Decision-Making Frameworks for Network Resilience
#
–
#
Managing and Mitigating Systemic (Cyber) Risk

Gregor Svindland[a] and Alexander Voß[a]

[a]Institute of Actuarial and Financial Mathematics & House of Insurance, Leibniz University Hannover, Germany

November 8, 2024

We introduce a decision-making framework tailored for the management of systemic risk in networks. This framework is constructed upon three fundamental components: (1) a set of acceptable network configurations, (2) a set of interventions aimed at risk mitigation, and (3) a cost function quantifying the expenses associated with these interventions. While our discussion primarily revolves around the management of systemic cyber risks in digital networks, we concurrently draw parallels to risk management of other complex systems where analogous approaches may be adequate.

1 Introduction

Modern societies and economies are increasingly dependent on systems that are characterized by complex forms of interconnectedness and interactions between different actors and system entities. Examples of such critical infrastructures are energy grids, transportation and communication systems, financial markets, and digital systems such as the internet.

However, the complexity of interaction channels also constitutes a major source of risk. The term *systemic risk* refers to the risk arising from the internal characteristics of a system. Typically, systemic risk is triggered by some initial failure or disruption in some part of the system, and then propagates and amplifies via various types of channels connecting the system entities. Therefore, the study of systemic risk involves not only understanding the individual components of a network but also examining its pattern of interactions and feedback mechanisms.

Our main focus in this paper is management of systemic cyber risk, which constitutes a significant part of the general cyber risk exposure, see [7] for a discussion of classes of cyber risk. Examples of systemic cyber risk incidences are the WannaCry (May 2017) and NotPetya (June 2017) worm-type malware attacks, or the recent IT outage caused by a security update of the cybersecurity firm CrowdStrike (July 2024).

A common way to understand complex systems is the representation of their components and interactions as *networks*—a term which we use synonymously with *graphs*. The nodes of the network represent the individual entities, and edges depict the connections or relationships between them. In cyber systems, these nodes could be computers, servers, or even individual users, while financial systems might have nodes representing banks, markets, or financial investors. Possible interpretations of nodes and edges in electrical systems or in the case of a public transport system are also obvious. Networks with multiple layers are applied to represent different classes of interdependent system entities and to model the risk impact of one class on the other. For illustration consider the potential threat of cyber risks to financial stability. Macroprudential regulators increasingly apply network models to develop a regulatory machinery to control those risks, see e.g. [25], [28], [29]. In that case the network consists of a cyber (sub)-network and the financial (sub)-network. So-called "cyber mappings" are used to identify systemically relevant network nodes in both the cyber network and the financial network and to analyse transmission channels of cyber risk to the financial system. A stylized illustration of a cyber map is given in Figure 1. These approaches are discussed, for example, in [15], [29], [36], and [60].

The task of a network *supervisor* is to assess the systemic risk of the supervised network and to regulate it in such a way that this risk remains controlled. Network supervisors are, for instance,

a) a *regulator* or *central planner* managing risk and resilience of (digital) systems and infrastructures from the perspective of society, see the discussion above.

b) an *insurance company* concerned with the limits of insurability of systemic accumulation risk and the design of policy exclusions. Indeed insurers act as *private regulators* by requiring or incentivising security and system standards among their policyholders through contractual obligations, see the discussion in [6].

c) a *(local) risk manager* or *system administrator* who is concerned with the network protection of a single firm or industry cluster.

In this paper we take the point of view of such a supervisor, and develop a theoretical
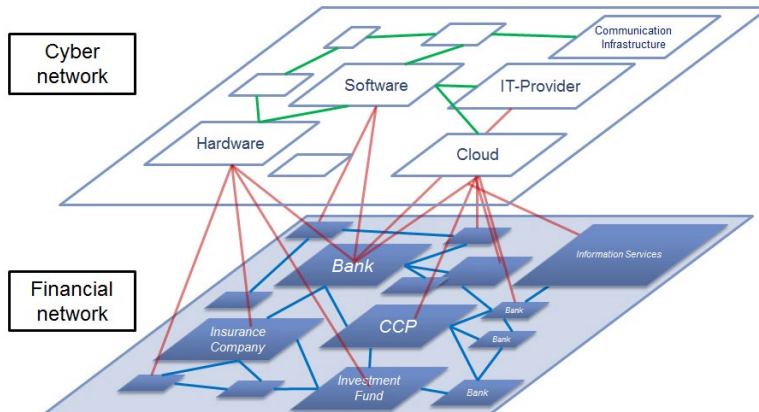
Figure 1: A stylized cyber map consisting of a cyber and a financial (sub-)network. The figure is taken from [29] and owned by Deutsche Bundesbank. Reproduced with permission.

framework for the assessment and management of systemic (cyber) risk. To this end, we follow a well-established approach to risk assessment based on three main ingredients:

- a set $\mathcal{A}$ of acceptable networks which are deemed to be secure enough,

- a set $\mathcal{I}$ of interventions to transform non-acceptable networks into acceptable ones,

- a quantification of the cost $\mathcal{C}$ (not necessarily in monetary terms) of making some network acceptable.

The triplet $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is then called a *decision-making framework for network resilience* (DMFNR). In the following we discuss why we identify the three components $\mathcal{A}, \mathcal{I}$, and $\mathcal{C}$ as the central building blocks for assessing systemic risk.

As regards the acceptance set, we find that the most fundamental question any system supervisor has to answer is whether there is a demand for regulation of that system or not. This requires an acceptance criterion as a basis for identifying those networks which the supervisor deems secure enough and those which need to be further secured. Accordingly, the *acceptance set* contains all secure enough networks. In contrast, networks which do not belong to the acceptance set are those which require further protecting measures. It is up to the supervisor to set the security standards by prescribing the acceptance set. Natural decision criteria in this process are network features such as the presence or absence of systemic parts which may induce concentration risks, or the resilience of the network with respect to (models of) concrete cyber attack scenarios such as the spread of malware (WannaCry, NotPetya) or service outages (CrowdStrike).

If a given network G does not meet the supervisor's acceptance criterion, that is $G \notin \mathcal{A}$, suitable risk mitigants are needed to secure the network. Those are the supervisor's *interventions* collected in $\mathcal{I}$. In case of cyber risk, well-known examples of risk mitigants in practice are e.g. firewalls, security patches, backups, controlling access to servers or computers, monitoring of data flows, re-configuring network communication and access

rules, or diversification of IT-service providers. In our theory, given a network G, any measures to improve the network's resilience are interpreted as operations on the given network G. The most basic available operations are addition or deletion of nodes and edges. For example, edge hardening measures securing particular network connections (firewalls, increased monitoring of particular network connections, or physical deletions of connections) may be identified with the deletion of the corresponding edge from the network, because the increased security erases this risk transmission channel. Backups can be modeled by a combination of node and edge additions, whereas diversification is achieved by node splitting where a node is split into two distinct nodes with the same operational tasks and a redistribution of the original edges. In Section 4 we discuss (theoretical) interventions on the network and their practical interpretations for regulation of systemic cyber risk. Note that a supervisor might typically not have all possible network interventions available, for instance due to legal issues. Therefore, we consider a set of available and admissible network interventions $\mathcal{I}$ from which the supervisor might choose in the regulation process. Also note that regulators are increasingly pursuing a "Zero Trust" principle according to which no one is trusted by default from inside or outside the network. In particular no parts of a network are deemed to be more secure than other parts which implies that interactions with other entities of the network cannot be based, for instance, on the security standards of the other. As a result, the risk management is left with creating secure and resilient network architectures, see [58] or [55, Section 3.5.3].

Apart from limitations as regards availability and admissibility of interventions, supervision is also subject to efficiency criteria which we represent by a cost function $\mathcal{C}$. We identify and study two main classes of costs, namely costs in terms of monetary investments needed for regulation, and costs in terms of loosing functionality of the network. The latter class of costs is based on well-known measures of network functionality, see Section 5.

Even though we will mostly limit our discussion to systemic cyber risks, we want to emphasize that this risk management approach can also be applied to other forms of systemic risk, including those where the trade-off between functionality and risk due to interconnectedness may be different from the cyber risk case. In electrical networks, for instance, an increase in interconnectedness may be desirable from a resilience-building perspective.

1.1 A Motivating Example

Recall the cyber mappings introduced earlier. A recent study [36, 60] provides a detailed cyber mapping analysis of publicly disclosed outsourcing activities by German public retail funds. The (layered) network analyzed in this study comprises two main classes of nodes: financial institutions (FIs), representing the financial system, and third-party providers (TPPs), which offer outsourcing services to these FIs. We identify two major cyber risks to the financial system that are either caused or exacerbated by outsourcing activities:

1. Outages of TPPs, which could severely disrupt the operations of critical parts of

the financial system.

2. Cyberattacks, such as WannaCry or NotPetya, which could spread rapidly through the increased digital interconnections between entities.

Let us discuss different ways a financial system supervisor might decide whether the described network is acceptable or not. One option is to control the number of connections, that is the *degree*, of each node, particularly of the TPP nodes. In the context of risk scenario 1, this strategy ensures that a TPP outage cannot simultaneously disrupt too many connected FIs. For risk scenario 2, controlling the degree helps contain the spread of malware from an infected node to the rest of the system. To manage node degrees effectively, the supervisor could examine the degree distribution of the network. Constraints on the moments of the degree distribution, as a foundation for acceptance sets $\mathcal{A}$, are discussed in detail in Section 6.1. On a related note, the supervisor might aim to identify central (systemic) parts of the network that require heightened surveillance. Apart from considering node degrees, there are alternative measures of node centrality which may be useful in this regard, see Section 6.2.1. Acceptance sets based on centrality constraints are discussed in detail in Section 6.2. Yet a different approach is to simulate risk scenarios using an external model. The network can then be evaluated based on its performance under such stress tests, see the discussion in Section 6.3.

Regarding the admissible interventions $\mathcal{I}$ of the supervisor, first note that it is reasonable to assume that not every node or connection in the network can be regulated. For example, the European Union's NIS2 Directive [31] on the regulation of digital critical infrastructure systems employs a size-cap rule that limits the directive's scope to entities of medium or large size within the targeted sectors. Appropriate interventions for these nodes might include backup requirements, diversification, or edge hardening measures as discussed above.

In terms of costs, forced diversification or backups on the TPP side are unlikely to affect the overall network functionality, though they may lead to an increase in the monetary cost of outsourced services. In contrast, edge hardening measures could potentially impact network functionality. If costs based on network functionality or true monetary costs do not apply, for instance due to lack of information, a straightforward way to measure costs is to count the number of interventions required to secure the network, aiming to keep this number as low as possible. This approach corresponds to a simplified model of monetary costs, where each intervention is assigned the same symbolic value (e.g., 1 unit). However, this model can be refined by assigning different (symbolic) costs to interventions based on factors such as the severity or complexity of the intervention. This would allow for a more nuanced approach to cost modeling, where more invasive or resource-intensive actions incur higher costs. Costs are discussed in Section 5.

Assume now that the regulator has decided on an DMFNR $(\mathcal{A}, \mathcal{I}, \mathcal{C})$. The implementation of this DMFNR can proceed as follows: First, the regulator must assess whether the given network G is acceptable, $G \in \mathcal{A}$, or if regulation is required, $G \notin \mathcal{A}$. If $G \notin \mathcal{A}$, protective strategies—these are consecutive application of interventions from $\mathcal{I}$—must be found to bring the network into an acceptable state. Suppose that the supervisor has

identified various such strategies. Then a reasonable choice amongst those strategies is the most cost-efficient strategy which is determined by means of the cost model $\mathcal{C}$.

Literature As regards the mathematical literature on cyber risk, we refer to the surveys [7] and [27] for a comprehensive overview. A few recent studies focusing on cyber insurance are [8], [10], [14], [21], [22], [43], [65], [67], and [66]. There is an increasing line of literature utilizing epidemic processes on networks known from theoretical biology (see, e.g. [50, 56]) to model the spread of contagious cyber risks in digital systems, see [3], [20], [32], [41], [42], [48], and [64]. The latter articles are mostly concerned with the pricing of cyber insurance policies. Further considerations on the significance of systemic cyber risks for the vulnerability of digitally networked societies and economies can be found in [37] and [63].

Systemic risk has long been studied in the context of financial systems, see for instance [38], [46], and [47] for an overview. In particular, models for contagion effects in financial networks have been proposed and studied in [2], [23], [24], [26], and [40], whereas, for example, [4], [11], [17], [33], [39], [44], and [45] consider risk measures for systemic risk in financial markets.

Various aspects of network resilience and robustness have for example been discussed in [1], [59] and [62]. In particular, [1] emphasizes the need to develop a more general resilience metric for complex networks.

An axiomatic approach to monetary risk measures goes back to [5], see also [12], [34], and [35] for an overview of the theory on monetary risk measures. It is from this theory that we adopt the idea to base the risk assessment on a set of acceptable configurations $\mathcal{A}$, a set of controls $\mathcal{I}$, and related costs $\mathcal{C}$.

Outline Section 2 introduces decision-making frameworks for network resilience alongside the formal framework and some foundational definitions. Section 3 is dedicated to acceptance sets and explores some desirable properties of acceptance sets from the perspective of systemic cyber risk regulation. In Section 4 we discuss theoretical network interventions $\mathcal{I}$ and their practical counterparts. Costs $\mathcal{C}$ are introduced and discussed in Section 5. Examples of DMFNRs are presented in Section 6. Section 7 offers an outlook on open questions and potential areas for future research. Finally, the appendix contains considerations and additional examples for undirected graphs.

2 Decision-Making Frameworks for Network Resilience

In this section we formally define decision-making frameworks for network resilience. To this end, in the following, we first need to specify and briefly discuss their domain of definition.

2.1 Graphs and Networks

A *graph* G is an ordered pair of sets $G = (\mathcal{V}_G, \mathcal{E}_G)$ where $\mathcal{V}_G$ is a finite set of elements, called *nodes* (or *vertices*), and $\mathcal{E}_G \subseteq \mathcal{V}_G \times \mathcal{V}_G$ a set of pairs, called *edges* (or *links*). In the

following, we will always assume $(v, v) \notin \mathcal{E}_G$, i.e, we do not allow for self-connections of nodes. Further, for the rest of the paper, we assume that all graphs are defined over the same non-empty countably infinite basis set of nodes $\mathbb{V}$, i.e., that $\mathcal{V}_G \subseteq \mathbb{V}$ for all graphs G. We denote the set of such graphs by

$$\mathcal{G} := \{G \mid G = (\mathcal{V}_G, \mathcal{E}_G), \mathcal{V}_G \subset \mathbb{V}, \mathcal{E}_G \subset (\mathcal{V}_G \times \mathcal{V}_G) \cap \mathbb{E}\}$$

where $\mathbb{E} := \{(v, w) \in \mathbb{V} \times \mathbb{V} \mid v \neq w\}$. The number of nodes $|\mathcal{V}_G|$ is called the *size* of graph G. A graph $G' = (\mathcal{V}', \mathcal{E}')$ with $\mathcal{V}' \subseteq \mathcal{V}_G$, $\mathcal{E}' \subseteq \mathcal{E}_G$ is called a *subgraph* of G.

A *network* is any structure which admits an abstract representation as a graph: The nodes represent the network's agents or entities, while the connecting edges correspond to a relation or interaction among those entities. In the following, we use the terms "graph" and "network" interchangeably.

An important subclass of $\mathcal{G}$ is the set of *undirected graphs*: A graph $G = (\mathcal{V}_G, \mathcal{E}_G) \in \mathcal{G}$ is called *undirected* if for all $v, w \in \mathcal{V}_G$ we have $(v, w) \in \mathcal{E}_G \Leftrightarrow (w, v) \in \mathcal{E}_G$. A graph which is not undirected is often referred to as being *directed*. There is a vast literature on undirected graphs, and many popular network models restrict themselves to this subclass. However, throughout this paper we will work with the complete set of directed graphs $\mathcal{G}$ since the direction of a possible information flow may be essential to understand the associated risk of a corresponding connection. Nevertheless, our results, or appropriate versions of the results, also hold if we restrict ourselves to the undirected case, see Appendix B for the details. Moreover, in Appendices B.2.3 and B.2.6 we provide examples which are peculiar to an undirected graph framework.

Example 2.1. *Consider our motivating example from Section 1.1 and the described service outage scenario. In that case the direction of risk propagation is opposite to the direction of outsourcing. Outages originate at the TPP nodes and spread to the FIs that rely on their services. As a result, the network is best viewed as a directed graph with edges running from TPPs to the FIs that outsource to them.*

Remark 2.2. *(Weighted Graphs) In some situations it could be reasonable to consider weights assigned to the edges, symbolizing the extent of transmissibility of a shock across each respective edge. Nonetheless, defining the precise nature and magnitude of these weights might pose a challenge. In our motivating example from Section 1.1, only the presence of a connection between an FI and a TPP can be reconstructed from the underlying dataset. There is no data available to meaningfully calibrate potential edge weights in that network.*

Also note that there are cases in which assigning edge weights is not appropriate. Again consider the motivating example. In the event of a TPP outage, all FIs outsourcing to that TPP are equally affected.

In this paper, we restrict ourselves to directed, but unweighted graphs. We briefly discuss the enhancement of our framework to weighted graphs in the Outlook Section 7.

In the following, we frequently reference key concepts from network theory, including adjacency matrices, node degrees (both incoming and outgoing), as well as walks and paths between nodes. For the reader not familiar with these concepts, the corresponding definitions and notations are detailed in Appendix A.

2.2 Acceptance Sets

Definition 2.3. *An acceptance set is any non-empty set $\mathcal{A} \subset \mathcal{G}$.*

The acceptance set is determined by the regulator and comprises all acceptable networks, i.e., the graphs which need no further regulatory interventions. The choice of the correct acceptance set is, of course, a challenging task. We devote Section 3 to study desirable properties of acceptance sets, and examples are provided in Section 6. Note that, apart from general network characteristics such as the degree distribution of the nodes, acceptability may depend on specific nodes or structure of a concrete network $G \in \mathcal{G}$ which the supervisor is managing.

2.3 Interventions

Interventions are the risk mitigants that are potentially available to the supervisor to secure networks. In general, an intervention can be defined as a mapping that transforms one network into another:

Definition 2.4. *A (network) intervention is a map $\kappa : \mathcal{G} \to \mathcal{G}$.*

Examples of interventions are given in Section 4. Here we also briefly mention, for the case of cyber security, possible interpretations of the presented interventions in terms of real-world measures to protect an IT-system.

In practice, the supervisor's ability to intervene may be limited. Regulatory approaches often target specific industry sectors and focus on essential network entities, while excluding smaller companies or private users. For instance, the European Union's NIS2 Directive [31] on digital critical infrastructure applies a size-cap rule, restricting its scope to medium and large entities within targeted sectors. Consequently, risk management is typically constrained to a set of *admissible* interventions. Whether an intervention is admissible may depend on the specific graph G that the supervisor must secure.

Definition 2.5. *Given a non-empty set $\mathcal{I}$ of interventions, an ($\mathcal{I}$-)strategy κ is a finite composition of interventions in $\mathcal{I}$, i.e. $\kappa = \kappa_1 \circ \ldots \circ \kappa_n$ where $\kappa_i \in \mathcal{I}$ for all $i = 1, \ldots, n$ and $n \in \mathbb{N}$. We let $[\mathcal{I}]$ denote the set comprising all $\mathcal{I}$-strategies and in addition, if not already included in $\mathcal{I}$, the intervention* id $: G \mapsto G$, *leaving the network unaltered. The set*

$$\sigma^{\mathcal{I}}(G) := \{\kappa(G) \mid \kappa \in [\mathcal{I}]\}$$

contains all networks that can be generated from G by applying $\mathcal{I}$-strategies.

Of course, the supervisor is constrained to strategies of admissible interventions. The following definition brings together acceptance sets and admissible interventions.

