NYILATKOZAT

Név: KÓSA BENDEGÚZ

ELTE Természettudományi Kar, szak: MATEMATIKA

NEPTUN azonosító: FCUTGK

Szakdolgozat címe: HÁLÓZATOK MEGBÍZHATÓSÁGÁNAK VIZSGÁLATA JÁTÉKELMÉLETI ESZKÖZÖKKEL

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2020. dec. 20

a hallgató aláírása

Measuring Network Reliability via Game Theory

ELTE Faculty of Sciences

Bendeguz Kosa

20 December 2020

Acknowledgments

First of all, I would like to thank David Szeszler for helping me start the journey of writing this thesis, and Janos Barath for helping me finish it. Many thanks go to Ferenc Peto and Andras Kiss for giving me support to take time off work to spend on finalizing the thesis. Last but not least I would like to thank my family who had my back during the whole time, and without whose support I wouldn't have been able to complete this work.

Introduction

One of the most prominent tendencies of the 21st century has been the integration of systems and data. With the rise of smart-phones and laptops and the spread of the Internet information has never been easier to reach.

With this great opportunity comes a great threat; news about hacking and data theft are sadly an every day occurrence. In this regard, the importance of network security cannot be overstated, both on a personal and on a business level.

The practical matters of data encryption and decryption are doubtless intriguing topics. However, we will look at things from a broader perspective. We will model networks with graphs to search for weak links in the system. We can model a communication network just as well as an electrical grid or a transit system, and will offer security metrics for all of these cases.

Using game theoretical tools, we will define a hypothetical two-player game between an "Attacker" and a "Defender" (the nature of the attack and defense will always depend on the property of the graph we will be trying to measure). The security metric will be determined by the Nash-equilibria of the aforementioned games. The notion behind this is that the larger a "winning" an Attacker can guarantee himself, the weaker we perceive the graph (and the network it symbolizes).

After a thorough overview of the game theoretical results on which we base our further work, in the following two chapters we will take a look at the different problems and the metrics we can assign to them, and we will briefly explore the computability of the defined metrics.

Chapter 1

Preliminaries in Graph Theory

Graph Theory is without a question one of the newer sub-branches of mathematics. Contrary to the fields of algebra and geometry which find their roots in ancient and medieval times, the first problems of Graph Theory arose during the 18th and 19th centuries. This relative newness in no way diminishes the importance of Graph Theory, many new scientific fields (including a few non-mathematical ones) such as Computer Science and Sociology are unimaginable without its results.

1.1 Basic definitions

Definition (Graphs)**.** *An (undirected)* ***graph*** *G is defined by a pair, $G = (V, E)$. The (non-empty and finite) set $V(G)$ defines the set of the so-called nodes or vertices, while the family of pairs $E(G)$ defines the edges of the graph. Each element of $E(G)$ is an unordered pair of two elements of $V(G)$.*

Note that we didn't specify that the elements of $E(G)$ should contain two *distinct* nodes, edges such as $e = \{v, v\}$ are called loops. It's also notable that $E(G)$ may contain a pair of nodes more than once, these are called *multiple edges*.

A graph with neither loops nor multiple edges is called a simple graph.

Remark. *An edge $e = \{v, w\}$ (or very often abbreviated as vw) connects the vertices u and v.*

Two edges (for example $e = \{v, w\}, f = \{v, z\}$) are adjacent *if they are incident with a common vertex (in this case v).*

A connected, simple graph with n vertices and $n - 1$ edges is a **tree**.

Definition. *A degree of a v vertex (denoted by $\deg(v)$ or $d(v)$) is the number of edges that are incident to v. Furthermore $\Delta(G)$ denotes the maximum degree, whereas $\delta(G)$ denotes the minimum degree of the vertices in the graph G. If $\forall v \in V(G) \quad d(v) = k$, then we call the graph k-regular.*

Definition. *A* ***path*** *P in a graph $G = (V, E)$ is a sequence*

$$P = (v_0, e_1, v_1, e_2, v_2, \dots, e_k, v_k),$$

where $k \geq 0$, $v_0, \dots, v_k \in V(G)$ are distinct vertices, and $e_1, \dots, e_k \in E(G)$ are edges where the edge e_i connects the vertices v_{i-1} and v_i.

Definition. *In a directed graph or **digraph** $D = (V, A)$, the elements of A are ordered pairs. The directed edge or* arc *(v, w) is said to run from v to w.*

We will furthermore use the following notations:

- $\delta(v) :=$ set of arcs leaving $v \in V$
- $\delta(U) := \{(u, v) \in A : u \in U, v \notin U\}$
- $\rho(v) :=$ set of arcs entering $v \in V$
- $\rho(U) := \{((u, v) \in A : u \notin U, v \in U\}$

1.2 Networks and flows

Definition (Cut)**.** *In an undirected graph G, a subset $C \subseteq E(G)$ is called a cut, if there exists a subset $U \subset V(G)$, where the edges in C are exactly the edges connecting U and $V \backslash U$.*

The set $B \subseteq A$ is a directed cut in $D = (V, A)$, if there exists $U \subset V$, where B contains exactly the arcs leaving U.

In both cases, if $s \in U$ and $t \notin U$, then we talk about $s - t$ cuts.

A classic result regarding the $s - t$ cuts is the following:

Theorem 1.2.1 (Menger)**.** *Let $G = (V, E)$ be an undirected graph, and the vertices $s, t \in V$ are given. The minimum size of an $s - t$ cut is equal to the number of edge-disjoint $s - t$ paths.*

Definition (Flow)**.** *Let $D = (V, A)$ be a digraph with two vertices s and t fixed, and let the (capacity) function $c : A \to \mathbb{R}^+$ be given. We call the function $f : A \to \mathbb{R}_0^+$ a flow subject to c, if the following hold:*

- $\forall e \in A : \quad f(e) \leq c(e)$
- $\forall v \in V \backslash \{s, t\}$:
$$\sum_{e \in \delta(v)} f(e) = \sum_{e \in \rho(v)} f(e)$$
- $\sum_{e \in \delta(s)} f(e) - \sum_{e \in \rho(s)} f(e) = \sum_{e \in \rho(t)} f(e) - \sum_{e \in \delta(t)} f(e)$

This last value is often called the value of the flow, which we'll be denoting as value(f)*.*

The connection between the previously defined cuts and flows was captured by the following notion (and first described in [2]):

Theorem 1.2.2 (Ford-Fulkerson)**.** *Let $D = (V, A)$ be a digraph, $s, t \in V$ and $c : A \to \mathbb{R}^+$ be a function. In this case, the maximal value of a $s - t$ flow (subject to c) in D equals the minimal c-value of an $s - t$ cut.*

T.C. Hu generalized the previous theorem in the case of two commodities in [5]. In this case, there are two source-sink pairs, and two flows, the sum of which has to be less than or equal to the given constraint c for every arc of the graph.

Theorem 1.2.3 (Hu's 2-commodity flow theorem)**.** *Let $D = (V, A)$ be a digraph, $s_1, s_2, t_1, t_2 \in V$ and let f_1 be a $s_1 - t_1$ flow, and f_2 be a $s_2 - t_2$ flow subject to constraining function c. Let C_1 and C_2 denote the minimum $s_1 - t_1$ and $s_2 - t_2$ cut, and C_3 denote the minimum cut that separates both $s_1 - t_1$ and $s_2 - t_2$. Then the two flows f_1 and f_2 are feasible if and only if following statements are true:*

1. $\text{value}(f_1) \leq C_1$,
2. $\text{value}(f_2) \leq C_2$,
3. $\text{value}(f_1) + \text{value}(f_2) \leq C_3$.

Furthermore the maximal sum of the values of the flows is equal to

$$\max(\text{value}(f_1) + \text{value}(f_2)) = C_3.$$

Chapter 2

Introduction to Game Theory

Allow us to introduce this simple problem to spark further interest:

Suppose that Sherlock Holmes hears from his aide Watson that the evil mastermind Professor James Moriarty was recently spotted in one neighborhood of London, and is rumored to be heading to another specific point of the city. Holmes still has enough time to reach any street in London, where if Moriarty's path crosses it, he finally intercepts the criminal and can put him in jail. Moriarty is afraid of the detective, and will take any path to lessen his chances of being caught. If we assume both men to be completely rational and having perfect knowledge of the streets of London, then what is the chance of Sherlock finally catching his arch-enemy?

Let us think of London as a graph, its streets as edges and junctions serving as vertices. Two special vertices are vertex s, the starting point, and vertex t, the terminal. In this model, the criminal needs to choose an s-t path P, while the detective chooses an edge e of the graph that he hopes is part of P.

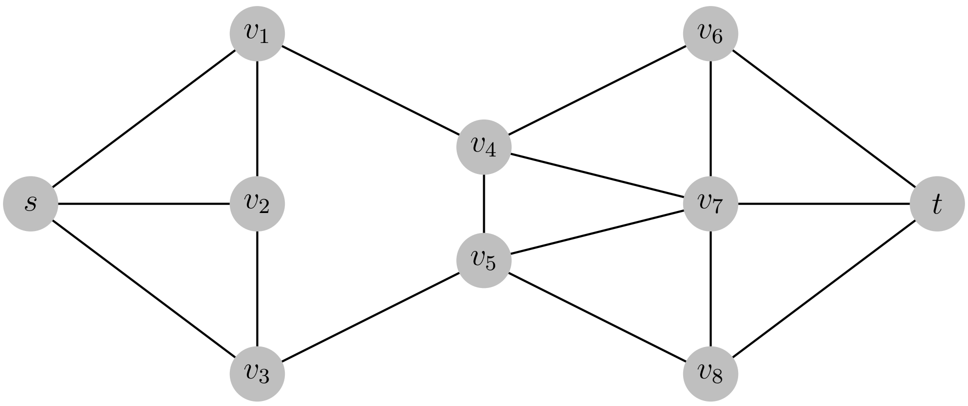


Figure 2.1: **Hypothetical map of London**

In Figure 2.1, the set of edges $C = \{v_1v_4, v_3v_5\}$ constitute a cut, as their removal results in the graph falling into two components. It can be noted that this is a minimum cut, as no single edge can be removed to the same effect, furthermore it is the only minimum cut. The nature of cuts require at least one edge of the path to cross it, therefore if Sherlock Holmes chooses one of the edges of cut C to investigate, he has at least 50 percent chance of catching the criminal.

Conversely we can see two edge-disjoint paths for Moriarty to take, the upper path $p_1 = (sv_1, v_1v_4, v_4v_6, v_6t)$ and similarly the lower path $p_2 = (sv_3, v_3v_5, v_5v_8, v_8t)$.

Since the detective can only patrol a single edge that cannot be part of both paths, he has at most 50 percent chance of catching him.

As we have seen this value to be at least this much, we find that if both people make their decisions optimally, then the chance of the criminal's detection is exactly $\frac{1}{2}$.

