Network Coding for Error Correction

Thesis by

Svitlana S. Vyetrenko

svitlana@caltech.edu

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2011

(Defended May 26, 2011)

To my parents

Acknowledgements

I would like to thank my advisor Tracey Ho for all her help and encouragement; Michelle Effros for her valuable suggestions; my thesis committee members Joel Tropp and Houman Owhadi for their helpful feedback on my work; Sidharth Jaggi for being a great host and sharing his enthusiasm about research; Theodoros Dikaliotis for being my best friend throughout Caltech; Derek Leong for interesting discussions and technical assistance; my family and Stanimir Kondov for their unconditional love and support.

Abstract

In this thesis, network error correction is considered from both theoretical and practical viewpoints. Theoretical parameters such as network structure and type of connection (multicast vs. nonmulticast) have a profound effect on network error correction capability. This work is also dictated by the practical network issues that arise in wireless ad-hoc networks, networks with limited computational power (e.g., sensor networks) and real-time data streaming systems (e.g., video/audio conferencing or media streaming).

Firstly, multicast network scenarios with probabilistic error and erasure occurrence are considered. In particular, it is shown that in networks with both random packet erasures and errors, increasing the relative occurrence of erasures compared to errors favors network coding over forwarding at network nodes, and vice versa. Also, fountain-like error-correcting codes, for which redundancy is incrementally added until decoding succeeds, are constructed. These codes are appropriate for use in scenarios where the upper bound on the number of errors is unknown a priori.

Secondly, network error correction in multisource multicast and nonmulticast network scenarios is discussed. Capacity regions for multisource multicast network error correction with both known and unknown topologies (coherent and noncoherent network coding) are derived. Several approaches to lower- and upper-bounding error-correction capacity regions of general nonmulticast networks are given. For 3-layer two-sink and nested-demand nonmulticast network topologies some of the given lower and upper bounds match. For these network topologies, code constructions that employ only intrasession coding are designed. These designs can be applied to streaming erasure correction code constructions.

Contents

Chapter 1

Introduction

1.1 Network coding for error correction

In today's practical communication networks such as the Internet and wireless networks, reliable data delivery is an important question to address. Traditional approaches to networking generally assume forwarding in the network, with robustness to packet loss achieved by retransmissions of lost packets and/or end-to-end forward error correction. The recent introduction of network coding, where network packets are mixed at internal nodes, offers significant benefits in performance and erasure robustness [1, 2].

It is known that mixing, or coding packets at internal network nodes, is required to maximize the network throughput in multicast transmission scenarios, where all source information is demanded by all receivers [1]. For these scenarios, it was shown in [3] that propagating linear combinations of incoming packets (i.e., linear network coding) suffices to achieve the maximum flow capacity from the source to each receiving node. Further, the linear combinations employed at network nodes can be randomly selected in a distributed manner; if the coding field size is sufficiently large the maximum flow capacity can be achieved with high probability by mixing network packets at internal nodes randomly [4].

Another important benefit of network coding is its robustness to packet losses [2, 5]. Creating linear combinations of packets at intermediate network nodes naturally acts as an erasure code, as it introduces redundancy to the coded packets so that information at the destination can be recovered even if only a subset of the coded packets is received.

However, network coding is vulnerable to malicious attacks from rogue users. Due to the mixing operations at internal nodes, the presence of even a small number of adversarial nodes can contaminate the majority of packets in a network, preventing sinks from decoding. In particular, an error on even a single link might propagate to multiple downstream destinations via network coding, which might lead to the extreme case in which all incoming links at all sinks appear erroneous. As a result, the vulnerability of communication systems that employ network coding to adversarial attacks is an important topic for research.

In networks that employ network coding, one error occurrence can result in many correlated errors in the network as the corrupted data is mixed with uncorrupted data streams. Classic forward error correction, which assumes independent errors, would fail to recognize that all erroneous packets originated from a single error occurrence. Therefore, the use of network coding demands that we redefine the notion of error correction [6, 7, 8]. The concept of network error correction, shows how to exploit the fact that the errors at the sinks are correlated and, thus, distill source information as if only one error has occurred.

While studying network error correction, there are two groups of questions to ask. What is the maximum number of packets that can be securely communicated when an adversary is present? How to communicate and efficiently reconstruct packets at the sinks? In this thesis, we provide partial answers to these questions under a variety on constraints on the network topology, type and level of adversarial attack, heterogeneity and nature of node capabilities.

1.2 Background and related work

In this thesis, we discuss error correction in packet networks where network coding is employed at internal nodes. We define network error as an adversarial link or packet whose value and location in the network are unknown. We consider network error correction in the context of multicast vs. nonmulticast network connections. In a multicast connection, all source packets need to be transmitted to all sinks. In a nonmulticast connection, each of the sinks demands a subset of the source packets. Finally, we define error-correction capacity region as the set of all information rate vectors corresponding to connections that can be established successfully under a given error model.

Network coding was first introduced by Ahlswede et al. in 2000 [1]. The famous example of the butterfly network (see Figure 1.1) highlights the use of network coding to achieve the maximum flow (or minimum cut) capacity in multicast networks. This seminal work opened a new field of research of the utility of network coding and its applications to network management, robustness and security.

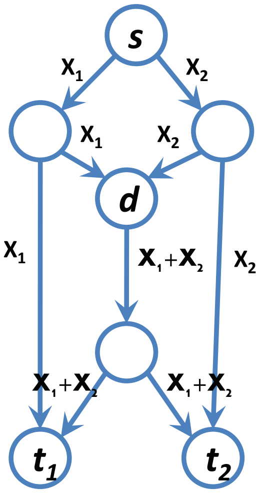


Figure 1.1: The butterfly network with source s and sinks t_1 and t_2 is an example of a network that requires coding to transmit messages x_1 and x_2 to both sinks. The presence of the bottleneck link that originates from node d makes network coding necessary to achieve the multicast rate 2.

Network coding in error-free multicast networks, where all sink nodes demand information from all sources, has been extensively studied. It was shown in [3] that linear network coding is sufficient to achieve the maximum flow capacity from the source to each receiving node in multicast transmission scenarios. An algebraic framework for linear network coding was presented in [9]. A decentralized approach to achieve the multicast capacity – random linear network coding – was proposed in [4], which showed that if the coding field size is sufficiently large, creating random linear combinations of the incoming packets at internal network nodes succeeds in transmitting at multicast network capacity with high probability. The recent work of [10] proposes universal and robust distributed network codes for multicast scenarios, such that coding field size does not need to be known a priori.

The information-theoretic network error correction problem, where an adversary arbitrarily corrupts transmissions on an unknown set of z links, was introduced by Cai and Yeung [6, 7, 8]. For a single-source, single-sink network, the capacity of the network with minimum cut m under arbitrary errors on up to z links is given by the cutset (i.e., minimum cut) bound

$$r \leq m - 2z \tag{1.1}$$

and can be achieved by a classical end-to-end error correction code over the multiple disjoint paths from the source to the sink. The single-source multicast network scenario has the same capacity region with m being the smallest minimum cut over all sinks, however, unlike the single-source, single-sink case, network coding is required in order for (1.1) to be achievable [7, 8]. An alternative approach to network error correction is to equip each network packet with a cryptographic signature (e.g. [11, 12]). Then, if each network node checks all packets and all nodes perform network coding, for any errors on up to z network links the information rate $m - z$ can be achieved in multicast networks without the need for further information-theoretic network error correction. However, this approach to error correction is more computationally expensive and may be infeasible at computationally limited nodes.

Two types of information-theoretic multicast network error correction problem are commonly considered. In the coherent case, there is a centralized knowledge of the network topology and the network code. Network error and erasure correction for this case has been addressed in [7] by generalizing classical coding theory to the network setting. In the non-coherent case, the network topology and/or network code are not known a priori. In this setting, [13] provided network error-correcting codes with a design and implementation complexity that is only polynomial in the size of network parameters. An elegant approach was introduced in [14], where information transmission occurs via the space spanned by the received packets/vectors, hence any generating set for the same space is equivalent to the sink [14]. Error correction techniques for the noncoherent case were also proposed in [15] in the form of rank metric codes, where the codewords are defined as subspaces of some ambient space. These code constructions primarily focus on the single-source multicast case and yield practical codes that have low computational complexity and are distributed and asymptotically rate-optimal.

For the noncoherent multisource multicast scenario without errors, the scheme of [4] achieves any point inside the rate region. An extension of subspace codes to multiple sources, for a noncoherent multiple-access channel model without errors, was provided in [16], which gave practical achievable (but not rate-optimal) algebraic code constructions, and in [17], which derived the capacity region and gave a rate-optimal scheme for two sources. For the multisource case with errors, [18] provided an efficient code construction achieving a strict subregion of the capacity region. In this thesis, we derive the error-correction capacity region for multisource multicast network scenarios in both coherent and noncoherent cases.

For nonmulticast networks, finding the capacity region of a general network even in the error-free case is an open problem. The capacity regions of certain nonmulticast network topologies, such as single-source two-sink networks [19, 20, 21] and single-source disjoint- or nested-demand networks [9] with any number of sinks, are known to be described by the cutset bounds in the error-free case. However, cutset bounds are not tight in general nonmulticast scenarios. Simple examples of nonmulticast networks whose error-free capacity regions are not described by the cutset bounds or are not polyhedral appear in [22, 23]. In this thesis, we derive upper and lower bounds on the error-correction capacity regions of general nonmulticast networks. We then consider error correction in two-sink and nested-demand network topologies, for which some of these bounds match.

The above-described results on multicast network error correction consider upper bounds and code constructions for the worst-case error model, in which the maximum number of erroneous network links z must be known in advance. Hence, the existing constructions rely on the inclusion of a fixed number of redundant bits in each packet. This approach can result in a very conservative upper bound in a probabilistic setting, for instance, when network errors occur randomly or some of the errors are corrected by cryptographic means. Our work gives a fountain-like error-correction code construction suitable for scenarios where an upper bound on the number of errors is not known a priori. We also look at noncoherent error and erasure correction under probabilistic error and erasure attack models, and show that there can be trade-offs between solutions for probabilistic attacks, where the optimal coding strategy for one increases vulnerability to the other.

1.3 Thesis outline and contributions

The thesis outline and contributions are as follows. In Chapter 2, we describe the basic network model and definitions that we use throughout this thesis.

In Chapter 3, we look at noncoherent correction of network errors and erasures with random locations in single-source multicast scenarios. Unlike existing results [7, 13], which consider performance limits for the worst-case location of a given numbers of errors and erasures, we consider the performance of fixed (not necessarily optimal) coding and forwarding strategies for given (not necessarily worst-case) models of error and erasure locations. In this case, random linear code at every node is not always optimal since it improves erasure resilience at the expense of error propagation. Our approach characterizes decoding success in terms of the rank of certain matrices corresponding to useful and erroneous information received at the sink nodes. We use this approach to analyze random coding and forwarding strategies on a family of simple networks with random error and erasure locations and argue that there can be trade-offs between solutions designed for error and erasure attacks, where the optimal solution for one increases vulnerability to the other. Simulation experiments on randomly generated hypergraphs representing wireless ad-hoc networks support these observations.

Chapter 4 discusses the combined use of cryptographic-based security and information-theoretic network error correction and proposes a fountain-like network error correction code construction suitable for network scenarios with computationally limited nodes. Unlike previous constructions that are oriented to worst-case error models and include a fixed number of redundant bits in each packet [13], we incrementally add redundancy until decoding succeeds. As a result, our code can be applied in networks where the upper bound on the number of errors is not known a priori. Our numerical investigations of example networks, where we optimize the proportion of packets undergoing cryptographic verification and/or coding subject to a computational budget constraint, suggest that appropriate hybrid use of both network error correction and cryptographic verification can outperform either approach separately.

In Chapter 5, we derive the capacity regions for coherent and noncoherent multisource multicast network error correction. In both cases, we provide outer bounds on the achievable rate region for communication and give corresponding communication schemes that operate at rates matching any point satisfying the outer bounds. Our codes are based on random subspace code design [14] and are "end-to-end," that is all nodes except the sources and the sinks are oblivious to the adversary present in the network and may simply implement predesigned linear network codes (random or otherwise). The codes are also fully distributed – different sources require no knowledge of the data transmitted by their peers.

In Chapters 6 and 7, we derive lower and upper bounds on the error correction capacity regions of general nonmulticast networks. In Chapter 6, we consider error correction in general nonmulticast networks. We give the achievability construction in the presence of errors based on the linear achievable region in the error-free case. We also refine the cutset upper bounds on the error correction capacity regions of non-multicast networks based on the topological structure of network cuts.

In Chapter 7, we specifically look at two-sink and nested-demand nonmulticast network topologies whose capacity regions are known to be given by the cutset bounds in the error-free case and show that it is not the case in networks with errors. We make a connection between erasure correction in real-time streaming data systems and nonmulticast erasure correction problems in 3-layer networks with nested sink demands. We further develop a set of tools that can be applied to construct cutset-refining upper bounds for nested-demand network topologies and use them to demonstrate how to design streaming systems tolerant to erasures so that no intersession coding is required between packets at different streaming checkpoints. In particular, we show that intrasession coding is sufficient to achieve the error and erasure correction capacity in 3-layer networks with nested demands in the case of one network erasure for any number of checkpoints. We also use the established proof techniques to show that our achievability construction in Chapter 6 is capacity-achieving for a family of two-sink 3-layer networks, and use this to derive tighter outer bounds for error- and erasure-correction capacity regions of arbitrary two-sink networks beyond those given in Chapter 6.

Parts of this work have appeared in [24], where we showed that in networks with both random packet erasures and errors, increasing the proportion of erasures compared to errors favors network coding over forwarding at network nodes, and vice versa; in [25], where we looked at hybrid approaches for computationally restricted scenarios and designed error-correcting code that allowed the combination of limited verification of cryptographic signatures with network coding error correction; in [26, 27], where we derived capacity regions for network error correction with both known and unknown topologies (coherent and non-coherent network coding) under a multisource multicast transmission scenario; and in [28], where we investigated the lower and upper bounds on the capacity regions of general non-multicast networks and gave a family of 3-layer two-sink networks for which these bounds are tight.

Chapter 2

Basic model and definitions

This chapter defines our basic network model, which is essentially based on that of [9, 29]. Throughout this thesis we represent a communication network by a directed acyclic graph $\mathcal{G}$. We denote the set of source nodes of $\mathcal{G}$ by $\mathcal{S} = \{s_1, s_2, \ldots, s_{|\mathcal{S}|}\}$ and the set of sink nodes of $\mathcal{G}$ by $\mathcal{T} = \{t_1, t_2, \ldots, t_{|\mathcal{T}|}\}$. We assume that each link of $\mathcal{G}$ has unit capacity and there can be multiple parallel edges connecting a pair of nodes.

For each $i = \{1, \ldots, |\mathcal{S}|\}$, independent discrete random processes $X_1^i, X_2^i, \ldots, X_{r_i}^i$ are observed at the source nodes. Each source process X_j^i is a stream of independent random bits of rate one bit per unit time. Then r_i is called the *rate* of source s_i. Each bitstream that corresponds to a source process X_j^i is divided into vectors of K bits. We call such a vector a *packet*.

There are a number of network *connections* that we may wish to establish. In a *multicast* connection, all source packets need to be transmitted to each of the sink nodes. In a *nonmulticast* connection each of the sink nodes demands a subset of the source packets from one or more source nodes. The set of all information rate vectors $(r_1, \ldots, r_{|\mathcal{S}|})$ that can be communicated to the sink nodes in $\mathcal{G}$ so that all desired connections are established successfully is called the *capacity region* of $\mathcal{G}$.

Network coding can be defined as an arbitrary causal mapping from network nodes' inputs to outputs [1]. In this thesis, we primarily discuss *linear network coding*, where nodes create linear combinations of the incoming packets and transmit them on their outgoing links. Linear network coding is known to be capacity-achieving in multicast network scenarios [3]. *Random linear network coding* , where the coefficients employed in linear combinations of the incoming packets are chosen uniformly at random from a finite field. This provides a decentralized solution to the information dissemination problem and multicast capacity-achieving with high probability when the field size is sufficiently large [30, 4].

In *intrasession coding*, coding is restricted to packets belonging to the same connection. In *intersession coding*, coding is allowed among packets belonging to different connections. When there exists a centralized knowledge of network topology and network code, we consider a *coherent* network coding scenario. When network topology and/or network code are not known a priori (for instance, when random linear coding is performed), we consider a *noncoherent* network coding scenario.

In this thesis, we examine *network error correction problems* defined on $\mathcal{G}$, where sinks need to reconstruct messages transmitted by sources in the presence of a *computationally unbounded adversary*, who can observe all network transmissions and inject his own packets on network links that may be chosen as a function of his knowledge of the network, the message, or the communication scheme. By *network error* we mean a corrupted packet whose value and location in the network are unknown. *Network erasures* are defined as network errors with a known location and unknown value. The set of all information rate vectors that can be communicated to the sink nodes in $\mathcal{G}$ so that all connections are established successfully when an adversary is present in the network is called the *error-correction capacity region* of $\mathcal{G}$.

Chapter 3

Noncoherent correction of errors and erasures with random locations

3.1 Introduction

Most existing results on multicast network error correction apply to worst-case error and erasure locations (see [13, 31]), for which random linear network coding achieves capacity. In this chapter, we investigate the performance of linear coding and routing strategies in non-worst-case scenarios where links may fail randomly, or an adversary may only succeed probabilistically in attempts to compromise network nodes. In this case, random linear coding at every node is not always optimal, since it improves erasure resilience at the expense of error propagation.

In this chapter we consider decentralized strategies, which we analyze by bringing topology considerations into the noncoherent subspace coding framework of [14]. We show that for a given realization of error and erasure locations, successful decoding can be characterized in terms of the rank of certain matrices that correspond to useful and erroneous information received at the sink node [24]. We analytically derive the probability of successful decoding for random coding and routing strategies on a family of simple network subgraphs consisting of multiple multihop paths with random error and erasure locations, and show how the relative performance of these strategies depends on the information rate, minimum cut capacity, and error and erasure probabilities. Simulation results on randomly generated hypergraphs representing wireless networks support the observations from the analysis.

3.2 Model

We consider single-source multicast over an acyclic network $\mathcal{G}$ with source $\mathcal{S}$ and a set of sink nodes $\mathcal{T}$. A network link l may be subject to an erasure, in which case no packet is received on l, or an error, in which case a packet of arbitrary value is received on l.

Following [14], we consider constant-dimension noncoherent network coding, defined as follows. Let V be the vector space of length-K vectors over the finite field $\mathbb{F}_q$, representing the set of all possible values of packets transmitted and received in the network. Let $\mathcal{P}(V)$ denote the set of all subspaces of V. A code $\mathcal{C}$ consists of a nonempty subset of $\mathcal{P}(V)$, where each codeword $U \in \mathcal{C}$ is a subspace of constant dimension R. To transmit codeword $U \in \mathcal{C}$, the source transmits a set of packets whose corresponding vectors span U. The sink receives the subspace $U' = \mathcal{H}_k(U) \oplus E$, where $\mathcal{H}_k$ projects U onto a k-dimensional subspace of U, and E is the subspace spanned by the error packets. Let $t = \dim(E)$, and let $\rho = (R-k)_+$.

In [14], t and ρ are referred to as the number of errors and erasures respectively. The concept of subspace errors and erasures is distinct from that of network errors and erasures. As will be seen later, the network topology and coding strategy determine what subspace errors and erasures result from given network errors and erasures. Thus, to avoid confusion, we refer to t as the number of additions, and ρ as the number of deletions. The distance between two spaces U_1, U_2 is defined as

$$d(U_1, U_2) \doteq \dim(U_1 + U_2) - \dim(U_1 \cap U_2). \tag{3.1}$$

It is shown in [14] that d is a metric for $\mathcal{P}(V)$. Subspace minimum distance decoding is successful if and only if there is no codeword $\tilde{U} \neq U$ in $\mathcal{C}$ for which $d(\tilde{U}, U') \leq d(U, U')$.

3.3 Main results

3.3.1 Noncoherent coding for errors and erasures

Let $\Delta \doteq \underset{U_1,U_2 \in \mathcal{C}: U_1 \neq U_2}{min} d(U_1, U_2)$ be the minimum distance of $\mathcal{C}$. In [14] the following result is shown:

Theorem 1. *The transmitted subspace $U \in \mathcal{C}$ can be successfully recovered from the received* *subspace U' if*

$$2(t+\rho) < \Delta. \tag{3.2}$$

Let r denote the code rate of $\mathcal{C}$. Theorem 2 gives a converse to this result for $r > (R-\Delta/2)/R$ and any $\mathcal{H}_k$. Concurrent independent work [32] gives a converse pertaining to the case where $\mathcal{H}_k$ is adversarially chosen subject to a minimum rank constraint. However, in our problem $\mathcal{H}_k$ depends on the coding/routing strategy employed.

Lemma 1. *Let $\mathcal{C}$ have minimum distance Δ. If $2t \geq \Delta$, then decoding is unsuccessful for some value of the transmitted subspace and the error packets.*

Proof. See Section 3.4.3. □

Note that for constant dimension codes, Δ is even and that for a given R and Δ, we have $r \leq (R-\Delta/2+1)/R$.

Theorem 2. *Let $\mathcal{C}$ have dimension R, minimum distance Δ, and code rate $r > (R-\Delta/2)/R$. If $2(t+\rho) \geq \Delta$, then decoding is unsuccessful for some value of the transmitted subspace and the error packets.*

Proof. See Section 3.4.3. □

Lemma 2. *For any given set of adversarial links and any given network code, putting a linearly independent adversarial error on each adversarial link results in the lowest probability of successful decoding.*

Proof. See Section 3.4.3. □

Lemma 2 implies that we can henceforth consider the case where each adversarial link is associated with a linearly independent error.

Let $\mathbb{F}_q^{m\times n}$ denote the set of all $m\times n$ matrices over finite field $\mathbb{F}_q$. Let $\mathcal{C}$ be a subspace code with codeword dimension R, minimum distance Δ, and code rate greater than $(R-\Delta/2)/R$. Let matrix $W \in \mathbb{F}_q^{R\times K}$ represent the transmitted codeword. Let ν be the number of incoming links of a sink $t \in \mathcal{T}$. Let $Q \in \mathbb{F}_q^{\nu\times R}$ be the network transfer matrix from the source packets to the packets received at t [9].

Let L denote the number of links in $\mathcal{G}$. An error on a link is modeled as addition of an arbitrary error packet to the packet being transmitted at that link. Let $Z \in \mathbb{F}_q^{L \times K}$ denote the error matrix whose ith row corresponds to the error packet that is injected on the ith link of $\mathcal{G}$. Let $B \in \mathbb{F}_q^{\nu \times L}$ be the transfer matrix from the error packets to the packets received at t.

Let $Y \in \mathbb{F}_q^{\nu \times K}$ be the matrix whose rows correspond to the packets received at t. Then

$$Y = QW + BZ \tag{3.3}$$

and the decodability condition given in Theorems 1 and 2 can be translated to our setting as follows:

Theorem 3. *For a given $\mathcal{C}$, let $y = \frac{\Delta}{2}$. Let the transmitted matrix W and the error matrix Z have linearly independent rows. Then decoding at $t \in \mathcal{T}$ is guaranteed to succeed iff*

$$R - rank(QW + BZ) + 2rank(BZ) < y. \tag{3.4}$$

Proof. See Section 3.4.3. □

3.3.2 Single path subgraph

We next apply the results from Section 3.3.1 to study error and erasure performance of coding and routing strategies on networks with randomly located errors and erasures. We analyze the probability that the error and erasure locations are such that not all error values can be corrected.

We first consider a simple building block network consisting of a simple multihop path with source $\mathcal{S}$ and sink $\mathcal{T}$(see Fig. 3.1(a)). Let the network consist of M hops. Let R, $\mathcal{C}$, Δ, y, W, L, and Z be defined as in the previous section. Let C be the number of parallel links on each hop of $\mathcal{G}_M$. Let $S \in \mathbb{F}_q^{C \times R}$ be the source coding matrix and let $A \in \mathbb{F}_q^{C \times C}$ be the transfer matrix from all links in the network to the packets received at $\mathcal{T}$. Let $B \in \mathbb{F}_q^{C \times L}$ be the transfer matrix from error packets to the packets received at $\mathcal{T}$. According to (3.3), we can write

$$Y = ASW + BZ. \tag{3.5}$$

Enumerate all nodes of $\mathcal{G}_M$ with node 0 corresponding to $\mathcal{S}$ and node M corresponding to $\mathcal{T}$. Assume that the jth hop refers to the transmission from the $(j-1)$th to the jth node.

Consider the jth hop of the single path multihop network. In our model, three mutually exclusive events can occur at the jth hop for any j: an erasure can occur on exactly one of the C links with probability p; an error can occur on exactly one of the C links with probability s; no errors and erasures occur at the jth hop with probability $(1-p-s)$. When an error or erasure occurs, any one of the C links has probability $\frac{1}{C}$ of being the affected link.

To solve the problem we are going to adopt the algebraic coding model given in (3.3). Choosing different network coding strategies at the non-source nodes corresponds to modifying A (and, consequently, B) in (3.3). We compare performance of random linear coding at the source paired with two different strategies at non-source nodes:

1. **Forwarding with random replication (FRR)**
   - Each node forwards all received packets to the outgoing links.
   - In case of a link erasure, the node replaces the erased packet with a copy of any one of the successfully received packets.
2. **Random linear coding (RLC)**
   - Each node creates random linear combinations of all received packets and sends them to the outgoing links.
   - In case of a link erasure, the node replaces the erased packet by creating a random linear combination of the successfully received packets.

Let I be the $C \times C$ identity matrix. Define $A_j \in \mathbb{F}_q^{C\times C}$ for RLC as a random matrix with entries from $\mathbb{F}_q$, and for FRR as $A_j \doteq I$. If no erasure occurs, define $E_j \in \mathbb{F}_q^{C\times C}$ as $E_j \doteq I$. If an erasure occurs on link i, define $E_j \in \mathbb{F}_q^{C\times C}$ as I with the ith row equal to the unit vector with 1 in the kth position if link k was replicated for FRR, and I with the ith row equal to the zero vector for RLC. If no error occurs, define $D_j \in \mathbb{F}_q^{C\times C}$ as $D_j \doteq I$. If an error occurs on the ith link, define $D_j \in \mathbb{F}_q^{C\times C}$ as I with the ith row equal to the zero vector. Define $D_j^* \in \mathbb{F}_q^{C\times C}$ as $D_j^* \doteq I - D_j$.

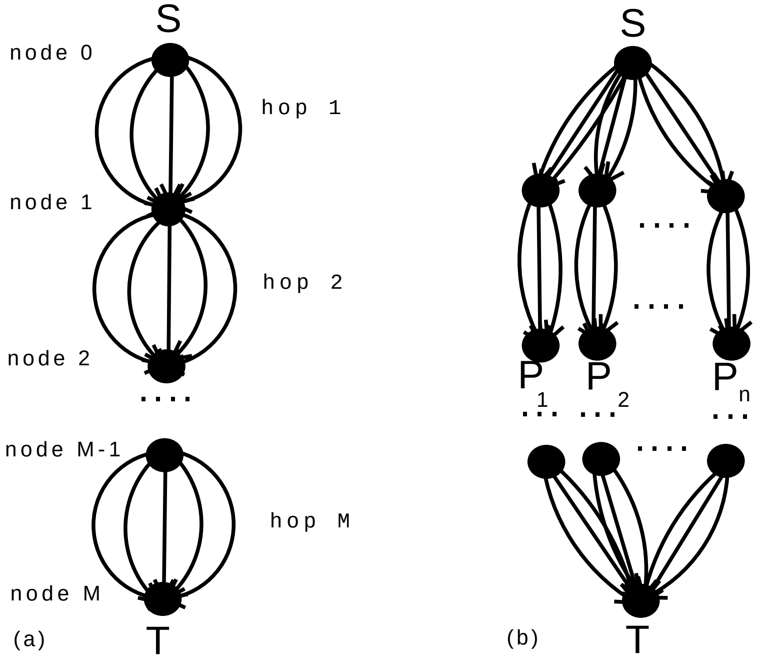


Figure 3.1: Schematic depiction of: (a) single path subgraph; (b) multiple path subgraph

Define

$$F_j = \begin{cases} D_j & \text{if an error occurs at the } j\text{th hop,} \\ E_j & \text{if an erasure occurs at the } j\text{th hop,} \\ I & \text{if neither error, nor erasure occur at the } j\text{th hop.} \end{cases}$$

Therefore, for both coding strategies we rewrite A and B in (3.5) as

$$\begin{aligned} A &= F_M A_M F_{M-1} A_{M-1} \ldots F_2 A_2 F_1 A_1 \\ B &= \left(\begin{array}{cccc} F_M A_M..F_2 A_2 D_1^* & F_M A_M..F_3 A_3 D_2^* & .. & D_M^* \end{array} \right) \end{aligned}$$

3.3.2.1 Random linear coding

Let $\mathcal{P}$ denote the probability of successful decoding. Let A and D be the random variables representing the number of dimension additions/deletions to/from $rowspace(W)$ in $\mathcal{G}_M$ respectively. Then according to Theorems 1 and 2, $\mathcal{P}$ can be computed as

$$\mathcal{P} = \text{Prob}\left(\mathsf{A} + \mathsf{D} \leq y - 1\right). \tag{3.6}$$

Let Y^j denote the subspace spanned by received packets at the jth node of $\mathcal{G}_M$. Let a_j and d_j be the number of dimension additions/deletions to/from $rowspace(W)$ present in Y^j respectively. Let us say that the jth node of $\mathcal{G}_M$ is in state i if, after random linear coding is performed at the jth node, we have $a_j + d_j = i$. Let $P^j_{i,k}$ denote the probability that given that the $(j-1)$th node of $\mathcal{G}_M$ is in state i, the jth node of $\mathcal{G}_M$ will be in state k after the data transmission from the $(j-1)$th to the jth hop.

Lemma 3. *When RLC is performed at every node of $\mathcal{G}_M$, for every node $j = 1, \ldots, M$ we have:*

$$\begin{aligned}
&\textit{if } 0 \leq i < C - R \\
&\quad P^j_{i,i} = 1 - s, P^j_{i,i+1} = s, P^j_{i,k} = 0 \textit{ for } k \neq i, i+1 \\
&\textit{if } i = C - R + 2m, m = 0, \ldots, R-1 \\
&\quad P^j_{i,i} = 1 - p - s, P^j_{i,i+1} = p, P^j_{i,i+2} = s, P^j_{i,k} = 0 \textit{ for } k \neq i, i+1, i+2 \\
&\textit{if } i = C - R + 2m + 1, m = 0, \ldots, R-1 \\
&\quad P^j_{i,i} = 1 - s, P^j_{i,i+1} = s, P^j_{i,k} = 0 \textit{ for } k \neq i, i+1 \\
&\textit{if } i = C + R \\
&\quad P^j_{i,i-1} = p, P^j_{i,i} = 1 - p, P^j_{i,k} = 0 \textit{ for } k \neq i-1, i
\end{aligned}$$

Proof. See Section 3.4.3. □

Lemma 3 implies that when RLC is performed, the system can be modeled as a Markov chain that has a probability transition matrix with entries P^j_{ik} for $i, k = 0 \ldots C + R$. Moreover, $\mathcal{P}$ can be computed using the distribution of this Markov chain after M transitions.

3.3.2.2 Forwarding with random replication

Lemma 4. *In case of FRR with RLC performed at S we have*

$$\begin{aligned}
\textit{rank}(BZ) &= \textit{rank}(F_M \ldots F_2 D^*_1 Z_1) + \ldots + \textit{rank}(D^*_M Z_M) && (3.7) \\
\textit{rank}(ASW + BZ) &= \textit{rank}(ASW) + \textit{rank}(BZ) && (3.8) \\
\textit{rank}(ASW) &= \min(R, \textit{rank}(A)) && (3.9)
\end{aligned}$$

Proof. See Section 3.4.3. □

Using Theorem 3 and Lemma 4, $\mathcal{P}$ can be computed as:

$$\begin{aligned}
\mathcal{P} &= \operatorname{Prob}\left(R - \operatorname{rank}(ASW + BZ) + 2\operatorname{rank}(BZ) \le y - 1\right) \qquad (3.10) \\
&= \sum_{f,l,z \in \mathcal{I}} \operatorname{Prob}\left(\operatorname{rank}(ASW) = l - z, \operatorname{rank}(BZ) = z, \operatorname{rank}(A) = f\right) \\
&= \sum_{f,l,z \in \mathcal{I}} \operatorname{Prob}\left(\operatorname{rank}(BZ) = z | \operatorname{rank}(A) = f\right) \operatorname{Prob}\left(\operatorname{rank}(A) = f\right) \\
\mathcal{I} &= \{f, z, l : 0 \le f \le C, 0 \le z \le y - 1, R + 2z - (y - 1) \le l \le C\}.
\end{aligned}$$

Lemmas 5, 6 and 7 provide auxiliary results that our further derivation relies on.

Lemma 5. *If D_1 is the identity matrix with a randomly chosen row substituted by a zero row, then*

$$Prob\left(rank(F_j \dots F_2 D_1) = f | rank(F_j \dots F_2) = f + 1\right) = \frac{f+1}{C}.$$

Proof. See Section 3.4.3. □

Lemma 6. *If D_1 is the identity matrix with a randomly chosen row substituted by a zero row, then*

$$\begin{aligned}
rank(F_j \dots F_2) &= f, rank(F_j \dots F_2 D_1) = f \Rightarrow rank(F_j \dots F_2 D_1^*) = 0 \\
rank(F_j \dots F_2) &= f + 1, rank(F_j \dots F_2 D_1) = f \Rightarrow rank(F_j \dots F_2 D_1^*) = 1
\end{aligned}$$

Proof. See Section 3.4.3. □

Lemma 7. *If E_1 is the identity matrix with a randomly chosen row substituted by a zero row, then*

$$Prob\left(rank(F_j \dots F_2 E_1) = f | \, rank(F_j \dots F_2) = f + 1\right) = \frac{f(f+1)}{C(C-1)}.$$

Proof. See Section 3.4.3. □

Now we can compute (3.10) by deriving explicit expressions for probability distributions $\operatorname{Prob}\left(\operatorname{rank}(A) = f\right)$ and $\operatorname{Prob}\left(\operatorname{rank}(BZ) = z | \operatorname{rank}(A) = f\right)$. Detailed derivations of these results are given in Sections 3.4.1 and 3.4.2 respectively.

3.3.3 Multiple path subgraph

Consider a multiple path subgraph $\mathcal{G}_n$ (see Fig. 3.1(b)) with source $\mathcal{S}$ and sink $\mathcal{T}$. Let $\mathcal{P} = \{P_1, P_2 \dots P_n\}$ be the set of edge-disjoint paths from $\mathcal{S}$ to $\mathcal{T}$. Let M_i be the number of hops on each path P_i. Let C_i be the number of parallel links on each hop of P_i. Let $C = \sum_{i=1}^{n} C_i$. For the case of multiple path subgraph, assume that $R \geq \max\limits_{1 \leq i \leq n} C_i$. Let $R_i \leq C_i$ be the rank of information packets that are transmitted on each P_i. We assume that $\sum\limits_{i=1}^{n} R_i \geq R$.

Let $A^i \in \mathbb{F}_q^{C_i \times C_i}$ and $B^i \in \mathbb{F}_q^{C_i \times C_i M_i}$ be the linear transformations applied by the network on each P_i to information and error packets respectively. For the multiple path network model that we defined, matrices A and B have the block-diagonal structure with A^i and B^i on the main diagonal.

Lemma 8. *For any given set of error and erasure locations and any given network code, the probability of successful decoding for $\mathcal{G}_n$ is maximized when R_i is chosen to be equal to C_i on each P_i.*

Proof. See Section 3.4.3. □

By Lemma 8 it is sufficient to consider $R_i = C_i$ for each P_i since it results in the highest probability of successful decoding.

3.3.3.1 Random linear coding

Let A and D be random variables representing the number of dimension additions/deletions to/from rowspace(W) in $\mathcal{G}_n$ respectively. Let A_i and D_i be random variables, that stand for the number of dimension additions/deletions to/from $rowspace(W)$ on each P_i respectively. Let a, d, a_i and d_i be the values that A, D, A_i and D_i can take.

Lemma 9. *If RLC is performed on all paths of $\mathcal{G}_n$ and $R_i = C_i$ $\forall i$, we have:*

$$a = \sum_{i=1}^{n} a_i \tag{3.11}$$

$$d = max(\sum_{i=1}^{n} d_i - (C - R), 0) \tag{3.12}$$

Proof. See Section 3.4.3. □

Now we can rewrite (3.6) as:

$$\begin{aligned}\mathcal{P} &= \text{Prob}\,(\mathsf{A}+\mathsf{D} \leq y-1) \\ &= \sum_{\substack{a_i,\, d_i\, : \\ \sum a_i + \max(\sum d_i - (C-R), 0) \leq y-1, \\ d_i = a_i \text{ or } d_i = a_i + 1}} \prod_{j=1}^{n} \text{Prob}\,(P_j \text{ in state } a_j + d_j \text{ after } M_j \text{ hops})\,,\end{aligned}$$

where the last equality follows from Lemmas 3, 9 and the independence between $\mathsf{A}_i, \mathsf{D}_i$ and $\mathsf{A}_j, \mathsf{D}_j$ for $i \neq j$. We can then use the derivation for a single path subgraph to evaluate Prob $(P_i$ in state $a_i + d_i$ after M_i hops) for each P_i.

