Spanning tree modulus and secure broadcast games

by

Kapila Kottegoda

B.Sc., University of Peradeniya, Sri Lanka, 2011

M.S., Kansas State University, 2015

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2020

Abstract

The theory of p-modulus provides a general framework for quantifying the richness of a family of objects on a graph. When applied to the family of spanning trees, p-modulus has an interesting probabilistic interpretation. In particular, the 2-modulus problem in this case has been shown to be equivalent to the problem of finding a probability distribution on spanning trees that utilizes the edges of the graph as fairly as possible. In this dissertation, we use the above fact to produce a game-theoretic interpretation of modulus by employing modulus to solve a secure broadcast game between a network broadcaster and an eavesdropper in a network.

First, we review the concept of modulus in the continuum, and the discrete modulus in networks in general. Then, a set of necessary and sufficient conditions for a mixed-strategy solution to the secure broadcast game is proven. An explicit connection between the 2-modulus problem (formulated as a *minimum expected overlap* problem) on the spanning trees of a graph and the solution to the game is provided. Moreover, we show a comparison between the solution method presented in this dissertation and other methods for solving the game from different literature.

This dissertation also provides an algorithm for computing the spanning tree modulus by recursively solving the secure broadcast game on subgraphs. The theories of matroids and network flows are used with modulus theory to implement this algorithm. We present a polynomial time worst-case upper bound for the time complexity along with some numerical computations.

In addition, we consider maximizing 2-modulus for families of objects on a graph. This idea can open new directions for spanning tree modulus for secure broadcast games with weight constraints, which we explain briefly and will investigate more as future research.

Spanning tree modulus and secure broadcast games

by

Kapila Kottegoda

B.Sc., University of Peradeniya, Sri Lanka, 2011

M.S., Kansas State University, 2015

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2020

Approved by:

Major Professor
Nathan Albin

Copyright

Abstract

The theory of p-modulus provides a general framework for quantifying the richness of a family of objects on a graph. When applied to the family of spanning trees, p-modulus has an interesting probabilistic interpretation. In particular, the 2-modulus problem in this case has been shown to be equivalent to the problem of finding a probability distribution on spanning trees that utilizes the edges of the graph as fairly as possible. In this dissertation, we use the above fact to produce a game-theoretic interpretation of modulus by employing modulus to solve a secure broadcast game between a network broadcaster and an eavesdropper in a network.

First, we review the concept of modulus in the continuum, and the discrete modulus in networks in general. Then, a set of necessary and sufficient conditions for a mixed-strategy solution to the secure broadcast game is proven. An explicit connection between the 2-modulus problem (formulated as a *minimum expected overlap* problem) on the spanning trees of a graph and the solution to the game is provided. Moreover, we show a comparison between the solution method presented in this dissertation and other methods for solving the game from different literature.

This dissertation also provides an algorithm for computing the spanning tree modulus by recursively solving the secure broadcast game on subgraphs. The theories of matroids and network flows are used with modulus theory to implement this algorithm. We present a polynomial time worst-case upper bound for the time complexity along with some numerical computations.

In addition, we consider maximizing 2-modulus for families of objects on a graph. This idea can open new directions for spanning tree modulus for secure broadcast games with weight constraints, which we explain briefly and will investigate more as future research.

Table of Contents

List of Figures

Acknowledgments

First and foremost, I would like to express my sincere gratitude to my advisor Dr. Nathan Albin for his guidance, support, encouragement, and patience throughout these years. You have been a vital part of my graduate career and I am forever grateful to you for teaching me skills that I will be using in my career as well as in real life. I could not imagine having a different advisor.

I would like to thank my committee members Dr. Sarah Reznikoff, Dr. Bacim Alali, and Dr. Michael Higgins for their support and guidance given to me and my research work. I would also like to thank all the faculty and staff members at the Department of Mathematics at Kansas State University for their friendliest support.

Next, I want to give a warm thanks to Kansas State University for giving me the opportunity to pursue my doctoral degree. Further, I want to thank all of my friends from USA, Sri Lanka, and all over the world for keeping me company and helping me when I need help.

Last but not least, I would like to show my greatest gratitude to my loving parents, wife, and two sisters. I would not have made it this far without their undying love, trust, and care. I am forever in your debt.

Dedication

I would like to dedicate this dissertation to my mother, my father, my loving wife, and my two sisters.

Chapter 1

Introduction

1.1 Secure broadcast games

A communication network is often modeled as a collection of nodes and links. For example, in a wired computer network, nodes can represent personal computers and links can represent transmission media such as Ethernet cables. Mathematically, such a network is often modeled by a graph $G = (V, E)$, where V is the set of vertices corresponding to the nodes and E is the set of edges corresponding to the links.

A (one-to-all) broadcast in a network is a method of sending a message from a source node to all other nodes in the network by utilizing a subset of the network links. If the goal is to use as few links as possible, then the set of links used will form a spanning tree of the graph G.

This dissertation concerns a secure broadcast game introduced and analyzed in [11]. Although many modified versions of this game exist (e.g., [10, 12, 14, 15, 19, 20]), the focus of this dissertation is on the connections between the original game and the theory of p-modulus. The game is illustrated in Figure 1.1. In this game, Player **B** (the broadcaster) wants to broadcast a message to all other nodes. This is accomplished by choosing a spanning tree from the set $\{\gamma_1, \gamma_2, \ldots, \gamma_8\}$ shown in Figure 1.2 to broadcast on. Player **E** (the eavesdropper) can observe the transmission along a single link in the link set $\{e_1, e_2, \ldots, e_5\}$. Player **B** wins

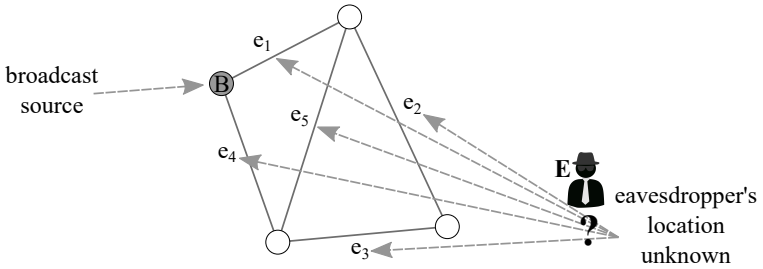


Figure 1.1: An illustration of the broadcast game.

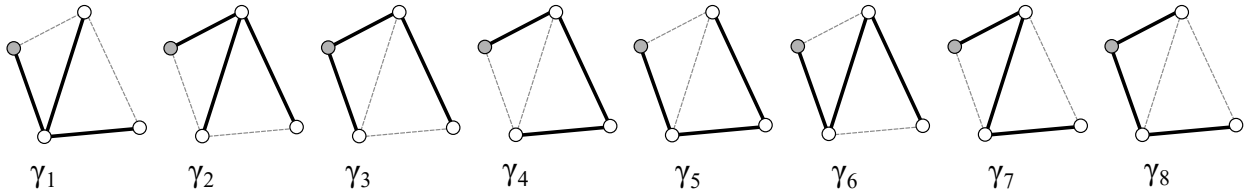


Figure 1.2: Spanning trees of the example network in Figure 1.1.

the game if the spanning tree avoids **E**'s edge, while Player **E** wins if the tree includes the edge. Posed in this way, this is a zero-sum game, because the net gain is zero. i.e. **B**'s gain or loss is equivalent to **E**'s gain or loss.

Figure 1.2 shows all possible spanning trees that **B** can use to broadcast. It is easy to see that no pure-strategy equilibrium exists. Indeed, if **B**'s spanning tree is known to **E**, then **E** can readily choose to listen on one of its edges. Moreover, if **E** has chosen an edge, **B** can easily avoid it. On the other hand, Nash's existence theorem [16] shows that a mixed-strategy equilibrium exists. Consider the following mixed strategies for Player **B**.

- Strategy 1: Use γ_1 or γ_2 with equal probability. In this case, **E** can listen on e_5 and always win.
- Strategy 2: Use $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ with equal probability. In this case, **E** can choose any strategy that uses only e_1 and e_2 and win 75% of the time.
- Strategy 3: Use all spanning trees with equal probability. In this case, **E** can choose any strategy that uses any edge except e_5 and win 62.5% of the time.
- Strategy 4: Use $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ with probabilities 2/5, 1/5, 1/5, 1/5 respectively. In this case, **E** wins 60% of the time with any strategy.

In fact, as a consequence of Theorem 3.2.2 and Theorem 3.3.1, Strategy 4 corresponds to a Nash equilibrium.

1.2 Modulus in the continuum

The classical theory of conformal modulus was originally developed in complex analysis several decades ago, see Ahlfors comment on p. 81 of [1]. Intuitively, p-modulus provides a method for quantifying the richness of a family of curves: modulus is large for families containing many short curves. The p in p-modulus refers to a parameter $p \in [1, \infty]$. Modulus tends to favor the "many curves" aspect when p is close to 1 and the "short curves" aspect as p becomes large.

Even though this dissertation is fully focused on modulus in the discrete setting, we shall recall some theory from modulus in the continuum. Let Ω be a region in $\mathbb{C}$, and Γ a set whose elements γ are rectifiable curves in Ω, e.g. $\Gamma = \Gamma_\Omega(E, F)$, where E, F are two continua in $\overline{\Omega}$, and the γs connect from E to F. Let the density $\rho : \Omega \mapsto [0, \infty)$ be a Borel measurable function. Then every γ has a well-defined ρ length

$$\ell_\rho(\gamma) = \int_\gamma \rho \, ds, \tag{1.1}$$

and the open set Ω has a ρ area

$$A_\rho(\Omega) = \iint_\Omega \rho^2 \, dA. \tag{1.2}$$

We define the minimum ρ length as

$$\ell_\rho(\Gamma) = \inf_{\gamma \in \Gamma} \ell_\rho(\gamma).$$

Definition 1.2.1. The extremal length of Γ in Ω is defined as

$$\lambda_\Omega(\Gamma) = \sup_\rho \frac{\ell_\rho(\Gamma)^2}{A_\rho(\Omega)}, \quad \text{where } 0 < A_\rho(\Omega) < \infty.$$

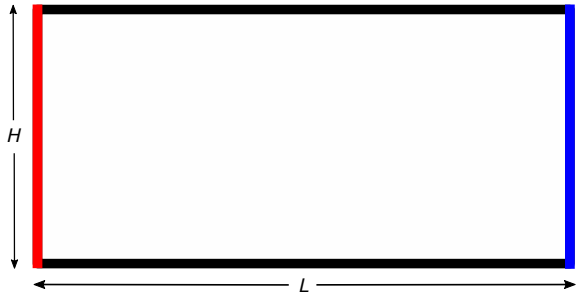
Note that the quantity $\ell_\rho(\Gamma)^2/A_\rho(\Omega)$ is homogeneous in the sense that it does not change when ρ is multiplied by a constant. This observation leads to the following equivalent characterization of extremal length.

We say that ρ is *admissible* for Γ and write $\rho \in \mathrm{Adm}(\Gamma)$ if $\ell_\rho(\Gamma) \geq 1$. Then we define the 2-modulus of Γ as

$$\mathrm{Mod}_2(\Gamma) := \inf_{\rho \in \mathrm{Adm}(\Gamma)} A_\rho(\Omega) = \inf_{\rho \in \mathrm{Adm}(\Gamma)} \iint_\Omega \rho^2 \, dA.$$

From the homogeneity of the objective function in Definition 1.2.1, it follows that extremal length is the reciprocal of the modulus.

Example 1.2.1. (The Rectangle). Consider a rectangle of height H and length L.



$$\Omega := \{z = x + iy \in \mathbb{C} : 0 < x < L, 0 < y < H\}$$

Set $E := \{z \in \overline{\Omega} : \mathrm{Re}\ z = 0\}$ and $F := \{z \in \overline{\Omega} : \mathrm{Re}\ z = L\}$ to be red vertical side and blue vertical side respectively. If $\Gamma = \Gamma_\Omega(E, F)$ then,

$$\mathrm{Mod}_2(\Gamma) = \frac{H}{L}. \tag{1.3}$$

To show this value for modulus, assume $\rho \in \mathrm{Adm}(\Gamma)$. Then for all $0 < y < H$, $\gamma_y(t) := t + iy$

is a curve in Γ parametrized by $t \in [0, L]$. Since ρ is assumed to be admissible, the ρ-length of this curve must satisfy

$$\ell_\rho(\gamma_y) = \int_{\gamma_y} \rho \, ds = \int_0^L \rho(t, y) \, dt \geq 1.$$

The Cauchy-Schwarz inequality yields,

$$1 \leq \left[\int_0^L \rho(t, y) dt \right]^2 \leq L \int_0^L \rho^2(t, y) dt \implies L^{-1} \leq \int_0^L \rho^2(t, y) dt.$$

Integrating over y, we obtain

$$\frac{H}{L} \leq \iint_\Omega \rho^2 \, dA.$$

Since ρ is an arbitrary admissible density, $\text{Mod}_2(\Gamma) \geq \frac{H}{L}$.

Now, define $\rho_0 = \frac{1}{L} \mathbb{1}_\Omega(z)$. Note that $\iint_\Omega \rho_0^2 \, dA = \frac{HL}{L^2} = \frac{H}{L}$. If we show that ρ_0 is admissible, then $\frac{H}{L}$ forms an upper bound for $\text{Mod}_2(\Gamma)$. To show this consider any $\gamma \in \Gamma$:

$$\int_0^L \frac{1}{L} |\dot{\gamma}(t)| dt \geq \frac{1}{L} \int_0^L |\text{Re } \dot{\gamma}(t)| dt \geq \frac{1}{L} (\text{Re } \gamma(1) - \text{Re } \gamma(0)) \geq 1.$$

This proves the formula for modulus in (1.3).

1.3 Connection to modulus

There are several natural analogs to p-modulus for families of paths on graphs [2, 9, 13, 18] and to more general families of objects including spanning trees. As in the continuum case, modulus provides a quantitative way of describing the richness of a family. Intuitively, modulus will be large for families containing many objects with small pairwise intersections [3, 5]. This can be made more precise through the *minimum expected overlap* formulation of modulus in (2.25), where the goal is to choose random spanning trees that share as few edges as possible on average. This goal is remarkably similar to that of the broadcaster in the game, which motivates the work in this dissertation. The main contribution of this dissertation is

to establish rigorous connections between the solution of the modulus problem on spanning trees and solutions to the broadcast game.

1.4 Outline of the dissertation

This dissertation is organized as follows. Chapter 2 reviews the basic definitions and theorems of p-modulus along with its probabilistic interpretation. Chapter 3 reviews the broadcast game and establishes necessary and sufficient conditions for Nash equilibria. Section 3.2 establishes the connection between the solution to the spanning tree modulus problem and the solution to the broadcast game. Section 3.3 explains some examples and describes the basic modulus algorithm and demonstrates its use in solving the game. Chapter 4 discusses a novel spanning tree modulus algorithm inspired by the secure broadcast game we solved in Chapter 3. Sections from 4.1 to 4.3 describe all the theories that help implementing the algorithm. Then we explain details about the algorithm along with all the other supporting sub-algorithms in Section 4.4. We also compute a time complexity bound for this algorithm and this is the first time that a complexity bound is proved for any existing spanning tree modulus algorithm.

Chapter 2

Modulus on networks

In this chapter we introduce the notion of p-modulus of families of objects on a graph. The Lagrangian duality, and the probabilistic interpretation of the 2-modulus modulus problem which leads to the minimum expected overlap problem (MEO) are also discussed.

In this discussion, $G = (V, E, \sigma)$ is a finite graph with vertex set V, edge set E and edge-weights $\sigma \in \mathbb{R}^E_{>0}$. The graph may be directed or undirected and need not be simple.

2.1 Families of objects

A *family of objects* on G is a pair $(\Gamma, \mathcal{N})$, where Γ is a countable (possibly infinite) index set and $\mathcal{N} \in \mathbb{R}^{\Gamma \times E}_{\geq 0}$ is a non-negative, possibly infinite matrix. Often, Γ alone is referred to as the family and $\mathcal{N}$ is called the *usage matrix* for Γ.

Families of objects used in practice often have a simple interpretation on the graph. For example, it is common to choose $\Gamma \subset 2^E$ and to define the rows of $\mathcal{N}$ as indicator functions.

Example 2.1.1. If Γ is the set of spanning trees of G (thought of as subsets of E), we can define

$$\mathcal{N}(\gamma, e) := \mathbb{1}_\gamma(e)$$

for $\gamma \in \Gamma$ and $e \in E$.

This is the family we shall use in this dissertation, however the theory of modulus applies to more general families of objects.

Example 2.1.2. If a and b are distinct vertices and if Γ is the family of walks in G beginning at a and ending at b, there are many different options for defining $\mathcal{N}$. For example, we could choose any of the following definitions.

- $\mathcal{N}(\gamma, e) = \mathbb{1}_\gamma(e)$,
- $\mathcal{N}(\gamma, e) =$ the number of times γ crosses edge e,
- $\mathcal{N}(\gamma, e) = \ell(\gamma)^{-1}\mathbb{1}_\gamma(e)$ where $\ell(\gamma)$ is the length of γ.

Since our goal in this dissertation is primarily concerned with the modulus of spanning trees, we will assume in the following discussion that the family Γ is finite. We further assume that Γ is *nontrivial* in the sense that $\Gamma \neq \varnothing$ and each object $\gamma \in \Gamma$ has positive usage on at least one edge. (So $\mathcal{N}$ has at least one row, and no row of $\mathcal{N}$ is identically zero.) While $\mathcal{N}$ can be thought of as a function $\mathcal{N} : \Gamma \times E \to \mathbb{R}_{\geq 0}$, it is often notationally convenient to represent $\mathcal{N}$ as a matrix with rows indexed by Γ and columns indexed by E. So the (γ, e) entry keeps a record of the usage of the edge e by the object γ.

2.2 Densities and admissible densities

A *density* on G is a vector $\rho \in \mathbb{R}^E_{\geq 0}$. Choosing a density can be thought of as assigning a cost $\rho(e)$ for the use of each edge e. Each density, ρ, induces a *ρ-length* or *total usage cost* on the family of objects Γ. The ρ-length of $\gamma \in \Gamma$ is defined as

$$\ell_\rho(\gamma) = \sum_{e \in E} \mathcal{N}(\gamma, e)\rho(e) = (\mathcal{N}\rho)(\gamma). \tag{2.1}$$

This is analogous to the ρ-length we defined in the continuum (see (1.1)). The modulus is defined through the minimization of an energy (defined shortly) over a set of admissible

densities. We say that a density ρ is *admissible for* Γ if,

$$\ell_\rho(\gamma) \geq 1 \quad \forall \gamma \in \Gamma, \qquad \text{or, equivalently,} \qquad \mathcal{N}\rho \geq \mathbf{1}, \tag{2.2}$$

where $\mathbf{1}$ is the vector of all ones in $\mathbb{R}^\Gamma$ and the inequality is understood elementwise. Using the latter notation, we define the set of all admissible densities as

$$\operatorname{Adm}\Gamma = \{\rho \in \mathbb{R}^E_{\geq 0} : \mathcal{N}\rho \geq \mathbf{1}\}.$$

An alternative notation that is sometimes useful is to define

$$\ell_\rho(\Gamma) := \min_{\gamma \in \Gamma} \ell_\rho(\gamma). \tag{2.3}$$

So another way of describing the admissible set is,

$$\operatorname{Adm}\Gamma = \{\rho \in \mathbb{R}^E_{\geq 0} : \ell_\rho(\Gamma) \geq 1\}.$$

Example 2.2.1. Let's consider the graph in Figure 1.1. Then the usage matrix $\mathcal{N}$ for the enumeration of the spanning trees in Figure 1.2 is given by

$$\mathcal{N} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Let the density ρ be $[\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}]^T$. Each spaninig tree has $|V| - 1 = 3$ edges. Then the

ρ-length is

$$\ell_\rho(\gamma) = 3 \cdot \frac{1}{3} = 1 \quad \forall \gamma \in \Gamma.$$

Therefore $\rho \in \operatorname{Adm} \Gamma$.

Remark 2.2.1. The length inequality constraints (2.2) are a straightforward translation of the corresponding length constraints from the original theory of conformal modulus in the complex plane. They can be difficult to understand intuitively in the generality of the present discussion, but they have a nice interpretation when the family $\Gamma = \Gamma(s,t)$ is the family of paths connecting two distinct vertices s and t in G and when $\mathcal{N}$ is of the form $\mathcal{N}(\gamma, e) = \mathbb{1}_\gamma(e)$. In this case, $\ell_\rho(\gamma)$ corresponds to the usual concept of path length with edge weights ρ:

$$\ell_\rho(\gamma) = \sum_{e \in E} \mathcal{N}(\gamma, e)\rho(e) = \sum_{e \in \gamma} \rho(e).$$

The interpretation of the admissible set in this case can be found in the proof of [2, Theorem 4.2], though it is not stated quite this way. Namely, $\rho \in \operatorname{Adm} \Gamma(s,t)$ if and only if there exists a vertex potential $\phi : V \to [0,1]$ satisfying

$$\phi(s) = 0, \quad \phi(t) = 1, \quad \text{and} \quad \rho(e) \geq |\phi(x) - \phi(y)| \text{ for all } e = \{x, y\} \in E. \tag{2.4}$$

See also Remark 2.3.1 for further implications of this observation.

2.3 Energy and modulus

Given an exponent $p \geq 1$ we define the *p-energy* of a density ρ as

$$\mathcal{E}_{p,\sigma}(\rho) = \sum_{e \in E} \sigma(e)\rho(e)^p.$$

The 2-energy is analogous to the energy we defined in the continuum (see (1.2)). For $p = \infty$, we also define ∞-energy as

$$\mathcal{E}_{\infty,\sigma}(\rho) = \lim_{p\to\infty} (\mathcal{E}_{p,\sigma^p}(\rho))^{\frac{1}{p}} = \max_{e\in E} \sigma(e)\rho(e).$$

Definition 2.3.1. Given a graph $G = (V, E, \sigma)$, a family of objects Γ with usage matrix $\mathcal{N} \in \mathbb{R}^{\Gamma\times E}$, and an exponent $1 \le p \le \infty$, the p-modulus of Γ is,

$$\mathrm{Mod}_{p,\sigma}(\Gamma) = \inf_{\rho\in \mathrm{Adm}\,\Gamma} \mathcal{E}_{p,\sigma}(\rho).$$

In standard optimization notation, p-modulus is the value of the problem

$$\begin{aligned} \text{minimize} \quad & \mathcal{E}_{p,\sigma}(\rho) \\ \text{subject to} \quad & \mathcal{N}\rho \ge \mathbf{1} \quad \text{and} \quad \rho \ge \mathbf{0} \end{aligned} \tag{2.5}$$

where each object $\gamma \in \Gamma$ determines an inequality constraint. Written in the form of (2.5), it is evident that the modulus problem is an ordinary convex optimization problem; geometrically, it can be described as the problem of finding the distance (in a weighted p-norm) between the closed set $\mathrm{Adm}\,\Gamma$ and the origin. Thus, a minimizer always exists, and uniqueness holds when $1 < p < \infty$ due to the strict convexity of the objective function (see [5]).

