Diversity and Reliability in Erasure Networks: Rate Allocation, Coding, and Routing

by

Shervan Fashandi

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2012

AUTHOR'S DECLARATION I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Shervan Fashandi

Abstract

Recently, *erasure networks* have received significant attention in the literature [1–7] as they are used to model both wireless and wireline packet-switched networks. Many packet-switched data networks like wireless mesh networks [8–10], the Internet [11–13], and Peer-to-peer networks [14] can be modeled as erasure networks. The reason is that each packet contains an internal error detection code, like the *Cyclic Redundancy Check* (CRC), which allows the receiver to detect and discard erroneous packets [12, 15–17].

In any erasure network (wireless mesh network, the Internet, or Peer-to-peer network), path diversity works by setting up multiple parallel connections between the end points using the topological path redundancy of the network. Our analysis of diversity over erasure networks studies the problem of *rate allocation* (RA) across multiple independent paths, coding over erasure channels, and the trade-off between rate and diversity gain in three consecutive chapters.

In chapter 2, *Forward Error Correction* (FEC) is applied across multiple independent paths to enhance the end-to-end reliability. We prove that the probability of irrecoverable loss (P_E) decays exponentially with the number of paths. Furthermore, the RA problem across independent paths is studied. Our objective is to find the optimal RA, i.e. the allocation which minimizes P_E. The RA problem is solved for a large number of paths. Moreover, it is shown that in such asymptotically optimal RA, each path is assigned a positive rate *iff* its *quality* is above a certain threshold. Finally, using memoization technique, a heuristic suboptimal algorithm with polynomial runtime is proposed for RA over a finite number of paths. This algorithm converges to the asymptotically optimal RA when the number of paths is large. For practical number of paths, the simulation results demonstrate the close-to-optimal performance of the proposed algorithm.

Chapter 3 addresses the problem of lower-bounding the probability of error (P_E) for any block code over an *input-independent* channel. First, we define an input-independent chan-

nel in a mathematically accurate way. For discrete memoryless channels, this definition coincides with that of row-symmetric (or simply symmetric) channels which are well-known in the literature. However, we propose a general definition which includes channels with memory extended over a block of N symbols. Next, we derive a lower-bound on P_E for a general input-independent channel and find the necessary and sufficient condition to meet this bound with equality. The rest of this chapter applies this lower-bound to three special input-independent channels: *erasure* channel, *super-symmetric* Discrete Memoryless Channel (DMC), and q-ary *symmetric* DMC. It is proved that *Maximum Distance Separable* (MDS) codes achieve the minimum probability of error over any erasure channel (with or without memory). Moreover, we prove that *perfect* codes achieve the minimum probability of error over super-symmetric channels. Furthermore, for the case of symmetric DMC, we simplify our general lower-bound and propose an algorithm to compute it based on the *method of types* [18] in information theory. We also prove that this lower-bound is exponentially the tightest lower-bound we can achieve. Finally, for ternary and 4-ary symmetric channels, the proposed lower-bound is compared with the previous lower-bounds on P_E in moderate block lengths.

Chapter 4 addresses a fundamental *trade-off* between rate and *diversity gain* of an end-to-end connection in *erasure networks*. An erasure network is modeled by a directed graph whose links are orthogonal erasure channels. Furthermore, the erasure status of the links is assumed to be fixed during each block of transmission and known only by the destination node. For each link e in the graph, a message transmitted on e is erased with probability $p^{\omega(e)}$. We define the diversity gain as $\lim_{p\to 0} \frac{\log P_E}{\log p}$ where P_E is the probability of error. Intuitively speaking, the diversity gain is the asymptotic slope of P_E versus $\frac{1}{p}$ in logarithmic scale. This definition is similar to the standard definition of diversity gain for the slow Rayleigh fading channel in the wireless communication literature [19] if $\frac{1}{p}$ is interpreted as Signal-to-Noise-Ratio (SNR).

First, we study the *homogeneous* erasure networks in which links have the same erasure probability and capacity. We derive the optimum trade-off between diversity gain and end-to-end rate. Then, we prove that a variant of the *conventional routing* strategy combined with an appropriate *forward error correction* (FEC) at the end-nodes achieves the optimum diversity-rate trade-off. Next, we consider general erasure networks in which different links may have different values of erasure probability and capacity. We prove that there exist general erasure networks for which any conventional routing strategy fails to achieve the

optimum diversity-rate trade-off. However, for any general erasure graph, we show that there exists a *linear network coding* strategy which achieves the optimum diversity-rate trade-off.

Finally, we study the diversity-rate trade-off through simulations. The erasure graphs are constructed according to the Barabasi-Albert and Waxman random models. The error probability is depicted for different network strategies and different rate values. The depicted results confirm the trade-off between rate and diversity gain for each network strategy. Moreover, diversity gain is plotted versus the rate for different conventional routing and the linear network coding strategies. It is observed that linear network coding outperforms all conventional routing strategies in terms of the diversity gain [1].

[1]The material of this thesis is also presented in [15, 16, 20, 21]

Acknowledgements

First and foremost, I wish to express my deep gratitude to my supervisor, Professor Amir K. Khandani for providing guidance and inspiration throughout the course of my PhD studies. I have benefited tremendously from his experience and broad knowledge. I value what I learned from him sincerely and would like to thank Amir for the many great opportunities he created for me.

I would like to thank the members of my dissertation committee, Professors Raouf Boutaba, Patrik Mitran, Catherine Rosenberg, and Muriel Medard for taking the time out of their busy schedules to carefully review my thesis, providing me with insightful questions and suggestions.

I was fortunate to collaborate with Shahab Oveis Gharan who is an incredible source of knowledge, encouragement, support, and friendship. I have enjoyed sharing and discussing ideas with him.

I offer my regards and blessings to all members of the Coding and Signal Transmission (CST) Lab, particularly Mahmoud Taherzadeh, Alireza Bayesteh, Kamyar Moshksar, Hamid Ebrahimzad, Vahid Pourahmadi, Behzad Nourani, Javad Abdoli, Mehdi Zamani, Javad Behroozi and Pooya Mahboobi, who supported me in all respects during the completion of my PhD.

I also have to thank three of my teachers in high school and middle school, Dr. Delavari, Mr. Abbas Mahyar, and Mr. Parsfar, who taught me many valuable lessons that I will never forget in my life .

Finally, and most importantly, I thank my parents, for their endless love and support, without which I could not have succeeded in my life. My special thanks and sincere appreciation are extended to my aunt Nooshin and brother Noban for their selfless love. Last but not least, I would like to thank my wife and the love of my life, Shabnam, for all her love and understanding which inspired me to complete my PhD.

Dedication

.

To my parents:

Nasrin and Sadra

and my brother and aunt

Noban and Nooshin

and to my beloved wife:

Shabnam

Contents

List of Tables

List of Figures

List of Abbreviations

CDN	Content Distribution Network
CRC	Cyclic Redundancy Check
DMC	Discrete Memoryless Channel
DRT	Diversity Rate Trade-off
FEC	Forward Error Correction
LDP	Large Deviation Principle
MDR	MDS Coding + Disjoint Routing
MDS	Maximum Distance Separable
MIMO	Multiple-Input Multiple-Output
MMR	MDS Max-Flow Routing
MMRD	MDS Max-Flow Routing with Detours
QoS	Quality of Service
RA	Rate Allocation
SNR	Signal-to-Noise-Ratio

Notation

Boldface Upper-Case Letters	Matrices
Boldface Lower-Case Letters	Vectors
Italic Upper-Case Letters	Graphs
Caligraphic Upper-Case Letters	Events and sets
$\mathbb{P}\{.\}$	Probability of an event
$\mathbb{E}\{.\}$	Expected value of a random variable
$\det(\mathbf{A})$	Determinant of the matrix $\mathbf{A}$
$\mathbf{A}'$	Transpose of $\mathbf{A}$
$\log(.)$	Logarithm function with Neperian base
$P_E \doteq e^{-u(\alpha)L}$	Asymptotic equivalency, $\lim_{L\to\infty} -\frac{\log P_E}{L} = u(\alpha)$
$P_E \dot{\geq} e^{-u(\alpha)L}$	$\lim_{L\to\infty} -\frac{\log P_E}{L} \geq u(\alpha)$
$P_E \dot{\leq} e^{-u(\alpha)L}$	$\lim_{L\to\infty} -\frac{\log P_E}{L} \leq u(\alpha)$
$f(L) = o(g(L))$	Small-O notation, $\lim_{L\to\infty} \frac{f(L)}{g(L)} = 0$
$f(L) = O(g(L))$	Big-O notation, $\exists L_0, M > 0$: $\forall L > L_0, \lvert f(L)\rvert < M \lvert g(L)\rvert$

Chapter 1

Introduction

This work covers three topics related to *erasure networks*: i) rate allocation across multiple paths, ii) coding over *input-independent* channels, iii) *diversity-rate trade-off* in erasure networks. All of these terms will be accurately defined in the next three chapters. Moreover, the next three sections of this chapter go through the motivation, background, and major contributions on each topic. However, before getting into that, it is important to emphasize on one point about the general theme of this thesis: all of the results of this work are valid only when the assumptions corresponding to the results (the models) hold. The model we use in chapter 2 captures the end-to-end channel, while the model in chapter 4 describes a network with one source, one destination, and many intermediate nodes and links. Although we have tried to justify our assumptions and models based on observations and facts from practical networks like wireless mesh networks and the Internet, we have to emphasize that one should use extreme caution in applying and extending the results of this thesis to real-world networks. The models we have considered in this work are, at best, abstractions of practical networks which capture their main concepts but ignore many details. The real-world networks, on the other hand, are extremely complex, and it is naive to expect them to behave as simply as our models do.

Moreover, many of the schemes introduced in this thesis (multi-path routing, network coding, etc) are not easy (although not impossible) to apply on legacy networks like the Internet. However, our results on them may provide valuable insight about the design of future networks for special purposes. These special purposes may include financial or medical applications, for which very high reliability and low latency are required [22, 23].

1.1 Rate Allocation Across Multiple Paths

1.1.1 Motivation

In recent years, *path diversity* over packet switched networks has received significant attention. This idea is applied over different types of networks like wireless mesh networks [8–10, 24], the Internet [11–13], and Peer-to-peer networks [14]. Many studies have shown that path diversity has the ability to simultaneously improve the end-to-end rate and reliability [11, 12, 16, 25–27]. In order to apply path diversity over any packet switched network, two problems need to be addressed: i) setting up multiple independent paths between the end-nodes (multipath routing) ii) utilizing the given independent paths to improve the end-to-end throughput and/or reliability. In this work, we focus on the second problem and try to develop a mathematical analysis of path diversity which is valid for any type of underlying network. Due to the inherent flexibility of wireless mesh networks, many routing protocols can be modified to support multipath routing over such networks [24, 28–34]. Thus, we consider a wireless network as the underlying network. However, it should be noted that the results of this work stay valid for any other underlying network (e.g. path diversity over the Internet) as long as multiple independent paths are given. Assuming a set of independent paths, we utilize *Forward Error Correction* (FEC) across the given paths and analyze the reliability gain achieved by path diversity mathematically. Furthermore, the *rate allocation* (RA) problem across the given paths is addressed, and a polynomial suboptimal algorithm is introduced for this purpose.

1.1.2 Relation to Previous Works

References [27], [12], and [35] study the RA problem over multiple independent paths. Assuming each path follows the leaky bucket model, reference [27] shows that a water-filling scheme provides the minimum end-to-end delay. On the other hand, reference [12] considers a scenario of multiple senders and a single receiver, assuming all the senders share the same source of data. The connection between each sender and the receiver is assumed to be independent from others and follow the *Gilbert model*. In order to benefit from path diversity, the authors apply FEC across independent paths. A *Maximum Distance Separable* (MDS) block code, like Reed-Solomon code, is used for FEC. [12] proposes a receiver-driven protocol for packet partitioning and rate allocation. The packet partitioning

algorithm ensures no sender sends the same packet, while the RA algorithm minimizes the probability of irrecoverable loss in the FEC scheme [12]. They only address the RA problem for the case of two paths. A brute-force search algorithm is proposed in [12] to solve the problem. Generalization of this algorithm over multiple paths results in an exponential complexity in terms of the number of paths. Moreover, it should be noted that the scenario of [12] is equivalent, without any loss of generality, to the case in which multiple independent paths connect a pair of end-nodes as they assume the senders share the same data.

Djukic and Valaee utilize path diversification to provide low probability of packet loss (PPL) in wireless networks [10]. Similar to our work, they consider each path as an erasure channel following the multi-state Markov model. Moreover, it is assumed that the feedback is not fast enough to acknowledge the receipt of each packet. Thus, an MDS code is applied across multiple independent paths as a FEC method. The authors of [10] compare two RA schemes: blind allocation and optimal allocation. The blind RA is used when the source has no information about the quality of the paths. Hence, it distributes the traffic across the paths uniformly. It is shown that even blind RA outperforms single-path transmission. When a feedback mechanism periodically provides the source with information about the quality of each path, the transmitter has the chance to find the RA which minimizes PPL (optimal allocation). The authors propose a greedy algorithm for this purpose.

Most recently, in an independent work, Li *et al.* have addressed the RA problem [35]. Same as [10, 12] and our work, the authors of [35] apply an MDS code for FEC across multiple independent paths. However, unlike [12], the authors study the problem for any general number of paths, denoted by L. Using the *discrete to continuous* approximation, the authors approximate the total number of lost packets over all paths with a continuous random variable. Furthermore, assuming a large number of paths with a large number of packets over each path, they apply the Central-Limit Theorem (CLT) [36] to approximate the distribution of the number of lost packets with the *Normal Distribution*. Using this distribution, the authors propose a pseudo-polynomial algorithm, based on *Dynamic Programming*, to estimate the optimal RA for a large number of paths. However, CLT can not be applied to solve this problem. The reason is that in this case, the variance of the fraction of lost packets scales as $O(\frac{1}{L})$ to zero. Instead, as we show in this work, the distribution of lost packets can be computed using *Large Deviation Principle* (LDP) which results in a distribution totally different from the normal distribution. Hence, the pseudo-polynomial

algorithm proposed in [35] can not necessarily approximate the optimal RA even for large number of paths.

1.1.3 Contribution

In this work, we utilize path diversity to improve the performance of FEC between two end-nodes over a general packet switched network. The details of path setup process is not discussed here. Similar to [10,12,27,35], it is assumed that L independent paths are set up by a smart multipath routing scheme or overlay network. Moreover, as in [10,35,37,38], each path is assumed to be an erasure channel modeled as a continuous M-state extended Gilbert model. It should be noted that the well-known 2-state Gilbert channel used in [12,17,39–41] is a special case of the extended Gilbert model studied here. Probability of irrecoverable loss (P_E) is defined as the measure of FEC performance. In another work, we have shown that MDS block codes have the minimum probability of error over any erasure channel with or without memory [21]. Hence, as in [10, 12, 35], MDS codes are applied for FEC throughout this work. The contributions of this work can be listed as follows:

- Path diversity is shown to simultaneously achieve an exponential decay in P_E and a linear increase in the end-to-end rate with respect to L, while the delay stays fixed. Furthermore, the decaying exponent is analyzed mathematically based on LDP.
- The RA problem is solved for the asymptotic case (large values of L).
- It is proved in the asymptotically optimal RA, each path is assigned a positive rate *iff* its *quality* is above a certain threshold. Quality of a path is defined as the percentage of the time it spends in the bad state. This result is important since for the first time in the literature, an analytical criterion is proposed to predict whether adding an extra path improves reliability.
- A heuristic suboptimal polynomial algorithm, based on the memoization technique, is introduced to solve the RA problem for any arbitrary number of paths. Unlike the brute-force search in [12], this algorithm has a polynomial complexity, in terms of L.
- The proposed algorithm is proved to converge to the asymptotically optimal RA as L grows.

- Through the simulation results, the proposed algorithm is shown to achieve a near-optimal performance for practical number of paths.

1.2 Coding over Input-Independent Channels

1.2.1 Motivation

This work is inspired by our previous work [21] on the optimality of *Maximum Distance Separable* (MDS) codes over erasure channels. In that work, we prove that MDS codes achieve the minimum probability of error over any erasure channel (with or without memory). In an attempt to extend that result, we define a new class of channels called *input-independent* channels of which erasure channels are a special case. Input-independent channels can be memoryless or have memory extended over the block length N. In the case of Discrete Memoryless Channels (DMC), the defined input-independent channel turns into the well-known *symmetric* DMC. Intuitively speaking, input-independent channels are the ones which behave the same way no matter which codeword is transmitted over them. According to this definition, it becomes obvious that erasure channels and symmetric DMC's are both input-independent.

In this work, we introduce a lower-bound on the probability of error (P_E) for any block code over an input-independent channel. This lower-bound is not entirely new and can be derived from Theorem 28 in [42]. However, our contribution is that

- we introduce a much simpler proof of this lower-bound for the specific case of input-independent channels.
- Using the properties of input-independent channels, we come up with the necessary and sufficient condition to satisfy the lower-bound with equality.

In the case of erasure channels, this lower-bound confirms our previous result on the optimality of MDS codes. For the symmetric MDC, the lower-bound turns into a much stronger (tighter) lower-bound than the previous sphere-packing based bounds on P_E [43–45], especially for short to moderate block lengths.

1.2.2 Related Work

Extending Shannon's work [46], Feinstein [47] was the first who observed that the error probability (P_E) for maximum likelihood decoding of a randomly-generated code can be upper-bounded by an exponentially decaying function with respect to the code block length N. This exponent is positive as long as the rate stays below the channel capacity, $R < C$. Following this result, tighter upper-bounds were proposed in the literature [48–50]. For rates below the critical rate, modifications of random coding are proposed to achieve tighter bounds [51]. There are also a number of lower-bounds on the probability of error for any codebook. The most famous of them is known as the *sphere packing* bound [43]. Lower-bounds on P_E are very important as they give us an idea how much the performance of a practical code with finite block length N can be improved.

Both the sphere packing lower-bound and the random coding upper-bound are exponentially tight for rates above the critical rate [52]. In other words, in the asymptotic case where N grows very large, they both converge to $e^{-NE_r(R)}$ where $E_r(R)$ is the famous random coding error exponent for the rate R [50]. However, the rate of convergence for sphere packing bound is shown to be very slow ($O(\frac{1}{\sqrt{N}})$) [44]. This makes the sphere packing bound practically useless for $N < 10000$ in most channels. There has been a number of works to improve this bound for moderate to short block lengths. Reference [44] tightens the sphere packing bound for finite-length codes by re-examining the original derivation of this bound and using better bounding techniques. More recently, [45] improves the sphere-packing bound for symmetric channels even further, while keeping the general framework of sphere packing bound in place.

Most recently, [42] introduces a series of upper and lower bounds on the size (equivalently rate) of any block code with the length N and the probability of error P_E over DMC and Additive White Gaussian Noise (AWGN) channels. Obviously, these bounds translate to upper and lower bounds on the probability of error for any block code with limited length and rate R over these channels. Indeed, Theorem 3.1 of our work can be derived by selecting a uniform output distribution in Theorem 28 of [42]. Moreover, Theorem 35 in [42] introduces a lower-bound on P_E of Binary Symmetric Channel (BSC) which matches our result in section 3.4 exactly. However, our lower-bound in section 3.4 is more general in the sense that it is valid for non-binary symmetric DMC as well.

The following list summarizes the previous lower-bounds on P_E of block codes over different channels and compares them with the lower-bound in section 3.4, denoted by

$L(N, K, \boldsymbol{\pi})$.

- SP59: this lower-bound [53] is valid for soft decoding of equal-energy codewords with Gaussian constellation over the AWGN channel. It can be used as a benchmark for comparison when the input constellation is M-PSK over the AWGN channel with hard or soft decoding.
- SP67: the original sphere packing lower-bound on P_E in [43], valid for any DMC. However, it can not be used for channels with infinite output alphabet size.
- VF2004: Velambois and Fossorier's [44] improvement on SP67, valid for any DMC. Moreover, it can be used for channels with infinite output alphabet size.
- ISP2008: the Improved Sphere-packing Bound (ISP) [45] for symmetric DMC. It is also valid for channels with infinite output alphabet size.
- BSC2010: introduced in Theorem 35 of [42] and is valid for BSC only. It exactly matches our lower-bound, $L(N, K, \boldsymbol{\pi})$, introduced in section 3.4. However, $L(N, K, \boldsymbol{\pi})$ can also be used for non-binary (q-ary) symmetric DMC.
- BEC2010: introduced in Theorem 38 of [42] and is valid for memoryless Binary Erasure Channel (BEC) only. In Theorem 3.3, we show that this lower-bound is achieved by MDS codes in the general case, i.e. q-ary erasure channel with memory.

The lower-bound $L(N, K, \boldsymbol{\pi})$ introduced in section 3.4 has its own limitations; it is valid for q-ary symmetric DMC only. Moreover, it is valid for symmetric DMC's with limited output alphabet size only. However, we have shown that for short to moderate block lengths, $L(N, K, \boldsymbol{\pi})$ outperforms other known lower-bounds (SP59, SP67, VF2004, ISP2008) significantly. For the case of BSC, it matches BSC2010 exactly. Moreover, similar to all of the above bounds, it is exponentially tight for asymptotically large block lengths. This asymptotic tightness is guaranteed by Theorem 3.5.

1.2.3 Contribution

The contributions of this work can be listed as follows:

- The input-independent channel is defined in a mathematically accurate way. The definition includes channels with memory extended over a block of N symbols. For the

case of a DMC, this definition can be simplified into the well-known row-symmetric (also sometimes called symmetric) channel.

- A lower-bound on P_E for a general input-independent channel is reintroduced. This result can be derived from Theorem 28 in [42]. However, we have offered a simpler proof which is based on the properties of input-independent channels. Moreover, the necessary and sufficient condition to meet this lower-bound with equality is given in this work.

- Applying the above lower-bound, we prove that MDS codes achieve the minimum probability of error over any erasure channel (with or without memory). This is not a new result. We have proved the same result in [21] using a *deterministic binning* technique. However, we offer a new proof in this work considering the erasure channel as a special case of the general input-independent channel.

- Again applying the above lower-bound, we prove that a perfect code achieves the minimum probability of error over a super-symmetric DMC (defined in this work).

- We simplify the introduced general lower-bound for the special case of a symmetric DMC and propose an algorithm to compute it using the method of types in information theory [18]. This algorithm has the complexity of $O(N^q)$, i.e. it is polynomial in terms of the block length N and exponential in terms of the alphabet size q. This imposes a restriction on applicability of the algorithm. However, it should be noted that the main application of this algorithm is on short to moderate block codes; for large values of N, the sphere packing bound and its improvements are already good enough. We have been able to run the algorithm for short to moderate block codes with small alphabet size on an average home computer.

- It is shown that the introduced lower-bound for symmetric DMC exponentially equals the random coding upper-bound, $e^{-NE_r(R)}$. This implies that in the asymptotic case, the introduced lower-bound is exponentially tight.

- For finite-length codes over ternary and 4-ary symmetric channels, we compare our lower-bound with the sphere packing bound [43] as well as the recent improvements to it [44, 45]. It is observed that our lower-bound is much tighter than the previous bounds, especially for smaller block lengths.

1.3 Diversity-Rate Trade-off in Erasure Networks

1.3.1 Motivation

Recently, *erasure networks* have received significant attention in the literature [1–7] as they are used to model both wireless and wireline networks. This work addresses a fundamental *trade-off* between rate and the *diversity gain* of an *end-to-end connection* over an erasure network whose links are orthogonal erasure channels. We show that in a general erasure network, *conventional routing*[1] fails to achieve the *optimum diversity-rate trade-off*, while *linear network coding* always achieves the optimum trade-off between rate and diversity gain. All the terms in the italic font are defined in a mathematically accurate way in section 4.2. Here, we aim to intuitively explain the main idea of this work through an example.

Example 1.1. It is easy to observe the diversity-rate trade-off in the erasure network of Fig. 1.1. This simple network consists of only two nodes and n disjoint links between them. Each link transfers one packet (or q-ary symbol) per time slot from source to the destination and may be in the erasure (OFF) mode with the probability p. If the link is OFF, it stays OFF for the entire transmission block. To achieve the maximum reliability, the source should transmit the same data symbol on all n links. Hence, for the rate $r = 1$, the probability of error would be $P_E = p^n$. To maximize the rate, the source has to transmit n different data symbols on the n links to the destination. Thus, for $r = n$ and small values of p, we have $P_E = np(1-p)^{n-1} \approx np \propto p$ where $\propto$ stands for the *proportional to* relation. Now the arising questions are:

- *What can we do between these two extreme points?*
- *Can we achieve some degree of reliability (diversity) without sacrificing too much rate?*
- *What is the maximum achievable reliability (diversity gain) given a certain end-to-end rate?*

[1]For the mathematically accurate definition of conventional routing refer to Definition 4.8 in subsection 4.2.4. Intuitively speaking, conventional routing includes any routing scheme in which the intermediate nodes forward or copy and forward the received messages (packets) to the outgoing links without performing any algebraic operation on the contents of the packets. In contrast, linear network coding works by forwarding a linear combination of the received packets at the outgoing links.

In the special case of Fig. 1.1, these questions can be answered as follows. Consider the case where the source intends to transmit r $(1 < r < n)$ data symbols to the destination. Applying a *Maximum Distance Separable* (MDS) code [21, 54] of size $[n, r]$ (like the Reed-Solomon code [55]), the source encodes the r data symbols to n symbols and transmits them over the n links to the destination. For any MDS code of size $[n, r]$, the receiver can decode the original data symbols if it receives at least r symbols out of the n transmitted symbols correctly [56]. Therefore, for small values of p, P_E can be approximated as $P_E \approx \binom{n}{n-r+1} p^{n-r+1} \propto p^{n-r+1}$. In section 4.3, we prove that the described scheme achieves the best result in terms of $\lim_{p\to 0} \frac{\log P_E}{\log p}$ (later defined as the diversity gain) for any rate r. ■

The reason we focus on the asymptotic region $(p \to 0)$ can be explained as follows. We expect P_E to be a continuous function of p. Using Taylor series [57], we can write P_E as $P_E = \sum_{i=0}^{\infty} K_i p^i$, where K_i's do not depend on p. Of course, K_i can be zero for certain values of i. Let us assume the smallest power of p (with nonzero coefficient) in the Taylor series is $0 \leq d$. For small enough values of p, P_E can be approximated as $P_E \approx K_d p^d$. This lets us quantify P_E with the exponent d and ignore the coefficient K_d. It is easy to observe that in this example, $\frac{1}{p}$ has the same role that Signal-to-Noise-Ratio (SNR) has in slow Rayleigh fading wireless channels [19] (for which $P_E \propto \mathrm{SNR}^d$). Thus, it is intuitively useful to interpret $\frac{1}{p}$ as the SNR in our work. Consequently, small values of p correspond to the high SNR region. Following the wireless communication terminology, we refer to the exponent of p as the *diversity gain*. In the wireless communication literature, the diversity gain d is the (decaying) slope of P_E versus SNR at the high SNR region.

In the example of Fig. 1.1, for any $1 \leq r \leq n$, the diversity gain $d = n - r + 1$ decreases as r increases. In sections 4.3 and 4.4, we show that the trade-off between the rate and diversity gain is present in any *erasure graph*. The objective of this work is to characterize the *optimum diversity-rate trade-off* in general erasure graphs. Intuitively speaking, the optimum diversity-rate trade-off achieves the maximum diversity gain among all end-to-end connections for a given rate[2].

The *trade-off* between diversity and multiplexing gain was first introduced in the context of wireless Multiple-Input Multiple-Output (MIMO) channels. Zheng and Tse [19] defined the multiplexing gain and diversity gain for the high-SNR block-Rayleigh fading MIMO channel. Multiplexing gain is proportional to rate and can be interpreted as the

[2]For the mathematically accurate definition, refer to Definition 4.12 in subsection 4.2.3.

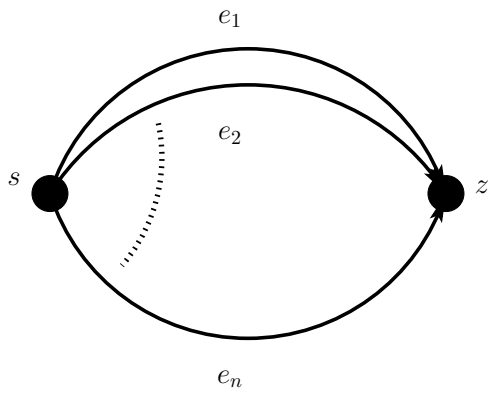


Figure 1.1: A simple erasure network consisting of n disjoint paths.

normalized rate (normalized by $\log(SNR)$). Next, they derived the optimal trade-off between the two gains. Although our model (erasure network) is totally different from the one in [19], an analogy between the trade-offs in both works can be observed if $\frac{1}{p}$ is interpreted as the SNR. The motivation in this work is partly due to this observation.