The previous findings hold true in a generalized case. Let the minimal cut value of another graph be k. According to Menger's theorem (see 1.2.1) Moriarty has k edge-disjoint paths from s to t. If he chooses one of these paths, then he has at least $\frac{k-1}{k}$ chance of escape.

On the other hand, if Sherlock chooses to barricade one of the edges of the minimal cut, he has at least $\frac{1}{k}$ chance of intercepting him. Therefore the chance of Moriarty's escape is no more than $\frac{k-1}{k}$.

Combining the two results, the chance that Sherlock catches the criminal is the reciprocal value of the minimum cut.

To summarize our findings, in this simple game the chance of detection is solely based on the graph, specifically on one property of the graph, the size of the minimum cut.

Our example was optimistic in a way that it guaranteed the capture of the criminal in case the two people crossed ways. Sadly however, we know that London's streets are very crowded, and Moriarty is very talented in making disguises. Because of this, from now on we consider Sherlock to (only) have p_e ($p_e \in (0, 1]$) chance of discovering and catching the professor if his path crosses the edge e that the detective is inspecting.

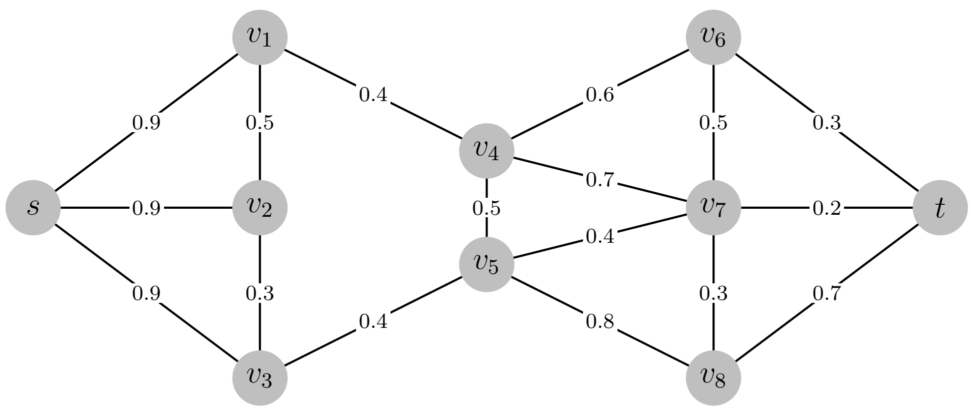


Figure 2.2: **Map of London with added detection probabilities**

This changes the strategy of our protagonists in a considerable way. No longer are many escape paths needed for Moriarty, if they all have high risk of detection, a single "secure" route consisting of low detection edges can be enough. A street that is part of many paths is useless for the detective if it is so busy that it is almost impossible to detect the passing criminal.

If Sherlock chooses an edge from $C = \{v_1v_4, v_3v_5\}$ as earlier, since $p_{v_1v_4} = p_{v_3v_5} = 0.4$, he has a probability of 0.2 of catching Moriarty. However, if we take a look at another cut $C' = \{sv_1, sv_2, sv_3\}$, we see that $p_{sv_1} = p_{sv_2} = p_{sv_3} = 0.9$, thus since the escape path has to use one of these three edges, the probability of detection is 0.3, which is higher than in the previous case.

Can Sherlock guarantee himself even higher probability of detection? Even in this relatively small graph using a heuristic approach, it's quite hard to determine the optimal strategy for the detective. To be able to better describe and fully understand this problem we need to have a deeper look into game theory. Our focus will be on two-player, zero-sum games.

2.1 Basic definitions of Game Theory

Although there are many types of games in Game Theory, we will be exclusively working with **strategic form games**.

Definition. *The following objects determine a two-player strategic form game:*

- *The sets S_1 and S_2 containing the possible actions or "pure" strategies of the corresponding players one and two, which define the set $S = S_1 \times S_2$, the set of strategy vectors.*
- *The payoff functions $u_1 : S \to \mathbb{R}$ and $u_2 : S \to \mathbb{R}$, where $u_1(s_1, s_2)$ defines the first player's winnings if he chooses strategy s_1, and his opponent strategy s_2. The second player's payoff function is defined likewise.*

Beginning with this definition we only look at things from one player's perspective, naturally everything can be defined for the second player similarly.

Definition. *An $s_1 \in S_1$ is a best response to $s_2 \in S_2$, if $\forall s_1' \in S_1$:*

$$u_1(s_1, s_2) \geq u_1(s_1', s_2).$$

In other words, we call the first player's strategy a best response to a certain choice of his opponent, if we know that the first player couldn't have achieved greater payoff by choosing another strategy.

Furthermore we call a best response a *strictly* best response, if $u_1(s_1, s_2) > u_1(s_1', s_2)$ for all $s_1' \neq s_1$, that is if any other choice would have meant a smaller winning.

Definition. *Let s_1, s_1' be two strategies of the first player. We say s_1 dominates the strategy s_1' (and s_1' is dominated by s_1), if $\forall s_2 \in S_2$:*

$$u_1(s_1, s_2) \geq u_1(s_1', s_2).$$

Furthermore we say s_1 strictly dominates s_1', if the first player's payoff is strictly greater with s_1 than s_1' regardless of player two's choice.

Definition. *We call $s = (s_1, s_2) \in S$ a*

- ***dominant strategy solution**, if for $i = 1, 2$ $\quad s_i$ dominates all other $s_i' \in S_i$.*
- ***strictly dominant strategy solution**, if all players' strategies strictly dominate their other potential strategies.*

Comparing it to the previous definitions, we get that a strategy vector is a dominant solution if and only if both of the players have chosen a best response to their adversary's choice.

Definition. *We call $s = (s_1, s_2) \in S$ a (pure) Nash-equilibrium, if*

$$\forall s_1' \in S_1, \forall s_2' \in S_2 : \quad u_1(s) \geq u_1(s_1', s_2) \quad \text{and} \quad u_2(s) \geq u_2(s_1, s_2').$$

This means each player's action is the best response to his/her opponent's strategies, for example if $s = (s_1, s_2)$ is a Nash-equilibrium, then s_1 is a best response to s_2, and vica versa.

It is important to remark that this equilibrium need not exist, furthermore it isn't always unique, although in special cases both of this can be achieved, see lemma further below for an example.

For a game without any Nash-equilibria, let us consider the following:

$$S_1 = S_2 = [0, 1] \quad u_1(s_1, s_2) = \begin{cases} s_1 & s_1 \neq 1 \text{ or } s_2 \neq 1 \\ 0 & s_1 = 1 \text{ and } s_2 = 1. \end{cases}$$

In this game both players choose a real number between 0 and 1. The payoff they receive is identical to the number they chose, in the exception of the case where both players chose 1, in which case they do not receive any winnings.

Let us assume to the contrary that there exists a Nash-equilibrium $s^* = (s_1, s_2)$ of this problem.

In the case where $s_1 = 1$ and $s_2 = 1$, then neither strategy is a best response to the other, for example $u_1(1, 1) = 0 < u_1(0.5, 1) = 0.5$ for the first player.

In the contrary case when at least one of s_1 and s_2 is less than 1, that can also not be a best response, since if for example $s_1 < 1$, then there is a possible choice of $s_1' = 1 - \frac{1-s_1}{2} > s_1$, and so $u_1(s_1, s_2) < u_1(s_1', s_2)$.

We found that s_1 and s_2 cannot be both best responses to one another, thus s^* is not a Nash-equilibrium.

Lemma 2.1.1. *If a strategy vector s taken from the set S is a dominant strategy solution, then it is a Nash-equilibrium. Furthermore, if it is a strictly dominant strategy solution, then it is the only Nash-equilibrium.*

Proof. The first statement is trivial, since if for the first player s_1 is a best response to all elements of S_2 (property of dominant strategies) then it is naturally a best response to the specific chosen $s_2 \in S_2$, similarly s_2 is a best response to s_1 and thus s is a Nash-equilibrium.

For the second part, let s be a strictly dominant strategy solution, and s' a Nash-equilibrium. The already proven first statement tells us that s is also a Nash-equilibrium. Assume towards contradiction that $s \neq s'$. Since s' is a Nash-equilibrium, we get:

$$u_1(s') = u_1(s_1', s_2') \geq u_1(s_1, s_2').$$

Similarly, since s is a dominant strategy solution, the following holds:

$$u_1(s_1, s_2') > u_1(s_1', s_2') = u_1(s').$$

Combining the two results, we get $u_1(s') > u_1(s')$, which is a contradiction, thus $s = s'$. □

2.2 Using mixed strategies

So far we have only looked at so-called pure strategies, where the game is only played once. We would like to look at cases where the same game is repeated over and over, and use the average winnings of the players to characterize the game. In real life, beginning with a game as simple as rock-paper-scissors, a player using the same strategy (i.e. showing rock every time) will become predictable and will be easily countered by his/her opponent.

From now on, we will allow players to use "mixed strategies", that is decide the probability with which they will choose each "pure" strategy. For instance, in the rock-paper-scissors game choosing each sign with $p = \frac{1}{3}$ is "optimal", i.e. results in a (mixed) Nash-equilibrium.

Let us define the following using S_1, S_2 and S as defined previously:

Definition.

- *A mixed strategy of player $i = 1, 2$, $m_i \in M_i$ is a probability distribution over the set S_i, formally:*

$$m_i : S_i \to [0,1]; \quad \sum_{s_i \in S_i} m_i(s_i) = 1.$$

- *$M = M_1 \times M_2$ is the set of mixed strategy vectors, where $m = (m_1, m_2) \in M$ is a mixed strategy vector.*

- *$u_1(m)$ is the expected value of the first player winnings according to the distribution m:*

$$u_1(m) = \sum_{s \in S} P_m(s) \cdot u_1(s) = \sum_{s \in S} \prod_i m_i(s_i) \cdot u_i(s),$$

where $P_m(s)$ denotes the probability of choosing s by the distribution m.

Definition. *$m = (m_1, m_2) \in M$ is a mixed Nash-equilibrium, if*

$$\forall m_1' \in M_1 : \quad u_1(m_1, m_2) \geq u_1(m_1', m_2)$$

and

$$\forall m_2' \in M_2 : \quad u_2(m_1, m_2) \geq u_2(m_1, m_2').$$

2.3 Two-player, zero-sum games

After this introduction, we shift our focus to a game that we will use later: (finite) two-player, zero-sum games. By finite we mean $|S_1| = m < \infty$ and $|S_2| = n < \infty$, that is both players have a finite number of strategies to choose from. Furthermore we call this game zero-sum, if $\forall s \in S : \quad u_1(s) + u_2(s) = 0$, in other words regardless of the chosen strategy, one player's gain equals the other player's loss. We like to think of it as if the losing player pays the winner a certain amount after the game.

Let us define the payoff matrix $A \in \mathbb{R}^{m \times n}$ in the following way: $a_{ij} := u_1(s_i, s_j)$; the j-th element in the i-th row will represent the first player's winnings/losses if she plays $s_i \in S_1$, and her opponent plays $s_j \in S_2$.

