Multishot Capacity of Adversarial Networks

Julia M. Shapiro

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Masters of Science
in
Mathematics

Gretchen Matthews, Chair
Mark Shimozono
Hiram López

May 4, 2024
Blacksburg, Virginia

Keywords: network decoding, adversarial network, multishot capacity

Multishot Capacity of Adversarial Networks

Julia M. Shapiro

(ABSTRACT)

Adversarial network coding studies the transmission of data over networks affected by adversarial noise. In this realm, the noise is modeled by an omniscient adversary who is restricted to corrupting a proper subset of the network edges. In 2018, Ravagnani and Kschischang established a combinatorial framework for adversarial networks. The study was recently furthered by Beemer, Kilic and Ravagnani, with particular focus on the one-shot capacity: a measure of the maximum number of symbols that can be transmitted in a single use of the network without errors. In this thesis, both bounds and capacity-achieving schemes are provided for families of adversarial networks in multiple transmission rounds. We also demonstrate scenarios where we transmit more information using a network multiple times for communication versus using the network once. Some results in this thesis are joint work with Giuseppe Cotardo (Virginia Tech), Gretchen Matthews (Virginia Tech) and Alberto Ravagnani (Eindhoven University of Technology).

Multishot Capacity of Adversarial Networks

Julia M. Shapiro

(GENERAL AUDIENCE ABSTRACT)

We study how to best transfer data across a communication network even if there is adversarial interference using network coding. Network coding is used in video streaming, autonomous vehicles, 5G and NextG communications, satellite networks, and Internet of Things (IoT) devices among other applications. It is the process that encodes data before sending it and decodes it upon receipt. It brings advantages such as increased network efficiency, improved reliability, reduced redundancy, enhanced resilience, and energy savings. We seek to enhance this valuable technique by determining optimal ways in which to utilize network coding schemes. We explore scenarios in which an adversary has partial access to a network. To examine the maximum data that can be communicated over one use of a network, we require the intermediate parts of the network process the information before forwarding it in a process called network decoding. In this thesis, we focus on characterizing when using a network multiple times for communication increases the amount of information that is received regardless of the worst-case adversarial attack, building on prior work that shows how underlying structure influences capacity. We design efficient methods for specific networks, to communicate at capacity.

Dedication

This thesis is dedicated to my family. Thank you for your continuous support of me.

Acknowledgments

This thesis marks the end for my degree of Master of Science in Mathematics at Virginia Tech. I will be continuing on as a Ph.D student in the Fall of 2024. I would like to take this opportunity to send out my gratitude to all that helped me with this thesis.

First and foremost, I would like to express my gratitude to my outstanding supervisor, Gretchen Matthews, for all the support and encouragement I received throughout my first two years at Virginia Tech. From the moment I arrived at Virginia Tech, Your positive energy, knowledge, experience and dedication have truly been a source of inspiration for me. I am amazed by the things you do and am so happy have an advisor who believes in me, consistently supports me through the highs and lows and takes any chance to tell me your proud of me. I appreciate everything you do for me. I thank you for always being there for me, willingness to lend a listening ear, and your honesty. Most importantly, for believing in me even when I was having a hard time adjusting to graduate school and lending a hand whenever I need. I am so lucky to be a part of our research group. I feel fortunate for the amazing opportunities to grow my skills, attend academic events and outreach you provided me over the past two years. I look forward to what we will accomplish together during my Ph.D.

I would like to thank Giuseppe Cotardo for his endless support, guidance and effort to make me feel apart of the group. Thank you for the countless hours you spent with me on this project, for teaching me how to write proofs (and in English), for practicing with me before presentations and for giving me advice at how to succeed in my Ph.D. Thank you for always pushing me to apply and attend many academic events, get involved in organizing seminars and for believing in me when I didn't believe in myself.

I would like to thank Alberto Ravagnani for his continuous support on this project

and willingness to help me with the background whenever I need. I am fortunate to have the opportunity to collaborate with you and am excite to work on future projects together.

I would like to thank my colleague Nic Swanson for being supportive of me and the willingness to always lend a hand when I need help. I am so glad we had the opportunity to take courses and experience graduate school together. I know you will do great things bestie.

I would also like to thank the other graduate students for being there for me (especially Anayse, Mason and Nic), forming study groups for tough classes and the countless game nights and potlucks. I look forward to our time together during my PhD.

A special thanks to my family and friends for being my number one fan and always supporting me through this journey. Thank you to my parents Sean and Teresa Shapiro, for always believing in me since I was a little girl and showing me how proud you were of me. Thank you for the countless hours moving in to new apartments and traveling for my internships and moving to graduate school and the continuous support everyday. I couldn't do this without you.

Contents

List of Figures

List of Symbols and Notation

$\boldsymbol{A}_{\mathscr{N}}$ The adversary

$\mathscr{A}$ The alphabet (set of symbols we are using)

$\mathbf{A}^{m\times n}$ The matrix of dimension $m \times n$

$\mathbb{F}_q$ A finite field with q elements.

$\mathscr{D}$ The Diamond Network

$\mathscr{S}$ The Mirrored Diamond Network

$\mathscr{E}$ The set of edges of a network.

$\mathscr{E}'$ An edge-cut.

$\mathscr{F}$ A network code.

$\mathscr{N}$ A general network.

$\mathscr{U}$ The set of edges the adversary can corrupt.

Ω The channel associated to $\mathscr{N}$

Ω^i The ith power channel associated to $\mathscr{N}$

$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ The one-shot capacity of an adversarial network.

$C_i(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ The i-shot (or multishot) capacity of a network.

$d_{\mathrm{H}}(x, y)$ is the Hamming distance between two codewords.

C A code.

Chapter 1

Introduction

Network coding is a communication strategy in computer networks where intermediate nodes in the network are allowed to perform coding operations on the data packets they receive. It was established in 2000 by Cai, Li and Yeung in [9]. Unlike traditional routing, where nodes simply forward packets, network coding enables nodes to combine multiple incoming packets algebraically before forwarding them. Some references are [4, 6, 8, 10, 11, 12, 13, 14, 15, 16]. This approach can enhance network efficiency by increasing throughput, improving reliability, enhancing security, and optimizing resource utilization. In [1], the authors provide new combinatorial techniques in the context of adversarial noise. In [2, 3, 5], the authors presented the problem of determining the network capacity in scenarios where errors may occur on a subset of the network edges and the concept of *network decoding* was introduced as an essential strategy for achieving capacity in networks with restricted adversaries. The treatment provided addresses the worst-case errors due to adversarial noise and provides guarantees in networks where there could be random noise, or both. The adversary is assumed to be *omniscient* meaning they may design attacks given full knowledge of the network topology, of the symbols sent along all its edges, and of the operations performed at the intermediate nodes due to the choice of families of functions known as the *network code*. Previous work focuses heavily on the one-shot capacity of a network, that is, the maximum number of symbols that can be sent over a network without errors.

In this thesis, we initiate the study of the multishot capacity of networks with restricted adversaries, that is, the maximum number of symbols that can be transmitted from one or multiple source(s) to the terminal(s). We restrict to the one source case for our results. Our goal is to compute the largest number of information packets that can be correctly received by all terminals on average over multiple uses of the network, meaning more than once. We focus on the Diamond Network(s) a family of networks introduced in [5] to determine the criteria for when there is a gain in capacity over multiple uses of a network. We show that the multishot capacity of the Diamond Network and the butterfly network [5] have a strict increase in comparison to its one-shot capacity in one adversarial model. On the other hand, the maximum capacity of the Mirrored Diamond Network and generalizations is the same over multiple uses of these networks.

The purpose of this thesis is to build the theoretical framework needed to understand the multishot capacity of known adversarial networks that are relatively vulnerable to noise provided by an adversary, differentiating our results and strategies from those available in the one-shot regime. We will compute the capacity of the Diamond Network and the Mirrored Diamond Network for different restrictions on the adversary. For some families of networks introduced in [5], the one-shot capacity has not been computed and requires new combinatorial techniques. We will derive strategies for the multishot capacity of some of these networks, without knowing the one-shot capacity.

Chapter 2

Motivation

The main questions are what is the largest number of packets of alphabet symbols that can be transmitted and correctly received over multiple transmission rounds and is there a gain in capacity with multiple uses? We are interested in understanding whether multiple uses of a communication network increases the capacity in comparison to using the communication strategy provided in the one-shot capacity regime. With some strategies, there is an immediate gain provided in the multiple transmission rounds. Consider the network $\mathscr{N}$ in Figure 2.1.

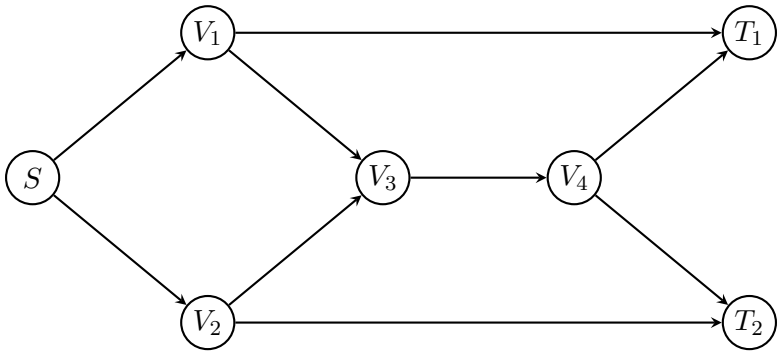

Figure 2.1: Butterfly Network $\mathscr{N}$

We assume that there is no adversary attacking this network. We will use routing as the preferred strategy of sending information over the network $\mathscr{N}$ and will demonstrate that there is a gain in sending information over this network in two rounds. Therefore, using this network multiple times provides an advantage. Some references on network coding theory and routing are [9, 16]. Figure 2.2 demonstrates sending information

over the network in one transmission round using routing.

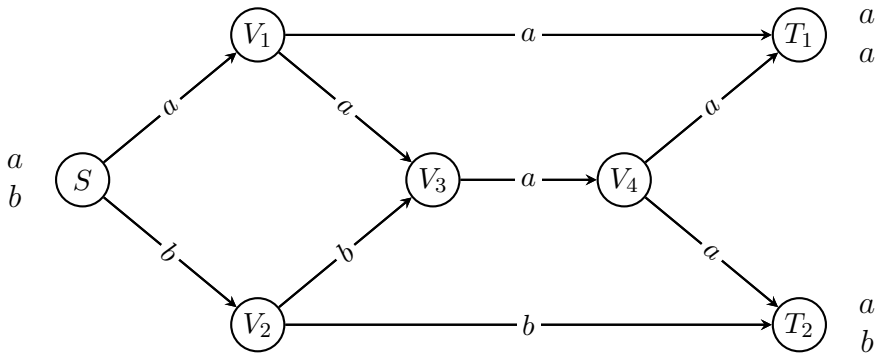

Figure 2.2: Network $\mathscr{N}$ with Strategy for One Transmission Round

We see that if we route a at V_3, terminal T_1 only receives the symbol a whereas terminal T_2 receives a and b. Alternatively, if b is routed at V_3, then terminal T_1 receives a and b and terminal T_2 only receives a. In either case, it is not possible for both T_1 and T_2 to receive both a and b. With this strategy, the most amount of symbols that can be sent over one transmission round without errors is 1 symbol using traditional well-known bounds on routing.

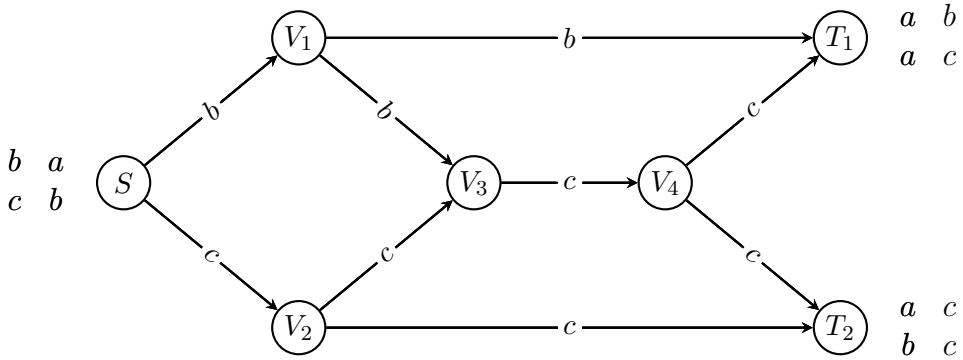

Figure 2.3: Network $\mathscr{N}$ with strategy for two transmission rounds.

In contrast, Figure 2.3 demonstrates that over 2 transmission rounds, both receivers (terminals) receive three symbols over two transmission rounds. In the first round, the source sends a and b, routing a as in Figure 2.2 with terminal T_1 receiving a and

terminal T_2 receiving a and b. Therefore over one round, only one symbol (a) can be decoded. In the second round, the source sends b and c, and strategically routes c over V_3, and both terminals T_1 and T_2 receive the symbols a, b and c over 2 transmission rounds. The amount of information that can be sent and decoded without errors in this case over two transmission rounds is $\frac{3}{2}$, which is greater than using the strategy from the first round twice. This contrast is the motivation for the work in this thesis.

2.1 Contributions

Some results of this thesis are from a collaboration that was published and presented here.

G. Cotardo, G. L. Matthews, A. Ravagnani, and J. Shapiro, Multishot adversarial network decoding, 2023 59th Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2023, pp. 1-8. doi: 10.1109/Allerton58177.2023.10313407.

Chapter 3

Background/Literature Review

3.1 Preliminaries

Throughout the thesis, let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. We start with some necessary definitions and notation.

Definition 3.1. Let G be a graph and let $\mathscr{E}$ be the set of edges of G. An edge cut of G is a set of edges $\mathscr{E}' \subseteq \mathscr{E}$ such that the edge deletion $G \setminus \mathscr{E}'$ is disconnected.

We now generally defining codes and functions associated to them.

Definition 3.2. (Code) A subset $C \subseteq \mathbb{F}_q^n$ is a code of length n. We say that C is an $(n, M, d)_q$ code if $|C| = M$ and $d = \min\{wt(c)|c \neq 0\}$, where $wt(c)$ is the number of nonzero coordinates of c, over the alphabet $\mathbb{F}_q$.

Definition 3.3. (Linear Code) A code C is a $[n, k, d]$ **linear code** over $\mathbb{F}_q$ if C is an $\mathbb{F}_q$ subspace of $\mathbb{F}_q^n$ and $\dim_{\mathbb{F}}(C) = k$.

A code C is able to recover $d-1$ erasures using information from all other $n - d + 1$ coordinates of the code.

Definition 3.4. (Non-linear Code) A code C is nonlinear if it is not an $\mathbb{F}_q$ subspace of $\mathbb{F}_q^n$.

We now define the Hamming distance and the rate of a code.

Definition 3.5. (Hamming Distance) Given two elements $x, y \in \mathbb{F}_q^n$, the Hamming distance between x and y, denoted by $d_{\mathrm{H}}(x, y)$, is the number of positions in which x and y differ.

Definition 3.6. The rate of an $[n, k, d]$ code is

$$r = \frac{k}{n}.$$

Let Enc : $M \to C$ be an injective function that takes a message in M to a codeword in C and let Dec : $\mathbb{F}_q^n \to M$ be a function that takes a corrupted codeword to a message in M. We now define $t-$error correcting code.

Definition 3.7. A code C is $t-$error correcting if for every $x \in M$ and every y such that $d_{\mathrm{H}}(y, \mathrm{Enc(x)}) \leq t$, $\mathrm{Dec}(y) = x$.

We next define a traditional bound on codes.

Theorem 3.8. *(Singleton Bound [18]). Let C be an $[n, k, d]$ code. Then*

$$k \leq n - d + 1.$$

Codes that attain this bound are called ***Maximum Distance Separable (MDS)*** *codes.*

We will discuss the Singleton-bound ported to network theory in Chapter 4 and will provide an extension of this bound to the multishot setting.

We use the following notation throughout this thesis:

- $\mathscr{N}$ is a network.

- $\mathscr{A}$ is the chosen alphabet (set of symbols).
- $\boldsymbol{A}_{\mathscr{N}}$ is the adversary
- $A^{m\times n}$ is a matrix of dimension $m \times n$.
- $\mathbb{F}_q$ is a finite field with q elements.
- $d_{\mathrm{H}}(x, y)$ is the Hamming distance between two codewords.
- $\mathscr{E}$ is a set of edges of a network.
- $\mathscr{E}'$ is an edge-cut.
- Ω is the channel associated to $\mathscr{N}$.
- Ω^i is the $i-$th power channel associated to $\mathscr{N}$.
- $C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ is the one-shot capacity of an adversarial network.
- $C_i(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ is the i-shot (or multishot) capacity of a network.
- $\mathscr{F}$ is a network code.
- C is a code.
- $\mathrm{H}_{\mathscr{N}}$ is a channel describing the action of the adversary on $\mathscr{N}$.
- $\mathscr{U}$ is the set of edges the adversary can corrupt.

3.2 Network Coding

In this section, we discuss results from network coding. This section will be split into two parts: Linear network coding and nonlinear network coding. We first define a combinatorial network.

Definition 3.9. A **network** is a 4-tuple $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \boldsymbol{S}, \boldsymbol{T})$ where:

1. $(\mathscr{V}, \mathscr{E})$ is a directed, acyclic and finite multigraph;
2. $\boldsymbol{S} \subseteq \mathscr{V}$ is the set of **sources**;
3. $\boldsymbol{T} \subseteq \mathscr{V}$ is the set of **terminals**.

We also assume the following:

4. $|\mathbf{S}| \geq 1$ and there exists a directed path from any $S \in \mathbf{S}$ to $T \in \mathbf{T}$.
5. $|\mathbf{T}| \geq 1$ and $\mathbf{S} \cap \mathbf{T} = \emptyset$.
6. For every $V \in \mathscr{V} \setminus (\mathbf{S} \cup \mathbf{T})$, there exists a directed path from $S \in \mathbf{S}$ to V and from V to a $T \in \mathbf{T}$.

The elements in the set $\mathscr{V}$ are called **vertices** (or **nodes**), and the elements in $\mathscr{E}$ are called **edges**. The elements in $V \in \mathscr{V} \setminus (\mathbf{S} \cup \mathbf{T})$ are referred to as the **intermediate vertices** (or **intermediate nodes**). For an intermediate vertex V, we denote the set of incoming and outgoing edges as $\text{in}(V)$ and $\text{out}(V)$. Their cardinalities are the **indegree** and **outdegree** of V denoted $\deg^-(V)$ and $\deg^+(V)$.

Definition 3.10. A network $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \boldsymbol{T})$ is **simple** if it has only one terminal T, i.e. $\boldsymbol{T} = \{T\}$.

For this thesis, we let $\mathbf{S} = \{S\}$, meaning we only consider networks with one-source. We consider the model in which each edge of the network $\mathscr{N}$ carries one element from an **alphabet** $\mathscr{A}$, $|\mathscr{A}| \geq 2$. The intermediate vertices V in the network $\mathscr{N}$ receive symbols from $\mathscr{A}$ over the incoming edges, process them according to a chosen set of functions, and then outputs the information over the outgoing edges. We model errors in the transmission as presented by an ominscent adversary A who can change the symbol on up to t edges from a fixed subset $\mathscr{U} \subseteq \mathscr{E}$ that is fixed. The adversary can change a symbol sent across one of the edges of $\mathscr{U}$ to any other symbol of $\mathscr{A}$. The pair $(\mathscr{N}, \mathbf{A})$, where $\boldsymbol{A}$ is the adversary is an **adversarial network**.

The next definition characterizes the edges of a network.

Definition 3.11. The edges $\mathscr{E}$ of a network $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ can be partially ordered as follows. Let $e, e' \in \mathscr{E}$. We say that e precedes e if there exists a directed path in $\mathscr{N}$ that starts with e and ends with e . The notation is $e \preceq e$.

Notice that the partial order $\preceq$ on $\mathscr{E}$ can be extended to a total order $\leq$ that is not necessarily unique and is a well known fact in graph theory. The total order extension satisfies the property: $e \preceq e'$ implies $e \leq e'$. Throughout this thesis, we assume that the total order has been fixed and illustrate the total order by the labeling of the edges.

3.2.1 Linear Network Coding

In this section we will discuss linear network coding. **Linear network coding** is a networking technique in which intermediate vertices transfer received data from source nodes to sink nodes using linear combinations.