3.3.3.2 Forwarding with random replication

Using the fact that the quantities rank(A^i) and rank$(B^i Z^i)$ associated with each P_i are independent of the corresponding quantities for P_j for $i \neq j$, we can write $\mathcal{P}$ as:

$$\mathcal{P} = \sum_{f_i, z_i \in \mathcal{I}} \prod_{j=1}^{n} \text{Prob}\left(\text{rank}(B^j Z^j) = z_j, \text{rank}(A^j) = f_j\right),$$

where $\mathcal{I} = \{f_i, z_i : 0 \leq f_i \leq C_i, \sum f_i = f; 0 \leq z_i \leq y-1,$
$\sum z_i = z; R + 2z - (y-1) \leq \min(f, R) + z \leq C\}$. We then apply the derivation for a single path case by setting $A = A^i$, $B = B^i$, $Z = Z^i$, $i = 1 \ldots n$.

3.3.4 Experimental results

Figure 3.2 shows the probabilities of successful decoding computed analytically for both strategies. Figure 3.3 depicts average probability of successful decoding curves obtained by running 500 experiments over 20 randomly generated one-source one-sink hypergraphs with 20 nodes. In our experiment, we assumed that each non-source node could become adversarial with probability s and each hyperarc could fail with probability p. In both Figure 3.2 and Figure 3.3, all curves are sketched against p for a fixed s when RLC is done at the source. Note that both analytical and experimental results suggest that RLC is more beneficial than FRR when information is transmitted at a higher rate.

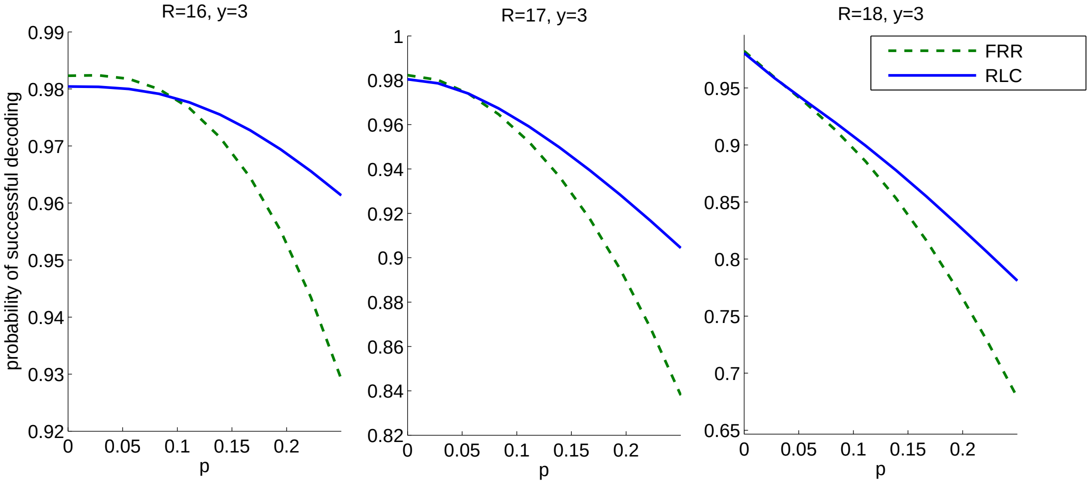


Figure 3.2: $n = 4$, $M = 3$, $R_i = C_i = 5, i = 1 \dots 4$, $s = 0.05$.

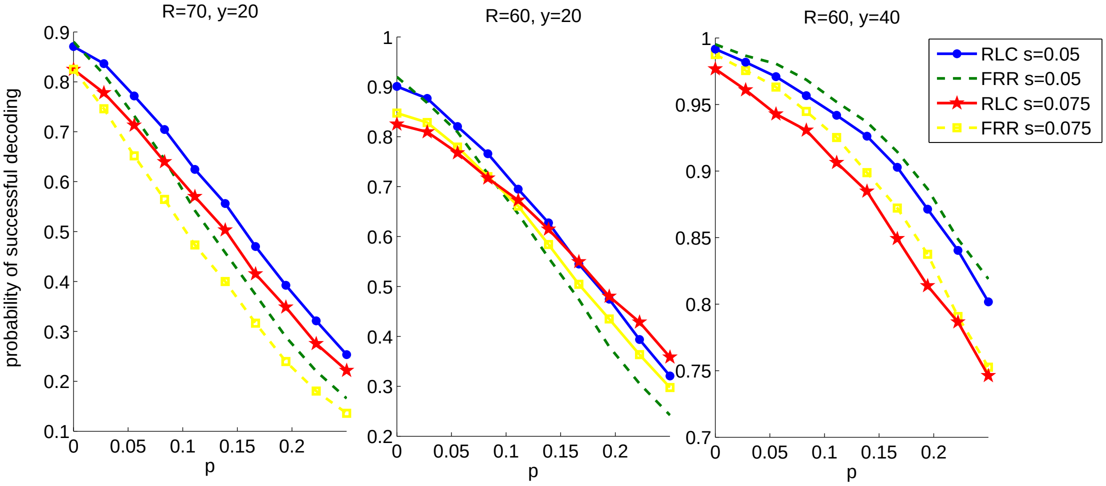


Figure 3.3: Average over randomly generated hypergraphs with mincut capacity equal to 100.

3.4 Detailed derivations and proofs

3.4.1 Derivation of $Prob\,(rank(A) = f)$

For FRR $A_i = I$, therefore, $Prob\,(rank(A) = f) = Prob\,(rank(F_M F_{M-1} \dots F_2 F_1) = f)$. For notational convenience denote $Prob\,(rank(F_j F_{j-1} \dots F_2 F_1) = f)$ by $\phi_j(f)$. Denote the number of error/erasure occurrences out of j hops by N_j. Compute $\phi_j(f)$ by conditioning on N_j, then

$$\phi_j(f) \;=\; \sum_{l=C-f}^{j} Prob\,(rank(F_j F_{j-1} \dots F_2 F_1) = f | N_j = l)\, Prob\,(N_j = l)$$

If $N_j = l$ suppose that all errors and/or erasures occurred on $i_1, i_2 \dots i_l$th hops. Then we have:

$$\begin{aligned}
\phi_j(f) &= \sum_{l=C-f}^{j} Prob\left(rank(F_{i_l} F_{i_{l-1}} \dots F_{i_2} F_{i_1}) = f\right) Prob\,(N_j = l) \\
&= \sum_{l=C-f}^{j} Prob\left(rank(F_{i_l} F_{i_{l-1}} \dots F_{i_2} F_{i_1}) = f\right) \sum_{\substack{k \text{ erasures,} \\ m \text{ errors:} \\ k+m=l}} \frac{j!}{k!m!(j-l)!} p^k s^m (1-p-s)^{j-l} \\
&= \sum_{l=C-f}^{j} Prob\left(rank(F_{i_l} F_{i_{l-1}} \dots F_{i_2} F_{i_1}) = f, \text{ erasures on } l \text{ hops}\right) \frac{j!}{l!(j-l)!} p^l (1-p-s)^{j-l} \\
&+ \sum_{l=C-f}^{j} \sum_{m=1}^{l} Prob\left(rank(F_{i_l} F_{i_{l-1}} \dots F_{i_2} F_{i_1}) = f, \text{ errors on } m \text{ hops}\right) \frac{j!}{(l-m)!m!(j-l)!} p^{l-m} s^m (1-p-s)^{j-l},
\end{aligned}$$

where the first term corresponds to the case when only erasures occurred on all hops i_g, $g = 1 \dots l$ and the second term corresponds to the case when both errors and erasures occurred on all hops i_g, $g = 1 \dots l$.

Therefore,

$$\begin{aligned}
\phi_j(f) &= \sum_{l=C-f}^{j} Prob\left(rank(E_{i_l} E_{i_{l-1}} \dots E_{i_2} E_{i_1}) = f\right) \frac{j!}{l!(j-l)!} p^l (1-p-s)^{j-l} \\
&+ \sum_{l=C-f}^{j} \sum_{m=1}^{l} Prob\left(rank(F_{i_l} F_{i_{l-1}} \dots F_{i_2} F_{i_1}) = f, \text{ errors on } m \text{ hops}\right) \frac{j!}{(l-m)!m!(j-l)!} p^{l-m} s^m (1-p-s)^{j-l}
\end{aligned}$$

1. $Prob\,(rank(E_{i_l}\dots E_{i_2}E_{i_1}) = f)$

Denote $Prob\,(rank(E_{i_l}\dots E_{i_2}E_{i_1}) = f)$ by $f_l(f)$. We can compute $f_l(f)$ by conditioning on $rank(E_{i_l}\dots E_{i_2})$ and Lemma 7.

For $l \geq 2$:

$$\begin{aligned} f_l(f) &= Prob\,(rank(E_{i_l}\dots E_{i_2}E_{i_1}) = f|\,rank(E_{i_l}\dots E_{i_2}) = f)\,Prob\,(rank(E_{i_l}\dots E_{i_2}) = f) \\ &+ Prob\,(rank(E_{i_l}\dots E_{i_2}E_{i_1}) = f|\,rank(E_{i_l}\dots E_{i_2}) = f+1)\,Prob\,(rank(E_{i_l}\dots E_{i_2}) = f+1) \\ &= \left(1 - \frac{f(f-1)}{C(C-1)}\right) f_{l-1}(f) + \frac{f(f+1)}{C(C-1)} f_{l-1}(f+1) \end{aligned}$$

with the base case

$$f_1(f) = \begin{cases} 1, & f = C-1; \\ 0, & \text{otherwise.} \end{cases}$$

2. $Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f,$ **errors on** m **hops**$\big)$

Denote $Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f, \text{ errors on } m \text{ hops}\big)$ by $g_l(f,m)$. We can compute $g_l(f,m)$ by conditioning on F_{i_1}, $rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2})$ and Lemmas 5 and 7.

$$\begin{aligned}
g_l(f,m) &= Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f|F_{i_1} = D_{i_1}\big)\, Prob\left(F_{i_1} = D_{i_1}\right) \\
&+ Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f|F_{i_1} = E_{i_1}\big)\, Prob\left(F_{i_1} = E_{i_1}\right) \\
&= \big(Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f|\, rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f, F_{i_1} = D_{i_1}\big)\big)\,. \\
&\times Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f|F_{i_1} = D_{i_1}\big) \\
&+ Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f|\, rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f+1, F_{i_1} = D_{i_1}\big) \\
&\times Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f+1|F_{i_1} = D_{i_1})\big)\, Prob\left(F_{i_1} = D_{i_1}\right) \\
&+ \big(Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f|\, rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f, F_{i_1} = E_{i_1}\big) \\
&\times Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f|F_{i_1} = E_{i_1}\big) \\
&+ Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}F_{i_1}) = f|\, rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f+1, F_{i_1} = E_{i_1}\big) \\
&\times Prob\big(rank(F_{i_l}F_{i_{l-1}}\dots F_{i_2}) = f+1|F_{i_1} = E_{i_1})\big)\, Prob\left(F_{i_1} = E_{i_1}\right).
\end{aligned}$$

Then for $m \geq 2$

$$\begin{aligned}
g_l(f,m) &= \left(\frac{C-f}{C}g_{l-1}(f,m-1) + \frac{f+1}{C}g_{l-1}(f+1,m-1)\right)\frac{m}{l} \\
&+ \left((1-\frac{f(f-1)}{C(C-1)})g_{l-1}(f,m) + \frac{f(f+1)}{C(C-1)}g_{l-1}(f+1,m)\right)\frac{l-m}{l}
\end{aligned}$$

and for $m = 1$

$$\begin{aligned}
g_l(f,m) &= \left(\frac{C-f}{C}f_{l-1}(f) + \frac{f+1}{C}f_{l-1}(f+1)\right)\frac{1}{l} \\
&+ \left((1-\frac{f(f-1)}{C(C-1)})g_{l-1}(f,1) + \frac{f(f+1)}{C(C-1)}g_{l-1}(f+1,1)\right)\frac{l-1}{l}
\end{aligned}$$

with the base case

$$g_1(f,1) = \begin{cases} 1, & f = C-1; \\ 0, & \text{otherwise.} \end{cases}$$

3.4.2 Derivation of $Prob\,(rank(BZ) = z|\, rank(A) = f)$

Recall that by Lemma 4 we have

$$rank(BZ) = rank(F_M \ldots F_2 D_1^* Z_1) + \ldots + rank(F_M D_{M-1}^* Z_{M-1}) + rank(D_M^* Z_M).$$

Denote $F_M \ldots F_{M-j+2} D_{M-j+1}^* Z_{M-j+1} + \ldots + F_M D_{M-1}^* Z_{M-1} + D_M^* Z_M$ by $B^j Z^j$ and $F_M \ldots F_{M-j+2} F_{M-j+1}$ by A^j. Let $\psi_j(f,z) = Prob\left(rank(B^j Z^j) = z|\, rank(A^j) = f\right)$. Note that

$\psi_M(f,z) = Prob\,(rank(BZ) = z|\, rank(A) = f)$. We can compute $\psi_j(f,z)$ by conditioning on F_{M-j+1}, $rank(F_M \ldots F_{M-j+2})$ and using Lemmas 5 and 7.

$$\begin{aligned}
\psi_j(f,z) &= Prob\left(rank(B^j Z^j) = z|\, rank(A^j) = f\right) \\
&= Prob(rank(B^j Z^j) = z|F_{M-j+1} = D_{M-j+1}, rank(A^j) = f)\, Prob(F_{M-j+1} = D_{M-j+1}|\, rank(A^j) = f) \\
&+ Prob(rank(B^j Z^j) = z|F_{M-j+1} = E_{M-j+1}, rank(A^j) = f)\, Prob(F_{M-j+1} = E_{M-j+1}|\, rank(A^j) = f) \\
&+ Prob(rank(B^j Z^j) = z|F_{M-j+1} = I, rank(A^j) = f)\, Prob(F_{M-j+1} = I|\, rank(A^j) = f)
\end{aligned}$$

with the base case

$$\psi_1(C,z) = \begin{cases} 1, & z = 0; \\ 0, & \text{otherwise}; \end{cases}$$

$$\psi_1(C-1,z) = \begin{cases} \frac{p}{p+s}, & z = 0; \\ \frac{s}{p+s}, & z = 1; \\ 0, & \text{otherwise}; \end{cases}$$

$$\psi_1(f,z) = 0 \text{ for any } f \leq C-2.$$

1. $Prob(rank(B^jZ^j) = z | F_{M-j+1} = D_{M-j+1}, rank(A^j) = f)$

$$\begin{aligned}
& Prob(rank(B^jZ^j) = z | F_{M-j+1} = D_{M-j+1}, rank(A^j) = f) \\
= \quad & Prob(rank(B^jZ^j) = z | \, rank(A^{j+1}D_{M-j+1}) = f) \\
= \quad & Prob\left(rank(B^jZ^j) = z | \, rank(A^{j+1}) = f, rank(A^{j+1}D_{M-j+1}) = f\right) \\
\times \quad & Prob\left(rank(A^{j+1}) = f | \, rank(A^{j+1}D_{M-j+1}) = f\right) \\
+ \quad & Prob\left(rank(B^jZ^j) = z | \, rank(A^{j+1}) = f+1, rank(A^{j+1}D_{M-j+1}) = f\right) \\
\times \quad & Prob\left(rank(A^{j+1}) = f+1 | \, rank(A^{j+1}D_{M-j+1}) = f\right)
\end{aligned}$$

$Prob\left(rank(B^jZ^j) = z | \, rank(A^{j+1}) = f, rank(A^{j+1}D_{M-j+1}) = f\right) = \psi_{j-1}(f, z)$ since by Lemma 6

$$\begin{cases} rank(A^{j+1}) = f \\ rank(A^{j+1}D_{M-j+1}) = f \end{cases} \Rightarrow rank(A^{j+1}D^*_{M-j+1}) = 0$$

$Prob\left(rank(B^jZ^j) = z | \, rank(A^{j+1}) = f+1, rank(A^{j+1}D_{M-j+1}) = f\right) = \psi_{j-1}(f, z - 1)$ since by Lemma 6

$$\begin{cases} rank(A^{j+1}) = f+1 \\ rank(A^{j+1}D_{M-j+1}) = f \end{cases} \Rightarrow rank(A^{j+1}D^*_{M-j+1}) = 1$$

Then

$$Prob(rank(B^jZ^j) = z | F_{M-j+1} = D_{M-j+1}, rank(A^j) = f) = \psi_{j-1}(f, z)b_1 + \psi_{j-1}(f+1, z-1)b_2,$$

where b_1 and b_2 can be evaluated by Bayes formula as

$$\begin{aligned}
b_1 &= Prob\left(rank(A^{j+1}) = f | \, rank(A^{j+1}D_{M-j+1}) = f\right) \\
&= \frac{\frac{C-f}{C}\phi_{j-1}(f)}{\frac{C-f}{C}\phi_{j-1}(f) + \frac{f+1}{C}\phi_{j-1}(f+1)} \\
b_2 &= Prob\left(rank(A^{j+1}) = f+1 | \, rank(A^{j+1}D_{M-j+1}) = f\right) \\
&= \frac{\frac{f+1}{C}\phi_{j-1}(f+1)}{\frac{C-f}{C}\phi_{j-1}(f) + \frac{f+1}{C}\phi_{j-1}(f+1)}
\end{aligned}$$

2. $Prob(F_{M-j+1} = D_{M-j+1} | \, rank(A^j) = f)$

$Prob(F_{M-j+1} = D_{M-j+1} | \, rank(A^j) = f)$ can be computed by Bayes formula and conditioning on $rank(A^{j+1})$:

$$\begin{aligned} & Prob(F_{M-j+1} = D_{M-j+1} | \, rank(A^j) = f) \\ = \; & \frac{q \, Prob(rank(A^j) = f | F_{M-j+1} = D_{M-j+1})}{Prob(rank(A^j) = f)} \\ = \; & \frac{q \left(\frac{f+1}{C} \phi_{j-1}(f+1) + \frac{f}{C} \phi_{j-1}(f) \right)}{\phi_j(f)} \end{aligned}$$

3. $Prob(rank(B^j Z^j) = z | F_{M-j+1} = E_{M-j+1}, rank(A^j) = f)$

If $F_{M-j+1} = E_{M-j+1}$, $D^*_{M-j+1} = 0$, therefore,

$$\begin{aligned} & rank(A^{j+1} D^*_{M-j+1} Z_{M-j+1}) + \ldots + rank(F_M D^*_{M-1} Z_{M-1}) + rank(D^*_M Z_M) \\ = \; & rank(A^{j+2} D^*_{M-j+2} Z_{M-j+2}) + \ldots + rank(F_M D^*_{M-1} Z_{M-1}) + rank(D^*_M Z_M) \end{aligned}$$

Then

$$\begin{aligned} & Prob(rank(B^j Z^j) = z | F_{M-j+1} = E_{M-j+1}, rank(A^j) = f) \\ = \; & Prob\left(rank(B^j Z^j) = z | \, rank(A^{j+1}) = f, rank(A^{j+1} E_{M-j+1}) = f\right) \\ \times \; & Prob\left(rank(A^{j+1}) = f | \, rank(A^{j+1} E_{M-j+1}) = f\right) \\ + \; & Prob\left(rank(B^j Z^j) = z | \, rank(A^{j+1}) = f+1, rank(A^{j+1} E_{M-j+1}) = f\right) \\ \times \; & Prob\left(rank(A^{j+1}) = f+1 | \, rank(A^{j+1} E_{M-j+1}) = f\right) \\ = \; & \psi_{j-1}(f, z) b'_1 + \psi_{j-1}(f+1, z) b'_2, \end{aligned}$$

where b'_1 and b'_2 can be evaluated by Bayes formula as

$$\begin{aligned}
b'_1 &= Prob\left(rank(A^{j+1}) = f|\, rank(A^{j+1}E_{M-j+1}) = f\right) \\
&= \frac{\left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f)}{\left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f) + \frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1)} \\
b'_2 &= Prob\left(rank(A^{j+1}) = f+1|\, rank(A^{j+1}) = f\right) \\
&= \frac{\frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1)}{\left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f) + \frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1)}
\end{aligned}$$

4. $Prob(F_{M-j+1} = E_{M-j+1}|\, rank(A^j) = f)$

   $Prob(F_{M-j+1} = E_{M-j+1}|\, rank(A^j) = f)$ can be computed by Bayes formula and conditioning on $rank(A^{j+1})$:

$$\begin{aligned}
& Prob(F_{M-j+1} = E_{M-j+1}|\, rank(A^j) = f) \\
= \;& \frac{p\, Prob(rank(A^j) = f|F_{M-j+1} = E_{M-j+1})}{Prob(rank(A^j) = f)} \\
= \;& \frac{p\left(\frac{f(f+1)}{C(C-1)}\phi_{j-1}(f+1) + \left(1 - \frac{f(f-1)}{C(C-1)}\right)\phi_{j-1}(f)\right)}{\phi_j(f)}
\end{aligned}$$

5. $Prob(rank(B^jZ^j) = z|F_{M-j+1} = I, rank(A^j) = f)$

$$Prob(rank(B^jZ^j) = z|F_{M-j+1} = I, rank(A^j) = f) = \psi_{j-1}(f, z)$$

6. $Prob(F_{M-j+1} = I|\, rank(A^j) = f)$

$$\begin{aligned}
& Prob(F_{M-j+1} = I|\, rank(A^j) = f) \\
= \;& \frac{(1-p-q)\, Prob(rank(A^j) = f|F_{M-j+1} = I)}{Prob(rank(A^j) = f)} \\
= \;& \frac{(1-p-q)\phi_{j-1}(f)}{\phi_j(f)}
\end{aligned}$$

3.4.3 Proofs

Proof of Lemma 1. Consider $U, \tilde{U} \in \mathcal{C}$ such that $d(U, \tilde{U}) = \Delta$. If U is sent and E is chosen as a subspace of $\tilde{U} \cap U^c$, then $d(\tilde{U}, U') \leq d(U, U')$ for received subspace $U' = U \oplus E$. □

Proof of Theorem 2. We only need to consider the case of $2(t+\rho) = \Delta$ by the information processing inequality. The sink receives the subspace $\mathcal{H}_k(U) \oplus E$ with $t = \dim(E)$ and $\rho = (R-k)_+$ such that $2(t+\rho) = \Delta$. Suppose that instead of adding E, we subject $\mathcal{H}_k(U)$ to a further t deletions resulting in the subspace $\mathcal{H}_{k'}(\mathcal{H}_k(U))$, where $k' = k - t$. Since there are altogether $\Delta/2$ deletions and $r > (R - \Delta/2)/R$, the mincut bound is violated [5], so for some $U \in \mathcal{C}$ there exists some $\tilde{U} \neq U$ in $\mathcal{C}$ such that $d(\tilde{U}, \mathcal{H}_{k'}(\mathcal{H}_k(U))) \leq d(U, \mathcal{H}_{k'}(\mathcal{H}_k(U)))$, which implies $\mathcal{H}_{k'}(\mathcal{H}_k(U))$ is also a subspace of $\tilde{U}$. Then $\tilde{U} + \mathcal{H}_k(U)$ has dimension at most $R + t$. If E is chosen as a subspace of $\tilde{U} \cap U^c$, then

$$\begin{aligned}
& d(\tilde{U}, \mathcal{H}_k(U) \oplus E) \\
= \quad & \dim(\tilde{U} + (\mathcal{H}_k(U) \oplus E)) - \dim(\tilde{U} \cap (\mathcal{H}_k(U) \oplus E)) \\
\leq \quad & \dim(\tilde{U} + \mathcal{H}_k(U)) - \dim(\mathcal{H}_{k'}(\mathcal{H}_k(U)) \oplus E) \\
\leq \quad & R + t - (k' + t) = R - k'; \\
& d(U, \mathcal{H}_k(U) \oplus E) \\
= \quad & \dim(U + (\mathcal{H}_k(U) \oplus E)) - \dim(U \cap (\mathcal{H}_k(U) \oplus E)) \\
= \quad & \dim(U \oplus E) - \dim(\mathcal{H}_k(U)) = R + t - k = R - k'.
\end{aligned}$$

Thus, decoding is unsuccessful. □

Proof of Lemma 2. Note that we can arrange rows of Z so that

$$Z = \begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = \begin{pmatrix} Z_1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ Z_2 \end{pmatrix},$$

where the rows of W and Z_2 are linearly independent, and the rows of W and Z_1 are not. Then we have

$$\begin{aligned}
Y &= QW + BZ = QW + B_1 \begin{pmatrix} Z_1 \\ 0 \end{pmatrix} + B_2 \begin{pmatrix} 0 \\ Z_2 \end{pmatrix} && (3.13) \\
&= QW + Q_1 W + B_2 Z^* = (Q + Q_1) W + B_2 Z^* && (3.14)
\end{aligned}$$

for some adversarial matrices $Q_1 \in \mathbb{F}_q^{\nu \times R}$, $B_2 \in \mathbb{F}_q^{\nu \times L}$ and $Z^* = \begin{pmatrix} 0 \\ Z_2 \end{pmatrix}$, where the term $Q_1 W$ corresponds to adversarial erasures and $B_2 Z^*$ corresponds to adversarial errors.

Consider link i of the network. According to (3.13), when the link i is error and erasure free we can write the received subspace as

$$Y = rowspan(TW + BZ^*)$$

for some network transform $T \in \mathbb{F}_q^{\nu \times R}$ and network error transform $B \in \mathbb{F}_q^{\nu \times L}$. Let $F \in \mathbb{F}_q^{L \times L}$ be the matrix of local coding coefficients of the labeled line graph of $\mathcal{G}$. Then as discussed in [9], $T = A(I - F)^{-1}C$, where $A \in \mathbb{F}_q^{\nu \times L}$, $C \in \mathbb{F}_q^{L \times R}$ and I is an $L \times L$ identity matrix. For the adjacency matrix F, let F_{-i} be the matrix F with the ith row substituted by a zero row. For any network transfer matrix T define $T_{-i} \doteq A(I - F_{-i})^{-1}C$.

Consider three network scenarios of transmitting the row space of W (call them scenario 1 and scenario 2), that differ only at link i. Let Q be the network transform that the packet content of link i has undergone. Suppose that an adversarial packet $z_1 \in rowspan(T_{-i}W + B_{-i}Z^*)$ was injected into the link i in scenario 1 and an adversarial packet $z_2 \notin rowspan(T_{-i}W + B_{-i}Z^*)$ was injected into the link i in scenario 2. Let Y^1 and Y^2 be the received subspaces in scenarios 1 and 2 respectively. Then we can write

$$\begin{aligned} Y^1 &= rowspan(T_{-i}W + B_{-i}Z^* + Pz_1); \\ Y^2 &= rowspan(T_{-i}W + B_{-i}Z^* + Pz_2). \end{aligned}$$

Note that since z_2 is chosen to be linearly independent of $rowspan(T_{-i}W + B_{-i}Z^*)$, $z_1 \in Y^2$.

Let a_j and d_j be the number of additions and deletions respectively that the row space of W has suffered in scenario j. To match the decodability condition given in Theorems 1 and 2, define the decodability function as

$$f_{dec}(Y^j) \doteq a_j + d_j,$$

where a_j is the number of additions and d_j is the number of deletions from the received subspace Y^j.

Case 1. Suppose $P = 0$, then we have

$$f_{dec}(Y^1) = f_{dec}(Y^2) = f_{dec}(Y^3).$$

Case 2. Let $P \neq 0$. Suppose $z_1 \in Y^1$. Since $z_1 \in Y^2$, we have

$$Y^2 = span(Y^1 \bigcup \{z_2\}).$$

Therefore,

$$\begin{aligned} a_2 &= a_1 + 1 \\ d_2 &= d_1 \end{aligned}$$

and

$$f_{dec}(Y^1) \leq f_{dec}(Y^2).$$

Now suppose $z_1 \notin Y^1$. Since $z_1 \in Y^2$, we have

$$Y^2 = span(Y^1 \bigcup \{z_1, z_2\}).$$

Therefore,

$$\begin{aligned} a_2 &= \begin{cases} a_1 + 1, & \text{if } z_1 \in W; \\ a_2 + 2, & \text{if } z_1 \notin W \end{cases} \\ d_2 &= \begin{cases} d_1 - 1, & \text{if } z_1 \in W; \\ d_1, & \text{if } z_1 \notin W \end{cases} \end{aligned}$$

and

$$f_{dec}(Y^1) \leq f_{dec}(Y^2).$$

Thus, in both cases decodability in scenario 2 implies decodability in scenario 1.

We showed that for any link i the probability of successful decoding is minimized when the adversary injects an erroneous packet linearly independent from the packets currently present in $\mathcal{G}$. Hence, the statement of the lemma follows for any given set of adversarial links. □

Proof of Theorem 3. The received space spanned by the rows of Y has dimension $\mathrm{rank}(QW+BZ)$ including $\mathrm{rank}(BZ)$ linearly independent errors with a total of

$$R - (\mathrm{rank}(QW + BZ) - \mathrm{rank}(BZ))$$

deletions and $\mathrm{rank}(BZ)$ additions, thus, the result follows from Theorems 1 and 2. □

Proof of Lemma 3. Let $w_1, w_2 \dots w_R$ be the basis of $\mathrm{rowspan}(W)$.

- For any $j = 1 \dots M$, suppose that the node $(j-1)$ is in state $0 \le i < C - R$, that is, $a_{j-1}+d_{j-1} = i$. Note that $a_{j-1} \le i < C-R$, therefore, $dim(Y^{j-1}) < R+(C-R) = C$.

  Suppose that an error z, such that z is linearly independent of $span(Y^{j-1})$, occurs on the jth hop of $\mathcal{G}_M$. Then since $dim(Y^{j-1}) < C$ and RLC with high probability preserves the data rank [4], we have

  $$Y^j = rowspan(Y^{j-1} \bigcup \{z\})$$

  and

  $$\begin{aligned} a_j &= a_{j-1} + 1 \\ d_j &= d_{j-1} \end{aligned}$$

  with $a_j + d_j = i + 1$.

  Now suppose that an erasure occurs on the jth hop of $\mathcal{G}_M$. Since $dim(Y^{j-1}) < C$, the remaining links span Y^{j-1}. Therefore, after RLC is performed

  $$dim(Y^{j-1}) = dim(Y^j)$$

  with

  $$a_j + d_j = i.$$

Therefore,

$$\begin{aligned} P^j_{i,i} &= p + (1-p-s) = 1-s \\ P^j_{i,i+1} &= s \\ P^j_{i,k} &= 0 \text{ for } k \neq i, i+1 \end{aligned}$$

- For any $j = 1 \dots M$, suppose that the node $(j-1)$ is in state $i = C - R$ and that all nodes f for $f = 0 \dots j-2$ are in state $i_f < C - R$. We have just shown that it is only possible as a result of $C - R$ additions and 0 deletions. Then $w_1 \dots w_R, z_1 \dots z_{C-R}$ be can be chosen as a basis of Y^{j-1}, where z_l denotes the erroneous packets. Note that $dim(Y^{j-1}) = C$, and that after RLC is performed at node $(j-1)$, $w_1 \dots w_R, z_1 \dots z_{C-R}$ remains the basis of the subspace contained at node $(j-1)$.

  Note that in the case when neither errors nor erasures occur on the jth hop of $\mathcal{G}_M$, we have $dim(Y^j) = C$ and

$$Y^j = span(w_1 \dots w_R, z_1 \dots z_{C-R}) \tag{3.15}$$

or

$$Y^j = span(p^j_1, \dots, p^j_C). \tag{3.16}$$

Suppose that an error z, such that z is linearly independent of $span(Y^{j-1})$, occurs on the jth hop at the mth link of $\mathcal{G}_M$. Since p^j_m is replaced by z in (3.16), z also has to replace w_f for some $f = 1 \dots R$ in (3.15) and the basis of Y^j becomes $w_1 \dots, w_{f-1}, w_{f+1}, \dots, w_R, z_1 \dots z_{C-R}, z$. Thus,

$$\begin{aligned} a_j &= C - R + 1 \\ d_j &= 1 \end{aligned}$$

with $a_j + d_j = i + 2$.

If an erasure occurs on the jth hop at the mth link of $\mathcal{G}_M$, p^j_m is eliminated from (3.16), and, correspondingly, for some $f = 1 \dots R$ w_f has to be eliminated from (3.15). Then the basis of Y^j becomes $w_1 \dots, w_{f-1}, w_{f+1}, \dots, w_R, z_1 \dots z_{C-R}$. Hence,

$$\begin{aligned} a_j &= C-R \\ d_j &= 1 \end{aligned}$$

with $a_j + d_j = i + 1$.

Therefore,

$$\begin{aligned} P^j_{i,i} &= 1-p-s \\ P^j_{i,i+1} &= p \\ P^j_{i,i+2} &= s \\ P^j_{i,k} &= 0 \text{ for } k \neq i, i+1, i+2 \end{aligned}$$

- For any $j = 1 \dots M$, suppose that the node $(j-1)$ is in state $i = C - R + 1$ and that all nodes f for $f = 0 \dots j-2$ are in state $i_f < C - R + 1$. We have just shown that it is only possible as a result of $C - R$ additions and 1 deletion. Without of loss of generality $w_1 \dots w_{R-1}, z_1 \dots z_{C-R}$ be can be chosen as a basis of Y^{j-1}, where z_l denotes the erroneous packets. Note that $dim(Y^{j-1}) = C - 1 < C$. Thus, the above described reasoning for the case when $i < C-R$can be applied to prove the statement of the lemma.

  Similarly, by incrementing m from 1 to $R-1$, we can observe that for any node $j-1$ in a state $i = C - R + 2m$, such that all nodes f for $f = 0 \dots j-2$ are in state $i_f < C - R + 2m$, the state $C - R + 2m$ can only be reached as a result of $C - R + m$ additions and m deletions and that $dim(Y^{j-1}) = C$. Therefore, the reasoning for the case when $i = C - R$ can be used. For any node $j-1$ in a state $i = C - R + 2m + 1$, such that all nodes f for $f = 0 \dots j-2$ are in state $i_f < C - R + 2m + 1$, note that the state $C - R + 2m + 1$ can only be reached as a result of $C - R + m$ additions and $m + 1$ deletions and that $dim(Y^{j-1}) = C - 1$. Hence, the reasoning for the case when $i = C - R + 1$ can be used.

- At last, suppose that for any $j = 1 \dots M$ the node $(j-1)$ is in state $i = C + R$, that is, $\mathcal{G}_{\mathcal{M}}$ has suffered C additions and R deletions. Hence, the basis of Y^{j-1} can be chosen as $z_1, z_2 \ldots z_C$, where all z_l are erroneous packets. Observe that $dim(Y^{j-1}) = C$, and that as a result of RLC performed at node $(j-1)$, $z_1, z_2 \ldots z_C$ remains the basis of the subspace contained at node $(j-1)$.

Note that $Y^{j-1} \bigcap W = \emptyset$ and that by the mincut restriction we require that $a_j \leq C$. Therefore, if a new error occurs at the jth hop, the state of node j will remain the same, i.e., $a_j + d_j = a_{j-1} + d_{j-1} = C + R$.

Note that in the case when neither errors nor erasures occur on the jth hop of $\mathcal{G}_M$, we have $dim(Y^j) = C$ and

$$Y^j = span(z_1 \ldots z_C) = span(p_1^j, \ldots, p_C^j). \tag{3.17}$$

Hence, if p_m^j is erased at the jth hop, for some $f = 1 \ldots C$ z_f is eliminated from the basis of Y^j. Therefore,

$$\begin{aligned} a_j &= a_{j-1} - 1 = C - 1 \\ d_j &= d_{j-1} + R \end{aligned}$$

and $a_j + d_j = C + R - 1$.