Proposition 2.3.1. Let G be a weighted graph, and let Γ be a family of objects on G. For $1 \le p \le \infty$ the following hold:

1. Γ-monotonicity: If $\Gamma \subset \Gamma'$, then $\mathrm{Mod}_{p,\sigma}(\Gamma) \le \mathrm{Mod}_{p,\sigma}(\Gamma')$.

2. Countable subadditivity:

$$\mathrm{Mod}_{p,\sigma}\left(\bigcup_{j=1}^{\infty} \Gamma_j\right) \le \sum_{j=1}^{\infty} \mathrm{Mod}_{p,\sigma}(\Gamma_j).$$

Proof. First, we prove the Γ-monotonicity. Note that if $\Gamma \subset \Gamma'$, then $\mathrm{Adm}\,\Gamma \supset \mathrm{Adm}\,\Gamma'$.

Therefore,

$$\mathrm{Mod}_{p,\sigma}(\Gamma) = \inf_{\rho \in \mathrm{Adm}\,\Gamma} \mathcal{E}_{p,\sigma}(\rho) \leq \inf_{\rho \in \mathrm{Adm}\,\Gamma'} \mathcal{E}_{p,\sigma}(\rho) = \mathrm{Mod}_{p,\sigma}(\Gamma').$$

Now, we prove the countable subadditivity. Assume that $1 \leq p < \infty$ and that $\mathrm{Mod}_{p,\sigma}(\Gamma_j) < \infty$ for all js. Pick $\rho_j \in \mathrm{Adm}\,\Gamma_j$ such that

$$\mathcal{E}_{p,\sigma}(\rho_j) = \mathrm{Mod}_{p,\sigma}(\Gamma_j).$$

Define $\rho := \left(\sum_{j=1}^{\infty} \rho_j^p \right)^{\frac{1}{p}}$, and let $\Gamma = \cup_{j=1}^{\infty} \Gamma_j$. For any $\gamma \in \Gamma$, there is $j \in \mathbb{N}$ such that $\gamma \in \Gamma_j$. Since $\rho \geq \rho_j$, we have $\rho \in \mathrm{Adm}\,\Gamma_j$, and $\ell_\rho(\Gamma) \geq \ell_{\rho_j}(\Gamma) \geq 1$. Therefore $\rho \in \mathrm{Adm}\,\Gamma$ and

$$\begin{aligned}\mathrm{Mod}_{p,\sigma}(\Gamma) \leq \mathcal{E}_{p,\sigma}(\rho) &= \sum_{e \in E} \rho(e)^p \sigma(e) = \sum_{e \in E} \sigma(e) \sum_{j=1}^{\infty} \rho_j(e)^p = \sum_{j=1}^{\infty} \sum_{e \in E} \rho_j(e)^p \sigma(e) \\ &= \sum_{j=1}^{\infty} \mathcal{E}_{p,\sigma}(\rho_j) = \sum_{j=1}^{\infty} \mathrm{Mod}_{p,\sigma}(\Gamma_j).\end{aligned}$$

We interchanged the summations according to Tonelli's Theorem.

Lets consider the $p = \infty$ case now. Similarly as before, pick $\rho_j \in \mathrm{Adm}\,\Gamma_j$ such that

$$\mathcal{E}_{\infty,\sigma}(\rho_j) = \mathrm{Mod}_{\infty,\sigma}(\Gamma_j).$$

Define $\rho := \sup_j \rho_j$. For any $\gamma \in \Gamma$, there is $j \in \mathbb{N}$ such that $\gamma \in \Gamma_j$. Moreover, $\rho \in \mathrm{Adm}\,\Gamma$, and $\max_{e \in E} \rho(e)\sigma(e) \leq \sup_j \max_{e \in E} \rho_j(e)\sigma(e)$. Therefore,

$$\begin{aligned}\mathrm{Mod}_{\infty,\sigma}(\Gamma) \leq \mathcal{E}_{\infty,\sigma}(\rho) = \max_{e \in E} \rho(e)\sigma(e) &= \max_{e \in E} \sup_j \rho_j(e)\sigma(e) \leq \sup_j \max_{e \in E} \rho_j(e)\sigma(e) \\ &= \sup_j \mathrm{Mod}_{\infty,\sigma}(\Gamma_j).\end{aligned}$$

In fact we have the stronger estimate for $p = \infty$ case. □

Theorem 2.3.2. *(Beurling's Criterion for Extremality). Let G be a weighted graph, Γ a family of objects on G, and $p \in (1, \infty)$. Then, a density $\rho \in \mathrm{Adm}\,\Gamma$ is extremal for*

$\mathrm{Mod}_{p,\sigma}(\Gamma)$, *if there is* $\tilde{\Gamma} \subset \Gamma$ *with* $\ell_\rho(\gamma) = 1\ \forall \gamma \in \tilde{\Gamma}$, *i.e.,* $\mathcal{N}(\tilde{\Gamma})\rho = 1$, *such that:*

$$\textit{whenever } h \in \mathbb{R}^E \textit{ and } \mathcal{N}(\tilde{\Gamma})h \geq 0 \textit{ then} \sum_{e\in E} h(e)\rho^{p-1}(e)\sigma(e) \geq 0. \tag{2.6}$$

Furthermore, for such a subfamily $\tilde{\Gamma}$ *we have*

$$\mathrm{Mod}_{p,\sigma}(\tilde{\Gamma}) = \mathrm{Mod}_{p,\sigma}(\Gamma). \tag{2.7}$$

Proof. Let $\tilde{\rho} \in \mathrm{Adm}\,\Gamma$. Set $h := \tilde{\rho} - \rho$. If $\gamma \in \tilde{\Gamma}$, then

$$\ell_h(\gamma) = \ell_{\tilde{\rho}}(\gamma) - \ell_\rho(\gamma) = \ell_{\tilde{\rho}}(\gamma) - 1 \geq 0.$$

By assumption 2.6 we can write

$$\sum_{e\in E} h(e)\rho^{p-1}(e)\sigma(e) = \sum_{e\in E} \tilde{\rho}(e)\rho^{p-1}(e)\sigma(e) - \sum_{e\in E} \rho^p(e)\sigma(e) \geq 0. \tag{2.8}$$

Therefore by Hölder's inequality:

$$\mathcal{E}_{p,\sigma}(\rho) = \sum_{e\in E} \sigma(e)\rho(e)^p \leq \sum_{e\in E} \tilde{\rho}(e)\rho^{p-1}(e)\sigma(e) \leq \Big(\sum_{e\in E} \tilde{\rho}^p(e)\sigma(e)\Big)^{\frac{1}{p}} \Big(\sum_{e\in E} \rho^p(e)\sigma(e)\Big)^{1-\frac{1}{p}}.$$

This yields,

$$\sum_{e\in E} \sigma(e)\rho(e)^p \leq \Big(\sum_{e\in E} \tilde{\rho}^p(e)\sigma(e)\Big)^{\frac{1}{p}} \Big(\sum_{e\in E} \rho^p(e)\sigma(e)\Big)^{1-\frac{1}{p}}. \tag{2.9}$$

Consequently,

$$\Big(\sum_{e\in E} \rho^p(e)\sigma(e)\Big)^{\frac{1}{p}} \leq \Big(\sum_{e\in E} \tilde{\rho}^p(e)\sigma(e)\Big)^{\frac{1}{p}}.$$

Raising to the p-th power of both sides we get that $\mathcal{E}_{p,\sigma}(\rho) \leq \mathcal{E}_{p,\sigma}(\tilde{\rho})$. Thus ρ is extremal. Since $\tilde{\rho}$ is an arbitrary admissible density for Γ we have $\mathrm{Mod}_{p,\sigma}(\Gamma) \leq \mathrm{Mod}_{p,\sigma}(\tilde{\Gamma})$. By monotonicity property of modulus in Proposition 2.3.1 we have the other direction since $\tilde{\Gamma} \subset \Gamma$, thus proving (2.7). □

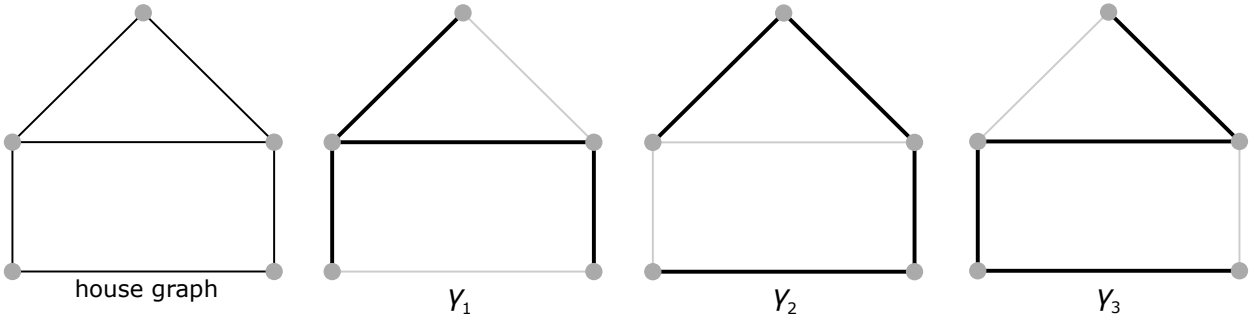


Figure 2.1: Beurling criterion.

Definition 2.3.2. Let Γ be a family of objects on a weighted graph G and $p \in (1, \infty)$. We say that a subfamily $\tilde{\Gamma} \subset \Gamma$ is a *Beurling subfamily* of Γ for $\mathrm{Mod}_{p,\sigma}(\Gamma)$, if $\ell_{\rho^*}(\gamma) = 1 \ \forall \gamma \in \tilde{\Gamma}$ and property (2.6) holds for the extremal density ρ^*. In particular, by (2.7), we always have $\mathrm{Mod}_{p,\sigma}(\tilde{\Gamma}) = \mathrm{Mod}_{p,\sigma}(\Gamma)$.

Example 2.3.1. Consider the house graph in Figure 2.1. Let $\rho = [\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}]^T$. We now test ρ using Beurling's Criterion for the unweighted graph when p=2. Let $\tilde{\Gamma} := \{\gamma_1, \gamma_2\, \gamma_3\}$. Suppose $h \in \mathbb{R}^4$ is such that $\ell_h(\gamma_1) \geq 0$, $\ell_h(\gamma_2) \geq 0$, and $\ell_h(\gamma_3) \geq 0$. So,

$$\begin{aligned}
\sum_{e \in E} h(e)\rho(e) &= \frac{1}{2}\Big(\sum_{e \in \gamma_1} h(e)\rho(e) + \sum_{e \in \gamma_2} h(e)\rho(e) + \sum_{e \in \gamma_3} h(e)\rho(e) \Big) \\
&= \frac{1}{8}\Big(\sum_{e \in \gamma_1} h(e) + \sum_{e \in \gamma_2} h(e) + \sum_{e \in \gamma_3} h(e) \Big) \\
&= \frac{1}{8}\Big(\ell_h(\gamma_1) + \ell_h(\gamma_2) + \ell_h(\gamma_3) \Big) \geq 0
\end{aligned}$$

Hence, by Beurling's Criterion, we can conclude that ρ is extremal for Γ, and $\tilde{\Gamma}$ is a Beurling subfamily. Therefore,

$$\mathrm{Mod}_{2,1}(\tilde{\Gamma}) = \mathrm{Mod}_{2,1}(\Gamma) = \big(\frac{1}{4}\big)^2 \cdot 6 = \frac{3}{8}.$$

In fact, as a consequence of Theorem 2.5.2 and Theorem 3.3.1, by choosing μ to be the uniform pmf on $\tilde{\Gamma}$, we can readily show that $\tilde{\Gamma}$ is a Beurling subfamily.

Since most of this dissertation is focused on the unweighted ($\sigma \equiv 1$), and $p = 2$ case, we

will typically drop the σ from the subscripts above and instead write $\mathcal{E}_2$ and Mod_2 for the energy and modulus respectively. As described in [3], this assumption is not very restrictive since the case of weighted graphs can always be approximated by unweighted multigraphs.

Remark 2.3.1. Continuing with the example $\Gamma = \Gamma(s,t)$ begun in Remark 2.2.1, we again refer to [2, Theorem 4.2] and its proof, wherein $\mathrm{Mod}_{p,\sigma}(\Gamma(s,t))$ is related to the current flow in a resistor network (with nonlinear resistors if $p \neq 2$). The connection arises because from (2.4) we can see that the inequalities should be satisfied as equalities for an optimal density ρ; that is, an optimal density is necessarily defined by a potential drop across the edges. This transforms the modulus problem into a potential problem that is equivalent to the problem of minimizing the dissipated power in a (generally nonlinear) resistor network. In this way, p-modulus can be thought of as a quantity akin to effective conductance wherein the special family $\Gamma(s,t)$ is replaced by a more general family of objects. In the general case, there may not be a meaningful concept of "potential," yet (2.5) still makes sense.

2.4 Lagrangian duality

We have shown before that p-modulus is an ordinary convex optimization problem. When p=2 the convex objective function is a quadratic function. Hence, 2-modulus problem below is a quadratic convex optimization problem.

$$\begin{aligned} \text{minimize} \quad & \mathcal{E}_{2,\sigma}(\rho) \\ \text{subject to} \quad & \mathcal{N}\rho \geq \mathbf{1} \quad \text{and} \quad \rho \geq \mathbf{0} \end{aligned} \tag{2.10}$$

Using the standard techniques from convex optimization, we can define the Lagrangian for this problem as follows.

$$L(\rho, \lambda, \theta) = \mathcal{E}_{2,\sigma}(\rho) + \sum_{\gamma \in \Gamma} \lambda(\gamma) \left(1 - \sum_{e \in E} \mathcal{N}(\gamma, e)\rho(e) \right) - \sum_{e \in E} \theta(e)\rho(e) \tag{2.11}$$

As shown in [2], when $1 \leq p < \infty$, the $\rho \geq 0$ constraints need not be explicitly enforced in (2.10). Therefore, we can omit the dual variable θ from (2.11). So, the simplified Lagrangian is,

$$L(\rho, \lambda) = \sum_{e \in E} \sigma(e)\rho(e)^2 + \sum_{\gamma \in \Gamma} \lambda(\gamma) \left(1 - \sum_{e \in E} \mathcal{N}(\gamma, e)\rho(e) \right). \tag{2.12}$$

This is a differentiable function in $\rho(e)$. Therefore, the value of the dual function $g(\lambda) = \inf_{\rho} L(\rho, \lambda)$ can be found by solving $\nabla_\rho L = 0$. So, by stationarity

$$\begin{aligned} 2\sigma(e)\rho_\lambda(e) - \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\lambda(\gamma) = 0 \\ \rho_\lambda(e) = \frac{1}{2\sigma(e)} \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\lambda(\gamma) \quad \forall e \in E. \end{aligned} \tag{2.13}$$

After plugging this into the Lagrangian

$$L(\rho_\lambda, \lambda) = g(\lambda) = \sum_{\gamma \in \Gamma} \lambda(\gamma) - \sum_{e \in E} \frac{1}{4\sigma(e)} \left(\sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\lambda(\gamma) \right)^2.$$

Therefore Lagrange dual optimization problem is

$$\begin{aligned} \text{maximize} \quad & \sum_{\gamma \in \Gamma} \lambda(\gamma) - \sum_{e \in E} \frac{1}{4\sigma(e)} \left(\sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\lambda(\gamma) \right)^2 \\ \text{subject to} \quad & \lambda(\gamma) \geq 0 \quad \forall \gamma \in \Gamma. \end{aligned} \tag{2.14}$$

Since inequality constraints in (2.10) are affine, it follows from the Theorem 28.2 of [17] that *strong duality* holds. i.e. that the minimum in (2.10) equals the maximum in (2.14). Therefore solving (2.14) is equivalent to computing modulus. Equation (2.13) provides a formula to compute the unique extremal density ρ^* from an extremal λ^*. Typically extremal λ^* are not unique.

2.5 Probabilistic interpretation

The relationship between modulus and secure broadcast games arises from the probabilistic interpretation of modulus developed in [5]. In this interpretation, we consider an object $\underline{\gamma}$ chosen at random according to a probability mass function (pmf) μ. (The underline in the notation $\underline{\gamma}$ is used to distinguish the random object from its possible values.) In other words, for each $\gamma \in \Gamma$, $\mu(\gamma)$ defines the probability that $\underline{\gamma} = \gamma$ or, in simpler notation, $\mu(\gamma) = \mathbb{P}_\mu(\underline{\gamma} = \gamma)$. Here we use the subscript notation $\mathbb{P}_\mu$ to specify exactly which pmf is being used. We will also represent the relationship between the random object $\underline{\gamma}$ and its pmf μ by the notation $\underline{\gamma} \sim \mu$. The set of all pmfs on Γ will be represented with the notation $\mathcal{P}(\Gamma) := \left\{\mu \in \mathbb{R}^\Gamma_{\geq 0} : \mu^T \mathbf{1} = 1\right\}$.

If $e \in E$, $\mu \in \mathcal{P}(\Gamma)$ and $\underline{\gamma} \sim \mu$, then $\mathcal{N}(\underline{\gamma}, e)$ is a real-valued random variable and we denote its expected value with respect to μ as $\mathbb{E}_\mu[\mathcal{N}(\underline{\gamma}, e)]$. That is,

$$\mathbb{E}_\mu[\mathcal{N}(\underline{\gamma}, e)] = \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\mu(\gamma) = (\mathcal{N}^T \mu)(e). \tag{2.15}$$

Thus, $(\mathcal{N}^T\mu)(e)$ represents the *expected usage* of edge e by the random object $\underline{\gamma} \sim \mu$. We will frequently use the variable η to represent the vector $\mathcal{N}^T\mu \in \mathbb{R}^E_{\geq 0}$.

With this notation, we can now summarize the relevant result from [5].

Theorem 2.5.1. *Let $G = (V, E, \sigma)$ be a graph and let Γ be a nontrivial finite family of objects on G with usage matrix $\mathcal{N}$. Then we have,*

$$\mathrm{Mod}_{2,\sigma}(\Gamma)^{-1} = \min_{\mu \in \mathcal{P}(\Gamma)} \sum_{e \in E} \sigma(e)^{-1} \mathbb{E}_\mu[\mathcal{N}(\underline{\gamma}, e)]^2. \tag{2.16}$$

The minimum is always attained and $\mu \in \mathcal{P}(\Gamma)$ is optimal if and only if

$$\mathbb{E}_\mu[\mathcal{N}(\underline{\gamma}, e)] = \frac{\sigma(e)\rho^*(e)}{\mathrm{Mod}_{2,\sigma}(\Gamma)}, \tag{2.17}$$

where ρ^* is the unique extremal density for $\mathrm{Mod}_{2,\sigma}(\Gamma)$.

Proof. By decomposing λ as $\lambda = \nu\mu$ with $\nu \geq 0$ and $\mu \in \mathcal{P}(\Gamma)$, we can rewrite (2.14) as

$$\max_{\nu \geq 0} \left\{ \nu - \left(\frac{\nu^2}{4}\right) \min_{\mu \in \mathcal{P}(\Gamma)} \sum_{e \in E} \sigma(e)^{-1} \left(\sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\mu(\gamma) \right)^2 \right\}. \tag{2.18}$$

The minimum over μ in (2.18) can be recognized as the minimum in (2.16). Let α be this minimum value. Then we can rewrite (2.18) as

$$\max_{\nu \geq 0} \quad \nu - \left(\frac{\nu^2}{4}\right)\alpha. \tag{2.19}$$

The maximum is attained when $\nu = \nu^* = 2/\alpha$, and strong duality implies that

$$\mathrm{Mod}_{2,\sigma}(\Gamma) = \nu^* - \left(\frac{\nu^{*^2}}{4}\right)\alpha = \frac{1}{\alpha}.$$

Thus,

$$\mathrm{Mod}_{2,\sigma}(\Gamma)^{-1} = \alpha = \min_{\mu \in \mathcal{P}(\Gamma)} \sum_{e \in E} \sigma(e)^{-1} \left(\sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\mu(\gamma) \right)^2 = \min_{\mu \in \mathcal{P}(\Gamma)} \sum_{e \in E} \sigma(e)^{-1} \mathbb{E}_{\mu}[\mathcal{N}(\underline{\gamma}, e)]^2.$$

From (2.13)

$$\begin{aligned} \rho^*(e) &= \frac{1}{2\sigma(e)} \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\lambda^*(\gamma) = \frac{1}{2\sigma(e)} \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\nu^*\mu^*(\gamma) \\ &= \frac{1}{\alpha\sigma(e)} \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\mu^*(\gamma) = \frac{\mathrm{Mod}_{2,\sigma}(\Gamma)}{\sigma(e)} \mathbb{E}_{\mu^*}[\mathcal{N}(\underline{\gamma}, e)] \quad \forall e \in E. \end{aligned} \tag{2.20}$$

Thus, proving (2.17). □

This probabilistic interpretation has a simple meaning under the assumptions that G is unweighted (i.e., $\sigma \equiv 1$), Γ is a collection of subsets of E, and $\mathcal{N}$ is a matrix of 0's and 1's (i.e., $\mathcal{N}(\gamma, e)$ is defined through indicator functions as in Example 2.1.1). Since $\mathcal{N}$ is a $(0,1)$-matrix, $\mathcal{N}(\underline{\gamma}, e)$ is an indicator random variable for the event $e \in \underline{\gamma}$. In this case, the

expected usage

$$\eta(e) := \mathbb{E}_\mu[\mathcal{N}(\underline{\gamma}, e)] = (\mathcal{N}^T\mu)(e) \tag{2.21}$$

in Equations (2.15) and (2.16) is actually a probability of inclusion

$$\eta(e) = \mathbb{P}_\mu(e \in \underline{\gamma}). \tag{2.22}$$

Moreover, the summation in the right-hand side of (2.16) can be rewritten as

$$\begin{aligned}\sum_{e\in E}\eta(e)^2 &= \sum_{e\in E}\left(\sum_{\gamma\in\Gamma}\mathcal{N}(\gamma,e)\mu(\gamma)\right)\left(\sum_{\gamma'\in\Gamma}\mathcal{N}(\gamma',e)\mu(\gamma')\right)\\ &= \sum_{\gamma\in\Gamma}\sum_{\gamma'\in\Gamma}\left(\sum_{e\in E}\mathcal{N}(\gamma,e)\mathcal{N}(\gamma',e)\right)\mu(\gamma)\mu(\gamma')\\ &= \sum_{\gamma\in\Gamma}\sum_{\gamma'\in\Gamma}|\gamma\cap\gamma'|\mu(\gamma)\mu(\gamma') =: \mathbb{E}_\mu|\underline{\gamma}\cap\underline{\gamma'}|.\end{aligned} \tag{2.23}$$

Here $\underline{\gamma}, \underline{\gamma'} \sim \mu$ are two independent Γ-valued random variables. The quantity $|\underline{\gamma} \cap \underline{\gamma'}|$ is the intersection (overlap) of these two random sets and is, therefore, an integer-valued random variable with expectation $\mathbb{E}_\mu|\underline{\gamma} \cap \underline{\gamma'}|$. This latter quantity is called the *expected overlap* of $\underline{\gamma}$ and $\underline{\gamma'}$.

