

Probability Distributions on Partially Ordered Sets and Network Security Games

Mathieu Dahan

Center for Computational Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, mdahan@mit.edu

Saurabh Amin

Department of Civil and Environmental Engineering, and Institute for Data, Systems, and Society,
Massachusetts Institute of Technology, Cambridge, MA 02139, amins@mit.edu

Patrick Jaillet

Department of Electrical Engineering and Computer Science, Laboratory for Information and Decision Systems,
and Operations Research Center, Massachusetts Institute of Technology Cambridge, MA 02139, jaillet@mit.edu

We consider the following problem: Does there exist a probability distribution over subsets of a finite partially ordered set (poset), such that a set of constraints involving marginal probabilities of the poset's elements and maximal chains is satisfied? In this article, we present a combinatorial algorithm to positively resolve this question. We show that this result plays a crucial role in the equilibrium analysis of a generic security game on a capacitated flow network. The game involves a routing entity that sends its flow through the network while facing path transportation costs, and an interdicator who simultaneously interdicts one or more edges while facing edge interdiction costs. The first (resp. second) player seeks to maximize the value of effective (resp. interdicted) flow net the total transportation (resp. interdiction) cost. Using our existence result on posets and strict complementary slackness in linear programming, we show that the equilibrium properties of this game can be described using primal and dual solutions of a minimum cost circulation problem. Our analysis provides a new characterization of the critical network components.

Key words: probability distributions on posets, network security games, duality theory.

1. Introduction. In this article, we study the problem of showing the existence of a probability distribution over a partially ordered set (or poset) that satisfies a set of constraints involving marginal probabilities of the poset's elements and maximal chains. This problem is directly motivated by the technical issues arising in the equilibrium analysis of a generic network security game, in which a strategic interdicator seeks to disrupt the flow of a routing entity. In particular, our existence result on posets enables us to show that the equilibrium structure of the game can be described using primal and dual solutions of a minimum cost circulation problem. Furthermore, we show that the set of critical components for our network security game can be characterized using strict complementary slackness in linear programming.

1.1. Probability distributions over posets. For a given finite nonempty poset, we consider a problem in which each element is associated with a value between 0 and 1; additionally, each

maximal chain has a value at most 1. We want to determine if there exists a probability distribution over the subsets of the poset such that: (i) The probability with which each element of the poset is in a subset is *equal to* its corresponding value; and (ii) the probability with which each maximal chain of the poset intersects with a subset is *as large as* its corresponding value. Solving this problem, denoted (\mathcal{D}) , is equivalent to resolving the feasibility of a polyhedral set. However, geometric ideas – such as the ones involving the use of Farkas’ lemma or Carathéodory’s theorem – cannot be applied to solve this problem, because they do not capture the structure of posets. We positively resolve problem (\mathcal{D}) under two conditions that are naturally satisfied for our purposes:

1. The value of each maximal chain is no more than the sum of the values of its elements.
2. The values of the maximal chains satisfy a conservation law. Particularly, let C be the union of two intersecting maximal chains. Then, for any decomposition of C into two maximal chains, the sum of the corresponding values is constant.

Under these two conditions, we prove the feasibility of problem (\mathcal{D}) (Theorem 1). First, we show that solving (\mathcal{D}) is equivalent to proving that the optimal value of an exponential-size linear optimization problem, denoted (\mathcal{Q}) , is no more than 1 (Proposition 1). Then, to optimally solve (\mathcal{Q}) , we design a combinatorial algorithm (Algorithm 1) that exploits the relation between the values associated with the poset’s elements and maximal chains. In particular, we show that the optimal value of (\mathcal{Q}) can be computed in closed form: it is equal to the largest value associated with an element or maximal chain of the poset, which is no more than 1 (Theorem 2). Each iteration of the algorithm involves constructing a subposet, selecting its set of minimal elements, and assigning a specific weight to it. The proof of optimality of the algorithm is carried out in three steps: First, we prove that it is well-defined (Proposition 2). Secondly, we show that it terminates and outputs a feasible solution of (\mathcal{Q}) (Proposition 3). Finally, we show that at termination, it assigns a total weight that is exactly equal to the optimal value of (\mathcal{Q}) (Proposition 4). Importantly, in the design of the algorithm, we need to ensure that the conservation law satisfied by the values associated with the maximal chains of the poset is preserved after each iteration. This design feature enables us to obtain a relation between maximal chains after each iteration (Lemma 3), which leads to optimality guarantee of the algorithm.

Next, we show that the feasibility of problem (\mathcal{D}) on posets is crucial for the equilibrium analysis of a class of two-player non-cooperative games on flow networks.

1.2. Network security games. We model a network security game between player 1 (routing entity) that sends its flow through the network while facing heterogeneous path transportation costs; and player 2 (interdictor) who simultaneously chooses an interdiction plan comprised of one or more edges. Player 1 (resp. player 2) seeks to maximize the value of effective (resp. interdicted)

flow net the transportation (resp. interdiction) cost. We adopt mixed strategy Nash equilibria as the solution concept of this game.

Our security game is rich and general in that it models heterogeneous costs of transportation and interdiction. It models the strategic situation in which player 1 is an operator who wants to route flow (e.g. water, oil, or gas) through pipelines, while player 2 is an attacker who targets multiple pipes in order to steal or disrupt the flow. An alternative setting is the one where player 1 is a malicious entity composed of routers who carry illegal (or dangerous) goods through a transportation network (i.e., roads, rivers, etc.), and player 2 is a security agency that dispatches interdictors to intercept malicious routers and prevent the illegal goods from crossing the network. In both these settings, mixed strategies can be viewed as the players introducing randomization in implementing their respective actions. For instance, player 1's mixed strategy models a randomized choice of paths for routing its flow of goods through the network, while player 2's mixed strategy indicates a randomized dispatch of interdictors to disrupt or intercept the flow.

The existing literature in network interdiction has dealt with this type of problems in a sequential (Stackelberg) setting (see Avenhaus and Canty [4], Ball et al. [6], Ratliff et al. [24], Wollmer [28]). Typically, these problems are solved using large-scale integer programming techniques, and are staple for designing system interdiction and defense (see Bertsimas et al. [9], Cormican et al. [10], Neumayer et al. [22], Sullivan and Cole Smith [25], Wood [29]). However, these models do not capture the situations in which the interdictor is capable of simultaneously interdicting multiple links, possibly in a randomized manner. Recently, Bertsimas et al. [8] considered a sequential game in which the interdictor first randomly interdicts a fixed number of edges, and then the operator routes a feasible flow in the network. The interdictor's goal is to minimize the largest amount of flow that reaches the destination node. Although this model is equivalent to a simultaneous game, our model is general in that we do not impose any restriction on the number of edges that can be simultaneously interdicted. Additionally, we account for transportation and interdiction costs faced by the players.

Our work is also motivated by previous problems studied in network security games (e.g. Baykal-Gürsoy et al. [7], Gueye et al. [13], Szeto [26]). However, the available results in this line of work are for simpler cases, and do not apply to our model. Related to our work are the network security games proposed by Washburn and Wood [27] and Gueye and Marbukh [14]. In Washburn and Wood [27], the authors consider a simultaneous game where an evader chooses one source-destination path and the interdictor inspects one edge. In this model, the interdictor's (resp. evader's) objective is to maximize (resp. minimize) the probability with which the evader is detected by the interdictor. Gueye and Marbukh [14] model an operator who routes a feasible flow in the network, and an attacker who disrupts one edge. The attacker's (resp. operator's) goal is to maximize (minimize)

the amount of lost flow. Additionally, the attacker faces a cost of attack. In contrast, our model allows the interdictor to inspect multiple edges simultaneously, and accounts for the transportation cost faced by the routing entity.

The generality of our model renders known methods for analyzing security games inapplicable to our game. Indeed, prior work has considered solution approaches based on max-flows and min-cuts, and used these objects as metrics of criticality for network components (see Assadi et al. [2], Dwivedi and Yu [11], Gueye et al. [13]). However, these objects cannot be applied to describe the critical network components in our game due to the heterogeneity of path interdiction probabilities resulting from the transportation costs. A related issue is that computing a Nash equilibrium of our game is hard because of the large size of the players' action sets. Indeed, player 1 (resp. player 2) chooses a probability distribution over an infinite number of feasible flows (resp. exponential number of subsets of edges). Therefore, well-known algorithms for computing (approximate) Nash equilibria are practically inapplicable for this setting (see Lipton et al. [19] and McMahan et al. [20]). Guo et al. [15] developed a column and constraint generation algorithm to approximately solve their network security game. However, it cannot be applied to our model due to the transportation and interdiction costs that we consider.

Instead, we propose an approach for analyzing equilibria of our game based on a minimum cost circulation problem, which we denote (\mathcal{M}) , and our existence problem on posets (\mathcal{D}) . In particular, we show (Proposition 5) that Nash equilibria of the game can be described using primal and dual optimal solutions of (\mathcal{M}) , if they satisfy the following conditions: (i) each network edge is interdicted with probability given by the corresponding optimal dual variable; and (ii) each source-destination path is interdicted with some probability, derived from the properties of the network, as well as the optimal dual solution. In fact, this problem is an instantiation of problem (\mathcal{D}) , and an equilibrium interdiction strategy can be constructed with our combinatorial algorithm (Algorithm 1).

The main insights from our equilibrium analysis are as follows:

1. An equilibrium strategy for player 1 is given by an optimal flow of (\mathcal{M}) , and marginal edge interdiction probabilities resulting from player 2's equilibrium strategy are given by the dual solutions of (\mathcal{M}) . This result circumvents the complexity of equilibrium computation for our game-theoretic model. Computing an equilibrium interdiction strategy with our algorithm is NP-hard due to the enumeration of exponentially many maximal chains. However, the marginal edge interdiction probabilities and route flows can be obtained in polynomial time by solving the minimum cost circulation problem (\mathcal{M}) (see Karmarkar [18] and Orlin et al. [23]).

2. Primal-dual pairs of solutions of (\mathcal{M}) that satisfy strict complementary slackness provide a new characterization of the critical components in the network. Specifically, the primal (resp. dual) solution provides the paths (resp. edges) that are chosen (resp. interdicted) in at least one Nash

equilibrium of the game (Theorem 3). This result generalizes the classical min-cut-based metrics of network criticality previously studied in the network interdiction literature (see Assimakopoulos [3], McMasters et al. [21], Washburn and Wood [27], Wood [29]). Indeed, we show that in our more general setting, multiple edges in a source-destination path may be interdicted in equilibrium, and cannot be represented with a single cut of the network. We address this issue by computing the dual solutions of (\mathcal{M}) , and by constructing an equilibrium interdiction strategy using our combinatorial algorithm (Algorithm 1) for posets.

The rest of the paper is organized as follows: In Section 2, we pose our existence problem on posets, and introduce our main feasibility result. Section 3 constructs a solution to the existence problem. The implications of our existence result are then demonstrated in Section 4, where we study our generic network security game. Lastly, we provide some concluding remarks in Section 5.

2. Problem formulation and main result. In this section, we first recall some standard definitions in order theory. We then pose our problem of proving the existence of probability distributions over partially ordered sets, and introduce our main result about its feasibility.

2.1. Order theoretic definitions. A finite *partially ordered set* or *poset* P is a pair (X, \preceq) , where X is a finite set and \preceq is a partial order on X , i.e., \preceq is a binary relation on X satisfying:

- Reflexivity: $\forall x \in X, x \preceq x$ in P .
- Antisymmetry: $\forall (x, y) \in X^2$, if $x \preceq y$ in P and $y \preceq x$ in P , then $x = y$.
- Transitivity: $\forall (x, y, z) \in X^3$, if $x \preceq y$ in P and $y \preceq z$ in P , then $x \preceq z$ in P .

Given $(x, y) \in X^2$, we denote $x \prec y$ in P if $x \preceq y$ in P and $x \neq y$. We say that x and y are *comparable* in P if either $x \prec y$ in P or $y \prec x$ in P . On the other hand, x and y are *incomparable* in P if neither $x \prec y$ in P nor $y \prec x$ in P . We say that x is *covered* in P by y , denoted $x \prec : y$ in P , if $x \prec y$ in P and there does not exist $z \in X$ such that $x \prec z$ in P and $z \prec y$ in P . When there is no confusion regarding the poset, we abbreviate $x \preceq y$ in P by writing $x \preceq y$, etc.

Let Y be a nonempty subset of X , and let $\preceq|_Y$ denote the restriction of \preceq to Y . Then, $\preceq|_Y$ is a partial order on Y , and $(Y, \preceq|_Y)$ is a *subposet* of P . A poset $P = (X, \preceq)$ is called a *chain* (resp. *antichain*) if every distinct pair of elements in X is comparable (resp. incomparable) in P . Given a poset $P = (X, \preceq)$, a nonempty subset $Y \subseteq X$ is a *chain* (resp. an *antichain*) in P if the subposet $(Y, \preceq|_Y)$ is a chain (resp. an antichain). A single element of X is both a chain and an antichain.

Given a poset $P = (X, \preceq)$, an element $x \in X$ is a *minimal* element (resp. *maximal* element) if there are no elements $y \in X$ such that $y \prec x$ (resp. $x \prec y$). Note that any chain has a unique minimal and maximal element. A chain $C \subseteq X$ (resp. antichain $A \subseteq X$) is *maximal* in P if there are no other chains C' (resp. antichains A') in P that contain C (resp. A). Let \mathcal{C} and \mathcal{A} respectively denote the set of maximal chains and antichains in P . A maximal chain $C \in \mathcal{C}$ of size n can be represented as $C = \{x_1, \dots, x_n\}$ where $\forall k \in \llbracket 1, n-1 \rrbracket, x_k \prec : x_{k+1}$. We state the following property:

LEMMA 1. *Given a finite nonempty poset P , the set of minimal elements of P is an antichain of P , and intersects with every maximal chain of P .*

Proof in Appendix A.

Given a poset $P = (X, \preceq)$, we consider its *cover graph*, denoted $H_P = (X, E_P)$. H_P is an undirected graph whose set of vertices is X , and whose set of edges is given by $E_P := \{(x, y) \in X^2 \mid x \prec y \text{ or } y \prec x\}$. When H_P is represented such that for all $x \prec y \in X$, the vertical coordinate of the vertex corresponding to y is higher than the vertical coordinate of the vertex corresponding to x , the resulting diagram is called a *Hasse diagram* of P .

We now introduce the notion of subposet generated by a subset of maximal chains. Given a poset $P = (X, \preceq)$, let $X' \subseteq X$ be a subset of elements, let $\mathcal{C}' \subseteq \mathcal{C}$ be a subset of maximal chains of P , and consider the binary relation $\preceq_{\mathcal{C}'}$ defined by $\forall (x, y) \in X'^2$, $x \preceq_{\mathcal{C}'} y \iff (x = y) \text{ or } (\exists C \in \mathcal{C}' \text{ such that } x, y \in C \text{ and } x \prec y)$. Furthermore, we consider that if $C^1 = \{x_{-k}, \dots, x_{-1}, x^*, x_1, \dots, x_n\}$ and $C^2 = \{y_{-l}, \dots, y_{-1}, x^*, y_1, \dots, y_m\}$ are in \mathcal{C}' and intersect in $x^* \in X'$, then \mathcal{C}' also contains $C_1^2 = \{x_{-k}, \dots, x_{-1}, x^*, y_1, \dots, y_m\}$ and $C_2^1 = \{y_{-l}, \dots, y_{-1}, x^*, x_1, \dots, x_n\}$. In other words, \mathcal{C}' preserves the decomposition of maximal chains intersecting in X' . Then, we have the following lemma:

LEMMA 2. *Consider the poset $P = (X, \preceq)$, a subset $X' \subseteq X$, and a subset $\mathcal{C}' \subseteq \mathcal{C}$ that preserves the decomposition of maximal chains intersecting in X' . Then, $P' = (X', \preceq_{\mathcal{C}'})$ is also a poset. Furthermore, for any maximal chain C of P' of size at least two, there exists a maximal chain C' in \mathcal{C}' such that $C = C' \cap X'$.*

Proof in Appendix A.

The subposet $P' = (X', \preceq_{\mathcal{C}'})$ of P in Lemma 2 satisfies the property that if two elements in X' are comparable in P , and belong to a same maximal chain $C \in \mathcal{C}'$, then they are also comparable in P' . Graphically, this is equivalent to removing the edges from the Hasse diagram H_P if their two end nodes do not belong to a same maximal chain $C \in \mathcal{C}'$.

EXAMPLE 1. Consider the poset P represented by the Hasse Diagram H_P in Figure 1.

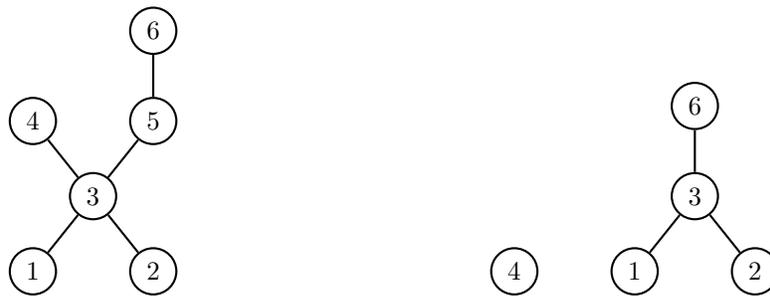


FIGURE 1. On the left is represented a Hasse diagram of a poset P . On the right is represented a Hasse diagram of the subposet $P' = (X', \preceq_{\mathcal{C}'})$ of P , where $X' = \{1, 2, 3, 4, 6\}$ and $\mathcal{C}' = \{\{1, 3, 5, 6\}, \{2, 3, 5, 6\}\}$.

We observe that $1 \prec 4$, $2 \prec 3$; 1 and 3 are comparable, but 4 and 6 are incomparable; $\{2, 4\}$ is a chain in P , but is not maximal since it is contained in the maximal chain $\{2, 3, 4\}$. Similarly, $\{4\}$ is an antichain in P , but is not maximal since it is contained in the maximal antichain $\{4, 5\}$. The set of maximal chains and antichains of P are given by $\mathcal{C} = \{\{1, 3, 4\}, \{2, 3, 5, 6\}, \{1, 3, 5, 6\}, \{2, 3, 4\}\}$ and $\mathcal{A} = \{\{1, 2\}, \{3\}, \{4, 5\}, \{4, 6\}\}$, respectively. The set of minimal elements of P is given by $\{1, 2\}$, and intersects with every maximal chain in \mathcal{C} . Finally, $P' = (X', \preceq_{C'})$, where $X' = \{1, 2, 3, 4, 6\}$ and $\mathcal{C}' = \{\{1, 3, 5, 6\}, \{2, 3, 5, 6\}\}$, is a poset, and is illustrated in Figure 1. \triangle

2.2. Existence of probability distributions over posets. Consider a finite nonempty poset $P = (X, \preceq)$. Let $\mathcal{P} := 2^X$ denote the power set of X , and let $\Delta(\mathcal{P}) := \{\sigma \in \mathbb{R}_+^{|\mathcal{P}|} \mid \sum_{S \in \mathcal{P}} \sigma_S = 1\}$ denote the set of probability distributions over \mathcal{P} . We are concerned with the setting where each element $x \in X$ is associated with a value $\rho_x \in [0, 1]$, and each maximal chain $C \in \mathcal{C}$ has a value $\pi_C \leq 1$. Our problem is to determine if there exists a probability distribution $\sigma \in \Delta(\mathcal{P})$ such that for every element $x \in X$, the probability that x is in a subset $S \in \mathcal{P}$ is equal to ρ_x ; and for every maximal chain $C \in \mathcal{C}$, the probability that C intersects with a subset $S \in \mathcal{P}$ is at least π_C . That is,

$$(\mathcal{D}): \quad \exists \sigma \in \mathbb{R}_+^{|\mathcal{P}|} \text{ such that } \begin{cases} \sum_{\{S \in \mathcal{P} \mid x \in S\}} \sigma_S = \rho_x, & \forall x \in X, & (1a) \\ \sum_{\{S \in \mathcal{P} \mid S \cap C \neq \emptyset\}} \sigma_S \geq \pi_C, & \forall C \in \mathcal{C}, & (1b) \\ \sum_{S \in \mathcal{P}} \sigma_S = 1. & & (1c) \end{cases}$$

For the case in which $\pi_C \leq 0$ for all maximal chains $C \in \mathcal{C}$, constraints (1b) can be removed, and the feasibility of (D) follows from Carathéodory's theorem. However, no known results can be applied to the general case. Note that although (1a)-(1c) form a polyhedral set, Farkas' lemma cannot be directly used to evaluate its feasibility. Instead, in this article, we study the feasibility of (D) using order-theoretic properties of the problem. We assume two natural conditions on $\rho = (\rho_x)_{x \in X}$ and $\pi = (\pi_C)_{C \in \mathcal{C}}$, which we introduce next.

