0}(\widehat{\theta}) = \gamma_i(\widehat{\theta}) / \sum_{\tilde{\theta}\in\Theta} \gamma_i(\tilde{\theta})$. In any future time period, the agents update their belief after communication with their neighboring agents, and according to the following update rule:

$$\mu_{i,t}(\widehat{\theta}) = \frac{\mu_{i,t-1}^{1+a_{ii}}(\widehat{\theta}) \prod_{j\in\mathcal{N}_i} \mu_{j,t-1}^{a_{ij}}(\widehat{\theta})}{\sum_{\tilde{\theta}\in\Theta} \mu_{i,t-1}^{1+a_{ii}}(\tilde{\theta}) \prod_{j\in\mathcal{N}_i} \mu_{j,t-1}^{a_{ij}}(\tilde{\theta})}, \text{for all } \widehat{\theta} \in \Theta \text{ and } t \in [T]. \tag{C.8}$$

The convergence of this algorithm relies on studying the behavior of the log-belief ratio between two states $\widehat{\theta}$ and $\breve{\theta}$, whose dynamics are governed by the powers of the primitive matrix $A + I$, see [343, Theorem 1], with modulus-ordered eigenvalues $0 < |\lambda_n(A + I)| \leq \cdots \leq |\lambda_2(A + I)| < \lambda_1(A + I) = 2$. Specifically,

[343, Theorem 1] state that there is a dominant term due to the maximum eigenvalue $\lambda_1(A + I) = 2$ that dominates the log-belief ratios for large t, and $n - 1$ terms that decay exponentially with rate $(|\lambda_2(A + I)|/2)^t$. The dominant term depends on the difference of the log-likelihoods between the states $\widehat{\theta}$ and $\breve{\theta}$, namely $\Lambda(\widehat{\theta}, \breve{\theta}) = \Lambda(\widehat{\theta}) - \Lambda(\breve{\theta})$. Subsequently, the log-belief ratio approaches $-\infty$ as $t \to \infty$ whenever $\breve{\theta} \in \Theta^\star$, and we can recover the MLEs.

C.5.2 Non-private Online Learning from Intermittent Streams

[343] give Algorithm 12 for the agents to determine the true state θ° from their streams of observations in the online learning regime.

Algorithm 12 Non-Private Distributed Online Learning

Every time $t \in \mathbb{N}_0$, each agent forms the likelihood product of the signals that it has received at that iteration: $\gamma_{i,t}(\widehat{\theta}) = \prod_{j=1}^{n_{i,t}} \ell_i(s_{i,t}^j|\widehat{\theta})$, if $n_{i,t} \geq 1$, and $\gamma_{i,t}(\widehat{\theta}) = 1$ if $n_{i,t} = 0$. The agent then updates its belief according to:

$$\mu_{i,t}(\widehat{\theta}) = \frac{\gamma_{i,t}(\widehat{\theta})\mu_{i,t-1}^{a_{ii}}(\widehat{\theta}) \prod_{j\in\mathcal{N}_i} \mu_{j,t-1}^{a_{ij}}(\widehat{\theta})}{\sum\limits_{\tilde{\theta}\in\Theta} \gamma_{i,t}(\tilde{\theta})\mu_{i,t-1}^{a_{ii}}(\tilde{\theta}) \prod_{j\in\mathcal{N}_i} \mu_{j,t-1}^{a_{ij}}(\tilde{\theta})}, \text{ for all } \widehat{\theta} \in \Theta \text{ and } t \in [T], \tag{C.9}$$

initialized by: $\mu_{i,0}(\widehat{\theta}) = \gamma_{i,0}(\widehat{\theta}) / \sum_{\tilde{\theta}\in\Theta} \gamma_{i,0}(\tilde{\theta})$.

[343] prove that this algorithm converges to learning the true state asymptotically. Their argument relies on the fact that the time average of the log-belief ratio between any state $\widehat{\theta} \in \Theta$ and the true state θ°, $(1/t)\log(\mu_{i,t}(\widehat{\theta})/\mu_{i,t}(\theta^\circ))$, converges to the weighted sum of the KL divergences of all agents, which is less than zero if the models are statistically identifiable.

C.6 Proofs and Convergence Analysis for Distributed, Private MLE

C.6.1 Log-Belief Ratio Notations

Let $\mu_{i,t}(\widehat{\theta})$ be the beliefs for the nonprivate system, and let $\nu_{i,k,t}(\widehat{\theta})$ be the private estimates for agent $i \in [n]$, at the time step $t \geq 0$ of round $k \in [K]$. For the non-private algorithm (Algorithm 11) all pairs $\widehat{\theta}, \breve{\theta} \in \Theta$ we let $\phi_{i,t}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\mu_{i,t}(\widehat{\theta})}{\mu_{i,t}(\breve{\theta})}\right)$ and $\lambda_i(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\gamma_i(\widehat{\theta})}{\gamma_i(\breve{\theta})}\right)$ be the log belief ratios and the log-likelihood ratios of the agent $i \in [n]$ in the time step $t \geq 0$. For the private algorithm (Algorithm 8) we let $\psi_{i,k,t}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\nu_{i,k,t}(\widehat{\theta})}{\nu_{i,k,t}(\breve{\theta})}\right)$, $\zeta_{i,k}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\sigma_{i,k}(\widehat{\theta})}{\sigma_{i,k}(\breve{\theta})}\right)$, and $\kappa_{i,k}(\widehat{\theta}, \breve{\theta}) = d_{i,k}(\widehat{\theta}) - d_{i,k}(\breve{\theta})$ be the private log-belief ratio, log-likelihood ratio and log of the noise ratio between states $\widehat{\theta}$ and $\breve{\theta}$ for agent $i \in [n]$ at time step $t \geq 0$ of round $k \in [K]$, and denote their vectorized versions by $\phi_t(\widehat{\theta}, \breve{\theta})$, $\psi_{k,t}(\widehat{\theta}, \breve{\theta})$, $\lambda(\widehat{\theta}, \breve{\theta})$, and $\zeta_k(\widehat{\theta}, \breve{\theta})$, respectively, where the vectorization is over the agents $i \in [n]$. We define $\Lambda(\widehat{\theta}, \breve{\theta}) = \mathbb{1}^T \lambda(\widehat{\theta}, \breve{\theta})$, $Z_k(\widehat{\theta}, \breve{\theta}) = \mathbb{1}^T \zeta_k(\widehat{\theta}, \breve{\theta}) = \mathbb{1}^T \left(\lambda(\widehat{\theta}, \breve{\theta}) + \kappa_k(\widehat{\theta}, \breve{\theta})\right)$.

We say that a stochastic process $\{X_t\}_{t \in \mathbb{N}}$ converges in L_2 to X, and write $X_t \xrightarrow{L_2} X$, if and only if $\lim_{t \to \infty} \mathbb{E}\left[\|X_t - X\|_2\right] = 0$. Convergence in L_2 implies convergence in probability (i.e., $X_t \xrightarrow{p} X$) due to Markov's inequality.

To prove the results, we need the following auxiliary lemma:

Lemma C.6.1. *Let $X_1, \ldots, X_n$ be i.i.d. draws from a distribution $\mathcal{D}$. Then, for every $i \in [n]$, we have $\mathbb{P}[X_i \geq \max_{j \neq i} X_j] = 1/n$.*

Let $E_i = \{X_i \geq \max_{j \neq i} X_j\}$. Note that because $X_1, \ldots, X_n$ are i.i.d. $\mathbb{P}[E_1] = \mathbb{P}[E_2] = \cdots = \mathbb{P}[E_n]$. Moreover, note that since the maximum is unique, we have that

$E_1, \ldots, E_n$ are a partition of the sample space. Therefore, we get $\sum_{i\in[n]} \mathbb{P}[E_i] = 1$, and subsequently $\mathbb{P}[E_i] = 1/n$. □

C.6.2 Proof of Theorem 4.2.1

Similarly to [343, Theorem 1], we have that for any $k \in [K]$

$$\begin{aligned}
\left\|\psi_{k,t}(\widehat{\theta},\breve{\theta}) - \frac{2^t}{n} Z_k(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2 &= \left\|\sum_{i=2}^{n}\left(\frac{\lambda_i(A+I)}{2}\right)^t l_i r_i^T \zeta_k(\widehat{\theta},\breve{\theta})\right\|_2 \\
&\leq \sum_{i=2}^{n}\left|\frac{\lambda_i(A+I)}{2}\right|^t \|l_i\|_2 \left|r_i^T \zeta_k(\widehat{\theta},\breve{\theta})\right| \\
&\leq \sum_{i=2}^{n}\left|\frac{\lambda_i(A+I)}{2}\right|^t \left\|\zeta_k(\widehat{\theta},\breve{\theta})\right\|_2 \\
&\leq \sum_{i=2}^{n}\left|\frac{\lambda_i(A+I)}{2}\right|^t \left(\left\|\lambda(\widehat{\theta},\breve{\theta})\right\|_2 + \left\|\kappa_k(\widehat{\theta},\breve{\theta})\right\|_2\right).
\end{aligned}$$

Taking expectations and applying Jensen's inequality, we can bound the above as

$$\mathbb{E}\left[\left\|\psi_{k,t}(\widehat{\theta},\breve{\theta}) - \frac{2^t}{n} Z_k(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2\right] \leq 2(n-1)\left|\frac{\lambda_2(A+I)}{2}\right|^t \left[n\Gamma_{n,\Theta} + \sum_{i=1}^{n}\sqrt{\mathbb{V}\left[d_{i,k}(\widehat{\theta})\right]}\right], \tag{C.10}$$

where $\Gamma_{n,\Theta} = \max_{i\in[n],\widehat{\theta}\in\Theta} |\log \gamma_i(\widehat{\theta})|$ and $|\lambda_2(A+I)|/2 < 1$ is the SLEM of $(A+I)/2$; A is doubly stochastic so $0 < |\lambda_n(A+I)| \leq \cdots \leq |\lambda_{n-1}(A+I)| < \lambda_1(A+I) = 2$. Note that the right-hand side in Equation (C.10) goes to 0 as $t \to \infty$, which implies that (by Markov's inequality) $\psi_{k,t}(\widehat{\theta},\breve{\theta}) \xrightarrow{L_2} \frac{2^t}{n} Z_k(\widehat{\theta},\breve{\theta})\mathbb{1}$.

Let $\theta^\star \in \Theta^\star$ and $\bar{\theta} \in \bar{\Theta}$. Based on our definition of $\Lambda(\cdot,\cdot)$ we should have $\Lambda(\bar{\theta},\theta^\star) < 0$ and the corresponding non-private algorithm would have $\phi_{i,t}(\bar{\theta},\theta^\star) \to -\infty$ for every $\bar{\theta} \in \bar{\Theta}$ and $\theta^\star \in \Theta^\star$. However, when noise is introduced,

there could be mistakes introduced in the log-belief ratios, even if $\Lambda(\bar{\theta}, \theta^\star) < 0$ we can have $Z_k(\bar{\theta}, \theta^\star) \geq 0$ which implies $\psi_{i,k,t}(\bar{\theta}, \theta^\star) \not\to -\infty$.

AM estimator. For all $\widehat{\theta} \in \Theta$ we let $Y_j(\widehat{\theta}) = \sum_{i=1}^n d_{i,k}(\widehat{\theta})$. We focus on a single $\theta^\star \in \Theta^\star$. It is easy to show that because the noise is independent across the agents, and i.i.d. between the states for a given agent i, then $Y_j(\bar{\theta})$ and $Y_j(\theta^\star)$ are also i.i.d. for all $\bar{\theta} \in \bar{\Theta}$, and therefore we have that (see Lemma C.6.1)

$$\lim_{T\to\infty} \mathbb{P}\left[\nu_{i,k,T}(\theta^\star) > 0\right] \geq \mathbb{P}\left[\bigcap_{\bar{\theta}\in\bar{\Theta}} \left\{Y_k(\bar{\theta}) \leq Y_k(\theta^\star)\right\}\right] = \frac{1}{|\bar{\Theta}|}.$$

Therefore, for the AM estimator we have the following:

$$\lim_{T\to\infty} \mathbb{P}\left[\nu^{\mathrm{AM}}_{i,T}(\theta^\star) = 0\right] = \lim_{T\to\infty} \mathbb{P}\left[\bigcap_{k\in[K]} \{\nu_{i,k,T}(\theta^\star) = 0\}\right] \leq \left(1 - \frac{1}{|\bar{\Theta}|}\right)^K \leq e^{-\frac{K}{|\bar{\Theta}|}}, \tag{C.11}$$

and the failure probability of the AM estimator can be calculated by applying the union bound as

$$\begin{aligned}
\lim_{T\to\infty} \mathbb{P}\left[\Theta^\star \not\subseteq \widehat{\Theta}^{\mathrm{AM}}_{i,T}\right] &= \lim_{T\to\infty} \mathbb{P}\left[\exists \theta^\star \in \Theta^\star : \nu^{\mathrm{AM}}_{i,T}(\theta^\star) = 0\right] \\
&\leq \lim_{T\to\infty} \sum_{\theta^\star\in\Theta^\star} \mathbb{P}\left[\nu^{\mathrm{AM}}_{i,T}(\theta^\star) = 0\right] \\
&\leq |\Theta^\star| e^{-\frac{K}{|\bar{\Theta}|}}.
\end{aligned}$$

Setting $K = |\bar{\Theta}| \log(|\Theta^\star|/(1-\beta))$, we can ensure that the Type II error rate is at most $1-\beta$.

GM estimator. Similarly, for $\nu^{\mathrm{GM}}_{i,T}$ we have the following:

$$\lim_{T\to\infty} \mathbb{P}\left[\nu_{i,k,T}(\bar{\theta}) = 0\right] \geq \mathbb{P}\left[\bigcap_{\theta^\star\in\Theta^\star} \left\{Y_k(\bar{\theta}) \leq Y_k(\theta^\star)\right\}\right] = \frac{1}{|\Theta^\star|},$$

for all $\bar{\theta} \in \bar{\Theta}$ and subsequently

$$\lim_{T\to\infty} \mathbb{P}\left[\nu_{i,T}^{\mathrm{GM}}(\bar{\theta}) > 0\right] = \lim_{T\to\infty} \mathbb{P}\left[\bigcap_{k\in[K]} \left\{\nu_{i,k,T}(\bar{\theta}) > 0\right\}\right] \leq \left(1 - \frac{1}{|\Theta^\star|}\right)^K \leq e^{-\frac{K}{|\Theta^\star|}},$$

and

$$\begin{aligned}
\lim_{T\to\infty} \mathbb{P}\left[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \not\subseteq \Theta^\star\right] &= \lim_{T\to\infty} \mathbb{P}\left[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \cap \bar{\Theta} \neq \emptyset\right] \\
&= \lim_{T\to\infty} \mathbb{P}\left[\exists \bar{\theta} \in \bar{\Theta} : \nu_{i,T}^{\mathrm{GM}}(\bar{\theta}) > 0\right] \\
&\leq \lim_{T\to\infty} \sum_{\bar{\theta}\in\bar{\Theta}} \mathbb{P}\left[\nu_{i,T}^{\mathrm{GM}}(\bar{\theta}) > 0\right] \\
&\leq |\bar{\Theta}| e^{-\frac{K}{|\Theta^\star|}}.
\end{aligned}$$

Therefore, selecting $K = |\Theta^\star| \log(|\bar{\Theta}|/\alpha)$ produces a Type I error rate of at most α.

Differentially Private Outputs. Due to the postprocessing property of DP (see Proposition 2.1 of [135]), the resulting estimates are ε-DP with respect to the private signals.

C.6.3 Proof of Theorem 4.2.2

For simplicity of exposition, we have set $\varrho^{\mathrm{AM}} = \varrho^{\mathrm{GM}} = \varrho$ which corresponds to $\tau^{\mathrm{AM}} = \tau^{\mathrm{GM}} = \tau$.

GM estimator. We let $Y_k(\widehat{\theta}) = \sum_{i\in[n]} d_{i,k}(\widehat{\theta})$. We define the event $F =$

$\left\{\exists k \in [K], \bar{\theta} \in \bar{\Theta}, \theta^\star \in \Theta^\star : Z^{\mathrm{GM}}(\bar{\theta}, \theta^\star) > \Lambda(\bar{\theta}, \theta^\star)\right\}$. We have that

$$\begin{aligned}
\mathbb{P}[F] &\overset{\text{(i)}}{\leq} \sum_{\bar{\theta}\in\bar{\Theta}} \mathbb{P}\left[\exists k \in [K], \theta^\star \in \Theta^\star : Z_k(\bar{\theta}, \theta^\star) > \Lambda(\bar{\theta}, \theta^\star)\right] \\
&\overset{\text{(ii)}}{=} \sum_{\bar{\theta}\in\bar{\Theta}} \left(1 - \mathbb{P}\left[\forall \theta^\star \in \Theta^\star : Z_1(\bar{\theta}, \theta^\star) \leq \Lambda(\bar{\theta}, \theta^\star)\right]\right)^K \\
&\overset{\text{(iii)}}{\leq} |\bar{\Theta}|\left(1 - \mathbb{P}\left[\bigcap_{\bar{\theta}\in\bar{\Theta}} \left\{Y_1(\bar{\theta}) \leq Y_1(\theta^\star)\right\}\right]\right)^K \\
&\overset{\text{(iv)}}{\leq} |\bar{\Theta}|\left(1 - \frac{1}{|\Theta^\star|}\right)^K \\
&\overset{\text{(v)}}{\leq} |\bar{\Theta}| e^{-K/|\Theta^\star|},
\end{aligned}$$

where the above follows (i) from the application of the union bound, (ii) using the fact that the K rounds are independent, (iii) the fact that $\{Z_1(\bar{\theta}, \theta^\star) \leq \Lambda(\bar{\theta}, \theta^\star)\} \supseteq \bigcap_{\bar{\theta}\in\bar{\Theta}} \left\{Y_k(\bar{\theta}) \leq Y_k(\theta^\star)\right\}$ and that $\{Y_k(\bar{\theta})\}_{\bar{\theta}\in\bar{\Theta}}$ and $Y_k(\theta^\star)$ are i.i.d., (iv) Lemma C.6.1, and (v) $1 + x \leq e^x$ for all $x \in \mathbb{R}$.

For each round k of the algorithm and each pair of states $\widehat{\theta}, \breve{\theta} \in \Theta$, the following holds for the log-belief ratio of the geometrically averaged estimates:

$$\psi_{i,t}^{\mathrm{GM}}(\widehat{\theta}, \breve{\theta}) = \frac{1}{K} \sum_{k\in[K]} \psi_{i,k,t}(\widehat{\theta}, \breve{\theta}).$$

We let $Z^{\mathrm{GM}}(\widehat{\theta}, \breve{\theta}) = \frac{1}{K}\sum_{k=1}^K Z_k(\widehat{\theta}, \breve{\theta})$. By the triangle inequality and Theorem 4.2.1

$$\mathbb{E}\left[\left\|\psi_t(\widehat{\theta}, \breve{\theta}) - \frac{2^t}{n} Z^{\mathrm{GM}}(\widehat{\theta}, \breve{\theta})\mathbb{1}\right\|_2\right] \leq \frac{1}{\sqrt{K}} \sum_{k=1}^K \mathbb{E}\left[\left\|\psi_{k,t}(\widehat{\theta}, \breve{\theta}) - \frac{2^t}{n} Z_k(\widehat{\theta}, \breve{\theta})\mathbb{1}\right\|_2\right]. \tag{C.12}$$

For every round $k \in [K]$,

$$\begin{aligned}\left\|\psi_{k,t}(\widehat{\theta},\breve{\theta}) - \frac{2^t}{n} Z_k(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2 &= \left\|\sum_{i=2}^{n}\left(\frac{\lambda_i(I+A)}{2}\right)^t l_i r_i^T \zeta_k(\widehat{\theta},\breve{\theta})\right\|_2 \\ &\le \sum_{i=2}^{n}\left|\frac{\lambda_i(I+A)}{2}\right|^t \|l_i\|_2 \left|r_i^T \zeta_k(\widehat{\theta},\breve{\theta})\right| \\ &\le \sum_{i=2}^{n}\left|\frac{\lambda_i(I+A)}{2}\right|^t \left\|\zeta_k(\widehat{\theta},\breve{\theta})\right\|_2 \\ &\le \sum_{i=2}^{n}\left|\frac{\lambda_i(I+A)}{2}\right|^t \left(\left\|\lambda(\widehat{\theta},\breve{\theta})\right\|_2 + \left\|\kappa_k(\widehat{\theta},\breve{\theta})\right\|_2\right).\end{aligned}$$

Taking expectations and applying Jensen's inequality, we can bound the above as

$$\mathbb{E}\left[\left\|\psi_{k,t}(\widehat{\theta},\breve{\theta}) - \frac{2^t}{n} Z_k(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2\right] \le 2(n-1)\left|\frac{\lambda_2(I+A)}{2}\right|^t \left[n\Gamma_{n,\Theta} + \sum_{i=1}^{n}\sqrt{\mathbb{V}\left[d_{i,k}(\widehat{\theta})\right]}\right]. \tag{C.13}$$

Using $a_n^\star = \left|\frac{\lambda_2(I+A)}{2}\right|$, and combining Equation (C.12) with Equation (C.13), we get:

$$\mathbb{E}\left[\left\|\psi_t(\widehat{\theta},\breve{\theta}) - \frac{2^t}{n} Z^{\mathrm{GM}}(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2\right] \le \frac{2(n-1)(a_n^\star)^t[n\Gamma_{n,\Theta} + V_{n,\Theta}]}{\sqrt{K}}. \tag{C.14}$$

By Markov's inequality and Equation (C.12), we get that for every $z > 0$

$$\mathbb{P}\left[\left\|\psi_t^{\mathrm{GM}}(\widehat{\theta},\breve{\theta}) - \frac{2^t}{n} Z^{\mathrm{GM}}(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2 > z\right] \le \frac{2(n-1)(a_n^\star)^t[n\Gamma_{n,\Theta} + V_{n,\Theta}]}{z\sqrt{K}}.$$

We let the RHS be equal to $\alpha/(|\Theta^\star||\bar{\Theta}|)$, which corresponds to letting $z = |\bar{\Theta}||\Theta^\star|\frac{2(n-1)(a_n^\star)^t[n\Gamma_{n,\Theta}+V_{n,\Theta}]}{\alpha\sqrt{K}}$. By applying a union bound over $\bar{\Theta}$ and $\Theta^\star$ we have that for every $\bar{\theta} \in \bar{\Theta}$ and $\theta^\star \in \Theta^\star$, with probability at least $1-\alpha$,

$$\psi_{i,t}^{\mathrm{GM}}(\bar{\theta},\theta^\star) \le \frac{2^t}{n} Z^{\mathrm{GM}}(\bar{\theta},\theta^\star) + |\bar{\Theta}||\Theta^\star|\frac{2(n-1)(a_n^\star)^t[n\Gamma_{n,\Theta} + V_{n,\Theta}]}{\alpha\sqrt{K}}. \tag{C.15}$$

Conditioned on F^c, the above becomes

$$\begin{aligned}\psi_{i,t}^{\mathrm{GM}}(\bar{\theta},\theta^\star) &\leq \frac{2^t}{n}\Lambda(\bar{\theta},\theta^\star) + |\bar{\Theta}||\Theta^\star|\frac{2(n-1)(a_n^\star)^t[n\Gamma_{n,\Theta}+V_{n,\Theta}]}{\alpha\sqrt{K}} \\ &\leq -\frac{2^t}{n}l_{n,\Theta} + |\Theta|^2\frac{(n-1)(a_n^\star)^t[n\Gamma_{n,\Theta}+V_{n,\Theta}]}{2\alpha\sqrt{K}}. \end{aligned} \tag{C.16}$$

Note that we have used $|\bar{\Theta}||\Theta^\star| = (|\Theta| - |\Theta^\star|)|\Theta^\star| \leq |\Theta|^2/4$. To make Equation (C.16) at most $-\varrho$ for some $\varrho > 0$, we need to set

$$t \geq \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2\alpha\varrho\sqrt{K}}\right)}{\log(1/a_n^\star)}\right\} = T.$$

The log-belief ratio threshold implies that for all $\theta^\star \in \Theta^\star, \bar{\theta} \in \bar{\Theta}$ we have that $\nu_{i,k,T}(\theta^\star) \geq e^{\varrho}\nu_{i,k,T}(\bar{\theta})$. To determine the belief threshold τ, note that

$$\begin{aligned} 1 &= \sum_{\widehat{\theta}\in\widehat{\Theta}_{i,T}^{\mathrm{GM}}} \nu_{i,k,T}(\widehat{\theta}) + \sum_{\widehat{\theta}\notin\widehat{\Theta}_{i,T}^{\mathrm{GM}}} \nu_{i,k,T}(\widehat{\theta}) \geq (1+e^{\varrho}) \max_{\widehat{\theta}\notin\Theta_{i,T}^{\mathrm{GM}}} \nu_{i,k,T}(\widehat{\theta}) \\ &\implies \max_{\widehat{\theta}\notin\Theta_{i,T}^{\mathrm{GM}}} \nu_{i,k,T}(\widehat{\theta}) \leq \frac{1}{1+e^{\varrho}}. \end{aligned}$$

Moreover, we can prove that $\min_{\widehat{\theta}\in\widehat{\Theta}_{i,T}^{\mathrm{GM}}} \nu_{i,k,T}(\widehat{\theta}) \geq \frac{1}{1+e^{-\varrho}} \geq \frac{1}{1+e^{\varrho}}$ since $\varrho > 0$ which shows that any value in $[1/(1+e^{\varrho}), 1/(1+e^{-\varrho})]$ is a valid threshold. This yields that $\mathbb{P}[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star|F^c] = \mathbb{P}[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \cap \bar{\Theta} = \emptyset|F^c] = \mathbb{P}[\exists\bar{\theta} \in \bar{\Theta} : \nu_{i,T}^{\mathrm{GM}}(\bar{\theta}) > \tau|F^c] \geq 1-\alpha$. Subsequently, by letting $K = |\Theta^\star|\log(|\bar{\Theta}|/\alpha)$, we get that

$$\mathbb{P}[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star] \geq \mathbb{P}[\widehat{\Theta}_{i,T}^{\mathrm{GM}} \subseteq \Theta^\star|F^c]\mathbb{P}[F^c] \geq (1-\alpha)^2 \geq 1-2\alpha.$$

AM estimator. We let $E = \left\{\exists k \in [K], \bar{\theta} \in \bar{\Theta}, \theta^\star \in \Theta^\star : Z_k(\theta^\star,\bar{\theta}) < \Lambda(\theta^\star,\bar{\theta})\right\}$. Using similar arguments to Theorem 4.2.2, we can deduce that $\mathbb{P}[E] \leq |\Theta^\star|e^{-K/|\bar{\Theta}|}$. By setting $K = |\bar{\Theta}|\log(|\Theta^\star|/(1-\beta))$, we make $\mathbb{P}[E] \leq 1-\beta$.

Conditioned on E^c and by applying Markov's inequality, similarly to Equation (C.16) for the GM estimator, we have that for all $\theta^\star \in \Theta^\star, \bar{\theta} \in \bar{\Theta}$ and run $k \in [K]$

$$\begin{aligned}\psi_{i,k,t}(\theta^\star, \bar{\theta}) &\geq \frac{2^t}{n} Z_k(\theta^\star, \bar{\theta}) - |\Theta^\star||\bar{\Theta}| \frac{2(n-1)(a_n^\star)^t(n\Gamma_{n,\Theta} + V_{n,\Theta})}{1-\beta'} \\ &\geq \frac{2^t}{n} \Lambda(\theta^\star, \bar{\theta}) - |\Theta|^2 \frac{(n-1)(a_n^\star)^t(n\Gamma_{n,\Theta} + V_{n,\Theta})}{2(1-\beta')} \\ &\geq \frac{2^t}{n} l_{n,\Theta} - |\Theta|^2 \frac{2(n-1)(a_n^\star)^t(n\Gamma_{n,\Theta} + V_{n,\Theta})}{2(1-\beta')},\end{aligned} \tag{C.17}$$

with probability β' for some $\beta' \in (0,1)$. To make the above at least ϱ for some $\varrho > 0$ it suffices to pick

$$t \geq \max\left\{ \frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2(1-\beta')\varrho}\right)}{\log(1/a_n^\star)} \right\} = T.$$

The log-belief ratio threshold implies that for all $\theta^\star \in \Theta^\star, \bar{\theta} \in \bar{\Theta}$ we have that $\nu_{i,k,T}(\theta^\star) \geq e^{\varrho} \nu_{i,k,T}(\bar{\theta})$. Similarly, any value in $[1/(1+e^{\varrho}), 1/(1+e^{-\varrho})]$ is a valid threshold, we can show that

$$
\begin{aligned}
\mathbb{P}[\Theta^\star \subseteq \widehat{\Theta}^{\mathrm{AM}}_{i,T} | E^c] &= \mathbb{P}\left[\forall \theta^\star \in \Theta^\star : \nu^{\mathrm{AM}}_{i,T}(\theta^\star) > \tau \middle| E^c\right] \\
&\geq \mathbb{P}\left[\bigcup_{k\in[K]} \{\forall \theta^\star \in \Theta^\star : \nu_{i,k,T}(\theta^\star) > \tau\} \middle| E^c\right] \\
&= 1 - \mathbb{P}\left[\bigcap_{k\in[K]} \{\exists \theta^\star \in \Theta^\star : \nu_{i,k,T}(\theta^\star) < \tau\} \middle| E^c\right] \\
&= 1 - \left(\mathbb{P}\left[\exists \theta^\star \in \Theta^\star : \nu_{i,k,T}(\theta^\star) < \tau \middle| E^c\right]\right)^K \\
&= 1 - \left(1 - \mathbb{P}\left[\forall \theta^\star \in \Theta^\star : \nu_{i,k,T}(\theta^\star) > \tau \middle| E^c\right]\right)^K \\
&= 1 - (\beta')^K \\
&\geq 1 - e^{-(1-\beta')K}.
\end{aligned}
$$

We set $1 - \beta' = \log(1/(1-\beta))/K$ and have that

$$
\mathbb{P}[\Theta^\star \subseteq \widehat{\Theta}^{\mathrm{AM}}_{i,T}] \geq \mathbb{P}[E^c]\mathbb{P}[\Theta^\star \subseteq \widehat{\Theta}^{\mathrm{AM}}_{i,T} | E^c] \geq (\beta)^2 \geq 1 - 2(1-\beta).
$$

These finally yield

$$
T = \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{|\Theta|^2(n-1)K(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2\log(1/(1-\beta))\varrho}\right)}{\log(1/a^\star_n)}\right\}.
$$

Privacy (for both estimators). Minimizing the convergence time T corresponds to minimizing $V_{n,\Theta}$. Since $V_{n,\Theta}$ is separable over the agents, it suffices to solve the problem of minimizing the variance of each noise variable independently.