In summary, when $i = C + R$,

$$\begin{aligned} P_{i,i-1}^j &= p \\ P_{i,i}^j &= 1 - p \\ P_{i,k}^j &= 0 \text{ for } k \neq i-1, i \end{aligned}$$

□

Proof of Lemma 4. From (3.6)

$$BZ = F_M \ldots F_2 D_1^* Z_1 + \ldots + F_M D_{M-1}^* Z_{M-1} + D_M^* Z_M. \tag{3.18}$$

In order to prove (3.7), we will show that the indices of the nonzero rows of $F_M \ldots F_2 D_1^* Z_1, \ldots, F_M D_{M-1}^* Z_{M-1}$ and $D_M^* Z_M$ are mutually disjoint, hence, the statement follows. Take any $i, j = 1 \ldots M$ such that $i < j$ and both $D_i^* Z_i$ and $D_j^* Z_j$ are nonzero matrices. Consider

$$F_M \dots F_{j+1} D_j^* Z_j = F_M \dots F_{j+1}(I - D_j) Z_j$$

and

$$F_M \dots F_{j+1} D_j F_{j-1} \dots F_{i+1} D_i^* Z_i = F_M \dots F_{j+1} D_j F_{j-1} \dots F_{i+1}(I - D_i) Z_i.$$

By definition, matrix $(I - D_j)Z_j$ has one nonzero row (let it be mth row). $F_M \dots F_{j+1}$ is a matrix whose rows can be unit and zero vectors. If the kth row of $F_M \dots F_{j+1}$ has 1 in the mth column, after right multiplication by any matrix X, the mth row of X will become the kth row of $F_M \dots F_{j+1}X$. Therefore, if no row of $F_M \dots F_{j+1}$ has 1 in the mth column, $F_M \dots F_{j+1} D_j^* Z_j$ is a zero matrix and the statement follows trivially. If rows $k_1 \dots k_l$ of $F_M \dots F_{j+1}$ have 1 in the mth column, then the rows $k_1 \dots k_l$ of $F_M \dots F_{j+1} D_j^* Z_j$ are the only rows that are nonzero. On the other hand, the nonzero rows of $(I - D_j)Z_j$ correspond to zero rows of $D_j X$ for any matrix X. Hence, the mth row of $D_j F_{j-1} \dots F_{i+1}(I - D_i)Z_i$ is a zero row and rows $k_1 \dots k_l$ of $F_M \dots F_{j+1} D_j F_{j-1} \dots F_{i+1}(I - D_i)Z_i$ are zero rows. Therefore, the nonzero rows of $F_M \dots F_{j+1} D_j^* Z_j$ and $F_M \dots F_{j+1} D_j F_{j-1} \dots F_{i+1} D_i^* Z_i$ are mutually disjoint and the statement of the lemma follows.

Recall the expansion of BZ into (3.18). To prove (3.8), we will show that the indices of the nonzero rows of ASW , $F_M \dots F_2 D_1^* Z_1, \dots, F_M D_{M-1}^* Z_{M-1}$ and $D_M^* Z_M$ are mutually disjoint, hence, the statement follows. Take any $i = 1 \dots M$ such that $D_i^* Z_i$ is a nonzero matrices. Consider

$$F_M \dots F_{i+1} D_i^* Z_i = F_M \dots F_{i+1}(I - D_i) Z_i.$$

Rewrite ASW as:

$$ASW = F_M \dots F_{i+1} D_i F_i \dots F_1.$$

Now use the reasoning of the proof of (3.7) to see that all nonzero rows of ASW and

$F_M \ldots F_{i+1} D_i^* Z_i$ are mutually disjoint. Since it holds for any i, we have:

$$\begin{aligned} rank(ASW + BZ) &= rank(ASW + F_M \ldots F_2 D_1^* Z_1 + \ldots + F_M D_{M-1}^* Z_{M-1} + D_M^* Z_M) \\ &= rank(ASW) + rank(F_M \ldots F_2 D_1^* Z_1 + \ldots + F_M D_{M-1}^* Z_{M-1} + D_M^* Z_M) \\ &= rank(ASW) + rank(BZ). \end{aligned}$$

Since S is a random linear coding matrix, any R rows of SW are with high probability linearly independent. (3.9) follows from combining this with the fact that for FRR A is a matrix whose rows can only be zero and unit vectors. □

Proof of Lemma 5. $F_j \ldots F_2$ is a matrix whose rows can be unit and zero vectors. Suppose that the kth row of D_1 is a zero row. If the ith row of $F_j \ldots F_2$ has 1 in the kth column, after multiplication with D_1, the kth row of D_1 will become the ith row of $F_j \ldots F_2 D_1$. $rank(F_j \ldots F_2) = f + 1$ means that $F_j \ldots F_2$ has $f + 1$ distinct unit rows; therefore, $rank(F_j \ldots F_2 D_1) = f$ only if one of the $f + 1$ distinct unit rows of $F_j \ldots F_2$ has 1 in the kth column. Thus,

$$Prob\left(rank(F_j \ldots F_2 D_1) = f \,|\, rank(F_j \ldots F_2) = f + 1\right) = \sum_{i=1}^{f+1} \frac{1}{C} = \frac{f+1}{C}$$

□

Proof of Lemma 6. According to the proof of Lemma 5, if $rank(F_j \ldots F_2) = f + 1$ and the kth row of D_1 is a zero row, $rank(F_j \ldots F_2 D_1) = f$ only if one of the $f + 1$ distinct unit rows of $F_j \ldots F_2$ has 1 in the kth column. Thus, $F_j \ldots F_2 D_1^*$ will have one non-zero row.

Similarly, if $rank(F_j \ldots F_2) = f$ and the kth row of D_1 is a zero row, $rank(F_j \ldots F_2 D_1) = f$ only if none of the f distinct unit rows of $F_j \ldots F_2$ have 1 in the kth column. Thus, $F_j \ldots F_2 D_1^*$ will have only zero rows. □

Proof of Lemma 7. $F_j \ldots F_2$ is a matrix whose rows can be unit and zero vectors. If the ith row of $F_j \ldots F_2$ has 1 in the kth column, after multiplication the kth row of E_1 will become the ith row of $F_j \ldots F_2 E_1$. $rank(F_j \ldots F_2) = f + 1$ means that $F_j \ldots F_2$ has $f + 1$ distinct unit rows. Suppose the two replicas of the only non-unique unit row of E_1 are located in rows r_1 and r_2. $rank(F_j \ldots F_2 E_1) = f$ only if one of the $f + 1$ distinct unit rows of $F_j \ldots F_2$

has 1 in r_1th column and another one has 1 in r_2th column. Thus,

$$Prob\,(rank(F_j \dots F_2 E_1) = f \,|\, rank(F_j \dots F_2) = f+1) = \sum_{i=1}^{f+1} \frac{1}{C} \sum_{k=1}^{f} \frac{1}{C-1} = \frac{f(f+1)}{C(C-1)}.$$

□

Proof of Lemma 8. Consider two network scenarios for $\mathcal{G}_n$ with the same error and erasure patterns (call than scenario 1 and scenario 2). Let R_i^1 be the rank of information packets transmitted on P_i in scenario 1 and let R_i^2 be the rank of information packets transmitted on P_i in scenario 2. Suppose $R_i^1 = C_i$ and $R_i^2 < C_i$. Let $\mathcal{P}_j$ denote the probability of successful decoding in scenario j, $j = 1, 2$. Our goal is to show that

$$\mathcal{P}_2 \leq \mathcal{P}_1. \tag{3.19}$$

According to Theorem 3

$$\mathcal{P}_j = Prob(R - rank(AS_jW + BZ) + 2\,rank(BZ) \leq y - 1),$$

where $S_j = \begin{pmatrix} H_j^1 G_j^1 \\ H_j^2 G_j^2 \\ \dots \\ H_j^n G_j^n \end{pmatrix}$ is the source coding matrix for scenario j. Note that by assumption for each i, $rank(H_1^i G_1^i W) = C_i$ and $rank(H_2^i G_2^i W) < C_i$.

For fixed A, B and Z, (3.19) holds iff

$$rank(AS_2W + BZ) \leq rank(AS_1W + BZ). \tag{3.20}$$

Note also that

$$rank(AS_jW) = min(\sum_{i=1}^{n} rank(A^i H_j^i G_j^i W), R). \tag{3.21}$$

In case of RLC, each A^i, $i = 1 \dots n$, is with high probability a square matrix of full rank; hence, for any matrix X, $rank(A^i X) = rank(X)$. Therefore, since for each i, $rank(H_2^i G_2^i W) \leq rank(H_1^i G_1^i W)$, we have $rank(A^i H_2^i G_2^i W) \leq rank(A^i H_1^i G_1^i W)$; hence by

(3.21) $rank(AS_2W) \leq rank(AS_1W)$. Let $r_1 = rowspace(AS_1W)$ and $r_2 = rowspace(AS_2W)$ with $r_1 \leq r_2$. Since RLC is performed at $\mathcal{S}$ and each non-source node of $\mathcal{G}_n$, every row of AS_1W is a random linear combination of r_1 rows of W and every row of AS_2W is a random linear combination of r_2 rows of W. Using this along with the fact that the rows of W and Z are mutually linearly independent, we have

$$rowspace(AS_2W) \subseteq rowspace(AS_1W)$$

and

$$rowspace(AS_2W + BZ) \subseteq rowspace(AS_1W + BZ).$$

In case of FRR, by Lemma 4 we have $rank(AS_jW + BZ) = rank(AS_jW) + rank(BZ)$. Therefore, in order to show (3.20) we need to show that $rank(AS_2W) \leq rank(AS_1W)$. Since for each i, $rank(H_2^iG_2^iW) \leq rank(H_1^iG_1^iW)$ and for FRR A^i is the matrix whose rows can only be zero and unit vectors and RLC is performed at the source, we have $rank(A^iH_2^iG_2^iW) \leq rank(A^iH_1^iG_1^iW)$; hence by (3.21) $rank(AS_2W) \leq rank(AS_1W)$. Therefore, (3.19) holds. □

Proof of Lemma 9. (3.11) is a direct consequence of the fact that $rank(BZ) = \sum_{i=1}^{n} rank(B^iZ^i)$ and the assumption that all error packets are linearly independent.

By assumption of the model on each P_i, $i = 1 \ldots n$, we have $R_i = C_i$. Define $r_i \doteq R_i - d_i = C_i - d_i$ to be the rank of information packets received on each P_i. Then the total rank of information packets received at $\mathcal{T}$ is equal to:

$$min(\sum_{i=1}^{n} r_i, R) = min(C - \sum_{i=1}^{n} d_i, R).$$

Hence,

$$d = \begin{cases} 0, & \text{if } R \leq C - \sum_{i=1}^{n} d_i \ ; \\ \sum_{i=1}^{n} d_i - (C - R), & \text{if } R > C - \sum_{i=1}^{n} d_i. \end{cases}$$

□

Chapter 4

Combining information-theoretic and cryptographic network error correction in a probabilistic setting

4.1 Introduction

In this chapter we consider the problem of adversarial errors in single-source multicast networks with limited computational power (e.g., wireless or sensor networks). Most existing results on information theoretic multicast network error correction assume a given bound on the number of adversarial errors (see [13, 31]), for which random linear network coding achieves capacity [7]. If z is the upper bound on the number of errors that can occur in the network, noncoherent network coding is used at all nodes and m is the minimum cut of the network, the error correcting code that achieves information rate $m-2z$ can be constructed [13].

An alternative approach to network error correction is equipping each network packet with a cryptographic signature (see [11, 12]). Then, if each network node checks all packets and all nodes perform network coding, for any number of network errors z_a the information rate $m - z_a$ can be achieved in multicast network scenarios without the need for further information-theoretic error correction. However, performing signature checks at all network nodes may limit throughput in a network with limited computational resources, since such cryptographic operations are typically more expensive than network coding operations. Therefore, we are interested in combining the benefits of both approaches. We consider probabilistic verification of a subset of packets in conjunction with information-theoretic redundancy so as to achieve intermediate information rates r with

$$m - 2z \leq r \leq m - z_a$$

subject to computational budget constraints at each node.

In order to solve this problem, we need to develop a framework to use network error correction in a probabilistic setting. In existing network error correcting algorithms, the deterministic bound on the number of erroneous packets needs to be known in advance for code construction [13]. This can result in a very conservative upper bound when packets are checked probabilistically. In this chapter we propose a fountain-like network error correcting code construction that can be used in networks where the upper bound on the number of errors is unknown a priori [25]. Instead of including a fixed number of redundant bits in each packet, we incrementally add redundancy until decoding succeeds.

4.2 Model

Let $\mathcal{G}$ be an acyclic multicast network with source $\mathcal{S}$ and sink $\mathcal{T}$. Let m be the minimum cut of $\mathcal{G}$. The nodes of $\mathcal{G}$ are limited in computational power and outgoing capacity. Let n be the number of nodes in $\mathcal{G}$. Errors can occur on some links of $\mathcal{G}$.

Let N^i_{in} be the number of packets incoming to node i, and let N^i_{out} be the number of packets outgoing from node i. Let A_i be the computational budget available at node i. Given A_i, we assume that in addition to forwarding all outgoing packets, each node i has the capacity to check a fraction ρ_i of incoming packets and to form a fraction γ_i of outgoing packets by creating random linear combinations of packets incoming to node i, so that

$$\rho_i N^i_{in} + \gamma_i N^i_{out} \leq A_i.$$

Let $\overrightarrow{\rho} = (\rho_1, \rho_2, \ldots, \rho_n)$ be the vector that defines the checking strategy at nodes of $\mathcal{G}$. Let $\overrightarrow{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n)$ be the vector that defines the network coding strategy at nodes of $\mathcal{G}$. Let $\overrightarrow{A} = (A_1, A_2, \ldots, A_n)$ be the vector of computational budgets available at nodes of $\mathcal{G}$. Let

$$\Sigma = \{\overrightarrow{\rho}, \overrightarrow{\gamma} \mid \overrightarrow{\rho}, \overrightarrow{\gamma} \text{ are feasible for a given } \overrightarrow{A}\}$$

be the set of all strategies feasible at nodes of $\mathcal{G}$ for a given budget constraint $\overrightarrow{A}$. Let $r_\sigma(\overrightarrow{A})$ be the information rate that can be achieved for a given $\sigma \in \Sigma$ and $\overrightarrow{A}$.

In this chapter, we focus on how to construct the error correcting code that achieves $r_\sigma(\overrightarrow{A})$ for a given $\sigma \in \Sigma$. For each $\sigma \in \Sigma$ the number of erroneous packets available at the sink is unknown in advance; therefore, we want to construct a code that can adapt to the actual number of errors present at the sink. Moreover, if an erroneous packet injected to link l remains unchecked due to computational budget constraints and random linear coding is performed, any subsequent signature check will identify packets contained on links downstream of l as erroneous and will eliminate them. Therefore, we require that the code that we construct be applicable in any network with an unknown, time-varying minimum cut and number of errors.

4.3 Main result

Throughout this section, we use the following notation. For any matrix A, let rows(A) denote the set of vectors that form rows of A. Let I_a denote an $a \times a$ identity matrix. Also, let $\mathbf{i_a}$ denote an $a^2 \times 1$ vector that is obtained by stacking columns of I_a one after the other. Let $\mathbb{F}_q$ be the finite field over which coding occurs. Each source packet contains K symbols from $\mathbb{F}_q$.

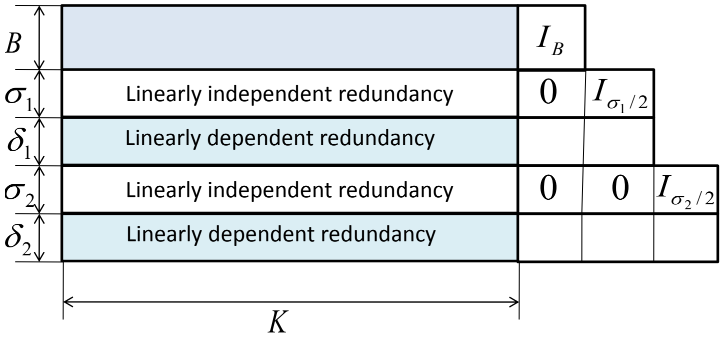
4.3.1 Encoder

In each block $\mathcal{S}$ transmits BK independent information symbols from $\mathbb{F}_q$ to $\mathcal{T}$. Let W be a $B \times K$ matrix whose elements are the information symbols. The source transmits rows(X_0), where $X_0 = \begin{pmatrix} W & I_B \end{pmatrix}$. Suppose that while transmitting rows(X_0) by means of random linear network coding, the network has incurred $z_0 > 0$ errors. Then since there are z_0 additions and $d_0 = B - z_0$ deletions to/from rowspace(X_0), $\mathcal{T}$ would not be able to recover X_0.

By [5], if there are $d_0 = B - z_0$ deletions and no additions from rowspace(X_0), sending $\delta = d_0$ additional linear combinations of rows(X_0) ensures successful decoding. Similarly, by [13], in case of z_0 additions and no deletions, sending $\sigma K > z_0 K$ redundant bits helps to decode. By making use of the two above-mentioned ideas, we propose an iterative algorithm that resembles a "digital error fountain" by incrementally adding redundancy, that ensures decoding of the source packets in finite number of iterations.

An end to end error detection scheme is needed so that the sink can determine when decoding is successful. For instance, the source can include a cryptographic signature, e.g. [12], in each packet. Upon failing to decode X_0 successfully from the initial transmission, $\mathcal{S}$ sends an additional batch of σ_1 linearly independent redundant packets and δ_1 linearly dependent redundant packets, and $\mathcal{T}$ attempts to decode using both the initial and the redundancy batch. Additional batches of redundant symbols are transmitted until decoding succeeds, whereupon the sink sends feedback telling the source to move onto the next batch.

The ith stage of the reencoding algorithm can be generalized as follows (see Fig. 4.1):



B
σ_1
δ_1
σ_2
δ_2
K
I_B
Linearly independent redundancy
0
$I_{\sigma_1/2}$
Linearly dependent redundancy
Linearly independent redundancy
0
0
$I_{\sigma_2/2}$
Linearly dependent redundancy

Figure 4.1: Code construction.

- For some $M > 0$, let $\sigma_i = M/2$. The encoder arranges the matrix of information symbols W in an $BK \times 1$ vector $\mathbf{w}$. Let S_i be a $\sigma_i K \times BK$ random matrix known to everyone. Define a vector of redundant symbols $\mathbf{y_i}$ as

$$\mathbf{y_i} = S_i\mathbf{w} \text{ or, equivalently,}$$
$$\begin{pmatrix} S_i & -I_{\sigma_i K} \end{pmatrix} \begin{pmatrix} \mathbf{w} \\ \mathbf{y_i} \end{pmatrix} = 0. \tag{4.1}$$

After computing $\mathbf{y_i}$, the encoder arranges it into a $\sigma_i \times (K + (i+1)M)$ matrix Y_i column by column. Set

$$A_i^1 = \begin{pmatrix} Y_i^1 & 0 & I_{\sigma_i} \end{pmatrix}, \tag{4.2}$$

where 0 is a $\sigma_i \times (B + (i-1)M)$ matrix with zero entries.

- Let $\delta_i = M/2$. Let D_i be a $\delta_i \times \left(B + \sum_{j=1}^{i} \sigma_j\right)$ matrix with random entries from $\mathbb{F}_q$. Define a $\delta_i \times (K + (B + iM))$ matrix A_i^2 as

$$A_i^2 = D_i \left(\begin{array}{ccccc} X_0 & 0 & 0 & \dots & 0 \\ \cline{1-2} \multicolumn{2}{c}{A_1^1} & 0 & \dots & 0 \\ \cline{1-3} \multicolumn{3}{c}{A_2^1} & \dots & 0 \\ \multicolumn{5}{c}{\dots} \\ \hline \multicolumn{5}{c}{A_i^1} \end{array}\right). \tag{4.3}$$

- At the ith stage, the source transmits $X_i = \begin{pmatrix} A_i^1 \\ A_i^2 \end{pmatrix}$.

4.3.2 Decoder

Let z_i be the number of errors, i.e., the number of packets corrupted by the adversary, at the ith stage. Let Z_i be the matrix whose rows are the error packets injected to the network at the ith stage that are linearly independent of the X_i packets, i.e., rowspace$(X_i) \cap$ rowspace$(Z_i) = 0$. Let

$$Y_i = T_i X_i + Q_i Z_i \tag{4.4}$$

be the matrix, such that rows(Y_i) are the packets received at $\mathcal{T}$ at the ith stage, where T_i is the transfer matrix from all links in $\mathcal{G}$ to the packets received at $\mathcal{T}$, and Q_i is the transfer matrix from error packets to the packets received at $\mathcal{T}$ at the ith stage. For notational convenience, define

$$
\begin{aligned}
Y^i &= \begin{pmatrix} Y_0 \\ Y_1 \\ \dots \\ Y_i \end{pmatrix} \quad T^i = \begin{pmatrix} T_0 & 0 & \dots & 0 \\ 0 & T_1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & T_i \end{pmatrix} \\
Q^i &= \begin{pmatrix} Q_0 & 0 & \dots & 0 \\ 0 & Q_1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & Q_i \end{pmatrix} \\
X^i &= \left(\begin{array}{ccccc} X_0 & 0 & 0 & \dots & 0 \\ \cline{1-2} \multicolumn{2}{c}{X_1} & 0 & \dots & 0 \\ \cline{1-3} \multicolumn{3}{c}{X_2} & \dots & 0 \\ \multicolumn{5}{c}{\dots} \\ \hline \multicolumn{5}{c}{X_i} \end{array} \right) \\
Z^i &= \left(\begin{array}{ccccc} Z_0 & 0 & 0 & \dots & 0 \\ \cline{1-2} \multicolumn{2}{c}{Z_1} & 0 & \dots & 0 \\ \cline{1-3} \multicolumn{3}{c}{Z_2} & \dots & 0 \\ \multicolumn{5}{c}{\dots} \\ \hline \multicolumn{5}{c}{Z_i} \end{array} \right)
\end{aligned}
$$

Note that for any i we can write

$$Y^i = T^i X^i + Q^i Z^i.$$

The source transmits at the minimum cut rate m. Thus, X_0 is transmitted in $N_B = \frac{B}{m}$ time units and each X_i, $i = 1, 2, \dots$ is transmitted in $N_M = \frac{M}{m}$ time units. For each $j = 1, 2, \dots, B$ denote the part of X_0 transmitted at the jth time unit by X_0^j. Similarly, for each $j = 1, 2, \dots, M$, $i = 1, 2, \dots$ denote the part of X_i by transmitted at the jth time unit by X_i^j. For each i, j, define E_i^j to be a random variable that corresponds to the number of errors that occurred in $\mathcal{G}$ while transmitting X_i^j. Define $E_0 = \sum_{j=1}^{N_B} E_i^j$ and $E_i = \sum_{j=1}^{N_M} E_i^j$, $i = 1, 2, \dots$. Recall that $\sigma_i = \delta_i = \frac{M}{2}$.

Lemma 10. *Suppose that for each i, j, there exists $\epsilon_i^j > 0$ such that*

$$\mathbb{E}[E_i^j] < \frac{m}{2} - \epsilon_i^j. \tag{4.5}$$

Then for some finite N, we will have

$$\sum_{i=0}^{N} z_i < \sum_{i=1}^{N} \delta_i \tag{4.6}$$

$$\sum_{i=0}^{N} z_i < \sum_{i=1}^{N} \sigma_i \tag{4.7}$$

Proof. See Section 4.4.2. □

Lemma 11. *If*

$$\sum_{i=0}^{N} z_i \leq \sum_{i=1}^{N} \delta_i, \tag{4.8}$$

then with high probability columns of T^N and Q^N span disjoint vector spaces.

Proof. See Section 4.4.2. □

Let N be such that conditions (4.6)-(4.7) are satisfied. Then in order to decode, we need to solve the following system of linear equations:

$$Y^N = T^N X^N + Q^N Z^N \tag{4.9}$$

$$\begin{pmatrix} S_1 & -I_{\frac{MK}{2}} & \dots & 0 \\ S_2 & 0 & \dots & 0 \\ & & \dots & \\ S_N & 0 & \dots & -I_{\frac{MK}{2}} \end{pmatrix} \begin{pmatrix} \mathbf{w} \\ \mathbf{y_1} \\ \dots \\ \mathbf{y_N} \end{pmatrix} = 0 \tag{4.10}$$

Theorem 4. *Let N be such that equations (4.6) and (4.7) are satisfied. Then with probability greater than $1 - q^{-\epsilon K}$, the system of linear equations (4.9)-(4.10) can be solved for* $\mathbf{x}$.

Proof. See Section 4.4.2. □

Theorem 5. *For each i, j, let E_i^j be random variables with the same mean such that (4.5) is satisfied. Let N be such that equations (4.6)-(4.7) are satisfied. Then the above-described* *code construction achieves the information rate*

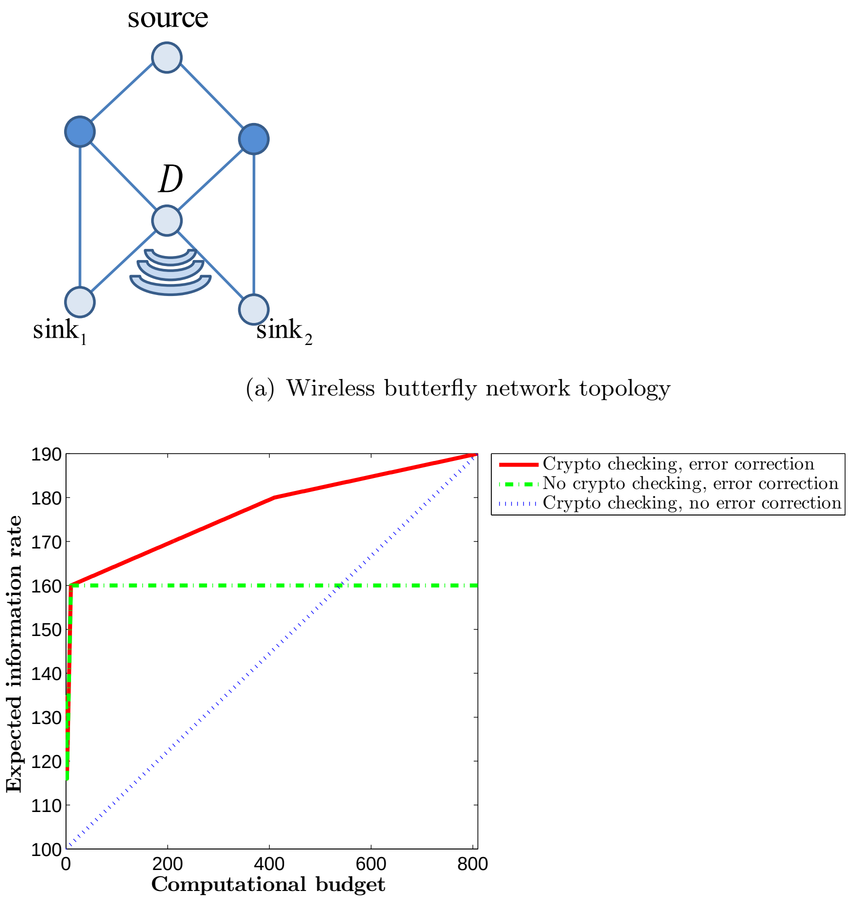
$$r \leq M_A - 2\mathbb{E}[E_0^1] - \epsilon, \tag{4.11}$$

where M_A is the average throughput of linearly independent packets, and ϵ decreases with increasing B.

Proof. See Section 4.4.2. □

4.4 Examples and proofs

4.4.1 Example: wireless butterfly network



(a) Wireless butterfly network topology

(b) Expected information rate for network of Fig. 4.2(a) with equal capacity links, minimum cut $= 200$, $z = 20$, $\frac{\text{cost of coding}}{\text{cost of checking}} = \frac{1}{40}$.

Figure 4.2: Example: wireless butterfly network example

To illustrate our ideas, we consider a wireless butterfly network where a computationally limited network coding node D receives z adversarial packets (see Figure 4.2(a)). For a varying computational budget constraint, we compare three strategies: when network error correction is performed without cryptographic checking, when cryptographic checking is performed without network error correction, and when both cryptographic checking and network error correction are performed. We derived analytical expressions for the expected information rate for all three strategies, which are plotted in Figure 4.2(b). Note that using our code construction the expected information rate can be approached. Our hybrid strategy outperforms both pure ones, since the decision node favors coding over checking for small budget constraints, and checking over coding for larger computational budgets.

4.4.2 Proofs

Proof of Lemma 4.5. Let $\epsilon = \min\limits_{i,j} \epsilon_i^j$. Note that

$$\begin{aligned} \mathbb{E}[E_0] &= \sum_{j=1}^{N_B} \mathbb{E}[E_0^j] < \frac{B}{2} - \epsilon N_B < \frac{B}{2} \\ \mathbb{E}[E_i] &= \sum_{j=1}^{N_M} \mathbb{E}[E_i^j] < \frac{M}{2} - \epsilon N_M, i = 1, 2, \ldots \end{aligned}$$

Then for $L^* > \frac{B}{2\epsilon N_M}$

$$\begin{aligned} \sum_{i=0}^{L^*} \mathbb{E}[E_i] &< \mathbb{E}[E_0] + \frac{ML^*}{2} - L^* \epsilon N_M \\ &< \frac{B}{2} + \frac{ML^*}{2} - L^* \epsilon N_M < \frac{ML^*}{2}. \end{aligned}$$

Therefore, for some finite $N > L^*$, we will have

$$\sum_{i=0}^{N} z_i \leq \sum_{i=0}^{N} \mathbb{E}[E_i] < \frac{MN}{2}, \tag{4.12}$$

hence, we have $\sum\limits_{i=0}^{N} z_i < \sum\limits_{i=1}^{N} \delta_i$ and $\sum\limits_{i=0}^{N} z_i < \sum\limits_{i=1}^{N} \sigma_i$. □

Proof of Lemma 11. Note that $\sum\limits_{i=1}^{N} \delta_i + \sum\limits_{i=1}^{N} \sigma_i + B = NM + B$. Then by adding $\sum\limits_{i=1}^{N} \sigma_i + B$

to both sides of (4.8), we get

$$\sum_{i=0}^{N} z_i + \sum_{i=1}^{N} \sigma_i + B \leq NM + B,$$

or

$$\operatorname{rank}(X^N) + \operatorname{rank}(Z^N) \leq Nm + B.$$

Therefore, if the error packets were replaced by additional source packets, the total number of source packets would be at most $NM + B$. By [4], with high probability, random linear network coding allows $\mathcal{T}$ to decode all source packets. This corresponds to $\begin{pmatrix} T^N & Q^N \end{pmatrix}$ having full column rank, hence, column spaces of T^N and Q^N being disjoint except in the zero vector. □

Proof of Theorem 4. The proof of this theorem is constructive and is similar to [13]. Note that

$$X^N = \left(\begin{array}{ccccc} X_0 & 0 & 0 & \dots & 0 \\ \cline{1-2} \multicolumn{2}{c}{X_1} & 0 & \dots & 0 \\ \cline{1-3} \multicolumn{3}{c}{X_2} & \dots & 0 \\ \multicolumn{5}{c}{\dots} \\ \hline \multicolumn{5}{c}{X_N} \end{array}\right) = \left(\begin{array}{ccccc} X_0 & 0 & 0 & \dots & 0 \\ \cline{1-2} \multicolumn{2}{c}{A_1^1} & 0 & \dots & 0 \\ \multicolumn{2}{c}{A_1^2} & 0 & \dots & 0 \\ \cline{1-3} \multicolumn{3}{c}{A_2^1} & \dots & 0 \\ \multicolumn{3}{c}{A_2^2} & \dots & 0 \\ \multicolumn{5}{c}{\dots} \\ \hline \multicolumn{5}{c}{A_N^1} \\ \multicolumn{5}{c}{A_N^2} \end{array}\right).$$

Define

$$\begin{aligned} X \quad &= \left(\begin{array}{ccccc} X_0 & 0 & 0 & \dots & 0 \\ \cline{1-2} \multicolumn{2}{c}{A_1^1} & 0 & \dots & 0 \\ \cline{1-3} \multicolumn{3}{c}{A_2^1} & \dots & 0 \\ \multicolumn{5}{c}{\dots} \\ \hline \multicolumn{5}{c}{A_N^1} \end{array}\right) \\ &= \begin{pmatrix} W & I_B & 0 & \dots & 0 \\ Y_1 & 0 & I_{M/2} & \dots & 0 \\ & & \dots & & \\ Y_N & 0 & 0 & \dots & I_{M/2} \end{pmatrix} \end{aligned} \tag{4.13}$$

Let $0_{a,b}$ denote a zero matrix with a rows and b columns. Note that by (4.3) $X^N = D^N X$, where

$$D^N = \left(\begin{array}{ccccc}
I_B & 0_{B,M/2} & 0_{B,M/2} & \cdots & 0_{B,M/2} \\
0_{M/2,B} & I_{M/2} & 0_{M/2,M/2} & \cdots & 0_{M/2,M/2} \\ \cline{1-2}
\multicolumn{2}{c}{D_1} & 0_{M/2,M/2} & \cdots & 0_{M/2,M/2} \\ \cline{1-2}
0_{M/2,B} & I_{M/2} & 0_{M/2,M/2} & \cdots & 0_{M/2,M/2} \\ \cline{1-3}
\multicolumn{3}{c}{D_2} & \cdots & 0_{M/2,M/2} \\ \cline{1-3}
\cdots & \cdots & \cdots & \cdots & \cdots \\
0_{M/2,B} & 0_{M/2,M/2} & 0_{M/2,M/2} & \cdots & I_{M/2} \\ \hline
\multicolumn{5}{c}{D_N}
\end{array}\right)$$

Let $T = T^N D^N$. Then (4.9) is equivalent to

$$Y = TX + QZ, \tag{4.14}$$

where $Y = Y^N$, $Q = Q^N$ and $Z = Z^N$.

Let $b = B + \sum_{i=1}^{N} \sigma_i = B + \dfrac{MN}{2}$. The identity matrix of dimension b sent by $\mathcal{S}$ undergoes the same transformation as the rest of the batch. Hence, $\hat{T} = TI_b + QL$, where $\hat{T}$ and L are the columns that correspond to the location of the identity matrix in Y and Z respectively. Then we can write

$$Y = \hat{T}X + Q(Z - LX) = \hat{T}X + E,$$

with $E = Q(Z - LX)$.

Assume that Y full row rank, otherwise, discard linearly dependent rows of Y. Define $z = \text{rank}(QZ)$. By Lemma 11 $z = \text{rank}(Y) - b$ and T^N and Q span disjoint vector spaces. Since columns of $T = T^N D^N$ are linear combinations of columns of T^N, T and Q also span disjoint vector spaces. Because the decoder cannot directly estimate the basis for the column space of E, it instead chooses a proxy error matrix T'' whose columns act as a proxy error basis for the columns of E. T'' is chosen as the matrix that corresponds to the first z columns of Y. As in [13], we then have

$$Y = \begin{pmatrix} T'' & \hat{T} \end{pmatrix} \begin{pmatrix} I_z & F^Z & 0 \\ 0 & F^X & I_b \end{pmatrix}. \tag{4.15}$$

Let $X = \begin{pmatrix} J_1 & J_2 & J_3 \end{pmatrix}$, where J_1 corresponds to the first z columns of X, J_3 corresponds to the last b columns of X, and J_2 corresponds to the remaining columns of X. Then by Lemma 4 in [13], (4.15) is equivalent to the matrix equation

$$\hat{T} J_2 = \hat{T}(F^X + J_1 F^Z). \tag{4.16}$$

Now, in order to decode, we need to solve the system formed by the linear equations (4.10) and (4.16).

For $i = 1, 2$ denote by $\mathbf{j_i}$ the vector obtained by stacking the columns of J_i one on top of the other. Note that by (4.13),

$$\begin{pmatrix} \mathbf{j_1} \\ \mathbf{j_2} \end{pmatrix} = P \begin{pmatrix} \mathbf{w} \\ \mathbf{y_1} \\ \dots \\ \mathbf{y_N} \end{pmatrix},$$

where P is a permutation matrix.