Using (2.23), the probabilistic interpretation (2.16) can be expressed as follows.

$$\mathrm{Mod}_2(\Gamma)^{-1} = \min_{\mu\in\mathcal{P}(\Gamma)} \mathbb{E}_\mu|\underline{\gamma}\cap\underline{\gamma'}|. \tag{2.24}$$

Thus, computing 2-modulus in this case is equivalent to finding a pmf that minimizes the expected overlap of two i.i.d. Γ-valued random variables. The right-hand side of (2.24) is called the *minimum expected overlap* (MEO) problem:

$$\begin{aligned}\text{minimize} \quad & \mathbb{E}_\mu|\underline{\gamma}\cap\underline{\gamma'}|\\ \text{subject to} \quad & \mu \in \mathcal{P}(\Gamma).\end{aligned} \tag{2.25}$$

When μ^* is optimal for the MEO problem (2.25), we define $\eta^* = \mathcal{N}^T \mu^*$. By (2.17),

$$\eta^*(e) = \mathbb{P}_{\mu^*}(e \in \underline{\gamma}) = \mathbb{E}_{\mu^*}[\mathcal{N}(\underline{\gamma}, e)] = \frac{\rho^*(e)}{\mathrm{Mod}_2(\Gamma)}. \tag{2.26}$$

Since ρ^* is unique, so is η^*. In general, however, the pmf μ^* is non-unique.

Theorem 2.5.2. *Let $\tilde{\Gamma} = \operatorname{supp} \mu^*$. Then $\tilde{\Gamma}$ is a Beurling subfamily, i.e. satisfies Beurling's criterion for ρ^*. Namely:*

(a) $\ell_{\rho^*}(\gamma) = 1 \ \forall \gamma \in \tilde{\Gamma}$ and

(b) for every $h \in \mathbb{R}^E$ with $\ell_h(\gamma) \geq 0 \ \forall \gamma \in \tilde{\Gamma}$ we have $\sum_{e \in E} h(e)\rho^*(e) \geq 0$.

Proof. Part (a) follows from complementary slackness. To prove Part (b) first we write η^* for $\tilde{\Gamma}$.

$$\eta^*(e) = \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\mu^*(\gamma) = \sum_{\gamma \in \tilde{\Gamma}} \mathcal{N}(\gamma, e)\mu^*(\gamma).$$

$$\begin{aligned} \sum_{e \in E} h(e)\eta^*(e) = \sum_{e \in E} h(e) \sum_{\gamma \in \tilde{\Gamma}} \mathcal{N}(\gamma, e)\mu^*(\gamma) &= \sum_{\gamma \in \tilde{\Gamma}} \mu^*(\gamma) \sum_{e \in E} h(e)\mathcal{N}(\gamma, e) \\ &= \sum_{\gamma \in \tilde{\Gamma}} \mu^*(\gamma)\ell_h(\gamma) \geq 0. \end{aligned}$$

Since $\eta^*(e)$ and $\rho^*(e)$ are parallel according to (2.26), it follows that

$$\sum_{e \in E} h(e)\rho^*(e) \geq 0.$$

□

Example 2.5.1. Consider the paw graph shown in Figure 2.2, with edges enumerated as indicated. This graph has 3 spanning trees: $\Gamma = \{\gamma_1, \gamma_2, \gamma_3\}$. The pairwise overlaps among these trees satisfy

$$|\gamma_i \cap \gamma_j| = \begin{cases} 3 & \text{if } i = j, \\ 2 & \text{otherwise.} \end{cases}$$

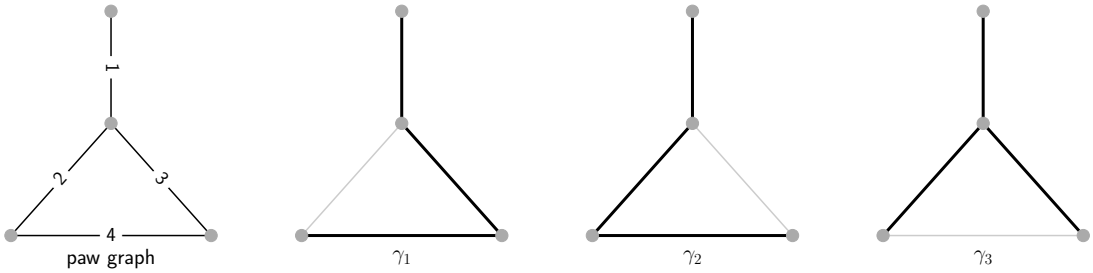


Figure 2.2: Spanning trees of the paw graph.

Let the density ρ take the value $3/7$ on edge 1 and $2/7$ on other edges. This density is admissible. Thus, its energy $\rho^T\rho = 3/7$ forms an upper bound for $\mathrm{Mod}_2(\Gamma)$.

On the other hand, let $\mu \in \mathcal{P}(\Gamma)$ be the uniform distribution. Then the expected overlap is,

$$\mathbb{E}_\mu|\underline{\gamma} \cap \underline{\gamma'}| = 3\mathbb{P}_\mu(\underline{\gamma} = \underline{\gamma'}) + 2\mathbb{P}_\mu(\underline{\gamma} \neq \underline{\gamma'}) = 3 \cdot \frac{1}{3} + 2 \cdot \frac{2}{3} = \frac{7}{3},$$

which forms an upper bound for $\mathrm{Mod}_2(\Gamma)^{-1}$ by (2.24). That is,

$$\frac{3}{7} = \frac{1}{\mathbb{E}_\mu|\underline{\gamma} \cap \underline{\gamma'}|} \leq \mathrm{Mod}_2(\Gamma) \leq \rho^T\rho = \frac{3}{7}.$$

Therefore,

$$\mathrm{Mod}_2(\Gamma) = 3/7,$$

and ρ and μ are optimal for their corresponding minimization problems.

Example 2.5.2. Consider the graph in Figure 1.1. This graph has 8 spanning trees, as shown in Figure 2.3. To derive an upper bound on $\mathrm{Mod}_2(\Gamma)$, observe that $\rho \equiv 1/3$ is an admissible density. Therefore,

$$\mathrm{Mod}_2(\Gamma) \leq \mathcal{E}_2(\rho) = \frac{5}{9}. \tag{2.27}$$

Now, consider the pmf $\mu \in \mathcal{P}(\Gamma)$ defined as

$$\mu(\gamma) = \begin{cases} \frac{3}{20} & \text{if } \gamma \text{ contains the diagonal,} \\ \frac{2}{20} & \text{otherwise.} \end{cases}$$

Let e_d be the diagonal edge. Since there are four spanning trees containing e_d,

$$\eta(e_d) = 4 \cdot \frac{3}{20} = \frac{3}{5}.$$

For all other edges, $e \neq e_d$

$$\begin{aligned} \eta(e) &= \mathbb{P}_\mu(e \in \underline{\gamma}) = \mathbb{P}_\mu(e \in \underline{\gamma} | e_d \in \underline{\gamma}) \mathbb{P}_\mu(e_d \in \underline{\gamma}) + \mathbb{P}_\mu(e \in \underline{\gamma} | e_d \notin \underline{\gamma}) \mathbb{P}_\mu(e_d \notin \underline{\gamma}) \\ &= \frac{1}{2}\left(4 \cdot \frac{3}{20}\right) + \frac{3}{4}\left(4 \cdot \frac{2}{20}\right) = \frac{3}{5}. \end{aligned}$$

With this pmf, all edges are equally likely to occur in $\underline{\gamma}$: $\eta(e) = 3/5$ on all edges. Therefore the expected overlap is, by (2.23),

$$\mathbb{E}_\mu |\underline{\gamma} \cap \underline{\gamma}'| = \sum_{e \in E} \eta(e)^2 = 5\left(\frac{3}{5}\right)^2 = \frac{9}{5} \geq \mathrm{Mod}_2(\Gamma)^{-1},$$

which forms a lower bound for $\mathrm{Mod}_2(\Gamma)$. This together with the upper bound (2.27) shows that both bounds are attained.

Although the optimal vectors ρ^* and η^* are unique, the optimal pmf μ^* need not be. In Section 1.1, we described another pmf, namely

$$\mu = \frac{2}{5}\delta_{\gamma_1} + \frac{1}{5}\delta_{\gamma_5} + \frac{1}{5}\delta_{\gamma_6} + \frac{1}{5}\delta_{\gamma_8}.$$

It is straightforward to verify that this pmf also has the property that $\mathbb{P}_\mu(e \in \underline{\gamma}) = 3/5$ for each edge e and is therefore optimal.

The uniform pmf $\mu \equiv 1/8$, on the other hand, is not optimal in this case, since $\eta(e_d) = 1/2$

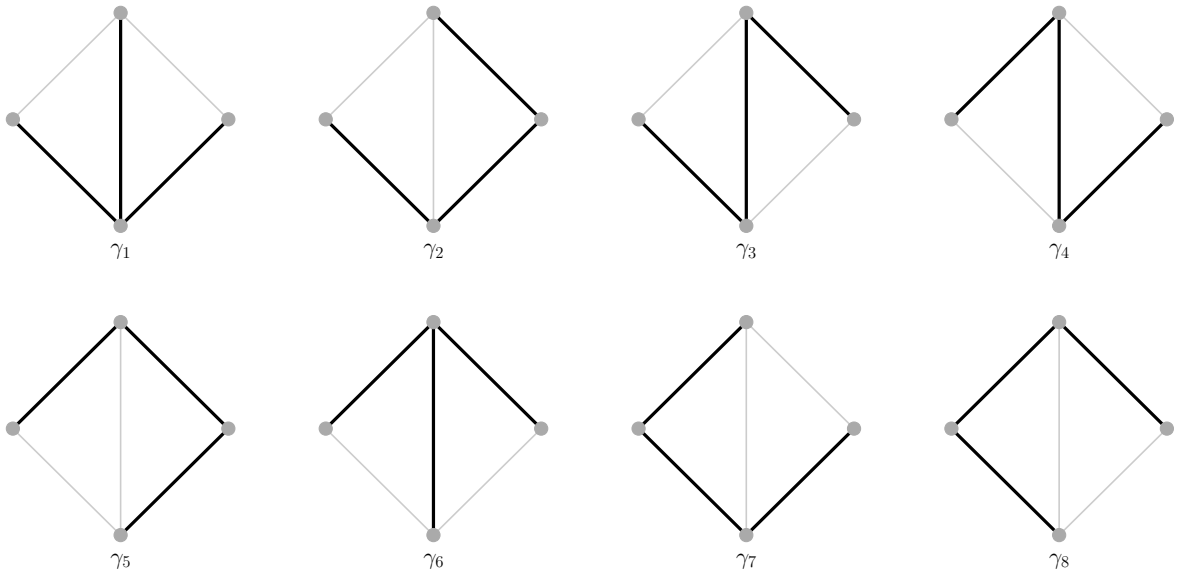


Figure 2.3: Spanning trees of the diamond graph.

while for all other edges $e \neq e_d$, $\eta(e) = 5/8$. For the uniform pmf, then, the expected overlap is

$$\mathbb{E}_\mu|\underline{\gamma} \cap \underline{\gamma'}| = \sum_{e \in E} \eta(e)^2 = \left(\frac{1}{2}\right)^2 + 4\left(\frac{5}{8}\right)^2 = \frac{29}{16} > \frac{9}{5}.$$

2.6 Detailed example

In this section we derive the spanning tree modulus and extremal density of the cycle+triangle graph given in Figure 2.4 for $n = |V| \geq 6$. These graphs are an example for non-homogeneous graphs we briefly discuss in Section 3.3.1 and they are widely discussed in [3].

First, note that the cycle+triangle graph has $n + 1$ edges. Consider ρ as in Figure 2.4, taking one value, ρ_1, on the edges of the triangle and a generally different value, ρ_2, on the remaining edges. As shown in Figure 2.5, there are only two possible ρ-lengths for the spanning trees of this graph. Spanning trees obtained from the removal of two edges from the triangle have length $\rho_1 + (n-2)\rho_2$, while trees obtained by removing one edge from the triangle have length $2\rho_1 + (n-3)\rho_2$. Hence, an upper bound for $\mathrm{Mod}_2(\Gamma)$ can be found by

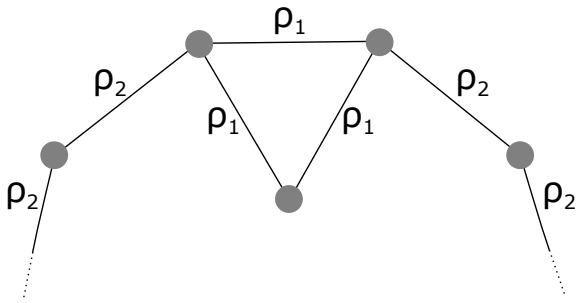
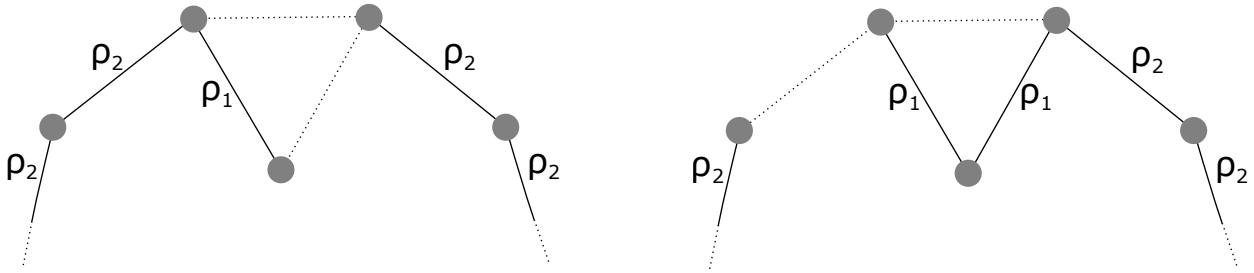


Figure 2.4: cycle+triangle graph with ρ.



(a) Spanning tree type 1

(b) Spanning tree type 2

Figure 2.5: Spanning trees of different ρ-lengths for the cycle+triangle graph. Dashed edges are the edges removed to obtain spanning trees.

solving the following quadratic convex optimization problem.

$$\begin{aligned} \textbf{minimize} \quad & 3\rho_1^2 + (n-2)\rho_2^2 \\ \textbf{subject to} \quad & \rho_1 + (n-2)\rho_2 \geq 1 \\ & 2\rho_1 + (n-3)\rho_2 \geq 1 \end{aligned}$$

The Lagrangian is,

$$L(\rho, \lambda, \beta) = 3\rho_1^2 + (n-2)\rho_2^2 + \lambda(1 - \rho_1 - (n-2)\rho_2) + \beta(1 - 2\rho_1 - (n-3)\rho_2).$$

From complementary slackness we have

$$\lambda(1 - \rho_1 - (n-2)\rho_2) = 0, \quad \beta(1 - 2\rho_1 - (n-3)\rho_2) = 0. \tag{2.28}$$

From Stationarity we can write

$$6\rho_1 - \lambda - 2\beta = 0, \quad 2(n-2)\rho_2 - (n-2)\lambda - (n-3)\beta = 0. \tag{2.29}$$

If $\lambda, \beta > 0$, Equation (2.28) implies,

$$1 - \rho_1 - (n-2)\rho_2 = 0, \quad 1 - 2\rho_1 - (n-3)\rho_2 = 0 \implies \rho_1 = \rho_2 = \frac{1}{(n-1)}.$$

Hence, from Equation (2.29),

$$\lambda + 2\beta = \frac{6}{n-1}, \quad (n-2)\lambda + (n-3)\beta = \frac{2(n-2)}{n-1}. \tag{2.30}$$

Solving the above yields,

$$\beta = \frac{4(n-2)}{(n-1)^2}, \quad \lambda = \frac{2(5-n)}{(n-1)^2}.$$

We clearly see that when $n \geq 6$, λ can no longer be non-negative. Hence, dual feasibility fails. In other words, $\rho_1 = \rho_2 = \dfrac{1}{(n-1)}$ only works when $n \leq 5$. (cycle+triangle graphs when $n \leq 5$ are an example for homogeneous graphs we discuss in Section 3.3.1.) Therefore, one of the dual variables must be zero when $n \geq 6$. If $\beta = 0$, it leads to a failure in the primal feasibility. So, we should choose $\lambda = 0$. Therefore, again from (2.29) we can write

$$6\rho_1 = 2\beta, \quad 2(n-2)\rho_2 = (n-3)\beta \implies \rho_2 = \frac{3(n-3)}{2(n-2)}\rho_1.$$

Plugging into Equation (2.28) yields,

$$\rho_1 = \frac{2(n-2)}{4(n-2) + 3(n-3)^2} \text{ and } \rho_2 = \frac{3(n-3)}{4(n-2) + 3(n-3)^2}.$$

Since we have restricted our attention to a particular subset of densities (those taking two distinct values, as shown in Figure 2.4), the energy of this density is an upper bound

for the $\mathrm{Mod}_2(\Gamma)$ since it is admissible. Therefore,

$$\begin{aligned}\mathrm{Mod}_2(\Gamma) &\leq 3\left[\frac{2(n-2)}{4(n-2)+3(n-3)^2}\right]^2 + (n-2)\left[\frac{3(n-3)}{4(n-2)+3(n-3)^2}\right]^2 \\ &= \frac{3(n-2)}{4(n-2)+3(n-3)^2}.\end{aligned}$$

To complete the proof, we will show that the value on the right-hand side above is also a lower bound for the modulus.

From the probabilistic interpretation of the modulus we know that any choice of pmf μ provides a lower bound on the modulus as follows.

$$\mathrm{Mod}_2(\Gamma) \geq (\mu^T \mathcal{N}\mathcal{N}^T \mu)^{-1}$$

In particular, consider the pmf that selects uniformly from the subset of spanning trees formed by removing a single edge from the triangle and the other edge from outside the triangle. There are $3(n-2)$ such trees, so μ gives probability $\frac{1}{3(n-2)}$ to each of these and probability 0 to the rest. i.e., to those formed by removing two edges from the triangle.

Let $\tilde{\mathcal{N}}$ be the usage matrix of the spanning trees without the trees formed by removing two edges from the triangle. So, we have,

$$\mu^T \mathcal{N}\mathcal{N}^T \mu = \frac{\mathbf{1}^T \tilde{\mathcal{N}}\tilde{\mathcal{N}}^T \mathbf{1}}{[3(n-2)]^2} = \frac{1}{[3(n-2)]^2}\|\tilde{\mathcal{N}}^T \mathbf{1}\|_2^2. \tag{2.31}$$

Pick an enumeration on edges as in Figure 2.6. Then,

$$\tilde{\mathcal{N}}^T \mathbf{1} = \begin{bmatrix} 2(n-2) & 2(n-2) & 2(n-2) & 3(n-3) & \dots & 3(n-3) \end{bmatrix}^T.$$

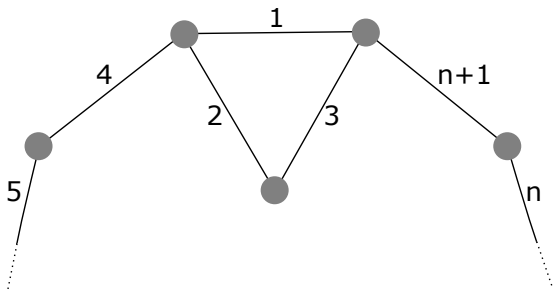


Figure 2.6: Enumeration on edges.

Plugging in to Equation (2.31) yields,

$$\mu^T \mathcal{N}\mathcal{N}^T \mu = \frac{3[2(n-2)]^2 + (n-2)[3(n-3)]^2}{[3(n-2)]^2} = \frac{3(n-2)[4(n-2)+3(n-3)^2]}{[3(n-2)]^2}$$
$$= \frac{[4(n-2)+3(n-3)^2]}{[3(n-2)]}.$$

Now we have,

$$\frac{3(n-2)}{4(n-2)+3(n-3)^2} = \rho^T \rho \geq \mathrm{Mod}_2(\Gamma) \geq \left(\mu^T \mathcal{N}\mathcal{N}^T \mu\right)^{-1} = \frac{3(n-2)}{4(n-2)+3(n-3)^2}.$$

Thus,

$$\mathrm{Mod}_2(\Gamma) = \frac{3(n-2)}{4(n-2)+3(n-3)^2},$$

and, in fact, ρ and μ are optimal for their respective minimization problems. The edge usage probability η^* is given as

$$\mathbb{P}_{\mu^*}(e \in \underline{\gamma}) = \frac{\rho^*(e)}{\mathrm{Mod}_2(\Gamma)} = \begin{cases} 2/3 & \text{for edges whose density is } \rho_1^*, \\ \dfrac{n-3}{n-2} & \text{for edges whose density is } \rho_2^*. \end{cases}$$

Chapter 3

Secure broadcast games

This chapter introduces a two-person zero sum game between a broadcaster and an eavesdropper in a communication network. First we prove necessary and sufficient conditions for the existence of pure and mixed strategy equilibria. Then we discuss how the solution to the spanning tree modulus problem can provide a solution to this game through the concept of feasible partitions. After that, some bounds for the value of the game are proved, and a comparison between the 1-modulus solution and 2-modulus solution is also provided. Some examples along with the effect of adding edges are given at the end of the chapter.

3.1 A secure broadcast game

When addressing secure broadcasting (or network security in general) a game-theoretic approach is natural due to the rich set of mathematical tools that this approach provides. In this section, we consider the solution of the secure broadcast game described in Section 1.1. We show that the solution to the spanning tree modulus problem provides a Nash equilibrium for the game.

To more carefully define the game, let $G = (V, E)$ be a simple, connected graph rep-

resenting a communications network and let Γ be the family of spanning trees on G. The game between **B** (the broadcaster) and **E** (the eavesdropper) proceeds as follows. Player **B** broadcasts a message by sending it along a spanning tree $\gamma \in \Gamma$. Player **E** eavesdrops by choosing a single edge $e \in E$ on which to listen. **E** wins if $e \in \gamma$. Otherwise, **B** wins. If we consider this a zero-sum game, we may assume without loss of generality that the payoff matrix P is equal to $\mathcal{N}$. That is, **E** wishes to maximize $\mathcal{N}(\gamma, e)$ while **B** wishes to minimize it. Written in this way, it is evident that a pure-strategy solution to the game generally does not exist. In fact, the following theorem gives necessary and sufficient conditions on the existence of a pure-strategy equilibrium.

Theorem 3.1.1. *A pure-strategy equilibrium to the secure broadcast game exists if and only if G is 1-edge-connected (that is, if there exists an edge $e \in E$ whose removal would disconnect the graph).*

Proof. First, suppose that such an edge e exists. Necessarily, this edge exists in every spanning tree and, thus, $\mathcal{N}(\gamma, e) = 1$ for all $\gamma \in \Gamma$. **E** wins by selecting this edge. Since **E** can force a win, this provides a pure-strategy equilibrium to the game.