If an adversary can eavesdrop only once and has access to any round $k \in [K]$, and we have $|\Theta|$ states, by the composition theorem, the budget ε should be

divided by $K|\Theta|$. Thus, the problem of finding the optimal distribution $\mathcal{D}_i(\varepsilon)$ on $\mathbb{R}$, corresponds to the following optimization problem studied in [247, 325], for all $k \in [K]$:

$$\begin{aligned} \min_{\mathcal{D}_i(\varepsilon) \in \text{Simplex}(\mathbb{R})} \quad & \mathbb{V}_{d_{i,k} \sim \mathcal{D}_i(\varepsilon)} [d_{i,k}] \\ \text{s.t.} \quad & \mathcal{D}_i(\varepsilon) \text{ is } \frac{\varepsilon}{K|\Theta|}\text{-DP and } \mathbb{E}_{d_{i,k} \sim \mathcal{D}_i(\varepsilon)} [d_{i,k}] = 0. \end{aligned} \tag{C.18}$$

The optimal solution to this problem is given by [247, 325]. For privatizing beliefs in our problem, this corresponds to selecting $\mathcal{D}_i^\star(\varepsilon) = \text{Lap}\left(\frac{\Delta_{n,\Theta} K|\Theta|}{\varepsilon}\right)$ where $\Delta_{n,\Theta}$ is the sensitivity of the log-likelihood of the i-th agent.

Differentially Private Outputs. Due to the postprocessing property of DP (see Proposition 2.1 of [135]), the resulting estimates are ε-DP with respect to the private signals.

□

C.6.4 Proof of Theorem 4.2.3

For simplicity, we define $p_2 = 1/|\bar{\Theta}|$ and $p_1 = 1 - 1/|\Theta^\star|$, and assume that $\varrho^{\text{thres},1} = \varrho^{\text{thres},2} = \varrho$ which implies that $\hat{\tau}^{\text{thres},1} = \hat{\tau}^{\text{thres},2} = \tau$ and $N_{i,t}^{\text{thres},1}(\widehat{\theta}) = N_{i,t}^{\text{thres},2}(\widehat{\theta}) = N_{i,T}(\widehat{\theta})$.

Type I estimator ($\widehat{\Theta}_{i,T}^{\text{thres},1}$). To determine the asymptotic Type I error probability α of $\widehat{\Theta}_{i,T}^{\text{thres},1}$, we assume that the threshold takes the form $\tau^{\text{thres},1} = (1 + \pi_1)p_1$. Then

$$\begin{aligned}
\lim_{T\to\infty} \mathbb{P}\left[\widehat{\Theta}_{i,T}^{\text{thres},1} \not\subseteq \Theta^\star\right] &\overset{\text{(i)}}{=} \lim_{T\to\infty} \mathbb{P}\left[\exists \bar{\theta} \in \bar{\Theta} : \bar{\theta} \in \widehat{\Theta}_{i,T}^{\text{thres},1}\right] \\
&\overset{\text{(ii)}}{\leq} \lim_{T\to\infty} \sum_{\bar{\theta}\in\bar{\Theta}} \mathbb{P}\left[\bar{\theta} \in \widehat{\Theta}_{i,T}^{\text{thres},1}\right] \\
&\overset{\text{(iii)}}{\leq} \lim_{T\to\infty} \sum_{\bar{\theta}\in\bar{\Theta}} \mathbb{P}\left[N_{i,T}(\bar{\theta}) \geq \tau^{\text{thres},1}\right] \\
&\leq \lim_{T\to\infty} \sum_{\bar{\theta}\in\bar{\Theta}} \mathbb{P}\left[N_{i,T}(\bar{\theta}) \geq (1+\pi_1)p_1\right] \\
&\overset{\text{(iv)}}{\leq} \lim_{T\to\infty} \sum_{\bar{\theta}\in\bar{\Theta}} \mathbb{P}\left[N_{i,T}(\bar{\theta}) \geq (1+\pi_1)\mathbb{E}\left[N_{i,T}(\bar{\theta})\right]\right] \\
&\overset{\text{(v)}}{\leq} |\bar{\Theta}| e^{-2K\pi_1^2},
\end{aligned} \tag{C.19}$$

where the result is derived by applying (i) the definition of $\widehat{\Theta}_{i,T}^{\text{thres},1}$, (ii) union bound, (iii) the definition of the threshold $\tau^{\text{thres},1} = (1+\pi_1)p_1$, (iv) the fact that $\mathbb{E}\left[N_{i,T}(\bar{\theta})\right] \leq p_1$ for all $\bar{\theta} \in \bar{\Theta}$ as $T \to \infty$, and the Chernoff bound on $N_{i,T}(\bar{\theta})$. Therefore, to make the above α, it suffices to choose $K = \frac{\log(|\bar{\Theta}|/\alpha)}{2\pi_1^2}$.

Type II estimator ($\widehat{\Theta}_{i,T}^{\text{thres},2}$). To determine the asymptotic Type II error probability $1-\beta$ of $\widehat{\Theta}_{i,T}^{\text{thres},2}$, we assume that the threshold takes the form $\tau^{\text{thres},2} = (1-\pi_2)p_2$. Then

$$\begin{aligned}
\lim_{T\to\infty} \mathbb{P}\left[\Theta^\star \not\subseteq \widehat{\Theta}_{i,T}^{\text{thres},2}\right] &\overset{\text{(i)}}{=} \lim_{T\to\infty} \mathbb{P}\left[\exists \theta^\star \in \Theta^\star : \theta^\star \notin \Theta_{i,T}^{\text{thres},2}\right] \\
&\overset{\text{(ii)}}{\leq} \lim_{T\to\infty} \sum_{\theta^\star\in\Theta^\star} \mathbb{P}\left[\theta^\star \notin \Theta_{i,T}^{\text{thres},2}\right] \\
&\overset{\text{(iii)}}{\leq} \lim_{T\to\infty} \sum_{\theta^\star\in\Theta^\star} \mathbb{P}\left[N_{i,T}(\theta^\star) \leq \tau^{\text{thres},2}\right] \\
&\overset{\text{(iii)}}{\leq} \lim_{T\to\infty} \sum_{\theta^\star\in\Theta^\star} \mathbb{P}\left[N_{i,T}(\theta^\star) \leq (1-\pi_2)p_2\right] \\
&\overset{\text{(iv)}}{\leq} \lim_{T\to\infty} \sum_{\theta^\star\in\Theta^\star} \mathbb{P}\left[N_{i,T}(\theta^\star) \leq (1-\pi_2)\mathbb{E}\left[N_{i,T}(\theta^\star)\right]\right] \\
&\overset{\text{(v)}}{\leq} |\Theta^\star| e^{-2K\pi_2^2},
\end{aligned} \tag{C.20}$$

where the result is derived by applying (i) the definition of $\widehat{\Theta}_{i,T}^{\text{thres},2}$, (ii) union bound, (iii) the definition of the threshold $\tau^{\text{thres},2} = (1-\pi_2)p_2$, (iv) the fact that $\mathbb{E}\left[N_{i,T}(\theta^\star)\right] \geq p_2$ for all $\theta^\star \in \Theta^\star$ as $T \to \infty$, and (v) the Chernoff bound on $N_{i,T}(\widehat{\theta})$. Therefore, to make the above less than $1-\beta$, it suffices to choose $K = \frac{\log(|\bar{\Theta}|/(1-\beta))}{2\pi_2^2}$.

Differentially Private Outputs. Due to the immunity to post-processing of DP [135, Proposition 2.1], the resulting estimates are ε-DP with respect to private signals.

□

C.6.5 Proof of Theorem 4.2.5

For simplicity, we assume that $\varrho^{\text{thres},1} = \varrho^{\text{thres},2} = \varrho$ which implies that $\widehat{\tau}^{\text{thres},1} = \widehat{\tau}^{\text{thres},2} = \tau$ and $N_{i,t}^{\text{thres},1}(\widehat{\theta}) = N_{i,t}^{\text{thres},2}(\widehat{\theta}) = N_{i,T}(\widehat{\theta})$.

Type I estimator. From the analysis of Theorem 4.2.2 (see Equation (C.16)),

setting

$$t \geq \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{(n-1)|\Theta|^2(n\Gamma_{n,\Theta}+V_{n,\Theta})}{q_1\varrho}\right)}{\log(1/a_n^\star)}\right\} = T,$$

guarantees that $\mathbb{E}\left[N_{i,T}(\bar{\theta})\right] = \mathbb{P}\left[\nu_{i,k,T}(\bar{\theta}) \leq \tau\right] \leq q_1$ for all $\bar{\theta} \in \bar{\Theta}$. Then following the analysis similar to Theorem 4.2.5, using the union bound and the Chernoff bound, we can prove that $\mathbb{P}[\Theta_{i,T}^{\text{thres},1} \subseteq \widehat{\Theta}^\star] \leq |\bar{\Theta}|e^{-2K\pi_1^2}$. Subsequently, setting $K \geq \frac{\log(|\Theta^\star|/\alpha)}{2\pi_1^2}$ makes the error to be at most α.

Type II estimator. From the analysis of Theorem 4.2.2 (see Equation (C.17)), setting

$$t \geq \max\left\{\frac{\log\left(\frac{2\varrho n}{l_{n,\Theta}}\right)}{\log 2}, \frac{\log\left(\frac{(n-1)|\Theta|^2(n\Gamma_{n,\Theta}+V_{n,\Theta})}{2(1-q_2)\varrho}\right)}{\log(1/a_n^\star)}\right\} = T,$$

guarantees that $\mathbb{E}\left[N_{i,T}(\theta^\star\right] = \mathbb{P}\left[\nu_{i,k,T}(\theta^\star) > \tau\right] \geq q_2$ for all $\theta^\star \in \Theta^\star$. Then following a similar analysis to Theorem 4.2.5 using the union bound and the Chernoff bound, we can prove that $\mathbb{P}[\Theta^\star \not\subseteq \widehat{\Theta}_{i,T}^{\text{thres},2}] \leq |\Theta^\star|e^{-2K\pi_2^2}$. Subsequently, setting $K \geq \frac{\log(|\Theta^\star|/(1-\beta))}{2\pi_2^2}$ makes the error at most $1-\beta$.

Optimal Distributions. The proof is exactly the same as in Theorem 4.2.2.

Differentially Private Outputs. Due to the post-processing property of DP (see Proposition 2.1 of [135]), the resulting estimates are ε-DP with respect to the private signals.

C.7 Proofs and Convergence Analysis for Distributed, Private Hypothesis Testing

C.7.1 Proof of Proposition 4.2.6

Let $0 < \alpha', \alpha'' < 1, \alpha' + \alpha'' = \alpha$ to be determined later. The centralized UMP test at level α'' defines a threshold ϱ_c such that $\theta = 0$ is rejected if $2\Lambda(1,0) \geq \varrho_c$. The threshold ϱ_c is selected such that $\mathbb{P}[2\Lambda(1,0) \geq \varrho_c | \theta = 0] = \alpha''$. For the decentralized test, by the GM algorithm convergence analysis, we know that after K runs and T iterations given by the GM algorithm with Type I guarantee α' and threshold $\varrho^{\text{GM}} = 1$ we have the following event

$$E = \left\{ \left| \frac{n}{2^{T-1}} \psi_{i,T}(1,0) - 2\Lambda(1,0) \right| \leq \frac{n}{2^{T-1}} \right\},$$

Thus, for these values of T, K we set $\varrho_d = \varrho_c - 1$. From the above relations, we get that under $\theta = 0$ and E: $\{2\Lambda(1,0) \geq \varrho_c\} \implies \{\psi_{i,T}(1,0) \geq \varrho_d\}$. This means that if the centralized test rejects, then the decentralized test also rejects $\theta = 0$ with probability at least $1 - \alpha'$. The Type I error is:

$$\begin{aligned}\mathbb{P}[\psi_{i,t}^{\text{GM}}(1,0) \geq \varrho_d | \theta = 0] &= \mathbb{P}[E]\mathbb{P}[\psi_{i,t}^{\text{GM}}(1,0) \geq \varrho_d | \theta = 0, E] + \mathbb{P}[E^c]\mathbb{P}[\psi_{i,t}^{\text{GM}}(1,0) \geq \varrho_d | \theta = 0, E^c] \\ &\leq \alpha'' + \alpha'.\end{aligned}$$

We choose $\alpha' = \alpha/2, \alpha'' = \alpha/2$ such that $\alpha' + \alpha'' = \alpha$. The privacy guarantee is a direct consequence of DP's post-processing property.

□

C.7.2 Extension to Composite Hypotheses

The extension to composite hypotheses is straightforward since, if we consider the generalized likelihood ratio test and run the GM algorithm with the parameters of Proposition 4.2.6 we would obtain that for T and K set as in above, with probability at least $1 - \alpha/2$ the log-belief ratio statistic

$$\left| \frac{n}{2^{T-1}} \psi_{i,T}^{\mathrm{GM}}(\tilde{\Theta}, \tilde{\Theta}_0) - \underbrace{\sum_{i \in [n]} 2 \log \left(\frac{\sup_{\tilde{\theta}_i \in \tilde{\Theta}} \ell_i(S_i | \tilde{\theta}_1)}{\sup_{\tilde{\theta}_0 \in \tilde{\Theta}_0} \ell_i(S_i | \tilde{\theta}_0)} \right)}_{\text{converges to } \chi^2_n \text{ for sufficiently large } n_i} \right| \leq \frac{n}{2^{T-1}}$$

If $\varrho_d = F^{-1}_{\chi^2_n}(1 - \alpha/2) - 1$ then the composite hypothesis test is ε-DP and has Type I error at most α.

C.8 Proofs and Convergence Analysis for Distributed, Private Online Learning

C.8.1 Log-Belief Ratio Notations

Let $\mu_{i,t}(\widehat{\theta})$ be the beliefs for the non-private system, and let $\nu_{i,t}(\widehat{\theta})$ be the private estimates for agent $i \in [n]$ and round $t \geq 0$. For the non-private algorithm (Algorithm 12) all pairs $\widehat{\theta}, \breve{\theta} \in \Theta$ we let $\phi_{i,t}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\mu_{i,t}(\widehat{\theta})}{\mu_{i,t}(\breve{\theta})}\right)$ and $\lambda_{i,t}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\gamma_{i,t}(\widehat{\theta})}{\gamma_{i,t}(\breve{\theta})}\right)$ be the log belief ratios and the log-likelihood ratios respectively for agent $i \in [n]$ round $t \geq 0$. For the private algorithm (Algorithm 10) we let $\psi_{i,t}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\nu_{i,t}(\widehat{\theta})}{\nu_{i,t}(\breve{\theta})}\right), \zeta_{i,t}(\widehat{\theta}, \breve{\theta}) = \log\left(\frac{\sigma_{i,t}(\widehat{\theta})}{\sigma_{i,t}(\breve{\theta})}\right)$, and $\kappa_{i,t}(\widehat{\theta}, \breve{\theta}) = d_{i,t}(\widehat{\theta}) - d_{i,t}(\breve{\theta})$ be

the private log-belief ratio, log-likelihood ratio, and noise difference ratios respectively for agent $i \in [n]$, and round $t \geq 0$. We also let the vectorized versions $\phi_t(\widehat{\theta}, \breve{\theta}), \psi_t(\widehat{\theta}, \breve{\theta}), \lambda_t(\widehat{\theta}, \breve{\theta}), \zeta_t(\widehat{\theta}, \breve{\theta})$ respectively, where the vectorization is over the agents $i \in [n]$. Finally, for each agent $i \in [n]$ and pair of states $\widehat{\theta}, \breve{\theta} \in \Theta$ we define the KL divergence between the states $\Lambda_i(\widehat{\theta}, \breve{\theta}) = \mathbb{E}_\theta\left[\log\left(\frac{\ell_i(s_{i,0}|\widehat{\theta})}{\ell_i(s_{i,0}|\breve{\theta})}\right)\right] = D_{KL}\left(\ell_i(\cdot|\widehat{\theta})|\ell_i(\cdot|\breve{\theta})\right)$.

C.8.2 Auxiliary Lemmas

Before proving the main result for online learning, we prove the following lemma regarding the rate of convergence of the Césaro means.

Lemma C.8.1. *Let $X_0, \ldots, X_{t-1}$ be i.i.d. random variables (vectors), let A be an irreducible doubly stochastic matrix with the second largest eigenvalue modulus $|\lambda_2(A)|$, and let $x_\tau = \frac{1}{n}\mathbb{1}^T X_\tau$ for all $0 \leq \tau \leq t-1$, with $\max_{1\leq\tau\leq t} \sqrt{\mathbb{V}[x_\tau]} \leq V$. Then*

$$\mathbb{E}\left[\left\|\frac{1}{t}\sum_{\tau=0}^{t-1} A^{t-\tau}X_\tau - \left(\frac{1}{t}\sum_{\tau=0}^{t-1} x_\tau\right)\mathbb{1}\right\|_2\right] \leq \frac{(n-1)V}{(1-|\lambda_2(A)|)t}.$$

Proof. For $0 \leq \tau \leq t-1$, we have

$$\begin{aligned}
\mathbb{E}\left[\left\|A^{t-\tau}X_\tau - x_\tau\mathbb{1}\right\|_2\right] &= \mathbb{E}\left[\left\|\frac{1}{n}\mathbb{1}\mathbb{1}^T X_\tau + \sum_{i=2}^n \lambda_i(A)^{t-\tau} r_i l_i^T X_\tau - x_\tau\mathbb{1}\right\|_2\right] \\
&= \mathbb{E}\left[\left\|x_\tau\mathbb{1} + \sum_{i=2}^n \lambda_i(A)^{t-\tau} r_i l_i^T X_\tau - x_\tau\mathbb{1}\right\|_2\right] \\
&\leq \sum_{i=2}^n |\lambda_i(A)|^{t-\tau} \|r_i\|_2 \|l_i\|_2 \mathbb{E}\left[\|X_\tau\|_2\right] \\
&\leq (n-1)|\lambda_2(A)|^{t-\tau}\mathbb{E}\left[\|X_\tau\|_2\right] \\
&\leq (n-1)|\lambda_2(A)|^{t-\tau}\mathbb{E}\left[\|X_0\|_2\right] \\
&\leq (n-1)|\lambda_2(A)|^{t-\tau}V.
\end{aligned}$$

Therefore,

$$\mathbb{E}\left[\left\|\frac{1}{t}\sum_{\tau=0}^{t-1}A^{t-\tau}X_\tau-\left(\frac{1}{t}\sum_{\tau=0}^{t-1}x_\tau\right)\mathbb{1}\right\|_2\right]\leq\frac{(n-1)V}{(1-|\lambda_2(A)|)t},$$

where we use $\sum_{\tau=0}^{t}|\lambda_2(A)|^{t-\tau}\leq\sum_{\tau\geq 0}|\lambda_2(A)|^{\tau}=\frac{1}{1-|\lambda_2(A)|}$. □

In the sequel, we show the main result for online learning.

C.8.3 Proof of Theorem 4.2.8

Similarly to the asymptotic case, it suffices to pick $K = 1$. We let $\Xi_n = \mathbb{V}\left[\sum_{i=1}^{n} n_{i,\tau}\right] = \sum_{i=1}^{n}\chi_i$. We define the following sequence of "bad" events:

$$B_{n,t}=\left\{\max_{i\in[n]}\left|\frac{1}{t}\sum_{\tau=0}^{t-1}n_{i,\tau}-\xi_i\right|\geq\sqrt{\frac{\Xi_n}{\eta t}}\right\}.$$

By applying the union bound and Chebyshev's inequality, we can show that $\mathbb{P}[B_{n,t}]\leq\eta$.

We condition on the "bad" event $B_{n,t}$ not happening. We can prove that, conditioned on $B_{n,t}^c$,

$$V'_{n,\Theta}=\max_{\tilde{\theta}\in\tilde{\Theta},\theta^\star\in\Theta^\star}\sqrt{\mathbb{V}\left[\frac{1}{nt}\sum_{i=1}^{n}\sum_{\tau=0}^{t-1}n_{i,\tau}\zeta_{i,\tau}(\widehat{\theta},\breve{\theta})\middle|B_{n,t}^c\right]}\leq\frac{\sqrt{2}}{n}(nQ_{n,\Theta}+V_{n,\Theta})\left(\max_{i\in[n]}\xi_i+\sqrt{\frac{\Xi_n}{\eta t}}\right).$$

The dynamics of the log-belief ratio obey $\psi_t(\widehat{\theta},\breve{\theta}) = A\psi_{t-1}(\widehat{\theta},\breve{\theta}) + \zeta_t(\widehat{\theta},\breve{\theta}) = \sum_{\tau=0}^{t-1}A^{t-\tau}\zeta_\tau(\widehat{\theta},\breve{\theta})$, where $\zeta_\tau(\widehat{\theta},\breve{\theta}) = \lambda_\tau(\widehat{\theta},\breve{\theta}) + \kappa_\tau(\widehat{\theta},\breve{\theta})$. We apply Lemma C.8.1, and get that

$$\mathbb{E}\left[\left\|\frac{1}{t}\psi_t(\widehat{\theta},\breve{\theta})-\frac{1}{nt}\sum_{\tau=0}^{t-1}\sum_{i=1}^{n}\zeta_{i,\tau}(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2\middle|B_{n,t}^c\right]\leq\frac{(n-1)V'_{n,\Theta}}{t(1-|\lambda_2(A)|)}.$$

Moreover,

$$\mathbb{E}\left[\left\|\frac{1}{nt}\sum_{\tau=0}^{t-1}\sum_{i=1}^{n}\zeta_{i,\tau}(\widehat{\theta},\breve{\theta})-\frac{1}{n}\sum_{i=1}^{n}\xi_i\Lambda_i(\widehat{\theta},\breve{\theta})\right\|_2\middle|B_{n,t}^c\right]\leq\frac{V'_{n,\Theta}}{t}.$$

Therefore, by Markov's inequality and the triangle inequality, we get that for every $z>0$

$$\mathbb{P}\left[\left\|\frac{1}{t}\psi_t(\widehat{\theta},\breve{\theta})-\frac{1}{n}\sum_{i=1}^{n}\xi_i\Lambda_i(\widehat{\theta},\breve{\theta})\mathbb{1}\right\|_2>z\middle|B_{n,t}^c\right]\leq\frac{V'_{n,\Theta}}{z(1-|\lambda_2(A)|)t}.$$

Therefore, we can show that by applying a union bound over $\Theta^\star$, we have that with probability $1-\eta$, for all $\bar{\theta}\in\bar{\Theta}$

$$\log\nu_{i,t}(\bar{\theta})\leq\psi_{i,t}(\bar{\theta},\theta^\star)\leq-\frac{t}{n}l_{n,\Theta}+\frac{|\Theta|V'_{n,\Theta}}{2\eta(1-|\lambda_2(A)|)}.$$

To make the RHS the log-belief threshold at most some value $-\varrho$ for some $\varrho>0$, we require

$$t\geq T=\frac{\varrho+\frac{|\Theta|V'_{n,\Theta}}{2\eta(1-|\lambda_2(A)|)}}{l_{n,\Theta}/n}$$

To determine ϱ, note that $\nu_{i,t}(\bar{\theta})\leq e^{-\varrho}$ for all $\bar{\theta}\neq\theta^\star$, and, thus,

$$\nu_{i,t}(\theta^\star)=1-\sum_{\bar{\theta}\neq\theta^\star}\nu_{i,t}(\bar{\theta})\geq 1-(|\Theta|-1)e^{-\varrho}.$$

To determine a valid value of ϱ, we require $1-(|\Theta|-1)e^{-\varrho}\geq e^{-\varrho}$ which yields $\varrho\geq\log(|\Theta|)$. Therefore, setting $\varrho=\log(|\Theta|)$ and subsequently

$$T=\frac{\log(|\Theta|)+\frac{|\Theta|\frac{\sqrt{2}}{n}(nQ_{n,\Theta}+V_{n,\Theta})\left(\max_{i\in[n]}\xi_i+\sqrt{\frac{\Xi_n}{\eta}}\right)}{2\eta(1-|\lambda_2(A)|)}}{l_{n,\Theta}/n},$$

we get that

$$\mathbb{P}\left[\theta^\star = \widehat{\theta}^{\mathrm{OL}}_{i,T}\right] \geq \mathbb{P}[B^c_{n,T}]\mathbb{P}\left[\theta^\star = \widehat{\theta}^{\mathrm{OL}}_{i,T} | B^c_{n,T}\right] \geq (1-\eta)^2 \geq 1 - 2\eta.$$

Privacy. Similarly to Theorem 4.2.2, the optimal distributions are those that minimize variance subject to privacy constraints. Because there are $|\Theta|$ states, the budget ε should be divided by $|\Theta|$, resulting in $\mathcal{D}^\star_{i,t}(\varepsilon) = \mathrm{Lap}\left(\frac{\Delta_{n,\Theta}|\Theta|}{\varepsilon}\right)$. □

Differentially Private Outputs. Due to the post-processing property of DP (see Proposition 2.1 of [135]), the resulting estimates are ε-DP with respect to the private signals.

C.9 Sensitivity of the Proportional Hazards Model

We derive the sensitivity of the proportional hazards model used in our experiments. Specifically, each center has n_i data points S_i, and the treatment variable is bounded above by 1 (that is, $\max_{1\leq j\leq n_i} |x_{i,j}| \leq B_x$). The state θ obeys $|\theta| \leq B_\theta$. Let S'_i be a data set of n_i points such that S_i and S'_i differ in patient k. The log partial likelihood can be written as

$$\log \ell_i(S_i|\theta) = \sum_{j=1}^{n_i} \delta_{ij}\left(\theta x_{ij} - \log \sum_{r\in R(j)} e^{\theta x_{ik}}\right) = \sum_{j=1}^{n_i} \delta_{ij}\theta x_{ij} - \sum_{j=1}^{n_i} \delta_{ij} \log \sum_{r\in R(j)} e^{\theta x_{ir}}$$

where $R(j) = \{j' : t_{ij'} \geq t_{ij}\}$ is the risk set of j. We are looking to bound $\max_{S_i, S'_i : \|S_i - S'_i\|_1 \leq 1} \left|\log \ell_i(S_i|\theta) - \log \ell_i(S'_i|\theta)\right|$, when patient k is added, removed, or modified:

- If k is removed and k is not in any risk set $R(j)$, removing k does not affect the likelihood.
- If k is removed and k in some risk sets, removing k affects the denominator $\sum_{r \in R(j)} e^{\theta x_{ir}}$ for all $R(j)$ such that $k \in R(j)$.
- If k is added or modified, adding or modifying k affects the numerator $e^{\theta x_{ik}}$ if k experiences an event, and the denominator $\sum_{r \in R(j)} e^{\theta x_{ir}}$ if $k \in R(j)$.

Thus, the term θx_{ij} in the numerator is always bounded by $B_\theta B_x$ due to Hölder's inequality. The denominator $\sum_{r \in R(j)} e^{\theta x_{ir}}$ is a sum of exponentials, and its change is bounded by $e^{B_\theta B_x}$ and its logarithm by $B_\theta B_x$. Therefore, $\Delta_{n,\Theta} = 2B_\theta B_x$.

C.10 Lower Bounds for Distributed Hypothesis Testing

In this section, we devise information-theoretic lower bounds that are applicable to any belief-exchange algorithms. We focus on the hypothesis testing scenario with Θ consisting of a null hypothesis ($\theta = 0$) and an alternative hypothesis ($\theta = 1$). Initially, each agent has access to a model $\ell_i(\cdot|\theta)$ and an ε-DP privacy mechanism $\mathcal{M}_i$ which the agent uses K times to construct a private signal $y_{i,k} = \mathcal{M}_i(s_{i,k})$. Agents can exchange the private signals $y_{i,k}$ that they possess in each iteration T, and have access to a statistical test $\mathcal{A} : \mathcal{R}^{nK} \to \{0, 1\}$ that, given private signals $y_{1,1}, \ldots, y_{n,K}$, outputs 1 if $\theta = 0$ is rejected and 0 if we fail to reject $\theta = 0$. We want to find a lower bound on communication complexity, $K \cdot T$, assuming that $\mathcal{A}$ achieves a Type I error rate of α and a Type II error rate of $1-\beta$. To devise the lower bound, we rely on classic results from the bandits literature [376].

Theorem C.10.1 (Lower Bound). *For any belief aggregation scheme, we need at least*

$$K \cdot T \geq \frac{|1-\alpha-\beta|\text{diam}\,(\mathcal{G})}{2\sum_{i\in[n]} D_{KL}\left(\widehat{\ell}_i(\cdot|\theta=1)|\widehat{\ell}_i(\cdot|\theta=0)\right)}, \quad \textit{where} \quad \widehat{\ell}_i(s|\theta) = \ell_i(\mathcal{M}_i(s)|\theta) = \ell_i \circ \mathcal{M}_i(s|\theta),$$

such that $\mathcal{A}$ achieves Type I error rate of α and Type II error rate of $1-\beta$.