Firstly, for feasibility of (D), ρ and π must satisfy the following inequality:

$$\forall C \in \mathcal{C}, \quad \sum_{x \in C} \rho_x \geq \pi_C. \quad (2)$$

Indeed, if (D) is feasible, then for $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ satisfying (1a)-(1c), the following holds:

$$\forall C \in \mathcal{C}, \quad \sum_{x \in C} \rho_x \stackrel{(1a)}{=} \sum_{x \in C} \sum_{\{S \in \mathcal{P} \mid x \in S\}} \sigma_S = \sum_{S \in \mathcal{P}} \sigma_S \sum_{x \in C} \mathbf{1}_{\{x \in S\}} = \sum_{S \in \mathcal{P}} \sigma_S |S \cap C| \geq \sum_{\{S \in \mathcal{P} \mid S \cap C \neq \emptyset\}} \sigma_S \stackrel{(1b)}{\geq} \pi_C.$$

That is, the necessity of (2) follows from the fact that for any probability distribution over \mathcal{P} , and any subset of elements $C \subseteq X$, the probability that C intersects with a subset $S \in \mathcal{P}$ is upper bounded by the sum of the probabilities with which each element in C is in a subset $S \in \mathcal{P}$.

Secondly, we consider that π satisfies a specific condition for each pair of maximal chains that intersect each other. Consider any pair of maximal chains C^1 and C^2 of P , with $C^1 \cap C^2 \neq \emptyset$. Let $x^* \in C^1 \cap C^2$, and let us rewrite $C^1 = \{x_{-k}, \dots, x_{-1}, x^*, x_1, \dots, x_n\}$ and $C^2 = \{y_{-l}, \dots, y_{-1}, x^*, y_1, \dots, y_m\}$. Then, P also contains two maximal chains $C_1^2 = \{x_{-k}, \dots, x_{-1}, x^*, y_1, \dots, y_m\}$ and $C_2^1 = \{y_{-l}, \dots, y_{-1}, x^*, x_1, \dots, x_n\}$ that satisfy $C^1 \cup C^2 = C_1^2 \cup C_2^1$; see Figure 2 for an illustration. We require that π satisfy the following condition:

$$\pi_{C^1} + \pi_{C^2} = \pi_{C_1^2} + \pi_{C_2^1}. \quad (3)$$

Thus, (3) can be viewed as a *conservation law* on the maximal chains in C .

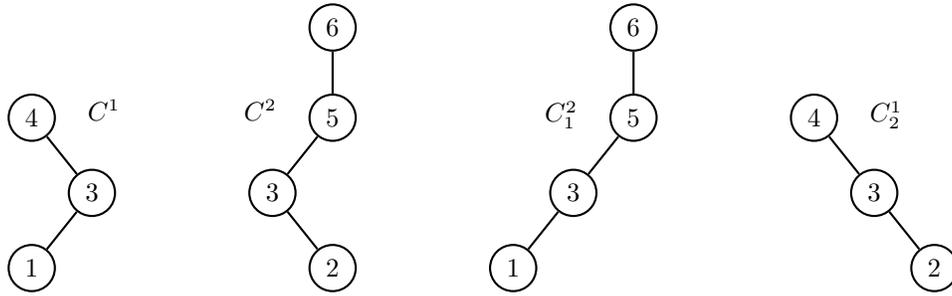


FIGURE 2. Four maximal chains of the poset shown in Figure 1.

We now present our main result regarding the feasibility of (\mathcal{D}) , under conditions (2) and (3):

THEOREM 1. *The problem (\mathcal{D}) is feasible for any finite nonempty poset (X, \preceq) , with parameters $\rho = (\rho_x) \in [0, 1]^{|X|}$ and $\pi = (\pi_C) \in]-\infty, 1]^{|C|}$ that satisfy (2) and (3).*

This result plays a crucial role in solving a generic formulation of network security game, which we study in Section 4. The game involves two players: a “router” who sends a flow of goods to maximize her value of flow crossing the network while facing transportation costs; and an “interdictor” who inspects one or more network edges to maximize the value of interdicted flow while facing interdiction costs. Our analysis in Section 4 shows that if a randomized network interdiction strategy interdicts each edge x with a probability ρ_x , and interdicts each path C with a probability at least π_C , then it is an interdiction strategy in a Nash equilibrium. Essentially, for this game, (ρ_x) and (π_C) are governed by network properties, such as edge transportation and interdiction costs, and naturally satisfy (2) and (3). In fact, when the network is a directed acyclic graph, a partial order can be defined on the set of edges, such that the set of maximal chains is exactly the set of source-destination paths of the network. Thus, showing the existence of interdiction strategies satisfying the above-mentioned requirements is an instantiation of the problem (\mathcal{D}) . Theorem 1 can then be used to derive several useful insights on the equilibrium strategies of this game.

Importantly, note that (\mathcal{D}) may not be feasible if P is not a poset. Let us consider the following example: $X = \{1, 2, 3\}$, $\mathcal{C} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, $\rho_x = 0.5$, $\forall x \in X$, and $\pi_C = 0.5$, $\forall C \in \mathcal{C}$. There is no poset that has \mathcal{C} as its set of maximal chains. If $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ satisfies (1a) and (1b), then necessarily, $\sigma_{\{x\}} = 0.5$, $\forall x \in X$. However, this implies that $\sum_{S \in \mathcal{P}} \sigma_S \geq 1.5 > 1$, which renders (\mathcal{D}) infeasible for this example.

Thus, in proving Theorem 1, we consider that the problem (\mathcal{D}) is defined for a poset. Next, we show that (\mathcal{D}) is feasible if and only if the optimal value of a linear program is no more than 1.

2.3. Equivalent optimization problem. Consider the problem (\mathcal{D}) for a given poset $P = (X, \preceq)$, and vectors $\rho \in [0, 1]^{|X|}$ and $\pi \in]-\infty, 1]^{|C|}$ satisfying (2) and (3). We can observe that when $\sum_{x \in X} \rho_x \leq 1$, a trivial solution for (\mathcal{D}) is given by: $\tilde{\sigma}_{\{x\}} = \rho_x$, $\forall x \in X$, and $\tilde{\sigma}_\emptyset = 1 - \sum_{x \in X} \rho_x$. The vector $\tilde{\sigma}$ so constructed indeed represents a probability distribution over \mathcal{P} , and satisfies constraints (1a). Furthermore, for each maximal chain $C \in \mathcal{C}$, $\sum_{\{S \in \mathcal{P} \mid S \cap C \neq \emptyset\}} \tilde{\sigma}_S = \sum_{x \in C} \rho_x \stackrel{(2)}{\geq} \pi_C$. Therefore, $\tilde{\sigma}$ is a feasible solution of (\mathcal{D}) . However, in general, $\sum_{x \in X} \rho_x$ may be larger than 1, which prevents the aforementioned construction of $\tilde{\sigma}$ from being a probability distribution. Thus, to construct a feasible solution of (\mathcal{D}) , we need to assign some probability to subsets of elements of size larger than 1. This is governed by the following quantity:

$$\forall C \in \mathcal{C}, \delta_C = \sum_{x \in C} \rho_x - \pi_C. \quad (4)$$

To highlight the role of $\delta = (\delta_C)_{C \in \mathcal{C}}$ when assigning probabilities to subsets of elements, we consider the following optimization problem:

$$\begin{aligned} (\mathcal{Q}): \quad & \text{minimize} && \sum_{S \in \mathcal{P}} \sigma_S \\ & \text{subject to} && \sum_{\{S \in \mathcal{P} \mid x \in S\}} \sigma_S = \rho_x, && \forall x \in X \end{aligned} \quad (5)$$

$$\begin{aligned} & && \sum_{\{S \in \mathcal{P} \mid |S \cap C| \geq 2\}} \sigma_S (|S \cap C| - 1) \leq \delta_C, && \forall C \in \mathcal{C} \\ & && \sigma_S \geq 0, && \forall S \in \mathcal{P}. \end{aligned} \quad (6)$$

Problems (\mathcal{Q}) and (\mathcal{D}) are related in that the set of constraints (1a)-(1b) is equivalent to the set of constraints (5)-(6); see the proof of Proposition 1 below. Furthermore, the objective function in (\mathcal{Q}) is analogous to the constraint (1c) in (\mathcal{D}) . The feasibility of (\mathcal{Q}) is straightforward (for example, $\tilde{\sigma}$ constructed above is a feasible solution); however, a feasible solution of (\mathcal{Q}) may not be a probability distribution.

Note that given a maximal chain $C \in \mathcal{C}$, constraint (6) bounds the total amount of probability that can be assigned to subsets that contain more than one element in C . One can see that for a

subset $S \in \mathcal{P}$ such that $|S \cap C| \leq 1$, the probability σ_S assigned to S does not influence constraint (6). However, the more elements from C a subset S contains, the smaller the probability that can be assigned to S , due to scaling by the factor $(|S \cap C| - 1)$. Thus, δ determines the amount of probability that can be assigned to larger subsets.

Let $z_{(\mathcal{Q})}^*$ denote the optimal value of (\mathcal{Q}) . We show the following equivalence between (\mathcal{D}) and (\mathcal{Q}) :

PROPOSITION 1. (\mathcal{D}) is feasible if and only if $z_{(\mathcal{Q})}^* \leq 1$.

Proof of Proposition 1. First, let us show that the set of constraints (1a)-(1b) is equivalent to the set of constraints (5)-(6). Let $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ that satisfies $\sum_{\{S \in \mathcal{P} | x \in S\}} \sigma_S = \rho_x, \forall x \in X$. For every maximal chain $C \in \mathcal{C}$, we have the following equality:

$$\sum_{x \in C} \rho_x = \sum_{x \in C} \sum_{\{S \in \mathcal{P} | x \in S\}} \sigma_S = \sum_{S \in \mathcal{P}} \sigma_S \sum_{x \in C} \mathbb{1}_{\{x \in S\}} = \sum_{\{S \in \mathcal{P} | S \cap C \neq \emptyset\}} \sigma_S |S \cap C|. \quad (7)$$

Therefore, for every maximal chain $C \in \mathcal{C}$, we obtain:

$$\sum_{\{S \in \mathcal{P} | S \cap C \neq \emptyset\}} \sigma_S \geq \pi_C \stackrel{(4),(7)}{\iff} \delta_C \geq \sum_{\{S \in \mathcal{P} | S \cap C \neq \emptyset\}} \sigma_S (|S \cap C| - 1) = \sum_{\{S \in \mathcal{P} | |S \cap C| \geq 2\}} \sigma_S (|S \cap C| - 1). \quad (8)$$

Now, let us show that (\mathcal{D}) is feasible if and only if the optimal value of (\mathcal{Q}) satisfies $z_{(\mathcal{Q})}^* \leq 1$.

– If $\exists \sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ that satisfies (1a)-(1c), then we showed that σ also satisfies (5)-(6). Therefore, σ is a feasible solution of (\mathcal{Q}) . Furthermore, the objective value of σ is equal to 1, which implies that $z_{(\mathcal{Q})}^* \leq 1$.

– If $z_{(\mathcal{Q})}^* \leq 1$, let σ^* be an optimal solution of (\mathcal{Q}) . Necessarily, $\sigma_\emptyset^* = 0$ and we can define a vector $\sigma \in \mathbb{R}^{|\mathcal{P}|}$ as follows: $\sigma_S = \sigma_S^*, \forall S \in \mathcal{P} \setminus \emptyset$, and $\sigma_\emptyset = 1 - \sum_{S \in \mathcal{P} \setminus \emptyset} \sigma_S^* = 1 - z_{(\mathcal{Q})}^* \geq 0$. Therefore, $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ and satisfies (5)-(6), which we showed is equivalent to satisfying (1a)-(1b). Finally, σ satisfies (1c) by construction. Therefore, σ is feasible for (\mathcal{D}) . \square

Therefore, proving Theorem 1 is equivalent to showing that $z_{(\mathcal{Q})}^* \leq 1$. In fact, we show a stronger result, which will be useful for our equilibrium analysis in Section 4:

THEOREM 2. $z_{(\mathcal{Q})}^* = \max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$.

It is easy to see that $z_{(\mathcal{Q})}^* \geq \max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. Indeed, any feasible solution $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ of (\mathcal{Q}) satisfies $\sum_{S \in \mathcal{P}} \sigma_S \geq \sum_{\{S \in \mathcal{P} | x \in S\}} \sigma_S = \rho_x, \forall x \in X$, and $\sum_{S \in \mathcal{P}} \sigma_S \geq \sum_{\{S \in \mathcal{P} | S \cap C \neq \emptyset\}} \sigma_S \stackrel{(8)}{\geq} \pi_C, \forall C \in \mathcal{C}$. To show the reversed inequality, we need to prove that there exists a feasible solution of (\mathcal{Q}) with objective value equal to $\max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. This is the focus of the next section.

3. Constructive proof of Theorem 2. We design a combinatorial algorithm to compute a feasible solution of (\mathcal{Q}) with objective value exactly equal to $\max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. Recall from Section 2.3 that such a feasible solution is optimal for (\mathcal{Q}) , and can be used to construct a feasible solution of (\mathcal{D}) ; see the proof of Proposition 1.

Before formally introducing our algorithm, we discuss the main ideas behind its design. In each iteration, the algorithm selects a subset of elements, and assigns a positive weight to it. Let us discuss the execution of the first iteration of the algorithm.

Firstly, we need to determine the collection of subsets that can be assigned a positive weight without violating any of the constraints in the problem (\mathcal{Q}) . Essentially, this is dictated by the maximal chains $C \in \mathcal{C}$ for which $\delta_C = 0$. Indeed, for any $C \in \mathcal{C}$ with $\delta_C = 0$, we have the following equivalence: $\sum_{\{S \in \mathcal{P} \mid |S \cap C| \geq 2\}} \underbrace{\sigma_S}_{\geq 0} \underbrace{(|S \cap C| - 1)}_{> 0} \leq 0 \iff \sigma_S = 0, \forall S \in \mathcal{P} \text{ such that } |S \cap C| \geq 2$. In other words, if a maximal chain $C \in \mathcal{C}$ is such that $\delta_C = 0$ (i.e., $\sum_{x \in C} \rho_x = \pi_C$), then a vector $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ is feasible for (\mathcal{Q}) only if its support does *not* contain any set $S \in \mathcal{P}$ that intersects C in more than one element. Therefore, our algorithm must select a subset of elements $S \in \mathcal{P}$ that satisfies $|S \cap C| \leq 1$, for all $C \in \mathcal{C}$ such that $\delta_C = 0$.

To precisely characterize this collection of subsets, we consider the notion of subposet generated by a subset of maximal chains, introduced in Section 2.1. In particular, by considering \mathcal{C}' the set of maximal chains $C \in \mathcal{C}$ such that $\delta_C = 0$, and X' the subset of elements $x \in X$ such that $\rho_x > 0$, we can show (in Proposition 2 below) that the condition stated in Lemma 2 is satisfied, and $P' = (X', \preceq_{\mathcal{C}'})$ is a poset. Interestingly, we can then deduce that the subsets of elements that we can select from at that iteration are the antichains of P' . In any poset, a chain and an antichain intersect in at most one element. By definition of $\preceq_{\mathcal{C}'}$, this implies that $|S \cap C| \leq 1$ for every antichain $S \subseteq X'$ of P' and every maximal chain $C \in \mathcal{C}$ of P such that $\delta_C = 0$.

Now, we need to determine which antichain of P' to select. Let $S' \subseteq X'$ denote the subset of elements selected by the algorithm in the first iteration. Recall that an optimal solution of (\mathcal{Q}) satisfies constraints (1a)-(1b) with the least total amount of weight assigned to subsets of elements of X . Thus, it is desirable that the weight assigned to S' in this iteration contribute towards satisfying all constraints (1b). To capture this requirement, our algorithm selects S' as the set of minimal elements of P' . The selected S' is an antichain of P' , intersects with every maximal chain of P , and provides further properties that enable us proving the optimality of the algorithm.

Secondly, we discuss how to determine the maximum amount of weight w' that can be assigned to S' in the first iteration, without violating any of the constraints (5) and (6). This is governed by the remaining chains $C \in \mathcal{C}$ for which $\delta_C > 0$ and the elements constituting S' . If w' is larger than

$\frac{\delta_C}{|S' \cap C| - 1}$ for $C \in \mathcal{C}$ such that $|S' \cap C| \geq 2$, then the corresponding constraint (6) will be violated. Similarly, w' cannot be larger than $\rho_x, \forall x \in S'$. Thus, the weight that we must assign to S' is:

$$w' = \min \left\{ \min \{ \rho_x, x \in S' \}, \min \left\{ \frac{\delta_C}{|S' \cap C| - 1}, C \in \mathcal{C} \mid \delta_C > 0 \text{ and } |S' \cap C| \geq 2 \right\} \right\}.$$

At the end of the iteration, we update the vectors ρ and δ , as well as the sets of elements X' and maximal chains \mathcal{C}' to consider in subsequent iterations. In particular, we will show that some maximal chains need to be removed in order to preserve the conservation law at each iteration. The algorithm terminates when there are no more elements $x \in X$ with positive ρ_x . This completes the discussion of the main points that we need to account for in designing the algorithm. We are now in the position to formally present Algorithm 1.

Algorithm 1 : Optimal solution of (Q)

Input: Finite nonempty poset $P = (X, \preceq)$, and vectors $\rho \in \mathbb{R}_+^{|X|}, \delta \in \mathbb{R}_+^{|\mathcal{C}|}$.

Output: Vector $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$.

- A1: $\mathcal{C}^1 \leftarrow \mathcal{C}, \quad \rho_x^1 \leftarrow \rho_x, \forall x \in X, \quad \delta_C^1 \leftarrow \delta_C, \forall C \in \mathcal{C}^1$
A2: $X^1 \leftarrow \{x \in X \mid \rho_x^1 > 0\}, \quad \bar{\mathcal{C}}^1 \leftarrow \{C \in \mathcal{C}^1 \mid \delta_C^1 = 0\}, \quad \hat{\mathcal{C}}^1 \leftarrow \{C \in \mathcal{C}^1 \mid \delta_C^1 > 0\}$
A3: $k \leftarrow 1$
A4: **while** $X^k \neq \emptyset$ **do**
A5: Construct the poset $P^k = (X^k, \preceq_{\bar{\mathcal{C}}^k})$
A6: Choose S^k the set of minimal elements of P^k
A7: $w^k = \min \{ \min \{ \rho_x^k, x \in S^k \}, \min \{ \frac{\delta_C^k}{|S^k \cap C| - 1}, C \in \hat{\mathcal{C}}^k \mid |S^k \cap C| \geq 2 \} \}$, and $\sigma_{S^k} \leftarrow w^k$
A8: $\rho_x^{k+1} \leftarrow \rho_x^k - w^k \mathbf{1}_{\{x \in S^k\}}, \forall x \in X$, and $\delta_C^{k+1} \leftarrow \delta_C^k - w^k (|S^k \cap C| - 1) \mathbf{1}_{\{|S^k \cap C| \geq 2\}}, \forall C \in \mathcal{C}$
A9: $\mathcal{C}^{k+1} \leftarrow \{C \in \mathcal{C}^k \mid \text{the minimal element of } C \cap X^k \text{ in } P \text{ is in } S^k\}$
A10: $X^{k+1} \leftarrow \{x \in X^k \mid \rho_x^{k+1} > 0\}, \bar{\mathcal{C}}^{k+1} \leftarrow \{C \in \mathcal{C}^{k+1} \mid \delta_C^{k+1} = 0\}, \hat{\mathcal{C}}^{k+1} \leftarrow \{C \in \mathcal{C}^{k+1} \mid \delta_C^{k+1} > 0\}$
A11: $k \leftarrow k + 1$
A12: **end while**
-

We illustrate Algorithm 1 with an example in Appendix B.

Let n^* denote the number of iterations of Algorithm 1. Since we have not yet shown that it terminates, we suppose that $n^* \in \mathbb{N} \cup \{+\infty\}$. For every maximal chain $C \in \mathcal{C}$, let us define the sequence $(\pi_C^k)_{k \in \llbracket 1, n^* + 1 \rrbracket}$ induced by Algorithm 1 as follows:

$$\pi_C^1 = \pi_C, \text{ and for every } k \in \llbracket 1, n^* \rrbracket, \pi_C^{k+1} = \pi_C^k - w^k \mathbf{1}_{\{S^k \cap C \neq \emptyset\}}. \quad (9)$$

Given $k \in \llbracket 1, n^* + 1 \rrbracket$, π_C^k (resp. ρ_x^k) represents the remaining value associated with the maximal chain $C \in \mathcal{C}$ (resp. the element $x \in X$) after the first $k - 1$ iterations of the algorithm. For convenience, we let $X^0 \leftarrow X$.

We now proceed with proving Theorem 2. Our proof consists of three main parts:

Part 1: Algorithm 1 is well-defined (Proposition 2);

Part 2: it terminates and outputs a feasible solution of (Q) (Proposition 3); and

Part 3: it assigns a total weight $\sum_{k=1}^{n^*} w^k$ equal to $\max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$ at termination (Proposition 4).