Consider the Butterfly Network $\mathscr{N}$ with the strategy depicted in the Figure 4.1. It can be seen that using linear combinations of the information x_1 and x_2 at V_3 allows

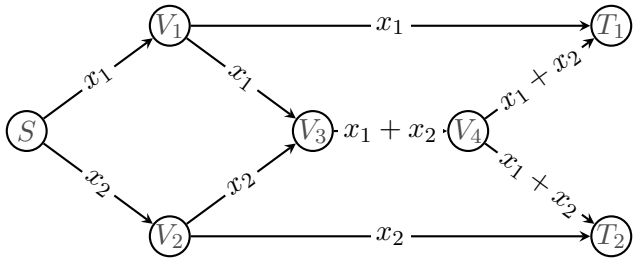

Figure 3.1: Butterfly Network $\mathscr{N}$ with linear network coding strategy for one transmission round.

for each receiver (terminal) to decode two symbols. Indeed, terminal T_1 receives x_1 and may recover x_2 since $x_2 = x_1 + x_2 - x_1$. Similarly, T_2 receives x_2 and may recover x_1 since $x_1 = x_2 + x_1 - x_2$. We now define linear network codes, to be used by the intermediate nodes so they can process information before forwarding.

Definition 3.12. (Linear Network Code) Let $\mathscr{A} = \mathbb{F}_q^m$ and some $m \geq 1$ an integer. A **linear network code** is a family of functions $\mathscr{F} = \{\mathscr{F}_V : V \in \mathscr{V} \setminus \{\mathbf{S} \cup \mathbf{T}\}\}$, where $\mathscr{F}_V : \mathscr{A}^{\text{out}(S)} \to \mathscr{A}^{\text{in}(V)}$, $x \mapsto x^T L_v$ for some matrix $L_v \in \mathbb{F}_q^{|\text{in}(V)| \times |\text{out}(V)|}$.

The **rate** or (one-shot capacity) of a network can be thought of as the maximum number of symbols that can be sent and decoded over a network in one transmission round without errors. The next result provides an upper bound on the rate.

Definition 3.13. The min-cut$(\mathbf{S}, \mathbf{T})$ is the minimum number of edges disconnecting $S \in \mathbf{S}$ from $T \in \mathbf{T}$.

Theorem 3.14. *(Min-cut bound [9]). The rate r of $\mathscr{N} = (V, \mathscr{E}, \mathbf{S}, \mathbf{T})$ with $|\mathbf{S}| = 1$ satisfies*

$$r \leq \min \text{min-cut}(S, T)$$

Definition 3.15. An optimal strategy on a network $\mathscr{N}$ is a strategy that attains the Min-cut bound.

Note that using the previous theorem, the maximum rate of the Butterfly Network in Figure 2.1 is 2 since the minimum edge cut is 2. Therefore, the strategy provided in Figure 4.1 is optimal.

It was shown in [7] that for a sufficiently large finite field $\mathbb{F}_q$, the bound in Theorem 3.14 is achievable using linear network coding. The result stated formally is as follows:

Theorem 3.16. *[7] Let $\mathscr{N} = (V, \mathscr{E}, S, \mathbf{T})$ be a single-source network. A rate (or capacity) of*

$$min_{T \in \mathbf{T}} \text{min-cut}(S, T)$$

is achievable, for sufficiently large q, using linear network coding techniques.

3.2.2 Nonlinear Network Coding

Definition 3.17. An (adversarial) channel is a map $\Omega : \mathscr{X} \to 2^{\mathscr{Y}} \setminus \{\emptyset\}$, where $\mathscr{X}$ and $\mathscr{Y}$ are finite non-empty sets. The sets $\mathscr{X}$ and $\mathscr{Y}$ are called the input and output alphabets. The We denote this adversarial channel by $\Omega : \mathscr{X} \dashrightarrow \mathscr{Y}$. An outer code $C \subset A^{\deg^+(S)}$ (finish). We say that a code $C \subseteq \mathscr{X}$ is called unambiguous (or good for) a channel if for $x, x' \in C$, with $x \neq x'$,

$$\Omega(x) \cap \Omega(x') = \emptyset.$$

Next we define the one-shot capacity of a channel Ω.

Definition 3.18. The (one-shot) capacity $C_1(\Omega)$ of a channel $\Omega : \mathscr{X} \dashrightarrow \mathscr{Y}$ is the real number

$$C_1(\Omega) := \max\{\log_2(|C|) : C \subseteq \mathscr{X} \text{ is good for } \Omega\}.$$

The next example demonstrates the one-shot capacity of an adversarial network.

Example 3.19. Let $\mathscr{X} = \mathbb{F}_2^3$. Suppose there is an adversary who is capable of corrupting at most one of the components of any $x \in \mathbb{F}_2^3$. The action of the adversary can be described by the channel $H : \mathbb{F}_2^3 \dashrightarrow \mathbb{F}_2^3$ defined by

$$H(x) := \{y \in \mathbb{F}_2^3 \mid d_{\mathrm{H}}(x, y) \leq 1\}$$

for all $x \in \mathbb{F}_2^3$. The code $C = \{(000), (111)\}$ is a good code for H, and there is no good code with larger cardinality. Therefore $C_1(H) = 1$.

We next introduce the *product* and *concatenation* of channels defined in [1].

Definition 3.20. Let $\Omega_1 : \mathscr{X}_1 \dashrightarrow \mathscr{Y}_1$ and $\Omega_2 : \mathscr{X}_2 \dashrightarrow \mathscr{Y}_2$ be channels and assume that $\mathscr{Y}_1 \subseteq \mathscr{X}_2$. The **product** of Ω_1 and Ω_2 is the channel $\Omega_1 \times \Omega_2 : \mathscr{X}_1 \times \mathscr{X}_2 \dashrightarrow \mathscr{Y}_1 \times \mathscr{Y}_2$ defined by

$$(\Omega_1 \times \Omega_2)(x_1, x_2) := \Omega_1(x_1) \times \Omega_2(x_2),$$

for all $(x_1, x_2) \in \mathscr{X}_1 \times \mathscr{X}_2$.

Definition 3.21. The **concatenation** of Ω_1 and Ω_2 is the channel $\Omega_1 \blacktriangleright \Omega_2 : \mathscr{X}_1 \dashrightarrow \mathscr{Y}_2$ defined by

$$(\Omega_1 \blacktriangleright \Omega_2)(x) := \bigcup_{y \in \Omega_1(x)} \Omega_2(y).$$

The next definition describes the $i-$th power channel, which will be useful when computing the multishot capacity in Chapter 4.

Definition 3.22 ([1, Definition 10])**.** Let $i \geq 1$ be an integer. The **i-th power** of a channel $\Omega : \mathscr{X} \dashrightarrow \mathscr{Y}$ is the channel

$$\Omega^i : \mathscr{X}^i \dashrightarrow \mathscr{Y}^i$$

where $\Omega^i := \Omega \times \ldots \times \Omega$ is the $i-$fold product.

We note that Ω^i models i uses of a network. We now introduce what it means for channels to be finer or coarser than one another.

Definition 3.23. Let Ω_1,$\Omega_2 : \mathscr{X} \dashrightarrow \mathscr{Y}$ be channels. We say that Ω_1 is finer than Ω_2 (or that Ω_2 is coarser than Ω_1) if $\Omega_1(x) \subseteq \Omega_2(x)$ for all $x \in \mathscr{X}$. In this case, we write $\Omega_1 \leq \Omega_2$.

Proposition 3.24. *[5, Proposition 3.6] Let $\Omega_1, \Omega_2 : \mathscr{X} \dashrightarrow \mathscr{Y}$ be channels with $\Omega_1 \leq \Omega_2$ as in the previous definition. Then $C_1(\Omega_1) \geq C_1(\Omega_2)$.*

The next definition defines the family of functions inside of the intermediate nodes.

Definition 3.25. (Network Code) Let $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ be a network. A **network code** $\mathscr{F}$ for $\mathscr{N}$ is a set of functions $\{\mathscr{F}_V : V \in \mathscr{V} \setminus \{\{S\} \cup \mathbf{T}\}\}$, where $\mathscr{F}_V : \mathscr{A}^{\text{in}(V)} \to \mathscr{A}^{\text{out}(V)}$ for all V.

The functions in $\mathscr{F}$ describe how $\mathscr{N}$ processes the information in each intermediate node coming from the incoming edges.

The next theorem provides an upper bound on the amount of information that can be sent in one transmission round, meaning the one-shot capacity.

Theorem 3.26. *[4, Theorem 4] Let $(\mathscr{N}, \boldsymbol{A})$ be a single source network and suppose $\boldsymbol{A}$ can corrupt up to t edges and that there exists a $t-$error correcting code for the network with source alphabet $\mathscr{A}$. The one-shot capacity of $\mathscr{N}$ satisfies*

$$C_1(\mathscr{N}, \boldsymbol{A}) \leq \max\left\{0, \min_{1 \leq i \leq k} \{\text{min-cut}(S, T_i)\} - 2t\right\}$$

where k is the number of terminals $T \in \mathbf{T}$.

The next two definitions compare edge cuts.

Definition 3.27. Let $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ be a network and let $\mathscr{E}_1, \mathscr{E}_2 \subseteq \mathscr{E}$ be subsets of edges of $\mathscr{N}$. We say that $\mathscr{E}_1$ **precedes** $\mathscr{E}_2$ if every path from S to an edge of $\mathscr{E}_2$ contains an edge of $\mathscr{E}_1$.

Definition 3.28. [5, Definition 8.1] Let $\mathscr{N}$ be a network and let $\mathscr{E}_1, \mathscr{E}_2 \subseteq \mathscr{E}$ be edge cuts such that $\mathscr{E}_1$ precedes $\mathscr{E}_2$. For some $e \in \mathscr{E}_2$ and $e' \in \mathscr{E}_1$, we can say that e' is an **immediate predecessor of** e **in** $\mathscr{E}_1$ if $e' \preccurlyeq e$ and there is no $e'' \in \mathscr{E}_1$ with $e' \preccurlyeq e'' \preccurlyeq e$ and $e' \neq e''$.

In [1], the authors provide a general method to port bounds for traditional channels to the networking context. The next result states the ported version of the Singleton Bound [18], providing an upper-bound on the one-shot capacity of an adversarial network.

Theorem 3.29 (The Singleton Cut-Set Bound [1])**.** *Let $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ be a network and $\mathscr{E}' \subseteq \mathscr{E}$ be an edge set of $\mathscr{N}$. Assume that an adversary $\boldsymbol{A}_{\mathscr{N}}$ can corrupt up to $t \geq 0$ edges from a subset $\mathscr{U} \subseteq \mathscr{E}$. Then the one-shot capacity of an adversarial network satisfies*

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq \min_{T \in \boldsymbol{T}} \min_{\mathscr{E}'} \left(|\mathscr{E}' \setminus \mathscr{U}| + \max\{0, |\mathscr{E}' \cap \mathscr{U}| - 2t\} \right)$$

where $\mathscr{E}' \subseteq \mathscr{E}$ ranges over all edge-cuts between S and T.

Remark 3.30. Notice that Theorem 3.26 is a corollary of the previous theorem. Namely, $\mathscr{U} = \mathscr{E}$ recovers the bound in Theorem 3.26.

The next example demonstrate the importance of the Singleton Cut-Set Bound.

Example 3.31. Suppose we have the network $\mathscr{N}$ in Figure 3.1. If we assume that there is no adversary attacking on the network ($t = 0$), then $\mathscr{U} = \emptyset$ and both bounds

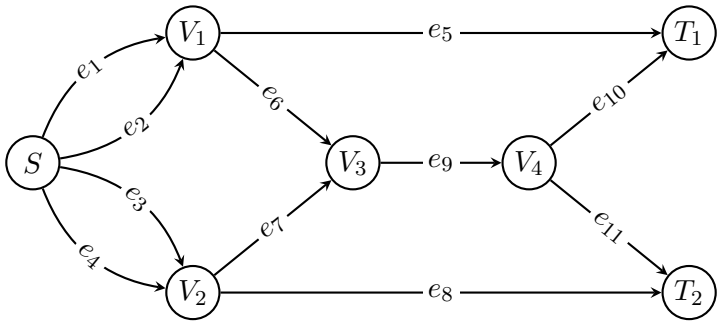

Figure 3.2: The Butterfly Network [5], $\mathscr{U} = \emptyset$, and $t = 0$.

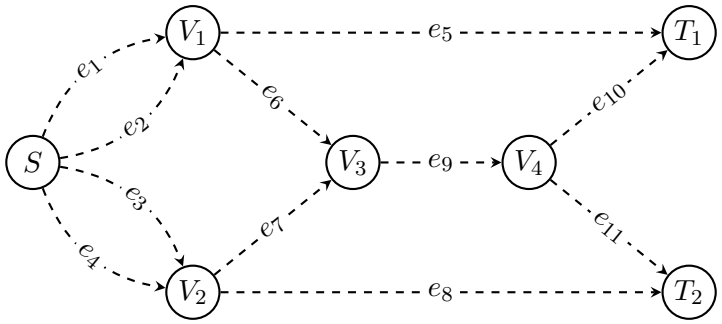

Figure 3.3: The Butterfly Network [5] and $\mathscr{U} = \mathscr{E}$.

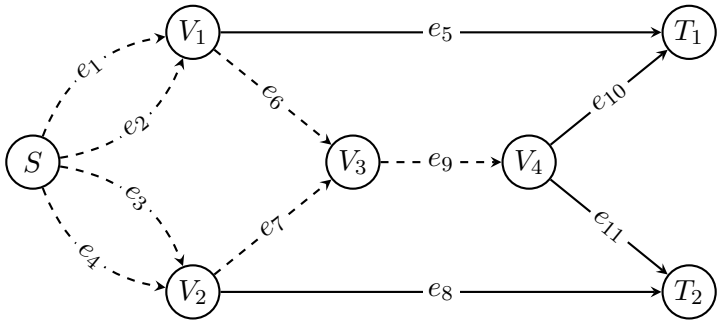

Figure 3.4: The Butterfly Network [5] where $\mathscr{U} \subset \mathscr{E}$.

tell us that

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq 2.$$

Notice that the minimum edge cut between S and T_i is 2 for all $i = 1, 2$. Now if we consider the network in Figure 3.3 and $t = 1$, using both bounds,

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq 0.$$

Therefore, we cannot decode any information at the terminals. Lastly, if we consider the network in Figure 3.4, we notice that $\mathscr{U}$ is a proper subset of the edges of $\mathscr{N}$. The Singleton Cut-Set Bound reads

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq 1.$$

For this thesis, we are most interested in the case where the adversary is restricted to corrupting a proper subset of network edges and does not have access to the entire network. The capacity of the previous network will be discussed in the next section, where *partial decoding* will be needed to achieve capacity, introducing the term *network decoding*.

3.3 Network Decoding

In this section, we introduce *network decoding*, a strategy used where intermediate vertices can perform *partial decoding* before forwarding information. We first start with a more formal definition of a channel.

Definition 3.32. Let $(\mathscr{N}, \boldsymbol{A})$ be an adversarial network with $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ and

let $\mathscr{U} \subseteq \mathscr{E}$ be a set of edges that the adversary can corrupt. Let $\mathscr{F}$ be a network code for $\mathscr{N}$ and $t \geq 0$ integer. Denote

$$\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, S \to T, \mathscr{U}, t] : \mathscr{A}^{\deg^+(S)} \to \mathscr{A}^{\deg^-(T)}$$

to be the channel representing the transfer from $S \in \mathbf{S}$ to $T \in \mathbf{T}$.

We note that again that we assume $|\mathbf{S}| = 1$. Notice that the vertices process and forward the information using $\mathscr{F}$, everything is defined by the total order $\leq$ and atmost t packets in $\mathscr{U}$ are corrupted. We call t the adversarial power.

Recall that this thesis is concerned with deriving communication schemes to achieve the capacity of networks over multiple transmission rounds. Therefore, we are mainly concerned with the construction of a code that is as large as possible but allows us to uniquely recover every element of C, regardless of the adversarial model. Therefore, we have the following definition:

Definition 3.33. An **outer code** for a network $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ is a subset $C \subseteq \mathscr{A}^{\deg^+(S)}$ with $|C| \geq 1$. An **unambiguous** (or **good**) code C for $(\mathscr{N}, \boldsymbol{A}, \mathscr{F})$ is code such that for all $x, y \in C$ with $x \neq y$ and for all $T \in \boldsymbol{T}$ we have

$$\Omega[\mathscr{N}, \boldsymbol{A}, \mathscr{F}, \text{out}(V) \to \text{in}(V)](x) \cap \Omega[\mathscr{N}, \boldsymbol{A}, \mathscr{F}, \text{out}(V) \to \text{in}(V)](y) = \emptyset$$

The intersection being empty guarantees that every element of C can be recovered by every terminal uniquely. The unambiguous property is important to make sure that each element of C can be recovered regardless of the action the adversary takes.

Next we define the notion of one-shot capacity of an adversarial network in the context of network decoding. Let $\boldsymbol{A}_{\mathscr{N}}$ be the adversary for $\mathscr{N}$.

Definition 3.34. [5, Definition 3.18] The **one-shot** capacity of an adversarial network $(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ is the maximum $\alpha \in \mathbb{R}$ such that there exists an unambiguous code C and a network code $\mathscr{F}$ with $\alpha = \log_{|\mathscr{A}|}(|C|)$, meaning

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) = \max\{\log_{|\mathscr{A}|} |C| : C \text{ is an unambiguous code for } (\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})\}.$$

Let $\mathscr{U} \subseteq \mathscr{E}$ be an edge set. The **(1-shot) linear capacity** of a network a network is the largest real $\alpha \in \mathbb{R}$ for which there exists an outer code $C \in \mathscr{A}^{\text{out}(S)}$ and a linear network code $\mathscr{F}$ for $(\mathscr{N}, \mathscr{A})$ such that $\alpha = \log_{|\mathscr{A}|}(|C|)$ such that C is good for the channel. We call the largest value $C_1^{\text{lin}}(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$.

For the rest of this thesis, we shorten the notation $C_1(\mathscr{N}, \mathscr{A}, \mathscr{U}, t)$ provided in [5] to $C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ and $C_1^{lin}(\mathscr{N}, \mathscr{A}, \mathscr{U}, t)$ to $C_1^{\text{lin}}(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ where the adversary can corrupt up to t edges of the network.

The following propositions provide a lower bound on the one-shot capacity of product channels and establish a connection between the one-shot capacity and the $i-$th shot capacity of a network.

Proposition 3.35. *[5, Proposition 3.6] Let $\Omega_1, \Omega_2 : \mathscr{X} \dashrightarrow \mathscr{Y}$ be channels with $\Omega_1 \leq \Omega_2$ as in the previous definition. Then $C_1(\Omega_1) \geq C_1(\Omega_2)$.*

The following proposition introduced in [5] tells us about the capacity of the concatenation of channels.

Proposition 3.36. *Let $\Omega_1 : \mathscr{X}_1 \dashrightarrow \mathscr{Y}_1$ and $\Omega_2 : \mathscr{X}_2 \dashrightarrow \mathscr{Y}_2$ to be channels, with $\mathscr{Y}_1 \subseteq \mathscr{X}_2$. Then $C_1(\Omega_1 \blacktriangleright \Omega_2) \leq \min\{C_1(\Omega_1), C_1(\Omega_2)\}$ [5].*

The following three results give lower bounds on the $i-$shot capacity.

Proposition 3.37. *[1, Proposition 8] Let Ω_1, Ω_2 be channels. Then $C_1(\Omega_1 \times \Omega_2) \leq C_1(\Omega_1) + C_1(\Omega_2)$.*

Proposition 3.38 ([1, Proposition 12])**.** *For a channel $\Omega : \mathscr{X} \dashrightarrow \mathscr{Y}$ and any $i \geq 1$, we have*

$$C_1(\Omega^i) \geq i \cdot C_1(\Omega).$$

We restrict to networks with a single source S and we follow the notation introduced in [5, Section V].

3.3.1 One-Shot Capacity of the Diamond Networks

Let $\mathscr{D}$ be the network in Figure 3.5 and let $\boldsymbol{A}_{\mathscr{D}}$ be an adversary that can corrupt at most one of the dashed edges meaning $t = 1$. The pair $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$ is the **Diamond Network**. It was shown in [3, Section III] and [2] that this is the smallest example of a network that does not meet the Singleton Cut-Set Bound [1, Corollary 66], which illustrates the importance of intermediate nodes performing *partial* decoding in order to achieve capacity.