Now, suppose that G is at least 2-edge-connected. Assume that **B** plays first, by choosing a tree $\gamma \in \Gamma$. Then **E** wins by choosing any $e \in \gamma$. On the other hand, assume that **E** plays first by choosing an edge $e \in E$. Let G' be the subgraph of G obtained by removing e. By assumption, G' is connected, so there exists a spanning tree $\gamma \in \Gamma$ that is also a spanning tree of G'. **B** wins by selecting this tree. Since neither player can force a win in this case, there is no pure-strategy equilibrium. □

In light of Theorem 3.1.1, a Nash equilibrium for the secure broadcast game will generally involve mixed strategies. Here we recast the game using probability notation in order to make the connection to modulus more apparent. More precisely, we suppose that **B** chooses a pmf $u \in \mathcal{P}(\Gamma)$ while **E** chooses a pmf $v \in \mathcal{P}(E)$. This is equivalent to **B** choosing a random tree $\underline{\gamma} \sim u$ while **E** chooses a random edge $\underline{e} \sim v$. The expected payoff for a particular choice of

strategies, then, is given by

$$\mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] := \sum_{\gamma \in \Gamma} \sum_{e \in E} \mathcal{N}(\gamma, e) u(\gamma) v(e). \tag{3.1}$$

This quantity has a number of useful interpretations. For example, if we define $\eta := \mathcal{N}^T u = \mathbb{P}_u(\cdot \in \underline{\gamma})$ as in (2.22), then

$$\mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] = \sum_{e \in E} \eta(e) v(e) = \mathbb{E}_v[\eta(\underline{e})]. \tag{3.2}$$

That is, the expected payoff is equal to the expected value of η on an edge randomly selected according to the distribution v. On the other hand, if we use the definition of $\ell_v(\gamma)$ in (2.1), then

$$\mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] = \sum_{\gamma \in \Gamma} \ell_v(\gamma) u(\gamma) = \mathbb{E}_u[\ell_v(\underline{\gamma})]. \tag{3.3}$$

With this interpretation, the expected payoff is the expected v-length of a random spanning tree chosen according to the distribution u. Equations (3.2) and (3.3) provide a useful way of looking at necessary and sufficient conditions for solving the game. We begin by reviewing the relevant concepts in the present context.

First, recall that a pair of mixed strategies $(u^*, v^*) \in \mathcal{P}(\Gamma) \times \mathcal{P}(E)$ *solves* the game (in the sense of Nash equilibrium [16]) if the following condition holds.

$$\mathbb{E}_{u^*,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] \leq \mathbb{E}_{u^*,v^*}[\mathcal{N}(\underline{\gamma}, \underline{e})] \leq \mathbb{E}_{u,v^*}[\mathcal{N}(\underline{\gamma}, \underline{e})] \qquad \forall u \in \mathcal{P}(\Gamma)\ \forall v \in \mathcal{P}(E). \tag{3.4}$$

Alternatively, we can express (3.4) as

$$\max_{v \in \mathcal{P}(E)} \mathbb{E}_{u^*,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] = \mathbb{E}_{u^*,v^*}[\mathcal{N}(\underline{\gamma}, \underline{e})] = \min_{u \in \mathcal{P}(\Gamma)} \mathbb{E}_{u,v^*}[\mathcal{N}(\underline{\gamma}, \underline{e})]. \tag{3.5}$$

This form is particularly enlightening when paired with the max-min inequality, which states

that for a general real-valued function f on a product space $X \times Y$,

$$\sup_{y \in Y} \inf_{x \in X} f(x, y) \leq \inf_{x \in X} \sup_{y \in Y} f(x, y).$$

When applied to the problem at hand, the max-min inequality becomes

$$\max_{v \in \mathcal{P}(E)} \min_{u \in \mathcal{P}(\Gamma)} \mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] \leq \min_{u \in \mathcal{P}(\Gamma)} \max_{v \in \mathcal{P}(E)} \mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma}, \underline{e})]. \tag{3.6}$$

Nash's existence theorem [16] guarantees a mixed-strategy solution to the game and, therefore, that the inequality in (3.6) is satisfied as equality. These observations lead to the following theorem.

Theorem 3.1.2. *Let $u \in \mathcal{P}(\Gamma)$ and $v \in \mathcal{P}(E)$ and define*

$$\eta = \mathcal{N}^T u \qquad \text{and} \qquad \ell_v(\Gamma) = \min_{\gamma \in \Gamma} \ell_v(\gamma).$$

Then (u, v) solves the game if and only if

$$\ell_v(\Gamma) \geq \|\eta\|_\infty. \tag{3.7}$$

Moreover, if (u, v) solves the game, then

$$\operatorname{supp} u \subseteq \{\gamma \in \Gamma : \ell_v(\gamma) = \ell_v(\Gamma)\} \tag{3.8}$$

and

$$\operatorname{supp} v \subseteq \{e \in E : \eta(e) = \|\eta\|_\infty\}. \tag{3.9}$$

Proof. From (3.2), we have

$$\max_{v \in \mathcal{P}(E)} \mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma}, \underline{e})] = \max_{v \in \mathcal{P}(E)} \mathbb{E}_v[\eta(\underline{e})] = \|\eta\|_\infty.$$

Similarly, by (3.3),

$$\min_{u\in\mathcal{P}(\Gamma)} \mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma},\underline{e})] = \min_{u\in\mathcal{P}(\Gamma)} \mathbb{E}_{u}[\ell_v(\underline{\gamma})] = \ell_v(\Gamma).$$

Substituting these two expressions into (3.5) shows that an equilibrium is characterized by the equality

$$\|\eta\|_\infty = \ell_v(\Gamma).$$

Moreover, substituting into the max-min inequality (3.6) shows that

$$\max_{v\in\mathcal{P}(E)} \ell_v(\Gamma) \le \min_{u\in\mathcal{P}(\Gamma)} \|\eta\|_\infty. \tag{3.10}$$

Thus, (3.7) is necessary and sufficient to characterize an equilibrium.

The additional necessary conditions (3.8) and (3.9) are a consequence of (3.5). Let (u, v) be an equilibrium point and let $\eta = \mathcal{N}^T u$. Then, (3.5) implies that

$$\|\eta\|_\infty = \mathbb{E}_{u,v}[\mathcal{N}(\underline{\gamma},\underline{e})] = \mathbb{E}_{v}[\eta(\underline{e})]. \tag{3.11}$$

This equality can only hold if v is supported on edges where η attains its maximum, establishing (3.9). A similar argument establishes (3.8). □

Remark 3.1.1. As can be seen in the proof, the inequality in (3.7) can be replaced with equality, since the opposite inequality is established in (3.10). Retaining the inequality sign in the theorem allows for slightly simpler arguments such as in the proof of Theorem 3.2.2 below.

Remark 3.1.2. Theorem 3.1.1 can also be seen as a corollary of Theorem 3.1.2. Indeed, if $\gamma \in \Gamma$ and $e \in E$ then the pure strategies $u = \delta_\gamma \in \mathcal{P}(\Gamma)$ and $v = \delta_e \in \mathcal{P}(E)$ have the properties that

$$\|\eta\|_\infty = 1 \qquad \text{and} \qquad \ell_v(\gamma') = \mathcal{N}(\gamma', e) \quad \forall \gamma' \in \Gamma.$$

Thus, by (3.7) in Theorem 3.1.2, the pair (u, v) solves the game if and only if $e \in \gamma'$ for every

$\gamma' \in \Gamma$, that is, if and only if e is a "bridge" in the graph.

Theorem 3.1.2 can be understood by formulating the involved quantities as probabilities. Namely,

$$\eta(e) = \mathbb{P}_u(e \in \underline{\gamma}) \quad \text{and} \quad \ell_v(\gamma) = \mathbb{P}_v(\underline{e} \in \gamma).$$

In words, η assigns to each edge the probability that this edge will be in the random tree selected by **B** while ℓ_v assigns to each spanning tree the probability that the random edge selected by **E** will appear in that tree. Suppose each player announces her strategy to the other. If **B** announces first (by choosing $u \in \mathcal{P}(\Gamma)$), **E** then knows η and will choose an edge where η is maximized. If **E** announces first (by choosing $v \in \mathcal{P}(E)$), then **B** knows ℓ_v and will choose a tree where ℓ_v is minimized. The usual game-theoretic interpretation of the max-min inequality (that the first player is weaker) shows that (3.10) must hold, so the opposite inequality (3.7) is both necessary and sufficient for an equilibrium solution.

Relations (3.8) and (3.9) have similarly intuitive interpretations. If **B** knows **E**'s strategy, then **B** will only select trees with minimum probability of intersecting **E**'s edge. On the other hand, if **E** knows **B**'s strategy, then **E** will only select edges with maximum probability of occurring in **B**'s tree. In an equilibrium solution (wherein each player may know the other's strategy), both (3.8) and (3.9) must hold.

3.2 Using modulus to solve the game

Now, we show that the solution to the spanning tree modulus problem provides a solution to the game. The connection is made through the concept of feasible partitions, as defined in [7].

Definition 3.2.1. A *feasible partition* Q of a graph $G = (V, E)$ is a partition of the vertex set V into $k_Q > 1$ pieces: $Q = \{V_1, V_2, \ldots, V_{k_Q}\}$ such that the subgraph of G induced by V_i is connected for each $i = 1, 2, \ldots, k_Q$. The edge set $E_Q \subseteq E$ of Q is the set of all edges of E that connect distinct pieces of the partition. The *weight* $w(Q)$ of Q is defined as $w(Q) = |E_Q|/(k_Q - 1)$. In the case $k_Q = 2$, the definition of a feasible partition coincides

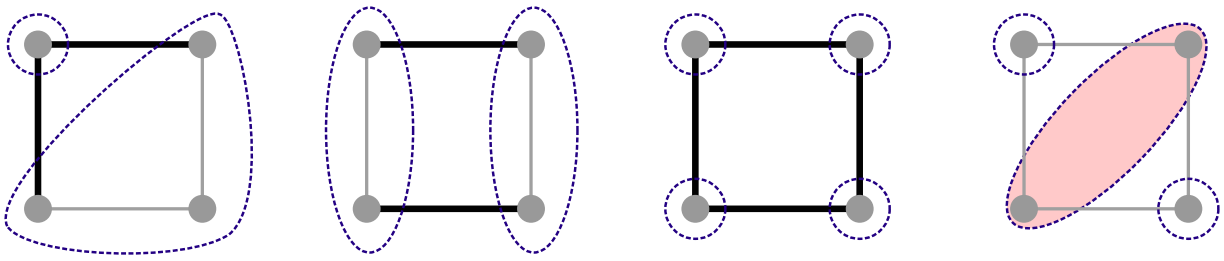


Figure 3.1: The leftmost three figures show feasible partitions of the vertex set (separated by dashed curves) of the cycle graph C_4. The associated edge sets E_P are shown with darkened edges. The final figure (on the right) shows a partition of the vertex set that is *not* a feasible partition. The shaded set of two vertices does not induce a connected subgraph.

with the definition of a global graph cut and $w(Q) = |E_Q|$ is the usual definition of the weight of such a cut. We denote by $\mathcal{F}(G)$ the set of all feasible partitions of G.

Note that, due to the connectedness requirement, not every partition of V yields a feasible partition. Figure 3.1 shows three examples of feasible partitions on C_4 along with a vertex partition that is not feasible. Since the trivial partition (third in the figure) that separates V into singleton subsets is always feasible, every connected graph on $n \geq 2$ vertices has at least one feasible partition.

An important relationship between spanning trees and feasible partitions arises from the fact that, for a given feasible partition Q and spanning tree γ, the spanning tree must connect all pieces of the partition, yielding the inequality (see [7, (2.2)])

$$|\gamma \cap E_Q| \geq k_Q - 1. \tag{3.12}$$

The relationship between modulus and the secure broadcast game is provided by the following theorem, proved in [3].

Theorem 3.2.1. *Let Γ be the family of spanning trees on the graph $G = (V, E)$ and let $\mu^* \in \mathcal{P}(\Gamma)$ be optimal for the MEO problem (2.25), with expected edge usage $\eta^* = \mathcal{N}^T \mu^*$. Define*

$$E_{Q^*} := \{e \in E : \eta^*(e) = \|\eta^*\|_\infty\}.$$

Then E_{Q^*} is the edge set for a feasible partition Q^* of V into $k_{Q^*} > 1$ pieces and has the following three properties.

$$|\gamma \cap E_{Q^*}| = k_{Q^*} - 1 \quad \forall \gamma \in \text{supp } \mu^*, \tag{3.13}$$

$$\eta^*(e) = \|\eta^*\|_\infty = w(Q^*)^{-1} \quad \forall e \in E_{Q^*}, \tag{3.14}$$

$$w(Q^*) = \min_{Q \in \mathcal{F}(G)} w(Q). \tag{3.15}$$

This provides the solution to the secure broadcast game as follows.

Theorem 3.2.2. *Using the definitions from Theorem 3.2.1, let $u^* = \mu^* \in \mathcal{P}(\Gamma)$ and let $v^* \in \mathcal{P}(E)$ be the uniform distribution on E_{Q^*}. Then (u^*, v^*) is a Nash equilibrium solution to the game. Moreover,*

$$\mathbb{E}_{u^*,v^*}[\mathcal{N}(\underline{\gamma}, \underline{e})] = \|\eta^*\|_\infty = w(Q^*)^{-1}. \tag{3.16}$$

Proof. In order to verify that the given mixed strategies solve the game, we use Theorem 3.1.2, which shows that it is sufficient to establish that (3.7) holds. Equation (3.14) establishes the second equality in (3.16). Let $\gamma \in \Gamma$ be any spanning tree. Then, since Q^* is a feasible partition, (3.12) shows that

$$\ell_{v^*}(\gamma) = \sum_{e \in E} \mathcal{N}(\gamma, e) v^*(e) = \frac{1}{|E_{Q^*}|} \sum_{e \in E_{Q^*}} \mathcal{N}(\gamma, e) = \frac{|\gamma \cap E_{Q^*}|}{|E_{Q^*}|} \geq \frac{k_{Q^*} - 1}{|E_{Q^*}|} = w(Q^*)^{-1} = \|\eta^*\|_\infty.$$

Taking the minimum with respect to $\gamma \in \Gamma$ establishes (3.7). The first equality in (3.16) then follows from (3.11). □

Remark 3.2.1. Although it was not formulated in the present game-theoretic notation, Cunningham [8] studied the quantity $w(Q^*)$ in (3.14), which he called the *strength* of G.

Remark 3.2.2. For general graphs, the solution (u^*, v^*) given by Theorem 3.2.2 need not be the only Nash equilibrium of the game. An example is given in Section 3.3.1 of a relatively simple graph for which **B** has a 5-parameter family of optimal strategies and **E** has a 1-

parameter family of optimal strategies. This nonuniqueness of solution appears to be general; to our knowledge, a simple characterization of graphs which admit a unique Nash equilibrium has not been found.

3.2.1 Bounds

In light of (3.16), bounds on the minimum feasible partition problem (3.15) immediately provide bounds on the value of the secure broadcast game. As an example, the following theorem establishes a bound on the game in terms of the edge connectivity, $\lambda(G)$, which is defined to be the minimum number of edges whose removal from G disconnects G. That is,

$$\lambda(G) := \min\{|E'| : E' \subseteq E \text{ and } G' = (V', E \setminus E') \text{ is disconnected}\}.$$

Theorem 3.2.3. *Let $G = (V, E)$ be a connected graph with edge connectivity $\lambda(G)$ and let Q^* be as defined in Theorem 3.2.1. Then*

$$w(Q^*) \leq \min\left\{\lambda(G), \frac{|E|}{|V| - 1}\right\}.$$

Proof. Since the edge connectivity of G is $\lambda(G)$, there must be a set of edges E' such that $|E'| = \lambda(G)$ and removing E' from G disconnects G into multiple connected components. Let G' be the graph obtained by removing the edges E' from G. The connected components of G' produce a partition of the vertex set $Q = \{V_1, V_2, \ldots, V_{k_Q}\}$ with each V_i corresponding to one of the connected components of G'. By construction, if $e \in E_Q$, then e must connect vertices in different parts of the partition and, thus, in different components of G'. Therefore, such an edge must also lie in E'. Therefore, $E_Q \subseteq E'$.

Since G' is disconnected, it follows that $k_Q \geq 2$ and, by definition that $|E_Q| \geq \lambda(G) = |E'|$. This implies that $E_Q = E'$. Finally, we claim that $k_Q = 2$. To see this, suppose instead that $k_Q > 2$ and let e be an arbitrary edge in E_Q. Adding this edge to G' would result in a graph with $k_Q - 1 \geq 2$ connected components. Thus, removing the set $E_Q \setminus \{e\}$ from G would disconnect the graph, but $|E_Q \setminus \{e\}| < \lambda(G)$, which is a contradiction.

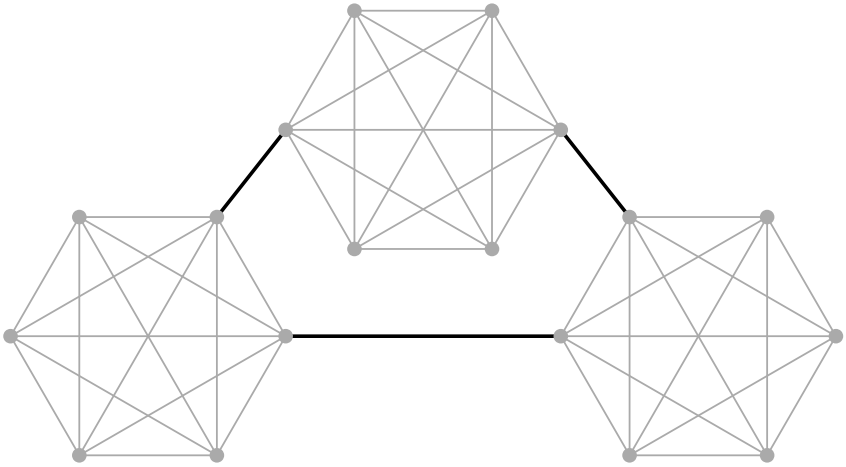


Figure 3.2: Example showing the strictness of the connectivity bound from Theorem 3.2.3.

This shows that the set E' must be the edge set for a feasible partition Q with $k_Q = 2$ and, therefore,

$$w(Q^*) \leq w(Q) = \frac{|E'|}{1} = \lambda(G).$$

Next, note that the trivial partition Q which separates each vertex into its own part is always feasible. In this case, the edge set $E_Q = E$ and $k_Q = |V|$. By (3.15), it follows that

$$w(Q^*) \leq w(Q) = \frac{|E|}{|V| - 1}.$$

□

For general graphs, neither bound is attained. Consider, for example, the graph in Figure 3.2. For this graph, $\lambda(G) = 2$ since one can disconnect the graph by removing any two of the three highlighted edges. **E**, therefore, can ensure a win at least 1/2 of the time by choosing between these two edges uniformly at random. However, **E** can also do much better. The three highlighted edges in this case are E_{Q^*}. Since **B** is forced to use at least two of these three edges in order to broadcast the message through the network, **E** can guarantee a win with probability at least 2/3 by selecting uniformly at random among all three edges. The best **B** can do to counter this strategy is to randomly select spanning trees that use

exactly two of the three highlighted edges and to do so in a way that makes each of these edges equally likely to appear in the tree. On the other hand, if $k_{Q^*} = 2$ then it follows that Q^* defines a graph cut and, therefore, that $w(Q^*) = \lambda(G)$.

Similarly, the bound obtained from the trivial partition is not generally attained; it is only attained for a special class of graphs, the *homogeneous graphs*, discussed in Section 3.3.2.

3.2.2 1-modulus versus 2-modulus

Above, we have given a method for solving the broadcast game using the solution of a 2-modulus problem. The solution given in [11, Theorem 2], on the other hand, is equivalent to the solution of the corresponding 1-modulus problem. Indeed, the Lagrangian dual to the 1-modulus problem is (see [2, Equation (7)])

$$\begin{aligned} \text{maximize} \quad & \mathbf{1}^T\lambda \\ \text{subject to} \quad & \mathcal{N}^T\lambda \leq \mathbf{1}, \lambda \geq \mathbf{0}. \end{aligned} \tag{3.17}$$

The connection between (3.17) and [11, Equation (16)] can be made through the probabilistic interpretation of modulus [5]. The primary difference between (3.17) and the optimization problem of [11] is one of scaling: λ is a maximizer of (3.17) if and only if $\lambda/(\mathbf{1}^T\lambda)$ is a maximizer for [11, Equation (16)]. Thus, although [11] does not explicitly use the vocabulary of modulus, we will refer to this method of solving the game as the 1-modulus approach.

While conceptually similar, the 1-modulus and 2-modulus approaches to the game have some significant differences. The 1-modulus approach involves first finding a *critical subset of edges* (essentially, finding Q^*). This provides the value of the game as well as an optimal strategy for **E**. Although not explicitly described in the paper, an optimal strategy for **B** would presumably then be found by solving the linear program [11, Equation (16)]. Recently in [20] the value of the game and strategies of both players were discussed in a more general matroid setting using a different approach.

A 2-modulus approach to solving the game, on the other hand, proceeds by first finding the optimal ρ^* for (2.5) by using an exterior-point algorithm as described in [5]. The edges

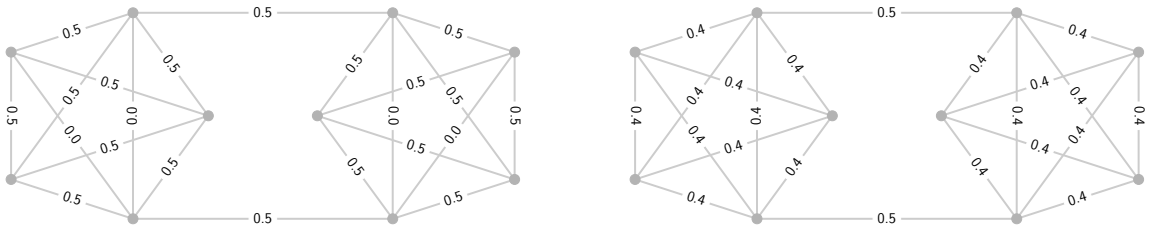


Figure 3.3: On the left, one possible choice of $\eta^*_\infty = \mathcal{N}^T \mu^*_\infty$ for the 1-modulus problem, on the right, the unique $\eta^* = \mathcal{N}^T \mu^*$ for the 2-modulus problem.

of Q^* are then readily obtained by locating the edges on which ρ^* is maximized, giving an optimal strategy for **E**. Although the algorithm described only provides an approximation $\rho' \approx \rho^*$ to within some specified tolerance, it is nevertheless possible to determine Q^* exactly by using a consequence of the *deflation process* described in [3]. Namely that the value $\rho^*(e)/\operatorname{Mod}_2(\Gamma)$ is a proper fraction on every edge with denominator bounded by $|E|$. Thus, by selecting a suitably small tolerance, one can determine on exactly which edges ρ^* is maximized by considering the edges on which ρ' is approximately maximized.