Definition 2.6. *Let $\mathcal{A} \subset \mathcal{G}$ be an acceptance set and further let $\mathcal{I}$ be a non-empty set of network interventions. $\mathcal{A}$ is said to be closed under $\mathcal{I}$ if $\sigma^{\mathcal{I}}(G) \subset \mathcal{A}$ for all $G \in \mathcal{A}$. In that case $\mathcal{I}$ is called risk-reducing for $\mathcal{A}$. A network intervention κ is called risk-reducing for $\mathcal{A}$ if the intervention set $\{\kappa\}$ is risk-reducing for $\mathcal{A}$.*

Lemma 2.7. *Suppose that the non-empty set $\mathcal{I}$ of interventions is not (partially) self-reverse in the sense that for all $G \in \mathcal{G}$ and all $\alpha \in [\mathcal{I}]$ with $\alpha(G) \neq G$, there is no $\kappa \in [\mathcal{I}]$ such that $\kappa \circ \alpha(G) = G$. Then*

$$G \preccurlyeq_{\mathcal{I}} H \quad :\Leftrightarrow \quad H \in \sigma^{\mathcal{I}}(G)$$

defines a partial order on $\mathcal{G}$. In particular, $\mathcal{I}$ is risk-reducing for $\mathcal{A}$ if and only if $\mathcal{A}$ is monotone with respect to $\preccurlyeq_I$, that is $G \in \mathcal{A}$ and $G \preccurlyeq_{\mathcal{I}} H$ implies $H \in \mathcal{A}$.

Proof. $\mathrm{id} \in [\mathcal{I}]$ implies reflexivity of $\preccurlyeq_{\mathcal{I}}$. As regards transitivity, for $H \in \sigma^{\mathcal{I}}(G)$ and an arbitrary $L \in \sigma^{\mathcal{I}}(H)$, we find $\kappa, \tilde{\kappa} \in [\mathcal{I}]$ with $\kappa(G) = H$, and $\tilde{\kappa}(H) = L$, respectively. Then $\tilde{\kappa} \circ \kappa \in [\mathcal{I}]$ and $\tilde{\kappa} \circ \kappa(G) = L$, so that $L \in \sigma^{\mathcal{I}}(G)$. Finally suppose that $G \preccurlyeq_{\mathcal{I}} H$ and $H \preccurlyeq_{\mathcal{I}} G$, then there are $\mathcal{I}$-strategies $\kappa, \tilde{\kappa}$ such that $H = \kappa(G)$ and $G = \tilde{\kappa}(H) = \tilde{\kappa} \circ \kappa(G)$. Since $\mathcal{I}$ is not partially self-reverse, we must have $H = \kappa(G) = G$. This proves antisymmetry of $\preccurlyeq_{\mathcal{I}}$. $\qquad\square$

2.4 Cost Function

The final ingredient to our risk management framework is the cost function representing some type of price we pay for altering a given network. The cost function measures the consequences of the supervisors decisions and potentially quantifies the resources needed to achieve acceptability. Therefore, the cost function may depend on the acceptance set and on the interventions applied to achieve acceptability.

Definition 2.8. *Given a network acceptance set $\mathcal{A} \subset \mathcal{G}$ and a set of interventions $\mathcal{I}$ which is risk-reducing for $\mathcal{A}$, a map $\mathcal{C} : \mathcal{G} \times \mathcal{G} \to \mathbb{R} \cup \{\infty\}$ with*

  C1 $\mathcal{C}(G, G) = 0$ for all $G \in \mathcal{G}$

  C2 $\mathcal{C}(G, H) \geq 0$ whenever $H \in \sigma^{\mathcal{I}}(G)$

is called a cost function for $(\mathcal{A}, \mathcal{I})$.

Property C1 means that not altering the network does not cost anything, while property C2 ensures that any strategy leading to a potential improvement comes at a non-negative cost.

2.5 Decision-Making Frameworks for Network Resilience

Definition 2.9. *A decision-making framework for network resilience (DMFNR) is a triplet $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ where*

- *$\mathcal{A}$ is an acceptance set,*

- *$\mathcal{I}$ is a set of admissible interventions which is risk-reducing for $\mathcal{A}$,*

- *$\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I})$.*

As previously discussed, the acceptance set $\mathcal{A}$ comprises all networks which the supervisor deems secure enough, strategies in $[\mathcal{I}]$ are the risk mitigants of the supervisor in case the network is not acceptable, and the cost function $\mathcal{C}$ determines the cost of securing a network. The requirement that $\mathcal{I}$ be risk-reducing for $\mathcal{A}$ is a minimal consistency between the risk mitigants and the notion of acceptability, meaning that an acceptable network cannot become unacceptable by applying risk mitigants. This could be strengthened, for instance by requirements of the form $\sigma^{\mathcal{I}}(G) \cap \mathcal{A} \neq \emptyset$ for all networks $G \in \mathcal{G}$. The latter would ensure that any network can be secured, an assumption which we find too strong at this level. Property C2 of the cost function is a minimal consistency between strategies securing a network and related costs.

At this stage the requirements on a DMFNR are rather weak and general. The aim is to provide a framework which we believe is flexible enough, yet structurally reasonable to assess and manage systemic risk. Clearly, a DMFNR is suited for handling systemic risk in many different situations as outlined in the introduction. It is the task of the supervisor to determine a suitable acceptance set, and to identify admissible interventions and related costs to deal with a particular risk situation. The problems here are similar to finding the 'right' risk measure in classical financial regulation (for banks or insurance companies). In Sections 3, 4, and 5 we will discuss further properties of acceptance sets, interventions, and costs that might be suited to handle certain risk scenarios. The discussion there is, however, mostly tailored to cyber risk in digital networks. In Section 6 we provide concrete examples of DMFNRs and we analyse properties of those.

Note that—in contrast to many approaches to handle risk in the literature—a DMFNR does a priori

Q1 not attempt to measure the systemic risk in terms of a quantification of risk. In particular, a DMFNR does not answer the question of minimal costs to achieve acceptability (if possible).

Q2 not necessarily allow to compare the risk of two or more networks.

The reason for that is—as is well-known from multivariate risk measure theory in mathematical finance—that a satisfactory answer to Q1 and Q2 might be hard to achieve:

- As regards Q1 (and also Q2), a reasonable quantification of risk, would be the mentioned minimal costs of achieving acceptability. But that would require complete knowledge of all admissible ways, and the related costs, to transform a network into an acceptable state. For large networks this presents a computability and complexity problem that might be difficult or impossible to solve. Also, depending on the incentives of the supervisor, she might not even be interested in achieving cost efficiency amongst all protection strategies.

- Dealing with Q2 may require to know the answer to Q1. Eventually it is questionable whether Q2 is really of interest, since in most applications in mind the supervisor is managing a *given* network, and is not free to choose an initial configuration to start with. This given network has to be secured somehow in an admissible and ideally efficient way.

A DMFNR sets the framework for the supervisor and can be applied in various ways. As previously emphasized, the acceptance set addresses whether regulation is necessary or not. The admissible risk-reducing interventions include risk mitigation strategies for the supervisor, and the cost function determines the associated costs. If multiple protection strategies are available, the supervisor might opt for the most cost-effective one. However, it may be (computationally) infeasible to determine whether this strategy is globally efficient. Additionally, other factors might be more important than cost efficiency.

However, if we temporarily set aside issues of computability and complexity, a natural way to obtain a (univariate) risk measure based on a DMFNR $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is to let $\rho(G)$ denote the infimal cost of achieving acceptability (if possible):

$$\rho(G) := \inf\{\mathcal{C}(G, \tilde{G}) \mid \tilde{G} \in \sigma^{\mathcal{I}}(G) \cap \mathcal{A}\}, \ G \in \mathcal{G}, \quad \text{where } \inf \emptyset := \infty. \tag{1}$$

This approach is in line with the construction of monetary risk measures for financial risk management, see [34] for a comprehensive discussion of monetary risk measures. Constructions of this kind have also been applied to the measurement of systemic financial risks, see for example [11].

Lemma 2.10. *The univariate measure ρ given in* (1) *satisfies*

1. *$\rho(G) \geq 0$ for $G \notin \mathcal{A}$,*

2. *$\rho(G) = 0$ whenever $G \in \mathcal{A}$.*

3. *Suppose, moreover, that there is a minimal cost of alterering a network, that is there exists $\nu > 0$ such that $\mathcal{C}(G, \tilde{G}) \geq \nu$ whenever $G \in \mathcal{G}$ and $\tilde{G} \in \sigma^{\mathcal{I}}(G) \setminus \{G\}$. Then $\rho(G) \geq \nu$ for all $G \notin \mathcal{A}$ and $\mathcal{A} = \{G \in \mathcal{G} \mid \rho(G) = 0\}$.*

Proof. 1. immediately follows from property *C2* of the cost function. 2. is a consequence of $\mathrm{id} \in [\mathcal{I}]$, thus $G \in \sigma^{\mathcal{I}}(G)$, and of $\mathcal{C}(G, G) = 0$ by property *C1*. 3. is easily verified. $\square$

Finally, note that, apart from complexity issues, in order to apply (1) one would have to check whether the infimum is a minimum whenever $\rho(G) < \infty$, that is whether there is a "best" acceptable version of the network G.

3 Properties of Acceptance Sets for Systemic Cyber Risk Management

Consider an acceptance set $\mathcal{A}$. In this section we present selected properties of $\mathcal{A}$ that are tailored to the management of systemic cyber risk.

P1 *For all $\mathcal{V} \subset \mathbb{V}$ such that $|\mathcal{V}| \geq 2$, we have $G = (\mathcal{V}, \emptyset) \in \mathcal{A}$..*

Property 1 indicates that edgeless graphs should be acceptable due to the absence of contagion channels or feedback mechanisms. Note the restriction $|\mathcal{V}| \geq 2$. Indeed, if $|\mathcal{V}| = 1$, the edgeless graph of size 1 is also a star graph and complete, see below. To maintain consistency with later axioms, we exclude graphs of size 1 from $\mathcal{A}$. This is also justified by observing that occurrence of an incident at the single node $v \in \mathcal{V} = \{v\}$ means that the full system is affected, which is worst case from a systemic point of view.

P2 *There exists an $N_0 \in \mathbb{N}$ such that for all $N \geq N_0$, the acceptance set $\mathcal{A}$ contains a weakly connected network with N nodes.*

In view of the functionality of a system, interconnectedness should be acceptable up to a certain degree. We refer the reader not familiar with the notion of weakly and strongly connected networks to Appendix A.3. The size restriction in P2 accounts for the observation that with an increasing number of nodes, maintaining functionality, that is the network being connected, while controlling the risk is more feasible.

Next we address system vulnerability by specifying worst-case arrangements of networks that exceed any reasonable limit of risk. For the notion of in- and out-neighborhoods of nodes $v \in \mathcal{V}_G$, denoted by $\mathcal{N}_v^{G,in}$ and $\mathcal{N}_v^{G,out}$, respectively, we refer to Appendix A.2.

Definition 3.1. *Consider a network $G \in \mathcal{G}$ and a node $v^* \in \mathcal{V}_G$.*

1. *We call v^* a super-spreader if $\mathcal{N}_{v^*}^{G,out} = \mathcal{V}_G \setminus \{v^*\}$.*

2. *If, moreover, $\mathcal{N}_{v^*}^{G,in} = \mathcal{N}_{v^*}^{G,out} = \mathcal{V}_G \setminus \{v^*\}$, then v^* is called a star node.*
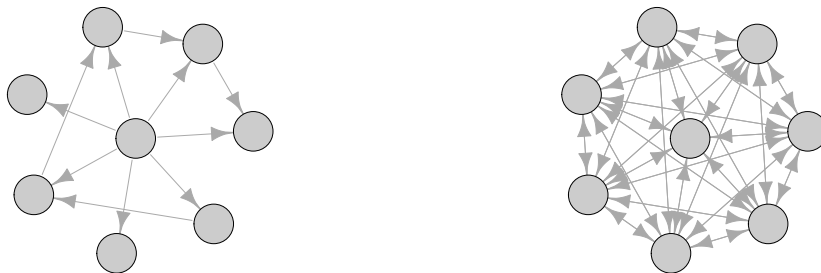

Figure 2: A graph that contains a super-spreader node (left), and a complete graph, where any node is a star node.

P3 aims to exclude networks where the infection or outage of a single node may affect all others. Note that P3 also excludes all networks with a star node, which have the additional disadvantage that they themselves may be infected by any other node, and then potentially pass on that infection. Specifically, this rules out any *complete graph* $G^c = (\mathcal{V}_{G^c}, (\mathcal{V}_{G^c} \times \mathcal{V}_{G^c}) \cap \mathbb{E})$, where each node is effectively a star node.

If we do not endow the single nodes $v \in \mathcal{V}_G$ of a network G with a particular meaning, one might identify networks which are structurally equal: Two graphs $G_1 = (\mathcal{V}_1, \mathcal{E}_1)$ and $G_2 = (\mathcal{V}_2, \mathcal{E}_2) \in \mathcal{G}$ are isomorphic if there is a bijection $\pi : \mathcal{V}_1 \to \mathcal{V}_2$ such that

$$(v, w) \in \mathcal{E}_1 \Leftrightarrow (\pi(v), \pi(w)) \in \mathcal{E}_2 \text{ for all } v, w \in \mathcal{V}_1.$$

π is called a *graph isomorphism* of G_1 and G_2.

P4 resembles the concept of distribution-invariant risk measures common in financial economics. Indeed, if graphs are isomorphic, then their degree distributions coincide. Note that in scenarios where network components represent specific entities, some of which may need to be prioritized for protection—such as those belonging to critical infrastructures—topological invariance is not suitable. For instance, topology-invariant acceptance sets may not be appropriate in our motivating example from Section 1.1, where we fundamentally distinguish between TPP and FI nodes.

4 Network Interventions

In this section, we present various types of interventions, beginning with elementary ones. Some of these manipulations have been previously applied in the literature on network risk management; see, for example, [6] and [18] for the case of cyber networks. In [52], edge shifts are evaluated for enhancing the robustness and resilience of air transportation networks. Throughout this section, $G = (\mathcal{V}_G, \mathcal{E}_G) \in \mathcal{G}$ denotes a generic graph.

4.1 Elementary Interventions on Edges and Nodes

$\mathcal{I}_{e\_del}$ *Edge Deletion*: Consider nodes $v, w \in \mathbb{V}$. The intervention

$$\kappa_{e\_del}^{(v,w)} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \setminus \{(v, w)\})$$

deletes the edge (v, w) if present. Indeed $\kappa_{e\_del}^{(v,w)}(G) = G$ if and only if $(v, w) \notin \mathcal{E}_G$. We set

$$\mathcal{I}_{e\_del} := \{\kappa_{e\_del}^{(v,w)} \mid v, w \in \mathbb{V}\}.$$

Operational interpretations of edge deletion for controlling cyber risk are physical deletion of connections, such as access to servers, or, if not possible, edge hardening, i.e., a strong protection of network connections via firewalls, the closing of open ports, or the monitoring of data flows using specific detection systems.

$\mathcal{I}_{e\_add}$ *Edge Addition*: The addition of edge (v, w) for $v, w \in \mathbb{V}$ with $v \neq w$ is given by

$$\kappa_{e\_add}^{(v,w)} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \cup (\{(v, w)\} \cap \mathcal{V}_G \times \mathcal{V}_G)),$$

where $\kappa_{e\_add}^{(v,w)}(G) = G$ is satisfied if either we already have $(v, w) \in \mathcal{E}_G$ or at least one of the nodes v and w is not present in the network G. We set

$$\mathcal{I}_{e\_add} := \{\kappa_{e\_add}^{(v,w)} \mid v, w \in \mathbb{V}\}.$$

Edge addition is, of course, the reverse of edge deletion and comes with the opposite operational meaning. In the context of electrical networks, edge addition may be interpreted as physical addition of power lines between nodes, thereby securing power supply.

$\mathcal{I}_{n\_del}$ *Node Deletion*: The deletion of a node $v \in \mathbb{V}$ is given by the intervention

$$\kappa_{n\_del}^{v} : G \mapsto (\mathcal{V}_G \setminus \{v\}, \mathcal{E}_G \cap (\mathcal{V}_G \setminus \{v\} \times \mathcal{V}_G \setminus \{v\}))$$

where $\kappa_{n\_del}^{v}(G) = G$ if and only if $v \notin \mathcal{V}_G$. We set

$$\mathcal{I}_{n\_del} := \{\kappa_{n\_del}^{v} \mid v \in \mathbb{V}\}.$$

Operationally node deletion corresponds, for instance, to removal of redundant servers or other access points.

$\mathcal{I}_{n\_add}$ *Node Addition*: An (isolated) node $v \in \mathbb{V}$ can be added to a network via

$$\kappa_{n\_add}^{v} : G \mapsto (\mathcal{V}_G \cup \{v\}, \mathcal{E}_G)$$

where $\kappa_{n\_add}^{v}(G) = G$ if and only if we already have $v \in \mathcal{V}_G$. We set

$$\mathcal{I}_{n\_add} := \{\kappa_{n\_add}^{v} \mid v \in \mathbb{V}\}.$$

Node addition, such as adding servers that serve as backups or take over tasks from very central servers, may improve network resilience to the spread of infectious malware when combined with edge addition or edge shifts (see below).

More complex interventions such as discussed in the following can be obtained by a consecutive application of the elementary interventions presented so far.

4.2 Isolation of Network Parts

Critical nodes or subgraphs can be isolated from the rest of the network by application of the following edge deletion procedures:

$\mathcal{I}_{s\_iso}$ *Node/Subgraph Isolation*: We isolate the subgraph $(\mathcal{W} \cap \mathcal{V}_G, \mathcal{E}_G \cap (\mathcal{W} \times \mathcal{W}))$ given by a set $\mathcal{W} \subset \mathbb{V}$ (or a node in case $\mathcal{W} = \{v\}$ for some $v \in \mathbb{V}$) from the rest of the network by

$$\kappa_{iso}^{\mathcal{W}} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \setminus [\mathcal{W} \times (\mathcal{V}_G \setminus \mathcal{W}) \cup (\mathcal{V}_G \setminus \mathcal{W}) \times \mathcal{W}]), \quad \mathcal{I}_{s\_iso} := \{\kappa_{iso}^{\mathcal{W}} \mid \mathcal{W} \subset \mathbb{V}\}.$$

Node or subgraph isolation corresponds to fully protecting that part of the network from the rest.

4.3 Shifting, Diversification and Centralization of Network Connections

Network tasks or data flows can be redistributed among existing nodes by utilizing interventions of the following type:

$\mathcal{I}_{shift}$ *Edge Shift*: If $(v, w) \in \mathcal{E}_G$ and $(q, r) \in \mathbb{E} \setminus \mathcal{E}_G$, $q, r \in \mathcal{V}_G$, then the edge (v, w) can be shifted to (q, r) by

$$\kappa_{shift}^{(v,w),(q,r)} : G \mapsto \begin{cases} (\mathcal{V}_G, \mathcal{E}_G \setminus \{(v, w)\} \cup \{(q, r)\}), & \text{if } (v, w) \in \mathcal{E}_G, q, r \in \mathcal{V}_G, (q, r) \in \mathbb{E} \setminus \mathcal{E}_G \\ G, & \text{else.} \end{cases}$$

We set
$$\mathcal{I}_{shift} := \{\kappa_{shift}^{(v,w),(q,r)} \mid v, w, q, r \in \mathbb{V}\}.$$

Combining node adding and edge shift operations, we can create more complex interventions which aim for risk diversification by separating critical contagion channels that pass through a chosen node v:

$\mathcal{I}_{split}$ *Node Splitting*: The split of a node v by rewiring edges contained in $\mathcal{L} \subset \mathbb{E}$ from v to a newly added node $\tilde{v} \in \mathbb{V}$ is described by

$$\kappa_{split}^{\mathcal{L},v,\tilde{v}} : G \mapsto \begin{cases} (\mathcal{V}_G \cup \{\tilde{v}\}, \mathcal{E}_G \setminus (\mathcal{L} \cap \mathcal{E}_G^v) \cup \tilde{\mathcal{L}}_{\tilde{v}}^G), & \text{if } \tilde{v} \notin \mathcal{V}_G \\ G, & \text{else,} \end{cases}$$

with $\tilde{\mathcal{L}}_{\tilde{v}}^G := \{(\tilde{v}, w) | (v, w) \in \mathcal{L} \cap \mathcal{E}_G\} \cup \{(w, \tilde{v}) | (w, v) \in \mathcal{L} \cap \mathcal{E}_G\}$. A true node splitting only takes place when $\tilde{v} \notin \mathcal{V}_G$ and $\mathcal{L} \cap \mathcal{E}_G^v \neq \emptyset$. Let

$$\mathcal{I}_{split} := \{\kappa_{split}^{\mathcal{L},v,\tilde{v}} \mid v, \tilde{v} \in \mathbb{V}, \mathcal{L} \subset \mathbb{E}\}.$$

Note that node splitting enters the practical discussion when, for instance, a required diversification of (outsourcing) service providers is considered by the regulator. In view of the motivating example from Section 1.1 such an intervention could reduce the impact of an outage or infection of a TTP to the financial system.
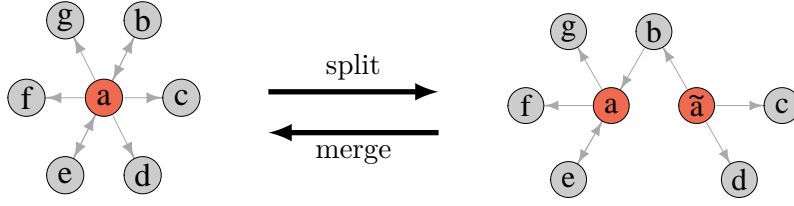
Figure 3: Splitting (left to right) and merging (right to left) as mutually reverse operations. Targeted nodes are coloured in red.