Denote by $\mathbf{f}^X$ the vector formed by stacking columns of the matrix F^X one on top of another, and by $f_{i,j}$ the (i, j)th entry of the matrix F^Z. Let $\alpha = K - z$. The system of linear equations given by (4.10) and (4.16) can be written in matrix form as

$$A \begin{pmatrix} \mathbf{j_1} \\ \mathbf{j_2} \end{pmatrix} = \begin{pmatrix} \hat{T}\mathbf{f}^X \\ \mathbf{0} \\ \dots \\ \mathbf{0} \end{pmatrix},$$

where A is given by

$$A = \left(\begin{array}{cccc|cccc} -f_{1,1}\hat{T} & -f_{2,1}\hat{T} & \dots & -f_{z,1}\hat{T} & \hat{T} & 0 & \dots & 0 \\ -f_{1,2}\hat{T} & -f_{2,2}\hat{T} & \dots & -f_{z,2}\hat{T} & 0 & \hat{T} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ -f_{1,\alpha}\hat{T} & -f_{2,\alpha}\hat{T} & \dots & -f_{z,\alpha}\hat{T} & 0 & 0 & \dots & \hat{T} \\ \hline \multicolumn{8}{c}{S_P} \end{array}\right)$$

$$\text{with } S_P = \begin{pmatrix} S_1 & -I_{\frac{MK}{2}} & 0 & \dots & 0 \\ S_2 & 0 & -I_{\frac{MK}{2}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ S_N & 0 & 0 & \dots & -I_{\frac{MK}{2}} \end{pmatrix} P^{-1}.$$

In order to show that we can decode, we need to prove that A has full column rank. By Lemma 11, $\hat{T}$ is a $(b+z) \times b$ matrix of full column rank. Therefore, the last αb columns of A have full column rank. Denote the first z block-columns of A by $\{u_1, u_2, \dots, u_z\}$, and the last α block-columns of A by $\{v_1, v_2, \dots, v_\alpha\}$. For each i, let $u_i = \begin{pmatrix} u_i^1 & u_i^2 \end{pmatrix}^T$, where u_i^1 are the first $\alpha(b+z)$ rows and u_i^2 are the remaining rows of u_i. Similarly, let $v_i = \begin{pmatrix} v_i^1 & v_i^2 \end{pmatrix}^T$, where v_i^1 are the first $\alpha(b+z)$ rows and v_i^2 are the remaining rows of v_i. Note that for each $i = 1 \dots z$, $u_i^1 + \sum_j f_{i,j} v_i^1 = 0$. Define $w_i = u_i^2 + \sum_j f_{i,j} v_i^2$. Let $\tilde{A}$ be the resulting matrix after Gaussian elimination is performed on the upper left-hand side of A. A has full rank iff the lower submatrix of $\tilde{A}$ formed by w_i and v_i^2 has full rank. Note that since P is a permutation matrix, P^{-1} is also a permutation matrix. Therefore, S_P is a permutation of columns of the random matrix $S = \begin{pmatrix} S_1 \\ S_2 \\ \dots \\ S_N \end{pmatrix}$ and the identity matrix; hence, u_i^2 and v_i^2 are the columns of S and the identity matrix. Since entries of S are independently and uniformly distributed in $\mathbb{F}_q$, so are w_i for fixed values of $f_{i,j}$. The probability that A does not have full column rank is $1 - \prod_{l=1}^{bz}\left(1 - \frac{1}{q^{\sum \sigma_i K - l + 1}}\right)$, which is upper-bounded by $q^{bz - \sum \sigma_i K}$. By the union bound over all $q^{\alpha z}$ possible values of variables $f_{i,j}$, we have $q^{bz - \sum \sigma_i K + \alpha z} \leq q^{K(z - \sum \sigma_i)}$. Therefore, decoding succeeds with probability at least $q^{-K\epsilon}$ if $\sum \sigma_i > z + \epsilon$, which follows from equation (4.7). □

Proof of Theorem 5. Define $\epsilon_1 = \frac{MN}{2} - \sum_{i=0}^{N} \mathbb{E}[E_i]$. By (4.12) $\epsilon_1 > 0$. Since for each i,j, the actual minimum cut of the network varies depending on the strategy used, define M_i^j to be the throughput of linearly independent packets while transmitting X_i^j. Then the achievable rate is given by:

$$\begin{aligned} r &\leq \frac{\sum_{j=1}^{N_B} M_0^j + \sum_{i=1}^{N}\sum_{j=1}^{N_M} M_i^j - \sum_{i=1}^{N} (\sigma_i + \delta_i)}{N_B + NN_M} \\ &= M_A - 2\frac{\sum_{j=1}^{N_B} \mathbb{E}[E_0^j] + \sum_{i=1}^{N}\sum_{j=1}^{N_M} \mathbb{E}[E_i^j]}{N_B + NN_M} - \frac{2\epsilon_1}{N_B + NN_M} \\ &= M_A - 2\frac{\mathbb{E}[E_0^1](N_B + NN_M)}{N_B + NN_M} - \frac{2\epsilon_1 m}{B + MN} \end{aligned}$$

with $\epsilon = \frac{2\epsilon_1 m}{B+MN}$. □

Chapter 5

Capacity regions for multisource multicast network error correction

5.1 Introduction

For a single-source, single-sink network with mincut m, the capacity of the network under arbitrary errors on up to z links is given by

$$r \leq m - 2z \tag{5.1}$$

and can be achieved by a classical end-to-end error correction code over multiple disjoint paths from source to the sink. This result is a direct extension of the Singleton bound [33]. Since the Singleton bound can be achieved by a maximum distance separable code, as for example a Reed-Solomon code, such a code also suffices to achieve the capacity in the single-source, single-sink case.

In the network multicast scenario, the situation is more complicated. For the single-source multicast the capacity region was shown [6, 7, 8] to be the same as (5.1), with m now representing the minimum of the mincuts [7]. However, unlike single-source single-sink networks, in the case of single-source multicast, network error correction is required: network coding is required in general for multicast even in the error-free case [1], and with the use of network coding errors in the sink observations become dependent and cannot be corrected by end-to-end codes.

In this chapter we address the error correction capacity region and the corresponding code design in both coherent and noncoherent multiple-source multicast scenarios [26, 27]. We prove the upper bound on the capacity region as well as give capacity-achieving com-

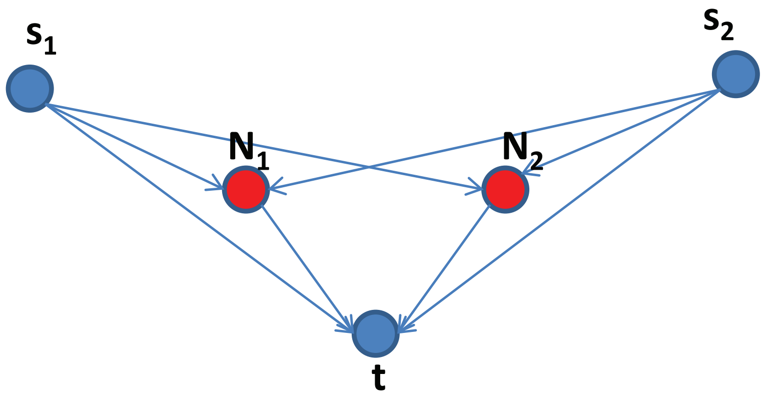


Figure 5.1: An example to show that in the multisource case network coding is required to achieve the network error correction capacity.

munication scheme in both coherent and noncoherent cases. Our achievable scheme for the noncoherent scenario is based on the random subspace code design of complexity that grows exponentially. Subsequent work of [34, 27] gives a polynomial-time capacity-achieving construction that uses a multiple-field extension technique.

5.2 Motivating example

The issues which arise in multisource network error correction problem are best explained with a simple example for a single sink, which is shown in Figure 5.1. Suppose that the sources s_1 and s_2 encode their information independently from each other. We can allocate one part of the network to carry only information from s_1, and another part to carry only information from s_2. In this case only one source is able to communicate reliably under one link error. However, if coding at the middle nodes N_1 and N_2 is employed, the two sources are able to share network capacity to send redundant information, and each source is able to communicate reliably at capacity 1 under a single link error. This shows that in contrast to the single source case, coding across multiple sources is required, so that sources can simultaneously use shared network capacity to send redundant information, even for a single sink.

We show that for the example network in Figure 5.1, the z-error correction capacity region is given by

$$\begin{aligned} r_1 &\leq m_{s_1} - 2z \\ r_2 &\leq m_{s_2} - 2z \\ r_1 + r_2 &\leq m_{s_1,s_2} - 2z, \end{aligned} \tag{5.2}$$

where for $i = 1, 2$, rate r_i is the information rate of s_i, m_{s_i} is the minimum cut capacity between s_i and sink t, m_{s_1,s_2} is the minimum cut capacity between s_1, s_2 and t and z is the known upper bound on the number of link errors. Hence, similarly to single-source multicast, the capacity region of a multisource multicast network is described by the cutset bounds. From that perspective, one may draw a parallel with point-to-point error correction. However, for multisource multicast networks point-to-point error-correcting codes do not suffice and a careful network code design is required. For instance, the work of [18], which applies single-source network error-correcting codes for this problem, achieves a rate region that is strictly smaller than the capacity region (5.2) when $m_{s_1} + m_{s_2} \neq m_{s_1,s_2}$.

5.3 Model

Consider a multicast network error correction problem on a directed acyclic graph $\mathcal{G}$ with n source nodes $\mathcal{S} = \{s_1, s_2, \ldots, s_n\}$ and a set of sink nodes $\mathcal{T}$. Each link has unit capacity, and there can be multiple parallel edges connecting a pair of nodes. Let r_i be the multicast transmission rate from s_i to each sink. For any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$, let $\mathcal{I}(\mathcal{S}')$ be the indices of the source nodes that belong to $\mathcal{S}'$. Let $m_{\mathcal{S}'}$ be the minimum cut capacity between any sink and $\mathcal{S}'$. For each $i, i = 1, \ldots, n$, let $\mathcal{C}_i$ be the code used by source i. Let $\mathcal{C}_{\mathcal{S}'}$ be the Cartesian product of the individual codes of the sources in $\mathcal{S}'$.

Let V be the vector space of length-K vectors over the finite field $\mathbb{F}_q$, representing the set of all possible values of packets transmitted and received in the network [14]. Let $\mathcal{P}(V)$ denote the set of all subspaces of V. A code $\mathcal{C}$ consists of a nonempty subset of $\mathcal{P}(V)$, where each codeword $U \in \mathcal{C}$ is a subspace of constant dimension.

Subspace errors are defined as additions of vectors to the transmitted subspace and subspace erasures are defined as deletions of vectors from the transmitted subspace [14]. Note that depending on the network code rate and network topology, network errors and erasures translate differently to subspace errors and erasures. For instance, subject to the position of adversary in the network, one network error can result in both dimension addition and deletion (i.e.,, both subspace error and subspace erasure in our terminology). Let ρ be the number of subspace erasures and let t be the number of subspace errors caused by z network errors.

The subspace metric [14] between two vector spaces $U_1, U_2 \in \mathcal{P}(V)$ is defined as

$$\begin{aligned} d_S(U_1, U_2) &\doteq \dim(U_1 + U_2) - \dim(U_1 \cap U_2) \\ &= \dim(U_1) + \dim(U_2) - 2\dim(U_1 \cap U_2). \end{aligned}$$

In [14] it shown that the minimum subspace distance decoder can successfully recover the transmitted subspace from the received subspace if

$$2(\rho + t) < D_S^{\min},$$

where $D_S^{\min}$ is the minimum subspace distance of the code. Note that d_S treats insertions and deletions of subspaces symmetrically. In [24] the converse of this statement for the case when information is transmitted at the maximum rate was shown.

In [32] a different metric on V, namely, the injection metric, was introduced and shown to improve upon the subspace distance metric for decoding of non-constant-dimension codes. The injection metric between two vector spaces $U_1, U_2 \in \mathcal{P}(V)$ is defined as

$$\begin{aligned} d_I(U_1, U_2) &\doteq \max(\dim(U_1), \dim(U_2)) - \dim(U_1 \cap U_2) \\ &= \dim(U_1 + U_2) - \min(\dim(U_1), \dim(U_2)). \end{aligned}$$

d_I can be interpreted as the number of error packets that an adversary needs to inject in order to transform input space U_1 into an output space U_2. The minimum injection distance decoder is designed to decode the received subspace as with as few error injections as possible. Note that for constant-dimensional codes d_S and d_I are related by

$$d_I(U_1, U_2) = \frac{1}{2} d_S(U_1, U_2).$$

5.4 Main results

5.4.1 Coherent multisource multicast

Theorem 6 characterizes the network error correction capacity of centralized network coding over a known network $\mathcal{G}$ in a multiple-source multicast scenario.

Theorem 6. *Consider a multiple-source multicast network error correction problem on network $\mathcal{G}$ with known topology. For any arbitrary errors on up to z links, the capacity region is given by:*

$$\sum_{i\in\mathcal{I}(\mathcal{S}')} r_i \leq m_{\mathcal{S}'} - 2z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{5.3}$$

Proof. See Section 5.5. □

5.4.2 Noncoherent multisource multicast

Theorem 7 gives the noncoherent capacity region. In the proof of Theorem 7 we show how to design noncoherent network codes that achieve upper bounds given by (5.4) when a minimum (or bounded) injection distance decoder is used at the sink nodes. Our code construction uses random linear network coding at intermediate nodes, single-source network error correction capacity-achieving codes at each source, and an overall global coding vector. Our choice of decoder relies on the observation that subspace erasures are not arbitrarily chosen by the adversary, but also depend on the network code. Since, as we show below, with high probability in a random linear network code, subspace erasures do not cause confusion between transmitted codewords, the decoder focuses on the discrepancy between the sent and the received codewords caused by subspace errors. The error analysis shows that injection distance decoding succeeds with high probability over the random network code. On the other hand, the subspace minimum distance of the code is insufficient to account for the total number of subspace errors and erasures that can occur. This is in contrast to constant dimension single-source codes, where subspace distance decoding is equivalent to injection distance decoding [32].

Theorem 7. *Consider a multiple-source multicast network error correction problem on network $\mathcal{G}$ whose topology may be unknown. For any errors on up to z links, when random* *linear network coding in a sufficiently large finite field is performed, the capacity region is given by:*

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i \leq m_{\mathcal{S}'} - 2z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{5.4}$$

Proof. See Section 5.5. □

Note that the capacity regions of coherent and non-coherent network coding given by Theorems 6 and 7 for the same multisource multicast network are the same. However, a noncoherent scheme includes an overhead of incorporating a global coding vector. Therefore, it achieves the outer bounds given by (5.4) only asymptotically in packet length. In contrast, in the coherent case, the full capacity region can be achieved exactly with packets of finite length. Hence, any non-coherent coding scheme can also be applied in the coherent setting when the network is known.

5.5 Proofs

Proof of Theorem 6. Converse. Let $l_{i,j}, j = 1, \ldots, n_i$, be the outgoing links of each source $s_i, i = 1, \ldots, n$. Take any $\mathcal{S}' \subseteq \mathcal{S}$. We construct the graph $\mathcal{G}_{\mathcal{S}'}$ from $\mathcal{G}$ by adding a virtual super source node $w_{\mathcal{S}'}$, and n_i links $l'_{i,j}, j = 1, \ldots, n_i$, from $w_{\mathcal{S}'}$ to source s_i for each $i \in \mathcal{I}(\mathcal{S}')$. Note that the minimum cut capacity between $w_{\mathcal{S}'}$ and any sink is at least $m_{\mathcal{S}'}$. Any network code that multicasts rate r_i from each source $s_i, i \in \mathcal{I}(\mathcal{S}')$ over $\mathcal{G}$ corresponds to a network code that multicasts rate $\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i$ from $w_{\mathcal{S}'}$ to all sinks over $\mathcal{G}_{\mathcal{S}'}$; the symbol on each link $l'_{i,j}$ is the same as that on link $l_{i,j}$, and the coding operations at all other nodes are identical for $\mathcal{G}$ and $\mathcal{G}_{\mathcal{S}'}$. The converse follows from applying the network Singleton bound [7] to $w_{\mathcal{S}'}$ for each $\mathcal{S}' \subseteq \mathcal{S}$.

Achievability. Suppose any $2z$ links on $\mathcal{G}$ suffer erasures. Construct the graph $\mathcal{G}_{\mathcal{S}'}$ from $\mathcal{G}$ by adding $2z$ extra sources in place of erasure links. Since the maxflow-mincut bound holds for $\mathcal{G}_{\mathcal{S}'}$, there exists a random linear network code $\mathcal{C}'$ such that all $n + 2z$ sources can be reconstructed at the sink [5].

Now construct the graph $\mathcal{G}_{\mathcal{S}}$ for the set of all source nodes $\mathcal{S}$ as in the proof of the converse. Then the code $\mathcal{C}'$ on $\mathcal{G}_{\mathcal{S}'}$ corresponds to a single-source network code $\mathcal{C}_{\mathcal{S}}$ on $\mathcal{G}_{\mathcal{S}}$ where the symbol on each link $l'_{i,j}$ is the same as that on link $l_{i,j}$, and the coding operations at all other nodes are identical for $\mathcal{G}_{\mathcal{S}'}$ and $\mathcal{G}_{\mathcal{S}}$.

For the single-source coherent case, the following are equivalent [35]:

1. a linear network code has network minimum distance at least $2z + 1$
2. the code corrects any error of weight at most z
3. the code corrects any erasure of weight at most $2z$.

This implies that $\mathcal{C}_{\mathcal{S}}$ has network minimum distance at least $2z+1$, and so it can correct any z errors.

Note that a general single-source network code on $\mathcal{G}_{\mathcal{S}}$ would not correspond to a valid n-source network code on $\mathcal{G}_{\mathcal{S}}$, since for independent sources the set of source codewords in $\mathcal{C}_{\mathcal{S}}$ must be the Cartesian product of a set of codewords from $s_1, s_2, \ldots, s_n$. □

Proof of Theorem 7. Converse. Follows from Theorem 6, since the noncoherent region is no larger than the coherent region.

Achievability. 1) *Code construction:* Consider any rate vector $(r_1, \ldots, r_{|\mathcal{S}|})$ such that

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} r_i < m_{\mathcal{S}'} - 2z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{5.5}$$

Let each $\mathcal{C}_i$, $i = 1, \ldots, |\mathcal{S}|$ be a code consisting of codewords that are k_i-dimensional linear subspaces. The codeword transmitted by source $\mathcal{S}_i$ is spanned by the packets transmitted by $\mathcal{S}_i$. From the single source case, for each source $i = 1, \ldots, |\mathcal{S}|$ we can construct a code $\mathcal{C}_i$ where

$$k_i > r_i + z \tag{5.6}$$

that corrects any z additions [13]. This implies that by [24], $\mathcal{C}_i$ has minimum subspace distance greater than $2z$, i.e., for any pair of distinct codewords V_i, $V_i' \in \mathcal{C}_i$

$$d_S(V_i, V_i') = \dim(V_i) + \dim(V_i') - 2\dim(V_i \cap V_i') > 2z.$$

Hence,

$$\dim(V_i \cap V_i') < k_i - z \quad \forall \ V_i, V_i' \in \mathcal{C}_i. \tag{5.7}$$

By (5.6), we have:

$$\sum_{i\in\mathcal{I}(\mathcal{S}')} k_i > \sum_{i\in\mathcal{I}(\mathcal{S}')} r_i + |\mathcal{S}'|z.$$

Therefore, by combining it with (5.5) and scaling all source rates and link capacities by a sufficiently large integer if necessary, we can assume without loss of generality that we can choose k_i satisfying

$$\sum_{i\in\mathcal{I}(\mathcal{S}')} k_i \leq m_{\mathcal{S}'} + (|\mathcal{S}'| - 2)z \ \forall \mathcal{S}' \subseteq \mathcal{S}. \tag{5.8}$$

We can make vectors from one source linearly independent of vectors from all other sources by prepending a length–($\sum\limits_{i\in\mathcal{I}(\mathcal{S})} k_i$) global encoding vector, where the jth global encoding vector, $j = 1, 2, \ldots, \sum_{i\in\mathcal{I}(\mathcal{S})} k_i$, is the unit vector with a single nonzero entry in the jth position. This adds an overhead that becomes asymptotically negligible as packet length grows. This ensures that

$$\dim(V_i \cap V_j) = 0 \ \forall i \neq j, V_i \in \mathcal{C}_i, V_j \in \mathcal{C}_j. \tag{5.9}$$

2) *Error analysis.* Let $X \in \mathcal{C}_\mathcal{S}$ be the sent codeword, and let R be the subspace received at a sink. Consider any $\mathcal{S}' \subseteq \mathcal{S}$. Let $\overline{\mathcal{S}'} = \mathcal{S} \setminus \mathcal{S}'$. Let $X = V \oplus W$, where $V \in \mathcal{C}_{\mathcal{S}'}, W \in \mathcal{C}_{\overline{\mathcal{S}'}}$ and V is spanned by the codeword V_i from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$. We will show that with high probability over the random network code, there does not exist another codeword $Y = V' \oplus W$, such that V' is spanned by a codeword $V'_i \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$, which could also have produced R under arbitrary errors on up to z links in the network.

Fix any sink t. Let $\mathcal{R}$ be the set of packets (vectors) received by t, i.e., R is the subspace spanned by $\mathcal{R}$. Each of the packets in $\mathcal{R}$ is a linear combination of vectors from V and W and error vectors, and can be expressed as $\mathbf{p} = \mathbf{u_p} + \mathbf{w_p}$, where $\mathbf{w_p}$ is in W and the global encoding vector of $\mathbf{u_p}$ has zero entries in the positions corresponding to sources in set $\mathcal{I}(\overline{\mathcal{S}'})$.

The key idea behind our error analysis is to show that with high probability subspace deletions do not cause confusion, and that more than z additions are needed for X be decoded wrongly at the sink, i.e we will show that

$$d_I(R, V' \oplus W) = \dim(R) - \dim(R \cap (V' \oplus W)) > z.$$

Let $P = \text{span}\{\mathbf{u_p} : \mathbf{p} \in \mathcal{R}\}$. Let M be the matrix whose rows are the vectors $\mathbf{p} \in \mathcal{R}$, where the jth row of M corresponds to the jth vector $\mathbf{p} \in \mathcal{R}$. Similarly, let $M_\mathbf{u}$ be the matrix whose jth row is the vector $\mathbf{u_p}$ corresponding to the jth vector $\mathbf{p} \in \mathcal{R}$, and let $M_\mathbf{w}$ be the matrix whose jth row is the vector $\mathbf{w_p}$ corresponding to the jth vector $\mathbf{p} \in \mathcal{R}$. Consider matrices A, B such that the rows of $AM_\mathbf{u}$ form a basis for $P \cap V'$ and, together with the rows of $BM_\mathbf{u}$, form a basis for P. The linear independence of the rows of $\begin{bmatrix} AM_\mathbf{u} \\ BM_\mathbf{u} \end{bmatrix}$ implies that the rows of $\begin{bmatrix} AM \\ BM \end{bmatrix}$ are also linearly independent, since otherwise there would be a nonzero matrix D such that

$$\begin{aligned} D \begin{bmatrix} AM \\ BM \end{bmatrix} = 0 \Rightarrow D \begin{bmatrix} AM_\mathbf{w} \\ BM_\mathbf{w} \end{bmatrix} = 0 \\ \Rightarrow D \begin{bmatrix} AM_\mathbf{u} \\ BM_\mathbf{u} \end{bmatrix} = 0, \end{aligned}$$

a contradiction. For $\mathbf{w_p}$ in W, $\mathbf{u_p} + \mathbf{w_p}$ is in $V' \oplus W$ only if $\mathbf{u_p}$ is in V', because the former implies $\mathbf{u_p} = \mathbf{u_p} + \mathbf{w_p} - \mathbf{w_p}$ is in $V' \oplus W$ and since $\mathbf{u_p}$ has zero entries in the positions of the global encoding vector corresponding to $\mathcal{I}(\overline{\mathcal{S}'})$ it must be in V'. Thus, since any vector in the row space of $BM_\mathbf{u}$ is not in V', any vector in the row space of BM is not in $V' \oplus W$. Since the row space of BM is a subspace of R, it follows that the number of rows of B is equal to $\dim(P) - \dim(P \cap V')$ and is less than or equal to $\dim(R) - \dim(R \cap (V' \oplus W))$. Therefore,

$$\begin{aligned} d_I(R, V' \oplus W) &= \dim(R) - \dim(R \cap (V' \oplus W)) \\ &\geq \dim(P) - \dim(P \cap V'). \end{aligned} \tag{5.10}$$

We next show that for random linear coding in a sufficiently large field, with high probability

$$\dim(P) - \dim(P \cap V') > z \tag{5.11}$$

for all V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$.

Consider first the network with each source i in $\mathcal{S}'$ transmitting k_i linearly independent packets from V_i, sources in $\overline{\mathcal{S}'}$ silent, and no errors. From the maxflow-mincut bound, any rate vector $(h_1, \ldots, h_{|\mathcal{S}'|})$, such that

$$\sum_{i \in \mathcal{S}''} h_i \leq m_{\mathcal{S}''} \quad \forall \mathcal{S}'' \subseteq \mathcal{S}'$$

can be achieved. Combining this with (5.8), we can see that in the error-free case, each $s_i \in \mathcal{S}'$ can transmit information to the sink at rate $k_i - \frac{(|\mathcal{S}'|-2)z}{|\mathcal{S}'|}$ for a total rate of

$$\sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z. \tag{5.12}$$

With sources in $\overline{\mathcal{S}'}$ still silent, consider the addition of z unit-rate sources corresponding to the error links. The space spanned by the received packets corresponds to P. Consider any V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$.

Let Z be the space spanned by the error packets, and let $z' \leq z$ be the minimum cut between the error sources and the sink. Let $P = P_V \oplus P_Z$, where $P_Z = P \cap Z$ and P_V is a subspace of V. There exists a routing solution, which we distinguish by adding tildes in our notation, such that $\dim \tilde{P}_Z = z'$ and, from (5.12), $\dim \tilde{P} \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z$, so

$$\dim(\tilde{P}_V) \geq \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'| - 2)z - z'. \tag{5.13}$$

Note that, by (5.9), a packet from V_i is not in any $V_j' \in \mathcal{C}_j, j \neq i$, and hence is in V' if and only if it is in V_i'. Therefore, by (5.7)

$$\dim(\tilde{P}_V \cap V') \leq \sum_{i \in \mathcal{I}(\mathcal{S}')} \dim(V_i \cap V_i') < \sum_{i \in \mathcal{I}(\mathcal{S}')} k_i - |\mathcal{S}'|z.$$

Therefore, using (5.13) we have

$$\begin{aligned}\dim(\tilde{P}_V \cup V') &= \dim(\tilde{P}_V) + \dim(V') - \dim(\tilde{P}_V \cap V')\\ &> \dim(\tilde{P}_V) + \dim(V') + |\mathcal{S}'|z - \sum_{i\in\mathcal{I}(\mathcal{S}')} k_i\\ &\geq \sum_{i\in\mathcal{I}(\mathcal{S}')} k_i - (|\mathcal{S}'|-2)z - z' + |\mathcal{S}'|z\\ &= \sum_{i\in\mathcal{I}(\mathcal{S}')} k_i + 2z - z' \geq \sum_{i\in\mathcal{I}(\mathcal{S}')} k_i + z.\end{aligned}$$

Then

$$\dim(\tilde{P} \cup V') > \sum_{i\in\mathcal{I}(\mathcal{S}')} k_i + z.$$

For random linear coding in a sufficiently large field, with high probability by its generic nature

$$\dim(P \cup V') \geq \dim(\tilde{P} \cup V') > \sum_{i\in\mathcal{I}(\mathcal{S}')} k_i + z,$$

and this also holds for any z or fewer errors, all sinks, and all V' spanned by a codeword $V_i' \neq V_i$ from each code $\mathcal{C}_i, i \in \mathcal{I}(\mathcal{S}')$. Then, (5.11) follows by

$$\dim(P) - \dim(P \cap V') = \dim(P \cup V') - \dim(V').$$

Hence, using (5.11) and (5.10),

$$\begin{aligned}d_I(R, V' \oplus W) &= \dim(R) - \dim(R \cap (V' \oplus W))\\ &\geq \dim(P) - \dim(P \cap V') > z.\end{aligned}$$

Thus, more than z additions are needed to produce R from $Y = V' \oplus W$. By the generic nature of random linear coding, with high probability this holds for any $\mathcal{S}'$. Therefore, at every sink the minimum injection distance decoding succeeds with high probability over the random network code.

Decoding complexity. Take any achievable rate vector $(r_1, r_2, \ldots, r_{|\mathcal{S}|})$. For each $i =$

$1, \ldots, |\mathcal{S}|$, s_i can transmit at most $q^{r_i K}$ independent symbols. Decoding can be done by exhaustive search, where the decoder checks each possible set of codewords to find the one with minimum distance from the observed set of packets, therefore, the decoding complexity of the minimum injection distance decoder is upper bounded by $O(q^{K \sum_{i=1}^{|\mathcal{S}|} r_i})$. □

Chapter 6

Network error correction in nonmulticast networks

6.1 Introduction

In this chapter we consider the problem of adversarial error correction in nonmulticast networks. Previous work on network error correction largely assumes multicast network scenarios. For single- and multiple-source multicast network scenarios, it has been proven that the cutset bounds are tight, and that linear network error-correcting codes are sufficient [7, 26].

For nonmulticast networks, however, finding the capacity region of a general network even in the error-free case is an open problem. In some network topologies, such as single-source two-sink networks as well as single-source disjoint- or nested-demand networks, the error-free capacity region is known to be described by the cutset bounds [19, 20, 21, 9]. In this chapter we show that this is generally not the case for erroneous networks. We propose an achievable scheme of for the multiple-source nonmulticast scenario in the presence of errors from a given error-free linear network code [26]. We also provide upper bounds on the error correction capacity regions of nonmulticast networks based on the topological structure of network cuts [28].

6.2 Model

Consider a network error correction problem on a directed acyclic graph $\mathcal{G}$ with n source nodes $\mathcal{S} = \{s_1, s_2, \dots, s_n\}$ and m sink nodes $\mathcal{T} = \{t_1, t_2, \dots, t_m\}$, where each source s_i is demanded by a given set of sink nodes $\mathcal{T}_i$, and arbitrary coding across sessions is permitted.

Each link has unit capacity, and there can be multiple parallel edges connecting a pair of nodes.

For each $i, i \in \{1, \dots, n\}$, let r_i be the error-free information rate of s_i. For any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$, let $\mathcal{I}(\mathcal{S}')$ be the indices of the source nodes that belong to $\mathcal{S}'$. Similarly, for any non-empty subset of $\mathcal{T}' \in \mathcal{T}$, let $\mathcal{I}(\mathcal{T}')$ be the indices of the sink nodes that belong to $\mathcal{T}'$. Define $m_{\mathcal{S}',\mathcal{T}'}$ to be the minimum cut capacity between $\mathcal{S}'$ and $\mathcal{T}'$.

Let $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \ldots \times \mathcal{C}_m$ be the code used by $\mathcal{S}$. A network code is z-error link-correcting if it can correct any t adversarial link errors for $t \leq z$. For each $i, i \in \{1, \dots, n\}$, let u_i be the information rate of s_i in case of any z network link errors.

Definition 1. *The set of all rate vectors $(u_1, u_2, \dots, u_n)$ that can be achieved on $\mathcal{G}$ under any z network link errors is called z-error correction capacity region.*

Define $\phi_l(\mathbf{x})$ as the error-free output of link l when the network input is $\mathbf{x} \in \mathcal{C}$. If an error vector $\mathbf{z}$ occurs, its components are added to the link inputs according to the coding order. Then the output of a link l is a function of both the network input $\mathbf{w}$ and the error vector $\mathbf{z}$ and it is denoted by $\psi_l(\mathbf{w}, \mathbf{z})$ [7].

Throughout this chapter, we assume the coherent network coding scenario, in which there is centralized knowledge of the network topology and network code.

6.3 Main results

6.3.1 Lower bound

Consider any linear network code $\mathcal{C}$. If the given linear network code $\mathcal{C}$ is a vector linear network code with vector length y, we can consider a modified network problem where each source is replaced with y co-located sources and each link with y parallel links joining the same nodes. The source rates and the number of errors are also scaled by y. Therefore, we may view the vector linear code $\mathcal{C}$ as a scalar linear code on the new network.

Prior to describing how to use $\mathcal{C}$ in order to construct a valid network code in the presence of network errors, we first generalize the concept of network distance, introduced in [35] for multicast, to nonmulticast as follows.

The Hamming weight of a vector $\mathbf{z}$ (the number of non-zero components of $\mathbf{z}$) is denoted by $w_H(\mathbf{z})$. As in [35], define a network erasure pattern ρ with Hamming weight $|\rho|$ as a set of channels in which an error may have occurred, whose location is known to all sink nodes. Abusing notation, we also use ρ to denote the set of vectors with nonzero entries corresponding to the erasure pattern ρ.

For any non-empty subset $\mathcal{S}' \subseteq \mathcal{S}$, let $A_{\mathcal{S}'}$ denote the transfer matrix mapping the length-$r_{\mathcal{S}'}$ vector $\mathbf{x}_{\mathcal{S}'}$ of source symbols of sources in $\mathcal{S}'$ to the corresponding incident outgoing links of the sources, where $r_{\mathcal{S}'} = \sum_{i \in \mathcal{S}'} r_i$. Let F_t be the transfer matrix from all links in the network to the incoming links of sink t. Let $Im(F_t)$ be the image of the map F_t. For any $t \in \mathcal{T}$, let $\mathcal{S}_t$ be the subset of sources demanded by sink node t, and $\overline{\mathcal{S}}_t$ the subset of sources not demanded by t. For any vector $\mathbf{y} \in Im(F_t)$ received at t, let

$$\Upsilon_t(\mathbf{y}) = \{\mathbf{z} : \ \exists \mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\mathcal{S}'}} \text{ s.t. } (\mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} + \mathbf{z}) F_t = \mathbf{y}\}$$

be the set of all error patterns that could result in $\mathbf{y}$ being observed at the sink. With this definition, we can, analogously to the multicast case in [35], develop the following definitions and results.

Definition 2. *For any sink node t, the network Hamming weight of a received vector $\mathbf{y} \in Im(F_t)$ is defined as*

$$W_t^{rec}(\mathbf{y}) = \min_{\mathbf{z} \in \Upsilon_t(\mathbf{y})} w_H(\mathbf{z}).$$

Definition 3. *For any sink node t, the network Hamming weight of a message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ is defined as*

$$W_t^{msg}(\mathbf{x}_{\mathcal{S}_t}) = W_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t).$$

Definition 4. *For any sink node t, the network Hamming distance between two received vectors $\mathbf{y}^1, \mathbf{y}^2 \in Im(F_t)$ is defined by*

$$D_t^{rec}(\mathbf{y}^1, \mathbf{y}^2) = W_t^{rec}(\mathbf{y}^1 - \mathbf{y}^2).$$

Definition 5. *For any sink node t, the network Hamming distance between two message vectors $\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$, is defined by*

$$D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) = W_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t} - \mathbf{x}^2_{\mathcal{S}_t}).$$

Lemma 12. *For any sink node t, let $\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^1_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ be message vectors, $\mathbf{y}, \mathbf{y}^1 \in Im(F_t)$ be* *received vectors. Then we have*

$$\begin{aligned} D_t^{rec}(\mathbf{y}, \mathbf{y}^1) &= D_t^{rec}(\mathbf{y}^1, \mathbf{y}) && (6.1) \\ D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^1_{\mathcal{S}_t}) &= D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}) && (6.2) \\ D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^1_{\mathcal{S}_t}) &= D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}^1_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t) && (6.3) \end{aligned}$$

Proof. See Section 6.4. □

Lemma 13 (Triangle inequality)**.** *For any sink node t, let $\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ be message vectors, $\mathbf{y}, \mathbf{y}^1, \mathbf{y}^2 \in Im(F_t)$ be received vectors. Then we have:*

$$\begin{aligned} D_t^{rec}(\mathbf{y}_1, \mathbf{y}_2) &\leq D_t^{rec}(\mathbf{y}_1, \mathbf{y}) + D_t^{rec}(\mathbf{y}, \mathbf{y}_2) && (6.4) \\ D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) &\leq D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}) + D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) && (6.5) \end{aligned}$$

Proof. See Section 6.4. □

Definition 6. *For each sink node t, the minimum distance of a network code is defined by:*

$$d_{\min,t} = \min\{D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) : \mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}, \mathbf{x}^1_{\mathcal{S}_t} \neq \mathbf{x}^2_{\mathcal{S}_t}\}$$

Definition 7. *The minimum distance of a network code is defined by:*

$$d_{min} = \underset{t \in \mathcal{T}}{min}\, d_{\min,t}$$

Theorem 8. *For a sink node t, the following properties of a linear network code are equivalent:*

1. *the code has $d_{\min,t} \geq 2z + 1$;*
2. *any error $\mathbf{z}$ such that $w_H(\mathbf{z}) \leq z$ can be corrected at t;*
3. *any erasure pattern ρ_t such that $|\rho_t| \leq 2z$ can be corrected at t.*

Proof. See Section 6.4. □

Theorem 8 is useful for proving Theorem 9:

Theorem 9. *Given any linear network code $\mathcal{C}$ that achieves rate vector $\mathbf{r} = (r_1, r_2, \ldots, r_n)$ in the error-free case, where r_i is the information rate of source s_i, $i = 1, \ldots, n$, we can obtain a network code $\tilde{\mathcal{C}}$ that achieves rate vector $\tilde{\mathbf{r}} = (r_1 - 2z, r_2 - 2z, \ldots, r_n - 2z)$ under arbitrary errors on up to z links in the network.*

Proof. See Section 6.4. □

Let $\mathbb{C} \subseteq \mathbb{R}^n$ be an error-free region achievable in $\mathcal{G}$ by linear coding. Then Theorem 9 allows us to construct an achievable error correction region $\mathbb{V}$ based on $\mathbb{C}$ as follows:

- Take any achievable rate vector $\mathbf{r} = (r_1, r_2, \ldots, r_n) \in \mathbb{C}$
- Define

$$f(\mathbf{r}) = (\max(r_1 - 2z, 0), \ldots, \max(r_n - 2z, 0)).$$

- By Theorem 9, $f(\mathbf{r}) \in \mathbb{V}$.
- By timesharing, for any $0 \leq \lambda \leq 1$ and any $\mathbf{v}, \mathbf{w} \in \mathbb{V}$, $\lambda\mathbf{v} + (1-\lambda)\mathbf{w} \in \mathbb{V}$.