1.3.2 Related Work

A *wireline network* is modeled by a directed graph $G = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ and $\mathcal{E}$ represent communication nodes and links, respectively. Moreover, the links are noiseless orthogonal channels with a specific capacity and no interference on each other. According to the well-known Ford-Fulkerson Theorem [58], conventional routing can achieve the *unicast* capacity of any wireline network which is equal to the *minimum-cut* of the corresponding weighted graph [59]. Li *et al.* [59] have shown that this result is not valid for the *multicast* case. Indeed, there exists simple wireline networks (such as the butterfly network [60]) such that an operation other than the simple routing and forwarding is needed in the intermediate nodes in order to achieve the multicast capacity [61]. Hence, linear network coding at the intermediate nodes is introduced to achieve the *multicast* capacity of wireline networks [59–61].

The wireline network model has many limitations and can not be applied in many practical networks. Recently, general networks in which links can be erroneous or interact with each other have received significant attention in the literature, e.g. see [1–7, 62]. Dana *et. al* consider the erasure network in which the broadcast nature of the wireless

networks is incorporated while no interference is assumed at the received side of each node. Assuming that the erasure locations on all links of the network are provided to the final destination, the authors derive the ergodic capacity of the network and show that *linear network coding* can achieve the capacity [1]. Most recently, Avestimehr *et. al* [4] show that linear network coding can achieve the (unicast and multicast) capacity of any linear deterministic network with the possible broadcast and interference nature. Yeung and Cai in [5, 6] study the general network whose links can be erroneous (not necessarily erasure). Generalizing the well-known lower-bounds and upper-bounds of the classical coding theory (Singleton bound, Hamming bound, and Gilbert-Varshamov bound), the authors obtain bounds for the number of errors that the network codes can correct in a general network. This subject is further investigated by Koetter and Kschischang in [7]. In contrast with the previous work, the authors assume noncoherent transmission strategy in which the source and destination nodes are unaware of the underlying network topology and the particular linear network coding operations performed at the intermediate nodes.

Among the general networks, the class of erasure networks is of particular interest. Many packet-switched data networks like wireless mesh networks, the Internet, or the virtual overlay networks can be modeled as erasure networks. The reason is that each packet contains an internal error detection code, like the *Cyclic Redundancy Check* (CRC), which lets us interpret the packet as a q-ary symbol transmitted over erasure links [12, 15–17].

Linear network coding is applied in [62, 63] in order to provide protection against network failures. Reference [62] studies the topic of network recovery and distinguishes between path, node, or link protection against non-ergodic link failures in the network. It is demonstrated that many traditional recovery methods (used in conventional routing) can be written in terms of the general framework provided by linear network coding. The authors of [62] consider two formulations for network management: centralized and node-based. In the centralized formulation, the whole network switches between several (end-to-end) linear network codes in order to combat non-ergodic link failures. In other words, the network (the receiver and/or intermediate nodes) adopts the appropriate network code, depending on the state of the network. The measure of performance (management requirement metric) is defined as the logarithm of the number of codes the network switches among. The rationale for this metric is that this equals the information bits one needs to encode the suitable network code for each state of the network. The node-based for-

mulation works similarly except that the metric is different. For this formulation, the network management requirement is defined as the sum over all nodes of the logarithm of the number of behaviors for each node. Again, the rationale for this metric is that this is the number of information bits one needs to inform each and every node of its appropriate behavior according to the network state. For each formulation, [62] considers two recovery schemes: receiver-based and network-wide. In the receiver-based scheme, the only nodes which are allowed to alter their input-output relations are the receiver nodes. In network-wide recovery schemes, on the other hand, the intermediate nodes are allowed to switch between different codes depending on the state of the network. Considering these formulations, [62] achieves lower and upper bounds on the network management metrics for recovery from all single-link failures. The lower-bound is valid for arbitrary connections, while the upper-bound holds for multi-transmitter multicast connections only.

The other reference [63] combines the problem of distributed source coding with linear network coding. It applies random linear network coding for transmission and compression of information in multi-source multicast scenarios with correlated sources. The beauty of this scheme is that intermediate nodes freely pick their coefficients from a large field with no coordination with each other. The only requirement is that the receivers should know the end-to-end transfer matrix of the network. The authors show that this approach achieves the multicast capacity as the network length increases. Moreover, they prove that this scheme compresses the information in a distributed manner, generalizing the known error-exponents for linear Slepian-Wolf coding [64] automatically. Finally, they demonstrate the potential advantages of linear network coding over conventional routing in two practical cases: i) distributed network setting, ii) dynamically varying connections. In the former case, the number of nodes is very large or the topology is changing. Thus, it is expensive or infeasible to maintain the routing states and we need to apply distributed randomized routing schemes. In the latter case, the source-destination pairs may vary or go through ON-OFF periods. They show that in both cases, linear network coding provides higher probability of successful decoding with much lower complexity.

1.3.3 Contribution

In this work, we study a network modeled by an acyclic directed graph $G = (\mathcal{V}, \mathcal{E})$ whose links are orthogonal erasure channels. Such a network is regarded as an *erasure graph* throughout the thesis. Each link $e \in \mathcal{E}$ has the maximum rate of $\sigma(e)$ and the erasure

probability of $p^{\omega(e)}$. Erasure status of the links are assumed to be fixed during one block of transmission[3]. Moreover, erasure status of the links is assumed to be known only by the destination node. Hence, neither the source nor the intermediate nodes are aware of the links' status. This is the case in many realtime applications where the source can not utilize any feedback or retransmission request due to the tight delay constraints.

Here, we study the behavior of *network strategies* for an end-to-end connection in an erasure graph in the asymptotic scenario where $p \to 0$. Network strategies are used to increase the end-to-end rate or to improve the end-to-end reliability. However, we show that there exists a fundamental trade-off between the end-to-end rate and reliability. The contributions of this work can be listed as follows:

- For any fixed rate r, as $p \to 0$, the error probability is shown to decay as p^d where d denotes the *diversity gain* of the corresponding end-to-end connection. Moreover, $d(r)$ is shown to be a decreasing function of r.

- In a homogeneous erasure graph where $\sigma(e) = \omega(e) = 1$ for all links $e \in \mathcal{E}$, it is proved that the combination of MDS coding at the source and appropriate conventional routing at the intermediate nodes achieves the optimum diversity-rate trade-off.

- For any general erasure graph, we show that there exists a *linear network coding* strategy which achieves the optimum diversity-rate trade-off.

- In general erasure graphs, it is proved that conventional routing is not optimum in terms of diversity-rate trade-off. More accurately, there exist general erasure graphs for which any conventional routing strategy fails to achieve the optimum diversity-rate trade-off.

Unlike the previous works which suggest the potential benefit of linear network coding in the error-free *multicast* scenario (in terms of the achievable rate), the above results introduce the benefit of linear network coding in the erasure *unicast* scenario (in terms of the diversity gain).

[3]For the mathematically accurate definition of the model, refer to section 4.2.

Chapter 2

Rate Allocation Across Multiple Paths

2.1 Introduction

2.1.1 Multipath Routing over Wireless Mesh Networks

In order to exploit path diversity, it is desirable to set multiple independent paths between the end nodes. This problem is addressed throughput the literature [28–34, 65, 66]. A set of paths are defined to be independent if their corresponding packet loss patterns are independent. According to the definition, any set of disjoint paths are independent. Even when the paths are not completely disjoint, their loss and delay patterns show a high degree of independence as long as they do not share any congestion points or bottlenecks [12, 67–72]. Many techniques are proposed to detect the shared congestion points, such as cross-correlation-based approach [73], entropy-based approach [74], and wavelet-based approach [75]. Hence, the independence of a set of paths can be verified by the mentioned bottleneck detection algorithms.

Many well-known mesh network routing protocols like AODV [76] and DSR [77] can be modified to support multipath routing. Indeed, DSR can find multiple paths naturally by its flooding behavior [77]. However, it does guarantee that the found paths are disjoint. The Split Multipath Routing (SMR) [28] solves this problem as it avoids dropping duplicate *Route Request* (RREQ) packets by the intermediate nodes. Of course, this is achieved at the cost of more RREQs and higher routing overhead. Similarly, the Multipath Source Routing

(MSR) [34] introduces a multiple path routing protocol extended from DSR. Based on the measurement of Round-Trip Times (RTT), MSR also proposes a scheme to distribute the load among multiple paths. Leung *et al.* [33] propose the MP-DSR protocol which focuses on a newly defined metric for the QoS called the *end-to-end reliability*. MP-DSR is an algorithm which selects multiple paths with low fail probability associated by stable radio links. [32] addresses the problem of transmitting video with double description in the case where non of the paths to the destination is significantly more reliable than the others. The problem is turned into an optimization which is too complex to have a closed-form solution. Thus, the authors apply the metaheuristic *genetic algorithm* to find a suboptimal solution. Then, it is shown that this method can be incorporated into many existing on-demand routing protocols like DSR [32]. Finally, the Robust Multipath Source Routing Protocol (RMPSR) is another extension to DSR to support multipath video communication over wireless networks.

AMODV [30] is an Ad-hoc On-demand Multipath Distance Vector routing protocol based on the concept of link reversal extending from AODV. In contrast with the DSR-based multipath routing protocols, AMODV discovers multiple link-disjoint loopfree paths. AODVM [31] is another extension to AODV which finds multiple reliable routing paths. Similarly, AODV-BR [29] introduces an algorithm to find back up routing paths over Ad hoc networks. [9] proposes a novel multipath hybrid routing protocol, Multipath Mesh (MMESH), which effectively discovers multiple paths over wireless mesh networks. Simulation results show that MMESH is able to balance the traffic by avoiding hot paths, i.e., the paths with higher traffic load. AMTP [65], an ad hoc multipath streaming protocol for multimedia delivery which selects multiple maximally disjointed paths with best QoS to maximize the aggregate end-to-end throughput. AMTP is able to accurately differentiate between packet losses due to different network conditions. In case of a path being broken, it seamlessly switches to a proper path and therefore maintains high streaming quality. When there are multiple channels between the wireless mesh nodes, it is easier to find multiple independent paths across the network. Reference [8] applies the idea of multipath routing in such a scenario to increase the end-to-end throughput. Wei *et al.* [26] address the problem of path selection over a wireless network by taking into account the interference between the wireless links. Their goal is to minimize the *packet drop probability* (PDP). The problem of optimal multipath selection is shown to be NP-hard. Therefore, they introduce a heuristic algorithm to find a close-to-optimal set of paths. A previous work

by the same authors [78] studies video multicast over wireless ad hoc networks. To take advantage of network path diversity in the multicast case, an algorithm to find multiple disjoint and near-disjoint trees is proposed. Finally, reference [24] introduces CodeCast, a network-coding-based ad hoc multicast protocol, for (mainly multimedia) applications which require limited (low) packet rate as well as limited (low) latency. For such applications, the authors have shown that path diversity can be used to mitigate the non-local packet loss problem with very small overhead.

2.1.2 Path Diversity over the Internet

In the Internet, the end-points have no control over the path selection process. Indeed, letting the end nodes set the paths requires modification of the IP routing protocol and extra signaling between the routers which are extremely costly. To avoid such an expense, *overlay networks* are introduced [70, 71, 79]. The basic idea of the overlay network is to equip very few nodes (smart nodes) with the desired new functionalities while the rest remain unchanged. The smart nodes form a virtual network connected through virtual or logical links on top of the physical network. Thus, overlay nodes can be used as relays to set up independent paths between the end nodes [13, 80–82].

Topology of the underlying physical network is an important factor in the design of the overlay network. Indeed, improper design of the overlay network can result in shared bottlenecks between different virtual links [83]. In such cases, even if two paths are disjoint in the virtual level, a large degree of dependency may be observed between them. Hence, a class of *topology-aware* overlay networks are proposed to maximize independence between the virtual links [83–89]. For instance, the overlay nodes can utilize latency [84, 85] or the underlying IP topological information [83, 86–89] to select the neighbors and form the overlay graph. It is shown that the topology-aware overlay networks can provide a satisfactory degree of independence between disjoint paths (disjoint in the virtual level) [83]. Moreover, distributed algorithms can be utilized to construct and/or maintain overlay networks. Reference [90] addresses the problem of distributed overlay network design based on a game theoretical approach, while [91] studies overlay networks failure detection and recovery through dynamic probing.

Another issue which may degrade path diversity in overlay networks is having bottlenecks in the links connecting the end-nodes to the network. To address this problem, the idea of *multihoming* is proposed [13, 92]. In this technique, the end users are connected to

more than one *Internet Service Providers* (ISP's) simultaneously. It is shown that multi-homing assists overlay networks to set up extra independent paths between the end-points, i.e. improves the end-to-end reliability considerably [13].

2.1.3 Applications of Path Diversity

Recently, path diversity is utilized in many applications (see [17, 93–97]). Reference [95] combines multiple description coding and path diversity to improve the quality of service (QoS) in video streaming. In [25], multiple descriptions of video are routed throughput different paths across a wireless mesh network. It is assumed that coding is *non-hierarchical* in the sense that none of the descriptions is the main description. Instead, the distortion decreases gradually as the receiver receives more descriptions of the video. Moreover, non of the paths has significantly better quality than the others, and each link is modeled by a 2-state Markov model called the Gilbert channel. [25] concludes that in this setup, utilizing multiple paths improves both the rate and reliability.

Packet scheduling over multiple paths is addressed in [98] to optimize the rate-distortion function of a video stream. Reference [97] utilizes path diversity to improve the quality of Voice over IP streams. According to [97], sending some redundant voice packets through an extra path helps the receiver buffer and the scheduler optimize the trade-off between the maximum tolerable delay and the packet loss ratio [97].

In [11], multipath routing of TCP packets is applied to control the congestion with minimum signaling overhead. When the underlying network is an ad hoc wireless network, a similar result is reported [99]. In other words, transmitting video over multiple paths is shown to decrease the average congestion and end-to-end distortion. [100] proposes a multiflow reatime transport protocol for wireless networks. Through both mathematical analysis and comprehensive simulation, it is shown that partitioning the video packets across multiple paths improves queuing performance of the multimedia data, resulting is less congestion, smaller delay, and higher utilization of the bottleneck link bandwidth [100].

Content Distribution Networks (CDN's) can also take advantage of path diversity for performance improvement. CDN's are a special type of overlay networks consisting of *Edge Servers* (nodes) responsible for delivery of the contents from an original server to the end users [79,101]. Current commercial CDN's like *Akamai* use path diversity based techniques like *SureRoute* to ensure that the edge servers maintain reliable connections to the original server. Video server selection schemes are discussed in [80] to maximize path diversity in

Table 2.1: Important Parameters

Notation	Refers to	Section
L	number of the paths	1.1.3
N	length of an FEC block (in packets)	2.2.2
K	number of information packets in an FEC block	2.2.2
$\alpha=(N-K)/N$	FEC overhead	2.2.2
T	transmission time of an FEC block	2.2.3
S_{req}	required end-to-end rate (pkt/sec)	2.2.3
N_i	number of packets transmitted on path i in each FEC block	2.2.3
S_i, W_i	rate and max. rate of path i (pkt/sec)	2.2.3
P_E	probability of irrecoverable loss	1.1.3
$x_i = B_i/T$	fraction of bad bursts on path i during T	2.3
ρ_i	fraction of end-to-end rate assigned to path i	2.3.1
J	number of path types	2.3.2
$\gamma_j = L_j/L$	fraction of paths of type j	2.3.2
η_j	fraction of the end-to-end rate allocated to paths of type j, see (2.7)	2.3.2
$\boldsymbol{\eta}^\star$	asymptotically optimal rate allocation vector	2.3.2
$\boldsymbol{\eta}^{opt}=\mathbf{N}^{opt}/N$	optimal rate allocation vector	2.3.2
N_j	number of packets transmitted on paths of type j in each FEC block	2.4
$P_e^{\mathbf{N}}(k,j)$	probability of having more than k errors over paths of types 1 to j for the allocation vector $\mathbf{N}$	2.4
$Q_j(n,k)$	probability of having exactly k errors out of the n packets sent over paths of type j	2.4
$\mathbf{N}^{opt}$	optimum allocation vector	2.4
$P_e^{opt}(n,k,j)$	$P_e^{\mathbf{N}^{opt}}(k,j)$, i.e., min P_E	2.4
$\hat{P}_e(n,k,j)$	lowerbound of $P_e^{opt}(n,k,j)$, see (2.16)	2.4
$\hat{\mathbf{N}}=(N_1,...,N_J)$	suboptimum allocation vector	2.4
$\mathbf{K}=(K_1,...,K_J)$	typical error event	2.4

CDN's.

2.1.4 Chapter Organization

The rest of this chapter is organized as follows. Section 2.2 describes the system model. Performance of FEC in two cases of multiple identical paths, and non-identical paths are analyzed in section 2.3. Section 2.4 studies the RA problem, and proposes a suboptimal RA algorithm. Finally, section 2.5 concludes the chapter.

2.2 System Modeling and Formulation

2.2.1 End-to-End Channel Model

From an end to end protocol's perspective, performance of the lower layers in the protocol stack can be modeled as a random *channel* called the *end-to-end channel*. Since each packet usually includes an internal error detection coding (for instance a Cyclic Redundancy Check), the end-to-end channel is modeled as an erasure channel.

Numerous measurements studies have suggested that bursty loss behavior is the most dominant characteristic of the end-to-end channel over different underlying networks, including wireless mesh networks and the Internet [10,38,102–104]. Hence, a variety of models have been proposed to capture this bursty behavior, including the 2-state Gilbert model, the M-state Extended Gilbert model, and the Hidden Markov model [37, 38, 102, 105, 106]. This chapter assumes the continuous time M-state extended Gilbert model for the end-to-end channel, see Fig. 2.1. This model achieves a good balance between model accuracy and simplicity [35, 37, 38]; it is much more accurate than the 2-state Gilbert Model, while only requires $2(M-1)$ parameters to be estimated (as opposed to M^2 parameters in the General Markov Model). It should be noted that the well-known 2-state Gilbert channel used in [12, 17, 39–41] is a special case of the extended Gilbert model studied here.

It is worth mentioning that the main results of this chapter remain valid for any end-to-end channel model. More precisely, P_E still decays exponentially versus L and the asymptotically optimal RA follows the same formula. However, the decaying exponent of P_E is a function of the bad burst probability distribution which should be recomputed according to the new end-to-end channel model. Moreover, in the proposed suboptimal RA algorithm, no assumption is made regarding the end-to-end channel model and/or the bad burst probability distribution. In other words, the input parameters to the proposed algorithm consist of the probability mass function (pmf) associated with the number of erasures over different paths. These input parameters are computed in polynomial time in appendix 2.6.8 for any general Markov model which obviously includes the extended Gilbert model as a special case.

The behavior of the continuous time extended Gilbert model can be described as follows. The channel spends an exponentially distributed random amount of time with the mean $\frac{1}{\mu_g}$ in the *Good* state. Then, it alternates to the first *Bad* state, B_1, and stays in that state for another random duration exponentially distributed with mean $\frac{1}{\mu_{b_1}+\kappa_1}$. Then, the

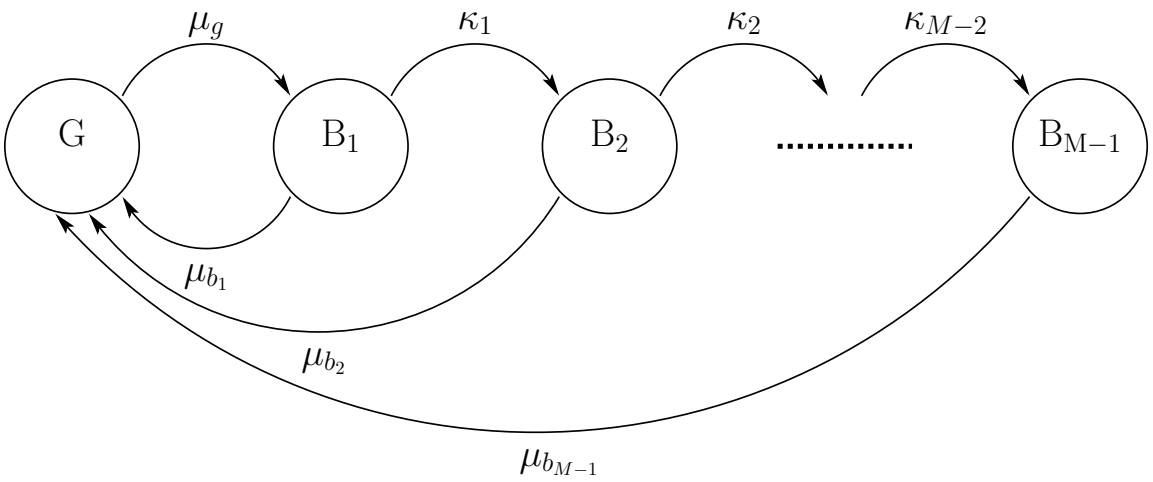


Figure 2.1: Continuous-time M-state Extended Gilbert model of the end-to-end channel

channel either goes back to the good state or transits to a deeper bad state, denoted by B_2. Similarly, the channel can move to deeper bad states consecutively before going back to the good state. The steady state probability of being in the good or any of the bad states are denoted by π_g and π_{b_i}. It is easy to observe that $\pi_g = \frac{1}{\mu_g \Xi}$ and $\pi_{b_i} = \frac{1}{(\mu_{b_i}+\kappa_i)\Xi}$ where $\Xi \triangleq \frac{1}{\mu_g} + \sum_{i=1}^{M-1} \frac{1}{\mu_{b_i}+\kappa_i}$. The packets transmitted during the good state are received correctly, while they are lost if transmitted during any of the bad states (B_1 to B_{M-1}). Therefore, the average probability of error, π_b, is equal to the steady state probability of being in any of the bad states, $\pi_b = \sum_{i=1}^{M-1} \pi_{b_i}$.

2.2.2 FEC Model

In real-time applications like video and audio over wireless mesh networks or IP, due to the delay requirement, conventional retransmission based schemes such as automatic repeat request (ARQ) are impractical. On the other hand, FEC is shown to be favorable for such real-time scenarios with tight QoS requirement [10, 39, 40, 107–109]. However, FEC could be ineffective when bursty packet loss occurs and such loss exceeds the recovery capability of the FEC codes. To mitigate this problem via path diversity, this work applies FEC across multiple paths.

Each packet is provided with an internal coding such as the Cyclic Redundancy Check (CRC) which enables the receiver to detect an error inside each packet. Hence, the receiver

can consider the end-to-end channel as an erasure channel. Assuming the length of each packet is r bits, the alphabet size of the end-to-end channel would be $q = 2^r$. Other than the coding inside each packet, a FEC scheme is applied between packets. Every K packets are encoded to a *Block* of N packets where $N > K$ to create some redundancy. The N packets of each block are distributed across the L available independent paths, and are received at the destination with some loss (erasure). The ratio of $\alpha \triangleq \frac{N-K}{N}$ defines the FEC overhead. It is proved that among all block codes of the same size, any *Maximum Distance Separable* (MDS) code, such as the Reed-Solomon code, provides the minimum probability of error over an erasure channel (either memoryless or with memory) [21]. Moreover, MDS codes can reconstruct the original K data packets at the receiver side if K or more of the N packets are received correctly [55]. This property makes MDS codes favorable FEC schemes over the erasure channels [35, 110–112].

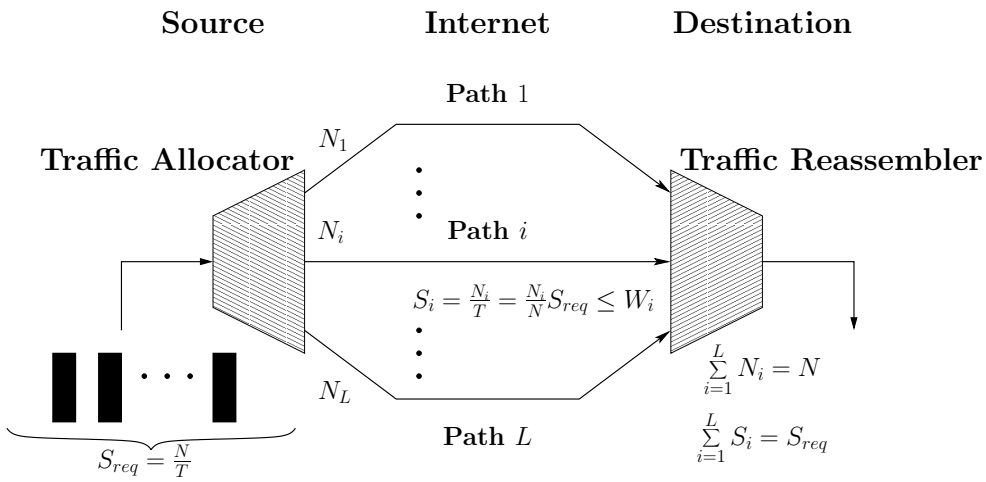
Since MDS codes are used for FEC, the probability of irrecoverable loss, P_E, is adopted as the reliability metric. An irrecoverable loss occurs when more than $N - K$ packets are lost in a block of N packets. It is shown in [21] that P_E is almost equal to the error probability of the maximum likelihood decoder for an MDS code, $P_{\mathcal{E}}$. More precisely, P_E can be bounded as

$$P_{\mathcal{E}} \leq P_E \leq \left(1 + \frac{1}{q-1}\right) P_{\mathcal{E}}$$

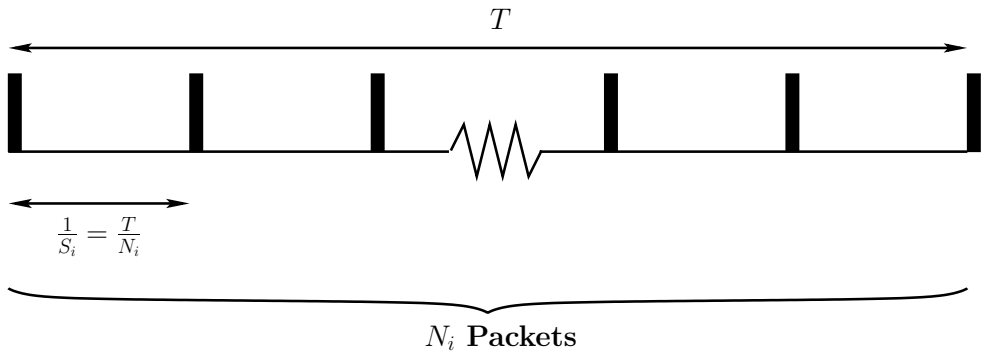
where q denotes the alphabet size of the MDS code which is very large in our application. The reason P_E is used as the measure of system performance is that while many practical low-complexity decoders for MDS codes work perfectly if the number of correctly received symbols is at least K, their probability of correct decoding is much less than that of maximum likelihood decoders when the number of correctly received symbols is less than K [55]. Thus, in the rest of this chapter, P_E is used as a close approximation of decoding error.

2.2.3 Rate Allocation Problem

The RA problem is formulated as follows. L independent paths, $1, 2, \ldots, L$, connect the source to the destination, as indicated in Fig. 2.2(a). Information bits are transmitted as packets, each of a constant length r. Each path has a rate constraint of W_i packets per second. This constraint can be considered as an upperbound imposed by the physical characteristics of the path. For a specific application and FEC scheme, we require the rate



(a)



(b)

Figure 2.2: RA problem: a block of N packets is being sent from the source to the destination through L independent paths over the network during the time interval T with the required rate $S_{req} = \frac{N}{T}$. The block is distributed over the paths according to the vector $\mathbf{N} = (N_1, \ldots, N_L)$ which corresponds to the RA vector $\mathbf{S} = (S_1, \ldots, S_L)$

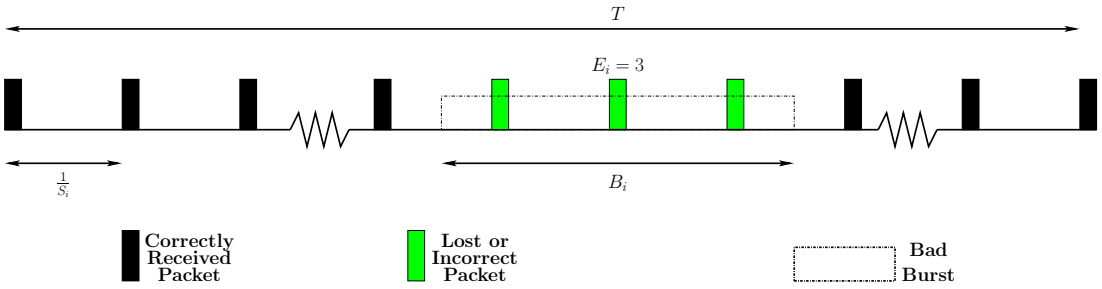


Figure 2.3: A bad burst of duration B_i happens in a block of length T. $E_i = 3$ packets are corrupted or lost during the interval B_i. Packets are transmitted every $\frac{1}{S_i}$ seconds, where S_i is the rate of path i in pkt/sec.

of S_{req} packets per second from the source to the destination. Obviously, we should have $S_{req} \leq \sum_{i=1}^{L} W_i$ to have a feasible solution. As mentioned in the previous subsection, the information packets are coded in blocks of length N packets. Hence, it takes $T = \frac{N}{S_{req}}$ seconds to transmit one block.