Moreover, the optimal dual variables λ^* can be rescaled to produce an optimal μ^* as described above, thus giving an optimal strategy for **B** with no additional work. This is particularly effective on larger graphs with large numbers of spanning trees; by using an exterior-point approach, one typically only needs to explore a tiny fraction of the constraints in order to get an accurate solution.

Another interesting aspect of the difference between the 1-modulus and 2-modulus approaches to the game is the fact that the 2-modulus problem is more restrictive; a 2-modulus solution will also be a 1-modulus solution, but not the other way around. A simple illustration of this idea can be seen in the following example.

Consider the graph shown in Figure 3.3, formed by connecting two copies of K_5 by two bridges. Since at least one of the two bridges must be used in any spanning tree, the value of the secure broadcast game must be at least $1/2$. An optimal strategy for **B** can be constructed as follows. Let γ_1 and γ_2 be the disjoint spanning trees of G shown in Figure 3.4. If μ is the pmf that chooses between these two trees with $1/2$ probability each, then the maximum

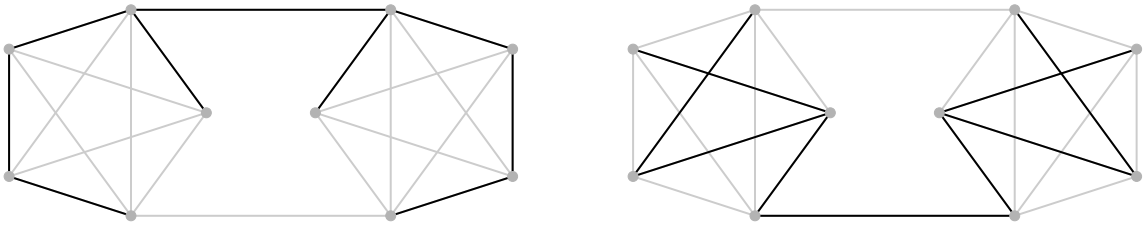


Figure 3.4: A pair of disjoint spanning trees, γ_1 and γ_2.

expected edge usage is $1/2$, attained on the edges of $\gamma_1 \cup \gamma_2$, as shown on the left of Figure 3.3. The optimal strategy for **E** is to choose between the two bridge edges uniformly.

On the other hand, consider the 2-modulus solution. In this case, even though the optimal pmf μ^* may not be unique, the optimal expected edge usage η^* is. These values are shown on the right of Figure 3.3. Observe that, following this strategy, **B** uses each non-bridge edge only $2/5$ of the time.

The difference between the two solutions can be understood through the probabilistic interpretation of modulus. The 1-modulus approach corresponds to finding a pmf μ and corresponding expected edge usage vector $\eta = \mathcal{N}^T \mu$ that minimizes $\|\eta\|_\infty$. The 2-modulus approach, on the other hand, corresponds to minimizing the variance of η (see [3]). Both options shown in Figure 3.3 minimize the maximum value, but only the one on the right minimizes the variance.

3.3 Examples

In this section, we demonstrate the connection between modulus and the broadcast game with a few illustrative examples.

3.3.1 The house graph

As a simple example of the theory developed above, consider the broadcast game on the house graph shown in Figure 3.5. We shall demonstrate how the theory of modulus can be

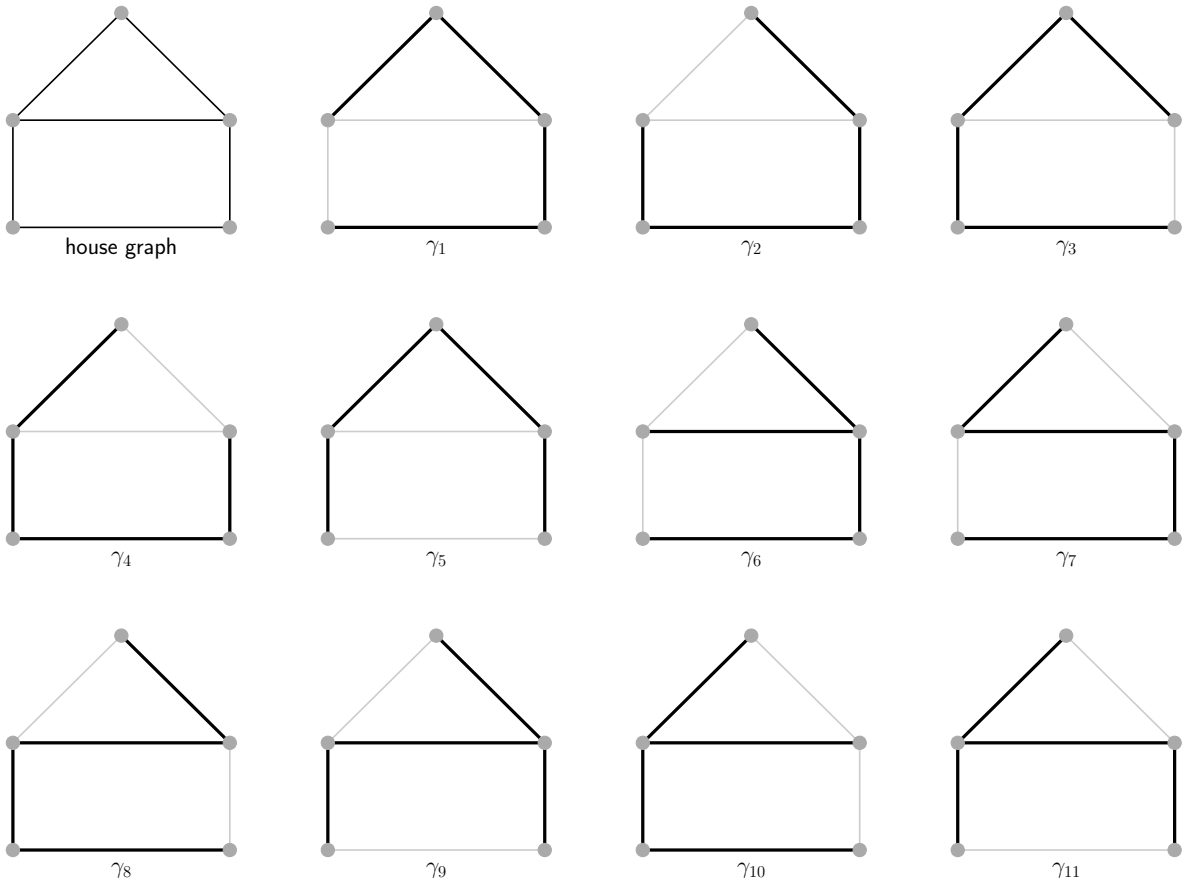


Figure 3.5: The house graph and its spanning trees.

used to solve the secure broadcast game, using the theory developed in [3]. We begin with a definition of the concept of a homogeneous graph.

Definition 3.3.1. A graph G is said to be *homogeneous* (with respect to spanning tree modulus) if the unique edge usage probability vector $\eta^* = \mathcal{N}^T \mu^*$ is constant (i.e., parallel to the vector $\mathbf{1}$). A graph that is not homogeneous is called *nonhomogeneous*.

Homogeneous graphs play a special role in the theory of spanning tree modulus; they essentially form a collection of "atoms" into which any graph can be decomposed. The reader is directed to [3] for details. Here, we reproduce one important theorem [3, Corollary 4.5]

Theorem 3.3.1. *A graph G is homogeneous if an only if there exists a pmf $\mu \in \mathcal{P}(\Gamma)$ so that $\mathbb{P}_\mu(e \in \underline{\gamma})$ is independent of $e \in E$. If such a pmf exists, it is optimal for the MEO problem (2.25) and*

$$\mathbb{P}_\mu(e \in \underline{\gamma}) = \frac{|V| - 1}{|E|}.$$

Proof. See [3, Corollary 4.5]. □

To see how this theorem applies in the case of the house graph, first note that the graph has 5 vertices and 6 edges, so $(|V| - 1)/|E| = 2/3$. If we can find a pmf μ that gives every edge a $2/3$ probability of inclusion in the random tree $\underline{\gamma}$, then Theorem 3.3.1 proves the optimality of μ. In fact, there are infinitely many such μ in this case. For example, using the enumeration of spanning trees in Figure 3.5, consider the pmf μ that selects uniformly among the three trees γ_1, γ_9 and γ_{10}. It is straightforward to verify that each edge appears in exactly two of these three trees and, therefore, that $\mathbb{P}_\mu(e \in \underline{\gamma}) = 2/3$ for this choice of μ.

Once one optimal pmf μ^* is found, the set of all optimal pmfs can be expressed as the polyhedron

$$\left\{ z \in \mathbb{R}^\Gamma : \mathcal{N}^T z = 0, \quad \mathbf{1}^T z = 0, \quad \mu^* + z \geq 0 \right\}.$$

For the house graph, this polyhedron can be shown to have six vertices, each of the form $\mu = \frac{1}{3}\left(\delta_{\gamma_i} + \delta_{\gamma_j} + \delta_{\gamma_k}\right)$. In other words, the polyhedron of optimal pmfs is generated by six pmfs, each of which is uniformly distributed on a set of three spanning trees. These six sets

are

$$\{\gamma_1, \gamma_9, \gamma_{10}\}, \{\gamma_1, \gamma_8, \gamma_{11}\}, \{\gamma_5, \gamma_7, \gamma_8\}, \{\gamma_3, \gamma_6, \gamma_{11}\}, \{\gamma_3, \gamma_7, \gamma_9\}, \text{ and } \{\gamma_5, \gamma_6, \gamma_{10}\}.$$

It is interesting to note that two spanning trees, γ_2 and γ_4, are absent from these sets. In other words, neither γ_2 nor γ_4 is in the support of any optimal pmf. These two trees are examples of the *forbidden trees* defined in [3]. There are several ways to see why such forbidden trees might exist in general. Here, we provide a proof specific to the house graph.

Theorem 3.3.2. *If $\mu \in \mathcal{P}(\Gamma)$ is optimal for the MEO problem (2.25) on the house graph, then*

$$\operatorname{supp} \mu \subset \Gamma \setminus \{\gamma_2, \gamma_4\},$$

using the spanning tree enumeration given in Figure 3.5.

Proof. As observed above, the pmf $\mu = \frac{1}{3}(\delta_{\gamma_1} + \delta_{\gamma_9} + \delta_{\gamma_{10}})$ has the property that $\mathbb{P}_\mu(e \in \underline{\gamma}) \equiv 2/3$. By Theorem 3.3.1, then, the house graph is homogeneous and μ is optimal for the MEO problem. By the uniqueness of η^* in (2.17), it follows that *every* optimal pmf has uniform edge usage probabilities equal to 2/3. Let μ be any optimal pmf and let $E' \subset E$ be the top three edges of the house graph (the roof and ceiling). Observe that

$$|\gamma \cap E'| = \begin{cases} 1 & \text{if } \gamma \in \{\gamma_2, \gamma_4\}, \\ 2 & \text{if } \gamma \in \Gamma \setminus \{\gamma_2, \gamma_4\}. \end{cases}$$

So,

$$\begin{aligned} 3 \cdot \frac{2}{3} = 2 = \sum_{e \in E'} \eta^*(e) &= \sum_{e \in E'} \sum_{\gamma \in \Gamma} \mathcal{N}(\gamma, e)\mu(\gamma) = \sum_{\gamma \in \Gamma} \mu(\gamma) \sum_{e \in E'} \mathcal{N}(\gamma, e) = \sum_{\gamma \in \Gamma} \mu(\gamma)|\gamma \cap E'| \\ &= 2\left(\sum_{\gamma \in \Gamma} \mu(\gamma)\right) - \mu(\gamma_2) - \mu(\gamma_4) = 2 - \mu(\gamma_2) - \mu(\gamma_4). \end{aligned}$$

This is only possible if $\mu(\gamma_2) = \mu(\gamma_4) = 0$. □

As stated in Remark 3.2.2, this shows that **B**'s optimal strategy in this case is nonunique; there is a 5-parameter family of strategies for the broadcaster. Similarly, **E**'s optimal strategy is not unique. Let $\theta \in [0,1]$ and define $v \in \mathcal{P}(E)$ so that v takes the value $(1-\theta)/6$ on the top triangle of the house graph and the value $(1+\theta)/6$ on the bottom three edges. We can verify that (u,v) chosen in this way is a Nash equilibrium through the necessary and sufficient condition in Theorem 3.1.2. **B**'s optimal strategies all result in $\eta \equiv 2/3$. Moreover, for all spanning trees γ other than the two forbidden trees, $\ell_v(\gamma) = (1-\theta)/3+(1+\theta)/3 = 2/3$ while, on the two forbidden trees, $\ell_v(\gamma_2) = \ell_v(\gamma_4) = (1-\theta)/6+(1+\theta)/2 = 2/3+\theta/3 \geq 2/3$.

3.3.2 Other homogeneous graphs

A consequence of the connection between modulus and the broadcast game is that the value of the game on a homogeneous graph is $(|V|-1)/|E|$. This is interesting because homogeneity can sometimes be established without an explicit construction of an optimal pmf. Take, for example, the complete graph K_n. From the symmetry of the graph, it is straightforward to show that the optimal density ρ^* for the modulus problem is uniform and, therefore, so is η^*. While it is possible to construct an optimal pmf for K_n (for example, choose a vertex uniformly at random and take the star of edges incident upon this vertex), we can use homogeneity to establish that the value of the broadcast game on K_n is $2/n$.

Similarly, consider an arbitrary connected d-regular graph. In [3], it was shown that almost every such graph is homogeneous. Thus, it follows that the value of the broadcast game on almost every d-regular graph is $\frac{2(|V|-1)}{d|V|}$. Unlike in the case of K_n, it is not as immediately evident how to construct an optimal pmf for an arbitrary d-regular graph.

3.3.3 The effect of adding edges

As a final example, we consider the effect that adding edges has on the value of the game. To begin, consider the graph shown in the upper left corner of Figure 3.6, formed by connecting a copy of K_5 to a copy of K_6 by a single bridge. This is an example of a 1-connected graph considered in Theorem 3.1.1. Since every spanning tree must use the bridge, the value of

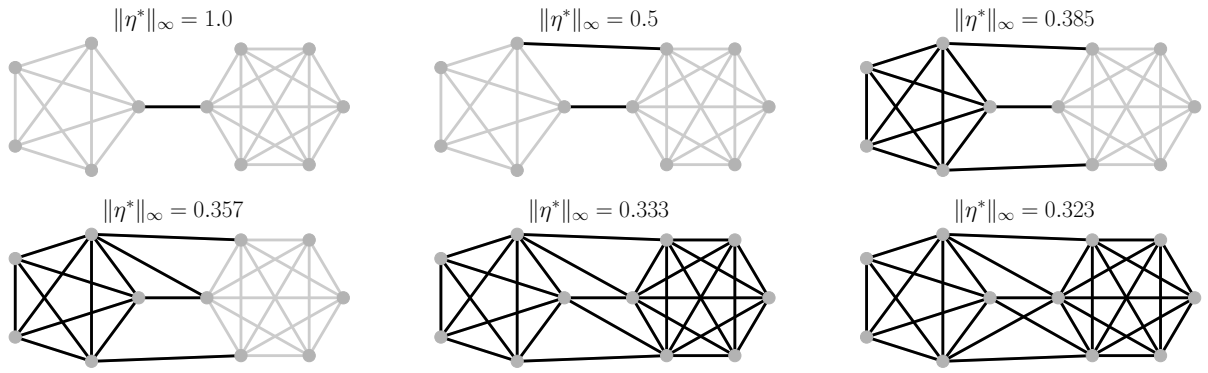


Figure 3.6: The maximum value of η^* (associated with 2-modulus) for a sequence of graphs. The darkened edges show where η^* attains its maximum.

the game is 1 (**E** always wins).

The top middle portion of the figure shows the effect of adding an additional bridge between the two complete components. In this case, the broadcaster is forced to use at least one of these two bridges. The solution to the game involves the broadcaster choosing trees that use *exactly* one of the bridges in such a way that each bridge is used half the time. The eavesdropper chooses among the two edges uniformly, giving a 50% chance that the eavesdropper will intercept the broadcast.

One might expect that adding a third bridge (the top right portion of the figure) would result in a game with value 1/3 (the broadcaster chooses trees that use exactly one of the three bridges and the eavesdropper chooses uniformly among the three edges). However, this pair of strategies is not optimal. Indeed, if **B** were to choose this strategy, then every spanning tree selected by **B** would restrict as a spanning tree to the K_5 component and, therefore, would use 4 of the 10 edges there. So **E** could win 40% of the time by choosing uniformly among the edges of the K_5 component. In the solution shown, the broadcaster is able to choose a random tree that performs better than this. The eavesdropper is forced to choose uniformly among a larger set of edges (the 13 darker edges) and will win only 38.5% of the time. In this case, the minimum feasible partition consists of placing all nodes of the K_6 component into a single part and separating each node of K_5 into its own part. This gives a partition Q with $k_Q = 6$ and $|E_Q| = 13$, so $w(Q)^{-1} = 5/13 \approx 0.3846$. When run on

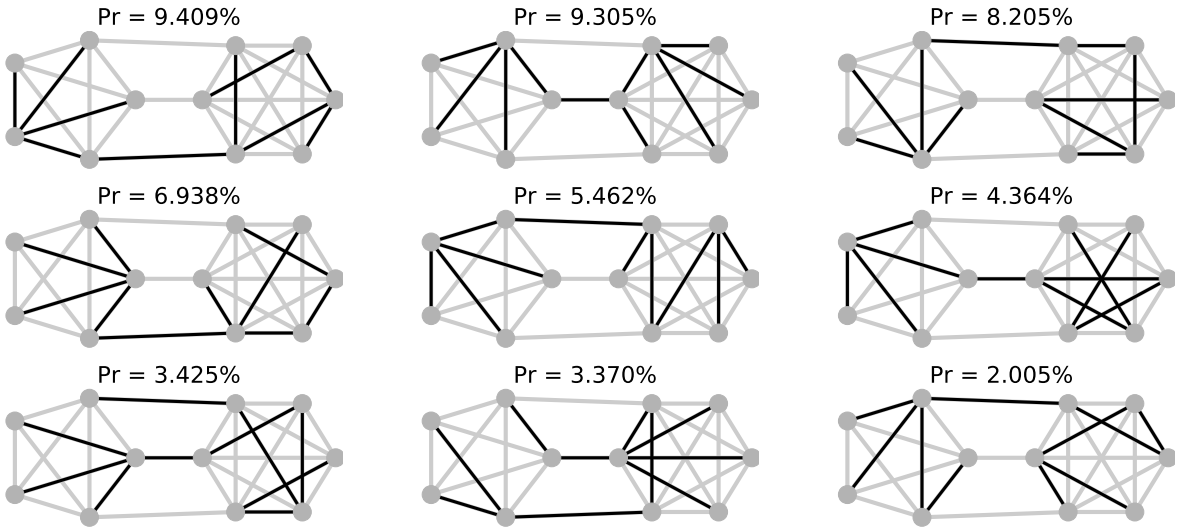


Figure 3.7: Nine spanning trees with largest value of μ^*.

this example, the modulus algorithm from [5] produces an optimal pmf μ^* supported on 23 trees. An optimal strategy for **B**, therefore, is to choose from among those 23 spanning trees according to the pmf μ^*. Figure 3.7 shows the first 9 spanning trees ordered according to the value of optimal pmf μ^*. Observe that the spanning trees shown always restrict as spanning trees of the K_6 component. This is a consequence of the fact that the K_6 subgraph, in this case, is a homogeneous core as described in [3]. On the other hand, the trees in the figure do not, in general, restrict as trees of the K_5 subgraph (which would require only one of the three bridge edges to be present). Indeed, the third row shows spanning trees that use two of the three bridges. Some of the lower-probability trees (not shown in the figure) even use all three bridges.

Adding a fourth bridge has a similar effect (bottom left portion of the figure). Upon adding a fifth bridge, the graph become homogeneous; the minimum feasible partition is the trivial one, separating each node into its own part. For this partition $k_Q = 11$, $|E_Q| = 30$ and $w(Q)^{-1} = 1/3$.

For comparison we have shown $\|\eta_0\|_\infty$ from the uniform pmf μ_0 in Figure 3.8. Again, we start with the graph in the upper left corner of Figure 3.8. Since every spanning tree has to use the bridge the expected edge usage is 1 on that edge, and **E** wins by listening there.

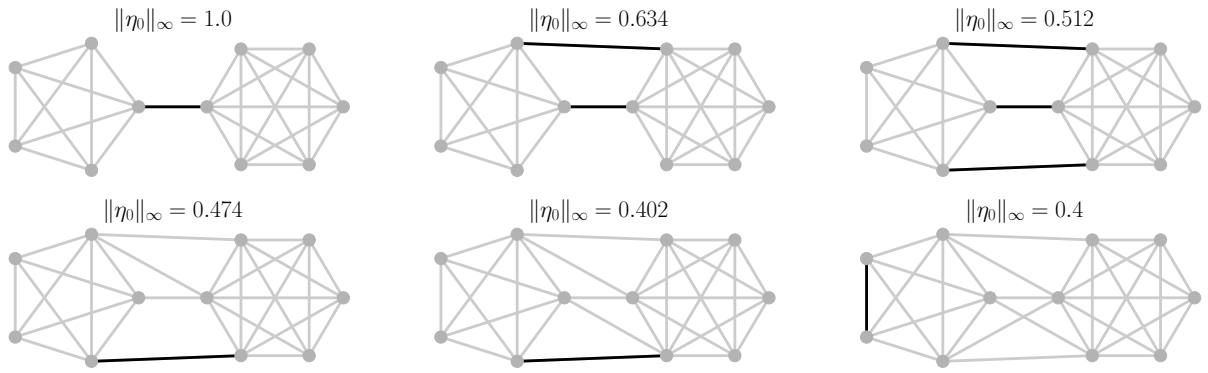


Figure 3.8: The maximum value of η_0 (associated with the uniform pmf μ_0) for a sequence of graphs. The darkened edges show where η_0 attains its maximum.

When a second edge is added, a broadcaster choosing uniformly among spanning trees will overuse the two bridges, sometimes picking trees that use both. (Compare this with the optimal strategy for $\mathbf{B}$ described above.) By the time a third bridge is added, the difference between the uniform and optimal strategies is striking. The uniform broadcaster uses each of the three bridges over half the time while the optimal broadcaster, by optimally using the minimum feasible partition, forces the eavesdropper to choose among 13 edges, each used no more than 38.5% of the time.

A key observation here is that choosing uniformly among spanning trees does not guarantee an even distribution of edge usage. Consider, for example, the bottom right portion of the figure. From the previous figure, we know it is possible for $\mathbf{B}$ to ensure that all edges are equally likely to occur. However, the uniform distribution uses one edge (the far left one) more than any other edge.