In accordance with the above described procedure, we define

$$\mathbb{A} = \{\mathbf{a} \in \mathbb{R}^n : \exists \mathbf{r} \in \mathbb{C} \text{ such that } \mathbf{a} = f(\mathbf{r})\}$$

to be the set of rate vectors that have a preimage in $\mathbb{C}$. Also define

$$\begin{aligned} \mathbb{T} \;\; = \;\; & \{\mathbf{t} \in \mathbb{R}^n \backslash \mathbb{A} : \exists k_1, k_2, \ldots, k_n, \sum_{i=1}^{n} k_i = n, \\ & \mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n \in \mathbb{A} \text{ such that } \mathbf{t} = \sum_{i=1}^{n} \frac{k_i}{n} \mathbf{r}_i\} \end{aligned}$$

to be the set of rate vectors that can be achieved under any z errors by timesharing of elements in $\mathbb{A}$. Note that by our construction $\mathbb{V} = \mathbb{A} \cup \mathbb{T}$.

Figure 6.1 illustrates the construction of $\mathbb{V}$ based on $\mathbb{C}$ for the two-source two-sink network,

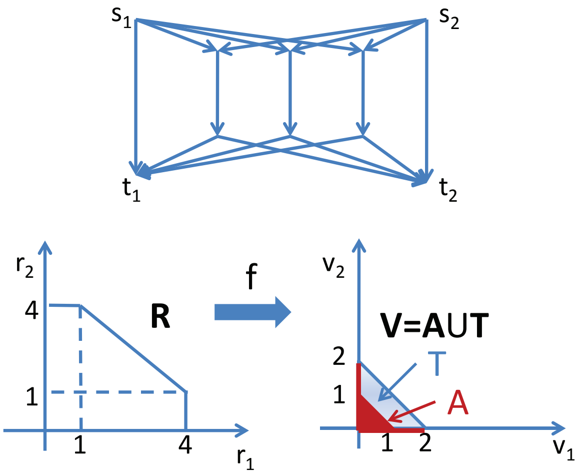


Figure 6.1: Example of the error correction achievability construction based on the known error-free capacity region for the two-source two-sink network.

for which in the error-free case the cutset bounds

$$\begin{aligned} r_1 &\leq m_{s_1,t_1} = 4 \\ r_2 &\leq m_{s_2,t_2} = 4 \\ r_1 + r_2 &\leq m_{s_1s_2,t_1t_2} = 5 \end{aligned}$$

are achieved.

6.3.2 Upper bound

In this section we consider an acyclic network $\mathcal{G} = (V, E)$ with source set $\mathcal{S}$ and sink set $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$. Let $X_1, X_2, \ldots, X_m$ be m independent source processes, such that each X_i is demanded by exactly one t_i (we require non-overlapping sink demands).

Define $P = (V_\mathcal{S}, V_\mathcal{T})$ to be a partition of V such that all sources are in $V_\mathcal{S}$ and all sinks are in $V_\mathcal{T}$. Define

$$\text{cut}(P) = \{(a, b) \in E | a \in V_\mathcal{S}, b \in V_\mathcal{T}\}.$$

Further, for any non-empty subset $T' \subseteq \mathcal{T}$ define

$$\begin{aligned} L^P_{T'} &= \{e \in \text{cut}(P) : e \text{ is upstream of all } t \in T' \\ &\qquad \text{and } e \text{ is not upstream of any } t \in \mathcal{T} \backslash T'\}. \end{aligned}$$

Note that for any $T', T'' \subseteq \mathcal{T}$ such that $T' \neq T''$, $L^P_{T'} \cap L^P_{T''} = \emptyset$, therefore,

$$|\text{cut}(P)| = \sum_{T' \subseteq \mathcal{T}} |L^P_{T'}| \tag{6.6}$$

As in [36, 37], we use the following definition:

Definition 8. *A subset of links $Q \subseteq$ cut(P) is said to satisfy the downstream condition (DC) if none of the remaining links in cut(P) are downstream of any link in Q.*

Let $\mathbb{U} = \{(u_1, u_2, \ldots, u_m)\}$ denote the z-error correction capacity region of $\mathcal{G}$. In Theorem 10, we derive an upper bound on $\mathbb{U}$ by considering an optimization that chooses subsets $S^P_{T'}$ of each set $L^P_{T'}$ of links on cut(P) such that the union of the chosen subsets satisfies DC and at most $2z$ chosen links are upstream of each sink.

Theorem 10. *For any $(u_1, u_2, \ldots, u_m) \in \mathbb{U}$*

$$\sum_{j=1}^{m} u_j \leq \min_{P=(V_\mathcal{S}, V_\mathcal{T})} (|cut(P)| - l^P),$$

where l^P is a solution to

$$\textit{maximize } l^P = \sum_{T' \subseteq \mathcal{T}} |S^P_{T'}| \tag{6.7}$$

$$\textit{subject to}$$

$$\forall t_i \in \mathcal{T} \quad \sum_{T' \subseteq \mathcal{T} : t_i \in T'} |S^P_{T'}| \leq 2z \tag{6.8}$$

$$\forall T' \subseteq \mathcal{T} \quad |S^P_{T'}| \leq |L^P_{T'}| \tag{6.9}$$

$$\bigcup_{T' \subseteq \mathcal{T} : t_i \in T'} S^P_{T'} \textit{ satisfies DC.} \tag{6.10}$$

Proof. See Section 6.4. □

In addition to an upper bound given by Theorem 10, in Chapter 7 we prove a tighter upper bound on the z-error correction capacity region of two-sink nonmulticast networks.

6.4 Proofs

Proof of Lemma 12. (6.1) and (6.2) follow from definitions of $W_t^{rec}(\mathbf{y})$, $W_t^{msg}(\mathbf{x}_{\mathcal{S}_t})$ and linearity of the code. To prove (6.3) note that:

$$\begin{aligned} D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^1_{\mathcal{S}_t}) &= W_t^{msg}(\mathbf{x}_{\mathcal{S}_t} - \mathbf{x}^1_{\mathcal{S}_t}) \\ &= W_t^{rec}((\mathbf{x}_{\mathcal{S}_t} - \mathbf{x}^1_{\mathcal{S}_t})A_{\mathcal{S}_t}F_t) \\ &= D_t^{rec}(\mathbf{x}_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t, \mathbf{x}^1_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t). \end{aligned}$$

□

Proof of Lemma 13. Consider $\mathbf{z}^1 \in \Upsilon_t(\mathbf{y}^1 - \mathbf{y})$ and $\mathbf{z}^2 \in \Upsilon_t(\mathbf{y} - \mathbf{y}^2)$ such that $D_t^{rec}(\mathbf{y}^1, \mathbf{y}) = w_H(\mathbf{z}^1)$ and $D_t^{rec}(\mathbf{y}, \mathbf{y}^2) = w_H(\mathbf{z}^2)$. By linearity of the code, $\mathbf{z}^1 + \mathbf{z}^2 \in \Upsilon_t(\mathbf{y}^1 - \mathbf{y}^2)$, therefore

$$\begin{aligned} D_t^{rec}(\mathbf{y}^1, \mathbf{y}^2) &= W_t^{rec}(\mathbf{y}^1 - \mathbf{y}^2) \\ &\leq w_H(\mathbf{z}^1 + \mathbf{z}^2) \\ &\leq w_H(\mathbf{z}^1) + w_H(\mathbf{z}^2) \\ &\leq D_t^{rec}(\mathbf{y}^1, \mathbf{y}) + D_t^{rec}(\mathbf{y}, \mathbf{y}^2). \end{aligned}$$

(6.5) follows from (6.4) and (6.3):

$$\begin{aligned} & D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) \\ = \; & D_t^{rec}(\mathbf{x}^1_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t, \mathbf{x}^2_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t) \\ \leq \; & D_t^{rec}(\mathbf{x}^1_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t, \mathbf{x}_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t) + D_t^{rec}(\mathbf{x}_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t, \mathbf{x}^2_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t) \\ = \; & D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}_{\mathcal{S}_t}) + D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}). \end{aligned}$$

□

Proof of Theorem 8. 1 ⇒ 2. For a message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ and an error vector $\mathbf{z}$, the received vector at t is given by

$$\mathbf{y}_t = \mathbf{x}_{\mathcal{S}_t}A_{\mathcal{S}_t}F_t + \mathbf{x}_{\overline{\mathcal{S}}_t}A_{\overline{\mathcal{S}}_t}F_t + \mathbf{z}F_t$$

for some $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$. We will show that if $d_{\min,t} \geq 2z+1$, the minimum distance decoding algorithm will always decode correctly for any message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ and any error vector $\mathbf{z}$ such that $w_H(\mathbf{z}) \leq z$. By (6.4) for any $\mathbf{x}'_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ such that $\mathbf{x}_{\mathcal{S}_t} \neq \mathbf{x}'_{\mathcal{S}_t}$ we have

$$\begin{aligned} & D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}'_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t) \\ \leq \; & D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t) + D_t^{rec}(\mathbf{x}'_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t). \qquad (6.11) \end{aligned}$$

Note that

$$\begin{aligned} & D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}'_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t) \\ = \; & D_t^{msg}(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}'_{\mathcal{S}_t}) \geq d_{\min,t} \geq 2z+1 \qquad (6.12) \\ & D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t) = W_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t - \mathbf{y}_t) \\ = \; & W_t^{rec}(\mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t) \leq w_H(\mathbf{z}) \leq z. \qquad (6.13) \end{aligned}$$

Now using (6.11)-(6.13), we get

$$\begin{aligned} & D_t^{rec}(\mathbf{x}'_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t) \\ \geq \; & D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{x}'_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t) - D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t). \\ \geq \; & z+1 > D_t^{rec}(\mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t, \mathbf{y}_t). \end{aligned}$$

Hence, the decoder outputs $\widehat{\mathbf{x}} = \mathbf{x}_{\mathcal{S}_t}$ and $1 \Rightarrow 2$ follows.

$2 \Rightarrow 1$. We will prove this by contradiction. Assume that any error $\mathbf{z}$ with $w_H(\mathbf{z}) \leq z$ can be corrected at t, but $d_{\min,t} \leq 2z$. Take any $\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}, \mathbf{x}^1_{\mathcal{S}_t} \neq \mathbf{x}^2_{\mathcal{S}_t}$ such that $W_t^{rec}((\mathbf{x}^1_{\mathcal{S}_t} - \mathbf{x}^2_{\mathcal{S}_t}) A_{\mathcal{S}_t} F_t) = D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) \leq 2z$. Then by definition of $W_t^{rec}(.)$ there exist error vectors $\mathbf{z}$ and $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that

$$(\mathbf{x}^1_{\mathcal{S}_t} - \mathbf{x}^2_{\mathcal{S}_t}) A_{\mathcal{S}_t} F_t = \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t \qquad (6.14)$$

with $w_H(\mathbf{z}) \leq 2z$. Hence, we can find error vectors $\mathbf{z}^1$ and $\mathbf{z}^2$ such that $\mathbf{z} = \mathbf{z}^2 - \mathbf{z}^1$, $w_H(\mathbf{z}^1) \leq z$ and $w_H(\mathbf{z}^2) \leq z$. Also, by linearity of the code, we can find $\mathbf{x}^1_{\overline{\mathcal{S}}_t}, \mathbf{x}^2_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that $\mathbf{x}_{\overline{\mathcal{S}}_t} = \mathbf{x}^2_{\overline{\mathcal{S}}_t} - \mathbf{x}^1_{\overline{\mathcal{S}}_t}$. Therefore, if $\mathbf{y}_t$ is received at t,by (6.14) we have two indistinguishable possibilities, a contradiction:

$$\mathbf{y}_t = \mathbf{x}^1_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}^1_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^1 F_t$$
$$\mathbf{y}_t = \mathbf{x}^2_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}^2_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^2 F_t.$$

1 ⇒ 3. Let $d_{\min,t} \geq 2z+1$ and $|\rho| \leq 2z$. In order to prove the implication, we need to show that for any received vector $\mathbf{y}_t$, there is a unique message vector $\mathbf{x}_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}$ and some $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ and error $\mathbf{z} \in \rho$, such that

$$\mathbf{y}_t = \mathbf{x}_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t.$$

Call such $(\mathbf{x}_{\mathcal{S}_t}, \mathbf{x}_{\overline{\mathcal{S}}_t}, \mathbf{z})$ a solution of the decoding problem. Suppose the problem has two distinct solutions $(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^1_{\overline{\mathcal{S}}_t}, \mathbf{z}^1)$ and $(\mathbf{x}^2_{\mathcal{S}_t}, \mathbf{x}^2_{\overline{\mathcal{S}}_t}, \mathbf{z}^2)$. Then we have

$$\begin{aligned} D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) &= W_t^{rec}((\mathbf{x}^1_{\mathcal{S}_t} - \mathbf{x}^2_{\mathcal{S}_t}) A_{\mathcal{S}_t} F_t) \\ &= W_t^{rec}((\mathbf{x}^2_{\overline{\mathcal{S}}_t} - \mathbf{x}^1_{\overline{\mathcal{S}}_t}) A_{\overline{\mathcal{S}}_t} F_t + (\mathbf{z}^2 - \mathbf{z}^1) F_t) \\ &\leq w_H(\mathbf{z}^2 - \mathbf{z}^1). \end{aligned}$$

Since both $\mathbf{z}^1, \mathbf{z}^2 \in \rho$, we have $D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) \leq w_H(\mathbf{z}^2 - \mathbf{z}^1) \leq 2z$, which contradicts the fact that $d_{\min,t} \geq 2z+1$.

3 ⇒ 1. Assume that any erasure pattern ρ with $|\rho| \leq 2z$ can be corrected at t, but $d_{\min,t} \leq 2z$. Take any $\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t} \in \mathbb{F}_q^{r_{\mathcal{S}_t}}, \mathbf{x}^1_{\mathcal{S}_t} \neq \mathbf{x}^2_{\mathcal{S}_t}$ such that $W_t^{msg}((\mathbf{x}^1_{\mathcal{S}_t} - \mathbf{x}^2_{\mathcal{S}_t}) A_{\mathcal{S}_t} F_t) = D_t^{msg}(\mathbf{x}^1_{\mathcal{S}_t}, \mathbf{x}^2_{\mathcal{S}_t}) \leq 2z$. Therefore, by definition of $W_t^{msg}(.)$ there exist error vectors $\mathbf{z}$ and $\mathbf{x}_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that

$$(\mathbf{x}^1_{\mathcal{S}_t} - \mathbf{x}^2_{\mathcal{S}_t}) A_{\mathcal{S}_t} F_t = \mathbf{x}_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z} F_t \tag{6.15}$$

with $w_H(\mathbf{z}) \leq 2z$. Hence, we can choose error vectors $\mathbf{z}^1, \mathbf{z}^2 \in \rho$ such that $\mathbf{z} = \mathbf{z}^2 - \mathbf{z}^1$. Also, by linearity of the code, we can find $\mathbf{x}^1_{\overline{\mathcal{S}}_t}, \mathbf{x}^2_{\overline{\mathcal{S}}_t} \in \mathbb{F}_q^{r_{\overline{\mathcal{S}}_t}}$ such that $\mathbf{x}_{\overline{\mathcal{S}}_t} = \mathbf{x}^2_{\overline{\mathcal{S}}_t} - \mathbf{x}^1_{\overline{\mathcal{S}}_t}$. Therefore, if $\mathbf{y}_t$ is received at t, by (6.15) we have two indistinguishable possibilities

$$\mathbf{y}_t = \mathbf{x}^1_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}^1_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^1 F_t$$
$$\mathbf{y}_t = \mathbf{x}^2_{\mathcal{S}_t} A_{\mathcal{S}_t} F_t + \mathbf{x}^2_{\overline{\mathcal{S}}_t} A_{\overline{\mathcal{S}}_t} F_t + \mathbf{z}^2 F_t.$$

Hence, 3 ⇒ 1 follows. □

Proof of Theorem 9. The network code $\tilde{\mathcal{C}}$ is obtained by applying a random linear pre-code at each source S_i. That is, the length-$(r_i - 2z)$ vector of source symbols $\tilde{\mathbf{x}}_i$ is multiplied by R_i, an $(r_i - 2z) \times r_i$ matrix with entries chosen uniformly at random from $\mathbb{F}_q$, to form the input

$$\mathbf{x}_i = \tilde{\mathbf{x}}_i R_i \tag{6.16}$$

to the original code. Let $\tilde{r}_{\mathcal{S}'} = \sum_{i \in \mathcal{S}'} (r_i - 2z) = r_{\mathcal{S}'} - 2|\mathcal{S}'|z$.

Consider any sink t. For any $\mathbf{x} \in \mathbb{F}_q^{\tilde{r}_{\mathcal{S}}}$, under the original code $\mathcal{C}$, in the absence of any errors or erasures, sink t receives

$$\mathbf{y}_t = \mathbf{x}M, \tag{6.17}$$

where $M = A_{\mathcal{S}} F_t$, and applies a decoding matrix B to obtain its demanded source symbols $\mathbf{x}MB = \mathbf{x}_{\mathcal{S}_t}$.

Consider any network erasure pattern ρ with $|\rho| = 2z$, and any $\mathbf{z} \in \rho$. Let $\mathbf{s}$ be the length-$2z$ vector of nonzero symbols in $\mathbf{z}$, and let Q be the $2z \times |In_t|$ network transfer matrix from the symbols in $\mathbf{s}$ to the symbols on the sink's incoming links In_t. The vector received at t is

$$\mathbf{y}' = \mathbf{x}M + \mathbf{s}Q.$$

Sink t applies its original decoding matrix B to obtain

$$\mathbf{y}'B = \mathbf{x}MB + \mathbf{s}QB = \mathbf{x}_{\mathcal{S}_t} + \mathbf{s}QB. \tag{6.18}$$

Let $a \leq 2z$ be the rank of QB, and let P be a submatrix of QB consisting of a linearly independent rows. Then $\mathbf{s}QB$ can be represented by $\mathbf{s}GP$, where $G \in \mathbb{F}_q^{2z \times a}$. Hence, (6.18) can be rewritten as

$$\mathbf{y}'B = \begin{pmatrix} \tilde{\mathbf{x}}_{\mathcal{S}_t} & \mathbf{s}' \end{pmatrix} \begin{pmatrix} R \\ P \end{pmatrix} \tag{6.19}$$

where $\mathbf{s}'$ is a length-a vector of unknowns, and from (6.16), $R \in \mathbb{F}_q^{\tilde{r}_{\mathcal{S}_t} \times r_{\mathcal{S}_t}}$ is a block diagonal matrix with blocks $R_i, i \in \mathcal{S}_t$. Since each R_i has $2z$ fewer rows than columns and has all entries chosen uniformly at random from $\mathbb{F}_q$, the rows of R are linearly independent of the $a \leq 2z$ rows of P. Thus, $\begin{pmatrix} R \\ P \end{pmatrix}$ has full row rank and (6.19) can be solved for $\tilde{\mathbf{x}}_{\mathcal{S}_t}$.

Therefore, we can construct code $\tilde{\mathcal{C}}$ that achieves rate vector $\mathbf{r}_{2z} = (r_1 - 2z, r_2 - 2z, \ldots, r_n - 2z)$ under any network erasure pattern ρ with $|\rho| \leq 2z$. Now Theorem 8 implies that $\tilde{\mathcal{C}}$ has minimum distance $d_{min} \geq 2z + 1$ and that $\tilde{\mathcal{C}}$ can correct arbitrary errors on up to z links in the network. □

Proof of Theorem 10. We prove the statement of this theorem by contradiction. Suppose there exists $(u_1^*, u_2^*, \ldots, u_m^*) \in \mathbb{U}_{1,m}$ such that for some $P = (V_{\mathcal{S}}, V_{\mathcal{T}})$

$$\sum_{i=j}^{m} u_j^* > M - l^P. \tag{6.20}$$

For notational convenience let $|\text{cut}(P)| = M$ and denote the links in cut(P) by $\{a_1, a_2, \ldots, a_m\}$ indexed in increasing topological order. By (6.20), for any $M - l^p$ links there exist two codewords $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m)$ and $\mathbf{y} = (\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_m)$ in $\mathcal{C}$, $\mathbf{x} \neq \mathbf{y}$, such that $\phi_{a_f}(\mathbf{x}) = \phi_{a_f}(\mathbf{y})$ for $M - l^p$ indexes a_f. Note that by (6.6) and (6.7), the set $\text{cut}(P) \backslash \left(\bigcup_{T' \subseteq \mathcal{T}} S_{T'}^P \right)$ has size

$$M - l^P = \sum_{T' \subseteq \mathcal{T}} \left(|L_{T'}^P| - |S_{T'}^P| \right),$$

therefore, by (6.20) we can choose $\mathbf{x}$ and $\mathbf{y}$ so that

$$\phi_{a_f}(\mathbf{x}) \;\; = \;\; \phi_{a_f}(\mathbf{y}),\ a_f \in \text{cut}(P) \backslash \left(\bigcup_{T' \subseteq \mathcal{T}} S_{T'}^P \right) \tag{6.21}$$

Since $\mathbf{x} \neq \mathbf{y}$, there exists at least one index $i \in \{1, \ldots, m\}$ such that $\mathbf{x}_i \neq \mathbf{y}_i$. We will now demonstrate that if (6.20) holds, then there exists an adversarial error pattern such that t_i will not be able to distinguish between $\mathbf{x}$ and $\mathbf{y}$. Define $L_I = \bigcup_{T' \subseteq \mathcal{T} : t_i \in T'} L_{T'}^P$ to be the subset of links of cut(P) upstream of t_i and let $I = |L_I|$. By (6.21), $\mathbf{x}$ and $\mathbf{y}$ were chosen so that $\phi_{a_f}(\mathbf{x}) = \phi_{a_f}(\mathbf{y})$ in at least $J = I - \sum_{T' \subseteq \mathcal{T} : t_i \in T'} |S_{T'}^P|$ positions. By constraint (6.8), $J \geq I - 2z$.

Define the error-free output of the links in L_I by

$$O(\mathbf{x}) = \{\phi_{f_1}(\mathbf{x}), \phi_{f_2}(\mathbf{x}), \dots, \phi_{f_I}(\mathbf{x})\},$$

where all links $f_l \in L_I$ and $\phi_{f_l}(.)$ are indexed in the increasing coding order. Hence, by (6.10) and (6.21) we can write

$$\begin{aligned} O(\mathbf{x}) &= \{x_1, x_2, \dots, x_J, x'_{J+1}, \dots, x'_I\} \\ O(\mathbf{y}) &= \{x_1, x_2, \dots, x_J, x''_{J+1}, \dots, x''_I\}. \end{aligned}$$

Assume the network input is $\mathbf{x}$. The adversary will inject z error symbols $\mathbf{z}_x = (z_{x_1}, z_{x_2}, \dots, z_{x_z})$ on links $a_{f_{J+1}}, \dots, a_{f_{J+z}}$ as follows. First it injects z_{x_1} on link $a_{f_{J+1}}$ so that

$$\psi_{a_{f_{J+1}}}(\mathbf{x}, (z_{x_1}, 0, 0, \dots, 0)) = x''_{J+1}.$$

Then the output of links $a_{f_{J+2}}, \dots, a_{f_I}$ is affected, but not of $a_{f_1}, \dots, a_{f_J}$. With this consideration, next the adversary injects the symbols z_{x_2} on link $a_{f_{J+2}}$ so that

$$\psi_{a_{f_{J+2}}}(\mathbf{x}, (z_{x_1}, z_{x_2}, 0 \dots, 0)) = x''_{J+2}.$$

The output of links $a_{f_{J+3}}, \dots, a_{f_I}$ is affected, but not of $a_{f_1}, \dots, a_{f_{J+1}}$. The process continues until the adversary finishes injecting z errors at links $a_{J+1}, \dots, a_{J+z}$. Let $E(\mathbf{x}, \mathbf{z}) = \{\psi_{a_{f_1}}(\mathbf{x}, \mathbf{z}), \dots, \psi_{a_{f_I}}(\mathbf{x}, \mathbf{z})\}$, then

$$E(\mathbf{x}, \mathbf{z}_x) = \{x_1, \dots, x_J, x''_{J+1}, \dots, x''_{J+z}, x'''_{J+z+1}, \dots, x'''_I\}.$$

Now suppose the network input is $\mathbf{y}$. The adversary will inject z error symbols $\mathbf{z}_y = (z_{y_1}, z_{y_2}, \dots, z_{y_z})$ on links $a_{f_{J+z+1}}, \dots, a_{f_I}$ as follows. First it injects z_{y_1} on link $a_{f_{J+z+1}}$ so that

$$\psi_{a_{f_{J+z+1}}}(\mathbf{x}, (z_{y_1}, 0, 0, \dots, 0)) = x'''_{J+z+1}.$$

Then the output of links $a_{f_{J+z+2}}, \dots, a_{f_I}$ is affected, but not of $a_{f_1}, \dots, a_{f_{J+z}}$. With this consideration, next the adversary injects the symbols z_{y_2} on link $a_{f_{J+z+2}}$ so that

$$\psi_{a_{f_{J+z+2}}}(\mathbf{x}, (z_{y_1}, z_{y_2}, 0 \ldots, 0)) = x'''_{J+2+1}.$$

The output of links $a_{f_{J+z+3}}, \ldots, a_{f_I}$ is affected, but not of $a_{f_1}, \ldots, a_{f_{J+z+1}}$. Similarly, the process continues until the adversary finishes injecting at most z errors at links $a_{J+z+1}, \ldots, a_I$. Then

$$E(\mathbf{x}, \mathbf{z}_y) \quad = \quad \{x_1, \ldots, x_J, x''_{J+1}, \ldots, x''_{J+z}, x'''_{J+z+1}, \ldots, x'''_I\}.$$

Therefore, since t_i is upstream of links only in L_I, it can observe only $E(\mathbf{x}, \mathbf{z}_x)$ and $E(\mathbf{y}, \mathbf{z}_y)$, hence, it would not be able to distinguish between $\mathbf{x}$ and $\mathbf{y}$.

Thus, for any $P = (V_\mathcal{S}, V_\mathcal{T})$

$$\sum_{j=1}^{m} u_j^* \leq |\text{cut}(P)| - l^P,$$

therefore,

$$\sum_{j=1}^{m} u_j \leq \min_{P=(V_\mathcal{S}, V_\mathcal{T})} (|\text{cut}(P)| - l^P).$$

□

Chapter 7

Network error correction in nested-demand and two-sink network topologies

7.1 Introduction

In this chapter we continue to investigate error correction capacity regions of nonmulticast networks. In particular, we consider nonmulticast network topologies with two sinks and nested-demands, whose capacity regions are known to be given by the cutset bounds in the error-free case [19, 20, 21, 9]. We show that cutset bounds are not tight in networks with with errors. We also make a connection between erasure correction in real-time streaming data systems and nonmulticast erasure correction problem in 3-layer networks with nested sink demands.

In real-time streaming of data such as audio or video conferencing time performance is critical, which severely constraints feasible erasure code constructions. In these scenarios, it is critical that network communications are decodable in real-time, that is with bounded delay, and that the code used is designed for the widest possible range of failure patterns that can occur during packet transmission. The work of [38] proposes delay-optimal convolutional codes that can be applied in streaming scenarios when erasures occur in bursts and are separated by a certain number of unerased symbols. However, in practice larger sets of erasure patterns need to be corrected. In this chapter, we propose a solution to the streaming erasure problem from the viewpoint of worst-case and sliding-window erasure models, under both of which the set of permissible erasure patterns is larger. We develop a set of tools that can be applied to refine cutset upper bounds for nested-demand network topologies and use them to design streaming systems tolerant to erasures so that no intersession coding is required between packets at different streaming checkpoints. Our code constructions combat a wider range of permissible erasure patterns using only intrasession coding.

We further apply the upper-bounding techniques established for nested-demand network topologies to construct an instance of multiple description codes that are designed so that the sink decodes at various quality levels depending of the number of erasures that occurred [39]. Another application of our cutset-refining upper bounds is to two-sink networks, where we use them to show that our achievability construction in Chapter 6 is capacity-achieving for a family of two-sink 3-layer networks, and employ them to derive tighter outer bounds for error- and erasure-correction capacity regions of arbitrary two-sink networks beyond those given in Chapter 6.

7.2 Model

7.2.1 3-layer networks

We consider a streaming system vulnerable to packet erasures, where the receiver needs to decode the source information at multiple time instances $\{m_1, m_2, m_3, \ldots\}$, so that at time m_1 message M_1 is decoded, at time m_2 messages M_1 and M_2 are decoded, at time m_3 messages M_1, M_2 and M_3 are decoded, and so on. Furthermore, all messages $M_1, M_2, M_3, \ldots$ are independent.

Definition 9. *A 3-layer network is a multisource, nonmulticast network that consists of the following elements:*

- *Four layers of nodes: the set of source nodes, the set of coding nodes, the set of relay nodes and the set of sink nodes.*
- *Three layers of directed edges: the first layer that connects the source nodes to the coding nodes, the second layer that connects the coding nodes to the relay nodes, and the third layer that connects the relay nodes to the sink nodes.*

A useful application of 3-layer networks is that one can view the above-described streaming erasure network scenario with n checkpoints as an erasure correction problem on a 3-layer network with n nested sink demands. That is, in the case of a streaming system with n

checkpoints $\{m_1, m_2, \ldots, m_n\}$, we need to consider a one-source n-sink 3-layer network $\mathcal{G}_s$ with sinks $\{t_1, t_2, \ldots, t_n\}$ constructed so that (see Figure 7.1 for example):

- There are m_n links in the second layer.
- There is an outgoing link from the source to each link in the second layer.
- Each sink t_i has m_i incoming links from the links $1, \ldots, m_i$ in the second layer.

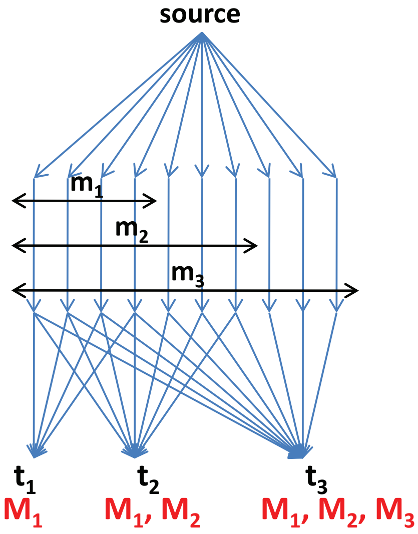


Figure 7.1: Example of $\mathcal{G}_s$ with three nested sink demands.

Hence, 3-layer networks are interesting as a tool for streaming code construction problems. They also provide a useful framework for studying the capacity regions of general nonmulticast networks. For instance, one may construct a 3-layer network that corresponds to every cut that separates some collection of sources from some collection of sinks in the original network by observing that all nodes on the source side of the cut can cooperate perfectly, which gives each sink at least as much information as it receives in the original network. Hence, the error-free and error capacity regions of a 3-layer network constructed in this way provide upper bounds on the corresponding error-free and error capacity regions of the original network. We explore this observation in greater detail in Section 7.3.4, where we give an upper bound on the error-correction capacity region for general two-sink networks.

7.2.2 Erasure model

The problem of streaming real-time data, such as in audio or video conferencing, or media streaming, puts specific constraints on permissible code constructions. This problem is especially challenging when erasures might happen in the course of normal transmission - the encoder has to design codes without knowing a priori which of a possible set of erasure patterns occurs. The assumption that any packet can fail with a certain probability (i.e., Markov erasure model) would be the most realistic description of streaming erasure systems, however, because of the large number of possible Markov states this problem is hard to handle theoretically. Real-life streaming systems generally transmit a large number of packets and have a large number of streaming checkpoints (i.e., nested sinks of $\mathcal{G}_s$). Worst-case erasure models, where at most z links of $\mathcal{G}_s$ can fail, are not realistic for such systems because in reality the number of erasures is proportional to the number of transmitted packets. Therefore, along with studying the worst-case erasure model, we adapt a more practical sliding-window erasure model with the assumption that at most x out any y consecutive links in the second layer of $\mathcal{G}_s$ can be erased. The work of [38] considers a similar streaming erasure problem; however, their erasure model assumes that any burst of at most x erasures is separated by at least $y-x$ unerased packets. Our sliding window erasure model removes this restriction, which leads to correction of a larger class of permissible erasure patterns.

Definition 10. *The set of all rate vectors $\mathbb{U} = (u_1, u_2, \ldots, u_n)$ that can be achieved on $\mathcal{G}_s$ under any z network link erasures is called z-erasure correction capacity region.*

Definition 11. *A set of consecutive links in the second layer of $\mathcal{G}_s$ is said to satisfy an x/y sliding-window erasure condition if at most x out of any y consecutive links are erased.*

Definition 12. *The set of all rate vectors $\mathbb{V} = (v_1, v_2, \ldots, v_n)$ that can be achieved on $\mathcal{G}_s$ if any set of y consecutive links in the second layer of $\mathcal{G}_s$ satisfies the x/y sliding-window erasure condition is called x/y-erasure correction capacity region.*

Index the links in the second layer of $\mathcal{G}_s$ by $1, 2, \ldots, m_n$, so that links $1, \ldots, m_1$ are upstream of t_1, and links $m_1 + 1, \ldots, m_2$ are upstream of t_2 and so on. Let $\mathcal{I}$ be the set of links in the second layer of $\mathcal{G}_s$. For every $i = 1, \ldots, n$, we can represent m_i as

$$m_i = \lfloor \frac{m_i}{y} \rfloor y + x_i, 0 \leq x_i \leq y - 1, \tag{7.1}$$

where x_i is the remainder of division of m_i modulo y.

Let E_i be the maximum number of erasures that can occur upstream of t_i under the x/y sliding-window erasure model.

Definition 13. *A set of consecutive links $k, \dots, j \in \mathcal{I}$ is said to satisfy an alternating x/y sliding-window erasure condition if link $i \in \mathcal{I}$ is erased if and only if $1 \leq (i - (k-1)) \mod y \leq x$.*

Denote the random processes transmitted on links $1, \dots, m_n$ by $X_1, X_2, \dots, X_{m_n}$. For any K, define the set of random processes transmitted on links $1, \dots, K$ by $X^K = \{X_1, X_2, \dots, X_K\}$.

Definition 14. *For any sink $i = 1, \dots, n$, define a set of random processes Y as a decoding information set for message M_i under the worst-case erasure model if $|Y| = m_i - z$ and Y is transmitted on links of the second layer of $\mathcal{G}_s$ upstream of sink t_i. Define $D_i = |Y|$ to be the size of any decoding information set for M_i under the worst-case erasure model.*

Definition 15. *For any sink $i = 1, \dots, n$, define a set of random processes Y as a decoding information set for message M_i under the x/y sliding-window erasure model if $|Y| = m_i - E_i$, where Y is transmitted on links of the second layer of $\mathcal{G}_s$ upstream of sink t_i and $X^{m_i} \diagdown Y$ satisfies the x/y sliding-window erasure condition.*

7.3 Main results

7.3.1 Nested-demand erasure correction capacity

Let $\mathcal{G}_s$ be a 3-layer network with nested sink demands as defined in Section 7.2.1. Prior to deriving a family of upper bounds on the erasure correction capacity regions for the worst-case erasure model, we prove several auxiliary statements that we subsequently use in our construction.

Lemma 14. *For any sink $i = 1, \dots, n$ of $\mathcal{G}_s$ and any random process Z transmitted on links $1, \dots, m_n$*

$$I(M_{i+1}, \dots, M_n; Z | M_1, \dots, M_i) = H(Z | M_1, \dots, M_i).$$

Proof. Proof given in Section 7.4.2. □

Lemma 15. *For any sink $i = 1, \ldots, n$ of $\mathcal{G}_s$ and any random process Y, such that Y is a decoding information set for message M_i*

$$H(Y|M_1, \ldots, M_{i-1}) = u_i + H(Y|M_1, \ldots, M_i).$$

Proof. Proof given in Section 7.4.2. □

Lemma 15 implies that $H(Y|M_1, \ldots, M_{i-1})$ can be interpreted as the residual capacity of what is left for $M_i, \ldots, M_n$ after $M_1, \ldots, M_{i-1}$.

Consider any set of random processes $Z = \{X_1, X_2, \ldots, X_{|Z|}\}$ transmitted on the links of the second layer of $\mathcal{G}_s$. Let S be the set of all lexicographically ordered subsets of $\{1, 2, \ldots, |Z|\}$. For any $\sigma \in S$, let $\sigma(k)$ be the kth element of σ. Let $\{Y_{\sigma_1}, Y_{\sigma_2}, \ldots, Y_{\sigma_F}\}$ be the set of all unordered subsets of Z of size D and let $F = \begin{pmatrix} |Z| \\ D \end{pmatrix}$.