Proof. For T, we always need $T \geq \text{diam}\,(\mathcal{G})$ for a signal from each agent to reach any other agent. To devise a lower bound for K, let

$$\mathbb{P}\left[\mathcal{A}(y_{1,1},\ldots,y_{n,K})=1|\theta=0\right] = 1-\alpha, \tag{C.21}$$

$$\mathbb{P}\left[\mathcal{A}(y_{1,1},\ldots,y_{n,K})=0|\theta=1\right] = \beta. \tag{C.22}$$

We let $P_{\theta_0}(\mathcal{B}_{i,T}) = \mathbb{P}\left[\mathcal{B}_{i,T}|\theta=\theta_0\right]$ for any event $\mathcal{B}_{i,T} \subset \Omega_{i,T}$, where $\Omega_{i,T}$ is the sample space for agent i at iteration T and corresponds to all the signals observed up to time T. From simple properties of the KL divergence (see [376]), we see that for any event $\mathcal{B}_{i,T} \subset \Omega_{i,T}$,

$$\begin{aligned}\left(P_1(\mathcal{B}_{i,T}) - P_0(\mathcal{B}_{i,T})\right)^2 &\leq D_{KL}\left(P_1|P_0\right) \\ &\leq 2K\sum_{i\in[n]} D_{KL}\left(\widehat{\ell}_i(\cdot|\theta=1)|\widehat{\ell}_i(\cdot|\theta=0)\right),\end{aligned}$$

for $T \geq \text{diam}\,(\mathcal{G})$, where $\widehat{\ell}_i$ is the likelihood of the privatized signal, that is, $\widehat{\ell}_i(s|\theta) = \ell_i(\mathcal{M}_i(s)|\theta)$. By setting $\mathcal{B}_{i,T} = \{\mathcal{A}(y_{1,1},\ldots,y_{n,K})=1\}$, we get the lower bound for K.

□

Remark about the Randomized Response. If the mechanism corresponds to the randomized response mechanism with probability of randomization equal

to $p_\varepsilon = \frac{1}{1+e^\varepsilon}$ and under $\theta = 0$ the signals follow Be(1/2) and under $\theta = 1$ the signals follow Be$(1/2 + \varepsilon_{\text{gap}}/2)$, then we can show that on this instance, the randomized response requires

$$K \cdot T \geq \frac{2|1-\alpha-\beta|}{\varepsilon_{\text{gap}}^2} \cdot \left(\frac{e^\varepsilon + 1}{e^\varepsilon - 1}\right)^2 \cdot \frac{\text{diam}\,(\mathcal{G})}{n},$$

because $D_{KL}\,(P_1|P_0) \leq \varepsilon_{\text{gap}}^2(1-2p_\varepsilon)^2$, where P_0, P_1 are defined in the theorem right above. Moreover, when epsilon is small, i.e., $\varepsilon \in (0,1)$, the lower bound on the communication complexity can be approximated as $K \cdot T \geq \frac{2(1-\eta)}{\varepsilon_{\text{gap}}^2} \cdot \frac{1}{\varepsilon^2} \cdot \frac{\text{diam}(\mathcal{G})}{n}$, yielding an $1/\varepsilon^2$ lower bound (with respect to the privacy budget) for the randomized response mechanism.

Finding the Additive DP mechanism that Minimizes the Communication Complexity Lower Bound. For given agent models $\ell_1, \ldots, \ell_n$, finding the mechanisms that minimize the lower bound of communication complexity requires maximizing the sum of KL divergences (after applying the DP mechanism). Assuming that the noise is additive on the signal and independent of it, i.e., the private signal of each agent is $y_i = s_i + d_i$, we have $\widehat{\ell}_i(\cdot|\theta) = \ell_i(\cdot|\theta) * p_{d_i}(\cdot)$ where $*$ denotes the convolution operator between the two distributions and p_{d_i} is the density of the noise. If the noise is continuous and the range of the mechanism is a subset of $\mathbb{R}^d$, the corresponding optimization problem becomes (e.g., for continuous signals and noise; see also [247] and [325]):

$$\max_{p_{d_i}(\cdot)} \quad D_{KL}\left(\ell_i(\cdot|\theta=1) * p_{d_i}(\cdot) | \ell_i(\cdot|\theta=0) * p_{d_i}(\cdot)\right) \tag{C.23}$$

$$\text{s.t.} \quad p_{d_i}(u) \geq 0, \quad \forall u \in \mathbb{R}^d$$

$$\int_{\mathbb{R}} p_{d_i}(u)du = 1$$

$$\left\|\nabla_s \log p_{d_i}(u-s)\right\|_\infty \leq \varepsilon, \quad \forall u \in \mathbb{R}^d$$

where $\ell_i(\cdot|\theta) * p_{d_i})(s) = \int_{\mathbb{R}^d} p_d(u)\ell_i(s-u|\theta)du$.

C.11 Additional Simulation Experiments

C.11.1 Toy Example: MLE and OL for a Single Treatment

We test the MLE and OL algorithms in an arrangement of $n = 5$ hospitals possible values $\Theta = \{0, -\log 2\}$, whereas the value of $-\log 2$ examines whether the patients are $1/2$ less likely to die. We use a privacy budget of $\varepsilon = 1$ and error bounds equal to $\alpha = 1 - \beta = 0.05$. The evolution of the beliefs and the beliefs at the terminal time T – calculated by applying Theorem 4.2.2 – are shown in Figure C.4(a). Algorithm 8 is able to successfully recover $\Theta^\star = \{-\log 2\}$ which is the true maximizer, that is, $\Lambda(-\log 2) > \Lambda(0)$. The DP algorithms are compared against the centralized baseline, which corresponds to all centers sharing their signals without privacy. In addition, Figure C.4(b) shows the result of applying the two threshold algorithm (with a single threshold), which is also able to recover successfully $\Theta^\star$, similar to the AM/GM algorithm.

We perform a similar analysis in an online manner, where we assume that

the centers perform survival analysis every 10 days (we achieve that by splitting the data evenly among these days). In Figure C.4(c), we report the time-averaged log-belief ratio as well as the beliefs at the terminal time T for the same choice of topology and privacy budget. The time-averaged log-belief ratio is shown against the limiting value of the non-DP baseline (see [343]). Again, agents collectively identify the true state $\theta^\circ = -\log 2$.

C.11.2 Time and Space Complexity

We first start by analyzing the time complexity of our method. Specifically, in the distributed MLE setting, if agent i has n_i data points and model ℓ_i which can be computed in $\mathcal{T}_i(n_i)$ for one value of $\theta \in \Theta$, then the distributed MLE is parallelizable between the agent and the total time complexity per agent is $O\left(|\Theta|K\left(\mathcal{T}_i(n_i) + T\deg_{\mathcal{G}}(i)\right)\right)$ which includes an initialization cost of $|\Theta|K\mathcal{T}_i(n_i)$ to calculate noisy likelihoods. For example, in the case of the distributed proportional hazards model, the likelihoods can be computed in $\mathcal{T}_i(n_i) = O(n_i \log n_i)$. Then, there is a communication cost, which consists of the number of belief exchanges dictated by the communication complexity KT, and the cost of propagation for each iteration, which is $O(|\Theta|K\deg_{\mathcal{G}}(i))$ for all states. Similarly, in the OL regime, the total time complexity per agent is $O\left(|\Theta|\sum_{t=1}^{T}\left(\mathcal{T}_i(n_{i,t}) + \deg_{\mathcal{G}}(i)\right)\right)$. Finally, in terms of space complexity, each agent can simply maintain their belief in each state, giving a space complexity $O(K|\Theta|)$ during communication.

C.11.3 Runtime Comparison with Homomorphic Encryption Methods

To further test the practical applicability of our method, we compare the runtime of our method with existing holomorphic encryption methods (HE) and, in particular, the FAHME method introduced in [163] as the number of providers (n) grows and the number of data grows. Both our method and FAHME are capable of performing survival analysis in a distributed regime; however, they apply different privacy protections and cannot be compared prima facie. Generally, HE methods have the strongest possible privacy. However, these protections fall short in scalability considerations, for which DP with a small ε is a better alternative in terms of efficiency. Furthermore, the most recent HE methods designed for multicenter trials do not have open-source implementations, making direct comparison difficult (see, e.g. [163, 176]).

First, our aim is to compare the two methods in the same dataset and experiment, which corresponds to distributed survival analysis with cancer data introduced in [359]. Specifically, [359] finds that tumor mutational burden (TMB) is a significant predictor of survival outcomes in patients with metastatic cancer undergoing immune checkpoint inhibitor (ICI) therapy. Analyzing data from 1,662 advanced cancer patients, the authors demonstrated that higher TMB levels are associated with better survival prospects.

[163] use the data from [359] and perform survival analysis (see Figure 2 in their paper) by splitting the data equally among n providers. Then, the authors report the runtime as a function of n for three datasets: with 4096 time points (t.p.), 8192 t.p., and a dataset that consists of 10 times the original data, and

report the total runtime in Figure 2(c). To construct the fairest possible comparison, we consider the same dataset and the distributed proportional hazards model with TMB as a covariate and two hypotheses – null ($\theta = 0$) and a composite alternative ($\theta \neq 0$) – similarly to our initial example for ACTG (see Section 4.2.2). The two first datasets (4096 and 8192 t.p.) are constructed by resampling the original data with replacement. We choose ε to be 0.1, which corresponds to a very strong privacy regime, significantly smaller than the one used in the 2020 US Census [80] and healthcare contexts [156, 134]. Finally, we chose the error bounds to be no more than 0.1. In Figure C.5, we report the per-agent cost of inference for $n \in \{6, 12, 24, 48, 96\}$ in a fully connected topology, in analogy to Figure 2(c) of [163]. Our reported runtimes vary from $\sim 10^{-2}$s to ~ 1s, which is a 10x – 1000x improvement over the runtimes reported in [163].

C.11.4 Comparison with First-order Methods

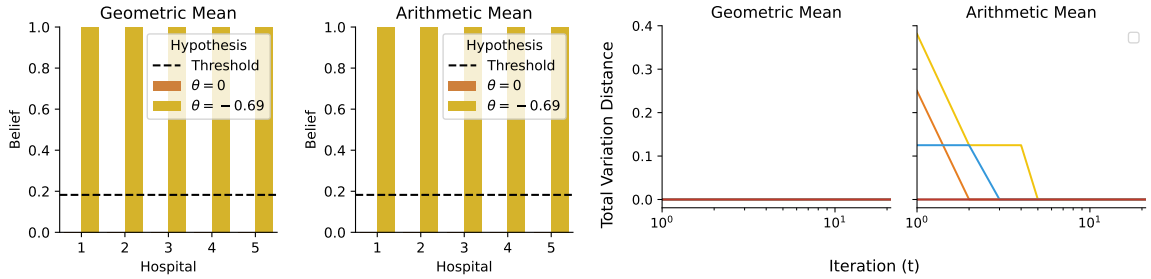
We compare with the first-order method of [354] with graph-homomorphic noise. The distributed optimization problem we are solving is

$$\max_{\theta \in \mathbb{R}} \frac{1}{n} \sum_{i \in [n]} 2 \left(\log \ell_i(S_i|\theta) - \log \ell_i(S_i|0) \right)$$

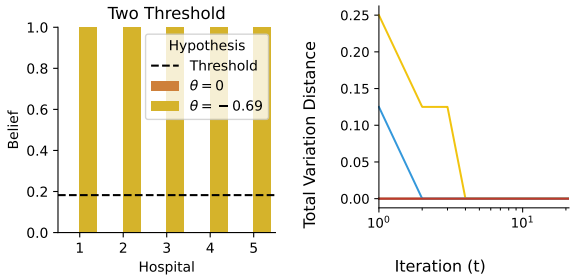
The distributed updates on the parameters with graph-homomorphic noise according to [354] are equivalent to

$$\theta_{i,t} = \sum_{j \in [n]} a_{ij} \theta_{j,t-1} + \eta_{\text{lr}} \text{Clip} \left(\frac{\mathrm{d} \log \ell_i(S_i|\theta_{i,t-1})}{\mathrm{d}\theta_{i,t-1}}, 2B_\theta B_x \right) + \text{Lap} \left(\frac{2B_x B_\theta T \eta_{\text{lr}}}{\varepsilon} \right),$$

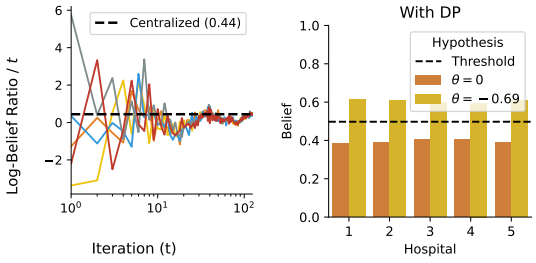
where η_{lr} is the learning ratem and the Clip operation clips the gradient to have L_1 norm at most $2B_\theta B_x$. To derive the Laplace noise, note that the sensitivity of the clipped gradient is, at most, $2\eta_{\text{lr}} B_\theta B_x$. Additionally, since the per-agent budget is ε, we need to scale the budget by T. In the simulations, we use $B_\theta = 1$, $\eta_{\text{lr}} = 0.001$, and in order to have a fair comparison to our algorithm, we set T to be equal to the number of iterations we run our algorithms. For large sample sizes the P values are given as $P_i = 1 - F_{\chi_1^2}\left(2\left[\log \ell_i(S_i|\theta_{i,T}) - \log \ell_i(S_i|0)\right]\right)$



(a) AM/GM Algorithm



(b) Two Threshold Algorithm



(c) Online Learning

Figure C.4: **Top (a):** Resulting beliefs and total variation distance between the beliefs and the ground truth for the GM and AM estimators (Algorithm 8) for the ACTG study data for $n = 5$ centers examining the effect the ddI treatment on patient survival assuming a proportional hazards model. Section 4.2.2 describes the model. The topology between the hospitals is taken to be the complete graph. We have set $\varepsilon = 1$, $\alpha = 1 - \beta = 0.05$ and $\varrho^{\mathrm{AM}} = \varrho^{\mathrm{GM}} = 1.5$. The resulting estimators recover $\Theta^\star = \{-\log 2\}$. The number of iterations T and the number of rounds K have been computed according to Theorem 4.2.2.
Bottom Left (b): Resulting beliefs and total variation distance between the beliefs and the ground truth for the Two Threshold algorithm. We have set $\varepsilon = 1$, $\alpha = 1 - \beta = 0.05$ and $\widehat{\tau}^{\mathrm{thres},1} = \widehat{\tau}^{\mathrm{thres},2} = 0$ and $\tau^{\mathrm{thres},1} = \tau^{\mathrm{thres},2} = 1.5$ (single-threshold recovery; cf Corollary 4.2.4). The resulting estimators recover $\Theta^\star$ successfully. The number of iterations T and number of rounds K have been computed according to Theorem 4.2.5.
Bottom Right (c): Resulting log-belief ratios and terminal beliefs for the online learning algorithm on the ACTG study. We assume that the centers exchange beliefs on a daily basis. The dashed line corresponds to the value that the time-averaged log-belief ratio converges in the non-DP regime.

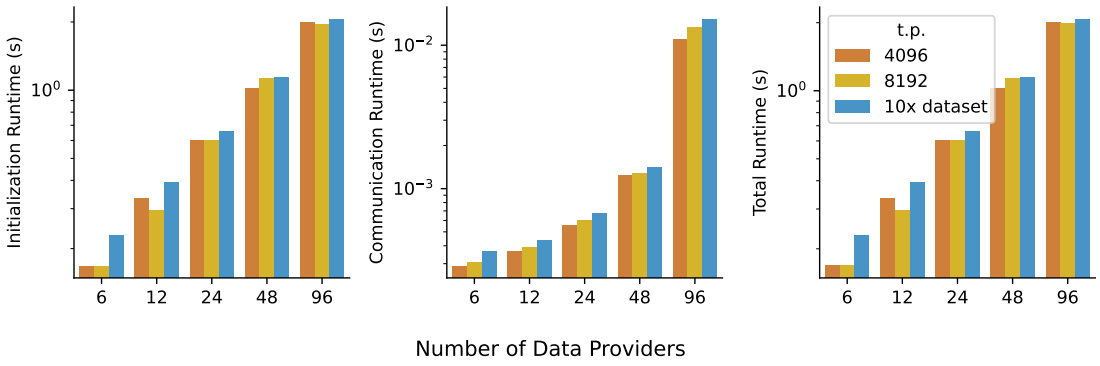
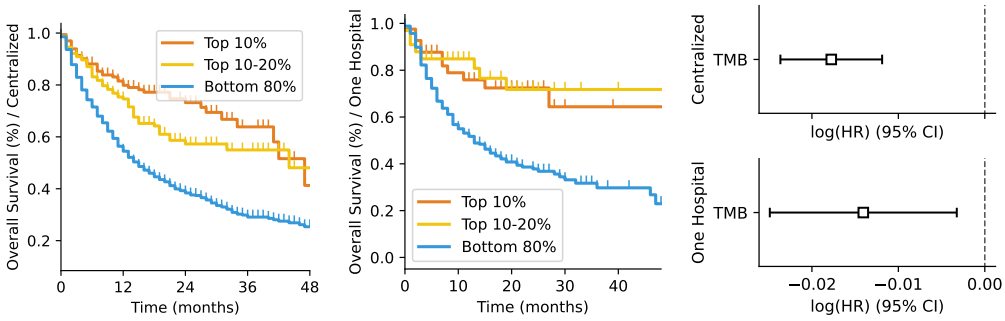


Figure C.5: Runtime of distributed MLE algorithm for the study by [359] for varying values of n used in measuring the performance of the FAHME method [163]. The privacy budget is set to $\varepsilon = 1$ (tight privacy), and the error rates are set to $\alpha = 1 - \beta = 0.05$, and the thresholds are set to $\varrho^{\mathrm{AM}} = \varrho^{\mathrm{GM}} = 0.1$. In accordance with [163], we have constructed 3 datasets: a dataset consisting of 4096 timepoints (t.p.) via resampling the original data with replacement, a dataset of 8192 t.p. via resampling the original data with replacement, and a dataset which consists of 10 times the original data.

C.11.5 Additional Experimental Results with the Cancer Dataset



(a) Centralized curves (b) Curves for one hospital (c) log Hazard Ratios

Figure C.6: **Left:** Kaplan-Meier survival curves for the cancer data. The three curves correspond to high TMB (top 10%), medium TMB (top 10%-20%) and low TMB (bottom 80%). **Middle:** Survival curves for one hospital (the data is split equally among 5 hospitals) for the same study. **Right:** Log hazard ratios with 95% confidence intervals from the fitted proportional hazards model for centralized and one hospital.

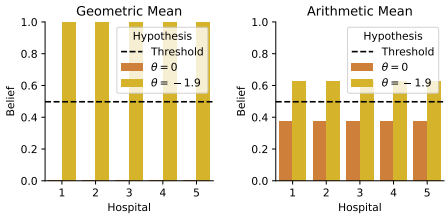


Figure C.7: Resulting beliefs $\nu_{i,T}^{\mathrm{GM}}(\theta)$ and $\nu_{i,T}^{\mathrm{GM}}(\theta)$ for the GM and AM estimators (Algorithm 8) for the cancer study data for $n = 5$ fully connected centers examining the effect of TMB on patient survival assuming a proportional hazards model and $\Theta = \{0, \log(0.15)\}$. We have set $\varepsilon = 1$, $\alpha = 1 - \beta = 0.05$ and $\varrho^{\mathrm{AM}} = \varrho^{\mathrm{GM}} = 0.1$. The resulting estimators yield $\{\log(0.15)\}$ as the MLE set which agrees with the ground truth.

C.11.6 Additional Experimental Results with the AIDS Dataset

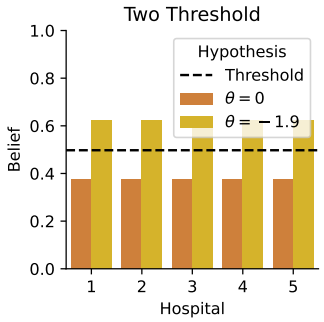


Figure C.8: Resulting beliefs $N_{i,T}(\theta)$ for the two threshold algorithm (Algorithm 9) for the cancer study data for $n = 5$ fully connected centers examining the effect of TMB on patient survival assuming a proportional hazards model. We have set $\varepsilon = 1$, $\alpha = 1 - \beta = 0.05$ and $\widehat{\tau}^{\text{thres},1} = \widehat{\tau}^{\text{thres},2} = 0$ and $\tau^{\text{thres},1} = \tau^{\text{thres},2} = 0.5$ (single-threshold recovery; cf Corollary 4.2.4). The resulting estimators yield $\{\log(0.15)\}$ as the MLE set. The number of iterations T and number of rounds K have been computed according to Theorem 4.2.5.

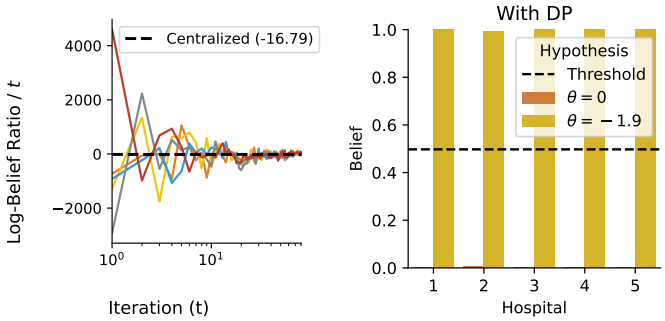


Figure C.9: Resulting log-belief ratios and terminal beliefs for the online learning algorithm on the cancer study. We assume that the centers exchange beliefs on a daily basis for $\varepsilon = 1$. Data is evenly split among $n = 5$ centers. The dashed line corresponds to the value that the time-averaged log-belief ratio converges in the non-DP regime.

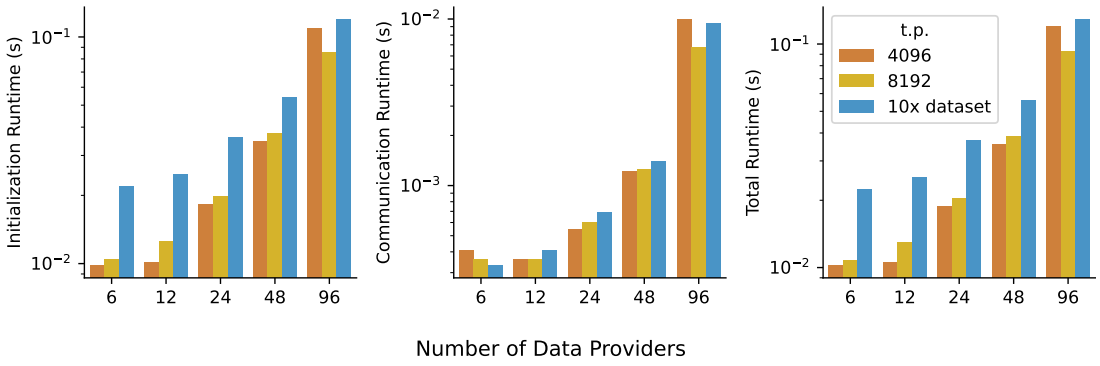


Figure C.10: Runtime of distributed MLE algorithm for the ATCG study for varying values of n used in measuring the performance of the FAHME method [163]. The value of the privacy budget is $\varepsilon = 0.1$ (tight privacy), and the value of the errors is $\alpha = 1 - \beta = 0.05$, and the thresholds are set as $\varrho^{\mathrm{AM}} = \varrho^{\mathrm{GM}} = 0.1$. In accordance with [163], we have constructed 3 datasets: a dataset consisting of 4096 timepoints (t.p.) via resampling the original data with replacement, a dataset of 8192 t.p. via resampling the original data with replacement, and a dataset which consists of 10 times the original data.

APPENDIX D

STYLIZED NETWORK MODELS FOR RESILIENCE

D.1 DIGAM Model

D.1.1 Reproducibility

Code and data needed to exactly reproduce are provided in the form of a Jupyter notebook and is available here[319]. The software has been developed in Python by the author and uses the following open–source libraries: numpy [406], scipy [410], networkx [192], matplotlib [207], pandas [280], and seaborn[417].

D.1.2 Qualitative Results Addendum

The analytical results which are briefly presented in Section 5.1.4 can be found below for the first three levels of the hierarchy. Groups enclosed in parentheses correspond to separate levels. In the faculty hiring networks the "All others" node represents all non–US institutions:

- *world–trade*: (Finland) (Hungary, Slovenia, Singapore, Chile) (Salvador, Iceland, Kuwait, Rep., Belgium, Poland, Moldava., Austria, Germany, Indonesia, Guatemala, Bolivia, Paraguay, Australia, Africa, Of)
- *london–underground*: (Bank) (Baker Street, Canning Town) (Kings Cross St. Pancras, Stratford, Willesden Junction, Earls Court)
- *open–arilines*: (AMS) (FRA, CDG) (IST, MUC, ATL, PEK)

- *cs–faculty*: (All others) (University of Illinois, Urbana Champaign, MIT) (Purdue University, University of Texas, Austin, Carnegie Mellon University, Stanford University)
- *history–faculty*: (All others) (Harvard University, Yale University, University of Chicago, University of Wisconsin, Madison, Columbia University) (UC Berkeley, UCLA, Princeton University, University of Michigan, University of Pennsylvania, Stanford University, Johns Hopkins University, Rutgers University, University of Virginia, Cornell University, University of Texas, Austin, New York University, Indiana University, Northwestern University, Ohio State University, University of Illinois, Urbana Champaign, University of North Carolina, Chapel Hill, Duke University, Brown University, University of Minnesota, Minneapolis, Michigan State University, UC San Diego, UC Santa Barbara, Brandeis University, University of Washington)
- *business–faculty*: (All others) (University of Michigan, University of Texas, Austin) (Ohio State University, Indiana University, Pennsylvania State University, University of Pennsylvania)

D.1.3 Global Clustering Coefficient of IGAM

For the number of closed triplets (i.e. triangles) we have

$$
\begin{aligned}
\mathbb{E}[T_C] &= \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=h(u)+1}^{h(w)} \sum_{u:h(u)=0}^{h(v)} b^{h(u)+h(v)+h(w)} c^{-3-2h(u)-h(v)} \\
&= \frac{1}{c^3} \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=h(u)+1}^{h(w)} b^{h(v)+h(w)} c^{-h(v)} \sum_{h(u)=0}^{h(v)} b^{h(u)} c_2^{-2h(u)} \\
&= \frac{1}{c^3} \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=0}^{h(w)} b^{h(v)+h(w)} c^{-h(v)} \Theta\left(\frac{b^{h(v)}}{c^{2h(v)}}\right) \\
&= \frac{1}{c^3} \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=0}^{h(w)} b^{h(w)} b^{h(w)} \Theta\left(\frac{b^{2h(w)}}{c^{3h(w)}}\right) = \Theta\left(\frac{b^{3H}}{c^{3H+3}}\right).
\end{aligned}
\tag{D.1}
$$

For the number of open triplets, we have that

$$
\begin{aligned}
\mathbb{E}[T_R] &= \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=h(u)+1}^{h(w)} \sum_{u:h(u)=0}^{h(v)} b^{h(u)+h(v)+h(w)} \gamma_{uvw} \\
&\leq 3 \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=h(u)+1}^{h(w)} \sum_{u:h(u)=0}^{h(v)} b^{h(u)+h(v)+h(w)} c^{-2-2h(u)} \\
&= \frac{3}{c^2} \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=0}^{h(w)} b^{h(v)+h(w)} \Theta\left(\frac{b^{h(v)}}{c^{2h(v)}}\right) \\
&= \frac{3}{c^2} \sum_{w:h(w)=0}^{H} b^{h(w)} \Theta\left(\frac{b^{2h(w)}}{c^{2h(w)}}\right) = \Theta\left(\frac{b^{3H}}{c^{2H+2}}\right).
\end{aligned}
\tag{D.2}
$$

Similarly, $\mathbb{E}[T_R] \geq 3 \sum_{w:h(w)=h(v)+1}^{H} \sum_{v:h(v)=h(u)+1}^{h(w)} \sum_{u:h(u)=0}^{h(v)} b^{h(u)+h(v)+h(w)} c^{-2-2h(v)} = \Theta\left(\frac{b^{3H}}{c^{2H+2}}\right)$. Therefore, $\mathbb{E}[T_R] = \Theta\left(\frac{b^{3H}}{c^{2H+2}}\right)$.

D.1.4 Other Properties of IGAM2

We describe the mathematical properties of IGAM2. First, we construct a coupling between IGAM2 and IGAM which we can use a proxy for the behaviour of IGAM2.

Remark. Throughout the proofs we use the following remark: For every two positive integers s, t with $s < t$ and for a positive integer constant $b \geq 2$ we have that $(1 - 1/b)b^t \leq b^t - b^{t-1} \leq b^t - b^s \leq b^t$. Therefore $b^t - b^s = \Theta(b^t)$ with constants $C_1 = 1 - 1/b$ and $C_2 = 1$.

Coupling Construction. We consider a randomly generated network $G \sim \text{IGAM2}(b, c_1, c_2, H_0, H) \equiv \text{IGAM}(b, c_1, H)$ for $1 < c_1 \leq c_2 < b$ and $0 \leq H_0 \leq H$ with edge law g. We also consider a network $G' \sim \text{IGAM2}(b, c_2, c_2, 0, H) \equiv \text{IGAM}(b, c_2, H)$ and a network $G'' \sim \text{IGAM2}(b, c_1, c_1, 0, H)$ with edges law g' and g'' coupled with G as follows:

- $\mathbb{P}[(u, v) \in E(G) | (u, v) \in E(G')] = 1$ and $\mathbb{P}[(u, v) \in E(G) | (u, v) \notin E(G')] = \frac{g(u,v) - g'(u,v)}{1 - g'(u,v)} \in [0, 1]$.
- $\mathbb{P}[(u, v) \in E(G'') | (u, v) \in E(G)] = 1$ and $\mathbb{P}[(u, v) \in E(G'') | (u, v) \notin E(G)] = \frac{g''(u,v) - g(u,v)}{1 - g(u,v)} \in [0, 1]$.