The RA vector $\mathbf{N} = (N_1, \ldots, N_L)$ is defined as the number of packets in one block sent through each path. The objective of the RA problem is to find the optimal RA vector, i.e. the RA vector minimizing the probability of irrecoverable loss, P_E, defined in the previous subsection. The RA vector should satisfy the constraints $\sum_{i=1}^{L} N_i = N$ and $\frac{N_i}{T} \leq W_i, \forall\ 1 \leq i \leq L$. The latter constraint follows from the bandwidth constraint, $S_i = \frac{N_i}{T} \leq W_i$.

The above formulation of RA problem is valid for any finite number of paths and any chosen values of N and T. However, in section 2.3 where the performance of path diversity is studied for a large number of paths, and also in Theorem 2.2 where the optimality of the proposed suboptimal algorithm is proved for the asymptotic case, we assume that N grows linearly in terms of the number of paths, i.e. $N = n_0 L$, for a fixed n_0. The reason behind this assumption is that when L grows asymptotically large, the number of paths eventually exceeds the block length, if N stays fixed. Thus, $L - N$ paths become useless for the values of N larger than N. At the same time, it is assumed that the delay imposed by FEC, T, stays fixed with respect to L. This model results in a linearly increasing rate as the number of paths grows.

2.2.4 Discrete to Continuous Approximation

To compute P_E, we have to find the probability of k_i packets being lost out of the N_i packets transmitted through path i, for all $1 \leq i \leq L,\ 0 \leq k_i \leq N_i$. Let us denote the number of erroneous or lost packets over the path i with the random variable E_i. Any two subsequent packets transmitted over the path i are $\frac{1}{S_i}$ seconds apart in time, where S_i is the transmission rate over the i'th path. Now, we define the continuous random variable B_i as the duration of time that path i spends in the bad state in a block duration, T. It is easily observed that the probability $\mathbb{P}\{E_i \geq k_i\}$ can be approximated with the continuous counterpart $\mathbb{P}\{B_i \geq \frac{k_i}{S_i}\}$ when the inter-packet interval is much shorter than the average bad burst duration. According to the extended Gilbert model, the average bad burst duration can be lower-bounded by $\frac{1}{\mu_{b_1}+\kappa_1}$. Therefore, as long as we have $\dfrac{1}{S_i} \ll \dfrac{1}{\mu_{b_1}+\kappa_1}$, the discrete to continuous approximation is valid (see Fig. 2.3).

The necessity of this condition can be justified as follows. In case this condition does not hold, any two consecutive packets have to be transmitted on two independent states of the channel. Thus, no gain would be achieved by applying diversity over multiple independent paths. The continuous approximation is just used in section 2.3. On the other hand, section 2.4 studies the RA problem in the original discrete format.

2.2.5 Notation and System Parameters

Table 2.2 summarizes the main assumptions made in our network model and problem formulation. The important parameters which are used throughout the chapter are summarized in Table 2.1. Moreover, the following mathematical notations are used in the rest of the chapter. $\mathbb{P}\{.\}$ and $\mathbb{E}\{.\}$ are defined as the probability and expected value operators, respectively. The notation $P_E \doteq e^{-u(\alpha)L}$ means $\lim_{L\to\infty} -\frac{\log P_E}{L} = u(\alpha)$. $f(L) = o(g(L))$ is equivalent to $\lim_{L\to\infty} \frac{f(L)}{g(L)} = 0$, and $f(L) = O(g(L))$ means that $\exists L_0, M > 0 : \forall L > L_0, |f(L)| < M\,|g(L)|$.

2.3 Performance Analysis of FEC on Multiple Paths

According to the discrete to continuous approximation in subsection 2.2.4, when the N_i packets of the FEC block are sent over path i, the loss count can be written as $\frac{B_i}{T}N_i$.

Table 2.2: Main Assumptions

Assumption	Comments
L independent paths	justified in subsection 2.1.1 and 2.1.2 used in sections 2.3 and 2.4
discrete to continuous approximation	justified in subsection 2.2.4 used in section 2.3
Extended Gilbert Model	justified in subsection 2.2.1 used in section 2.3 results valid without this assumption see subsections 2.2.1 and 2.3.1 for details

Hence, the total ratio of lost packets is equal to

$$\sum_{i=1}^{L} \frac{B_i N_i}{TN} = \sum_{i=1}^{L} \frac{B_i \rho_i}{T}$$

where $\rho_i \triangleq \frac{S_i}{S_{req}}$, $0 \leq \rho_i \leq 1$, denotes the portion of the bandwidth assigned to path i. $x_i \triangleq \frac{B_i}{T}$ is defined as the portion of time that path i has been in the bad state ($0 \leq x_i \leq 1$). Hence, the probability of irrecoverable loss for an MDS code is equal to

$$P_E = \mathbb{P}\left\{ \sum_{i=1}^{L} \rho_i x_i > \alpha \right\}. \tag{2.1}$$

In order to find the optimum rate allocation, P_E has to be minimized with respect to the allocation vector (ρ_i's), subject to the following constraints:

$$0 \leq \rho_i \leq \min\left\{1, \frac{W_i}{S_{req}}\right\}, \quad \sum_{i=1}^{L} \rho_i = 1 \tag{2.2}$$

where W_i is the bandwidth constraint on path i defined in subsection 2.2.3.

2.3.1 Identical Paths

When the paths are identical and have equal bandwidth constraints[1] ($W_i = W$ for $\forall\ 1 \leq i \leq L$), due to the symmetry of the problem, the uniform RA ($\rho_i = \frac{1}{L}$) is obviously the

[1]The case where W_i's are different is discussed in Remark 2.4 of subsection 2.3.2

optimum solution. Of course, the solution is feasible only when we have $\frac{1}{L} \leq \frac{W}{S_{req}}$. Then, the probability of irrecoverable loss can be simplified as

$$P_E = \mathbb{P}\left\{\frac{1}{L}\sum_{i=1}^{L} x_i > \alpha\right\}. \tag{2.3}$$

Let us define $Q(x)$ as the probability density function of x. Since x is defined as $x = \frac{B}{T}$, clearly we have $Q(x) = Tf_B(xT)$, where $f_B(t)$ is the probability density function (pdf) of B. Defining $\mathbb{E}\{\}$ as the expected value operator throughout this chapter, $\mathbb{E}\{x\}$ can be computed based on $Q(x)$. We observe that in (2.3), the random variable x_i's are bounded and independent. Hence, the following well-known upperbound in large deviation theory [113] can be applied

$$P_E \leq e^{-u(\alpha)L}$$
$$u(\alpha) = \begin{cases} 0 & \text{for } \alpha \leq \mathbb{E}\{x\} \\ \lambda\alpha - \log(\mathbb{E}\{e^{\lambda x}\}) & \text{otherwise} \end{cases} \tag{2.4}$$

where the log function is computed in Neperian base, and λ is the solution of the following non-linear equation, which is shown to be unique by Lemma 2.1.

$$\alpha = \frac{\mathbb{E}\{xe^{\lambda x}\}}{\mathbb{E}\{e^{\lambda x}\}}. \tag{2.5}$$

Since λ is unique, we can define $l(\alpha) = \lambda$. Even though being an upperbound, inequality (2.4) is exponentially tight for large values of L [113]. More precisely

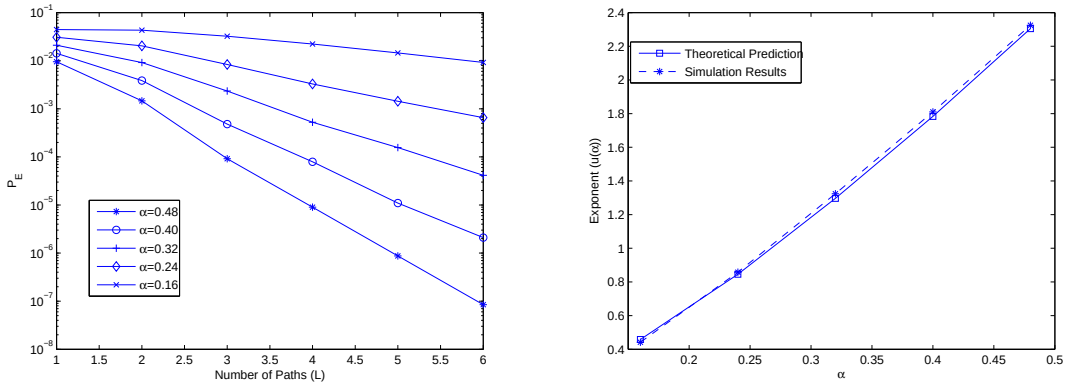
$$P_E \doteq e^{-u(\alpha)L} \tag{2.6}$$

where the notation $\doteq$ means $\lim_{L\to\infty} -\frac{\log P_E}{L} = u(\alpha)$. Note that $u(\alpha)$ depends on the pdf of B, $f_B(t)$, which is computed in appendix 2.6.1. Of course, equation (2.6) is valid regardless of the pdf of B.

Next, we state the following lemmas which are required for the analysis of the next subsection. The proofs can be found in the appendices 2.6.2 and 2.6.3, respectively.

Lemma 2.1. *$u(\alpha)$ and $l(\alpha)$ have the following properties:*

1. $\frac{\partial}{\partial\alpha} l(\alpha) > 0$



(a) (b)

Figure 2.4: (a) P_E vs. L for different values of α. (b) The exponent (slope) of plot (a) for different values of α: experimental versus theoretical values.

2. $l(\alpha = 0) = -\infty$

3. $l(\alpha = \mathbb{E}\{x\}) = 0$

4. $l(\alpha = 1) = +\infty$

5. $\frac{\partial}{\partial\alpha}u(\alpha) = l(\alpha) > 0$ *for* $\alpha > \mathbb{E}\{x\}$

Lemma 2.2. *Defining* $y = \frac{1}{L}\sum_{i=1}^{L} x_i$, *where* x_i*'s are i.i.d. random variables as already defined, the probability density function of* y *satisfies* $f_y(\alpha) \doteq e^{-u(\alpha)L}$, *for all* $\alpha > \mathbb{E}\{x\}$.

Remark 2.1. A special case is when the block code uses all the bandwidth of the paths. In this case, we have $N = LWT$, where W is the maximum bandwidth of each path, and T is the block duration. Assuming $\alpha > \mathbb{E}\{x\}$ is a constant independent of L, we observe that the information packet rate is equal to $\frac{K}{T} = (1-\alpha)WL$, and the error probability is $P_E \doteq e^{-u(\alpha)L}$. This shows using MDS codes over multiple independent paths provides an exponential decay in the irrecoverable loss probability and a linearly growing end-to-end rate in terms of the number of paths, simultaneously.

Example 2.1. Consider the scenario of transmitting a video stream with the DVD quality (using either MPEG-2 or MPEG-4) over multiple identical paths. The bitrate per path is

selected to be 1 Mbps. The number of paths varies from $L = 1$ to $L = 6$. Hence, the end-to-end video bitrate varies in the range of $1 - 6$ Mbps, in accordance with [114–118]. The block transmission time is $T = 200$ ms which imposes an acceptable end-to-end delay for the video stream. The payload of each video packet is assumed to be 4 kb. Accordingly, the block length equals to $N = n_0 L$ where n_0 can be written as $n_0 = \frac{1 \text{ Mbps}}{4 \text{ kb}} T = 50$. The end-to-end channel follows a 2-state Gilbert model with $\frac{1}{\mu_g} = 2500$ ms and $\frac{1}{\mu_b} = 52$ ms, in accordance with [12, 17]. Coding overhead is changed from $\alpha = 0.16$ to $\alpha = 0.48$. Figure 2.4 compares the result of (2.6) with the simulation results. P_E is plotted versus L in semilogarithmic scale in Fig. 2.4(a) for different values of α. We observe that as L increases, $\log P_E$ decays linearly which is expected noting equation (2.6). Also, Fig. 2.4(b) compares the slope of each plot in Fig. 2.4(a) with $u(\alpha)$. Figure 2.4 shows a good agreement between the theory and the simulation results for practical number of paths. Moreover, it verifies the fact that the stronger the FEC code is (larger α), the higher is the gain we achieve through path diversity (larger exponent).

2.3.2 Non-Identical Paths

Now, let us assume there are J types of paths between the source and the destination, consisting of L_j identical paths of type j ($\sum_{j=1}^{J} L_j = L$). Without loss of generality, we assume that the paths are ordered according to their associated type, i.e. the paths from $1 + \sum_{k=1}^{j-1} L_k$ to $\sum_{k=1}^{j} L_k$ are of type j. We denote $\gamma_j = \frac{L_j}{L}$. According to the i.i.d. assumption, it is obvious that ρ_i has to be the same for all paths of the same type. η_j and y_j are defined as

$$\begin{aligned} \eta_j &= \sum_{\sum_{k=1}^{j-1} L_k < i \leq \sum_{k=1}^{j} L_k} \rho_i \\ y_j &= \frac{\eta_j}{L\gamma_j} \sum_{\sum_{k=1}^{j-1} L_k < i \leq \sum_{k=1}^{j} L_k} x_i. \end{aligned} \tag{2.7}$$

Following Lemma 2.2, we observe that $f_{y_j}(\beta_j) \doteq e^{-\gamma_j u_j(\frac{\beta_j}{\eta_j})L}$. We define the sets $\mathcal{S}_I$, $\mathcal{S}_O$ and $\mathcal{S}_T$ as

$$\begin{aligned}
\mathcal{S}_I &= \left\{(\beta_1,\beta_2,\cdots,\beta_J)\,|0\le\beta_j\le 1,\ \sum_{j=1}^{J}\beta_j>\alpha\right\}\\
\mathcal{S}_O &= \left\{(\beta_1,\beta_2,\cdots,\beta_J)\,|0\le\beta_j\le 1,\ \sum_{j=1}^{J}\beta_j=\alpha\right\}\\
\mathcal{S}_T &= \left\{(\beta_1,\beta_2,\cdots,\beta_J)\,|\eta_j\mathbb{E}\left\{x_j\right\}\le\beta_j,\sum_{j=1}^{J}\beta_j=\alpha\right\}
\end{aligned}$$

respectively. Hence, P_E can be written as

$$\begin{aligned}
P_E &= \mathbb{P}\left\{\sum_{j=1}^{J}y_j>\alpha\right\}\\
&= \int_{\mathcal{S}_I}\prod_{j=1}^{J}f_{y_j}(\beta_j)d\beta_j\\
&\doteq \int_{\mathcal{S}_I} e^{-L\sum_{j=1}^{J}\gamma_j u_j(\frac{\beta_j}{\eta_j})}\prod_{j=1}^{J}d\beta_j\\
&\overset{(a)}{\doteq} e^{-L\min\limits_{\boldsymbol{\beta}\in\mathcal{S}_I\cup\mathcal{S}_O}\sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j}{\eta_j}\right)}\\
&\overset{(b)}{\doteq} e^{-L\min\limits_{\boldsymbol{\beta}\in\mathcal{S}_O}\sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j}{\eta_j}\right)}\\
&\overset{(c)}{\doteq} e^{-L\min\limits_{\boldsymbol{\beta}\in\mathcal{S}_T}\sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j}{\eta_j}\right)}\\
&\overset{(d)}{\doteq} e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{\beta_j^\star}{\eta_j}\right)}
\end{aligned}\tag{2.8}$$

where (a) follows from Lemma 2.3, (b) follows from the fact that $u_j(\alpha)$ is a strictly increasing function of α, for $\alpha>\mathbb{E}\{x_j\}$, and (c) can be proved as follows. Let us denote the vector which minimizes the exponent over the set $\mathcal{S}_O$ as $\hat{\boldsymbol{\beta}}^\star$. Since $\mathcal{S}_T$ is a subset of

$\mathcal{S}_O$, $\hat{\boldsymbol{\beta}}^\star$ is either in $\mathcal{S}_T$ or in $\mathcal{S}_O - \mathcal{S}_T$. In the former case, (c) is obviously valid. When $\hat{\boldsymbol{\beta}}^\star \in \mathcal{S}_O - \mathcal{S}_T$, we can prove that $0 \leq \hat{\beta}_j^\star \leq \eta_j \mathbb{E}\{x_j\}$, for all $1 \leq j \leq J$, by contradiction. Let us assume the opposite is true, i.e., there is at least one index $1 \leq j \leq J$ such that $0 \leq \hat{\beta}_j^\star \leq \eta_j \mathbb{E}\{x_j\}$, and at least one other index $1 \leq k \leq J$ such that $\eta_k \mathbb{E}\{x_k\} < \hat{\beta}_k^\star$. Then, knowing that the derivative of of $u_j(\alpha)$ is zero for $\alpha = \mathbb{E}\{x_j\}$ and strictly positive for $\alpha > \mathbb{E}\{x_j\}$, a small increase in $\hat{\beta}_j^\star$ and an equal decrease in $\hat{\beta}_k^\star$ reduces the objective function, $\sum_{j=1}^{J} \gamma_j u_j \left(\frac{\beta_j}{\eta_j}\right)$, which contradicts the assumption that $\hat{\boldsymbol{\beta}}^\star$ is a minimum point. Knowing that $0 \leq \hat{\beta}_j^\star < \eta_j \mathbb{E}\{x_j\}$, for all $1 \leq j \leq J$, it is easy to show that the minimum value of the objective function is zero over $\mathcal{S}_O$, and $\mathcal{S}_T$ has to be an empty set. Defining the minimum value of the positive objective function as zero over an empty set ($\mathcal{S}_T$) makes (c) valid for the latter case where $\hat{\boldsymbol{\beta}}^\star \in \mathcal{S}_O - \mathcal{S}_T$. Finally, applying Lemma 2.4 results in (d) where $\boldsymbol{\beta}^\star$ is defined in the lemma.

Lemma 2.3. *For any continuous positive function $h(\mathbf{x})$ over a convex set $\mathcal{S}$, and defining $H(L)$ as*

$$H(L) = \int_{\mathcal{S}} e^{-h(\mathbf{x})L} d\mathbf{x}$$

we have

$$\lim_{L\to\infty} -\frac{\log(H(L))}{L} = \inf_{\mathcal{S}} h(\mathbf{x}) = \min_{cl(\mathcal{S})} h(\mathbf{x})$$

where $cl(\mathcal{S})$ denotes the closure of $\mathcal{S}$ (refer to [119] for the definition of the closure operator).

Proof of Lemma 2.3 can be found in appendix 2.6.4.

Lemma 2.4. *There exists a unique vector $\boldsymbol{\beta}^\star$ with the elements $\beta_j^\star = \eta_j l_j^{-1}\left(\frac{\nu\eta_j}{\gamma_j}\right)$ which minimizes the convex function $\sum_{j=1}^{J} \gamma_j u_j(\frac{\beta_j}{\eta_j})$ over the convex set $\mathcal{S}_T$, where ν satisfies the following condition*

$$\sum_{j=1}^{J} \eta_j l_j^{-1}\left(\frac{\nu\eta_j}{\gamma_j}\right) = \alpha. \tag{2.9}$$

$l^{-1}()$ denotes the inverse of the function $l()$ defined in subsection 2.3.1.

Proof of Lemma 2.4 can be found in appendix 2.6.5.

Equation (2.8) is valid for any fixed value of $\boldsymbol{\eta}$. To achieve the most rapid decay of P_E,

the exponent must be maximized over $\boldsymbol{\eta}$.

$$\lim_{L\to\infty} -\frac{\log P_E}{L} = \max_{0\le\eta_j\le 1} \sum_{j=1}^{J} \gamma_j u_j \left(\frac{\beta_j^\star}{\eta_j}\right) \tag{2.10}$$

where $\boldsymbol{\beta}^\star$ is defined for any value of the vector $\boldsymbol{\eta}$ in Lemma 2.4. Theorem 2.1 solves the maximization problem in (2.10) and identifies the asymptotically optimum RA. The proof can be found in appendix 2.6.6.

Theorem 2.1. *Consider a point-to-point connection over the network with L independent paths from the source to the destination, with a large enough bandwidth constraint[2]. The paths are from J different types, L_j paths from the type j. Assume a block FEC of size $[N, K]$ is sent during a time interval T. Let N_j denote the number of packets in a block of size N assigned to the paths of type j, such that $\sum_{j=1}^{J} N_j = N$. The RA vector $\boldsymbol{\eta}$ is defined as $\eta_j = \frac{N_j}{N}$. For fixed values of $\gamma_j = \frac{L_j}{L}$, $n_0 = \frac{N}{L}$, $k_0 = \frac{K}{L}$, T and asymptotically large number of paths L, the optimum rate allocation vector $\boldsymbol{\eta}^\star$ equals to*

$$\eta_j^\star = \begin{cases} 0 & \text{if } \alpha \le \mathbb{E}\{x_j\} \\ \dfrac{\gamma_j l_j(\alpha)}{\displaystyle\sum_{i=1,\ \alpha>\mathbb{E}\{x_i\}}^{J} \gamma_i l_i(\alpha)} & \text{otherwise} \end{cases} \tag{2.11}$$

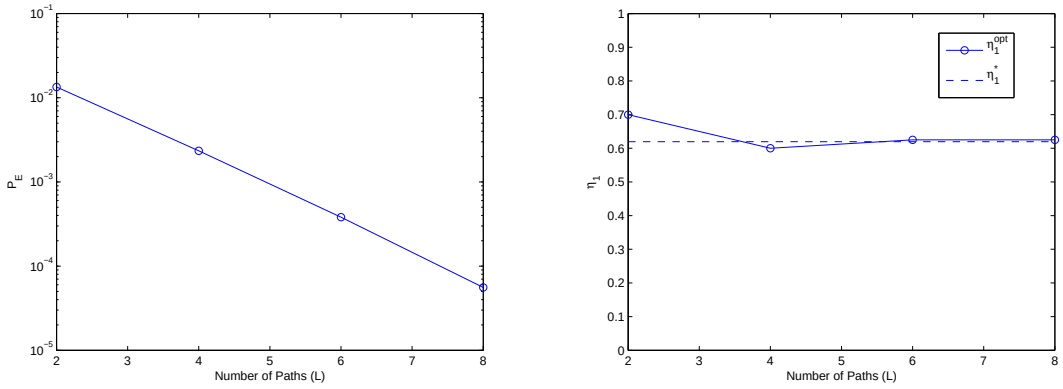
if there is at least one $1 \le j \le J$ for which $\alpha > \mathbb{E}\{x_j\}$. Furthermore, the probability of irrecoverable loss corresponding to $\boldsymbol{\eta}^\star$ decays as

$$P_E \doteq e^{-L\sum_{j=1}^{J} \gamma_j u_j(\alpha)}. \tag{2.12}$$

In the case where $\alpha \le \mathbb{E}\{x_j\}$ for $1 \le j \le J$, $P_E \doteq 1$ independent of the allocation vector $\boldsymbol{\eta}$.

Remark 2.2. Theorem 2.1 can be interpreted as follows. For large values of L, adding a new

[2]By the term 'large enough', we mean the bandwidth constraint on a path of type j, W_j, satisfies the condition $\frac{\eta_j n_0}{T\gamma_j} \le W_j$. The reason is that η_j must satisfy both conditions of $0 \le \eta_j \le 1$ and $\frac{N_j}{TL_j} = \frac{\eta_j n_0 L}{T\gamma_j L} \le W_j$, simultaneously. When W_j is large enough such that $\frac{\eta_j n_0}{T\gamma_j} \le W_j$, the latter condition is automatically satisfied, and the optimization problem can be solved.



(a) (b)

Figure 2.5: (a) P_E versus L for the combination of two path types, half from type I and half from type II. (b) The normalized aggregated weight of type I paths in the optimal rate allocation (η_1^{opt}), compared with the value of η_1 which maximizes the exponent of equation (2.10) ($\eta_1^{\star}$).

type of path contributes to the path diversity *iff* the path satisfies the quality constraint $\alpha > \mathbb{E}\{x\}$, where x is the percentage of time that the path spends in the bad state during the time interval $[0, T]$. Only in this case, adding the new type of path exponentially improves the performance of the system in terms of the probability of irrecoverable loss.

Remark 2.3. Observing the exponent coefficient corresponding to the optimum allocation vector $\boldsymbol{\eta}^{\star}$, we can see that the typical error event occurs when the ratio of the lost packets on all types of paths is the same as the total fraction of the lost packets, α. However, this is not the case for any arbitrary RA vector $\boldsymbol{\eta}$.

Remark 2.4. An interesting extension of Theorem 2.1 is the case where all types have identical erasure patterns ($u_j(x) = u_k(x)$ for $\forall\ 1 \leq j, k \leq J$ and $\forall x$), but different bandwidth constraints. Adopting the notation of Theorem 2.1, the bandwidth constraint on η_j can be written as $\frac{\eta_j n_0 L}{T \gamma_j L} \leq W_j$, where W_j is the maximum bandwidth for a path of type j. Let us define $\tilde{\boldsymbol{\eta}}^{\star}$ as the allocation vector which maximizes the objective function of equation (2.10), and satisfies the bandwidth constraints too. $\boldsymbol{\eta}^{\star}$ is the maximizing vector for the unconstrained problem, defined in Theorem 2.1. According to equation (2.11), we have $\eta_j^{\star} = \gamma_j$ for $\forall 1 \leq j \leq J$. It is obvious that $\tilde{\boldsymbol{\eta}}^{\star} = \boldsymbol{\eta}^{\star}$ if $\eta_j^{\star} \leq \frac{\gamma_j W_j T}{n_0}$ for all j. In case $\eta_j^{\star}$ does not satisfy the bandwidth constraint for some j, $\tilde{\boldsymbol{\eta}}^{\star}$ can be found by the water-filling

algorithm. More accurately, we have

$$\tilde{\eta}_j^\star = \begin{cases} \dfrac{\gamma_j W_j T}{n_0} & \text{if } \tilde{\eta}_j^\star \leq \gamma_j \Upsilon \\ \gamma_j \Upsilon & \text{if } \tilde{\eta}_j^\star < \dfrac{\gamma_j W_j T}{n_0} \end{cases} \tag{2.13}$$

where Υ can be found by imposing the condition $\sum_{j=1}^{J} \tilde{\eta}_j^\star = 1$. Figure 2.6 depicts water-filling among identical paths with four different bandwidth constraints. Proof of equation (2.13) can be found in appendix 2.6.7.

Example 2.2. Consider the scenario of transmitting a video stream with the DVD quality (using either MPEG-2 or MPEG-4) over multiple paths of two types. The number of paths for each type are equal, i.e. $\gamma_1 = \gamma_2 = 0.5$. The total number of paths varies from $L = 2$ to $L = 8$. Both type of paths are modeled as 2-state Gilbert channels with $\frac{1}{\mu_g} = 2500$ ms, in accordance with [12,17]. Furthermore, the average bad burst duration are equal to $\frac{1}{\mu_{b_1}} = 50$ ms for the first type and $\frac{1}{\mu_{b_2}} = 100$ ms for the second type. The block transmission time is $T = 200$ ms which imposes an acceptable end-to-end delay for the video stream. The payload of each video packet is assumed to be 5 kb. The end-to-end rate increases linearly with L such that $\frac{S_{req}}{L} = 1$ Mbps. Hence, the block length equals to $N = 40L$. The coding overhead is $\alpha = 0.3$. Figure 2.5(a) shows P_E of the optimum RA versus L. The optimal RA, $\boldsymbol{\eta}^{opt}$, is found by exhaustive search among all possible allocation vectors. The figure depicts a linear behavior in semi-logarithmic scale with the exponent of 0.9137, which is comparable to 0.9256 predicted by (2.11).

In this scenario, let us denote $\eta_1^\star$ as the value of the first element of $\boldsymbol{\eta}^\star$, given in equation (2.11). Obviously, $\eta_1^\star$ does not depend on L. Moreover, η_1^{opt} is defined as the normalized aggregated weight of type I paths in the optimal RA. Figure 2.5(b) compares η_1^{opt} with $\eta_1^\star$ for different number of paths. It is observed that η_1^{opt} converges rapidly to $\eta_1^\star$ as L grows.