Lemma 16. *For a set of random processes Z defined as above:*

$$|Z| \sum_{\sigma \in S} H(Y_\sigma) \geq D \begin{pmatrix} |Z| \\ D \end{pmatrix} H(Z). \tag{7.2}$$

Proof. Proof given in Section 7.4.2. □

Lemma 17. *For any set of random processes Y and a set of random processes Z defined as above:*

$$|Z| \sum_{\sigma \in S} H(Y, Y_\sigma) \geq D \begin{pmatrix} |Z| \\ D \end{pmatrix} H(Y, Z). \tag{7.3}$$

Proof. Proof given in Section 7.4.2. □

For each $i = 1, \ldots, n$, let S_i be the set of all lexicographically ordered subsets of $\{1, 2, \ldots, m_i\}$. For any $\sigma \in S_i$, let $\sigma(k)$ be the kth element of σ. Also let $\{Y^i_{\sigma_1}, Y^i_{\sigma_2}, \ldots, Y^i_{\sigma_{F_i}}\}$ be the set of all decoding information sets for M_i under the worst-case erasure model, where $F_i = \begin{pmatrix} m_i \\ D_i \end{pmatrix}$.

We know that for any $\sigma \in S$

$$H(Y^1_\sigma) \leq D_1.$$

Then by Lemma 15

$$H(Y^1_\sigma) = u_1 + H(Y^1_\sigma|M_1) \leq D_1. \tag{7.4}$$

Note that in the case where there is only one sink in $\mathcal{G}_s$, $H(Y^1_\sigma|M_1) = 0$ and

$$u_1 \leq D_1. \tag{7.5}$$

We describe the procedure to obtain higher-dimensional constraints from (7.4) by considering all possible types of decoding information sets for each message M_i.

- *Step 1.* Summing (7.4) over the $\begin{pmatrix} m_1 \\ D_1 \end{pmatrix}$ choices of $Y^1_\sigma \subseteq X^{m_1}$, we get

  $$\begin{pmatrix} m_1 \\ D_1 \end{pmatrix} u_1 + \sum_{\sigma \in S_1} H(Y^1_\sigma|M_1) \leq \begin{pmatrix} m_1 \\ D_1 \end{pmatrix} D_1.$$

  After multiplying by m_1, Lemma 16 gives

  $$m_1 \begin{pmatrix} m_1 \\ D_1 \end{pmatrix} u_1 + D_1 \begin{pmatrix} m_1 \\ D_1 \end{pmatrix} H(X^{m_1}|M_1) \leq \begin{pmatrix} m_1 \\ D_1 \end{pmatrix} D_1 m_1,$$

  or

  $$\frac{m_1}{D_1} u_1 + H(X^{m_1}|M_1) \leq m_1. \tag{7.6}$$

  Consider any Y^2_Δ, $\Delta \in S_2$ such that $X^{m_1} \subseteq Y^2_\Delta$, that is, $Y^2_\Delta = \{X^{m_1}, Z^2\}$ for some set of random processes Z^2 such that $H(Z^2) \leq m_2 - m_1 - z$. Then

  $$H(Y^2_\Delta|M_1) \leq H(X^{m_1}|M_1) + H(Z^2|M_1) \leq H(X^{m_1}|M_1) + m_2 - m_1 - z. \tag{7.7}$$

  Therefore, after adding $m_2 - m_1 - z$ to both sides of (7.6), we get:

  $$\frac{m_1}{D_1} u_1 + H(Y^2_\Delta|M_1) \leq m_2 - z = D_2. \tag{7.8}$$

  Note that for every $\Delta \in S_2$, Y^2_Δ is a decoding information set for M_2, therefore, by

Lemma 15,

$$H(Y^2_\Delta|M_1) = u_2 + H(Y^2_\Delta|M_1, M_2).$$

Then (7.8) can be rewritten as:

$$\frac{m_1}{D_1}u_1 + u_2 + H(Y^2_\Delta|M_1M_2) \leq D_2. \tag{7.9}$$

Note that in the case where there are two sinks in $\mathcal{G}_s$, $H(Y^2_\Delta|M_1M_2) = 0$ and (7.9) can be rewritten as

$$\frac{m_1}{D_1}u_1 + u_2 \leq D_2. \tag{7.10}$$

Otherwise, summing (7.9) over the $\begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}$ choices of Y^2_Δ, $\Delta \in S_2$, for which $X^{m_1} \subseteq Y^2_\Delta$, gives:

$$\frac{m_1}{D_1}\begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}u_1 + \begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}u_2 + \sum_{\Delta \in S_2 : X^{m_1} \subseteq Y^2_\Delta} H(Y^2_\Delta|M_1M_2) \leq D_2 \begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}. \tag{7.11}$$

Applying Lemma 17 to $\sum_{\Delta \in S_2 : X^{m_1} \subseteq Y^2_\Delta} H(Y^2_\Delta|M_1M_2)$ and repeating*Step 1*, extend the resulting constraints to three dimensions.

- *Step 2.* Consider any Y^2_Δ, $\Delta \in S_2$ such that $X^{m_1} \nsubseteq Y^2_\Delta$, but $Y^1_\sigma \subseteq Y^2_\Delta$. Then $Y^2_\Delta = \{Y^1_\sigma, Z^2\}$ for some set of random processes Z^2 such that $H(Z^2) \leq m_2 - m_1$. Then

$$H(Y^2_\Delta|M_1) \leq H(Y^1_\sigma|M_1) + H(Z^2|M_1) \leq H(Y^1_\sigma|M_1) + m_2 - m_1.$$

Therefore, after adding $m_2 - m_1$ to both sides of (7.4), we get:

$$u_1 + H(Y^2_\Delta|M_1) \leq D_1 + m_2 - m_1 = D_2. \tag{7.12}$$

Note that for every $\Delta \in S_2$, Y^2_Δ is a decoding information set for M_2, therefore, by

Lemma 15 $H(Y^2_\Delta|M_1) = u_2 + H(Y^2_\Delta|M_1, M_2)$. Then (7.12) can be rewritten as:

$$u_1 + u_2 + H(Y^2_\Delta|M_1M_2) \leq D_2. \tag{7.13}$$

Now sum over all $Y^2_\Delta, \Delta \in S_2$ using (7.9) and (7.13) (there are $\begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}$ choices of Y^2_Δ such that $X^{m_1} \subseteq Y^2_\Delta$ and $\begin{pmatrix} m_2 \\ D_2 \end{pmatrix} - \begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}$ choices of Y^2_Δ such that $X^{m_1} \nsubseteq Y^2_\Delta$). Thus:

$$\frac{m_1}{D_1}\begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}u_1 + \left(\begin{pmatrix} m_2 \\ D_2 \end{pmatrix} - \begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix}\right)u_1 + \begin{pmatrix} m_2 \\ D_2 \end{pmatrix}u_2 + \sum_{\Delta \in S_2} H(Y^2_\Delta|M_1M_2) \leq D_2\begin{pmatrix} m_2 \\ D_2 \end{pmatrix}.$$

Applying Lemma 16 to $\sum_{\Delta \in S_2} H(Y^2_\Delta|M_1M_2)$ and proceeding as in *Step 1* and *Step 2*, extends the resulting constraints to three dimensions.

Note that the family of inequalities derived as explained above upper-bounds the z-erasure correction capacity region of $\mathcal{G}_s$. Each one of the upper-bounding inequalities is a cutset-refining bound.

Theorem 11. *The family of inequalities derived as explained above gives an upper bound on the z-erasure correction capacity region of $\mathcal{G}_s$.*

Theorem 12. *In a two-sink case network, explicit characterization of the z-erasure correction capacity region of $\mathcal{G}_s$ is given by*

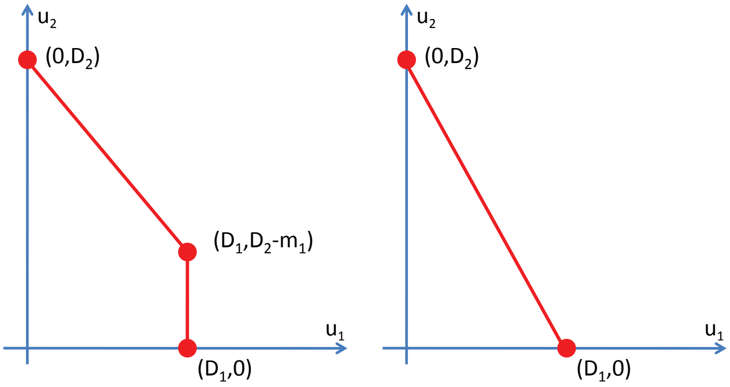
1. *if $m_2 - m_1 \geq z$*

$$u_1 \leq D_1$$
$$\frac{m_1}{D_1}u_1 + u_2 \leq D_2$$

2. *if $m_2 - m_1 < z$*

$$\frac{u_1}{D_1} + \frac{u_2}{D_2} \leq 1.$$

This region can be achieved by intrasession coding for any z(see Figure 7.2(a)- 7.2(b)).



(a) z-erasure correction capacity region when $m_2 - m_1 \geq z$ and $n = 2$.

(b) z-erasure correction capacity region when $m_2 - m_1 < z$ and $n = 2$.

Figure 7.2: Explicit characterization of the z-erasure correction capacity region of a two-sink nested-demand network $\mathcal{G}_s$.

Proof. Proof given in Section 7.4.2. □

We observe that the corner points in low-dimensional cases can be achieved by intrasession coding. We want to show that no intersession coding is required even in larger cases. This would prove that intrasession coding is sufficient to achieve the z-erasure correction capacity region of $\mathcal{G}_s$. In order to prove this, we will show that if the rate vector $(u_1, u_2, \ldots, u_n)$ cannot be achieved for a given intrasession procedure, then it cannot be achieved by any other strategy.

The rate vector $(u_1, u_2, \ldots, u_n)$ satisfies the achievable intrasession solution if and only if for every set of unerased links $P \subseteq \mathcal{I}$ under any z link erasures there exist $y_i^j \geq 0$ such that

$$\forall j = 1, \ldots, n \qquad u_j \leq \sum_{i \in P \cup \{1, \ldots, m_i\}} y_i^j \tag{7.14}$$

$$\forall i = 1, \ldots, m_n \qquad \sum_{j=1}^{n} y_i^j \leq 1. \tag{7.15}$$

Note that $y_i^j = 0$, $i = m_j + 1, \ldots, m_n$ for all $j = 1, \ldots, n-1$. Choose y_i^j so that

- $y_i^1 = T_{1,1}$, $i = 1, \ldots, m_1$
- $y_i^2 = T_{2,1}$, $i = 1, \ldots, m_1$ and $y_i^2 = T_{2,2}$, $i = m_1 + 1, \ldots, m_2$

- $y_i^3 = T_{3,1},\ i = 1,\ldots,m_1,\ y_i^3 = T_{3,2},\ i = m_1+1,\ldots,m_2$ and $y_i^3 = T_{3,3},\ i = m_2+1,\ldots,m_3$
- $\ldots$
- $y_i^n = T_{n,1}, i = 1,\ldots,m_1, y_i^n = T_{n,2}, i = m_1+1,\ldots,m_2, y_i^n = T_{n,3}, i = m_2+1,\ldots,m_3 \ldots y_i^n = T_{n,n}, i = m_{n-1},\ldots,m_n$

for some $T_{i,j} \geq 0$. Let T be the lower triangular $n \times n$ matrix, whose (i,j)th entry is $T_{i,j}$. We consider the case when for every $i = 1,\ldots,n-1$, $m_{i+1} - m_i > z$. For each $i = 1,\ldots,n$, $j = 1,\ldots,i$, assign $T_{i,j}$ so that:

$$T_{1,1} = \frac{u_1}{D_1} \tag{7.16}$$

$$\forall i = 2,\ldots,n \qquad T_{i,1} = \min(1 - \sum_{k=1}^{i-1} T_{k,1}, \frac{u_i}{D_i}) \tag{7.17}$$

$$\forall i = 2,\ldots,n, j = 2,\ldots n \qquad T_{i,j} = \min(1 - \sum_{k=1}^{i-1} T_{k,j}, \frac{u_i - \sum_{k=1}^{j-1} T_{i,k}}{D_j - m_{j-1}}) \tag{7.18}$$

In other words, $T_{i,j}$ are assigned so that the rate to each sink is spread as uniformly as possible subject to the capacity constraints from previous receivers.

For each $k = 1,\ldots,n$, define

$$P_k = m_k - \sum_{i=1}^{k}\sum_{j=1}^{k} T_{i,j}(m_j - m_{j-1}), \tag{7.19}$$

where $m_0 = 0$.

Lemma 18. *The assignment of $T_{i,j}$ given by (7.16)-(7.18) is such that for every $i = 1,\ldots,n$ and $j = 1,\ldots,n-1$*

$$T_{i,j} \leq T_{i,j+1}.$$

Proof. Proof given in Section 7.4.2. □

Lemma 19. *For each $k = 1,\ldots,n-1$, if $H(X^{m_k}|M_1,\ldots,M_k) \leq P_k$ and $z = 1$, then*

$$H(X^{m_{k+1}}|M_1,\ldots,M_{k+1}) \leq P_{k+1}.$$

Proof. Proof given in Section 7.4.2. □

Theorem 13. *The $z-$erasure correction capacity region of $\mathcal{G}_s$ can be achieved by intrasession coding when $z = 1$.*

Proof. Proof given in Section 7.4.2. □

We conjecture (but do not prove) that the z-erasure correction capacity region of $\mathcal{G}_s$ can be achieved by "as uniform as possible" intrasession allocation procedure given by (7.16)-(7.18) for any z. For an example of explicit construction of the family of upper-bounds and corner points that achieve them in four dimensions, see Section 7.4.1. Also, a detailed derivation of the n-dimensional z-erasure correction capacity region when $m_1 \geq m_n - z$ is given in the proof of Theorem 17.

7.3.2 Asymptotic behavior

In this section we study the asymptotic behavior of infinite one-dimensional streaming systems under the assumption that $m_2 - m_1 = m_3 - m_2 = \ldots = m_n - m_{n-1} = \ldots = d$ and $u_1 = u_2 = \ldots = u_n = \ldots = u$. We want to examine the influence of the initial offset m_1 on the performance of capacity-achieving transmission strategies. This setting is motivated by practical video streaming applications where video content starts playing after the initial playout delay that allows for packet buffering.

Theorem 14. *For any number of sinks n, an upper bound on the z-erasure correction capacity region is given by*

$$u \leq \frac{d - z + \frac{zm_1}{d} - (d-z)\left(\frac{d-z}{d}\right)^{n-1}}{1 + \frac{z}{d}\frac{m_1}{m_1 - z} - \left(\frac{d-z}{d}\right)^{n-1}}. \tag{7.20}$$

In particular,

$$u \leq \frac{d - z + \frac{zm_1}{d}}{1 + \frac{z}{d}\frac{m_1}{m_1 - z}}. \tag{7.21}$$

as $n \to \infty$.

Proof. See Section 7.4.2. □

Theorem 15. *As $n \to \infty$, the upper bound (7.21) can be achieved without intersession coding when $m_1 \leq \frac{1}{4}(3d+z) + \frac{1}{4}\sqrt{9d^2 - 2dz + z^2}$ for any z.*

Proof. See Section 7.4.2. □

Theorem 16. *As $n \to \infty$, an upper bound on the z-erasure correction capacity region is given by*

$$u \leq d. \tag{7.22}$$

Proof. See Section 7.4.2. □

Our experimental results show that as the initial offset m_1 grows, d can be achieved by intrasession coding in the limit as $m_1 \to \infty$ (see Figure 7.3).

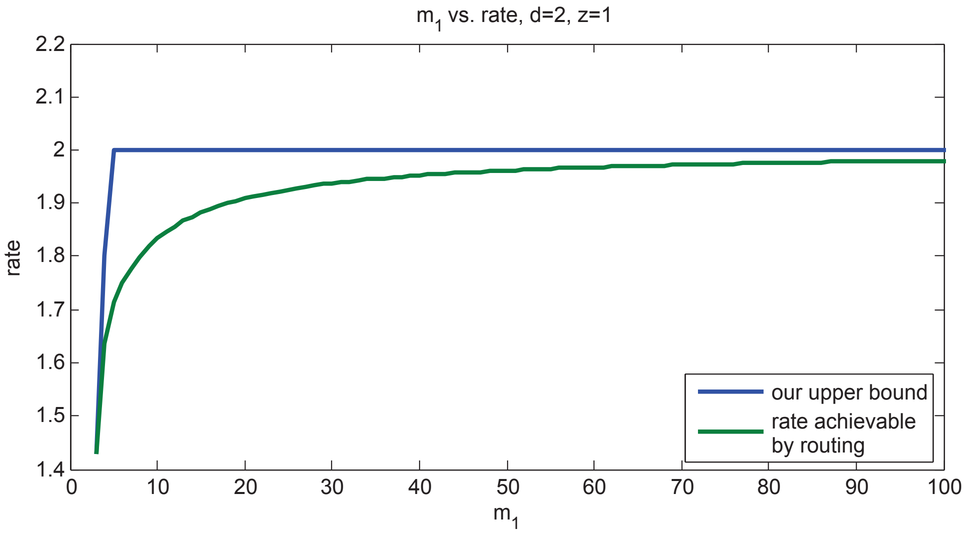


Figure 7.3: Experimental results with $d = 2$, $z = 1$.

7.3.3 Multiple desciption code

Consider an erasure-free 3-layer network $\mathcal{G}_M$ that is constructed so that:

- $\mathcal{G}_M$ has D_n links in the second layer.
- There are $\begin{pmatrix} D_n \\ D_1 \end{pmatrix}$ sinks that are connected to all D_1-element subsets in the second layer and demand message M_1.

- There are $\begin{pmatrix} D_n \\ D_2 \end{pmatrix}$ sinks that are connected to all D_2-element subsets in the second layer and demand message M_2.

- ...

- There is one sink that is connected to all links in the second layer and demands message M_n.

Let $\mathbb{U} = \{u_1, u_2, \dots, u_n\}$ be the erasure-free capacity region of $\mathcal{G}_M$. Studying $\mathbb{U}$ is important as any code that achieves $\mathbb{U}$ can be interpreted as a multiple description code when a single code is designed so that the sink can decode at various quality levels depending on the number of erasures in a system that occurs during the course of packet transmission [39]. In Theorem 17, we use proof techniques that we developed in Section 7.3.1 to find $\mathbb{U}$.

Theorem 17 (Multiple description code)**.** *The erasure-free capacity region* $\mathbb{U}$ *of* $\mathcal{G}_M$ *is given by*

$$\frac{u_1}{D_1} + \frac{u_2}{D_2} + \ldots + \frac{u_n}{D_n} \leq 1 \tag{7.23}$$

and can be achieved by intrasession coding for any z*.*

Proof. Proof given in Section 7.4.2. □

Note that Theorem 17 can be viewed as a special case of the z-erasure correction capacity region of $\mathcal{G}_s$ when $m_n - z \leq m_1$.

7.3.4 Two-sink networks

In this section we consider any acyclic network $\mathcal{G}_2 = (V, E)$ with source set $\mathcal{S}$ and sink set $\mathcal{T} = \{t_1, t_2\}$ that demand independent (nonoverlapping) source processes. Let sink t_1 demand message M_1 and let sink t_2 demand message M_2. We use proof techniques established in Section 7.3.1 to derive tighter upper bounds on the error and erasure correction capacity regions of $\mathcal{G}_2$ than those given by Theorem 10 in Chapter 6.

Let $P = (V_\mathcal{S}, V_\mathcal{T})$ be a partition of V such that all sources are in $V_\mathcal{S}$ and all sinks are in $V_\mathcal{T}$ and cut(P) contains no feedback links.

Definition 16. *A related 3-layer network $\mathcal{G}_2(P)$ is a one-source 2-sink 3-layer network that is constructed as follows (see Figure 7.5(a) for example):*

- *For each link $l \in cut(P)$, we connect a source directly to the start node of l.*
- *For each sink $t \in \mathcal{T}$, we connect the end node of l directly to sink t if t is downstream of l in $\mathcal{G}$.*

Note that construction of the related 3-layer network $\mathcal{G}_2(P)$ for each source-sink partition P of $\mathcal{G}_2$ essentially allows all nodes on the source side of the cut to cooperate perfectly and gives each sink at least as much information as it receives in the original network $\mathcal{G}_2$. Therefore, the error correction capacity region of $\mathcal{G}_2(P)$ is an upper bound on the error correction capacity region of $\mathcal{G}_2$.

Let m_1 be the number of links upstream of t_1 but not t_2 in $\mathcal{G}_2(P)$, m_2 be the number of links upstream of t_2 but not t_1 in $\mathcal{G}_2(P)$, and m_{12} be the number of links upstream of both t_1 and t_2 (i.e., the total number of links in the second layer) in $\mathcal{G}_2(P)$. Denote the z-erasure correction capacity region of $\mathcal{G}$ by $\mathbb{U}_2(P) = \{u_1, u_2\}$.

Theorem 18. *For every partition $P = (V_{\mathcal{S}}, V_{\mathcal{T}})$, the z-erasure correction capacity region $\mathbb{U}_2(P)$ of $\mathcal{G}_2(P)$ is given by*

$$\begin{aligned} u_1 &\leq m_1 - z && (7.24)\\ u_2 &\leq m_2 - z && (7.25)\\ &u_1(m_2 - z - \max(m_{12} - m_1 - z, 0)) + u_2(m_1 - z - \max(m_{12} - m_2 - z, 0)) && (7.26)\\ &\leq (m_1 - z)(m_2 - z) - \max(m_{12} - m_1 - z, 0)\max(m_{12} - m_2 - z, 0) \end{aligned}$$

and can be achieved by intrasession coding for any z.

Proof. See Section 7.4.2. □

Theorem 19. *For every partition $P = (V_{\mathcal{S}}, V_{\mathcal{T}})$, the z-error correction capacity region of $\mathcal{G}_2(P)$ is given by the rate pairs (u_1, u_2) such that:*

$$\begin{aligned} u_1 &\leq m_1 - 2z && (7.27)\\ u_2 &\leq m_2 - 2z && (7.28)\\ &u_1(m_2 - 2z - \max(m_{12} - m_1 - 2z, 0)) + u_2(m_1 - 2z - \max(m_{12} - m_2 - 2z, 0)) && (7.29)\\ &\leq (m_1 - 2z)(m_2 - 2z) - \max(m_{12} - m_1 - 2z, 0)\max(m_{12} - m_2 - 2z, 0) \end{aligned}$$

and can be achieved by intrasession coding for any z.

Proof. See Section 7.4.2. □

Hence, by Theorems 18 and 19, the $2z$-erasure correction capacity region $U_2(P)$ of $\mathcal{G}_2(P)$ is equal to the z-error correction capacity region of $\mathcal{G}_2(P)$.

Corollary 1. *The upper-bound on the z-error correction capacity region of $\mathcal{G}_2(P)$ given by Theorem 10 in Chapter 6 is tight, when $m_1 = m_2$ or both $m_{12} - m_1 - 2z \geq 0$ and $m_{12} - m_1 - 2z \geq 0$.*

Proof. See Section 7.4.2. □

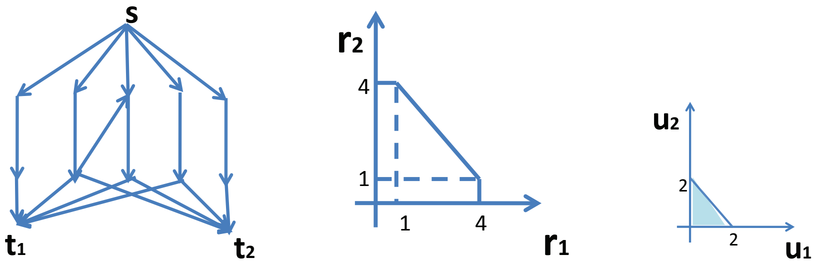
Theorem 20. *An outer bound on the z-error correction capacity region (or a $2z$-erasure correction capacity region) $\mathbb{U} = \{u_1, u_2\}$ of any two-sink network $\mathcal{G}_2$ is given by*

$$\begin{aligned} u_1 &\leq m_{\mathcal{S},t_1} - 2z \\ u_2 &\leq m_{\mathcal{S},t_2} - 2z \\ \mathbb{U} &\subseteq \bigcap_{\substack{P=(V_{\mathcal{S}},V_{\mathcal{T}}) \\ cut(P) \text{ has no} \\ \text{feedback links}}} \mathbb{U}_2(P). \end{aligned}$$

Proof. See Section 7.4.2. □

Figure 7.4(a) depicts a one-source, two-sink network topology with one feedback link across the second layer. The capacity region of this network in the error-free case is given by the cutset bounds [19, 20, 21] (see Figure 7.4(b)). In the presence of one error, the cutset bound $u_1 + u_2 \leq 5 - 2 = 3$ is not achieved (see Figure 7.4(c)). By comparing the achievable region constructed using the procedure described in Chapter 6 and the upper-bound $u_1 + u_2 \leq 2$ given by Theorem 10, we see that in this case the upper-bound given by Theorem 10 is tight.

Figure 7.5(a) shows a one-source two-sink 3-layer network topology, whose capacity region in case of one network error given by the constraints $u_1 \leq 4$, $u_2 \leq 2$, $2u_1 + 3u_2 \leq 8$ (as follows from Theorem 18, shaded area in Figure 7.5(c)). However, as one can observe from



(a) One-source two sink network with one backward link across the cut.

(b) Error-free capacity region given by $r_1 \leq 4, r_2 \leq 4, r_1 + r_2 \leq 5$.

(c) z-error correction capacity region, which coincides with the constructed achievable region using the procedure of Chapter 6 and the outer bound of Theorem 10.

Figure 7.4: Example of the one-source two-sink network with backward link across the cut whose error correction capacity region is given by the upper bound in Theorem 10 when $z = 1$.

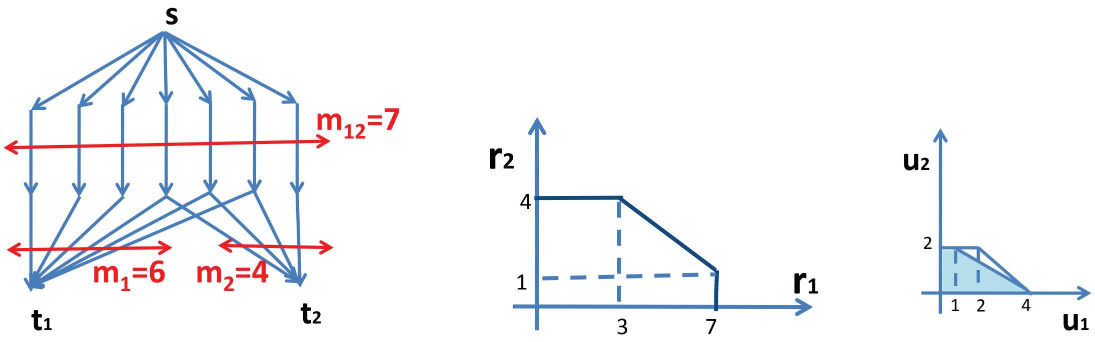
the unshaded area in Figure 7.5(c), for this network the upper bound $u_1 + u_2 \leq 4$ given by Theorem 10 is not tight when $z = 1$.

7.3.5 Applications to sliding-window erasure model

In this section we examine 3-layer networks with nested demands whose x/y-erasure correction capacity region is achieved without intersession coding. This family of networks is particularly important in streaming scenarios as it allows the establishment of streaming checkpoints so that packets designated for each one of the checkpoints are not mixed with packets designated for other checkpoints.

Lemma 20. *The maximum number of erasures on the set consecutive links $k, \ldots, j \in \mathcal{I}$ of $\mathcal{G}_s$ under the x/y sliding-window erasure model occurs when the set of consecutive links $k, \ldots, j \in \mathcal{I}$ satisfies an alternating x/y sliding window erasure condition.*

Lemma 21. *For $i = 1, \ldots, n$, the maximum number of erasures upstream of sink t_i under the x/y sliding-window erasure model occurs when the set of all links upstream of t_i satisfies*



(a) One-source two-sink 3-layer network with $m_1 = 6$, $m_2 = 4$ and $m_{12} = 7$.

(b) Error-free capacity region described by $r_1 \leq 6, r_2 \leq 4, r_1 + r_2 \leq 7$.

(c) Error-correction capacity region described by $u_1 \leq 4, u_2 \leq 2, 2u_1 + 3u_3 \leq 8$ when $z = 1$ (shaded area) vs. the upper bound $u_1 + u_2 \leq 4$ given by Theorem 10 (unshaded area).

Figure 7.5: Example of the one-source two-sink 3-layer network for which the upper bound given by Theorem 10 is not tight when $z = 1$.

an alternating x/y sliding window erasure condition and is given by

$$E_i = \lfloor \frac{m_i}{y} \rfloor x + \min(x_i, x). \tag{7.30}$$

Proof. Follows from Lemma 20. □

Lemma 22 (Alternating pattern cutset bound)**.** *The x/y-erasure correction capacity region of $\mathcal{G}_s$ is upper-bounded by*

$$\begin{aligned} v_1 &\leq m_1 - E_1 && (7.31)\\ v_1 + v_2 &\leq m_2 - E_2 && (7.32)\\ &\dots \\ v_1 + v_2 + \ldots + v_n &\leq m_n - E_n && (7.33) \end{aligned}$$

Proof. Follows by Lemma 7.8. □

Theorem 21 suggests how to set streaming checkpoints in order to achieve the n-dimensional capacity region without intersession coding. The conditions of Theorem 21, provide the largest flexibility in checkpoint placement when x and y are comparable in size.

Theorem 21. *If $x_i \leq x$ for each $i = 1, \ldots, n-1$, then the x/y sliding-window erasure correction capacity region of $\mathcal{G}_s$ is given by inequalities (7.31)-(7.33), and can be achieved by intrasession coding.*

Proof. See Section 7.4.2. □

Theorem 22 gives a constant rate streaming code construction. The work of [38, 40] provides a delay-optimal solution to a similar streaming erasure correction problem, however, their erasure model assumes that any burst of at most x erasures is separated by at least $y - x$ unerased packets. Our x/y sliding window erasure model removes this restriction, which leads to correction of a larger class of permissible erasure patterns. Also, we give a purely intrasession code construction, whereas, the burst-erasure correction codes of [38, 40] are convolutional (i.e., intersession).

For example, consider a streaming system, in which the checkpoints are set at the multiples of 5, i.e., $m_1 = 5$, $m_2 = 10$, $m_3 = 15$ and so on. Assume that in this system at most 2 out of any 5 consecutive packets can fail. Theorem 22 describes how to achieve rate $\frac{3}{5}$ transmission at each of the checkpoints in this scenario. Our code has a decoding delay of at most 4. However, the $\frac{3}{5}$ code of [38, 40], which is proven to correct any burst of 2 out of 5 erasures with an optimal delay of 3, fails under our 2/5 sliding window erasure model (for instance, if every first and third packets in the system are erased).

Theorem 22. *Let $m_1 = m_2 - m_1 = m_3 - m_2 = \ldots = m_n - m_{n-1}$ and $v_1 = v_2 = \ldots = v_n$. Then the x/y sliding-window erasure correction capacity region of $\mathcal{G}_s$ is given by*

$$v_i \leq m_1 - E_1$$

for each $i = 1, \ldots, n$ and can be achieved by intrasession coding.

Proof. See Section 7.4.2. □

We next consider the case of so-called "two-level" checkpoint code design (given by Theorem 24) when we relax the conditions of Theorem 21. This enables the checkpoints to be set at equal distances from each other, so that x_i is arbitrary compared to x when i is odd, and $x_i = 0$ when i is even for every $i = 1, \ldots, n$. This scenario can is useful in video streaming applications when two type of packets - the smaller and the larger ones - have to be transmitted [41]. We also note that since the equispaced placement of checkpoints "repeats itself," the routing scheme that we propose is straightforward to implement in practice for any number of checkpoints n.

First consider the case when $n = 2$. We are going to derive the x/y sliding-window erasure-correction capacity region for $\mathcal{G}_s$ with two sinks by showing that the rate pairs (A, B) and (C, D) as given below can be achieved by intrasession coding and define the corner points of the x/y sliding-window erasure-correction capacity region (see Figure 7.6 for example of geometry of such rate region):

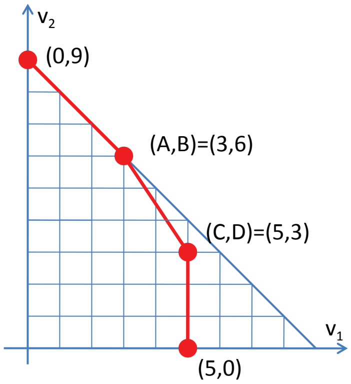


Figure 7.6: The x/y sliding-window erasure-correction capacity region of $\mathcal{G}_s$ with $n = 2$, $m_1 = 9$, $m_2 = 16$, $x = 2$, $y = 5$, $x_1 = 4$ given by $v_1 \leq 5$, $v_1 + v_2 \leq 9$, $3v_1 + 2v_2 \leq 21$.

- $(A, B) = (\lfloor \frac{m_1}{y} \rfloor (y - x), m_2 - E_2 - \lfloor \frac{m_1}{y} \rfloor (y - x))$
- $(C, D) = (m_1 - E_1, m_2 - m_1 - E')$, where E' denotes the maximum number of erasures that can occur on links $m_1 + 1, \ldots, m_2$ under the x/y sliding-window erasure model (by Lemma 20, $E' = \lfloor \frac{m_2 - m_1}{y} \rfloor x + \min(x', x)$ if $m_2 - m_1 = \lfloor \frac{m_2 - m_1}{y} \rfloor y + x', 0 \leq x' \leq y - 1$).

Theorem 23. *If $x_1 > x$ and $n = 2$, then the x/y sliding-window erasure correction capacity region of $\mathcal{G}_s$ is given by (7.31), (7.32) and*

$$(B - D)v_1 + (C - A)v_2 \leq CB - AD. \tag{7.34}$$

This region can be achieved by intrasession coding.

Proof. See Section 7.4.2. □

Theorem 24. *Let m_2 be the multiple of y. Also let $m_1 = m_3 - m_2 = m_5 - m_4 = \ldots = m_{2k-1} - m_{2(k-1)}$, $m_2 = m_4 - m_2 = m_6 - m_4 = \ldots = m_{2k} - m_{2(k-1)}$, $v_1 = v_3 = \ldots = v_{2k-1}$ and $v_2 = v_4 = \ldots = v_{2k}$ for any even $n = 2k$. Then the x/y sliding-window erasure correction capacity region of $\mathcal{G}_s$ is given by*

$$\begin{aligned} v_{2i-1} &\leq m_1 - E_1 &(7.35)\\ (B-D)v_{2i-1} + (C-A)v_{2i} &\leq CB - AD &(7.36)\\ v_{2i-1} + v_{2i} &\leq m_2 - E_2 &(7.37) \end{aligned}$$

for each $i = 1, \ldots, k$ and can be achieved without intersession coding.

Proof. See Section 7.4.2. □

7.4 Proofs and examples

7.4.1 Example of explicit derivation of the z-erasure correction capacity region using techniques described in Section 7.4.1

Consider $\mathcal{G}_s$ with four checkpoints such that $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, and $m_4 = 10$. We compute the z-erasure correction capacity when at most $z = 1$ erasure can occur in $\mathcal{G}_s$. After following the procedure described in Section 7.3.1 (see Figure 7.7 for the schematic illustration of this procedure) the upper bound on the z-erasure correction capacity region of $\mathcal{G}_s$ is given by the following inequalities:

1. $u_1 \leq 2$
2. $3u_1 + 2u_2 \leq 8$
3. $3u_1 + 2u_2 + u_3 \leq 9$
4. $6u_1 + 5u_2 + 4u_3 \leq 24$
5. $6u_1 + 4u_2 + 2u_3 + u_4 \leq 20$
6. $9u_1 + 6u_2 + 4u_3 + 3u_4 \leq 36$
7. $6u_1 + 5u_2 + 4u_3 + 2u_4 \leq 28$

8. $6u_1 + \frac{9}{2}u_2 + 4u_3 + 3u_4 \leq 30$

9. $9u_1 + \frac{15}{2}u_2 + 7u_3 + 6u_4 \leq 54$

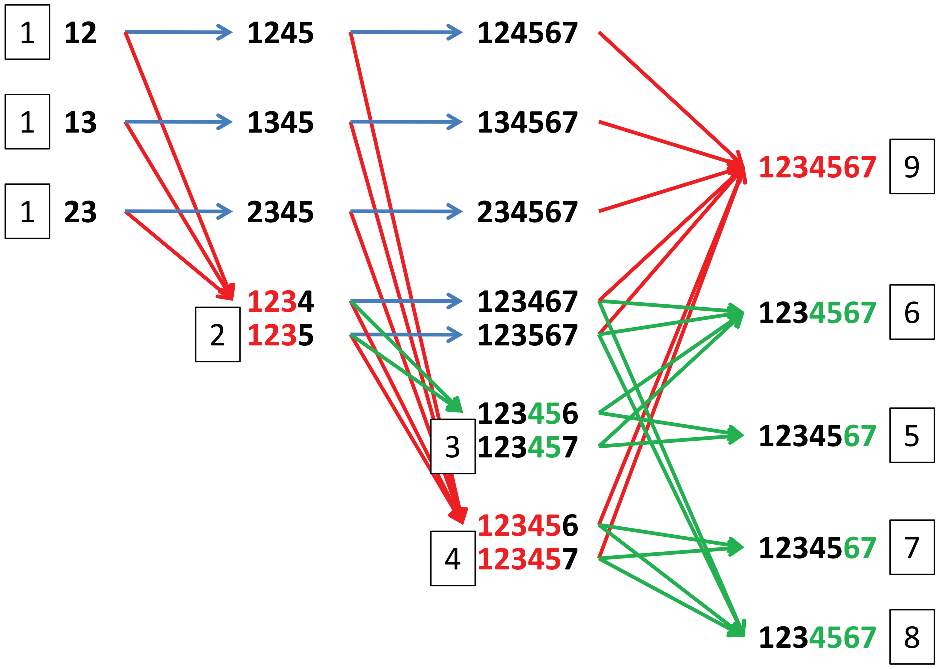


Figure 7.7: Schematic illustration of the derivation of the upper bound on the z-erasure correction capacity region of $\mathcal{G}_s$ with $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $m_4 = 10$ and $z = 1$.