Chapter 4

An algorithm for computing spanning tree modulus

In this chapter we introduce a new algorithm to compute spanning tree modulus based on the secure broadcast game we solved in the previous chapter. This chapter is structured as follows. We start by defining graph vulnerability, a value which turns out to be equal to the value of the game $\|\eta^*\|_\infty$ from Chapter 3, and show a method to compute $\|\eta^*\|_\infty$ along with an edge set $E_{\tilde{Q}} \subseteq \{e \in E : \eta^*(e) = \|\eta^*\|_\infty\}$. This set of edges is the edge set for a minimum feasible partition $\tilde{Q}$, which we show is also a critical set in the context of graph vulnerability. This method involves transforming the graph vulnerability problem into a minimization problem which includes the rank function associated with the graphic matroid of G, and then reduces it to one of polymatroid bases. After a suitable modification to an existing greedy algorithm to work with integer arithmetic, we compute graph vulnerability exactly and find a critical subset of edges. We continue recursively solving the game on subgraphs until no edges are left and $\eta^*(e)$ values are found for all edges. Finally we estimate an overall worst-case time complexity bound for this algorithm.

Before making the connection to modulus we discuss some mathematical tools we need to implement the algorithm.

4.1 Graph vulnerability

Let $G = (V, E)$ be a connected undirected graph with at least one edge, and let Γ be the family of spanning trees. In this chapter we use a notation similar to that of Cunningham [8] and Gueye [11].

Definition 4.1.1. For $J \subseteq E$, define

$$\mathcal{M}(J) := \min_{\gamma \in \Gamma} |\gamma \cap J| \quad \text{and} \quad \theta(J) := \begin{cases} \frac{\mathcal{M}(J)}{|J|} & \text{if } J \neq \emptyset, \\ 0 & \text{if } J = \emptyset. \end{cases} \tag{4.1}$$

The quantity $\mathcal{M}(J)$ is the minimum possible overlap between the edge set J and any spanning tree of G. The value $\theta(J)$ is called the *vulnerability* of J. The *vulnerability* of the graph G, $\theta(G)$, is the maximum vulnerability of subsets of its edges. That is

$$\theta(G) := \max_{J \subseteq E} \theta(J). \tag{4.2}$$

A set J is said to be *critical* if

$$\theta(J) = \theta(G). \tag{4.3}$$

There can be more than one critical set.

It is clear that $M(J) \leq |\gamma| = |V| - 1$, and also $M(J) \leq |J|$. Since $J \subseteq E$, it implies that $|J| \leq |E|$. Thus, for any $\emptyset \neq J \subseteq E$,

$$\frac{\mathcal{M}(J)}{|J|} \in \Theta := \left\{ \frac{p}{q} : 1 \leq p \leq \min\{|V| - 1, q\},\ 1 \leq q \leq |E| \right\}. \tag{4.4}$$

Since there are finitely many options for the numerator and denominator in $\theta(J)$, there are finitely many possible values for $\theta(G)$. In [8], Cunningham described a method of exploiting this fact to compute $\theta(G)$. Essentially, one performs a binary search on the set of possible values, making use of an oracle that Cunningham described in order to determine whether or not $\theta(G) \leq \frac{p}{q}$ for a given fraction $\frac{p}{q}$. This oracle is derived by performing a few transfor-

mations on the problem that convert it to a problem on a matroid, which Cunningham then provides a greedy algorithm to solve.

Lemma 4.1.1. *For any $p, q \geq 1$, we have*

$$\theta(G) \leq \frac{p}{q} \iff 0 \leq \min_{J \subseteq E} \Big(\frac{p}{q}|J| - \mathcal{M}(J) \Big). \tag{4.5}$$

Proof.

$$\begin{aligned} \theta(G) \leq \frac{p}{q} \iff \max_{J \subseteq E} \theta(J) \leq \frac{p}{q} &\iff \theta(J) \leq \frac{p}{q}, \quad \forall J \subseteq E \\ &\iff 0 \leq \frac{p}{q}|J| - \mathcal{M}(J), \quad \forall J \subseteq E \\ &\iff 0 \leq \min_{J \subseteq E} \Big(\frac{p}{q}|J| - \mathcal{M}(J) \Big). \end{aligned}$$

□

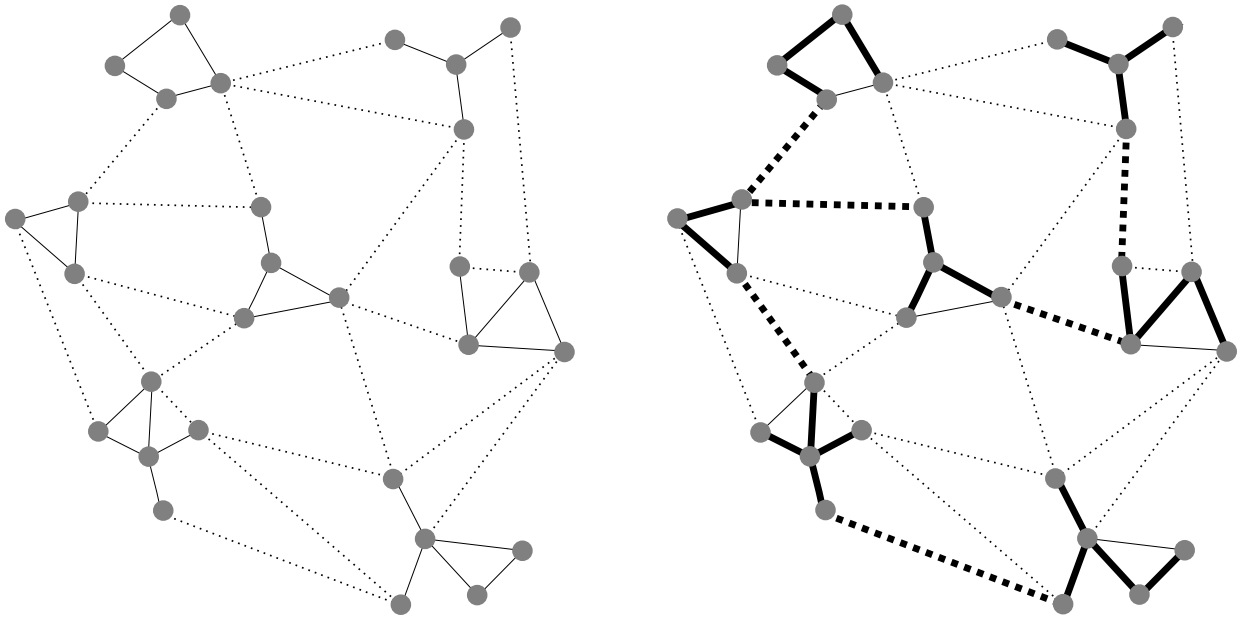
From this lemma, we can see that checking whether $\theta(G) \leq \frac{p}{q}$ is equivalent to solving the minimization problem in (4.5), which we later write in terms of the rank function associated with the graphic matroid of G. Cunnigham called this minimization problem the *optimal attack* problem.

Lemma 4.1.2. *Let $G_J = (V, J)$ be a subgraph of G which only contains edges in J, and let $Q(G_J)$ be the number of connected components of G_J. For any $J \subseteq E$,*

$$\mathcal{M}(J) = Q(G_{\overline{J}}) - 1. \tag{4.6}$$

Proof. After the edges in J are removed from the graph, the connected components induce a partition of the remaining edges, $\overline{J}$, into two or more subsets $\{\overline{J}_1, \overline{J}_2, \ldots, \overline{J}_k\}$, where $k = Q(G_{\overline{J}})$. Any spanning tree $\gamma \in \Gamma$ has to connect these components together and, therefore, must contain at least $k - 1$ edges of J, showing that $\mathcal{M}(J) \geq Q(G_{\overline{J}}) - 1$.

To see that equality holds, we will produce a spanning tree γ such that $|\gamma \cap J| = Q(G_{\overline{J}}) - 1$. Let γ_i be a spanning tree in the subgraph induced by $\overline{J}_i$ for $i = 1, 2, \ldots, k$.



(a) Graph G and its components.

(b) A spanning tree γ of G.

Figure 4.1: An example demonstrating the construction in the proof of Lemma 4.1.2.

The union of the γ_i form a spanning forest of G containing k trees. If $k = 1$, we are done. Otherwise, since G is connected, it is possible to add $k-1$ edges of E to this forest to produce a spanning tree γ. Note that none of these edges may belong to $\overline{J}$ since this would necessarily introduce a cycle in one of the $\overline{J}_i$. Therefore, each of these new edges lies in J and thus $|\gamma \cap J| = Q(G_{\overline{J}}) - 1$ as desired. □

The example shown in Figure 4.1 illustrates Lemma 4.1.2. Figure 4.1a shows a graph G. Edges in J are indicated by dashed lines and edges in $\overline{J}$ by solid lines. After the dashed lines are removed, there are 7 connected components, so $Q(G_{\overline{J}}) = 7$.

Figure 4.1b shows the construction of a spanning tree γ satisfying $\mathcal{M}(J) = Q(G_{\overline{J}}) - 1 = 6$. The thick solid lines in each component indicate the spanning trees γ_i and the thick dashed lines are the edges added in order to complete the spanning tree γ. As described in the proof to the lemma, there are 6 such edges, and all must come from J. This shows that $\mathcal{M}(J) = 6 = Q(G_{\overline{J}}) - 1$ for this example.

In the next section we will make a connection between the rank function of the graphic matroid of G and the graph vulnerability.

4.2 Matroids and polymatroids

4.2.1 Vulnerability and the graphic matroid

First, we define

$$f(J) = |V| - Q(G_J). \tag{4.7}$$

The function $f(J)$ is called the *rank function* of the graphic matroid associated with G. Therefore, using Lemma 4.1.2 we can write

$$\mathcal{M}(J) = |V| - 1 - f(\overline{J}).$$

So, the minimization (4.5) can be rewritten as

$$0 \leq \min_{J \subseteq E} \Big(\frac{p}{q}|J| - |V| + 1 + f(\overline{J}) \Big).$$

Thus, an oracle can test whether $\theta(G) \leq \frac{p}{q}$ by testing whether

$$\min_{J \subseteq E} \left(\frac{p}{q}|J| + f(\overline{J}) \right) \geq |V| - 1. \tag{4.8}$$

As shown in [8], the minimum value on the left-hand side is related to the concept of polymatroid bases.

4.2.2 Matroids and polymatroids

Here, we briefly review the key points of this relationship. We start by defining a matroid. In what follows E is a finite set, and $f : 2^E \to \mathbb{N}$ is a mapping from the family of subsets of E to $\mathbb{N}$.

Definition 4.2.1. $M = (E, f)$ is said to be a **matroid** if it satisfies the following properties.

1. $\forall J \subseteq E, f(J) \leq |J|$,
2. If $J' \subseteq J \subseteq E$, then $f(J') \leq f(J)$,

3. If $J, J' \subseteq E$, then $f(J \cup J') + f(J \cap J') \leq f(J) + f(J')$.

An important example of a matroid in the context of this dissertation is the graphic matroid $M = (E, f)$ where E is the edge set of a connected graph, and f is defined in (4.7).

Definition 4.2.2. The function f is a **polymatroid function** if it satisfies the following conditions:

1. $f(\emptyset) = 0$,
2. If $J' \subseteq J \subseteq E$, then $f(J') \leq f(J)$,
3. If $J, J' \subseteq E$, then $f(J \cup J') + f(J \cap J') \leq f(J) + f(J')$.

Definition 4.2.3. We define the **polymatroid** to be the following polytope associated to f:

$$P(f) = \{x \in \mathbb{R}^E_{\geq 0},\ x(J) \leq f(J), \forall J \subseteq E\}. \tag{4.9}$$

For any $y \in \mathbb{R}^E_{\geq 0}$, any maximal vector $x \in P(f)$ with $x \leq y$ is called a $P(f)$-basis of y.

Theorem 4.2.1. *For any $y \in \mathbb{R}^E_{\geq 0}$ and x be any $P(f)$-basis of y, we have*

$$x(E) = \min_{J \subseteq E} \big(y(J) + f(\bar{J})\big), \tag{4.10}$$

where

$$x(E) = \sum_{e \in E} x(e) \qquad \textit{and similarly} \qquad y(J) = \sum_{j \in J} y(j).$$

Proof. Some intuition about the proof can be gained from the discussion in Section 4.2.4. □

4.2.3 The polymatroid theorem for graph vulnerability

To see how Theorem 4.2.1 can be applied to the graph vulnerability problem, we note that if $G = (V, E)$ is a graph and f is the rank function on G defined in (4.7), then (E, f) is a matroid and f is a polymatroid function. Thus, if we define $y \equiv \frac{p}{q}$ (the constant function) and let x be a $P(f)$-basis of y, then Theorem 4.2.1 implies that the inequality in (4.8) holds

if and only if $x(E) \geq |V| - 1$. This reduces the graph vulnerability question to one of polymatroid bases.

4.2.4 Cunningham's greedy algorithm

In order to understand the proof of Theorem 4.2.1, first note that if $x \in P(f)$, if $x \leq y$ and if $J \subseteq E$, then

$$x(E) = x(J) + x(\overline{J}) \leq y(J) + f(\overline{J}). \tag{4.11}$$

The theorem implies that if x is a $P(f)$-basis of y, then there exists a J for which (4.11) holds as equality. In [8], Cunningham presented a greedy algorithm that finds such an x and J. A pseudocode listing of this algorithm is shown in Algorithm 1.

Algorithm 1 Cunningham's algorithm
Input: G=(V,E), y

```
1: x ← 0
2: J̄ ← ∅
3: for all j ∈ E do
4:     ϵ, J'(j) ← min(f(J') − x(J') : j ∈ J')
5:     if ϵ < y(j) − x(j) then
6:         J̄ ← J̄ ∪ J'(j)
7:     else
8:         ϵ = y(j) − x(j)
9:     end if
10:    x(j) ← x(j) + ϵ
11: end for
12: return sum(x), E \ J̄
```

At the beginning of the algorithm, x is initialized to the zero vector and $\overline{J}$ is initialized to the empty set (in other words, J is initialized to all of E). The algorithm proceeds by looping over all edges j of E. On each iteration of the loop, one computes the value

$$\epsilon_{\max}(j) = \max\{\epsilon : x + \epsilon \mathbf{1}_j \in P(f)\} \tag{4.12}$$

along with a set $J'(j)$ containing j and satisfying

$$f(J'(j)) = x(J'(j)) + \epsilon_{\max}(j).$$

The value $\epsilon_{\max}$ is the largest value by which we can increment x on edge j without leaving $P(f)$ and the set $J'(j)$ is a constraint that would be violated if we were to increase x by any more on that edge.

Next in the algorithm is a decision. If $x(j)$ can be increased by $\epsilon_{\max}$ without violating the constraint that $x(j) \leq y(j)$, then $x(j)$ is incremented by that amount and the edges in $J'(j)$ are added to $\overline{J}$ (equivalently, J is intersected with $\overline{J'(j)}$). Otherwise, $x(j)$ is set to $y(j)$ and $\overline{J}$ is not changed.

A first step in understanding Cunningham's algorithm is the following lemma, which relates to tight sets. A set $\overline{J} \subseteq E$ is called *tight* with respect to $x \in P(f)$ if $x(\overline{J}) = f(\overline{J})$.

Lemma 4.2.1. *When Cunningham's algorithm terminates, all three of the following properties hold.*

1. $x \in P(f)$,
2. $x \leq y$, *and*
3. $\overline{J}$ *is tight with respect to* x.

Proof. Note that all three properties hold before entering the loop when $x = 0$ and $\overline{J} = \emptyset$. In order to prove the lemma, then, we need only show that these properties cannot be changed by a single iteration of the loop. To clarify notation, let x_0 and $\overline{J}_0$ be the values of these variables at the beginning of a loop iteration and let x and $\overline{J}$ be the values at the end of the loop iteration.

By the definition of ϵ, $x \in P(f)$ and $x \leq y$ at the end of each iteration. To finish the proof, we must show that if $\overline{J}_0$ is tight with respect to x_0, then $\overline{J}$ is tight with respect to x.

There are two cases to consider. First, suppose that $j \in \overline{J}_0$. By assumption, $\overline{J}_0$ is tight with respect to x_0, so $x_0(j)$ cannot be increased without violating the polymatroid

constraint. In this case, $\epsilon_{\max} = 0$ and $x = x_0$ (in fact, one can modify the algorithm to skip j if it is already contained in $\overline{J}_0$). Thus, $\overline{J} = \overline{J}_0 \cup J'(j)$ is the union of two sets that are both tight with respect to $x = x_0$. Lemma 4.2.2 below implies that $\overline{J}$ is also tight.

Otherwise, it must be the case that $j \notin \overline{J}_0$. Here, there are two subcases. In one subcase, $\epsilon_{\max} \geq y(j) - x_0(j)$. In this case, $x(j) = y(j)$ and $\overline{J} = \overline{J}_0$. Since $j \notin \overline{J}_0$ and since x differs from x_0 only on the edge j, it follows that

$$x(\overline{J}) = x(\overline{J}_0) = x_0(\overline{J}_0) = f(\overline{J}_0) = f(\overline{J}),$$

so $\overline{J}$ is tight with respect to x.

In the second subcase, $\epsilon_{\max} < y(j) - x_0(j)$. This case is a little more subtle. First, note that $\overline{J}_0$ is tight with respect to x (again, since $j \notin \overline{J}_0$ and since x and x_0 agree everywhere except on j). Moreover, by construction,

$$x(J'(j)) = x_0(J'(j)) + \epsilon_{\max}(j) = f(J'(j)),$$

so $J'(j)$ is tight with respect to x. The fact that $\overline{J}$ is tight with respect to x follows from the following lemma showing that the union of two tight sets is tight.

□

Lemma 4.2.2. *Let $x \in P(f)$ and suppose $B, C \subseteq E$ are tight with respect to x. Then $B \cup C$ is also tight.*

Proof. By assumption, $x(B) = f(B)$, and $x(C) = f(C)$. So,

$$\begin{aligned}
f(B \cup C) &\leq f(B) + f(C) - f(B \cap C) && ; f \text{ is a polymatroid function} \\
&= x(B) + x(C) - f(B \cap C) \\
&= x(B \cup C) + x(B \cap C) - f(B \cap C) \\
&= x(B \cup C) - (f(B \cap C) - x(B \cap C)) \\
&\leq x(B \cup C) \leq f(B \cup C) && ; x \in P(f)
\end{aligned}$$

□

Now we show that Cunningham's algorithm produces a $P(f)$-basis of y. Doing so actually proves a weaker version of Theorem 4.2.1, which is sufficient for understanding the graph vulnerability computation.

Theorem 4.2.2. *Let x and J be the result of Algorithm 1. Then x is a $P(f)$-basis of y and*

$$x(E) = \min_{J' \subseteq E} \left(y(J') + f(\overline{J}') \right).$$

Proof. As in (4.11), we see that

$$x(E) \leq \min_{J' \subseteq E} \left(y(J') + f(\overline{J}') \right) \leq y(J) + f(\overline{J}). \tag{4.13}$$

Moreover, by Lemma 4.2.1, $x(\overline{J}) = f(\overline{J})$.

Now consider an edge $j \in J$. Since $j \notin \overline{J}$, j did not belong to any of the tight sets whose union formed $\overline{J}$. Thus, when j was encountered in the loop, $x(j)$ was set to $y(j)$. This implies that $x(J) = y(J)$ and, therefore, that

$$x(E) = x(J) + x(\overline{J}) = y(J) + f(\overline{J}),$$

which implies that all inequalities in (4.13) hold as equality.

To see that x is a $P(f)$-basis of y, we need to show that x is maximal. Suppose not, then there must be an $x' \in P(f)$ such that $x' \neq x$ and $x \leq x' \leq y$. But this would imply that

$$x'(E) > x(E) = y(J) + f(\overline{J}),$$

which contradicts (4.11). □

The most computationally challenging part of Cunninham's algorithm is in minimizing $f(J) - x(J)$ over all $J \subseteq E$ containing a particular edge j. Although this appears combinato-

rially difficult at first look, Cunningham's approach was to recast this optimization problem as a maximum network flow problem.

4.3 Network flow

Let $G = (V, E)$ be a connected graph. Let f be the graphic matroid associated with G defined as in (4.7). There is an equivalent linear definition for the polymatroid $P(f)$ which is

$$P(f) = \{x \in \mathbb{R}^E_{\geq 0} : \ x(\gamma(U)) \leq |U| - 1, \ \forall U, \ \emptyset \neq U \subseteq V\}, \tag{4.14}$$

where $\gamma(U)$ denotes the set of edges with both ends in U. This equivalency is proved as follows.

Theorem 4.3.1. *Let* $P(f) = \{x \in \mathbb{R}^E_{\geq 0}, \ x(J) \leq f(J), \forall J \subseteq E\}$, *and* $Q(f) = \{x \in \mathbb{R}^E_{\geq 0}, \ x(\gamma(U)) \leq |U| - 1, \ \forall U, \ \emptyset \neq U \subseteq V\}$, *where* $\gamma(U) = \{e \in E : \text{both ends of } e \text{ are in } U\}$. *Then* $P(f) \equiv Q(f)$.

Proof. To see that $P(f) \subseteq Q(f)$, let $x \in P(f)$ and let $U \subseteq V$ be nonempty. Define $J = \gamma(U) \subseteq E$. Then

$$x(\gamma(U)) = x(J) \leq f(J) \leq |U| - 1. \tag{4.15}$$

The last inequality can be seen by considering the rank of the subgraph induced by the vertices in U. This shows that $x \in Q(f)$.

On the other hand, to see that $Q(f) \subseteq P(f)$, let $x \in Q(f)$ and $J \subseteq E$. Let $\{J_1, J_2, \ldots J_k\}$ be the edge sets of the connected components of the graph induced by J. Let their corresponding sets of vertices be $\{U_1, U_2, \ldots, U_k\}$. The U_i are pairwise disjoint. Since $x \in Q(f)$ and since the graph induced by each J_i is connected, $x(\gamma(U_i)) \leq |U_i| - 1 = f(J_i)$. Since $J_i \subseteq \gamma(U_i)$ and $x \geq 0$, it follows that

$$x(J_i) \leq x(\gamma(U_i)) \leq f(J_i).$$

Summing over i shows that

$$x(J) = \sum_{i=1}^{k} x(J_i) \leq \sum_{i=1}^{k} f(J_i) = f\left(\bigcup_{i=1}^{k} J_i\right) = f(J),$$

where we have used the fact that the rank of a disjoint union of graphs is equal to the sum of the ranks of these graphs. □

Theorem 4.3.2. *For a given $x \in P(f)$ and $j \in E$,*

$$\min\{f(J) - x(J) : J \subseteq E, j \in J\} = \min\{|U| - 1 - x(\gamma(U)) : U \subseteq V, j \in \gamma(U)\}. \quad (4.16)$$

Moreover, if U^* is a minimizer for the right-hand side problem, then $J^* := \gamma(U^*)$ is a minimizer for the left-hand side problem.

