TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Network Decoding Against Restricted Adversaries

Citation for published version (APA):
Beemer, A., Kiliç, A. B., & Ravagnani, A. (2022). Network Decoding Against Restricted Adversaries. *IFAC-PapersOnLine*, *55*(30), 236-241. https://doi.org/10.1016/j.ifacol.2022.11.058

DOI:
10.1016/j.ifacol.2022.11.058

Document status and date:
Published: 01/01/2022

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Download date: 17. Nov. 2023

Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 55-30 (2022) 236–241

Network Decoding Against Restricted Adversaries

Allison Beemer * **Altan B. Kılıç** ** **Alberto Ravagnani** ***

* *University of Wisconsin-Eau Claire, WI 54701, USA (e-mail: beemera@uwec.edu)*

** *Eindhoven University of Technology, 5612 AZ Eindhoven, The Netherlands (e-mail: a.b.kilic@tue.nl)*

*** *Eindhoven University of Technology, 5612 AZ Eindhoven, The Netherlands (e-mail: a.ravagnani@tue.nl)*

Abstract: We initiate the study of the one-shot capacity of communication (coded) networks with an adversary having access only to a proper subset of the network edges. We introduce the Diamond Network as a minimal example to show that known cut-set bounds are not sharp in general, and that their non-sharpness comes precisely from restricting the action of the adversary to a region of the network. We give a capacity-achieving scheme for the Diamond Network that implements an adversary detection strategy. We also show that linear network coding does not suffice in general to achieve capacity, proving a strong separation result between the one-shot capacity and its linear version. We then give a sufficient condition for tightness of the Singleton Cut-Set Bound in a family of two-level networks. Finally, we discuss how the presence of nodes that do not allow local encoding and decoding does or does not affect the one-shot capacity.

Copyright © 2022 The Authors. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)

Keywords: Network coding, adversarial network, capacity, cut-set bound.

1. INTRODUCTION

As the prevalence of interconnected devices grows, vulnerable communication networks must be able to counter the actions of malicious actors; a unified understanding of the fundamental communication limits of these networks is therefore paramount. The correction of errors introduced by adversaries in networks has been studied in a number of previous works. Cai and Yeung give generalizations of some classical coding bounds to the network setting in Yeung and Cai (2006); Cai and Yeung (2006). Other bounds and related code constructions for adversarial networks are presented in, e.g., Yang and Yeung (2007); Jaggi et al. (2007); Matsumoto (2007); Yang et al. (2007, 2008); Ravagnani and Kschischang (2018). The work most closely related to this paper is Ravagnani and Kschischang (2018), where a unified combinatorial framework for adversarial networks and a method for porting point-to-point coding-theoretic results to the network setting are established. In contrast to works that address random errors in networks, or a combination of random and adversarial errors, Ravagnani and Kschischang (2018) focuses purely on adversarial, or *worst-case*, errors. The results presented here assume the same model in a single-use regime.

Problem formulation. In contrast to most previous work, in this paper we concentrate on networks with an adversary who can possibly corrupt only a *proper subset* of the network edges. This paper is the first stepping stone of a long-term project aimed at understanding how the topology of the vulnerable region of a network determines (or at least affects) its capacity. We focus on networks whose inputs are drawn from a finite alphabet and whose intermediate nodes may process information before forwarding. We assume that an omniscient adversary can corrupt up to some fixed number of alphabet symbols sent along a subset of network edges. The one-shot capacity of such an adversarial network measures the number of symbols that can be sent with zero error during a single transmission round. A universal approach to forming cut-set bounds, which are derived by reducing the capacity problem to a minimization across cut-sets of the underlying directed graph of the network, is presented in Ravagnani and Kschischang (2018). Any coding-theoretic bound may be ported to the networking setting, including the famous Singleton Bound.

Our contribution. In this paper, we exhibit a minimal example showing that known cut-set bounds for the one-shot capacity of a network subject to adversarial noise are not sharp in general. More precisely, we construct a network for which the Singleton Bound gives the best established upper bound on one-shot capacity, and show that it is not tight (regardless of the size of the network alphabet). The non-tightness of the bound comes precisely from limiting the adversary to operation on a certain region of the network. Our example, which we call the *Diamond Network*, requires that a single symbol be sacrificed to the task of locating the adversary within the network. Interestingly, this requirement results in a non-integer-valued one-shot capacity (which we are able to compute). We note that the requirement that the receiver locate the adversary

⋆ A. B. K. is supported by the Dutch Research Council through grant VI.Vidi.203.045. A. R. is supported by the Dutch Research Council through grants VI.Vidi.203.045, OCENW.KLEIN.539, and by the Royal Academy of Arts and Sciences of the Netherlands.

2405-8963 Copyright © 2022 The Authors. This is an open access article under the CC BY-NC-ND license.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2022.11.058

is related to the problem of authentication in networks (see, e.g. Kosut and Kliewer (2016); Sangwan et al. (2019); Beemer et al. (2020)). In our capacity-achieving scheme for the Diamond Network, one intermediate vertex must be able to either sound an alarm (if the adversary is detected), or decode correctly (when the adversary is absent). On the other hand, in our presented scheme for a modification of the Diamond Network, called the *Mirrored Diamond Network*, the way in which intermediate vertices sound the alarm must simultaneously serve as the way in which a particular alphabet symbol is transmitted. This interplay between authentication and correction is reminiscent of the work in Beemer et al. (2020), and the connection warrants further investigation.