The corner points of the 4-dimensional polytope described by these inequalities are: $(0, 0, 0, 0)$, $(0, 0, 0, 9)$, $(0, 0, 6, 0)$, $(0, 0, 6, 2)$, $(0, 4, 0, 0)$, $(0, 4, 0, 4)$, $(0, 4, 1, 0)$, $(0, 4, 1, 2)$, $(2, 0, 0, 0)$, $(2, 0, 0, 6)$, $(2, 0, 3, 0)$, $(2, 0, 3, 2)$, $(2, 1, 0, 0)$, $(2, 1, 0, 4)$, $(2, 1, 1, 0)$, $(2, 1, 1, 2)$. All of the corner points of this polytope can be achieved greedily without intersession coding. Hence, the z-erasure correction capacity region of $\mathcal{G}_s$ is given by the derived polytope, which can be achieved without intersession coding by timesharing of the corner points.

7.4.2 Proofs

Proof of Lemma 14. By the definition of mutual information,

$$I(M_{i+1}, \ldots, M_n; Z|M_1, \ldots, M_i) = H(Z|M_1, \ldots, M_i) - H(Z|M_1, \ldots, M_n) = H(Z|M_1, \ldots, M_i),$$

where the last equality follows by the fact that the random process Z is a function of $M_1, \ldots, M_n$. □

Proof of Lemma 15. By Lemma 14, $H(Y|M_1,\ldots,M_{i-1}) = I(M_i,\ldots,M_n;Y|M_1,\ldots,M_{i-1})$. Therefore, by the chain rule for mutual information

$$H(Y|M_1,\ldots,M_{i-1}) = I(M_i;Y|M_1,\ldots,M_{i-1}) + I(M_{i+1},\ldots,M_n;Y|M_1,\ldots,M_i). \quad (7.38)$$

Consider the first term in expansion (7.38):

$$\begin{aligned} & I(M_i;Y|M_1,\ldots,M_{i-1}) = H(M_i|M_1,\ldots,M_{i-1}) - H(M_i|M_1,\ldots,M_{i-1},Y) \\ = \quad & H(M_i|M_1,\ldots,M_{i-1}) = H(M_i) = u_i, \end{aligned}$$

which follows from the fact that Y is a decoding information set for M_i and independence of $M_1,\ldots,M_i$.

Consider the second term in expansion (7.38):

$$I(M_{i+1},\ldots,M_n;Y|M_1,\ldots,M_i) = H(Y|M_1,\ldots,M_i) - H(Y|M_1,\ldots,M_n) = H(Y|M_1,\ldots,M_i),$$

since the random process Y is a function of $M_1,\ldots,M_n$.

Therefore,

$$H(Y|M_1,\ldots,M_{i-1}) = u_i + H(Y|M_1,\ldots,M_i).$$

□

Proof of Lemma 16. By expanding the left- and right-hand sides of (7.2) using the chain rule, we get:

$$|Z|\sum_{\sigma\in S}\sum_{d=1}^{D} H(X_{\sigma(d)}|X_{\sigma(1)},\ldots,X_{\sigma(d-1)}) \geq D\begin{pmatrix} |Z| \\ D \end{pmatrix}\sum_{d=1}^{|Z|} H(X_{k_d}|X_{k_1},\ldots,X_{k_{d-1}}).$$

Note that for a given index d, the number of terms of the form $H(X_{k_d}|\ldots)$ on the left- and right-hand sides of the above inequality is equal to $|Z|\begin{pmatrix} |Z|-1 \\ D-1 \end{pmatrix} = D\begin{pmatrix} |Z| \\ D \end{pmatrix}$. Also note that the entropies on the left-hand side are conditioned on the same or fewer variables than the entropies on the right-hand side, therefore, (7.2) holds. □

Proof of Lemma 17. By expanding the left- and right-hand sides of (7.3) using the chain rule, we get:

$$\begin{aligned} & |Z| \sum_{\sigma \in S} \left(H(Y, X_{\sigma(1)}) + \sum_{d=2}^{D} H(X_{\sigma(d)} | Y, X_{\sigma(1)}, \ldots, X_{\sigma(d-1)}) \right) \\ \geq \quad & D \begin{pmatrix} |Z| \\ D \end{pmatrix} \left(H(Y, X_{k_1}) + \sum_{d=2}^{|Z|} H(X_{k_d} | Y, X_{k_1}, \ldots, X_{k_{d-1}}) \right). \end{aligned}$$

Note that for a given index d, the number of terms of the form $H(Y, X_{k_d}|\ldots)$ or $H(X_{k_d}|\ldots)$ on the left-hand sides of the above inequality is equal to $|Z| \begin{pmatrix} |Z|-1 \\ D-1 \end{pmatrix} = D \begin{pmatrix} |Z| \\ D \end{pmatrix}$, where the latter one is the number of terms of the form $H(X_{k_d}|\ldots)$ when $d \neq 1$ or $H(Y, X_{k_1}|\ldots)$ when $d = 1$. Also note that the entropies on the left-hand side are conditioned on the same or fewer variables than the entropies on the right-hand side and for any d

$$H(Y, X_{k_d}|\ldots) \geq H(X_{k_d}|\ldots),$$

therefore, (7.3) holds. □

Proof of Theorem 12. Converse follows from (7.5), (7.10) and Theorem 17. Achievability follows from the fact that the corner points formed by the upper bounds in both cases can be achieved by intrasession coding. □

Proof of Lemma 18. The statement of the lemma follows from (7.17) and (7.18). □

Proof of Lemma 19. Suppose the assignment of $T_{i,j}$ is such that for some $f \geq 0$

$$T_{k+1,k-f+1} = T_{k+1,k-f+2} = \ldots = T_{k+1,k+1} \tag{7.39}$$

and

$$T_{k+1,k-f} \neq T_{k+1,k+1-f}.$$

Note that by the uniformity of assignment of $T_{i,j}$

$$\sum_{i=1}^{k+1}\sum_{j=1}^{k-f} T_{i,j}(m_j - m_{j-1}) = \sum_{j=1}^{k-f}(m_j - m_{j-1})\sum_{i=1}^{k+1} T_{i,j} = \sum_{j=1}^{k-f}(m_j - m_{j-1}) = m_{k-f} \tag{7.40}$$

and that for all i such that $k-f+1 < i \leq k+1$

$$T_{i,k-f+1} = T_{i,k-f+2} = \ldots = \tag{7.41}$$

Also, by Lemma 18

$$u_k = \sum_{j=1}^{k-1} T_{k,j}(m_j - m_{j-1}) + T_{k,k}(D_k - m_{k-1}). \tag{7.42}$$

For every $q = 0, \ldots, f$, take any $Y_\sigma^{k+1} \in S_{k+1}$ such that $X^{m_{k-f+q}} \subseteq Y_\sigma^{k+1}$ but $X^{m_{k-f+1+q}} \nsubseteq Y_\sigma^{k+1}$, then similarly to (7.7):

$$\begin{aligned} & H(Y_\sigma^{k+1}|M_1,\ldots,M_{k-f+q}) \leq H(X^{m_{k-f+q}}|M_1,\ldots,M_{k-f+q}) + D_{k+1} - m_{k-f+q} \\ \leq \quad & P_{k-f+q} + D_{k+1} - m_{k-f+q}. \end{aligned}$$

Note that Y_σ^{k+1} is a decoding set for $M_{k-f+q+1}, \ldots, M_{k+1}$, therefore, after applying Lemma 17 $(f+1-q)$ times:

$$H(Y_\sigma^{k+1}|M_1,\ldots,M_{k+1}) \leq P_{k-f+q} + D_{k+1} - m_{k-f+q} - \sum_{h=k-f+1+q}^{k+1} u_h. \tag{7.43}$$

For each $q = 0, \ldots, f$, define $C_q = P_{k-f+q} + D_{k+1} - m_{k-f+q} - \sum_{h=k-f+1+q}^{k+1} u_h$.

Using (7.42) and (7.39):

$$\begin{aligned}
C_0 &= P_{k-f} + D_{k+1} - m_{k-f} - \sum_{h=k-f+1}^{k+1} u_h \\
&= D_{k+1} - \sum_{i=1}^{k-f}\sum_{j=1}^{k-f} T_{i,j}(m_j - m_{j-1}) - \sum_{h=k-f+1}^{k+1}\sum_{j=1}^{h} T_{h,j}(m_j - m_{j-1}) + z \sum_{h=k-f+1}^{k+1} T_{h,h} \\
&= D_{k+1} - \sum_{i=1}^{k-f}\sum_{j=1}^{k-f} T_{i,j}(m_j - m_{j-1}) - \sum_{i=k-f+1}^{k+1}\sum_{j=1}^{k+1} T_{i,j}(m_j - m_{j-1}) + z \sum_{h=k-f+1}^{k+1} T_{h,h} \\
&= D_{k+1} - \sum_{i=1}^{k+1}\sum_{j=1}^{k+1} T_{i,j}(m_j - m_{j-1}) + z \sum_{h=k-f+1}^{k+1} T_{h,h} \\
&= P_{k+1} - z + z \sum_{h=k-f+1}^{k+1} T_{h,h}
\end{aligned}$$

Hence, for $z = 1$

$$C_0 = P_{k+1} - 1 + \sum_{h=k-f+1}^{k+1} T_{h,h}. \tag{7.44}$$

$$\begin{aligned}
& C_{q+1} - C_q \\
= \quad & P_{k-f+q+1} + D_{k+1} - m_{k-f+q+1} - \sum_{h=k-f+2+q}^{k+1} u_h - P_{k-f+q} - D_{k+1} + m_{k-f+q} + \sum_{h=k-f+1+q}^{k+1} u_h \\
= \quad & P_{k-f+q+1} - m_{k-f+q+1} - (P_{k-f+q} - m_{k-f+q}) + u_{k-f+q+1} \\
= \quad & \sum_{i=1}^{k-f+q} \sum_{j=1}^{k-f+q} T_{i,j}(m_j - m_{j-1}) - \sum_{i=1}^{k-f+q+1} \sum_{j=1}^{k-f+q+1} T_{i,j}(m_j - m_{j-1}) + u_{k-f+q+1} \\
= \quad & \sum_{i=1}^{k-f+q} \sum_{j=1}^{k-f+q} T_{i,j}(m_j - m_{j-1}) - \sum_{i=1}^{k-f+q} \sum_{j=1}^{k-f+q} T_{i,j}(m_j - m_{j-1}) \\
- \quad & \sum_{i=1}^{k-f+q} T_{i,k-f+q+1}(m_{k-f+q+1} - m_{k-f+q}) - \sum_{j=1}^{k-f+q+1} T_{k-f+q+1,j}(m_j - m_{j-1}) + u_{k-f+q+1} \\
= \quad & -\sum_{i=1}^{k-f+q} T_{i,k-f+q+1}(m_{k-f+q+1} - m_{k-f+q}) - \sum_{j=1}^{k-f+q+1} T_{k-f+q+1,j}(m_j - m_{j-1}) + u_{k-f+q+1} \\
= \quad & -\sum_{i=1}^{k-f+q} T_{i,k-f+q+1}(m_{k-f+q+1} - m_{k-f+q}) - u_{k-f+q+1} - zT_{k-f+q+1,k-f+q+1} + u_{k-f+q+1} \\
= \quad & -\sum_{i=1}^{k-f+q} T_{i,k-f+q+1}(m_{k-f+q+1} - m_{k-f+q}) - zT_{k-f+q+1,k-f+q+1} \\
= \quad & -zT_{k-f+q+1,k-f+q+1}
\end{aligned}$$

Hence, for $z = 1$

$$C_{q+1} - C_q = -T_{k-f+q+1,k-f+q+1}. \tag{7.45}$$

For $z = 1$, there is a total of $\binom{m_{k+1} - m_{k-f}}{D_{k+1} - m_{k-f}} = m_{k+1} - m_{k-f}$ choices of $Y_\sigma^{k+1} \in S^{k+1}$ such that $X^{m_{k-f}} \subseteq Y_\sigma^{k+1}$, out of which for each $q = 0, \ldots, f$ there are

$$\binom{m_{k+1} - m_{k-f+q}}{D_{k+1} - m_{k-f+q}} - \binom{m_{k+1} - m_{k-f+q+1}}{D_{k+1} - m_{k-f+q+1}} = m_{k-f+q+1} - m_{k-f+q}$$

choices of $Y_\sigma^{k+1} \in S_{k+1}$ such that $X^{m_{k-f+q}} \subseteq Y_\sigma^{k+1}$ but $X^{m_{k-f+1+q}} \nsubseteq Y_\sigma^{k+1}$.

Sum all (7.43) over all $Y_\sigma^{k+1} \in S_{k+1}$ such that $X^{m_{k-f}} \subseteq Y_\sigma^{k+1}$ and apply (7.44) and

(7.45) :

$$\begin{aligned}
& \sum_{Y_\sigma^{k+1}\in S_{k+1}:X^{m_{k-f}}\subseteq Y_\sigma^{k+1}} H(Y_\sigma^{k+1}|M_1,\dots,M_{k+1}) \\
\leq\ & \sum_{q=0}^{f} C_q\left(\begin{pmatrix} m_{k+1}-m_{k-f+q} \\ D_{k+1}-m_{k-f+q}\end{pmatrix} - \begin{pmatrix} m_{k+1}-m_{k-f+q+1} \\ D_{k+1}-m_{k-f+q+1}\end{pmatrix}\right) \\
=\ & C_0\begin{pmatrix} m_{k+1}-m_{k-f} \\ D_{k+1}-m_{k-f}\end{pmatrix} + \sum_{q=0}^{f-1}(C_{q+1}-C_q)\begin{pmatrix} m_{k+1}-m_{k-f+q+1} \\ D_{k+1}-m_{k-f+q+1}\end{pmatrix} \\
=\ & C_0\begin{pmatrix} m_{k+1}-m_{k-f} \\ D_{k+1}-m_{k-f}\end{pmatrix} - \sum_{q=0}^{f-1}T_{k-f+q+1,k-f+q+1}\begin{pmatrix} m_{k+1}-m_{k-f+q+1} \\ D_{k+1}-m_{k-f+q+1}\end{pmatrix} \\
\leq\ & C_0(m_{k+1}-m_{k-f}) - \sum_{h=k-f+1}^{k} T_{h,h}(m_{k+1}-m_h).
\end{aligned}$$

After applying Lemma 17:

$$\begin{aligned}
& H(X^{m_{k+1}}|M_1,\dots,M_{k+1}) \\
=\ & \frac{C_0(m_{k+1}-m_{k-f})-\sum_{h=k-f+1}^{k}T_{h,h}(m_{k+1}-m_h)}{m_{k+1}-m_{k-f}-1} \\
=\ & \frac{(P_{k+1}-1+\sum\limits_{h=k-f+1}^{k+1}T_{h,h})(m_{k+1}-m_{k-f})-\sum\limits_{h=k-f+1}^{k}T_{h,h}(m_{k+1}-m_h)}{m_{k+1}-m_{k-f}-1} \\
=\ & \frac{P_{k+1}(m_{k+1}-m_{k-f})-\left(m_{k+1}-m_{k-f}-(m_{k+1}-m_{k-f})\sum\limits_{h=k-f+1}^{k+1}T_{h,h}+\sum\limits_{h=k-f+1}^{k}T_{h,h}(m_{k+1}-m_h)\right)}{m_{k+1}-m_{k-f}-1} \\
=\ & \frac{P_{k+1}(m_{k+1}-m_{k-f})-\left(m_{k+1}-m_{k-f}+\sum\limits_{h=k-f+1}^{k+1}T_{h,h}(m_{k-f}-m_h)\right)}{m_{k+1}-m_{k-f}-1} \qquad (7.46) \\
=\ & \frac{P_{k+1}(m_{k+1}-m_{k-f})-P_{k+1}}{m_{k+1}-m_{k-f}-1} \\
=\ & P_{k+1},
\end{aligned}$$

where (7.46) follows from (7.41), (7.19) and the fact that matrix T is lower triangular. □

Proof of Theorem 13. Take any $Y_\sigma^{k+1}\in S_{k+1}$ such that $X^{m_k}\subseteq Y_\sigma^{k+1}$. Then similarly to (7.7):

$$H(Y_\sigma^{k+1}|M_1,\dots,M_k)\leq H(X^{m_k}|M_1,\dots,M_k)+D_{k+1}-m_k.$$

Apply Lemma 15:

$$u_{k+1} + H(Y_\sigma^{k+1}|M_1, \dots, M_{k+1}) \leq H(X^{m_k}|M_1, \dots, M_k) + D_{k+1} - m_k,$$

$H(Y_\sigma^{k+1}|M_1, \dots, M_{k+1}) = 0$ in a $(k+1)$-sink network $\mathcal{G}_s$, hence,

$$u_{k+1} \leq H(X^{m_k}|M_1, \dots, M_k) + D_{k+1} - m_k.$$

Therefore, in order to maximize u_{k+1}, one need to maximize $H(X^{m_k}|M_1, \dots, M_k)$. By Lemma 19,

$$H(X^{m_k}|M_1, \dots, M_k) \leq P_k.$$

Moreover, for the assignment of $T_{i,j}$ given by (7.16)-(7.18),

$$H(X^{m_k}|M_1, \dots, M_k) = P_k.$$

Thus, since the given choice of $T_{i,j}$ satisfies the routing linear program (7.14)-(7.15), the z-erasure correction capacity region of $\mathcal{G}_s$ can be achieved by intrasession coding. □

Proof of Theorem 14. We going to prove the statement of this theorem by utilizing the upper-bounding techniques described in Section 7.3.1. In this proof, we are also going to use the notation introduced in Section 7.3.1.

By (7.9), for every Y_Δ^2, $\Delta \in S_2$ such that $X^{m_1} \subseteq Y_\Delta^2$:

$$\frac{m_1}{D_1} u_1 + u_2 + H(Y_\Delta^2|M_1 M_2) \leq D_2. \tag{7.47}$$

Sum (7.47) over all Y_Δ^2, $\Delta \in S_2$ such that $X^{m_1} \subseteq Y_\Delta^2$ (there are $\begin{pmatrix} m_2 - m_1 \\ D_2 - m_1 \end{pmatrix} = \begin{pmatrix} d \\ d - z \end{pmatrix}$ choices of such Y_Δ^2)

$$\frac{m_1}{D_1} \begin{pmatrix} d \\ d - z \end{pmatrix} u_1 + \begin{pmatrix} d \\ d - z \end{pmatrix} u_2 + \sum_{\Delta \in S_2 : X^{m_1} \subseteq Y_\Delta^2} H(Y_\Delta^2|M_1 M_2) \leq D_2 \begin{pmatrix} d \\ d - z \end{pmatrix}.$$

Multiply both sides by d:

$$d\frac{m_1}{D_1}\binom{d}{d-z}u_1 + d\binom{d}{d-z}u_2 + d\sum_{\Delta\in S_2: X^{m_1}\subseteq Y^2_\Delta} H(Y^2_\Delta|M_1M_2) \le dD_2\binom{d}{d-z}.$$

Apply Lemma 17 to $\sum_{\Delta\in S_2: X^{m_1}\subseteq Y^2_\Delta} H(Y^2_\Delta|M_1M_2)$:

$$d\frac{m_1}{D_1}\binom{d}{d-z}u_1 + d\binom{d}{d-z}u_2 + (d-z)\binom{d}{d-z}H(X^{m_2}|M_1M_2) \le dD_2\binom{d}{d-z},$$

or

$$d\frac{m_1}{D_1}u_1 + du_2 + (d-z)H(X^{m_2}|M_1M_2) \le dD_2. \tag{7.48}$$

Consider any Y^3_γ, $\gamma\in S_3$ such that $X^{m_2}\subseteq Y^3_\gamma$ (note that there are $\binom{m_3-m_2}{D_3-m_2} = \binom{d}{d-z}$ choices of such Y^3_γ), that is, $Y^3_\gamma = \{X^{m_2}, Z^3\}$ for some set of random processes Z^3 such that $H(Z^3)\le m_3-m_2-z = d-z$. Then

$$H(Y^3_\gamma|M_1M_2) \le H(X^{m_2}|M_1M_2) + H(Z^3|M_1M_2) \le H(X^{m_2}|M_1M_2) + d - z.$$

Therefore, after adding $(d-z)^2$ to both sides of (7.48), we get:

$$d\frac{m_1}{D_1}u_1 + du_2 + (d-z)H(Y^3_\gamma|M_1M_2) \le dD_2 + (d-z)^2.$$

Note that for every $\gamma\in S_3$, Y^3_γ is a decoding information set for M_3, therefore, by Lemma 15:

$$d\frac{m_1}{D_1}u_1 + du_2 + (d-z)u_3 + (d-z)H(Y^3_\gamma|M_1M_2M_3) \le dD_2 + (d-z)^2.$$

Now sum over all Y^3_γ, $\gamma\in S_3$ such that $X^{m_2}\subseteq Y^3_\gamma$ (there are $\binom{m_3-m_2}{D_3-m_2} = \binom{d}{d-z}$

choices of such Y_γ^3):

$$\begin{aligned} d\frac{m_1}{D_1}\begin{pmatrix} d \\ d-z \end{pmatrix} u_1 + d\begin{pmatrix} d \\ d-z \end{pmatrix} u_2 + (d-z)\begin{pmatrix} d \\ d-z \end{pmatrix} u_3 & \\ + \quad (d-z)\sum_{\gamma\in S_3 : X^{m_2}\subseteq Y_\gamma^3} H(Y_\gamma^3|M_1M_2M_3) \leq \begin{pmatrix} d \\ d-z \end{pmatrix}\left(dD_2 + (d-z)^2\right). & \end{aligned}$$

Multiply by d:

$$\begin{aligned} d^2\frac{m_1}{D_1}\begin{pmatrix} d \\ d-z \end{pmatrix} u_1 + d^2\begin{pmatrix} d \\ d-z \end{pmatrix} u_2 + d(d-z)\begin{pmatrix} d \\ d-z \end{pmatrix} u_3 & \\ + \quad (d-z)d\sum_{\gamma\in S_3 : X^{m_2}\subseteq Y_\gamma^3} H(Y_\gamma^3|M_1M_2M_3) \leq d\begin{pmatrix} d \\ d-z \end{pmatrix}\left(dD_2 + (d-z)^2\right). & \end{aligned}$$

Apply Lemma 17:

$$\begin{aligned} d^2\frac{m_1}{D_1}\begin{pmatrix} d \\ d-z \end{pmatrix} u_1 + d^2\begin{pmatrix} d \\ d-z \end{pmatrix} u_2 + d(d-z)\begin{pmatrix} d \\ d-z \end{pmatrix} u_3 & \\ + \quad (d-z)^2\begin{pmatrix} d \\ d-z \end{pmatrix} H(X^{m_3}|M_1M_2M_3) \leq d\begin{pmatrix} d \\ d-z \end{pmatrix}\left(dD_2 + (d-z)^2\right), & \end{aligned}$$

or

$$d^2\frac{m_1}{D_1}u_1 + d^2u_2 + d(d-z)u_3 + (d-z)^2H(X^{m_3}|M_1M_2M_3) \leq d\left(dD_2 + (d-z)^2\right).$$

Consider any Y_Θ^4, $\Theta \in S_4$ such that $X^{m_3} \subseteq Y_\Theta^4$ (note that there are $\begin{pmatrix} m_4-m_3 \\ D_4-m_3 \end{pmatrix} = \begin{pmatrix} d \\ d-z \end{pmatrix}$ choices of such Y_Θ^4), that is, $Y_\Theta^4 = \{X^{m_3}, Z^4\}$ for some set of random processes Z^4 such that $H(Z^4) \leq m_4 - m_3 - z = d - z$. Then

$$H(Y_\gamma^4|M_1M_2M_3) \leq H(X^{m_3}|M_1M_2M_3) + H(Z^4|M_1M_2M_3) \leq H(X^{m_3}|M_1M_2M_3) + d - z.$$

Therefore, after adding $(d-z)^3$ to both sides of (7.49), we get:

$$\begin{aligned} & d^2\frac{m_1}{D_1}u_1 + d^2u_2 + d(d-z)u_3 + (d-z)^2 H(Y_\Theta^4|M_1M_2M_3) \\ \leq \;& d\left(dD_2 + (d-z)^2\right) + (d-z)^3 = d^2D_2 + d(d-z)^2 + (d-z)^3. \end{aligned}$$

Note that for every $\Theta \in S_4$, Y_Θ^4 is a decoding information set for M_4, therefore, by Lemma 15:

$$\begin{aligned} & d^2\frac{m_1}{D_1}u_1 + d^2u_2 + d(d-z)u_3 + (d-z)^2u_4 + (d-z)^2 H(Y_\Theta^4|M_1M_2M_3M_4) \\ \leq \;& d^2D_2 + d(d-z)^2 + (d-z)^3. \end{aligned}$$

Similarly, for any Y_ρ^5, $\rho \in S_5$ such that $X^{m_4} \subseteq Y_\rho^5$:

$$\begin{aligned} & d^3\frac{m_1}{D_1}u_1 + d^3u_2 + d^2(d-z)u_3 + d(d-z)^2u_4 + (d-z)^3u_5 + (d-z)^3 H(Y_\rho^5|M_1M_2M_3M_4M_5) \\ \leq \;& d(d^2D_2 + d(d-z)^2 + (d-z)^3) + (d-z)^4 = d^3D_2 + d^2(d-z)^2 + d(d-z)^3 + (d-z)^4 \\ = \;& d^3D_2 + (d-z)^2\left(d^2 + d(d-z) + (d-z)^2\right). \end{aligned}$$

Proceeding similarly, if there are n sinks in $\mathcal{G}_s$:

$$d^{n-2}\frac{m_1}{D_1}u_1 + \sum_{k=0}^{n-2} d^{n-2-k}(d-z)^k u_{k+2} \leq d^{n-2}D_2 + (d-z)^2\sum_{k=0}^{n-3} d^{n-3-k}(d-z)^k.$$

Now if we set $u_1 = u_2 = \ldots = u$:

$$\left(d^{n-2}\frac{m_1}{D_1} + \sum_{k=0}^{n-2} d^{n-2-k}(d-z)^k\right)u \leq d^{n-2}D_2 + (d-z)^2\sum_{k=0}^{n-3} d^{n-3-k}(d-z)^k,$$

which can be written as:

$$\left(d^{n-2}\frac{m_1}{D_1} + \frac{d^{n-1} - (d-z)^{n-1}}{z}\right)u \leq d^{n-2}D_2 + (d-z)^2\frac{d^{n-2} - (d-z)^{n-2}}{z},$$

or

$$\left(zd^{n-2}\frac{m_1}{D_1} + d^{n-1} - (d-z)^{n-1}\right)u \leq zd^{n-2}D_2 + (d-z)^2(d^{n-2} - (d-z)^{n-2}).$$

Divide by d^{n-1}:

$$\left(\frac{z}{d}\frac{m_1}{D_1} + 1 - \left(\frac{d-z}{d}\right)^{n-1}\right) u \le \frac{z}{d}D_2 + \frac{(d-z)^2}{d} - (d-z)\left(\frac{d-z}{d}\right)^{n-1},$$

or

$$u \le \frac{d - z + \frac{zm_1}{d} - (d-z)\left(\frac{d-z}{d}\right)^{n-1}}{1 + \frac{z}{d}\frac{m_1}{m_1-z} - \left(\frac{d-z}{d}\right)^{n-1}}.$$

Hence, (7.20) holds. □

Proof of Theorem 15. We will now demonstrate that the upper bound (7.21) is tight and can be achieved without intersession coding for any number of sinks n. Precisely, we will show that

$$u^* = \frac{d - z + \frac{zm_1}{d}}{1 + \frac{z}{d}\frac{m_1}{m_1-z}},$$

maximizes u subject to

$$\forall j = 1,\dots,n \qquad u \le \sum_{i \in P \cup \{1,\dots,m_i\}}^{m_i} y_i^j \tag{7.49}$$

$$\forall i = 1,\dots,m_n \qquad \sum_{j=1}^{n} y_i^j \le 1. \tag{7.50}$$

for some $y_i^j \ge 0$, $i = 1,\dots,m_n$, $j = 1,\dots,n$ and every set of unerased links $P \subseteq \mathcal{I}$ under any z link erasures.

Note that $y_i^j = 0$, $i = m_j + 1,\dots,m_n$ for all $j = 1,\dots,n-1$. Choose y_i^j so that

- $y_i^1 = A$, $i = 1,\dots,m_1$
- $y_i^2 = B$, $i = 1,\dots,m_1$ and $y_i^2 = C$, $i = m_1+1,\dots,m_2$
- $y_i^3 = 0$, $i = 1,\dots,m_1$, $y_i^3 = D$, $i = m_1+1,\dots,m_2$ and $y_i^3 = C$, $i = m_2+1,\dots,m_3$
- $y_i^4 = 0$, $i = 1,\dots,m_2$, $y_i^4 = D$, $i = m_2+1,\dots,m_3$ and $y_i^4 = C$, $i = m_3+1,\dots,m_4$
- $\dots$

When $m \leq \frac{1}{4}(3d+z)+\frac{1}{4}\sqrt{9d^2-2dz+z^2}$, this choice of y_i^j satisfies (7.49) and (7.50). In particular, there exists a solution to the linear system

$$\begin{aligned}
u^* &= (m_1 - z)A \\
u^* &= m_1 B + (d-z)C \\
u^* &= dD + (d-z)C \\
A + B &= 1 \\
C + D &= 1
\end{aligned}$$

given by $A = \frac{d^2-dz+m_1z}{dm-dz+mz}$, $B = \frac{d(m-d)}{dm-dz+mz}$, $C = \frac{2dm-m^2-dz+mz}{dm-dz+mz}$, $D = \frac{m(m-d)}{dm-dz+mz}$ with $0 \leq A \leq 1$, $0 \leq B \leq 1$, $0 \leq C \leq 1$, $0 \leq D \leq 1$. □

Proof of Theorem 16. The upper bound follows from the fact that $u_1+\ldots+u_n \leq m_n - z = m_1 + d(n-1) - z$. Hence, $u \leq d\frac{n-1}{n} + \frac{m_1}{n} - \frac{z}{n}$. □

Proof of Theorem 17. We proceed along the lines of the procedure described in Section 7.3.1 for general 3-layer erasure networks with nested demands.

By the cutset bound, we know that for any $\sigma \in S_1$

$$H(Y_\sigma^1) \leq D_1.$$

On the other hand, by Lemma 15

$$H(Y_\sigma^1) = u_1 + H(Y_\sigma^1|M_1) \leq D_1.$$

Fix any Y_Δ^2, $\Delta \in S_2$. Sum over all $\sigma \in S_1$ such that $Y_\sigma^1 \subseteq Y_\Delta^2$ (note that for every Y_Δ^2 there are $\left(\begin{array}{c} D_2 \\ D_1 \end{array}\right)$ choices of $Y_\sigma^1 \subseteq Y_\Delta^2$), we get

$$\left(\begin{array}{c} D_2 \\ D_1 \end{array}\right) u_1 + \sum_{\sigma \in S_1, Y_\sigma^1 \subseteq Y_\Delta^2} H(Y_\sigma^1|M_1) \leq \left(\begin{array}{c} D_2 \\ D_1 \end{array}\right) D_1.$$

Multiply by D_2:

$$\binom{D_2}{D_1} D_2 u_1 + D_2 \sum_{\sigma \in S_1, Y_\sigma^1 \subseteq Y_\Delta^2} H(Y_\sigma^1 | M_1) \leq \binom{D_2}{D_1} D_1 D_2.$$

Now by using Lemma 16

$$D_2 \binom{D_2}{D_1} u_1 + D_1 \binom{D_2}{D_1} H(Y_\Delta^2 | M_1) \leq \binom{D_2}{D_1} D_1 D_2.$$

After canceling by $\binom{D_2}{D_1}$

$$D_2 u_1 + D_1 H(Y_\Delta^2 | M_1) \leq D_1 D_2. \tag{7.51}$$

Note that for every $\Delta \in S_2$, Y_Δ^2 is a decoding information set for M_2, therefore, by Lemma 15 $H(Y_\Delta^2|M_1) = u_2 + H(Y_\Delta^2|M_1, M_2)$. Then (7.51) can be rewritten as:

$$D_2 u_1 + D_1 u_2 + D_1 H(Y_\Delta^2 | M_1, M_2) \leq D_1 D_2.$$

Fix any Y_γ^3, $\gamma \in S_3$. Sum over all $\Delta \in S_2$ such that $Y_\Delta^2 \subseteq Y_\gamma^3$ (note that for every Y_γ^3 there are $\binom{D_3}{D_2}$ choices of $Y_\Delta^2 \subseteq Y_\gamma^3$), we get

$$\binom{D_3}{D_2} D_2 u_1 + \binom{D_3}{D_2} D_1 u_2 + D_1 \sum_{\Delta \in S_2, Y_\Delta^2 \subseteq Y_\gamma^3} H(Y_\Delta^2 | M_1 M_2) \leq \binom{D_3}{D_2} D_1 D_2.$$

Multiply by D_3:

$$\binom{D_3}{D_2} D_2 D_3 u_1 + \binom{D_3}{D_2} D_1 D_3 u_2 + D_1 D_3 \sum_{\Delta \in S_2, Y_\Delta^2 \subseteq Y_\gamma^3} H(Y_\Delta^2 | M_1 M_2) \leq \binom{D_3}{D_2} D_1 D_2 D_3.$$

Now by using Lemma 16

$$\binom{D_3}{D_2} D_2 D_3 u_1 + \binom{D_3}{D_2} D_1 D_3 u_2 + D_1 D_2 \binom{D_3}{D_2} H(Y_\gamma^3 | M_1 M_2) \leq \binom{D_3}{D_2} D_1 D_2 D_3.$$

After canceling by $\begin{pmatrix} D_3 \\ D_2 \end{pmatrix}$

$$D_2 D_3 u_1 + D_1 D_3 u_2 + D_1 D_2 H(Y_\gamma^3 | M_1 M_2) \leq D_1 D_2 D_3. \tag{7.52}$$

Note that for every $\gamma \in S_3$, Y_γ^3 is a decoding information set for M_3, therefore, by Lemma 15 $H(Y_\gamma^3|M_1M_2) = u_3 + H(Y_\gamma^3|M_1M_2M_3)$. Then (7.52) can be rewritten as:

$$D_2 D_3 u_1 + D_1 D_3 u_2 + D_1 D_2 u_3 + D_1 D_2 H(Y_\gamma^3 | M_1 M_2 M_3) \leq D_1 D_2 D_3.$$

Proceeding similarly, after n steps we get:

$$\sum_{k=1}^{n-1} D_1 \dots D_{k-1} D_{k+1} \dots D_n u_k + D_1 \dots D_{n-1} \left(u_n + H(Y_\delta^n | M_1, M_2, \dots, M_n) \right) \leq D_1 \dots D_n,$$

where Y_δ^n is a decoding information set for M_n. Note that $H(Y_\delta^n|M_1, M_2, \dots, M_n) = 0$ since Y_δ^n is a function of $M_1, M_2, \dots, M_n$.

Therefore,

$$\sum_{k=1}^{n} D_1 \dots D_{k-1} D_{k+1} \dots D_n u_k \leq D_1 \dots D_n, \tag{7.53}$$

or

$$\frac{u_1}{D_1} + \frac{u_2}{D_2} + \dots + \frac{u_n}{D_n} \leq 1.$$

Now note that the rate vectors $(D_1, 0, 0, \dots, 0, 0)$, $(0, D_2, 0, \dots, 0, 0)$, $(0, 0, D_3, \dots, 0, 0)$, $\dots$, $(0, 0, 0, \dots, 0, D_n)$ are all trivially achievable by intrasession coding and lie on the plane given by (7.53). Now since there are n points on the n-dimensional plane that are achieved by intrasession coding, (7.53) is also achievable by intrasession coding, and hence the statement of the theorem holds. □

Proof of Theorem 18. Converse. Consider any rate vecttor $(u_1, u_2) \in \mathbb{U}_2(P)$. By applying the cutset bounds to each sink individually, (7.27) and (7.28) are satisfied for (u_1, u_2). Now we show that for any $(u_1, u_2) \in \mathbb{U}_2(P)$, (7.29) is also satisfied.