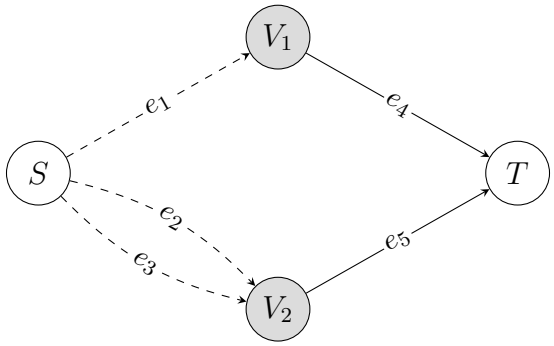

Figure 3.5: The Diamond Network $\mathscr{D}$

In particular, the following holds.

Theorem 3.39 ([3, Theorem 13]). *For any alphabet $\mathscr{A}$, the one-shot capacity of $\mathscr{D}$ is*

$$C_1(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1).$$

The strategy provided in [3] gives an explanation for why the bound is not achievable for the Diamond Network. In particular, the authors show that one symbol needs to be reserved from $\mathscr{A}$ to implement an adversary detection strategy, rendering the non-integer value capacity shown above. Reserve $\star \in \mathscr{A}$ to denote the location of the adversary. V_1 simply forwards the received symbol and V_2 proceeds as follows: If the two incoming symbols from $\mathscr{A}'$ match, forward that symbol. Otherwise, forward $\star$. One can check that any symbol from $\mathscr{A}'$ can be uniquely decoded. However, the symbol $\star$ is therefore sacrificed, establishing that $C_1(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$.

In [3, Section 3 and 4], it was shown that the network obtained by adding an edge to the Diamond Network, as in Figure 3.6, attains the Network Singleton Cut-Set Bound. The pair $(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}})$ is called **Mirrored Diamond Network**. The next result provides the one-shot capacity of $\mathscr{S}$.

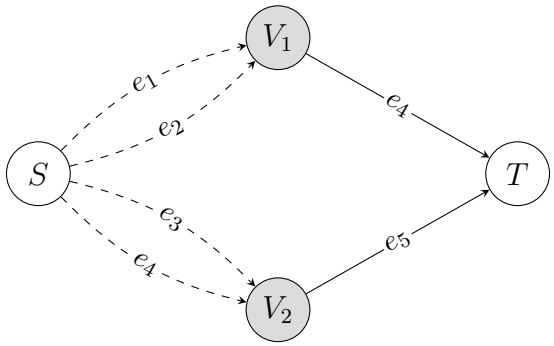

Figure 3.6: The Mirrored Diamond Network $\mathscr{S}$

Theorem 3.40 ([3, Proposition 14]). *For any alphabet $\mathscr{A}$, the one-shot capacity of $\mathscr{S}$ is $C_1(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = 1$.*

The proof of the previous result provided in [3, Proposition 14] uses the Singleton Cut-Set Bound and a communication scheme that uses a symbol from $\mathscr{A}$ to pass information about where the adversary is acting on the network. In strong contrast with the Diamond Network, the proposed strategy comes at no cost, as the "reserved" alphabet symbol can be sent and decoded like any other symbol from $\mathscr{A}$. Fix $\star \in \mathscr{A}$ to denote the location of the adversary. The source S encodes values from the alphabet via a $4-$times repetition code. Vertices V_1 and V_2 proceed as follows: if the two incoming symbols match, forward that symbol. Otherwise, forward $\star$. At the terminal, if the two symbols match, decode to that symbol. Otherwise, decode to the symbol that is not $\star$. All symbols of $\mathscr{A}$ can be sent in this scheme, rendering $C_1(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) \leq 1$.

In Chapter 4, we will discuss results on the multishot capacity of $\mathscr{D}$ and $\mathscr{S}$.

3.3.2 One-Shot Capacity of Families of Networks

In this section, assume that an adversary can attack up to t edges on the first level of each family of networks. Let $\mathscr{U}_S$ be the set of outgoing edges from the source. The Diamond Networks were further generalized in [5, Section V.C]. We begin with the following notation:

We will now discuss $m-$level networks and their matrix representation.

Notation 1. *Let $\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ be a network, $\mathbf{S} = \{S\}$ and let $V, V' \in \mathscr{V}$. We say that V' **covers** V if $(V, V') \in \mathscr{E}$. We call $\mathscr{N}$ an m-**level** network if $\mathscr{V} = \mathscr{V}_0 \sqcup \ldots \sqcup \mathscr{V}_m$ such that $\mathscr{V}_0 = \{S\}$, $\mathscr{V}_m = \mathbf{T}$. It is also necessary that each node in $\mathscr{V}_k$, for $k \in \{1, ..., m-1\}$, is only covered by elements of $\mathscr{V}_{k+1}$ and only covers elements of $\mathscr{V}_{k-1}$. $\mathscr{V}_k$ is called the k-**th layer** of $\mathscr{N}$. Now we fix an enumeration of the elements of each $\mathscr{V}_k$,*

$k \in \{0, ..., m\}$. We let $M^{m,k}$ be the matrix representing the graph induced by the nodes in layers $k-1$ and k of $\mathscr{N}_n$, for $k \in \{1, ..., n\}$. We have that the dimension of $M^{m,k}$ is $|\mathscr{V}_{k-1}| \times |\mathscr{V}_k|$, and $M^{m,k}_{ij} = \ell$ if and only if there are ℓ edges from node i of $\mathscr{V}_{k-1}$ to node j of $\mathscr{V}_k$. We then denote $\mathscr{N}_m$ $(M^{m,1}, M^{m,2}, \ldots, M^{m,m})$.

We now define simple 2−level and simple 3−level networks.

Definition 3.41. A 2-level network is **simple** if it has a single terminal. A 3-level network is **simple** if it has a single terminal, each intermediate node at distance 1 from the source has in-degree equal to 1, and each intermediate node at distance 1 from the terminal has out-degree equal to 1.

Using the notation and definition above, we have the following example.

Example 3.42. Consider the Mirrored Diamond Network $\mathscr{S}$ of Section 5.1 (see Figure 5.2). Using the above notation, $\mathscr{S}$ can be written as $([2, 2], [1, 1]^T)$ and the Diamond Network (Figure 5.1) can be represented as $([1, 2], [1, 1]^T)$. Since both $\mathscr{S}$ and $\mathscr{D}$ are simple 2−level networks, we can write $[1, 1]$ instead of $[1, 1]^T$.

For simple 2−level networks, we can use the following notation.

Notation 2. *[5, Notation 6.1] Let $n \geq 2$ be an integer. We define simple 2−level networks as*

$$\mathscr{N} = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T}) = ([a_1, \ldots, a_n], [b_1, \ldots, b_n])$$

We now define the Generalized Network Singleton Bound for 2−level networks.

Corollary 3.43. *[5, Generalized Network Singleton Bound] Let $\mathscr{A}$ be an alphabet , $\mathscr{N}$ a simple 2-level network and $\mathscr{U}_S$ be the set of edges connected to the source. Let an adversary $\boldsymbol{A}$ be able to corrupt up to t edges of $\mathscr{N}$. Then the one-shot capacity of $\mathscr{N}$*

satisfies

$$\mathrm{C}_1\left(\mathscr{N}, \boldsymbol{A}\right) \leq \min_{P_1 \sqcup P_2 = \{1,\ldots,n\}} \left(\sum_{i \in P_1} b_i + \max\left\{0, \sum_{i \in P_2} a_i - 2t\right\}\right)$$

with P_1 and P_2 are two partitions of the set $\{0, \ldots, n\}$ and the minimum is taken over all possible $2-$partitions.

We now define the following families of networks.

Definition 3.44. (Family $\mathfrak{A}_t$ [3, Section V.C]) Family $\mathfrak{A}_t$ consists of the simple $2-$level networks defined by

$$\mathfrak{A}_t = ([t, 2t], [t, t]), t \geq 1$$

The Generalized Network Singleton Bound for $\mathfrak{A}_t$ reads $C_1(\mathfrak{A}_t, \boldsymbol{A}_{\mathfrak{A}_t}) \leq t$.

Definition 3.45. (Family $\mathfrak{B}_s$ [5, Section V.C]) Family $\mathfrak{B}_s$ consists of the simple $2-$level networks defined by

$$\mathfrak{B}_s = ([1, s+1], [1, s]), s \geq 1$$

The index s is used because for this family, we will always restrict an adversary $\boldsymbol{A}_{\mathfrak{B}_s}$ to corrupt atmost 1 edge ($t = 1$). The Generalized Network Singleton Bound for $\mathfrak{B}_s$ reads $C_1(\mathfrak{B}_s, \boldsymbol{A}_{\mathfrak{B}_s}) \leq s$.

Definition 3.46. (Family $\mathfrak{C}_t$ [5, Section V.C]) Family $\mathfrak{C}_t$ consists of the simple $2-$level networks defined by

$$\mathfrak{C}_t = ([t, t+1], [t, t]), t \geq 2$$

The Generalized Network Singleton Bound for $\mathfrak{C}_t$ reads $C_1(\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}) \leq 1$.

Definition 3.47. (Family $\mathfrak{D}_t$ [5, Section V.C]) Family $\mathfrak{D}_t$ consists of the simple $2-$level

networks defined by

$$\mathfrak{D}_t = ([2t, 2t], [1, 1]), t \geq 1$$

The Generalized Network Singleton Bound for $\mathfrak{D}_t$ reads $C_1(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) \leq 1$.

Definition 3.48. (Family $\mathfrak{E}_t$ [5, Section V.C]) Family $\mathfrak{E}_t$ consists of the simple $2-$level networks defined by

$$\mathfrak{E}_t = ([t, t+1], [1, 1]), t \geq 1$$

The Generalized Network Singleton Bound for $\mathfrak{E}_t$ reads $C_1(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) \leq 1$.

We start with the main result for Family $\mathfrak{A}_t$.

Theorem 3.49. *[5, Theorem 6.16] Let $\mathfrak{A}_t$ be a member of Family $\mathfrak{A}_t$ as in Definition 3.44. Let $\mathscr{U}_S$ be the set of edges outgoing the source. Let an adversary $\boldsymbol{A}_{\mathfrak{A}_t}$ for $\mathfrak{A}_t$ be restricted to corrupting up to t edges of the set $\mathscr{U}_S$. Therefore, the one-shot capacity of Family $\mathfrak{A}_t$ satisfies*

$$C_1(\mathfrak{A}_t, \boldsymbol{A}_{\mathfrak{A}_t}) < t.$$

The authors prove that there does not exist an unambiguous code C such that $|C| = |\mathscr{A}|^t$. Therefore, the Generalized Network Singleton Bound is not achievable. The one-shot capacity of Family $\mathfrak{A}_t$ is still an open problem and needs new strategies to compute it's one-shot capacity. However, the authors showed a strategy for the lower bound when $t = 2$ using a 6-times repetition code in [5, Proposition 7.3] namely, $C_1(\mathfrak{A}_t, \boldsymbol{A}_{\mathfrak{A}_t}) \geq 1$. Therefore, using a $3t$-times repetition code and a similar strategy for $t \geq 2$ will allow the decoding of atleast 1 symbol in one transmission round.

The next result provides a not-sharp bound on the capacity of Family $\mathfrak{B}_s$.

Theorem 3.50. *[5, Theorem 6.9] Let $\mathfrak{B}_s$ be a member of Family $\mathfrak{B}_s$ as in Definition 3.45. Let an adversary $\boldsymbol{A}_{\mathfrak{B}_s}$ be restricted to corrupting only one edge ($t = 1$). Then*

the one-shot capacity of Family $\mathfrak{B}_s$ *satisfies*

$$C_1(\mathfrak{B}_s, \boldsymbol{A}_{\mathfrak{B}_s}) < s.$$

The authors prove that $|C| < |\mathscr{A}|^s$. Therefore, the Generalized Network Singleton Bound is not achievable. The capacity of Family $\mathfrak{B}_s$ in one transmission round for large alphabets is still an open problem.

The next two results shows that the Generalized Network Singleton Bound is achievable for $\mathfrak{C}_t$ and $\mathfrak{D}_t$.

Theorem 3.51. *[5, Theorem 7.8] Let* $\mathfrak{C}_t$ *be a member of Family* $\mathfrak{C}_t$ *and let* $t \geq 2$*. Let* $\mathscr{A}$ *be an alphabet and let* $\mathscr{U}_S$ *be the set of edges of* $\mathfrak{C}_t$ *outgoing the source* S*. Let* $\boldsymbol{A}_{\mathfrak{C}_t}$ *be an adversary that is restricted to corrupt up to* t *edges of* $\mathscr{U}_S$*. Then the one-shot capacity of Family* $\mathfrak{C}_t$ *is*

$$C_1(\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}) = 1.$$

Therefore, the Generalized Network Singleton Bound is achievable for $\mathfrak{C}_t$.

Theorem 3.52. *[5, Theorem 7.11] Let* $\mathfrak{D}_t$ *be a member of Family* $\mathfrak{D}_t$*. Let* $\mathscr{A}$ *be an alphabet, let* $\mathscr{U}_S$ *be the set of edges of* $\mathfrak{D}_t$ *outgoing the source* S *and let* $\boldsymbol{A}_{\mathfrak{D}_t}$ *be an adversary able to corrupt up to* t *of* $\mathscr{U}_S$ *of* $\mathfrak{D}_t$*. Then the one-shot capacity of Family* $\mathfrak{D}_t$ *is*

$$C_1(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) = 1.$$

Therefore, the Generalized Network Singleton Bound is met with equality for $\mathfrak{D}_t$.

The next theorem shows that it is also the case for Family $\mathfrak{E}_t$, that the Generalized

Network Singleton Bound is not achievable.

Theorem 3.53. *[5, Theorem 6.15] Let $\mathfrak{E}_t = (\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ be a member of Family $\mathfrak{E}_t$. Let $\mathscr{A}$ be any network alphabet, let $\mathscr{U}_S$ be the set of edges of $\mathfrak{E}_t$ directly connected to S and let $\boldsymbol{A}_{\mathfrak{E}_t}$ be an adversary able to corrupt up to t edges of $\mathscr{U}_S$ of $\mathfrak{E}_t$. Then the one-shot capacity of Family $\mathfrak{E}_t$ satisfies*

$$C_1(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) < 1.$$

Therefore the Generalized Network Singleton Bound is not met for $\mathfrak{E}_t$. The proof idea is as follows: (and provided in [5, Theorem 6.15]) Assume towards a contradiction that there exists an unambiguous code C for $\Omega(\mathfrak{E}_t)$ such that $|C| = |\mathscr{A}|$. Since C is considered to be unambiguous, it must be the case that C has minimum distance equal to at least $2t+1$. The contradiction happens if we take two $x, y \in C, x \neq y$ it is shown that $\Omega(x) \cap \Omega(y) \neq \emptyset$, contradicting the assumption that C is an unambiguous code. We will provide an extension of this proof in the multishot setting when considering a more-restricted adversarial model in Section 6.2.

3.3.3 Linear Capacity of some Families of Networks

We note that non-linear codes are used to achieve capacity for the Diamond and Mirrored Diamond Network. One may ask why we cannot use linear codes in this setting. In [5], the authors showed that the linear one-shot capacity of $\mathfrak{D}_t$ is

$$C_1^{\text{lin}}(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) = 0.$$

In particular, $C_1^{\text{lin}}(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = 0$, since $\mathscr{S}$ is a member of Family $\mathfrak{D}_t$. As a consequence of this, the authors showed in [5, Theorem 9.4] that

$$C_1^{\text{lin}}(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = 0.$$

It can be observed that $\mathfrak{E}_t \subseteq \mathfrak{D}_t$ (sub-network) for all t. Therefore, $C_1^{\text{lin}}(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = 0$, that is, the linear one-shot capacity of $\mathscr{D}$ is 0.

The authors computed a lower bound one the linear one-shot capacity of a network. In particular, the following holds.

Proposition 3.54. *[5, Proposition 9.5] Let $\mathscr{N}$ be a simple two level network with $\mathscr{N} = ([a_1, \ldots, a_n], [b_1, \ldots, b_n])$. Let $\mathscr{A} = \mathbb{F}_q$ with q sufficiently large, $t \geq 0$ and $\mathscr{U}_s$ be the set of edges connected to the source. Then the linear one-shot capacity of $\mathscr{N}$ satisfies*

$$C_1^{\text{lin}}(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \geq \max\{0, \sum_{i=0}^{n} \min\{a_i, b_i\} - 2t\}$$

Interestingly, we can say something about the linear one-shot capacity of $\mathfrak{B}_s$.

Theorem 3.55. *[5, Corollary 9.6]. Let $\mathscr{A}$ be an alphabet and $\boldsymbol{A}_{\mathfrak{B}_s}$ be an adversary able to corrupt up to s edges of the set $\mathscr{U}_S$, the edges outgoing the source. Then the one-shot capacity of Family $\mathfrak{B}_s$ satisfies*

$$s > C_1(\mathfrak{B}_s, \boldsymbol{A}_{\mathfrak{B}_s}) \geq C_1^{\text{lin}}(\mathfrak{B}_s, \boldsymbol{A}_{\mathfrak{B}_s}) \geq s - 1.$$

The proof follows from $C_1(\mathfrak{B}_s, \boldsymbol{A}_{\mathfrak{B}_s}) < s$ and using the bound in Proposition 3.54 we have that $C_1^{\text{lin}}(\mathfrak{B}_s, \boldsymbol{A}_{\mathfrak{B}_s}) \geq s - 1$.

3.3.4 One-Shot Capacity of 3-level Networks

In this section, we provide previous results on the one-shot capacity of 3−level networks introduced in [5]. We start with the following definition of 3−level networks.

Recall that a simple 3-level network is a network that has one terminal, each intermediate node V_i that is at distance 1 from the source gives $\text{in}(V_i) = 1$, and each intermediate node V_i at distance 1 from T gives $\text{out}(V_i) = 1$.

Using notation 1, in a simple 2-level network, there are two matrices $M^{2,1}$ and $M^{2,2}$ (adjacency matrices), and in a 3-level network we have three matrices $M^{3,1}$ and $M^{3,2}$, and $M^{3,3}$. In a simple 3-level network, $M^{3,1}$ and $M^{3,3}$ will always reduce to the all-ones vectors. We will also denote $M^{2,2}$ (as an abuse of notation) as a row vector in a simple 2-level network (instead of as a column vector). We now discuss the reduction of simple 3−level networks to simple 2−level networks as discussed in [5, Section 4.2].

Let $\mathscr{N}_3$ be a simple 3-level network that can be defined by the matrix $M^{3,2}$, along with all-ones matrices $M^{3,1}$ and $M^{3,3}$. The authors constructed a simple 2−level network $\mathscr{N}_2$, defined by two matrices via $M^{2,1}$ and $M^{2,2}$ as follows. Let $G^{3,2}$ be the bipartite graph corresponding to adjacency matrix $M^{3,2}$; if $G^{3,2}$ has ℓ connected components, then $M^{2,1}$ and $M^{2,2}$ both have dimensions $1 \times \ell$ Here the simplified representation for a simple 2-level network is considered, see Example 4.4 in [5]. We now let $M^{2,1}_{1i} = a \iff$ the ith connected component of $G^{3,2}$ has a vertices in $\mathscr{V}_1$, and let $M^{2,2}_{1i} = b \iff$ the ith connected component of $G^{3,2}$ has b vertices in $\mathscr{V}_2$. Observe that the sum of the entries of $M^{2,1}$ is equal to the sum of the entries of $M^{3,1}$, and similarly with $M^{2,2}$ and $M^{3,3}$. We call $\mathscr{N}_2$ the simple 2−level network **associated to** $\mathscr{N}_3$. Using this construct, we provide the following theorem.

Theorem 3.56. *[5, Theorem 5.8] Let $\mathscr{N}_3$ be a simple 3-level network, and let $\mathscr{N}_2$ be*

the simple 2-level network associated to it (by construction). Let $\mathscr{U}_2$ and $\mathscr{U}_3$ be the set of edges outgoing the sources of $\mathscr{N}_2$ and $\mathscr{N}_3$, respectively and let an adversary have the ability to corrupt up to t edges of $\mathscr{U}_2$ and $\mathscr{U}_3$. Then for all $\mathscr{A}$ and for all $t \geq 0$ the one-shot capacity of $\mathscr{N}_3$ satisfies

$$C_1(\mathscr{N}_3, \boldsymbol{A}_{\mathscr{N}_3}) \leq C_1(\mathscr{N}_2, \boldsymbol{A}_{\mathscr{N}_2}).$$

The previous result gives an upper bound on the capacity of $\mathscr{N}_3$, namely that the one-shot capacity of $\mathscr{N}_3$ is upper bounded by the one-shot capacity of $\mathscr{N}_2$. Therefore, we have a relationship between simple 3−level networks and simple 2−level networks associated to them. Therefore, strategies provided for simple 2−level networks can be extended to the simple 3−level network setting. One may ask what happens if we have a 3−level network that is not simple. The next two results discuss how to construct a simple 3−level network $\mathscr{N}'$ from a 3−level network $\mathscr{N}$ and that the one-shot capacity of $\mathscr{N}$ is upperbounded by $\mathscr{N}'$.