Node splits can be reversed by *merging* nodes v and $\tilde{v}$. This operation corresponds to a centralization of network connections, the formalism is left to the reader.

Creating node copies has an obvious practical interpretation as installing backups:

$\mathcal{I}_{n\_copy}$ *Node Copying:* A node $v \in \mathcal{V}_G$ can be copied by

$$\kappa_{copy}^{v,w} : G \mapsto \begin{cases} (\mathcal{V}_G \cup \{w\}, \mathcal{E}_G \cup \{(u,w)|(u,v) \in \mathcal{E}_G\} \cup \{(w,u)|(v,u) \in \mathcal{E}_G\}), & \text{if } v \in \mathcal{V}_G, w \notin \mathcal{V}_G \\ G, & \text{else.} \end{cases}$$

Note that a copy of node v can be stored at node w only if $v \in \mathcal{V}_G$ and $w \notin \mathcal{V}_G$. We set

$$\mathcal{I}_{n\_copy} := \{\kappa_{copy}^{v,w} \mid v, w \in \mathbb{V}\}.$$

5 Cost Functions

The following two types of cost functions appear naturally:

1. A quantification of the *monetary* cost of transforming a graph G into $H \in \sigma^{\mathcal{I}}(G)$, see Section 5.1.

2. A quantification of the cost of transforming a graph G into $H \in \sigma^{\mathcal{I}}(G)$ in terms of the corresponding *impact on network functionality*, see Section 5.2.

In the case studies in Sections 5.1 and 5.2 we will also consider further properties of a cost function which we introduce next. To this end, let $\mathcal{A}$ be an acceptance set, $\mathcal{I}$ be a set of risk reducing interventions for $\mathcal{A}$, and suppose that $\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I})$.

C3 Every non-trivial network intervention comes at a real cost, i.e.,

$$\mathcal{C}(G, H) = 0 \Rightarrow G = H \text{ for all } H, G \in \mathcal{G}.$$

C4 The absolute cost of a direct transformation of G to H should not be more expensive than first transforming to an intermediate configuration M, i.e., for all $G, H, M \in \mathcal{G}$ such that $M \in \sigma^{\mathcal{I}}(G)$, and $H \in \sigma^{\mathcal{I}}(M)$ we have

$$\mathcal{C}(G, H) \leq \mathcal{C}(G, M) + \mathcal{C}(M, H).$$

16

5.1 Monetary Cost Functions

Consider any acceptance set $\mathcal{A} \subset \mathcal{G}$ and a set of interventions $\mathcal{I}$ that is risk-reducing for $\mathcal{A}$. In the following, we illustrate monetary cost functions by presenting an example of a cost function constructed based on the costs of the basic interventions $\kappa \in \mathcal{I}$. These costs are assumed to be initially given.

Suppose we associate an initial cost $\tilde{p}(\kappa) \in [0, \infty)$ with each $\kappa \in \mathcal{I}$ and let $\tilde{p}(\mathrm{id}) = 0$. For any $\mathcal{I}$-strategy κ set

$$p(\kappa) := \inf \left\{ \sum_{i=1}^{n} \tilde{p}(\kappa_i) \mid \kappa = \kappa_n \circ \cdots \circ \kappa_1, \kappa_i \in \mathcal{I}, i = 1, \ldots, n, n \in \mathbb{N} \right\}. \tag{2}$$

Then consider the minimal total cost for the transformation of G into H:

$$\mathcal{C}(G, H) := \inf\{p(\kappa) \mid \kappa \in [\mathcal{I}], \kappa(G) = H\}, \quad \inf \emptyset := \infty. \tag{3}$$

Note that p conincides with $\tilde{p}$ on $\mathcal{I}$ if and only if $\tilde{p}$ is *consistent*, that is if $\kappa \in \mathcal{I}$ satisfies $\kappa = \kappa_n \circ \cdots \circ \kappa_1$ for some interventions $\kappa_i \in \mathcal{I}$, $i = 1, \ldots, n$, $n \in \mathbb{N}$, we must have $\tilde{p}(\kappa) = \sum_{i=1}^{n} \tilde{p}(\kappa_i)$. Of course, consistency of $\tilde{p}$ on $\mathcal{I}$ is automatically satisfied in case that $\kappa = \kappa_n \circ \cdots \circ \kappa_1$ for some $\kappa, \kappa_1, \ldots, \kappa_n \in \mathcal{I}$ implies that $\kappa_j = \kappa$ for some $j \in \{1, \ldots, n\}$ and $\kappa_i = \mathrm{id}$ for all $i \neq j$. The following lemma is easily verified.

Lemma 5.1. *p is subadditive in the sense that for all $\kappa, \alpha \in [\mathcal{I}]$ we have $p(\kappa \circ \alpha) \leq p(\kappa) + p(\alpha)$.*

Proposition 5.2. *Suppose that $\mathcal{C}$ is given by (3). Then:*

1. *$\mathcal{C}(G, H) < \infty$ if and only if $H \in \sigma^{\mathcal{I}}(G)$.*

2. *$\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I})$ which satisfies C4.*

3. *Further suppose that $\inf\{\tilde{p}(\kappa) \mid \kappa \in \mathcal{I} \setminus \{\mathrm{id}\}\} > 0$, then C3 is satisfied.*

4. *Moreover, if $\mathcal{I}$ is finite and $\tilde{p}(\kappa) > 0$ for all $\kappa \in \mathcal{I}$ such that $\kappa \neq \mathrm{id}$, then the infimum in (3) is attained whenever $H \in \sigma^{\mathcal{I}}(G)$. In other words, if $H \in \sigma^{\mathcal{I}}(G)$, then there are optimal $\mathcal{I}$-strategies κ for transforming G into H in the sense that $\kappa(G) = H$ and $p(\kappa) = \mathcal{C}(G, H)$.*

Proof. 1. is obvious.

2. $\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I})$ which satisfies C4: C1 follows from $p(\mathrm{id}) = 0$, whereas C2 is implied by $\tilde{p}(\kappa) \geq 0$ for each $\kappa \in \mathcal{I}$. As for C4 consider $G, M, H \in \mathcal{G}$ and suppose that there is $\kappa, \alpha \in [\mathcal{I}]$ with $\alpha(G) = M$ and $\kappa(M) = H$. Then $\kappa \circ \alpha(G) = H$, and by Lemma 5.1 above we have that $\mathcal{C}(G, H) \leq \mathcal{C}(G, M) + \mathcal{C}(M, H)$.

3. Clearly, if $\nu := \inf\{p(\kappa) \mid \kappa \in \mathcal{I} \setminus \{\mathrm{id}\}\} > 0$, then $p(\kappa) > \nu$ for all $\kappa \in [\mathcal{I}^{\downarrow}]$ such that $\kappa \neq \mathrm{id}$. Hence, $\mathcal{C}(G, H) = 0$ is only possible if $H = G$.

4. In order to show that there are optimal $\mathcal{I}$-strategies in case $H \in \sigma^{\mathcal{I}}(G)$, pick any $\kappa \in [\mathcal{I}]$ such that $\kappa(G) = H$. Note that $\nu = \min\{\tilde{p}(\kappa) \mid \kappa \in \mathcal{I} \setminus \{\mathrm{id}\}\} > 0$, and

let $m \in \mathbb{N}$ be such that $m\nu > p(\kappa)$. Denote by $[\mathcal{I}]_m$ the set of all $\mathcal{I}$-strategies which allow for a decomposition $\alpha = \alpha_k \circ \ldots \alpha_1$ where $\alpha_1, \ldots, \alpha_k \in \mathcal{I}$ and $k \leq m$. Note that $p(\alpha) \geq m\nu > p(\kappa)$ for all $\alpha \in [\mathcal{I}] \setminus [\mathcal{I}]_m$. Therefore, it follows that

$$\mathcal{C}(G, H) = \inf\{p(\alpha) \mid \alpha \in [\mathcal{I}]_m, \alpha(G) = H\}.$$

Now the assertion follows from $[\mathcal{I}] \setminus [\mathcal{I}]_m$ being a finite set. $\qquad \square$

5.2 Examples of Cost Functions based on Loss of Network Functionality

In this section we consider cost functions which quantify the difference in functionality $\mathcal{F} : \mathcal{G} \to \mathbb{R}$ between two networks:

$$\mathcal{C}(G, H) = h(\mathcal{F}(G) - \mathcal{F}(H)) \tag{4}$$

where $h : \mathbb{R} \to \mathbb{R}$. Note that the Properties *C1* and *C4* solely depend on the choice of h, and one easily verifies the following result:

Lemma 5.3. *Consider a cost function of type* (4). *Then*

1. *Property C1 is satisfied if and only if $h(0) = 0$.*

2. *If h is sub-additive, then C4 holds.*

Network functionality is typically measured by considering the average node distance within the network: A smaller average value corresponds to a faster or more efficient data flow. In following we recall two common concepts to define the distance between nodes. To this end, we refer the reader not familiar with basic notions for graphs such as paths and adjacency matrices to Appendix A.

- *Shortest path length:* Given two nodes v and w in a network G, we denote by l_{vw}^G the length of a path from node v to w that passes through a minimum number of edges. If there is no path from v to w, then we set $l_{vw}^G = \min \emptyset := \infty$. However, note that it has been emphasized, see e.g. [30], that considering shortest paths only provides an incomplete picture of the flow of information, data, or goods in a network since that may take place through many different routes.

- *Communicability:* Compared to shortest path length, *communicability* attempts to provide a more holistic view of the communication channels between nodes. Consider a graph G of size N with enumerated vertices $v_1, \ldots, v_N$. The communicability $\mathfrak{c}_{v_i v_j}^G$ between nodes v_i and v_j is defined as the (i, j)-th entry of the matrix exponential e^{A_G} of the adjacency matrix A_G, i.e.,

$$\mathfrak{c}_{v_i v_j}^G := \sum_{k=0}^{\infty} \frac{(A_G^k)(i,j)}{k!} = e^{A_G}(i, j), \text{ where } e^{A_G} := I_N + A_G + \frac{A_G^2}{2!} + \frac{A_G^3}{3!} + \cdots = \sum_{k=0}^{\infty} \frac{A_G^k}{k!}$$

and I_N is the identity matrix in $\mathbb{R}^{N \times N}$. Note that $A_G^k(i, j)$ gives the number of walks of length k from node v_i to v_j, and therefore $\mathfrak{c}_{v_i v_j}^G$ is a weighted sum of all walks from v_i to v_j.

5.2.1 Functionality Based on Shortest Paths

A global measure of network functionality based on shortest paths is given by the *graph efficiency* as defined in [51]:

$$\mathcal{F}(G) = \frac{1}{|\mathcal{V}_G|(|\mathcal{V}_G| - 1)} \sum_{v,w,v \neq w} \frac{1}{l_{vw}^G} \qquad \left(\frac{1}{\infty} := 0\right). \tag{5}$$

Proposition 5.4. *Consider an acceptance set $\mathcal{A}$ and a set of admissible interventions $\mathcal{I}$ which is risk-reducing for $\mathcal{A}$ such that $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso}$. Then $\mathcal{C}$ given by (4) and (5) and a strictly increasing function h with $h(0) = 0$ is a cost function for $(\mathcal{A}, \mathcal{I})$. Moreover, $\mathcal{C}$ satisfies the following constrained version of C3:*

$$\forall G \in \mathcal{G}, \forall H \in \sigma^{\mathcal{I}}(G): \quad \mathcal{C}(G, H) = 0 \Rightarrow G = H. \tag{6}$$

Proof. C1 follows from $h(0) = 0$. In order to prove *C2* and (6), we show that $\mathcal{F}(G)$ is non-increasing whenever we apply a intervention in $\mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso}$ to G, and even strictly decreasing if the intervention alters G. As a consequence, for all $\kappa \in [\mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso}]$, and thus for all $\kappa \in [\mathcal{I}]$, we obtain that $\mathcal{F}(\kappa(G)) \leq \mathcal{F}(G)$, which implies $h(\mathcal{F}(G) - \mathcal{F}(\kappa(G))) \geq h(0) = 0$, demonstrating *C2*. Additionally, $\mathcal{F}(\kappa(G)) < \mathcal{F}(G)$ when $\kappa(G) \neq G$, implying $h(\mathcal{F}(G) - \mathcal{F}(\kappa(G))) > h(0) = 0$, which corresponds to (6).

Let us first consider edge deletions: Fix $G \in \mathcal{G}$ and delete an edge $(q, r) \in \mathbb{E}$. Let $\tilde{G} := \kappa_{e\_del}^{(q,r)}(G)$. The deletion of the edge (q, r) does not create any new paths, and therefore $l_{vw}^G \leq l_{vw}^{\tilde{G}}$ for all nodes $v, w \in \mathcal{V}_G$. Moreover, if $(q, r) \in \mathcal{E}_G$, then we necessarily have $l_{qr}^G < l_{qr}^{\tilde{G}}$, i.e., there is at least one node pair where the inequality is strict. We thus obtain $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$ for all networks $G \in \mathcal{G}$ and $(q, r) \in \mathbb{E}$, and "=" holds exactly when we have $(q, r) \notin \mathcal{E}_G$, i.e., if and only if $\tilde{G} = G$.

Note that the isolation of a subgraph, that is $\tilde{G} := \kappa_{iso}^{\mathcal{W}}(G)$ where $\mathcal{W} \subset \mathbb{V}$, is a sequence of edge deletions, namely deleting all edges connecting nodes in $\mathcal{V}_G \setminus \mathcal{W}$ with some node in $\mathcal{W}$. Hence, also in this case we obtain $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$, and "=" holds exactly when $v \notin \mathcal{V}_G$ for all $v \in \mathcal{W}$ or when the subgraph given by the nodes $\mathcal{W} \cap \mathcal{V}_G$ is already in G, i.e., if and only if $\tilde{G} = G$. $\qquad \square$

However, measuring network functionality in terms of shortest paths may come with some difficulties when allowing for $\mathcal{I}_{n\_split} \subseteq \mathcal{I}$ as is illustrated by the following example.

Example 5.5. *Let H be the result of a node split in a network G of size N. For $\mathcal{F}$ to be monotonically decreasing under this intervention, the shortest path lengths in H must satisfy:*

$$\frac{N-1}{N+1} \sum_{v,w \in \mathcal{V}_H, v \neq w} \frac{1}{l_{vw}^H} \leq \sum_{v,w \in \mathcal{V}_G, v \neq w} \frac{1}{l_{vw}^G}. \tag{7}$$

Consider a graph $G = G_1 \cup G_2$ consisting of two components, where G_1 is as shown in Figure 4, and G_2 is a graph of $N - 3$ isolated nodes such that $\mathcal{V}_{G_1} \cap \mathcal{V}_{G_2} = \emptyset$. Assume node $b \in \mathcal{V}_{G_1}$ is split as in Figure 4, transforming G_1 into H_1.

Figure 4: Node b is split by adding node $\tilde{b} \notin \mathcal{V}_G$ and replacing edges $\{(b,c),(c,b)\}$ with $\{(\tilde{b},c),(c,\tilde{b})\}$.

We obtain:

$$\sum_{v,w \in \mathcal{V}_{H_1}, v \neq w} \frac{1}{l_{vw}^{H_1}} = 2 \cdot \left(1 + 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + 1\right) = \sum_{v,w \in \mathcal{V}_{G_1}, v \neq w} \frac{1}{l_{vw}^{G_1}} + \frac{8}{3},$$

and since G_1 and G_2 are not connected, we have:

$$\sum_{v,w \in \mathcal{V}_H, v \neq w} \frac{1}{l_{vw}^H} = \sum_{v,w \in \mathcal{V}_{H_1}, v \neq w} \frac{1}{l_{vw}^{H_1}}, \qquad \sum_{v,w \in \mathcal{V}_G, v \neq w} \frac{1}{l_{vw}^G} = \sum_{v,w \in \mathcal{V}_{G_1}, v \neq w} \frac{1}{l_{vw}^{G_1}}.$$

Thus, (7) becomes:

$$\frac{N-1}{N+1}\left(\sum_{v,w \in \mathcal{V}_G, v \neq w} \frac{1}{l_{vw}^G} + \frac{8}{3}\right) \leq \sum_{v,w \in \mathcal{V}_G, v \neq w} \frac{1}{l_{vw}^G}.$$

This inequality is violated when N is large enough, which can be achieved by increasing the size of G_2. Hence, if $h : \mathbb{R} \to \mathbb{R}$ is strictly increasing with $h(0) = 0$, condition C2 is not satisfied.

5.2.2 Functionality Based on Network Communicability

Taking the average over all the communicabilities yields the global measure

$$\mathcal{F}(G) = \frac{1}{|\mathcal{V}_G|^2} \sum_{v,w} \mathfrak{c}_{vw}^G \tag{8}$$

for a network G. In contrast to shortest paths, it may be useful to include self-communicabilities, that are entities $\mathfrak{c}_{vv}$, into the consideration since walks of from a node to itself correspond to closed communication loops. Basing the cost function on communicability we do not only satisfy *C2* in case of edge deletions, but—in contrast to shortest path based costs—also when risk-reduction is achieved by node splitting.

Proposition 5.6. *Consider an acceptance set $\mathcal{A}$ and a set of admissible interventions $\mathcal{I}$ which is risk-reducing for $\mathcal{A}$ such that $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$. Then $\mathcal{C}$ given by (4) and (8) and a strictly increasing function h with $h(0) = 0$ is a cost function for $(\mathcal{A}, \mathcal{I})$ which satisfies (6).*

Proof. *C1* follows from $h(0) = 0$. As in the proof of Proposition 5.4 we prove *C2* and (6) by showing that $\mathcal{F}(G)$ is non-increasing whenever we apply a intervention in $\mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$ to G, and even strictly decreasing if the intervention alters G.

Let $G \in \mathcal{G}$ with adjacency matrix A_G, given some enumeration of the nodes $\mathcal{V}_G$. Let us first consider edge deletions. To this end, let $\tilde{G} = \kappa_{e\_del}^{(v_i, v_j)}(G)$ where $v_i, v_j \in \mathcal{V}_G$. If $(v_i, v_j) \in \mathcal{E}_G$, then $A_{\tilde{G}}(i, j) < A_G(i, j)$, and indeed $A_{\tilde{G}}^k(l, m) < A_G^k(l, m)$ for every $k \geq 1$ and l, m such that (v_i, v_j) is element of a walk of length k from v_l to v_m. Hence, $\mathfrak{c}_{vw}^{\tilde{G}} < \mathfrak{c}_{vw}^G$ for all $v, w \in \mathcal{V}_G$ where (v_i, v_j) lies on a walk from v to w, yielding $\mathcal{F}(\tilde{G}) < \mathcal{F}(G)$. Therefore, we conclude that $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$ and $\mathcal{F}(\tilde{G}) = \mathcal{F}(G)$ if and only if $G = \tilde{G}$. Conversely, if $\tilde{G}$ is obtained by adding an edge to the network G, and thus G is obtained by an edge deletion in $\tilde{G}$, the previous arguments show that $\mathfrak{c}_{vw}^{\tilde{G}} > \mathfrak{c}_{vw}^G$, and thus $\mathcal{F}(\tilde{G}) > \mathcal{F}(G)$ unless $G = \tilde{G}$.