If $m_1 \in M_1$ and $m_2 \in M_2$ are the two mixed strategies chosen by the players, then let us represent them with the vectors $p \in \mathbb{R}^m$ and $q \in \mathbb{R}^n$, where $p_i = m_1(s_i) \quad \forall s_i \in S_1 \quad (i = 1 \dots m)$ and $q_j = m_2(s_j) \quad \forall s_j \in S_2 \quad (j = 1 \dots n)$. Furthermore we introduce the following notation broadening the interpretation of the payoff functions: $u_i(p, q) := u_i(m_1, m_2)$ for $i = 1, 2$.

For the players' winnings we get: $u_1(p, q) = pAq$ and naturally $u_2(p, q) = -pAq = pBq$, where $B = -A$. Note that we assume that all vectors are row/column vectors consistent with reason.

Both of the players' goal is to maximize their winnings/minimize their losses (the game is zero-sum, therefore this is the same thing). The question is how should the players choose their mixed strategies? Player one should choose a $p^* \in M_1$, where:

$$\min_{q \in M_2} p^* A q = \max_{p \in M_1} \min_{q \in M_2} pAq.$$

This translates to choosing a strategy where the worst case winnings are maximal, the maximin strategy.

Similarly for the second player, he should choose a q^*, where:

$$\min_{p \in M_1} pBq^* = \max_{q \in M_2} \min_{p \in M_1} pBq.$$

Using the fact that $B = -A$, and $\min -x = -\max x$, we get the following:

$$\max_{p \in M_2} pAq^* = \min_{q \in M_2} \max_{p \in M_1} pAq.$$

This is the so-called minimax strategy, player two chooses a strategy that her losses in the worst case will be minimal.

A natural question would be to ask what the relationship is between the maximin and minimax strategies. The "Minimax" theorem states that these are equal:

Theorem 2.3.1 (von Neumann, 1928). *In a two-player, finite, zero-sum game, the maximum guaranteed winnings of one player equals the minimum guaranteed losses (negated value of maximum guaranteed winnings) of the other player:*

$$\max_{p \in M_1} \min_{q \in M_2} pAq = \min_{q \in M_2} \max_{p \in M_1} pAq.$$

Remark. *This common value is often called the Game Value (shorthand: GV) corresponding to the matrix A.*

The original proof in [1] is based on the properties of bilinear forms, which we will omit in favor of a much shorter proof using the duality theorem of linear programming (LP), which was also first described by von Neumann.

Proof. We will give an LP form of the problem, but to do that, we need to first prove a couple of lemmas.

Lemma 2.3.2. *The second player's strategy s_j is a best (pure) response to $p \in M_1$ if and only if $(pA)_j$ (i.e. the jth coordinate of the vector $pA \in \mathbb{R}^n$) is the minimum coordinate.*

Proof. For sufficiency consider that if $(pA)_j$ is the minimum, then pAq is minimal when $q = e_j$ (jth unit vector), now $u_2(p,q) = -pAq$ is maximal, so s_j is truly a best response to p.

Necessity is also easily seen; assume to the contrary that $\exists k$ such that $(pA)_k < (pA)_j$ for all j, where $j \neq k$, then for $q = e_j$ and $q' = e_k$ we find that $u_2(p,q) < u_2(p,q')$, thus s_j can't be a pure best response to p, which is a contradiction. □

Very similarly we can state that $s_i \in S_1$ is a best pure response if and only if $(Aq)_i$ is the minimum coordinate. With these results we can give a formula for the guaranteed losses/wins:

Lemma 2.3.3. *Let $w, z \in \mathbb{R}^+$ be two given constants, and let $\mathbb{1}$ denote the all-one vector (of implicit size). If $pA \geq \mathbb{1}w$, then if player one chooses the strategy p, then she is guaranteed at least w winnings. Similarly if $Aq \leq \mathbb{1}z$, then the second player (playing q) is guaranteed to have no more than z losses.*

Proof. We will only prove the first part, the statement about the second player can be proved in an analogous way.

If $pA \geq \mathbb{1}w$, then specifically $\min_{j=1\ldots n}(pA)_j = (pA)_k \geq w$. The opponent's best response to this is $q = e_k$, but even then $u_1(p, e_k) = (pA)_k \geq w$, player one is guaranteed w in winnings. □

With this knowledge, we can finally formulate the first player's maximal guaranteed winnings (w^*) and the second player's minimal guaranteed losses (z^*) as a primal/dual problem.

Primal problem:

$$(P) \qquad \max\{w : p \in \mathbb{R}^m, \quad p \geq 0, \quad \mathbb{1}p = 1, \quad pA \geq \mathbb{1}w\}$$

Dual problem:

$$(D) \qquad \min\{z : q \in \mathbb{R}^n, \quad q \geq 0, \quad \mathbb{1}q = 1, \quad Aq \leq \mathbb{1}z\}$$

According to the duality theorem (see Theroem 5.4 in [12]), the optimum values of these problems are equal, thus $w^* = z^*$. □

Corollary 2.3.3.1. *In two-player, zero sum games the Nash-equilibria are exactly vectors containing the two players' maximin strategies.*

Proof. First we will prove that the maximin strategies are Nash-equilibria. Let (p^*, α), and (q^*, α) be optimal solutions of the LP problem stated above, this means that if the strategy vector $s = (p^*, q^*)$, then $u_1(s) = \alpha$ and $u_2(s) = -\alpha$. Since p^* is a maximin strategy, if the second player chooses a different (mixed) strategy, then the first player is still guaranteed at least α winnings, and so the second player α losses (or $-\alpha$ "winnings").

$$\forall q : \quad u_1(p^*, q) > \alpha \quad u_2(p^*, q) < -\alpha = u_2(s) = u_2(p^*, q^*)$$

This means that q^* is a best response to p^* (the reverse is true in a similar way), so we find that (p^*, q^*) is a Nash-equilibrium.

For the second part, we need to prove that the possible Nash-equilibria of two-player, zero sum games are maximin strategies. By law of contraposition, this is equivalent with the statement that a strategy that is not maximin cannot be a Nash-equilibrium. Let us suppose that p is not a maximin strategy of the first player. Our goal is to prove that $\forall q \in M_2$, (p, q) is not a Nash-equilibrium. Since p is not maximin, there exists a q' such that $u_1(p, q') < \alpha$, and since the game is zero-sum this means that $u_2(p, q') > \alpha$. If $u_2(p, q)$ were not greater than α, it would mean that

$$u_2(p, q) \leq -\alpha < u_2(p, q') \quad \Rightarrow \quad u_2(p, q) < u_2(p, q'),$$

thus (p, q) would not be a Nash-equilibrium (q would not be a best response for the second player to p).

If $u_2(p, q)$ were indeed greater than $-\alpha$, then we know that $u_1(p, q) < \alpha$, and:

$$u_1(p, q) < \alpha = u_1(p^*, q) \quad \Rightarrow \quad u_1(p, q) < u_1(p^*, q),$$

thus (p, q) is not a Nash-equilibrium in this case either, since p is not a best response to q.

To conclude our proof, we can similarly show that if q is not a maximin strategy, then for all $p \in M_1$, (p, q) is not a Nash-equilibrium. □

We will be leaning heavily on this theorem and its corollary in the future chapters, since these guarantee us a Nash-equilibrium in two-player, zero-sum games which we will use to define our new security metrics.

Chapter 3

Interdiction problems

In this section we will a look at the so-called interdiction problems, similar to the first problem which we introduced in chapter 2. This type of two-player game is played between an interdictor and an evader, where the goal of the interdictor is to catch the evaders. In the introductory problem the two players were Sherlock Holmes and James Moriarty, but we can also use this game to model the real life struggle between drug cartels and the police force, or between human traffickers and the border patrol. The first complete review of this interdiction problem was published by Washburn in [11].

3.1 Simple interdiction game

Definition. *We call the following a simple path interdiction game:*

Suppose that the directed graph $D = (V, A)$, the vertices $s, t \in V$, and the detection probability vector $p \in [0, 1]^{|A|}$ are given, and known by both players. Furthermore, the interdictor's set of strategies contains a probability distribution over the set of arcs, whereas the evader's set of strategies contains probability distributions over the set $\mathcal{P}$ of $s - t$ paths. In case the players choose the vectors $x \in \mathbb{R}^{|A|}$ and $y \in \mathbb{R}^{|\mathcal{P}|}$ the interdictor's payoff is:

$$u_1(x, y) = \sum_{e \in A} \sum_{P \in \mathcal{P}} x_e y_P p_e \chi_P(e),$$

where $\chi_P(e) = \begin{cases} 1 & e \in P \\ 0 & e \notin P \end{cases}$.

Lastly the game is zero sum: $u_2(x, y) = -u_1(x, y)$.

In chapter 2 we saw the equilibrium of this game in the special case where the interdiction probability p was uniformly 1 across all arcs of the graph to be $\frac{1}{|C_{min}|}$ where C_{min} denotes the minimumum directed $s - t$ cut of the graph.

In the general case, the following statement can be made regarding the game value:

Theorem 3.1.1. *If we denote $r_i := \frac{1}{p_i}$ and $r(C) := \sum_{c_i \in C} r_i$, then following statement is true:*

$$GV = \max \left\{ \frac{1}{r(C)} : C \textit{ is an } s - t \textit{ cut} \right\}$$

Proof. Let the maximum in the expression above be denoted by μ. Suppose that C' is a directed $s-t$ cut, where $\frac{1}{r(C')} = \mu$, and C' contains the arcs $e_1, \ldots, e_k$ (with the corresponding probabilities denoted by $p_1, \ldots, p_k$). Let r_i denote $\frac{1}{p_i}$ for all $i = 1 \ldots k$ and $r(C') := \sum_{e_i \in C'} r_i$. Suppose that the interdictor chose the following mixed strategy: she monitored only the arcs of C', each arc e_i with a probability of $\frac{r_i}{r(C')}$. If the evader chooses a path containing e_i, he has a $p_i \cdot \frac{r_i}{r(C')} = \frac{1}{r(C')}$ chance of getting caught, note that this is equal for all edges of the cut. Since his path covers at least one of these edges (because C' is a cut), the first player has an expected winning of at least $\frac{1}{r(C')}$, thus her maximum guaranteed winnings are also at least μ.

On the other hand, let us define the following weight on the edges: $g_i := \mu \cdot r_i$ for all $e_i \in A$. This is a positive value, and because of the definition of μ, we find that $f(C) = \frac{r(C')}{r(C)} \geq 1$ for all $s-t$ cuts C, and that $r(C') = 1$. As a result of the Ford-Fulkerson theorem (see 1.2.2) , we know that there exists an f flow subject to g in our graph, where $value(f) = 1$. It is a well-known statement that a flow can be decomposed into a (finite) sum of directed $s-t$ paths and directed cycles (see 10.3 in [12]). Let us take such a decomposition (disregarding the potential cycles), we get the directed paths $P_1, \ldots, P_n$ from s to t, with the weights $a_1, \ldots, a_n$ in a way that $\sum a_i = 1$ and

$$\sum_{i=1}^{n} a_i \chi 1_{P_i}(e) \leq \mu r_e \quad \forall e \in A.$$

We will show that choosing the paths $P_1, \ldots, P_n$ with $a_i, \ldots, a_n$ (and all others with zero) probability will maximize the evader's losses at μ. For this, suppose the interdictor chose any edge e to inspect, then the payoff would be:

$$\sum_{i=1}^{n} a_i \chi_{P_i}(e) p_e \leq \mu r_e p_e = \mu \frac{1}{p_e} p_e = \mu.$$

This strategy maximizes losses at μ, thus the optimal minimax strategy's payoff is also no more than μ.