Theorem 3.57. *(Double-Cut-Set Bound) [5, Theorem 8.6]. Let $\mathscr{N}$ be a network, $\mathscr{A}$ be a network alphabet, $\mathscr{U} \subseteq \mathscr{E}$ be a set of edges. Assume that an adversary $\boldsymbol{A}_{\mathscr{N}}$ can attack up to $t \geq 0$ edges of $\mathscr{N}$. Let $T \in \mathbf{T}$ and let $\mathscr{E}_1$ and $\mathscr{E}_2$ be edge-cuts between S and T with $\mathscr{E}_1$ preceding $\mathscr{E}_2$. Then the one-shot capacity of $\mathscr{N}$ satisfies*

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq \max_{\mathscr{F}} C_1(\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t])$$

where the maximum is taken over all the network codes $\mathscr{F}$ for the adversarial network $(\mathscr{N}, \boldsymbol{A})$.

The next corollary directly follows from the previous theorem, providing an upper-bound on the capacity of 3−level networks. In particular, the one-shot capacity of $\mathscr{N}$

is upperbound by the one-shot capacity of $\mathscr{N}'$, where $\mathscr{N}'$ is the simple 3−level network associated to $\mathscr{N}$.

Corollary 3.58. *[5, Corollary 8.7] Let $\mathscr{N}$ be a network, $t \geq 0$, $\mathscr{A}$ a network alphabet, $\mathscr{U} \subseteq \mathscr{E}$ a set of edges. Let $T \in \mathbf{T}$ and let $\mathscr{E}_1$ and $\mathscr{E}_2$ be edge-cuts between S and T with $\mathscr{E}_1$ preceding $\mathscr{E}_2$. Consider a simple 3-level network $\mathscr{N}'$. The vertices of V_1 are in bijection with the edges of $\mathscr{E}_2$ and the vertices of V_2 with the edges of $\mathscr{E}_2$. A vertex $V \in V_1$ is connected to vertex $V' \in V_2$ if and only if the edge of $\mathscr{E}_1$ corresponding to V is an immediate predecessor of the edge of $\mathscr{E}_2$ corresponding to V'; see 3.28. Denote by $\mathscr{E}'_S$ to be the edges directly connected with the source of $\mathscr{N}$, which we identify with the edges of $\mathscr{E}_1$ (consistently with how we identified these with the vertices in V_1). The one-shot capacity of $\mathscr{N}$ satisfies*

$$C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq C_1(\mathscr{N}', \boldsymbol{A}_{\mathscr{N}'}).$$

The previous corollary and the reduction from 3 to 2−level networks provided in [5, Section V B] shows that under certain assumptions, any network can be upper bounded by the capacity of a simple 3-level network constructed from it and any simple 3−level network can be upper-bounded by the simple 2−level network associated to it.

We will now provide an example of the previous corollary, introduced in [5]. Namely, we will discuss the capacity of the Butterfly Network $\mathscr{B}$ with the adversary restricted to corrupting 1 edge of the set $\mathscr{U} = \{e_1, e_2, e_3, e_4, e_5, e_6, e_9\}$ shown in Figure 3.4.

Example 3.59. [5, Example 8.8]. We focus on terminal T_1 (a similar approach can be taken for T_2, since the network is symmetric) and consider the two edge-cuts $\mathscr{E}_1 = \{e_1, e_2, e_9\}$ and $\mathscr{E}_2 = \{e_5, e_{10}\}$ depicted in. Clearly, $\mathscr{E}_1$ precedes $\mathscr{E}_2$. Using Corollary 3.58, we can construct a simple 3-level network $\mathscr{N}'$. We have that layer $\mathscr{V}_1 \in \mathscr{N}'$ is in

bijection with $\mathscr{E}_1$, therefore $|\mathscr{V}_1| = 3$ and layer $\mathscr{V}_2$ is in bijection with $\mathscr{E}_2$, therefore $|\mathscr{V}| = 2$. The resulting simple 3−level network is in Figure 5.3.

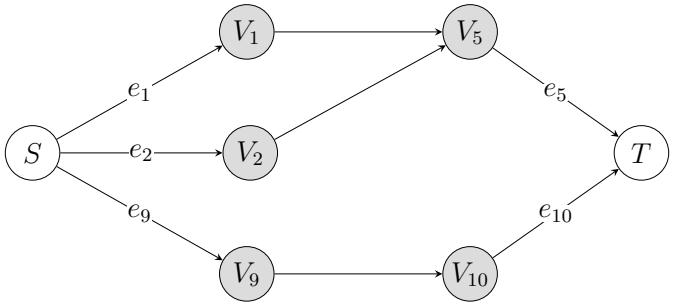

Figure 3.7: The 3-level network $\mathscr{N}'$ induced by the Butterfly network $\mathscr{B}$ in Figure 4.4.

We let $\mathscr{E}_S = \{e_1, e_2, e_9\}$ and recall that $\mathscr{U} = \{e_1, e_2, e_3, e_4, e_5, e_6 e_9\}$ is the set of vulnerable edges of the Butterfly network depicted in Figure 4.4. We make the edges vulernable of $\mathscr{U} \cap \mathscr{E}_S = \{e_1, e_2, e_9\}$, as depicted in Figure 5.4.

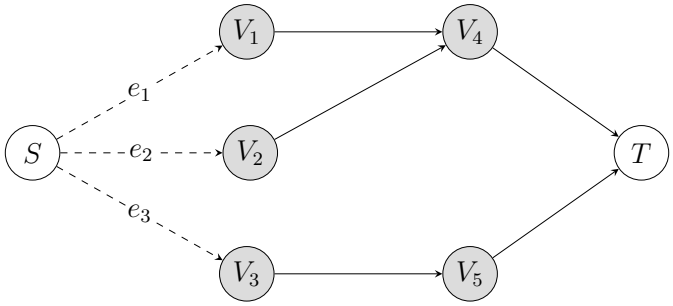

Figure 3.8: The 3-level network $\mathscr{N}'$ where the vulnerable edges are dashed.

Using notation 1 and the discussion above, Figure 5.3 and 5.4 can be represented as

$$\left(\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right).$$

It remains to discuss the reduction of $\mathscr{N}'$ to a simple 2−level network using the process described in [5, Section V-B]. Let $G^{3,2}$ be the bipartite graph corresponding to the

adjacency matrix

$$M^{3,2} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

One can easily see that $G^{3,2}$ has two connected components. Therefore, $M^{2,1}$ and $M^{2,2}$ of the simple 2−level network we are constructing have dimension 1×2. It remains to compute the entries of these matrices. We have that $M^{2,1}_{1,1} = 2$, since the first connected component has 2 vertices in $\mathscr{V}_1$ and $M^{2,1}_{1,2} = 1$, since the second connected component has 1 vertex in $\mathscr{V}_1$. Therefore $M^{2,1} = [2, 1]$. Now $M^{2,2}_{1,1} = 1$ since the first connected component has 1 vertex in $\mathscr{V}_2$ and $M^{2,2}_{1,2} = 1$ since the second connected component has 1 vertex in $\mathscr{V}_2$. Therefore, we get the two-level network $\mathscr{N}_2 = ([2, 1], [1, 1])$. Notice that by graph isomorphism, we can rewrite as $\mathscr{N}_2 = ([1, 2], [1, 1])$. Notice that $\mathscr{N}_2$ is exactly the Diamond Network. Therefore using Theorem 3.56, Corollary 3.58 and the one-shot capacity of the Diamond Network, the upper bound one-shot capacity of the Butterfly network $\mathscr{B}$ is $C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \leq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$.

We will now explain the capacity-achieving strategy discussed in [5]. .

Theorem 3.60. *[5, Theorem 8.9] Let $\mathscr{A}$ be an alphabet and $\boldsymbol{A}_{\mathscr{B}}$ be an adversary able to corrupt up to 1 edge of $\mathscr{U}$ defined above. Then the one-shot capacity of $\mathscr{B}$ is*

$$C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1).$$

A strategy similar to the Diamond Network is applied to this network, that is, reserving a symbol to denote the location of the adversary. The authors show that this symbol is therefore sacrificed in this adversary-detection scheme, rendering that $C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$. The strategy is as follows: Reserve a symbol $\star \in \mathscr{A}$ to be used as an adversary detection scheme and information is encoded by the source using a repetition

code in $\mathscr{A}^4$. Vertices V_1 and V_2 process information by the following rules: If the symbols that appear on their incoming edges are the same, they forward that symbol; otherwise they output $\star$. Vertex V_3 checks if one of the two received symbols is different from $\star$ then it forwards that symbol. If both received symbols are different from $\star$, then it outputs $\star$ over the edge e_9. The vertex V_4 just forwards the received symbol. Decoding proceeds at the termimals as follows: T_1 and T_2 look at the edges e_5 and e_8, respectively. If the terminals do not receive $\star$ over those edges, they trust the received symbol. If one of them is $\star$, then the corresponding terminal trusts the outgoing edge from V_4. For example, if e_5 carries $\star$, then T_1 trusts e_{10}. This scheme defines a network code $\mathscr{F} = (\mathscr{F}_{V_1}, \mathscr{F}_{V_2}, \mathscr{F}_{V_3}, \mathscr{F}_{V_4})$ for $(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}})$ and an unambiguous outer code

$$C = \{(a, a, a, a), a \in \mathscr{A}^4 \setminus \{(\star, \star, \star, \star)\}\}$$

of cardinality $|\mathscr{A}|-1$. Therefore $C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$.

The previous example demonstrates the relationship between 3−level networks and the 2−level networks associated to them. Namely, this process can be used to derive upper bounds on 3−level networks that can be reduced to simple 2−level networks in this way, making something more complicated easier to understand with the tools provided. We will revisit the Butterfly Network $\mathscr{B}$ in Figure 3.4 Chapter 5 when discussing its multishot capacity.

Chapter 4

Multishot Capacity of Adversarial Networks

This chapter is dedicated to original results on the multishot capacity of adversarial networks. For the remainder of the thesis, let $i \in \mathbb{N}$ be the number of uses of a network. We let multiple uses represent more than one use of a network. A formal definition of the multishot capacity that extends Definition 3.34, is the following.

Definition 4.1. [17, Definition II.7] Let i be a positive integer. The **i-shot capacity** of $(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ is the maximum $\alpha \in \mathbb{R}$ such that there exists an unambiguous code C for $(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ with $\alpha = \frac{\log_{|\mathscr{A}|}(|C|)}{i}$, meaning

$$C_i(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) = \max\left\{\alpha = \frac{\log_{|\mathscr{A}|}(|C|)}{i} : C \text{ is an unambiguous code for } (\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})\right\}.$$

Intuitively, the multishot capacity can be thought of as the maximum number of symbols we can send over i transmission rounds without errors and is an extension of the original one-shot capacity in Definition 3.34. Notice that $i = 1$ recovers the original definition.

The remainder of the thesis is organized according to the following adversarial models:

A.1 The adversary attacks the same t edges over i uses of the network.

A.2 The adversary can change the t edges to attack over i uses of the network.

4.1 Multishot Capacity of the Diamond Network(s)

In this section, we will to compute the multishot capacity of the Diamond Network $\mathscr{D}$ and the Mirrored Diamond Network $\mathscr{S}$ in each of the adversarial models in Scenario A.1 and A.2.

4.1.1 The Diamond Network

Scenario A.1

Let $t = 1$ in this section, meaning, the adversary can corrupt at most 1 edge per transmission round but cannot change the edge attacked after the first transmission round. We will demonstrate that in this scenario, the $i-$shot capacity of $\mathscr{D}$ in Scenario A.1 is

$$C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)}{i}.$$

Therefore, the largest unambiguous code we can construct for $\mathscr{D}$ has cardinality $|\mathscr{A}|^i - 1$.

Notice that reusing the strategy previously proposed in [3, Proposition 11] one can easily show that $C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$. We let $\Omega[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \text{out}(S) \to \text{in}(T)]$ be the channel representing the transfer from S to T of the Diamond Network as in Definition 5 for the remainder of the paper. The aim of this section is to explicitly compute the multishot capacity of the Diamond Network in Scenario A.1. We provide a construction of an unambiguous code of cardinality $|\mathscr{A}|^i - 1$ for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F})$ that models i transmission rounds. We show that this is the maximum possible in this

setting. In particular, we prove that

$$\mathrm{C}_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)}{i}.$$

We start with the following result.

Proposition 4.2. *[17, Proposition III.1] Let $\mathscr{F}$ be a network code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$. If $C \subseteq (\mathscr{A}^i)^3$ is an unambiguous code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F})$, then $|C| \geq |A|^i - 1$.*

Proof. Let $\star \in \mathscr{A}$. We want to show that

$$C = \{(a \mid a \mid a) : a \in \mathscr{A} \setminus (\star, \ldots, \star)\} \subseteq (\mathscr{A}^i)^3$$

is unambiguous for the Diamond Network in Scenario A.1. Let $\mathscr{F}$ be a network code as in the proof of [3, Proposition 11], which provides the strategy for the lower bound in the one-shot case. The strategy is reused in each transmission round. Suppose the adversary corrupts e_1 and changes the symbol on e_1. For any $a \in \mathscr{A}^i$, we have that

$$\Omega^i[\mathscr{D}, \boldsymbol{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)]((a \mid a \mid a)) = \{(b \mid a)\}$$

for some $b \in \mathscr{A}^i \setminus \{(\star, \ldots, \star)\}$. On the other hand, if the adversary corrupts e_2 or e_3 then, for any $a \in \mathscr{A}^i \setminus \{(\star, \ldots, \star)\}$, we get

$$\Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)]((a \mid a \mid a)) = \{(a \mid \star, \ldots, \star)\}.$$

It follows that, for any $c, c' \in C$, we have

$$\Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](c) \cap \Omega[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](c') \neq \emptyset$$

if and only if $c = c'$ which implies that the code C is unambiguous. This concludes the proof. □

Note that the construction of C in Proposition 4.2 heavily relies on the adversary not being able to change the edge attacked for the next $i-1$ uses. Therefore, we know the exact location of the adversary after the first transmission round. Thus, the strategy provided in [3, Proposition 11] can be applied to i transmission rounds by modeling the unambiguous code in $(\mathscr{A}^i)^3$. The lower bound provided in Proposition 4.2 is a strict improvement on the lower bound provided by Proposition 3.38. This provides a gain in capacity of using $\mathscr{D}$ multiple times for communication. In the next result, we will show that C is the largest unambiguous code we can construct for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$.

The action of the adversary on $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$ can be defined as the channel $\mathrm{H}_{\mathscr{D}} : \mathscr{A}^3 \dashrightarrow \mathscr{A}^3$ defined as $\mathrm{H}_{\mathscr{D}}(x) := \{y \in \mathscr{A}^3 : d_{\mathrm{H}}(x, y) \leq 1\}$ for all $x \in \mathscr{A}^3$, where d_{H} is the Hamming distance as in [1, Example 4]. Therefore, a code $C \subseteq \mathscr{A}^3$ is unambiguous for $\mathrm{H}_{\mathscr{D}}$ if $d_{\mathrm{H}}(C) = 3$. We can extend this to i uses of the network and describe the adversary as a power channel $\mathrm{H}_{\mathscr{D}}^i$. Let $x = (x_1, \ldots, x_{3i}) \in (\mathscr{A}^3)^i$ and we can define $x^{(j)} := (x_{3j+1}, x_{3j+2}, x_{3j+3})$ for all $j \in \{0, \ldots, i-1\}$. Then, for any $x \in C$, we have

$$\mathrm{H}_{\mathscr{D}}(x) = \{y \in (\mathscr{A}^3)^i : d_{\mathrm{H}}(x^{(j)}, y^{(j)}) \text{ for all } j \in \{0, \ldots, i-1\}\}.$$

Hence $C \subseteq (\mathscr{A}^i)^3$ is good code for $\mathrm{H}_{\mathscr{D}}^i$ if and only if for all $x, y \in C$, with $x \neq y$ we have $d_{\mathrm{H}}(x^{(j)}, y^{(j)}) = 3$ for some $j \in \{0, \ldots, i-1\}$.

Let $s \in \{1, 2, 3\}$ and define $\pi_s^i : \mathscr{A}^{3i} \longrightarrow \mathscr{A}^i$ to be the projection onto the components in the set $\{3j+s : j \in \{0, \ldots, i-1\}\}$. Intuitively, these are the components corresponding to the edge e_s in each round. Let $\mathscr{F}$ be a network code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$. The following

generalizes [3, Claim A].

Lemma 4.3. *[17, Lemma III.2] If $C \subseteq \mathscr{A}^{3i}$ is an unambiguous code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F})$, then $|\pi_1^i(C)| = |C|$.*

Proof. We already showed that C is unambiguous for the Diamond Network if and only if for any $x, y \in C$, with $x \neq y$, $d_{\mathrm{H}}(x^{(j)}, y^{(j)}) = 3$ for some $j \in \{0, \ldots, i-1\}$ in the above argument. Suppose, towards a contradiction, that there exist $x, y \in C$ with $x \neq y$ and $\pi^i(x) = \pi^i(y)$. It implies that $x_{3j+1} = y_{3j+1}$ and therefore $d_{\mathrm{H}}(x^{(j)}, y^{(j)}) \leq 2$ for all $j \in \{0, \ldots, i-1\}$. This leads to a contradiction. □

The following result generalizes [3, Claim B] for multiple transmission rounds.

Lemma 4.4. *[17, Lemma III.3] If $C \subseteq (\mathscr{A}^i)^3$ is an unambiguous code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F})$ then the restriction of $\mathscr{F}_{V_1}$ to $\pi_1^i(C)$ is injective.*

Proof. Suppose, towards a contradiction, that there exist $x, y \in C$ such that $x \neq y$ and $\mathscr{F}_{V_1}(\pi_1^i(x)) = \mathscr{F}_{V_2}(\pi_1^i(x))$. One can check that the vector

$$\left(\mathscr{F}_{V_1}(\pi_1^i(x)) \mid \mathscr{F}_{V_2}\left(\pi_2^i(x) \mid \pi_3^i(y)\right)\right) \in \mathscr{A}^{2i}$$

is in $\Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](x) \cap \Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](y)$. This implies that C is not unambiguous for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$ which is a contradiction. □

Following the notation in [3], we let

$$\begin{aligned}\overline{\Omega}^i :=& \Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \{e_1, e_2, e_3\} \to \{e_2, e_3\}],\\ \Omega^i :=& \Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \{e_1, e_2, e_3\} \to \{e_5\}]\end{aligned}$$

which is well-defined since $\{e_1, e_2, e_3\}$ precedes $\{e_5\}$. The following result generalizes [3, Claim C].

Lemma 4.5. *[17, Lemma III.4] Let $\mathscr{F}$ be a network code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$. If $C \subseteq \mathscr{A}^{3i}$ is an unambiguous code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F})$, then there exists at most one element $x \in C$ such that $|\Omega^i(x)| = 1$.*

Proof. Suppose, towards a contradiction, that there exist $x, y \in C$ such that $|\Omega^i(x)| = |\Omega^i(y)| = 1$ and $x \neq y$. It implies $|\mathscr{F}_{V_2}(\overline{\Omega}^i(x))| = |\mathscr{F}_{V_2}(\overline{\Omega}^i(y))| = 1$. Since $(\pi_2^i(x) \mid \pi_3^i(x)), (\pi_2^i(x) \mid \pi_3^i(y)) \in \overline{\Omega}^i(x)$ and $(\pi_2^i(y) \mid \pi_3^i(y)), (\pi_2^i(x) \mid \pi_3^i(y)) \in \overline{\Omega}^i(y)$, we have

$$\begin{aligned}\mathscr{F}_{V_2}(\pi_2^i(x) \mid \pi_3^i(x)) &= \mathscr{F}_{V_2}(\pi_2^i(x) \mid \pi_3^i(y)) \\ &= \mathscr{F}_{V_2}(\pi_2^i(y) \mid \pi_3^i(y)).\end{aligned}$$

It follows that

$$\Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](x) \cap \Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](y) \neq \emptyset$$

since the adversary can corrupt the edge e_1. This is a contradiction. □

We are now ready to prove a result analogous to [3, Proposition 12].