Part 1: Well-definedness of Algorithm 1. To show that Algorithm 1 is well-defined, we need to ensure that at each iteration $k \in \llbracket 1, n^* \rrbracket$ of the algorithm, P^k is a poset. Lemma 2 can be applied to show this, provided that we are able to prove that $\overline{\mathcal{C}}^k$ preserves the decomposition of maximal chains intersecting in X^k . This property, and some associated results, are stated below:

PROPOSITION 2. *Each iteration of Algorithm 1 is well-defined. In particular, for every $k \in \llbracket 1, n^* + 1 \rrbracket$, the following hold:*

(i) *For every maximal chain $C \in \mathcal{C}$, δ_C^k determines the remaining weight that can be assigned to subsets that intersect C at more than one element:*

$$\forall C \in \mathcal{C}, \quad \delta_C^k = \sum_{x \in C} \rho_x^k - \pi_C^k, \quad (10)$$

$$\forall C \in \mathcal{C}^k, \quad \delta_C^k \geq 0. \quad (11)$$

(ii) *\mathcal{C}^k preserves the decomposition of maximal chains intersecting in X^{k-1} :*

$$\forall (C^1, C^2) \in \mathcal{C}^2 \mid C^1 \cap C^2 \cap X^{k-1} \neq \emptyset, (C^1, C^2) \in (\mathcal{C}^k)^2 \implies (C_1^2, C_2^2) \in (\mathcal{C}^k)^2.$$

(iii) *π^k satisfies the conservation law on the maximal chains of \mathcal{C}^k that intersect in X^{k-1} :*

$$\forall (C^1, C^2) \in (\mathcal{C}^k)^2 \mid C^1 \cap C^2 \cap X^{k-1} \neq \emptyset, \quad \pi_{C^1}^k + \pi_{C^2}^k = \pi_{C_1^2}^k + \pi_{C_2^2}^k. \quad (12)$$

(iv) *$P^k = (X^k, \preceq_{\overline{\mathcal{C}}^k})$ is a poset.*

Proof of Proposition 2. We show (i) – (iv) by induction.

First, consider $k = 1$. Since $\mathcal{C}^1 = \mathcal{C}$, $\rho^1 = \rho$, $\pi^1 = \pi$, and $\delta^1 = \delta$, then (i) follows from (2) and (4). Since $X^0 = X$, and $\mathcal{C}^1 = \mathcal{C}$ contains all maximal chains, then (ii) is automatically satisfied. (iii) is a direct consequence of (3).

Now we apply Lemma 2 to show (iv), i.e., $P^1 = (X^1, \preceq_{\overline{\mathcal{C}}^1})$ is a poset. Specifically, we show that $\overline{\mathcal{C}}^1$ preserves the decomposition of maximal chains intersecting in X^1 . Consider $C^1, C^2 \in \overline{\mathcal{C}}^1$ such that $C^1 \cap C^2 \cap X^1 \neq \emptyset$, and let us consider the other two maximal chains C_1^2 and C_2^2 , which we know from (ii) are in \mathcal{C}^1 , since $X^1 \subseteq X^0$. We need to show that they are also in $\overline{\mathcal{C}}^1$. Let $x^* \in C^1 \cap C^2 \cap X^1$, and let us rewrite $C^1 = \{x_{-k}, \dots, x_{-1}, x_0 = x^*, x_1, \dots, x_n\}$ and $C^2 = \{y_{-l}, \dots, y_{-1}, y_0 = x^*, y_1, \dots, y_m\}$. Then, $C_1^2 = \{x_{-k}, \dots, x_{-1}, x^*, y_1, \dots, y_m\}$ and $C_2^2 = \{y_{-l}, \dots, y_{-1}, x^*, x_1, \dots, x_n\}$. We now use (i) – (iii):

Since $C^1, C^2 \in \bar{\mathcal{C}}^1$; the conservation law is satisfied by π^1 on the maximal chains in \mathcal{C}^1 intersecting in X^0 ; $C_1^2, C_2^1 \in \mathcal{C}^1$; and since $\delta^1 \geq 0$ on \mathcal{C}^1 , we have:

$$\sum_{i=-k}^n \rho_{x_i}^1 + \sum_{j=-l}^m \rho_{y_j}^1 = \pi_{C^1}^1 + \pi_{C^2}^1 = \pi_{C_1^2}^1 + \pi_{C_2^1}^1 = \sum_{x \in C_1^2} \rho_x^1 + \sum_{x \in C_2^1} \rho_x^1 - \delta_{C_1^2}^1 - \delta_{C_2^1}^1 \leq \sum_{i=-k}^n \rho_{x_i}^1 + \sum_{j=-l}^m \rho_{y_j}^1.$$

Therefore, $\delta_{C_1^2}^1 = \delta_{C_2^1}^1 = 0$, and C_1^2 and C_2^1 are in $\bar{\mathcal{C}}^1$. From Lemma 2, we conclude that $P^1 = (X^1, \preceq_{\bar{\mathcal{C}}^1})$ is a poset.

We now assume that (i) – (iv) hold for $k \in \llbracket 1, n^* \rrbracket$, and show that they also hold for $k+1$:

(i) Since P^k is a poset, the k -th iteration of the algorithm is well-defined, and we can consider the set S^k and the weight w^k at that iteration. Then, for every $C \in \mathcal{C}$, (A8) and (9) give us:

$$\sum_{x \in C} \rho_x^{k+1} - \pi_C^{k+1} = \sum_{x \in C} \rho_x^k - \pi_C^k - w^k |C \cap S^k| + w^k \mathbf{1}_{\{S^k \cap C \neq \emptyset\}} = \delta_C^k - w^k (|C \cap S^k| - 1) \mathbf{1}_{\{S^k \cap C \neq \emptyset\}} = \delta_C^{k+1}.$$

Now, consider a maximal chain $C \in \mathcal{C}^k$. Since $\delta^k \geq 0$ on \mathcal{C}^k , then $C^k = \bar{\mathcal{C}}^k \cup \hat{\mathcal{C}}^k$ (from (A10)).

(a) If $C \in \bar{\mathcal{C}}^k$, then by definition of $\preceq_{\bar{\mathcal{C}}^k}$, $C \cap X^k$ is a chain in P^k . From Lemma 1, we know that S^k is an antichain of P^k . Therefore, $|S^k \cap (C \cap X^k)| \leq 1$. Since $S^k \subseteq X^k$, we obtain that $|S^k \cap C| = |(S^k \cap X^k) \cap C| = |S^k \cap (C \cap X^k)| \leq 1$. Thus, $\delta_C^{k+1} \stackrel{(A8)}{=} \delta_C^k - w^k (|C \cap S^k| - 1) \mathbf{1}_{\{|S^k \cap C| \geq 2\}} = \delta_C^k = 0$.

(b) If $C \in \hat{\mathcal{C}}^k$, then by definition of w^k , we have $\delta_C^{k+1} \stackrel{(A8)}{=} \delta_C^k - w^k (|S^k \cap C| - 1) \mathbf{1}_{\{|S^k \cap C| \geq 2\}} \stackrel{(A7)}{\geq} 0$.

In summary, for all $C \in \mathcal{C}^k$, $\delta_C^{k+1} \geq 0$. Since $\mathcal{C}^{k+1} \stackrel{(A9)}{\subseteq} \mathcal{C}^k$, then for all $C \in \mathcal{C}^{k+1}$, $\delta_C^{k+1} \geq 0$.

(ii) Consider $C^1, C^2 \in \mathcal{C}^{k+1} \subseteq \mathcal{C}^k$ such that $C^1 \cap C^2 \cap X^k \neq \emptyset$, and let C_1^2 and C_2^1 be the other two maximal chains such that $C_1^2 \cup C_2^1 = C^1 \cup C^2$. Since $X^k \stackrel{(A10)}{\subseteq} X^{k-1}$, then $C^1 \cap C^2 \cap X^{k-1} \neq \emptyset$. Therefore, by inductive hypothesis, $C_1^2, C_2^1 \in \mathcal{C}^k$ as well. Let x_1 (resp. y_1) denote the minimal element of the chain $C^1 \cap X^k$ (resp. $C^2 \cap X^k$) in P . Since $C^1, C^2 \in \mathcal{C}^{k+1}$, then $(x_1, y_1) \stackrel{(A9)}{\in} (S^k)^2$. Let $x^* \in X^k$ denote an intersecting point of C^1 and C^2 . Since $C^1 \cap X^k$ is a chain in P , contains x^* , and whose minimal element is x_1 , then necessarily, $x_1 \preceq x^*$. Similarly, we obtain that $y_1 \preceq x^*$. Therefore, the minimal element of $C_1^2 \cap X^k$ (resp. $C_2^1 \cap X^k$) is x_1 (resp. y_1), which is in S^k . Thus, $C_1^2, C_2^1 \in \mathcal{C}^{k+1}$, and \mathcal{C}^{k+1} preserves the decomposition of maximal chains of P intersecting in X^k .

(iii) Now, given C^1, C^2 in \mathcal{C}^{k+1} that intersect in X^k , we just proved that C_1^2 and C_2^1 are in \mathcal{C}^{k+1} as well. Therefore, $\forall C \in \{C^1, C^2, C_1^2, C_2^1\}$, we have $\pi_C^{k+1} \stackrel{(9)}{=} \pi_C^k - w^k$ (since $S^k \cap C \neq \emptyset$). By inductive hypothesis, since $\mathcal{C}^{k+1} \subseteq \mathcal{C}^k$ and $X^{k+1} \subseteq X^k$, π^k satisfies the conservation law between C^1, C^2, C_1^2 , and C_2^1 . Thus, we can conclude that $\pi_{C^1}^{k+1} + \pi_{C^2}^{k+1} = \pi_{C^1}^k + \pi_{C^2}^k - 2w^k = \pi_{C_1^2}^k + \pi_{C_2^1}^k - 2w^k = \pi_{C_1^2}^{k+1} + \pi_{C_2^1}^{k+1}$.

(iv) This is a consequence of (i) – (iii); the proof is analogous to the one derived for the first step of the induction.

Therefore, we conclude by induction that (i) – (iv) hold for every $k \in \llbracket 1, n^* + 1 \rrbracket$. \square

The proof of Proposition 2 highlights the importance of our construction of \mathcal{C}^{k+1} for $k \in \llbracket 1, n^* \rrbracket$ as given in (A9). This step of the algorithm ensures that \mathcal{C}^{k+1} preserves the decomposition of maximal chains intersecting in X^k . It also ensures that each maximal chain in \mathcal{C}^{k+1} intersects S^k . A direct consequence is that π^{k+1} satisfies the conservation law on the maximal chains of \mathcal{C}^{k+1} that intersect in X^k . We then deduce that $\overline{\mathcal{C}}^{k+1}$ preserves the decomposition of maximal chains intersecting in X^{k+1} , which implies that P^{k+1} is a poset (Lemma 2). The issue however is that some maximal chains in \mathcal{C}^k may be removed when constructing \mathcal{C}^{k+1} , and we must ensure that the corresponding constraints (6) will still be satisfied by the output of the algorithm. This is the focus of the next part.

Part 2: Feasibility of Algorithm 1's output. Now that we have shown the algorithm to be well-defined, the second main part of the proof of Theorem 2 is to show that the algorithm terminates, and outputs a feasible solution of (Q). Showing that the algorithm terminates is based on the fact that there are finite numbers of elements and maximal chains. To show the feasibility of the solution generated by the algorithm, we need to verify that constraints (5) and (6) are satisfied. From (A10), we deduce that constraints (5) are automatically satisfied at termination, since an element $x \in X$ is removed whenever the remaining value ρ_x^k is 0. Similarly, from Proposition 2, we obtain that constraints (6) are satisfied for all maximal chains in \mathcal{C}^{n^*+1} , i.e., the maximal chains that are not removed by the algorithm. As mentioned before, the main issue in showing the feasibility of Algorithm 1's output is with regards to the constraints (6) corresponding to the maximal chains that have been removed at some iteration of the algorithm. For such maximal chains $C \in \mathcal{C} \setminus \mathcal{C}^{n^*+1}$, we create a finite sequence of “dominating” maximal chains, and show that constraint (6) being satisfied for the last maximal chain of the sequence implies that it is also satisfied for the initial maximal chain C . To carry out this argument, we essentially need the following lemma:

LEMMA 3. *Consider $C^{(1)} \in \mathcal{C}$, and suppose that $\exists k_1 \in \llbracket 1, n^* \rrbracket$ such that $C^{(1)} \in \mathcal{C}^{k_1} \setminus \mathcal{C}^{k_1+1}$ and $C^{(1)} \cap X^{k_1} \neq \emptyset$. Then, $\exists C^{(2)} \in \mathcal{C}^{k_1+1}$ such that $\delta_{C^{(1)}}^{k_1} \geq \delta_{C^{(2)}}^{k_1}$ and $C^{(2)} \cap X^{k_1} \supseteq C^{(1)} \cap X^{k_1}$.*

Proof of Lemma 3. Consider $C^{(1)} \in \mathcal{C}$, and suppose that $\exists k_1 \in \llbracket 1, n^* \rrbracket$ such that $C^{(1)} \in \mathcal{C}^{k_1}$, $C^{(1)} \cap X^{k_1} \neq \emptyset$, but $C^{(1)} \notin \mathcal{C}^{k_1+1}$. This case arises when the minimal element of $C^{(1)} \cap X^{k_1}$ in P is not a minimal element of P^{k_1} . Then, we can find a chain in P^{k_1} whose maximal element is the minimal element of $C^{(1)} \cap X^{k_1}$ in P , and whose minimal element is a minimal element of P^{k_1} . From the definition of P^{k_1} and Lemma 2, this chain is contained in a maximal chain in $\overline{\mathcal{C}}^{k_1}$. We can then exploit (i) – (iii) in Proposition 2 to show that there exists a maximal chain in \mathcal{C}^{k_1+1} that satisfies the desired properties.

Formally, let x^* denote the minimal element of $C^{(1)} \cap X^{k_1}$ in P . Since $C^{(1)} \notin \mathcal{C}^{k_1+1}$, then $x^* \notin S^{k_1}$, i.e., x^* is not a minimal element of P^{k_1} . Let $C' \subseteq X^{k_1}$ denote a maximal chain of P^{k_1} that contains

x^* . From Lemma 1, we know that the minimal element of C' in P^{k_1} , which we denote y_1 , is a minimal element of P^{k_1} . Therefore $y_1 \in S^{k_1}$ and $y_1 \neq x^*$. Thus, C' is of size at least two, and there exists a maximal chain $C^2 \in \overline{\mathcal{C}}^{k_1}$ such that $C' = C^2 \cap X^{k_1}$ (Lemma 2). Since $C^{(1)} \cap C^2 \cap X^{k_1-1} \supseteq \{x^*\} \neq \emptyset$, let us consider the other two maximal chains $C_1^2, C_2^1 \in \mathcal{C}$ such that $C_1^2 \cup C_2^1 = C^{(1)} \cup C^2$. Since $C^{(1)}$ and C^2 are in \mathcal{C}^{k_1} , then from Proposition 2, C_1^2 and C_2^1 are in \mathcal{C}^{k_1} as well. Let us rewrite $C^{(1)} = \{x_{-m}, \dots, x_0 = x^*, \dots, x_n\}$, $C^2 = \{y_{-q}, \dots, y_0, y_1, \dots, y_p = x^*, \dots, y_{p+r}\}$, $C_1^2 = \{x_{-m}, \dots, x_{-1}, y_p, \dots, y_{p+r}\}$, and $C_2^1 = \{y_{-q}, \dots, y_p, x_1, \dots, x_n\}$; they are illustrated in Figure 3.

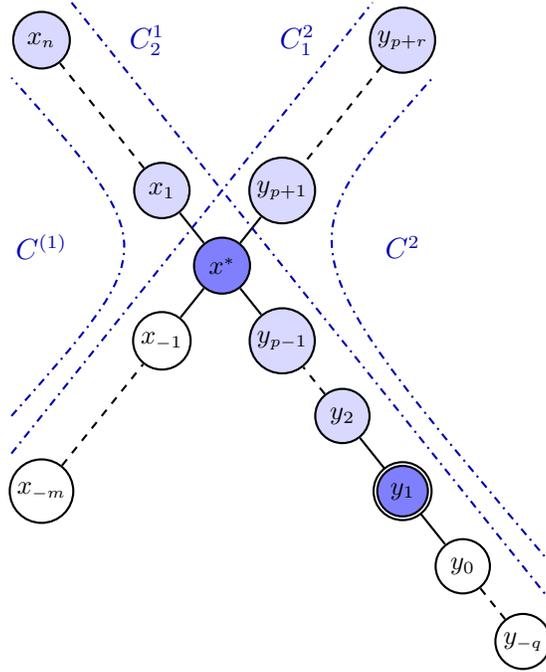


FIGURE 3. Illustration of $C^{(1)}$, C^2 , C_1^2 , and C_2^1 . In dark blue are the elements in X^{k_1} , in light blue are the elements that may or may not be in X^{k_1} , and in white are the elements that are not in X^{k_1} . The “double” node y_1 is in S^{k_1} .

Since x^* is the minimal element of $C^{(1)} \cap X^{k_1}$ in P , then $\forall i \in \llbracket -m, -1 \rrbracket$, $x_i \notin X^{k_1}$ and $\rho_{x_i}^{k_1} = 0$. Since $C^2 \in \overline{\mathcal{C}}^{k_1}$ and $C_1^2 \in \mathcal{C}^{k_1}$, and from the conservation law between $C^{(1)}$, C^2 , C_1^2 and C_2^1 , we obtain:

$$\pi_{C_2^1}^{k_1} - \pi_{C^{(1)}}^{k_1} \stackrel{(12)}{=} \pi_{C^2}^{k_1} - \pi_{C_1^2}^{k_1} \stackrel{(10)}{=} \sum_{j=-q}^{p+r} \rho_{y_j}^{k_1} - \underbrace{\delta_{C^2}^{k_1}}_{=0} - \sum_{i=-m}^{-1} \underbrace{\rho_{x_i}^{k_1}}_{=0} - \sum_{j=p}^{p+r} \rho_{y_j}^{k_1} + \underbrace{\delta_{C_1^2}^{k_1}}_{\geq 0} \stackrel{(11)}{\geq} \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1}. \quad (13)$$

This implies that:

$$\delta_{C^{(1)}}^{k_1} \stackrel{(10)}{=} \sum_{i=0}^n \rho_{x_i}^{k_1} - \pi_{C^{(1)}}^{k_1} + \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1} - \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1} \stackrel{(10)}{=} \delta_{C_2^1}^{k_1} + \pi_{C_2^1}^{k_1} - \pi_{C^{(1)}}^{k_1} - \sum_{j=-q}^{p-1} \rho_{y_j}^{k_1} \stackrel{(13)}{\geq} \delta_{C_2^1}^{k_1}.$$

Furthermore, since y_1 is the minimal element of $C^2 \cap X^{k_1}$ in P^{k_1} , it is also the minimal element of $C^2 \cap X^{k_1}$ in P . This implies that y_1 is the minimal element of $C_2^1 \cap X^{k_1}$ in P . Since y_1 belongs to S^{k_1} , we deduce that $C_2^1 \in \mathcal{C}^{k_1+1}$.

Finally, since $\forall i \in \llbracket -m, -1 \rrbracket$, $x_i \notin X^{k_1}$, then $C_2^1 \cap X^{k_1} \supseteq \{x^*, x_1, \dots, x_n\} \cap X^{k_1} = C^{(1)} \cap X^{k_1}$, as illustrated in Figure 3. In conclusion, given $C^{(1)} \in \mathcal{C}^{k_1} \setminus \mathcal{C}^{k_1+1}$ such that $C^{(1)} \cap X^{k_1} \neq \emptyset$, $\exists C^{(2)} := C_2^1 \in \mathcal{C}^{k_1+1}$ such that $\delta_{C^{(1)}}^{k_1} \geq \delta_{C^{(2)}}^{k_1}$ and $C^{(2)} \cap X^{k_1} \supseteq C^{(1)} \cap X^{k_1}$. \square

As shown in the next proposition, one of the implications of Lemma 3 is that if a maximal chain $C^{(1)}$ is removed after the k_1 -th iteration of the algorithm, then there exists another maximal chain $C^{(2)}$, which dominates $C^{(1)}$ in the sense that if the output of the algorithm satisfies constraint (6) for $C^{(2)}$, then it also satisfies that constraint for $C^{(1)}$. Additionally, it is guaranteed that $C^{(2)}$ is not removed before the $k_1 + 1$ -th iteration of the algorithm. We can now show the second main part of the proof of Theorem 2:

PROPOSITION 3. *Algorithm 1 terminates, and outputs a feasible solution of (Q).*

Proof of Proposition 3. We recall that the algorithm terminates after iteration n^* if $X^{n^*+1} = \emptyset$. First, we note that $X^1 \subseteq X$ and $\forall k \in \llbracket 1, n^* \rrbracket$, $X^{k+1} \stackrel{(A10)}{\subseteq} X^k$. Additionally, $\widehat{\mathcal{C}}^1 \subseteq \mathcal{C}$, and from (A8), we have $\forall k \in \llbracket 1, n^* \rrbracket$, $\widehat{\mathcal{C}}^{k+1} \subseteq \widehat{\mathcal{C}}^k$. Now, consider $k \in \llbracket 1, n^* \rrbracket$, and the weight w^k chosen by the algorithm at iteration k . From (A7), $\exists x \in X^k$ such that $w^k = \rho_x^k$, or $\exists C \in \widehat{\mathcal{C}}^k$ such that $w^k = \frac{\delta_C^k}{|S^k \cap C| - 1}$. In the first case, we deduce that $x \notin X^{k+1}$, so $X^{k+1} \subsetneq X^k$. In the second case, either $C \notin \mathcal{C}^{k+1}$, or $C \in \mathcal{C}^{k+1}$ and $\delta_C^{k+1} = 0$, which both imply that $C \in \overline{\mathcal{C}}^{k+1}$. Therefore, $C \notin \widehat{\mathcal{C}}^{k+1}$ and $\widehat{\mathcal{C}}^{k+1} \subsetneq \widehat{\mathcal{C}}^k$.