Under this coupling, which we denote as ν, we have that $\mathbb{P}[(u, v) \in E(G)] = \mathbb{P}[(u, v) \in E(G) | (u, v) \in E(G')]\mathbb{P}[(u, v) \in E(G')] + \mathbb{P}[(u, v) \in E(G) | (u, v) \notin E(G')]\,\mathbb{P}[(u, v) \notin E(G')] = g'(u, v) \cdot 1 + (1 - g'(u, v)) \cdot \frac{g(u,v) - g'(u,v)}{1 - g'(u,v)} = g'(u, v) + g(u, v) - g'(u, v) = g(u, v)$ and, similarly, $\mathbb{P}[(u, v) \in E(G'')] = g''(u, v)$. The coupling also satisfies that G' is a subgraph of G ($G' \subseteq G$) since $(u, v) \in E(G')$ implies $(u, v) \in E(G)$. Moreover, G is a subgraph of G'' ($G \subseteq G''$) since every edge of G belongs to the edge set of G''.

Sublinear Dominating Set. We let $(G', G, G'') \sim \nu$. We know that G' is generated from a simple IGAM model therefore it has a dominating set of size $b^{O(\log(2c_2 H \log b)/\log(b/c)} = b^{o(H)} = o(n)$. Since $G' \subseteq G$, the dominating set of G has

size at most the dominating set of G'. Therefore, G has a dominating set of size $b^{O(\log(2c_2 H \log b)/\log(b/c)} = b^{o(H)} = o(n)$.

Degree Distribution. We fix a node $u \in V$. We have the following

If $h(u) > H_0$ then the law that is obeyed is $g(u,v) = c_2^{-1-\min\{h(u),h(v)\}}$. From the simple IGAM model we have calculated the degree in this case to be $\Theta\left(b^{H+1}/c_2^{h(u)+1}\right)$.

If $h(u) \leq H_0$ then

$$\begin{aligned}\bar{d}_h \approx \sum_{r=0}^{H_0} b^r c_1^{-\min\{h(u),r\}-1} + \sum_{r=H_0+1}^{H} b^r c_2^{-\min h(u),r\}-1} &= \Theta\left(\frac{b^{H_0+1}}{c_1^{h(u)+1}}\right) + \sum_{r=H_0+1}^{H} b^r c_2^{-1-h(u)} \\ &= \Theta\left(\frac{b^{H_0+1}}{c_1^{h(u)+1}}\right) + \Theta\left(\frac{b^{H+1}}{c_2^{h(u)+1}}\right).\end{aligned}$$

Therefore, every node, parametrized by its height h has average degree

$$\bar{d}_h \approx \begin{cases} \Theta\left(\frac{b^{H+1}}{c_2^{h+1}}\right) & h > H_0, \\ \Theta\left(\frac{b^{H_0+1}}{c_1^{h+1}}\right) + \Theta\left(\frac{b^{H+1}}{c_2^{h+1}}\right) & h \leq H_0 \end{cases}.$$

To bound the average number of edges we refer to the coupling ν and deduce that the average number of edges $\bar{m}$ of G is at most the average number of edges of G', say $\bar{m}' = \Theta(b^{2H}/c_2^H)$ (as we showed in the main part of the paper) due to the subgraph relationship. Therefore, the average number of edges is $\bar{m} = O(b^{2H}/c_2^H)$. A better bound can be obtained by calculating the expected value analytically using the form of $\bar{d}_h$ we derived above. Namely,

$$\begin{aligned}\bar{m} &= \sum_{h=0}^{H_0} b^h \bar{d}_h + \sum_{h=H_0+1}^{H} b^h \bar{d}_h \\ &= \sum_{h=0}^{H_0} b^h \left[\Theta\left(\frac{b^{H_0+1}}{c_1^{h+1}}\right) + \Theta\left(\frac{b^{H+1}}{c_2^{h+1}}\right)\right] + \sum_{h=H_0+1}^{H} b^h \Theta\left(\frac{b^{H+1}}{c_2^{h+1}}\right) \\ &= \Theta\left(\frac{b^{2H_0}}{c_1^{H_0}}\right) + \Theta\left(\frac{b^{H+H_0}}{c_1^{H_0}}\right) + \Theta\left(\frac{b^{2H}}{c_2^{H}}\right).\end{aligned}$$

We still observe that $\bar{m} = O(b^{2H}/c_2^H)$. Moreover, using the fact that the edges $\bar{m}''$ of G'' are $\Theta(b^{2H}/c_1^H)$ we get, in the same logic, that $\bar{m} \geq \bar{m}''$, and, thus $\bar{m} = \Omega(b^{2H}/c_1^H)$. Note that setting $c_1 = c_2$ and $H_0 = 0$ recovers the result for the simple IGAM model.

Small-world Behaviour. We let $(G', G, G'') \sim \nu$. Since $G' \subseteq G$, the diameter of G is at most the diameter of G' because every path between two nodes in G' is a path in G. Since the diameter of G' is close to $\Theta(\log b/\log(b/c_2)) = O(1)$ a.a.s., then the diameter of G is also close to $O(1)$ a.a.s..

Global Clustering Coefficient. Let $(G', G, G'') \sim \nu$. Let uvw be a triplet in G such that $h(u) \leq h(v) \leq h(w)$. The probability that uvw is a triangle in G' is β'_{uvw}, β_{uvw} if uvw is a triangle in G and β''_{uvw} if uvw is a triangle in G''. From the subgraph relationship we have that $c_2^{-3-2h(u)-h(v)} = \beta'_{uvw} \leq \beta_{uvw} \leq \beta''_{uvw} = c_1^{-3-2h(u)-h(v)}$. Therefore, the number of triangles T_C (respectively T'_C for G' and T''_C for G'') satisfies $\mathbb{E}[T'_C] \leq \mathbb{E}[T_C] \leq \mathbb{E}[T''_C]$. Using Equation (D.1) we deduce that $\mathbb{E}[T''_C] = \Theta\left(\frac{b^{3H}}{c_1^{3H+3}}\right)$ and $\mathbb{E}[T'_C] = \Theta(b^{3H}/c_2^{3H+3})$.

The probability γ_{uvw} of uvw being a triplet in G (respectively γ'_{uvw} in G' and γ''_{uvw} in G'') satisfies $3c_2^{-2-2h(v)} \leq \gamma'_{uvw} \leq \gamma_{uvw} \leq \gamma''_{uvw} \leq 3c_2^{-2-2h(u)}$. The expected number of

triplets is denoted by $\mathbb{E}[T_R]$ ($\mathbb{E}[T'_R]$ for G' and $\mathbb{E}[T''_R]$ for G'') can be found by using Equation (D.2). If we execute the sum mutatis mutandis, we arrive at the fact that $\Omega(b^{3H}/c_2^{2H+2} = \mathbb{E}[T_R] = O(b^{3H}/c_1^{2H+2})$. McDiarmid's Inequality[130] states that $\mathbb{P}\left[T_C \leq \mathbb{E}[T_C] + O(b^H)\right] = 1 - O\left(e^{-b^H}\right)$, and $\mathbb{P}\left[T_R \geq \mathbb{E}[T_R] - O(b^H)\right] = 1 - O\left(e^{-b^H}\right)$. because T_C, T_R are $\Theta(b^H)$–Lipschitz functions [In general, for a graph G with n nodes the number of triangles of G as a function of the edge variables is a $3n$–Lipschitz per edge, since deleting or adding an edge can change the number of triangles by $3n$, and, similarly, the number of triplets is a $2n$–Lipschitz function since each edge is part of at most $2n$ paths on 3 vertices]. Thus, with probability $1 - O\left(e^{-b^H}\right)$ we have that $\frac{T_C}{T_R} \leq \frac{\mathbb{E}[T_C]}{\mathbb{E}[T_R]} + O(b^{-H}) = O\left(\frac{c_2^{2H+2}}{c_1^{3H+3}} + b^{-H}\right)$.

Core–periphery Conductance. Let $(G', G, G'') \sim \nu$. Let the partition $(S_\tau, \bar{S}_\tau)$ be at level τ, i.e. all nodes with height $h \leq \tau$ and the periphery $\bar{S}$ with $h \geq \tau$. From the subgraph relationship we get that $e'(S_\tau, \bar{S}_\tau) \leq e(S_\tau, \bar{S}_\tau) \leq e''(S_\tau, \bar{S}_\tau)$, and subsequently $\mathbb{E}[e'(S_\tau, \bar{S}_\tau)] \leq \mathbb{E}[e(S_\tau, \bar{S}_\tau) \leq \mathbb{E}[e''(S_\tau, \bar{S}_\tau)]$. Thus $\bar{\phi}'(S_\tau) \leq \bar{\phi}(S_\tau) \leq \bar{\phi}''(S_\tau)$. Using the fact about the core-periphery conductance we proved for the simple IGAM model, since G', G'' are equivalently produced from the simple IGAM model, we get that, on expectation, $\Omega\left(\frac{b^H}{c_2^\tau}\right) = \bar{\phi}(S_\tau) = O\left(\frac{b^H}{c_1^\tau}\right)$. If we take $\tau = H_0 = O(\log H)$ to be the core, we can deduce that the core conductance is $\Theta(b^H/H)$ as in the case of the simple IGAM model.

D.1.5 Data Preprocessing

We have ignored directionality in the examined networks and have removed nodes with degree less than or equal to 4 (except in the london–underground network where almost all degrees are very small). The removal of nodes with

degree less than or equal to 4 is done (i) to remove outlier nodes and, (ii) to refer to the removal of non–engaged nodes.

D.1.6 Code and Data

The data used in this study are publicly available and are located in the following resources

- world–trade [119].
- {cs, history, business}–faculty [107].
- polblogs [10].
- airports [111].
- open–airlines [222].
- celegans [224]. 8
- london–underground [222].

D.2 CIGAM Model

D.2.1 Core Size of CIGAM

Coupling construction. Let a CIGAM model G_1 with parameters λ and $1 < c_1 \leq c_2 \cdots \leq c_L < e^{\lambda}$ be given and let a CIGAM model G_2 have parameters λ and one layer with value c_L. We construct the coupling ν as follows: We first

1. The input is provided as a dataset of m edges $\mathcal{D} = \{e_1, \ldots, e_m\}$.
2. Calculate the degree $\bar{y}_u$ of every node u in the sample.
3. We sort the degrees in descending order.
4. For all fanouts $b \in \{2, \ldots, n-1\}$
5. We build a tree by attributing heights to the nodes in descending order of their degree
6. We calculate $\bar{z}_h = \log\left(\sum_{u:h(u)=h} \bar{y}_u\right)$, that is the log-total number of edges on level h as indicated by the samples.
7. We fit a linear least squares relation between h and $\bar{z}_h$ that has the form $\widehat{z}_h = ah + b$
8. We calculate $c = b \cdot e^{-a}$, since the slope a is roughly $\log(b/c)$.
9. We calculate the log–likelihood of the parametrization which equals

$$\sum_{u<v} \Big(\mathbf{1}\{(u,v) \in \mathcal{D}\} \log(c^{-1-\min\{h(u),h(v)\}}) + (1 - \mathbf{1}\{(u,v) \in \mathcal{D}\}) \log(1 - c^{-1-\min\{h(u),h(v)\}}) \Big).$$

10. We return the set of parameters that maximize the computed likelihood.
11. *(Optional: Swaps)* Iterate on every edge $(u,v) \in \mathcal{D}$ and swap $h(u)$ with $h(v)$ if the log–likelihood increases, otherwise do nothing. Iterate until no more swaps are possible.

Algorithm 13: IGAM Fitting Algorithm Pseudocode.

sample the rank vector r (common for both G_1 and G_2) and then construct the hyperedges as follows: (i) If a hyperedge appears on G_2 then with probability 1 is appears on G_1, and (ii) if a hyperedge does does not appear on G_2 then it appears on G_1 with probability $\frac{f_1(e)-f_2(e)}{1-f_2(e)}$. We can easily show that the marginals satisfy $\mathbb{P}[e \in E(G_1)|r] = f_2(e) \cdot 1 + (1-f_2(e)) \frac{f_1(e)-f_2(e)}{1-f_2(e)} = f_1(e)$ and $\mathbb{P}[e \in E(G_2)|r] = f_2(e)$. Finally, we integrate over r to get that $\mathbb{P}[e \in E(G_1)] = f_1(e)$ and $\mathbb{P}[e \in E(G_2)] = f_2(e)$. Therefore ν is a valid coupling. Under ν we have that always $G_2 \subseteq G_1$. Therefore, it suffices to prove the Theorem for G_2 to get a result that holds for G_1.

Core size. We prove the statement in the case that G_1 is k-uniform. Since by the coupling construction $G_2 \subseteq G_1$, proving a statement for the size of the core on G_2 will also hold for G_1 since a dominating set in G_2 is a dominating set in G_1. Let $t \in [0, 1]$ be a threshold value to be determined later. Define

$$N_k(t) = \sum_{(j_1,\dots j_{k-1}) \in \binom{[n]}{k-1}} \mathbf{1}\{\max\{r(j_1), \dots, r(j_{k-1})\} \geq t\}$$

be the number of nodes with ranks at least t. Note that by a simple combinatorial argument

$$\begin{aligned} N_k(t) &= \binom{n}{k-1} - \left| J \in \binom{[n]}{k-1} : \forall j \in J, r_j < t \right| \\ &= \binom{n}{k-1} - \binom{n - N_2(t)}{k-1} \end{aligned}$$

where $N_2(t) \sim \text{Bin}(n, 1 - F(t))$ is the number of nodes with $r_j \geq t$ and $\binom{x}{y} = \frac{\Gamma(x+1)}{\Gamma(y+1)\Gamma(x-y+1)}$ is the generalized biniomial coefficient. The function $g(\nu) = \binom{n}{k-1} - \binom{n-\nu}{k-1}$ is strictly increasing for $0 \leq \nu \leq n$. Therefore, we can directly devise a concentration bound for $N_k(t)$ via concentration bounds for $N_2(t)$. Indeed, by the Chernoff bound

$$\begin{aligned} &\mathbb{P}\left[N_k(t) \geq \binom{n}{k-1} - \binom{n - \mathbb{E}\left[N_2(t)\right] + \sqrt{n \log n/2}}{k-1} \right] \\ &\quad = \mathbb{P}[N_2(t) \geq \mathbb{E}\left[N_2(t)\right] - \sqrt{n \log n/2}] \geq 1 - \frac{1}{n} \end{aligned}$$

as long as $t \leq F^{-1}(1 - \sqrt{\log n/(2n)})$. Note that the probability that a node $i \in [n]$ is not dominated by any core-hyperedge is given by

$$
\begin{aligned}
&\mathbb{P}[i \text{ is not dominated by the core}] \\
&= \prod_{J \in \binom{[n]}{k-1}} \left(1 - c_L^{-2+\max_{j \in J \cup \{i\}} r_j}\right)^{\mathbf{1}\{\max_{j \in J} r_j \geq t\}} \\
&\leq \prod_{J \in \binom{[n]}{k-1}} \left(1 - c_L^{-2+t}\right)^{\mathbf{1}\{\max_{j \in J} r_j \geq t\}} \\
&= \left(1 - c_L^{-2+t}\right)^{N_k(t)} \leq \exp(-N_k(t) c_L^{-2+t}).
\end{aligned}
$$

If $N_k(t) \geq \frac{2 \log n}{c_L^{-2+t}}$ then by the union bound $\mathbb{P}[\exists i : i \text{ is not dominated by the core} | N_k(t) \geq 2 \log n / c_L^{-2+t}] \leq \frac{1}{n}$. Subsequently, the complementary event (i.e. $\forall i$, i is dominated by the core) happens with probability at least $1 - 1/n$. We let t to be such that

$$
\frac{2 \log n}{c_L^{-2+t}} = \binom{n}{k-1} - \binom{nF(t) + \sqrt{n \log n / 2}}{k-1}, \tag{D.3}
$$

in order for $\mathbb{P}[N_k(t) \geq 2 \log n / c_L^{-2+t}] \geq 1 - \frac{1}{n}$. Finally we have that given t that satisfies (D.3)

$$
\mathbb{P}\left[\text{Core at threshold } t\right] \geq \left(1 - \frac{1}{n}\right)^2 \geq 1 - \frac{2}{n}.
$$

Existence and Uniqueness of threshold t. We define

$$
\Phi(t) = \frac{2 \log n}{c_L^{-2+t}} - \binom{n}{k-1} + \binom{nF(t) + \sqrt{n \log n / 2}}{k-1} \tag{D.4}
$$

in the range $[0, t']$ where $t' = F^{-1}\left(1 - \sqrt{\frac{\log n}{2n}}\right)$ is the point where the difference

of the binomial coefficients becomes 0. Note that Φ is continuous and differentiable in $[0, t']$ with derivative

$$\begin{aligned}
\Phi'(t) &= -2\log c_L \log n/c_L^{-2+t} + \binom{nF(t) + \sqrt{n\log n/2}}{k-1} nf(t)\psi(nF(t) \\
&\quad + \sqrt{n\log n/2}) \\
&\geq -2e^{2\lambda}\lambda e^{-\lambda t}\log n + \binom{nF(t) + \sqrt{n\log n/2}}{k-1} nf(t)\psi(nF(t) \\
&\quad + \sqrt{n\log n/2}) \\
&\geq nf(t)\left[-2e^{2\lambda} + \binom{nF(t) + \sqrt{n\log n/2}}{k-1}\psi(nF(t) + \sqrt{n\log n/2})\right] \\
&\geq nf(t)\left[-2e^{2\lambda} + \binom{\sqrt{n\log n/2}}{k-1}\psi(\sqrt{n\log n/2})\right] \\
&\geq nf(t)\left[-2e^{2\lambda} + \sqrt{n\log n/2}\psi(\sqrt{n\log n/2})\right] \\
&\geq nf(t)\left[-2e^{2\lambda} + \sqrt{n\log n/2}\left[\frac{1}{2}\log(n\log n/2) - \frac{1}{\sqrt{n\log n/2}}\right]\right] \\
&\geq nf(t)\left[-3e^{2\lambda} + \sqrt{n/8}\right] > 0.
\end{aligned}$$

for $\lambda < \frac{\ln(n/72)}{4} \in o(\log n)$. $\psi(x) = \frac{\Gamma'(x)}{\Gamma(x)}$ is the digamma function. For the inequalities we have used the facts: (i) $c_L < e^{\lambda}$, (ii) $\log n \leq n$, (iii) monotonicity of the Gamma and the digamma function for $t \geq 0$, (iv) $\binom{n}{k-1} \geq n$ for $k < n-1$, (v) $\psi(x) \geq \log x - \frac{1}{x}$, (vi) $n \geq 2$. Therefore $\Phi(t)$ is strictly increasing. Note that $\Phi(0) = 2c_L^2 \log n - \binom{n}{k-1} + \binom{\sqrt{n\log n}}{k-1} < 0$ for large enough n and since $c_L = o(n)$. Moreover note that $\Phi(t') = 2\log n/c_L^{-2+t'} > 0$. Therefore $\Phi(0)\Phi(t') < 0$. Thus by Bolzano's theorem and the fact that $\Phi'(t) > 0$ we get that there exists a unique threshold $t \in [0, t']$ such that $\Phi(t) = 0$.

Upper Bound. Note that the threshold is maximized when $k = 2$, i.e. in the graph case, and therefore the expected size of the core satisfies $\mathbb{E}[\text{Core size}] \leq$

$n(1 - F(t(k = 2))) = \sqrt{n \log n/2} + 2 \log n/c_L^{-2+t} = \tilde{O}(\sqrt{n})$ (see also Figure 5.11).

Empirical Core Thresholds

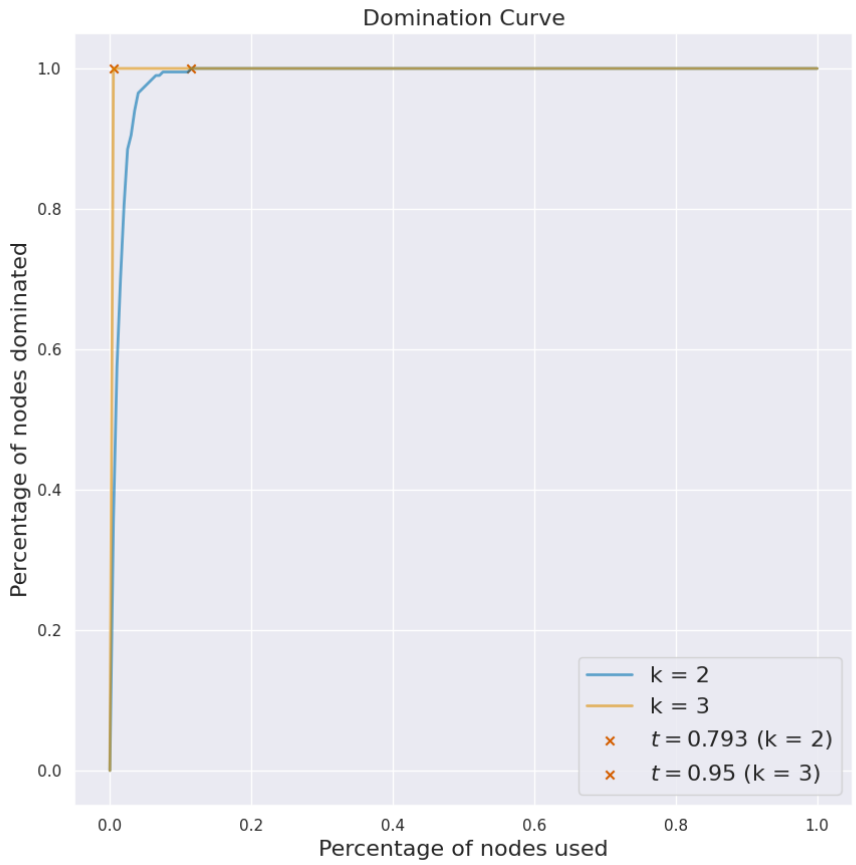


Figure D.1: Empirical core Threshold on generated instances for single layer model with $n = 200$, $b = 3.5$, $c_1 = 3$ for $k \in \{2, 3\}$. By "x" we denote the sample core threshold values.

D.2.2 Sampling

Uniformly Sampling from $\binom{[n]}{k}$. To sample a k-tuple uniformly at random we use a rejection sampling algorithm:

1. Initialize $S \leftarrow \emptyset$.
2. While $|S| \leq k$ repeat: Sample i uniformly from $[n]$, and if $i \notin S$, add i to S.

Ball-dropping (Single-Layer / k-uniform). For each $i \in [n]$ we create a set $\mathcal{B}_i$ in which we sample M_i edges by sampling an edge e uniformly from $\binom{[n]}{k-1}$ (with i being the dominant node, and if $e \cup \{i\}$ does not belong to $\mathcal{B}_i$ we add it to $\mathcal{B}_i$.

Sampling Negative Edges. To sample edges from $e \in \bar{E}$ (i.e. $e \notin E$) we maintain a set $\mathcal{B}$ of certain size b and while $|\mathcal{B}| \leq b$ we sample uniformly an order $\{K = k\}$ with probability $\frac{\tilde{m}_k}{\tilde{m}}$ and then we sample $\bar{e}$ from $\binom{[n]}{k}$ uniformly. If $\bar{e} \notin (E \cup \mathcal{B})$ then we update $\mathcal{B} \leftarrow \mathcal{B} \cup \{\bar{e}\}$.

D.2.3 Implementations

Methods. We implement point estimation and Bayesian inference algorithms as part of the evaluation process, which are available in the code supplement. Table 5.1 shows the costs of fitting CIGAM on various occasions.

1. *Point Estimation (MLE/MAP).* We implement point estimation for the parameters (λ, c) (or (λ, c, θ)) of CIGAM with PyTorch using the log-barrier method. We use Stochastic Gradient Descent (SGD) to train the model for a certain number of epochs, until the learned parameters have converged to their final values. To avoid underflows, and because the resulting probabilities at each epoch are $\ll 1$ we use a smoothing parameter γ (here we use $\gamma = 10^{-10}$). which we add to the corresponding probabilities to avert underflow. For MAP we add priors/regularization to λ, c (see App. D.3).

Table D.1: Experiments with Regularization $\alpha_c = 100, \alpha_\lambda = 1, \beta_\lambda = 2$ (LCC + 2-core) for the StackExchange datasets for SGD with step-size 0.001 and 10 epochs.

Dataset	c^*	λ^*	c^*	λ^*
	Hypergraph		Projected	
threads-ask-ubuntu	[11.1]	1.3	[11.1]	1.3
threads-math-sx	[1522]	1.9	[44.1]	1.7
threads-stack-overflow	[8.6e+11]	10.5	[2.1e+5]	10.9

For Logistic-CP we use the following architecture to learn z_i's: `Linear(`d`,` d`)` $\rightarrow$ `ReLU` $\rightarrow$ `Linear(`d`,` `1)`.

2. *Bayesian Inference (BI).* We implement the posterior sampling procedures with *mc-stan* [173] which offers highly efficient sampling using Hamiltonian Monte Carlo with No-U-Turn-Sampling (HMC-NUTS) [202] and compiles a C++ model for BI. Note that $\mathcal{K}$ is a *convex polytope*. Finally, we add priors (see App. D.3) on the parameters to form a posterior density to sample from. For BI, the stan model samples from the truncated density via defining the parameter `c0` as a `positive_ordered` vector (which induces a log-barrier constraint on the log-posterior) and the parameter `c` is devised as `c0 + 1` in the `transformed parameters` block. The preprocessing takes place in the `transformed data` block, and the `model` block is responsible for the log-posterior oracle.

D.3 Priors & Regularization

For notational convenience, we refer to the priors using the variables defined in the stan model. For CIGAM we can use *exponential* priors for `c` (or `c0` respectively), i.e. we can impose a penalty of the form $p(\texttt{c0}) \propto e^{-\alpha_c \sum_{i \in [L]} \texttt{c0}_i}$. Moreover, a stronger penalty can be applied in terms of a Pareto prior, i.e.

$p(\subset) \propto e^{-\alpha_c \sum_{i \in [L]} \log(\subset_i)}$. For the rank parameter λ we impose a $\texttt{Gamma}(\alpha_\lambda, \beta_\lambda)$ prior.

For Logistic-CP we can use L2 regularization for z_i which corresponds to a Gaussian prior $p(z) \propto e^{-\frac{\alpha_\theta}{2} \sum_{i \in [n]} z_i^2}$ to penalize large values of the core scores both in terms of core ($z_i \geq 0$) and periphery ($z_i < 0$) nodes.

Table D.1 shows the learned parameters when regularization is applied.

APPENDIX E

MODELING NETWORKS WITH LARGE LANGUAGE MODELS

E.1 Experimental Procedure

In our study, we performed experiments to assess whether key network principles at both the micro-level (such as preferential attachment, triadic closure, and homophily) and the macro-level (including community structure and weak ties) align with classical network models. Subsequently, we utilized real-world networks to determine the factors that are most heavily weighted by LLMs.

Network Formation Process

Our experiments span a time series of T steps, with a sequence of network structures denoted as $G_1, G_2, \ldots, G_T$ with vertex sets $V_1, \ldots, V_T$. The initial network, G_1, is referred to as the *seed network*. At each step t, we select a *query node* i_t (which may either be a new arrival or an existing node in the graph) and assign it the task of forming new links. This is accomplished by selecting nodes from a set of alternatives A_t (meaning potential candidates for link formation) and initiating a query call $Q(A_t, i_t, \delta)$ to the LLM (as outlined in Algorithm 15) to create up to δ new links. The edge set selection process involves presenting the LLMs with personal or network features of the alternatives, denoted as $F(A_t) = \{f_a : a \in A_t\}$, which may include information such as the neighbors of the nodes, node degrees, common connections with i_t, and community memberships, formatted in JSON. We adopt a zero-shot learning approach, avoiding the provision of exam-

ples to the model to prevent bias, in line with relevant studies such as [78]. This approach allows for the exploration of the innate preferences of LLMs.

We employ multiple temperatures to account for the variability in response generation by LLM systems, which is also observed in classical statistical models of network formation [210]. Our study conducts experiments using three temperatures for all models except Claude 3.5: 0.5, 1.0, and 1.5. For Claude 3.5 the temperature range is between 0 and 1, and we run experiments with two temperatures: 0.5, and 1.0.

Moreover, the model is tasked with outputting a JSON object indicating the node chosen for link formation and the rationale behind the choice. This approach is adopted because LLMs have demonstrated proficiency in processing code-like structures, such as HTML and JSON.

E.1.1 Feature Representations for Prompts

Below, we give examples of the features used in the prompt presented in Algorithm 15. The features are formatted as a list of JSON objects which are provided to the prompt.

Principle 1: Preferential Attachment. We have the following features:

```
[
    {
        "name" : 0,
        "neighbors" : [5, 7, 1, 6]
    },
    ...
]
```

Principle 2: Triadic Closure. We have the following features:

```
[
    {
        "name" : 0,
        "common_neighbors" : [5, 7, 1, 6]
    },
    ...
]
```

Principle 3: Homophily. We have the following features:

```
[
    {
        "name" : 0,
        "favorite_color" : "red",
        "hobby" : "hiking",
        "location" : "Boston"
    },
    ...
]
```

Principle 5: Small-World. We have the following features:

```
[
    {
        "name" : 0,
        "neighbors" : [5, 7, 1, 6]
    },
    ...
]
```

Real-World Data. We have the following features:

```
[
    {
```

```
        "name" : 0,
        "status" : "student",
        "major" : 10,
        "second major" : 93,
        "accommodation" : "house",
        "high_school" : 5,
        "graduation_year" : 2008
    },
    ...
]
```

We note that the initial Facebook100 dataset included gender information as a feature. We chose not to include gender as one of the features as it has been shown that language models exhibit gender bias [409, 246, 68]. An example of the prompt using real-world social network data is given at Algorithm 14.

E.1.2 Robustness Checks

We tried the following LLM models:

- GPT-3.5 (`gpt-3.5-turbo`)
- GPT-4o Mini (`gpt-4o-mini`)
- Llama 3 (`llama-3-70b-instruct`)
- Claude 3.5 Sonnet (`claude-3-5-sonnet-20240620`).