Outline. This paper is organized as follows. In Section 2 we introduce necessary notation and background. Sections 3 and 4 together establish the exact one-shot capacity of the Diamond Network, proving that the Singleton Cut-Set Bound is not tight. In Section 5, we establish the (bound-achieving) one-shot capacity of the Mirrored Diamond Network. In Section 6 we compute the linear one-shot capacity of the Mirrored Diamond Network, showing that there is strong separation between the linear and the non-linear one-shot capacities. Section 7 expands our focus to the broader class of two-level networks, and gives a sufficient condition for a network in this class to meet the best cut-set bound. In Section 8 we include some examples showing that the presence of *damming* nodes (see Section 7 for the definition) may or may not compromise the achievability of the Singleton Cut-Set Bound. We conclude with future directions in Section 9.

2. PRELIMINARIES

We introduce the terminology and notation for the remainder of the paper. We start by formally defining communication networks as in Ravagnani and Kschischang (2018).

Definition 1. A (**single-source communication) network** is a 4-tuple $\mathcal{N} = (\mathcal{V}, \mathcal{E}, S, \mathbf{T})$, where:

(A) $(\mathcal{V}, \mathcal{E})$ is a finite, directed and acyclic multigraph;
(B) $S \in \mathcal{V}$ is the **source**;
(C) $\mathbf{T} \subseteq \mathcal{V}$ is the set of **terminals**.
(D) $|\mathbf{T}| \geq 1$ and $S \notin \mathbf{T}$;
(E) there exists a directed path from S to any $T \in \mathbf{T}$;
(F) for every $V \in \mathcal{V} \backslash (\{S\} \cup \mathbf{T})$ there exists a directed path from S to V and from V to some terminal $T \in \mathbf{T}$.

The elements of $\mathcal{V}$ are called **vertices** or **nodes**, and those of $\mathcal{E}$ are called **edges**. The elements of $\mathcal{V} \setminus (\{S\} \cup \mathbf{T})$ are the **intermediate vertices/nodes**. The set of incoming and outgoing edges of a vertex V are denoted by $\text{in}(V)$ and $\text{out}(V)$, respectively. Their cardinalities are the **indegree** and **outdegree** of V, which are denoted by $\deg^-(V)$ and $\deg^+(V)$, respectively.

Our communication model is as follows: all edges of a network $\mathcal{N}$ can carry precisely one element from a set $\mathcal{A}$ of cardinality at least 2, which we call the **alphabet**. The vertices of the network collect alphabet symbols over the incoming edges, process them according to functions, and send the outputs over the outgoing edges. Vertices are memoryless and transmissions are delay-free. We model errors as being introduced by an adversary $\mathbf{A}$, who can corrupt the value of up to t edges from a fixed set $\mathcal{U} \subseteq \mathcal{E}$. An alphabet symbol sent along one of the edges in $\mathcal{U}$ can be changed to any other alphabet symbol at the discretion of the adversary. We focus on correcting *any* error pattern that can be introduced by the adversary. We call the pair $(\mathcal{N}, \mathbf{A})$ an **adversarial network**.

It is well-known that an acyclic directed graph $(\mathcal{V}, \mathcal{E})$ defines a partial order on the set of its edges, $\mathcal{E}$. More precisely, $e_1 \in \mathcal{E}$ **precedes** $e_2 \in \mathcal{E}$ (in symbols, $e_1 \preccurlyeq e_2$) if there exists a directed path in $(\mathcal{V}, \mathcal{E})$ whose first edge is e_1 and whose last edge is e_2. We may extend this partial order to a total order on $\mathcal{E}$, which we fix once and for all and denote by $\leq$. Important to note is that the results in this paper do not depend on the particular choice of $\leq$.

We now introduce the concept of a *network code*, which describes how the messages are processed by the intermediate nodes of a network.

Definition 2. Let $\mathcal{N} = (\mathcal{V}, \mathcal{E}, S, \mathbf{T})$ be a network. A **network code** $\mathcal{F}$ for $\mathcal{N}$ is a family of functions

$$\{\mathcal{F}_V \mid V \in \mathcal{V} \setminus (\{S\} \cup \mathbf{T})\},$$

where $\mathcal{F}_V : \mathcal{A}^{\deg^-(V)} \to \mathcal{A}^{\deg^+(V)}$ for all V.

A network code $\mathcal{F}$ describes how the vertices of a network $\mathcal{N}$ process the inputs received on the incoming edges. There is a unique interpretation for these operations thanks to the choice of the total order $\leq$.

Definition 3. Let $\mathcal{N} = (\mathcal{V}, \mathcal{E}, S, \mathbf{T})$ be a network and let $\mathcal{U}, \mathcal{U}' \subseteq \mathcal{E}$ be non-empty subsets. We say that $\mathcal{U}$ **precedes** $\mathcal{U}'$ if every path from S to an edge of $\mathcal{U}'$ contains an edge from $\mathcal{U}$.