2.4 Suboptimal Rate Allocation

In order to compute the complexity of the RA problem, we focus our attention on the original discrete formulation in subsection 2.2.3. According to the model of subsection 2.3.2, we assume the available paths are from J types, L_j paths from type j, such that $\sum_{j=1}^{J} L_j =$

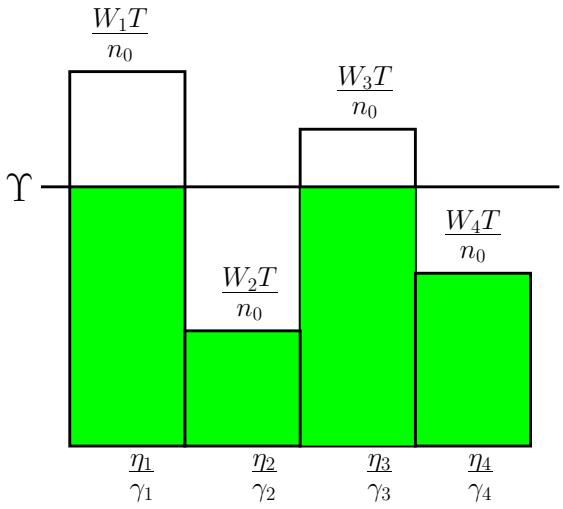


Figure 2.6: WaterFilling algorithm over identical paths with four different bandwidth constraints.

L. Obviously, all the paths from the same type should have equal rate. Therefore, the RA problem is turned into finding the vector $\mathbf{N} = (N_1, \ldots, N_J)$ such that $\sum_{j=1}^{J} N_j = N$, and $0 \leq N_j \leq L_j W_j T$ for all j. N_j denotes the number of packets assigned to all the paths of type j. Let us temporarily assume that all paths have enough bandwidth such that N_j can vary from 0 to N for all j. There are $\binom{N+J-1}{J-1}$ L-dimensional non-negative vectors of the form $(N_1, \ldots, N_J)$ which satisfy the equation $\sum_{j=1}^{J} N_j = N$ each representing a distinct RA. Hence, the number of candidates is exponential in terms of J.

First, we prove the RA problem is NP [120] in the sense that P_E can be computed in polynomial time for any candidate vector $\mathbf{N} = (N_1, \ldots, N_J)$. Let us define $P_e^{\mathbf{N}}(k, j)$ as the probability of having more than k errors over the paths of types 1 to j for a specific allocation vector $\mathbf{N}$. We also define $Q_j(n, k)$ as the probability of having exactly k errors out of the n packets sent over the paths of type j. In appendices 2.6.8 and 2.6.9, $Q_j(n, k)$'s are computed for any general M-state Markov channel model with polynomial complexity. Hence, we can assume that $Q_j(n, k)$'s are precomputed and stored for all n and k and path

types. Then, the following recursive formula holds for $P_e^{\mathbf{N}}(k,j)$

$$\begin{aligned} P_e^{\mathbf{N}}(k,j) &= \begin{cases} \sum_{i=0}^{N_j} Q_j(N_j,i) P_e^{\mathbf{N}}(k-i,j-1) & \text{if } k \geq 0 \\ 1 & \text{if } k < 0 \end{cases} \\ P_e^{\mathbf{N}}(k,1) &= \sum_{i=k+1}^{N_1} Q_1(N_1,i). \end{aligned} \tag{2.14}$$

To compute $P_e^{\mathbf{N}}(K,J)$ by the above recursive formula, we apply a well-known technique in the theory of algorithms called *memoization* [121]. Memoization works by storing the computed values of a recursive function in an array. By keeping this array in the memory, memoization avoids recomputing the function for the same arguments when it is called later. To compute $P_e^{\mathbf{N}}(K,J)$, an array of size $O(KJ)$ is required. This array should be filled with the values of $P_e^{\mathbf{N}}(k,j)$ for $0 < k \leq K$, and $1 \leq j \leq J$. Computing $P_e^{\mathbf{N}}(k,j)$ requires $O(K)$ operations assuming the values of $P_e^{\mathbf{N}}(i,j-1)$ and $Q_j(N_j,i)$ and $\sum_{i=k+1}^{N_j} Q_j(N_j,i)$ are already computed for $0 \leq i \leq k$. Thus, $P_e^{\mathbf{N}}(K,J)$ can be computed with the complexity of $O(K^2J)$ if the values of $Q_j(N_j,k)$ are given for all N_j and $0 \leq k \leq K$. Following appendix 2.6.9, we note that for each j, $Q_j(N_j,k)$ for $0 \leq k \leq K$ is computed offline with the complexity of $O(K^2L_j) + O\left(M^2 \frac{N_j}{L_j} K\right)$. Hence, the total complexity of computing $P_e^{\mathbf{N}}(K,J)$ adds up to

$$\begin{aligned} & O(K^2J) + \sum_{j=1}^{J} O\left(K^2L_j + M^2 \frac{N_j}{L_j} K\right) \\ \overset{(a)}{=} \; & O(K^2J) + \sum_{j=1}^{J} O\left(K^2L_j + M^2 N_j K\right) \\ \overset{(b)}{=} \; & O\left(K^2L + M^2 KN\right) \end{aligned} \tag{2.15}$$

where (a) follows from the fact that $\frac{N_j}{L_j} < N_j$, and the term $O(K^2J)$ is omitted in (b) since we know that $J < L$.

Now, we propose a suboptimal polynomial time algorithm to estimate the best path allocation vector, $\mathbf{N}^{opt}$. Let us define $P_e^{opt}(n,k,j)$ as the probability of having more than k errors for a block of length n over the paths of types 1 to j minimized over all possible

RA's ($\mathbf{N} = \mathbf{N}^{opt}$). First, we find a lowerbound $\hat{P}_e(n,k,j)$ for $P_e^{opt}(n,k,j)$ from the following recursive formula

$$\hat{P}_e(n,k,j) = \begin{cases} \min\limits_{0 \le n_j \le \min\{n, \lfloor L_j W_j T \rfloor\}} \sum\limits_{i=0}^{n_j} Q_j(n_j,i) \cdot \\ \qquad \hat{P}_e(n-n_j, k-i, j-1) & \text{if } k > 0 \\ \\ 1 & \text{if } k \le 0 \end{cases}$$

$$\hat{P}_e(n,k,1) = \sum_{i=k+1}^{n} Q_1(n,i). \tag{2.16}$$

Using memoization technique, we need an array of size $O(NKJ)$ to store the values of $\hat{P}_e(n,k,j)$ for $0 < n \le N$, $0 < k \le K$, and $1 \le j \le J$. According to the recursive definition above, computing $\hat{P}_e(n,k,j)$ requires $O(NK)$ operations assuming the values of $Q_j(n_j,i)$ and $\hat{P}_e(n-n_j,k-i,j-1)$ and $\sum_{i=k+1}^{n_j} Q_j(n_j,i)$ are already computed for all i and n_j. Thus, it is easy to verify that $\hat{P}_e(N,K,J)$ can be computed with the complexity of $O(N^2K^2J)$ when the values of $Q_j(n_j,i)$ are given for all $0 < n_j \le N$ and $0 \le i \le n_j$. According to appendix 2.6.9, for each $1 \le j \le J$, $Q_j(n_j,i)$ can be computed for all $0 < n_j \le N$ and $0 \le i \le n_j$ with the complexity of $O(N^3L_j) + O(M^2\frac{N^2}{L_j})$. Thus, computing $Q_j(n_j,i)$ for all $1 \le j \le J$, and $0 < n_j \le N$, and $0 \le i \le n_j$, has the complexity of $\sum_{j=1}^{J} O(N^3L_j) + O(M^2\frac{N^2}{L_j}) = O(N^3L + M^2N^2J)$. Finally, $\hat{P}_e(N,K,J)$ can be computed with the total complexity of $O(N^2K^2J + N^3L + M^2N^2J)$.

The following lemma guarantees that $\hat{P}_e(n,k,j)$ is in fact a lowerbound for $P_e^{opt}(n,k,j)$. The proof is given in appendix 2.6.10.

Lemma 2.5. $P_e^{opt}(n,k,j) \ge \hat{P}_e(n,k,j)$.

Algorithm 1 recursively finds a suboptimum allocation vector $\hat{\mathbf{N}}$ based on the lowerbound of Lemma 2.5.

Intuitively speaking, the proposed suboptimal algorithm recursively finds the typical error event (K_j's) which has the maximum contribution to the error probability, and assigns the RA ($\hat{N}_j$'s) such that the estimated typical error probability ($\hat{P}_e$) is minimized. Indeed, Lemma 2.5 shows that the estimate used in the algorithm ($\hat{P}_e$) is a lower-bound for the minimum achievable error probability (P_e^{opt}). Comparing (2.16) and the **while** loop in Algorithm 1, we observe that the values of $\hat{N}_j$ and K_j can be found in $O(1)$ during the

Algorithm 1 Proposed Suboptimal RA Algorithm

Require: $N,\ K,\ J,\ (L_1,\ldots,L_J),\ Q_j(\cdot,\cdot),\ \hat{P}_e(\cdot,\cdot,\cdot)$
Ensure: $(\hat{N}_1,\ldots,\hat{N}_J)$
  Initialize $j \leftarrow J$; $n \leftarrow N$; $k \leftarrow K$;
  while $j > 1$ and $k \geq 0$ **do**
    $\hat{N}_j \leftarrow \underset{0\leq n_j \leq \min\{n, \lfloor L_j W_j T \rfloor\}}{\operatorname{argmin}} \sum_{i=0}^{n_j} \hat{P}_e(n-n_j, k-i, j-1)\cdot Q_j(n_j, i)$;
    $K_j \leftarrow \underset{0\leq i\leq \hat{N}_j}{\operatorname{argmax}} Q_j(\hat{N}_j, i)\hat{P}_e(n-\hat{N}_j, k-i, j-1)$;
    Update $n \leftarrow n-\hat{N}_j$; $k \leftarrow k-K_j$; $j \leftarrow j-1$;
  end while
  for $m = 1$ to j **do**
    $\hat{N}_m \leftarrow \lfloor \frac{n}{j} \rfloor$;
  end for
  for $m = 1$ to $(n$ **mod** $j)$ **do**
    $\hat{N}_m \leftarrow \hat{N}_m + 1$;
  end for
  return $(\hat{N}_1,\ldots,\hat{N}_J)$;

computation of $\hat{P}_e(N,K,J)$. Hence, complexity of the proposed algorithm is the same as that of computing $\hat{P}_e(N,K,J)$ which is $O(N^2K^2J + N^3L + M^2N^2J)$.

The following theorem guarantees that the output of the above algorithm converges to the asymptotically optimal RA introduced in Theorem 2.1 of section 2.3.2, and accordingly, it performs optimally for large number of paths. The proof can be found in appendix 2.6.11.

Theorem 2.2. *Consider a point-to-point connection over the network with L independent paths from the source to the destination, each with a large enough bandwidth constraint. The paths are from J different types, L_j paths from the type j. Assume a block FEC of the size $[N,K]$ is sent during an interval time T. For fixed values of $\gamma_j = \frac{L_j}{L},\ n_0 = \frac{N}{L},\ k_0 = \frac{K}{L},\ T$ and asymptotically large number of paths (L) we have*

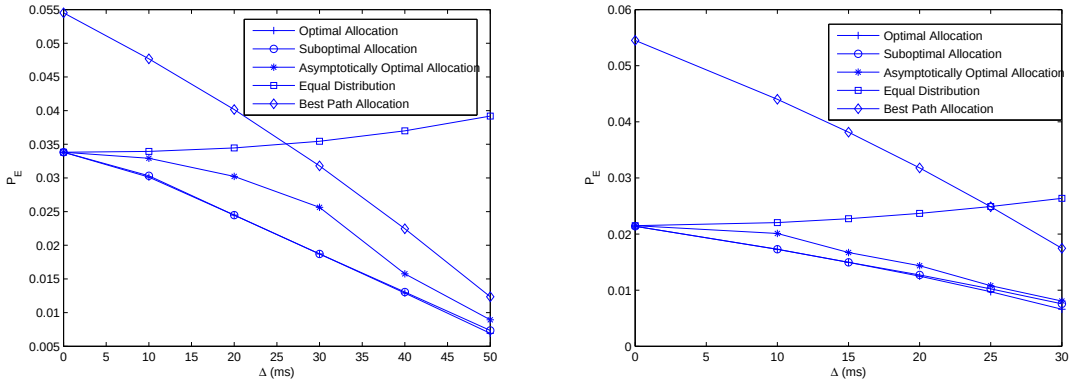
1. $\hat{P}_e(N,K,J) \doteq P_e^{opt}(N,K,J) \doteq e^{-L\sum_{j=1}^{J}\gamma_j u_j(\alpha)}$
2. $\frac{\hat{N}_j}{N} = \eta_j^\star + o(1)$
3. $\frac{K_j}{\hat{N}_j} = \alpha + o(1)$ *for* $\alpha > \mathbb{E}\{x_j\}$.

where $\alpha = \frac{k_0}{n_0}$ *and* $u_j()$ *are defined in subsections 2.3.1 and 2.3.2.* $\hat{P}_e(N, K, J)$ *is the lower-bound for* $P_e^{opt}(n, k, j)$ *defined in equation* (2.16). $\hat{N}_j$ *is the total number of packets assigned to the paths of type* j *by the suboptimal rate allocation algorithm.* $\eta_j^\star$ *is the asymptotically optimal RA given in equation* (2.11). K_j *is also defined in Algorithm 1.*

Example 2.3. The proposed algorithm is compared with four other allocation schemes over $L = 4$ and $L = 3$ paths in Fig. 2.7. The optimal method uses exhaustive search over all possible allocations. '*Best Path Allocation*' assigns everything to the best path only, ignoring the rest. '*Equal Distribution*' scheme distributes the packets among all paths equally. Finally, the '*Asymptotically Optimal*' allocation assigns the rates based on equation (2.11). A DVD-quality video stream with the end-to-end rate of $S_{req} = 3.2$ Mbps is studied in both scenarios of Fig. 2.7. The block transmission time is $T = 250$ ms which imposes an acceptable end-to-end delay for the video stream. The payload of each packet is adopted to be 4 kb. Accordingly, the block length would be equal to $N = S_{req}T = 200$ packets. The FEC coding overhead is fixed at $\alpha = 0.2$. The paths follow the 2-state Gilbert model with $\frac{1}{\mu_g} = 2500$ ms. However, quality of the paths are different as they have different average bad burst durations: (a) In the case of 3 paths, the average bad burst of the paths ($\frac{1}{\mu_b}$'s) are listed as $[75 \text{ ms}, 75 \text{ ms} \pm \Delta]$; (b) In the case of 4 paths, the average bad burst of the paths ($\frac{1}{\mu_b}$'s) are listed as $[75 \text{ ms} \pm \frac{\Delta}{2}, 75 \text{ ms} \pm \frac{3\Delta}{2}]$; As observed, the median of $\frac{1}{\mu_b}$ of paths is fixed at 75 ms in both scenarios. Δ represents a measure of deviation from this median. $\Delta = 0$ describes the case where all the paths are identical. The larger is Δ, the more variety we have among the paths and the more diversity gain might be achieved using a judicious RA.

As seen, our suboptimal algorithm tracks the optimal algorithm so closely that the corresponding curves are not easily distinguishable in most cases. However, the '*Asymptotically Optimal*' RA results in lower performance since L is relatively small which makes the asymptotic analysis assumptions invalid. Comparing Fig. 2.7(a) and Fig. 2.7(b), it is observed that increasing L from 3 to 4 paths reduces the gap between the '*Asymptotically Optimal*' RA and the optimal RA considerably.

When $\Delta = 0$, the '*Equal Distribution*' scheme obviously coincides with the optimal allocation. This scheme eventually diverges from the optimal algorithm as Δ grows. However, it still outperforms the best path allocation method as long as Δ is not too large. For very large values of Δ, the best path dominates all the other ones, and we can ignore the rest of the paths. Hence, the best path allocation eventually converges to the optimal



(a) (b)

Figure 2.7: Optimal and suboptimal RA's are compared with equal distribution and best path allocation schemes for different values of Δ: (a) $L = 3$, (b) $L = 4$.

scheme when Δ increases.

2.5 Conclusion

In this chapter, we have studied the performance of *Forward Error Correction* over a block of packets sent through multiple independent paths. Adopting MDS codes, the probability of irrecoverable loss (P_E) is shown to decay exponentially with the number of paths. Furthermore, the *rate allocation* (RA) problem across independent paths is studied. It is shown that in the asymptotically optimal RA, each path is assigned a positive rate *iff* its *quality* is above a certain threshold. Finally, the RA problem is studied for any arbitrary number of paths. A heuristic suboptimal algorithm is proposed which computes a near-optimal allocation in polynomial time. For large values of L, the result of this algorithm is shown to converge to the optimal RA. Simulation results verify the validity of the theoretical analysis in several practical scenarios and also show the near-optimal performance of the proposed suboptimal algorithm.

2.6 Appendices

2.6.1 Probability Distribution of B_i

First, we compute the distribution of B_i for the 2-state Gilbert model. We denote the values of B_i with the parameter t to emphasize that they are expressed in the unit of time. Here, we focus on one path, for example path 1. Therefore, the index i can be temporarily dropped in analyzing the probability density function (pdf) of B_i.

We define the events g and b, respectively, as the channel being in the good or bad states at the start of a block. Then, the pdf of B can be written as

$$f_B(t) = f_{B|b}(t)\pi_b + f_{B|g}\pi_g. \tag{2.17}$$

Let $\mathcal{N}_s^T$ denote the number of consecutive states the channel experiences during the interval T. For instance, $\mathcal{N}_s^T = 3$ means that the channel switches its state twice in a block transmission time. Now, we define $f_{B|b}^m(t)$ as

$$f_{B|b}^m(t) = \lim_{\delta\to 0} \frac{\mathbb{P}\left\{t \le B < t+\delta \ \&\ \mathcal{N}_s^T = m|b\right\}}{\delta}. \tag{2.18}$$

$f_{B|g}^m(t)$ can be defined similarly.

For $m = 1$, due to the memoryless nature of the exponential distribution, we have

$$\begin{aligned} f_{B|b}^1(t) &= \delta(t-T)e^{-\mu_b T} \\ f_{B|g}^1(t) &= \delta(t)e^{-\mu_g T}. \end{aligned} \tag{2.19}$$

For odd values of $m > 1$, let τ_1 to τ_m denote the times the channel spends in different states. If the channel starts from the bad state, we have $\sum_{i=1}^{\frac{m+1}{2}} \tau_{2i-1} = t$ and $\sum_{i=1}^{\frac{m-1}{2}} \tau_{2i} = T - t$. Thus $f_{B|b}^m(t)$ can be written as

$$\begin{aligned} f_{B|b}^m(t) =& \int_{\mathcal{D}} \mu_b e^{-\mu_b\tau_1}\mu_g e^{-\mu_g\tau_2}\ldots\mu_g e^{-\mu_g\tau_{m-1}}e^{-\mu_b\tau_m}\prod_{i=1}^{m-2}\tau_i \\ =& \mu_b^{\frac{m-1}{2}}\mu_b^{\frac{m-1}{2}}e^{-\mu_b t}e^{-\mu_g(T-t)}\triangle_{\frac{m-1}{2}}(t)\triangle_{\frac{m-3}{2}}(T-t) \end{aligned} \tag{2.20}$$

where $\mathcal{D}$ and $\triangle_k(t)$ are defined as

$$\begin{aligned}\mathcal{D} &\triangleq \left\{ (\tau_1, \ldots, \tau_m) \,\middle|\, \forall i : \tau_i > 0, \sum_{i=1}^{\frac{m+1}{2}} \tau_{2i-1} = t, \right. \\ &\qquad \left. \sum_{i=1}^{\frac{m-1}{2}} \tau_{2i} = T - t \right\}, \\ \triangle_k(t) &\triangleq \int_{z_i>0} \ldots \int_{\sum_{i=1}^{k} z_i \leq t} dz_1 \ldots dz_k.\end{aligned}$$

It is easy to observe that $\triangle_k(t)$ is the volume of a k-dimensional simplex with the edge of length t. By mathematical induction on k, it can be shown that $\triangle_k(t) = \frac{t^k}{k!}$. Therefore, making similar arguments for the even values of m, we have

$$f^m_{B|b}(t) = \begin{cases} \mu_g \dfrac{(\mu_b t)^{\frac{m-1}{2}} \left(\mu_g (T-t)\right)^{\frac{m-3}{2}}}{\left(\frac{m-1}{2}\right)! \left(\frac{m-3}{2}\right)!} e^{-\mu_b t} e^{-\mu_g (T-t)} & \text{for } m \text{ odd} \\ \mu_b \dfrac{(\mu_b t \mu_g (T-t))^{\frac{m}{2}-1}}{\left(\frac{m}{2}-1\right)! \left(\frac{m}{2}-1\right)!} e^{-\mu_b t} e^{-\mu_g (T-t)} & \text{for } m \text{ even} \end{cases}$$

Based on similar arguments, $f^m_{B|g}(t)$ can be written as

$$f^m_{B|g}(t) = \begin{cases} \mu_b \dfrac{(\mu_b t)^{\frac{m-3}{2}} \left(\mu_g (T-t)\right)^{\frac{m-1}{2}}}{\left(\frac{m-3}{2}\right)! \left(\frac{m-1}{2}\right)!} e^{-\mu_b t} e^{-\mu_g (T-t)} & \text{for } m \text{ odd} \\ \mu_g \dfrac{(\mu_b t \mu_g (T-t))^{\frac{m}{2}-1}}{\left(\frac{m}{2}-1\right)! \left(\frac{m}{2}-1\right)!} e^{-\mu_b t} e^{-\mu_g (T-t)} & \text{for } m \text{ even} \end{cases}$$

Having $f^m_{B|b}(t)$ and $f^m_{B|g}(t)$ for all m, we can write

$$\begin{aligned} f_{B|b}(t) &= \sum_{m=1}^{\infty} f^m_{B|b}(t) \\ f_{B|g}(t) &= \sum_{m=1}^{\infty} f^m_{B|g}(t). \end{aligned} \tag{2.21}$$

Combining the above equations with (2.17), $f_B(t)$ can be computed. Noting the factorial

terms in the denominator of $f^m_{B|b}(t)$ and $f^m_{B|g}(t)$ and the fact that $\max\{t, T-t\} = T$ for $0 \leq t \leq T$, it can be verified that both $f^m_{B|b}(t)$ and $f^m_{B|g}(t)$ decrease very rapidly for $\frac{m-3}{2} > \max\{\mu_b T, \mu_g T\}$. Therefore, in the practical cases, we do not need to compute an infinite summation to get a close approximation of $f_B(t)$.

For the Extended Gilbert model, the pdf of B can be computed as follows. Here, equation (2.17) should be replaced with $f_B(t) = f_{B|g}(t)\pi_g + \sum_{i=1}^{M-1} f_{B|b_i}(t)\pi_{b_i}$. Moreover, for any specific sequence of state transitions $(\tau_1, \ldots, \tau_m)$ of length m, similar to the argument of equation (2.20), it can be shown that $f_{B|b_i}(\tau_1, \ldots, \tau_m)$ only depends on the summation of τ_i's which belong to the same state. Accordingly, similar to (2.21), $f_{B|b_i}(t)$ and $f_{B|g}(t)$ can be recomputed by summing over all lengths m and all state transition sequences of length m.

2.6.2 Proof of Lemma 2.1

1) We define the function $v(\lambda)$ as

$$v(\lambda) = \frac{\mathbb{E}\{xe^{\lambda x}\}}{\mathbb{E}\{e^{\lambda x}\}}. \tag{2.22}$$

Then, the first derivative of $v(\lambda)$ will be

$$\frac{\partial}{\partial \lambda} v(\lambda) \;=\; \frac{\mathbb{E}\{x^2 e^{\lambda x}\}\mathbb{E}\{e^{\lambda x}\} - [\mathbb{E}\{xe^{\lambda x}\}]^2}{[\mathbb{E}\{e^{\lambda x}\}]^2}. \tag{2.23}$$

According to Cauchy-Schwarz inequality, the following statement is always true for any two functions of $f()$ and $g()$

$$\left(\int_x f(x)g(x)dx\right)^2 < \int_x f^2(x)dx \int_x g^2(x)dx \tag{2.24}$$

unless $f(x) = Kg(x)$ for a constant K and all values of x. If we choose $f(x) = \sqrt{x^2 Q(x) e^{x\lambda}}$ and $g(x) = \sqrt{Q(x)e^{x\lambda}}$, they can not be proportional to each other for all values of x. Therefore, the numerator of equation (2.23) has to be strictly positive for all λ. Since the function $v(\lambda)$ is strictly increasing, it has an inverse $v^{-1}(\alpha)$ which is also strictly increasing. Moreover, the non-linear equation $v(\lambda) = \alpha$ has a unique solution of the form $\lambda = v^{-1}(\alpha) = l(\alpha)$.

2) To show that $l(\alpha = 0) = -\infty$, we prove an equivalent statement of the form $\lim_{\lambda \to -\infty} v(\lambda) = 0$. Since x is a random variable in the range $[0, 1]$ with the probability density function $Q(x)$, for any $0 < \epsilon < 1$, we can write

$$\begin{aligned}
\lim_{\lambda \to -\infty} v(\lambda) &= \lim_{\lambda \to -\infty} \frac{\int_0^\epsilon xQ(x)e^{x\lambda}dx + \int_\epsilon^1 xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \\
&\leq \lim_{\lambda \to -\infty} \frac{\int_0^\epsilon xQ(x)e^{x\lambda}dx}{\int_0^\epsilon Q(x)e^{x\lambda}dx} + \frac{\int_\epsilon^1 xQ(x)dx}{\int_0^\epsilon Q(x)e^{(x-\epsilon)\lambda}dx} \\
&\overset{(a)}{=} \lim_{\lambda \to -\infty} \frac{\int_0^\epsilon xQ(x)e^{x\lambda}dx}{\int_0^\epsilon Q(x)e^{x\lambda}dx} \\
&\overset{(b)}{=} \lim_{\lambda \to -\infty} \frac{x_1 Q(x_1)e^{\lambda x_1}}{Q(x_2)e^{\lambda x_2}}
\end{aligned} \tag{2.25}$$

for some $x_1, x_2 \in [0, \epsilon]$. (a) follows from the fact that for $x \in [0, \epsilon]$, $(x - \epsilon)\lambda \to +\infty$ when $\lambda \to -\infty$, and (b) is a result of the mean value theorem for integration [57]. This theorem states that for every continuous function $f(x)$ in the interval $[a, b]$, we have

$$\exists\ x_0 \in [a, b] \quad s.t. \quad \int_a^b f(x)dx = f(x_0)[b - a]. \tag{2.26}$$

Equation (2.25) is valid for any arbitrary $0 < \epsilon < 1$. If we choose $\epsilon \to 0$, x_1 and x_2 are both squeezed in the interval $[0, \epsilon]$. Thus, we have

$$\lim_{\lambda \to -\infty} v(\lambda) \leq \lim_{\lambda \to -\infty} \lim_{\epsilon \to 0} \frac{x_1 Q(x_1)e^{\lambda x_1}}{Q(x_2)e^{\lambda x_2}} = \lim_{\epsilon \to 0} x_1 = 0 \tag{2.27}$$

Based on the distribution of x, $v(\lambda)$ is obviously non-negative for any λ. Hence, the inequality in (2.27) can be replaced by equality.

3) By observing that $v(\lambda = 0) = \mathbb{E}\{x\}$, it is obvious that $l(\alpha = \mathbb{E}\{x\}) = 0$.