For each of the models except Claude 3.5 we used three temperatures: 0.5, 1.0, 1.5. For the Claude 3.5 model we used temperatures 0.5 and 1.0 (since the model does not allow temperatures above 1.0). Finally, we experimented with

different environmental prompts (e.g., friendship, collaboration, community) to test prompt sensitivity.

E.2 Details for Small-World Experiments

The algorithm for the altered Watts-Strogatz model is described as follows:

1. Similarly to Watts-Strogatz, we first create a ring network with n nodes. After that, for each node $[n]$, we create k edges where $k/2$ edges connect to its rightmost neighbors and $k/2$ edges connect to its leftmost neighbors.
2. To create G_t, for each node $[n]$, we take its $k/2$ rightmost neighbors and rewire them with probability β. For each of the $k/2$ rightmost neighbors that are to be rewired, we make one query to the LLM, which indicates how the edge will be rewired. The choice is made by providing the LLM with all the network nodes and each node's neighbors (i.e., the network structure).

The model closely resembles the Watts-Strogatz model, with the primary distinction being the method of edge rewiring. Instead of randomly selecting edges for rewiring, as in the Watts-Strogatz model, we determine the rewiring of an edge by inquiring about the LLM and providing it with the current network structure.

E.3 The Discrete Choice Model in Real-World Network Experiments

For each node i_t that we consider at time t, we randomly remove one of its current friends from the real-world network. After we remove a neighbor for each of $i_1, \ldots, i_T$, we end up with the network G_1, which we use as a seed network for the LLM agents.

Subsequently, during the link formation process, we present each node i_t with a set of candidate nodes (denoted by A_t), comprising one of the previously removed friends and other nodes that are not their friends. We then instruct the LLM to form a link with one of the candidates, providing the attributes of the candidates and the social network structure to aid its decision-making. These choices are made sequentially.

We use the *utility* of the model for each node for each sequential decision of network formation:

$$U_{ij,t} = \theta_{\text{PA}} \log d_{j,t} + \theta_{\text{H}} \log w_{ij} + \theta_{\text{TC}} \log c_{ij,t} + \epsilon_{ij,t}.$$

In this equation, θ_{PA} measures the strength of preferential attachment based on the degree $d_{j,t}$ of j at step t, θ_{H} measures the strength of homophily based on the similarity w_{ij} (i.e. number of common attributes) between i and j, and θ_{TC} measures the strength of triadic closure, based on the number of common neighbors $c_{ij,t}$ between i and j at step t. The error term $\epsilon_{ij,t}$ is distributed as i.i.d. standard Gumbel.[1] All variables are first normalized based on their range, and then the log transformation is taken.

[1] The standard Gumbel distribution has CDF $e^{e^{-x}}$.

The multinomial logit model (MNL) indicates that the probability that i links to j at step t is given by

$$p_{ij,t} = \mathbb{P}\left[\text{argmax}_{r \in A_t} U_{ir,t} = j\right] = \frac{d_{j,t}^{\theta_{\text{PA}}} w_{ij}^{\theta_{\text{H}}} c_{ij,t}^{\theta_{\text{TC}}}}{\sum_{r \in A_t} d_{r,t}^{\theta_{\text{PA}}} w_{ir}^{\theta_{\text{H}}} c_{ir,t}^{\theta_{\text{TC}}}}.$$

Given a sequence of nodes $i_1, \ldots, i_T \in V$ and choices (denoted by subscripted j) $j_1 \in A_1, \ldots, j_T \in A_T$, the parameters can be found by maximizing the log-likelihood function. To get the standard errors of the coefficients and the corresponding P-values, we follow the process outlined in [315].

E.4 Estimating the Parameters of the Discrete Choice Model

To estimate the parameters of the discrete choice model, we optimize the following log-likelihood function

$$(\widehat{\theta}_{\text{PA}}, \widehat{\theta}_{\text{TC}}, \widehat{\theta}_{\text{H}}) = \text{argmax}_{(\theta_{\text{PA}}, \theta_{\text{TC}}, \theta_{\text{H}}) \in \mathbf{R}^3} \sum_{t=1}^{T} \left(\theta_{\text{PA}} \log d_{j_t,t} + \theta_{\text{H}} \log w_{i_t j_t} + \theta_{\text{TC}} \log c_{i_t j_t,t} - \log \left(\sum_{r \in A_t} d_{r,t}^{\theta_{\text{PA}}} w_{i_t r}^{\theta_{\text{H}}} c_{i_t r,t}^{\theta_{\text{TC}}} \right) \right),$$

where $i_1, \ldots, i_T$ are the chooser nodes (i.e., the LLM agents who want to form a link), and $j_1, \ldots, j_T$ are the nodes which are chosen from the alternative sets $A_1, \ldots, A_T$. The likelihood function is convex, and we optimize it with the L-BFGS-B method [271]. The standard errors of the coefficients are approximated as $\sqrt{-H^{-1}/N}$ where H is the Hessian matrix of the log-likelihood at $(\widehat{\theta}_{\text{PA}}, \widehat{\theta}_{\text{TC}}, \widehat{\theta}_{\text{H}})$ and N is the number of data points (cf. [315, 393]).

E.5 Data and Code Availability

Data and code are available on GitHub at the following link:

https://github.com/papachristoumarios/llm-network-formation

The real-world social network data have been taken from the sources of [394] and [431].

E.6 Full Regression Table for GPT-4 (gpt-4-1106-preview) and the Facebook100 Data

In Table E.1, we report the regression coefficient for the regression in the real-world network data for all temperatures and GPT-4 (gpt-4-1106-preview). The first column corresponds to the temperature, the next three columns correspond to the fitted coefficients from the regression model of Section 1.C (also shown in Figure 5) accompanied by the standard errors (in parentheses) and the P-values indicated by stars (the null hypothesis corresponds to the parameters being set to 0). Next, LL corresponds to the log-likelihood of the fitted model, and AIC corresponds to the Akaike Information Criterion. Finally, we report the percent change in the accuracy compared to random guessing, the percent change in the average path length (as a measure of the small-world phenomenon), and the clustering coefficient (as a measure of the small-world phenomenon and the triadic closure), as well as the t-statistic for the change in modularity (Q) between the ground truth network dataset (before the edge deletions) and the network after the network formation process.

We observe that $\widehat{\theta}_{\text{H}} > \widehat{\theta}_{\text{TC}} > \widehat{\theta}_{\text{PA}} > 0$ accross all settings. LLM agents do better than random guessing, reinforce the small-world phenomenon, and weaken the triadic closure. Finally, the community structure is strengthened after new links are formed.

Temp.	$\widehat{\theta}_{\text{PA}}$	$\widehat{\theta}_{\text{H}}$	$\widehat{\theta}_{\text{TC}}$	LL	AIC	% Change Acc.	% Change L	% Change C	ΔQ (t-stat)
Caltech36 (769 nodes, 33,312 edges)									
0.5	0.41*** (0.01)	1.95*** (0.02)	0.59*** (0.01)	-1,377.47	2,762.94	171.8	-0.008	-9.94	3.45**
1.0	0.36*** (0.005)	1.85*** (0.02)	0.58*** (0.01)	-1,435.07	2,878.13	179.6	-0.18	-11.08	3.49**
1.5	0.36*** (0.006)	1.72*** (0.01)	0.55*** (0.007)	-1,522.47	3,052.94	127.6	-0.06	-11.46	3.37**
Swarthmore42 (1,659 nodes, 12,2100 edges)									
0.5	0.18*** (0.003)	1.62*** (0.006)	0.65*** (0.002)	-2,838.33	5,684.66	124.2	0.01	-11.46	7.42***
11.0	0.26*** (0.002)	1.70*** (0.008)	0.58*** (0.003)	-2,927.99	5,863.97	91.6	-0.10	-4.25	1.96*
1.5	0.19*** (0.004)	1.50*** (0.008)	0.59*** (0.002)	-3,139.42	6,286.83	87.39	-0.20	-4.52	4.03***
UChicago30 (6,591 nodes, 416,206 edges)									
0.5	0.23*** (0.001)	2.00*** (0.005)	0.41*** (0.002)	-3,444.33	6,896.67	217.2	-0.24	-2.52	7.46*** [0.34]
1.0	0.23*** (0.002)	1.98*** (0.004)	0.38*** (0.001)	-3,578.18	7,164.36	219.2	-0.12	-2.66	9.56*** [1.05]
1.5	0.22*** (0.004)	1.78*** (0.008)	0.41*** (0.002)	-2,033.49	4,074.98	222.4	-0.17	-2.42	10.19*** [0.24]

Notes $\widehat{\theta}_{\text{PA}}$ = Coefficient of log degree, $\widehat{\theta}_{\text{H}}$ = Coefficient of log # of common attributes, $\widehat{\theta}_{\text{TC}}$ = Coefficient of log # common neighbors
LL = Log-likelihood, AIC = Akaike Information Criterion
Acc. = Accuracy, L = Average Path Length, C = Average Clustering Coefficient, ΔQ (t-stat) = Modularity change t-statistic
$^{*}: P < 0.05$, $^{**}: P < 0.01$, $^{***}: P < 0.001$

Table E.1: Multinomial logit coefficients for three networks from the Facebook100 dataset and GPT-4 (gpt-4-1106-preview). The standard errors of the estimates are shown in parentheses. The null hypothesis corresponds to the respective parameter being equal to 0. We report the percent change in accuracy, average path length, and average clustering coefficient compared to the initial network (before the deletion of edges). For the change in modularity, we run the Louvain algorithm ten times and perform a t-test with the resulting modularities. For the UChicago30 dataset, we report the t-statistic value in the subgraph induced by the 2,000 sampled nodes, since the newly added edges would have a very small effect on the change in the community structure if we were to measure it in the whole network. We also report the modularity change (t-statistic) of the whole graph inside brackets.

E.6.1 Analytical Regression Tables for GPT-4 (gpt-4-1106-preview)

We present the regression tables for all the combinations of coefficients for each of the three real-world network datasets. For all datasets, we observe that $\widehat{\theta}_{\text{PA}}$ is smaller than both $\widehat{\theta}_{\text{TC}}$ and $\widehat{\theta}_{\text{H}}$ in all models where any pair is included. Similarly, $\widehat{\theta}_{\text{TC}}$ is always smaller than $\widehat{\theta}_{\text{H}}$ in all models that are both included. Finally, note that whenever only $\widehat{\theta}_{\text{PA}}$ and $\widehat{\theta}_{\text{TC}}$ are considered, then $\widehat{\theta}_{\text{PA}} < 0$ and the result is not statistically significant ($P > 0.05$).

Temp.	$\widehat{\theta}_{\text{PA}}$	$\widehat{\theta}_{\text{H}}$	$\widehat{\theta}_{\text{TC}}$	Log Likelihood	AIC
0.5	0.50*** (0.001)			-2,236.36	4,476.71
0.5		2.78*** (0.003)		-1,511.42	3,026.85
0.5			1.53*** (0.002)	-1,506.01	3,016.02
0.5	0.64*** (0.002)	2.99*** (0.007)		-1,414.71	2,835.41
0.5	-0.02 (0.003)		1.53*** (0.003)	-1,505.95	3,017.90
0.5		1.43*** (0.004)	0.82*** (0.002)	-1,406.39	2,818.78
0.5	0.41*** (0.01)	1.95*** (0.02)	0.59*** (0.01)	-1,377.47	2,762.94
1.0	0.48*** (0.001)			-2,242.85	4,489.70
1.0		2.69*** (0.003)		-1,558.67	3,121.34
1.0			1.47*** (0.002)	-1,556.68	3,117.37
1.0	0.58*** (0.002)	2.86*** (0.003)		-1,473.13	2,952.26
1.0	-0.04 (0.002)		1.47*** (0.002)	-1,556.24	3,118.48
1.0		1.40*** (0.01)	0.79*** (0.002)	-1,457.76	2,921.52
1.0	0.36*** (0.005)	1.85*** (0.02)	0.58*** (0.01)	-1,435.07	2,878.13
1.5	0.50*** (0.001)			-2,233.25	4,470.50
1.5		2.51*** (0.003)		-1,646.83	3,297.65
1.5			1.36*** (0.001)	-1,636.20	3,276.40
1.5	0.57*** (0.002)	2.65*** (0.005)		-1,559.57	3,125.15
1.5	-0.01 (0.002)		1.37*** (0.002)	-1,636.19	3,278.37
1.5		1.29*** (0.004)	0.75*** (0.002)	-1,546.78	3,099.55
1.5	0.36*** (0.006)	1.72*** (0.01)	0.55*** (0.007)	-1,522.47	3,052.94
Note				$^{*}: P < 0.05$, $^{**}: P < 0.01$, $^{***}: P < 0.001$	

Table E.2: Multinomial logit coefficients for Caltech36 and GPT-4 (gpt-4-1106-preview). The standard errors of the estimates are shown in parentheses.

Temp.	$\widehat{\theta}_{\text{PA}}$	$\widehat{\theta}_{\text{H}}$	$\widehat{\theta}_{\text{TC}}$	Log Likelihood	AIC
0.5	0.33*** (0.0007)			-4,978.28	9,960.56
0.5		2.91*** (0.001)		-3,027.03	6,058.06
0.5			1.37*** (0.0006)	-3,014.28	6,032.57
0.5	0.44*** (0.004)	2.99*** (0.003)		-2,948.91	5,903.82
0.5	-0.18*** (0.002)		1.36*** (0.002)	-3,002.17	6,010.35
0.5		1.42*** (0.003)	0.72*** (0.002)	-2,847.16	5,700.32
0.5	0.18*** (0.003)	1.62*** (0.006)	0.65*** (0.002)	-2,838.33	5,684.66
1.0	0.38*** (0.0007)			-4,959.02	9,922.04
1.0		2.83*** (0.001)		-3,119.06	6,242.11
1.0			1.32*** (0.0006)	-3,118.13	6,240.26
1.0	0.50*** (0.004)	2.92*** (0.002)		-3,018.85	6,043.71
1.0	-0.11** (0.002)		1.32*** (0.002)	-3,113.21	6,232.43
1.0		1.41*** (0.004)	0.69*** (0.003)	-2,947.89	5,901.78
1.0	0.26*** (0.002)	1.70*** (0.008)	0.58*** (0.003)	-2,927.99	5,863.97
1.5	0.36*** (0.0007)			-4,952.51	9,909.02
1.5		2.64*** (0.001)		-3,324.71	6,653.43
1.5			1.24*** (0.0006)	-3,306.06	6,616.11
1.5	0.44*** (0.003)	2.71*** (0.001)		-3,241.67	6,489.35
1.5	-0.14*** (0.003)		1.24*** (0.001)	-3,298.07	6,602.13
1.5		1.30*** (0.003)	0.67*** (0.002)	-3,150.29	6,306.57
1.5	0.19*** (0.004)	1.50*** (0.008)	0.59*** (0.002)	-3,139.42	6,286.83
Note				$^{*}: P < 0.05,\ ^{**}: P < 0.01,\ ^{***}: P < 0.001$	

Table E.3: Multinomial logit coefficients for Swarthmore42 and GPT-4 (gpt-4-1106-preview). The standard errors of the estimates are shown in parentheses.

E.7 Network Evolution and Omitted Simulations

Here we depict the evolution of the networks generated by the LLM agents, as well as omitted simulations.

E.7.1 Principle 1: Preferential Attachment

Network Evolution

We plot the evolution of the LLM-based preferential attachment networks at three timesteps, together with the degree distribution alongside the degree distribution of a BA graph with the same number of nodes. We observe that for the

Temp.	$\widehat{\theta}_{\text{PA}}$	$\widehat{\theta}_{\text{H}}$	$\widehat{\theta}_{\text{TC}}$	Log Likelihood	AIC
0.5	0.28*** (0.02)			-5,983.56	11,971.13
0.5		2.93*** (0.05)		-3,637.18	7,278.37
0.5			1.11*** (0.02)	-3,740.78	7,485.55
0.5	0.38*** (0.04)	3.06*** (0.21)		-3,523.06	7,052.12
0.5	-0.04 (0.08)		1.11*** (0.04)	-3,739.31	7,484.61
0.5		1.68*** (0.13)	0.51*** (0.07)	-3,477.37	6,960.75
0.5	0.23*** (0.06)	2.00*** (0.24)	0.41*** (0.09)	-3,444.33	6,896.67
1.0	0.28*** (0.02)			-5,982.66	11,969.32
1.0		2.85*** (0.05)		-3,759.78	7,523.56
1.0			1.07*** (0.02)	-3,879.04	7,762.08
1.0	0.36*** (0.07)	2.96*** (0.31)		-3,649.84	7,305.68
1.0	-0.04 (0.06)		1.07*** (0.03)	-3,877.83	7,761.66
1.0		1.67*** (0.11)	0.49*** (0.08)	-3,611.48	7,228.95
1.0	0.23*** (0.10)	1.98*** (0.17)	0.38*** (0.06)	-3,578.18	7,164.36
1.5	0.30*** (0.03)			-3,241.67	6,487.34
1.5		2.71*** (0.06)		-2,145.02	4,294.03
1.5			1.03*** (0.02)	-2,175.32	4,354.64
1.5	0.37*** (0.08)	2.81*** (0.10)		-2,080.67	4,167.34
1.5	-0.01 (0.04)		1.03*** (0.04)	-2,175.25	4,356.49
1.5		1.50*** (0.10)	0.51*** (0.04)	-2,051.61	4,109.23
1.5	0.22*** (0.12)	1.78*** (0.27)	0.41*** (0.07)	-2,033.49	4,074.98
Note				$^{*}: P < 0.05,\ ^{**}: P < 0.01,\ ^{***}: P < 0.001$	

Table E.4: Multinomial logit coefficients for UChicago30 and GPT-4 (gpt-4-1106-preview). The standard errors of the estimates are shown in parentheses.

temperature being 0.5 we have a core-periphery-like formation which diverges from the BA model, whereas for the temperature being 1.5 the network has the same degree distribution as the BA model.

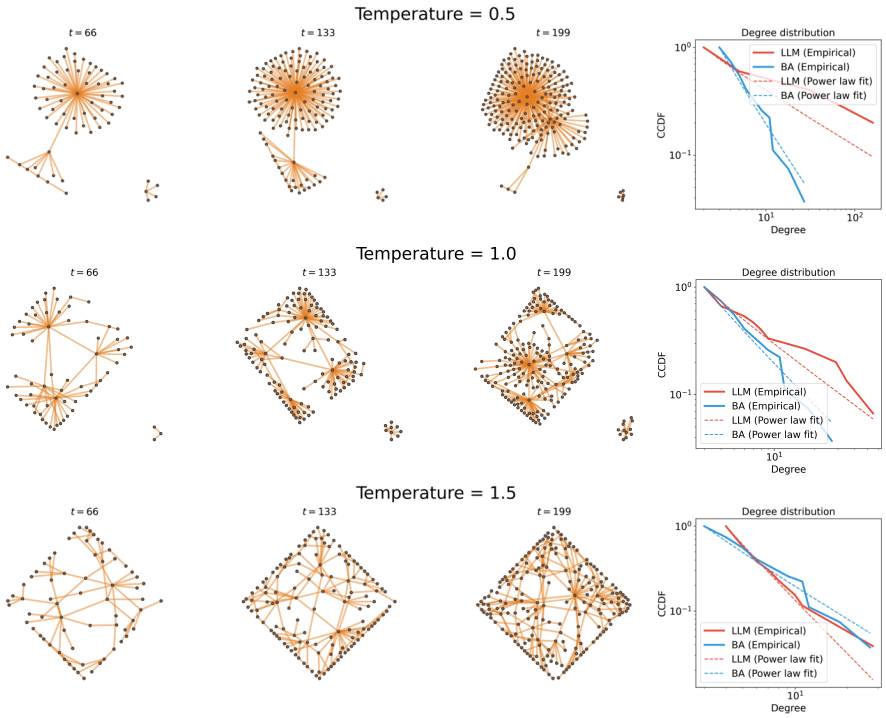


Figure E.1: Dynamic evolution of networks created based on Principle 1.

Simulations with Degree Information

In Figure E.2 we provide the results with degree-information only. We observe that the agents form connections around high-degree nodes only (see Figure E.2). The same result (star-like networks) holds for the other LLM models and temperatures.

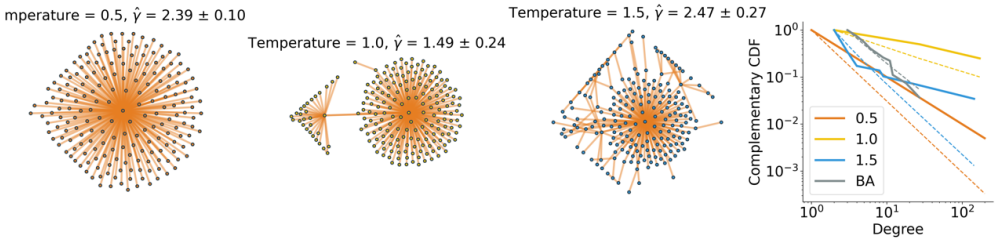


Figure E.2: **Results for Principle 1 (preferential attachment):** We display simulated networks comprising 200 nodes across different temperatures. For the degree-based simulations, node degree data $\{d_{j,t} : j \in V_t\}$ was provided (V_t corresponds to the vertex set of the network G_t at round t). With degree information only, the networks form more unrealistic star-like structures, diverging from scale-free configurations and more closely mirroring a core-periphery network structure.

E.7.2 Principle 2: Triadic Closure

Network Evolution

We plot the evolution of the LLM-generated networks based on the triadic closure principle, together with the transitivity measure and the algebraic connectivity (which corresponds to the second-smallest eigenvalue of the graph Laplacian). We observe that the algebraic connectivity gradually increases as new edges between the clusters are created. Specifically, the algebraic connectivity reaches a higher value for higher temperatures, indicating the more frequent creation of new intra-cluster edges. Moreover, we observe that the transitivity initially increases and then decreases until it reaches its final value.

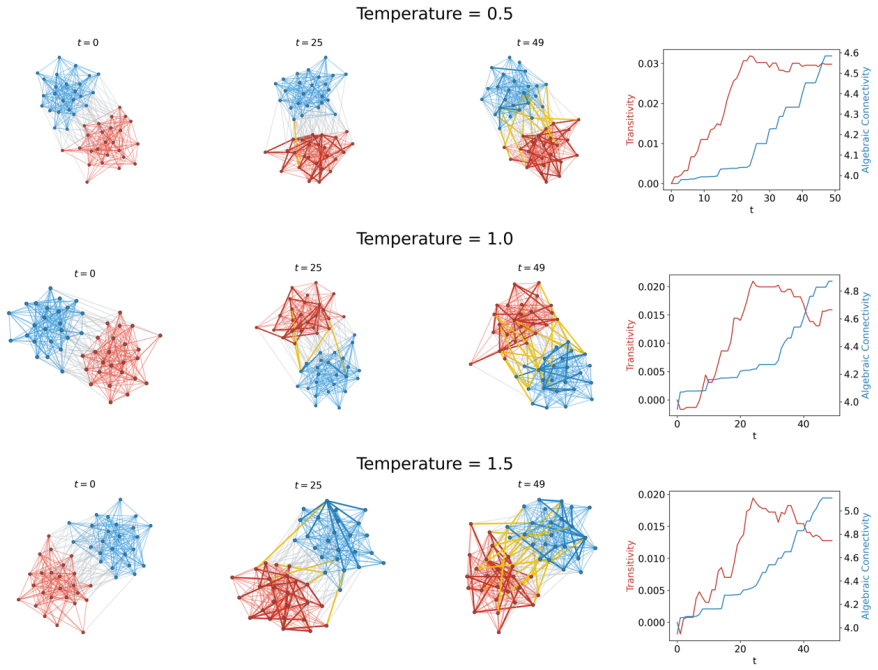


Figure E.3: Dynamic evolution of networks created based on Principle 2.

Simulations with the Number of Common Neighbors

Instead of giving the neighborhood information, the simulations presented in Figure E.4 use the number of common neighbors. We observe behavior similar to Figure 6.2.

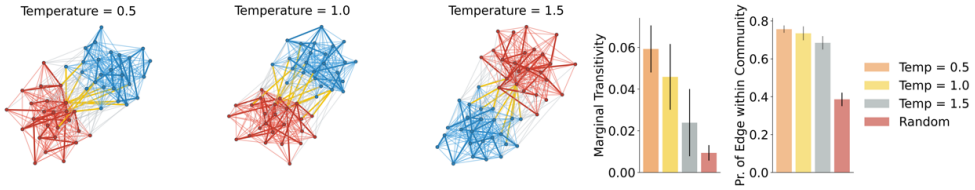
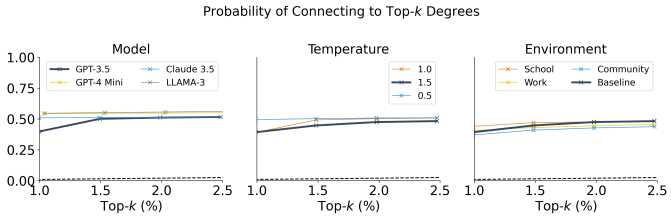


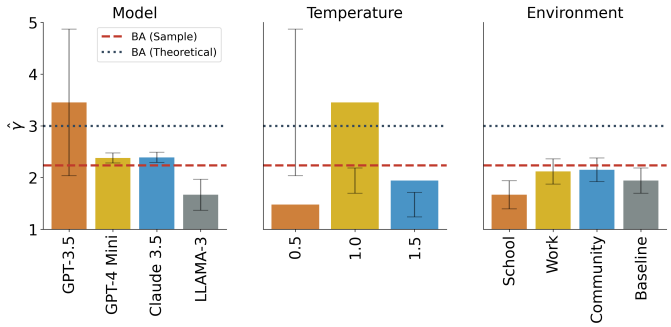
Figure E.4: **Results for Principle 2 (triadic closure).** The figure shows the same networks as in Figure 6.2 with the only change that instead of the intersection of neighborhoods between the query node and each alternative, we provide the number of common neighbors (i.e., the size of the intersection) between the query node and each alternative. Similarly, we observe that the probability of forming an edge within the same community and the marginal transitivity, which indicate triadic closure, is significantly larger than randomly creating links ($P < 0.001$, t-test). The error bars correspond to 95% confidence intervals.

E.8 Chain-of-Thought Experiments

We experiment with Chain-of-Thought (CoT) reasoning [421]. To induce CoT reasoning, we ask the LLM agents to output the reason and then their choice (i.e., by reversing the order of `reason` and `name` in the prompt. The resulting prompt can be found at Algorithm 16. In the following figures, we show the results from the same experiments as the ones of the main text with the difference that CoT is used.



(a) Probability of connecting to top-k nodes for different models, temperatures, and environments



(b) Power law fits ($\hat{\gamma}$) and standard errors for different models, temperatures, and environments

Figure E.5: **Results for Principle 1 with CoT reasoning (preferential attachment)** The multi-LLM setup was given neighborhood information $\{N_{j,t} : j \in V_t\}$. **Top:** Probability of connecting to top-k-degree nodes for varying model (temperature is fixed to 1.0 and environment to baseline), temperature (model fixed to GPT-3.5 and environment to baseline) and environment (model fixed to GPT-3.5 and environment temperature to 1.5) for networks generated according to Principle 1 with $n = 200$ nodes. **Bottom:** Power Law exponents and standard errors for varying model, temperature, and environment.

Algorithm 14 Example prompt regarding social network data.

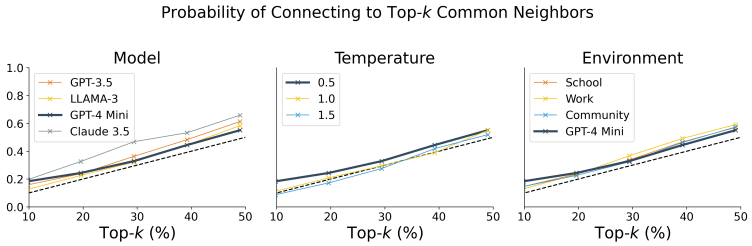
```
# Task
You are located in a school. Your task is to select a set of people to be friends
 with.

# Profile
Your profile is given below after chevrons:
<PROFILE>
    {
        "name" : "Person 0",
        "favorite subject" : "Chemistry",
        "neighbors" : ["Person 3", "Person 432", "Person 4", "Person 3", "Person
         32"]
    }
</PROFILE>

# Candidate Profiles
The candidate profiles to be friends with are given below after chevrons:

<PROFILES>
[
    {
        "name" : "Person 1",
        "favorite subject" : "Mathematics",
        "neighbors" : ["Person 3", "Person 4", "Person 23", "Person 65"]
    },
    {
        "name" : "Person 33",
        "favorite subject" : "History",
        "neighbors" : ["Person 342", "Person 2", "Person 12"]
    }, ...
]

</PROFILES>

# Output
The output should be given a list of JSON objects with the following structure

[
    {{
        "name" : name of the person you selected,
        "reason" : reason for selecting the person
    }}, ...
]

# Notes
- The output must be a list of JSON objects ranked in the order of preference.
- You can make at most 1 selection.
```

Algorithm 15 General Prompt used to implement $Q(A_t, i_t, \delta)$.