Our next step is to define outer codes for a network and give conditions for decodability. We do this by introducing the notion of an adversarial channel.

Definition 4. Let $(\mathcal{N}, \mathbf{A})$ denote an adversarial network with $\mathcal{N} = (\mathcal{V}, \mathcal{E}, S, \mathbf{T})$ and let $\mathcal{U}, \mathcal{U}' \subseteq \mathcal{E}$ be non-empty such that $\mathcal{U}$ precedes $\mathcal{U}'$. Let $\mathcal{F}$ be a network code for $\mathcal{N}$. For $\mathbf{x} \in \mathcal{A}^{|\mathcal{U}|}$, we denote by

$$\Omega[\mathcal{N}, \mathbf{A}, \mathcal{F}, \mathcal{U} \to \mathcal{U}'](\mathbf{x}) \subseteq \mathcal{A}^{|\mathcal{U}'|} \tag{1}$$

the set of vectors over the alphabet that can be exiting the edges of $\mathcal{U}'$ when:

- the coordinates of $\mathbf{x}$ are the alphabet values entering the edges of $\mathcal{U}$,
- vertices process information according to $\mathcal{F}$ and the total order $\leq$.

Note that (1) is well-defined because $\mathcal{U}$ precedes $\mathcal{U}'$. Furthermore, $\mathcal{U} \cap \mathcal{U}'$ need not be empty. We refer to the discussion following (Ravagnani and Kschischang, 2018, Definition 41, Example 42).

Example 5. Let $(\mathcal{N}, \mathbf{A})$ be the network in Figure 1, where the edges are ordered according to their indices. We consider an adversary capable of corrupting up to one of the dashed edges. Let $\mathcal{F}_{V_1}$ be the identity function and $\mathcal{F}_{V_2}$ be the projection onto the second coordinate of the input pair. Then, for $\mathbf{x} = (x_1, x_2, x_3) \in \mathcal{A}^3$ we have that

$$\Omega[\mathcal{N}, \mathbf{A}, \mathcal{F}, \{e_1, e_2, e_3\} \to \{e_4, e_5\}](\mathbf{x}) \subseteq \mathcal{A}^2$$

is the set of vectors $\mathbf{y} = (y_1, y_2) \in \mathcal{A}^2$ for which $d_{\text{H}}((y_1, y_2), (x_1, x_3)) \leq 1$, where d_{H} denotes the Hamming distance.

We now define error-correcting codes in the context of adversarial networks.

Definition 6. An (**outer**) **code** for a network $\mathcal{N} = (\mathcal{V}, \mathcal{E}, S, \mathbf{T})$ is a subset $C \subseteq \mathcal{A}^{\deg^+(S)}$ with $|C| \geq 1$. If $\mathcal{F}$ is a network code for $\mathcal{N}$ and $\mathbf{A}$ is an adversary, then we say that C is **unambiguous** (or **good**) for $(\mathcal{N}, \mathbf{A}, \mathcal{F})$ if for all $\mathbf{x}, \mathbf{x}' \in C$ with $\mathbf{x} \neq \mathbf{x}'$ and for all $T \in \mathbf{T}$ we have

$$\Omega[\mathcal{N}, \mathbf{A}, \mathcal{F}, \mathrm{out}(S) \to \mathrm{in}(T)](\mathbf{x}) \cap \Omega[\mathcal{N}, \mathbf{A}, \mathcal{F}, \mathrm{out}(S) \to \mathrm{in}(T)](\mathbf{x}') = \emptyset.$$

The last condition in the above definition guarantees that every element of C can be uniquely recovered by every terminal, despite the action of the adversary. Finally, we define the one-shot capacity of an adversarial network.

Definition 7. The (**one-shot**) **capacity** of an adversarial network $(\mathcal{N}, \mathbf{A})$ is the maximum $\alpha \in \mathbb{R}$ for which there exists a network code $\mathcal{F}$ and an unambiguous code C for $(\mathcal{N}, \mathbf{A}, \mathcal{F})$ with $\alpha = \log_{|\mathcal{A}|} |C|$. We denote this maximum value by $\mathrm{C}_1(\mathcal{N}, \mathbf{A})$.

In Ravagnani and Kschischang (2018), a general method was developed to "lift" bounds for Hamming-metric channels to the networking context. The method allows any classical coding bound to be lifted to the network setting. The next result states the lifted version of the well-known Singleton Bound. Recall that an edge-cut between source S and terminal T is a set of edges whose removal would separate S from T.

Theorem 8. (The Singleton Cut-Set Bound). Let $\mathcal{N}$ be a network with edge set $\mathcal{E}$. Assume an adversary $\mathbf{A}$ can corrupt up to $t \geq 0$ edges from a subset $\mathcal{U} \subseteq \mathcal{E}$. Then

$$\mathrm{C}_1(\mathcal{N}, \mathbf{A}) \leq \min_{T \in \mathbf{T}} \min_{\mathcal{E}'} \left(|\mathcal{E}' \setminus \mathcal{U}| + \max\{0, |\mathcal{E}' \cap \mathcal{U}| - 2t\} \right),$$

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

3. THE DIAMOND NETWORK: ACHIEVABILITY

We present a minimal example of a network for which the *best* known bound, namely the Singleton Cut-Set Bound, is not sharp. The example will serve to illustrate the necessity of performing *partial* decoding at the intermediate nodes in order to achieve capacity.