Proof. Given $J \subseteq E$ with $j \in J$, we first show that there exists $U \subseteq V$ with $j \in \gamma(U)$ such that

$$|U| - 1 - x(\gamma(U)) \leq f(J) - x(J). \quad (4.17)$$

Let $\{J_1, J_2, \ldots J_k\}$ be the edge sets of the connected components of the graph induced by J. Then,

$$f(J) - x(J) = \sum_{i=1}^{k} f(J_i) - \sum_{i=1}^{k} x(J_i) = \sum_{i=1}^{K} (f(J_i) - x(J_i)).$$

Therefore $f(J_i) - x(J_i) \leq f(J) - x(J)$ for $i \in 1, 2, \ldots, k$, and $j \in J_i$. Let, ℓ be the index such that $j \in J_\ell$. Let U be the vertices of the subgraph induced by J_ℓ. Since J_ℓ is connected, $f(J_\ell) = |U| - 1$, and since $\gamma(U) \supseteq J_\ell$, $x(\gamma(U)) \geq x(J_\ell)$ it follows that $|U| - 1 - x(\gamma(U)) \leq f(J_\ell) - x(J_\ell) \leq f(J) - x(J)$. It follows that the minimum on the right of (4.16) is less than or equal to the minimum on the left.

To establish the opposite inequality, we show that given $U \subseteq V$ with $j \in \gamma(U)$, there exists $J \subseteq E$ with $j \in J$ such that $f(J) - x(J) \leq |U| - 1 - x(\gamma(U))$. Define $J = \gamma(U)$. So, $x(J) = x(\gamma(U))$ and $f(J) \leq |U| - 1$.

From this, it also follows that, if U^* is optimal for the right-hand side problem, then $J^* :=$

$\gamma(U^*)$ is optimal for the left-hand side. Indeed, if $J \subseteq E$ contains j, then the construction at the beginning of the proof finds a corresponding U with $j \in \gamma(U)$ satisfying (4.17). From this, it follows that

$$f(J^*) - x(J^*) \leq |U^*| - 1 - x(\gamma(U^*)) \leq |U| - 1 - x(\gamma(U)) \leq f(J) - x(J).$$

□

Our goal from the previous section is to find a subset $J \subseteq E$, containing a given edge j that minimizes $f(J) - x(J)$. From Theorem 4.3.2 this is equivalent to finding a set of vertices U with $j \in \gamma(U)$ that minimizes $|U| - 1 - x(\gamma(U))$ over all such U. To find such a subset, we follow [8] and construct an undirected capacitated graph G' for a given $x \in P(f)$, and $j \in E$. The vertex set for G' is $V \cup \{r, s\}$, where r and s are new vertices, namely, source and the sink. Each edge $e \in E$ is an edge in G', having capacity $\frac{1}{2}x_e$. Edges connecting from s to each vertex $v \in V$ has capacity 1. The edges from r to $v \in V$ either have capacity ∞ if v is an end of j, or, $\frac{1}{2}x(\delta(v))$ otherwise. Here $\delta(U) = \{e \in E,\ e \text{ has exactly one end in } U \subseteq V\}$, and $\delta(v)$ is as same as $\delta(\{v\})$. (These nodes correspond to *star* nodes in the graph.)

Now consider a cut in the formed graph G' induced by $U \cup \{r\}$. So, an edge in the cut set has one end in $U \cup \{r\}$ and the other end in $V \backslash U \cup \{r\}$. The capacity of such cut is

$$\begin{aligned} |U| + \frac{1}{2}x(\delta(U)) + x(\gamma(V\backslash U)) + \frac{1}{2}x(\delta(U)) &= |U| + x(\delta(U)) + x(\gamma(V\backslash U)) \\ &= |U| + x(E) - x(\gamma(U)) \\ &= |U| - 1 - x(\gamma(U)) + (x(E) + 1). \end{aligned} \tag{4.18}$$

If we explain the terms in the left hand side of (4.18); the first term corresponds to edges going from vertices in U to s. There are $|U|$ such edges and each has a capacity of 1. The second term corresponds to edges going from U to $V\backslash U$. The third and fourth terms both correspond to edges going from the root vertex r to vertices in $V\backslash U$.

Then we can see that a cut induced by $U \cup \{r\}$ where $j \notin \gamma(U)$ will have infinite capacity. Therefore finding a minimum cut in G' will minimize $|U| - 1 - x(\gamma(U))$, where $j \in \gamma(U)$,

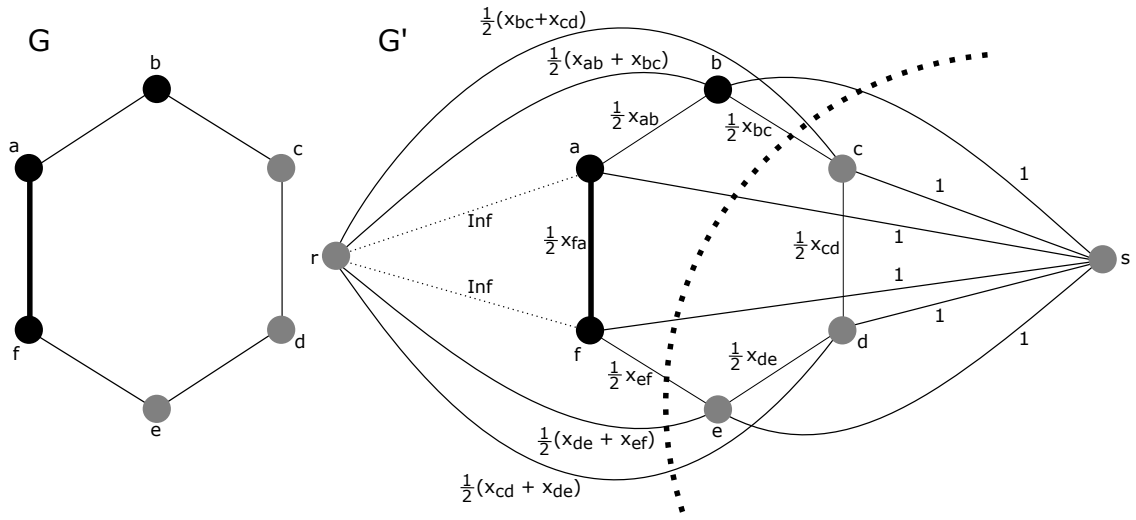


Figure 4.2: The cut induced by $U \cup \{r\} = \{a, b, f, r\}$.

and $U \subseteq V$.

Consider the following example in Figure 4.2. Here $U = \{a, b, f\}$ and the edge we consider is $j = (a, f)$.

$$\begin{aligned}\text{The capacity of the cut} &= 3 + \frac{1}{2}x_{bc} + \frac{1}{2}x_{ef} + \frac{1}{2}(x_{bc} + x_{cd}) + \frac{1}{2}(x_{de} + x_{ef}) + \frac{1}{2}(x_{cd} + x_{de}) \\ &= \underbrace{3}_{|U|} + \underbrace{\frac{1}{2}(x_{bc} + x_{ef})}_{\frac{1}{2}x(\delta(U))} + \underbrace{x_{cd} + x_{de}}_{x(\gamma(V\setminus U))} + \underbrace{\frac{1}{2}(x_{bc} + x_{ef})}_{\frac{1}{2}x(\delta(U))} \\ &= 3 + x_{bc} + x_{cd} + x_{de} + x_{ef}.\end{aligned} \tag{4.19}$$

Lets consider the next example in Figure 4.3 where $U = \{a, b, c\}$ and the edge we consider now, $j = (a, f)$, does not connect two vertices in U. We can see in this case that the capacity of the cut induced by $U \cup \{r\}$ is equal to ∞ as we discussed before.

Therefore, any network flow algorithm can be used to solve the minimization problem in Cunningham algorithm. So, we have used a polynomial implementation of the max-flow min-cut theorem by Ford and Fulkerson.

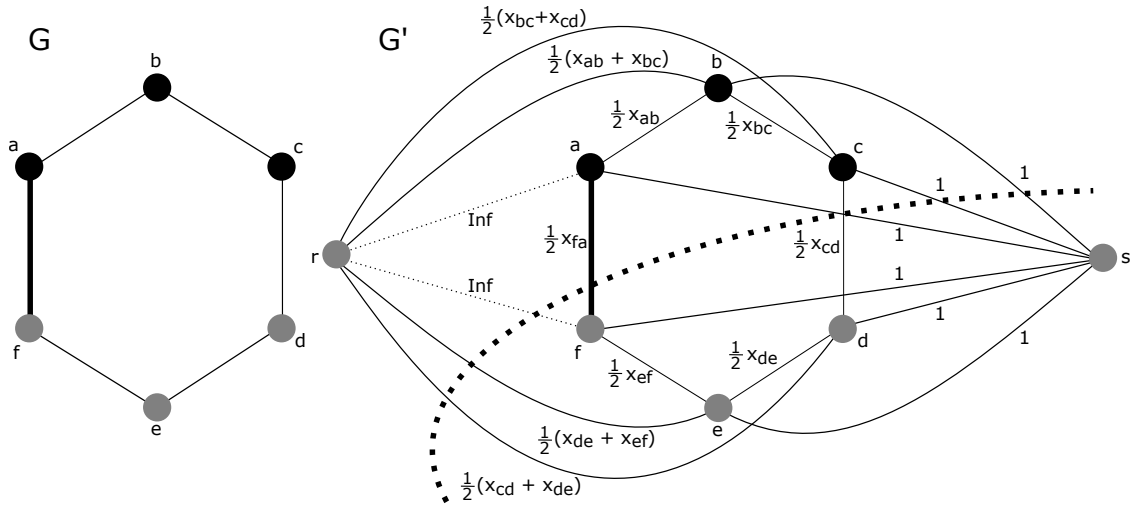


Figure 4.3: The cut induced by $U \cup \{r\} = \{a, b, c, r\}$.

4.4 Spanning tree modulus algorithm

4.4.1 Modified Cunningham algorithm

After a suitable modification, we can use the greedy algorithm of Cunningham (and its max flow implementation) to find x using only *integer arithmetic*. This is useful both because integer arithmetic is somewhat faster than floating point arithmetic on most modern computers and because using integers allows us to avoid roundoff errors. This modification uses the observation that if f is a polymatroid function (see Definition 4.2.2) and if $q > 0$, then qf is a polymatroid function.

Theorem 4.4.1. *Let x be a $P(f)$-basis of y. Then qx is a $P(qf)$-basis of qy, for any $q > 0$.*

Proof. Let's first show that $P(qf) = qP(f)$. By definition,

$$\begin{aligned} P(qf) &= \{x \in \mathbb{R}^E_{\geq 0} : \ x(J) \leq qf(J) \quad \forall J \subseteq E\} \\ &= \{x \in \mathbb{R}^E_{\geq 0} : \ \frac{1}{q}x(J) \leq f(J) \quad \forall J \subseteq E\} \\ &= \{qx \in \mathbb{R}^E_{\geq 0} : \ x(J) \leq f(J) \quad \forall J \subseteq E\} = qP(f). \end{aligned} \tag{4.20}$$

Since x is a $P(f)$-basis of y, we have $qx \leq qy$. Thus, in order to show that qx is a $P(qf)$

basis of qy, we need only verify maximality. If there exists $z \in P(qf)$ such that $z \leq qy$ and $qx \leq z$ then $\frac{1}{q}z \in P(f)$, $\frac{1}{q}z \leq y$, and $x \leq \frac{1}{q}z$, which implies that $\frac{1}{q}z = x$ and, therefore, that $z = qx$. □

Now we can write 4.14 accordingly as follows.

$$\begin{aligned} P(qf) = qP(f) &= \{qx \in \mathbb{R}^E_{\geq 0} : \ x(\gamma(U)) \leq |U| - 1, \ \forall U, \ \emptyset \neq U \subseteq V\} \\ &= \{x \in \mathbb{R}^E_{\geq 0} : \ x(\gamma(U)) \leq q(|U| - 1), \ \forall U, \ \emptyset \neq U \subseteq V\} \end{aligned} \tag{4.21}$$

Next, we discuss a problem with Cunningham's method and describe a way to fix this problem. Cunningham's approach relies on the concept of *tight* sets. That is, sets for which $x(\overline{J}) = qf(\overline{J})$. It appears to be implied in his work that if $\overline{J}$ is a tight set, then J is a critical set. However, we have noticed a problem in this argument that arises in computation, namely.

Theorem 4.4.2. *If $\theta(G) = \frac{p}{q}$ and if x is a $P(f)$-basis for $\frac{p}{q}\mathbf{1}$, then E is tight.*

Proof. Since $\theta(G) = \frac{p}{q}$,

$$x(E) = \min_{J \subseteq E} \left(\frac{p}{q}|J| + f(\overline{J}) \right) = (|V| - 1) = f(E).$$

□

In practice, the algorithm Cunningham describes will return $\overline{J} = E$ as the tight set when $\frac{p}{q}$ is exactly $\theta(G)$. Since $J = \overline{E} = \emptyset$, this does not provide us with a critical set, because the critical set is the complement of the tight set.

Our modified version proceeds as follows. First, we use Cunningham's algorithm to determine $\theta(G) = \frac{p}{q}$ using a binary search. Once this value is known, we run Cunningham's algorithm one additional time to find a $P(q'f)$-basis, $\tilde{x}$, for $p'\mathbf{1}$, along with a tight set J for this modified problem. The idea is to choose p' and q' so that $\frac{p'}{q'} < \frac{p}{q}$ and

$$\left(\frac{p'}{q'}, \frac{p}{q} \right] \cap \Theta = \left\{ \frac{p}{q} \right\}. \tag{4.22}$$

Theorem 4.4.3. *Suppose that $\theta(G) = \frac{p}{q}$, and $\frac{p'}{q'}$ satisfies (4.22). Let $\tilde{x}$ be a $P(q'f)$-basis for $p'\mathbf{1}$ and that $\overline{J}$ is tight. Then J is a critical set.*

Proof. First, we show that $\overline{J}$ cannot be E. If it were, then we would have

$$q'(|V| - 1) = \tilde{x}(E) = \min_{J \subseteq E} \left(p'|J| + q' f(\overline{J}) \right),$$

which would imply that

$$\theta(G) \leq \frac{p'}{q'} < \frac{p}{q} = \theta(G),$$

yielding a contradiction.

Now, when Cunningham's algorithm terminates, we have both $\tilde{x}$ and the tight set $\overline{J}$ with the property that $\tilde{x} = p'\mathbf{1}$ on $J \neq \emptyset$. Moreover, since $\theta(G) > \frac{p'}{q'}$,

$$q'(|V| - 1) > \min_{J \subseteq E} \left(p'|J| + q' f(\overline{J}) \right).$$

Since $\overline{J}$ is tight, this implies that

$$\begin{aligned} p'|J| &< q'(|V| - 1) - q' f(\overline{J}) \\ &= q'(|V| - 1 - f(\overline{J})) = q' \mathcal{M}(J). \end{aligned}$$

Thus, we have that

$$\frac{p'}{q'} < \frac{\mathcal{M}(J)}{|J|} \leq \theta(G) = \frac{p}{q}.$$

□

By choosing p' and q' so that (4.22) holds, this guarantees that $\mathcal{M}(J)/|J| = p/q$ and, thus, that J is critical. A choice for p' and q' can be found using the following simple lower bound on the distance between distinct numbers in Θ. If $p/q, p'/q' \in \Theta$ and $p'/q' < p/q$, then

$$\frac{p}{q} - \frac{p'}{q'} = \frac{pq' - qp'}{qq'} \geq \frac{1}{|E|^2}. \tag{4.23}$$

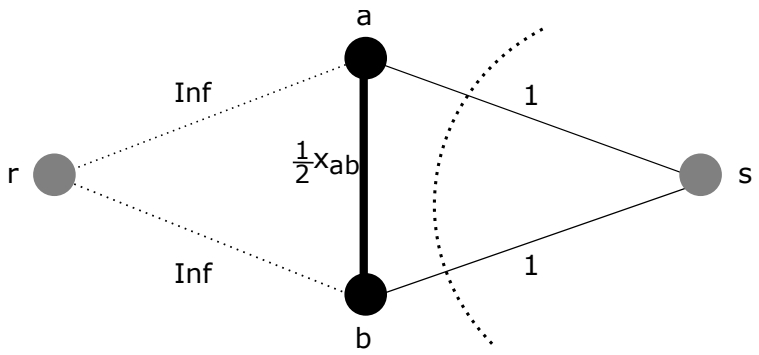


Figure 4.4: Empty critical set.

Thus, choosing

$$\frac{p'}{q'} = \frac{p}{q} - \frac{1}{|E|^2} = \frac{p|E|^2 - q}{q|E|^2}$$

guarantees that (4.22) holds.

The path graph of two nodes in Figure 4.4 shows how Cunningham's algorithm can return the whole edge set E as the tight set. Hence, an empty set will be returned as the critical set.

4.4.2 Explanation of the algorithm

According to Equation (4.21) we can rewrite the graph cut in 4.18 to support integer arithmetic and modify the Algorithm 1 as follows. This significantly improves the computational time of the algorithm.

Algorithm 2 Integer arithmetic version of Cunningham's algorithm
Input: $G = (V, E), p, q$

1: $x' \leftarrow 0$
2: $\overline{J} \leftarrow \emptyset$
3: **for all** $j \in E$ **do**
4: $\quad \epsilon, J'(j) \leftarrow \min(qf(J') - x'(J') : j \in J')$
5: $\quad$ **if** $\epsilon < p - x'(j)$ **then**
6: $\quad\quad \overline{J} \leftarrow \overline{J} \cup J'(j)$
7: $\quad$ **else**
8: $\quad\quad \epsilon = p - x'(j)$
9: $\quad$ **end if**
10: $\quad x'(j) \leftarrow x'(j) + \epsilon$
11: **end for**
12: **return** $sum(x'), E \setminus \overline{J}$

Algorithm 1 and Algorithm 2 are equivalent with $x' = qx$. Initially x' goes in as an integer in step 1. Since $qf(J')$ is an integer, ϵ is also an integer in step 4. Since p is an integer ϵ gets updated as an integer in step 8. In step 10, the updated x' is also an integer. Therefore, at any pass of the loop x stays as an integer.

Note that in 4.18, $|U|$ is an integer. Moreover, as described above, qx is an integer-valued vector. Multiplying 4.18 through by $2q$, then, yields

$$2q|U| + x'(\delta(U)) + 2x'(\gamma(V \backslash U)) + x'(\delta(U)) = 2q(|U| - 1) - 2x'(\gamma(U)) + (2x'(E) + 2q). \quad (4.24)$$

Following Cunningham's argument, the quantity on the left is the capacity of the cut as in Equation (4.18) except with capacities multiplied by $2q$. Each of these modified capacities is integer-valued, allowing the use of integer arithmetic in the network flow solver. The right-hand side of (4.24) is

$$2\left[q(|U| - 1) - x'(\gamma(U)) + x'(E) + q\right]. \quad (4.25)$$

Algorithm 3 Network flow algorithm
Input: $G = (V, E), x', (u, v), q$

1: $V = V \cup \{r, s\}$
2: **for all** $(u', v') \in E$ **do**
3: $\quad capacity(u', v') = x'(u', v')$
4: **end for**
5: **for all** $v' \in V$ **do**
6: $\quad capacity(s, v') = 2q$
7: $\quad$ **if** $v' \in \{u, v\}$ **then**
8: $\quad\quad capacity(r, v') = \infty$
9: $\quad$ **else**
10: $\quad\quad capacity(r, v') = sum(x'(neighbors\ of\ v'))$
11: $\quad$ **end if**
12: **end for**
13: $\epsilon, J' = mincut(G, r, s, capacity)$
14: $\epsilon = \epsilon - (sum(x') + q)$
15: **return** ϵ, J'

Algorithm 3 is used to solve the minimization problem in Algorithm 2. The value ϵ in step 13 of the Algorithm 3 is the value we get by dividing Equation (4.25) by 2, but we want to recover $q(|U| - 1) - x'(\gamma(U))$ only. Therefore, we need to update ϵ with $\epsilon - (x'(E) + q)$ in every iteration.

Now what's left to do is choosing p and q carefully using a binary search algorithm with slight modifications to match integer arithmetic and after fixing the issue (to get a non-empty critical set) in Cunningham's algorithm.

Algorithm 4 Binary search algorithm
Input: $G(V, E)$

$ratios = sorted(\frac{p}{q}\ ratios)$
$lbound = 0$
$ubound = |ratios| - 1$
while $ubound > lbound$ **do**
    $i = (ubound + lbound)/2$
    $pq = ratios(i)$
    $p, q = numerator(pq), denominator(pq)$
    $sum(x'), J = Cunningham(G, p, q)$
    if $sum(x') \geq q \cdot (|V| - 1)$ **then**
        $ubound = i$
    else
        $lbound = i + 1$
    end if
end while
$pq = ratios(lbound)$
$p, q = numerator(pq), denominator(pq)$
$p' = p \cdot |E|^2 - q$
$q' = q \cdot |E|^2$
$sum(x'), J = Cunningham(G, p', q')$
return J, pq

So, Algorithm 4 returns a critical set J, and the graph vulnerability $\theta(G) = pq$.

4.4.3 Modulus algorithm

Theorem 1 (Critical Subset Attack Theorem) in [11] shows that the strategy of the eavesdropper is choosing an edge uniformly over a critical subset. In Chapter 3 we discussed the same zero sum game with the same payoff matrix from the modulus point of view. Therefore, according to Theorem 3.2.2 the edge set

$$E_{Q^*} := \{e \in E : \eta^*(e) = \|\eta^*\|_\infty\}$$

forms such a critical set.

The optimal payoff or the value of the game in [11] is equal to graph vulnerability $\theta(G)$. Therefore, $\theta(G)$ must be equal to $\|\eta^*\|_\infty$. The oracle that solves (4.2) outputs a critical set

$E_{\tilde{Q}} \subseteq E_{Q^*}$ and also $\theta(G)$ (i.e. $\|\eta^*\|_\infty$). The critical set $E_{\tilde{Q}}$ is the edge set for a minimum feasible partition $\tilde{Q}$. If we remove $E_{\tilde{Q}}$ from E and then compute the spanning tree modulus again for the sub-graph (all the connected components) the original η^* we had for the initial graph remain intact (as a consequence of [3, Theorem 3.3]). Therefore, we continue this process of recursively solving the game on sub-graphs until no edges are left and η^* is found for all edges.