Thus, $\forall k \in \llbracket 1, n^* \rrbracket$, $|X^{k+1} \times \widehat{\mathcal{C}}^{k+1}| < |X^k \times \widehat{\mathcal{C}}^k|$. Since $|X^1 \times \widehat{\mathcal{C}}^1| \in \mathbb{N}$, if n^* were equal to $+\infty$, we would obtain an infinite decreasing sequence of natural integers. Therefore, we conclude that $n^* \in \mathbb{N}$, i.e., the algorithm terminates. At termination, we have $X^{n^*+1} = \emptyset$.

Next, we show that the output $\sigma \in \mathbb{R}_+^{|\mathcal{P}|}$ of the algorithm is a feasible solution of (Q). First, the equality constraints (5) are trivially satisfied:

$$\forall x \in X, \rho_x \stackrel{(A1)}{=} \rho_x^1 \stackrel{(A8)}{=} \underbrace{\rho_x^{n^*+1}}_{=0} + \sum_{k=1}^{n^*} w^k \mathbf{1}_{\{x \in S^k\}} \stackrel{(A7)}{=} \sum_{k=1}^{n^*} \sigma_{S^k} \mathbf{1}_{\{x \in S^k\}} = \sum_{\{S \in \mathcal{P} \mid x \in S\}} \sigma_S.$$

Regarding constraints (6), we first show the following equality:

$$\forall C \in \mathcal{C}, \delta_C^{n^*+1} \stackrel{(A8)}{=} \delta_C^1 - \sum_{k=1}^{n^*} w^k (|S^k \cap C| - 1) \mathbf{1}_{\{|S^k \cap C| \geq 2\}} \stackrel{(A1), (A7)}{=} \delta_C - \sum_{\{S \in \mathcal{P} \mid |S \cap C| \geq 2\}} \sigma_S (|S \cap C| - 1).$$

Therefore, constraints (6) are satisfied if and only if $\forall C \in \mathcal{C}$, $\delta_C^{n^*+1} \geq 0$.

From Proposition 2, we know that $\forall C \in \mathcal{C}^{n^*+1}$, $\delta_C^{n^*+1} \geq 0$. Now, consider $C^{(1)} \in \mathcal{C}$, and suppose that $\exists k_1 \in \llbracket 1, n^* \rrbracket$ such that $C^{(1)} \in \mathcal{C}^{k_1} \setminus \mathcal{C}^{k_1+1}$. If $C^{(1)} \cap X^{k_1} = \emptyset$, then $\forall l \in \llbracket k_1, n^* \rrbracket$, $|S^l \cap C^{(1)}| = 0$

since $S^l \stackrel{(A6)}{\subseteq} X^l$ and $X^l \stackrel{(A10)}{\subseteq} X^{k_1}$. Therefore, since $C^{(1)} \in \mathcal{C}^{k_1}$, we have $\delta_{C^{(1)}}^{n^*+1} \stackrel{(A8)}{=} \delta_{C^{(1)}}^{k_1} - \sum_{l=k_1}^{n^*} w^l (|S^l \cap C^{(1)}| - 1) \mathbb{1}_{\{|S^l \cap C^{(1)}| \geq 2\}} = \delta_{C^{(1)}}^{k_1} \stackrel{(11)}{\geq} 0$.

If $C^{(1)} \cap X^{k_1} \neq \emptyset$, then $\exists C^{(2)} \in \mathcal{C}^{k_1+1}$ such that $\delta_{C^{(1)}}^{k_1} \geq \delta_{C^{(2)}}^{k_1}$ and $C^{(2)} \cap X^{k_1} \supseteq C^{(1)} \cap X^{k_1}$ (Lemma 3). Consider $i \in \llbracket k_1, n^* \rrbracket$. Since $S^i \stackrel{(A6),(A10)}{\subseteq} X^{k_1}$, then $S^i \cap C^{(2)} \supseteq S^i \cap C^{(1)}$, and we obtain:

$$\begin{aligned} \forall l \in \llbracket k_1, n^* + 1 \rrbracket, \delta_{C^{(1)}}^l &\stackrel{(A8)}{=} \delta_{C^{(1)}}^{k_1} - \sum_{i=k_1}^{l-1} w^i (|S^i \cap C^{(1)}| - 1) \mathbb{1}_{\{|S^i \cap C^{(1)}| \geq 2\}} \\ &\geq \delta_{C^{(2)}}^{k_1} - \sum_{i=k_1}^{l-1} w^i (|S^i \cap C^{(2)}| - 1) \mathbb{1}_{\{|S^i \cap C^{(2)}| \geq 2\}} \stackrel{(A8)}{=} \delta_{C^{(2)}}^l. \end{aligned} \quad (14)$$

In particular, $\delta_{C^{(1)}}^{n^*+1} \geq \delta_{C^{(2)}}^{n^*+1}$. We note that $C^{(2)} \in \mathcal{C}^{k_1+1}$, and two cases can arise:

1) $C^{(2)} \in \mathcal{C}^{n^*+1}$. In this case, $\delta_{C^{(2)}}^{n^*+1} \geq 0$ (Proposition 2).

2) $\exists k_2 \in \llbracket k_1 + 1, n^* \rrbracket$ such that $C^{(2)} \in \mathcal{C}^{k_2} \setminus \mathcal{C}^{k_2+1}$. Then we reiterate the same argument:

(a) If $C^{(2)} \cap X^{k_2} = \emptyset$, then $\delta_{C^{(2)}}^{n^*+1} = \delta_{C^{(2)}}^{k_2} \stackrel{(11)}{\geq} 0$.

(b) If $C^{(2)} \cap X^{k_2} \neq \emptyset$, then there exists $C^{(3)} \in \mathcal{C}^{k_2+1}$ such that $\delta_{C^{(2)}}^{k_2} \geq \delta_{C^{(3)}}^{k_2}$ and $C^{(3)} \cap X^{k_2} \supseteq C^{(2)} \cap X^{k_2}$ (Lemma 3). Analogous calculations to (14) show that $\delta_{C^{(2)}}^{n^*+1} \geq \delta_{C^{(3)}}^{n^*+1}$.

By induction, we construct a sequence of maximal chains $(C^{(s)})$, a sequence of increasing integers (k_s) , and a termination point $s^* \in \mathbb{N}^*$, such that $\forall s \in \llbracket 1, s^* - 1 \rrbracket$, $C^{(s)} \in \mathcal{C}^{k_s} \setminus \mathcal{C}^{k_s+1}$, $\delta_{C^{(s)}}^{n^*+1} \geq \delta_{C^{(s+1)}}^{n^*+1}$, and $\delta_{C^{(s^*)}}^{n^*+1} \geq 0$. Note that s^* exists since $k_s \leq n^* + 1$. Then, we deduce that $\delta_{C^{(1)}}^{n^*+1} \geq \dots \geq \delta_{C^{(s^*)}}^{n^*+1} \geq 0$.

Thus, $\forall C \in \mathcal{C}$, $\delta_C^{n^*+1} \geq 0$, and constraints (6) are satisfied by the output σ of the algorithm. In conclusion, the algorithm outputs a feasible solution of (Q). \square

The output of Algorithm 1, by design, satisfies constraints (5), and also constraints (6) for the maximal chains in \mathcal{C}^{n^*+1} . Recall that the remaining maximal chains were removed after an iteration k in order to maintain the conservation law on the resulting set \mathcal{C}^{k+1} . This conservation law played an essential role in proving Proposition 3, i.e., in showing that constraints (6) are also satisfied for the maximal chains that are not in \mathcal{C}^{n^*+1} (see the proof of Lemma 3). Thus, Algorithm 1's output is a feasible solution of (Q). Next, we show that this solution is optimal.

Part 3: Optimality of Algorithm 1. The final part of the proof of Theorem 2 consists in showing that the total weight used by the algorithm is exactly $\max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. This is done by considering the following quantity: $\forall k \in \llbracket 1, n^* + 1 \rrbracket$, $W^k := \max\{\max\{\rho_x^k, x \in X\}, \max\{\pi_C^k, C \in \mathcal{C}\}\}$. First, we show that $\forall k \in \llbracket 1, n^* \rrbracket$, $W^{k+1} = W^k - w^k$. Then, we show that $W^{n^*+1} = 0$. Using a telescoping series, we obtain the desired result. This part of the proof also uses Lemma 3 to conclude that $\max\{\pi_C^k, C \in \mathcal{C}\}$ is attained by a maximal chain $C \in \mathcal{C}^{k+1}$.

PROPOSITION 4. *The total weight used by the algorithm when it terminates is $\max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$.*

Proof of Proposition 4. For all $k \in \llbracket 1, n^* + 1 \rrbracket$, let $W^k := \max\{\max\{\rho_x^k, x \in X\}, \max\{\pi_C^k, C \in \mathcal{C}\}\}$. First, we show that $\forall k \in \llbracket 1, n^* \rrbracket$, $W^{k+1} = W^k - w^k$. Consider $k \in \llbracket 1, n^* \rrbracket$, and let $C \in \mathcal{C} \setminus \mathcal{C}^{k+1}$. Then, there exists $k_1 \leq k$ such that $C \in \mathcal{C}^{k_1} \setminus \mathcal{C}^{k_1+1}$. If $C \cap X^{k_1} = \emptyset$, then $\pi_C^{k+1} \leq \pi_C^k \leq \pi_C^{k_1} \stackrel{(10)}{=} -\delta_C^{k_1} \stackrel{(11)}{\leq} 0$. If $C \cap X^{k_1} \neq \emptyset$, then $\exists C^{(2)} \in \mathcal{C}^{k_1+1}$ such that $\delta_C^{k_1} \geq \delta_{C^{(2)}}^{k_1}$ and $C^{(2)} \cap X^{k_1} \supseteq C \cap X^{k_1}$ (Lemma 3). This implies that $\forall l \in \llbracket k_1, n^* + 1 \rrbracket$, $\delta_C^l \geq \delta_{C^{(2)}}^l \stackrel{(14)}{\geq}$, and $C^{(2)} \cap X^l \supseteq C \cap X^l$. Then, we obtain:

$$\forall l \in \llbracket k_1, n^* + 1 \rrbracket, \pi_C^l \stackrel{(10)}{=} \sum_{x \in C \cap X^l} \rho_x^l - \delta_C^l + \pi_{C^{(2)}}^l + \delta_{C^{(2)}}^l - \sum_{x \in C \cap X^l} \rho_x^l - \sum_{x \in (C^{(2)} \cap X^l) \setminus (C \cap X^l)} \rho_x^l \stackrel{(14)}{\leq} \pi_{C^{(2)}}^l.$$

In particular, we deduce that $\pi_C^k \leq \pi_{C^{(2)}}^k$ and $\pi_C^{k+1} \leq \pi_{C^{(2)}}^{k+1}$. As in Proposition 3, we construct a sequence of maximal chains $(C^{(s)})$, a sequence of increasing integers (k_s) , and a termination point $s' \in \mathbb{N}^*$, such that $C^{(1)} = C$, $\forall s \in \llbracket 1, s' - 1 \rrbracket$, $C^{(s)} \in \mathcal{C}^{k_s} \setminus \mathcal{C}^{k_s+1}$, $\pi_{C^{(s)}}^k \leq \pi_{C^{(s+1)}}^k$, and $\pi_{C^{(s)}}^{k+1} \leq \pi_{C^{(s+1)}}^{k+1}$. At termination, $C^{(s')} \in \mathcal{C}^{k_{s'}}$, and either $k_{s'} = k + 1$, or $k_{s'} < k + 1$ and $C^{(s')} \cap X^{k_{s'}} = \emptyset$. If $k_{s'} = k + 1$, then we conclude that $\pi_C^k \leq \pi_{C^{(s')}}^k$ and $\pi_C^{k+1} \leq \pi_{C^{(s')}}^{k+1}$, with $C^{(s')} \in \mathcal{C}^{k+1}$. If $k_{s'} < k + 1$ and $C^{(s')} \cap X^{k_{s'}} = \emptyset$, then $\pi_C^{k+1} \stackrel{(9)}{\leq} \pi_C^k \leq \pi_{C^{(s')}}^k \stackrel{(9)}{\leq} \pi_{C^{(s')}}^{k_{s'}} \stackrel{(10)}{=} -\delta_{C^{(s')}}^{k_{s'}} \stackrel{(11)}{\leq} 0 \leq \rho_x^{k+1} \stackrel{(8)}{\leq} \rho_x^k, \forall x \in X$. Thus, we deduce that $W^k = \max\{\max\{\rho_x^k, x \in X\}, \max\{\pi_C^k, C \in \mathcal{C}^{k+1}\}\}$, and $W^{k+1} = \max\{\max\{\rho_x^{k+1}, x \in X\}, \max\{\pi_C^{k+1}, C \in \mathcal{C}^{k+1}\}\}$.

Since $k \in \llbracket 1, n^* \rrbracket$ and Algorithm 1 terminates after the n^* -th iteration, we know that $X^k \neq \emptyset$. Furthermore, since $\forall x \in X^k$, $\rho_x^k \geq \rho_x^{k+1} \geq 0$, and $\forall x \in X \setminus X^k$, $\rho_x^k = \rho_x^{k+1} = 0$, then $\max\{\rho_x^k, x \in X\} = \max\{\rho_x^k, x \in X^k\}$, and $\max\{\rho_x^{k+1}, x \in X\} = \max\{\rho_x^{k+1}, x \in X^k\}$.

Next, we consider $x \in X^k \setminus S^k$. Then, $\exists y \neq x \in X^k$ such that $y \preceq_{\overline{\mathcal{C}}^k} x$, and $y \in S^k$ is a minimal element in P^k . By definition, $\exists C \in \overline{\mathcal{C}}^k$ such that $y, x \in C$, and $y \prec x$. In fact, y is the minimal element of $C \cap X^k$ in P^k , and $C \in \mathcal{C}^{k+1}$. Since $C \in \overline{\mathcal{C}}^k$, then $\pi_C^k \stackrel{(10)}{=} \sum_{x' \in C} \rho_{x'}^k \geq \rho_x^k + \rho_y^k \geq \rho_x^k$. Furthermore, since $y \in S^k$, then $w^k \stackrel{(A7)}{\leq} \rho_y^k$. Thus, we obtain that $\rho_x^{k+1} = \rho_x^k \leq \pi_C^k - \rho_y^k \leq \pi_C^k - w^k \stackrel{(9)}{=} \pi_C^{k+1}$, from which we conclude that $W^k = \max\{\max\{\rho_x^k, x \in S^k\}, \max\{\pi_C^k, C \in \mathcal{C}^{k+1}\}\}$, and $W^{k+1} = \max\{\max\{\rho_x^{k+1}, x \in S^k\}, \max\{\pi_C^{k+1}, C \in \mathcal{C}^{k+1}\}\}$.

Finally, we note that $\forall C \in \mathcal{C}^{k+1}$, $\pi_C^{k+1} \stackrel{(9)}{=} \pi_C^k - w^k$ since $S^k \cap C \neq \emptyset$, and $\forall x \in S^k$, $\rho_x^{k+1} \stackrel{(A8)}{=} \rho_x^k - w^k$. Putting everything together, we conclude:

$$\begin{aligned} W^{k+1} &= \max\{\max\{\rho_x^{k+1}, x \in S^k\}, \max\{\pi_C^{k+1}, C \in \mathcal{C}^{k+1}\}\} \\ &= \max\{\max\{\rho_x^k, x \in S^k\}, \max\{\pi_C^k, C \in \mathcal{C}^{k+1}\}\} - w^k = W^k - w^k. \end{aligned}$$

Next, we show that $W^{n^*+1} = 0$. First, we know that $\forall x \in X$, $\rho_x^{n^*+1} = 0$. Secondly, $\forall C \in \mathcal{C}^{n^*+1}$, we have $\pi_C^{n^*+1} \stackrel{(10)}{=} -\delta_C^{n^*+1} \stackrel{(11)}{\leq} 0$. Thirdly, $S^{n^*} \neq \emptyset$ since P^{n^*} is a nonempty poset. This implies that $W^{n^*+1} = \max\{\max\{\rho_x^{n^*+1}, x \in S^{n^*}\}, \max\{\pi_C^{n^*+1}, C \in \mathcal{C}^{n^*+1}\}\} = 0$. Finally, using a telescoping series, we obtain:

$$\sum_{S \in \mathcal{P}} \sigma_S \stackrel{(A7)}{=} \sum_{k=1}^{n^*} w^k = \sum_{k=1}^{n^*} W^k - W^{k+1} = W^1 - \underbrace{W^{n^*+1}}_{=0} \stackrel{(A1),(9)}{=} \max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}.$$

□

In conclusion, Propositions 2, 3, and 4 enable us to show that Algorithm 1 outputs a feasible solution of (\mathcal{Q}) with objective value equal to $\max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. Therefore $z_{(\mathcal{Q})}^* \leq \max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. Since we already established the reversed inequality at the end of Section 2.3, we conclude that $z_{(\mathcal{Q})}^* = \max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$, thus proving Theorem 2.

Furthermore, since $\forall x \in X, \rho_x \leq 1$, and $\forall C \in \mathcal{C}, \pi_C \leq 1$, then $z_{(\mathcal{Q})}^* \leq 1$. From Proposition 1, this implies that (\mathcal{D}) is feasible: Given the output σ of Algorithm 1, $\hat{\sigma}$ obtained from σ by additionally assigning $1 - z_{(\mathcal{Q})}^*$ to \emptyset satisfies (1a)-(1c), and proves Theorem 1.

We note that (\mathcal{Q}) is a generalization of a classical graph theoretic problem. The comparability graph of the poset $P = (X, \preceq)$ is an undirected graph whose set of vertices is X and whose edges are given by the pairs of comparable elements in P . In the special case where $\forall C \in \mathcal{C}, \sum_{x \in C} \rho_x = \pi_C$ (i.e., inequality (2) is tight), (\mathcal{Q}) is equivalent to the minimum-weighted fractional coloring problem on the comparability graph of P . Algorithm 1 can then be refined into Hoàng's $O(|X|^2)$ -time algorithm [16].

4. Applications to network security. In this section, we use Theorem 1 on the existence of probability distributions on posets for the purpose of equilibrium analysis of a generic security game. The game involves a routing entity and an interdicator interacting on a flow network.

4.1. Game-theoretic model. Consider a flow network, modeled as a directed connected acyclic graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where \mathcal{V} (resp. \mathcal{E}) represents the set of nodes (resp. the set of edges) of the network. For each edge $(i, j) \in \mathcal{E}$, let $c_{ij} \in \mathbb{R}_+^*$ denote its capacity. We consider that a single commodity can flow in \mathcal{G} from a source node $s \in \mathcal{V}$ to a destination node $t \in \mathcal{V}$. An $s - t$ path λ of size n is a sequence of edges $\{e_1 = (s_1, t_1), \dots, e_n = (s_n, t_n)\}$ such that $s_1 = s, t_n = t$, and for all $k \in \llbracket 1, n - 1 \rrbracket, t_k = s_{k+1}$. We denote Λ the set containing all $s - t$ paths of \mathcal{G} .

A flow, defined by the vector $f \in \mathbb{R}_+^{|\Lambda|}$, enters the network from s and leaves from t . A flow f is said to be feasible if the flow through each edge does not exceed its capacity; that is, for all $(i, j) \in \mathcal{E}, f_{ij} := \sum_{\{\lambda \in \Lambda \mid (i, j) \in \lambda\}} f_\lambda \leq c_{ij}$. Let \mathcal{F} denote the set of feasible flows of \mathcal{G} . Given a feasible flow $f \in \mathcal{F}$, let $F(f) = \sum_{\lambda \in \Lambda} f_\lambda$ denote the amount of flow sent from the node s to the node t . Each edge $(i, j) \in \mathcal{E}$ is associated with a marginal transportation cost, denoted $b_{ij} \in \mathbb{R}_+^*$. Thus, for each $s - t$ path $\lambda \in \Lambda, b_\lambda := \sum_{(i, j) \in \lambda} b_{ij}$ represents the cost of transporting one unit of flow through λ . Given a feasible flow $f \in \mathcal{F}, T(f) := \sum_{\lambda \in \Lambda} b_\lambda f_\lambda$ denotes the total transportation cost of f .

Consider a two-player strategic game $\Gamma := \langle \{1, 2\}, (\mathcal{F}, \mathcal{I}), (u_1, u_2) \rangle$, played on the flow network \mathcal{G} . Player 1 (**P1**) is the routing entity that chooses to route a flow $f \in \mathcal{F}$ of goods through the network, and player 2 (**P2**) is the interdicator who simultaneously chooses a subset of edges $I \in 2^\mathcal{E}$

to interdict. The action set for **P1** (resp. **P2**) is \mathcal{F} (resp. $\mathcal{I} := 2^{\mathcal{E}}$). For every edge $(i, j) \in \mathcal{E}$, $d_{ij} \in \mathbb{R}_+^*$ denotes the cost of interdicting (i, j) . Thus, the cost of any interdiction $I \in \mathcal{I}$ is given by $C(I) := \sum_{(i,j) \in I} d_{ij}$. In this model, **P2** (resp. **P1**) gains (resp. loses) the flow that crosses the edges that are interdicted by **P2**; furthermore, **P1** cannot re-route its flow after **P2**'s interdiction.¹ The *effective flow*, denoted f^I , when a flow f is chosen by **P1** and an interdiction I is chosen by **P2** can be expressed as follows: $\forall \lambda \in \Lambda$, $f_\lambda^I = f_\lambda \mathbf{1}_{\{\lambda \cap I = \emptyset\}}$. We also suppose that the transportation cost incurred by **P1** is for the initial flow f and not for the effective flow f^I . This modeling choice reflects a monetary transaction between the routing entity and the network owner; for example, an advance fee incurred by the routing entity for accessing and sending a quantity of flow through the edges of the network.