We have seen that $\mu \leq \max\min u_1$ and that $\min\max u_2 \leq \mu$. Neumann's theorem (see 2.3.1) guarantees that the minimax strategies' payoffs are equal, thus both are $\mu = \frac{1}{r(C')}$, which is what we wanted to prove. □

As a side-note our results of the specialized case can also be confirmed via the results of this theorem. If the interdiction probability p is uniformly 1 across all arcs, then its reciprocal value r is also uniformly 1, and thus $r(C) = \sum_{c_i \in C} 1 = |C|$. Lastly $\max\left\{\frac{1}{|C|}\right\} = \frac{1}{|C_{min}|}$.

3.2 Generalizations of the interdiction problem

We have multiple different directions in which we can generalize this problem, we will be reviewing each of these cases in order.

In the original simplified model we presumed to know the exact starting and end points of the evader's route, but oftentimes we only have vague information. He may start from any point in the set of $S = \{s_1, \ldots, s_k\}$ and arrive to any point of $T =$

$\{t_1, \dots, t_l\}$. In this case, let us construct the directed graph $D' = (V', A')$ as follows: we will add two extra nodes, $V' = V \cup \{s', t'\}$ and we add directed edges from s' to all s_i and from all t_j to t', that is $A' = A \cup \{(s', s_1), \dots, (s', s_k)\} \cup \{(t_1, t'), \dots, (t_l, t')\}$, furthermore we set the detection probability to zero for all the new edges. This guarantees us that these edges will never be chosen by the interdictor, and so the game value of a simple interdiction game in this newly defined D' between the nodes s' and t' will be equal to the game value of an evader running from $s_i \in S$ to $t_j \in T$.

We can also allow interdiction at vertices (i.e. crossroads or junctions) by vertex-splitting. If we know that the evader has a chance p_v of getting detected in node v, then we introduce the new nodes v', v'' which replace v, connect them with a (v', v'') arc, and for all (u, v) and (v, w) arcs we add $(u, v')$and (v'', w) respectively. These new arcs retain their original p values, we set $p_{(v',v'')}$ to p_v.

In our basic model we explicitly stated that Sherlock "still had time to reach any place", which meant that the only thing the interdictor had to keep in mind when choosing his strategies were the p values. This is not realistic, we can almost always associate "costs" to the edges, whether that represents the time/money spent reaching it or costs regarding the interdiction attempt (such as the costs placements of traffic enforcement cameras along road routes) is not important in our case. It would be quite natural for the interdictor to try to minimize their costs while maximizing their interdiction probabilities.

Let the values c_e for all $e \in A(G)$ be given. We talk about a general interdiction problem, when the payoff for the interdictor is changed to:

$$u_1(x, y) = \sum_{P \in \mathcal{P}} \sum_{e \in A} x_e y_P p_e \chi_P(e) - \sum_{e \in A} x_e c_e$$

(Note that the game is still thought to be zero sum).

Regarding the game value of this generalized interdiction game, we can prove the following statement.

Theorem 3.2.1. *Let us use the following notation,* $r_i := \frac{1}{p_i}$, $r(C) := \sum\limits_{e_i \in C} r_q$, $q_i := \frac{c_i}{p_i}$, $q(C) := \sum\limits_{e_i \in C} q_i$. *The game value of the general interdiction game is:*

$$\max \left\{ \left\{ \frac{1 - q(C)}{r(C)} : C \textit{ is an } s - t \textit{ cut} \right\} \cup \{-c(e) : e \in A\} \right\}$$

Proof. Once again let us denote the value of the above maximum with μ.

For the first step, we would like to show that the interdictor always has a strategy, which guarantees them at least μ expected winnings. Let us suppose that $\mu = -c(e)$ for an arbitrary $e \in A$. In this case the interdictor can choose this arc with a probability of 1, and all other arcs with a probability of 0, and their winnings are guaranteed to be at least $-c(e) = \mu$. Let us suppose now that the maximum is taken from the other set, that $\mu = \frac{1-q(C)}{r(C)}$ for an $s - t$ cut C. In this case the interdictor can choose an arc e_i of C with a probability of $\frac{r_i}{r(C)}$, and all further arcs with zero probability. If a chosen e_i is part of the evader's path, then the interdictor's gains are incremented by the following value:

$$\frac{r_i}{r(C)}(p_i - c_i) = \frac{\frac{1}{p_i}(p_i - c_i)}{r(C)} = \frac{1 - \frac{c_i}{p_i}}{r(C)} = \frac{1 - q_i}{r(C)}.$$

When e_i is not part of the chosen path, then it contributes $\frac{r_i}{r(C)}(-c_i) = \frac{-q_i}{r(C)}$ to the interdictor's winnings. The total expected gain can be described as:

$$\sum_{e_i \in C} \frac{\chi_{P_i}(e_i) - q_i}{r(C)} = \frac{\sum\limits_{e_i \in C} \chi_{P_i}(e_i) - q(C)}{r(C)}.$$

We know that the evader's path contains at least one arc of the directed cut, thus the above value is at least $\frac{1-q(C)}{r(C)} = \mu$. With this we have now shown that in all cases the interdictor can guarantee herself μ winnings, thus the game value is at least this much.

As the second step, similarly to the proof of the theorem 3.1.1, we will intruduce a capacity function $g(e_i) = \mu \cdot r_i + q_i = \frac{\mu + c_i}{p_i}$. The definition of μ necessitates it to be at least $-c_i$, thus $g(e_i) \geq 0$ for all $e_i \in A$. Furthermore all capacities of the $s - t$ cuts are at least 1, thus according to the Ford-Fulkerson theorem (see: 1.2.2) there exists an $s - t$ flow f with a value of 1.

Let us divide this flow into the $s - t$ paths $P_1, \ldots, P_k$ of values $a_1, \ldots, a_k$ respectively, $\sum\limits_{i=1}^{k} a_i = 1$. The nature of flows dictates that the flow values on individual arcs cannot be higher than the capacity.

$$\sum_{j: e_i \in P_j} a_j \leq g(e_i) = \mu r_i + q_i \quad \forall e_i \in A$$

If the evader chooses the paths P_1 to P_k each with its respective probability of a_1 to a_k, then his losses can be described as:

$$\sum_{j: e_i \in P_j} a_j(p_i - c_i) - \sum_{j: e_i \notin P_j} a_j c_i \quad = \quad p_i \sum_{j: e_i \in P_j} a_j - c_i$$

This value is at most $p_i g(e_i) - c_i$, which in turn using the definition of g equal to $p_i(\mu r_i + q_i) - c_i = p_i(\mu \frac{1}{p_i} + \frac{c_i}{p_i}) - c_i \mu$.

This strategy therefore guarantees the evader a maximum loss of μ. As we previously saw the minimum guaranteed winnings of the interdictor to also be μ, Neumann's theorem guarantees us that this is indeed the Nash-equilibrium. □

As proposed in [19] we can also think of the game value as the minimal value of ν, where there exists a flow f with a value of 1 with the non-negative constraint function $g(e_i) = \nu r_i + q_i$.

The inequation $g(e_i) \geq 0$ is equivalent to $\nu \geq -c_i \forall e_i \in A$. For a cut C of the digraph the flow value is dominated by the constraint, that is $1 \leq g(C) = \nu r(C) - q(C)$. Thus we get $\nu \geq \frac{1-q(C)}{r(C)}$ for every $s - t$ cut C. Combining with the previous result we see that $\nu \geq \mu$, and so naturally the minimum ν which satisfies all previous conditions is equal to the optimal μ.

In [10] it is shown that by maximum $|A|$ computations of the max flow problem one can calculate the minimum value of ν. Since a flow with a value of 1 can be decomposed into a convex combination of paths and directed cycles also in a strongly polynomial time, the entire algorithm of calculating the Nash-equilibrium of this game is strongly polynomial.

3.3 Multiple evaders, interdictors

As the last part of this chapter, we will take a very quick glance at the next step logical step in generalizing the interdiction problem. What we can say in the case of multiple evaders and/or interdictors? Suppose a drug cartel has N worth of drugs in s and they want to send it to t. They choose k runners, each receiving $n_i(i = 1 \dots k)$ shipment, where $\sum_{i=1}^{k} n_i \leq N$. In the meantime, the police are planning a large razzia and send m officers to try to catch as much illegal cargo as possible.

Due to length constraint reasons a detailed description of this case will be omitted, and rather an overview about different results will be given.

Hu's theorem which we saw previously (see 1.2.3) can be used to help in the special two evader, one interdictor case, this is done in [16].

The original paper by Washburn [11] already touches on the subject of one evader with multiple interdictors. Different payoff functions are discussed in relation to interdictors placed at the same arc. The question is quite natural, are their interdiction probabilities independent from each other, or not?

In [14] the general case is discussed in depth, and Nash-equilibria are provided for different cases. The multiple evaders are modelled by an $s - t$ flow of "bad", whereas the interdictors are a "blockage" set of arcs.

Chapter 4

Connectivity Based Metrics

Before getting started, here are two important concepts that should be recalled:

A graph $G = (V, E)$ has **edge-connectivity** k, if it is k-edge-connected, but not $(k+1)$-edge-connected; in other words, k is the minimum number of edges that have to be removed for the graph to lose its connectivity.

Similarly, a graph $G = (V, E)$ has **vertex-connectivity** k, if it is k-vertex-connected, but not $(k+1)$-vertex-connected; that means that we have to remove at least k vertices (and all the edges incident to them) for the remaining graph to be disconnected.

It must be noted that for complete graphs no such k exists, therefore vertex-connectivity of a K_n is said to be infinity.

Remark. *Vertex-connectivity is a metric stronger than edge-connectivity in the following sense: for any k, it can be shown that there exists a graph (for example two K_{k+1}-s with a common vertex) which has a vertex-connectivity of* 1 *and edge-connectivity of k.*

4.1 Graph Strength

4.1.1 Introduction

We familiarized ourselves with the basic definition of edge-connectivity. This is a useful metric in many occasions, however going forward it has two basic flaws.