Proposition 4.6. *[17, Proposition III.5] Let $\mathscr{F}$ be a network code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$. If $C \subseteq \mathscr{A}^{3i}$ is an unambiguous code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F})$ then*

$$|C|^2 + |C| - 1 - |\mathscr{A}|^{2i} \leq 0.$$

Therefore, $|C| \leq |\mathscr{A}|^i - 1$.

Proof. Let

$$\begin{aligned}
\widehat{\Omega}^i :=& \Omega^i[\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}, \mathscr{F}, \{e_1, e_2, e_3\} \to \{e_4, e_5\}], \\
\widehat{\Omega}^i_1 :=& \{y \in \widehat{\Omega}^i : \mathscr{F}_{V_1}(\pi^i_1(y)) = \pi^i_1(x)\}, \\
\widehat{\Omega}^i_2 :=& \{y \in \widehat{\Omega}^i : \mathscr{F}_{V_2}((\pi^i_2(y) \mid \pi^3_2(y))) = (\pi^i_2(x) \mid \pi^3_2(x))\}
\end{aligned}$$

for any $x \in C$, and let $\widehat{\Omega}^i(x) = \widehat{\Omega}^i_1(x) \cup \widehat{\Omega}^i_2(x)$. By definition, we have $|\widehat{\Omega}^i(x)| = |\widehat{\Omega}^i_1(x)| + |\widehat{\Omega}^i_2(x)| - 1$. Using the lemmas provided above

$$\begin{aligned}
\sum_{x \in C} |\widehat{\Omega}^i(x)| &\geq 1 - 2(|C| - 1) + \sum_{x \in C} |C| - |C| \\
&= 2|C| - 1 + |C|^2 - |C| \\
&= |C|^2 - |C| - 1.
\end{aligned} \tag{4.1.1}$$

Since we showed that the code is unambiguous, we have

$$\sum_{x \in C} |\widehat{\Omega}^i(x)| \leq |\mathscr{A}|^{2i}.$$

Combining this with (4.1.1) we get the statement. □

As a consequence of Propositions 4.2 and 4.6, we have that in the Scenario A.1 the maximum size of an unambiguous code for $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$ is exactly $|\mathscr{A}|^i - 1$ Thus, $\mathrm{C}_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)}{i}$.

Therefore, we showed that in using the $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$ multiple times for communication, we have a gain in capacity. Notice that if we used the strategy provided in [3], we would expect that the largest unambiguous code for $\mathscr{D}$ we could construct would have cardinality $(|\mathscr{A}| - 1)^i$. We showed that the largest unambiguous code we can construct

for $\mathscr{D}$ was $|\mathscr{A}|^i - 1$ in Scenario A.2. In comparison, $|\mathscr{A}|^i - 1 \geq (|\mathscr{A}| - 1)^i$ for $i \geq 1$, which is consider gain in the information we can send over i uses of the network without errors. We wish to understand if this is the case for Scenario A.2.

Scenario A.2:

Recall that in this scenario, the adversary can attack 1 edge but can change the edge attacked each transmission round.

One can easily check that $C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) \leq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$ using [1, Proposition 12]. We will show that

$$C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1),$$

therefore the largest unambiguous code we can construct for $\mathscr{D}$ in Scenario A.2 has cardinality $(|\mathscr{A}| - 1)^i$. Therefore, $C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = C_1(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$. Therefore, there is no advantage in using the Diamond Network multiple times for communication in this scenario in contrast with A.1. In the following examples, we provide a characterization of an unambiguous code for $\mathrm{H}_{\mathscr{D}}$, the adversarial channel associated to $\mathscr{D}$.

Example 4.7. Let $\mathrm{H}_{\mathscr{D}}$ be the adversarial channel for $\mathscr{D}$ as in Scenario A.1. The source S can send any symbol of $\mathscr{A}' = \mathscr{A} \setminus \{\star\}$, where $\star$ is a reserved symbol in the alphabet $\mathscr{A}$. It can be checked that the largest unambiguous code for $\mathrm{H}_{\mathscr{D}}$ has cardinality $|\mathscr{A}| - 1$. The source S cannot send the reserved symbol $\star$, implying $C_1(\mathrm{H}_{\mathscr{D}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$.

The argument provided is similar to the one in Scenario A.1 and shows that a code $C \subseteq (\mathscr{A}^3)^i$ is unambiguous for $\mathrm{H}^i_{\mathscr{D}}$ if and only if, for all $x, y \in C$ with $x \neq y$, we have $d^{\mathrm{H}}(x^{(j)}), y^{(j)}) \geq 3$, with $j \in \{1, \ldots, i-1\}$. In the next example, we show that there does not exist a code C with $|C| = (|\mathscr{A}| - 1)^i + 1$ for i uses of the Diamond Network,

that is, $|C| \leq (|\mathscr{A}| - 1)^i$. We follow the strategy provided in [1, Example 56].

Example 4.8. Assume towards a contradiction that there exists an unambiguous code $C \subseteq (\mathscr{A}^3)^i$ for $\mathrm{H}^i_{\mathscr{D}}$ such that $|C| = (|\mathscr{A}| - 1)^i + 1$. For any $x = (x_1, \ldots, x_{3i}) \in (\mathscr{A}^3)^i$, we let $x^1 := (x_1, x_2, x_3), \ldots, x^i := (x^i_1, x^i_2, x^i_3)$ and $c_1, \ldots, c_{(|\mathscr{A}|-1)^i+1}$ be elements in C. We claim that there are no two codewords of C that coincide in the first $(|\mathscr{A}| - 1)^i$ components. Assume, towards a contradiction, that $c^1_1 = c^1_2$ for $c^1_1 \neq c^1_2$ and we let $c_1 = 0$, without loss of generality. This implies that $c^1_2 = 0$ and that $c^1_3, \ldots, c^1_{(|\mathscr{A}|-1)^i+1}$ must have Hamming weight at least 3. Observe that if c^1_3 has Hamming weight less than 3, then one of $\{c^2_1, c^2_2, c^2_3\}, \ldots, \{c^i_1, c^i_2, c^i_3\}$ is a code in $\mathscr{A}^3$ of cardinality 3 with minimum Hamming distance 3, contradicting $C_1(\mathrm{H}_{\mathscr{D}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$. On the other hand, since $c^1_3, \ldots, c^1_{(|\mathscr{A}|-1)^i+1}$ have Hamming weight at least 3 which implies that the Hamming distance between any two elements in $\{c^1_3, \ldots, c^1_{(|\mathscr{A}|-1)^i+1}\}$ is at most 2. Since we assumed that C is unambiguous for $\mathrm{H}^i_{\mathscr{D}}$, we have that one of $\{c^2_1, c^2_2, c^2_3\}, \ldots, \{c^i_1, c^i_2, c^i_3\}$ must be a code with cardinality 3 and minimum Hamming distance 3, which again contradicts the capacity of $\mathrm{H}_{\mathscr{D}}$.

We introduce the following notation.

Notation 3. *We let Ω^i, the $i-$fold product of $(\Omega_{\mathscr{F}_1}[\mathrm{out}(S) \to \mathrm{in}(T)] \blacktriangleright \mathrm{H}_{\mathscr{D}})$, be the channel modeling i uses of the network $(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$, where $\mathscr{F}_j$ denotes the network code used in transmission round j, with $j \in \{1, \ldots, i\}$. Note that $\Omega_i : (\mathscr{A}^3)^i \dashrightarrow (\mathscr{A}^2)^i$.*

We are now ready to prove the main theorem of this section.

Theorem 4.9. *Let $\mathscr{A}$ be an alphabet and $\boldsymbol{A}_{\mathscr{D}}$ be an adversary able to corrupt up to 1 edge of the set of edges outgoing the source of $\mathscr{D}$. Then the i-shot capacity of the Diamond Network in Scenario A.2 is*

$$\mathrm{C}_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1).$$

Proof. We first show that $|C| \leq (|\mathscr{A}|-1)^i$. Assume that an adversary $\boldsymbol{A}_{\mathscr{D}}$ can corrupt at most of the edges in the set $\{e_1, e_2, e_3\}$. We observe that, for an $x = (x_1, \ldots, x_{3i}) \in \mathscr{A}^{3i}$, we have

$$\Omega^i(x) = \mathrm{H}^i_{\mathscr{D}}(\mathscr{F}^1(x_1, x_2, x_3), \ldots, \mathscr{F}^i(x_{3i-2}, x_{3i-1}, x_{3i})).$$

We assume that there exists an unambiguous code $C \subseteq \mathscr{A}^{3i}$ for Ω^i with $|C| = (|\mathscr{A}| - 1)^i + 1$. The code

$$C' := \{\mathscr{F}^1(x_1, x_2, x_3), \ldots, \mathscr{F}^i(x_{3i-2}, x_{3i-1}, x_{3i}))\} \subseteq (\mathscr{A}^3)^i$$

is unambiguous for $\mathrm{H}^i_{\mathscr{D}}$ of cardinality $(|\mathscr{A}| - 1)^i + 1$. Since $|C'| = (|\mathscr{A}| - 1)^i + 1$, there must exist $a, a' \in C$, $a \neq a'$ such that $(a_1, \ldots, a_{(|\mathscr{A}|-1)^i}) = (a'_1, \ldots, a'_{(|\mathscr{A}|-1)^i})$. Thus $C' \in (\mathscr{A}^3)^i$ is an unambiguous code for $\mathrm{H}^i_{\mathscr{D}}$ with two different code words that coincide in the first $(|\mathscr{A}|-1)^i$ components. However, such a code does not exist by Example 4.8. It follows $C_1(\Omega^i) < \log_{|\mathscr{A}|}((|\mathscr{A}| - 1)^i + 1)$ and hence $|C| \leq (|\mathscr{A}| - 1)^i$. It remains to show that $|C| \geq (|\mathscr{A}| - 1)^i$. This immediately follows by applying [1, Proposition 12] and the strategy introduced in [3, Proposition 11] to the argument above. □

It is interesting to note that when the adversary can change the edge attacked in each transmission round, we recover the same scheme as in [3]. Again, there is no gain of using the Diamond Network multiple times for communication in this scenario.

4.1.2 The Mirrored Diamond Network

In this section, we compute the multishot capacity of the Mirrored Diamond Network $\mathscr{S}$ in both scenarios.

Scenario A.1

Using [1, Proposition 12], it immediately follows that $C_i(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) \leq 1$. We will show that

$$C_i(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = 1$$

indicating that using $\mathscr{S}$ multiple times does not provide a gain in capacity in comparison to the one-shot capacity. We begin with the following necessary notation and examples.

Notation 4. *We let*

$$\Omega^{i\prime} := (\Omega_{\mathscr{F}_1}[\mathrm{out}(S) \to \mathrm{in}(T)] \blacktriangleright \mathrm{H}_{\mathscr{S}}) \times \cdots \times (\Omega_{\mathscr{F}_i}[\mathrm{out}(S) \to \mathrm{in}(T)] \blacktriangleright \mathrm{H}_{\mathscr{S}})$$

represent the channel describing i uses of the network $(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}})$, where $\mathscr{F}_j$ denotes the network code used in transmission round j, with $j \in \{1, \ldots, i\}$. Notice that $\Omega'_i : (\mathscr{A}^4)^i \dashrightarrow (\mathscr{A}^2)^i$.

The next example describes the one-shot capacity of the adversarial channel $\mathrm{H}_{\mathscr{S}}$ that represents the action of the adversary on $\mathscr{S}$.

Example 4.10. Following [1, Example 4], let $\mathrm{H}_{\mathscr{S}}$ be the adversarial channel for $\mathscr{S}$, with $\mathrm{H}_{\mathscr{S}} : \mathscr{A}^4 \dashrightarrow \mathscr{A}^4$. Note that $\mathrm{H}_{\mathscr{S}}$ represents an adversary $\boldsymbol{A}_{\mathscr{S}}$ being able to attack 1 edge from the subset of edges $\{e_1, e_2, e_3, e_4\}$ of $\mathscr{S}$ defined by $\mathrm{H}_{\mathscr{S}}(a) := \{b \in \mathscr{A}' : d_{\mathrm{H}_{\mathscr{S}}}(a, b) \leq 1\}$ for all $a \in \mathscr{A}$. Notice that the largest unambiguous code for $H_{\mathscr{S}}$ has cardinality $|\mathscr{A}|$ and there is no unambiguous code with larger cardinality. Thus $C_1(\mathrm{H}_{\mathscr{S}}) = 1$.

The next example shows that there does not exist an unambiguous code C for $H^i_{\mathscr{S}}$ such that $|C| = |\mathscr{A}|^i + 1$, that is, $|C| < |\mathscr{A}|^i + 1$.

Example 4.11. For $x \in (\mathscr{A}^4)^i$, we let $x^j := (x_{4j+1}, x_{4j+2}, x_{4j+3}, x_{4j+4})$ for all $j \in 0, \dots, i-1$. The code $C \subseteq (\mathscr{A}^4)^i$ is unambiguous for $\mathrm{H}^i_{\mathscr{S}}$ if and only if one among $d^{\mathrm{H}}(x^1, y^1), \dots, d^{\mathrm{H}}(x^i, y^i)$ has Hamming distance at least 3 for all x, y with $x \neq y$. Let $c_1, \dots, c_{|\mathscr{A}|^i+1}$ be elements in C. We want to show that there are no two codewords of C that coincide in the first $|\mathscr{A}|^i$ components. Assume, towards a contradiction, that $c_1^1 = c_2^1$. We can also assume that $c_1 = 0$ without loss of generality, which implies $c_2^1 = 0$. It follows that $c_3^1, \dots, c_{|\mathscr{A}|^i+1}^1$ must have Hamming weight at least 3. If c_3^1 has Hamming weight less than 3, then one among $\{c_1^2, c_2^2, c_3^2\}, \dots, \{c_1^i, c_2^i, c_3^i\}$ is an unambiguous code for $\mathrm{H}_{\mathscr{S}}$ of cardinality 3 with minimum Hamming distance 3, which contradicts the fact that $C_1(\mathrm{H}_{\mathscr{S}}) = 1$. On the other hand, since $c_3^1, \dots, c_{|\mathscr{A}|^i+1}^1$ have Hamming weight at least 3, we have that the Hamming distance between two elements in $\{c_3^1, \dots, c_{|\mathscr{A}|^i+1}^1\}$ is at most 2. Therefore assuming that C is good for $\mathrm{H}^i_{\mathscr{S}}$ implies that one of $\{c_1^2, c_2^2, c_3^2\}, \dots, \{c_1^i, c_2^i, c_3^i\}$ must be a code with cardinality 3 and minimum Hamming distance 3, which again contradicts $C_1(\mathrm{H}_{\mathscr{S}}) = 1$.

We are now ready to prove the main result of this subsection.

Proposition 4.12. *Let $\mathscr{A}$ be an alphabet and $\boldsymbol{A}_{\mathscr{S}}$ be an adversary able to corrupt up to 1 edge of the set of outgoing edges of the source of $\mathscr{S}$. Then the i-shot capacity of $\mathscr{S}$ in Scenario A.1 is*

$$C_i(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = 1.$$

Proof. We use an approach similar to the one in [1, Example 56]. Let $\mathscr{F}$ be a network code for $(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}})$ and assume that $\boldsymbol{A}$ can corrupt at most 1 edge from $\{e_1, e_2, e_3, e_4\}$. Let $x = (x_1, \dots, x_{4i}) \in \mathscr{A}^{4i}$. We have that

$$\Omega'_i(x) = \mathrm{H}^i_{\mathscr{S}}(\mathscr{F}^1(x_1, x_2, x_3, x_4), \dots, \mathscr{F}^i(x_{4i-3}, x_{4i-2}, x_{4i-1}, x_{4i})).$$

We want to show that $C_1(\Omega_i') < |\mathscr{A}|^i + 1$. Assume that there exists a code $C \subseteq (\mathscr{A}^4)^i$ with $|C| = |\mathscr{A}|^i + 1$ which is good for Ω_i'. Then

$$C' := \{\mathscr{F}^1(x_1, x_2, x_3, x_4), \ldots, \mathscr{F}^i(x_{4i-3}, x_{4i-2}, x_{4i-1}, x_{4i})) : x \in C\} \subseteq \mathscr{A}^{2i}$$

is an unambiguous code for $\mathrm{H}^i_{\mathscr{S}}$ with $|C'| = |\mathscr{A}|^i + 1$. We have that there must exist $a, a' \in C$, $a \neq a'$ such that $(a_1, \ldots, a_{|\mathscr{A}|^i}) = (a'_1, \ldots, a'_{|\mathscr{A}|^i})$. Therefore, C' is a good code for $\mathrm{H}^i_{\mathscr{S}}$ which has two different code words that coincide in the first $|\mathscr{A}|^i$ components. However, by Example 4.11, this code does not exist. This implies that $C_1(\Omega_i') < \log_{|\mathscr{A}|}(|\mathscr{A}|^i + 1)$ and we get $C_i(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) \leq 1$. □

In particular, we have that

$$C_i(\Omega_{\mathscr{S}}) = \frac{C_1(\Omega^i_{\mathscr{S}})}{i} \geq \frac{iC_1(\Omega_{\mathscr{S}})}{i} = C_1(\Omega_{\mathscr{S}}) = 1.$$

Therefore, $C_i(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = C_1(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = 1$ and there is no advantage of using $\mathscr{S}$ multiple times for communication.

Scenario A.2

It is not hard to check that for an adversary able to attack up to 1 edge and can change the edge attacked each transmission round, $C_i(\mathscr{S}, \boldsymbol{A}_{\mathscr{S}}) = 1$ in Scenario A.2. This follows by using arguments similar to the ones in Example 4.11 and in the proof of Proposition 4.12. For the lower bound, the strategy provided for the one-shot case can be reused each transmission round.

4.2 Multishot Capacity of Families of Networks

In this section, we compute bounds on the multishot capacity of families of networks introduced in [5, Section V-C].

4.2.1 Family $\mathfrak{C}_t$ and $\mathfrak{D}_t$

In this section, we will compute the multishot capacity of Family $\mathfrak{C}_t$ and Family $\mathfrak{D}_t$ in both scenarios. Recall that we assume that $t \geq 2$, since $t = 1$ recovers the Diamond Network. We start with the following notation.

Notation 5. *Let $\mathscr{A}$ be an alphabet. Denote*

$$\Omega^i_{\mathfrak{C}_t} := \Omega_{\mathfrak{C}_t}[\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)] \times \cdots \times \Omega_{\mathfrak{C}_t}[\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)]$$

to be the $i-$th power channel for $\mathfrak{C}_t$. Suppose an adversary $\boldsymbol{A}_{\mathfrak{C}_t}$ can corrupt up to t edges of $\mathfrak{C}_t$ on the first level. Let $\mathrm{H}_{\mathfrak{C}_t}$ be the channel that describes the action of the adversary, given by

$$\mathrm{H}_{\mathfrak{C}_t} : \mathscr{A}^{2t+1} \dashrightarrow \mathscr{A}^{2t+1}, \mathrm{H}_{\mathfrak{C}_t}(x) := \{y \in \mathscr{A}^{2t+1} : d_H(x, y) \leq t\}.$$

It is easy to check that the largest unambiguous code for $\mathrm{H}_{\mathfrak{C}_t}$ is $|\mathscr{A}|$ and there is no larger code. This implies that $C_1(\mathrm{H}_{\mathfrak{C}_t}) = 1$.

Note that C is an unambiguous code for $\mathrm{H}^i_{\mathfrak{C}_t}$ if and only if for $x, y \in C$ one of $d_{\mathrm{H}}(x^1, y^1) \geq 2t + 1, \ldots, d_{\mathrm{H}}(x^i, y^i) \geq 2t + 1$. The next example provides the size of the largest unambiguous code for $\mathrm{H}^i_{\mathfrak{C}_t}$.