Example 9. (The Diamond Network). Consider the network $\mathcal{D}$ of Figure 1 and an adversary $\mathbf{A}_\mathcal{D}$ able to corrupt at most one of the dashed edges, and we call the pair $(\mathcal{D}, \mathbf{A}_\mathcal{D})$ the **Diamond Network**.

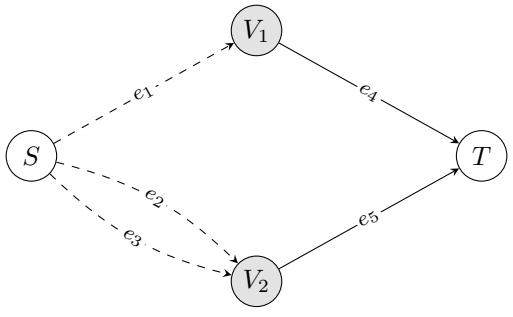

Fig. 1. The Diamond Network

Corollary 10. For the Diamond Network $(\mathcal{D}, \mathbf{A}_\mathcal{D})$,

$$\mathrm{C}_1(\mathcal{D}, \mathbf{A}_\mathcal{D}) \leq 1.$$

We will prove in this section and the next that the Diamond Network has capacity

$$\mathrm{C}_1(\mathcal{D}, \mathbf{A}_\mathcal{D}) = \log_{|\mathcal{A}|}(|\mathcal{A}| - 1). \tag{2}$$

In particular, this shows that the best known cut-set bound is not sharp. In order to achieve the capacity, one alphabet symbol needs to be reserved to implement an adversary detection strategy.

Proposition 11. For the Diamond Network $(\mathcal{D}, \mathbf{A}_\mathcal{D})$ we have

$$\mathrm{C}_1(\mathcal{D}, \mathbf{A}_\mathcal{D}) \geq \log_{|\mathcal{A}|}(|\mathcal{A}| - 1).$$

Proof. We isolate a symbol $* \in \mathcal{A}$ and define $\mathcal{A}' = \mathcal{A} \backslash \{*\}$. Consider the scheme where the source S can send any symbol of $\mathcal{A}'$ via a three-times repetition code over its outgoing edges. Vertex V_1 simply forwards the received input, while vertex V_2 proceeds as follows: If the two received inputs coincide and are equal to $a \in \mathcal{A}'$, then it forwards a. Otherwise, it transmits $*$. It is not difficult to check that any symbol from $\mathcal{A}'$ can be uniquely decoded, showing that the proposed scheme is unambiguous. □

The communication strategy on which the previous proof is based reserves an alphabet symbol $* \in \mathcal{A}$ to pass information about the location of the adversary (more precisely, the symbol $*$ reveals whether or not the adversary is acting on the lower "stream"). The source is not allowed to emit the reserved symbol $*$, rendering $\log_{|\mathcal{A}|}(|\mathcal{A}|-1)$ the maximum rate achievable by this scheme. It is natural to then ask whether the reserved symbol $*$ can simultaneously be a part of the source's codebook, achieving a rate of $1 = \log_{|\mathcal{A}|} |\mathcal{A}|$ message per channel use. In the next section, we will formally answer this question in the negative; see Proposition 12. In Section 5, we consider a modification of the Diamond Network and present a scheme where one symbol is reserved for adversary detection, but can nonetheless also be used as a message symbol.

4. THE DIAMOND NETWORK: THE CONVERSE

In this section, we establish an inequality for the cardinality of any unambiguous code C for the Diamond Network.

Proposition 12. Let $\mathcal{F}$ be a network code for $(\mathcal{D}, \mathbf{A}_\mathcal{D})$ and let $C \subseteq \mathcal{A}^3$ be an outer code. If C is unambiguous for $(\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F})$, then $|C|^2 + |C| - 1 - |\mathcal{A}|^2 \leq 0$. In particular, we have $|C| \leq |\mathcal{A}| - 1$.

Proof. The argument is organized into various claims. We denote by $\pi : \mathcal{A}^3 \to \mathcal{A}$ the projection onto the first coordinate.

Claim A. We have $|\pi(C)| = |C|$.

This follows from the fact that $C \subseteq \mathcal{A}^3$ must have minimum Hamming distance 3 in order to be unambiguous, as one can easily check. □

Claim B. The restriction of $\mathcal{F}_{V_1}$ to $\pi(C)$ is injective.