4) To show that $l(\alpha = 1) = +\infty$, we prove the equivalent statement of the form $\lim_{\lambda \to +\infty} v(\lambda) = 1$. For any $0 < \epsilon < 1$ and $x \in [1 - \epsilon, 1]$, $(x - 1 + \epsilon)\lambda \to +\infty$ when $\lambda \to +\infty$. Then,

defining $\zeta = 1 - \epsilon$, we have

$$\lim_{\lambda \to +\infty} \frac{\int_0^{\zeta} xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \leq \lim_{\lambda \to +\infty} \frac{\int_0^{\zeta} xQ(x)dx}{\int_{\zeta}^1 Q(x)e^{(x-\zeta)\lambda}dx} = 0. \tag{2.28}$$

Since the fraction in (2.28) is obviously non-negative for all λ, this inequality can be replaced by an equality. Similarly, we have

$$\lim_{\lambda \to +\infty} \frac{\int_0^{\zeta} Q(x)e^{x\lambda}dx}{\int_{\zeta}^1 xQ(x)e^{x\lambda}dx} \leq \lim_{\lambda \to +\infty} \frac{\int_0^{\zeta} Q(x)dx}{\int_{\zeta}^1 xQ(x)e^{(x-\zeta)\lambda}dx} = 0. \tag{2.29}$$

which can also be replaced by equality. Now, the limit of $v(\lambda)$ is written as

$$\begin{aligned}
\lim_{\lambda \to +\infty} v(\lambda) &= \lim_{\lambda \to +\infty} \frac{\int_0^{\zeta} xQ(x)e^{x\lambda}dx + \int_{\zeta}^1 xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \\
&\overset{(a)}{=} \lim_{\lambda \to +\infty} \frac{\int_{\zeta}^1 xQ(x)e^{x\lambda}dx}{\int_0^1 Q(x)e^{x\lambda}dx} \\
&\overset{(b)}{=} \left(\lim_{\lambda \to +\infty} \frac{\int_0^{\zeta} Q(x)e^{x\lambda}dx + \int_{\zeta}^1 Q(x)e^{x\lambda}dx}{\int_{\zeta}^1 xQ(x)e^{x\lambda}dx} \right)^{-1} \\
&\overset{(c)}{=} \left(\lim_{\lambda \to +\infty} \frac{\int_{\zeta}^1 Q(x)e^{x\lambda}dx}{\int_{\zeta}^1 xQ(x)e^{x\lambda}dx} \right)^{-1} \\
&\overset{(d)}{=} \left(\lim_{\lambda \to +\infty} \frac{Q(x_1)e^{x_1\lambda}}{x_2 Q(x_2)e^{x_2\lambda}} \right)^{-1}
\end{aligned} \tag{2.30}$$

for some $x_1, x_2 \in [1-\epsilon, 1]$. (a) follows from equation (2.28), and (b) is valid since the final result shows that $\lim_{\lambda \to +\infty} v(\lambda)$ is finite and non-zero [57]. (c) follows from equation (2.29), and (d) is a result of the mean value theorem for integration. If we choose $\epsilon \to 0$, x_1 and x_2 are both squeezed in the interval $[1-\epsilon, 1]$. Then, equation (2.30) turns into

$$\lim_{\lambda \to +\infty} v(\lambda) = \left(\lim_{\lambda \to +\infty} \lim_{\epsilon \to 0} \frac{Q(x_1)e^{x_1\lambda}}{x_2 Q(x_2)e^{x_2\lambda}} \right)^{-1} = \left(\lim_{\epsilon \to 0} \frac{1}{x_2} \right)^{-1} = 1.$$

5) According to equations (2.4) and (2.5), the first derivative of $u(\alpha)$ is

$$\frac{\partial u(\alpha)}{\partial \alpha} = l(\alpha) + \alpha \frac{\partial l(\alpha)}{\partial \alpha} - \frac{\mathbb{E}\{xe^{\lambda x}\}}{\mathbb{E}\{e^{\lambda x}\}} \frac{\partial l(\alpha)}{\partial \alpha} = l(\alpha).$$

2.6.3 Proof of Lemma 2.2

Based on the definition of probability density function, we have

$$\begin{aligned}
& \lim_{L\to\infty} -\frac{1}{L}\log\left(f_y(\alpha)\right) \\
= & \lim_{L\to\infty} -\frac{1}{L}\log\left(\lim_{\delta\to\ 0}\frac{\mathbb{P}\{y>\alpha\}-\mathbb{P}\{y>\alpha+\delta\}}{\delta}\right) \\
\overset{(a)}{=} & \lim_{\delta\to\ 0}\lim_{L\to\infty} -\frac{1}{L}\log\left(\frac{\mathbb{P}\{y>\alpha\}-\mathbb{P}\{y>\alpha+\delta\}}{\delta}\right) \\
\geq & \lim_{\delta\to\ 0}\lim_{L\to\infty} \frac{1}{L}\left(-\log\left(\mathbb{P}\{y>\alpha\}\right)+\log\delta\right) \\
\overset{(b)}{=} & u(\alpha)
\end{aligned} \tag{2.31}$$

where (a) is valid since log is a continuous function, and both limitations do exist and are interchangeable. (b) follows from equation (2.6). The exponent of $f_y(\alpha)$ can be upper-bounded as

$$\begin{aligned}
& \lim_{L\to\infty} -\frac{1}{L}\log\left(f_y(\alpha)\right) \\
\overset{(a)}{=} & \lim_{\delta\to\ 0}\lim_{L\to\infty} \frac{-\log\left(\mathbb{P}\{y>\alpha\}-\mathbb{P}\{y>\alpha+\delta\}\right)+\log\delta}{L} \\
\overset{(b)}{\leq} & \lim_{\delta\to\ 0}\lim_{L\to\infty} \frac{-\log\left(e^{-L(u(\alpha)+\epsilon)}-e^{-L(u(\alpha+\delta)-\epsilon)}\right)+\log\delta}{L} \\
= & \lim_{\delta\to\ 0}\lim_{L\to\infty} u(\alpha)+\epsilon-\frac{\log\left(1-e^{-L\chi}\right)}{L} \\
\overset{(c)}{=} & u(\alpha)+\epsilon
\end{aligned} \tag{2.32}$$

where $\chi = u(\alpha+\delta)-u(\alpha)-2\epsilon$. Since $u(\alpha)$ is a strictly increasing function (Lemma 2.1), we can make χ positive by choosing ϵ small enough. (a) is valid since log is a continuous function, and both limits do exist and are interchangeable. (b) follows from the definition of limit if L is sufficiently large, and (c) is a result of χ being positive. Selecting ϵ arbitrarily

small, results (2.31) and (2.32) prove the lemma.

2.6.4 Proof of Lemma 2.3

According to the definition of infimum, we have

$$\begin{aligned} & \lim_{L\to\infty} -\frac{\log(H(L))}{L} \\ \geq & \lim_{L\to\infty} -\frac{1}{L}\log\left(e^{-L\inf\limits_{\mathcal{S}} h(\mathbf{x})}\int_{\mathcal{S}} d\mathbf{x}\right) \\ \overset{(a)}{=} & \inf_{\mathcal{S}} h(\mathbf{x}). \end{aligned} \tag{2.33}$$

where (a) follows from the fact that $\mathcal{S}$ is a bounded region. Since $h(\mathbf{x})$ is a continuous function, it has a minimum in the bounded closed set $cl(\mathcal{S})$ which is denoted by $\mathbf{x}^\star$. Due to the continuity of $h(\mathbf{x})$ at $\mathbf{x}^\star$, for any $\epsilon > 0$, there is a neighborhood $\mathcal{B}(\epsilon)$ centered at $\mathbf{x}^\star$ such that any $\mathbf{x} \in \mathcal{B}(\epsilon)$ has the property of $|h(\mathbf{x}) - h(\mathbf{x}^\star)| < \epsilon$. Moreover, since $\mathcal{S}$ is a convex set, we have $\text{vol}\left(\mathcal{B}(\epsilon) \cap \mathcal{S}\right) > 0$. Now, we can write

$$\begin{aligned} & \lim_{L\to\infty} -\frac{\log(H(L))}{L} \\ \leq & \lim_{L\to\infty} -\frac{1}{L}\log\left(\int_{\mathcal{S}\cap\mathcal{B}(\epsilon)} e^{-Lh(\mathbf{x})} d\mathbf{x}\right) \\ \leq & \lim_{L\to\infty} -\frac{1}{L}\log\left(e^{-L(h(\mathbf{x}^\star)+\epsilon)}\int_{\mathcal{S}\cap\mathcal{B}(\epsilon)} d\mathbf{x}\right) \\ = & h(\mathbf{x}^\star) + \epsilon. \end{aligned} \tag{2.34}$$

Selecting ϵ to be arbitrarily small, (2.33) and (2.34) prove the lemma.

2.6.5 Proof of Lemma 2.4

According to Lemma 2.1, $u_j(x)$ is increasing and convex for $\forall 1 \leq j \leq J$. Thus, the objective function $f(\boldsymbol{\beta}) = \sum_{j=1}^{J} \gamma_j u_j(\frac{\beta_j}{\eta_j})$ is also convex, and the region $\mathcal{S}_T$ is determined by J convex inequality constraints and one affine equality constraint. Hence, in this case, KKT conditions are both necessary and sufficient for optimality [122]. In other words, if

there exist constants ϕ_j and ν such that

$$\frac{\gamma_j}{\eta_j} l_j(\frac{\beta_j^\star}{\eta_j}) - \phi_j - \nu = 0 \quad \forall 1 \leq j \leq J \tag{2.35}$$

$$\phi_j \left[\eta \mathbb{E}\{x_j\} - \beta_j^\star\right] = 0 \quad \forall 1 \leq j \leq J \tag{2.36}$$

then the point $\boldsymbol{\beta}^\star$ is a global minimum.

Now, we prove that either $\beta_j^\star = \eta_j \mathbb{E}\{x_j\}$ for all $1 \leq j \leq J$, or $\beta_j^\star > \eta_j \mathbb{E}\{x_j\}$ for all $1 \leq j \leq J$. Let us assume the opposite is true, and there are at least two elements of the vector $\boldsymbol{\beta}^\star$, indexed with k and m, which have the values of $\beta_k^\star = \eta_k \mathbb{E}\{x_k\}$ and $\beta_m^\star > \eta_m \mathbb{E}\{x_m\}$, respectively. For any arbitrary $\epsilon > 0$, the vector $\boldsymbol{\beta}^{\star\star}$ can be defined as below

$$\beta_j^{\star\star} = \begin{cases} \beta_j^\star + \epsilon & \text{if } j = k \\ \beta_j^\star - \epsilon & \text{if } j = m \\ \beta_j^\star & \text{otherwise.} \end{cases} \tag{2.37}$$

Then, we have

$$\begin{aligned} & \lim_{\epsilon \to 0} \frac{f(\boldsymbol{\beta}^{\star\star}) - f(\boldsymbol{\beta}^\star)}{\epsilon} \\ = & \lim_{\epsilon \to 0} \frac{1}{\epsilon} \left\{ \gamma_k u_k \left(\frac{\beta_k^\star + \epsilon}{\eta_k} \right) + \gamma_m u_m \left(\frac{\beta_m^\star - \epsilon}{\eta_m} \right) \right. \\ & \qquad \left. - \gamma_m u_m \left(\frac{\beta_m^\star}{\eta_k} \right) \right\} \\ \overset{(a)}{=} & \lim_{\epsilon \to 0} \frac{\gamma_k}{\eta_k} l_k \left(\frac{\beta_k^\star + \epsilon'}{\eta_k} \right) - \frac{\gamma_m}{\eta_m} l_m \left(\frac{\beta_m^\star + \epsilon''}{\eta_m} \right) \\ = & -\frac{\gamma_m}{\eta_m} l_m \left(\frac{\beta_m^\star}{\eta_m} \right) < 0 \end{aligned} \tag{2.38}$$

where $\epsilon', \epsilon'' \in [0, \epsilon]$, and (a) follows from the Taylor's theorem. Thus, moving from $\boldsymbol{\beta}^\star$ to $\boldsymbol{\beta}^{\star\star}$ decreases the function which contradicts the assumption of $\boldsymbol{\beta}^\star$ being the global minimum.

Out of the remaining possibilities, the case where $\beta_j^\star = \eta_j \mathbb{E}\{x_j\}$ $(\forall 1 \leq j \leq J)$ obviously agrees with Lemma 2.4 for the special case of $\nu = 0$. Therefore, the lemma can be proved assuming $\beta_j^\star > \eta_j \mathbb{E}\{x_j\}$ $(\forall 1 \leq j \leq J)$. Then, equation (2.36) turns into $\phi_j = 0$ $(\forall 1 \leq j \leq J)$. By rearranging equation (2.35) and using the condition $\sum_{j=1}^{J} \beta_j = \alpha$,

Lemma 2.4 is proved.

2.6.6 Proof of Theorem 2.1

Sketch of the proof: First, it is proved that $\eta_j^\star > 0$ if $\mathbb{E}\{x_j\} < \alpha$. At the second step, we prove that $\eta_j^\star = 0$, if $\mathbb{E}\{x_j\} \geq \alpha$. Then, KKT conditions [122] are applied for the indices $1 \leq k \leq J$ where $\mathbb{E}\{x_k\} < \alpha$ to find the maximizing allocation vector, $\boldsymbol{\eta}^\star$.

Proof: The parameter ν is obviously a function of the vector $\boldsymbol{\eta}$. Differentiating equation (2.9) with respect to η_k results in

$$\frac{\partial \nu}{\partial \eta_k} = -\frac{v_k\left(\frac{\nu\eta_k}{\gamma_k}\right) + \frac{\nu\eta_k}{\gamma_k} v_k'\left(\frac{\nu\eta_k}{\gamma_k}\right)}{\sum_{j=1}^{J} \frac{\eta_j^2}{\gamma_j} v_j'\left(\frac{\nu\eta_j}{\gamma_j}\right)} \tag{2.39}$$

where $v_j(x) = l_j^{-1}(x)$, and $v_j'(x)$ denotes its derivative with respect to its argument. The objective function can be simplified as

$$g(\boldsymbol{\eta}) \triangleq \sum_{j=1}^{J} \gamma_j u_j(\frac{\beta_j^\star}{\eta_j}) = \sum_{j=1}^{J} \gamma_j u_j\left(v_j(\frac{\nu\eta_j}{\gamma_j})\right). \tag{2.40}$$

$\nu^\star$ is defined as the value of ν corresponding to $\boldsymbol{\eta}^\star$. Next, we show that $\nu^\star > 0$. Let us assume the opposite is true, i.e., $\nu^\star \leq 0$. Then, according to Lemma 2.1, we have $v_j(\frac{\nu^\star\eta_j}{\gamma_j}) \leq \mathbb{E}\{x_j\}$ for all j which results in $g(\boldsymbol{\eta}^\star) = 0$. However, it is possible to achieve a positive value of $g(\boldsymbol{\eta})$ by setting $\eta_j = 1$ for the one vector which has the property of $\mathbb{E}\{x_j\} < \alpha$, and setting $\eta_j = 0$ for the rest. Thus, $\boldsymbol{\eta}^\star$ can not be the maximal point. This contradiction proves the fact that $\nu^\star > 0$.

At the first step, we prove that $\eta_j^\star > 0$ if $\mathbb{E}\{x_j\} < \alpha$. Assume the opposite is true for an index $1 \leq k \leq J$. Since $\sum_{j=1}^{J} \eta_j^\star = 1$, there should be at least one index m such that $\eta_m^\star > 0$. For any arbitrary $\epsilon > 0$, the vector $\boldsymbol{\eta}^{\star\star}$ can be defined as below

$$\eta_j^{\star\star} = \begin{cases} \epsilon & \text{if } j = k \\ \eta_j^\star - \epsilon & \text{if } j = m \\ \eta_j^\star & \text{otherwise.} \end{cases} \tag{2.41}$$

$\nu^{\star\star}$ is defined as the corresponding value of ν for the vector $\boldsymbol{\eta}^{\star\star}$. Based on equation (2.39), we can write

$$\begin{aligned}
&\Delta\nu = \\
&\nu^{\star\star} - \nu^{\star} = \\
&\frac{v_m\left(\frac{\nu^{\star}\eta_m^{\star}}{\gamma_m}\right) + \frac{\nu^{\star}\eta_m^{\star}}{\gamma_m} v_m'\left(\frac{\nu^{\star}\eta_m^{\star}}{\gamma_m}\right) - \mathbb{E}\{x_k\}}{\sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^{\star}\eta_j^{\star}}{\gamma_j}\right)}\epsilon + O(\epsilon^2).
\end{aligned} \tag{2.42}$$

Then, we have

$$\begin{aligned}
&\lim_{\epsilon\to 0} \frac{g(\boldsymbol{\eta}^{\star\star}) - g(\boldsymbol{\eta}^{\star})}{\epsilon} \\
&= \lim_{\epsilon\to 0} \frac{1}{\epsilon}\left\{ \frac{\nu^{\star 2}\eta_k^{\star}}{\gamma_k} v_k'\left(\frac{\nu^{\star}\eta_k^{\star}}{\gamma_k}\right)\epsilon - \frac{\nu^{\star 2}\eta_m^{\star}}{\gamma_m} v_m'\left(\frac{\nu^{\star}\eta_m^{\star}}{\gamma_m}\right)\epsilon \right. \\
&\qquad \left. + \nu^{\star}\Delta\nu \sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^{\star}\eta_j^{\star}}{\gamma_j}\right) + O(\epsilon^2) \right\} \\
&\overset{(a)}{=} \nu^{\star}\left\{ v_m\left(\frac{\nu^{\star}\eta_m^{\star}}{\gamma_m}\right) - \mathbb{E}\{x_k\} \right\}
\end{aligned} \tag{2.43}$$

where (a) follows from (2.42). If the value of (2.43) is positive for an index m, moving in that direction increases the objective function which contradicts with the assumption of $\boldsymbol{\eta}^{\star}$ being a maximal point. If the value of (2.43) is non-positive for all indices m whose $\eta_m^{\star} > 0$, we can write

$$\mathbb{E}\{x_k\} \geq \sum_{m=1}^{J} \eta_m^{\star} v_m\left(\frac{\nu^{\star}\eta_m^{\star}}{\gamma_m}\right) = \alpha \tag{2.44}$$

which obviously contradicts the assumption of $\mathbb{E}\{x_k\} < \alpha$.

At the second step, we prove that $\eta_j^{\star} = 0$ if $\mathbb{E}\{x_j\} \geq \alpha$. Assume the opposite is true for an index $1 \leq r \leq J$. Since $\sum_{j=1}^{J} \eta_j^{\star} = 1$, we should have $\eta_s^{\star} < 1$ for all other indices s.

For any arbitrary $\epsilon > 0$, the vector $\boldsymbol{\eta}^{\star\star\star}$ can be defined as

$$\eta_j^{\star\star\star} = \begin{cases} \eta_j^\star - \epsilon & \text{if } j = r \\ \eta_j^\star + \epsilon & \text{if } j = s \\ \eta_j^\star & \text{otherwise.} \end{cases} \tag{2.45}$$

$\nu^{\star\star\star}$ is defined as the corresponding value of ν for the vector $\boldsymbol{\eta}^{\star\star\star}$. Based on equation (2.39), we can write

$$\begin{aligned} \Delta\nu =& \nu^{\star\star\star} - \nu^\star \\ =& \frac{\epsilon}{\sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^\star \eta_j^\star}{\gamma_j}\right)} \left\{ v_r\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) + \frac{\nu^\star \eta_r^\star}{\gamma_r} v_r'\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) \right. \\ & \left. - v_s\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right) - \frac{\nu^\star \eta_s^\star}{\gamma_s} v_s'\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right) \right\} + O(\epsilon^2). \end{aligned} \tag{2.46}$$

Then, we have

$$\begin{aligned} & \lim_{\epsilon \to 0} \frac{g(\boldsymbol{\eta}^{\star\star\star}) - g(\boldsymbol{\eta}^\star)}{\epsilon} \\ =& \lim_{\epsilon \to 0} \frac{1}{\epsilon} \left\{ \frac{\nu^{\star 2} \eta_s^\star}{\gamma_s} v_s'\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right) \epsilon - \frac{\nu^{\star 2} \eta_r^\star}{\gamma_r} v_r'\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) \epsilon \right. \\ & \left. + \nu^\star \Delta\nu \sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^\star \eta_j^\star}{\gamma_j}\right) + O(\epsilon^2) \right\} \\ \overset{(a)}{=}& \nu^\star \left\{ v_r\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) - v_s\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right) \right\} \end{aligned} \tag{2.47}$$

where (a) follows from (2.46). If the value of (2.47) is positive for an index s, moving in that direction increases the objective function which contradicts with the assumption of $\boldsymbol{\eta}^\star$ being a maximal point . If the value of (2.47) is non-positive for all indices s whose $\eta_s^\star > 0$, we can write

$$\mathbb{E}\{x_r\} < v_r\left(\frac{\nu^\star \eta_r^\star}{\gamma_r}\right) \leq \sum_{s=1}^{J} \eta_s^\star v_s\left(\frac{\nu^\star \eta_s^\star}{\gamma_s}\right) = \alpha \tag{2.48}$$

which obviously contradicts the assumption of $\mathbb{E}\{x_r\} \geq \alpha$.

Now that the boundary points are checked, we can safely use the KKT conditions [122] for all $1 \leq k \leq J$, where $\mathbb{E}\{x_k\} < \alpha$, to find the maximizing allocation vector, $\boldsymbol{\eta}^\star$.

$$\begin{aligned}\zeta &= \frac{\nu^{\star 2}\eta_k^\star}{\gamma_k} v_k'\left(\frac{\nu^\star \eta_k^\star}{\gamma_k}\right) + \nu^\star \sum_{j=1}^{J} \frac{\eta_j^{\star 2}}{\gamma_j} v_j'\left(\frac{\nu^\star \eta_j^{\star 2}}{\gamma_j}\right) \frac{\partial \nu}{\partial \eta_k}|_{\nu=\nu^\star} \\ &\overset{(a)}{=} -\nu^\star v_k\left(\frac{\nu^\star \eta_k^\star}{\gamma_k}\right) \end{aligned} \tag{2.49}$$

where ζ is a constant independent of k, and (a) follows from (2.39). Using the fact that $\sum_{j=1}^{J} \eta_j = 1$ together with equations (2.9) and (2.49) results in

$$\begin{aligned}\zeta &= -\alpha\nu^\star \\ \nu^\star &= \sum_{\mathbb{E}\{x_j\}<\alpha} \gamma_j l_j(\alpha). \end{aligned} \tag{2.50}$$

Combining equations (2.49) and (2.50) results in equation (2.11) and $g(\boldsymbol{\eta}^\star) = \sum_{j=1}^{J} \gamma_j u_j(\alpha)$.

2.6.7 Proof of Remark 2.4

Based on the arguments similar to the ones in appendix 2.6.6, it can be shown that $\tilde{\eta}_j^\star = 0$ *iff* $\mathbb{E}\{x_j\} \geq \alpha$. Since all the types are identical here, this means $\tilde{\eta}_j^\star > 0$ for all j. Similar to equation (2.49), applying KKT conditions [122], gives us

$$v_j\left(\frac{\tilde{\nu}^\star \tilde{\eta}_j^\star}{\gamma_j}\right) = \begin{cases} -\zeta & \text{if } \tilde{\eta}_j^\star < \dfrac{\gamma_j W_j T}{n_0} \\ -\zeta - \sigma_j & \text{if } \tilde{\eta}_j^\star = \dfrac{\gamma_j W_j T}{n_0} \end{cases} \tag{2.51}$$

where σ_j's are non-negative parameters [122]. Putting $\Upsilon = \frac{l_j(-\zeta)}{\tilde{\nu}^\star}$ proves equation (2.13).

2.6.8 Discrete Analysis of One Path

$Q(n, k, l)$ is defined as the probability of having exactly k errors out of the n packets sent over the path l. To compute $Q(n, k, l)$ for any general M-state Markov model, the following parameters are required: 1) a $M \times M$ matrix $\mathbf{\Pi}$ with the elements $\pi_{s'|s}$ which represents

the channel transition behavior. $\pi_{s'|s}$ is the probability of the channel being in the state s' provided that it has been in the state s when the last packet was transmitted; 2) a vector $\mathbf{q} = (q_1, \ldots, q_M)$ where q_s denotes the probability of having erasure conditioned on being in the state s.

For $\forall\ s \in \{1, \ldots, M\}$, π_s is defined as the steady state probability of being in the state s. Obviously, the steady state probability vector $\boldsymbol{\pi} = (\pi_1, \ldots, \pi_M)$ can be computed using the equation set $\boldsymbol{\pi} = \boldsymbol{\Pi}\boldsymbol{\pi}$ and $\sum_{s=1}^{M} \pi_s = 1$.

Depending on the initial state of the path l, $P_s(n, k, l)$ is defined as the probability of having k errors out of the n packets sent over this path when we start the transmission in the state s. It is easy to see that

$$Q(n, k, l) = \sum_{s=1}^{M} \pi_s P_s(n, k, l). \tag{2.52}$$

$P_s(n, k, l)$ can be computed from the following recursive equation

$$\begin{aligned} P_s(n, k, l) \;\; = \;\; & \sum_{s'=1}^{M} q_s \pi_{s'|s} P_{s'}(n-1, k-1, l) + \\ & \sum_{s'=1}^{M} (1 - q_s)\, \pi_{s'|s} P_{s'}(n-1, k, l) \end{aligned} \tag{2.53}$$

with the initial conditions

$$\begin{aligned} &P_s(n, k, l) = 0 \qquad \text{for } k > n \\ &P_s(n, k, l) = 0 \qquad \text{for } k < 0 \\ &P_s(n, k, l) = 1 \qquad \text{for } k = n = 0. \end{aligned} \tag{2.54}$$

According to the recursive equations in (2.53), to compute $P_s(n, k, l)$ by memoization technique, the functions $P_s()$ should be calculated at the following set of points denoted as $\mathcal{S}(n, k)$

$$\mathcal{S}(n, k) = \left\{(n', k') \mid 0 \le k' \le k,\ n' - n + k \le k' \le n'\right\}.$$

Cardinality of the set $\mathcal{S}(n, k)$ is of the order $|\mathcal{S}(n, k)| = O\left(k\,(n - k)\right)$. Since $O(M)$ operations are needed to compute the recursive functions $P_s()$ at each point and M functions

$P_s(n,k,l)$ $(s=1,\ldots,M)$ have to be computed, $P_s(n,k,l)$ is computable with the complexity of $O\left(M^2k\left(n-k\right)\right)$ which give us $Q(n,k,l)$ according to equation (2.52). It is worth mentioning that if the M-state extended Gilbert model is adopted, the computational complexity of obtaining $Q(n,k,l)$ would be reduced to $O\left(Mk\left(n-k\right)\right)$.

2.6.9 Discrete Analysis of One Type

When there are n packets to be distributed over L_j identical paths of type j, uniform distribution is obviously the optimum. However, since the integer n may be indivisible by L_j, the L_j dimensional vector $\mathbf{N}$ is selected as

$$N_l = \begin{cases} \lfloor \frac{n}{L_j} \rfloor + 1 & \text{for } 1 \le l \le \text{Rem}(n, L_j) \\ \\ \lfloor \frac{n}{L_j} \rfloor & \text{for } \text{Rem}(n, L_j) < l \le L_j \end{cases} \tag{2.55}$$

where $\text{Rem}(a,b)$ denotes the remainder of dividing a by b. $\mathbf{N}$ represents the closest integer vector to a uniform distribution.

$E^{\mathbf{N}}(k,l)$ is defined as the probability of having exactly k erasures among the n packets transmitted over the identical paths 1 to l with the allocation vector $\mathbf{N}$. According to the definitions of $Q_j(n,k)$ and $E^{\mathbf{N}}(k,l)$, it is obvious that $Q_j(n,k) = E^{\mathbf{N}}(k,L_j)$. $E^{\mathbf{N}}(k,l)$ can be computed recursively as

$$\begin{aligned} E^{\mathbf{N}}(k,l) &= \sum_{i=0}^{k} E^{\mathbf{N}}(k-i,l-1)Q(N_l,i,l) \\ E^{\mathbf{N}}(k,1) &= Q(N_1,k,1) \end{aligned} \tag{2.56}$$

where $Q(N_l,i,l)$ is given in appendix 2.6.8. Since all the paths are assumed to be identical here, $Q(N_l,k,l)$ is the same for all path indices, l. According to the recursive equations in (2.53), the values of $Q(N_l,i,l)$ for all $0 \le i \le k$ and $1 \le l \le L_j$ can be calculated with the complexity of $O(M^2N_lk) = O\left(M^2\frac{n}{L_j}k\right)$. According to the recursive equations in (2.56), computing $E^{\mathbf{N}}(k,l)$ requires memoization over an array of size $O(kl)$ whose entries can be calculated with $O(k)$ operations each. Thus, $E^{\mathbf{N}}(k,l)$ is computable with the complexity of $O(k^2l)$ if $Q(N_l,i,l)$'s are already given. Finally, noting that $Q_j(n,k) = E^{\mathbf{N}}(k,L_j)$, we

can compute $Q_j(n,k)$ with the overall complexity of $O(k^2 L_j) + O\left(M^2 \frac{n}{L_j} k\right)$.

2.6.10 Proof of Lemma 2.5

The lemma is proved by induction on j. The case of $j = 1$ is obviously true as $\hat{P}_e(n,k,1) = P_e^{opt}(n,k,1)$. Let us assume this statement is true for $j = 1$ to $J-1$. Then, for $j = J$, we have

$$\begin{aligned}
& \hat{P}_e(n,k,J) \\
\overset{(a)}{\leq} & \sum_{i=0}^{N_J} Q_J(N_J^{opt}, i) \hat{P}_e(n - N_J^{opt}, k-i, J-1) \\
\overset{(b)}{\leq} & \sum_{i=0}^{N_J} Q_J(N_J^{opt}, i) P_e^{opt}(n - N_J^{opt}, k-i, J-1) \\
\overset{(c)}{\leq} & \sum_{i=0}^{N_J} Q_J(N_J^{opt}, i) P_e^{\mathbf{N}^{opt}}(k-i, J-1) \\
\overset{(d)}{=} & P_e^{\mathbf{N}^{opt}}(k, J) = P_e^{opt}(n,k,J)
\end{aligned}$$

where $\mathbf{N}^{opt}$ denotes the optimum allocation of n packets among the J types of paths such that the probability of having more than k lost packets is minimized. (a) follows from the recursive equation (2.14), and (b) is the induction assumption. (c) comes from the definition of $P_e^{opt}(n,k,l)$, and (d) is a result of equation (2.16).