Firstly, it only measures how many edges we have to remove for the graph to "fall apart", but does not care how the graph behaves after removing even more edges. For instance, consider the following two graphs: G_1 is two K_n-s ($n \geq 3$) joined by two edges ("bridges"); G_2 can be a circuit on n vertices. In both cases the removal of a two edges can result in two components, therefore both graphs have edge-connectivity two. However, in the case of G_1 we have to remove a minimum of $n + 1$ edges to have the graph fall into three components (and $2n$ edges for four components and so on), while removing k ($k \leq n$) edges from G_2 always results in k components. In this regard we feel G_2 to be a "weaker" graph than G_1, but the edge-connectivity metric does not differentiate them.

A new metric that solves this problem was first proposed by Dan Gusfield in 1983 [7].

Let the comp function denote the number of connected components of $G - U = (V, E \setminus U)$.

Definition (Graph Strength). *In case of a connected graph G, its strength can be defined by the following formula:*

$$\sigma(G) = \min\left\{\frac{|U|}{\text{comp}(G-U)-1} : U \subseteq E(G), \text{comp}(G-U) > 1\right\}.$$

This new metric is better suited for finding networks which repel initial attacks, but are overcome after multiple assaults.

Using our previous example where both G_1 and G_2 had edge-connectivity 2, we find that $\sigma(G_1) = 2$, but $\sigma(G_2) = \frac{n+1}{n-1}$.

Note that networks which are vulnerable to early attacks, but are (relatively) more resistant later on are not differentiated from ones that are vulnerable to all attacks.

Consider the following two new graphs: G_3 is two K_n-s joined by a single edge, G_4 is an arbitrary tree. Both graphs have edge-connectivity one, and their strengths are also one. The key difference is that for any subset of edges U of G_4, the removal of U always results in $|U|$ new components, whereas for G_3 there exists a single $U^* = \{e^*\}$, where $\frac{|U^*|}{\text{comp}(G-U^*)-1} = 1$, for all other subset of edges U the ratio between $|U|$ and the new components gained by erasing U is significantly greater than one.

This phenomenon will not be a problem going forward, because we will be reviewing network vulnerability in an adversarial environment. The network will be attacked by a cognitive being associated with perfect judgment and evaluation skills, thus a network with a single "weak point"' that can be exploited by the adversary will be viewed equally as vulnerable as a network with many equally weak points.

Since the removal of a single edge can only result in one new component at maximum, the removal of U results in at most $|U|$ components. Thus $\sigma(G) \geq 1$. Although there is no upper bound for $\sigma(G)$ in general, for (simple) graphs where we limit the number of nodes, we find:

Lemma 4.1.1. *For all simple graphs $G = (V, E)$, where $|V(G)| = n$:*

$$1 \leq \sigma(G) \leq \frac{n}{2}$$

Proof. The first inequality was shown earlier. For the upper bound consider that in the case where $U = E$, then the removal of all of the edges results in $n - 1$ new components. Since there are at most $\binom{n}{2}$ edges in a simple graph, consequently $|E| \leq \binom{n}{2} = \frac{n(n-1)}{2}$. We find that in this case:

$$\sigma(G) \leq \frac{|E|}{\text{comp}(G-E)-1} = \frac{\frac{n(n-1)}{2}}{n-1} = \frac{n}{2}.$$

□

It should be noted that the reciprocal value of $\sigma(G)$ is:

$$T = \frac{1}{\sigma(G)} = \max\left\{\frac{\text{comp}(G-U)-1}{|U|} : U \subseteq E(G), \text{comp}(G-U) > 1\right\}.$$

In other words T measures the maximum number of new components per edges removed.

T's importance as a property of a graph was also realized by Gusfield as he wrote: "It seems reasonable that T can be used as a measure of vulnerability; the larger the ratio, the more vulnerable is the graph to large amounts of disconnection for few edge deletions."[7]

4.1.2 Weighted Graph Strength

The other problem that we had with edge-connectivity still remains unsolved. So far we have only been interested in the quantity of the removed edges, but not the quality. From a practical standpoint this is questionable, oftentimes we have information that some part of the system is more vulnerable than the rest; and we would like this knowledge reflected in our metric.

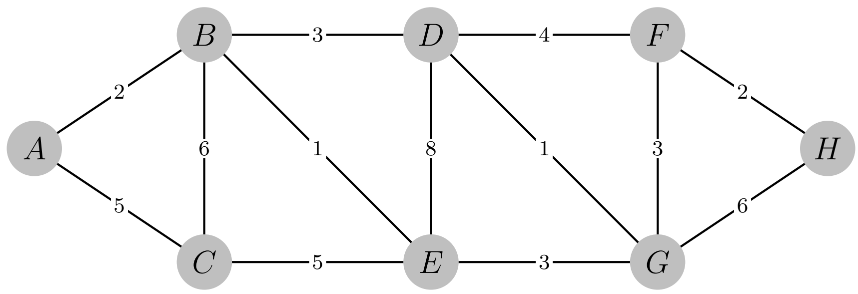
William Cunningham was the first to generalize Gusfield's graph strength by giving each edge in the graph a weight [9]. Following his footsteps let $s : E(G) \to \mathbb{R}^+$ be a weight function on the edges of the graph. The value of $s(e)$ is perceived to symbolize the individual strength of edge e; the larger the value, the stronger we believe it to repel attacks or the more it costs for a potential attacker to destroy this edge. For any $U \subset E$, we use the following notation: $s(U) := \sum\limits_{e \in U} s(e)$.

Definition (Weighted Graph Strength)**.** *For a connected graph G, its weighted strength with regard to the weight function s is defined as:*

$$\sigma_s(G) = \min \left\{ \frac{s(U)}{\text{comp}(G-U) - 1} : U \subseteq E(G), \text{comp}(G-U) > 1 \right\}.$$

Similar to the unweighted case, $\frac{1}{\sigma_s(G)}$ represents the maximum number of components created per the weight of the removed edges.

To further enhance our understanding of this metric, let us take a look at the following graph, where the numbers on the edges represent the s-values:



In this example, deleting the edges AB and AC turns A into an isolated vertex, thus creating a new graph component, and making the set $\{AB, AC\}$ a cut. The combined weight of the deleted edges is 7, it can easily be seen that this is also the minimal cut value in this graph. The picture below depicts a valid flow with a value of 7. Since a cut value is always greater than or equal to a flow value, in case of equality they are both optimal, i.e. the cut value is minimal, whereas the flow value is maximal.

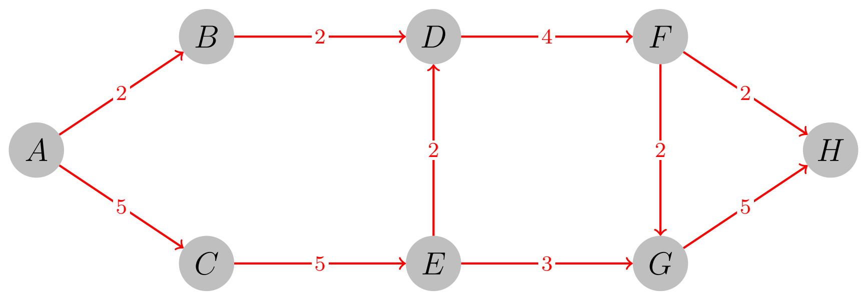


Figure 4.1: A flow with a value of 7

Following the preceding logic, we can state that the minimum cut-value is always an upper bound on the (weighted) strength, since:

$$\sigma_s(G) = \min\left\{\frac{s(U)}{\text{comp}(G-U)-1} : U \subseteq E(G), \text{comp}(G-U) > 1\right\} \leq \frac{s(C)}{\text{comp}(G-C)-1} = s(C)$$

In a different approach, let us choose the following subset of edges to delete: $U = \{DF, DG, EG, FG, FH\}$. In this case, we see that $s(U) = 13$ and the deletion of U results in 2 new components, thus we get $\sigma_s(G) \leq \frac{13}{2}$. Further deleting the edge GH (i.e. if $U' = U \cup \{GH\}$) we find that $s(U') = 19$ and since $\frac{19}{3} < \frac{13}{2}$, this further reduces the upper bound of this graph's strength.

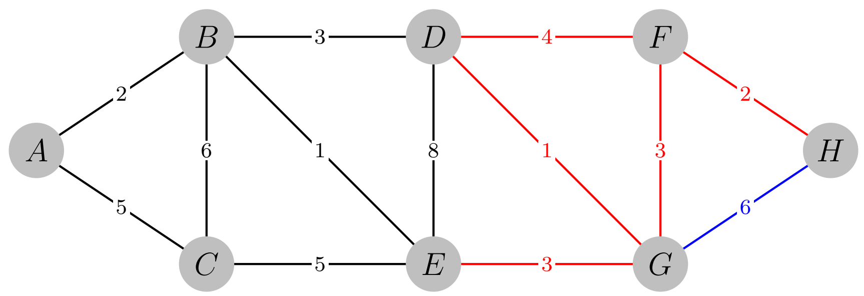


Figure 4.2: Red edges represent U, red and blue together U'

In the end, we find that the strength of this graph does not exceed $\frac{19}{3}$. However, using this quasi-heuristic approach we cannot prove that this is exactly the graph strength value.

Going forward not only would we like a general computation algorithm for graph strength, we would also like it to be polynomial among other things, since a metric that is not (quickly and reliably) calculable is sadly mostly useless from a practical perspective. Fortunately this is not the case with graph strength.

4.1.3 Calculating (Weighted) Graph Strength

We use the notation $\kappa(U) = \text{comp}(G-U) - 1$ to describe the number of new components created by the removal of U.

Theorem 4.1.2. *Given a graph $G = (V, E)$, and the function $s : E \to \mathbb{R}$, let U^* be a subset of edges, and $q := \frac{s(U^*)}{\kappa(U^*)}$, then the following holds:*

$$\sigma_s(G) = q \quad \Leftrightarrow \quad \min\{s(U) - q\kappa(U) : U \subseteq E\} = 0 \tag{4.1}$$
$$\sigma_s(G) < q \quad \Leftrightarrow \quad \min\{s(U) - q\kappa(U) : U \subseteq E\} < 0 \tag{4.2}$$

Proof. We shall only prove the first statement, the second can be proved likewise.

For sufficiency, since $q = \sigma_s(G) = \min\left\{\frac{s(U)}{\kappa(U)} : U \subseteq E\right\}$ and $\kappa(U) > 0$:

$$q \leq \frac{s(U)}{\kappa(U)} \qquad \forall U \subseteq E$$
$$0 \leq s(U) - q\kappa(U) \qquad \forall U \subseteq E,$$

thus $\min\{s(U) - q\kappa(U) : U \subseteq E\} \geq 0$. Furthermore since $q = \frac{s(U^*)}{\kappa(U^*)}$, we get $s(U^*) - q\kappa(U^*) = 0$, thus we see the minimum of 0 taken on, and so the first part of the proof is finished.