- *Case 1.*

$$\begin{aligned} m_{12} - m_2 &\geq z && (7.54) \\ m_{12} - m_1 &\geq z. && (7.55) \end{aligned}$$

If (7.54) and (7.55) are satisfied, then (7.29) can be simplified as

$$u_1 + u_2 \leq m_{12} - z. \qquad (7.56)$$

Note that (7.54) and (7.55) imply that using the notation of Theorem 10 in Chapter 6

$$\begin{aligned} |L^P_{t_1}| &\geq z \\ |L^P_{t_2}| &\geq z. \end{aligned}$$

Then $l^P = 2z$ solves (6.7)-(6.10) with respect to partition P and by Theorem 10 in Chapter 6.

$$u_1 + u_2 \quad \leq \quad m_{12} - 2z,$$

which matches (7.56).

- *Case 2.*

$$\begin{aligned} m_{12} - m_2 &\leq z && (7.57) \\ m_{12} - m_1 &> z. && (7.58) \end{aligned}$$

If (7.57) and (7.58) are satisfied, then (7.29) can be simplified as

$$(m_1 + m_2 - m_{12})u_1 + (m_1 - z)u_2 \leq (m_1 - z)(m_2 - z). \qquad (7.59)$$

Inequalities (7.57) and (7.58) imply that

$$\begin{aligned} m_1 &\leq m_2 \\ m_1 - z &\leq m_1 + m_2 - m_{12}. \end{aligned}$$

Note that $m_1 + m_2 - m_{12}$ is the number of links upstream of both t_1 and t_2. Since $m_1 - z$ is the size of decoding information set for M_1, the z-erasure capacity region of $\mathcal{G}_2$ is upper-bounded by that of a two-sink nested-demand 3-layer network constructed so that there are $m_1 + m_2 - m_{12}$ links in the second layer upstream of sink 1 and m_2 links upstream of sink 2. Then using (7.10) in Section 7.3.1:

$$(m_1 + m_2 - m_{12})u_1 + (m_1 - z)u_2 \leq (m_1 - z)(m_2 - z),$$

which matches (7.59).

- *Case 3.*

$$\begin{aligned} m_{12} - m_2 &< z && (7.60) \\ m_{12} - m_1 &< z. && (7.61) \end{aligned}$$

If (7.60) and (7.61) are satisfied, then (7.29) can be simplified as

$$(m_2 - z)u_1 + (m_1 - z)u_2 \leq (m_1 - z)(m_2 - z) \tag{7.62}$$

Suppose $m_1 \leq m_2$. From (7.60) it follows that

$$\begin{aligned} m_1 - z &< m_1 + m_2 - m_{12} \\ m_2 - z &< m_1 + m_2 - m_{12}. \end{aligned}$$

Note that $m_1 + m_2 - m_{12}$ is the number of links upstream of both t_1 and t_2. Since $m_1 - z$ is the size of decoding information set for M_1, $m_2 - z$ is the size of decoding information set for M_2, the z-erasure capacity region of $\mathcal{G}_2$ is upper-bounded by that of a two-sink nested-demand 3-layer network constructed so that there are $m_1 + m_2 - m_{12}$ links in the second layer upstream of sink 1 and m_2 links upstream of sink 2, which corresponds to the multiresolution case described in Section 7.3.3 of Chapter 6. Then using Theorem 17:

$$(m_2 - z)u_1 + (m_1 - z)u_2 \leq (m_1 - z)(m_2 - z),$$

which matches (7.62).

Achievability. Since $\mathcal{G}_2(P)$ is a one-source two-sink network with nonoverlapping demands, its error-free capacity region is given by the cut set bounds [9] and achieved by time sharing among the rate pairs $(0,0)$, $(m_1,0)$, $(m_1,m_{12}-m_1)$, $(m_{12}-m_2,m_2)$ and $(0,m_2)$. Since the erasure-free capacity region can be achieved by linear network coding, by the achievability construction described in Chapter 6, the rate pairs $(0,0)$, $(m_1-z,0)$, $(m_1-z,\max(m_{12}-m_1-z,0))$, $(\max(m_{12}-m_2-z,0),m_2-z)$ and $(0,m_2-z)$ are also achievable. Constraints (7.27)-(7.29) correspond to the time-sharing of these rate pairs, hence, $\mathbb{U}_2(P)$ can be achieved by intrasession coding. □

Proof of Theorem 19. The converse can be proved using same technique as that of Theorem 18. Also, similar to Theorem 18, the achievability is implied by construction that uses the error-free linear code and is described in Chapter 6. □

Proof of Corollary 1. When both $m_{12}-m_1-2z \geq 0$ and $m_{12}-m_2-2z \geq 0$, the proof corresponds to *Case 1* of the proof of Theorem 18. When $m_1 = m_2$, $m_{12}-m_1-2z < 0$, $m_{12}-m_2-2z < 0$, then $l^P = |L_2^P| + z$ solves (6.7)-(6.10) in Chapter 6 with respect to partition P and by Theorem 10 $u_1 + u_2 \leq m_1 - 2z$, which matches the achievable region constructed from the erasure-free capacity region of $\mathcal{G}_2(P)$ using the procedure described in Chapter 6. □

Proof of Theorem 20. By construction of $\mathcal{G}_2(P)$, $\mathbb{U}$ is upper-bounded by $\mathbb{U}_2(P)$ for every partition P such that $\text{cut}(P)$ does not contain feedback links. Hence, the statement of the theorem follows by Theorem 19 for the z-error correction capacity region (or Theorem 18 for the $2z$-erasure correction capacity region). □

Proof of Theorem 21. Note that by assumption of the theorem $x_i \leq x$, $i = 1, \ldots, n-1$.

Consider the rate vector $(a_1, a_2, \ldots, a_n)$, where

$$\begin{aligned}
a_1 &= m_1 - E_1 = \lfloor\frac{m_1}{y}\rfloor(y-x) \\
a_2 &= m_2 - E_2 - a_1 = \left(\lfloor\frac{m_2}{y}\rfloor - \lfloor\frac{m_1}{y}\rfloor\right)(y-x) \\
a_3 &= m_3 - E_3 - a_1 - a_2 = \left(\lfloor\frac{m_3}{y}\rfloor - \lfloor\frac{m_2}{y}\rfloor\right)(y-x) \\
\ldots \\
a_n &= m_n - E_n - a_1 - a_2 - \ldots - a_{n-1} = m_n - E_n - \lfloor\frac{m_{n-1}}{y}\rfloor(y-x).
\end{aligned}$$

We will demonstrate that the rate vector $(a_1, a_2, \ldots, a_n)$ can be achieved by the following strategy:

- Perform random linear coding of the a_1 symbols of source message M_1 into $\lfloor\frac{m_1}{y}\rfloor y$ symbols and subsequently forward them on links $1, \ldots, \lfloor\frac{m_1}{y}\rfloor y$.
- Perform random linear coding of the a_2 symbols of source message M_2 into $\left(\lfloor\frac{m_2}{y}\rfloor - \lfloor\frac{m_1}{y}\rfloor\right) y$ symbols and subsequently forward them on links $\lfloor\frac{m_1}{y}\rfloor y + 1, \ldots, \lfloor\frac{m_2}{y}\rfloor y$.
- Perform random linear coding of the a_3 symbols of source message M_3 into $\left(\lfloor\frac{m_3}{y}\rfloor - \lfloor\frac{m_2}{y}\rfloor\right) y$ symbols and subsequently forward them on links $\lfloor\frac{m_2}{y}\rfloor y + 1, \ldots, \lfloor\frac{m_3}{y}\rfloor y$.
- $\ldots$
- Perform random linear coding of the a_n symbols of source message M_n into $m_n - \lfloor\frac{m_{n-1}}{y}\rfloor y$ symbols and subsequently forward them on links $\lfloor\frac{m_{n-1}}{y}\rfloor y + 1, \ldots, m_n$.

If any x out of y consecutive links in the second layer are erased:

- At most $\lfloor\frac{m_1}{y}\rfloor x$ erasures can occur on links $1, \ldots, \lfloor\frac{m_1}{y}\rfloor y$.
- At most $\left(\lfloor\frac{m_2}{y}\rfloor - \lfloor\frac{m_1}{y}\rfloor\right) x$ erasures can occur on links $\lfloor\frac{m_1}{y}\rfloor y + 1, \ldots, \lfloor\frac{m_2}{y}\rfloor y$.
- At most $\left(\lfloor\frac{m_3}{y}\rfloor - \lfloor\frac{m_2}{y}\rfloor\right) x$ erasures can occur on links $\lfloor\frac{m_2}{y}\rfloor y + 1, \ldots, \lfloor\frac{m_3}{y}\rfloor y$.
- $\ldots$
- At most $(\lfloor\frac{m_n}{y}\rfloor - \lfloor\frac{m_{n-1}}{y}\rfloor)x + \min(x, x_n) = E_n - \lfloor\frac{m_{n-1}}{y}\rfloor x$ erasures can occur on links $\lfloor\frac{m_{n-1}}{y}\rfloor y + 1, \ldots, m_n$.

Therefore, the rate vector $(a_1, a_2, a_3, \dots, a_n)$ is achievable by intrasession coding. By the nested structure of $\mathcal{G}_s$, the rate vectors $(0, a_1 + a_2, a_3, \dots, a_n)$, $(0, 0, a_1 + a_2 + a_3, \dots, a_n)$, $\dots$, $(0, 0, 0, \dots, \sum_{k=1}^{n} a_k)$ are also achievable by intrasession coding, and since $\sum_{k=1}^{n} a_k = m_n - E_n$, these rate vectors lie on the plane (7.33). Hence, we identified n points that lie on the n-dimensional plane, thus, the inequality (7.33) is achievable by intrasession coding. By the similar argument, one can show that all of the constraints (7.31)-(7.33) are achievable by intrasession coding. Finally, since the rate vector $(a_1, a_2, a_3, \dots, a_n)$ lies on the intersection of the planes (7.31)-(7.33), (7.31)-(7.33) is the x/y-erasure correction capacity region of $\mathcal{G}_s$ and can be achieved by intrasession coding. □

Proof of Theorem 23. Converse. Consider the following erasure pattern $\mathcal{E}$ (see Figure 7.8):

- Link $i \in \mathcal{I}, i = 1, \dots, \lfloor \frac{m_1}{y} \rfloor y$ is erased if and only if

$$i \bmod y \in \{1, \dots, x\}$$

.

- Link $i \in \mathcal{I}, i = \lfloor \frac{m_1}{y} \rfloor y + 1, \dots, m_2$ is erased if and only if

$$i \bmod y \in \{y - x + x_2, \dots, y - 1, 0, 1, \dots, x_2\}.$$

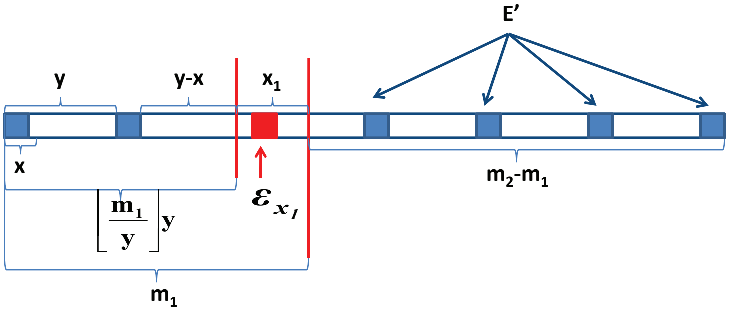


Figure 7.8: Erasure pattern $\mathcal{E}$.

Define the subset $\mathcal{E}_{x_1}$ of $\mathcal{E}$ as follows (see Figure 7.8):

$$\mathcal{E}_{x_1} = \{i \in \mathcal{E} : \lfloor \frac{m_1}{y} \rfloor y + 1 \leq i \leq m_1\}.$$

Note that by construction of erasure pattern $\mathcal{E}$ (see Figure 7.8), $|\mathcal{E}_{x_1}| \leq x$ and $E_2 = \lfloor \frac{m_1}{y} \rfloor x + E' + |\mathcal{E}_{x_1}|$. Then using the definition of the rate pairs (A, B) and (C, D), we can write $B - D = x_1 - |\mathcal{E}_{x_1}|$ and $C - A = x_1 - x$; therefore, (7.34) can be rewritten as

$$(x_1 - |\mathcal{E}_{x_1}|)v_1 + (x_1 - x)v_2 \leq (m_1 - E_1)(x_1 - |\mathcal{E}_{x_1}|) + D(x_1 - x). \tag{7.63}$$

Define

$$\begin{aligned} F &= \begin{pmatrix} x_1 - |\mathcal{E}_{x_1}| \\ x_1 - x \end{pmatrix} \\ \mathcal{Y} &= \{i \in \mathcal{I} : 1 \leq i \leq \lfloor \frac{m_1}{y} \rfloor y \text{ and } i \notin \mathcal{E}\} \\ \mathcal{Y}_{x_1} &= \{i \in \mathcal{I} : \lfloor \frac{m_1}{y} \rfloor y + 1 \leq i \leq m_1 \text{ and } i \notin \mathcal{E}_{x_1}\} \\ \mathcal{Z} &= \{i \in \mathcal{I} : m_1 + 1 \leq i \leq m_2 \text{ and } i \notin \mathcal{E}\}. \end{aligned}$$

Denote the set of random processes transmitted on $\mathcal{Y}$ by Y and the set of random processes transmitted on $\mathcal{Z}$ by Z. Denote the random processes transmitted on each one of the $x_1 - |\mathcal{E}_{x_1}|$ links of $\mathcal{Y}_{x_1}$ by by $Y^{x_1} = \{X_1, X_2, \ldots, X_{x_1 - |\mathcal{E}_{x_1}|}\}$. Let S_x be the set of all lexicographically ordered $(x_1 - x)$-size subsets of $\{1, \ldots, x_1 - |\mathcal{E}_{x_1}|\}$. For any $\sigma \in S_x$, let $\sigma(i)$ be the ith element of σ. Let $\{Y_{\sigma_1}, Y_{\sigma_2}, \ldots, Y_{\sigma_F}\}$ be the set of all unordered subsets of Y^{x_1} of size $(x_1 - x)$.

Note that $|Y| = \lfloor \frac{m_1}{y} \rfloor (y - x)$ and for every $\sigma \in S_x$, $\{Y, Y_\sigma\}$ is a decoding information set for M_1 under the x/y sliding-window erasure model. Also, $\{Y, Y^{x_1}, Z\}$ is a decoding information set for M_2 under the x/y sliding-window erasure model.

The rest of the proof of the converse parallels the upper-bound construction for 3-layer networks with nested demands under the worst-case erasure model that we developed in Section 7.3.1. By the cutset bound, for every $\sigma \in S_x$ we have

$$H(Y, Y_\sigma) \leq m_1 - E_1.$$

On the other hand, because $\{Y, Y_\sigma\}$ is a decoding informations set for M_1, by Lemma 15

$$H(Y, Y_\sigma) = v_1 + H(Y, Y_\sigma | M_1) \leq m_1 - E_1.$$

Sum over all $\sigma \in S_x$, we get

$$Fv_1 + \sum_{\sigma \in S_x} H(Y, Y_\sigma | M_1) \le F(m_1 - E_1).$$

Multiply by $(x_1 - |\mathcal{E}_{x_1}|)$:

$$F(x_1 - |\mathcal{E}_{x_1}|)v_1 + (x_1 - |\mathcal{E}_{x_1}|) \sum_{\sigma \in S_x} H(Y, Y_\sigma | M_1) \le F(m_1 - E_1)(x_1 - |\mathcal{E}_{x_1}|).$$

Then by Lemma 17:

$$F(x_1 - |\mathcal{E}_{x_1}|)v_1 + F(x_1 - x)H(Y, Y^{x_1} | M_1) \le F(m_1 - E_1)(x_1 - |\mathcal{E}_{x_1}|).$$

After canceling by F:

$$(x_1 - |\mathcal{E}_{x_1}|)v_1 + (x_1 - x)H(Y, Y^{x_1} | M_1) \le (m_1 - E_1)(x_1 - |\mathcal{E}_{x_1}|). \tag{7.64}$$

Note that by definition $H(Z) \le m_2 - m_1 - E' = D$

$$H(Y, Y^{x_1}, Z | M_1) \le H(Y, Y^{x_1} | M_1) + H(Z | M_1) \le H(Y, Y^{x_1} | M_1) + D.$$

Therefore, after adding D to both sides of (7.64):

$$(x_1 - |\mathcal{E}_{x_1}|)v_1 + (x_1 - x)H(Y, Y^{x_1}, Z | M_1) \le (m_1 - E_1)(x_1 - |\mathcal{E}_{x_1}|) + D(x_1 - x).$$

Now because $\{Y, Y^{x_1}, Z\}$ is a decoding informations set for M_2, by Lemma 15

$$(x_1 - |\mathcal{E}_{x_1}|)v_1 + (x_1 - x)v_2 + (x_1 - x)H(Y, Y^{x_1}, Z | M_1, M_2) \le (m_1 - E_1)(x_1 - |\mathcal{E}_{x_1}|) + D(x_1 - x),$$

which proves (7.63) since $H(Y, Y^{x_1}, Z | M_1, M_2) = 0$.

Achievability. We first demonstrate that the rate pairs (A, B) and (C, D) can be achieved without intersession coding.

The rate pair (A, B) can be achieved by the following strategy:

- Perform random linear coding of the A symbols of source message M_1 into $\lfloor \frac{m_1}{y} \rfloor y$ symbols and subsequently forward them on links $1, \ldots, \lfloor \frac{m_1}{y} \rfloor y$.

- Perform random linear coding of the B symbols of source message M_2 into $m_2 - \lfloor \frac{m_1}{y} \rfloor y$ symbols and subsequently forward them on links $\lfloor \frac{m_1}{y} \rfloor y + 1, \ldots, m_2$.

If any x out of y consecutive links in the second layer are erased, at most $\lfloor \frac{m_1}{y} \rfloor x$ erasures can occur on links $1, \ldots, \lfloor \frac{m_1}{y} \rfloor y$. Note that $m_2 = \lfloor \frac{m_2}{y} \rfloor y + x_2$, then $m_2 - \lfloor \frac{m_1}{y} \rfloor y = (\lfloor \frac{m_2}{y} \rfloor - \lfloor \frac{m_1}{y} \rfloor) y + x_2$, where $0 \leq x_2 \leq y - 1$; hence, by Lemma 20 at most $(\lfloor \frac{m_2}{y} \rfloor - \lfloor \frac{m_1}{y} \rfloor) x + \min(x, x_2) = E_2 - \lfloor \frac{m_1}{y} \rfloor x$ erasures can occur on links $\lfloor \frac{m_1}{y} \rfloor y + 1, \ldots, m_2$. Therefore, the rate pair (A, B) is achievable by intrasession coding.

The rate pair (C, D) can be achieved by the following strategy:

- Perform random linear coding of the C symbols of source message M_1 into m_1 symbols and subsequently forward them on links $1, \ldots, m_1$.

- Perform random linear coding of the D symbols of source message M_2 into $m_2 - m_1$ symbols and subsequently forward them on links $m_1 + 1, \ldots, m_2$.

If any x out of y consecutive links in the second layer are erased, at most E_1 erasures can occur on links $1, \ldots, m_1$ and at most E' erasures can occur on links $m_1 + 1, \ldots, m_2$, hence, the rate pair (C, D) is achievable by intrasession coding.

The rate vectors $(C, 0)$ and $(0, m_2 - E_2)$ are achieved trivially by transmitting only randomly coded symbols for M_1 on all links upstream of t_1 and only randomly coded symbols for M_2 on all links upstream of t_2 respectively. Now the achievability of the region in the statement of the theorem follows by the fact that $(0, m_2 - E_2)$, (A, B), (C, D) and $(C, 0)$ are the cornerpoints of the rate region given in the statement of the theorem. □

Proof of Theorem 22. By (7.31), $v_1 \leq m_1 - E_1$. Since we impose the condition that all v_i are equal, for every $i = 1, \ldots, n$ $v_i \leq m_1 - E_1$ and the converse holds. Now because $m_1 = \lfloor \frac{m_1}{y} \rfloor y + x_1$ and $m_1 = m_2 - m_1 = m_3 - m_2 = \ldots = m_n - m_{n-1}$, one can write

$$m_1 = m_i - m_{i-1} = \lfloor \frac{m_i - m_{i-1}}{y} \rfloor y + x^i = \lfloor \frac{m_1}{y} \rfloor y + x_1$$

for some $0 \leq x^i \leq y - 1$, $i = 2, \ldots, n$. Hence, $x^i = x_1$. Therefore, by Lemma 20

$$E_1 = \lfloor \frac{m_1}{y} \rfloor x + \min(x_1, x) = \lfloor \frac{m_i - m_{i-1}}{y} \rfloor x + \min(x^i, x)$$

is the maximum number of erasures under the x/y sliding window erasure model that can occur upstream of t_i, but not $t_1, \ldots, t_{i-1}$ for each $i = 1, \ldots, n$. Thus, $(v_1, v_2, \ldots, v_n) = (m_1 - E_1, m_1 - E_1, \ldots, m_1 - E_1)$ is achievable by random linear coding of $m_1 - E_1$ symbols of source message M_i into $m_i - m_{i-1}$ symbols and subsequently forwarding them on links $m_{i-1} + 1, \ldots, m_1$ for each $i = 1, \ldots, n$. □

Proof of Theorem 24. By (7.31), $v_1 \leq m_1 - E_1$. Since we impose the condition that all v_{2i-1} are equal, (7.35) holds for every $i = 1, \ldots, k$. By Theorem 23,

$$(B - D)v_1 + (C - A)v_2 \quad \leq \quad CB - AD,$$

therefore, since $v_1 = v_3 = \ldots = v_{2k-1}$ and $v_2 = v_4 = \ldots = v_{2k}$, all $(B-D)v_{2i-1} + (C-A)v_{2i}$ are equal and (7.36) holds for every $i = 1, \ldots, k$. Simialrly, all $v_{2i-1} + v_{2i}$ are equal and (7.37) holds for every $i = 1, \ldots, k$.

By Theorem 23, (7.35)-(7.37) can be achieved by intrasession coding when $n = 2$. Moreover, by Theorem 22, (7.37) can be achieved by transmitting only coded symbols of M_{2i-1} and M_{2i} upstream of $m_{2(i-1)} + 1, \ldots, m_{2i}$ for each $i = 1, \ldots, k$. We will now show that the cornerpoints of the rate region (7.35)-(7.37), namely, $(v_{2i-1}, v_{2i}) = (0, m_2 - E_2)$, $(v_{2i-1}, v_{2i}) = (A, B)$, $(v_{2i-1}, v_{2i}) = (C, D)$ and $(v_{2i-1}, v_{2i}) = (C, 0)$ can be achieved without intersession coding for every $i = 1, \ldots, k$.

Note that if m_2 is a multiple of y, all m_{2i} are multiples of y for $i = 1, \ldots, k$. Hence, $E_2 = \frac{m_2}{y}x = \frac{m_{2i} - m_{2(i-1)}}{y}x$ for all $i = 1, \ldots, k$. Therefore:

$$\begin{aligned}
A &= \lfloor \frac{m_1}{y} \rfloor (y - x) = \lfloor \frac{m_{2i-1} - m_{2(i-1)}}{y} \rfloor (y - x) = \lfloor \frac{m_{2i-1}}{y} \rfloor y - m_{2(i-1)} - \lfloor \frac{m_{2i-1} - m_{2(i-1)}}{y} \rfloor x \\
B &= m_2 - E_2 - \lfloor \frac{m_1}{y} \rfloor (y - x) = m_{2i} - m_{2(i-1)} - E_2 - \lfloor \frac{m_{2i-1} - m_{2(i-1)}}{y} \rfloor (y - x) \\
&= \frac{m_{2i}}{y} - \lfloor \frac{m_{2i-1}}{y} \rfloor - \left(\frac{m_{2i}}{y} - \lfloor \frac{m_{2i-1}}{y} \rfloor \right) x \\
C &= m_1 - E_1 = m_{2i-1} - m_{2(i-1)} - E_1 \\
D &= m_2 - m_1 - E' = m_{2i} - m_{2i-1} - E'
\end{aligned}$$

For every $i = 1, \ldots, k$, the rate pair $(v_{2i-1}, v_{2i}) = (A, B)$ can be achieved by intrasession coding using the following strategy:

- Perform random linear coding of the A symbols of source message M_{2i-1} into $\lfloor \frac{m_{2i-1}}{y} \rfloor y - m_{2(i-1)}$ symbols and subsequently forward them on links $m_{2(i-1)} + 1 \ldots, \lfloor \frac{m_{2i-1}}{y} \rfloor y$.

- Perform random linear coding of the B symbols of source message M_{2i} into $m_{2i} - \lfloor\frac{m_{2i-1}}{y}\rfloor y$ symbols and subsequently forward them on links $\lfloor\frac{m_{2i-1}}{y}\rfloor y + 1, \ldots, m_{2i}$.

If any x out of y consecutive links in the second layer are erased, at most $\lfloor\frac{m_{2i-1}-m_{2(i-1)}}{y}\rfloor x$ erasures can occur on links $m_{2(i-1)} + 1 \ldots, \lfloor\frac{m_{2i-1}}{y}\rfloor y$. Note that $m_{2i} - \lfloor\frac{m_{2i-1}}{y}\rfloor y$ is a multiple of y. Therefore, by Lemma 20, at most $\left(\frac{m_{2i}}{y} - \lfloor\frac{m_{2i-1}}{y}\rfloor\right) x$ erasures can occur upstream of $\lfloor\frac{m_{2i-1}}{y}\rfloor y + 1, \ldots, m_{2i}$. Hence, the rate pair $(v_{2i-1}, v_{2i}) = (A, B)$ is achievable.

For every $i = 1, \ldots, k$, the rate pair $(v_{2i-1}, v_{2i}) = (C, D)$ can be achieved by intrasession coding using the following strategy:

- Perform random linear coding of the C symbols of source message M_{2i-1} into $m_{2i-1} - m_{2(i-1)}$ symbols and subsequently forward them on links $m_{2(i-1)} + 1, \ldots, m_{2i-1}$.

- Perform random linear coding of the D symbols of source message M_{2i} into $m_{2i} - m_{2i-1}$ symbols and subsequently forward them on links $m_{2i-1} + 1, \ldots, m_{2i}$.

Note that

$$m_1 = m_{2i-1} - m_{2(i-1)} = \lfloor\frac{m_1}{y}\rfloor y + x_1 = \lfloor\frac{m_{2i-1} - m_{2(i-1)}}{y}\rfloor y + x^i$$

for some $0 \le x^i \le y - 1$. Hence, $x^i = x_1$. Then, if any x out of y consecutive links in the second layer are erased, by Lemma 20 at most

$$\lfloor\frac{m_{2i-1} - m_{2(i-1)}}{y}\rfloor x + \min(x^i, x) = \lfloor\frac{m_1}{y}\rfloor x + \min(x_1, x) = E_1$$

erasures can occur on links $m_{2(i-1)} + 1, \ldots, m_{2i-1}$.

Similarly,

$$m_2 - m_1 = m_{2i} - m_{2i-1} = \lfloor\frac{m_2 - m_1}{y}\rfloor y + x' = \lfloor\frac{m_{2i} - m_{2i-1}}{y}\rfloor y + x^i$$

for some $0 \le x^i \le y - 1$. Hence, $x^i = x'$. Then, if any x out of y consecutive links in the second layer are erased, by Lemma 20 at most

$$\lfloor\frac{m_{2i} - m_{2i-1}}{y}\rfloor x + \min(x^i, x) = \lfloor\frac{m_2 - m_1}{y}\rfloor x + \min(x', x) = E'$$

erasures can occur on links $m_{2i-1} + 1, \ldots, m_{2i}$, hence, the rate pair $(v_{2i-1}, v_{2i}) = (C, D)$ is achievable. Similarly, the rate vector $(v_{2i-1}, v_{2i}) = (C, 0)$ can be achieved by transmitting only randomly coded symbols for M_{2i-1} on links $m_{2(i-1)} + 1, \ldots, m_{2i-1}$.

Also,

$$m_2 = m_{2i} - m_{2(i-1)} = \lfloor \frac{m_2}{y} \rfloor y + x_= \lfloor \frac{m_{2i} - m_{2(i-1)}}{y} \rfloor y + x^i$$

for some $0 \leq x^i \leq y - 1$. Hence, $x^i = x_2$. Then, if any x out of y consecutive links in the second layer are erased, by Lemma 20 at most

$$\lfloor \frac{m_{2i} - m_{2(i-1)}}{y} \rfloor x + \min(x^i, x) = \lfloor \frac{m_2}{y} \rfloor x + \min(x_2, x) = E_2$$

erasures can occur on links $m_{2(i-1)} + 1, \ldots, m_{2i}$, hence, the rate vector $(v_{2i-1}, v_{2i}) = (0, m_2 - E_2)$ can be achieved by transmitting only randomly coded symbols for M_{2i} on links $m_{2(i-1)} + 1, \ldots, m_{2i}$. □

Chapter 8

Summary

In this thesis we examined error correction problem in general networks. We discussed noncoherent correction of network errors and erasures with random locations and showed that the relative performance of coding and routing strategies under the probabilistic error and erasure occurrence model depends on the erasure and error probabilities. Then we considered the pollution attack in network coded systems where network nodes are computationally limited, and designed a fountain-like network error correction code that allows us to combine benefits of cryptographic signature-based and information-theoretic security. We also derived error correction capacity regions for coherent and noncoherent multisource multicast network scenarios. We further gave some lower and upper bounds for general nonmulticast error correction problems, and then focused our discussion on nested-demand and two-sink network topologies for which these bounds match. We concluded our discussion by defining a class of 3-layer two-sink and nested-demand networks for which intrasession coding is error- and erasure- correction capacity-achieving.

Finding the error-free capacity region of a general nonmulticast network remains an open problem. Therefore, nonmulticast network scenarios pose a variety of research problems in both error-free and erroneous cases. It is important to continue classification of nonmulticast network topologies for which matching lower and upper bounds can be obtained. In Chapter 7, we conjectured that the z-erasure correction capacity region of a general 3-layer nested-demand network can be achieved by intrasession coding and proved this statement for the case when $z = 1$. It would be interesting to prove or disprove this conjecture for any z and to see whether it extends to the case of a sliding-window erasure model for streaming systems with an arbitrary number of checkpoints.

Our work illustrates a variety of useful tools for analysis and code design in practical error-tolerant networks. For general networks, it seems intractable to find the globally optimal coding strategy. The type and level of attack as well as the network topology play an important role in choosing the best practical strategy. Also, it is common that the nodes in real-world networks are heterogeneous in their capabilities. Therefore, it is critical to characterize the types of networks and the parameters, such as network topology, degree of node heterogeneity, level of attack, etc., that are useful for determining good hybrid strategies that achieve the best performance for a given network scenario and constraints.

Bibliography

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

[2] R. K. D. S. Lun, M. Medard and M. Effros, "On coding for reliable communication over packet networks," *Physical Communication*, vol. 1, no. 5, Mar. 2008.

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

[4] T. Ho, M. Médard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4413–4430, October 2006.

[5] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Transactions on Information Theory*, vol. 52, pp. 789–804, 2006.

[6] N. Cai and R. W. Yeung, "Network coding and error correction," in *ITW2002 Bangalore*, 2002.

[7] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.

[8] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.

[9] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.

[10] T. Ho, S. Jaggi, S. Vyetrenko, and L. Xia, "Universal and robust distributed network codes," in *IEEE Infocom*, April 2011.

[11] F. Zhao, T. Kalker, M. Medard, and K. J. Han, "Signatures for content distribution with network coding," in *Proc. 2007 IEEE International Symposium on Information Theory (ISIT 2007)*, 2007.

[12] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: signature schemes for network coding," *Lecture Notes Comp. Science*, vol. 5443, pp. 68–87, 2009.

[13] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, and M. Effros, "Resilient network coding in the presence of byzantine adversaries," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2596 –2603, June 2008.

[14] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, August 2008.

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

[16] M. J. Siavoshani, C. Fragouli, and S. Diggavi, "Noncoherent multisource network coding," in *Proc. IEEE Int. Symposium on Inform. Theory*, Toronto, Canada, Jul. 2008, pp. 817–821.

[17] S. Mohajer, M. Jafari, S. Diggavi, and C. Fragouli, "On the capacity of multisource non-coherent network coding," in *Proc. of the IEEE Information Theory Workshop*, 2009.

[18] M. Siavoshani, C. Fragouli, and S. Diggavi, "Code construction for multiple sources network coding," in *Proc. of the MobiHoc*, 2009.

[19] E. Erez and M. Feder, "Capacity region and network codes for two receivers multicast with private and common data," in *Proc. IEEE International Symposium on Information Theory*, 2003.

[20] C. Ngai and R. Yeung, "Multisource network coding with two sinks," in *Communications, Circuits and Systems, 2004. ICCCAS 2004. 2004 International Conference on*, vol. 1, June 2004, pp. 34 – 37.

[21] A. Ramamoorthy and R. D. Wesel, “The single source two terminal network with network coding,” in *in Canadian Workshop on Information Theory*, 2005.

[22] T. Chan and A. Grant, “Mission impossible: Computing the network coding capacity region,” in *Proc. IEEE International Symposium on Information Theory*, July 2008, pp. 320 –324.

[23] N. Harvey and R. Kleinberg, “Tighter cut-based bounds for k-pairs communication problems,” in *Proc. 43rd Allerton Conference on Communication, Control, and Computing, Monticello, IL*, September 2005.

[24] S. Vyetrenko, T. Ho, and E. Erez, “On noncoherent correction of network errors and erasures with random locations,” in *Proc. IEEE International Symposium on Information Theory*, June 2009.

[25] S. Vyetrenko, A. Khosla, and T. Ho, “On combining information-theoretic and cryptographic approachers to network coding security against the pollution attack,” in *Asilomar Conference on Systems, Signals and Computers*, November 2009.

[26] S. Vyetrenko, T. Ho, M. Effros, J. Kliewer, and E. Erez, “Rate regions for coherent and noncoherent multisource network error correction,” in *Proc. IEEE International Symposium on Information Theory*, June 2009, pp. 1001 –1005.

[27] T. Dikaliotis, T. Ho, S. Jaggi, S. Vyetrenko, H. Yao, M. Effros, J. Kliewer, and E. Erez, “Multiple-access network information-flow and correction codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1067–1079, February 2011.

[28] S. Vyetrenko, T. Ho, and T. Dikaliotis, “Outer bounds on the error correction capacity region for non-multicast networks,” in *Allerton conference on Communication, Control, and Computing*, September 2010.

[29] T. Ho and D. Lun, *Network coding: an introduction.* Cambridge University Press, 2008.

[30] T. Ho, “Networking from a network coding perspective,” Ph.D. dissertation, Massachusetts Institute of Technology, May 2004.

[31] S. Yang and R. W. Yeung, “Refined coding bounds for network error correction,” in *Proc. 2007 IEEE Information Theory Workshop (ITW 2007)*, July 2007.

[32] D.Silva and F. R. Kschischang, “On metrics for error correction in network coding,” *IEEE Transactions on Information Theory*, vol. 55, pp. 5479–5490, 2009.

[33] R. M. Roth, *Introduction to Coding Theory.* Cambridge University Press, 2006.

[34] H. Yao, T. K. Dikaliotis, S. Jaggi, and T. Ho, “Multi-source operator channels: Efficient capacity-achieving codes,” in *Proc. IEEE Information Theory Workshop*, August 2010.

[35] S. Yang and R. W. Yeung, “Characterizations of network error correction/detection and erasure correction,” in *NetCod 2007*, Jan 2007.

[36] S. Kim, T. Ho, M. Effros, and S. Avestimehr, “Network error correction with unequal link capacities,” in *Proc. of the 47th annual Allerton Cnference on Communication, Control, and Computing*, September 2009, pp. 1387–1394.

[37] O. Kosut, L. Tong, and D. Tse, “Nonlinear network coding is necessary to combat general byzantine attacks,” in *Proc. of the 47th annual Allerton conference on Communication, control, and computing*, September 2009, pp. 593 – 599.

[38] E. Martinian and C.-E.Sundberg, “Burst erasure correction codes with low decoding delay,” *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2494–2502, October 2005.

[39] V. K. Goyal, “Multiple description coding: Compression meets the network,” *IEEE Signal Processing Mag.*, vol. 18, no. 5, pp. 74–93, Sep. 2001.

[40] E. Martinian, “Dynamic information and constraints in source and channel coding,” Ph.D. dissertation, Massachusetts Institute of Technology, September 2004.

[41] H. Seferoglu and A. Markopoulou, “Video-aware opportunistic network coding over wireless networks,” *IEEE JSAC, Special Issue on Network Coding for Wireless Communication Networks*, vol. 27, no. 5, Jun. 2009.