The payoff of **P1** is defined as the value of effective flow assessed by **P1** net the cost of transporting the initial flow: $u_1(f, I) = p_1 F(f^I) - T(f)$, where $p_1 \in \mathbb{R}_+^*$ is the marginal value of effective flow for **P1**. Similarly, the payoff of **P2** is defined as the value of interdicted flow assessed by **P2** net the cost of interdiction: $u_2(f, I) = p_2(F(f) - F(f^I)) - C(I)$, where $p_2 \in \mathbb{R}_+^*$ is the marginal value of interdicted flow for **P2**.

We consider that **P1** can route goods in the network using a flow f realized from a chosen probability distribution on the set \mathcal{F} , and **P2** can interdict subsets of edges according to a probability distribution on the set \mathcal{I} . Specifically, **P1** and **P2** respectively choose a mixed routing strategy $\sigma^1 \in \Delta(\mathcal{F})$ and a mixed interdiction strategy $\sigma^2 \in \Delta(\mathcal{I})$, where $\Delta(\mathcal{F}) = \{\sigma^1 \in \mathbb{R}_+^{|\mathcal{F}|} \mid \sum_{f \in \mathcal{F}} \sigma_f^1 = 1\}$, and $\Delta(\mathcal{I}) = \{\sigma^2 \in \mathbb{R}_+^{|\mathcal{I}|} \mid \sum_{I \in \mathcal{I}} \sigma_I^2 = 1\}$ denote the strategy sets. Here, σ_f^1 (resp. σ_I^2) represents the probability assigned to the flow f (resp. interdiction I) by **P1**'s routing strategy σ^1 (resp. **P2**'s interdiction strategy σ^2). The players' strategies are independent randomizations. Given a strategy profile $\sigma = (\sigma^1, \sigma^2) \in \Delta(\mathcal{F}) \times \Delta(\mathcal{I})$, the respective expected payoffs are expressed as:

$$U_1(\sigma^1, \sigma^2) = p_1 \mathbb{E}_\sigma[F(f^I)] - \mathbb{E}_\sigma[T(f)], \quad (15)$$

$$U_2(\sigma^1, \sigma^2) = p_2 (\mathbb{E}_\sigma[F(f)] - \mathbb{E}_\sigma[F(f^I)]) - \mathbb{E}_\sigma[C(I)]. \quad (16)$$

Thus, the mixed extension of the game Γ is $\langle \{1, 2\}, (\Delta(\mathcal{F}), \Delta(\mathcal{I})), (U_1, U_2) \rangle$.

We seek to study the mixed strategy Nash equilibria of this game. A strategy profile $(\sigma^{1*}, \sigma^{2*}) \in \Delta(\mathcal{F}) \times \Delta(\mathcal{I})$ is a mixed strategy *Nash Equilibrium* (NE) of game Γ if: $\forall \sigma^1 \in \Delta(\mathcal{F})$, $U_1(\sigma^{1*}, \sigma^{2*}) \geq U_1(\sigma^1, \sigma^{2*})$, and $\forall \sigma^2 \in \Delta(\mathcal{I})$, $U_2(\sigma^{1*}, \sigma^{2*}) \geq U_2(\sigma^{1*}, \sigma^2)$. Equivalently, in a NE $(\sigma^{1*}, \sigma^{2*})$, σ^{1*} (resp. σ^{2*}) is a best response to σ^{2*} (resp. σ^{1*}). We denote Σ the set of NE of Γ . We will also use the notations $U_i(\sigma^1, I) = U_i(\sigma^1, \mathbf{1}_{\{I\}})$ and $U_i(f, \sigma^2) = U_i(\mathbf{1}_{\{f\}}, \sigma^2)$ for $i \in \{1, 2\}$.

We now proceed with the equilibrium analysis of the game Γ .

¹ We do not consider partial edge interdictions for the sake of simplicity.

4.2. Properties of Nash equilibria. We first note that Γ is strategically equivalent to a zero-sum game. In particular, the following transformation preserves the set of NE:

$$\forall (f, I) \in \mathcal{F} \times \mathcal{I}, \quad \frac{1}{p_1} u_1(f, I) + \frac{1}{p_2} C(I) = F(f') - \frac{1}{p_1} T(f) + \frac{1}{p_2} C(I) =: \tilde{u}_1(f, I), \quad (17)$$

$$\forall (f, I) \in \mathcal{F} \times \mathcal{I}, \quad \frac{1}{p_2} u_2(f, I) - F(f) + \frac{1}{p_1} T(f) = -F(f') + \frac{1}{p_1} T(f) - \frac{1}{p_2} C(I) =: -\tilde{u}_1(f, I). \quad (18)$$

Therefore, Γ and $\tilde{\Gamma} := (\{1, 2\}, (\mathcal{F}, \mathcal{I}), (\tilde{u}_1, -\tilde{u}_1))$ have the same equilibrium set. Additionally, NE of Γ are interchangeable, i.e., if $(\sigma^{1*}, \sigma^{2*}) \in \Sigma$ and $(\sigma^{1'}, \sigma^{2'}) \in \Sigma$, then $(\sigma^{1*}, \sigma^{2'}) \in \Sigma$ and $(\sigma^{1'}, \sigma^{2*}) \in \Sigma$.

In principle, NE of Γ can be obtained by using linear programming techniques. However, this would entail solving a linear program with an infinite number of variables and an exponential number of constraints (since \mathcal{F} is the set of feasible flows in \mathcal{G} , and $|\mathcal{I}| = 2^{|\mathcal{E}|}$). We now present our approach for analyzing the NE of the game Γ . Our approach, which utilizes the existence result on posets Theorem 1, is based on a minimum cost circulation problem. Essentially, we show that its primal solutions are equilibrium routing strategies for **P1**, and that its dual solutions give properties of equilibrium interdiction strategies for **P2**.

Specifically, consider the following network flow problem:

$$\begin{aligned} (\mathcal{M}) \quad & \text{maximize } F(f) - \frac{1}{p_1} T(f) \\ & \text{subject to } \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda \leq \min \left\{ \frac{d_{ij}}{p_2}, c_{ij} \right\}, \forall (i, j) \in \mathcal{E} \\ & f_\lambda \geq 0, \quad \forall \lambda \in \Lambda. \end{aligned}$$

This problem can be viewed as a minimum cost circulation problem in a graph $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ such that $\mathcal{V}' = \mathcal{V}$, $\mathcal{E}' = \mathcal{E} \cup \{(t, s)\}$. The capacity of each edge $(i, j) \in \mathcal{E}$ is given by $\min\{\frac{d_{ij}}{p_2}, c_{ij}\}$, and edge (t, s) is uncapacitated. The transportation cost of each edge $(i, j) \in \mathcal{E}$ is given by $\frac{b_{ij}}{p_1}$, and the transportation cost of edge (t, s) is -1 .

Equivalently, (\mathcal{M}) consists in finding a feasible flow f in \mathcal{F} that maximizes $u_1(f, \emptyset)$ with the requirement that the flow through each edge (i, j) is no more than $\frac{d_{ij}}{p_2}$. Game theoretically, this threshold captures **P2**'s best response to **P1**: If $f_{ij} > \frac{d_{ij}}{p_2}$ for some $(i, j) \in \mathcal{E}$, then **P2** has an incentive to interdict (i, j) , resulting in an increase of **P2**'s payoff (since $u_2(f, \{(i, j)\}) = p_2 f_{ij} - d_{ij} > 0$). Thus, (\mathcal{M}) can be viewed as the problem in which **P1** maximizes its payoff while limiting **P2**'s incentive to interdict any of the edges. For each $s - t$ path $\lambda \in \Lambda$, let us denote $\pi_\lambda^0 := 1 - \frac{b_\lambda}{p_1}$. Then,

the value $p_1\pi_\lambda^0$ represents the gain in **P1**'s payoff when one unit of flow traveling along λ reaches the destination node. The primal and dual formulations of (\mathcal{M}) are given as follows:

$$\begin{array}{l|l}
(\mathcal{M}_P): \max \sum_{\lambda \in \Lambda} \pi_\lambda^0 f_\lambda & (\mathcal{M}_D): \min \sum_{(i,j) \in \mathcal{E}} \left(\frac{d_{ij}}{p_2} \rho_{ij} + c_{ij} \mu_{ij} \right) \\
\text{s.t.} \quad \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda \leq \frac{d_{ij}}{p_2}, \quad \forall (i,j) \in \mathcal{E} & \text{s.t.} \quad \sum_{(i,j) \in \lambda} (\rho_{ij} + \mu_{ij}) \geq \pi_\lambda^0, \quad \forall \lambda \in \Lambda \\
\sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda \leq c_{ij}, \quad \forall (i,j) \in \mathcal{E} & \rho_{ij} \geq 0, \quad \forall (i,j) \in \mathcal{E} \\
f_\lambda \geq 0, \quad \forall \lambda \in \Lambda & \mu_{ij} \geq 0, \quad \forall (i,j) \in \mathcal{E}
\end{array}$$

Let f^* and (ρ^*, μ^*) denote optimal solutions of (\mathcal{M}_P) and (\mathcal{M}_D) , respectively. By strong duality, the optimal value of (\mathcal{M}_P) is identical to that of (\mathcal{M}_D) ; we denote it by $z_{(\mathcal{M})}^*$. Note that (\mathcal{M}_P) and (\mathcal{M}_D) may have an exponential number of variables and constraints, respectively. However, equivalent primal and dual formulations of (\mathcal{M}) of polynomial size can be derived; see Appendix C. Thus, f^* and (ρ^*, μ^*) can be computed in an efficient manner by using an interior point method (Karmarkar [18]) or a dual network simplex algorithm (Orlin et al. [23]).

The following properties for a pair of optimal solutions f^* and (ρ^*, μ^*) of (\mathcal{M}_P) and (\mathcal{M}_D) can be obtained from complementary slackness:

$$\forall (i,j) \in \mathcal{E}, \rho_{ij}^* > 0 \implies f_{ij}^* = \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda^* = \frac{d_{ij}}{p_2}, \quad (19)$$

$$\forall (i,j) \in \mathcal{E}, \mu_{ij}^* > 0 \implies f_{ij}^* = \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda^* = c_{ij}, \quad (20)$$

$$\forall \lambda \in \Lambda, f_\lambda^* > 0 \implies \sum_{(i,j) \in \lambda} (\rho_{ij}^* + \mu_{ij}^*) = \pi_\lambda^0. \quad (21)$$

These properties, along with Theorem 1, enable us to derive the following result:

PROPOSITION 5. *Consider f^* and (ρ^*, μ^*) optimal solutions of (\mathcal{M}_P) and (\mathcal{M}_D) , respectively. Theorem 1 guarantees the existence of an interdiction strategy $\tilde{\sigma}^2 \in \Delta(\mathcal{I})$ satisfying:*

$$\forall (i,j) \in \mathcal{E}, \quad \sum_{\{I \in \mathcal{I} \mid (i,j) \in I\}} \tilde{\sigma}_I^2 = \rho_{ij}^*, \quad (22)$$

$$\forall \lambda \in \Lambda, \quad \sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 \geq \pi_\lambda^*, \quad (23)$$

where $\forall \lambda \in \Lambda, \pi_\lambda^* := \pi_\lambda^0 - \sum_{(i,j) \in \lambda} \mu_{ij}^*$.

The strategy profile $(f^*, \tilde{\sigma}^2) \in \mathcal{F} \times \Delta(\mathcal{I})$ is a NE of the game Γ . The corresponding equilibrium payoffs are $U_1(f^*, \tilde{\sigma}^2) = p_1 \sum_{(i,j) \in \mathcal{E}} c_{ij} \mu_{ij}^*$ and $U_2(f^*, \tilde{\sigma}^2) = 0$.

Thus, a solution f^* (resp. (ρ^*, μ^*)) of the primal (resp. dual) formulation of (\mathcal{M}) can be used to describe a NE of Γ . In particular, f^* is a pure equilibrium strategy for **P1**. Furthermore, for all

$(i, j) \in \mathcal{E}$, ρ_{ij}^* is the probability with which edge (i, j) is interdicted by **P2** in equilibrium. To draw this conclusion, we need to show the existence of an interdiction strategy $\tilde{\sigma}^2 \in \Delta(\mathcal{I})$ satisfying (22) and (23). In fact, this existence problem is an instantiation of problem (D) that we introduced earlier, and positively answered in Theorem 1.

Additional properties of **P2**'s equilibrium interdiction strategy $\tilde{\sigma}^2$ are given by μ^* : Given an $s-t$ path $\lambda \in \Lambda$, π_λ^0 is the probability above which λ should be interdicted in equilibrium by **P2**. However, when edges belonging to λ have high interdiction costs, **P2** does not interdict these edges, and may not be able to interdict λ with probability π_λ^0 . The reduction of interdiction probability of λ is captured by $\sum_{(i,j) \in \lambda} \mu_{ij}^*$. Indeed, by complementary slackness (20), $\mu_{ij}^* > 0$ for $(i, j) \in \lambda$ only when $c_{ij} = f_{ij}^* \leq \frac{d_{ij}}{p_2}$, i.e., when the interdiction cost of (i, j) is too high. The resulting interdiction probability of λ in equilibrium is then given by $\pi_\lambda^* = \pi_\lambda^0 - \sum_{(i,j) \in \lambda} \mu_{ij}^*$.

Consequently, if an $s-t$ path $\lambda \in \Lambda$ is such that $\sum_{(i,j) \in \lambda} \mu_{ij}^* > 0$, then each unit of flow sent through λ increases **P1**'s payoff by $p_1 \sum_{(i,j) \in \lambda} \mu_{ij}^*$. This is captured by **P1**'s equilibrium strategy f^* , which saturates every edge $(i, j) \in \mathcal{E}$ for which $\mu_{ij}^* > 0$ (see (20)). Since f^* only takes $s-t$ paths that are interdicted with probability exactly π^* (from (21)-(23)), the resulting equilibrium payoff for **P1** can then be derived from μ^* ; see Proposition 5. Recall that f^* is such that interdicting any edge does not increase **P2**'s payoff. Furthermore, **P2** only interdicts edges for which the value of interdicted flow compensates the interdiction cost (from (19)). Thus, her payoff is 0 in equilibrium.

We note that **P1** does not need to randomize its flow in the game Γ . Indeed, for every routing strategy $\sigma^1 \in \Delta(\mathcal{F})$, the flow \bar{f} defined by $\forall \lambda \in \Lambda$, $\bar{f}_\lambda = \mathbb{E}_{\sigma^1}[f_\lambda]$, satisfies the following properties: $\bar{f} \in \mathcal{F}$, and $\forall i \in \{1, 2\}$, $\forall \sigma^2 \in \Delta(\mathcal{I})$, $U_i(\sigma^1, \sigma^2) = U_i(\bar{f}, \sigma^2)$.

Proof of Proposition 5. Let f^* and (ρ^*, μ^*) be optimal solutions of (\mathcal{M}_P) and (\mathcal{M}_D) , respectively. First, we define the following binary relation on \mathcal{E} , denoted $\preceq_{\mathcal{G}}$. Given $(u, v) \in \mathcal{E}^2$, $u \preceq_{\mathcal{G}} v$ if either $u = v$, or there exists an $s-t$ path $\lambda \in \Lambda$ that traverses u and v in this order. Since \mathcal{G} is a directed acyclic connected graph, we have the following lemma, which is proven separately in Appendix A:

LEMMA 4. $P = (\mathcal{E}, \preceq_{\mathcal{G}})$ is a poset, whose set of maximal chains is the set of $s-t$ paths Λ .

Thus, showing that there exists $\tilde{\sigma}^2 \in \Delta(\mathcal{I})$ that satisfies (22) and (23) is an instantiation of problem (D). Since (ρ^*, μ^*) is a feasible solution of (\mathcal{M}_D) , then condition (2) is satisfied, i.e., $\forall \lambda \in \Lambda$, $\sum_{(i,j) \in \lambda} \rho_{ij}^* \geq \pi_\lambda^*$. Additionally, for any $s-t$ path $\lambda \in \Lambda$, $\pi_\lambda^* = 1 - \sum_{(i,j) \in \lambda} (\frac{b_{ij}}{p_1} + \mu_{ij}^*)$, and π^* is an affine function of the elements constituting each $s-t$ path. Therefore, π^* satisfies the conservation law described in (3). Finally, since $\forall (i, j) \in \mathcal{E}$, $\rho_{ij}^* \in [0, 1]$, and $\forall \lambda \in \Lambda$, $\pi_\lambda^* \leq 1$, all conditions of Theorem 1 are satisfied, and we obtain the existence of an interdiction strategy $\tilde{\sigma}^2 \in \Delta(\mathcal{I})$ satisfying (22) and (23).

Next, we show that $(f^*, \tilde{\sigma}^2)$ is a NE. We can write the following inequality for **P1**'s payoff:

$$\begin{aligned} \forall f \in \mathcal{F}, U_1(f, \tilde{\sigma}^2) &\stackrel{(15)}{=} p_1 \sum_{\lambda \in \Lambda} f_\lambda \mathbb{E}_{\tilde{\sigma}^2} [1 - \mathbb{1}_{\{I \cap \lambda \neq \emptyset\}}] - \sum_{\lambda \in \Lambda} b_\lambda f_\lambda = p_1 \sum_{\lambda \in \Lambda} \pi_\lambda^0 f_\lambda - p_1 \sum_{\lambda \in \Lambda} f_\lambda \sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 \\ &\stackrel{(23)}{\leq} p_1 \sum_{\lambda \in \Lambda} f_\lambda \sum_{(i,j) \in \mathcal{E}} \mu_{ij}^* = p_1 \sum_{(i,j) \in \mathcal{E}} f_{ij} \mu_{ij}^* \leq p_1 \sum_{(i,j) \in \mathcal{E}} c_{ij} \mu_{ij}^*. \end{aligned} \quad (24)$$

Now, given $\lambda \in \Lambda$ such that $f_\lambda^* > 0$, we obtain:

$$\sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 \leq \sum_{I \in \mathcal{I}} \tilde{\sigma}_I^2 |I \cap \lambda| = \sum_{(i,j) \in \mathcal{E}} \sum_{I \in \mathcal{I}} \tilde{\sigma}_I^2 \mathbb{1}_{\{(i,j) \in I\}} \stackrel{(22)}{=} \sum_{(i,j) \in \lambda} \rho_{ij}^* \stackrel{(21),(23)}{\leq} \sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2. \quad (25)$$

Furthermore, $\forall (i,j) \in \mathcal{E}$ such that $\mu_{ij}^* > 0$, $f_{ij}^* \stackrel{(20)}{=} c_{ij}$. Then, inequality (24) is tight for f^* , and $U_1(f^*, \tilde{\sigma}^2) = p_1 \sum_{(i,j) \in \mathcal{E}} c_{ij} \mu_{ij}^*$.

Similarly, regarding **P2**'s payoff, we first derive the following inequality:

$$\forall I \in \mathcal{I}, \sum_{(i,j) \in I} \frac{d_{ij}}{p_2} \geq \sum_{(i,j) \in I} \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda^* = \sum_{\lambda \in \Lambda} f_\lambda^* |I \cap \lambda| \geq \sum_{\lambda \in \Lambda} f_\lambda^* \mathbb{1}_{\{I \cap \lambda \neq \emptyset\}} = F(f^*) - F(f^{*I}). \quad (26)$$

Therefore, $\forall I \in \mathcal{I}$, $U_2(f^*, I) \stackrel{(16)}{=} p_2(F(f^*) - F(f^{*I})) - \sum_{(i,j) \in I} d_{ij} \stackrel{(26)}{\leq} 0$.

Now, given $\lambda \in \Lambda$ such that $f_\lambda^* > 0$, we obtain:

$$\pi_\lambda^0 - \sum_{(i,j) \in \lambda} \mu_{ij}^* \stackrel{(21)}{=} \sum_{(i,j) \in \lambda} \rho_{ij}^* \stackrel{(22)}{=} \sum_{I \in \mathcal{I}} \tilde{\sigma}_I^2 |S \cap \lambda| \geq \sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 \stackrel{(23)}{\geq} \pi_\lambda^0 - \sum_{(i,j) \in \lambda} \mu_{ij}^*. \quad (27)$$

Therefore, $\forall I \in \text{supp}(\tilde{\sigma}^2)$, $|I \cap \lambda| \leq 1$. Furthermore, given $I \in \text{supp}(\tilde{\sigma}^2)$ and $(i,j) \in I$, $\sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda^* \stackrel{(19)}{=} \frac{d_{ij}}{p_2}$, since $\rho_{ij}^* > 0$. Thus, $\forall I \in \text{supp}(\tilde{\sigma}^2)$, inequality (26) is tight, and $U_2(f^*, I) = 0$. Therefore, $U_2(f^*, \tilde{\sigma}^2) = 0$, and $(f^*, \tilde{\sigma}^2)$ is a NE. \square

We remark that in the simpler case where each $s-t$ path has an identical transportation cost, (\mathcal{M}) can be viewed as a maximum flow problem. Then, our approach simply computes a NE of the game Γ from a maximum flow for **P1**, and a minimum-cut set for **P2**.