For necessity, let the subset of edges U' be where the minimum is taken on, $s(U') - q\kappa(U') = 0$, and since this is a minimum and $\kappa(U) > 0$:

$$s(U') - q\kappa(U') \leq s(U) - q\kappa(U) \qquad \forall U \subseteq E$$
$$0 \leq s(U) - q\kappa(U) \qquad \forall U \subseteq E$$
$$q \leq \frac{s(U)}{\kappa(U)} \qquad \forall U \subseteq E$$
$$q \leq \min\left\{\frac{s(U)}{\kappa(U)} : U \subseteq E\right\} = \sigma_s(G),$$

and since $q = \frac{s(U^*)}{\kappa(U^*)} \geq \min\left\{\frac{s(U)}{\kappa(U)} : U \subseteq E\right\}$, thus $q = \sigma_s(G)$, which concludes our proof. □

For a more thorough examination of this theorem and its use in fractional programming see [6].

With this theorem we found a neccessary and sufficient condition to check whether a quotient q is optimal, i.e. equals the graph strength.

Let us define the following algorithm as in [9].

Algorithm 1 Cunningham's algorithm

```
1: U* := E
2: q := s(U*)/κ(U*)
3: while min(s(U) − qκ(U) : U ⊆ E) < 0 do
4:     U* := minimizer of s(U) − qκ(U)
5:     q := s(U*)/κ(U*)
```

The previous algorithm works theoretically. However we need to show that it converges rapidly, that there is no chance of being stuck in an infinite loop.

Lemma 4.1.3. *Let us suppose that for a $q > \sigma_s(G)$ the subset of edges U' minimizes $\{s(U) - q\kappa(U) : U \subseteq E\}$. Let us define $q' := \frac{s(U')}{\kappa(U')}$. If $\exists U''$ such that $0 > s(U'') - q'\kappa(U'')$, then $\kappa(U'') < \kappa(U')$.*

Proof. As a first step, we show that $q - q' > 0$. From our previous theorem, since $q > \sigma_s(G)$, we know that $s(U') - q\kappa(U') = \min\{s(U) - q\kappa(U) : U \subseteq E\} < 0$

$$\begin{aligned} s(U') - q\kappa(U') &< 0 \\ s(U') &< q\kappa(U') \\ \frac{s(U')}{\kappa(U')} &< q \\ q' &< q \\ 0 &< q - q'. \end{aligned}$$

Furthermore:

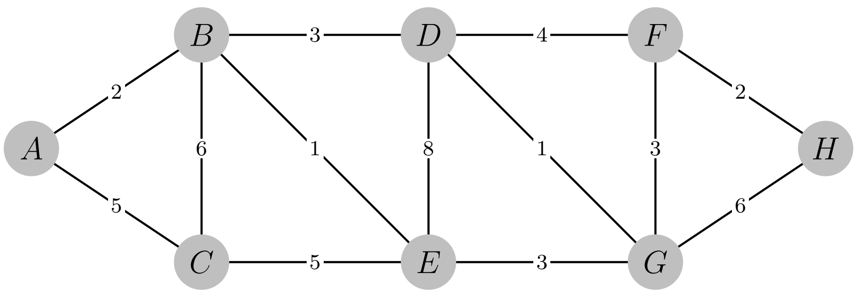
$$\begin{aligned} 0 &> s(U'') - q'\kappa(U'') \\ &= s(U'') - q\kappa(U'') + q\kappa(U'') - q'\kappa(U'') \\ &\geq s(U') - q\kappa(U') + q\kappa(U'') - q'\kappa(U'') && \text{since } U' \text{ is a minimizer} \\ &= q'\kappa(U') - q\kappa(U') + q\kappa(U'') - q'\kappa(U'') && \text{since } q' = \frac{s(U')}{\kappa(U')} \\ &= (\kappa(U'') - \kappa(U')) \underbrace{(q - q')}_{>0} \end{aligned}$$

$$\Rightarrow \quad \kappa(U'') - \kappa(U') < 0 \quad \Rightarrow \quad \kappa(U'') < \kappa(U').$$ □

For us this lemma means that if we start from $q = \frac{s(E)}{\kappa(E)}$, then until the program terminates and the optimal weighted graph strength is found the minimizer subroutine is called a maximum of $|V| = n$ times, since for all U the value $\kappa(U)$ is a positive integer not exceeding $n - 1$.

For this work, the minimizer subroutine will be treated as an "oracle". A strongly polynomial algorithm for it can be found in [8], thus our complete algorithm is also polynomial.

Let us take another look at the graph from earlier, and see how its strength is calculated using our algorithm.



We initialize our algorithm with $U_1 = E$ and $q_1 = \frac{S(E)}{\kappa(E)} = \frac{49}{7} = 7$. Our first call to the oracle will be

$$\min(s(U) - 7\kappa(U) : U \subseteq E).$$

We receive that the minimum is -2 and that a minimizer is $U_2 = \{DF, DG, EG, FG, FH, GH\}$, so $q_2 := \frac{s(U_2)}{\kappa U_2} = \frac{19}{3}$. We make our second call to the oracle $\min(s(U) - \frac{19}{3}\kappa(U) : U \subseteq E\}$.

However, we receive that the minimum is zero, thus according to our theorem $\frac{19}{3}$ is the weighted strength of the graph.

4.1.4 Spanning Tree Game

The connection between connectivity and spanning trees is obvious, a graph is connected if and only if it contains a tree as a spanning subgraph. Moreover, if a graph has k mutually edge-disjoint spanning trees, then its edge-connectivity is at least k.

The following theorem was proved almost simultaneously by Tutte [4] and Nash-Williams [3], both published their findings in 1961:

Theorem 4.1.4. *Let G be a finite, non-null graph. A necessary and sufficient condition for G to contain k edge-disjoint spanning trees:*

$$k(\text{comp}(G - U) - 1) \leq |U|$$

for all $U \subseteq E(G)$

From this theorem we can deduce the following:

Corollary 4.1.4.1. *If a connected graph G has a maximum of M edge-disjoint spanning trees, and its strength is $\sigma(G)$, then:*

$$M \leq \sigma(G) < M + 1$$

Proof. The previous theorem states that to have M edge-disjoint spanning trees, the condition $M(\text{comp}(G - U) - 1) \leq |U|$ for all $U \subseteq E(G)$ is necessary. Since this inequality stands for any subset U of edges, it naturally stands for any subsets U' whose removal results in new components, that is where $\text{comp}(G - U') > 1$. Dividing both sides of the inequality by the number of new components generated by the removal of U' results in:

$$M \leq \frac{|U'|}{comp(G - U') - 1}$$

Since this inequality stands for all U', where $\text{comp}(G - U') > 1$, as a special case it stands for a U^*, where this ratio is minimal; this minimal ratio is what we defined in 4.1.1 as the strength of the graph. From this we get $M \leq \sigma(G)$, which is the first part we wanted to prove.

For the second part, suppose to the contrary that $\sigma(G) \geq M + 1$. That would mean that for all U', where $\text{comp}(G - U') > 1$,

$$|U'| \geq (M + 1)(\text{comp}(G - U') - 1)$$

However this also stands for subsets U'' which removal does not result in new components, since in this case the previous statement is simply $|U''| \geq 0$, which is naturally true.

So we have

$$(M + 1)(\text{comp}(G - U) - 1) \leq |U|$$

for all $U \subset E(G)$, so according to the previous theorem G contains (at least) $M + 1$ edge-disjoint spanning trees, which is impossible since we know that it contains no more than M.

Thus the second part $\sigma(G) < M + 1$ is also proven.

□

This result shows us how deeply connected our new metric is with spanning trees. From this it will be quite natural to use spanning trees in our game whose eventual equilibrium we would like to grasp the value of graph strength.

Defining the Spanning Tree game

Let us take a look at the following two-player game, played between Player A ("Anne") and Player B ("Bob"):

Player A will be the defending player, her job will be to choose a spanning tree T from the set $\mathcal{T}(G)$ containing the spanning trees of graph G. Player B will be the attacker, and he will choose an edge e of the graph to be attacked. The goal of the players will be quite natural, the attacker will try to hit one of the edges of the secretly chosen spanning tree, while the defender will try to choose a spanning tree that is hardest to hit.

Every round, Player B will pay $c(e)$ cost to Player A for attacking edge e, and will receive $d(e)$ in return if he successfully hits the tree.

The idea behind this game is the following: if Player B has a good strategy for winning in the long run, that means that the graph is not secure. In the contrary case, if his winnings are low, that tells us the network is reliable. We conjecture that the reciprocal value of the game will prove to be an adequate metric of the graph. Formal definition:

Definition. *We call the following two-player, zero-sum game a* ***Spanning Tree Game****:*

Assume that a connected graph $G = (V, E)$, and the functions $d : E(G) \to \mathbb{R}^+$ and $c : E(G) \to \mathbb{R}$ are given and known by both players.The mixed strategy set of the first player (M_1) contains probability distributions over the set of spanning trees of G, while M_2 contains probability distributions over $E(G)$.

If the strategies $x \in M_1$ and $y \in M_2$ are chosen, the second player's (attacker's) payoff function is:

$$u_2(x, y) = \sum_{T \in \mathcal{T}(G)} \sum_{e \in E(G)} x_T y_e d(e) \chi_T(e) - \sum_{e \in E(G)} y_e c(e),$$

where $\chi_T(e) = \begin{cases} 1 & e \in T \\ 0 & e \notin T \end{cases}$

In the special case where we assume that no cost is payed for the attack, and the damage is uniformly 1 across all edges, we get the following important result. [13]

Theorem 4.1.5. *If $d(e) = 1$ and $c(e) = 0$ for all $e \in E(G)$, then the game value of the Spanning Tree Game is the reciprocal value of the graph's (unweighted) strength.*

$$GV = \frac{1}{\sigma(G)}$$

Proof. For any non-empty subset U of edges let $\mathcal{M}(U)$ denote the minimum spanning tree cover number, and $\mathcal{T}_U \subseteq \mathcal{T}$ the set of spanning trees where this minimum value is taken:

$$\mathcal{M}(U) := \min_{T \in \mathcal{T}(G)} |T \cap U|, \quad \mathcal{T}_U := \{T \in \mathcal{T}(G) : |T \cap U| = \mathcal{M}(U)\}.$$

Let us look at the following graph G:

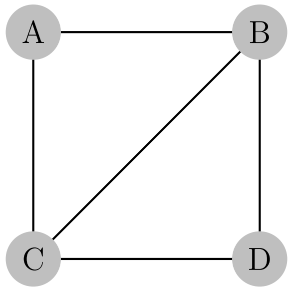


Figure 4.3: **Graph** G

If we choose the subset $U = \{AB, AC\}$, then $\mathcal{M}(U) = 1$, as all spanning trees contain at least one of these edges, but not necessarily both. The set $\mathcal{T}(U)$ contains all of the spanning trees of the graph that have exactly one edge in common with U.