Example 4.13. Assume C is an unambiguous code for $\mathrm{H}^i_{\mathfrak{C}_t}$ with $|C| = |\mathscr{A}|^i + 1$. Define $x^1 = (x_1, \ldots, x_{2t+1}), \ldots, x^i = (x^i_1, \ldots, x^i_{2t+1})$. With the same approach that was applied in Example 4.12 and [5, Example 9], we claim that there are no two codewords that coincide in the first $|\mathscr{A}|^i$ components. Let $c_1, \ldots, c_{|\mathscr{A}|^i+1} \in C$. Without loss of generality, we can assume that for $c_1, c_2 \in C$, $c^1_1 = c^1_2$ and $c_1 = 0$. This implies that $c^1_3, \ldots, c^1_{|\mathscr{A}|^i+1}$ must have Hamming weight $2t+1$. If not, assume that c^1_3 has Hamming weight less than $2t+1$. This allows one of $\{c^2_1, c^2_2, c^2_3\}, \ldots, \{c^i_1, c^i_2, c^i_3\}$ to be a good code of Hamming distance atleast $2t+1$ and of cardinality 3, contradicting the original capacity for $\mathrm{H}_{\mathfrak{C}_t}$. Since we have that $c^1_3, \ldots, c^1_{|\mathscr{A}|^i+1}$ have Hamming weight $2t+1$, a comparison of any two elements gives Hamming distance at most $t+1$. We assume that C is good for $\mathrm{H}^i_{\mathfrak{C}_t}$, therefore one of $\{c^2_1, c^2_2, c^2_3\}, \ldots, \{c^i_1, c^i_2, c^i_3\}$ has to be an unambiguous code for $\mathrm{H}_{\mathfrak{C}_t}$ with cardinality 3 and minimum Hamming distance $2t+1$ contradicting $C_1(\mathrm{H}_{\mathfrak{C}_t}) = 1$.

Finally, we are ready to compute the multishot capacity of $\mathfrak{C}_t$.

Proposition 4.14. *Let $\mathscr{A}$ be an alphabet. Recall that $\boldsymbol{A}_{\mathfrak{C}_t}$ can corrupt up to t edges of the first level of $\mathfrak{C}_t$. Then the i-shot capacity of $\mathfrak{C}_t$ is*

$$C_i(\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}) = 1.$$

Proof. We first show that $|C| \leq |\mathscr{A}|^i$. Let $\boldsymbol{A}_{\mathfrak{C}_t}$ be an adversary who is restricted to corrupting t edges of the network $\mathfrak{C}_t$ on the first level. The action the adversary may take is described by $\mathrm{H}_{\mathfrak{C}_t}$ as in Notation 5. Let $\mathscr{F}$ be a network code for $\mathfrak{C}_t$, where $\mathscr{F}_V : \mathscr{A}^{2t+1} \to \mathscr{A}^{2t+1}$ for $V \notin \mathbf{S} \cup \mathbf{T}$, with $\mathbf{S} = S, \mathbf{T} = T$. We will use $\mathfrak{C}_t$ in i transmission rounds with network codes $\mathscr{F}_1, \ldots, \mathscr{F}_i$ respectively. We have that i uses of $\mathfrak{C}_t$ is represented by $\Omega^i_{\mathfrak{C}_t}$ as in Notation 5. For $x = (x_1, \ldots, x_{(2t+1)i}) \in \mathscr{A}^{2t+1} \times \cdots \times$

$\mathscr{A}^{2t+1}$, we have that

$$\Omega^i_{\mathfrak{C}_t}(x) := \mathrm{H}^i_{\mathfrak{C}_t}(\mathscr{F}^1_V(x_1,\dots,x_{2t+1}),\dots,\mathscr{F}^i(x_{(2t+1)(i-1)+1},\dots,x_{(2t+1)i}).$$

Assume that there exists an unambiguous code C with $|C| = |\mathscr{A}|^i + 1$. Then there exists a good code

$$C' := \{\mathscr{F}^1(x_1,\dots,x_{2t+1}),\dots,\mathscr{F}^i(x_{(2t+1)(i-1)+1},\dots,x_{(2t+1)i}))\} \subseteq \mathscr{A}^{2t+1}\times\cdots\times\mathscr{A}^{2t+1}$$

which is good for $\mathrm{H}^i_{\mathfrak{C}_t}$ of cardinality $|\mathscr{A}|^i + 1$. Since we have that $|C'| = (|\mathscr{A}|)^i + 1$, there must exist $y, y' \in C$, $y \neq y'$ such that they coincide in the first $|\mathscr{A}|^i$ components, such that $C' \in \mathscr{A}^{2t+1}\times\cdots\times\mathscr{A}^{2t+1}$ a good code for $\mathrm{H}^i_{\mathfrak{C}_t}$ which has two different code words that coincide in the first $|\mathscr{A}|^i$ components. However, it was shown in Example 4.13, a code of this type does not exist. Therefore $|C| \leq |\mathscr{A}|^i$.

It remains to show that $C_i(\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}) \geq 1$. This immediately follows from [1, Proposition 12] using the channel $\Omega^i_{\mathfrak{C}_t}$ associated to $\mathfrak{C}_t$, with

$$C_i(\Omega_{\mathfrak{C}_t}, \boldsymbol{A}_{\mathfrak{C}_t}) = C_1(\Omega^i_{\mathfrak{C}_t}, \boldsymbol{A}_{\mathfrak{C}_t})\frac{C_1(\Omega^i_{\mathfrak{C}_t})}{i} \geq \frac{iC_1(\Omega_{\mathfrak{C}_t})}{i} = C_1(\Omega_{\mathfrak{C}_t}, \boldsymbol{A}_{\mathfrak{C}_t}) = 1.$$

Combining achieves the desired result.

□

Therefore, there is no gain in using $\mathfrak{C}_t$ multiple times for communication.

We now would like to compute the multishot capacity of Family $\mathfrak{D}_t$. For the following

proofs, we make no assumption on the adversary, therefore they can be extended in both scenarios. We start with some necessary notation.

Notation 6. *Let $\mathscr{A}$ be an alphabet and $\boldsymbol{A}_{\mathfrak{D}_t}$ be an adversary acting on $\mathfrak{D}_t$. Denote*

$$\Omega^i_{\mathfrak{D}_t} := \Omega_{\mathfrak{D}_t}[\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)] \times \cdots \times \Omega_{\mathfrak{D}_t}[\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)]$$

to be the $i-$th power channel for $\mathfrak{D}_t$ that represents i uses of $\mathfrak{D}_t$.

Notation 7. *Suppose an adversary $\boldsymbol{A}$ can corrupt up to t edges of $\mathfrak{D}_t$. Let $\mathrm{H}_{\mathfrak{D}_t}$ be the channel that describes the action of the adversary with $\mathrm{H}_{\mathfrak{D}_t} : \mathscr{A}^{4t} \dashrightarrow \mathscr{A}^{4t}$ defined by $\mathrm{H}_{\mathfrak{D}_t}(x) := \{y \in \mathscr{A}^{4t} : d_H(x, y) \leq t\}$. We note that the largest unambiguous code for $\mathrm{H}_{\mathfrak{D}_t}$ is $|\mathscr{A}|$ and there is no larger code. This implies that $C_1(\mathrm{H}_{\mathfrak{D}_t}) = 1$.*

Proposition 4.15. *Let $\mathscr{A}$ be an alphabet and let $\boldsymbol{A}_{\mathfrak{D}_t}$ be an adversary that is able to corrupt up to t edges on the first level of $\mathfrak{D}_t$. Then $C_i(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) \geq 1$.*

Proof. This is an immediate result from applying [1, Proposition 12] using the power channel $\Omega^i_{\mathfrak{D}_t}$. In particular,

$$C_i(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) = C_i(\Omega_{\mathfrak{D}_t}) = \frac{C_1(\Omega^i_{\mathfrak{D}_t})}{i} \geq \frac{iC_1(\Omega_{\mathfrak{D}_t})}{i} = C_1(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) = 1.$$

□

We described a structural property for which a code C is good for H. We find that a code C is good for H^i if and only if one of $d_{\mathrm{H}}(x^1, y^1) \geq 3t, \ldots, d_{\mathrm{H}}(x^i, y^i) \geq 3t$.

We wish to show that the largest unambiguous code for $\mathfrak{D}_t$ is $|C| = |\mathscr{A}|^i$. We provide a similar proof as in the upper bound of the Mirrored Diamond Network $\mathscr{S}$.

Example 4.16. We let C be any good code for $\mathrm{H}^i_{\mathfrak{D}_t}$ with $|C| = |\mathscr{A}|^i + 1$. Define $x^1 = (x_1, \ldots, x_{4t}), \ldots, x^i = (x^i_1, \ldots, x^i_{4t})$. With the same approach that was applied in Example 4.12 and [1, Example 9], we wish to show that there are no two codewords that coincide in the first $|\mathscr{A}|^i$ components. Let $c_1, \ldots, c_{|\mathscr{A}|^i+1} \in C$. Without loss of generality, we can assume that for $c_1, c_2 \in C$, $c^1_1 = c^1_2$ and $c_1 = 0$. This implies that $c^1_3, \ldots, c^1_{|\mathscr{A}|^i+1}$ must have Hamming weight $3t$. If not, assume that c^1_3 has Hamming weight less than $3t$. This allows one of $\{c^2_1, c^2_2, c^2_3\}, \ldots, \{c^i_1, c^i_2, c^i_3\}$ to be a good code of Hamming distance atleast $3t$ and of cardinality 3 contradicting the fact that $C_1(\mathrm{H}_{\mathfrak{D}_t}) = 1$. Since we have that $c^1_3, \ldots, c^1_{|\mathscr{A}|^i+1}$ have Hamming weight atleast $3t$, a comparison of any two elements gives Hamming distance atmost $2t$. We assume that C is good for $\mathrm{H}^i_{\mathfrak{D}_t}$, therefore one of $\{c^2_1, c^2_2, c^2_3\}, \ldots, \{c^i_1, c^i_2, c^i_3\}$ is an unambiguous code for $\mathrm{H}_{\mathfrak{D}_t}$ with cardinality 3 and minimum Hamming distance $3t$ contradicting again the capacity of $\mathrm{H}_{\mathfrak{D}_t}$.

We are now ready to compute the multishot capacity of Family $\mathfrak{D}_t$ in Scenario A.1 and A.2.

Proposition 4.17. *Let $\mathscr{A}$ be an alphabet and let $\boldsymbol{A}_{\mathfrak{D}_t}$ be an adversary that can corrupt up to t edges on the first level of $\mathfrak{D}_t$. Then the i-shot capacity of $\mathfrak{D}_t$ is*

$$C_i(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) = 1.$$

Proof. Consider an adversary $\boldsymbol{A}_{\mathfrak{D}_t}$ who is restricted to corrupting t edges of the network $\mathfrak{D}_t$ on the first level. The action the adversary may take is described by the channel $\mathrm{H}_{\mathfrak{D}_t} := \mathscr{A}^{4t} \dashrightarrow \mathscr{A}^{4t}$ denoted by

$$H(x) := \{y \in \mathscr{A}^{4t} : d_{\mathrm{H}}(x, y) \leq t\}.$$

Let $\mathscr{F}$ be a network code for $\mathfrak{D}_t$ with $\mathscr{F} : \mathscr{A}^{4t} \to \mathscr{A}^2$. Assume we use the network i times with network codes $\mathscr{F}_1, \ldots, \mathscr{F}_i$. We have that i uses of $\mathfrak{D}_t$ is represented by $\Omega^i_{\mathfrak{D}_t}$ as in 6. For $x = (x_1, \ldots, x_{4it}) \in \mathscr{A}^{4t} \times \cdots \times \mathscr{A}^{4t}$, we have that

$$\Omega^i_{\mathfrak{D}_t}(x) := \mathrm{H}^i_{\mathfrak{D}_t}(\mathscr{F}^1_V(x_1, \ldots, x_{4t}), \ldots, \mathscr{F}^i(x_{4(i-1)t+1}, \ldots, x_{4it}).$$

We will show that $C_1(\Omega^i_{\mathfrak{D}_t}) \leq |\mathscr{A}|^i$. Assume towards a contradiction that there exists an unambiguous code C such that $|C| = |\mathscr{A}|^i + 1$. Then this implies that we have a good code

$$C' := \{\mathscr{F}^1(x_1, \ldots, x_{4t}), \ldots, \mathscr{F}^i(x_{4(i-1)t+1}, \ldots, x_{4it}))\} \subseteq \mathscr{A}^{4t} \times \cdots \times \mathscr{A}^{4t}$$

which is good for $\mathrm{H}^i_{\mathfrak{D}_t}$ of cardinality $|\mathscr{A}|^i + 1$. Since we have that $|C'| = (|\mathscr{A}|)^i + 1$, there must exist $y, y' \in C$, $y \neq y'$ such that they coincide in the first $|\mathscr{A}|^i$ components, making $C' \in \mathscr{A}^{4t} \times \cdots \times \mathscr{A}^{4t}$ a good code for $\mathrm{H}^i_{\mathfrak{D}_t}$ which has two different code words that coincide in the first $|\mathscr{A}|^i$ components. However, by example 4.16, a code of this type does not exist. Therefore $|C| \leq |\mathscr{A}|^i$. Combining with Proposition 4.15 gives the desired result.

□

Therefore, there is no gain in using $\mathfrak{D}_t$ multiple times for communication. Notice that the proof does not depend on whether the adversary does or does not changes the edges attacked each transmission round, therefore can be reused in both scenarios. That is, $C_i(\mathfrak{C}_t, \boldsymbol{A}_{\mathfrak{C}_t}) = C_i(\mathfrak{D}_t, \boldsymbol{A}_{\mathfrak{D}_t}) = 1$ in Scenario A.2.

Remark 4.18. There is no strategy that we can provide for Family $\mathfrak{C}_t$ and Family $\mathfrak{D}_t$ that provides a gain in capacity in Scenario A.1 as there is for the Diamond Network $\mathscr{D}$.

4.2.2 Family $\mathfrak{E}_t$

In this section, we compute the multishot capacity of Family $\mathfrak{E}_t$ in both scenarios.

Scenario A.1:

We first consider the multishot capacity of Family $\mathfrak{E}_t$ in Scenario A.1. We assume that the adversary can attack t edges but cannot change the edges attacked each transmission round.

Let $\mathscr{U}_S$ be the set of edges directly connected to the source S. Let $\boldsymbol{A}_{\mathfrak{E}_t}$ be an adversary able to corrupt up to t edges of $\mathscr{U}_S$ of $\mathfrak{E}_t$. In [5, Theorem 6.15], it was shown that the one-shot capacity of $\mathfrak{E}_t$ satisfies

$$C_1(\mathfrak{E}_t, \mathbf{A}_{\mathfrak{E}_t}) < 1.$$

Let B be a set of reserved vectors in $\mathscr{A}^{2t+1}$ with $|B| = b$. Let $C \subseteq \mathscr{A}^{2t+1}$ be the largest unambiguous code for $\mathfrak{E}_t$ for $\Omega[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(T), \mathscr{U}_S, t]$, with $|C| = |\mathscr{A}| - b$ and let there exist a communication scheme that attains this. Then

$$C_1(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - b).$$

Our goal is to show that the $i-$shot capacity of $\mathfrak{E}_t$ in Scenario A.1 is

$$C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - b)}{i}.$$

Notation 8. *We define the sets*

$$B^i := \{\underbrace{(k|\ldots|k)}_{i\text{-times}} : k \in B\},$$
$$B_1^i := \{(k_1,\ldots,k_t|\ldots|k_1,\ldots,k_t) : k \in B\},$$
$$B_2^i := \{(k_{t+1},\ldots,k_{2t+1}|\ldots|k_{t+1},\ldots,k_{2t+1}) : k \in B\}.$$

Note that B^i, B_1^i and B_2^i also have cardinality b. We begin with a motivating example.

Example 4.19. Consider the Diamond Network $\mathscr{D}$ in Scenario A.1. Recall that in this scenario the adversary can attack 1 edge of $\{e_1, e_2, e_3\}$ but cannot the edge attacked each transmission round. Notice that $\mathscr{D}$ is the network $\mathfrak{E}_1$, where $t = 1$. For this network, the reserved set of vectors $B \in \mathscr{A}^{3i}$ has cardinality 1, where $(\star,\ldots,\star) \in \mathscr{A}^i$ is the reserved vector that can detect where the adversary is acting. Therefore, we showed in Section 6.1.1 that $C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i-1)}{i}$.

We now start with some necessary notation and definitions.

Notation 9. *[5, Notation 5.3] If we have an outer code $C \subseteq \mathscr{A}^{a_1+a_2+\ldots+a_n}$. For a given $x \in C$, we denote by $B_t^H(x)$ the Hamming ball of radius t with center x, and $S_t^H(x)$ the shell of that ball. We define them as*

$$B_t^H(x) = \{y \in \mathscr{A}^{a_1+a_2+\ldots+a_n} : d_{\mathrm{H}}(x,y) \leq t\}, S_t^H(x) = \{y \in B_t^H(x) : d_{\mathrm{H}}(x,y) = t\}.$$

Definition 4.20. Define $\pi_k^i : \mathscr{A}^{(2t+1)i} \to \mathscr{A}^i$ to be the projection onto the coordinates corresponding to the edges to intermediate node V_k of the simple two level network $\mathscr{N}$.

The following theorem provides a construction of the maximum unambiguous code for $\mathfrak{E}_t$ with cardinality $|\mathscr{A}|^i - b$, that is, $C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i-b)}{i}$.

Theorem 4.21. *Let $\mathscr{A}$ be an alphabet, $\mathscr{U}_S$ be the set of sources connected to the source S and let $\boldsymbol{A}_{\mathfrak{E}_t}$ be an adversary able to corrupt up to t edges of $\mathscr{U}_S$ of $\mathfrak{E}_t$. Then the $i-$shot capacity of $\mathfrak{E}_t$ in Scenario A.1 is*

$$C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - b)}{i}.$$

Proof. We first start with the lower bound. Our goal is to show that the code

$$C = \{(a|\dots|a) \in (\mathscr{A}^i)^{2t+1} : (a_1, \dots, a_{(2t+1)i}) \notin B^i\} \subseteq (\mathscr{A}^i)^{2t+1}$$

is unambiguous for $\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(T), \mathscr{U}_S, t]$. Recall that the adversary can attack t edges but **cannot change** the edges attacked each transmission round. We send a $(2t+1)i-$repetition code and we fix a network code $\mathscr{F} = \mathscr{F}_1, \mathscr{F}_2$. Suppose that the adversary change t symbols in the network. We have two cases:

Case 1: If $\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(V_1), \mathscr{U}_S, t](a|\dots|a) = (b_1|\dots|b_j|a|\dots|a)$, $j \geq t/2$, then the terminal receives

$$\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(T), \mathscr{U}_S, t](a|\dots|a) = \{(k|a), a \in \mathscr{A}^{(t+1)i} \setminus B_2^i, k \in B_1^i\}$$

and trusts and decodes the symbols from V_2.

Case 2: If $\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(V_2), \mathscr{U}_S, t](a|\dots|a) = (b_1|\dots|b_l|a|\dots|a)$ with $l \geq t/2 + 1$, then the terminal receives

$$\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(T), \mathscr{U}_S, t](a|\dots|a) = \{(a|k), a \in \mathscr{A}^{ti} \setminus B_1^i, k \in B_2^i\}.$$

and trusts and decodes the symbols from V_1.

It follows that for any $c, c' \in C$, we have that

$$\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T), \mathscr{U}_S, t](c) \cap \Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T), \mathscr{U}_S, t](c') \neq \emptyset$$

if and only if $c = c'$. This shows that C is an unambiguous code. One can easily check that $|C| \geq |\mathscr{A}|^i - b$.

It remains to show the upperbound. The following generalizes [5, Theorem 6.15] in the multishot setting. Assume towards a contradiction that there exists an unambiguous code C for $\Omega^i[\mathfrak{E}_t, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T), \mathscr{U}_S, t]$ such that $|C| = |\mathscr{A}|^i - b + 1$ for some choice of network code $\mathscr{F} = \mathscr{F}_1, \mathscr{F}_2$. We note that for any unambiguous code, any subcode is also unambiguous. Let $x = (x_1, \ldots, x_{(2t+1)i})$ with $x_1 = (x_1, \ldots, x_{2t+1}), \ldots x_i = (x_{(2t+1)(i-1)+1}, \ldots, x_{(2t+1)i})$. Since C is unambiguous, it must be the case that one of $d_{\mathrm{H}}(x_1, y_1) \geq 2t+1, \ldots, d_{\mathrm{H}}(x_i, y_i) \geq 2t+1$. Then $\pi_1^i(C)$ contains $|\mathscr{A}|^i - b + 1$ distinct elements. It follows that $\mathscr{F}_1(\pi_1^i(C)) = |\mathscr{A}|^i \setminus |B|^i + 1$.