2.6.11 Proof of Theorem 2.2

Sketch of the proof: First, the asymptotic behavior of $Q_j(n,k)$ is analyzed, and it is shown that for large values of L_j (or equivalently L), equation (2.60) computes the exponent of $Q_j(n,k)$ versus L. Next, we prove the first part of the theorem by induction on J. The proof of this part is divided to two different cases, depending on whether $\frac{K}{N}$ is larger than $\mathbb{E}\{x_J\}$ or vice versa. Finally, the second and the third parts of the theorem are proved by induction on j while the total number of path types, J, is fixed. Again, the proof is divided into two different cases, depending on whether $\frac{K}{N}$ is larger than $\mathbb{E}\{x_j\}$ or vice versa.

Proof: First, we compute the asymptotic behavior of $Q_j(n,k)$ for $k > n\mathbb{E}\{x_j\}$, and n

growing proportionally to L_j, i.e. $n = n'L_j$. Here, we can apply Sanov's Theorem [113,123] as n and k are discrete variables and n' is a constant.

Sanov's Theorem. *Let $X_1, X_2, \ldots, X_n$ be i.i.d. discrete random variables from an alphabet set $\mathcal{X}$ with the size $|\mathcal{X}|$ and probability mass function (pmf) $Q(x)$. Let $\mathcal{P}$ denote the set of pmf's in $\mathbb{R}^{|\mathcal{X}|}$, i.e. $\mathcal{P} = \left\{\mathbf{P} \in \mathbb{R}^{|\mathcal{X}|} |\ P(i) \geq 0,\ \sum_{i=1}^{|\mathcal{X}|} P(i) = 1\right\}$. Also, let $\mathcal{P}_L$ denote the subset of $\mathcal{P}$ corresponding to all possible empirical distributions of $\mathcal{X}$ in L observations [123], i.e. $\mathcal{P}_L = \{\mathbf{P} \in \mathcal{P} |\ \forall i,\ LP(i) \in \mathbb{Z}\}$. For any dense and closed set [119] of pmf's $E \subseteq \mathcal{P}$, the probability that the empirical distribution of L observations belongs to the set E is equal to*

$$\mathbb{P}\{E\} = \mathbb{P}\{E \cap \mathcal{P}_L\} \doteq e^{-LD(\mathbf{P}^\star||\mathbf{Q})} \tag{2.57}$$

where $\mathbf{P}^\star = \underset{\mathbf{P}\in E}{\operatorname{argmin}}\, D(\mathbf{P}||\mathbf{Q})$ and $D(\mathbf{P}||\mathbf{Q}) = \sum_{i=1}^{|\mathcal{X}|} P(i) \log \frac{P(i)}{Q(i)}$.

Focusing our attention on the main problem, assume that $\mathbf{P}$ is defined as the empirical distribution of the number of errors in each path, i.e. for $\forall i,\ 1 \leq i \leq n',\ P(i)$ shows the ratio of the total paths which contain exactly i lost packets. Similarly, for $\forall i,\ 1 \leq i \leq n',\ Q(i)$ denotes the probability of exactly i packets being lost out of the n' packets transmitted on a path of type j. The sets E and E_{out} are defined as follows

$$\begin{aligned} E &= \{\mathbf{P} \in \mathcal{P} | \sum_{i=0}^{n'} iP(i) \geq \beta\} \\ E_{out} &= \{\mathbf{P} \in \mathcal{P} | \sum_{i=0}^{n'} iP(i) = \beta\} \end{aligned} \tag{2.58}$$

where $\beta = \dfrac{k}{n}$. Noting E and E_{out} are dense sets, we can compute $Q_j(n,k)$ as

$$Q_j(n,k) \overset{(a)}{=} \mathbb{P}\{E_{out}\} \overset{(b)}{\doteq} e^{-L_j \min\limits_{\mathbf{P}\in E_{out}} D(\mathbf{P}||\mathbf{Q})} \tag{2.59}$$

where (a) follows from the definition of $Q_j(n,k)$ as the probability of having exactly k errors out of the n packets sent over the paths of type j given in section 2.4, and (b) results from Sanov's Theorem.

Knowing the fact that the Kullback Leibler distance, $D(\mathbf{P}||\mathbf{Q})$, is a convex function of $\mathbf{P}$ and $\mathbf{Q}$ [124], we conclude that its minimum over the convex set E either lies on an

interior point which is a global minimum of the function over the whole set $\mathcal{P}$ or is located on the boundary of E. However, we know that the global minimum of Kullback Leibler distance occurs at $\mathbf{P} = \mathbf{Q} \notin E$. Thus, the minimum of $D(\mathbf{P}||\mathbf{Q})$ is located on the boundary of E. This results in

$$\begin{aligned} Q_j(n,k) &\overset{(a)}{\doteq} e^{-L_j \min\limits_{\mathbf{P}\in E_{out}} D(\mathbf{P}||\mathbf{Q})} \\ &= e^{-L_j \min\limits_{\mathbf{P}\in E} D(\mathbf{P}||\mathbf{Q})} \overset{(b)}{\doteq} e^{-\gamma_j L u_j(\frac{k}{n})} \end{aligned} \tag{2.60}$$

where (a) and (b) follow from equations (2.59) and (2.6), respectively.

2.6.11.1 First Part of Theorem

We prove the first part of the theorem by induction on J. When $J = 1$, the statement is correct for both cases of $\frac{K}{N} > \mathbb{E}\{x_1\}$ and $\frac{K}{N} \leq \mathbb{E}\{x_1\}$, recalling the fact that $\hat{P}_e(n,k,1) = P_e^{opt}(n,k,1)$ and $u_1(x) = 0$ for $x \leq \mathbb{E}\{x_1\}$. Now, let us assume the first part of the theorem is true for $j = 1$ to $J-1$. We prove the same statement for J as well. The proof can be divided into two different cases, depending on whether $\frac{K}{N}$ is larger than $\mathbb{E}\{x_J\}$ or vice versa.

Case 1: $\dfrac{K}{N} > \mathbb{E}\{x_J\}$

According to the definition, the value of $\hat{P}_e(N,K,J)$ is computed by minimizing $\sum_{i=0}^{n_J} Q_J(n_J,i)\hat{P}_e(N-n_J, K-i, J-1)$ over n_J (see equation (2.16)). Now, we show that for any value of n_J, the corresponding term in the minimization is asymptotically at least equal to $P_e^{opt}(N,K,J)$. n_J can take integer values in the range $0 \leq n_J \leq N$. We split this range into three non-overlapping intervals of $0 \leq n_J \leq \epsilon L$, $\epsilon L \leq n_J \leq N(1-\epsilon)$, and $N(1-\epsilon) < n_J \leq N$ for any arbitrary constant $\epsilon \leq \min\left\{\gamma_j, 1-\frac{K}{N}\right\}$. The reason is that equation (2.60) is valid in the second interval only, and we need separate analyses for the first and last intervals.

First, we show the statement for $\epsilon L \leq n_J \leq N(1-\epsilon)$. Defining $i_J = \lfloor n_J \frac{K}{N} \rfloor$, we have

$$\begin{aligned} \frac{i_J}{n_J} &= \frac{K}{N} + O(\frac{1}{L}), \\ \frac{K-i_J}{N-n_J} &= \frac{K}{N} + O(\frac{1}{L}) \end{aligned} \tag{2.61}$$

as ϵ is constant, and $K = O(L)$, $N = O(L)$. Hence, we have

$$\begin{aligned}
& \sum_{i=0}^{n_J} Q_J(n_J, i)\hat{P}_e(N - n_J, K - i, J - 1) \\
\geq\ & Q_J(n_J, i_J)\hat{P}_e(N - n_J, K - i_J, J - 1) \\
\overset{(a)}{\doteq}\ & e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N} + O\left(\frac{1}{L}\right)\right)} \\
\overset{(b)}{\doteq}\ & e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}
\end{aligned} \tag{2.62}$$

where (a) follows from (2.60) and the induction assumption, and (b) follows from the fact that $u_j()$'s are differentiable functions according to Lemma 2.1 in subsection 2.3.1.

For $0 \leq n_J \leq \epsilon L$, since $\epsilon < \gamma_j$, the number of packets assigned to the paths of type J is less than the number of such paths. Thus, one packet is allocated to n_J of the paths, and the rest of the paths of type J are not used. Defining $\pi_{b,J}$ as the probability of a path of type J being in the bad state, we can write

$$Q_J(n_J, n_J) = \pi_{b,J}^{n_J} = e^{-n_J \log\left(\frac{1}{\pi_{b,J}}\right)}. \tag{2.63}$$

Therefore, for $0 \leq n_J \leq \epsilon L$, we have

$$\begin{aligned}
& \sum_{i=0}^{n_J} Q_J(n_J, i)\hat{P}_e(N - n_J, K - i, J - 1) \\
\geq\ & Q_J(n_J, n_J)\hat{P}_e(N - n_J, K - n_J, J - 1) \\
\doteq\ & e^{-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K - n_J}{N - n_J}\right) - n_J \log\left(\frac{1}{\pi_{b,J}}\right)} \\
\overset{(a)}{\geq}\ & e^{-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K}{N}\right) - L\epsilon \log\left(\frac{1}{\pi_{b,J}}\right)} \\
\overset{(b)}{\doteq}\ & e^{-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K}{N}\right)} \geq e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}
\end{aligned} \tag{2.64}$$

where (a) follows from the fact that $\frac{K-n_J}{N-n_J} \leq \frac{K}{N}$, and (b) results from the fact that we can select ϵ arbitrarily small.

Finally, we prove the statement for the case $n_J > N(1-\epsilon)$. In this case, we have

$$\begin{aligned} & \sum_{i=0}^{n_J} Q_J(n_J, i)\hat{P}_e(N-n_J, K-i, J-1) \\ \geq \; & Q_J(n_J, K)\hat{P}_e(N-n_J, 0, J-1) \\ \overset{(a)}{\geq} \; & e^{-L\gamma_J u_J\left(\frac{K}{N(1-\epsilon)}\right)} \\ \overset{(b)}{\dot{\geq}} \; & e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)} \end{aligned} \tag{2.65}$$

where (a) follows from the fact that $\epsilon < 1 - \frac{K}{N}$ and $\hat{P}_e(n, 0, j) = 1$, for all n and j. Setting ϵ small enough results in (b).

Inequalities (2.62), (2.64), and (2.65) result in

$$\hat{P}_e(N, K, J) \;\dot{\geq}\; e^{-L\sum_{j=1}^{J}\gamma_j u_j(\alpha)} \tag{2.66}$$

Combining (2.66) with Lemma 2.5 proves the first part of Theorem 2.2 for the case when $\frac{K}{N} > \mathbb{E}\{x_J\}$.

Case 2: $\dfrac{K}{N} \leq \mathbb{E}\{x_J\}$

Similar to Case 1 ($\dfrac{K}{N} > \mathbb{E}\{x_J\}$), we show that for any value of $0 \leq n_J \leq N$, the corresponding term of the minimization in equation (2.16) is asymptotically at least equal to $P_e^{opt}(N, K, J)$. Again, the range of n_J is partitioned into three non-overlapping intervals.

For any arbitrary $0 < \epsilon < \min\left\{\gamma_J, 1 - \frac{K}{N}, \frac{1}{K}\right\}$, and for all n_J in the range of $\epsilon L < n_J \leq N(1-\epsilon)$, we define i_J as $i_J = \lceil n_J \mathbb{E}\{x_J\} \rceil$. We have

$$\begin{aligned} \frac{i_J}{n_J} &= \mathbb{E}\{x_J\} + O\left(\frac{1}{L}\right) \geq \mathbb{E}\{x_J\} \\ \frac{K-i_J}{N-n_J} &< \frac{K}{N} + O\left(\frac{1}{L}\right) \end{aligned} \tag{2.67}$$

Hence,

$$\begin{aligned}
& \sum_{i=0}^{n_J} Q_J(n_J,i)\hat{P}_e(N-n_J,K-i,J-1) \\
\geq\ & Q_J(n_J,i_J)\hat{P}_e(N-n_J,K-i_J,J-1) \\
\overset{(a)}{\doteq}\ & e^{-L\gamma_J u_J\left(\frac{i_J}{n_J}\right)-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K-i_J}{N-n_J}\right)} \\
\overset{(b)}{\geq}\ & e^{-L\gamma_J u_J\left(\mathbb{E}\{x_J\}+O\left(\frac{1}{L}\right)\right)-L\sum_{j=1}^{J-1}\gamma_j u_j\left(\frac{K}{N}+O\left(\frac{1}{L}\right)\right)} \\
\overset{(c)}{\doteq}\ & e^{-L\sum_{j=1}^{J}\gamma_j u_j\left(\frac{K}{N}\right)}
\end{aligned} \tag{2.68}$$

where (a) follows from (2.60) and the induction assumption, and (b) is based on (2.67). (c) results from the facts that $u_j()$'s are differentiable functions, and we have $u_J\left(\mathbb{E}\{x_J\}\right)=0$, both according to Lemma 2.1 in subsection 2.3.1.

For $0 \leq n_J \leq \epsilon L$, the analysis of the Case 1 and inequality (2.64) are still valid. For $n_J > (1-\epsilon)N$, we set $i_J = \lceil \mathbb{E}\left\{x_J\right\} n_J \rceil$. Now, we have

$$i_J \geq n_J \mathbb{E}\{x_J\} > (1-\epsilon)N\mathbb{E}\{x_J\} \geq (1-\epsilon)K. \tag{2.69}$$

The above inequality can be written as

$$K - i_J < \epsilon K < 1 \tag{2.70}$$

since $\epsilon < \frac{1}{K}$. Noting that K and i_J are integer values, it is concluded that $K \leq i_J$. Now,

we can write

$$\begin{aligned}
& \sum_{i=0}^{n_J} Q_J(n_J,i)\hat{P}_e(N-n_J,K-i,J-1) \\
\geq\ & Q_J(n_J,i_J)\hat{P}_e(N-n_J,K-i_J,J-1) \\
\overset{(a)}{=}\ & Q_J(n_J,i_J) \\
\dot{\geq}\ & e^{-L\gamma_J u_J\left(\mathbb{E}\{x_J\}+\frac{1}{n_J}\right)} \\
\overset{(b)}{\dot{\geq}}\ & e^{-L\gamma_J u_J\left(\mathbb{E}\{x_J\}+\frac{1}{(1-\epsilon)N}\right)} \\
\doteq\ & e^{-L\gamma_J u_J\left(\mathbb{E}\{x_J\}+O\left(\frac{1}{L}\right)\right)} \overset{(c)}{\doteq} 1
\end{aligned} \tag{2.71}$$

where (a) follows from the fact that $K \leq i_J$, and $\hat{P}_e(n,k,j) = 1$, for $k \leq 0$. (b) and (c) result from $n_J > (1-\epsilon)N$ and $u_J(\mathbb{E}\{x_J\}) = 0$, respectively.

Hence, inequalities (2.64), (2.68), and (2.71) result in

$$\hat{P}_e(N,K,J) \ \dot{\geq}\ e^{-L\sum_{j=1}^{J}\gamma_j u_j(\alpha)} \tag{2.72}$$

which proves the first part of Theorem 2.2 for the case of $\frac{K}{N} \leq \mathbb{E}\{x_J\}$ when combined with Lemma 2.5.

2.6.11.2 Second and Third Parts of Theorem

We prove the second and the third parts of the theorem by induction on j while the total number of types, J, is fixed. The proof of the statements for the base of the induction, $j = J$, is similar to the proof of the induction step, from $j+1$ to j. Hence, we just give the proof for the induction step. Assume the second and the third parts of the theorem are true for $m = J$ to $j+1$. We prove the same statements for j. The proof is divided into two different cases, depending on whether $\frac{K}{N}$ is larger than $\mathbb{E}\{x_j\}$ or vice versa.

Before we proceed further, it is helpful to introduce two new parameters N' and K' as

$$\begin{aligned} N' &= N - \sum_{m=j+1}^{J} \hat{N}_j \\ K' &= K - \sum_{m=j+1}^{J} K_j. \end{aligned}$$

According to the above definitions and the induction assumptions, it is obvious that

$$\frac{K'}{N'} = \frac{K}{N} + o(1) = \alpha + o(1). \tag{2.73}$$

Case 1: $\dfrac{K}{N} > \mathbb{E}\{x_j\}$

First, by contradiction, it will be shown that for small enough values of $\epsilon > 0$, we have $\hat{N}_j > \epsilon N'$. Let us assume the opposite is true, i.e. $\hat{N}_j \leq \epsilon N'$. Then, we can write

$$\begin{aligned} & \hat{P}_e(N', K', j) \\ \overset{(a)}{=} & \sum_{i=0}^{\hat{N}_j} \hat{P}_e(N' - \hat{N}_j, K' - i, j-1) Q_j(\hat{N}_j, i) \\ \geq & \hat{P}_e(N' - \hat{N}_j, K' - \hat{N}_j, j-1) Q_j(\hat{N}_j, \hat{N}_j) \\ \overset{(b)}{\doteq} & Q_j(\hat{N}_j, \hat{N}_j) e^{-L \sum_{r=1}^{j-1} \gamma_r u_r \left(\frac{K' - \hat{N}_j}{N' - \hat{N}_j} \right)} \\ \overset{(c)}{\geq} & e^{-L n_0 \left(1 - \sum_{r=j+1}^{J} \eta_r \right) \epsilon \log \left(\frac{1}{\pi_{b,j}} \right)} \cdot \\ & e^{-L \sum_{r=1}^{j-1} \gamma_r u_r \left(\frac{K'}{N'} \right)} \\ \overset{(d)}{\dot{>}} & e^{-L \sum_{r=1}^{j} \gamma_r u_r (\alpha)} \end{aligned} \tag{2.74}$$

where (a) follows from equation (2.16) and step (2) of our suboptimal algorithm, (b) results from the first part of Theorem 2.2, and (c) can be justified using arguments similar to those of inequality (2.64). (d) is obtained assuming ϵ is small enough such that the corresponding

term in the exponent is strictly less than $L\gamma_j u_j\left(\frac{K'}{N'}\right)$ and also the fact that $\frac{K'}{N'} = \alpha + o(1)$. The result in (2.74) is obviously in contradiction with the first part of Theorem 2.2, proving that $\hat{N}_j > \epsilon N'$.

Now, we show that if $\hat{N}_j > (1-\epsilon)N'$ for arbitrarily small values of ϵ, we should have $\mathbb{E}\{x_r\} > \alpha$ for all $1 \le r \le j-1$. In such a case, we observe $\frac{\hat{N}_j}{N'} = 1 + o(1)$, proving the second statement of Theorem 2.2. To show this, let us assume $\hat{N}_j > (1-\epsilon)N'$. Hence,

$$\begin{aligned}\hat{P}_e(N', K', j) &= \sum_{i=0}^{\hat{N}_j} \hat{P}_e(N' - \hat{N}_j, K' - i, j-1) Q_j(\hat{N}_j, i) \\ &\dot{\geq} \hat{P}_e(N' - \hat{N}_j, 0, j-1) Q_j(\hat{N}_j, K') \\ &\overset{(a)}{\dot{\geq}} e^{-L\gamma_j u_j\left(\frac{K'}{(1-\epsilon)N'}\right)} \overset{(b)}{\doteq} e^{-L\gamma_j u_j(\alpha + o(1))}\end{aligned} \tag{2.75}$$

where (a) follows from the fact that $\hat{P}_e(n, 0, j) = 1$, for all values of n and j, and the fact that $\hat{N}_j \geq (1-\epsilon)N'$. (b) is obtained by making ϵ arbitrarily small and using equation (2.73). Applying (2.75) and knowing the fact that $\hat{P}_e(N', K', j) \doteq e^{-L\sum_{r=1}^{j}\gamma_r u_r(\alpha)}$, we conclude that $\mathbb{E}\{x_r\} > \alpha$, for all values of $1 \le r \le j-1$.

$\hat{P}_e(N', K', j)$ can be written as

$$\begin{aligned}&\hat{P}_e(N', K', j) \\ = \;& \min_{0 \le N_j \le N'} \sum_{i=0}^{N_j} \hat{P}_e(N' - N_j, K' - i, j-1) Q_j(N_j, i) \\ \overset{(a)}{\doteq} \;& \min_{\epsilon N' \le N_j \le (1-\epsilon)N'} \; \max_{0 \le i \le N_j} \\ & \hat{P}_e(N' - N_j, K' - i, j-1) Q_j(N_j, i) \\ \overset{(b)}{\doteq} \;& \min_{\epsilon N' \le N_j \le (1-\epsilon)N'} \; \max_{\mathbb{E}\{x_j\} N_j < i \le N_j} \\ & e^{-L\gamma_j u_j\left(\frac{i}{N_j}\right) - L\sum_{r=1}^{j-1}\gamma_r u_r\left(\frac{K'-i}{N'-N_j}\right)} \\ \doteq \;& e^{-L \max\limits_{\epsilon N' \le N_j \le (1-\epsilon)N'} \; \min\limits_{\mathbb{E}\{x_j\} N_j < i \le N_j} M_d(i, N_j)} \\ \overset{(c)}{\doteq} \;& e^{-L \max\limits_{\epsilon \le \lambda_j \le (1-\epsilon)} \; \min\limits_{\mathbb{E}\{x_j\}\lambda_j < \beta_j \le \lambda_j} M_c(\beta_j, \lambda_j)}.\end{aligned} \tag{2.76}$$

where $M_d(i, N_j)$ and $M_c(\beta_j, \lambda_j)$ are defined as

$$\begin{aligned} M_d(i, N_j) &= \gamma_j u_j \left(\frac{i}{N_j}\right) + \sum_{r=1}^{j-1} \gamma_r u_r \left(\frac{K' - i}{N' - N_j}\right) \\ M_c(\beta_j, \lambda_j) &= \gamma_j u_j \left(\frac{\beta_j}{\lambda_j}\right) + \sum_{r=1}^{j-1} \gamma_r u_r \left(\frac{\alpha - \beta_j}{1 - \lambda_j}\right). \end{aligned}$$

In (2.76), (a) follows from the fact that $\hat{N}_j$ is bounded as $\epsilon N' \leq \hat{N}_j \leq (1-\epsilon)N'$. (b) results from equation (2.60), $\hat{P}_e(n, k, j)$ being a decreasing function of k, and the fact that we have $Q_j(N_j, i) \leq 1 \doteq Q_j(N_j, \mathbb{E}\{x_j\} N_j)$ for $i < \mathbb{E}\{x_j\} N_j$. β_j and λ_j are defined as $\beta_j = \frac{i}{N'}$ and $\lambda_j = \frac{N_j}{N'}$. (c) is a result of having $M_c(\beta_j, \lambda_j) = M_d(i, N_j) + O\left(\frac{1}{L}\right)$. Hence, the discrete to continuous relaxation is valid.

Let us define $\left(\beta_j^*, \lambda_j^*\right)$ as the values of (β_j, λ_j) which solve the max-min problem in (2.76). Differentiating $M_c(\beta_j, \lambda_j)$ with respect to β_j and λ_j results in

$$\begin{aligned} 0 &= \frac{\gamma_j}{\lambda_j^*} l_j \left(\frac{\beta_j^*}{\lambda_j^*}\right) - \sum_{\substack{r=1, \\ \mathbb{E}\{x_r\} < \zeta}}^{j-1} \frac{\gamma_r}{1 - \lambda_j^*} l_r(\zeta) \\ 0 &= \left\{ -\frac{\gamma_j \beta_j^*}{\lambda_j^{*2}} l_j \left(\frac{\beta_j^*}{\lambda_j^*}\right) + \sum_{\substack{r=1, \\ \mathbb{E}\{x_r\} < \zeta}}^{j-1} \frac{\gamma_r (\alpha - \beta_j^*)}{(1 - \lambda_j^*)^2} l_r(\zeta) \right. \\ &\quad \left. + \left(\frac{\gamma_j}{\lambda_j^*} l_j \left(\frac{\beta_j^*}{\lambda_j^*}\right) - \sum_{\substack{r=1, \\ \mathbb{E}\{x_r\} < \zeta}}^{j-1} \frac{\gamma_r}{1 - \lambda_j^*} l_r(\zeta) \right) \frac{\partial \beta_j^*}{\partial \lambda_j}|_{\lambda_j = \lambda_j^*} \right\} \end{aligned}$$

where $\zeta = \dfrac{\alpha - \beta_j^*}{1 - \lambda_j^*}$. Solving the above equations gives the unique optimum solution (β_j^*, λ_j^*) as

$$\begin{aligned} \beta_j^* &= \alpha \lambda_j^* \\ \lambda_j^* &= \frac{\gamma_j l_j(\alpha)}{\sum_{r=1, \alpha > \mathbb{E}\{x_r\}}^{j} l_r(\alpha)} \end{aligned} \tag{2.77}$$

Hence, the integer parameters $K_j, \hat{N}_j$ defined in the suboptimal algorithm have to satisfy $\frac{K_j}{N'} = \beta_j^* + o(1)$ and $\frac{\hat{N}_j}{N'} = \lambda_j^* + o(1)$, respectively. Based on the induction assumption, it is easy to show that

$$\frac{N'}{N} = \frac{\sum_{r=1,\mathbb{E}\{x_r\}<\alpha}^{j} \gamma_r u_r(\alpha)}{\sum_{r=1,\mathbb{E}\{x_r\}<\alpha}^{J} \gamma_r u_r(\alpha)} \tag{2.78}$$

which completes the proof for the case of $\mathbb{E}\{x_j\} < \frac{K}{N}$.

Case 2: $\frac{K}{N} \leq \mathbb{E}\{x_j\}$

In this case, we show that $\frac{\hat{N}_j}{N} = o(1)$. Defining $i_j = \lceil \mathbb{E}\{x_j\}\hat{N}_j \rceil$, we have

$$\frac{K' - i_j}{N' - \hat{N}_j} = \alpha - (\mathbb{E}\{x_j\} - \alpha)\frac{\hat{N}_j}{N' - \hat{N}_j} + o(1) \tag{2.79}$$

using equation (2.73). Now, we have

$$\begin{aligned}
& \hat{P}_e(N', K', j) \\
= & \sum_{i=0}^{\hat{N}_j} \hat{P}_e(N' - \hat{N}_j, K' - i, j-1) Q_j(\hat{N}_j, i) \\
\geq & \hat{P}_e(N' - \hat{N}_j, K' - i_j, j-1) Q_j(\hat{N}_j, i_j) \\
\overset{(a)}{\doteq} & e^{-L\gamma_j u_j \left(\mathbb{E}\{x_j\} + o(1)\right)} \cdot \\
& e^{-L\sum_{r=1}^{j-1} \gamma_r u_r \left(\alpha - (\mathbb{E}\{x_j\} - \alpha)\frac{\hat{N}_j}{N' - \hat{N}_j}\right)} \\
\doteq & e^{-L\sum_{r=1}^{j-1} \gamma_r u_r \left(\alpha - (\mathbb{E}\{x_j\} - \alpha)\frac{\hat{N}_j}{N' - \hat{N}_j}\right)}
\end{aligned} \tag{2.80}$$

where (a) follows from the first part of Theorem 2.2 and (2.60). On the other hand,

according to the result of the first part of Theorem 2.2, we know that

$$\hat{P}_e(N', K', j) \doteq e^{-L\sum_{r=1}^{j-1}\gamma_r u_r(\alpha)}. \tag{2.81}$$

According to Lemma 2.1, $u_r(\beta)$ is an increasing function of β for all $1 \leq r \leq j-1$. Thus, $\sum_{r=1}^{j-1}\gamma_r u_r(\beta)$ is also a one-to-one increasing function of β. Noting this fact and comparing (2.80) and (2.81), we conclude that $\frac{\hat{N}_j}{N'} = o(1)$ as $\mathbb{E}\{x_j\} - \alpha$ is strictly positive. Noting (2.78), we have $\frac{\hat{N}_j}{N} = o(1)$ which proves the second part of Theorem 2.2 for the case of $\frac{K}{N} \leq \mathbb{E}\{x_j\}$.

Chapter 3

Coding over Input-Independent Channels

In this chapter, we focus on a general class of channels called input-independent channels, of which erasure channels are a special case. Input-independent channels can be memoryless or have a memory extended over the block length. Symmetric discrete memoryless channels are also a special case of input-independent channels. First, we define this class in a mathematically accurate way. Next, we derive a lower-bound on P_E of any code over an input-independent channel. Using this lower-bound, we prove the optimality of MDS codes over erasure channels (with or without memory).