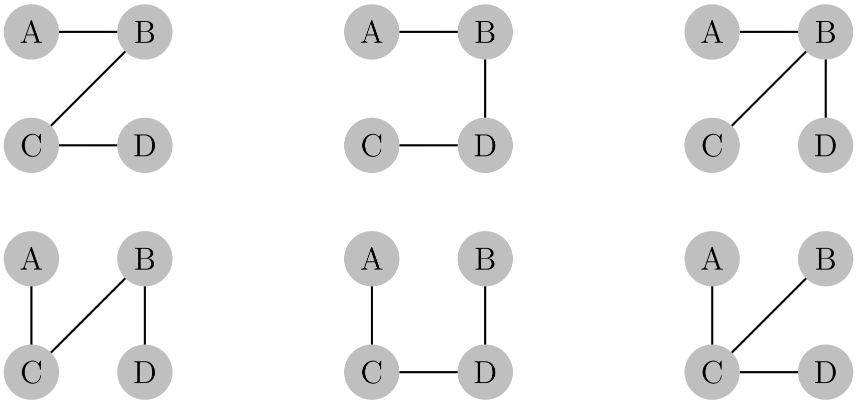


Figure 4.4: **Elements of the set** $\mathcal{T}(U)$

Furthermore let $\vartheta(U)$ denote the ratio between this minimum cover number and the number of elements of U. (This is perceived as the vulnerability of U):

$$\vartheta(U) := \frac{\mathcal{M}(U)}{|U|}$$

From the definition we see that $\vartheta(U)$ is a rational number between 0 and 1.

We call a subset U' of edges **critical**, if $\vartheta(U') = \max_{U \subset E(G)} \{\vartheta(U)\}$, that is, if it achieves maximum vulnerability. Using our previous example, the vulnerability of $U = \{AB, AC\}$ is $\frac{1}{2}$.

This subset is not critical, as the maximum vulnerability is $\frac{3}{5}$. The maximum vulnerability in this case is reached when $U' = E$.

Regarding the critical subsets, the following can be proven:

Lemma 4.1.6. *For all critical subsets U' of the graph G, there exists a Nash-equilibrium under which the defender only chooses minimum U'-cover spanning trees and the attacker uniformly attacks the edges of U'.*

Proof. According to the statement let U' be a fixed critical subset. Furthermore let the mixed strategies of the players be:

$$m_1(T) = \begin{cases} x_T \geq 0 & \text{if } T \in \mathcal{T}_{U'} \\ x_T = 0 & \text{otherwise} \end{cases} \qquad m_2(e) = y_e = \begin{cases} \frac{1}{|U'|} & \text{if } e \in U' \\ 0 & \text{if } e \notin U' \end{cases}.$$

Furthermore, the values x_T shall be chosen in a way that the following two conditions also hold true:

$$x(e') := \sum_{T\in\mathcal{T}} x_T \chi_T(e') = \vartheta(U') \quad \forall e' \in U', \tag{4.3}$$

$$x(e'') \leq \vartheta(U') \quad \forall e'' \notin U' \tag{4.4}$$

In [13] it is proven that an x strategy vector can be chosen satisfying conditions 4.3 and 4.4.

As a first step we take a look at the winnings of the players if they choose m_1 and m_2, respectively.

$$\begin{aligned} u_2(m_1,m_2) = -u_1(m_1,m_2) &= \sum_{e\in E}\sum_{T\in\mathcal{T}} m_1(T) m_2(e) \chi_T(e) \\ &= \sum_{e\in E}\sum_{T\in\mathcal{T}} x_T y_e \chi_T(e) \\ &= \sum_{e\in E} y_e \underbrace{\sum_{T\in\mathcal{T}} x_T \chi_T(e)}_{x(e)} \\ &= \sum_{e'\in U'} y_{e'} x(e') + \sum_{e''\notin U'} \underbrace{y_{e''}}_{0} x(e'') \\ &= \sum_{e'\in U'} \frac{1}{|U'|} \vartheta(U') + 0 = \vartheta(U'). \end{aligned}$$

Now let us take a look at the case, if the second player chooses a different $m_2' \in M_2$:

$$\begin{aligned} u_2(m_1,m_2') &= \sum_{e'\in U'} \vartheta(U') m_2'(e') + \sum_{e''\notin U'} x(e'') m_2'(e'') \\ &\leq \sum_{e'\in U'} \vartheta(U') m_2'(e') + \sum_{e''\notin U'} \vartheta(U') m_2'(e'') \qquad \text{(by condition 4.4)} \\ &= \vartheta(U') \sum_{e\in E} m_2'(e) = \vartheta(U') = u_2(m_1,m_2). \end{aligned}$$

We see that for any m_2', the inequality $u_2(m_1,m_2) \geq u_2(m_1,m_2')$ holds, this shows that m_2 is a best response to m_1. Similarly we can prove that m_1 is a best response to m_2, as for any $m_1' \in M_1$, the following holds:

$$\begin{aligned} u_1(m_1',m_2) &= -\sum_{T\in\mathcal{T}}\sum_{e\in E} m_1'(T) \overbrace{m_2(e)}^{\frac{1}{|U'|}} \chi_T(e) \\ &= -\frac{1}{|U'|} \sum_{T\in\mathcal{T}} m_1'(T) \sum_{e\in E} \chi_T(e) \\ &= -\frac{1}{|U'|} \sum_{T\in\mathcal{T}} m_1'(T) |T \cap U'| \\ &\leq -\frac{1}{|U'|} \sum_{T\in\mathcal{T}} m_1'(T) \mathcal{M}(U') = -\vartheta(U') = u_1(m_1,m_2). \end{aligned}$$

In the last step, we used $-|T \cap U'| \leq -\mathcal{M}(U')$, which is true since $|T \cap U'| \geq \mathcal{M}(U') = \min\{|T \cap U'| : T \in \mathcal{T}\}$.

We have proven that m_1 and m_2 are best responses to each other, this means that they constitute a mixed Nash-equilibrium (see 2.2). □

It is imperatively important to note that we did not necessarily find *all* Nash-equilibria of this problem, but because it is a two-player, zero sum game, the Neumann-theorem (see 2.3.1) guarantees us that all equilibria have the same payoff.

As the final step, we only need to show that $\vartheta(G) = \frac{1}{\sigma(G)}$. Using the definitions of these metrics:

$$\vartheta(G) = \max\left\{\frac{\mathcal{M}(U)}{|U|}\right\} \qquad \sigma(G)^{-1} = \max\left\{\frac{\mathrm{comp}(G-U)-1}{|U|}\right\},$$

we find that showing $\mathcal{M}(U) = \mathrm{comp}(G-U) - 1$ is sufficient.

The inequality $\mathcal{M}(U) \geq \mathrm{comp}(G-U) - 1$ is trivial, even a minimum U-cover spanning tree T must reach all components, and thus have at least $\mathrm{comp}(G-U)-1$ common edges with U.

Conversely, $\mathcal{M}(U) \leq \mathrm{comp}(G-U) - 1$ can be seen as follows. For all spanning trees T, where $|T \cap U| > \mathrm{comp}(G-U) - 1$ we can design a T' (from T by switching U-covered edges with edges within the connected components), where $|T' \cap U| = \mathrm{comp}(G-U) - 1$, thus the minimum $\mathcal{M}(U) \leq \mathrm{comp}(G-U) - 1$.

□

A similar result in [18] states that if we define the function $p(e) = \frac{1}{d(e)}$ for all $e \in E(G)$, then the game value in the case of $c \equiv 0$ and arbitrary d will be $\frac{1}{\sigma_p(G)}$.

These results are encouraging in a sense that it shows that our game has managed to capture the essence of (weighted) graph strength, and because we receive the reciprocal values of these metrics in the simplest cases it is natural to assume that the reciprocal value of the Nash-equilibrium in the general case is a competent metric that in turn generalizes graph strength.

The game value of the general case is also proved in [18]:

Theorem 4.1.7. *Let the graph $G = (V, E)$ and the functions $c, d : E \to \mathbb{R}^+$ be given. Then the Game Value is:*

$$GV = \max_{\emptyset \neq U \subseteq E(G)} \frac{\mathrm{comp}(G-U) - 1 - \frac{c(U)}{d(U)}}{\sum\limits_{e \in U} \frac{1}{d(e)}}.$$

It must be noted that the last two results were proven in an even more general environment, as a matroid base game.

4.2 Graph Persistence

4.2.1 Introduction

In this section we take a look at a slightly different model. So far we have been working with so-called "many-to-many" networks, where the individual nodes are of equal importance. Some networks, such as military communications networks, are different from a topological standpoint. In these cases (the so-called "one-to-many" networks) there is one designated partner that stands above the others in hierarchy.

We will change our model in the following way: we promote a vertex $v_0 \in V(G)$ to be a "headquarter" or HQ, the rest of the nodes $(v_1, \ldots, v_n)$ will symbolize subordinate units. We model the asymmetry in communications by using a directed graph $G = (V, A)$ to symbolize the line of communication. The goal will be the HQ's message reaching the other units, i.e. a directed path between v_0 and v_1, v_0 and v_2 and so on. The importance of the message to reaching unit i will be represented by a positive real number $d_i (i = 1 \ldots n)$. Furthermore the "damage" done by removing a subset of edges U (disrupting these lines of communication) will be denoted by $\lambda(U) = \sum\{d_i : v_i \text{ is unreachable from } v_0 \text{ after deleting } U\}$.

Definition (Graph Persistence)**.** *Let $G = (V, A)$ be a digraph, $v_0 \in V(G)$ a designated node, and $d \in \mathbb{R}_+^{|V|}$. Then the **persistence** of G is:*

$$\pi(G) = \min\left\{\frac{|U|}{\lambda(U)} : U \subseteq A(G), \lambda(U) > 0\right\}$$

This metric was originally called "directed graph strength" in [9], the term "persistence" was first coined in [15]. The reason behind moving away from the original name is two-fold. Firstly it implied connection with the (undirected) graph strength (see 4.1.1), while they have inherently different meanings. One measures connectivity between a certain node and the rest of the nodes; the other the connectivity between all pairs of nodes. Secondly the term "directed" is also misleading, persistence can be interpreted on undirected graphs too.

Note that in our model we only allowed the jamming of lines of communication, but not the destruction of communication centers/devices (i.e. the nodes of the graph). Realistically potential adversaries are just as (if not more) likely to target the latter. Therefore we should define a more general *edge-node-persistence* as below:

$$\pi_v(G) = \min\left\{\frac{|X|}{\lambda(X)} : X \subseteq \{A(G) \cup V(G)\}, \lambda(X) > 0\right\}.$$

It should be noted that in this case we broaden the domain of the function d to include $V(G)$, and define λ accordingly. However, using the technique of node-splitting it can be shown that for any graph G there exists a G' (and the $G \to G'$ mapping is injective) such that $\pi_v(G) = \pi(G')$.[15] As a result of this we will only consider the original (edge) persistence in the following segments.

4.2.2 Rooted Spanning Tree Game

We will once again introduce a two-player game which will try to capture the notion behind our newest metric. Player one will be the network operator, she will choose a rooted spanning tree of the graph (symbolizing the lines of communication). The second player will be the attacker, he will choose an edge of the graph to disrupt, this edge will become incapable of transmitting the message. The payoff will be based on the importance of the units not receiving the orders of the HQ.