To conclude, there must exist $x, y \in C$ and some $e \in \mathscr{A}^{(2t+1)i}$ such that

$$x \neq y, \mathscr{F}_1(\pi_1^i(x)) = \mathscr{F}_1(\pi_1^i(e)) \quad \text{and} \quad d_{\mathrm{H}}(\pi_1^i(e), \pi_1^i(y)) \leq ti - 1.$$

We then have that

$$x' := (x_1, \ldots, x_{ti}, x_{ti+1}, y_{ti+2}, \ldots, y_{(2t+1)i}) \in B_t^H(x),$$

$$y' := (e_1, \ldots, e_{ti}, x_{ti+1}, y_{ti+2}, \ldots, y_{(2t+1)i}) \in B_t^H(y).$$

Lastly, we can observe that

$$(\mathscr{F}_1(\pi_1^i(x'), \mathscr{F}_2(\pi_2^i(x')) = (\mathscr{F}_1(\pi_1^i(y'), \mathscr{F}_2(\pi_2^i(y')) \in \Omega^i(x) \cap \Omega^i(y),$$

which contradicts C being an unambiguous code. Therefore $C_i(\mathfrak{E}_t, \boldsymbol{A}, \mathscr{U}_S, t) \leq \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - b)}{i}$. Combining we obtain

$$C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - b)}{i}.$$

□

The above theorem shows a gain in using $\mathfrak{E}_t$ multiple times for communication without having to compute the one-shot capacity. Note that if $t = 1$, we have the Diamond Network $\mathscr{D}$ where the multishot capacity was computed as $C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)}{i}$.

Scenario A.2

Recall that in this scenario, we assume that the adversary can attack up to t edges of the first level of $\mathfrak{E}_t$, but **can change** the edges attacked each transmission round. We will show that

$$C_1(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - b).$$

Let $\Omega^i_{\mathfrak{E}_t}$ be the power channel for $\mathfrak{E}_t$. We begin with the following notation.

Notation 10. *Suppose that an adversary $\boldsymbol{A}$ can corrupt up to t components of $x \in \mathscr{A}^{2t+1}$, that is, the adversary can corrupt up to t edges of $\mathfrak{E}_t$. The action of the adversary can be represented as the channel*

$$\mathrm{H}_{\mathfrak{E}_t} : \mathscr{A}^{2t+1} \dashrightarrow \mathscr{A}^{2t+1}, \mathrm{H}_{\mathfrak{E}_t}(x) = \{y \in \mathscr{A}^{2t+1} : d_{\mathrm{H}}(x, y) \leq t\}.$$

From the construction of the unambiguous code for $C_1(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t})$, the largest unambigu-

ous code for $H_{\mathfrak{E}_t}$ has cardinality $|\mathscr{A}|-b$ and there is no larger code (since b vectors are reserved). Thus $C_1(\mathrm{H}_{\mathfrak{E}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}|-b)$.

The next example is similar to the proofs of the upperbound for Family $\mathfrak{C}_t$ and $\mathfrak{D}_t$.

Example 4.22. Let C be a good code for $H^i_{\mathfrak{E}_t}$ with $|C| = (|\mathscr{A}|-b)^i+1$. Define $x^1 = (x_1,\ldots,x_{2t+1}),\ldots,x^i = (x^i_1,\ldots,x^i_{2t+1})$. With the same approach that was applied in [1, Example 9], we claim that there are no two codewords that coincide in the first $(|\mathscr{A}|-b)^i$ components. Let $c_1,\ldots,c_{(|\mathscr{A}|-b)^i+1} \in C$. Without loss of generality, we can assume that for $c_1,c_2 \in C$, $c^1_1 = c^1_2$ and $c_1 = 0$. This implies that $c^1_3,\ldots,c^1_{(|\mathscr{A}|-b)^i+1}$ must have Hamming weight $2t+1$. If not, assume that c^1_3 has Hamming weight less than $2t+1$. This allows one of $\{c^2_1,c^2_2,c^2_3\},\ldots,\{c^i_1,c^i_2,c^i_3\}$ to be a good code of Hamming distance atleast $2t+1$ and of cardinality 3, contradicting the original capacity for $\mathrm{H}_{\mathfrak{E}_t}$. Since we have that $c^1_3,\ldots,c^1_{(|\mathscr{A}|-b)^i+1}$ have Hamming weight $2t+1$, a comparison of any two elements gives Hamming distance atmost $t+1$. We assume that C is good for $\mathrm{H}^i_{\mathfrak{C}_t}$, therefore one of $\{c^2_1,c^2_2,c^2_3\},\ldots,\{c^i_1,c^i_2,c^i_3\}$ has to be an unambiguous code for $\mathrm{H}_{\mathfrak{C}_t}$ with cardinality 3 and minimum Hamming distance $2t+1$ contradicting $C_1(\mathrm{H}_{\mathfrak{C}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}|-b)$.

The next proposition computes $C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t})$ in Scenario 2.

Proposition 4.23. *Let $\mathscr{A}$ be an alphabet, $\mathscr{U}_S$ be the set of sources connected to the source S and let $\boldsymbol{A}_{\mathfrak{E}_t}$ be an adversary able to corrupt up to t edges of $\mathscr{U}_S$ of $\mathfrak{E}_t$. Then the $i-$shot capacity of $\mathfrak{E}_t$ in Scenario A.2 is $C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}|-b)$.*

Proof. Assume that the code we are using each round is a $2t+1$-times repetition code $(a,\cdots,a)$ for $a \in \mathscr{A}$. We first show that $|C| \leq (|\mathscr{A}|-b)^i$. Let $\boldsymbol{A}_{\mathfrak{E}_t}$ be an adversary who is restricted to corrupting t edges of the network $\mathfrak{E}_t$ on the first level. The action

the adversary is described by $\mathrm{H}_{\mathfrak{E}_t}$ as described above. Let $\mathscr{F}$ be a network code for $\mathfrak{E}_t$, where $\mathscr{F}_V : \mathscr{A}^{2t+1} \to \mathscr{A}^{2t+1}$. We will use the same network code each transmission round. We have that i uses of $\mathfrak{C}_t$ is represented by $\Omega^i_{\mathfrak{E}_t}$. For $x = (x_1, \ldots, x_{(2t+1)i}) \in \mathscr{A}^{2t+1} \times \cdots \times \mathscr{A}^{2t+1}$, we have that

$$\Omega^i_{\mathfrak{E}_t}(x) := \mathrm{H}^i_{\mathfrak{E}_t}(\mathscr{F}^1_V(x_1, \ldots, x_{2t+1}), \ldots, \mathscr{F}^i(x_{(2t+1)(i-1)+1}, \ldots, x_{(2t+1)i}).$$

Now assume that there exists an unambiguous code C with $|C| = (|\mathscr{A}| - b)^i + 1$. Then there exists a good code

$$C' := \{\mathscr{F}^1(x_1, \ldots, x_{2t+1}), \ldots, \mathscr{F}^i(x_{(2t+1)(i-1)+1}, \ldots, x_{(2t+1)i}))\} \subseteq \mathscr{A}^{2t+1} \times \cdots \times \mathscr{A}^{2t+1}$$

which is good for $\mathrm{H}^i_{\mathfrak{E}_t}$ of cardinality $(|\mathscr{A}| - b)^i + 1$. Therefore there must exist $y, y' \in C$, $y \neq y'$ such that they coincide in the first $(|\mathscr{A}| - b)^i$ components, such that $C' \in \mathscr{A}^{2t+1} \times \cdots \times \mathscr{A}^{2t+1}$ a good code for $\mathrm{H}^i_{\mathfrak{E}_t}$ which has two different code words that coincide in the first $(|\mathscr{A}| - b)^i$ components. However, it was shown in Example 4.22, a code of this type does not exist. Therefore $|C| \leq (|\mathscr{A}| - b)^i$.

The lower bound comes directly from [1, Proposition 12], that is, we have that

$$C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = C_1(\Omega^i_{\mathfrak{E}_t}) \geq \frac{iC_1(\Omega_{\mathfrak{E}_t})}{i} = C_1(\Omega_{\mathfrak{E}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - b).$$

Combining we achieve the desired result.

□

The above proposition shows that $C_i(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = C_1(\mathfrak{E}_t, \boldsymbol{A}_{\mathfrak{E}_t}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - b)$, therefore there is no gain in using $\mathfrak{E}_t$ multiple times for communication in this scenario.

4.3 Multishot Capacity of Simple 3-level Networks

In [5], a reduction from 3−level networks to 2−level networks was provided, bounding the capacity of a 3−level network by the 2−level network associated to it. In this section, we will provide bounds on the multishot capacity of some 3−level networks and extend the Double Cut-Set Bound [5, Theorem 8.6] to the multishot realm. We start with the following notation that describes the transfer of information from $\mathscr{E}_1$ to $\mathscr{E}_2$, where $\mathscr{E}_1, \mathscr{E}_2$ are edge cuts such that $\mathscr{E}_1$ *precedes* $\mathscr{E}_2$. We say that for two edge cuts $\mathscr{E}_1, \mathscr{E}_2$, $\mathscr{E}_1$ precedes $\mathscr{E}_2$ if there exists a directed path in $\mathscr{N}$ that starts with $\mathscr{E}_1$ and ends with $\mathscr{E}_2$. The notation is $\mathscr{E}_1 \preccurlyeq \mathscr{E}_2$.

Notation 11. *[5] Let $(\mathscr{V}, \mathscr{E}, \mathbf{S}, \mathbf{T})$ be a network, $\mathscr{E}_1$ and $\mathscr{E}_2$ be two edge cuts such that $\mathscr{E}_1$ precedes $\mathscr{E}_2$. Let $\mathscr{A}$ be a network alphabet and $\mathscr{F}$ a network code for $(\mathscr{N}, \mathscr{A})$, $\mathscr{U} \subseteq \mathscr{E}$ be a set of edges, and $t \geq 0$, then we denote by*

$$\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t] : \mathscr{A}^{|\mathscr{E}_1|} \dashrightarrow \mathscr{A}^{|\mathscr{E}_2|} \tag{4.3.1}$$

the channel that describes the transfer from the edges of $\mathscr{E}_1$ to those of $\mathscr{E}_2$, when an adversary can corrupt up to t edges from $\mathscr{U} \cap \mathscr{E}_1$.

We begin with the following proposition, that extends [5, Theorem 5.8] to the multishot setting.

Proposition 4.24. *Let $\mathscr{N}_3$ be a simple 3-level network, and let $\mathscr{N}_2$ be the simple 2-level network associated to it introduced in [5]. Define $\mathscr{U}_3$ and $\mathscr{U}_2$ to be the set of edges directly connected to the sources of $\mathscr{N}_3$ and $\mathscr{N}_2$ and define $\boldsymbol{A}_{\mathscr{N}_3}, \boldsymbol{A}_{\mathscr{N}_2}$ to be the adversary able to corrupt up to t edges of $\mathscr{U}_3$ and $\mathscr{U}_2$ respectively. Then for all alphabets $\mathscr{A}$,*

$$C_i(\mathscr{N}_3, \boldsymbol{A}_{\mathscr{N}_3}) \leq C_i(\mathscr{N}_2, \boldsymbol{A}_{\mathscr{N}_2}). \tag{4.3.2}$$

Proof. Let $\mathscr{F}_3$ be a network code and C_3 be an outer code for an alphabet $\mathscr{A}$ and the simple 3−level network $\mathscr{N}_3$. We note that the same network code is used each transmission round. Let C_3 be an unambiguous code for $\Omega^i[\mathscr{N}_3, \mathscr{A}, \mathscr{F}_3, S \to \mathbf{T}, \mathscr{U}_3, t]$, where Ω^i is the channel associated to i uses of $\mathscr{N}_3$. Let $G^{3,2}$, V^3_{ij}, $\mathscr{F}_{V^3_{ijk}}$ and the neighborhood of V^3_{ij} be defined as in [5, Theorem 4.8]. We wish to show that there exists $\mathscr{F}_2$ such that C_3 is unambiguous for $\Omega^i[\mathscr{N}_2, \mathscr{A}, \mathscr{F}_2, S \to \mathbf{T}, \mathscr{U}_2, t]$. Define $\mathscr{F}_2$ and more specifically $\mathscr{F}_{V_i}$ as in [5, Theorem 5.8], we have for each intermediate node V_i in $\mathscr{N}_2$ that corresponds to connected component i of $G^{3,2}$ as a composition of functions at nodes in V_1 and V_2 of $\mathscr{N}_3$. Since it was shown in the proof of [5, Theorem 4.8] that the fan out sets of $\Omega[\mathscr{N}_3, \mathscr{A}, \mathscr{F}_3, S \to \mathbf{T}, \mathscr{U}_3, t]$ and $\Omega[\mathscr{N}_2, \mathscr{A}, \mathscr{F}_2, S \to \mathbf{T}, \mathscr{U}_2, t]$ are exactly equal, it is easy to check that this is the case for $\Omega^i[\mathscr{N}_3, \mathscr{A}, \mathscr{F}_3, S \to \mathbf{T}, \mathscr{U}_3, t]$ and $\Omega^i[\mathscr{N}_2, \mathscr{A}, \mathscr{F}_2, S \to \mathbf{T}, \mathscr{U}_2, t]$, by definition of Ω^i. We can conclude that C_3 is unambiguous for $\Omega^i[\mathscr{N}_2, \mathscr{A}, \mathscr{F}_2, S \to \mathbf{T}, \mathscr{U}_2, t]$. Therefore $C_i(\mathscr{N}_3, \mathscr{A}, \mathscr{U}_3, t) \leq C_i(\mathscr{N}_2, \mathscr{A}, \mathscr{U}_2, t)$. □

The previous proposition tells us that for a simple 3−level network $\mathscr{N}_3$ and the simple 2−level network $\mathscr{N}_2$ associated to it, we have that the multishot capacity of $\mathscr{N}_3$ is upperbounded by the multishot capacity of $\mathscr{N}_2$, with the assumption that the network code $\mathscr{F}$ is the same in each transmission round. Before proving the main results, we need the following remark:

Remark 4.25. Note that same as in [5], we do not require the edge-cuts $\mathscr{E}_1$ and $\mathscr{E}_2$ to be minimal or even *antichain* cuts (i.e., cuts where any two different edges cannot be compared with respect to the order $\preccurlyeq$). Furthermore, since the channel $\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]$ considers the immediate predecessors in the network topology first, we also have that $\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]$ also considers the immediate predecessors first in the network topology. Therefore, we also have that the

channel $\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]$ provides the value of each edge of the edge cut$\mathscr{E}_2$ as a *function* of the values of the immediate predecessors in $\mathscr{E}_1$.

The following proposition generalizes the Double Cut-Set Bound [5, Theorem 8.6] in the multishot scenario.

Proposition 4.26 (The Multishot Double Cut-Set Bound)**.** *Let $\mathscr{N}$ be a network, $\mathscr{A}$ be an alphabet and $\mathscr{U} \subseteq \mathscr{E}$ be a set of edges. Let $\mathscr{E}_1$ and $\mathscr{E}$ be edge cuts such that $\mathscr{E}_1$ precedes $\mathscr{E}_2$. Let $\mathscr{F}$ be a network code and $\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, S \to \mathbf{T}, \mathscr{U}, t]$ be the channel associated to $\mathscr{N}$ and $\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, S \to T, \mathscr{U}, t]$ be the channel that represents i uses of $\mathscr{N}$. Then the one-shot capacity of $\mathscr{N}$ satisfies*

$$C_1(\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, S \to \mathbf{T}, \mathscr{U}, t]) \leq \max_{\mathscr{F}} C_1(\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U}, t])$$

with the maximum taken over all network codes $\mathscr{F}$ for $(\mathscr{N}, \mathscr{A})$.

Proof. Let $\mathscr{F}$ be a network code for $(\mathscr{N}, \mathscr{A})$. Using a similar approach as in [5, Theorem 8.6], consider the scenario where an adversary $\boldsymbol{A}$ can corrupt up to t edges of $\mathscr{U} \cap \mathscr{E}_1$. This scenario is modeled by the channel

$$\Omega^* := \Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathscr{E}_1, \mathscr{U} \cap \mathrm{out}(S), 0] \blacktriangleright \Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t] \blacktriangleright$$

$$\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_2 \to \mathrm{in}(\mathbf{T}), \mathscr{U} \cap \mathscr{E}_2, 0]$$

Therefore $\Omega^i := \prod_{n=1}^{i} \Omega^*$. Using [1, Proposition 18],

$$\Omega^{i'} := (\prod_{n=1}^{i} \Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathscr{E}_1, \mathscr{U} \cap \mathrm{out}(S), 0]) \blacktriangleright (\prod_{n=1}^{i} \Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t])$$

$$\blacktriangleright(\prod_{n=1}^{i}\Omega[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_2\to \text{in}\mathbf{T},\mathscr{U}\cap\mathscr{E}_2,0]).$$

Rewriting we get

$$\Omega^{i'}:=\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\text{out}(S)\to\mathscr{E}_1,\mathscr{U}\cap\text{out}(S),0])\blacktriangleright(\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_1\to\mathscr{E}_2,\mathscr{U}\cap\mathscr{E}_1,t])\blacktriangleright$$

$$\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_2\to\text{in}(\mathbf{T}),\mathscr{U}\cap\mathscr{E}_2,0]).$$

We notice that the first and last channel are deterministic and for ease of notation we will use the notation Ω_1^i and Ω_2^i. We note that the channel $\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},S\to\mathbf{T},\mathscr{U},t]$ is coarser than $\Omega_1^i\blacktriangleright\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_1\to\mathscr{E}_2,\mathscr{U}\cap\mathscr{E}_1,t]\blacktriangleright\Omega_2^i$ since in the second channel,the errors can only occur on $\mathscr{U}\cap\mathscr{E}_1$ and not all of $\mathscr{U}$. By Propositions 3.35 and 3.36, we have that

$$\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},S\to\mathbf{T},\mathscr{U},t])\geq\Omega_1^i\blacktriangleright\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_1\to\mathscr{E}_2,\mathscr{U}\cap\mathscr{E}_1,t]\blacktriangleright\Omega_2^i$$

and

$$C_1(\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},S\to\mathbf{T},\mathscr{U},t]))\leq C_1(\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_1\to\mathscr{E}_2,\mathscr{U}\cap\mathscr{E}_1,t]).$$

Since we chose $\mathscr{F}$ arbitrarily, this applies for the maximum $\mathscr{F}$, we see that

$$C_1(\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},S\to\mathbf{T},\mathscr{U},t]))\leq\max_{\mathscr{F}}C_1(\Omega^i[\mathscr{N},\mathscr{A},\mathscr{F},\mathscr{E}_1\to\mathscr{E}_2,\mathscr{U}\cap\mathscr{E}_1,t])$$

as desired. □

The previous proposition allows us to extend the Double Cut-Set bound provided in [5] to the multishot setting, so we can discuss results on 3−level networks. The next result is a corollary that extends [5, Corollary 8.7] also to the multishot setting.