Suppose by contradiction that there exist $\mathbf{x}, \mathbf{y} \in C$ with $\pi(\mathbf{x}) \neq \pi(\mathbf{y})$ and $\mathcal{F}_{V_1}(\pi(\mathbf{x})) = \mathcal{F}_{V_1}(\pi(\mathbf{y}))$. Then it is easy to see that the sets $\Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \mathrm{out}(S) \to \mathrm{in}(T)](\mathbf{x})$ and $\Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \mathrm{out}(S) \to \mathrm{in}(T)](\mathbf{y})$ intersect non-trivially. Indeed, if $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$, then the final output

$$(\mathcal{F}_{V_1}(x_1), \mathcal{F}_{V_2}(x_2, y_3)) \in \mathcal{A}^2$$

belongs to both sets. □

To simplify notation, let $\Omega := \Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \{e_1, e_2, e_3\} \to \{e_5\}]$, which is well-defined because $\{e_1, e_2, e_3\}$ precedes e_5; see Definition 3.

Claim C. There exists at most one codeword $\mathbf{x} \in C$ for which the cardinality of $\Omega(\mathbf{x})$ is 1.

Towards a contradiction, suppose that there are $\mathbf{x}, \mathbf{y} \in C$ with $\mathbf{x} \neq \mathbf{y}$ and $|\Omega(\mathbf{x})| = |\Omega(\mathbf{y})| = 1$. We write $\Omega' := \Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \{e_1, e_2, e_3\} \to \{e_2, e_3\}]$ and observe that $|\mathcal{F}_{V_2}(\Omega'(\mathbf{x}))| = |\mathcal{F}_{V_2}(\Omega'(\mathbf{y}))| = 1$. Let $\mathbf{x} = (x_1, x_2, x_3), \mathbf{y} = (y_1, y_2, y_3)$. Since $(x_2, x_3), (x_2, y_3) \in \Omega'(\mathbf{x})$ and $(y_2, y_3), (x_2, y_3) \in \Omega'(\mathbf{y})$, we have

$$\mathcal{F}_{V_2}(x_2, x_3) = \mathcal{F}_{V_2}(x_2, y_3) = \mathcal{F}_{V_2}(y_2, y_3).$$

By observing that the adversary may corrupt the symbol sent on e_1, this implies that the sets $\Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \mathrm{out}(S) \to \mathrm{in}(T)](\mathbf{x})$ and $\Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \mathrm{out}(S) \to \mathrm{in}(T)](\mathbf{y})$ intersect non-trivially, a contradiction. □

To simplify further, denote the transfer from S to T by

$$\Omega'' := \Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \{e_1, e_2, e_3\} \to \{e_4, e_5\}].$$

Since C is unambiguous, we have

$$\sum_{\mathbf{x} \in C} |\Omega''(\mathbf{x})| \leq |\mathcal{A}|^2. \tag{3}$$

For all $\mathbf{x} \in C$, write $\Omega''(\mathbf{x}) = \Omega''_1(\mathbf{x}) \cup \Omega''_2(\mathbf{x})$, where

$$\Omega''_1(\mathbf{x}) = \{\mathbf{z} \in \Omega''(\mathbf{x}) \mid z_1 = \mathcal{F}_{V_1}(x_1)\},$$
$$\Omega''_2(\mathbf{x}) = \{\mathbf{z} \in \Omega''(\mathbf{x}) \mid z_2 = \mathcal{F}_{V_2}(x_2, x_3)\}.$$

By definition, we have $|\Omega''(\mathbf{x})| = |\Omega''_1(\mathbf{x})| + |\Omega''_2(\mathbf{x})| - 1$. Summing over all $\mathbf{x} \in C$ and using Claims A, B and C we find

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

Combining this with (3), we find $|C|^2 + |C| - 1 \leq |\mathcal{A}|^2$, which is the desired inequality. □

We can now compute the capacity of the Diamond Network by combining Propositions 11 and 12.

Theorem 13. For the Diamond Network $(\mathcal{D}, \mathbf{A}_\mathcal{D})$,

$$\mathrm{C}_1(\mathcal{D}, \mathbf{A}_\mathcal{D}) = \log_{|\mathcal{A}|}(|\mathcal{A}| - 1).$$

The Diamond Network is admittedly a small example. However, we believe that it will provide valuable insight into the general behavior of the one-shot capacity of larger networks.

5. THE MIRRORED DIAMOND NETWORK

It is interesting to observe that by adding a single vulnerable edge from S to V_1 in the Diamond Network (as in Figure 2), the capacity will be exactly the one predicted by the Singleton Cut-Set Bound of Theorem 8. We call this new network the **Mirrored Diamond Network**. The adversary can corrupt at most one edge from the four exiting S. The notation for the network-adversary pair is $(\mathcal{S}, \mathbf{A}_\mathcal{S})$.

Proposition 14. We have $\mathrm{C}_1(\mathcal{S}, \mathbf{A}_\mathcal{S}) = 1$.

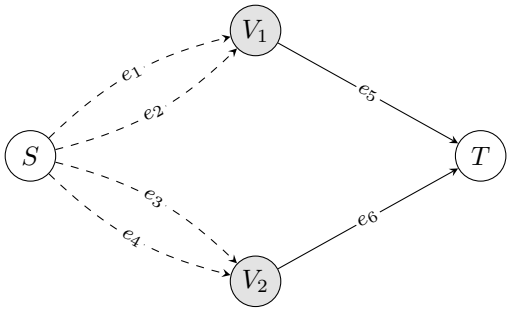

Fig. 2. The Mirrored Diamond Network.