Formal definition:

Definition. *We call the following two-player game a **Rooted Spanning Tree Game**:*

Assume that a connected digraph $G = (V, A)$, the specially designated node v_0, and the function $d : A(G) \to \mathbb{R}^+$ are given and known by both players. The mixed strategy set of the first player contains probability distributions over the set of rooted spanning trees of G, whereas the second players' contains probability distributions over the set of arcs $A(G)$: In case of $x \in M_1, y \in M_2$ the second player's (attacker's) payoff function is:

$$u_2(x, y) = \sum_{T \in \mathcal{RST}(G)} \sum_{e \in A(G)} x_T y_e \lambda(T, e) \chi_T(e) - \sum_{e \in A(G)} y_e c(e)$$

where $\lambda(T, e) := \sum\{d(v_i) : v_i \text{ is unreachable in } T - e\}$. The game is assumed to be zero sum: $\forall x \in M_1, y \in M_2 : \quad u_1(x, y) = -u_2(x, y)$

In [17] the following is proven:

Theorem 4.2.1.

$$GV = \frac{\lambda(U) - c(U)}{|U|}$$

Corollary 4.2.1.1. *In the special case where $c \equiv 0$, then:*

$$GV = \frac{1}{\pi(G)}$$

As the reader might remember, in the previous section we saw that the game value of the special case of the (normal) Spanning-Tree Game was the reciprocal value of the graph strength. Similarly we now observe the reciprocal value of the graph persistence as the equilibrium. Following the previous thought process regarding the generalization of the graph strength we can also accept the game value of the Rooted Spannning-Tree Game in turn to generalize the metric of graph persistence.

4.2.3 Headquarter selection

Suppose a company has a number of offices, and a well-built communications system between them. They know the cost of how much it require to operate their headquarters from office v_i ($c(v_i)$), and would naturally try to minimize their expenditures while having a "safe" network (with a persistence of at least π_0).

This leads us to the following problem:

Definition. *We call the following a Headquarter Selection problem:*

INPUT: Directed graph G, functions $c, d : V(G) \to \mathbb{R}^+$ and the value $\pi_0 \in \mathbb{R}^+$.

SOLUTION: Node $v^* \in V(G)$, such that $c(v^*) = \min\{c(v) : \pi(G, v) \geq \pi_0\}$

(By $\pi(G, v)$ we mean the persistence calculated with v as the HQ)

Lemma 4.2.2. *$\pi(G, v^*) \geq \pi_0$ if and only if there exists an $s' - t'$ flow f subject to g in G', where:*

1. $G' = (V', E'), \quad V' = V \cup \{s', t'\}$, *and* $E' = E \cup \{(s', v^*)\} \cup \{(v_1, t'), \dots, (v_n, t')\}$,
2. $g(s', v^*) = \infty, \quad g(v_i, t') = d(v_i)$ *for all* $i = 1 \dots n$ *and for all* $e \in E : g(e) = 1$,
3. $\text{value}(f) = \pi_0 \cdot d(V)$.

Proof. For $W \subseteq V(G)$, the set of edges leaving W is $\delta(W)$, the number of them is $|\delta(W)|$. Remember that we defined $\pi(G)$ as the minimal $\frac{|U|}{\lambda(U)}$ ratio. For the set U' which minimizes the previous expression $\exists! X$, such that $\delta(X) = U'$. This implies that $|U'| = |\delta(X)|$ and $\lambda(U') = d(\overline{X}) = d(V) - d(X)$.

As a result of multiplying by the non-zero value of $d(\overline{X})$, we find that:

$$\pi(G) \geq \pi_0 \quad \Leftrightarrow \quad |\delta(X)| \geq \pi_0 \cdot d(\overline{X}) \quad \Leftrightarrow \quad |\delta(X)| + \pi_0 \cdot d(X) \geq \pi_0 \cdot d(V). \quad (4.5)$$

Let us shift our focus to our graph G^*. According to the Ford-Fulkerson theorem (see [2]), the maximum flow in G^* equals the minimum g-capacity cut, that is $\min_{X \subseteq E(G')} \{g(\delta(X)) : \nexists s' - t' \text{ path in } G' \backslash \delta(X)\}$. If $v^* \notin X$, then the cut value is infinity, otherwise it is equal to $|\delta(X)| + \pi_0 \cdot d(X)$. Furthermore:

$$\forall X : |\delta(X)| + \pi_0 \cdot d(X) \geq \pi_0 \cdot d(V) \quad \Leftrightarrow \quad \exists \text{ a } \pi_0 \cdot d(V)\text{-valued flow in } G^* \quad (4.6)$$

Combining 4.5 and 4.6 we reach the statement we want to prove. □

As a corollary of this lemma, one way to solve the HQ selection problem would be to use a greedy algorithm, sort the nodes in ascending order according to their costs, and use the Ford-Fulkerson algorithm as a subroutine to check if G' has a large enough flow. In the worst case scenario this is iterated n times, thus the whole algorithm is still polynomial (though not necessarily optimal).

Another way to solve the original problem would be to characterize it as an IP problem, then use a well-known solver. (Since we don't know which node will be v^*, in this construction of G' we will add edges (s', v_i) for all v_i. Instead of infinity we will assign them a weight of K, a sufficiently large constant)

VARIABLES:
$x \in \{0,1\}^{|V(G)|}, \quad f \in \mathbb{R}_+^{|E(G')|}$
CONSTANTS:
$\pi_0, K \in \mathbb{R}_+, \quad c, d \in \mathbb{R}_+^{|V(G)|}$
CONSTRAINTS:

1. $0 \leq x \leq \mathbb{1}$
2. $\mathbb{1} \cdot x = 1$
3. $\forall e \in E(G) : 0 \leq f(e) \leq 1$
4. $\forall e' = (s', v_i) : 0 \leq f(e') \leq (Kx)_i$
5. $\forall e'' = (v_i, t') : f(e'') = \pi_0 \cdot d_(v_i)$

6. $\forall v \in V(G)$

$$\sum_{(u,v)\in E(G)} f((u,v)) = \sum_{(v,u)\in E(G)} f((u,v))$$

SOLVE: minimize $c \cdot x$

The first two constraints guarantee us that we will choose exactly one HQ, the conditions $3-6$ guarantee us an adequate flow in G', condition five in particular ensures us that all (v_i, t) edges are fully saturated, thus we will have an optimum solution.

A further generalization of this problem, when we allow multiple co-headquarters and only demand connectivity with one of them in case of an attack can be found in [15].

Chapter 5

Conclusion

In this work, we see how the security metrics of networks and systems can be defined and calculated based on hypothetical two-player games. Interdiction games are introduced to model the defense against drug runners and human smugglers. We find that the knowledge of the interdiction possibilities at specific checkpoints or border entries defines the probability of catching an adversary making optimal decisions. Furthermore we see how this probability is computable in (strongly) polynomial time.

We familiarize ourselves with the connectivity-based metrics graph strength and graph persistence. In the case of graph strength, we see how this metric generalizes edge-connectivity. The introduced Spanning-Tree Game is shown to have a deep connection to graph strength, and we accept that its Nash-equilibrium in turn generalizes graph strength. In contrast to graph strength, which describes "many-to-many" networks, graph persistence is in turn the metric of "one-to-many" networks. The Rooted Spanning-Tree allows us to capture the essence of graph persistance in a special case, and is also useful for generalizing the notion behind it in the general case. Finally the problem of headquarter selection is also described, and we provide multiple ways of computing the optimal solution for it.

Contents

Bibliography

1. Von Neumann, J. Zur Theorie der Gesellschaftsspiele. *Mathematische Annalen* **100,** 295–320 (1928).
2. R Ford Jr, L. & Fulkerson, D. R. Maximal Flow Through a Network. *Canadian Journal of Mathematics* **8,** 399–404 (Jan. 1956).
3. Nash-Williams, C. S. A. Edge-Disjoint Spanning Trees of Finite Graphs. *Journal of the London Mathematical Society* **s1-36,** 445–450. eprint: `https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms/s1-36.1.445`. `https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-36.1.445` (1961).
4. Tutte, W. T. On the Problem of Decomposing a Graph into n Connected Factors. *Journal of the London Mathematical Society* **s1-36,** 221–230. eprint: `https://londmathsoc.onlinelibrary.wiley.com/doi/pdf/10.1112/jlms/s1-36.1.221`. `https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms/s1-36.1.221` (1961).
5. Hu, T. C. Multi-Commodity Network Flows. *Oper. Res.* **11,** 344–360. ISSN: 0030-364X. `http://dx.doi.org/10.1287/opre.11.3.344` (June 1963).
6. Dinkelbach, W. On Nonlinear Fractional Programming. *Management Science* **13,** 492–498. ISSN: 00251909, 15265501. `http://www.jstor.org/stable/2627691` (1967).
7. Gusfield, D. Connectivity and edge-disjoint spanning trees. *Information Processing Letters* **16,** 87 –89. ISSN: 0020-0190. `http://www.sciencedirect.com/science/article/pii/0020019083900315` (1983).
8. Cunningham, W. Testing membership in matroid polyhedra. *Journal of Combinatorial Theory, Series B* **36,** 161–188 (Apr. 1984).
9. Cunningham, W. H. Optimal Attack and Reinforcement of a Network. *J. ACM* **32,** 549–561. ISSN: 0004-5411. `http://doi.acm.org/10.1145/3828.3829` (July 1985).
10. Radzik, T. in *Complexity in Numerical Optimization* 351–386 (1993). `https://www.worldscientific.com/doi/abs/10.1142/9789814354363_0016`.
11. Washburn, A. & Wood, K. Two-Person Zero-Sum Games for Network Interdiction. *Operations Research* **43,** 243–251. ISSN: 0030364X, 15265463. `http://www.jstor.org/stable/171833` (1995).
12. Schrijver, A. *Combinatorial Optimization - Polyhedra and Efficiency* (Springer, 2003).

13. Gueye, A., Walrand, J. & Anantharam, V. *Design of Network Topology in an Adversarial Environment* in (Nov. 2010), 1–20.

14. Hong, S. & Wooders, M. Strategic Network Interdiction (2010).

15. Lászka, Buttyán, L. & Szeszlér, D. *Optimal selection of sink nodes in wireless sensor networks in adversarial environments* in *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* (June 2011), 1–6.

16. Calinescu, G., Kapoor, S., Quinn, M. & Shin, J. *Adversary Games in Secure/Reliable Network Routing* in. **75** (Jan. 2012).

17. Laszka, A., Szeszlér, D. & Buttyán, L. *Game-theoretic Robustness of Many-to-one Networks* in *Game Theory for Networks* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2012), 88–98. ISBN: 978-3-642-35582-0.

18. Szeszlér, D. Security Games on Matroids. *Math. Program.* **161,** 347–364. ISSN: 0025-5610. `https://doi.org/10.1007/s10107-016-1011-9` (Jan. 2017).

19. Szeszlér, D. Hitting a path: a generalization of weighted connectivity via game theory. *Journal of Combinatorial Optimization* (Nov. 2018).