Next let us consider node splittings. If $\tilde{G}$ results from a node splitting intervention in G, then, conversely, G can be obtained by a node merging intervention in $\tilde{G}$. Therefore, it suffices to prove that $\mathcal{F}$ is increasing under node merging. So let $G = \kappa_{merge}^{v_i, v_j}(\tilde{G})$ be the graph obtained after merging two nodes $v_i, v_j \in \mathcal{V}_{\tilde{G}}$ in a network $\tilde{G}$ of size N. In case this merge operation is non-trivial, that is $G \neq \tilde{G}$, assuming $i < j$, this intervention can be described by a matrix operation on the adjacency matrix $A_{\tilde{G}}$, i.e., $A_G = \hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T$ with $\hat{M} \in \{0, 1\}^{(N-1) \times N}$ defined as

$$\hat{M}(l, m) = \begin{cases} 1, & \text{for } l = m < j \\ 1, & \text{for } l = i, m = j \\ 1, & \text{for } j \leq l \leq N - 1, m = l + 1 \\ 0, & \text{else.} \end{cases}$$

One verifies that the product $\hat{M}^T \hat{M}$ equals 1 on the diagonal. Let $I_N \in \mathbb{R}^{N \times N}$ denote the identity matrix. Then it follows that $\hat{M}^T \hat{M} \geq I_N$ in the sense that componentwise we have $(\hat{M}^T \hat{M})(l, m) \geq I_N(l, m)$ for all $l, m = 1, \ldots, N$. Since all entries in $A_{\tilde{G}}$ are non-negative we estimate

$$\begin{aligned} (A_G)^k &= (\hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T)^k \\ &= \hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T \cdot \hat{M} \cdot A_{\tilde{G}} \cdot \hat{M}^T \cdot \hat{M} \cdot A_{\tilde{G}} \cdots A_{\tilde{G}} \hat{M}^T \\ &\geq \hat{M} \cdot A_{\tilde{G}} \cdot I_N \cdot A_{\tilde{G}} \cdot I_N \cdot A_{\tilde{G}} \cdots A_{\tilde{G}} \hat{M}^T \\ &= \hat{M} \cdot (A_{\tilde{G}})^k \cdot \hat{M}^T. \end{aligned}$$

Thus we obtain

$$\sum_{l=1}^{N-1} \sum_{m=1}^{N-1} (A_G)^k(l, m) \geq \sum_{l=1}^{N-1} \sum_{m=1}^{N-1} (\hat{M} \cdot (A_{\tilde{G}})^k \cdot \hat{M}^T)(l, m) = \sum_{l=1}^{N} \sum_{m=1}^{N} (A_{\tilde{G}})^k(l, m)$$

for all $l, m = 1, \cdots, N$, and therefore

$$\sum_{v_i, v_j \in \mathcal{V}_G} \mathfrak{c}_{v_i v_j}^G \geq \sum_{v_i, v_j \in \mathcal{V}_{\tilde{G}}} \mathfrak{c}_{v_i v_j}^{\tilde{G}} \tag{9}$$

for the sum of all communicabilities. Further, since $\tilde{G}$ is larger than G, this yields strict inequality when taking the average value, i.e., $\mathcal{F}(\tilde{G}) < \mathcal{F}(G)$. Therefore, we conclude that $\mathcal{F}(\tilde{G}) \leq \mathcal{F}(G)$ for all $\tilde{G}$ obtained by performing a node splitting on G, and $\mathcal{F}(\tilde{G}) = \mathcal{F}(G)$ if and only if $G = \tilde{G}$

$\square$

Remark 5.7. *Note that we find ">" in* (9) *if and only if there is a matrix entry* (l, m) *with* $A_{\tilde{G}}\hat{M}^T\hat{M}A_{\tilde{G}}(l, m) > A_{\tilde{G}}I_N A_{\tilde{G}}(l, m)$, *which means that*

$$A_{\tilde{G}}\hat{M}^T\hat{M}A_{\tilde{G}}(l, m) = \sum_{p=1}^{N}\sum_{o=1}^{N} A_{\tilde{G}}(l, o)\hat{M}^T\hat{M}(o, p)A_{\tilde{G}}(p, m) > \sum_{o=1}^{N} A_{\tilde{G}}(l, o)A_{\tilde{G}}(o, m).$$

This is the case if and only if $A_{\tilde{G}}(l, i) > 0$ *and* $A_{\tilde{G}}(j, m) > 0$, *or* $A_{\tilde{G}}(l, j) > 0$ *and* $A_{\tilde{G}}(i, m) > 0$, *which means that* $\mathcal{N}_{v_i}^{\tilde{G},in}, \mathcal{N}_{v_j}^{\tilde{G},out} \neq \emptyset$, *or* $\mathcal{N}_{v_i}^{\tilde{G},out}, \mathcal{N}_{v_j}^{\tilde{G},in} \neq \emptyset$. *In other words, a node split reduces some communicabilities in a network if and only if the split corresponds to an actual separation of contagion channels.*

6 Examples

The examples presented in this section will all be based on network acceptance sets $\mathcal{A}$ of the form

$$\mathcal{A} = \{G \in \mathcal{G} \mid Q(G) \leq l_{|\mathcal{V}_G|}\}, \tag{10}$$

where a specific network quantity $Q : \mathcal{G} \to \mathbb{R} \cup \{-\infty, \infty\}$ needs to be bounded for acceptability of a network G, and the bounds $l_N \in \mathbb{R}$, $N \in \mathbb{N}$, may depend on the network size N.

Definition 6.1. *Let* $\mathcal{I}$ *be a non-empty set of network interventions and let* $Q : \mathcal{G} \to \mathbb{R} \cup \{-\infty, \infty\}$. *We call* Q $\mathcal{I}$-*monotone if* $Q(\kappa(G)) \leq Q(G)$ *for all* $G \in \mathcal{G}$ *and* $\kappa \in \mathcal{I}$.

The following lemma is easily verified.

Lemma 6.2. *Suppose that* Q *is* $\mathcal{I}$-*monotone. Then*

1. *$Q(\kappa(G)) \leq Q(G)$ for all $G \in \mathcal{G}$ and $\kappa \in [\mathcal{I}]$,*

2. *$\mathcal{I}$ is risk-reducing for $\mathcal{A}$.*

If, moreover, $\mathcal{I}$ *is not partially self-revers, then* $\mathcal{I}$-*monotonicity is the same as* Q *being decreasing with respect to the partial order* $\preccurlyeq_{\mathcal{I}}$ *given in Lemma 2.7.*

6.1 DMFNR Based on Moments of the Degree Distribution

In this section we consider examples of the function Q in (10) depending on moments of the degree distribution. To this end, we write $k_v^{G,in} = |\mathcal{N}_v^{G,in}|$ and $k_v^{G,out} = |\mathcal{N}_v^{G,out}|$ for the in- and out-degrees of nodes $v \in \mathcal{V}_G$, see also Section A.2. Given a network $G \in \mathcal{G}$, we let $P_G^{out}(k)$ denote the fraction of nodes v with out-degree k, or, equivalently, the

probability that a node v which is chosen uniformly at random comes with out-degree k. The corresponding distribution P_G^{out} over all possible out-degrees is called the *out-degree distribution* of the network G. Analogously, we can define the *in-degree distribution* P_G^{in}. Let K_G^{out} denote a random variable which represents the out-degree of a randomly chosen node given the probability distribution P_G^{out}, i.e. $\mathbb{P}(K_G^{out} = k) = P_G^{out}(k)$ for all $k = 0, 1, \ldots, |\mathcal{V}_G| - 1$. We define K_G^{in} analogously. The *n-th moment* of the in- and out-degree distributions are given by

$$\mathbb{E}[(K_G^{in})^n] := \sum_{k \in \mathbb{N}_0} k^n P_G^{in}(k), \quad \mathbb{E}[(K_G^{out})^n] := \sum_{k \in \mathbb{N}_0} k^n P_G^{out}(k), \quad n \in \mathbb{N}.$$

Clearly any network acceptance set such that Q only depends on the degree distribution is topological invariant:

Lemma 6.3. *If $\mathcal{A}$ is given by* (10) *where Q only depends on the in-, out-degree distribution, then $\mathcal{A}$ satisfies P4.*

Remark 6.4. *As regards in- and out-degree distributions, note that the following examples indicate that for the management of systemic cyber risk, the distribution of outgoing, not incoming, node degrees is the relevant entity.*

6.1.1 Variance of Degree Distributions

Obviously, not all functions Q based on moments of node degrees are suited risk controls. Indeed, in the following we show that the variance of either in- or out-degree distributions is not a satisfactory control.

Proposition 6.5. *Suppose that the network acceptance set $\mathcal{A}$ satisfies* (10) *where Q equals the variance of either the in- or out-degree distribution, and that $l_N \geq 0$ for all $N \in \mathbb{N}$. In both cases, $\mathcal{A}$ satisfies P1, but violates P3. Moreover, Q is not $\mathcal{I}$-monotone for any choice of $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{e\_add} \cup \mathcal{I}_{n\_del} \cup \mathcal{I}_{n\_add}$ such that $\mathcal{I} \neq \emptyset$, that is for no non-trivial set of elementary network interventions.*

Proof. The in- and out-degree distributions of all edgeless and all complete graphs have zero variance. Thus, P1 is always satisfied while P3 is violated.

As regards the monotonicity of Q, variance, of either the in- our out-degree distribution, increases by adding edges to the edgeless graph, or by deleting edges in the complete graph. Moreover, the variance of a complete graph increases when adding an isolated node to the network. As regards node deletion, note that any circular graph given by $\mathcal{V}_{G^\circ} = \{v_1, \cdots, v_N\}$ and

$$\mathcal{E}_{G^\circ} = \{(v_1, v_2), (v_2, v_1), \cdots, (v_{N-1}, v_N), (v_N, v_{N-1}), (v_N, v_1), (v_1, v_N)\},$$

see Figure 5, comes with zero variance for both in- and out-degree distributions since each node has the in- and out-degree 2. However, when deleting node v_N, the network equals the undirected line graph, see Figure 5, with vertex set $\{v_1, \cdots, v_{N-1}\}$ and edges

$$\{(v_1, v_2), (v_2, v_1), \cdots, (v_{N-2}, v_{N-1}), (v_{N-1}, v_{N-2})\}.$$

If $N \geq 4$, in contrast to all the other nodes, v_1 and v_{N-1} only have one incoming and one outgoing edge. Therefore, the variance of both the in- and out-degree distribution now is positive. $\qquad\square$
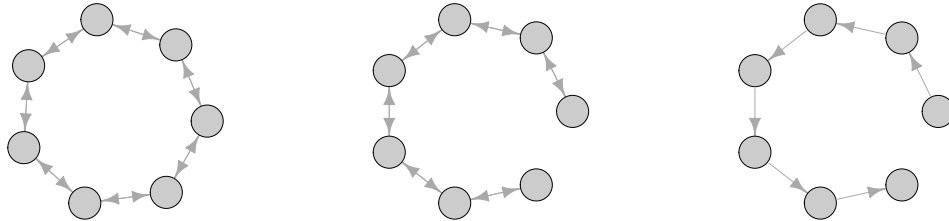

Figure 5: An undirected ring graph (left), an undirected line graph (middle), and a directed line graph (right), all consisting of $N = 7$ nodes.

6.1.2 Average Degrees

Next we consider the *average in-* and *-out degree* of a network G. Note that these first moments are equal since every edge that emanates from a node v needs to arrive at another one, that is we have

$$\mathbb{E}\big[K_G^{in}\big] = \frac{1}{N} \sum_{i=1}^{N} k_{v_i}^{G,in} = \frac{|\mathcal{E}_G|}{|\mathcal{V}_G|} = \frac{1}{N} \sum_{i=1}^{N} k_{v_i}^{G,out} = \mathbb{E}\big[K_G^{out}\big]. \tag{11}$$

Proposition 6.6. *Consider $\mathcal{A}$ as in (10) with $Q(G) = \mathbb{E}\big[K_G^{out}\big](= \mathbb{E}\big[K_G^{in}\big])$. Then Q is $\mathcal{I}$-monotone for any $\mathcal{I}$ that is composed of edge deletions and node splittings, i.e. $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$. Hence, $\mathcal{I}$ is risk-reducing for $\mathcal{A}$ whenever $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$.*

Proof. The result follows directly from Equation (11): For any $\kappa \in \mathcal{I}_{e\_del}$ and network G we have that $|\mathcal{V}_{\kappa(G)}| = |\mathcal{V}_G|$ and $|\mathcal{E}_{\kappa(G)}| \leq |\mathcal{E}_G|$. In case of node splittings $\kappa \in \mathcal{I}_{split}$ we have $|\mathcal{E}_{\kappa(G)}| = |\mathcal{E}_G|$ and $|\mathcal{V}_{\kappa(G)}| \geq |\mathcal{V}_G|$. $\qquad\square$

Corollary 6.7. *Suppose that $\mathcal{I}$ is non-empty and satisfies $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$, and suppose that $l_{N_0} \geq 0$ for some $N_0 \in \mathbb{N}$. Then, $\mathcal{A}$ given in (10) with $Q(G) = \mathbb{E}\big[K_G^{out}\big]$ is a topology invariant network acceptance set. $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR for any cost function $\mathcal{C}$ for $(\mathcal{A}, \mathcal{I})$.*

Proof. Combine Proposition 6.6 with Lemma 6.3. Note that $l_{N_0} \geq 0$ for some $N_0 \in \mathbb{N}$ ensures that $\mathcal{A}$ is non-empty. $\qquad\square$

Remark 6.8. *Propositions 5.4 and 5.6 show how, apart from monetary costs, the cost function $\mathcal{C}$ in Proposition 6.6 can be based on a loss of network functionality. Communicability-based costs work for any choice of $\mathcal{I}$ as in Proposition 6.6, whereas costs based on shortest paths require a further restriction of $\mathcal{I}$ to be a subset of $\mathcal{I}_{e\_del}$.*

Proposition 6.9. *The acceptance set $\mathcal{A}$ as in (10) with $Q(G) = \mathbb{E}[K_G^{out}](= \mathbb{E}[K_G^{in}])$ cannot satisfy P2 and P3 simultaneously. More precisely, if P2 is satisfied, then P3 is violated, and vice versa.*

For the following and later proofs the notion of a *directed star graph* will be important: $G^* = (\mathcal{V}_{G^*}, \mathcal{E}_{G^*})$ is a directed star graph with super-spreader v^* if $\emptyset \neq \mathcal{V}_{G^*} \subset \mathbb{V}$ and

$$\mathcal{E}_{G^*} = \{(v^*, w) \mid w \in \mathcal{V}_{G^*} \setminus \{v^*\}\}.$$

Proof. Let G be a weakly connected network of size N. Consider the undirected version of G given by $\tilde{G} = (\mathcal{V}_G, \mathcal{E}_{\tilde{G}})$ with $\mathcal{E}_{\tilde{G}} = \{(v, w) | (v, w) \in \mathcal{E}_G \text{ or } (w, v) \in \mathcal{E}_G\}$. By definition, we have $|\mathcal{E}_G| \geq |\mathcal{E}_{\tilde{G}}|/2$, and $\tilde{G}$ is strongly connected. The latter implies that $|\mathcal{E}_{\tilde{G}}| \geq 2(N - 1)$ since $\tilde{G}$ must contain an undirected spanning tree, and every undirected tree graph of size N contains $2(N-1)$ directed edges, see [13, Corollary 7 and 8]. This yields $|\mathcal{E}_G| \geq N - 1$, and thus $Q(G) \geq (N - 1)/N$. Now consider a directed star graph G^* of size N. G^* only contains $|\mathcal{V}_{G^*} \setminus \{v^*\}| = N - 1$ edges, thus $Q(G^*) = (N - 1)/N$. Therefore, if a weakly connected network is acceptable, then the directed star graph of the same size is also acceptable. The latter constitutes a violation of P3. Conversely, if P3 is satisfied, so in particular no directed star graph is acceptable, then we cannot have any acceptable weakly connected graph. $\square$

Remark 6.10. *The average node degree only provides a measure of overall graph connectivity in the mean, considering the number of edges in comparison to the number of nodes. However, it does not evaluate characteristics which relate closer to the topological arrangement of edges within the network, that is for example the presence hubs which may act as risk amplifiers. Networks can have a very different risk profile, even if they contain the same number of edges and nodes, see for example the analysis in [6]. Hence, one may doubt whether acceptance sets given by $Q(G) = \mathbb{E}[K_G^{out}](= \mathbb{E}[K_G^{in}])$ are reasonable choices. In that respect, Proposition 6.9 shows that if $Q(G) = \mathbb{E}[K_G^{out}]$, $\mathcal{A}$ cannot satisfy P2 and P3 simultaneously.*

6.1.3 Second In- and Out-Moments

Proposition 6.11. *Consider $\mathcal{A}$ as in (10) with $Q(G) = \mathbb{E}[(K_G^{out})^2]$ or $Q(G) = \mathbb{E}[(K_G^{in})^2]$. Then Q is $\mathcal{I}$-monotone for any $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$.*

Proof. Clearly, the second moments are reduced when deleting edges in a network. Further, the second moment of the in- or out-degree distribution is also decreasing under node splitting: Let v be the node in a network G of size N which is split into v and $\tilde{v}$, and $\tilde{G}$ the resulting network. Due to $k_v^{G,in} = k_v^{\tilde{G},in} + k_{\tilde{v}}^{\tilde{G},in}$ and $k_v^{G,out} = k_v^{\tilde{G},out} + k_{\tilde{v}}^{\tilde{G},out}$, we have

$$(k_v^{\tilde{G},in})^2 + (k_{\tilde{v}}^{\tilde{G},in})^2 \leq (k_v^{\tilde{G},in})^2 + (k_{\tilde{v}}^{\tilde{G},in})^2 + 2k_v^{\tilde{G},in}k_{\tilde{v}}^{\tilde{G},in} = (k_v^{\tilde{G},in} + k_{\tilde{v}}^{\tilde{G},in})^2 = (k_v^{G,in})^2, \quad (12)$$

and thus

$$\mathbb{E}[(K_{\tilde{G}}^{in})^2] = \frac{1}{N+1} \Big(\sum_{w \neq v, \tilde{v}} (k_w^{\tilde{G},in})^2 + (k_v^{\tilde{G},in})^2 + (k_{\tilde{v}}^{\tilde{G},in})^2 \Big)$$

$$\leq \frac{1}{N} \Big(\sum_{w \neq v, \tilde{v}} (k_w^{\tilde{G},in})^2 + (k_v^{G,in})^2 \Big) = \frac{1}{N} \Big(\sum_{w \neq v, \tilde{v}} (k_w^{G,in})^2 + (k_v^{G,in})^2 \Big) = \mathbb{E}[(K_G^{in})^2].$$

$\square$

Corollary 6.12. *Let $\mathcal{A}$ be given by (10) with $Q(G) = \mathbb{E}[(K_G^{out})^2]$ or $Q(G) = \mathbb{E}[(K_G^{in})^2]$ and let $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$ be non-empty. Then $\mathcal{I}$ is risk-reducing for $\mathcal{A}$. Thus, $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is DMFNR for any cost function $\mathcal{C}$ for $(\mathcal{A}, \mathcal{I})$.*

Proposition 6.13. *Consider a network acceptance set $\mathcal{A}$ as in (10) with $Q(G) = \mathbb{E}[(K_G^{out})^2]$ or $Q(G) = \mathbb{E}[(K_G^{in})^2]$.*

1. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,*

2. *$\mathcal{A}$ satisfies P2 if and only if there is a $N_0 \in \mathbb{N}$ such that $l_N \geq (N-1)/N$ for all $N \geq N_0$,*

3. *If $Q(G) = \mathbb{E}[(K_G^{out})^2]$, then $\mathcal{A}$ satisfies P3 if and only if $l_N < (N-1)^2/N$ for all $N \geq 1$.*

4. *If $Q(G) = \mathbb{E}[(K_G^{in})^2]$, then $\mathcal{A}$ cannot satisfy the P2 and P3 simultaneously.*

Proof. 1. The second moment of the (out- or ingoing) node degrees of any edgeless graph equals zero by definition.

2. We only prove the assertion for the out-degree distribution, The same proof holds true in case of the in-degree distribution. Since $k \leq k^2$ for all $k \in \mathbb{N}$, we find that

$$\mathbb{E}[(K_G^{out})^2] \geq \frac{1}{N} \sum_{v \in \mathcal{V}_G} k_v^{G,out} = \frac{|\mathcal{E}_G|}{N} = \mathbb{E}[K_G^{out}] \tag{13}$$

for any network G of size N. Recall that a weakly connected network G of size N contains at least $N - 1$ edges, see the proof of Proposition 6.9. Therefore, any weakly connected network G satisfies

$$\mathbb{E}[(K_G^{out})^2] \geq \frac{N-1}{N}. \tag{14}$$

Equality in (14) is realized by every directed line graph G^L where $\mathcal{V}_{G^L} = \{v_1, \cdots, v_N\}$ and $\mathcal{E}_{G^L} = \{(v_1, v_2), (v_2, v_3), \cdots, (v_{N-1}, v_N)\}$, see Figure 5. Therefore, $\mathcal{A}$ contains a weakly connected graph if and only if $\mathcal{A}$ contains a directed line graph of the same size.