Proof. By Theorem 8, $\mathrm{C}_1(\mathcal{S}, \mathbf{A}_\mathcal{S}) \leq 1$, so we only need to prove achievability. Select $* \in \mathcal{A}$, and consider the scheme where the source S sends any symbol of $\mathcal{A}$ via a four-times repetition code. Vertices V_1 and V_2 both proceed as follows: If the two received inputs coincide and are equal to $a \in \mathcal{A}$, the vertex forwards a; otherwise it transmits $*$. At T, if the received symbols match and are equal to $a \in \mathcal{A}$, decode to a. Otherwise, decode to the symbol that is not equal to $*$. It is clear that any symbol from $\mathcal{A}$ can be uniquely decoded, including $*$. □

As in the proof of Proposition 11, the above scheme uses an alphabet symbol to pass information about the location of the adversary. In strong contrast with the Diamond Network however, in the Mirrored Diamond Network this strategy comes at no cost, as the "reserved" alphabet symbol can be used by the source like any other symbol.

6. LINEAR CAPACITY

It is well-known that in the context of adversarial network coding capacity can be achieved by combining a rank-metric (outer) code with a *linear* network code; see Silva et al. (2008); Dikaliotis et al. (2011). This result applies to an adversary capable of corrupting *any* t network edges. In this section we argue that the same result is far from being true when the adversary is restricted to operate on a proper subset of the network edges. More precisely, we establish a strong separation result between the capacity and the "linear" capacity.

Definition 15. Following the notation of Definition 2, we say that $\mathcal{F}$ is a **linear** network code if $\mathcal{A}$ is a finite field and each function $\mathcal{F}_V$ is linear.

We next define the linear version of the one-shot capacity.

Definition 16. The **linear one-shot capacity** of an adversarial network $(\mathcal{N}, \mathbf{A})$ is the maximum $\alpha \in \mathbb{R}$ for which there exists a linear network code $\mathcal{F}$ and an unambiguous code C for $(\mathcal{N}, \mathbf{A}, \mathcal{F})$ with $\alpha = \log_{|\mathcal{A}|} |C|$. We denote this maximum value by $\mathrm{C}_1^{\mathrm{lin}}(\mathcal{N}, \mathbf{A})$.

Note that, in the definition of linear one-shot capacity, we do not require that C is a linear code.

In Proposition 14 we proved that the one-shot capacity of the Mirrored Diamond Network is equal to 1. The next result shows that its linear capacity is 0, exhibiting an example of *strong separation* between the one-shot capacity and its linear version, in the sense that the capacities are separated asymptotically in alphabet size.

Theorem 17. We have $\mathrm{C}_1^{\mathrm{lin}}(\mathcal{S}, \mathbf{A}_\mathcal{S}) = 0$.

Proof. Fix any linear network code $\mathcal{F}$ for $(\mathcal{S}, \mathbf{A}_\mathcal{S})$ and let C be a good code for $(\mathcal{S}, \mathbf{A}_\mathcal{S}, \mathcal{F})$. Suppose that $|C| \geq 2$ and let $x, a \in C$ with $x \neq a$. Write

$$x = (x_1, x_2, x_3, x_4), \quad a = (a_1, a_2, a_3, a_4)$$

and

$$\mathcal{F}_{V_1}(u, v) = \lambda_1 u + \lambda_2 v, \quad \mathcal{F}_{V_2}(u, v) = \lambda_3 u + \lambda_4 v,$$

where $\lambda_r \in \mathcal{A}$ for $1 \leq r \leq 4$ and $u, v \in \mathcal{A}$. We let $\Omega := \Omega[\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F}, \{e_1, e_2, e_3, e_4\} \to \{e_5, e_6\}]$ to simplify the notation throughout the proof.

We start by observing that λ_1, λ_2 can not be both equal to 0. Similarly, λ_3, λ_4 can not be both equal to 0. Indeed, is easy to see that the adversary can create a collision otherwise. Therefore, without loss of generality, we shall assume $\lambda_1 \neq 0$ and $\lambda_3 \neq 0$. Define:

- $y = (x_1, x_2, a_3 + \lambda_3^{-1}\lambda_4(a_4 - x_4), x_4)$,
- $b = (x_1 + \lambda_1^{-1}\lambda_2(x_2 - a_2), a_2, a_3, a_4)$.

Observe that $d_\mathrm{H}(x, y) = d_\mathrm{H}(a, b) = 1$, which implies

$$\left(\sum_{r=1}^{2} \lambda_r y_r, \ \sum_{r=3}^{4} \lambda_r y_r \right) \in \Omega(x)$$

and

$$\left(\sum_{r=1}^{2} \lambda_r b_r, \ \sum_{r=3}^{4} \lambda_r b_r \right) \in \Omega(a).$$

However, by definition we have

$$\left(\sum_{r=1}^{2} \lambda_r y_r, \ \sum_{r=3}^{4} \lambda_r y_r \right) = \left(\sum_{r=1}^{2} \lambda_r b_r, \ \sum_{r=3}^{4} \lambda_r b_r \right),$$

which shows that $\Omega(x) \cap \Omega(a) \neq \emptyset$. This contradicts the assumption that C is a good code for $(\mathcal{S}, \mathbf{A}_\mathcal{S}, \mathcal{F})$. □

The previous result implies that the linear capacity of the Diamond Network is equal to 0, as well.