Next, we characterize the set of $s-t$ paths (resp. set of edges) that are chosen (resp. interdicted) in at least one NE. This involves using the notion of *strict complementary slackness*. Specifically, optimal solutions f^\dagger and $(\rho^\dagger, \mu^\dagger)$ of (\mathcal{M}_P) and (\mathcal{M}_D) satisfy strict complementary slackness if:

$$\forall (i,j) \in \mathcal{E}, \text{ either } \rho_{ij}^\dagger > 0 \text{ or } f_{ij}^\dagger = \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda^\dagger < \frac{d_{ij}}{p_2}, \quad (28)$$

$$\forall (i,j) \in \mathcal{E}, \text{ either } \mu_{ij}^\dagger > 0 \text{ or } f_{ij}^\dagger = \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f_\lambda^\dagger < c_{ij}, \quad (29)$$

$$\forall \lambda \in \Lambda, \text{ either } f_\lambda^\dagger > 0 \text{ or } \sum_{(i,j) \in \lambda} (\rho_{ij}^\dagger + \mu_{ij}^\dagger) > \pi_\lambda^0. \quad (30)$$

We say that f^\dagger and $(\rho^\dagger, \mu^\dagger)$ form a *strictly complementary primal-dual pair* of optimal solutions of (\mathcal{M}) . Such a pair is guaranteed to exist by the Goldman-Tucker theorem [12], and can be computed using any of the existing methods in the literature (see Balinski and Tucker [5], Adler et al. [1], Jansen et al. [17]). From Proposition 5, we already know that there exists a NE of Γ where $\mathbf{P1}$'s strategy is f^\dagger and $\mathbf{P2}$'s strategy is such that each edge (i, j) is interdicted with probability ρ_{ij}^\dagger . In fact, we can show that f^\dagger and ρ^\dagger characterize the $s - t$ paths and edges that are chosen by both players in equilibrium:

THEOREM 3. *Let f^\dagger and $(\rho^\dagger, \mu^\dagger)$ be a strictly complementary primal-dual pair of optimal solutions of (\mathcal{M}) . The set of $s - t$ paths (resp. the set of edges) that are chosen with positive probability by $\mathbf{P1}$'s strategy (resp. $\mathbf{P2}$'s strategy) in at least one NE is given by $\text{supp}(f^\dagger)$ (resp. $\text{supp}(\rho^\dagger)$):*

$$\bigcup_{(\sigma^{1*}, \sigma^{2*}) \in \Sigma} \bigcup_{f \in \text{supp}(\sigma^{1*})} \{\lambda \in \Lambda \mid f_\lambda > 0\} = \text{supp}(f^\dagger), \quad \bigcup_{(\sigma^{1*}, \sigma^{2*}) \in \Sigma} \bigcup_{I \in \text{supp}(\sigma^{2*})} I = \text{supp}(\rho^\dagger).$$

Proof of Theorem 3. Let f^\dagger and $(\rho^\dagger, \mu^\dagger)$ be optimal solutions of (\mathcal{M}_P) and (\mathcal{M}_D) that satisfy strict complementary slackness. We denote $\tilde{\sigma}^2 \in \Delta(\mathcal{I})$ the interdiction strategy, constructed from Algorithm 1, which interdicts every edge $(i, j) \in \mathcal{E}$ with probability ρ_{ij}^\dagger , and interdicts every $s - t$ path $\lambda \in \Lambda$ with probability at least $\pi_\lambda^\dagger := \pi_\lambda^0 - \sum_{(i,j) \in \lambda} \mu_{ij}^\dagger$. Given Σ the set of NE of the game Γ , let $\mathcal{H}_1 := \bigcup_{(\sigma^{1*}, \sigma^{2*}) \in \Sigma} \bigcup_{f \in \text{supp}(\sigma^{1*})} \{\lambda \in \Lambda \mid f_\lambda > 0\}$ and $\mathcal{H}_2 := \bigcup_{(\sigma^{1*}, \sigma^{2*}) \in \Sigma} \bigcup_{I \in \text{supp}(\sigma^{2*})} I$.

From Proposition 5, we know that $(f^\dagger, \tilde{\sigma}^2)$ is a NE. Consequently, $\mathcal{H}_1 \supseteq \text{supp}(f^\dagger)$, and $\mathcal{H}_2 \supseteq \text{supp}(\rho^\dagger)$. To show the reversed inclusions, we exploit properties of zero-sum games: Recall that the game Γ is strategically equivalent to the game $\tilde{\Gamma} = \langle \{1, 2\}, (\mathcal{F}, \mathcal{I}), (\tilde{u}_1, -\tilde{u}_1) \rangle$ where \tilde{u}_1 is given by (17). Therefore, each player's payoff in $\tilde{\Gamma}$ is identical in any NE. We note the following equality:

$$\mathbb{E}_{\tilde{\sigma}^2}[\mathbb{F}(f^\dagger) - \mathbb{F}(f^{\dagger I})] \stackrel{(27)}{=} \sum_{\lambda \in \Lambda} f_\lambda^\dagger \mathbb{E}_{\tilde{\sigma}^2}[|I \cap \lambda|] \stackrel{(22)}{=} \sum_{\lambda \in \Lambda} f_\lambda^\dagger \sum_{(i,j) \in \lambda} \rho_{ij}^\dagger \stackrel{(29),(30)}{=} z_{(\mathcal{M})}^* - \sum_{(i,j) \in \mathcal{E}} c_{ij} \mu_{ij}^\dagger, \quad (31)$$

where $z_{(\mathcal{M})}^*$ is the optimal value of (\mathcal{M}) . This enables us to obtain $\mathbf{P1}$'s equilibrium payoff in the zero-sum game $\tilde{\Gamma}$: For every $(\sigma^{1*}, \sigma^{2*}) \in \Sigma$,

$$\begin{aligned} \tilde{U}_1(\sigma^{1*}, \sigma^{2*}) &= \tilde{U}_1(f^\dagger, \tilde{\sigma}^2) \stackrel{(17)}{=} \mathbb{E}_{\tilde{\sigma}^2}[\mathbb{F}(f^{\dagger I})] - \mathbb{F}(f^\dagger) + \mathbb{F}(f^\dagger) - \frac{1}{p_1} \mathbb{T}(f^\dagger) + \frac{1}{p_2} \sum_{I \in \mathcal{I}} \tilde{\sigma}_I^2 \sum_{(i,j) \in I} d_{ij} \\ &\stackrel{(22)}{=} -\mathbb{E}_{\tilde{\sigma}^2}[\mathbb{F}(f^\dagger) - \mathbb{F}(f^{\dagger I})] + z_{(\mathcal{M})}^* + \frac{1}{p_2} \sum_{(i,j) \in \mathcal{E}} d_{ij} \rho_{ij}^\dagger \stackrel{(31)}{=} z_{(\mathcal{M})}^*. \end{aligned} \quad (32)$$

Consider $(\sigma^{1*}, \sigma^{2*}) \in \Sigma$. Then, $(f^\dagger, \sigma^{2*}) \in \Sigma$ as well. Thus:

$$\forall I \in \text{supp}(\sigma^{2*}), \quad z_{(\mathcal{M})}^* \stackrel{(32)}{=} \tilde{U}_1(f^\dagger, I) \stackrel{(17)}{=} \frac{1}{p_2} \mathbb{C}(I) + \mathbb{F}(f^{\dagger I}) - \mathbb{F}(f^\dagger) + \mathbb{F}(f^\dagger) - \frac{1}{p_1} \mathbb{T}(f^\dagger) \stackrel{(26)}{\geq} z_{(\mathcal{M})}^*.$$

Therefore, for $I \in \text{supp}(\sigma^{2*})$, (26) is tight, i.e., $\forall (i, j) \in I$, $\frac{d_{ij}}{p_2} = \sum_{\{\lambda \in \Lambda \mid (i, j) \in \lambda\}} f_\lambda^\dagger$. From (28), we deduce that $\forall (i, j) \in I$, $\rho_{ij}^\dagger > 0$, i.e., $(i, j) \in \text{supp}(\rho^\dagger)$. We can then conclude that $\mathcal{H}_2 \subseteq \text{supp}(\rho^\dagger)$, and we obtain that $\mathcal{H}_2 = \text{supp}(\rho^\dagger)$.

We now show the remaining inclusion for \mathcal{H}_1 . Given $(\sigma^{1*}, \sigma^{2*}) \in \Sigma$, we know that $(\sigma^{1*}, \tilde{\sigma}^2) \in \Sigma$ as well. Recall that $\forall S \in \text{supp}(\tilde{\sigma}^2)$, (26) is tight. This implies that for every $f \in \text{supp}(\sigma^{1*})$,

$$z_{(\mathcal{M})}^* \stackrel{(32)}{=} \tilde{U}_1(f, \tilde{\sigma}^2) \stackrel{(17)}{=} \frac{1}{p_1} U_1(f, \tilde{\sigma}^2) + \frac{1}{p_2} \mathbb{E}_{\tilde{\sigma}^2}[\mathbb{C}(I)] \stackrel{(26), (31)}{=} \frac{1}{p_1} U_1(f, \tilde{\sigma}^2) + z_{(\mathcal{M})}^* - \sum_{(i, j) \in \mathcal{E}} c_{ij} \mu_{ij}^\dagger \stackrel{(24)}{\leq} z_{(\mathcal{M})}^*.$$

Therefore, $\forall f \in \text{supp}(\sigma^{1*})$, (24) is tight, i.e., $\forall \lambda \in \Lambda \mid f_\lambda > 0$, $\sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 = \pi_\lambda^0 - \sum_{(i, j) \in \lambda} \mu_{ij}^\dagger$. However, this is not enough to invoke strict complementary slackness (30). We also need to show (by contradiction) that $\forall I \in \text{supp}(\tilde{\sigma}^2)$, $\forall f \in \text{supp}(\sigma^{1*})$, $\forall \lambda \in \Lambda$ such that $f_\lambda > 0$, we have $|I \cap \lambda| \leq 1$.

Let us assume that $\exists (I', f', \lambda') \in \text{supp}(\tilde{\sigma}^2) \times \text{supp}(\sigma^{1*}) \times \Lambda$ such that $f'_{\lambda'} > 0$ and $|I' \cap \lambda'| \geq 2$. Since I' interdicts at least two edges belonging to λ' , which is taken by a flow in the support of σ^{1*} , then we can construct another interdiction strategy $\sigma^{2'}$ that provides **P2** with a better payoff than $\tilde{\sigma}^2$ does. This is done by reassigning some probability initially assigned to I' by $\tilde{\sigma}^2$ to a non trivial partition of I' . This is possible because no interdiction \emptyset belongs to the support of $\tilde{\sigma}^2$, which is guaranteed by Theorem 2.

Specifically, from Theorem 2, we know that $\tilde{\sigma}_\emptyset^2 = 1 - \max\{\max\{\rho_{ij}^\dagger, (i, j) \in \mathcal{E}\}, \max\{\pi_\lambda^\dagger, \lambda \in \Lambda\}\}$. Since $\forall (i, j) \in \mathcal{E}$, $b_{ij} > 0$ and $\mu_{ij}^\dagger \geq 0$, then $\forall \lambda \in \Lambda$, $\pi_\lambda^\dagger = 1 - \sum_{(i, j) \in \lambda} (\frac{b_{ij}}{p_1} + \mu_{ij}^\dagger) < 1$. By optimality of ρ^\dagger in (\mathcal{M}_D) , we deduce that $\forall (i, j) \in \mathcal{E}$, $\rho_{ij}^\dagger < 1$. Therefore, $\tilde{\sigma}_\emptyset^2 > 0$. Now, let $\epsilon = \min\{\tilde{\sigma}_\emptyset^2, \tilde{\sigma}_{I'}^2\} > 0$, and let $e \in I' \cap \lambda'$. Then, we construct the strategy $\sigma^{2'} \in \Delta(\mathcal{I})$ defined by $\sigma_{I'}^{2'} = \tilde{\sigma}_{I'}^2 - \epsilon$, $\sigma_{I' \setminus \{e\}}^{2'} = \tilde{\sigma}_{I' \setminus \{e\}}^2 + \epsilon$, $\sigma_{\{e\}}^{2'} = \tilde{\sigma}_{\{e\}}^2 + \epsilon$, $\sigma_\emptyset^{2'} = \tilde{\sigma}_\emptyset^2 - \epsilon$, and $\sigma_I^{2'} = \tilde{\sigma}_I^2$, $\forall I \in \text{supp}(\tilde{\sigma}^2) \setminus \{I', I' \setminus \{e\}, \{e\}, \emptyset\}$.

First, we note that the edge interdiction probabilities are preserved between $\tilde{\sigma}^2$ and $\sigma^{2'}$, i.e., $\forall (i, j) \in \mathcal{E}$, $\mathbb{E}_{\sigma^{2'}}[\mathbb{1}_{\{(i, j) \in I\}}] = \mathbb{E}_{\tilde{\sigma}^2}[\mathbb{1}_{\{(i, j) \in I\}}] \stackrel{(22)}{=} \rho_{ij}^\dagger$. Secondly, each $s - t$ path $\lambda \in \Lambda$ is interdicted by $\sigma^{2'}$ with a probability no less than the probability with which λ is interdicted by $\tilde{\sigma}^2$, i.e., $\forall \lambda \in \Lambda$, $\mathbb{E}_{\sigma^{2'}}[\mathbb{1}_{\{I \cap \lambda \neq \emptyset\}}] \geq \mathbb{E}_{\tilde{\sigma}^2}[\mathbb{1}_{\{I \cap \lambda \neq \emptyset\}}]$. Thirdly, given λ' , since $|I' \cap \lambda'| \geq 2$ and $e \in I' \cap \lambda'$, then $I' \setminus \{e\} \cap \lambda' \neq \emptyset$ as well. This implies that $\mathbb{E}_{\sigma^{2'}}[\mathbb{1}_{\{I \cap \lambda' \neq \emptyset\}}] = \mathbb{E}_{\tilde{\sigma}^2}[\mathbb{1}_{\{I \cap \lambda' \neq \emptyset\}}] + \epsilon$.

Putting everything together, we obtain:

$$U_2(\sigma^{1*}, \sigma^{2'}) \stackrel{(16)}{\geq} U_2(\sigma^{1*}, \tilde{\sigma}^2) + p_2 \mathbb{E}_{\sigma^{1*}}[f_{\lambda'} \epsilon] \geq U_2(\sigma^{1*}, \tilde{\sigma}^2) + p_2 \sigma_{I'}^{1*} f_{\lambda'} \epsilon > U_2(\sigma^{1*}, \tilde{\sigma}^2).$$

This contradicts $(\sigma^{1*}, \tilde{\sigma}^2)$ being a NE. Therefore, we deduce that $\forall I \in \text{supp}(\tilde{\sigma}^2)$, $\forall f \in \text{supp}(\sigma^{1*})$, $\forall \lambda \in \Lambda \mid f_\lambda > 0$, $|I \cap \lambda| \leq 1$. Then, we obtain:

$$\forall f \in \text{supp}(\sigma^{1*}), \forall \lambda \in \Lambda \mid f_\lambda > 0, \pi_\lambda^0 - \sum_{(i, j) \in \lambda} \mu_{ij}^\dagger = \sum_{I \in \mathcal{I}} \tilde{\sigma}_I^2 \mathbb{1}_{\{I \cap \lambda \neq \emptyset\}} = \sum_{I \in \mathcal{I}} \tilde{\sigma}_I^2 |I \cap \lambda| \stackrel{(22)}{=} \sum_{(i, j) \in \lambda} \rho_{ij}^\dagger.$$

From (30), we deduce that $\forall f \in \text{supp}(\sigma^{1*})$, $\forall \lambda \in \Lambda$ such that $f_\lambda > 0$, we have $f_\lambda^\dagger > 0$ as well, i.e., $\lambda \in \text{supp}(f^\dagger)$. Therefore, $\mathcal{H}_1 \subseteq \text{supp}(f^\dagger)$, and we can conclude that $\mathcal{H}_1 = \text{supp}(f^\dagger)$. \square

Thus, from Theorem 3, we obtain a complete characterization of the $s - t$ paths that are taken by **P1**'s equilibrium strategy, and the edges that are interdicted by **P2**'s equilibrium strategy. By computing f^\dagger and $(\rho^\dagger, \mu^\dagger)$ a strictly complementary primal-dual pair of optimal solutions of (\mathcal{M}) , the set of critical $s - t$ paths of the network is given by $\text{supp}(f^\dagger)$, and the set of critical network edges is given by $\text{supp}(\rho^\dagger)$.

We note that in the setting that we consider, **P2** may need to interdict edges that are not part of any minimum-cut set, and can even belong to different cut sets; Figure 4 illustrates an example. In this example, the equilibrium interdiction strategy targets edges $(s, 1)$ and $(2, t)$ that do not belong to a same cut set. Thus, Theorem 3 generalizes the previously studied max-flow min-cut-based metrics of network criticality (see Assadi et al. [2], Dwivedi and Yu [11], Gueye et al. [13]).

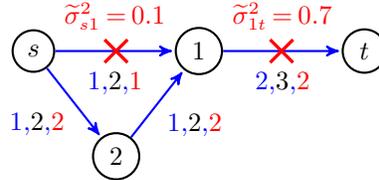


FIGURE 4. NE when $p_1 = 10$, $p_2 = 1$. $b_{ij} = 1$, $\forall (i, j) \in \mathcal{E}$. The label of each edge (i, j) represents $(f_{ij}^\dagger, c_{ij}, d_{ij})$. Edge $(s, 1)$ is interdicted by the equilibrium interdiction strategy $\tilde{\sigma}^2$, but is not part of the minimum-cut set.

Finally, we can derive additional equilibrium properties for the setting where each edge is potentially worth interdicting by **P2**, i.e., when $\frac{d_{ij}}{p_2} < c_{ij}$, $\forall (i, j) \in \mathcal{E}$. Recall that $\frac{d_{ij}}{p_2}$ is the threshold on the flow f_{ij} that determines **P2**'s incentive to interdict edge (i, j) or not. If edge (i, j) is such that $\frac{d_{ij}}{p_2} \geq c_{ij}$, then for any feasible flow $f \in \mathcal{F}$, $f_{ij} \leq \frac{d_{ij}}{p_2}$, and interdicting that edge does not increase **P2**'s payoff. On the other hand, if $\frac{d_{ij}}{p_2} < c_{ij}$, then **P2** has an incentive to interdict (i, j) if **P1** routes more than $\frac{d_{ij}}{p_2}$ units of flow through that edge. Next, we exploit the strategic equivalence to the zero-sum game $\tilde{\Gamma}$, as well as Theorems 1 and 2, to derive additional results for this special case.

PROPOSITION 6. *If $\forall (i, j) \in \mathcal{E}$, $\frac{d_{ij}}{p_2} < c_{ij}$, then any NE $\sigma^* = (\sigma^{1*}, \sigma^{2*}) \in \Sigma$ satisfies the following properties:*

- (i) *Both players' equilibrium payoffs are constant and given by: $U_1(\sigma^{1*}, \sigma^{2*}) = U_2(\sigma^{1*}, \sigma^{2*}) = 0$.*
- (ii) ***P1**'s routing strategy satisfies: $\mathbb{E}_{\sigma^{1*}}[p_1 F(f) - T(f)] = p_1 z_{(\mathcal{M})}^*$.*
- (iii) *The expected cost of **P2**'s interdiction strategy is given by: $\mathbb{E}_{\sigma^{2*}}[C(I)] = p_2 z_{(\mathcal{M})}^*$.*
- (iv) *The expected amount of interdicted flow is given by: $\mathbb{E}_{\sigma^*}[F(f) - F(f^I)] = z_{(\mathcal{M})}^*$.*

Proof of Proposition 6. In (32), we established that $\forall (\sigma^{1*}, \sigma^{2*}) \in \Sigma$, $\tilde{U}_1(\sigma^{1*}, \sigma^{2*}) = z_{(\mathcal{M})}^*$. Let f^* and (ρ^*, μ^*) denote optimal solutions of (\mathcal{M}_P) and (\mathcal{M}_D) , respectively. Since $\forall (i, j) \in \mathcal{E}$, $\frac{d_{ij}}{p_2} < c_{ij}$, then $\forall (i, j) \in \mathcal{E}$, $f_{ij}^* \leq \frac{d_{ij}}{p_2} < c_{ij}$. Therefore, from (20), we deduce that $\forall (i, j) \in \mathcal{E}$, $\mu_{ij}^* = 0$. Let $\tilde{\sigma}^2 \in \Delta(\mathcal{I})$ denote the interdiction strategy constructed from Algorithm 1 that satisfies (22) and

(23). We denote $f^0 \in \mathcal{F}$ the action of not sending any flow in the network, i.e., $f_\lambda^0 = 0, \forall \lambda \in \Lambda$, and we denote $f' := (1 + \epsilon)f^*$, with $\epsilon = \min\{p_2 \frac{c_{ij}}{d_{ij}} - 1, (i, j) \in \mathcal{E}\} > 0$. Then, $f' \in \mathcal{F}$.