3. According to Proposition 6.11, Q is $\mathcal{I}_{e\_del}$-monotone. Therefore, it suffices to consider the networks which contain a super-spreader but otherwise have minimal amount of

edges, that is the directed star graphs. The second moment of the out-degree distribution of a directed star graph G^* of size N is given by

$$\mathbb{E}[(K_{G^*}^{out})^2] = \frac{1}{N}(1 \cdot (N-1)^2 + (N-1) \cdot 0) = \frac{(N-1)^2}{N}.$$

4. Similar to (13) above we obtain that

$$\mathbb{E}[(K_G^{in})^2] \geq \frac{|\mathcal{E}_G|}{N} \tag{15}$$

for any network G of size N. Consider any weakly connected network G with N nodes for some $N \in \mathbb{N}$. Then (15) yields $\mathbb{E}[(K_G^{in})^2] \geq (N-1)/N$ (proof of Proposition 6.9). A directed star graph G^* of size N satisfies

$$\mathbb{E}[(K_{G^*}^{in})^2] = \frac{1}{N}((N-1) \cdot 1 + 1 \cdot 0) = \frac{N-1}{N},$$

because the super-spreader has in-degree 0, and all the other nodes come with a in-degree of 1. Hence, acceptability of a weakly connected graph of size N implies $l_N \geq (N-1)/N$, and thus that the directed star graph of the same size is acceptable, which violates P3. Conversely, if we exclude any directed star graph, then necessarily $l_N < (N-1)/N$ for all $N \in \mathbb{N}$, so there cannot be an acceptable weakly connected graph, so P2 is violated. □

6.2 DMFNR Based on Hub Control via Centrality Measures

In this section we consider as control Q in (10) the maximal centrality

$$Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}(v, G), \tag{16}$$

where the *centrality* $\mathfrak{C}(v, G)$ of a node v of graph G will be given by a centrality measure $\mathfrak{C}$ as discussed in the following Section 6.2.1. Controlling the maximal centrality limits the impact of the most central/systemic nodes within the network.

6.2.1 Node Centralities

A *node centrality measure* is a map

$$\mathfrak{C}^n : \mathbb{V} \times \mathcal{G} \to \mathbb{R}_+ \cup \{\emptyset\} \qquad \text{such that} \quad \mathfrak{C}(v, G) = \emptyset \Leftrightarrow v \notin \mathcal{V}_G.$$

The simplest way to measure the centrality of a node is by its in-, out-degree:

$$\mathfrak{C}_{in}^{deg}(v, G) = k_v^{G,in}, \quad \mathfrak{C}_{out}^{deg}(v, G) = k_v^{G,out}$$

in case $v \in \mathcal{V}_G$, and $\mathfrak{C}_{in}^{deg}(v, G) = \mathfrak{C}_{out}^{deg}(v, G) = \emptyset$ if $v \notin \mathcal{V}_G$.

There are a number of extensions of the concept of degree centrality where connections to high-degree nodes are more important than those to nodes with a low degree level.

Usually, this leads to a definition of centrality that is based on the entries of the normalized (left or right) eigenvector associated with the largest eigenvalue of the adjacency matrix, see Section 7.1 in [54] for details.

Alternatively, centrality can also be defined in terms of shortest paths instead of node degrees. *In-* or *out-closeness centrality*, respectively, calculate the average distance from a node to others, either in terms of incoming or outgoing paths:

$$\mathfrak{C}_{in}^{close}(v, G) = \frac{1}{|\mathcal{V}_G| - 1} \sum_{w \neq v} \frac{1}{l_{wv}^G}, \quad \mathfrak{C}_{out}^{close}(v, G) = \frac{1}{|\mathcal{V}_G| - 1} \sum_{w \neq v} \frac{1}{l_{vw}^G} \tag{17}$$

in case $v \in \mathcal{V}_G$ and $|\mathcal{V}_G| \geq 2$, $\mathfrak{C}_{in}^{close}(v, G) = \mathfrak{C}_{out}^{close}(v, G) = 0$ whenever $G = (\{v\}, \emptyset)$, and $\mathfrak{C}_{in}^{close}(v, G) = \mathfrak{C}_{out}^{close}(v, G) = \emptyset$ if $v \notin \mathcal{V}_G$. Note that we set $1/\infty := 0$.

Another prominent example of a path-based centrality measure in the literature is *betweenness centrality*

$$\mathfrak{C}^{bet}(v, G) = \sum_{\substack{u,w \\ u,w \neq v}} \frac{\sigma_{uw}^G(v)}{\sigma_{uw}^G} \quad \text{if } v \in \mathcal{V}_G, \quad \mathfrak{C}^{bet}(v, G) = \emptyset \quad \text{if } v \notin \mathcal{V}_G, \tag{18}$$

where σ_{uw}^G denotes the total number of shortest paths from node u to w in G, and $\sigma_{uw}^G(v)$ is the number of these paths that go through node v, and where we set $0/0 := 0$. Note that slightly different definitions can be found in the literature, f.e., in [54], where also paths with $u = v$ or $w = v$ are considered.

6.2.2 DMFRN based on In- and Out-Degree Centrality

Proposition 6.14. *Consider an acceptance set $\mathcal{A}$ as in (10) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{deg}(v, G)$ or $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{deg}(v, G)$. Then Q is $\mathcal{I}$-monotone for any non-empty $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{split}$, and $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR whenever $\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I})$.*

Proof. Clearly, deleting an edge does not increase the in- or out-degree of any node in a graph G. The same holds when an arbitrary node split is applied. $\square$

Proposition 6.15. *Consider an acceptance set $\mathcal{A}$ as in (10) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{deg}(v, G)$ or $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{deg}(v, G)$. Then*

1. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,*

2. *$\mathcal{A}$ satisfies P2 if and only if there is a N_0 such that $l_N \geq 1$ for all $N \geq N_0$.*

3. *If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{deg}(v, G)$, then $\mathcal{A}$ satisfies P3 if and only if $l_N < N - 1$ for all $N \geq 1$.*

4. *If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{deg}(v, G)$, then $\mathcal{A}$ cannot satisfy P2 and P3 simultaneously.*

Proof.   1. The in- and out-degree of every node in an edgeless graph equals zero.

2. If a network $G \in \mathcal{G}$ with $|\mathcal{V}_G| \geq 2$ is weakly connected, then there are nodes $v, w \in \mathcal{V}_G$ with $|\mathcal{N}_v^{G,out}|, |\mathcal{N}_w^{G,in}| \geq 1$. This proves necessity. Sufficiency follow by considering the directed line graph of size N (see Figure 5).

3. The out-degree of a super-spreader equals $N - 1$ by definition.

4. Q is $\mathcal{I}_{e\_del}$-monotone according to Proposition 6.14. Therefore, if $\mathcal{A}$ would contain a network with a super-spreader, then $\mathcal{A}$ would in particular also contain the directed star graph of the same size. For a directed star graph G^*, however, of size $|\mathcal{V}_{G^*}| \geq 2$ with super-spreader v^*, we find $\mathfrak{C}_{in}^{deg}(v, G) = 1$ for all $v \in \mathcal{V}_G \setminus \{v^*\}$, and $\mathfrak{C}_{in}^{deg}(v^*, G) = 0$. Thus, $Q(G^*) = 1$. Recall that for any weakly connected network G with $|\mathcal{V}_G| \geq 2$ we have $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{deg}(v, G) \geq 1$, see 2. Hence, 4. follows. $\square$

6.2.3 In- and Out-Closeness Centrality

We first note that for path-based centrality measures node splits may indeed worsen the situation.

Example 6.16. *Consider again the setting from Example 5.5. For all nodes $v = a, b, c$ from the initial network component G_1, we have*

$$\mathfrak{C}_{in}^{close}(v, G) = \mathfrak{C}_{out}^{close}(v, G) = \frac{1}{N-1}\Big(\frac{1}{1} + \frac{1}{1}\Big) = \frac{2}{N-1}.$$

Now, after the node split, the nodes a and c come with in- and out-closeness centralities of

$$\mathfrak{C}_{in}^{close}(v, H) = \mathfrak{C}_{out}^{close}(v, H) = \frac{1}{N}\Big(\frac{1}{1} + \frac{1}{1} + \frac{1}{2}\Big) = \frac{5}{2N}, \quad v = a, c,$$

and we find that

$$\max_{v \in \mathcal{V}_G} \mathfrak{C}_*^{close}(v, G) < \max_{v \in \mathcal{V}_H} \mathfrak{C}_*^{close}(v, H) \Leftrightarrow \frac{2}{N-1} < \frac{5}{2N} \Leftrightarrow 5 < N, \quad v = a, c,$$

for $* = in, out$. Thus, the maximal in- and out-closeness centrality is increased under the node split if the component G_2 consists of at least three isolated nodes.

Similarly, the betweenness centrality as defined in (18) of all nodes $v \in \mathcal{V}_{G_1}$ equals zero. However, after the split of node b, we have that the shortest paths from node b to $\tilde{b}$ and vice versa both pass through nodes a and c, thus

$$Q(H) = \mathfrak{C}^{bet}(a, H_1) = \mathfrak{C}^{bet}(c, H_1) = 2 > 0 = Q(G).$$

Proposition 6.17. *Consider a set $\mathcal{A} \subset \mathcal{G}$ as in (10) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G)$ or $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{close}(v, G)$. Then*

1. *Q is $\mathcal{I}$-monotone for any non-empty $\mathcal{I} \subset \mathcal{I}_{e\_del} \cup \mathcal{I}_{s\_iso} \cup \{id\}$. In that case $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR whenever $\mathcal{C}$ is a cost function $(\mathcal{A}, \mathcal{I})$.*

2. $\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,

3. $\mathcal{A}$ satisfies P2 if and only if there is a $N_0 \in \mathbb{N}$ such that $l_N \geq 1/(N-1)$ for all $N \geq N_0$.

4. If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, G)$, then $\mathcal{A}$ satisfies P3 if and only if $l_1 < 0$ and $l_N < 1$ for all $N \geq 2$.

5. If $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{close}(v, G)$, then $\mathcal{A}$ cannot satisfy P2 and P3 simultaneously. More precisely, P2 implies that P3 is violated and vice versa.

Proof.   1. The same arguments apply as in the proof of Property C2 in Proposition 5.4.

2. By definition, we have $\mathfrak{C}_{out}^{close}(v, G), \mathfrak{C}_{in}^{close}(v, G) \geq 0$, and for every node v in an edgeless graph $\mathfrak{C}_{out}^{close}(v, G) = \mathfrak{C}_{in}^{close}(v, G) = 0$.

3. If G of size $N \geq 2$ is weakly connected, we must have $Q(G) \geq 1/(N-1)$ for both the in- and out-closeness centrality since there is a node with an incoming, and a node with an outgoing edge. This proves that $l_N \geq 1/(N-1)$ for all $N \geq N_0$, where $N_0 \in \mathbb{N}$, is necessary for P2. The super-spreader v^* of a directed star graph G^* of size $N \geq 2$ satisfies $\mathfrak{C}_{in}^{close}(v^*, G^*) = 0$ whereas $\mathfrak{C}_{in}^{close}(v, G^*) = 1/(N-1)$ for $v \in \mathcal{V}_{G^*} \setminus \{v^*\}$, which proves $Q(G^*) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{in}^{close}(v, G^*) = 1/(N-1)$. Analogously, considering a graph $\hat{G}$ obtained by inverting the direction of the edges of the directed star graph G^*, that is $\mathcal{V}_{\hat{G}} = \mathcal{V}_{G^*}$ and $\mathcal{E}_{\hat{G}} = \{(u, v) \mid (v, u) \in \mathcal{E}_{G^*}\}$, we find $Q(\hat{G}) = \max_{v \in \mathcal{V}_G} \mathfrak{C}_{out}^{close}(v, \hat{G}) = 1/(N-1)$. Since G^* and $\hat{G}$ are weakly connected, sufficiency of there exists $N_0 \in \mathbb{N}$ such that $l_N \geq 1/(N-1)$ for all $N \geq N_0$ for P2 follows.

4. The super-spreader v^* of a directed star graph G^* of size $|\mathcal{V}_{G^*}| \geq 2$ satisfies $\mathfrak{C}_{out}^{close}(v^*, G^*) = 1$. The same applies to a star node in a bidirectional star graph.

5. This follows from the proof of 3.

$\square$

6.2.4 DMFNR Based on Betweenness Centrality

In this section we illustrate that centrality measures which define centrality of a node not in absolute terms but relative to the centrality of other nodes may not be suitable control for systemic (cyber) risk. To this end, recall the betweenness centrality given in (18).

Proposition 6.18. *Consider the acceptance set $\mathcal{A}$ in (10) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{bet}(v, G)$. If $\mathcal{A}$ satisfies P1, then P3 is violated. Conversely, if $\mathcal{A}$ satisfies P3, then P1 is violated.*

Proof. If G^c is a complete graph, then there is only one shortest path between two distinct nodes $u, w \in \mathcal{V}$, namely the edge between them. Therefore, in complete graphs we have $\sigma_{uw}(v) = 0$ if $v \notin \{u, w\}$, and we thus find $\mathfrak{C}^{bet}(v, G^c) = 0$ for all $v \in \mathcal{V}_{G^c}$. Hence, $Q(G^c) = 0$. Clearly, any edge-less graph $G^\emptyset = (\mathcal{V}, \emptyset)$ also satisfies $Q(G^\emptyset) = 0$. $\square$

6.3 DMFNR Based on Stress Test Scenarios

Suppose that the supervisor applies an (external) risk model operating on the supervised network. This model could, for instance, describe the evolution or spread of a risk throughout the network. Typical examples of such processes include bond or bootstrap percolation ([20, 23]), as well as continuous-time SIR or SIS epidemic models, as used in [6, 18, 19, 64]. This external risk model is naturally employed to assess networks via stress-test simulations. Note that a macroprudential cyber stress testing framework for financial risk regulation has recently been proposed in [28, 57], comprising four stages: scenario type (*context*), initial cyber incident or attack (*shock*), propagation through the network (*amplification*), and the system-wide impact (*systemic event*). The stages context, shock, and amplification define the dynamics of the cyber scenario. As these dynamics unfold, an initial shock results in specific outcomes, such as the total number of nodes affected by the cyber attack. The term *systemic event* refers to outcomes that significantly disrupt the (financial) system's ability to perform critical functions. In order to define systemic events, the supervisor may establish an *impact tolerance threshold*, as discussed in [57]. For example, this threshold might be a critical fraction $\alpha \in (0,1)$, indicating the proportion of nodes affected during the incident.

Let $\mathcal{S}(G)$ denote the systemic event. Suppose that a network is deemed acceptable if the probability of such a systemic shock, $\mathbb{P}[\mathcal{S}(G)]$, does not exceed a specified threshold $\lambda \in (0,1)$. The corresponding acceptance set is

$$\mathcal{A} = \{G \mid \mathbb{P}[\mathcal{S}(G)] \leq \lambda\}. \tag{19}$$

Note that $\mathcal{A}$ is of type (10), with $Q(G) = \mathbb{P}[\mathcal{S}(G)]$ and $l_{|\mathcal{V}_G|} \equiv \lambda$.

Remark 6.19. *Observe the similarity of* (19) *to the acceptability criterion defining the Value-at-Risk (VaR) risk measure well-known in financial risk regulation, see, e.g., [34, Section 4.4]. Notably, as in the case of the VaR, the acceptability criterion defining $\mathcal{A}$ might neglect tail risks.*

In the following we discuss a stress test based DMFNR where the external risk model is given by a SIR infection process.

6.3.1 Stress Tests Based on an SIR Contagion Scenario

Consider Scenario 2 in our motivating example in the introduction, focusing on the spread of a cyber incident. The stress test begins by identifying *initial shocks*, which can be modeled in various ways; for instance, infections might randomly occur at any network node. In the *amplification* phase, selecting an appropriate risk propagation model is essential. Cyber risks spread via interactions within the network. Epidemic models from mathematical biology provide a framework for such contagious risks. In the continuous-time SIR Markov model, which we will apply in this section, nodes are categorized into compartments: *susceptible* (S), *infected* (I), and *recovered* (R). For a network G with N enumerated nodes, the state of the process at time $t \geq 0$ is given by:

$$X(t) = (X_1(t), \ldots, X_N(t)) \in E^N,$$

where $E = \{S, I, R\}$. State changes occur over time, starting at $t_0 = 0$ when the initial shock impacts the system. In this model, a node may become infected by its infected in-neighbors, while recovery is independent of the states of other nodes in the network. Recovery corresponds to permanent immunity, meaning individuals do not face reinfection. The state transitions are described as follows:

$$X_i : S \to I \quad \text{at rate} \quad \tau \sum_{j=1}^{N} a_{ji} \mathbb{1}_{\{X_j(t)=I\}}, \tag{20}$$

$$X_i : I \to R \quad \text{at rate} \quad \gamma,$$

where $\tau > 0$ is the infection rate and $\gamma > 0$ is the recovery rate.
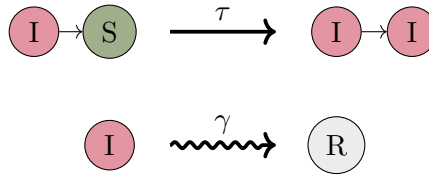

Figure 6: Infection and recovery for the SIR network model.

We define a systemic event $\mathcal{S}(G)$ in G as the case where at least a fraction $\alpha \in (0, 1)$ of nodes becomes infected over the course of the epidemic.

Proposition 6.20. *Let $\mathcal{A}$ be as defined in* (19) *with stress test described above based on the SIR contagion model. Then, for any non-empty intervention set $\mathcal{I}$ consisting of edge deletions $\mathcal{I} \subseteq \mathcal{I}_{e\_del}$, the quantity $Q(G) = \mathbb{P}[\mathcal{S}(G)]$ is $\mathcal{I}$-monotone. Consequently, $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR whenever $\mathcal{C}$ is a cost function for $(\mathcal{A}, \mathcal{I})$.*

Proof. The continuous-time SIR Markov model can be isomorphically represented as a random graph known as the *epidemic percolation network* (EPN), as demonstrated in [49] and [50, Section 6.3.3]. In particular, the distribution of final epidemic outcomes coincides with the distribution of the combined out-components that originate from initially infected nodes in the EPN. For a given network $G \in \mathcal{G}$ the corresponding EPN $\tilde{G}$ is constructed as follows:

1. Initialize the vertex set $\mathcal{V}_{\tilde{G}} = \mathcal{V}_G$ and set the edge set $\mathcal{E}_{\tilde{G}} = \emptyset$.

2. For each node $v \in \mathcal{V}_G$, perform the following:

    a) Sample the (potential) infection duration for node v from an exponential distribution with rate γ. Given this duration, the transmissions from v to its neighbors occur independently.

    b) Choose an out-neighbor $w \in \mathcal{N}_v^{G,out}$ and determine the transmission time from v to w. This is done by sampling from an exponential distribution with rate τ.

c) If the transmission time from v to w is less than the infection duration of v, include the edge (v, w) in the edge set $\mathcal{E}_{\tilde{G}}$.

d) Repeat steps (b) and (c) for all other out-neighbors of v in G.