The rest of this chapter is organized as follows. Section 3.1 defines the input- independent channel and introduces a lower-bound on P_E for a general input-independent channel. Section 3.2 applies this lower-bound on erasure channels (with or without memory) and proves optimality of MDS codes over this class of channels. In section 3.3, the super-symmetric DMC is studied and it is shown that perfect codes are optimal across this channel. Finally, we simplify the proposed lower-bound for symmetric DMC and compare it with the previously-known bounds on P_E in section 3.4.

3.1 Input-Independent Channel

This section first defines an input-independent channel in a mathematically accurate way. The definition includes channels with memory extended over a block of N symbols. Next, we prove the main theorem on input-independent channels which has applications in the

rest of the chapter.

Definition 3.1. *Input-Independent Channels*: consider a channel with the input alphabet $\mathcal{A} = \{a_1, a_2, \ldots, a_{|\mathcal{A}|}\}$ and the output alphabet $\mathcal{B} = \{b_1, b_2, \ldots, b_{|\mathcal{B}|}\}$. A block of N transmitted symbols is denoted by the vector $\mathbf{x} \in \mathcal{A}^N$ and the received vector by $\mathbf{y} \in \mathcal{B}^N$. The channel is *input-independent* iff for any $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{A}^N$, there is a one-to-one mapping $\sigma_{12} : \mathcal{B}^N \to \mathcal{B}^N$ such that for all $\mathbf{y} \in \mathcal{B}^N$, we have $\mathbb{P}\{\mathbf{y}|\mathbf{x}_2\} = \mathbb{P}\{\sigma_{12}(\mathbf{y})|\mathbf{x}_1\}$.

The one-to-one mapping $\sigma_{12}()$ may seem confusing. However, it simply represents a permutation of the elements in $\mathcal{B}^N$. Intuitively speaking, the above definition means that the channel shows the same response regardless of the input vector. In other words, $\mathbb{P}\{\mathbf{y}|\mathbf{x}\}$ follows the same probability mass function (pmf) for all $\mathbf{x}$. Next, a specific ordering of the values in this pmf is defined.

Definition 3.2. *Sorted pmf Vector*: consider an input-independent channel as defined in Definition 3.1. For any $\mathbf{x} \in \mathcal{A}^N$, we sort the values of $\mathbb{P}\{\mathbf{y}|\mathbf{x}\}$ for all $\mathbf{y} \in \mathcal{B}^N$ in the non-increasing order into a vector of length $\mathfrak{B} \triangleq |\mathcal{B}|^N$. Due to the input-independent characteristic of the channel, the sorted vector is the same for all $\mathbf{x} \in \mathcal{A}^N$. Thus, we can define the sorted pmf vector corresponding to the channel $\mathbf{p} \triangleq [p_1, p_2, \ldots, p_{\mathfrak{B}}]'$, such that $p_1 \geq p_2 \geq \ldots \geq p_{\mathfrak{B}}$.

To complete the definitions required in our main theorem, we need to define a code (codebook) over the input-independent channel and the decoder corresponding to it.

Definition 3.3. *Codebook*: consider an input-independent channel as defined in Definition 3.1 and the corresponding sorted pmf vector as defined in Definition 3.2. A code (codebook) of size M and length N is a set of M codewords of length N from the alphabet $\mathcal{A}$, each representing a message. In other words the code $\mathcal{C}$ can be written as $\mathcal{C} \triangleq \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\}$ such that $\forall i,\ 1 \leq i \leq M :\ \mathbf{c}_i \in \mathcal{A}^N$.

Definition 3.4. *Decoder*: corresponding to a code $\mathcal{C}$ of size M and length N (Definition 3.3), a decoder is defined as a partitioning of the received vector set $\mathcal{B}^N$ to M disjoint subsets, each consisting of the received vectors mapped to a specific message (codeword). We introduce 3 notations associated with a decoder:

- For any $\mathbf{c}_i \in \mathcal{C}$, $\mathcal{D}(\mathbf{c}_i)$ is defined as the subset of $\mathcal{B}^N$ which includes all the received vectors mapped to $\mathbf{c}_i$. We refer to $\mathcal{D}(\mathbf{c}_i)$ as the *decision region* corresponding to $\mathbf{c}_i$.

- Conversely, for any $\mathbf{y} \in \mathcal{B}^N$, we define $f_{dec}(\mathbf{y}) = \mathbf{c} \in \mathcal{C}$ iff $\mathbf{y} \in \mathcal{D}(\mathbf{c})$.
- Assuming an equiprobable codebook, the average probability of error is defined as

$$P_E \triangleq \frac{1}{M} \sum_{i=1}^{M} \mathbb{P}\{f_{dec}(\mathbf{y}) \neq \mathbf{c}_i | \mathbf{x} = \mathbf{c}_i\}$$

  where $\mathbf{x} \in \mathcal{A}^N$ and $\mathbf{y} \in \mathcal{B}^N$ are the transmitted and received vectors, respectively.

Hence, $f_{dec}()$ denotes the decoding function which maps the received vector $\mathbf{y}$ to one of the codewords. Now, we are ready to prove the main theorem of the chapter which provides a lower-bound on the probability of error of any code over an input-independent channel.

Theorem 3.1. *Consider a codebook $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\}$ with M equiprobable codewords of length N over an input-independent channel (with or without memory) with the input alphabet $\mathcal{A}$ and the output alphabet $\mathcal{B}$ as defined in Definition 3.1. We have the following lower-bound on the average probability of error for any decoder*

$$P_E \geq 1 - \sum_{i=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} p_i - \frac{\mathrm{mod}(\mathfrak{B}, M)}{M} \; p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1}$$

where $\lfloor x \rfloor$ denotes the largest integer number smaller than x, and $\mathrm{mod}(a, b)$ indicates the remainder of dividing a by b. $\mathbf{p}$ represents the sorted pmf vector described in Definition 3.2, and $\mathfrak{B} = |\mathcal{B}|^N$.

Proof This theorem can be proved by selecting a uniform distribution on the output alphabet in Theorem 28 of [42]. However, we provide an alternative proof in Appendix 3.6.1 which is based on the properties of input-independent channels. ■

Next, we state a necessary and sufficient condition on the codebook (and the decoder) which achieves the lower-bound in Theorem 3.1.

Theorem 3.2. *Consider a codebook $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\}$ with M equiprobable codewords of length N over an input-independent channel (with or without memory) with the input alphabet $\mathcal{A}$ and the output alphabet $\mathcal{B}$ as defined in Definition 3.1. Let P_E denote the*

average probability of error for the decoder associated with the code as described in Definition 3.4. P_E satisfies the inequality in Theorem 3.1 with equality iff the following condition is satisfied:

$$\min_{\mathbf{c}\in\mathcal{C}} \min_{\mathbf{y}\in\mathcal{D}(\mathbf{c})} \mathbb{P}\{\mathbf{y}|\mathbf{c}\} \geq \max_{\mathbf{c}\in\mathcal{C}} \max_{\mathbf{y}\notin\mathcal{D}(\mathbf{c})} \mathbb{P}\{\mathbf{y}|\mathbf{c}\}. \tag{3.1}$$

Proof See Appendix 3.6.2. ■

3.2 Erasure Channels with Memory

This section applies Theorem 3.1 and Theorem 3.2 to study general q-ary erasure channels and obtain an optimality result. The result achieved here is NOT new, but the proof is. We have published the same result in [21] (however, for linear MDS codes) with a different proof. The importance of the new proof is that the optimality result can be interpreted as a special case of the general theorems we proved in the previous section. Moreover, the MDS code does not have to be linear. We start with the formal definition of an erasure channel.

Definition 3.5. An erasure channel is defined as the one which maps every input symbol to either itself or to an erasure symbol ξ. More accurately, an arbitrary channel (memoryless or with memory) with the input vector $\mathbf{x} \in \mathcal{A}^N$, $|\mathcal{A}| = q$, the output vector $\mathbf{y} \in (\mathcal{A} \cup \{\xi\})^N$, and the transition probability $\mathbb{P}\{\mathbf{y}|\mathbf{x}\}$ is defined to be erasure *iff* it satisfies the following conditions:

1. $\mathbb{P}\{y_j \notin \{x_j, \xi\} | x_j\} = 0, \ \forall\, j$, where x_j and y_j denote the j'th elements of the vectors $\mathbf{x}$ and $\mathbf{y}$.

2. Defining the *erasure identifier vector* $\mathbf{e}$ as

$$e_j \triangleq \begin{cases} 1 & y_j = \xi \\ 0 & \text{otherwise} \end{cases}$$

   $\mathbb{P}\{\mathbf{e}|\mathbf{x}\} = \mathbb{P}\{\mathbf{e}\}$, i.e. $\mathbf{e}$ is independent of $\mathbf{x}$.

It is easy to check that the erasure channel defined above is indeed an input-independent one. Therefore, the two theorems in the previous section can be used to find a lower-bound on its P_E. Here, we generalize our previous result in [21] to non-linear MDS codes and provide an alternative proof for it.

Theorem 3.3. *A (linear or non-linear) block code of length N with M equiprobable codewords over an arbitrary erasure channel (memoryless or with memory) of alphabet size q has the minimum probability of error (assuming optimum, i.e., maximum likelihood decoding) among all block codes of the same size if that code is Maximum Distance Separable (MDS).*

Proof It is important to note that the straightforward application of Theorem 3.1 (with the output alphabet size of $q+1$) does not result in a tight lower-bound. The intuitive reason behind this fact is that when a codeword of length N is transmitted over an erasure channel, the number of possible received vectors is much less than $(q+1)^N$. Therefore, we analyze the erasure channel as a combination of multiple (parallel) input-independent channels with smaller received vector sets; we can do that since in an erasure channel, the receiver always knows the erasure pattern before decoding the codeword. This technique is explained in Appendix 3.6.3. ■

3.3 Super-Symmetric DMC

In this section, we focus on super-symmetric discrete memoryless channels (DMC). This channel is depicted in Fig. 3.1. Each transmitted symbol is received flawlessly with the probability $1-\pi$ or goes to one of the other $q-1$ symbols with the equal probability $\pi' = \frac{\pi}{q-1}$. We also assume that $1-\pi > \pi'$ or equivalently $\pi < \frac{q-1}{q}$ which not a strict condition for large alphabet sizes. Applying the theorems of section 3.1 to this simple channel, we get the following neat result.

Theorem 3.4. *A (linear or non-linear) block code of length N with M equiprobable codewords over a super-symmetric discrete memoryless channel of alphabet size q has the minimum probability of error (assuming optimum, i.e., maximum likelihood decoding) among all block codes of the same size if that code is a perfect code. A code is perfect if it satisfies the Hamming inequality, $M\sum_{k=0}^{t}\binom{N}{k}(q-1)^k \leq q^N$, with equality.*

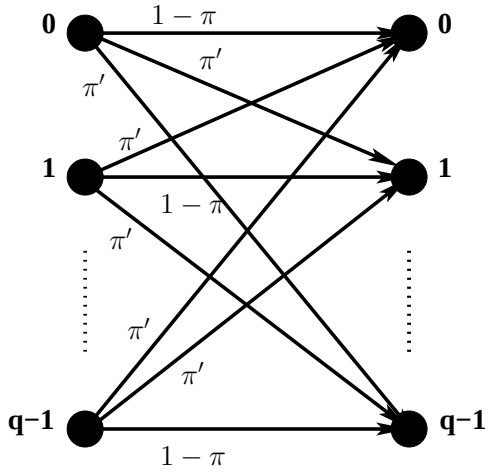


Figure 3.1: Super-symmetric memoryless discrete channel with alphabet size q. Each symbol goes to itself with the probability $1-\pi$ and goes to each one of the other symbols with the probability $\pi' = \frac{\pi}{q-1}$.

Proof See Appendix 3.6.4. ■

3.4 Symmetric DMC

This section proposes a lower-bound on P_E for any code of length N with q^K equiprobable codewords over a symmetric discrete memoryless channel (DMC). This channel is a more general one than the super-symmetric DMC studied throughout section 3.3. The definition of symmetric DMC we use in this work is the same as the one in [18]. Comparing the following definition with Definition 3.1, it is obvious that the symmetric DMC is an input-independent channel.

Definition 3.6. Consider a DMC with the input and output alphabet $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$. Let us define the $q \times q$ *channel transition matrix* $\mathbf{S} = [s_{ij}]$ where $s_{ij} \triangleq \mathbb{P}\{a_j \text{ received}|\ a_i \text{ transmitted}\}$. The channel is symmetric if all rows and all columns of $\mathbf{S}$ are permutations of a sorted probability vector $\boldsymbol{\pi}$ where $\pi_1 \geq \pi_2 \geq \cdots \geq \pi_q \geq 0$ and $\sum_{i=1}^{q} \pi_i = 1$.

Based on the above definition, we can define a permutation corresponding to each input symbol in the alphabet as follows. For each input symbol $a_k \in \mathcal{A}$, we know that the transition probabilities conditioned on a_k being transmitted are a permutation of the

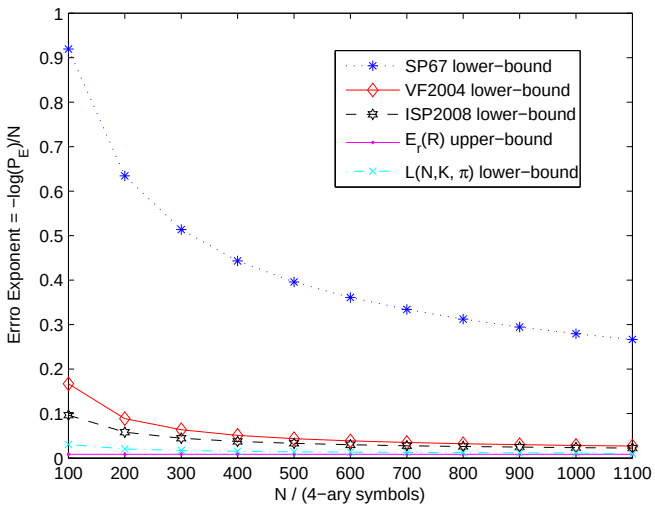


Figure 3.2: Error exponent of $L(N, K, \boldsymbol{\pi})$, i.e. $\frac{-\log L(N,K,\boldsymbol{\pi})}{N}$, for a quadratic symmetric channel with $\boldsymbol{\pi} = [0.90, 0.05, 0.03, 0.02]$ and the rate of $R = \frac{K}{N}\log q = 0.6 \log q$ is compared with error exponents of lower-bounds SP67 [43], VF2004 [44], and ISP2008 [45] for different values of N . Random coding error exponent $E_r(R)$ (lower-bound on error exponent) is shown as the horizontal line.

vector $\boldsymbol{\pi}$. Let us denote this permutation by $\sigma_{a_k}()$. Then for any output symbol $a_l \in \mathcal{A}$, we have $\mathbb{P}\{a_l|a_k\} = \pi_j$ where $j = \sigma_{a_k}(a_l)$.

Let us consider an arbitrary code of length N with q^K equiprobable codewords over the symmetric channel defined in Definition 3.6. A codeword $\mathbf{c} \in \mathcal{C}$ is transmitted, and any vector $\mathbf{y} \in \mathcal{A}^N$ can be received. We define the vector $\mathbf{N}$ with the length q and entries N_j as $N_j \triangleq \sum_{i=1}^{N} I(j = \sigma_{c_i}(y_i))$. In this definition, c_i and y_i denote the i'th entries of vectors $\mathbf{c}$ and $\mathbf{y}$, respectively. $I(s)$ is the indicator function, i.e. $I(s) = 1$ if the statement s is true, and $I(s) = 0$ otherwise. We also define the *extended distance* between $\mathbf{c}$ and $\mathbf{y}$ as $\mathbf{d}(\mathbf{c}, \mathbf{y}) \triangleq \mathbf{N}$.

Since the channel is memoryless, we have $\mathbb{P}\{\mathbf{y}|\mathbf{c}\} = \prod_{j=1}^{q} \pi_j^{N_j}$ for all of the received vectors whose extended distance satisfies $\mathbf{d}(\mathbf{c}, \mathbf{y}) = \mathbf{N}$. There exist $\binom{N}{\mathbf{N}} = \dfrac{N!}{\prod_{j=1}^{q} N_j!}$ such vectors. Following a similar terminology in [18], we call this group of vectors the *type* associated with $\mathbf{N}$. The number of different types we can have equals the number of solutions to the equation $\sum_{j=1}^{q} N_j = N$ such that $N_j \geq 0$ for all j. Thus, there exist

$\binom{N+q-1}{q-1} = O(N^{q-1})$ different types[1]. The big-O notation is defined as $f(N) = O(g(N))$ iff $\exists \Omega, N_0$ such that $\forall N > N_0$, we have $|f(N)| \leq \Omega |g(N)|$.

The output vector space has the cardinality of q^N, and there are q^K codewords in the codebook. Using Theorem 3.1, we have the following lower-bound $L(N, K, \boldsymbol{\pi}) \triangleq 1 - \sum_{i=1}^{q^{N-K}} p_i$ on P_E for any code. p_1 to $p_{q^{N-K}}$ denote the q^{N-K} largest values in the set $\{\mathbb{P}\{\mathbf{y}|\mathbf{c}\}\}_{\mathbf{y}\in\mathcal{A}^N}$. To identify these values, we need to sort different types based on their probabilities (probability of each vector in the type being received given a codeword is transmitted). Therefore, we form the table T with $\binom{N+q-1}{q-1}$ rows and two columns. Each row corresponds to one of the possible types; the first column of the t'th row $T(t,1) = \prod_{j=1}^{q} \pi_j^{N_j}$ represents the probability of each member of the type being received given a codeword is transmitted. The second column $T(t,2) = \binom{N}{\mathbf{N}}$ equals the number of vectors in the type. Next, we can use the *quick sort* algorithm to sort the rows in T based on their first column values. We define $t^\star$ as

$$t^\star \triangleq \min_{\sum_{t'=1}^{t} T(t',2) \geq q^{N-K}} t. \tag{3.2}$$

In other words, $t^\star$ denotes the minimum number of types (rows) we need to include to form a decision region of size q^{N-K}. Using $t^\star$, we can find the lower-bound of P_E

$$\begin{aligned} L(N, K, \boldsymbol{\pi}) &= 1 - \sum_{t=1}^{t^\star - 1} T(t,1)T(t,2) - \\ &\qquad T(t^\star, 1)\left(\sum_{t=1}^{t^\star} T(t,2) - q^{N-K}\right). \end{aligned} \tag{3.3}$$

The above equation is based on the simple principle that we should include the more probable types before the less probable ones.

Having $L(N, K, \boldsymbol{\pi})$, the arising question is that *how tight this lower-bound on P_E is.* In other words, c*an we find a lower-bound which is larger than $L(N, K, \boldsymbol{\pi})$ and is still valid for codes over the symmetric DMC*? To answer these questions in the asymptotic case, we define a new notation. We define $f(N) \doteq g(N)$ iff $\frac{1}{N}\lim_{N\to\infty} f(N) = \frac{1}{N}\lim_{N\to\infty} g(N)$. Comparators $\dot{\geq}$ and $\dot{\leq}$ are also defined similarly. Then, we have the following theorem on

[1]Although there exist $O(N^{q-1})$ different types, the number of vectors in each type is in the order of $O(q^N)$. Thus, we need $O(N)$ bytes to store the number of vectors for each type. The total memory we need for all types is in the order of $O(N^q)$.

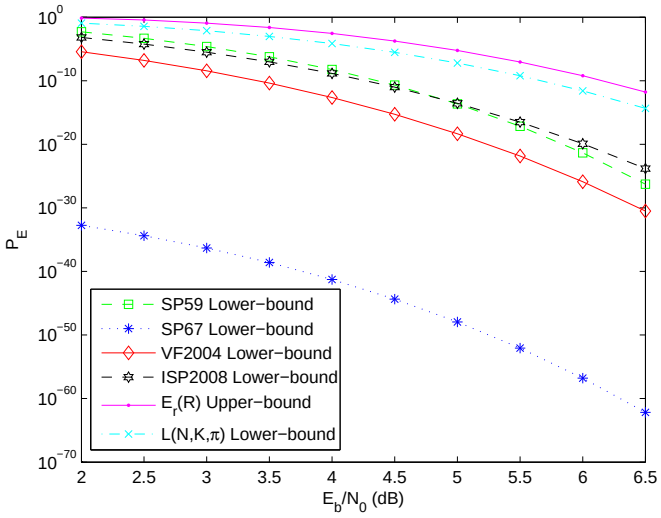


Figure 3.3: For block length $N = 128$, $K = 48$, and 3-PSK constellation with hard decoding in presence of AWGN noise (a ternary DMC), $L(N, K, \boldsymbol{\pi})$ is compared with lower-bounds SP59 [53], SP67 [43], VF2004 [44], and ISP2008 [45] for different values of $\frac{E_b}{N_0}$.

the asymptotic behavior of $L(N, K, \boldsymbol{\pi})$ when $\frac{K}{N}$ is constant as N grows.

Theorem 3.5. *Consider a symmetric DMC as described in Definition 3.6. For* $\frac{K}{N} = r < \frac{C}{\log q}$, *we have* $L(N, K, \boldsymbol{\pi}) \doteq e^{-NE_r(R)}$ *where* $R = r \log q$ *is the transmission rate of the code. Moreover,* $C = \log q - H(\boldsymbol{\pi})$ *denotes capacity of the channel, and* $E_r(R)$ *is the random coding error exponent of the channel as defined by Gallager in [50]. Furthermore, any other lower-bound on* P_E, *say* $L'(N, K, \boldsymbol{\pi})$, *is asymptotically smaller than* $L(N, K, \boldsymbol{\pi})$, *i.e. we have* $L(N, K, \boldsymbol{\pi}) \dot{\geq} L'(N, K, \boldsymbol{\pi})$.

Proof See Appendix 3.6.5. ■

Finally, we compare $L(N, K, \boldsymbol{\pi})$ with four other lower-bounds and the random coding upper-bound $e^{-NE_r(R)}$ [50]:

- SP59: this lower-bound [53] is valid for soft decoding of equal-energy codewords with Gaussian constellation over the AWGN channel. It can be used as a benchmark for comparison when the input constellation is M-PSK over the AWGN channel with hard or soft decoding.

- SP67: the original sphere packing lower-bound on P_E in [43], valid for any DMC.

- VF2004: Velambois and Fossorier's [44] improvement on SP67, valid for any DMC.
- ISP2008: the Improved Sphere-packing Bound (ISP) [45] for symmetric DMC.

In Fig. 3.2, error exponent of $L(N, K, \boldsymbol{\pi})$, i.e. $\frac{-\log L(N,K,\boldsymbol{\pi})}{N}$, is compared with error exponents of lower-bounds SP67 [43], VF2004 [44], and ISP2008 [45] for different values of N. The channel is a quadratic one with $\boldsymbol{\pi} = [0.90, 0.05, 0.03, 0.02]$ and rate $R = \frac{K}{N}\log q = 0.6 \log q$. Random coding error exponent $E_r(R)$ (lower-bound on error exponent) is shown as the horizontal line. We know that all of the exponents converge to $E_r(R)$ as N grows. However, it is clearly seen that $L(N, K, \boldsymbol{\pi})$ converges much faster (in shorter block lengths) than the other lower-bounds.

Figure 3.3 considers the block length $N = 128$, $K = 48$, and a ternary DMC resulting from 3-PSK constellation with hard decoding in presence of AWGN noise. $L(N, K, \boldsymbol{\pi})$ is compared with lower-bounds SP59 [53], SP67 [43], VF2004 [44], and ISP2008 [45] for different values of $\frac{E_b}{N_0}$. It is observed that in very low $\frac{E_b}{N_0}$, SP59 is the tightest of the previous lower-bounds, while ISP2008 becomes the tightest as $\frac{E_b}{N_0}$ grows. However, in any case, the best of the previous lower-bounds remain almost 2dB below the upper-bound for typical values of P_E (10^{-4} to $10^{-}10$). On the other hand, $L(N, K, \boldsymbol{\pi})$ (our new lower-bound) follows the upper-bound ($e^{-NE_r(R)}$) with almost 0.5dB gap. This translates to a huge improvement in lower-bounding P_E for short block lengths.

Figure 3.4 considers the block length $N = 64$, $K = 32$, and a quadratic DMC resulting from QPSK constellation with hard decoding in presence of AWGN noise. $L(N, K, \boldsymbol{\pi})$ is compared with lower-bounds SP59 [53], SP67 [43], VF2004 [44], and ISP2008 [45]. Among the previous lower-bounds, ISP2008 is the tightest except in very low $\frac{E_b}{N_0}$ in which SP59 dominates. Examining the plot for typical values of P_E, from 10^{-4} to 10^{-10}, it is observed that for a fixed P_E, $L(N, K, \boldsymbol{\pi})$ is just 0.5dB below the upper-bound. This should be compared to the tightest of the previous lower-bounds, ISP2008, which is typically 1.5 to 2dB below the upper-bound. Again, we see that our proposed lower-bound by far outperforms the previous ones.

3.5 Conclusion

We study the problem of lower-bounding the probability of error (P_E) over *input- independent* channels. An input-independent is defined in the general case (channels with mem-

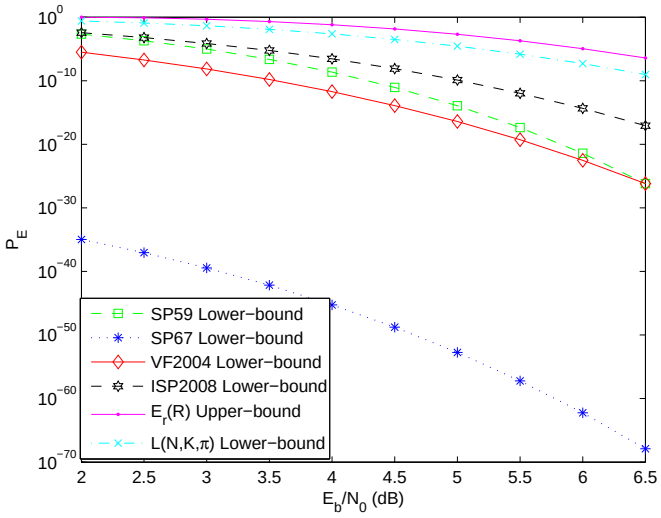


Figure 3.4: For block length $N = 64$, $K = 32$, and QPSK constellation with hard decoding in presence of AWGN noise (a quadratic DMC), $L(N, K, \boldsymbol{\pi})$ is compared with lower-bounds SP59 [53], SP67 [43], VF2004 [44], and ISP2008 [45] for different values of $\frac{E_b}{N_0}$.

ory), and a lower-bound on P_E is introduced. Next, we apply this general lower-bound on three special input-independent channels: erasure channel, super-symmetric Discrete Memoryless Channel (DMC), and q-ary symmetric DMC. We show that *Maximum Distance Separable* (MDS) codes achieve the minimum probability of error over any erasure channel (with or without memory). Moreover, we prove that *perfect* codes achieve the minimum probability of error over a super-symmetric channel. Finally, we propose a new lower-bound for P_E of any block code over symmetric DMC and show that this bound is exponentially tight. For ternary and 4-ary symmetric channels, the proposed lower-bound is compared with the previous lower-bounds in moderate to short block lengths. It is shown that our lower-bound by far outperforms the previous bounds, especially for shorter block lengths.