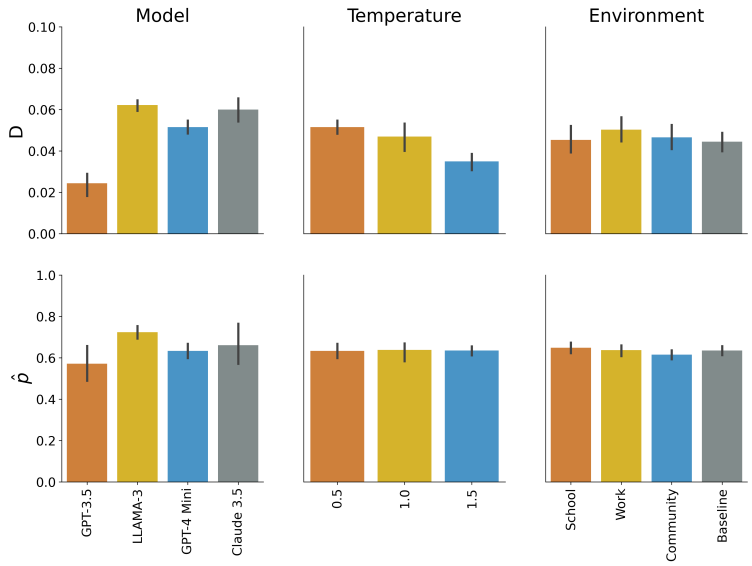
```
# Task
Your task is to select a set of people to be friends with.

# Profile
Your profile is given below after chevrons:
<PROFILE>F({i_t})</PROFILE>

# Candidate Profiles
The candidate profiles to be friends with are given below after chevrons:

<PROFILES>F(A_t)</PROFILES>

# Output
The output should be given a list of JSON objects with the following structure

[
    {{
        "name" : name of the person you selected,
        "reason" : reason for selecting the person
    }}, ...
]

# Notes
- The output must be a list of JSON objects ranked in the order of preference.
- You can make at most δ selections.
```

Algorithm 16 Example prompt regarding social network data with Chain-of-Thought reasoning. Note that compared to the prompt without CoT the order of the fields `name` and `reason` in the output format is reversed.

```
# Task
You are located in a school. Your task is to select a set of people to be friends
 with.

# Profile
Your profile is given below after chevrons:
<PROFILE>
    {
        "name" : "Person 0",
        "favorite subject" : "Chemistry",
        "neighbors" : ["Person 3", "Person 432", "Person 4", "Person 3", "Person
         32"]
    }
</PROFILE>

# Candidate Profiles
The candidate profiles to be friends with are given below after chevrons:

<PROFILES>
[
    {
        "name" : "Person 1",
        "favorite subject" : "Mathematics",
        "neighbors" : ["Person 3", "Person 4", "Person 23", "Person 65"]
    },
    {
        "name" : "Person 33",
        "favorite subject" : "History",
        "neighbors" : ["Person 342", "Person 2", "Person 12"]
    }, ...
]

</PROFILES>

# Output
The output should be given a list of JSON objects with the following structure

[
    {{
        "reason" : reason for selecting the person,
        "name" : name of the person you selected
    }}, ...
]

# Notes
- The output must be a list of JSON objects ranked in the order of preference.
- You can make at most 1 selection.
```

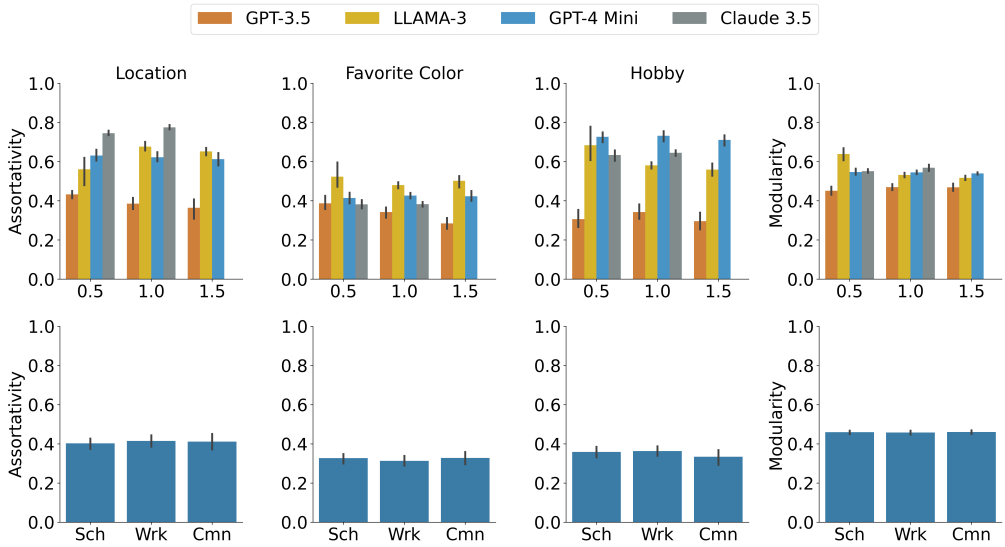


(a) Probability of connecting to top-k for different models, temperatures, and environments



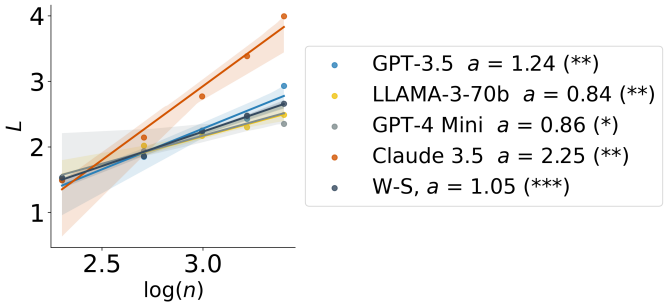
(b) Marginal transitivity (D) and probability of an edge within a community ($\hat{p}$) for different models, temperatures, and environments

Figure E.6: **Results for Principle 2 with CoT reasoning (triadic closure). Top:** Probability of connecting to top-k nodes (in terms of common neighbors) for varying model (temperature is fixed to 1.0 and environment to baseline), temperature (model fixed to GPT-4 Mini and environment to baseline) and environment (model fixed to GPT-4 Mini and environment temperature to 0.5) for networks generated according to Principle 2 ($n = 50$, 10 simulations for each model, environment and temperature). **Bottom:** Marginal transitivity (D) and probability of an edge within a community ($\hat{p}$) for networks generated according to Principle 2 in different models, temperatures, and environments.



(a) Assortativity and Louvain Modularity with different LLM models and environments

Figure E.7: **Results for Principle 3 (Homophily) and Principle 4 (Community structure due to homophily) with CoT reasoning. Top:** Assortativities and Louvain modularity according to Principle 3 ($n = 50$, 5 simulations for each row) in different environments (school, work, community) using different models. The statistical significance is $P < 0.001$ for all t-tests (comparing with 0).



(a) Regression plot for different models and environments for $\beta = 0.25$ and $k = 5$.

Figure E.8: **Fitted results for Principle 5 with CoT reasoning (small world).** Regression plot for the relation $L \sim \log(n)$ for different LLM models for $\beta = 0.25$ and $k = 5$. The legend shows the effect size (a) and the P-value. (*: $P < 0.05$; **: $P < 0.01$, and ***: $P < 0.001$.)

APPENDIX F

CODE AND DATASETS

The code and datasets for the simulations of this thesis can be found at (Accessed on July 1, 2025):

- Chapter 2
  - Code: https://github.com/papachristoumarios/financial-contagion and https://github.com/papachristoumarios/dynamic-clearing.
  - Datasets: The SafeGraph dataset has been obtained from https://www.safegraph.com under an academic license. The TLC data are openly available at https://www.nyc.gov/site/tlc/about/tlc-trip-record-data.page, and the Venmo data can be found at https://github.com/sa7mon/venmo-data.
- Chapter 3
  - Code: https://github.com/papachristoumarios/supply-chain-resilience
  - Dataset: The dataset has been obtained from [422].
- Chapter 4
  - Code: https://github.com/papachristoumarios/dp-distributed-estimation and https://github.com/papachristoumarios/dp-social-learning.
  - Datasets: The data have been obtained from [419] for the US power grid, and from [286] for the GEM openHouse. The AIDS Clinical

Trials Dataset was obtained from Kaggle: https://www.kaggle.com/datasets/tanshihjen/aids-clinical-trials. Original information about the clinical trial can be found at https://clinicaltrials.gov/study/NCT00000625. The data set for the cancer clinical trial was obtained from [359].

- Chapter 5
  - Code: https://github.com/papachristoumarios/core-periphery-hypergraphs
  - Datasets: The coauth-MAG-KDD and ghtorrent-projects datasets can be found at https://doi.org/10.5281/zenodo.6639983. The StackExchange datasets can be found at https://www.cs.cornell.edu/~arb/data.
- Chapter 6
  - Code: https://github.com/papachristoumarios/llm-network-formation
  - Datasets: The Facebook100 data are taken from [394] and the Andorra and company datasets are taken from [431].

BIBLIOGRAPHY

[1] Ali E Abbas. A kullback-leibler view of linear and log-linear pools. *Decision Analysis*, 6(1):25–37, 2009.

[2] Rediet Abebe, Jon M Kleinberg, and S Matthew Weinberg. Subsidy allocations in the presence of income shocks. In *AAAI*, pages 7032–7039, 2020.

[3] Daron Acemoglu, Ufuk Akcigit, and William Kerr. Networks and the macroeconomy: An empirical exploration. *NBER Macroeconomics Annual*, 30(1):273–335, 2016.

[4] Daron Acemoglu, Vasco M Carvalho, Asuman Ozdaglar, and Alireza Tahbaz-Salehi. The network origins of aggregate fluctuations. *Econometrica*, 80(5):1977–2016, 2012.

[5] Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asu Ozdaglar. Too much data: Prices and inefficiencies in data markets. *American Economic Journal: Microeconomics*, 14(4):218–256, 2022.

[6] Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asuman Ozdaglar. Privacy-constrained network formation. *Games and Economic Behavior*, 105:255–275, 2017.

[7] Daron Acemoglu, Asuman Ozdaglar, and Alireza Tahbaz-Salehi. Networks, shocks, and systemic risk. Technical report, National Bureau of Economic Research, 2015.

[8] Daron Acemoglu, Asuman Ozdaglar, and Alireza Tahbaz-Salehi. Systemic risk and stability in financial networks. *American Economic Review*, 105(2):564–608, 2015.

[9] Krishna Acharya, Franziska Boenisch, Rakshit Naidu, and Juba Ziani. Personalized differential privacy for ridge regression. *arXiv preprint arXiv:2401.17127*, 2024.

[10] Lada A Adamic and Natalie Glance. The political blogosphere and the 2004 us election: divided they blog. In *Proceedings of the 3rd international workshop on Link discovery*, pages 36–43, 2005.

[11] Gati V Aher, Rosa I Arriaga, and Adam Tauman Kalai. Using large language models to simulate multiple humans and replicate human subject studies. In *International Conference on Machine Learning*, pages 337–371. PMLR, 2023.

[12] Dohyun Ahn and Kyoung-Kuk Kim. Optimal intervention under stress scenarios: A case of the korean financial system. *Operations Research Letters*, 47(4):257–263, 2019.

[13] Andreea B Alexandru and George J Pappas. Private weighted sum aggregation. *IEEE Transactions on Control of Network Systems*, 9(1):219–230, 2021.

[14] Andreea B Alexandru, Anastasios Tsiamis, and George J Pappas. Towards private data-driven control. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 5449–5456. IEEE, 2020.

[15] Franklin Allen and Douglas Gale. Financial contagion. *Journal of political economy*, 108(1):1–33, 2000.

[16] Victor Amelkin and Rakesh Vohra. Yield uncertainty and strategic formation of supply chain networks. *preprint arXiv:1907.09943*, 2019.

[17] Hamed Amini, Rama Cont, and Andreea Minca. Stress testing the resilience of financial networks. *International Journal of Theoretical and applied finance*, 15(01):1250006, 2012.

[18] Hamed Amini and Zachary Feinstein. Optimal network compression. *European Journal of Operational Research*, 306(3):1439–1455, 2023.

[19] Anita Anand, Michael J Trebilcock, and Michael Rosenstock. Institutional design and the new systemic risk in banking crises. *Available at SSRN 2437217*, 2014.

[20] Anthropic. Claude: Large language model by anthropic, 2024. Accessed: 2024-09-18.

[21] Apple Differential Privacy Team. Learning with privacy at scale. https://machinelearning.apple.com/research/learning-with-privacy-at-scale, 2017. Accessed: 2023-05-18.

[22] Çağın Ararat and Nurtai Meimanjan. Computation of systemic risk measures: a mixed-integer programming approach. *Operations Research*, 2023.

[23] ARPA-H. ARPA-H Launches Groundbreaking Funding Opportunity to Improve Clinical Trials. https://arpa-h.gov/news-and-events/arpa-h-launches-groundbreaking-funding-opportunity-improve-clinical-trials, 2024. Accessed: 2024-12-13.

[24] Oriol Artime, Marco Grassia, Manlio De Domenico, James P Gleeson, Hernán A Makse, Giuseppe Mangioni, Matjaž Perc, and Filippo Radicchi. Robustness and resilience of complex networks. *Nature Reviews Physics*, pages 1–18, 2024.

[25] Esso-Hanam Atake. Health shocks in sub-saharan africa: are the poor and uninsured households more vulnerable? *Health economics review*, 8(1):1–13, 2018.

[26] Nikolay Atanasov, Roberto Tron, Victor M. Preciado, and George J. Pappas. Joint estimation and localization in sensor networks. *IEEE Conference on Decision and Control (CDC)*, pages 6875–6882, 2014.

[27] Nikolay A Atanasov, Jerome Le Ny, and George J Pappas. Distributed algorithms for stochastic source seeking with mobile robot networks. *Journal of Dynamic Systems, Measurement, and Control*, 2014.

[28] R. J. Aumann. Agreeing to disagree. *The annals of statistics*, pages 1236–1239, 1976.

[29] Chen Avin, Zvi Lotker, David Peleg, Yvonne Anne Pignolet, and Itzik Turkel. Core-periphery in networks: An axiomatic approach. *arXiv preprint arXiv:1411.2242*, 2014.

[30] Jordan Awan and Aleksandra Slavković. Differentially private uniformly most powerful tests for binomial data. *Advances in Neural Information Processing Systems*, 31, 2018.

[31] Christoph Aymanns and Co-Pierre Georg. Contagious synchronization and endogenous network formation in financial networks. *Journal of Banking & Finance*, 50:273–285, 2015.

[32] Ana Babus. The formation of financial networks. *Tinbergen Institute Discussion Paper*, 2013.

[33] Raghu Raj Bahadur. A representation of the joint distribution of responses to n dichotomous items. *Studies in item analysis and prediction*, pages 158–168, 1961.

[34] Eytan Bakshy, Itamar Rosenn, Cameron Marlow, and Lada Adamic. The role of social networks in information diffusion. In *Proceedings of the 21st international conference on World Wide Web*, pages 519–528, 2012.

[35] Abhijit Banerjee, Emily Breza, Arun G Chandrasekhar, and Markus Mobius. Naive learning with uninformed agents. *American Economic Review*, 111(11):3540–3574, 2021.

[36] Abhijit Banerjee, Arun G Chandrasekhar, Esther Duflo, and Matthew O Jackson. The diffusion of microfinance. *Science*, 341(6144):1236498, 2013.

[37] Siddhartha Banerjee, Daniel Freund, and Thodoris Lykouris. Pricing and optimization in shared vehicle systems: An approximation framework. *Operations Research*, 2021.

[38] Tathagata Banerjee, Alex Bernstein, and Zachary Feinstein. Dynamic clearing and contagion in financial networks. *arXiv preprint arXiv:1801.02091*, 2018.

[39] Tathagata Banerjee and Zachary Feinstein. Price mediated contagion through capital ratio requirements with vwap liquidation prices. *European Journal of Operational Research*, 295(3):1147–1160, 2021.

[40] Tathagata Banerjee and Zachary Feinstein. Pricing of debt and equity in a financial network with comonotonic endowments. *Operations Research*, 70(4):2085–2100, 2022.

[41] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, 1999.

[42] Michael Barbaro, Tom Zeller, and Saul Hansell. A face is exposed for aol searcher no. 4417749. *New York Times*, 9(2008):8, 2006.

[43] Shane Barratt and Stephen Boyd. Multi-period liability clearing via convex optimal control. *Available at SSRN 3604618*, 2020.

[44] Shane Barratt and Stephen Boyd. Multi-period liability clearing via convex optimal control. *Optimization and Engineering*, 24(2):1387–1409, 2023.

[45] Paolo Bartesaghi, Michele Benzi, Gian Paolo Clemente, Rosanna Grassi, and Ernesto Estrada. Risk-dependent centrality in economic and financial networks. *SIAM Journal on Financial Mathematics*, 11(2):526–565, 2020.

[46] Stefano Battiston, Domenico Delli Gatti, Mauro Gallegati, Bruce Greenwald, and Joseph E Stiglitz. Liaisons dangereuses: Increasing connectivity, risk sharing, and systemic risk. *Journal of economic dynamics and control*, 36(8):1121–1141, 2012.

[47] Stefano Battiston, Michelangelo Puliga, Rahul Kaushik, Paolo Tasca, and Guido Caldarelli. Debtrank: Too central to fail? financial networks, the fed and systemic risk. *Scientific reports*, 2(1):1–6, 2012.

[48] Morten L Bech and Enghin Atalay. The topology of the federal funds market. *Physica A: Statistical mechanics and its applications*, 389(22):5223–5246, 2010.

[49] Omri Ben-Eliezer, Talya Eden, Joel Oren, and Dimitris Fotakis. Sampling multiple nodes in large networks: Beyond random walks. In *Proceedings of the fifteenth ACM international conference on web search and data mining*, pages 37–47, 2022.

[50] Austin R Benson. Three hypergraph eigenvector centralities. *SIAM Journal on Mathematics of Data Science*, 1(2):293–312, 2019.

[51] Austin R Benson, Rediet Abebe, Michael T Schaub, Ali Jadbabaie, and Jon Kleinberg. Simplicial closure and higher-order link prediction. *Proceedings of the National Academy of Sciences*, 115(48):E11221–E11230, 2018.

[52] Sebastian Benthall and Rachel Cummings. Integrating differential privacy and contextual integrity. In *2022 USENIX Conference on Privacy Engineering Practice and Respect*, 2022.

[53] Nils Bertschinger, Martin Hoefer, and Daniel Schmand. Strategic payments in financial networks. *arXiv preprint arXiv:1908.01714*, 2019.

[54] Sara Biagini and Marco Frittelli. A unified framework for utility maximization problems: an orlicz space approach. 2008.

[55] Ginestra Bianconi and A-L Barabási. Competition and multiscaling in evolving networks. *Europhysics letters*, 54(4):436, 2001.

[56] P. J. Bickel and K. A. Doksum. *Mathematical Statistics: Basic Ideas and Selected Topics, volume I*, volume I. CRC Press, 2015.

[57] Kostas Bimpikis, Ozan Candogan, and Shayan Ehsani. Supply disruptions and optimal network structures. *Management Science*, 65(12):5504–5517, 2019.

[58] Kostas Bimpikis, Douglas Fearing, and Alireza Tahbaz-Salehi. Multisourcing and miscoordination in supply chain networks. *Operations Research*, 66(4):1023–1039, 2018.

[59] Philippe Blaettchen, Andre P Calmon, and Georgina Hall. Traceability technology adoption in supply chain networks. *preprint arXiv:2104.14818*, 2021.

[60] Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre. Fast unfolding of communities in large networks. *Journal of statistical mechanics: theory and experiment*, 2008(10):P10008, 2008.

[61] Avrim Blum, Jamie Morgenstern, Ankit Sharma, and Adam Smith. Privacy-preserving public information for sequential games. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, pages 173–180, 2015.

[62] Lawrence Blume, David Easley, Jon Kleinberg, Robert Kleinberg, and Éva Tardos. Network formation in the presence of contagious risk. *ACM Transactions on Economics and Computation (TEAC)*, 1(2):1–20, 2013.

[63] Béla Bollobás. *Random graphs*. Number 73. Cambridge university press, 2001.

[64] Béla Bollobás and Bollobás Béla. *Random graphs*. Number 73. Cambridge university press, 2001.

[65] Anthony Bonato, Jeannette Janssen, and Paweł Prałat. Geometric protean graphs. *Internet Mathematics*, 8(1-2):2–28, 2012.

[66] Anthony Bonato, Marc Lozier, Dieter Mitsche, Xavier Pérez-Giménez, and Paweł Prałat. The domination number of on-line social networks and random geometric graphs. In *International Conference on Theory and Applications of Models of Computation*, pages 150–163. Springer, 2015.

[67] Kallista Bonawitz, Peter Kairouz, Brendan McMahan, and Daniel Ramage. Federated learning and privacy: Building privacy-preserving systems for machine learning and data science on decentralized data. *Queue*, 19(5):87–114, 2021.

[68] Shikha Bordia and Samuel R Bowman. Identifying and reducing gender bias in word-level language models. *arXiv preprint arXiv:1904.03035*, 2019.

[69] Stephen P Borgatti and Martin G Everett. Models of core/periphery structures. *Social networks*, 21(4):375–395, 2000.

[70] Stephen P Borgatti and Xun Li. On social network analysis in a supply chain context. *Journal of supply chain management*, 45(2):5–22, 2009.

[71] Christian Borgs, Michael Brautbar, Jennifer Chayes, and Brendan Lucier. Maximizing social influence in nearly optimal time. In *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 946–957. SIAM, 2014.

[72] Christian Borgs, Jennifer Chayes, Ayalvadi Ganesh, and Amin Saberi. How to distribute antidote to control epidemics. *Random Structures & Algorithms*, 37(2):204–222, 2010.

[73] V. Borkar and P.P. Varaiya. Asymptotic agreement in distributed estimation. *IEEE Transactions on Automatic Control*, 27(3):650–655, 6 1982.

[74] S. Boyd, A. Gosh, B. Prabhakar, and D. Shah. Gossip algorithms: Design, analysis and applications. In *Proceedings of IEEE INFOCOM 2005*, volume 3, pages 1653–1664, Miami, mar 2005. IEEE.

[75] Stephen Boyd, Persi Diaconis, and Lin Xiao. Fastest mixing markov chain on a graph. *SIAM review*, 46(4):667–689, 2004.

[76] Stephen Boyd, Arpita Ghosh, Balaji Prabhakar, and Devavrat Shah. Randomized gossip algorithms. *IEEE Transactions on Information Theory*, 52(6):2508–2530, 2006.

[77] Michael J Braunscheidel and Nallan C Suresh. The organizational antecedents of a firm's supply chain agility for risk mitigation and response. *Journal of operations Management*, 27(2):119–140, 2009.

[78] Philip Brookins and Jason Matthew DeBacker. Playing games with gpt:

What can we learn about a large language model from canonical strategic games? *Available at SSRN 4493398*, 2023.

[79] Francesco Bullo, Jorge Cortés, and Sonia Martinez. *Distributed control of robotic networks: a mathematical approach to motion coordination algorithms*, volume 27. Princeton University Press, 2009.

[80] US Census Bureau. 2020 census results. 2021.

[81] Ricardo J Caballero and Alp Simsek. Fire sales in a model of complexity. *The Journal of Finance*, 68(6):2549–2587, 2013.

[82] Bryan Cai, Constantinos Daskalakis, and Gautam Kamath. Priv'it: Private and sample efficient identity testing. In *International Conference on Machine Learning*, pages 635–644. PMLR, 2017.

[83] Giuseppe Calafiore, Giulia Fracastoro, and Anton V Proskurnikov. Control of dynamic financial networks. *IEEE Control Systems Letters*, 2022.

[84] Thomas B Campbell, Laura M Smeaton, N Kumarasamy, Timothy Flanigan, Karin L Klingman, Cynthia Firnhaber, Beatriz Grinsztejn, Mina C Hosseinipour, Johnstone Kumwenda, Umesh Lalloo, et al. Efficacy and safety of three antiretroviral regimens for initial treatment of hiv-1: a randomized clinical trial in diverse multinational settings. *PLoS One*, 2012.

[85] Clément L Canonne, Gautam Kamath, Audra McMillan, Adam Smith, and Jonathan Ullman. The structure of optimal private tests for simple hypotheses. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 310–321, 2019.

[86] Agostino Capponi and Peng-Chu Chen. Systemic risk mitigation in financial networks. *Journal of Economic Dynamics and Control*, 58:152–166, 2015.

[87] Adrian Rivera Cardoso and Ryan Rogers. Differentially private histograms under continual observation: Streaming selection into the unknown. In *International Conference on Artificial Intelligence and Statistics*, pages 2397–2419. PMLR, 2022.

[88] Vasco M Carvalho and Alireza Tahbaz-Salehi. Production networks: A primer. *Annual Review of Economics*, 11:635–663, 2019.

[89] George Casella and Roger L Berger. *Statistical inference*, volume 2. Duxbury Pacific Grove, CA, 2002.

[90] Damon Centola, Joshua Becker, Devon Brackbill, and Andrea Baronchelli. Experimental evidence for tipping points in social convention. *Science*, 360(6393):1116–1119, 2018.

[91] Apostolos Chalkis, Vissarion Fisikopoulos, Marios Papachristou, and Elias Tsigaridas. Truncated log-concave sampling with reflective hamiltonian monte carlo. *ACM Transactions on Mathematical Software*, 2023.

[92] Apostolos Chalkis, Vissarion Fisikopoulos, Marios Papachristou, and Elias Tsigaridas. volesti: A c++ library for sampling and volume computation on convex bodies. *Journal of Open Source Software*, 10(108):7886, 2025.

[93] J-F Chamberland and Venugopal V Veeravalli. Decentralized detection in sensor networks. *IEEE Transactions on Signal Processing*, 51(2):407–416, 2003.

[94] Sourav Chatterjee. Spectral gap of nonreversible markov chains. *arXiv preprint arXiv:2310.10876*, 2023.

[95] Bernard Chazelle. The total s-energy of a multiagent system. *SIAM Journal on Control and Optimization*, 49(4):1680–1706, 2011.

[96] Chen Chen, Garud Iyengar, and Ciamac C Moallemi. An axiomatic approach to systemic risk. *Management Science*, 59(6):1373–1388, 2013.

[97] Hong Chen, Tan Wang, and David D Yao. Financial network and systemic risk a dynamic model. Technical report, working paper, 2016.

[98] Kedong Chen, Ankur Mani, Kevin W Linderman, and Bing Wang. Where to invest in resilience in a facility network? *SSRN*, 2023.

[99] Wei Chen, Chi Wang, and Yajun Wang. Scalable influence maximization for prevalent viral marketing in large-scale social networks. In *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 1029–1038, 2010.

[100] Yi-Cheng Chen, Ping-En Lu, Cheng-Shang Chang, and Tzu-Hsuan Liu. A time-dependent sir model for covid-19 with undetectable infected per-

sons. *IEEE Transactions on Network Science and Engineering*, 7(4):3279–3294, 2020.

[101] Yiting Chen, Tracy Xiao Liu, You Shan, and Songfa Zhong. The emergence of economic rationality of gpt. *arXiv preprint arXiv:2305.12763*, 120(51):e2316205120, 2023.

[102] Robert Chew, John Bollenbacher, Michael Wenger, Jessica Speer, and Annice Kim. Llm-assisted content analysis: Using large language models to support deductive coding. *arXiv preprint arXiv:2306.14924*, 2023.

[103] Carsten Chong and Claudia Kluppelberg. Contagion in financial systems: A bayesian network approach. *SIAM Journal on Financial Mathematics*, 9(1):28–53, 2018.

[104] Felix Chopra and Ingar Haaland. Conducting qualitative interviews with ai. *CESifo Working Paper*, 2023.

[105] Fan Chung and Linyuan Lu. The diameter of sparse random graphs. *Advances in Applied Mathematics*, 26(4):257–279, 2001.

[106] Fan Chung and Linyuan Lu. The average distance in a random graph with given expected degrees. *Internet Mathematics*, 1(1):91–113, 2004.

[107] Aaron Clauset, Samuel Arbesman, and Daniel B Larremore. Systematic inequality and hierarchy in faculty hiring networks. *Science advances*, 1(1):e1400005, 2015.

[108] Aaron Clauset, Mark EJ Newman, and Cristopher Moore. Finding community structure in very large networks. *Physical review E*, 70(6):066111, 2004.

[109] Aaron Clauset, Cosma Rohilla Shalizi, and Mark EJ Newman. Power-law distributions in empirical data. *SIAM review*, 51(4):661–703, 2009.

[110] Robert T Clemen and Robert L Winkler. Combining probability distributions from experts in risk analysis. *Risk analysis*, 19:187–203, 1999.

[111] Vittoria Colizza, Romualdo Pastor-Satorras, and Alessandro Vespignani. Reaction–diffusion processes and metapopulation models in heterogeneous networks. *Nature Physics*, 3(4):276–282, 2007.

[112] Larissa Conradt, Christian List, and Timothy J Roper. Swarm intelligence: When uncertainty meets conflict. *The American Naturalist*, 182(5):592–610, 2013.

[113] Colin Cooper, Ralf Klasing, and Michele Zito. Lower bounds and algorithms for dominating sets in web graphs. *Internet Mathematics*, 2(3):275–300, 2005.

[114] J. Cortes, S. Martinez, and F. Bullo. Analysis and design tools for distributed motion coordination. In *Proceedings of the American Control Conference*, pages 1680–1685, Portland, OR, jun 2005.

[115] David R Cox. Regression models and life-tables. *Journal of the Royal Statistical Society: Series B (Methodological)*, 34(2):187–202, 1972.

[116] M Dahleh, Alireza Tahbaz-Salehi, John N Tsitsiklis, and Spyros I Zoumpoulis. On global games in social networks of information exchange. Technical report, Working paper, 2012.

[117] Krishna Dasaratha, Santosh Venkatesh, and Rakesh Vohra. Optimal bailouts in diversified financial networks. *arXiv preprint arXiv:2406.12818*, 2024.

[118] Giordano De Marzo, Luciano Pietronero, and David Garcia. Emergence of scale-free networks in social interactions among large language models. *arXiv preprint arXiv:2312.06619*, 2023.

[119] Wouter De Nooy, Andrej Mrvar, and Vladimir Batagelj. *Exploratory social network analysis with Pajek: Revised and expanded edition for updated software*, volume 46. Cambridge University Press, 2018.

[120] Veronique de Rugy and Gary Leff. The 2020 bailouts left airlines, the economy, and the federal budget in worse shape than before. *Special Edition Policy Brief*, 2022.

[121] M. H. DeGroot. Reaching a consensus. *Journal of American Statistical Association*, 69:118–121, 1974.

[122] Gabrielle Demange. Contagion in financial networks: a threat index. *Management Science*, 64(2):955–970, 2018.

[123] P. M. DeMarzo, D. Vayanos, and J. Zwiebel. Persuasion bias, social influence, and unidimensional opinions. *The Quarterly Journal of Economics*, 118:909–968, 2003.