3. The resulting EPN is then given by $\tilde{G} = (\mathcal{V}_{\tilde{G}}, \mathcal{E}_{\tilde{G}})$.

The *out-component* $\mathcal{V}_{\tilde{G}_v^{out}}$ contains v and all nodes $w \in \mathcal{V}_{\tilde{G}} \setminus \{v\}$ for which there is a path from v to w in network $\tilde{G}$. These are those nodes that are eventually infected in case that v is infected. The final set of all infected nodes, $\mathcal{V}_G^{fin}$, during the epidemic for an initially infected set $\tilde{\mathcal{V}} \subseteq \mathcal{V}_G$, is represented by the union of their out-components in the EPN $\tilde{G}$:

$$\mathcal{V}_G^{fin} = \bigcup_{v \in \tilde{\mathcal{V}}} \mathcal{V}_{\tilde{G}_v^{out}}.$$

Clearly, the probability of a systemic outbreak event, defined as $|\mathcal{V}_G^{fin}| \geq \alpha |\mathcal{V}_G|$, cannot be increased when an edge is removed from G. $\qquad \square$

Remark 6.21. *It can be shown that $Q(G) = \mathbb{P}[\mathcal{S}(G)]$ is not monotone for node splits. Indeed, this will happen under any contagion model, not only the SIR-model. Recall that node splits are related to diversification in the network. Thus, we observe another similarity to the VaR risk measure mentioned in Remark 6.19 above, namely that diversification may be penalized in this risk model.*

Remark 6.22. *To analyze properties P1-P3, one must determine the probability distribution of outbreak sizes in the network under the given contagion model. This depends on the underlying model parameters, including the infection and recovery rates, as well as the distribution of the initial shock in the network. Moreover, closed forms of these distributions typically do not exist, necessitating approaches like Monte Carlo simulations. It is therefore a rather challenging exercise which is not in the scope of this paper.*

Remark 6.23. *(Alternative Interventions) In principle, in cases where an external risk model is applied, interventions other than those introduced in Section 4 could be considered, namely interventions which target the parameters of the external model, such as the infection rate τ and the recovery rate γ in the SIR model. Our framework does, in general, not assume such an external model. Therefore, we do not consider such interventions, even though they are conceivable in an extension of the decision-making framework. Such extensions are left to future research. Also note that, even if external risk models are applied, there are reasons to limit the interventions to the topological interventions we consider in this paper.*

Firstly, supervisors often have to consider various (external models for different) types of vulnerabilities, not just one. In that case it is natural to regulate the system's structure itself. The mentioned Zero Trust approach advocates for a fundamental robustification of the system architecture to become resistent to various threat scenarios.

Secondly, a standard approach to stress testing is to pre-calibrate the parameters of the external risk model to existing data, and then to leave this model decribing a particular

attack scenario unaltered while different network configurations (as a result of different protecting interventions) are stress-tested. In that case the interventions should not alter the parameters of the attack scenario.

Thirdly, in the case of the SIR model, for instance, the operational interpretation of altering parameters such as infection and recovery rate does not seem to be obvious. One would have to specify how real-world measures influence the parameters of the external model.

Finally, inventions altering the parameters of the external risk model might not be enough. Consider the epidemic threshold of the continuous-time SIR model over an undirected network with countably infinite number of nodes, given by

$$\frac{\tau}{\tau + \gamma} \frac{\mathbb{E}[K_G^2 - K_G]}{\mathbb{E}[K_G]} > 1, \tag{21}$$

see [9, Chapter 10], [50, Chapter 6.2], and [56, Section V.B.4]. Here K_G is (a random variable with) the degree distribution of G. If (21) is satisfied, then epidemic outbreaks are possible; otherwise, they are not. We can consider the infinite network a proxy for very large real-world networks, such as the internet, which often exhibit significant heterogeneity. These networks typically feature a few hubs and many sparsely connected nodes. These so-called scale-free networks often follow a power-law degree distribution, given by $\mathbb{P}(K_G = k) \sim k^{-\alpha}$. As the network size increases, the second moment of this degree distribution diverges, ensuring that (21) is satisfied regardless of the values of the infection and recovery parameters τ and γ. Consequently, with increasing network size epidemic outbreaks remain possible despite changes to these parameters. However, topological interventions aim to modify the topology and, therefore, the degree distribution of the network, potentially avoiding the conditions set by (21).

7 Outlook

In the following we collect a few of open questions and challenges for future research:

Calibration to Real World Networks While this study provides the theoretical foundation and also presents first stylized examples of decision-making frameworks for networks resilience (DMFNR), the next step is to apply such DMFNRs to managing real world networks, such as the cyber mapping mentioned in the motivating example in the introduction. In this context particularly suitable DMFNRs will be identified together with important parameters such as a desired minimal levels of network functionality, the border between acceptability and non-acceptability in practice, etc.

Computational Challenges Computational problems stem primarily from the high dimensionality of the networks. Determining suitable or even optimal network manipulations may therefore be challenging. A possible solution may be to develop new machine learning-based algorithms to identify good, not necessarily strictly optimal, ways to secure some given network.

Model Uncertainty   A major problem in practice is that the supervisor might only possess incomplete information about the network she has to secure.

Weighted Networks   As mentioned in Remark 2.2, network models may benefit from adding edge weights. For example, in models of financial systems edge weights represent the liabilities between financial institutions. Default contagion occurs when a financial institution's failure to meet its liabilities——represented by its outgoing edges to other institutions——triggers a cascade of defaults among connected institutions, see [24]. The extension of the presented framework to weighted graphs would, however, require a number of modifications, for instance as regards the interventions which now also target the edge weights.

Area of Application   Even though, on the most basic level, this paper introduces decision-making frameworks for network resilience for any type of network, the later discussion is tailored to systemic cyber risk. It would be interesting to explore applications to other examples of critical infrastructure networks such as power grids, transportation systems, and production networks.

A Basic Notions for Graphs

A.1 Adjacency Matrix

For a network of size N, the nodes can be enumerated, say as $v_1, \cdots, v_N$. Given an enumeration of the vertex set $\mathcal{V}_G$, the *network topology*, i.e., the spatial pattern of interconnections, of a network G is described by its *adjacency matrix* $A_G = (A_G(i,j))_{i,j=1,\cdots,N} \in \{0,1\}^{N \times N}$, where

$$A_G(i,j) = \begin{cases} 1, & \text{if } (v_i, v_j) \in \mathcal{E}_G \\ 0, & \text{else.} \end{cases}$$

Note that G is undirected if and only if A_G is a symmetric matrix.

A.2 Neighborhoods of Nodes and Node Degrees

For a graph $G = (\mathcal{V}_G, \mathcal{E}_G)$ and node $v \in \mathcal{V}_G$, we define $\mathcal{N}_v^{G,in} := \{w \in \mathcal{V}_G | (w,v) \in \mathcal{E}_G\}$ and $\mathcal{N}_v^{G,out} := \{w \in \mathcal{V}_G | (v,w) \in \mathcal{E}_G\}$ as the *in-* and *out-neighborhoods* of node v. The *neighborhood* is $\mathcal{N}_v^G := \mathcal{N}_v^{G,in} \cup \mathcal{N}_v^{G,out}$. A network G is undirected if and only if $\mathcal{N}_v^{G,in} = \mathcal{N}_v^{G,out} = \mathcal{N}_v^G$ for all $v \in \mathcal{V}_G$.

The *incoming* or *in-degree*, i.e., the number of edges arriving at node v, is defined as $k_v^{G,in} = |\mathcal{N}_v^{G,in}|$, and the *outgoing* or *out-degree* as $k_v^{G,out} = |\mathcal{N}_v^{G,out}|$. The *(total) degree* k_v^G of node v in network G is defined as

$$k_v^G = \frac{1}{2}(k_v^{G,in} + k_v^{G,out}).$$

Typically, total degrees are studied in the context of undirected networks G where we find that $k_v^G = k_v^{G,in} = k_v^{G,out}$ due to the fact that $\mathcal{N}_v^{G,out} = \mathcal{N}_v^{G,in}$ for all $v \in \mathcal{V}_G$.

A.3 Walks, Paths, and Connectivity of Graphs

Given a graph G, a *walk* of length n from node v to node w in G is an $(n+1)$-tuple of nodes $(v_1, v_2, \ldots, v_{n+1})$ such that $(v_i, v_{i+1}) \in \mathcal{E}_G$ for all $1 \leq i \leq n$ and $v_1 = v$ and $v_{n+1} = w$. A *path* from v to w is a walk where all nodes are distinct.

A graph G is called *strongly connected* if for each node pair $v, w \in \mathcal{V}_G$ there exist paths from v to w and from w to v. A directed graph G is called *weakly connected* if its undirected version, that is the graph $\tilde{G} = (\mathcal{V}_G, \mathcal{E}_{\tilde{G}})$ with $\mathcal{E}_{\tilde{G}} = \{(v,w)|(v,w) \in \mathcal{E}_G$ or $(w,v) \in \mathcal{E}_G\}$, is strongly connected. A *(weakly connected) component* $\tilde{G}$ of network G is a (weakly) connected subgraph, and two components $G_1 = (\mathcal{V}_1, \mathcal{E}_1)$, $G_2 = (\mathcal{V}_1, \mathcal{E}_2)$ of G are called *disconnected* if there are no $v \in \mathcal{V}_1$ and $w \in \mathcal{V}_2$ such that there is a path from v to w or from w to v in G.

B Undirected Networks

We denote the set of undirected networks by

$$\mathcal{G}^{ud} := \{G = (\mathcal{V}_G, \mathcal{E}_G) \in \mathcal{G} | (v,w) \in \mathcal{E}_G \Leftrightarrow (w,v) \in \mathcal{E}_G\} \subset \mathcal{G}.$$

The pair $\{(v, w), (w, v)\} \in \mathcal{E}_G$ will be referred to as a *full edge* of the undirected graph $G = (\mathcal{V}_G, \mathcal{E}_G)$. In the following, we discuss how the presented theory in the main part of this paper would change if we restrict the domain to $\mathcal{G}^{ud}$ instead of $\mathcal{G}$. Indeed, most of the definitions and results can easily be adapted to this class of networks and we leave this to the reader apart from a few comments and additional examples which are collected in this section. Regarding the Properties P2 and P3 presented in Section 3, note that an undirected graph is weakly connected if and only if it is strongly connected, which in this case is only referred to as being connected. Moreover, for an arbitrary graph $G \in \mathcal{G}^{ud}$, any super-spreader $v^* \in \mathcal{V}_G$ is a star node. We thus obtain the following versions of P2 and P3 for undirected graphs:

- P2: There exists $N_0 \in \mathbb{N}$ such that there is a connected graph in $\mathcal{A}$ of size N for all $N \geq N_0$.

- P3: Any network with a star node is not acceptable.

B.1 Interventions for Undirected Networks

If we restrict the discussion to the class $\mathcal{G}^{ud}$, then any undirected graph should always be transformed into a new undirected graph. For convenience, as we view the undirected networks $\mathcal{G}^{ud}$ as a subset of the potentially directed networks $\mathcal{G}$, the following elementary interventions on undirected graphs are defined on $\mathcal{G}$, that is $\kappa : \mathcal{G} \to \mathcal{G}$, but satisfy $\kappa(\mathcal{G}^{ud}) \subseteq \mathcal{G}^{ud}$. Note that only those interventions from Section 4 that come with a manipulation of network edges need to be adjusted.

$\mathcal{I}_{e\_del}^{ud}$ *Edge Deletion*: Consider a node tuple $v, w \in \mathbb{V}$. We let

$$\kappa_{e\_del}^{v,w} := \kappa_{e\_del}^{(w,v)} \circ \kappa_{e\_del}^{(v,w)} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \setminus \{(v, w), (w, v)\})$$

denote the deletion of the full edge between nodes v and w. Clearly, $\kappa_{e\_del}^{v,w} = \kappa_{e\_del}^{w,v}$. We set

$$\mathcal{I}_{e\_del}^{ud} := \{\kappa_{e\_del}^{v,w} \mid v, w \in \mathbb{V}\}.$$

$\mathcal{I}_{e\_add}^{ud}$ *Edge Addition*: The addition of an edge between nodes $v, w \in \mathbb{V}$ with $v \neq w$ is given by

$$\kappa_{e\_add}^{v,w} := \kappa_{e\_add}^{(w,v)} \circ \kappa_{e\_add}^{(v,w)} : G \mapsto (\mathcal{V}_G, \mathcal{E}_G \cup (\{(v, w), (w, v)\} \cap \mathcal{V}_G \times \mathcal{V}_G)),$$

and we let

$$\mathcal{I}_{e\_add}^{ud} := \{\kappa_{e\_add}^{v,w} \mid v, w \in \mathbb{V}\}.$$

$\mathcal{I}_{shift}^{ud}$ *Edge Shift*: An existing full edge between v and w can be shifted to a full edge between q and r by

$$\kappa_{shift}^{\{v,w\},\{q,r\}} := \kappa_{shift}^{(w.v),(r,q)} \circ \kappa_{shift}^{(v,w),(q,r)}.$$

We set

$$\mathcal{I}_{shift}^{ud} := \{\kappa_{shift}^{\{v,w\},\{q,r\}} \mid v, w, q, r \in \mathbb{V}\}.$$

$\mathcal{I}^{ud}_{split}$ *Node Splitting*: For node splitting in undirected networks, we need to restrict to interventions from the set

$$\mathcal{I}^{ud}_{split} := \{\kappa^{\mathcal{L},v,\tilde{v}}_{split}|v,\tilde{v}\in\mathcal{V},\mathcal{L}\subset\mathcal{E},(q,r)\in\mathcal{L}\Leftrightarrow(r,q)\in\mathcal{L}\}\subset\mathcal{I}_{split}.$$

B.2 Examples

As in the main part of this paper, we consider examples based on acceptance sets $\mathcal{A}\subset\mathcal{G}^{ud}$ of the form

$$\mathcal{A}=\{G\in\mathcal{G}^{ud}|Q(G)\le l_{|\mathcal{V}_G|}\} \tag{22}$$

where $Q:\mathcal{G}^{ud}\to\mathbb{R}\cup\{-\infty,\infty\}$ and $l_N\in\mathbb{R}$ for all $N\in\mathbb{N}$. In principle, any Q from the previous discussion on directed networks can also be applied here and the results from the directed case essentially also apply to the undirected case. Only some proofs or bounds l_N need to be adjusted as we will see in the following.

B.2.1 DMFNR Based on the Average Total Degree

For undirected networks we consider the distribution of the total degree k^G_v, see Section A.2, which, of course, equals the in- and out-degree distributions. Let K_G be a random variable, the law of which coincides with the total degree distribution. Similar to the directed case, choosing $Q(G)=\mathbb{E}[K_G]$ in (22) yields a DMFNR but $\mathcal{A}$ does not satisfy P2 and P3 simultaneously. Indeed recall Proposition 6.9 and compare to Proposition B.1 below. In this case the proof is based on *tree graphs*: a connected undirected acyclic graph $G^T\in\mathcal{G}^{ud}$ is called an *undirected tree*.

Figure 7: An undirected tree graph (left) and undirected star graph (right) consisting of $N=7$ nodes. Note that both the undirected line graph from Figure 5 and the undirected star graph are special cases of a tree since they do not contain any cycles.

Proposition B.1. *Suppose that $\mathcal{A}$ is given by (22) with $Q(G)=\mathbb{E}[K_G]$. If P2 is satisfied, then P3 is violated, and vice versa.*

Proof. An undirected connected graph G of size N must contain a spanning tree $\tilde{G}$, see Corollary 7 in [13]. Moreover, since Q is $\mathcal{I}_{e\_del}$-monotone, we have $Q(\tilde{G})\le Q(G)$.

However, $\tilde{G}$ has the same number of edges as any undirected star graph G^* of the same size since both are undirected tree graphs, see [13, Corollary 8], and therefore $Q(G) \geq Q(\tilde{G}) = Q(G^*) = 2(N-1)/N$. This proves the assertion. $\qquad\square$

B.2.2 DMFNR Based on the Second Moment of the Degree Distribution

As in the directed case, we find that choosing $Q(G) = \mathbb{E}[K_G^2]$ in (22) is a suitable way to define acceptance sets $\mathcal{A}$ which satisfy properties P1-P4. For the proof, we need the following lemma:

Lemma B.2. *Fix $N \in \mathbb{N}$. The minimal second moment $Q(G^T) = \mathbb{E}[K_{G^T}^2]$ among all undirected tree graphs $G^T \in \mathcal{G}^{ud}$ of size N is attained by the undirected line graphs $G^L = (\mathcal{V}_{G^L}, \mathcal{E}_{G^L})$, where for $\mathcal{V}_{G^L} = \{v_1, \cdots, v_N\} \subset \mathbb{V}$ we have $\mathcal{E}_{G^L} = \{(v_1, v_2), (v_2, v_1), \cdots, (v_{N-1}, v_N), (v_N, v_{N-1})\}$.*

Proof. We prove the result by induction. First, note that for $N = 2$ and some arbitrary $v_1, v_2 \in \mathbb{V}$, the only undirected tree G^T is given by $G^T = (\{v_1, v_2\}, \{(v_1, v_2), (v_2, v_1)\})$, which is a line graph. Now, suppose that the statement holds for some $N \geq 2$, and consider a tree G^T of size $N + 1$. Then G^T contains at least two nodes with a total degree of 1, called *leaves*, see Corollary 9 in [13]. Consider an enumeration of the nodes $\mathcal{V}_{G^T}$ such that v_{N+1} is a leaf of G^T with (only) neighbor v_N. Delete node v_{N+1} such that we obtain the network $H = \kappa_{n\_del}^{v_{N+1}}(G^T)$. Note that H is a tree graph of size N. Now consider the line graph G^L of the same size defined on the vertex set $\mathcal{V}_{G^T} \setminus \{v_{N+1}\}$ with leaf v_N. By induction hypothesis, we have

$$\mathbb{E}[K_{G^L}^2] \leq \mathbb{E}[K_H^2], \quad \text{and thus} \quad \sum_{i=1}^{N} (k_{v_i}^{G^L})^2 \leq \sum_{i=1}^{N} (k_{v_i}^H)^2.$$

Now, let $\tilde{G}^L = (\mathcal{V}_{G^T}, \mathcal{E}_{G^L} \cup \{(v_N, v_{N+1}), (v_{N+1}, v_N)\})$, which is a line graph of size $N + 1$. Since node v_N is a leave in G^L, we find $1 = k_{v_N}^{G^L} \leq k_{v_N}^H$. Moreover, $k_{v_i}^{\tilde{G}^L} = k_{v_i}^{G^L}$, $k_{v_i}^{G^T} = k_{v_i}^H$ for $i = 1, \cdots, N-1$, and we have $k_{v_N}^{\tilde{G}^L} = k_{v_N}^{G^L} + 1 = 2$, $k_{v_N}^{G^T} = k_{v_N}^H + 1 \geq 2$, and $k_{v_{N+1}}^{G^T} = k_{v_{N+1}}^{\tilde{G}^L} = 1$. In total, this yields

$$\mathbb{E}[K_{\tilde{G}^L}^2] = \frac{1}{N+1} \sum_{i=1}^{N+1} (k_{v_i}^{\tilde{G}^L})^2 = \frac{1}{N+1} \Big(\sum_{i=1}^{N-1} (k_{v_i}^{G^L})^2 + (k_{v_N}^{G^L} + 1)^2 + 1^2 \Big)$$

$$= \frac{1}{N+1} \Big(\sum_{i=1}^{N} (k_{v_i}^{G^L})^2 + 2k_{v_N}^{G^L} + 1 + 1 \Big) = \frac{1}{N+1} \Big(\sum_{i=1}^{N} (k_{v_i}^{G^L})^2 + 3 + 1 \Big)$$

$$\leq \frac{1}{N+1} \Big(\sum_{i=1}^{N} (k_{v_i}^H)^2 + 3 + 1 \Big) = \frac{1}{N+1} \Big(\sum_{i=1}^{N-1} (k_{v_i}^H)^2 + (k_{v_N}^{G^T} - 1)^2 + 3 + 1 \Big)$$

$$= \frac{1}{N+1} \Big(\sum_{i=1}^{N} (k_{v_i}^{G^T})^2 - 2k_{v_N}^{G^T} + 1 + 3 + 1 \Big) \leq \frac{1}{N+1} \Big(\sum_{i=1}^{N} (k_{v_i}^{G^T})^2 + 1 \Big) = \mathbb{E}[K_{G^T}^2].$$

$\square$

Proposition B.3. *Suppose that $\mathcal{A}$ is given by* (22) *with $Q(G) = \mathbb{E}\big[(K_G^2)\big]$.*

1. *Q is $\mathcal{I}$-monotone for any $\mathcal{I} \subset \mathcal{I}_{e\_del}^{ud} \cup \mathcal{I}_{split}^{ud}$. Hence $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR for any cost function for $(\mathcal{A}, \mathcal{I})$.*

2. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,*

3. *$\mathcal{A}$ satisfies P2 if and only if there is a N_0 such that $l_N \geq 4 - 6/N$ for all $N \geq N_0$.*

4. *$\mathcal{A}$ satisfies P3 if and only if $l_N < N - 1$ for all $N \geq 1$.*

Proof. 1. and 2. are straightforward modifications of the proof of the corresponding results in Propositions 6.11 and 6.13.