Let us consider $\tilde{\sigma}^1 \in \Delta(\mathcal{F})$ defined by: $\tilde{\sigma}_{f'}^1 = \frac{1}{1+\epsilon}$, and $\tilde{\sigma}_{f^0}^1 = \frac{\epsilon}{1+\epsilon}$. Then, we show that $(\tilde{\sigma}^1, \tilde{\sigma}^2)$ is a NE. Regarding $\mathbf{P1}$'s payoff, since $\mu_{ij}^* = 0, \forall (i, j) \in \mathcal{E}$, we can rewrite (24) as follows:

$$\forall f \in \mathcal{F}, U_1(f, \tilde{\sigma}^2) \stackrel{(15)}{=} p_1 \sum_{\lambda \in \Lambda} \pi_\lambda^0 f_\lambda - p_1 \sum_{\lambda \in \Lambda} f_\lambda \sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 \stackrel{(23)}{\leq} p_1 \sum_{\lambda \in \Lambda} \pi_\lambda^0 f_\lambda - p_1 \sum_{\lambda \in \Lambda} f_\lambda \pi_\lambda^0 = 0.$$

Trivially, we obtain that $U_1(f^0, \tilde{\sigma}^2) = 0$. Furthermore, we know from (25) that $\forall \lambda \in \Lambda$ such that $f_\lambda^* > 0, \sum_{\{I \in \mathcal{I} \mid I \cap \lambda \neq \emptyset\}} \tilde{\sigma}_I^2 = \pi_\lambda^0$. Since $f_\lambda^* > 0 \iff f'_\lambda > 0$, we deduce that $U_1(f', \tilde{\sigma}^2) = 0$. Therefore $U_1(\tilde{\sigma}^1, \tilde{\sigma}^2) = 0$.

Regarding $\mathbf{P2}$'s payoff, we know that $\forall \sigma^2 \in \Delta(\mathcal{I}), U_2(\tilde{\sigma}^1, \sigma^2) = U_2(\mathbb{E}_{\tilde{\sigma}^1}[f], \sigma^2) = U_2(f', \sigma^2)$. Therefore, $U_2(\tilde{\sigma}^1, \tilde{\sigma}^2) = U_2(f', \tilde{\sigma}^2) \geq U_2(f', \sigma^2) = U_2(\tilde{\sigma}^1, \sigma^2), \forall \sigma^2 \in \Delta(\mathcal{I})$. Thus, $(\tilde{\sigma}^1, \tilde{\sigma}^2)$ is a NE.

We now consider $(\sigma^{1*}, \sigma^{2*}) \in \Sigma$. Then, we know that $(\sigma^{1*}, \tilde{\sigma}^2) \in \Sigma$ and $(\tilde{\sigma}^1, \sigma^{2*}) \in \Sigma$. Since $f^0 \in \text{supp}(\tilde{\sigma}^1)$, we obtain that $p_2 \tilde{U}_1(f^0, \sigma^{2*}) \stackrel{(17)}{=} \mathbb{E}_{\sigma^{2*}}[C(I)] \stackrel{(32)}{=} p_2 z_{(\mathcal{M})}^*$. Similarly, since $\emptyset \in \text{supp}(\tilde{\sigma}^2)$, then $p_1 \tilde{U}_1(\sigma^{1*}, \emptyset) \stackrel{(17)}{=} \mathbb{E}_{\sigma^{1*}}[p_1 F(f) - T(f)] \stackrel{(32)}{=} p_1 z_{(\mathcal{M})}^*$. We deduce the players' equilibrium payoffs:

$$\begin{aligned} U_1(\sigma^{1*}, \sigma^{2*}) &\stackrel{(17)}{=} p_1 \tilde{U}_1(\sigma^{1*}, \sigma^{2*}) - \frac{p_1}{p_2} \mathbb{E}_{\sigma^{2*}}[C(I)] \stackrel{(32)}{=} p_1 z_{(\mathcal{M})}^* - p_1 z_{(\mathcal{M})}^* = 0, \\ U_2(\sigma^{1*}, \sigma^{2*}) &\stackrel{(18)}{=} p_2 (-\tilde{U}_1(\sigma^{1*}, \sigma^{2*})) + p_2 \mathbb{E}_{\sigma^{2*}}[F(f) - \frac{1}{p_1} T(f)] \stackrel{(32)}{=} -p_2 z_{(\mathcal{M})}^* + p_2 z_{(\mathcal{M})}^* = 0. \end{aligned}$$

Finally, we characterize the expected amount of flow that is interdicted in any equilibrium: $\mathbb{E}_{\sigma^*}[F(f) - F(f^I)] = \frac{1}{p_2} U_2(\sigma^{1*}, \sigma^{2*}) + \frac{1}{p_2} \mathbb{E}_{\sigma^{2*}}[C(I)] = z_{(\mathcal{M})}^*$. \square

From (i) – (iv) in Proposition 6, we observe that some quantities (such as expected interdiction cost and expected amount of interdicted flow) in equilibrium can be computed in closed form using the parameters of the game and the optimal value of (\mathcal{M}) . Thus, our results in Section 4 provide a new approach to study the generic security game Γ , and derive equilibrium properties for settings involving heterogeneous cost parameters and general network topologies.

5. Concluding remarks. In this article, we studied an existence problem of probability distributions over partially ordered sets, and showed its implications to a class of security games on flow networks. In the existence problem, we considered a poset, where each element and each maximal chain is associated with a value. Under two practically relevant conditions on these values, we showed that there exists a probability distribution over the subsets of this poset, with the following properties: the probability that each element (resp. maximal chain) is contained in a subset (resp. intersects with a subset) is equal to (resp. as large as) the corresponding value. We provided a constructive proof of this result by designing a combinatorial algorithm that exploits structural properties of the problem.

By applying this existence result, we were able to study a generic formulation of network security game between a routing entity and an interdictor. To overcome the computational and analytical challenges of the formulation, we proposed a new approach for analyzing equilibria of the game. This approach relies on our existence result on posets, as well as optimal primal and dual solutions of a minimum cost circulation problem. Furthermore, we showed that a pair of optimal solutions of the circulation problem that satisfy strict complementary slackness provides a new characterization of the critical network components that are chosen in equilibrium by both players.

Appendix A: Remaining proofs.

Proof of Lemma 1. Let P be a finite nonempty poset, and let S be the set of minimal elements of P . If $|S| = 1$, then S is an antichain of P . Now, assume that $|S| \geq 2$, and consider $x \neq y \in S$. Since x (resp. y) is a minimal element of P , then $y \not\prec x$ (resp. $x \not\prec y$). Therefore, x and y are incomparable, and S is an antichain of P .

Now, consider a maximal chain $C \in \mathcal{C}$, and assume that C does not contain any minimal element of P . Let x be the minimal element of $(C, \preceq|_C)$. Since x is not a minimal element of P , there exists $y \in X \setminus C$ such that $y \prec x$. By transitivity of \preceq , we deduce that $y \prec x', \forall x' \in C$. Therefore, $C \cup \{y\}$ is a chain containing C , which contradicts the maximality of C . Thus, every maximal chain of P intersects with the set of minimal elements of P . \square

Proof of Lemma 2. Consider $X' \subseteq X$, and $\mathcal{C}' \subseteq \mathcal{C}$ that preserves the decomposition of maximal chains intersecting in X' . Let us show that $\preceq_{\mathcal{C}'}$ defined in Section 2.1 is a partial order on X' :

- Reflexivity: For every $x \in X'$, $x \preceq_{\mathcal{C}'} x$ by definition.
- Antisymmetry: Consider $(x, y) \in (X')^2$ such that $x \preceq_{\mathcal{C}'} y$ and $y \preceq_{\mathcal{C}'} x$. If $x \neq y$, then we would have $x \prec y$ and $y \prec x$, which contradicts \preceq being a partial order. Therefore, $x = y$.
- Transitivity: Consider $(x, y, z) \in (X')^3$, and assume that $x \preceq_{\mathcal{C}'} y$ and $y \preceq_{\mathcal{C}'} z$. If $x = y$ or $y = z$, then we trivially obtain that $x \preceq_{\mathcal{C}'} z$. Now, let us assume that $x \neq y$ and $y \neq z$. By definition of $\preceq_{\mathcal{C}'}$, $\exists C^1 \in \mathcal{C}' \mid (x, y) \in (C^1)^2$ and $x \prec y$. Similarly, $\exists C^2 \in \mathcal{C}' \mid (y, z) \in (C^2)^2$ and $y \prec z$. We can rewrite C^1 and C^2 as follows: $C^1 = \{x_0, \dots, x_l = x, x_{l+1}, \dots, x_{l+m} = y, x_{l+m+1}, \dots, x_{l+m+n}\}$ and $C^2 = \{y_0, \dots, y_q = y, y_{q+1}, \dots, y_{q+r} = z, y_{q+r+1}, \dots, y_{q+r+s}\}$. Now, consider the maximal chain $C_1^2 = \{x_0, \dots, x_l = x, x_{l+1}, \dots, x_{l+m} = y, y_{q+1}, \dots, y_{q+r} = z, y_{q+r+1}, \dots, y_{q+r+s}\}$, as illustrated in Figure 5.

Since C^1 and C^2 intersect in $y \in X'$, and \mathcal{C}' preserves the decomposition of maximal chains intersecting in X' , we deduce that $C_1^2 \in \mathcal{C}'$ as well. Furthermore, $(x, z) \in (C_1^2)^2$, and the transitivity of \preceq implies that $x \prec z$. Therefore, $x \preceq_{\mathcal{C}'} z$.

Thus, $\preceq_{\mathcal{C}'}$ is a partial order on X' , and $P' = (X', \preceq_{\mathcal{C}'})$ is a poset.

Let $C \subseteq X'$ be a maximal chain of P' of size at least two. Let us rewrite $C = \{x_1, \dots, x_n\}$ with $n \geq 2$, where $\forall k \in \llbracket 1, n-1 \rrbracket$, $x_k \prec_{\mathcal{C}'} x_{k+1}$. We show by induction on $k \in \llbracket 2, n \rrbracket$ that $\exists C' \in \mathcal{C}'$

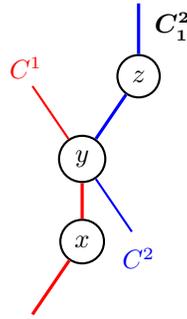


FIGURE 5. Illustration of the transitivity of $\preceq_{C'}$. C_1^2 is represented by the thick chain.

such that $\{x_1, \dots, x_k\} \subseteq C'$. If $k = 2$, then by definition, $\exists C' \in \mathcal{C}'$ such that $\{x_1, x_2\} \subseteq C'$. Now, assume that the result is true for $k \in \llbracket 2, n-1 \rrbracket$. Consider $C^1 \in \mathcal{C}'$ such that $\{x_1, \dots, x_k\} \subseteq C^1$. Since $x_k \prec_{C'} x_{k+1}$, then $\exists C^2 \subseteq \mathcal{C}'$ such that $(x_k, x_{k+1}) \in (C^2)^2$. Analogously, we can show that C_1^2 (illustrated in Figure 5), which is in \mathcal{C}' , contains $\{x_1, \dots, x_{k+1}\}$. Therefore, by induction, we obtain that $\exists C' \in \mathcal{C}'$ such that $C = \{x_1, \dots, x_n\} \subseteq C'$. Since $C \subseteq X'$, then we have $C = C \cap X' \subseteq C' \cap X'$.

Now, assume that $\exists x' \in C' \cap X' \setminus C$. For every $k \in \llbracket 1, n \rrbracket$, $(x_k, x') \in (C')^2$. Therefore, x' is comparable in P' with every element of the chain C . This implies that $C \cup \{x'\}$ is a chain in P' , which contradicts the maximality of C in P' . Therefore, $C = C' \cap X'$. \square

Proof of Lemma 4. Let us show that $\preceq_{\mathcal{G}}$ is a partial order on \mathcal{E} .

- Reflexivity: For every $u \in \mathcal{E}$, $u \preceq_{\mathcal{G}} u$ by definition.
- Antisymmetry: Consider $(u, v) \in \mathcal{E}^2$ such that $u \preceq_{\mathcal{G}} v$ and $v \preceq_{\mathcal{G}} u$. If $u \neq v$, then there exists λ^1 and λ^2 in Λ such that λ^1 traverses u and v in this order, and λ^2 traverses v and u in this order. They can be written as follows: $\lambda^1 = \{u_1, \dots, u_n, u, u_{n+1}, \dots, u_{n+m}, v, u_{n+m+1}, \dots, u_{n+m+p}\}$ and $\lambda^2 = \{v_1, \dots, v_q, v, v_{q+1}, \dots, v_{q+r}, u, v_{q+r+1}, \dots, v_{q+r+s}\}$. Then, $\{u, u_{n+1}, \dots, u_{n+m}, v, v_{q+1}, \dots, v_{q+r}\}$ is a cycle (see Figure 6), which contradicts \mathcal{G} being acyclic. Therefore $u = v$.

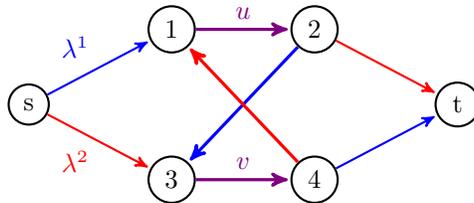


FIGURE 6. Proof of antisymmetry of $\preceq_{\mathcal{G}}$ by contradiction: if $u \preceq_{\mathcal{G}} v$, $v \preceq_{\mathcal{G}} u$, and $u \neq v$, then one can see that u and v necessarily belong to a cycle (shown in thick edges), although \mathcal{G} is acyclic.

- Transitivity: Consider $(u, v, w) \in \mathcal{E}^3$, and assume that $u \preceq_{\mathcal{G}} v$ and $v \preceq_{\mathcal{G}} w$. If $u = v$ or $v = w$, then we trivially obtain that $u \preceq_{\mathcal{G}} w$. Now, let us assume that $u \neq v$ and $v \neq w$. Then, there exists λ^1 and λ^2 in Λ such that λ^1 traverses u and v in this order, and λ^2 traverses v and w in this order. They can be written as $\lambda^1 = \{u_1, \dots, u_n, u, u_{n+1}, \dots, u_{n+m}, v, u_{n+m+1}, \dots, u_{n+m+p}\}$

and $\lambda^2 = \{v_1, \dots, v_q, v, v_{q+1}, \dots, v_{q+r}, w, v_{q+r+1}, \dots, v_{q+r+s}\}$. Then, $\lambda_1^2 = \{u_1, \dots, u_n, u, u_{n+1}, \dots, u_{n+m}, v, v_{q+1}, \dots, v_{q+r}, w, v_{q+r+1}, \dots, v_{q+r+s}\}$ is an $s-t$ path (see Figure 7), and traverses u and w in this order. Therefore, $u \preceq_{\mathcal{G}} w$.

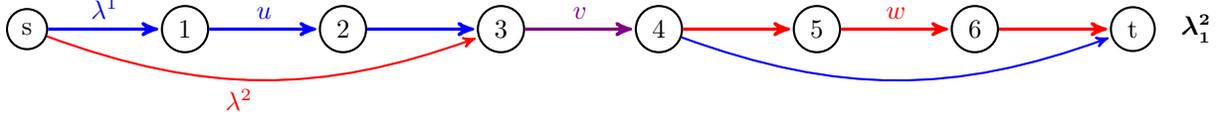


FIGURE 7. Proof of transitivity of $\preceq_{\mathcal{G}}$: if $u \preceq_{\mathcal{G}} v$, and $v \preceq_{\mathcal{G}} w$, then one can construct an $s-t$ path λ_1^2 (in thick line) that traverses u and w in this order.

In conclusion, $P = (\mathcal{E}, \preceq_{\mathcal{G}})$ is a poset.

Next, we prove that the set of maximal chains \mathcal{C} of P is Λ . First, we show that $\mathcal{C} \subseteq \Lambda$. Consider a maximal chain $C \in \mathcal{C}$ of P . If $C = \{u\}$ is of size 1, then necessarily $u = (s, t)$, because \mathcal{G} is connected. Therefore, $C = \{u\}$ is an $s-t$ path. Now, assume that $|C| \geq 2$. Let us write $C = \{u_1, \dots, u_n\}$, where $\forall k \in \llbracket 1, n-1 \rrbracket$, $u_k \prec_{\mathcal{G}} u_{k+1}$. Since $u_1 \prec_{\mathcal{G}} u_2$ and $u_2 \prec_{\mathcal{G}} u_3$, then there exist λ^1 and λ^2 in Λ such that λ^1 traverses u_1 and u_2 in this order, and λ^2 traverses u_2 and u_3 in this order. When showing the transitivity of $\preceq_{\mathcal{G}}$ in the proof of Lemma 4, we deduced that there exists $\lambda_1^2 \in \Lambda$ that traverses u_1 , u_2 , and u_3 in this order. If we repeat this process, we obtain an $s-t$ path $\lambda \in \Lambda$ such that $C \subseteq \lambda$.

Now, assume that $\exists u \in \lambda \setminus C$. Since $C \subseteq \lambda$, and $u \in \lambda$, then we deduce (by definition of $\preceq_{\mathcal{G}}$) that u is comparable with every element of C . Therefore $C \cup \{u\}$ is a chain in P , which contradicts the maximality of C . Therefore $C = \lambda$ and $\mathcal{C} \subseteq \Lambda$.

To show the reversed inclusion, consider an $s-t$ path $\lambda \in \Lambda$. From the definition of $\preceq_{\mathcal{G}}$, λ is a chain in P . Let us assume that λ is not a maximal chain of P , i.e., there exists a maximal chain $C \in \mathcal{C}$ such that $\lambda \subsetneq C$. Let us write $\lambda = \{u_1, \dots, u_n\}$ where $\forall k \in \llbracket 1, n-1 \rrbracket$, $u_k \prec_{\mathcal{G}} u_{k+1}$, and let $v \in C \setminus \lambda$. Since $\lambda \subset C$ and $v \in C$, then v is comparable with every element of λ . By transitivity of $\preceq_{\mathcal{G}}$, if $\exists k \in \llbracket 1, n \rrbracket$ such that $v \prec_{\mathcal{G}} u_k$, then $\forall l \in \llbracket k, n \rrbracket$, $v \prec_{\mathcal{G}} u_l$. Similarly, if $\exists k \in \llbracket 1, n \rrbracket$ such that $u_k \prec_{\mathcal{G}} v$, then $\forall l \in \llbracket 1, k \rrbracket$, $u_l \prec_{\mathcal{G}} v$. Therefore, three cases can arise:

- $v \prec_{\mathcal{G}} u_1$. In this case, $\exists \lambda^1 = \{w_1, \dots, w_n, v, w_{n+1}, \dots, w_{n+m}, u_1, w_{n+m+1}, \dots, w_{n+m+p}\} \in \Lambda$. However, since λ is an $s-t$ path, then the start node of u_1 is s , which is also the start node of w_1 . Therefore, $\{w_1, \dots, w_n, v, w_{n+1}, \dots, w_{n+m}\}$ is a cycle, which is a contradiction.

- $u_n \prec_{\mathcal{G}} v$. In this case, $\exists \lambda^1 = \{v_1, \dots, v_q, u_n, v_{q+1}, \dots, v_{q+r}, v, v_{q+r+1}, \dots, v_{q+r+s}\} \in \Lambda$. Analogously, we deduce that the end nodes of u_n and v_{q+r+s} are the destination node t , which implies that $\{v_{q+1}, \dots, v_{q+r}, v, v_{q+r+1}, \dots, v_{q+r+s}\}$ is a cycle in the acyclic graph \mathcal{G} .

- $u_k \prec_{\mathcal{G}} v \prec_{\mathcal{G}} u_{k+1}$ for $k \in \llbracket 1, n-1 \rrbracket$. In this case, there exist two $s-t$ paths $\lambda^1 = \{v_1, \dots, v_q, u_k, v_{q+1}, \dots, v_{q+r}, v, v_{q+r+1}, \dots, v_{q+r+s}\} \in \Lambda$ and $\lambda^2 = \{w_1, \dots, w_n, v, w_{n+1}, \dots, w_{n+m}, u_{k+1}, w_{n+m+1}, \dots, w_{n+m+p}\} \in \Lambda$. One can verify that

$\{v_{q+1}, \dots, v_{q+r}, v, w_{n+1}, \dots, w_{n+m}\}$ is a cycle in \mathcal{G} since the start node of v_{q+1} is the end node of w_{n+m} . This is in fact the end node of u_k , which is also the start node of u_{k+1} since λ is a path. This contradicts \mathcal{G} being acyclic.

Thus, $\lambda = C$, and $\Lambda \subseteq C$. In conclusion, $C = \Lambda$. \square

Appendix B: Illustration of Algorithm 1. Consider the poset P represented by the Hasse diagram given in Figure 8.

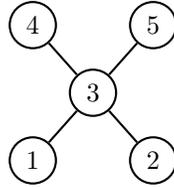


FIGURE 8. Hasse diagram of a poset P .

In this poset P , the set of maximal chains is given by $\mathcal{C} = \{\{1, 3, 4\}, \{2, 3, 5\}, \{1, 3, 5\}, \{2, 3, 4\}\}$. We assume that the values assigned to each maximal chain are $\pi_{134} = \pi_{135} = 0.8$ and $\pi_{234} = \pi_{235} = 0.6$, and the values assigned to each element are $\rho_1 = 0.4$, $\rho_2 = 0.3$, $\rho_3 = 0.5$, $\rho_4 = 0.5$, $\rho_5 = 0.7$.