Corollary 18. We have $\mathrm{C}_1^{\mathrm{lin}}(\mathcal{D}, \mathbf{A}_\mathcal{D}) = 0$.

Proof. Every pair $(\mathcal{F}, C)$, where $\mathcal{F}$ is a linear network code for the Diamond Network $(\mathcal{D}, \mathbf{A}_\mathcal{D})$ and C is good for $(\mathcal{D}, \mathbf{A}_\mathcal{D}, \mathcal{F})$, naturally gives a pair $(\mathcal{F}', C')$ for the Mirrored Diamond Network, where $\mathcal{F}'$ is linear, C' is good for $(\mathcal{S}, \mathbf{A}_\mathcal{S}, \mathcal{F}')$ and $|C| = |C'|$. We conclude by applying Theorem 17. □

7. TWO-LEVEL NETWORKS

In this section we initiate a systematic study of communication with restricted adversaries. Since a global treatment is out of reach at the moment, we start by concentrating on a small but sufficiently interesting family of highly structured networks. These are defined as follows.

Definition 19. A **two-level network** is a network $\mathcal{N} = (\mathcal{V}, \mathcal{E}, S, \{T\})$ with a single terminal T such that any path from S to T is of length 2.

By applying the Singleton Cut-Set Bound of Theorem 8 to two-level networks with vulnerable edges restricted to the first level (outgoing edges of S), we establish the following.

Theorem 20. Consider a two-level network $\mathcal{N}$ where the adversary $\mathbf{A}$ can act on up to t edges of the first level. Then, $C_1(\mathcal{N}, \mathbf{A})$ is upper bounded by the following value:

$$\min_{\mathcal{V}_1, \mathcal{V}_2} \left(\sum_{V_i \in \mathcal{V}_1} \deg^+(V_i) + \max \left\{ 0, \sum_{V_i \in \mathcal{V}_2} \deg^-(V_i) - 2t \right\} \right),$$

where the minimum is taken over all 2-partitions $\mathcal{V}_1, \mathcal{V}_2$ of the set of intermediate vertices $\{V_1, \ldots, V_n\}$.

To understand when the Singleton Cut-Set Bound is achievable in a two-level network, we introduce the following terminology.

Definition 21. Consider a network where an adversary can act simultaneously on up to t edges. We call an intermediate vertex in the network **damming** if

$$\deg^+(V_i) + 1 \leq \deg^-(V_i) \leq \deg^+(V_i) + 2t - 1.$$

Notice that such a vertex is present in *both* the Diamond Network and the Mirrored Diamond Network.

The next result gives a sufficient condition for the achievability of the Singleton Cut-Set Bound in a family of two-level networks. The proof will appear in the extended version of this work.

Theorem 22. In a two-level network where an adversary can act on up to t edges of the first level, and where no intermediate vertex is damming, the Singleton Cut-Set Bound is achievable for sufficiently large alphabet size.

Note that the results of Section 5 demonstrate that the converse of Theorem 22 does not hold. Indeed, both intermediate vertices of the Mirrored Diamond Network are damming but its capacity is as predicted by the Singleton Cut-Set Bound; see Proposition 14.

8. SOME DAMMING NODE EXAMPLES

In this section we include examples to illustrate that the presence of damming nodes in a two-level network may or may not compromise the achievability of the Singleton Cut-Set Bound (which is the best known cut-set bound for sufficiently large alphabets). These examples illustrate that the presence of damming nodes alone unfortunately does not determine whether or not the Singleton Cut-Set Bound is achievable. The phenomenon we wish to illustrate is already visible in two-level networks with just two streams. Therefore we focus there for ease of exposition.

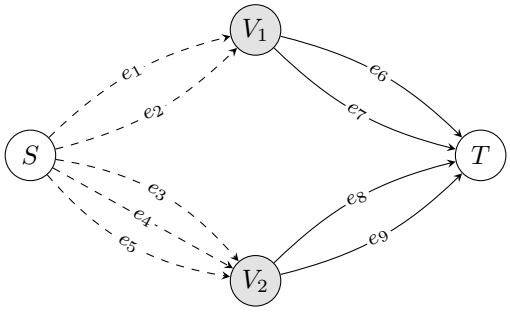

Fig. 3. The network for Example 23.

We start by observing that Theorem 22 shows that the Singleton Cut-Set Bound is achievable if both intermediate nodes are not damming. The Diamond Network is an example where only one of the two intermediate nodes is damming, and where the Singleton Cut-Set Bound is not achievable. The Mirrored Diamond Network, on

the other hand, shows that there are networks where both intermediate vertices are damming, and where the Singleton Cut-Set Bound is achievable. The next example provides a network where only one of the intermediate nodes is damming, and where the Singleton Cut-Set Bound is achievable.

Example 23. Consider the network of Figure 3 and an adversary able to corrupt at most two of the dashed edges. The Singleton Bound reads as 1 and it can be checked that is met with equality.

The network of the next example has two damming nodes, but the Singleton Cut-Set Bound is not achievable.