3.: Note that since $Q(G) = \mathbb{E}\big[K_G^2\big]$ is $\mathcal{I}_{e\_del}$-monotone according to 1., and every connected network contains a spanning tree, it suffices to determine the minimizer of Q among all undirected tree graphs. The second moment of total degrees is minimized among all undirected tree graphs of a fixed size N by the undirected line graphs, see Lemma B.2, and can be calculated for $N \geq 2$ as

$$\mathbb{E}\big[K_L^2\big] = \frac{1}{N}\big(2 \cdot 1 + (N-2) \cdot 4\big) = \frac{4N-6}{N} = 4 - \frac{6}{N}.$$

4.: For the undirected star graph G^* of size N we obtain

$$\mathbb{E}\big[(K_{G^*})^2\big] = \frac{1}{N}\Big(1 \cdot (N-1)^2 + (N-1) \cdot 1^2\Big) = \frac{1}{N}\big((N-1)^2 + (N-1)\big) = N - 1.$$

$\square$

B.2.3 DMFNR Based on Epidemic Threshold

Recall the epidemic threshold of the SIR model for undirected networks given in (21). Rearranging the inequality shows that the ratio of second and first moment may be a promising candidate for the control of network contagion

$$Q(G) = \begin{cases} \frac{\mathbb{E}\big[K_G^2\big]}{\mathbb{E}\big[K_G\big]} & \text{if } \mathbb{E}\big[K_G\big] > 0 \\ 0 & \text{if } \mathbb{E}\big[K_G\big] = 0. \end{cases} \tag{23}$$

Note, however, that risk management with respect to this quantity is not completely compatible with edge deletions:

Proposition B.4. *Q as given in* (23) *is not $\mathcal{I}_{e\_del}^{ud}$-monotone.*

Proof. Suppose we delete the edges $\{(v,w), (w,v)\}$ between two adjacent nodes $v, w \in \mathcal{V}_G$ in a network G of size $N \geq 3$, and let $\tilde{G} = \kappa_{e\_del}^{v,w}(G)$. Further suppose that $\tilde{G}$ does contain edges, so that $\mathbb{E}[K_{\tilde{G}}], \mathbb{E}[K_{\tilde{G}}^2] > 0$ and thus $Q(\tilde{G}) = \mathbb{E}[K_{\tilde{G}}^2]/\mathbb{E}[K_{\tilde{G}}]$. If Q were $\mathcal{I}_{e\_del}^{ud}$-monotone, then

$$\frac{\mathbb{E}\big[K_G^2\big]}{\mathbb{E}\big[K_G\big]} - \frac{\mathbb{E}\big[K_{\tilde{G}}^2\big]}{\mathbb{E}\big[K_{\tilde{G}}\big]} \geq 0, \quad \text{i.e. } \mathbb{E}[K_{\tilde{G}}]\mathbb{E}[K_G^2] - \mathbb{E}[K_G]\mathbb{E}[K_{\tilde{G}}^2] \geq 0. \tag{24}$$

We can express the moments of $\tilde{G}$ in terms of the moments of G by

$$\mathbb{E}[K_{\tilde{G}}] = \mathbb{E}[K_G] - \frac{2}{N}, \qquad \mathbb{E}[K_{\tilde{G}}^2] = \mathbb{E}[K_G^2] + \frac{2}{N}(1 - (k_v^G + k_w^G)).$$

Therefore,

$$\mathbb{E}[K_{\tilde{G}}]\mathbb{E}[K_G^2] - \mathbb{E}[K_G]\mathbb{E}[K_{\tilde{G}}^2] = \left(\mathbb{E}[K_G] - \frac{2}{N}\right)\mathbb{E}[K_G^2] - \mathbb{E}[K_G]\left(\mathbb{E}[K_G^2] + \frac{2}{N}(1 - (k_v^G + k_w^G))\right)$$

$$= \frac{2}{N}\left(-\mathbb{E}[K_G^2] - \mathbb{E}[K_G] + \mathbb{E}[K_G](k_v^G + k_w^G)\right).$$

Hence, (24) is satisfied if and only if $\mathbb{E}[K_G](k_v^G + k_w^G) - (\mathbb{E}[K_G^2] + \mathbb{E}[K_G]) \geq 0$, i.e., when

$$(k_v^G + k_w^G) \geq \frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]} + 1. \tag{25}$$

One easily constructs examples where (25) is not satisfied. $\qquad\square$

For the management of risk under edge deletions in a given network G, we thus need to restrict ourselves to those edge deletions that satisfy (25), i.e., that target edges between nodes with sufficiently large degrees.

Proposition B.5. *Let $\mathcal{A}$ be given by (22) and Q in (23). Then*

1. *Q is $\mathcal{I}$-monotone for any $\mathcal{I} \subset \mathcal{I}_{split}^{ud}$, and $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR for any cost function for $(\mathcal{A}, \mathcal{I})$.*

2. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$.*

3. *$\mathcal{A}$ satisfies P2 if and only if there is a N_0 such that $l_N \geq 2 - \frac{1}{N-1}$ for all $N \geq N_0$.*

4. *Suppose that $l_1 < 0$, $l_N < N/2$ for all $2 \leq N \leq 6$ and that $l_N < \frac{4N-1}{N+1}$ for all $N \geq 7$. Then $\mathcal{A}$ satisfies P3.*

Proof. 1. Let $v \in \mathcal{V}_G$ be a node of the network G which is split into v and $\tilde{v}$ with a resulting network $\tilde{G}$. Again, utilizing (12) and $(N+1)\mathbb{E}[K_{\tilde{G}}] = N\mathbb{E}[K_G]$, we see that

$$\frac{\mathbb{E}[K_{\tilde{G}}^2]}{\mathbb{E}[K_{\tilde{G}}]} = \frac{\frac{1}{N+1}\left(\sum_{w \neq v, \tilde{v}}(k_w^{\tilde{G}})^2 + (k_v^{\tilde{G}})^2 + (k_{\tilde{v}}^{\tilde{G}})^2\right)}{\frac{1}{N+1}\left(\sum_{w \neq v, \tilde{v}} k_w^{\tilde{G}} + k_v^{\tilde{G}} + k_{\tilde{v}}^{\tilde{G}}\right)} \leq \frac{\sum_{w \in \mathcal{V}_G}(k_w^G)^2}{\sum_{w \in \mathcal{V}_G} k_w^G} = \frac{\mathbb{E}[K_G^2]}{\mathbb{E}[K_G]}.$$

2. is obvious.

3. For a undirected line graph G^L of size $N \geq 2$, we obtain

$$Q(G^L) = \frac{\mathbb{E}[K_{G^L}^2]}{\mathbb{E}[K_{G^L}]} = \frac{4 - \frac{6}{N}}{2 - \frac{2}{N}} = \frac{2N-3}{N-1}.$$

41

We show that for any connected graph $H \in \mathcal{G}^{ud}$ of size $N \geq 2$ we have

$$Q(H) \geq \frac{2N - 3}{N - 1} = 2 - \frac{1}{N - 1}. \tag{26}$$

To this end, consider the following three cases: If $k_v^H \geq 2$ for all $v \in \mathcal{V}_H$, it follows that $(k_v^H)^2 \geq 2k_v^H$ for all $v \in \mathcal{V}_H$ and thus

$$\mathbb{E}[K_H^2] \geq 2\mathbb{E}[K_H] \geq \left(2 - \frac{1}{N - 1}\right)\mathbb{E}[K_H],$$

so (26) holds. Suppose that $k_v^H \leq 2$ for all $v \in \mathcal{V}_H$. Then H is either a undirected ring graph (i.e. $k_v^H = 2$ for all $v \in \mathcal{V}_H$) or an undirected line graph. In case of the undirected ring graph choose arbitrary $v, w \in \mathcal{V}_H$ such that $(v, w) \in \mathcal{E}_H$ (and thus also $(w, v) \in \mathcal{E}_H$). Note that v, w satisfy condition (25) in the proof of Proposition B.4, so that deleting the edges (v, w) and (w, v) decreases Q. Notice that after the deletion of those edges we are left with an undirected line graph. As a last case, suppose that there exists $v, w \in \mathcal{V}_H$ such that $k_v^H \geq 3$ and $k_w^H = 1$. Choose a neighbor $s \in \mathcal{V}_H$ of v such that

- $s \neq w$,
- s is not a neighbor of w,
- there is a path from v to w not passing through the edge (v, s).

This is possible because $k_v^H \geq 3$. Indeed, if w happens to be a neighbor of v, then choose as s any of the other neighbors of v. If w is not a neighbor of v and there is a neighbor u of v such that any path from u to w passes through the node v, then let $s = u$. Finally, if w is not a neighbor of v and all neighbors u of v allow for a path from u to w which does not pass through v, then at most one of those neighbors can be a neighbor of w ($k_w^H = 1$), so let s be one of the other neighbors. Now let $\tilde{H}$ denote the graph obtained from H by removing the edges (s, v) and (v, s) and adding the edges (s, w) and (w, s). Note that $\tilde{H}$ is connected, because any path through (v, s) or (s, v) can be redirected to a path passing through w. Then $\mathbb{E}[K_H] = \mathbb{E}[K_{\tilde{H}}]$ since we did not alter the total number of edges. However,

$$
\begin{aligned}
\mathbb{E}[K_{\tilde{H}}^2] &= \frac{1}{N}\left(\sum_{\substack{u \in \mathcal{V}_H \\ u \neq v, w}} (k_u^H)^2 + (k_v^H - 1)^2 + (k_w^H + 1)^2\right) \\
&\leq \frac{1}{N}\left(\sum_{\substack{u \in \mathcal{V}_H \\ u \neq v, w}} (k_u^H)^2 + (k_v^H)^2 + (k_w^H)^2\right) = \mathbb{E}[K_H^2]
\end{aligned}
$$

since $x^2 + y^2 \geq (x-1)^2 + (y+1)^2$ whenever $x - y \geq 1$. Consequently, $Q(\tilde{H}) \leq Q(H)$. If $\tilde{H}$ falls under one of the first two cases, the assertion is proved. Otherwise, $\tilde{H}$ itself falls under the third case and can again be altered accordingly, with decreasing Q, until we finally satisfy the conditions of one of the first two cases.

4. Suppose that $G \in \mathcal{G}^{ud}$ has $N \geq 2$ nodes and contains a star node $v^* \in \mathcal{V}_G$. Let $\tilde{G} = \kappa_{n\_del}^{v^*}(G)$. We estimate

$$Q(G) = \frac{\mathbb{E}\left[K_G^2\right]}{\mathbb{E}\left[K_G\right]} = \frac{N + 2\mathbb{E}\left[K_{\tilde{G}}\right] + \mathbb{E}\left[K_{\tilde{G}}^2\right]}{2 + \mathbb{E}\left[K_{\tilde{G}}\right]} \geq \frac{N + 3\mathbb{E}\left[K_{\tilde{G}}\right]}{2 + \mathbb{E}\left[K_{\tilde{G}}\right]}$$

where we used that $\mathbb{E}\left[K_H^2\right] \geq \mathbb{E}\left[K_H\right]$ for any $H \in \mathcal{G}^{ud}$ since K_H is non-negative integer valued. Note that the function $f(x) = \frac{N+3x}{2+x}$, $x > -2$, non-decreasing for $N \leq 6$ and decreasing for $N \geq 7$. Also note that $\mathbb{E}\left[K_{\tilde{G}}\right]$ ranges between 0 and $N - 1$. Hence, for $N \leq 6$ we obtain that $Q(G) \geq N/2$ and for $N \geq 7$ we deduce that $Q(G) \geq (4N - 1)/(N + 1)$.

$\qquad\square$

Note that $(4N - 1)/(N + 1)$ is increasing in N and larger than 3 for $N \geq 7$, so there are sequences $(l_N)_{N \in \mathbb{N}}$ simultaneously satisfying the constraints given in 3. and 4. of Proposition B.6, and, of course, also 2.

B.2.4 DMFNR Based on Degree Centrality

Let $\mathfrak{C}^{deg}(v, G) = k_v^G$ for $v \in \mathcal{V}_G$ (and $\mathfrak{C}^{deg}(v, G) = \emptyset$ if $v \notin \mathcal{V}_G$).

Proposition B.6. *Consider a set $\mathcal{A} \subset \mathcal{G}^{ud}$ as in (22) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{deg}(v, G)$. Then*

1. *Q is $\mathcal{I}$-monotone for any $\mathcal{I} \subset \mathcal{I}_{e\_del}^{ud} \cup \mathcal{I}_{split}^{ud}$. Hence $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR for any cost function for $(\mathcal{A}, \mathcal{I})$.*

2. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,*

3. *$\mathcal{A}$ satisfies P2 if and only if there is a N_0 such that $l_N \geq 2$ for all $N \geq N_0$.*

4. *$\mathcal{A}$ satisfies P3 if and only if $l_N < N - 1$ for all $N \geq 1$.*

Proof. 1. and 2. are straightforward modifications of the corresponding results in Propositions 6.14 and 6.15.
3.: Note that any undirected tree graph of size $N \geq 3$ contains at least one node with a total degree of at least 2, and as before the tree graphs represent the connected graphs with minimal Q in $\mathcal{G}^{ud}$ for a given network size N since $Q(G)$ is $\mathcal{I}_{e\_del}$-monotone. This shows the 'only if'-part, and for the 'if'-part consider undirected line graphs.
4.: For a star node v^* in an undirected star graph G^* we obtain

$$k_{v^*}^{G^*} = \frac{1}{2}\left(k_{v^*}^{G^*,in} + k_{v^*}^{G^*,out}\right) = \frac{1}{2}(|\mathcal{V}_G| - 1 + |\mathcal{V}_G| - 1) = |\mathcal{V}_G| - 1.$$

$\qquad\square$

B.2.5 DMFNR Based on Closeness Centrality

Consider $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{close}(v, G)$ where

$$\mathfrak{C}^{close}(v, G) := \frac{1}{2}(\mathfrak{C}^{close}_{in}(v, G) + \mathfrak{C}^{close}_{out}(v, G)).$$

Proposition B.7. *Consider a set $\mathcal{A} \subset \mathcal{G}^{ud}$ as in (22) with $Q(G) = \max_{v \in \mathcal{V}_G} \mathfrak{C}^{close}(v, G)$. Then*

1. *Q is $\mathcal{I}$-monotone for any $\mathcal{I} \subset \mathcal{I}^{ud}_{e\_del} \cup \mathcal{I}^{ud}_{s\_iso}$. Hence $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR for any cost function for $(\mathcal{A}, \mathcal{I})$.*

2. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,*

3. *$\mathcal{A}$ satisfies P2 if and only if there is a N_0 such that $l_N \geq (1/(N-1)) \sum_{j=1}^{(N-1)/2}(2/j)$ for all $N \geq N_0$ which are odd, and $l_N \geq (1/(N-1))(\sum_{j=1}^{(N-2)/2}(2/j) + 2/N)$ for all $N \geq N_0$ which are even.*

4. *$\mathcal{A}$ satisfies P3 if and only if $l_1 < 0$ and $l_N < 1$ for all $N \geq 2$.*

Proof. See the proof of Proposition 6.17 for 1. and 2. For 4., note that the star node v^* in an undirected star graph G^* of size $|\mathcal{V}_{G^*}| \geq 2$ comes with $\mathfrak{C}^{close}_{in}(v^*, G^*) = \mathfrak{C}^{close}_{out}(v^*, G^*) = 1$, and thus $Q(G^*) = 1$.

Regarding 3., it suffices again to restrict the discussion to tree graphs since Q is $\mathcal{I}_{e\_del}$-monotone. Consider a tree graph G^T of size N, and let $v, w \in \mathcal{V}_{G^T}$ be two nodes (not necessarily unique) that come with a maximal distance $l^{G^T}_{vw}(= l^{G^T}_{wv}) \leq N - 1$ among all node pairs. Moreover, note that the path $p^{G^T}_{vw} := (v, v_2, \cdots, w)$ connecting v and w in G^T is unique since a tree graph contains no cycles. Now we distinguish between two cases:

1. Suppose $l^{G^T}_{vw}$ is even. Then the number of nodes on the path $p^{G^T}_{vw}$ is odd. Thus we find a node $u \in p^{G^T}_{vw}$ that lies in the center of the path connecting v and w, coming with $l^{G^T}_{vu}(= l^{G^T}_{uv}) = l^{G^T}_{wu}(= l^{G^T}_{uw}) = l^{G^T}_{vw}/2$. Moreover, since v and w come with the maximal distance among all node pairs, we have $l^{G^T}_{uq} \leq l^{G^T}_{vw}/2$ for all nodes $q \in \mathcal{V}_{G^T}$:

   a) The statement is clear for each node q that lies on the path connecting v and w.

   b) Suppose the path $p^{G^T}_{vq}$ between q and v or $p^{G^T}_{wq}$ between q and w does not intersect with the path $p^{G^T}_{vw}$ connecting v and w (apart from the node v or w). W.l.o.g. assume $p^{G^T}_{vq} \setminus \{v\} \cap p^{G^T}_{vw} = \emptyset$. Since all node pairs in G^T are connected by exactly one path due to the absence of cycles in G^T, we thus have $l^{G^T}_{wq} = l^{G^T}_{vw} + l^{G^T}_{vq} > l^{G^T}_{vw}$. But this contradicts the assumption that v and w come with the maximal distance among all node pairs.

c) For the last case, consider the possibility that the paths connecting node q to v and to w depart from a node $r \in p_{vw}^{G^T}$. Then $l_{vq}^{G^T} = l_{vr}^{G^T} + l_{rq}^{G^T}$ and $l_{wq}^{G^T} = l_{wr}^{G^T} + l_{rq}^{G^T}$. We can now either have $r = u$, or if not, then for either v or w, namely the node with a larger distance to q, u must lie on the path connecting v and q, or w and q, respectively. If we had the case that $l_{uq}^{G^T} > l_{vw}^{G^T}/2$, then again, since G^T contains no cycles, the path between v and q or between w and q now must be larger than $l_{vw}^{G^T}$, contradicting our initial assumption.

Now, since u lies in the centre of the path between v and w, for any distance $j \le l_{vw}^{G^T}/2$, we find two different nodes x, y on the path $p_{vw}^{G^T}$ with $l_{ux}^{G^T}, l_{uy}^{G^T} = j$. Moreover, due to $l_{uq}^{G^T} \le l_{vw}^{G^T}/2$ for all $q \in \mathcal{V}_{G^T}$ we obtain

$$\sum_{q \in \mathcal{V}_{G^T} \setminus \{u\}} \frac{1}{l_{uq}^{G^T}} \ge \sum_{j=1}^{l_{vw}^{G^T}/2} 2 \cdot \frac{1}{j} + \sum_{q \notin p_{vw}^{G^T}} \frac{1}{l_{vw}^{G^T}/2} = \sum_{j=1}^{l_{vw}^{G^T}/2} 2 \cdot \frac{1}{j} + (N - l_{vw}^{G^T} - 1) \cdot \frac{1}{l_{vw}^{G^T}/2}$$

If N is odd, then $N - l_{vw}^{G^T} - 1$ is even, and because of $l_{vw}^{G^T} \le N - 1$ we then find

$$\sum_{q \in \mathcal{V}_{G^T} \setminus \{u\}} \frac{1}{l_{uq}^{G^T}} \ge \sum_{j=1}^{(N-1)/2} 2 \cdot \frac{1}{j}.$$

In the case that N is even, we find that $N - l_{vw}^{G^T} - 1$ is odd, thus

$$\sum_{q \in \mathcal{V}_{G^T} \setminus \{u\}} \frac{1}{l_{uq}^{G^T}} \ge \sum_{j=1}^{(N-2)/2} 2 \cdot \frac{1}{j} + \frac{1}{l_{vw}^{G^T}/2} \ge \sum_{j=1}^{(N-2)/2} 2 \cdot \frac{1}{j} + \frac{2}{N-1} \ge \sum_{j=1}^{(N-2)/2} 2 \cdot \frac{1}{j} + \frac{2}{N}.$$

2. Suppose that $l_{vw}^{G^T}$ is odd. Then we find two nodes u_v and u_w in the center of the path between v and w, where $l_{vu_v}^{G^T}, l_{wu_w}^{G^T} = (l_{vw} - 1)/2$, and $l_{wu_v}^{G^T}, l_{vu_w}^{G^T} = (l_{vw} + 1)/2$. Moreover, analogously to the considerations from 1., we then find that $l_{u_v q}^{G^T}, l_{u_w q}^{G^T} \le (l_{vw}^{G^T} + 1)/2 \le N/2$ for all nodes $q \in \mathcal{V}_{G^T}$. Thus, for $u \in \{u_v, u_w\}$ we have

$$\sum_{q \in \mathcal{V}_{G^t} \setminus \{u\}} \frac{1}{l_{uq}^{G^T}} = \sum_{j=1}^{(l_{vw}^{G^T}-1)/2} 2 \cdot \frac{1}{j} + \frac{1}{(l_{vw}^{G^T}+1)/2} + \sum_{q \notin p_{vw}^{G^T}} \frac{1}{l_{uq}^{G^T}} \ge \sum_{j=1}^{(l_{vw}^{G^T}-1)/2} \frac{2}{j} + (N - l_{vw}^{G^T}) \cdot \frac{1}{(l_{vw}^{G^T}+1)/2}.$$

Now, if N is odd, then we must have $l_{u_v q}^{G^T}, l_{u_w q}^{G^T} \le (l_{vw}^{G^T} + 1)/2 \le (N - 1)/2$, and $N - l_{vw}^{G^T}$ is even, which together yields

$$\sum_{q \in \mathcal{V}_{G^T} \setminus \{u\}} \frac{1}{l_{uq}^{G^T}} \ge \sum_{j=1}^{(N-1)/2} \frac{2}{j}.$$

If N is even, then $N - l_{vw}^{G^T}$ is odd, and therefore, we can estimate

$$\sum_{q \in \mathcal{V}_{G^T}\setminus\{u\}} \frac{1}{l_{uq}^{G^T}} \geq \sum_{j=1}^{(N-1)/2} \frac{2}{j} + \frac{1}{N/2} = \sum_{j=1}^{(N-1)/2} \frac{2}{j} + \frac{2}{N}.$$

Finally, for the line graph of size N we indeed have

$$\sum_{q \in \mathcal{V}_{G^L}\setminus\{u\}} \frac{1}{l_{uq}^{G^L}} = \sum_{j=1}^{(N-1)/2} \frac{2}{j}$$

if N is odd (which then is equivalent to $l_{vw}^{G^L}$ being even). In the case that N is even (and thus $l_{vw}^{G^L}$ is odd), then

$$\sum_{q \in \mathcal{V}_{G^L}\setminus\{u\}} \frac{1}{l_{uq}^{G^L}} = \sum_{j=1}^{(N-1)/2} \frac{2}{j} + \frac{2}{N}.$$

$\square$

B.2.6 Control of the Spectral Radius of Undirected Graphs

Dynamic systems on networks are usually described by operators that depend on the adjacency matrix A_G of the graph G. The linear analysis of steady states and stability properties of these states typically leads to an analysis of the spectral properties of the adjacency matrix. Of particular importance here is the largest eigenvalue λ_1^G of A_G, called the *spectral radius* of G. For details, we refer to Section 17.4 in [54].