[124] Matthew Desmond. *Evicted: Poverty and profit in the American city*. Crown, 2016.

[125] Emily Diana, Hadi Elzayn, Michael Kearns, Aaron Roth, Saeed Sharifi-Malvajerdi, and Juba Ziani. Differentially private call auctions and market impact. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 541–583, 2020.

[126] Franz Dietrich, Christian List, and Richard Bradley. Belief revision generalized: A joint characterization of bayes' and jeffrey's rules. *Journal of Economic Theory*, 162:352–371, 2016.

[127] A. D.G. Dimakis, A. D. Sarwate, and M. J. Wainwright. Geographic gossip: Efficient averaging for sensor networks. *Signal Processing, IEEE Transactions on*, 56(3):1205–1216, 2008.

[128] Ian Dobson, Benjamin A Carreras, and David E Newman. A branching process approximation to cascading load-dependent system failure. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, pages 10–pp. IEEE, 2004.

[129] Ian Dobson, Benjamin A Carreras, and David E Newman. A loading-dependent model of probabilistic cascading failure. *Probability in the Engineering and Informational Sciences*, 19(1):15–32, 2005.

[130] Joseph L Doob. Regularity properties of certain families of chance variables. *Transactions of the American Mathematical Society*, 47(3):455–486, 1940.

[131] Kimon Drakopoulos, Asuman Ozdaglar, and John Tsitsiklis. An efficient curing policy for epidemics on graphs. In *53rd IEEE Conference on Decision and Control*, pages 4447–4454. IEEE, 2014.

[132] Kimon Drakopoulos, Asuman Ozdaglar, and John N Tsitsiklis. When is a network epidemic hard to eliminate? *Mathematics of Operations Research*, 42(1):1–14, 2017.

[133] Cynthia Dwork. A firm foundation for private data analysis. *Communications of the ACM*, 54(1):86–95, 2011.

[134] Cynthia Dwork, Nitin Kohli, and Deirdre Mulligan. Differential privacy in practice: Expose your epsilons! *Journal of Privacy and Confidentiality*, 9(2), 2019.

[135] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

[136] Dean Eckles, Hossein Esfandiari, Elchanan Mossel, and M Amin Rahimian. Seeding with costly network information. *Operations Research*, 2022.

[137] Beni Egressy and Roger Wattenhofer. Bailouts in financial networks. *arXiv preprint arXiv:2106.12315*, 2021.

[138] Nicole Eikmeier, Arjun S Ramani, and David Gleich. The hyperkron graph model for higher-order features. In *2018 IEEE International Conference on Data Mining (ICDM)*, pages 941–946. IEEE, 2018.

[139] Larry Eisenberg and Thomas H Noe. Systemic risk in financial systems. *Management Science*, 47(2):236–249, 2001.

[140] Andrew Elliott, Angus Chiu, Marya Bazzi, Gesine Reinert, and Mihai Cucuringu. Core–periphery structure in directed networks. *Proceedings of the Royal Society A*, 476(2241):20190783, 2020.

[141] Matthew Elliott, Benjamin Golub, and Matthew O Jackson. Financial networks and contagion. *American Economic Review*, 104(10):3115–53, 2014.

[142] Matthew Elliott, Benjamin Golub, and Matthew V Leduc. Supply network formation and fragility. *American Economic Review*, 112(8):2701–47, 2022.

[143] Matthew Elliott and Matthew O Jackson. Supply chain disruptions, the structure of production networks, and the impact of globalization. *Available at SSRN*, 2023.

[144] Helmut Elsinger, Alfred Lehar, and Martin Summer. Network models and systemic risk assessment. *Handbook on Systemic Risk*, 1(1):287–305, 2013.

[145] Ozlem Ergun, Wallace J. Hopp, and Pinar Keskinocak. A structured overview of insights and opportunities for enhancing supply chain resilience. *IISE Transactions*, 55(1):57–74, 2023.

[146] U Erlingsson. Learning statistics with privacy, aided by the flip of a coin. *Google Security Blog, October*, 2014.

[147] Ulfar Erlingsson. Learning statistics with privacy, aided by the flip of a coin. https://ai.googleblog.com/2014/10/learning-statistics-with-privacy-aided.html, 2014. Accessed: 2023-05-18.

[148] Selman Erol. Network hazard and bailouts. *Available at SSRN 3034406*, 2019.

[149] Selman Erol and Rakesh Vohra. Network formation and systemic risk. *European Economic Review*, 148:104213, 2022.

[150] Bahare Fatemi, Jonathan Halcrow, and Bryan Perozzi. Talk like a graph: Encoding graphs for large language models. *arXiv preprint arXiv:2310.04560*, 2023.

[151] Uriel Feige. A threshold of ln n for approximating set cover. *Journal of the ACM (JACM)*, 45(4):634–652, 1998.

[152] Zachary Feinstein. Obligations with physical delivery in a multilayered financial network. *SIAM Journal on Financial Mathematics*, 10(4):877–906, 2019.

[153] Zachary Feinstein, Weijie Pang, Birgit Rudloff, Eric Schaanning, Stephan Sturm, and Mackenzie Wildman. Sensitivity of the eisenberg–noe clearing vector to individual interbank liabilities. *SIAM Journal on Financial Mathematics*, 9(4):1286–1325, 2018.

[154] Zachary Feinstein, Birgit Rudloff, and Stefan Weber. Measures of systemic risk. *SIAM Journal on Financial Mathematics*, 8(1):672–708, 2017.

[155] Zachary Feinstein and Andreas Sojmark. A dynamic default contagion model: From eisenberg-noe to the mean field. *arXiv preprint arXiv:1912.08695*, 2019.

[156] Joseph Ficek, Wei Wang, Henian Chen, Getachew Dagne, and Ellen Daley. Differential privacy in health research: A scoping review. *Journal of the American Medical Informatics Association*, 28(10):2269–2276, 2021.

[157] James H Fowler and Nicholas A Christakis. Dynamic spread of happi-

ness in a large social network: longitudinal analysis over 20 years in the framingham heart study. *Bmj*, 337, 2008.

[158] Linton C Freeman. A set of measures of centrality based on betweenness. *Sociometry*, pages 35–41, 1977.

[159] Daniel Freund, Shane G Henderson, and David B Shmoys. Minimizing multimodular functions and allocating capacity in bike-sharing systems. In *International Conference on Integer Programming and Combinatorial Optimization*, pages 186–198. Springer, 2017.

[160] Yoav Freund and Robert E Schapire. A decision-theoretic generalization of on-line learning and an application to boosting. *Journal of computer and system sciences*, 55(1):119–139, 1997.

[161] Tom Friedetzky, David C Kutner, George B Mertzios, Iain A Stewart, and Amitabh Trehan. Payment scheduling in the interval debt model. In *International Conference on Current Trends in Theory and Practice of Computer Science*, pages 267–282. Springer, 2023.

[162] Noah E Friedkin and Eugene C Johnsen. Social influence and opinions. *Journal of Mathematical Sociology*, 15(3-4):193–206, 1990.

[163] David Froelicher, Juan R Troncoso-Pastoriza, Jean Louis Raisaro, Michel A Cuendet, Joao Sa Sousa, Hyunghoon Cho, Bonnie Berger, Jacques Fellay, and Jean-Pierre Hubaux. Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption. *Nature communications*, 12(1):5910, 2021.

[164] Xavier Gabaix. The granular origins of aggregate fluctuations. *Econometrica*, 79(3):733–772, 2011.

[165] Axel Gandy and Luitgard AM Veraart. A bayesian methodology for systemic risk assessment in financial networks. *Management Science*, 63(12):4428–4446, 2017.

[166] Chen Gao, Xiaochong Lan, Zhihong Lu, Jinzhu Mao, Jinghua Piao, Huandong Wang, Depeng Jin, and Yong Li. S3: Social-network simulation system with large language model-empowered agents. *arXiv preprint arXiv:2307.14984*, 2023.

[167] Sarah Yini Gao, David Simchi-Levi, Chung-Piaw Teo, and Zhenzhen Yan.

Disruption risk mitigation in supply chains: The risk exposure index revisited. *Operations Research*, 67(3):831–852, 2019.

[168] Michael R Garey and David S Johnson. Computers and intractability. *A Guide to the*, 1979.

[169] Simson Garfinkel. Differential privacy and the 2020 US census. Technical report, MIT Schwarzman College of Computing, 2022.

[170] Paul H Garthwaite, Joseph B Kadane, and Anthony O'Hagan. Statistical methods for eliciting probability distributions. *Journal of the American Statistical Association*, 100(470):680–701, 2005.

[171] J. D. Geanakoplos and H. M. Polemarchakis. We can't disagree forever. *Journal of Economic Theory*, 28(1):192–200, 1982.

[172] Martin Geissdoerfer, Paulo Savaget, Nancy MP Bocken, and Erik Jan Hultink. The circular economy–a new sustainability paradigm? *Journal of Cleaner Production*, 143:757–768, 2017.

[173] Andrew Gelman, Daniel Lee, and Jiqiang Guo. Stan: A probabilistic programming language for bayesian inference and optimization. *Journal of Educational and Behavioral Statistics*, 40(5):530–543, 2015.

[174] Christian Genest, Samaradasa Weerahandi, and James V Zidek. Aggregating opinions through logarithmic pooling. *Theory and Decision*, 17(1):61–70, 1984.

[175] Christian Genest and James V Zidek. Combining probability distributions: A critique and an annotated bibliography. *Statistical Science*, pages 114–135, 1986.

[176] Ravit Geva, Alexander Gusev, Yuriy Polyakov, Lior Liram, Oded Rosolio, Andreea Alexandru, Nicholas Genise, Marcelo Blatt, Zohar Duchin, Barliz Waissengrin, et al. Collaborative privacy-preserving analysis of oncological data using multiparty homomorphic encryption. *Proceedings of the National Academy of Sciences*, 120(33):e2304415120, 2023.

[177] G. L. Gilardoni and M. K. Clayton. On reaching a consensus using DeGroot's iterative pooling. *The Annals of Statistics*, pages 391–401, 1993.

[178] Corrado Gini. Measurement of inequality of incomes. *The Economic Journal*, 31(121):124–126, 1921.

[179] Paul Glasserman and H Peyton Young. How likely is contagion in financial networks? *Journal of Banking & Finance*, 50:383–399, 2015.

[180] Paul Glasserman and H Peyton Young. Contagion in financial networks. *Journal of Economic Literature*, 54(3):779–831, 2016.

[181] Olivier Goldschmidt, Patrick Jaillet, and Richard Lasota. On reliability of graphs with node failures. *Networks*, 24(4):251–259, 1994.

[182] B. Golub and M. O. Jackson. Naïve Learning in Social Networks and the Wisdom of Crowds. *American Economic Journal: Microeconomics*, 2(1):112–149, feb 2010.

[183] Benjamin Golub and Matthew O. Jackson. How homophily affects the speed of learning and best-response dynamics. *The Quarterly Journal of Economics*, 127(3):1287–1338, 2012.

[184] Georgios Gousios. The ghtorrent dataset and tool suite. In *Proceedings of the 10th Working Conference on Mining Software Repositories*, MSR '13, pages 233–236, Piscataway, NJ, USA, 2013. IEEE Press.

[185] Georgios Gousios and Diomidis Spinellis. Ghtorrent: Github's data from a firehose. In *2012 9th IEEE Working Conference on Mining Software Repositories (MSR)*, pages 12–21. IEEE, 2012.

[186] M Gowtham and S Sobitha Ahila. Privacy enhanced data communication protocol for wireless body area network. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 1–5. IEEE, 2017.

[187] Amit Goyal, Wei Lu, and Laks VS Lakshmanan. Celf++ optimizing the greedy algorithm for influence maximization in social networks. In *Proceedings of the 20th international conference companion on World wide web*, pages 47–48, 2011.

[188] Mark S Granovetter. The strength of weak ties. *American journal of sociology*, 78(6):1360–1380, 1973.

[189] Dabo Guan, Daoping Wang, Stephane Hallegatte, Steven J Davis, Jingwen Huo, Shuping Li, Yangchun Bai, Tianyang Lei, Qianyu Xue, D'Maris Coffman, et al. Global supply-chain effects of covid-19 control measures. *Nature Human Behaviour*, 4(6):577–587, 2020.

[190] Miguel Guevara. Enabling developers and organizations to use differential privacy. https://developers.googleblog.com/2019/09/enabling-developers-and-organizations.html, 2019. Accessed: 2023-05-18.

[191] Haresh Gurnani, Anuj Mehrotra, and Saibal Ray. *Supply chain disruptions: Theory and practice of managing risk*. Springer, 2012.

[192] Aric Hagberg, Pieter Swart, and Daniel S Chult. Exploring network structure, dynamics, and function using networkx. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States), 2008.

[193] Stéphane Hallegatte. An adaptive regional input-output model and its application to the assessment of the economic cost of katrina. *Risk Analysis: An International Journal*, 28(3):779–799, 2008.

[194] Becky Ham. Companies use mit research to identify and respond to supply chain risks. https://news.mit.edu/2022/companies-use-mit-research-identify-respond-supply-chain-risks-0615, 2022.

[195] Scott M Hammer, David A Katzenstein, Michael D Hughes, Holly Gundacker, Robert T Schooley, Richard H Haubrich, W Keith Henry, Michael M Lederman, John P Phair, Manette Niu, et al. A trial comparing nucleoside monotherapy with combination therapy in hiv-infected adults with cd4 cell counts from 200 to 500 per cubic millimeter. *New England Journal of Medicine*, 335(15):1081–1090, 1996.

[196] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. Differential privacy techniques for cyber physical systems: a survey. *IEEE Communications Surveys & Tutorials*, 22(1):746–789, 2019.

[197] Y. Hatano and M. Mesbahi. Agreement over random networks. *IEEE Transactions on Automatic Control*, 50(11):1867–1872, 2005.

[198] Jan Hązła, Ali Jadbabaie, Elchanan Mossel, and M Amin Rahimian. Bayesian decision making in groups is hard. *Operations Research*, 69(2):632–654, 2021.

[199] James He, Felix Wallis, and Steve Rathje. Homophily in an artificial social network of agents powered by large language models. *OSF*, 2023.

[200] R. Hegselmann and U. Krause. Opinion dynamics and bounded confidence models, analysis and simulation. *Journal of Societies and Social Simulation*, 5(3), 2002.

[201] Martin Hoefer, Carmine Ventre, and Lisa Wilhelmi. Algorithms for claims trading. *arXiv preprint arXiv:2402.13627*, 2024.

[202] Matthew D Hoffman, Andrew Gelman, et al. The no-u-turn sampler: adaptively setting path lengths in hamiltonian monte carlo. *J. Mach. Learn. Res.*, 15(1):1593–1623, 2014.

[203] Jessica Hoffmann, Matt Jordan, and Constantine Caramanis. Quarantines as a targeted immunization strategy. *arXiv preprint arXiv:2008.08262*, 2020.

[204] James Honaker, Gary King, and Matthew Blackwell. Amelia ii: A program for missing data. *Journal of statistical software*, 45(1):1–47, 2011.

[205] John J Horton. Large language models as simulated economic agents: What can we learn from homo silicus? Technical report, National Bureau of Economic Research, 2023.

[206] Michael Horvath. Cyclicality and sectoral linkages: Aggregate fluctuations from independent sectoral shocks. *Review of Economic Dynamics*, 1(4):781–808, 1998.

[207] John D Hunter. Matplotlib: A 2d graphics environment. *IEEE Annals of the History of Computing*, 9(03):90–95, 2007.

[208] Hiroyasu Inoue and Yasuyuki Todo. The propagation of economic impacts through supply chains: The case of a mega-city lockdown to prevent the spread of covid-19. *PloS one*, 15(9):e0239251, 2020.

[209] M. O. Jackson. *Social and Economic Networks*. Princeton University Press, Princeton, NJ, 2008.

[210] Matthew O Jackson et al. *Social and economic networks*, volume 3. Princeton university press Princeton, 2008.

[211] Matthew O Jackson and Agathe Pernoud. Optimal regulation and investment incentives in financial networks. *Available at SSRN 3311839*, 2019.

[212] Matthew O Jackson and Agathe Pernoud. What makes financial networks special? distorted investment incentives, regulation, and systemic risk measurement. *Distorted Investment Incentives, Regulation, and Systemic Risk Measurement (March 1, 2019)*, 2019.

[213] Matthew O Jackson and Agathe Pernoud. Credit freezes, equilibrium multiplicity, and optimal bailouts in financial networks. *SSRN*, 2020.

[214] Matthew O Jackson and Agathe Pernoud. Systemic risk in financial networks: A survey. *Annual Review of Economics*, 13:171–202, 2021.

[215] Abigail Z Jacobs and Duncan J Watts. A large-scale comparative study of informal social networks in firms. *Management Science*, 67(9):5489–5509, 2021.

[216] A. Jadbabaie, J. Lin, and A. S. Morse. Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*, 48(6):988–1001, 2003.

[217] A. Jadbabaie, P. Molavi, A. Sandroni, and A. Tahbaz-Salehi. Non-bayesian social learning. *Games and Economic Behavior*, 76(1):210–225, 2012.

[218] Eaman Jahani, Samuel P Fraiberger, Michael Bailey, and Dean Eckles. Long ties, disruptive life events, and economic prosperity. *Proceedings of the National Academy of Sciences*, 120(28):e2211062120, 2023.

[219] Akhil Jalan and Deepayan Chakrabarti. Strategic negotiations in endogenous network formation. *arXiv preprint arXiv:2402.08779*, 2024.

[220] Akhil Jalan, Deepayan Chakrabarti, and Purnamrita Sarkar. Incentive-aware models of dynamic financial networks. *preprint arXiv:2212.06808*, 2022.

[221] Akhil Jalan and Marios Papachristou. Opinion dynamics with multiple adversaries. *arXiv preprint arXiv:2502.15931*, 2025.

[222] Junteng Jia and Austin R Benson. Random spatial network models for core-periphery structure. In *Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining*, pages 366–374, 2019.

[223] Zach Jorgensen, Ting Yu, and Graham Cormode. Conservative or Liberal? personalized Differential Privacy. In *IEEE International Conference on Data Engineering (ICDE 2015)*, pages 1023–1034. IEEE, 2015.

[224] Marcus Kaiser and Claus C. Hilgetag. Nonoptimal component placement, but short processing paths, due to long-distance projections in neural systems. *PLoS Computational Biology*, 2(7):e95, 2006.

[225] Georgios A Kaissis, Marcus R Makowski, Daniel Rückert, and Rickmer F Braren. Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence*, 2(6):305–311, 2020.

[226] Panagiotis Kanellopoulos, Maria Kyropoulou, and Hao Zhou. Forgiving debt in financial network games. *arXiv preprint arXiv:2202.10986*, 2022.

[227] Justin Kang, Ramtin Pedarsani, and Kannan Ramchandran. The fair value of data under heterogeneous privacy constraints. *arXiv preprint arXiv:2301.13336*, 2023.

[228] Edward L Kaplan and Paul Meier. Nonparametric estimation from incomplete observations. *Journal of the American statistical association*, 53(282):457–481, 1958.

[229] S. Kar, J.M.F. Moura, and K. Ramanan. Distributed parameter estimation in sensor networks: Nonlinear observation models and imperfect communication. *IEEE Transactions on Information Theory*, 58, no. 6, pp. 3575–3605, 2012.

[230] Richard M Karp. On the computational complexity of combinatorial problems. *Networks*, 5(1):45–68, 1975.

[231] Leo Katz. A new status index derived from sociometric analysis. *Psychometrika*, 18(1):39–43, 1953.

[232] Mert Kayaalp, Yunus Inan, Emre Telatar, and Ali H Sayed. On the arithmetic and geometric fusion of beliefs for distributed inference. *IEEE Transactions on Automatic Control*, 69(4):2265–2280, 2023.

[233] Zeki Kazan, Kaiyan Shi, Adam Groce, and Andrew P Bray. The test of tests: A framework for differentially private hypothesis testing. In *International Conference on Machine Learning*, pages 16131–16151. PMLR, 2023.

[234] Michael Kearns, Mallesh Pai, Aaron Roth, and Jonathan Ullman. Mechanism design in large games: Incentives and privacy. In *Proceedings of the 5th conference on Innovations in theoretical computer science*, pages 403–410, 2014.

[235] Frank Kelly and Elena Yudovina. *Stochastic networks*, volume 2. Cambridge University Press, 2014.

[236] David Kempe, Jon Kleinberg, and Éva Tardos. Maximizing the spread of influence through a social network. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 137–146, 2003.

[237] Hichem Kenniche and Vlady Ravelomananana. Random geometric graphs as model of wireless sensor networks. In *2010 The 2nd international conference on computer and automation engineering (ICCAE)*, volume 4, pages 103–107. IEEE, IEEE, 2010.

[238] Aein Khabazian and Jiming Peng. Vulnerability analysis of the financial network. *Management Science*, 65(7):3302–3321, 2019.

[239] Ariah Klages-Mundt and Andreea Minca. Optimal intervention in economic networks using influence maximization methods. *European Journal of Operational Research*, 300(3):1136–1148, 2022.

[240] Jon Kleinberg. The small-world phenomenon: An algorithmic perspective. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 163–170, 2000.

[241] Jon M Kleinberg. Small-world phenomena and the dynamics of information. In *Advances in neural information processing systems*, pages 431–438, 2002.

[242] Paul R Kleindorfer and Germaine H Saad. Managing disruption risks in supply chains. *Production and Operations Management*, 14(1):53–68, 2005.

[243] Yoav Kolumbus and Noam Nisan. How and why to manipulate your own agent: On the incentives of users of learning agents. *Advances in Neural Information Processing Systems*, 35:28080–28094, 2022.

[244] Raed Kontar, Naichen Shi, Xubo Yue, Seokhyun Chung, Eunshin Byon, Mosharaf Chowdhury, Jionghua Jin, Wissam Kontar, Neda Masoud, Ma-

her Nouiehed, et al. The internet of federated things (IoFT). *IEEE Access*, 9:156071–156113, 2021.

[245] Vasilis Kostakis and Marios Papachristou. Commons-based peer production and digital fabrication: The case of a reprap-based, lego-built 3d printing-milling machine. *Telematics and Informatics*, 31(3):434–443, 2014.

[246] Hadas Kotek, Rikker Dockum, and David Sun. Gender bias and stereotypes in large language models. In *Proceedings of The ACM Collective Intelligence Conference*, pages 12–24, 2023.

[247] Fragkiskos Koufogiannis, Shuo Han, and George J Pappas. Optimality of the laplace mechanism in differential privacy. *arXiv preprint arXiv:1504.00065*, 2015.

[248] Fragkiskos Koufogiannis and George J Pappas. Diffusing private data over networks. *IEEE Transactions on Control of Network Systems*, 5(3):1027–1037, 2017.

[249] V. Krishnamurthy and H. V. Poor. Social learning and bayesian games in multiagent signal processing: How do local and global decision makers interact? *IEEE Signal Processing Magazine,*, 30(3):43–57, 2013.

[250] Eduard Kromer, Ludger Overbeck, and Katrin Zilch. Systemic risk measures on general measurable spaces. *Mathematical Methods of Operations Research*, 84:323–357, 2016.

[251] Paul Krugman. Increasing returns and economic geography. *Journal of political economy*, 99(3):483–499, 1991.

[252] Ravi Kumar, Jasmine Novak, Bo Pang, and Andrew Tomkins. On anonymizing query logs via token-based hashing. In *Proceedings of the 16th international conference on World Wide Web*, pages 629–638, 2007.

[253] Michael Kusnetsov and Luitgard Anna Maria Veraart. Interbank clearing in financial networks with multiple maturities. *SIAM Journal on Financial Mathematics*, 10(1):37–67, 2019.

[254] A. Lalitha, A. Sarwate, and T. Javidi. Social learning and distributed hypothesis testing. *IEEE International Symposium on Information Theory*, pages 551–555, 2014.

[255] Anusha Lalitha, Tara Javidi, and Anand D Sarwate. Social learning and distributed hypothesis testing. *IEEE Transactions on Information Theory*, 64(9):6161–6179, 2018.

[256] Tian Lan and Mung Chiang. An axiomatic theory of fairness in resource allocation. *George Washington University, http://www. seas. gwu. edu/tlan/papers/fairness. pdf, Tech. Rep*, 2011.

[257] Tian Lan, David Kao, Mung Chiang, and Ashutosh Sabharwal. *An axiomatic theory of fairness in network resource allocation*. IEEE, 2010.

[258] Eun Lee, Aaron Clauset, and Daniel B Larremore. The dynamics of faculty hiring networks. *arXiv preprint arXiv:2105.02949*, 2021.

[259] Keith Lehrer and Carl Wagner. *Rational Consensus in Science and Society, A Philosophical and Mathematical Study*. D. Reidel Publishing Company, Dordrecht, Holland, 1981.

[260] Yan Leng, Tara Sowrirajan, Yujia Zhai, and Alex Pentland. Interpretable stochastic block influence model: measuring social influence among homophilous communities. *IEEE Transactions on Knowledge and Data Engineering*, 2023.

[261] Jure Leskovec, Lada A Adamic, and Bernardo A Huberman. The dynamics of viral marketing. *ACM Transactions on the Web (TWEB)*, 1(1):5–es, 2007.

[262] Jure Leskovec, Deepayan Chakrabarti, Jon Kleinberg, Christos Faloutsos, and Zoubin Ghahramani. Kronecker graphs: an approach to modeling networks. *Journal of Machine Learning Research*, 11(2), 2010.

[263] Jure Leskovec, Jon Kleinberg, and Christos Faloutsos. Graph evolution: Densification and shrinking diameters. *ACM Transactions on Knowledge Discovery from Data*, 1(1):2–es, 2007.

[264] Jure Leskovec, Andreas Krause, Carlos Guestrin, Christos Faloutsos, Jeanne VanBriesen, and Natalie Glance. Cost-effective outbreak detection in networks. In *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 420–429, 2007.

[265] Jure Leskovec, Mary McGlohon, Christos Faloutsos, Natalie Glance, and Matthew Hurst. Patterns of cascading behavior in large blog graphs. In

Proceedings of the 2007 SIAM international conference on data mining, pages 551–556. SIAM, 2007.

[266] D. A. Levin, Y. Peres, and E. L. Wilmer. *Markov Chains and Mixing Times*. American Mathematical Society, 2009.

[267] Chencheng Li, Pan Zhou, Li Xiong, Qian Wang, and Ting Wang. Differentially private distributed online learning. *IEEE Transactions on Knowledge and Data Engineering*, 30(8):1440–1453, 2018.

[268] Ming Li, Wenjing Lou, and Kui Ren. Data security and privacy in wireless body area networks. *IEEE Wireless communications*, 17(1):51–58, 2010.

[269] Jack Liell-Cock, Ian R Manchester, and Guodong Shi. Preserving privacy of the influence structure in Friedkin-Johnsen systems. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 6254–6259. IEEE, 2020.

[270] Christian List and Clemens Puppe. Judgment aggregation: A survey. *Handbook of Rational and Social Choice*, 2009.

[271] Dong C Liu and Jorge Nocedal. On the limited memory bfgs method for large scale optimization. *Mathematical programming*, 45(1):503–528, 1989.

[272] Ming Liu and Jeremy Staum. Sensitivity analysis of the eisenberg–noe model of contagion. *Operations Research Letters*, 38(5):489–491, 2010.

[273] Yuxin Liu and M Amin Rahimian. Differentially private sequential learning. *arXiv preprint arXiv:2502.19525*, 2025.

[274] John B Long Jr and Charles I Plosser. Real business cycles. *Journal of political Economy*, 91(1):39–69, 1983.

[275] Robert E Lucas et al. Understanding business cycles. *Essential readings in economics*, pages 306–327, 1995.

[276] Ding Lyu, Yuan Yuan, Lin Wang, Xiaofan Wang, and Alex Pentland. Investigating and modeling the dynamics of long ties. *Communications Physics*, 5(1):87, 2022.

[277] Benjamin S Manning, Kehang Zhu, and John J Horton. Automated social science: A structural causal model-based approach. *SSRN*, 2024.

[278] Jason R Marden and Jeff S Shamma. Revisiting log-linear learning: Asynchrony, completeness and payoff-based implementation. *Games and Economic Behavior*, 75(2):788–808, 2012.

[279] Daniel McFadden. Conditional logit analysis of qualitative choice behavior. *Working Paper*, 1972.

[280] Wes McKinney et al. pandas: a foundational python library for data analysis and statistics. *Python for High Performance and Scientific Computing*, 14(9):1–9, 2011.

[281] Samuel McLaughlin, Vikram Krishnamurthy, and Subhash Challa. Managing data incest in a distributed sensor network. In *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'03)*, volume 5, pages V–269. IEEE, 2003.

[282] Brendan McMahan and Abhradeep Thakurta. Federated learning with formal differential privacy guarantees. *Google AI Blog*, 2022. Accessed: 2024-03-26.

[283] Miller McPherson, Lynn Smith-Lovin, and James M Cook. Birds of a feather: Homophily in social networks. *Annual review of sociology*, 27(1):415–444, 2001.

[284] Filippo Menczer. Growing and navigating the small world web by local content. *Proceedings of the National Academy of Sciences*, 99(22):14014–14019, 2002.

[285] M. Mesbahi and M. Egerstedt. *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press, 2010.

[286] Filip Milojkovic. Gem house opendata: German electricity consumption in many households over three years 2018–2020 (fresh energy), 2018.

[287] Pooya Molavi, Alireza Tahbaz-Salehi, and Ali Jadbabaie. A theory of non-bayesian social learning. *Econometrica*, 86(2):445–490, 2018.

[288] F Molnár, Sameet Sreenivasan, Boleslaw K Szymanski, and Gyorgy Korniss. Minimum dominating sets in scale-free network ensembles. *Scientific reports*, 3(1):1–10, 2013.

[289] L. Moreau. Stability of multiagent systems with time-dependent communication links. *IEEE Transactions on Automatic Control*, 50(2):169–182, 2005.