Example 24. The network of Figure 4 is a two-level network with vulnerable edges confined to the first level. We consider an adversary able to corrupt at most two of the dashed edges.

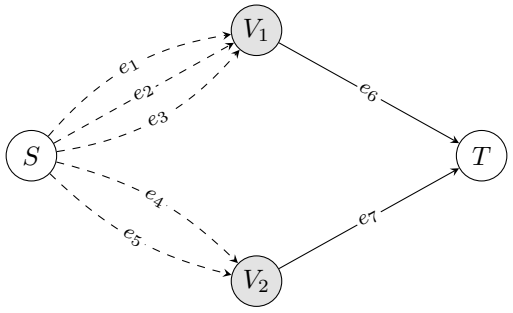

Fig. 4. The network for Example 24.

It can be shown that the Singleton Cut-Set Bound, equal to 1, is not achievable. The proof is omitted here.

9. DISCUSSION AND FUTURE WORK

We considered the problem of determining the one-shot capacity of communication networks with adversarial noise. In contrast with the typical scenario considered in the context of network coding, we allow the noise to affect only a subset of the network's edges. This restriction potentially increases the capacity of the adversarial network at hand.

We then defined the Diamond Network and computed its capacity, illustrating that previously known cut-set bounds are not sharp in general. We also studied the family of two-level networks, giving a sufficient condition under which the Singleton Cut-Set Bound is sharp over a sufficiently large alphabet.

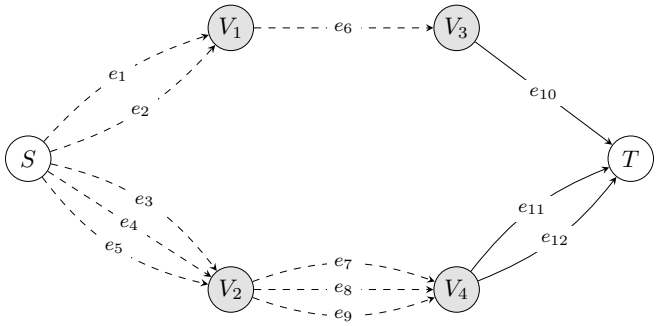

Fig. 5. An example of an adversarial network.

The problem of computing the capacity of a general network with restricted adversarial noise remains wide open and will be addressed in the extended version of this work. A very interesting unsolved example is provided by the network of Figure 5 for particular adversarial patterns. If the adversary is not restricted, the capacity predicted by the Singleton Bound is met with equality. However, when the adversary can corrupt at most one of the dashed edges in Figure 5, the predicted capacity by the Singleton Bound increases and can be proven that it is not achievable. The exact one-shot capacity of this network, to the best of our knowledge, is unknown.

REFERENCES

Beemer, A., Graves, E., Kliewer, J., Kosut, O., and Yu, P. (2020). Authentication and partial message correction over adversarial multiple-access channels. In *IEEE Conference on Communications and Network Security*, 1–6.

Cai, N. and Yeung, R.W. (2006). Network error correction, II: Lower bounds. *Communications in Inf. & Systems*, 6(1), 37–54.

Dikaliotis, T.K., Ho, T., Jaggi, S., Vyetrenko, S., Yao, H., Effros, M., Kliewer, J., and Erez, E. (2011). Multiple-access network information-flow and correction codes. *IEEE Trans. Info. Theory*, 57(2), 1067–1079.

Jaggi, S., Langberg, M., Katti, S., Ho, T., Katabi, D., and Médard, M. (2007). Resilient network coding in the presence of byzantine adversaries. In *26th IEEE Int'l Conference on Computer Communications*, 616–624. IEEE.

Kosut, O. and Kliewer, J. (2016). Network equivalence for a joint compound-arbitrarily-varying network model. In *IEEE Inf. Theory Workshop*, 141–145.

Matsumoto, R. (2007). Construction algorithm for network error-correcting codes attaining the singleton bound. *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, 90(9), 1729–1735.

Ravagnani, A. and Kschischang, F.R. (2018). Adversarial network coding. *IEEE Trans. on Inf. Theory*, 65(1), 198–219.

Sangwan, N., Bakshi, M., Dey, B.K., and Prabhakaran, V.M. (2019). Multiple access channels with adversarial users. In *IEEE Int'l Symp. on Inf. Theory*, 435–439. IEEE.

Silva, D., Kschischang, F., and Koetter, R. (2008). A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9), 3951–3967.

Yang, S., Ngai, C.K., and Yeung, R.W. (2007). Construction of linear network codes that achieve a refined Singleton bound. In *IEEE Int'l Symp. on Inf. Theory*, 1576–1580.

Yang, S. and Yeung, R.W. (2007). Refined coding bounds for network error correction. In *IEEE Inf. Theory Workshop on Inf. Theory for Wireless Networks*, 1–5.

Yang, S., Yeung, R.W., and Zhang, Z. (2008). Weight properties of network codes. *European Trans. on Telecommunications*, 19(4), 371–383.

Yeung, R.W. and Cai, N. (2006). Network error correction, I: Basic concepts and upper bounds. *Communications in Inf. & Systems*, 6(1), 19–35.