Corollary 4.27. *Let $\mathscr{N}$ be a network, $\mathscr{A}$ a network alphabet, $\mathscr{U} \subseteq \mathscr{E}$ a set of edges and $t \geq 0$. Let $\mathscr{E}_1$ and $\mathscr{E}_2$ be edge-cuts between S and T such that $\mathscr{E}_1$ precedes $\mathscr{E}_2$. Let $\mathscr{N}'$ be a simple $3-$level network. As in [5], the vertices of V_1 are in bijection with the edges of $\mathscr{E}_1$ and the vertices of V_2 with the edges of $\mathscr{E}_2$. We say that a vertex $V \in V_1$ is connected to vertex $V' \in V_2$ if and only if the edge of $\mathscr{E}_1$ corresponding to V is an immediate predecessor of the edge of $\mathscr{E}_2$ corresponding to V', see Definition 3.28. Let $\mathscr{E}'_S$ be the set of edges directly connected with the source of $\mathscr{N}'$, which can be identified with the edges of $\mathscr{E}_1$ (consistent with how we identified these with the vertices in V_1). Let $\boldsymbol{A}_{\mathscr{N}}$ be the adversary able to corrupt up to t edges of $\mathscr{N}$ from $\mathscr{U}$ and let $\boldsymbol{A}_{\mathscr{N}'}$ be the adversary able to corrupt t edges of $\mathscr{N}'$ from $\mathscr{U} \cap \mathscr{E}'_S$. We then have*

$$\mathrm{C}_i(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) \leq \mathrm{C}_i(\mathscr{N}', \boldsymbol{A}_{\mathscr{N}'}). \tag{4.3.3}$$

Proof. Similar to the strategy in the proof of [5, Corollary 8.7], we will prove that

$$\mathrm{C}_i(\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]) \leq \mathrm{C}_i(\mathscr{N}', \mathscr{A}, \mathscr{U} \cap \mathscr{E}'_S, t)$$

for every network code $\mathscr{F}$, where $\mathscr{F}$ is the same for all i transmission rounds and for $(\mathscr{N}, \mathscr{A})$, which in turn establishes the corollary due to Proposition 4.26. We note that this proof is an extension of [5, Corollary 8.7]. We fix $\mathscr{F}$ and let $\Omega^i := \Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, 0]$, be the deterministic auxillary channel. By the Remark 4.25, we know that the channel Ω^i expresses the value of each edge $e \in \mathscr{E}_2$ as a function of the values of its immediate predecessors in $\mathscr{E}_1$. By the construction of $\mathscr{N}'$, we can find a network code $\mathscr{F}'$ that depends on $\mathscr{F}$) for $(\mathscr{N}', \mathscr{A})$ such that

$$\Omega^i = \Omega^i[\mathscr{N}', \mathscr{A}, \mathscr{F}', \mathscr{E}'_S \to \mathrm{in}(T), \mathscr{U} \cap \mathscr{E}'_S, 0], \tag{4.3.4}$$

where the edges of $\mathscr{E}_1$ and $\mathscr{E}_2$ are identified with those of $\mathscr{E}'_S$ and $\text{in}(T)$ in $\mathscr{N}'$. Following the strategy in the proof of [5, Theorem 8.7], we observe that the channel $\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]$ can be written as the concatenation

$$\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t] = (\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_1, \mathscr{U} \cap \mathscr{E}_1, t] \blacktriangleright \Omega)^i = \quad (4.3.5)$$

$$\Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_1, \mathscr{U} \cap \mathscr{E}_1, t] \blacktriangleright \Omega^i \quad (4.3.6)$$

where the first channel in the concatenation simply describes the action of the adversary on the edges of $\mathscr{U} \cap \mathscr{E}_1$ (in the terminology of [1]) over i transmission rounds and the last line coming from [1, Proposition 18]. By (4.3.4) and (4.3.5) and using the identifications between $\mathscr{E}_1$ and $\mathscr{E}'_S$, we can write

$$\begin{aligned}\Omega^i[\mathscr{N}', \mathscr{A}, \mathscr{F}', \mathscr{E}'_S \to (T), \mathscr{U} \cap \mathscr{E}'_S, t] &= \Omega^i[\mathscr{N}', \mathscr{A}, \mathscr{F}', \mathscr{E}'_S \to \mathscr{E}'_S, \mathscr{U} \cap \mathscr{E}'_S, t] \\ &\quad \blacktriangleright \Omega^i[\mathscr{N}', \mathscr{A}, \mathscr{F}', \mathscr{E}'_S \to (T), \mathscr{U} \cap \mathscr{E}'_S, 0] \\ &= \Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_1, \mathscr{U} \cap \mathscr{E}_1, t] \blacktriangleright \Omega^i \\ &= \Omega^i[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]. \quad (4.3.7)\end{aligned}$$

By definition, we have that $C_i(\mathscr{N}', \mathscr{A}, \mathscr{U} \cap \mathscr{E}'_S, t) \geq C_1(\Omega^i[\mathscr{N}', \mathscr{A}, \mathscr{F}', \mathscr{E}'_S \to in(T), \mathscr{U} \cap \mathscr{E}'_S, t])$, and combining this with (4.3.7), leads to

$$C_i(\mathscr{N}', \boldsymbol{A}_{\mathscr{N}'}) \geq C_1(\Omega^i[\mathscr{N}', \mathscr{A}, \mathscr{F}', \mathscr{E}'_S \to \text{in}(T), \mathscr{U} \cap \mathscr{E}'_S, t]) = \text{C}_i(\Omega[\mathscr{N}, \mathscr{A}, \mathscr{F}, \mathscr{E}_1 \to \mathscr{E}_2, \mathscr{U} \cap \mathscr{E}_1, t]).$$

Since we assumed that $\mathscr{F}$ was an arbitrary for $(\mathscr{N}, \mathscr{A})$ for i transmission rounds, the result follows. □

We now will illustrate the previous corollary with the following example. Consider the Butterfly Network in Figure 3.4, we call this $\mathscr{B}$. Recall that the one-shot capacity of

this network is $C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$ as provided in [5, Theorem 8.9]. This result followed from the fact that this network's one-shot capacity is upperbounded by the one-shot capacity of the Diamond Network $\mathscr{D}$. We will show that in Scenario A.1,

$$C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)}{i}$$

which demonstrates a gain in capacity over multiple uses of $\mathscr{B}$ in this scenario. In contrast, when in Scenario A.2, we will show that

$$C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$$

with $C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}})$.

4.3.1 Scenario A.1 for $\mathscr{B}$

Recall in this scenario that the adversary is restricted to corrupting $(t = 1)$ of the set $\mathscr{U} = \{e_1, e_2, e_3, e_4, e_5, e_6, e_9\}$ edge but cannot change the edge attacked each transmission round. We start with the following proposition.

Proposition 4.28. *Let $i \in \mathbb{N}$ and $\mathscr{F}$ be a network code for $(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}})$. If $C \subseteq \mathscr{A}^{4i}$ is an unambiguous code for $(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}, \mathscr{F})$ then the $i-$shot capacity of $\mathscr{B}$ in Scenario A.1 is*

$$C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1).$$

Proof. We reserve $\star \in \mathscr{A}$. We would like to show that the code

$$C = \{(c_1, \ldots, c_i, c_1, \ldots, c_i, c_1, \ldots, c_i, c_1, \ldots, c_i) \in \mathscr{A}^{4i} : (c_1, \ldots, c_i) \neq (\star, \ldots, \star)\} \subseteq \mathscr{A}^{4i}$$

is unambiguous for $\mathscr{B}$. We have that for any $c \in C$, $c = (a \mid a \mid a \mid a)$, with $a \in \mathscr{A}^i \setminus \{(\star, \ldots, \star)\}$. During each transmission round, we use the same network code $\mathscr{F}$ and strategy as in the proof provided for [5, Theorem 8.9]. Suppose the adversary corrupts e_1 or e_2 and is forced to change the symbol. One can easily show that

$$\Omega^i[\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)]((a \mid a \mid a \mid a)) = \{((\star, \ldots, \star) \mid a\}$$

for any $a \in \mathscr{A}^i \setminus \{(\star, \ldots, \star)\}$ and $T \in \mathbf{T}$. Similarly, if the adversary corrupts e_3 or e_4, we have that

$$\Omega^i[\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)]((a \mid a \mid a \mid a)) = \{(a \mid (\star, \ldots, \star)\}$$

for any $a \in \mathscr{A}^i \setminus \{(\star, \ldots, \star)\}$. It remains to show that C is unambiguous. Let $c, c' \in C$. It follows that

$$\Omega^i[\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](c) \cap \Omega^i[\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T)](c') \neq \emptyset$$

if and only if $c = c'$, therefore implying that C is unambiguous. Lastly, one can easily see that $|C| \geq |\mathscr{A}|^i - 1$. Thus $C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)$

The upperbound follows from Propositions 4.28, 4.26 and the observation in [5] that the reduction of $\mathscr{B}$ to a simple 2-level network is exactly the Diamond Network $\mathscr{D}$. Therefore $C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \leq \log_{|\mathscr{A}|}(|\mathscr{A}|^i - 1)$.

Combining we achieve the desired result.

□

We observe here that using the butterfly network multiple times for communication also provides a gain in capacity, given that the network's multishot capacity is upper

bounded by that of the Diamond Network.

4.3.2 Scenario A.2 for $\mathscr{B}$

Recall in this scenario that the adversary can attack one edge but can change the edge attacked each transmission round. We have the following result.

Proposition 4.29. *Let $\mathscr{A}$ be an alphabet and let $\boldsymbol{A}_{\mathscr{B}}$ be an adversary able to attack up to t edges of the first level. The $i-$shot capacity of the Butterfly Network $\mathscr{B}$ in Scenario A.2 is*

$$C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1).$$

Proof. The proof follows directly from the fact that $C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \leq C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}})$ and with our assumption that the adversary can change the edge attacked, we showed that $C_i(\mathscr{D}, \boldsymbol{A}_{\mathscr{D}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$. Therefore $C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) \leq \log_{|\mathscr{A}|}(|\mathscr{A}| - 1)$. The lower bound comes from applying the strategy in [5, Theorem 8.9] independently, meaning applying the strategy i times over i transmission rounds. □

The previous result tells us that there is no gain in using $\mathscr{B}$ multiple times for communication in Scenario A.2. Therefore,

$$C_i(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = C_1(\mathscr{B}, \boldsymbol{A}_{\mathscr{B}}) = \log_{|\mathscr{A}|}(|\mathscr{A}| - 1).$$

We note that the results of the Butterfly Network mirror those of the Diamond Network.

4.3.3 Other Adversarial Models

In this section, we provide results on more restrictive adversarial models. We discuss results on Family $\mathfrak{A}_t$ in these adversarial models. Recall that $\mathfrak{A}_t = ([t, 2t], [t, t]), t \geq 1$. The top half of the network refers to the t edges incoming V_1 and t edges outgoing V_1 and the bottom half of the network refers to the $2t$ edges incoming V_2 and the t edges outgoing V_2.

Adversarial model 1: Assume that the adversary is restricted to attacking $\lceil \frac{t}{2} \rceil$ symbols in the top half and $\lfloor \frac{t}{2} \rfloor$ symbols in bottom half, but cannot change two symbols from the same pair to the same symbols (ex: (a, a) to (b, b)). Let C be an unambiguous code for $H^i_{\mathfrak{A}_t}$, with

$$C = \{(a|b|\ldots|t, a|a|\ldots, |t|t) \in (\mathscr{A}^i)^{3t} \backslash B^i, a \neq b \neq \ldots \neq t, \text{ for } x, y \in C, d_{\mathrm{H}}(x^i, y^i) \geq 2t\}$$

Let Ω^i be the $i-$th power channel of Ω for $\mathfrak{A}_t$.

Let $\mathscr{F} = (\mathscr{F}_1, \mathscr{F}_2)$ be the network code, defined as follows:

$$\mathscr{F}_1(x_1, \ldots, x_t) = (x_1, \ldots, x_t)$$

$$\mathscr{F}_2 = \begin{cases} x_i & \text{if} \quad x_i = x_j \\ k, k \in B & \text{otherwise} \end{cases}$$

where $\mathscr{F}_2$ compares consecutive pairs of edges. The intermediate vertex V_2 is used to

denote where the adversary is acting. Without loss of generality,

$$\Omega[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(V_1), \mathscr{U}_S, t](a|b|\dots|t|a|a|\dots|t|t) \\ = (k|\lceil\frac{t}{2}\rceil + 1|\dots|t), k \in B_2^i, \lceil\frac{t}{2}\rceil + 1, \dots, t \in \mathscr{A}^i$$

and

$$\Omega[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(V_2), \mathscr{U}_S, t](a|a|\dots|c|c) \\ = (k|\lfloor\frac{t}{2}\rfloor|\dots|t), k \in B_3^i, \frac{t}{2}\rfloor, \dots, t \in \mathscr{A}^i$$

In this scenario, without loss of generality the terminal receives

$$\Omega[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \mathrm{out}(S) \to \mathrm{in}(T), \mathscr{U}_S, t](a|b|\dots|t|a|a|\dots|t|t) \\ = (k_1|\lceil\frac{t}{2}\rceil + 1|\dots|t|k_2|\lfloor\frac{t}{2}\rfloor|\dots|t), k_1 \in B_2^i, k_2 \in B_3^i, \lfloor\frac{t}{2}\rfloor, \dots, t \in \mathscr{A}^i$$

and always trusts the symbols that are not one of the reserved vectors from V_2.

Therefore

$$C_1(\mathfrak{A}_t, \boldsymbol{A}_{\mathfrak{A}_t}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}|^{\lceil\frac{t}{2}\rceil} - b).$$

Adversarial model 2: Attack t in top, 0 in bottom or 0 in top, t in bottom, but cannot change the edges attacked. Let B be the set of reserved vectors with $|B| = b$ to denote the location of the adversary. Let C be the code

$$\{(a|b|\dots|t|a|a, \dots|t|t) \mid (a|b|c|\dots|t|a|a|\dots|t|t) \notin B^i, d_{\mathrm{H}}(x^i, y^i) \geq 2t \text{ for } x, y \in C, x \neq y.\}$$

The pairs of vectors move together, meaning if a moves positions in the top half of

the network, then aa moves to the same 2 positions in the bottom half of the network. An example is the codewords $(a|b|a|a|b|b)$ and $(b|a|b|b|a|a)$ are the only two choices for $t = 2$, since if we have two codewords $(a|b|a|a|b|b)$ and $(a|b|b|b|a|a)$ then the code would not be unambiguous.

Let $\mathscr{F} = (\mathscr{F}_1, \mathscr{F}_2)$ be the network code such that $\mathscr{F}_1(x_1, \ldots, x_t) = (x_1, \ldots, x_t)$ and $\mathscr{F}_2$ as follows

$$\mathscr{F}_2 = \begin{cases} x_i & \text{if} \quad x_i = x_j \\ k, k \in B & \text{otherwise} \end{cases}$$

where $\mathscr{F}_2$ compares consecutive pairs of edges. V_2 is used to denote where the adversary is acting.

We have the following two cases:

Case 1: Attack t edges in top half of the network, 0 in bottom half, meaning attack all t edges in the top half. We have that

$\Omega^i[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(V_1), \mathscr{U}_S, t](a|\ldots|t) = k, k \in B_t^i$

$\Omega^i[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(V_2), \mathscr{U}_S, t](a|a|\ldots|c|c) = (a|b|\ldots|t), a, b, \ldots, t \in \mathscr{A}^i$ and the terminal trusts V_2.

Case 2: Attack 0 edges in the top half of the network, t edges in the bottom half. We have that

$$\Omega^i[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(V_1), \mathscr{U}_S, t](a|\ldots|t) = (a|\ldots|t), a, b \ldots, t \in \mathscr{A}^i$$

and

$$\Omega^i[\mathfrak{A}_t, \mathscr{A}, \mathscr{F}, \text{out}(S) \to \text{in}(V_2), \mathscr{U}_S, t](a|a| \dots |c|c) = k, k \in B_t^i$$

and the terminal trusts V_1.

Then $C_1(\mathfrak{A}_t, \boldsymbol{A}_{\mathfrak{A}_t}) \geq \log_{|\mathscr{A}|}(|\mathscr{A}|^3 - b)$ and $C_i(\mathfrak{A}_t, \boldsymbol{A}_{\mathfrak{A}_t}) \geq \frac{\log_{|\mathscr{A}|}(|\mathscr{A}|^{3i} - b)}{i}$ and there is a gain in capacity over multiple uses.

4.4 Future Work

We conclude the thesis with some conjectures on multishot capacity of families of networks.

Conjecture 4.30. *If the Network Singleton Bound is not met, then there is gain in capacity over multiple uses of the network in Scenario A.1.*

Remark 4.31. We see that this is the case for the Diamond Network $\mathscr{D}$ and Family $\mathfrak{E}_t$, when the adversary is restricted to attacking t edges but not changing the edges attacked.

Conjecture 4.32. *If the Network Singleton Bound is met, then there is no gain in capacity over multiple uses of the network in neither Scenario A.1 or Scenario A.2.*

Remark 4.33. We notice this pattern with the Mirrored Diamond Network $\mathscr{S}$ and Families $\mathfrak{C}_t$ and $\mathfrak{D}_t$.

Chapter 5

Conclusions

In this thesis we have investigated the multishot capacity of networks with restricted adversaries focusing on the Diamond Network and the Mirrored Diamond Network and known families of networks as elementary building blocks of a general theory. We focused on two adversarial models. In Scenario A.1, the adversary can attack up to t edges of a network from a subset of the network edges but cannot change the edges attacked and in Scenario A.2, the adversary can attack up to t edges from a subset of network edges but can change the edges attacked each transmission round. We extended the double cut-set bound in [5] to the multishot setting, that can be used to describe the multishot capacity of 3−level networks that can be reduced to 2−level networks with known one-shot and multishot capacities.

Through our results, we showed that for the Diamond Network $\mathscr{D}$, the Butterfly Network $\mathscr{B}$ and Family $\mathfrak{E}_t$, there is a gain in capacity over multiple uses of the network in Scenario A.1. This happens in the setting that the adversary is more restricted where it cannot change the edges attacked each transmission round. The ability to use information from the first transmission round and knowing exactly where the adversary is attacking was possible. In Scenario A.2, where the adversary is more free to change the edges attacked, we have that $C_1(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}}) = C_i(\mathscr{N}, \boldsymbol{A}_{\mathscr{N}})$ for networks $\mathscr{D}, \mathfrak{E}_t$ and $\mathscr{B}$. Strategies provided for Scenario A.1 were not able to be used due to their reliance on the adversary not being able to change the edges attacked each transmission round.

For networks $\mathfrak{C}_t, \mathfrak{D}_t$ and $\mathscr{S}$, we showed that in either scenario, there is no gain in using these networks multiple times for communication, regardless of the adversarial model. Strategies for these networks were adapted from the strategies provided in the one-shot regime.

We would like to continue investigating the multishot capacities of Family $\mathfrak{A}_t$ and $\mathfrak{B}_s$ without knowing the one-shot capacity to determine if there is a gain in using these networks multiple times for communication. This relies on new combinatorial techniques, as the one-shot capacities of these networks has yet to be established. Another interesting direction is the scenario where the subset of edges the adversary can attack on also changes, has not yet been investigated in the multishot setting. We are also interested in the multishot capacity of networks in the general n-level network case. A general theory for $n-$level networks in the multishot setting has not been established yet.

Bibliography

[1] F. Kschichang and A. Ravagnani, "Adversarial network coding," in IEEE Transactions on Information Theory, vol. 65, no. 1, pp. 198–219, 2018.

[2] A. Beemer and A. Ravagnani, "The curious case of the diamond network," unpublished, arXiv:2107.02144, 2021.

[3] A. Beemer, A. Kılıç, and A. Ravagnani, "Network decoding against restricted adversaries," IFAC-PapersOnLine, vol. 55, pp. 236–241, 2022.

[4] N. Cai and R. Yeung, "Network error correction, part I: Basic concepts and upper bounds", Communications in Information and Systems, vol. 6, pp. 19–36, 2006.

[5] A. Beemer, A. Kılıç, and A. Ravagnani, "Network decoding,", IEEE Transactions On Information Theory, 2023.

[6] U. Martínez-Peñas and F. Kschischang, "Reliable and secure multishot network coding using linearized Reed-Solomon codes," IEEE Transactions on Information Theory vol. 65.8, pp. 4785–4803, 2019.

[7] S. Li, R. Yeung, and N. Cai, "Linear network coding," IEEE Transactions on Information Theory, vol. 49, pp. 371–381, 2003.

[8] R. Nóbrega and B. Uchôa-Filho, "Multishot codes for network coding: Bounds and a multilevel construction," in IEEE International Symposium on Information Theory, 2009.

[9] R. Ahlswede, N. Cai, S. Li, and R. Yeung, "Network information flow," in IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1204–-1216, 2000.

[10] R. Köetter and F. Kschischang, "Coding for errors and erasures in random network coding," in IEEE Transactions on Information theory vol. 54.8, pp. 3579–3591, 2008.

[11] D. Silva, F. R. Kschischang, and R. Köetter, "A rank-metric approach to error control in random network coding," in IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 3951–3967, 2008.

[12] L. Nutman and M. Langberg, "Adversarial models and resilient schemes for network coding," in IEEE International Symposium on Information Theory, pp. 171–175, 2008.

[13] R. Kötter and M. Médard. "An algebraic approach to network coding," in IEEE/ACM Transactions on Networking, vol. 11, pp. 782–795, 2003.

[14] D. Wang, D. Silva, and F. Kschischang, "Constricting the adversary: A broadcast transformation for network coding," 45th Annual Allerton Conference on Communications, Control and Computing, 2007.

[15] S. Mohajer, M. Jafari, S. N. Diggavi, and C. Fragouli, "On the capacity of multisource non-coherent network coding," in IEEE Information Theory Workshop on Networking and Information Theory, pp. 130–134, 2009.

[16] R. Yeung, S. Li, N. Cai, and Z. Zhang, "Network coding theory", 2006, doi: 10.1561/0100000007.

[17] G. Cotardo, G. Matthews, A. Ravagnani and J. Shapiro, "Multishot adversarial network decoding", 2023 59th Annual Allerton Conference on Communication, Control, and Computing, 2023, pp 1–8, doi:10.1109/Allerton58177.2023.10313407.

[18] R. Singleton, “Maximum distance q-nary codes”, in IEEE Transaction on Information Theory, 10 (2): 116–118, 1964, doi:10.1109/TIT.1964.1053661