Example B.8. *A commonly applied model for the propagation of contagious threats in (cyber) networks is the SIS (*Susceptible-Infected-Susceptible*) Markov process, see Section 3.2 in [7]. The single node infection dynamics of the system can be described by a set of ordinary differential equations, according to Kolmogorov's forward equation. A major problem as regards the solvability of this system of ordinary differential equations is the fact that this system is not closed as higher order moments appear, cascading up to the network size. A simplified model can be obtained when assuming that all infection probabilities in the network are pairwise uncorrelated. Given a network G of size N with enumerated nodes, this so-called* NIMFA *approximation or individual-based model is governed by the set of equations*

$$\frac{d\mathbb{E}[I_i(t)]}{dt} = \tau\Big(\sum_{j=1}^{N} A_G(i,j)\big(1 - \mathbb{E}[I_i(t)]\big)\mathbb{E}[I_j(t)]\Big) - \gamma\mathbb{E}[I_i(t)], \quad i = 1,\ldots,N, \qquad (27)$$

where $\tau,\gamma > 0$ are the infection and recovery rates, and $I_i(t) = 1$ if node v_i is infected at time t, and $I_i(t) = 0$ if node v_i is susceptible at time t. The infection probabilities of this model provide upper bounds for the actual infection probabilities and can therefore be used for a conservative estimation, see Theorem 3.3 in [50]. The stability of steady states of system (27), in particular of the disease-free state $(I_1, \cdots, I_N) = (0, \cdots, 0)$, is now relevant in the analysis of the epidemic vulnerability of the network G. Linearizing

the individual-based model from (27) around the disease-free state induces the eigenvalue problem

$$\det(\tau A_G - \gamma \mathbb{I}_N - \lambda \mathbb{I}_N) = 0$$

where $\mathbb{I}_N$ is the N-dimensional identity matrix and the largest eigenvalue of $\tau A_G - \gamma \mathbb{I}_N$ is given by $\tau \lambda_1^G - \gamma$. If G is undirected and connected, it can be shown that if $\tau/\gamma < 1/\lambda_1^G$, then the disease free state is stable and no endemic state exists; if $\tau/\gamma > 1/\lambda_1^G$, then the disease-free state is unstable and there exists a unique endemic state, which is stable. For details, we refer to Section 3.4.4 in [50] and Section 17.4 in [53].

Remark B.9. *In the setting of directed graphs, however, the information of the graph spectrum may have little or no relevance in terms of graph vulnerability. For example, the only element in the spectrum of both the edgeless and the directed star graph is =. Consequently, Properties P1 and P3 cannot jointly be satisfied in a directed graph setting when choosing $Q(G) = \lambda_1^G$ for acceptance set $\mathcal{A}$. Moreover, the spectrum of directed graphs can be complex due to the lack of the adjacency matrix' symmetry.*

The following definition is needed for the proof of the next proposition:

Definition B.10. *Given a graph $G \in \mathcal{G}^{ud}$ and two nodes $v, u \in \mathcal{V}_G$, a Kelmans operation in G is a $\mathcal{I}_{shift}$-strategy where each undirected edge $\{(v,w),(w,v)\} \in \mathcal{E}_G$ is replaced by $\{(u,w),(w,u)\}$ if $w \neq u$ and $\{(u,w),(w,u)\} \cap \mathcal{E}_G = \emptyset$.*

Proposition B.11. *Consider a set $\mathcal{A} \subset \mathcal{G}^{ud}$ as in (22) with $Q(G) = \lambda_1^G$. Then*

1. *Q is $\mathcal{I}$-monotone for any $\mathcal{I} \subset \mathcal{I}_{e\_del}^{ud} \cup \mathcal{I}_{split}^{ud}$. Hence $(\mathcal{A}, \mathcal{I}, \mathcal{C})$ is a DMFNR for any cost function for $(\mathcal{A}, \mathcal{I})$.*

2. *$\mathcal{A}$ satisfies P1 if and only if $l_N \geq 0$ for all $N \geq 2$,*

3. *$\mathcal{A}$ satisfies P2 if and only if there is a N_0 such that $l_N \geq \max_{j \in \{1, \cdots, N\}} \cos(\pi j/(N+1))$ for all $N \geq N_0$. In particular, this is the case if there is a N_0 such that $l_N \geq 2$ for all $N \geq N_0$.*

4. *$\mathcal{A}$ satisfies P3 if and only if $l_N < \sqrt{(N-1)}$ for all $N \geq 1$.*

Proof. 1. Q is $\mathcal{I}_{e\_del}^{ud}$-monotone according to [16, Proposition 3.1.1]. Standard results show that Q is also $\mathcal{I}_{split}^{ud}$-monotone: Let $G \in \mathcal{G}^{ud}$, and $H = \kappa_{split}^{\mathcal{J},v,\tilde{v}}(G)$ a network resulting from a split of node v by adding a new node $\tilde{v}$ and rewiring edges contained in $\mathcal{J}$, where $(v,w) \in \mathcal{J} \Leftrightarrow (w,v) \in \mathcal{J}$. Then we can construct a new graph H' from H by a consecutive edge shift where all edges $(\tilde{v}, w)$ are replaced by (v, w) and all $(w, \tilde{v})$ by (w, v). This is a particular example of a Kelmans operation, see Section 3.1.3 in [16] for details, since $\mathcal{N}_v^H \cap \mathcal{N}_{\tilde{v}}^H = \emptyset$. Note that $H' = G \dot{\cup}(\{\tilde{v}\}, \emptyset)$ is a disjoint union of G and the isolated node $\tilde{v}$. Therefore, we have $\lambda_1^{H'} = \lambda_1^G$, and the spectral radius of a graph is non-decreasing under a Kelmans operation, see [16, Proposition 3.1.5]. This gives $\lambda_1^H \leq \lambda_1^{H'} = \lambda_1^G$.

2. trivial

3. Note that undirected line graphs of size N have a minimal spectral radius among all connected graphs of this size in $\mathcal{G}^{ud}$, cf. [61, Lemma 1]. Their spectrum consists of the eigenvalues $\lambda_j = 2\cos(\pi j/(N+1))$, $j = 1, \cdots, N$, see [16, Section 1.4.4].

4. For an undirected star graph of size N, simple calculations show that the spectrum consists of the eigenvalues $\sqrt{N-1}$ and $-\sqrt{N-1}$, both with a multiplicity of one, and the eigenvalue 0 with multiplicity of $N-2$.

$\square$

References

[1] Afrin, T. & Yodo, N. (2018) A concise survey of advancements in recovery strategies for resilient complex networks. *Journal of Complex Networks*, **7**(3), 393–420.

[2] Amini, H., Cont, R. & Minca, A. (2016) Resilience to contagion in financial networks. *Mathematical Finance*, **26**(2), 329–365.

[3] Antonio, Y., Indratno, S. W. & Simanjuntak, R. (2021) Cyber Insurance Ratemaking: A Graph Mining Approach. *Risks*, **9**(12).

[4] Armenti, Y., Crépey, S., Drapeau, S. & Papapantoleon, A. (2018) Multivariate Shortfall Risk Allocation and Systemic Risk. *SIAM Journal on Financial Mathematics*, **9**(1), 90–126.

[5] Artzner, P., Delbaen, F., Eber, J.-M. & Heath, D. (1999) Coherent Measures of Risk. *Mathematical Finance*, **9**(3), 203–228.

[6] Awiszus, K., Bell, Y., Lüttringhaus, J., Svindland, G., Voß, A. & Weber, S. (2024) Building resilience in cybersecurity: An artificial lab approach. *Journal of Risk and Insurance*, **91**(3), 753–800.

[7] Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A. & Weber, S. (2023) Modeling and pricing cyber insurance. *European Actuarial Journal*, **13**, 1–53.

[8] Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D. & Williams, J. (2017) Contagion in cyber security attacks. *Journal of the Operational Research Society*, **68**, 780–791.

[9] Barabási, A.-L. & Pósfai, M. (2016) *Network Science*. Cambridge University Press.

[10] Bessy-Roland, Y., Boumezoued, A. & Hillairet, C. (2021) Multivariate Hawkes process for cyber insurance. *Annals of Actuarial Science*, **15**, 14–39.

[11] Biagini, F., Fouque, J.-P., Frittelli, M. & Meyer-Brandis, T. (2019) A unified approach to systemic risk measures via acceptance sets. *Mathematical Finance*, **29**(1), 329–367.

[12] Biagini, F., Meyer-Brandis, T. & Svindland, G. (2014) The Mathematical Concept of Measuring Risk. In Klüppelberg, C., Straub, D. & Welpe, I. M., editors, *Risk - A Multidisciplinary Introduction*, pages 133–150, Cham. Springer International Publishing.

[13] Bollobás, B. (1998) *Modern Graph Theory*. Graduate Texts in Mathematics 184. Springer.

[14] Boumezoued, A., Cherkaoui, Y. & Hillairet, C. (2023) Cyber risk modeling using a two-phase Hawkes process with external excitation. Working paper.

[15] Brauchle, J.-P., Göbel, M., Seiler, J. & von Busekist, C. (2020) Cyber Mapping the Financial System. *Carnegie Endowment for International Peace.*

[16] Brouwer, A. E. & Haemers, W. H. (2012) *Spectra of graphs.* Berlin: Springer.

[17] Chen, C., Iyengar, G. & Moallemi, C. C. (2013) An Axiomatic Approach to Systemic Risk. *Management Science*, **59**(6), 1373–1388.

[18] Chernikova, A., Gozzi, N., Boboila, S., Angadi, P., Loughner, J., Wilden, M., Perra, N., Eliassi-Rad, T. & Oprea, A. (2022) Cyber Network Resilience Against Self-Propagating Malware Attacks. In Atluri, V., Di Pietro, R., Jensen, C. D. & Meng, W., editors, *Computer Security – ESORICS 2022*, pages 531–550, Cham. Springer International Publishing.

[19] Chernikova, A., Gozzi, N., Perra, N., Boboila, S., Eliassi-Rad, T. & Oprea, A. (2023) Modeling self-propagating malware with epidemiological models. *Applied Network Science*, **8**(52).

[20] Chiaradonna, S., Jevtić, P. & Lanchier, N. (2023) Framework for cyber risk loss distribution of hospital infrastructure: Bond percolation on mixed random graphs approach. *Risk Analysis*, **43**(12), 2450–2485.

[21] Dacorogna, M., Debbabi, N. & Kratz, M. (2023) Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research*, **311**(2), 708–729.

[22] Dacorogna, M. & Kratz, M. (2023) Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal.*

[23] Detering, N., Mayer-Brandis, T., Panagiotou, K. & Ritter, D. (2019a) Systemic Risk in Networks. In *Network Science. An Aerial View*, pages 59–77. Springer.

[24] Detering, N., Meyer-Brandis, T., Panagiotou, K. & Ritter, D. (2019b) Managing Default Contagion in Inhomogeneous Financial Networks. *SIAM Journal on Financial Mathematics*, **10**(2), 578–614.

[25] Eisenbach, T. M., Kovner, A. & Lee, M. J. (2021) Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis. Technical Report 909, Federal Reserve Bank of New York.

[26] Eisenberg, L. & Noe, T. H. (2001) Systemic Risk in Financial Systems. *Management Science*, **47**(2), 236–249.

[27] Eling, M. (2020) Cyber risk research in business and actuarial science. *European Actuarial Journal*, pages 1–31.

[28] ESRB, editor (2020) *Systemic cyber risk*. European Systemic Risk Board.

[29] ESRB, editor (2022) *Mitigating systemic cyber risk*. European Systemic Risk Board.

[30] Estrada, E., Hatano, N. & Benzi, M. (2012) The physics of communicability in complex networks. *Physics Reports*, **514**(3), 89–119.

[31] European Union (2022) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). .

[32] Fahrenwaldt, M., Weber, S. & Weske, K. (2018) Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin: The Journal of the IAA*, **48**(3), 1175–1218.

[33] Föllmer, H. & Klüppelberg, C. (2014) Spatial Risk Measures: Local Specification and Boundary Risk. In Crisan, D., Hambly, B. & Zariphopoulou, T., editors, *Stochastic Analysis and Applications 2014*, pages 307–326, Cham. Springer International Publishing.

[34] Föllmer, H. & Schied, A. (2016) *Stochastic Finance: An Introduction in Discrete Time*. Walter de Gruyter, 4 edition.

[35] Föllmer, H. & Weber, S. (2015) The Axiomatic Approach to Risk Measures for Capital Determination. *Annual Review of Financial Economics*, **7**(1), 301–337.

[36] Foroutan, N., Schröder, M. & Dengel, A. (2024) CO-Fun: A German Dataset on Company Outsourcing in Fund Prospectuses for Named Entity Recognition and Relation Extraction. .

[37] Forscey, D., Bateman, J., Beecroft, N. & Woods, B. (2022) Systemic Cyber Risk: A Primer. *Carnegie Endowment for International Peace and the Aspen Institute*.

[38] Fouque, J.-P. & Langsam, J. A., editors (2013) *Handbook on Systemic Risk*. Cambridge University Press.

[39] Föllmer, H. (2014) Spatial risk measures and their local specification: The locally law-invariant case. *Statistics & Risk Modeling*, **31**(1), 79–101.

[40] Gandy, A. & Veraart, L. A. M. (2017) A Bayesian Methodology for Systemic Risk Assessment in Financial Networks. *Management Science*, **63**(12), 4428–4446.

[41] Hillairet, C. & Lopez, O. (2021) Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models. *Scandinavian Actuarial Journal*, pages 1–24.

[42] Hillairet, C., Lopez, O., d'Oultremont, L. & Spoorenberg, B. (2022) Cyber-contagion model with network structure applied to insurance. *Insurance: Mathematics and Economics*, **107**, 88–101.

[43] Hillairet, C., Réveillac, A. & Rosenbaum, M. (2023) An expansion formula for Hawkes processes and application to cyber-insurance derivatives. *Stochastic Processes and their Applications*, **160**, 89–119.

[44] Hoffmann, H., Meyer-Brandis, T. & Svindland, G. (2016) Risk-consistent conditional systemic risk measures. *Stochastic Processes and their Applications*, **126**(7), 2014–2037.

[45] Hoffmann, H., Meyer-Brandis, T. & Svindland, G. (2018) Strongly consistent multivariate conditional risk measures. *Mathematics and Financial Economics*, **12**, 413–444.

[46] Hurd, T. R. (2016) *Contagion! Systemic Risk in Financial Networks*. Springer.

[47] Jackson, M. O. & Pernoud, A. (2021) Systemic Risk in Financial Networks: A Survey. *Annual Review of Economics*, **13**(1), 171–202.

[48] Jevtić, P. & Lanchier, N. (2020) Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology. *Insurance: Mathematics and Economics*, **91**, 209–223.

[49] Kenah, E. & Robins, J. M. (2007) Second look at the spread of epidemics on networks. *Phys. Rev. E*, **76**, 036113.

[50] Kiss, I. Z., Miller, J. C. & Simon, P. L. (2017) *Mathematics of Epidemics on Networks*, volume 46 of *Interdisciplinary Applied Mathematics*. Springer.

[51] Latora, V. & Marchiori, M. (2001) Efficient Behavior of Small-World Networks. *Phys. Rev. Lett.*, **87**, 198701.

[52] Louzada, V. H. P., Daolio, F., Herrmann, H. J. & Tomassini, M. (2013) Smart rewiring for network robustness. *Journal of Complex Networks*, **1**(2), 150–159.

[53] Mieghem, P. V. (2014) *Performance Analysis of Complex Networks and Systems*. Cambridge University Press, Cambridge.

[54] Newman, M. (2018) *Networks*. Oxford University Press.

[55] Norwegian Ministry of Justice and Public Security (2022-2023) National control and cyber resilience to safeguard national security. As open as possible, as secure as necessary. Technical Report Meld. St. 9.

[56] Pastor-Satorras, R., Castellano, C., Van Mieghem, P. & Vespignani, A. (2015) Epidemic processes in complex networks. *Reviews of Modern Physics*, **87**, 925–979.

[57] Ros, G., editor (2020) *The making of a cyber crash: a conceptual model for systemic risk in the financial sector*, number 16. European Systemic Risk Board.

[58] Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020) Zero Trust Architecture. Technical report, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.

[59] Schaeffer, S. E., Valdés, V., Figols, J., Bachmann, I., Morales, F. & Bustos-Jiménez, J. (2021) Characterization of robustness and resilience in graphs: a mini-review. *Journal of Complex Networks*, **9**(2), cnab018.

[60] Schröder, M., Krüger, J., Foroutan, N., Horn, P., Fricke, C., Delikanli, E., Maus, H. & Dengel, A. (2024) Towards Cyber Mapping the German Financial System with Knowledge Graphs. In Meroño Peñuela, A., Dimou, A., Troncy, R., Hartig, O., Acosta, M., Alam, M., Paulheim, H. & Lisena, P., editors, *The Semantic Web*, pages 270–288, Cham. Springer Nature Switzerland.

[61] van Dam, E. & Kooij, R. (2007) The minimal spectral radius of graphs with a given diameter. *Linear Algebra and its Applications*, **423**(2), 408–419.

[62] Ventresca, M. & Aleman, D. (2014) Network robustness versus multi-strategy sequential attack. *Journal of Complex Networks*, **3**(1), 126–146.

[63] Welburn, J. W. & Strong, A. M. (2022) Systemic Cyber Risk and Aggregate Impacts. *Risk Analysis*, **42**(8), 1606–1622.

[64] Xu, M. & Hua, L. (2019) Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, **23**(2), 220–249.

[65] Zeller, G. & Scherer, M. (2021) A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*, pages 1–53.

[66] Zeller, G. & Scherer, M. (2023) Risk mitigation services in cyber insurance: optimal contract design and price structure. *The Geneva Papers on Risk and Insurance - Issues and Practice*, **48**, 502–547.

[67] Zeller, G. & Scherer, M. (2024) Is accumulation risk in cyber methodically underestimated?. *European Actuarial Journal*.