First, we can see that $\forall C \in \mathcal{C}$, $\sum_{x \in C} \rho_x \geq \pi_C$, and $\pi_{134} + \pi_{235} = \pi_{135} + \pi_{234}$. Therefore, conditions (2) and (3) are satisfied, and we can run Algorithm 1 to optimally solve (Q) (and construct a feasible solution of (D)). Figure 9a (resp. Figure 9b), illustrates each iteration of the algorithm using the poset P (resp. the posets P^k , for $k \in \llbracket 1, n^* \rrbracket$).

- **$k = 1$:** $X^1 = X = \llbracket 1, 5 \rrbracket$, $\mathcal{C}^1 = \mathcal{C}$, $\rho_x^1 = \rho_x$, $\forall x \in X$. Note that $\delta_{134} = 0.6$, $\delta_{235} = 0.9$, $\delta_{135} = 0.8$, and $\delta_{234} = 0.7$. Since $\forall C \in \mathcal{C}$, $\delta_C^1 = \delta_C > 0$, then $\bar{\mathcal{C}}^1 = \emptyset$, and $\hat{\mathcal{C}}^1 = \mathcal{C}$. Therefore, each pair of elements in $P^1 = (X^1, \preceq_{\bar{\mathcal{C}}^1})$ is incomparable, and $S^1 = \{1, 2, 3, 4, 5\}$. Then one can check that $\min_{x \in S^1} \rho_x^1 = 0.3$ and $\min_{\{C \in \hat{\mathcal{C}}^1 \mid |S^1 \cap C| \geq 2\}} \frac{\delta_C^1}{|S^1 \cap C| - 1} = 0.3$. Therefore, $\sigma_{S^1} = w^1 = 0.3 = \rho_2^1 = \frac{\delta_{134}^1}{|S^1 \cap \{1, 3, 4\}| - 1}$.

Next, the values are updated as follows: $\rho_1^2 = 0.1$, $\rho_2^2 = 0$, $\rho_3^2 = 0.2$, $\rho_4^2 = 0.2$, $\rho_5^2 = 0.4$, and $\delta_{134}^2 = 0$, $\delta_{235}^2 = 0.3$, $\delta_{135}^2 = 0.2$, $\delta_{234}^2 = 0.1$. Since each maximal chain's minimal element is in S^1 , then $\mathcal{C}^2 = \mathcal{C}$. We conclude the first iteration of the algorithm by letting $X^2 = \{1, 3, 4, 5\}$, $\bar{\mathcal{C}}^2 = \{\{1, 3, 4\}\}$, and $\hat{\mathcal{C}}^2 = \{\{2, 3, 5\}, \{1, 3, 5\}, \{2, 3, 4\}\}$.

- **$k = 2$:** The set of minimal elements of the new poset $P^2 = (X^2, \preceq_{\bar{\mathcal{C}}^2})$ is given by $S^2 = \{1, 5\}$ (see Figure 9b). Furthermore, $\min_{x \in S^2} \rho_x^2 = 0.1$ and $\min_{\{C \in \hat{\mathcal{C}}^2 \mid |S^2 \cap C| \geq 2\}} \frac{\delta_C^2}{|S^2 \cap C| - 1} = 0.2$, which imply that $\sigma_{S^2} = w^2 = 0.1 = \rho_1^2$. Then, the values are updated as follows: $\rho_1^3 = 0$, $\rho_2^3 = 0$, $\rho_3^3 = 0.2$, $\rho_4^3 = 0.2$, $\rho_5^3 = 0.3$, and $\delta_{134}^3 = 0$, $\delta_{235}^3 = 0.3$, $\delta_{135}^3 = 0.1$, $\delta_{234}^3 = 0.1$.

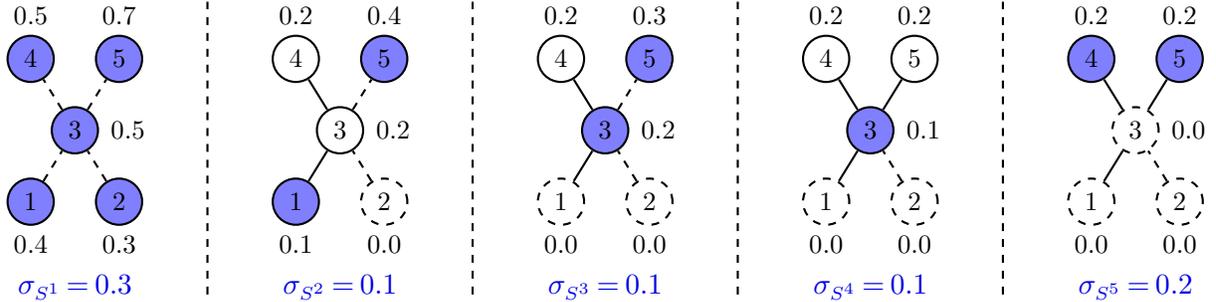
Now, one can see that the minimal element of $\{2, 3, 5\} \cap X^2$ and $\{2, 3, 4\} \cap X^2$ in P is 3, which does not belong to S^2 . Therefore, $\mathcal{C}^3 = \{\{1, 3, 4\}, \{1, 3, 5\}\}$. The new sets are then given by $X^3 = \{3, 4, 5\}$, $\bar{\mathcal{C}}^3 = \{\{1, 3, 4\}\}$, and $\hat{\mathcal{C}}^3 = \{\{1, 3, 5\}\}$.

• **$k = 3$** : The set of minimal elements of $P^3 = (X^3, \preceq_{\overline{\mathcal{C}}^3})$ is given by $S^3 = \{3, 5\}$ (see Figure 9b). Since $\min_{x \in S^3} \rho_x^3 = 0.2$, and $\min_{\{C \in \overline{\mathcal{C}}^3 \mid |S^3 \cap C| \geq 2\}} \frac{\delta_C^3}{|S^3 \cap C| - 1} = 0.1$, then $\sigma_{S^3} = w^3 = 0.1 = \frac{\delta_{135}^3}{|S^3 \cap \{1, 3, 5\}| - 1}$. The values are updated as follows: $\rho_1^4 = 0$, $\rho_2^4 = 0$, $\rho_3^4 = 0.1$, $\rho_4^4 = 0.2$, $\rho_5^4 = 0.2$, and $\delta_{134}^4 = 0$, $\delta_{235}^4 = 0.2$, $\delta_{135}^4 = 0$, $\delta_{234}^4 = 0.1$. Then, $X^4 = \{3, 4, 5\}$, $\mathcal{C}^4 = \mathcal{C}^3$, $\overline{\mathcal{C}}^4 = \{\{1, 3, 4\}, \{1, 3, 5\}\}$, and $\widehat{\mathcal{C}}^4 = \emptyset$.

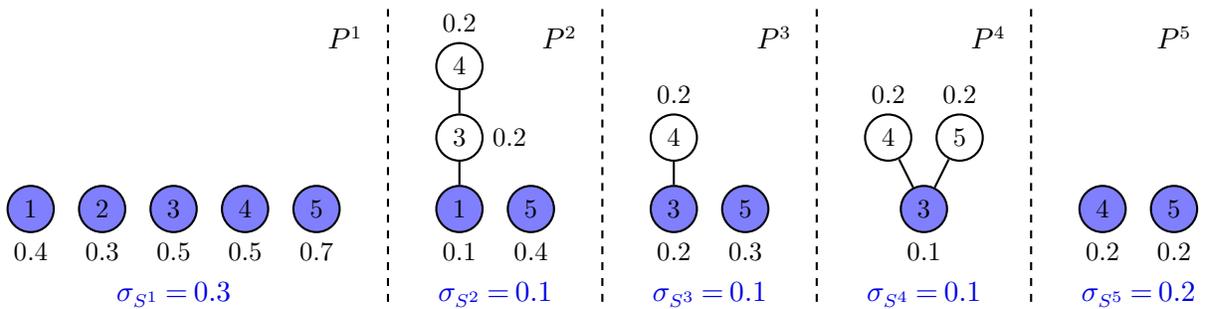
• **$k = 4$** : The set of minimal elements of $P^4 = (X^4, \preceq_{\overline{\mathcal{C}}^4})$ is $S^4 = \{3\}$ (see Figure 9b). Then, $\sigma_{S^4} = w^4 = \min_{x \in S^4} \rho_x^4 = \rho_3^4 = 0.1$, and the new values are: $\rho_1^5 = 0$, $\rho_2^5 = 0$, $\rho_3^5 = 0$, $\rho_4^5 = 0.2$, $\rho_5^5 = 0.2$, and $\delta_C^5 = \delta_C^4$, $\forall C \in \mathcal{C}$. The new sets are $X^5 = \{4, 5\}$, $\mathcal{C}^5 = \mathcal{C}^4$, $\overline{\mathcal{C}}^5 = \{\{1, 3, 4\}, \{1, 3, 5\}\}$, and $\widehat{\mathcal{C}}^5 = \emptyset$.

• **$k = 5$** : The set of minimal elements of $P^5 = (X^5, \preceq_{\overline{\mathcal{C}}^5})$ is given by $S^5 = \{4, 5\}$ (Figure 9b), and the weight associated with it is $\sigma_{S^5} = w^5 = \rho_4^5 = \rho_5^5 = 0.2$. The updated values are given by: $\rho_x^6 = 0$, $\forall x \in X$, and $\delta_C^6 = \delta_C^5$, $\forall C \in \mathcal{C}$.

Since $X^6 = \emptyset$, the algorithm terminates, and outputs σ . One can check that σ satisfies constraints (5) and (6), and has a total weight $\sum_{S \in \mathcal{P}} \sigma_S$ of $0.8 = \max\{\max\{\rho_x, x \in X\}, \max\{\pi_C, C \in \mathcal{C}\}\}$. Therefore, from Theorem 2, σ is an optimal solution of (Q). Since $0.8 \leq 1$, then $\widehat{\sigma} \in \mathbb{R}_+^{|\mathcal{P}|}$ given by $\widehat{\sigma}_S = \sigma_S$, $\forall S \in \mathcal{P} \setminus \emptyset$, and $\widehat{\sigma}_\emptyset = 0.2$, is a feasible solution of (D).



(a) Poset P at the beginning of each iteration of the algorithm. The solid nodes are in X^k , the dashed nodes are in $X \setminus X^k$, and the blue nodes are in S^k . An edge is solid if there exists a maximal chain in $\overline{\mathcal{C}}^k$ that contains both end nodes of the edge. The values ρ_x^k are given next to each element.



(b) P^k , for $k \in [1, 5]$. The values ρ_x^k are given next to each element. S^k is given by the blue nodes.

FIGURE 9. Illustration of Algorithm 1 for the poset P given in Figure 8.

Appendix C: Minimum cost circulation problem. Primal and dual linear formulations of (\mathcal{M}) of polynomial size are given as follows:

$$\begin{aligned}
(\mathcal{M}'_P) \quad & \text{maximize} \quad \sum_{\{i \in \mathcal{V} \mid (i,t) \in \mathcal{E}\}} f_{it} - \sum_{(i,j) \in \mathcal{E}} \frac{b_{ij}}{p_1} f_{ij} \\
& \text{subject to} \quad \sum_{\{j \in \mathcal{V} \mid (j,i) \in \mathcal{E}\}} f_{ji} = \sum_{\{j \in \mathcal{V} \mid (i,j) \in \mathcal{E}\}} f_{ij}, \quad \forall i \in \mathcal{V} \setminus \{s, t\} \\
& \quad 0 \leq f_{ij} \leq c_{ij}, \quad \forall (i, j) \in \mathcal{E} \\
& \quad 0 \leq f_{ij} \leq \frac{d_{ij}}{p_2}, \quad \forall (i, j) \in \mathcal{E}.
\end{aligned}$$

$$\begin{aligned}
(\mathcal{M}'_D) \quad & \text{minimize} \quad \sum_{(i,j) \in \mathcal{E}} c_{ij} \rho_{ij} + \frac{d_{ij}}{p_2} \mu_{ij} \\
& \text{subject to} \quad y_i - y_j + \rho_{ij} + \mu_{ij} \geq -\frac{b_{ij}}{p_1}, \quad \forall (i, j) \in \mathcal{E} \mid i \neq s \text{ and } j \neq t \\
& \quad -y_j + \rho_{sj} + \mu_{sj} \geq -\frac{b_{sj}}{p_1}, \quad \forall j \in \mathcal{V} \mid (s, j) \in \mathcal{E} \\
& \quad y_i + \rho_{it} + \mu_{it} \geq 1 - \frac{b_{it}}{p_1}, \quad \forall i \in \mathcal{V} \mid (i, t) \in \mathcal{E} \\
& \quad \rho_{ij} \geq 0, \quad \forall (i, j) \in \mathcal{E} \\
& \quad \mu_{ij} \geq 0, \quad \forall (i, j) \in \mathcal{E}.
\end{aligned}$$

Let $z_{(\mathcal{M}')}^*$ denote the optimal value of (\mathcal{M}'_P) and (\mathcal{M}'_D) . We show the following result:

LEMMA 5. *Any $s-t$ path decomposition of any optimal solution f' of (\mathcal{M}'_P) is an optimal solution of (\mathcal{M}_P) . Furthermore, given any optimal solution (ρ', μ', y') of (\mathcal{M}'_D) , (ρ', μ') is an optimal solution of (\mathcal{M}_D) .*

Proof of Lemma 5. Let $f^* \in \mathbb{R}_+^{|\Lambda|}$ be an optimal solution of (\mathcal{M}_P) . Then, $f' \in \mathbb{R}_+^{|\mathcal{E}|}$ defined by $f'_{ij} = \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f^*_\lambda$ is a feasible solution of (\mathcal{M}'_P) . Therefore, $z_{(\mathcal{M}')}^* \geq \sum_{\{i \in \mathcal{V} \mid (i,t) \in \mathcal{E}\}} f'_{it} - \sum_{(i,j) \in \mathcal{E}} \frac{b_{ij}}{p_1} f'_{ij} = \sum_{\lambda \in \Lambda} \pi_\lambda^0 f^*_\lambda = z_{(\mathcal{M})}^*$. Now, let $f' \in \mathbb{R}_+^{|\mathcal{E}|}$ be an optimal solution of (\mathcal{M}'_P) . From the flow decomposition theorem, there exists a vector $f^* \in \mathbb{R}_+^{|\Lambda|}$ such that $\forall (i, j) \in \mathcal{E}$, $f'_{ij} = \sum_{\{\lambda \in \Lambda \mid (i,j) \in \lambda\}} f^*_\lambda$. Since f^* is a feasible solution of (\mathcal{M}_P) , we deduce that $z_{(\mathcal{M})}^* \geq z_{(\mathcal{M}')}^*$. In conclusion, $z_{(\mathcal{M})}^* = z_{(\mathcal{M}')}^*$, and an optimal solution of (\mathcal{M}_P) can be obtained by decomposing an optimal solution of (\mathcal{M}'_P) into $s-t$ paths.

Now, consider an optimal solution (ρ', μ', y') of (\mathcal{M}'_D) . Then, one can verify that for every $s-t$ path $\lambda \in \Lambda$, $\sum_{(i,j) \in \lambda} (\rho'_{ij} + \mu'_{ij}) \geq 1 - \frac{1}{p_1} \sum_{(i,j) \in \lambda} b_{ij} = \pi_\lambda^0$ (the y' cancel in a telescopic manner along each $s-t$ path). Therefore, (ρ', μ') is a feasible solution of (\mathcal{M}_D) . Since $z_{(\mathcal{M}')}^* = z_{(\mathcal{M})}^*$, we can conclude that (ρ', μ') is an optimal solution of (\mathcal{M}_D) . \square

Acknowledgments This work was supported in part by the Singapore National Research Foundation through the Singapore MIT Alliance for Research and Technology (SMART), FORCES (Foundations Of Resilient CybEr-Physical Systems), which receives support from the National Science Foundation (NSF award numbers CNS-1238959, CNS-1238962, CNS-1239054, CNS-1239166), NSF CAREER award CNS-1453126, and the AFRL LABLET - Science of Secure and Resilient Cyber-Physical Systems (Contract ID: FA8750-14-2-0180, SUB 2784-018400).

References

- [1] Adler, Ilan, Renato D. C. Monteiro. 1992. A geometric view of parametric linear programming. *Algorithmica* **8**(1) 161–176.
- [2] Assadi, Sepehr, Ehsan Emamjomeh-Zadeh, Ashkan Norouzi-Fard, Sadra Yazdanbod, Hamid Zarrabi-Zadeh. 2014. The minimum vulnerability problem. *Algorithmica* **70**(4) 718–731.
- [3] Assimakopoulos, Nikitas. 1987. A network interdiction model for hospital infection control. *Computers in Biology and Medicine* **17**(6) 413 – 422.
- [4] Avenhaus, Rudolf, Morton John Canty. 2009. Inspection games. Robert A. Meyers, ed., *Encyclopedia of Complexity and Systems Science*. Springer, 4855–4868.
- [5] Balinski, M., A. Tucker. 1969. Duality theory of linear programs: A constructive approach with applications. *SIAM Review* **11**(3) 347–377.
- [6] Ball, Michael O., Bruce L. Golden, Rakesh V. Vohra. 1989. Finding the most vital arcs in a network. *Oper. Res. Lett.* **8**(2) 73–76.
- [7] Baykal-Gürsoy, Melike, Zhe Duan, H. Vincent Poor, Andrey Garnaev. 2014. Infrastructure security games. *European Journal of Operational Research* **239**(2) 469–478.
- [8] Bertsimas, Dimitris, Ebrahim Nasrabadi, James B. Orlin. 2016. On the power of randomization in network interdiction. *Operations Research Letters* **44**(1) 114 – 120.
- [9] Bertsimas, Dimitris, Ebrahim Nasrabadi, Sebastian Stiller. 2013. Robust and adaptive network flows. *Operations Research* **61**(5) 1218–1242.
- [10] Cormican, Kelly J., David P. Morton, R. Kevin Wood. 1998. Stochastic Network Interdiction. *Operations Research* **46**(2).
- [11] Dwivedi, A., X. Yu. 2013. A maximum-flow-based complex network approach for power system vulnerability analysis. *IEEE Transactions on Industrial Informatics* **9**(1) 81–88.
- [12] Goldman, A. J., A. W. Tucker. 1957. Theory of linear programming. H. W. Kuhn, A. W. Tucker, eds., *Linear Inequalities and Related Systems, Annals of Mathematics Studies 35*, vol. 38. Princeton University Press, 53–98.
- [13] Gueye, A., V. Marbukh, J. C. Walrand. 2012. Towards a metric for communication network vulnerability to attacks: A game theoretic approach. Vikram Krishnamurthy, Qing Zhao, Minyi Huang, Yonggang Wen, eds., *Game Theory for Networks*. Springer Berlin Heidelberg, Berlin, Heidelberg, 259–274.

- [14] Gueye, Assane, Vladimir Marbukh. 2012. A game-theoretic framework for network security vulnerability assessment and mitigation. Jens Grossklags, Jean Walrand, eds., *Decision and Game Theory for Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 186–200.
- [15] Guo, Q., B. An, Y. Zick, C. Miao. 2016. Optimal interdiction of illegal network flow. *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*. IJCAI'16, 2507–2513.
- [16] Hoàng, Chính T. 1994. Efficient algorithms for minimum weighted colouring of some classes of perfect graphs. *Discrete Applied Mathematics* **55**(2) 133 – 143.
- [17] Jansen, B., C. Roos, T. Terlaky. 1994. The theory of linear programming: skew symmetric self-dual problems and the central path. *Optimization* **29**(3) 225–233.
- [18] Karmarkar, N. 1984. A new polynomial-time algorithm for linear programming. *Combinatorica* **4**(4) 373–395.
- [19] Lipton, R. J., E. Markakis, A. Mehta. 2003. Playing large games using simple strategies. *Proceedings of the 4th ACM Conference on Electronic Commerce*. EC '03, ACM, New York, NY, 36–41.
- [20] McMahan, H. Brendan, Georey J Gordon, Avrim Blum. 2003. Planning in the presence of cost functions controlled by an adversary. *In ICML*. 536–543.
- [21] McMasters, Alan W., Thomas M. Mustin. 1970. Optimal interdiction of a supply network. *Naval Research Logistics Quarterly* **17**(3) 261–268.
- [22] Neumayer, S., G. Zussman, R. Cohen, E. Modiano. 2008. Assessing the impact of geographically correlated network failures. *Military Communications Conference, 2008. MILCOM 2008. IEEE*. 1–6.
- [23] Orlin, James B., Serge A. Plotkin, Éva Tardos. 1993. Polynomial dual network simplex algorithms. *Mathematical Programming* **60**(1) 255–276.
- [24] Ratliff, H. Donald, G. Thomas Sicilia, S. H. Lubore. 1975. Finding the n most vital links in flow networks. *Management Science* **21**(5) 531–539.
- [25] Sullivan, Kelly M., J. Cole Smith. 2014. Exact algorithms for solving a euclidean maximum flow network interdiction problem. *Networks* **64**(2) 109–124.
- [26] Szeto, W.Y. 2013. Routing and scheduling hazardous material shipments: Nash game approach. *Transportmetrica B: Transport Dynamics* **1**(3) 237–260.
- [27] Washburn, Alan, Kevin Wood. 1995. Two-person zero-sum games for network interdiction. *Operations Research* **43**(2) 243 – 251.
- [28] Wollmer, R. 1964. Removing Arcs from a Network. *Operations Research* **12**(6) 934–940.
- [29] Wood, R. K. 1993. Deterministic network interdiction. *Mathematical and Computer Modelling* **17**(2) 1 – 18.