Algorithm 5 Modulus algorithm
Input: G = (V,E)

$g = \{G\}$
while $|g| > 0$ **do**
  $H = pop(g)$
  $J, \theta(H) = binarysearch(H)$
  for all $e \in J$ **do**
    $\eta^*(e) \leftarrow \theta(H)$
    $E = E \backslash \{e\}$
  end for
  $C = components(H)$
  for all $c \in C$ **do**
    if $|c| > 1$ **then**
      $h = G(subgraph(c))$
      $g = g + h$
    end if
  end for
end while
$modulus = \left(\sum_{e \in E} \eta^*(e)^2\right)^{-1}$

4.4.4 Time complexity

Here we estimate an overall worst-case time complexity bound for Algorithm 5. The time complexity of each iteration of the loop in Algorithm 2 is dominated by the complexity of Algorithm 3, and Algorithm 3's complexity is dominated by the cost of finding a minimum cut. One of the most efficient known algorithms for computing the minimum cut is the highest-label preflow-push algorithm which has time complexity $O(|V|^2\sqrt{|E|})$ (see [6]). Since the loop in Algorithm 2 is executed at most once for each edge in E, the overall complexity of Algorithm 2 is $O(|V|^2|E|^{\frac{3}{2}})$. Algorithm 4 performs a binary search over a set of $O(|V||E|)$

options for the ratio $\frac{p}{q}$ and, therefore will call Algorithm 2 on the order of $O(\log|V|)$ times. Thus, finding the critical set has a time complexity of $O(|V|^2|E|^{\frac{3}{2}}\log|V|)$. Each execution of Algorithm 4 is guaranteed to identify η^* on at least one edge and, therefore, Algorithm 5 will call Algorithm 4 no more than $|E|$ times. This provides an upper bound on the time complexity of computing the modulus in this way of $O(|V|^2|E|^{\frac{5}{2}}\log|V|)$.

4.4.5 Numerical computations

In this section we will discuss an illustrative computational example showing the steps of the algorithm. Let's consider the graph in Figure 4.5. This is the underlying graph of the famous Zachary's karate club network, and it is 1-connected. To begin, consider the graph shown in the upper left corner. 1-connectedness is due to the edge colored in red. This single edge is the first critical set found by the algorithm and let's denote it by $E_{Q_1^*}$. Every spanning tree must use that edge (a bridge). i.e., $E_{Q_1^*} := \{e \in E : \eta^*(e) = 1 = \|\eta^*\|_\infty\}$. The top middle portion of the figure is obtained by removing $E_{Q_1^*}$. After running the algorithm on that sub-graph whose edge set is $E\backslash E_{Q_1^*}$, we find the next critical set (colored in red) $E_{Q_2^*}$, where $E_{Q_2^*} := \{e \in E\backslash E_{Q_1^*} : \eta^*(e) = 1/2\}$. When the algorithm is run again on rest of the graph (top right portion of the figure) whose edge set now is $E\backslash(E_{Q_1^*} \cup E_{Q_2^*})$, the next critical set $E_{Q_3^*}$ is found (colored in red). Here, $E_{Q_3^*} := \{e \in E\backslash(E_{Q_1^*} \cup E_{Q_2^*}) : \eta^*(e) = 2/5\}$. So, we continue this process until we find all the critical sets and hence, no edges are left for removal. For this graph there are only five distinct $\eta^*(e)$ values, namely, 1, 1/2, 2/5, 3/8 and 6/17, and

$$\mathrm{Mod}_2(\Gamma) = \frac{680}{9969} \approx 0.068.$$

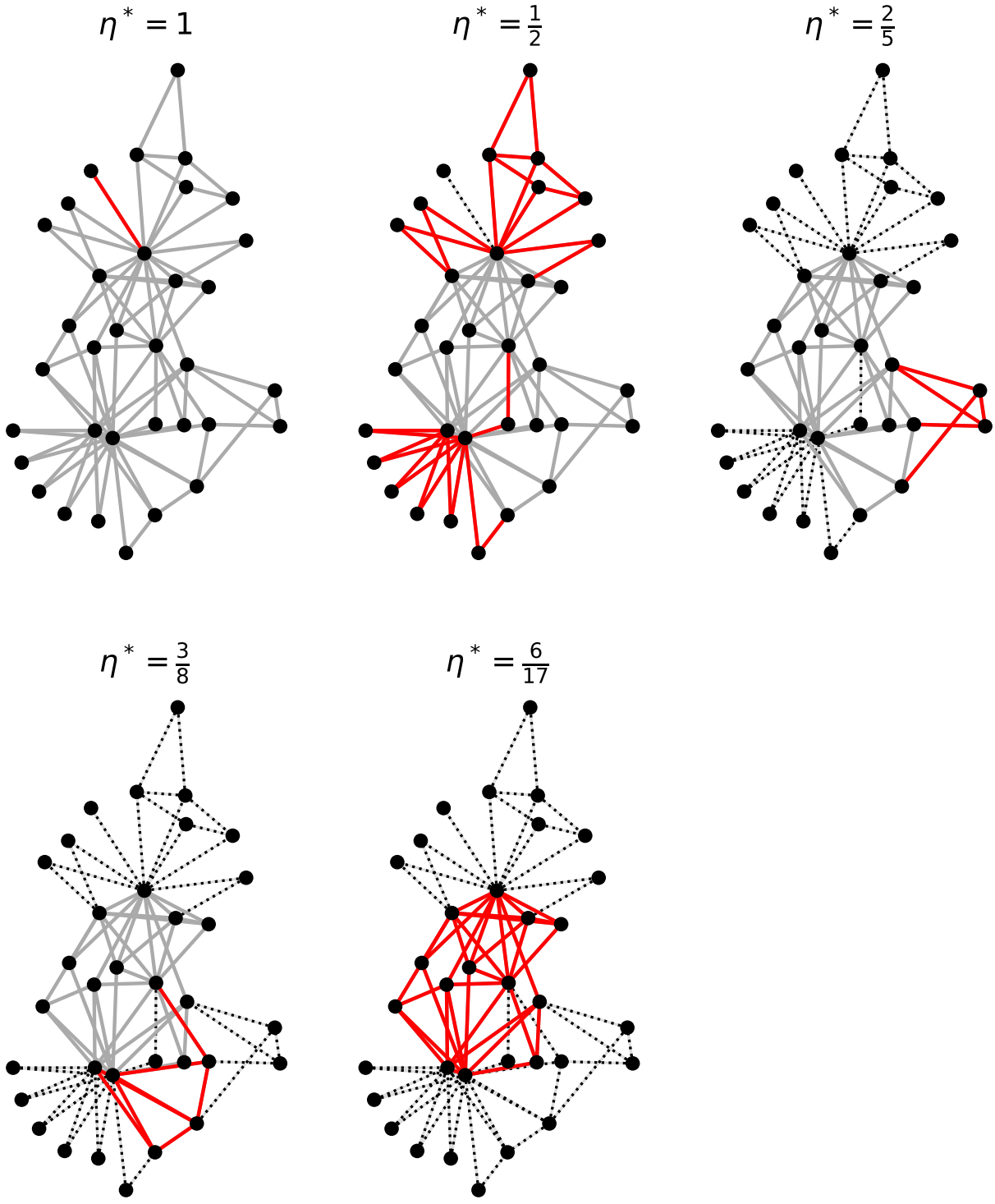


Figure 4.5: Spanning tree modulus algorithm in action.

Chapter 5

Future research and conclusion

5.1 Conclusion

In this dissertation, we have shown that the solution to the spanning tree modulus problem can provide a solution to a secure broadcast game between a broadcaster and an eavesdropper in a communication network. We made this connection explicit by proving a Nash Equilibrium when spanning tree modulus problem is posed as a minimum expected overlap problem.

Moreover, we implemented a new spanning tree modulus algorithm based on the secure broadcast game we solved. This algorithm recursively solves the broadcast game on subgraphs. We also proved a polynomial time worst-case upper bound for the time complexity of this algorithm. This is the first time that a time complexity bound for a spanning tree modulus algorithm was proved.

5.2 Future research

In the near future we will work on the question stated below in Section 5.2.1 pertaining specifically to our current research.

5.2.1 Fortifying the network

The relationship between 2-modulus and the secure broadcast game leads to the following question. Suppose the broadcaster has resources to fortify the network against the eavesdropper's attacks. How should these resources be used? We assume that these resources can be allocated in the form of edge weights σ. Hence, strengthening an edge with larger σ means it is harder to intercept on that edge by the eavesdropper. So, the next question that arises is how should we allocate these weights optimally. Since 2-modulus is a concave function in σ (see Lemma 5.2.1), it leads to the question of how to maximize 2-modulus under weight constraints.

So, we start by proving the following Lemma.

Lemma 5.2.1. *The function $\sigma \mapsto \operatorname{Mod}_{2,\sigma}(\Gamma)$ is concave.*

Proof. Let $\sigma_1, \sigma_2 \in \mathbb{R}^E_{>0}$ and let $\theta \in [0,1]$. Let ρ_1, ρ_2 and ρ^* be extremal densities for σ_1, σ_2 and $\sigma^* = \theta\sigma_1 + (1-\theta)\sigma_2$, respectively. So, σ^* is a convex combination of σ_1 and σ_2. Then

$$\begin{aligned}\theta \operatorname{Mod}_{2,\sigma_1}(\Gamma) + (1-\theta)\operatorname{Mod}_{2,\sigma_2}(\Gamma) &\le \theta \sum_{e\in E} \sigma_1(e)\rho^*(e)^2 + (1-\theta)\sum_{e\in E}\sigma_2(e)\rho^*(e)^2 \\ &= \sum_{e\in E}\sigma^*(e)\rho^*(e)^2 = \operatorname{Mod}_{2,(\theta\sigma_1+(1-\theta)\sigma_2)}(\Gamma).\end{aligned}$$

□

Now, we explain the minimum expected overlap problem for the weighted case. Notice that the summation in the right-hand side of (2.23) for the weighted case can be written as

$$\begin{aligned}\sum_{e\in E}\sigma(e)^{-1}\eta(e)^2 &= \sum_{e\in E}\sigma(e)^{-1}\left(\sum_{\gamma\in\Gamma}\mathcal{N}(\gamma,e)\mu(\gamma)\right)\left(\sum_{\gamma'\in\Gamma}\mathcal{N}(\gamma',e)\mu(\gamma')\right) \\ &= \sum_{\gamma\in\Gamma}\sum_{\gamma'\in\Gamma}\left(\sum_{e\in E}\sigma(e)^{-1}\mathcal{N}(\gamma,e)\mathcal{N}(\gamma',e)\right)\mu(\gamma)\mu(\gamma') \qquad (5.1) \\ &= \sum_{\gamma\in\Gamma}\sum_{\gamma'\in\Gamma}\sigma^{-1}(\gamma\cap\gamma')\mu(\gamma)\mu(\gamma') =: \mathbb{E}_\mu[\sigma^{-1}(\gamma\cap\gamma')].\end{aligned}$$

Here $\underline{\gamma}, \underline{\gamma'} \sim \mu$ are two independent Γ-valued random variables. The quantity $\sigma^{-1}(\gamma \cap \gamma')$ is the weighted intersection (overlap) of these two random sets and is, therefore, a random variable with expectation $\mathbb{E}_\mu[\sigma^{-1}(\gamma \cap \gamma')]$. This latter quantity is called the *expected weighted overlap* of $\underline{\gamma}$ and $\underline{\gamma'}$.

Using (5.1), the probabilistic interpretation (2.16) for the weighted case can be expressed as follows.

$$\mathrm{Mod}_{2,\sigma}(\Gamma)^{-1} = \min_{\mu \in \mathcal{P}(\Gamma)} \mathbb{E}_\mu[\sigma^{-1}(\gamma \cap \gamma')]. \tag{5.2}$$

Thus, computing 2-modulus in this case is equivalent to finding a pmf that minimizes the weighted expected overlap of two i.i.d. Γ-valued random variables. The right-hand side of (5.2) is called the *minimum expected weighted overlap* (MEWO) problem:

$$\begin{aligned} \text{minimize} \quad & \mathbb{E}_\mu[\sigma^{-1}(\gamma \cap \gamma')] \\ \text{subject to} \quad & \mu \in \mathcal{P}(\Gamma). \end{aligned} \tag{5.3}$$

Next, we discuss how to minimize this MEWO under weight constraints.

Theorem 5.2.1. *Let $G = (V, E, \sigma)$ be a graph and let Γ be a nontrivial finite family of objects on G with usage matrix $\mathcal{N}$ and $\Sigma = diag(\sigma_1, \sigma_2, \ldots, \sigma_{|E|})$ be the diagonal matrix with edge weights. Then we have,*

$$\max_{\substack{\sigma > 0 \\ \sigma^T \mathbf{1} = 1}} \mathrm{Mod}_{2,\sigma}(\Gamma) = \left(\min_{\substack{\eta = \mathcal{N}^T \mu \\ \mu \in \mathcal{P}(\Gamma)}} \eta(E)^2 \right)^{-1} \tag{5.4}$$

where $\eta(E) = \sum_{e \in E} \eta(e)$, and the maximizer $\sigma^*(e) = \frac{\eta(e)}{\eta(E)}$ (if $\eta > 0$).

Proof. First observe that solving $\max_{\substack{\sigma > 0 \\ \sigma^T \mathbf{1} = 1}} \mathrm{Mod}_{2,\sigma}(\Gamma)$ is equivalent to solving $\min_{\substack{\sigma > 0 \\ \sigma^T \mathbf{1} = 1}} \mathrm{Mod}_{2,\sigma}(\Gamma)^{-1}$. Define

$$F(\sigma_0) = \inf_{\substack{\sigma \geq \sigma_0 \mathbf{1} \\ \sigma^T \mathbf{1} \leq 1}} \inf_{\substack{\eta = \mathcal{N}^T \mu \\ \mu \in \mathcal{P}(\Gamma)}} \eta^T \Sigma^{-1} \eta.$$

If we have $\sigma_0 \geq \sigma_0'$ this would imply that $F(\sigma_0) \geq F(\sigma_0')$. So, we can write

$$\lim_{\sigma_0 \to 0^+} F(\sigma_0) = \inf_{\sigma_0 > 0} F(\sigma_0) = \inf_{\sigma_0 > 0} \inf_{\substack{\sigma \geq \sigma_0 \mathbf{1} \\ \sigma^T \mathbf{1} \leq 1}} \inf_{\substack{\eta = \mathcal{N}^T \mu \\ \mu \in \mathcal{P}(\Gamma)}} \eta^T \Sigma^{-1} \eta.$$

Now define

$$G(\eta) = \inf_{\sigma_0 > 0} \inf_{\substack{\sigma \geq \sigma_0 \mathbf{1} \\ \sigma^T \mathbf{1} \leq 1}} \eta^T \Sigma^{-1} \eta.$$

Then we have

$$\lim_{\sigma_0 \to 0^+} F(\sigma_0) = \inf_{\substack{\eta = \mathcal{N}^T \mu \\ \mu \in \mathcal{P}(\Gamma)}} G(\eta). \tag{5.5}$$

Note that, $\sigma \mapsto \eta^T \Sigma^{-1} \eta$ is a convex function of $\sigma \geq \sigma_0 \mathbf{1}$ for fixed $\sigma_0 > 0, \eta \geq 0$, and Slater's condition is satisfied when σ_0 is sufficiently small. The Lagrangian is

$$L(\sigma, \nu, \gamma) = \sum_{e \in E} \sigma(e)^{-1} \eta(e)^2 + \sum_{e \in E} \nu(e)(\sigma_0 - \sigma(e)) + \gamma \left(\sum_{e \in E} \sigma(e) - 1 \right).$$

From stationarity we have that

$$-\sigma^*(e)^{-2} \eta(e)^2 - \nu^*(e) + \gamma^* = 0 \quad \text{for all } e \in E. \tag{5.6}$$

Since $\nu^* \geq 0$ by the dual feasibility constraints, this means that

$$\gamma^* \geq \max_{e \in E} \sigma^*(e)^{-2} \eta(e)^2.$$

Since $\sigma^* \geq \sigma_0 > 0$ by primal feasibility and since $\eta(e)$ is positive on at least one edge, this implies that $\gamma^* > 0$.

If $\eta(e) = 0$ on some edge e, then (5.6) implies that $\nu^*(e) = \gamma^* > 0$, which implies that $\sigma^*(e) = \sigma_0$ by complementary slackness. Now we show that for $\sigma_0 > 0$ sufficiently small, we may satisfy the KKT conditions choosing $\sigma^*(e) > \sigma_0$ on the other edges (i.e., where $\eta(e) > 0$). If we do this, then complementary slackness requires that $\nu^*(e) = 0$ on these edges and, by (5.6) we must choose $\sigma^*(e) = \frac{\eta(e)}{\sqrt{\gamma^*}}$.

Let $Z(\eta) = |\{e : \eta(e) = 0\}|$. For feasibility of σ^*, we need

$$1 = \sum_{e \in E} \sigma^*(e) = Z(\eta)\sigma_0 + \frac{\eta(E)}{\sqrt{\gamma^*}} \implies \sqrt{\gamma^*} = \frac{\eta(E)}{1 - Z(\eta)\sigma_0}.$$

Here $\eta(E) = \sum_{e \in E} \eta(e)$.

This means that on edges where $\eta(e) > 0$, we should choose $\sigma^*(e) = (1 - Z(\eta)\sigma_0)\frac{\eta(e)}{\eta(E)}$. This choice will satisfy the assumption from earlier that $\sigma^*(e) > \sigma_0$ when $\eta(e) > 0$ if

$$\sigma_0 < \frac{1 - Z(\eta)\sigma_0}{\eta(E)} \min\{\eta(e) : e \in E, \eta(e) \neq 0\}.$$

Since the right-hand side converges to a positive value as $\sigma_0 \to 0$, this inequality is satisfied for sufficienlty small σ_0.

Thus, for sufficiently small σ_0, the construction above satisifies the KKT conditions and is, therefore, optimal. For these σ_0, we may evaluate $G(\eta)$ as follows.

On any edge where $\eta(e) = 0$,

$$\sigma^*(e)^{-1}\eta(e)^2 = 0 = (1 - Z(\eta)\sigma_0)^{-1}\eta(e)\eta(E).$$

On other edges,

$$\sigma^*(e)^{-1}\eta(e)^2 = (1 - Z(\eta)\sigma_0)^{-1}\eta(e)\eta(E),$$

for our choice of σ^*. So,

$$\begin{aligned} G(\eta) &= \inf_{\sigma_0 > 0} \inf_{\substack{\sigma \geq \sigma_0 \mathbf{1} \\ \sigma^T \mathbf{1} \leq 1}} \eta^T \Sigma^{-1} \eta = \inf_{\sigma_0 > 0} \sum_{e \in E} \sigma^*(e)^{-1}\eta(e)^2 \\ &= \lim_{\sigma_0 \to 0^+} \sum_{e \in E} (1 - Z(\eta)\sigma_0)^{-1}\eta(e)\eta(E) \\ &= \eta(E) \sum_{e \in E} \eta(e) = \eta(E)^2. \end{aligned}$$

The theorem follows from (5.5). □

Proposition 5.2.2. When Γ is the family of spanning trees on G

$$\max_{\substack{\sigma>0 \\ \sigma^T\mathbf{1}=1}} \mathrm{Mod}_{2,\sigma}(\Gamma) = \frac{1}{(|V|-1)^2}. \tag{5.7}$$

Proof. The proof is simple. For spanning trees, if μ is any pmf and $\eta = \mathcal{N}^T\mu$,

$$\eta(E) = \eta^T\mathbf{1} = \mu^T\mathcal{N}\mathbf{1} = \mu^T(|V|-1)\mathbf{1} = |V|-1. \tag{5.8}$$

□

Even though the proof is simple this shows that maximizing 2-modulus can be done by choosing any pmf that assigns a positive expected usage on each edge, i.e. $\eta(e) > 0$. Such an η satisfies (5.8) and the corresponding σ^* takes the value $\sigma^*(e) = \eta(e)/\eta(E) > 0$.

So, our near future research is to do a thorough investigation about how this solution helps us modify the existing mathematical model we have for the secure broadcast game and fortify the network with edge weights that correspond to resource allocation by the broadcaster with a meaningful interpretation.

Bibliography

[1] Ahlfors, L. V. *Conformal invariants: topics in geometric function theory*, vol. 371. American Mathematical Society, Providence, RI, 2010.

[2] Albin, N., Brunner, M., Perez, R., Poggi-Corradini, P., and Wiens, N. Modulus on graphs as a generalization of standard graph theoretic quantities. *Conformal Geometry and Dynamics of the American Mathematical Society 19*, 13 (2015), 298–317.

[3] Albin, N., Clemens, J., Hoare, D., Poggi-Corradini, P., Sit, B., and Tymochko, S. Fairest edge usage and minimum expected overlap for random spanning trees. *arXiv preprint arXiv:1805.10112* (2018).

[4] Albin, N., Kottegoda, K., and Poggi-Corradini, P. Spanning tree modulus for secure broadcast games. *Networks* (2020), 1–16.

[5] Albin, N., and Poggi-Corradini, P. Minimal subfamilies and the probabilistic interpretation for modulus on graphs. *The Journal of Analysis 24*, 2 (2016), 183–208.

[6] Cheriyan, J., and Mehlhorn, K. An analysis of the highest-level selection rule in the preflow-push max-flow algorithm. *Information Processing Letters 69*, 5 (1999), 239–242.

[7] Chopra, S. On the spanning tree polyhedron. *Operations Research Letters 8*, 1 (Feb 1989), 25–29.

[8] Cunningham, W. H. Optimal attack and reinforcement of a network. *Journal of the ACM (JACM) 32*, 3 (1985), 549–561.

[9] Duffin, R. The extremal length of a network. *Journal of Mathematical Analysis and Applications 5*, 2 (1962), 200–215.

[10] Gueye, A., Marbukh, V., and Walrand, J. C. Towards a metric for communication network vulnerability to attacks: A game theoretic approach. In *International Conference on Game Theory for Networks* (2012), Springer, pp. 259–274.

[11] Gueye, A., Walrand, J. C., and Anantharam, V. Design of network topology in an adversarial environment. In *International Conference on Decision and Game Theory for Security* (2010), Springer, pp. 1–20.

[12] Gueye, A., Walrand, J. C., and Anantharam, V. A network topology design game: How to choose communication links in an adversarial environment? In *Proc. of the 2nd International ICST Conference on Game Theory for Networks, GameNets* (2011), vol. 11.

[13] Haïssinsky, P. Empilements de cercles et modules combinatoires. *Annales de l'Institut Fourier 59*, 6 (2009), 2175–2222.

[14] Laszka, A., and Gueye, A. Quantifying network topology robustness under budget constraints: General model and computational complexity. In *International Conference on Decision and Game Theory for Security* (2013), Springer, pp. 154–174.

[15] Laszka, A., Szeszlér, D., and Buttyán, L. Game-theoretic robustness of many-to-one networks. In *International Conference on Game Theory for Networks* (2012), Springer, pp. 88–98.

[16] Nash, J. F. Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences 36*, 1 (1950), 48–49.

[17] Rockafellar, R. *Convex Analysis: (PMS-28)*. Princeton Landmarks in Mathematics and Physics. Princeton University Press, 2015.

[18] Schramm, O. Square tilings with prescribed combinatorics. *Israel Journal of Mathematics 84*, 1-2 (1993), 97–118.

[19] Schwartz, G. A., Amin, S., Gueye, A., and Walrand, J. Network design game with both reliability and security failures. In *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (2011), IEEE, pp. 675–681.

[20] Szeszlér, D. Security games on matroids. *Mathematical Programming 161*, 1-2 (2017), 347–364.