[290] Mohsen Mosleh, Dean Eckles, and David Gertler Rand. Tendencies toward triadic closure: Field-experimental evidence. Technical report, Center for Open Science, 2024.

[291] Elchanan Mossel and Sebastien Roch. On the submodularity of influence in social networks. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 128–134, 2007.

[292] Nuno Mota, Negar Mohammadi, Palash Dey, Krishna P Gummadi, and Abhijnan Chakraborty. Fair partitioning of public resources: Redrawing district boundary to minimize spatial inequality in school funding. 2021.

[293] Kundan Munjal and Rekha Bhatia. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, 9(4):3759–3786, 2023.

[294] Jose C Nacher and Tatsuya Akutsu. Dominating scale-free networks with variable scaling exponent: heterogeneous networks are not difficult to control. *New Journal of Physics*, 14(7):073005, 2012.

[295] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 111–125, 2008.

[296] National Academies of Sciences, Engineering, and Medicine. Net metering practices should be revised to better reflect the value of integrating distributed electricity generation into the nation's power grid. https://www.nationalacademies.org/news/2023/05/net-metering-practices-should-be-revised-to-better-reflect-the-value-of-integrating-distributed-electricity-generation-into-the-nations-power-grid, 2023. Accessed: 2023-05-20.

[297] National Academies of Sciences, Engineering, and Medicine. The role of net metering in the evolving electricity system. https://www.nationalacademies.org/our-work/the-role-of-net-metering-in-the-evolving-electricity-system, 2023. Accessed: 2023-05-20.

[298] National Institute of Allergy and Infectious Diseases. A randomized, double-blind phase ii/iii trial of monotherapy vs. combination therapy

with nucleoside analogs in hiv-infected persons with cd4 cells of 200-500/mm3. https://clinicaltrials.gov/study/NCT00000625, 1995. Accessed: 2024-12-13.

[299] Angelia Nedić, Alex Olshevsky, and César A Uribe. Fast convergence rates for distributed non-bayesian learning. *arXiv preprint arXiv:1508.05161*, 62(11):5538–5553, 2015.

[300] Angelia Nedić, Alex Olshevsky, and César A Uribe. Nonasymptotic Convergence Rates for Cooperative Learning over Time-varying Directed Graphs. In *American Control Conference (ACC 2015)*, pages 5884–5889. IEEE, 2015.

[301] Roger J Nemeth and David A Smith. International trade and world-system structure: A multiple network analysis. *Review (Fernand Braudel Center)*, 8(4):517–560, 1985.

[302] George L Nemhauser and Laurence A Wolsey. Best algorithms for approximating the maximum of a submodular set function. *Mathematics of operations research*, 3(3):177–188, 1978.

[303] George L Nemhauser, Laurence A Wolsey, and Marshall L Fisher. An analysis of approximations for maximizing submodular set functions—i. *Mathematical programming*, 14(1):265–294, 1978.

[304] Tommaso Nesti, Fiona Sloothaak, and Bert Zwart. Emergence of scale-free blackout sizes in power grids. *Physical Review Letters*, 125(5):058301, 2020.

[305] Mark EJ Newman. Mixing patterns in networks. *Physical review E*, 67(2):026126, 2003.

[306] Mark EJ Newman. Modularity and community structure in networks. *Proceedings of the national academy of sciences*, 103(23):8577–8582, 2006.

[307] Mark EJ Newman and Michelle Girvan. Finding and evaluating community structure in networks. *Physical review E*, 69(2):026113, 2004.

[308] Solmaz Niknam, Harpreet S Dhillon, and Jeffrey H Reed. Federated learning for wireless communications: Motivation, opportunities, and challenges. *IEEE Communications Magazine*, 58(6):46–51, 2020.

[309] Helen Nissenbaum. Privacy in context. In *Privacy in Context*. Stanford University Press, 2009.

[310] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 75–84, 2007.

[311] R. Olfati-Saber and J. Shamma. Consensus filters for sensor networks and distributed sensor fusion. *IEEE Conference on Decision and Control*, pages 6698 – 6703, 2005.

[312] Alex Olshevsky. Linear time average consensus on fixed graphs and implications for decentralized optimization and multi-agent control. *arXiv preprint arXiv:1411.4186*, 2014.

[313] Alex Olshevsky. Linear time average consensus and distributed optimization on fixed graphs. *SIAM Journal on Control and Optimization*, 55(6):3990–4014, 2017.

[314] OpenAI. Gpt-4 technical report. *arXiv*, pages 2303–08774, 2023.

[315] Jan Overgoor, Austin Benson, and Johan Ugander. Choosing to grow a graph: Modeling network formation as discrete choice. In *The World Wide Web Conference*, pages 1409–1420, 2019.

[316] Lawrence Page, Sergey Brin, Rajeev Motwani, and Terry Winograd. The pagerank citation ranking: Bringing order to the web. Technical report, Stanford InfoLab, 1999.

[317] Marios Papachristou. Software clusterings with vector semantics and the call graph. In *Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 1184–1186, 2019.

[318] Marios Papachristou. Sublinear domination and core–periphery networks. *Scientific Reports*, 11(1):1–16, 2021.

[319] Marios Papachristou. Supplementary Source Code. https://colab.research.google.com/drive/1xb8cT_1Y9hcJP04VaZpUAQIjaJEOi80W#scrollTo=yJlGboymTLfA&uniqifier=2, Jun v. 1.0, 2021.

[320] Marios Papachristou, Siddhartha Banerjee, and Jon Kleinberg. Dynamic

interventions for networked contagions. In *Proceedings of the Web Conference 2023*, 2023.

[321] Marios Papachristou, Siddhartha Banerjee, and Jon Kleinberg. Optimally allocating resources to remediate networked contagions. *Working Paper*, 2023.

[322] Marios Papachristou and Jon Kleinberg. Allocating stimulus checks in times of crisis. In *Proceedings of the Web Conference 2022*, 2022.

[323] Marios Papachristou and Jon Kleinberg. Core-periphery models for hypergraphs. In *KDD*, 2022.

[324] Marios Papachristou and M Amin Rahimian. Production networks resilience: Cascading failures, power laws and optimal interventions. *arXiv preprint arXiv:2303.12660*, 2023.

[325] Marios Papachristou and M Amin Rahimian. Differentially private distributed estimation and learning. *IISE Transactions*, (just-accepted):1–26, 2024.

[326] Marios Papachristou and M Amin Rahimian. Differentially private distributed inference. *Working paper*, 2024.

[327] Marios Papachristou, Longqi Yang, and Chin-Chia Hsu. Leveraging large language models for collective decision-making. *ACM Conference on Computer-Supported Cooperative Work (CSCW) 2025 (to appear).*, 2025.

[328] Marios Papachristou and Yuan Yuan. Network formation and dynamics among multi-llms. *Working Paper*, 2024.

[329] Pál András Papp and Roger Wattenhofer. Sequential defaulting in financial networks. *arXiv preprint arXiv:2011.10485*, 2020.

[330] Pál András Papp and Roger Wattenhofer. Default ambiguity: finding the best solution to the clearing problem. In *International Conference on Web and Internet Economics*, pages 391–409. Springer, 2021.

[331] Joon Sung Park, Joseph O'Brien, Carrie Jun Cai, Meredith Ringel Morris, Percy Liang, and Michael S Bernstein. Generative agents: Interactive simulacra of human behavior. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, pages 1–22, 2023.

[332] Patrick S Park, Joshua E Blumenstock, and Michael W Macy. The strength of long-range ties in population-scale social networks. *Science*, 362(6421):1410–1413, 2018.

[333] Binghui Peng. Dynamic influence maximization. *Advances in Neural Information Processing Systems*, 34:10718–10731, 2021.

[334] Supun Perera, Michael GH Bell, and Michiel CJ Bliemer. Network science approach to modelling the topology and robustness of supply chain networks: a review and perspective. *Applied network science*, 2(1):1–25, 2017.

[335] Bryan Perozzi, Bahare Fatemi, Dustin Zelle, Anton Tsitsulin, Mehran Kazemi, Rami Al-Rfou, and Jonathan Halcrow. Let your graph do the talking: Encoding structured data for llms. *arXiv preprint arXiv:2402.05862*, 2024.

[336] Anton Pichler, Marco Pangallo, R Maria del Rio-Chanona, François Lafond, and J Doyne Farmer. Production networks and epidemic spreading: How to restart the uk economy? *preprint arXiv:2005.10585*, 2020.

[337] Tiancheng Qin, S Rasoul Etesami, and Cesár A Uribe. Decentralized federated learning for over-parameterized models. In *2022 IEEE 61st Conference on Decision and Control (CDC)*, pages 5200–5205. IEEE, 2022.

[338] Scott R. Baker, Robert A Farrokhnia, Steffen Meyer, Michaela Pagel, and Constantine Yannelis. Income, liquidity, and the consumption response to the 2020 economic stimulus payments. *Review of Finance*, 27(6):2271–2304, 2023.

[339] Michael G Rabbat, Robert D Nowak, and James A Bucklew. Generalized consensus computation in networked systems with erasure links. In *Signal Processing Advances in Wireless Communications, 2005 IEEE 6th Workshop on*, pages 1088–1092. IEEE, 2005.

[340] M. A. Rahimian and A. Jadbabaie. Learning without recall: A case for log-linear learning. *IFAC-PapersOnLine*, 48(22):46–51, 2015.

[341] M. A. Rahimian, S. Shahrampour, and A. Jadbabaie. Learning without recall by random walks on directed graphs. *IEEE Conference on Decision and Control (CDC)*, 2015.

[342] M Amin Rahimian and Ali Jadbabaie. Bayesian learning without re-

call. *IEEE Transactions on Signal and Information Processing over Networks*, 3(3):592–606, 2016.

[343] M Amin Rahimian and Ali Jadbabaie. Distributed estimation and learning over heterogeneous networks. In *Communication, Control, and Computing (Allerton), 2016 54th Annual Allerton Conference on*, pages 1314–1321. IEEE, 2016.

[344] M Amin Rahimian and Ali Jadbabaie. Group decision making and social learning. In *Decision and Control (CDC), 2016 IEEE 55th Conference on*, pages 6783–6794. IEEE, 2016.

[345] M Amin Rahimian, Fang-Yi Yu, and Carlos Hurtado. Differentially private network data collection for influence maximization. In *Proceedings of the 2023 International Conference on Autonomous Agents and Multiagent Systems*, pages 2795–2797, 2023.

[346] M Amin Rahimian, Fang-Yi Yu, and Carlos Hurtado. Seeding with differentially private network information. *arXiv preprint arXiv:2305.16590*, 2023.

[347] Aida Rahmattalabi, Shahin Jabbari, Himabindu Lakkaraju, Phebe Vayanos, Max Izenberg, Ryan Brown, Eric Rice, and Milind Tambe. Fair influence maximization: A welfare optimization approach. *arXiv preprint arXiv:2006.07906*, 2020.

[348] Iyad Rahwan, Manuel Cebrian, Nick Obradovich, Josh Bongard, Jean-François Bonnefon, Cynthia Breazeal, Jacob W Crandall, Nicholas A Christakis, Iain D Couzin, Matthew O Jackson, et al. Machine behaviour. *Nature*, 568(7753):477–486, 2019.

[349] Amanah Ramadiah, Fabio Caccioli, and Daniel Fricke. Reconstructing and stress testing credit networks. *Journal of Economic Dynamics and Control*, 111:103817, 2020.

[350] Arjun S Ramani, Nicole Eikmeier, and David F Gleich. Coin-flipping, ball-dropping, and grass-hopping for generating random graphs from matrices of edge probabilities. *SIAM Review*, 61(3):549–595, 2019.

[351] Heidi L Rehm, Angela JH Page, Lindsay Smith, Jeremy B Adams, Gil Alterovitz, Lawrence J Babb, Maxmillian P Barkley, Michael Baudis, Michael JS Beauvais, Tim Beck, et al. Ga4gh: International policies and

standards for data sharing across genomic research and healthcare. *Cell genomics*, 1(2), 2021.

[352] W. Ren and RW Beard. Consensus seeking in multiagent systems under dynamically changing interaction topologies. *IEEE Transactions on Automatic Control*, 50(5):655–661, 2005.

[353] Aria Rezaei, Jie Gao, and Anand D Sarwate. Influencers and the giant component: The fundamental hardness in privacy protection for socially contagious attributes. In *Proceedings of the 2021 SIAM International Conference on Data Mining (SDM)*, pages 217–225. SIAM, 2021.

[354] Elsa Rizk, Stefan Vlaski, and Ali H Sayed. Enforcing privacy in distributed learning with performance guarantees. *arXiv preprint arXiv:2301.06412*, 2023.

[355] E. M. Rogers. *Diffusion of Innovations*. Simon and Schuster, 5th edition, 2003.

[356] Leonard CG Rogers and Luitgard Anna Maria Veraart. Failure and rescue in an interbank network. *Management Science*, 59(4):882–898, 2013.

[357] Ryan Rogers, Subbu Subramaniam, Sean Peng, David Durfee, Seunghyun Lee, Santosh Kumar Kancha, Shraddha Sahay, and Parvez Ahammad. Linkedin's audience engagements api: A privacy preserving data analytics system at scale. *arXiv preprint arXiv:2002.05839*, 2020.

[358] M. J. Rufo, J. Martin, C. J. Pérez, et al. Log-linear pool to combine prior distributions: A suggestion for a calibration-based approach. *Bayesian Analysis*, 7(2):411–438, 2012.

[359] Robert M Samstein, Chung-Han Lee, Alexander N Shoushtari, Matthew D Hellmann, Ronglai Shen, Yelena Y Janjigian, David A Barron, Ahmet Zehir, Emmet J Jordan, Antonio Omuro, et al. Tumor mutational load predicts survival after immunotherapy across multiple cancer types. *Nature genetics*, 51(2):202–206, 2019.

[360] Ali H Sayed et al. Adaptation, learning, and optimization over networks. *Foundations and Trends® in Machine Learning*, 7(4-5):311–801, 2014.

[361] Manfred Schroeder and M Herbich. Fractals, chaos, power laws. *Pure and Applied Geophysics*, 147(3):601–601, 1996.

[362] Steffen Schuldenzucker, Sven Seuken, and Stefano Battiston. Finding clearing payments in financial networks with credit default swaps is ppad-complete. *LIPIcs: Leibniz International Proceedings in Informatics*, (67), 2017.

[363] Steffen Schuldenzucker, Sven Seuken, and Stefano Battiston. Default ambiguity: Credit default swaps create new systemic risks in financial networks. *Management Science*, 66(5):1981–1998, 2020.

[364] E. Seneta. *Non-negative matrices and Markov chains*. Springer, 2006.

[365] Shahin Shahrampour, Alexander Rakhlin, and Ali Jadbabaie. Distributed detection: Finite-time analysis and impact of network topology. *IEEE Transactions on Automatic Control*, 61(11):3256–3268, 2015.

[366] Thomas M Shapiro et al. *The hidden cost of being African American: How wealth perpetuates inequality*. Oxford University Press, USA, 2004.

[367] Naichen Shi, Fan Lai, Raed Al Kontar, and Mosharaf Chowdhury. Ensemble models in federated learning for improved generalization and uncertainty quantification. *IEEE Transactions on Automation Science and Engineering*, 2023.

[368] Christoph Siebenbrunner. Clearing algorithms and network centrality. In *International Conference on Complex Networks and their Applications*, pages 499–507. Springer, 2018.

[369] Christoph Siebenbrunner. Clearing algorithms and network centrality. In *Complex Networks and Their Applications VII: Volume 2 Proceedings The 7th International Conference on Complex Networks and Their Applications COMPLEX NETWORKS 2018 7*, pages 499–507. Springer, 2019.

[370] David Simchi-Levi, William Schmidt, and Yehua Wei. From superstorms to factory fires: Managing unpredictable supply chain disruptions. *Harvard Business Review*, 92(1-2):96–101, 2014.

[371] David Simchi-Levi, William Schmidt, Yehua Wei, Peter Yun Zhang, Keith Combs, Yao Ge, Oleg Gusikhin, Michael Sanders, and Don Zhang. Identifying risks and mitigating disruptions in the automotive supply chain. *Interfaces*, 45(5):375–390, 2015.

[372] David Simchi-Levi, William Schmidt, Yehua Wei, Peter Yun Zhang, Keith

Combs, Yao Ge, Oleg Gusikhin, Michael Sanders, and Don Zhang. Identifying risks and mitigating disruptions in the automotive supply chain. *Interfaces*, 45(5):375–390, 2015.

[373] David Simchi-Levi, He Wang, and Yehua Wei. Increasing supply chain robustness through process flexibility and inventory. *Production and Operations Management*, 27(8):1476–1491, 2018.

[374] Sean R Sinclair, Siddhartha Banerjee, and Christina Lee Yu. Adaptive discretization in online reinforcement learning. *Operations Research*, 71(5):1636–1652, 2023.

[375] Arnab Sinha, Zhihong Shen, Yang Song, Hao Ma, Darrin Eide, Bo-June Hsu, and Kuansan Wang. An overview of microsoft academic service (mas) and applications. In *Proceedings of the 24th international conference on world wide web*, pages 243–246, 2015.

[376] Aleksandrs Slivkins et al. Introduction to multi-armed bandits. *Foundations and Trends® in Machine Learning*, 12(1-2):1–286, 2019.

[377] David Snyder and Edward L Kick. Structural position in the world system and economic growth, 1955-1970: A multiple-network analysis of transnational interactions. *American journal of Sociology*, 84(5):1096–1126, 1979.

[378] Isaac Sonin and Konstantin Sonin. A continuous-time model of financial clearing. *University of Chicago, Becker Friedman Institute for Economics Working Paper*, (2020-101), 2020.

[379] Ravi Srinivasan. Galton-watson branching process. *M375T/M396C: Topics in Complex Networks Course*, 2013.

[380] Despina Stasi, Kayvan Sadeghi, Alessandro Rinaldo, Sonja Petrović, and Stephen E Fienberg. *beta*-models for random hypergraphs with a given degree sequence. *arXiv preprint arXiv:1407.1004*, 2014.

[381] Ana-Andreea Stoica and Christos Papadimitriou. Strategic clustering. In *Learning in the presence of strategic behaviour Workshop (StratML), in Neural Information Processing Systems*, 2021.

[382] Latanya Sweeney. Weaving technology and policy together to maintain confidentiality. *The Journal of Law, Medicine & Ethics*, 25(2-3):98–110, 1997.

[383] Latanya Sweeney. Only you, your doctor, and many others may know. *Technology Science*, 2015092903(9):29, 2015.

[384] Henri Tajfel, Michael G Billig, Robert P Bundy, and Claude Flament. Social categorization and intergroup behaviour. *European journal of social psychology*, 1(2):149–178, 1971.

[385] Eduard Talamàs and Rakesh Vohra. Free and perfectly safe but only partially effective vaccines can harm everyone. *Games and Economic Behavior*, 122:277–289, 2020.

[386] Jie Tang, Jing Zhang, Limin Yao, Juanzi Li, Li Zhang, and Zhong Su. Arnetminer: extraction and mining of academic social networks. In *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 990–998, 2008.

[387] H. Tanner, A. Jadbabaie, and G. Pappas. Flocking in fixed and switching networks. *IEEE Transactions on Automatic Control*, 52(5):863–868, 2007.

[388] Robert L Thorndike. Who belongs in the family? *Psychometrika*, 18(4):267–276, 1953.

[389] New York Times. Where $5 trillion in pandemic stimulus money went, 2022. Accessed: 2024-06-17.

[390] Marcel P Timmer, Erik Dietzenbacher, Bart Los, Robert Stehrer, and Gaaitzen J De Vries. An illustrated user guide to the world input–output database: the case of global automotive production. *Review of International Economics*, 23(3):575–605, 2015.

[391] Behrouz Touri and Angelia Nedic. Distributed consensus over network with noisy links. In *2009 12th International Conference on Information Fusion*, pages 146–154. IEEE, 2009.

[392] Hugo Touvron, Louis Martin, Kevin Stone, Peter Albert, Amjad Almahairi, Yasmine Babaei, Nikolay Bashlykov, Soumya Batra, Prajjwal Bhargava, Shruti Bhosale, Dan Bikel, Lukas Blecher, Cristian Canton Ferrer, Moya Chen, Guillem Cucurull, David Esiobu, Jude Fernandes, Jeremy Fu, Wenyin Fu, Brian Fuller, Cynthia Gao, Vedanuj Goswami, Naman Goyal, Anthony Hartshorn, Saghar Hosseini, Rui Hou, Hakan Inan, Marcin Kardas, Viktor Kerkez, Madian Khabsa, Isabel Kloumann, Artem Korenev, Punit Singh Koura, Marie-Anne Lachaux, Thibaut Lavril, Jenya

Lee, Diana Liskovich, Yinghai Lu, Yuning Mao, Xavier Martinet, Todor Mihaylov, Pushkar Mishra, Igor Molybog, Yixin Nie, Andrew Poulton, Jeremy Reizenstein, Rashi Rungta, Kalyan Saladi, Alan Schelten, Silva Ruan, Smith Eric Michael, Subramanian Ranjan, Tan Xiaoqing Ellen, Tang Binh, Taylor Ross, Williams Adina, Xiang Jian, Xu Kuan Puxin, Yan Zheng, Zarov Iliyan, Zhang Yuchen, Fan Angela, Kambadur Melanie, Narang Sharan, Rodriguez Aurelien, Stojnic Robert, Edunov Sergey, and Scialom Thomas. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2310.12345*, 2023.

[393] Kenneth E Train. *Discrete choice methods with simulation*. Cambridge university press, 2009.

[394] Amanda L Traud, Peter J Mucha, and Mason A Porter. Social structure of facebook networks. *Physica A: Statistical Mechanics and its Applications*, 391(16):4165–4180, 2012.

[395] Stacey Truex, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig, Rui Zhang, and Yi Zhou. A hybrid approach to privacy-preserving federated learning. In *Proceedings of the 12th ACM workshop on artificial intelligence and security*, pages 1–11, 2019.

[396] Nguyen Truong, Kai Sun, Siyao Wang, Florian Guitton, and YiKe Guo. Privacy preservation in federated learning: An insightful survey from the gdpr perspective. *Computers & Security*, 110:102402, 2021.

[397] Alan Tsang, Bryan Wilder, Eric Rice, Milind Tambe, and Yair Zick. Group-fairness in influence maximization. *arXiv preprint arXiv:1903.00967*, 2019.

[398] J. N. Tsitsiklis and M. Athans. Convergence and asymptotic agreement in distributed decision problems. *Automatic Control, IEEE Transactions on*, 29(1):42–50, 1984.

[399] John N. Tsitsiklis. Decentralized detection. *Advances in Statistical Signal Processing*, 2(2):297–344, 1993.

[400] Charalampos E Tsourakakis. A note on computing betweenness centrality from the 2-core. *arXiv preprint arXiv:2408.01157*, 2024.

[401] Francesco Tudisco and Desmond J Higham. A nonlinear spectral method for core–periphery detection in networks. *SIAM Journal on Mathematics of Data Science*, 1(2):269–292, 2019.

[402] Francesco Tudisco and Desmond J Higham. Core-periphery detection in hypergraphs. *arXiv preprint arXiv:2202.12769*, 2022.

[403] Christian Upper. Simulation methods to assess the danger of contagion in interbank markets. *Journal of financial stability*, 7(3):111–125, 2011.

[404] Christian Upper and Andreas Worms. Estimating bilateral exposures in the german interbank market: Is there a danger of contagion? *European economic review*, 48(4):827–849, 2004.

[405] US Census. 2020 decennial census: Processing the count: Disclosure avoidance modernization. https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance.html, 2020. Accessed: 2023-05-18.

[406] Stefan Van Der Walt, S Chris Colbert, and Gael Varoquaux. The numpy array: a structure for efficient numerical computation. *Computing in science & engineering*, 13(2):22–30, 2011.

[407] Luitgard Anna Maria Veraart. When does portfolio compression reduce systemic risk? *Mathematical Finance*, 32(3):727–778, 2022.

[408] Veniamin Veselovsky, Manoel Horta Ribeiro, and Robert West. Artificial artificial artificial intelligence: Crowd workers widely use large language models for text production tasks, 2023.

[409] Jesse Vig, Sebastian Gehrmann, Yonatan Belinkov, Sharon Qian, Daniel Nevo, Yaron Singer, and Stuart Shieber. Investigating gender bias in language models using causal mediation analysis. *Advances in neural information processing systems*, 33:12388–12401, 2020.

[410] Pauli Virtanen, Ralf Gommers, Travis E Oliphant, Matt Haberland, Tyler Reddy, David Cournapeau, Evgeni Burovski, Pearu Peterson, Warren Weckesser, Jonathan Bright, et al. Scipy 1.0: fundamental algorithms for scientific computing in python. *Nature methods*, 17(3):261–272, 2020.

[411] Johan Wahlström, Isaac Skog, Patricio S La Rosa, Peter Händel, and Arye Nehorai. The *beta*-model for random graphs—regression, cramér-rao bounds, and hypothesis testing. *arXiv preprint arXiv:1611.05699*, 2016.

[412] Immanuel Wallerstein. World-systems analysis. *Social theory today*, 3, 1987.

[413] Terrie Walmsley, Adam Rose, and Dan Wei. The impacts of the coronavirus on the economy of the united states. *Economics of Disasters and Climate Change*, 5(1):1–52, 2021.

[414] Zhiyu Wan, James W Hazel, Ellen Wright Clayton, Yevgeniy Vorobeychik, Murat Kantarcioglu, and Bradley A Malin. Sociotechnical safeguards for genomic data privacy. *Nature Reviews Genetics*, 23(7):429–445, 2022.

[415] Y. Wang and P. M. Djuric. Social learning with bayesian agents and random decision making. *IEEE Transactions on Signal Processing*, 63(12):3241–3250, 2015.

[416] Stanley L Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965.

[417] Michael L Waskom. Seaborn: statistical data visualization. *Journal of Open Source Software*, 6(60):3021, 2021.

[418] Duncan J Watts, Peter Sheridan Dodds, and Mark EJ Newman. Identity and search in social networks. *science*, 296(5571):1302–1305, 2002.

[419] Duncan J Watts and Steven H Strogatz. Collective dynamics of 'small-world'networks. *nature*, 393(6684):440–442, 1998.

[420] Karol Wegrzycki, Piotr Sankowski, Andrzej Pacuk, and Piotr Wygocki. Why do cascade sizes follow a power-law? In *Proceedings of the 26th International Conference on World Wide Web*, pages 569–576, 2017.

[421] Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, Fei Xia, Ed Chi, Quoc V Le, Denny Zhou, et al. Chain-of-thought prompting elicits reasoning in large language models. *Advances in neural information processing systems*, 35:24824–24837, 2022.

[422] Sean P Willems. Data set—real-world multiechelon supply chains used for inventory optimization. *Manufacturing & Service Operations Management*, 10(1):19–23, 2008.

[423] Royce J Wilson, Celia Yuxin Zhang, William Lam, Damien Desfontaines, Daniel Simmons-Marengo, and Bryant Gipson. Differentially private sql with bounded user contribution. *Proceedings on privacy enhancing technologies*, 2020(2):230–250, 2020.

[424] GR Wood and BP Zhang. Estimation of the lipschitz constant of a function. *Journal of Global Optimization*, 8:91–103, 1996.

[425] Bohan Wu and César A Uribe. Frequentist guarantees of distributed (non)-bayesian inference. *arXiv preprint arXiv:2311.08214*, 2023.

[426] L. Xiao, S. Boyd, and S. Lall. A scheme for robust distributed sensor fusion based on average consensus. In *Fourth International Symposium on Information Processing in Sensor Networks (IPSN)*, pages 63–70, 2005.

[427] L. Xiao, S. Boyd, and S. Lall. A space-time diffusion scheme for peer-to-peer least-squares estimation. In *Proceedings of the 5th international conference on Information Processing in Sensor Networks*, pages 168–176, 2006.

[428] Qian Xu, Pinyi Ren, Houbing Song, and Qinghe Du. Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions. *IEEE Internet of Things Journal*, 4(6):1924–1933, 2017.

[429] Yeojoon Youn, Zihao Hu, Juba Ziani, and Jacob Abernethy. Randomized quantization is all you need for differential privacy in federated learning. *arXiv preprint arXiv:2306.11913*, 2023.

[430] Shimin Yu, Fang-Ming Shao, and Huajun Meng. Uniformly optimal graphs in some classes of graphs with node failures. *Discrete mathematics*, 310(1):159–166, 2010.

[431] Yuan Yuan, Ahmad Alabdulkareem, and Alex Pentland. An interpretable approach for social network formation among heterogeneous agents. *Nature communications*, 9(1):4704, 2018.

[432] Yubai Yuan and Annie Qu. Community detection with dependent connectivity. *The Annals of Statistics*, 49(4):2378–2428, 2021.

[433] Xubo Yue, Raed Al Kontar, and Ana María Estrada Gómez. Federated data analytics: A study on linear models. *IISE Transactions*, pages 1–25, 2022. in-press.

[434] Heng Zhang, Yuanchao Shu, Peng Cheng, and Jiming Chen. Privacy and performance trade-off in cyber-physical systems. *IEEE Network*, 30(2):62–66, 2016.

[435] Xiao Zhang, Travis Martin, and Mark EJ Newman. Identification of core-periphery structure in networks. *Physical Review E*, 91(3):032803, 2015.

[436] Xinwei Zhang, Xiangyi Chen, Mingyi Hong, Zhiwei Steven Wu, and Jinfeng Yi. Understanding clipping for federated learning: Convergence and client-level differential privacy. In *International Conference on Machine Learning, ICML 2022*, 2022.

[437] Xuhui Zhou, Hao Zhu, Leena Mathur, Ruohong Zhang, Haofei Yu, Zhengyang Qi, Louis-Philippe Morency, Yonatan Bisk, Daniel Fried, Graham Neubig, et al. Sotopia: Interactive evaluation for social intelligence in language agents. *arXiv preprint arXiv:2310.11667*, 2023.

[438] Juba Ziani. How differential privacy impacts data elicitation. *ACM SIGecom Exchanges*, 20(2):75–81, 2022.