3.6 Appendices

3.6.1 Proof of Theorem 3.1

We define $P_c \triangleq 1 - P_E$. Then, proving the theorem is equivalent to finding an upper-bound on P_c as follows

$$\begin{aligned} P_c &= \frac{1}{M}\sum_{i=1}^{M}\mathbb{P}\left\{f_{dec}(\mathbf{y}) = \mathbf{c}_i | \mathbf{x} = \mathbf{c}_i\right\} \\ &\overset{(a)}{=} \frac{1}{M}\sum_{i=1}^{M}\mathbb{P}\left\{\mathbf{y} \in \mathcal{D}(\mathbf{c}_i) | \mathbf{x} = \mathbf{c}_i\right\} \\ &= \frac{1}{M}\sum_{i=1}^{M}\sum_{\mathbf{y}\in\mathcal{D}(\mathbf{c}_i)}\mathbb{P}\left\{\mathbf{y} | \mathbf{x} = \mathbf{c}_i\right\} \\ &\overset{(b)}{\leq} \frac{1}{M}\sum_{i=1}^{M}\sum_{j=1}^{|\mathcal{D}(\mathbf{c}_i)|} p_j \\ &\overset{(c)}{=} \frac{1}{M}\sum_{l=1}^{\mathfrak{B}} k_l p_l \end{aligned} \tag{3.4}$$

where (a) follows from the definition of $f_{dec}()$ and $\mathcal{D}(\mathbf{c}_i)$ (Definition 3.4). (b) results from the definition of the sorted pmf vector in Definition 3.2. (c) is true if the vector $\mathbf{k} = [k_1, k_2, \ldots, k_{\mathfrak{B}}]'$ is defined as follows

$$k_l \triangleq \sum_{i=1}^{M} I\left(|\mathcal{D}(\mathbf{c}_i)| \geq l\right) \tag{3.5}$$

where $I()$ is the indicator function, i.e. $I(s) = 1$ if the statement s is true, and $I(s) = 0$ otherwise. According to the above definition, k_l denotes the number of decision regions ($\mathcal{D}(\mathbf{c}_i)$) whose cardinality is larger than or equal to l. As we have only M decision regions, the vector $\mathbf{k}$ obviously satisfies the following inequalities

$$M \geq K_1 \geq K_2 \geq \ldots \geq K_{\mathfrak{B}} \geq 0. \tag{3.6}$$

Moreover, the number of decision regions with cardinality l equals $k_l - k_{l+1}$. The total number of vectors $\mathbf{y}$ in all decision regions (with any cardinality) is

$$\mathfrak{B}k_{\mathfrak{B}} + \sum_{l=1}^{\mathfrak{B}-1} l(k_l - k_{l+1}) = \sum_{l=1}^{\mathfrak{B}} k_l = \mathfrak{B}. \tag{3.7}$$

Using the above two results on the vector $\mathbf{k}$, we can write

$$\begin{aligned}
MP_c &\overset{(a)}{\leq} \sum_{l=1}^{\mathfrak{B}} k_l \; p_l \\
&\overset{(b)}{\leq} \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l \; p_l + p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} \sum_{l=\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2}^{\mathfrak{B}} k_l \\
&\overset{(c)}{=} \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l \; p_l + p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} \left(\mathfrak{B} - \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l \right) \\
&= M \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} p_l - \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} (M - k_l) p_l + \\
&\quad k_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} + p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} \left(\mathfrak{B} - \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l \right) \\
&\overset{(d)}{\leq} M \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} p_l - p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} (M - k_l) + \\
&\quad k_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} + p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} \left(\mathfrak{B} - \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l \right) \\
&= M \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} p_l - p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} (\mathfrak{B} - \mathrm{mod}(\mathfrak{B}, M) \\
&\quad + \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l) + p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} \left(\mathfrak{B} - \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} k_l \right) \\
&\overset{(e)}{\leq} M \sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} p_l + \mathrm{mod}(\mathfrak{B}, M) p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1}
\end{aligned} \tag{3.8}$$

where (a) follows from (3.4), while (b) and (d) and (e) result from the fact that the elements in the sorted pmf vector $\mathbf{p}$ are listed in the non-increasing order. (c) is based on (3.7). ■

3.6.2 Proof of Theorem 3.2

Necessary Condition: let us assume (3.1) is true. For any $\mathbf{c}_0 \in \mathcal{C}$ and any $\mathbf{y}_1 \in \mathcal{D}(\mathbf{c}_0)$ and $\mathbf{y}_2 \notin \mathcal{D}(\mathbf{c}_0)$, we can easily write

$$\begin{aligned}\mathbb{P}\{\mathbf{y}_1|\mathbf{c}_0\} &\geq \min_{\mathbf{c}\in\mathcal{C}} \min_{\mathbf{y}\in\mathcal{D}(\mathbf{c})} \mathbb{P}\{\mathbf{y}|\mathbf{c}\} \\ &\geq \max_{\mathbf{c}\in\mathcal{C}} \max_{\mathbf{y}\notin\mathcal{D}(\mathbf{c})} \mathbb{P}\{\mathbf{y}|\mathbf{c}\} \geq \mathbb{P}\{\mathbf{y}_2|\mathbf{c}_0\}. \end{aligned} \tag{3.9}$$

Defining the set $\mathcal{P}(\mathbf{c}_0) \triangleq \{\mathbb{P}\{\mathbf{y}|\mathbf{c}_0\}|\mathbf{y} \in \mathcal{D}(\mathbf{c}_0)\}$ and using the above result, we conclude that

$$\mathcal{P}(\mathbf{c}_0) = \{p_1, p_2, \ldots, p_{|\mathcal{D}(\mathbf{c}_0)|}\} \tag{3.10}$$

where p_i denotes the i'th element of the sorted pmf vector. In other words, the $|\mathcal{D}(\mathbf{c}_0)|$ elements in $\mathcal{P}(\mathbf{c}_0)$ take their highest possible values.

Similar to the proof of Theorem 3.1, we define $P_c = 1 - P_E$. Using the result in (3.10), it is seen that the inequality (b) in (3.4) turns into an equality. Therefore we can write

$$P_c = \frac{1}{M} \sum_{l=1}^{\mathfrak{B}} k_l p_l \tag{3.11}$$

where k_l is defined in 3.5.

Next, using (3.10) and the non-increasing order of the sorted pmf vector, the condition in (3.1) translates to

$$p_{\overline{D}} \geq p_{1+\underline{D}} \tag{3.12}$$

where we define $\overline{D} \triangleq \max_{\mathbf{c}\in\mathcal{C}} |D(\mathbf{c})|$ and $\underline{D} \triangleq \min_{\mathbf{c}\in\mathcal{C}} |D(\mathbf{c})|$. Now, we can imagine two possible cases:

1. Cardinality of the decision region corresponding to $\mathbf{c}$, i.e. $|\mathcal{D}(\mathbf{c})|$, is the same for all $\mathbf{c} \in \mathcal{C}$. Since the decision regions altogether must cover all of the space $\mathcal{B}$, this is equivalent of $|\mathcal{D}(\mathbf{c})| = \frac{\mathfrak{B}}{M}$ for all $\mathbf{c} \in \mathcal{C}$. According to the definition of k_l in (3.5), we have $k_l = M$ for $1 \leq l \leq \frac{\mathfrak{B}}{M}$ and $l = 0$ for all other l. Replacing the values of

k_l in (3.11), it is easy to verify that the inequality in Theorem 1 is satisfied with equality.

2. At least two decision regions have different cardinalities, i.e. $|\mathcal{D}(\mathbf{c})|$ is NOT the same for all $\mathbf{c} \in \mathcal{C}$. This means that $\overline{D} \geq 1 + \underline{D}$. Due to the non-increasing order of the sorted pmf vector, we conclude that $p_{\overline{D}} \leq p_{1+\underline{D}}$. Combining this result with (3.12), we have

$$p_{1+\underline{D}} = p_{2+\underline{D}} = \cdots = p_{\overline{D}} = p_0 \tag{3.13}$$

for a constant p_0.

Using the fact that $\sum_{i=1}^{M} |\mathcal{D}(\mathbf{c}_i)| = \mathfrak{B}$, it is easy to show that

$$\begin{aligned} \overline{D} &> \lfloor \frac{\mathfrak{B}}{M} \rfloor \\ \underline{D} &< \lfloor \frac{\mathfrak{B}}{M} \rfloor + 1 \end{aligned} \tag{3.14}$$

Having this bound for $\lfloor \frac{\mathfrak{B}}{M} \rfloor$, we are ready to prove the necessarily condition as follows.

$$\begin{aligned} M\ P_c &\overset{(a)}{=} \sum_{l=1}^{\mathfrak{B}} k_l p_l \\ &\overset{(b)}{=} M \sum_{l=1}^{\underline{D}} p_l + p_0 \sum_{l=1+\underline{D}}^{\overline{D}} k_l \\ &\overset{(c)}{=} M \sum_{l=1}^{\underline{D}} p_l + p_0 \left(\mathfrak{B} - M\underline{D}\right) \\ &\overset{(d)}{=} M \sum_{l=1}^{\underline{D}} p_l + p_0 M \left(\lfloor \frac{\mathfrak{B}}{M} \rfloor - \underline{D} \right) + \\ &\quad p_0 \bmod (\mathfrak{B}, M) \\ &\overset{(e)}{=} M \sum_{l=1}^{\underline{D}} p_l + M \sum_{l=\underline{D}+1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} p_l + \\ &\quad p_{1+\lfloor \frac{\mathfrak{B}}{M} \rfloor} \bmod (\mathfrak{B}, M) \end{aligned} \tag{3.15}$$

where (a) follows from (3.11). (b) and (e) result from (3.13) and the definition of k_l in (3.5) which gives us $k_l = M$ for $l \leq \underline{D}$ and $k_l = 0$ for $l > \overline{D}$. (c) follows from (3.7),

and (d) is a direct result of the fact that $\mathfrak{B} = M\lfloor \frac{\mathfrak{B}}{M} \rfloor + \mathrm{mod}(\mathfrak{B}, M)$. Replacing P_c with $1 - P_E$ in (3.15) proves the necessary condition for case (2).

Sufficient Condition: we assume that the code (and the decoder) satisfies the inequality in Theorem 3.1 with equality and prove that (3.1) must follow. The proof is obvious when $\overline{D} = \underline{D}$. Thus, we give the proof only for the case where at least two decision regions have different cardinalities.

Let us focus on (3.8) in the proof of Theorem 3.1. According to our assumption, inequalities (a), (b), and (d) in (3.8) are satisfied with equality, i.e. are *tight*. Replacing (a) with equality leads to inequality (b) in (3.4) being tight. This in turn requires the condition in (3.10) to hold. In other words, the set $\mathcal{P}(\mathbf{c}_0) \triangleq \{\mathbb{P}\{\mathbf{y}|\mathbf{c}_0\}|\mathbf{y} \in \mathcal{D}(\mathbf{c}_0)\}$ must include the $|\mathcal{D}(\mathbf{c}_0)|$ highest values for all $\mathbf{c}_0 \in \mathcal{C}$. In the proof of the necessary condition, we have already shown that under the condition in (3.10), (3.12) and (3.1) are equivalent. Hence, we need to prove (3.12) instead of (3.1).

Going back to (3.8) and replacing inequality (b) with equality, we get

$$\sum_{l=\lfloor \frac{\mathfrak{B}}{M} \rfloor + 3}^{\mathfrak{B}} k_l \left(p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} - p_l \right) \overset{(a)}{=}$$
$$\sum_{l=\lfloor \frac{\mathfrak{B}}{M} \rfloor + 3}^{\overline{D}} k_l \left(p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} - p_l \right) = 0$$

where (a) follows from the definition of k_l in (3.5). Due to the non-increasing order of the sorted pmf vector, none of the terms in the summation can be negative. Thus, all of the terms should be equal to zero. Moreover, by definition, $k_l > 0$ for $l \leq \overline{D}$. Hence, we must have

$$p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2} = p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 3} = \cdots = p_{\overline{D}} \tag{3.16}$$

if $\lfloor \frac{\mathfrak{B}}{M} \rfloor + 2 \leq \overline{D}$.

Similarly, replacing inequality (d) in (3.8) with equality, we get

$$\sum_{l=1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} (M - k_l) \left(p_l - p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} \right) \stackrel{(a)}{=} \sum_{l=\underline{D}+1}^{\lfloor \frac{\mathfrak{B}}{M} \rfloor} (M - k_l) \left(p_l - p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1} \right) = 0$$

where (a) follows from the fact that $k_l = M$ for $l \leq \underline{D}$ by definition. Again, all the terms are non-negative. Thus, they all should be zero. Moreover, by definition, $k_l < M$ for $l \geq \underline{D} + 1$. Hence, we must have

$$p_{\underline{D}+1} = p_{\underline{D}+2} = \cdots = p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor} = p_{\lfloor \frac{\mathfrak{B}}{M} \rfloor + 1}. \tag{3.17}$$

Combining (3.16) and (3.17) with (3.14), we see that condition (3.13) is satisfied. Having (3.13), (3.12) is satisfied. As explained earlier, this is equivalent of (3.1) being proved. Therefore, the proof of the sufficient condition is complete. ■

3.6.3 Proof of Theorem 3.3

The trick used in the proof of this theorem is *adaptive* decision regions in the decoder. Due to the nature of the erasure channel, the decoder can immediately extract the erasure identifier vector $\mathbf{e}$ from the received vector $\mathbf{y}$. Therefore, it can adjust the decision regions according to $\mathbf{e}$.

We start by the definition of the MDS code. A code is MDS iff it satisfies the Singleton bound by equality, i.e. if we have $M = q^{N-d+1}$ where d is the *minimum Hamming distance* of the code. Next, let m denote the number of non-zero elements in the binary vector $\mathbf{e}$, i.e. $m \triangleq \sum_{i=1}^{N} e_i$. For any erasure pattern (vector) $\mathbf{e}$, we define the set $\mathcal{Y}(\mathbf{e})$ as the set of all possible received vectors if one of the codewords in the codebook $\mathcal{C}$ is transmitted and the erasure pattern $\mathbf{e}$ is observed, i.e.

$$\begin{aligned} \mathcal{Y}(\mathbf{e}) \triangleq \Big\{ & \mathbf{y} \in (\mathcal{A} \cup \{\xi\})^N \,|\exists\, \mathbf{c} \in \mathcal{C} \;: \\ & \mathbb{P}\{\mathbf{y}|\mathbf{x} = \mathbf{c} \;\&\; \mathbf{e} \text{ occurred}\} > 0 \Big\}. \end{aligned} \tag{3.18}$$

Now, we consider the following two cases.

1. $m \leq d-1$: let us assume any two distinct codewords $\mathbf{c}_1 \in \mathcal{C}$ and $\mathbf{c}_2 \in \mathcal{C}$ are transmitted. It is easy to see that the corresponding received vectors $\mathbf{y}_1$ and $\mathbf{y}_2$ must be distinct as well. The reason is that if this is not true, the distance between $\mathbf{c}_1$ and $\mathbf{c}_1$ would be less than d which is impossible by the definition of d. Therefore, in this case, we have $|\mathcal{Y}(\mathbf{e})| = M$ and each $\mathbf{y} \in \mathcal{Y}(\mathbf{e})$ corresponds to exactly one codeword. The decision regions $\{\mathcal{D}(\mathbf{c}_i)\}_{i=1}^{M}$ are chosen as follows. For each $\mathbf{y} \in \mathcal{Y}(\mathbf{e}) \subseteq (\mathcal{A} \cup \{\xi\})^N$, $\mathbf{y}$ is placed at $\mathcal{D}(\mathbf{c}_i)$ of the codeword $\mathbf{c}_i$ it corresponds to. All other vectors $\mathbf{y} \in (\mathcal{A} \cup \{\xi\})^N - \mathcal{Y}(\mathbf{e})$ are impossible to occur and can be placed in an arbitrary decision region, say $\mathcal{D}(\mathbf{c}_1)$. Using (3.4), probability of correct decoding given $\mathbf{e}$ can be written as $P_{c|\mathbf{e}} = 1$.

2. $d \leq m \leq N$: consider an arbitrary possible received vector $\mathbf{y}_i \in \mathcal{Y}(\mathbf{e})$. We choose $m-d+1$ erasure symbols (ξ) in specific locations in $\mathbf{y}_i$. There are q^{m-d+1} distinct ways to *enhance* $\mathbf{y}_i$ by replacing these $m-d+1$ erasure symbols with elements from the input alphabet set $\mathcal{A}$. We define $\mathcal{C}_i$ as the set of all such enhanced vectors from $\mathbf{y}_i$. Obviously, we have $|\mathcal{C}_i| = q^{m-d+1}$ where $|.|$ is the cardinality operator. We can do the same enhancement for all other $\mathbf{y} \in \mathcal{Y}(\mathbf{e})$ and obtain disjoint sets $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{|\mathcal{Y}(\mathbf{e})|}$.

   Now, consider the union of all such sets $\bar{\mathcal{C}} \triangleq \bigcup_{i=1}^{|\mathcal{Y}(\mathbf{e})|} \mathcal{C}_i$. Since $\bar{\mathcal{C}}$ includes all possible enhancements of $\mathcal{Y}(\mathbf{e})$, i.e. partial codewords with $N-m$ non-erased symbols, it is obvious that $\bar{\mathcal{C}}$ should include all the partial codewords with $N-d+1$ non-erased symbols (at the specified locations). Hence, we have $|\bar{\mathcal{C}}| \overset{(a)}{=} |\mathcal{Y}(\mathbf{e})| q^{m-d+1} \geq M$ where (a) follows from the fact that $\bar{\mathcal{C}}$ is the union of $|\mathcal{Y}(\mathbf{e})|$ disjoint sets $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{|\mathcal{Y}(\mathbf{e})|}$.

   On the other hand, we know that members of $\bar{\mathcal{C}}$ are vectors of length $N-d+1$ entries from the input alphabet $\mathcal{A}$. Hence, we have $|\bar{\mathcal{C}}| \leq q^{N-d+1} \overset{(a)}{=} M$ where (a) follows from the definition of the an MDS code. Combining this with the lower-bound on the cardinality of $\bar{\mathcal{C}}$ in the previous paragraph, we get $|\bar{\mathcal{C}}| = M = q^{N-d+1}$. In other words, each member of $\bar{\mathcal{C}}$ corresponds to the partial vector of exactly one codeword in the codebook $\mathcal{C}$.

   Finally, since $|\mathcal{C}_i| = q^{m-d+1}$ for all i, we conclude that $|\mathcal{Y}(\mathbf{e})| = q^{N-m}$. This means that every $\mathbf{y}_i \in \mathcal{Y}(\mathbf{e})$ may be associated to any of the q^{m-d+1} codewords $\mathbf{y}_i$ can be enhanced to. We pick one of such q^{m-d+1} codewords arbitrarily. By proper labeling of the codewords, we can assume that $\mathbf{y}_i$ is mapped to $\mathbf{c}_i$ for $1 \leq i \leq |\mathcal{Y}(\mathbf{e})| = q^{N-m}$.

Then obviously, we have $\mathbb{P}\{\mathbf{y}_i|\mathbf{x}=\mathbf{c}_i \ \& \ \mathbf{e} \text{ occurred}\}=1$. As in the previous case, all other vectors $\mathbf{y}\in(\mathcal{A}\cup\{\xi\})^N-\mathcal{Y}(\mathbf{e})$ are impossible to occur and can be placed in an arbitrary decision region, say $\mathcal{D}(\mathbf{c}_{|\mathcal{Y}(\mathbf{e})|+1})$. It should be noted that in the defined decoder here, we have $|\mathcal{D}(\mathbf{c}_i)|=1$ for $1\leq i\leq|\mathcal{Y}(\mathbf{e})|=q^{N-m}$, while $\mathcal{D}(\mathbf{c}_i)=\emptyset$ for $q^{N-m}<i\leq M$.

It is easy to check that the above-described decoder (with the defined decision regions) satisfies condition (3.1) in Theorem 3.2 readily. Therefore, an MDS code satisfies the lower-bound of Theorem 3.1 on P_E and is optimal. Using (3.4), probability of correct decoding given $\mathbf{e}$ can be written as

$$\begin{aligned} P_{c|\mathbf{e}} &= \frac{1}{M}\sum_{i=1}^{M}\sum_{\mathbf{y}\in\mathcal{D}(\mathbf{c}_i)}\mathbb{P}\left\{\mathbf{y}|\mathbf{x}=\mathbf{c}_i \ \& \ \mathbf{e} \text{ occurred}\right\} \\ &= \frac{1}{M}\sum_{i=1}^{|\mathcal{Y}(\mathbf{e})|}1=\frac{1}{q^{m-d+1}}. \end{aligned} \tag{3.19}$$

Combining the above two cases, we conclude that

$$\begin{aligned} P_E^{MDS} &= 1-\sum_{\mathbf{e}}\mathbb{P}\{\mathbf{e}\}P_{c|\mathbf{e}} \\ &= 1-\sum_{m=d}^{N}\sum_{\mathbf{e}:w(\mathbf{e})=m}\mathbb{P}\{\mathbf{e}\}\left(1-\frac{1}{q^{m-d+1}}\right) \end{aligned}$$

where $w(\mathbf{e})$ denotes the Hamming weight of the binary vector $\mathbf{e}$. Moreover, it is easy to see that in the described decoder, we have $\mathbb{P}\{\mathbf{y}|\mathbf{x}=f_{dec}(\mathbf{y})\}=1$ for all $\mathbf{y}\in\mathcal{Y}(\mathbf{e})$. The vectors in $\mathbf{y}\in(\mathcal{A}\cup\{\xi\})^N-\mathcal{Y}(\mathbf{e})$ are impossible to occur given $\mathbf{e}$. For such vectors we have $\mathbb{P}\{\mathbf{y}|\mathbf{x}=\mathbf{c}\}=0$ for all $\mathbf{c}\in\mathcal{C}$. Therefore, this decoder obviously satisfies the maximum likelihood condition, i.e. $\mathbb{P}\{\mathbf{y}|\mathbf{x}=f_{dec}(\mathbf{y})\}\geq P\{\mathbf{y}|\mathbf{x}=\mathbf{c}\}$ for all $\mathbf{y}\in(\mathcal{A}\cup\{\xi\})^N$ and $\mathbf{c}\in\mathcal{C}$. ■

3.6.4 Proof of Theorem 3.4

We start by the definition of perfect codes. A code is perfect if it satisfies the Hamming inequality, $M\sum_{k=0}^{t}\binom{N}{k}(q-1)^k\leq q^N$, with equality. t is defined as $t\triangleq\lfloor\frac{d-1}{2}\rfloor$. Graphically speaking, this means that each codeword is surrounded by a sphere of radius (Hamming

distance) t. Such spheres are obviously disjoint (use the triangle inequality on the Hamming distance metric and the fact that $2t < d$). If the union of these spheres for all codewords covers the received vector space $\mathcal{A}^N$, the code is perfect.

For every $\mathbf{y} \in \mathcal{A}^N$ and $\mathbf{c} \in \mathcal{C}$, we have $\mathbb{P}\{\mathbf{y}|\mathbf{x} = \mathbf{c}\} = (1-\pi)^{N-d(\mathbf{y},\mathbf{c})}\pi'^{d(\mathbf{y},\mathbf{c})}$ where $d(\mathbf{y}, \mathbf{c})$ denotes the Hamming distance between $\mathbf{y}$ and $\mathbf{c}$. This is a decreasing function of $d(\mathbf{y}, \mathbf{c})$ as we assumed $1 - \pi > \pi'$.

For each $\mathbf{c} \in \mathcal{C}$, we set $\mathcal{D}(\mathbf{c})$ as all of the received vectors in the sphere of radius t centered at $\mathbf{c}$. Since the code is perfect, these decision regions cover the received vector space. With this structure of decision regions, we have

$$\min_{\mathbf{c}\in\mathcal{C}} \min_{\mathbf{y}\in\mathcal{D}(\mathbf{c})} \mathbb{P}\{\mathbf{y}|\mathbf{c}\} \geq (1-\pi)^{N-t}\pi'^{t} \geq \max_{\mathbf{c}\in\mathcal{C}} \max_{\mathbf{y}\notin\mathcal{D}(\mathbf{c})} \mathbb{P}\{\mathbf{y}|\mathbf{c}\}$$

and the condition (3.1) in Theorem 3.2 is satisfied. Therefore, the perfect code is optimal and achieves the lower-bound of Theorem 3.1 on P_E. Moreover, the structure of the decision regions implies that the decoder is a maximum likelihood decoder. ■

3.6.5 Proof of Theorem 3.5

We know that $T(t, 1) = e^{N\sum_{j=1}^{q} n_j \log \pi_i}$. Moreover, based on the method of types in [18], it is easy to verify that $T(t, 2) \doteq e^{N(H(\mathbf{n})+o(1))}$ where $\mathbf{n} \triangleq \frac{\mathbf{N}}{N}$ and $H(.)$ is the entropy function. Thus, we have $T(t, 1)T(t, 2) \doteq e^{-N(D(\mathbf{n}||\boldsymbol{\pi})+o(1))}$ where $D(.||.)$ denotes the Kullback-Leibler distance defined in [18]. Next, we write

$$\begin{aligned} L(N, K, \boldsymbol{\pi}) &\overset{(a)}{\geq} \sum_{t=t^\star+1}^{\binom{N+q-1}{q-1}} T(t, 1)T(t, 2) \\ &\doteq \sum_{t=t^\star+1}^{\binom{N+q-1}{q-1}} e^{-ND(\mathbf{n}||\boldsymbol{\pi})} \\ &\overset{(b)}{\doteq} e^{-ND(\mathbf{n}^{\star\star}||\boldsymbol{\pi})} \\ &\overset{(c)}{\geq} e^{-ND(\mathbf{n}^{\star}||\boldsymbol{\pi})} \end{aligned} \tag{3.20}$$

where $\mathbf{n}^{\star\star} \triangleq \underset{\mathbf{n}\in\mathcal{S}_1}{\operatorname{argmin}} D(\mathbf{n}||\boldsymbol{\pi})$, and $\mathcal{S}_1$ is defined as the set of all types which correspond to the rows $t^\star + 1$ to the last row in the sorted table T. Similarly, we define

$\mathbf{n}^\star \triangleq \underset{\mathbf{n}\in\mathcal{S}_2}{\operatorname{argmin}} D(\mathbf{n}||\boldsymbol{\pi})$ and $\mathcal{S}_2 \triangleq \{\mathbf{n}|e^{NH(\mathbf{n})} \dot{\geq} q^{N-K} = e^{N(1-r)\log q}\}$. In the above inequality, (a) follows from (3.3). (b) results from the fact that the dominant term in a summation with a polynomial number of terms (polynomial in terms of N) is the term with the largest exponent. (c) is based on $\mathcal{S}_2 \subseteq \mathcal{S}_1$, i.e. any $\mathbf{n} \in \mathcal{S}_2$ can not correspond to any of the types in the first $t^\star$ rows of the table T.

According to (3.20), the problem of lower-bounding $L(N, K, \boldsymbol{\pi})$ reduces to solving the following optimization problem

$$\begin{aligned} &\min D(\mathbf{n}||\boldsymbol{\pi}) \\ &\text{s.t. } H(\mathbf{n}) \geq (1-r)\log q \text{ and } \textstyle\sum_{j=1}^{q} n_j = 1. \end{aligned} \tag{3.21}$$

Since $D(\mathbf{n}||\boldsymbol{\pi})$ is a convex function of $\mathbf{n}$ and has a global minimum of zero at $\mathbf{n} = \boldsymbol{\pi}$ outside of the optimization region, it is easy to show that the minimum point resides on the edge where $H(\mathbf{n}) = (1-r)\log q$. Using the Lagrangian method, we get

$$D(\mathbf{n}^\star||\boldsymbol{\pi}) = (\beta-1)\frac{\sum_{j=1}^{q}\pi_j^\beta \log \pi_j}{\sum_{j=1}^{q}\pi_j^\beta} - \log\left(\sum_{j=1}^{q}\pi_j^\beta\right) \tag{3.22}$$

where the parameter β is the solution of the following non-linear equation

$$R = \log q + \beta\frac{\sum_{j=1}^{q}\pi_j^\beta \log \pi_j}{\sum_{j=1}^{q}\pi_j^\beta} - \log\left(\sum_{j=1}^{q}\pi_j^\beta\right). \tag{3.23}$$

Also, it can be shown that $\frac{1}{2} \leq \beta \leq 2$, or equivalently $0 \leq \frac{1-\beta}{\beta} \leq 1$.

On the other hand, random coding error exponent [50] is defined as

$$E_r(R) \triangleq \max_{0\leq\rho\leq 1}\left\{-\rho R + \max_{\mathbf{Q}} E_0(\rho, \mathbf{Q})\right\} \tag{3.24}$$

where $\mathbf{Q}$ is the input distribution, and $E_0(\rho, \mathbf{Q})$ equals

$$E_0(\rho, \mathbf{Q}) \triangleq -\log\left(\sum_{j=1}^{q}\left[\sum_{k=1}^{q} Q(k)\mathbb{P}\{j|k\}^{\frac{1}{1+\rho}}\right]^{1+\rho}\right).$$

Due to the symmetry of the channel, the uniform input distribution maximizes $E_0(\rho, \mathbf{Q})$ for each ρ. Therefore, the value of ρ which maximizes (3.24) can be found by solving the equation $R = \dfrac{\partial E_0(\rho, \mathbf{Q})}{\partial \rho}$. Solving this equation, we see that

$$E_r(R) = -\frac{\rho_m \sum_{j=1}^{q} \pi_j^{\frac{1}{1+\rho_m}} \log \pi_j}{(1+\rho_m) \sum_{j=1}^{q} \pi_j^{\frac{1}{1+\rho_m}}} - \log\left(\sum_{j=1}^{q} \pi_j^{\frac{1}{1+\rho_m}}\right) \tag{3.25}$$

where ρ_m is the solution to the following non-linear equation

$$R = \log q + \frac{\sum_{j=1}^{q} \pi_j^{\frac{1}{1+\rho_m}} \log \pi_j}{(1+\rho_m) \sum_{j=1}^{q} \pi_j^{\frac{1}{1+\rho_m}}} - \log\left(\sum_{j=1}^{q} \pi_j^{\frac{1}{1+\rho_m}}\right). \tag{3.26}$$

Setting $\beta = \frac{1}{1+\rho_m}$, we clearly see that equations (3.25) and (3.26) are identical to (3.22) and (3.23). Therefore, we have $D(\mathbf{n}^\star || \boldsymbol{\pi}) = E_r(R)$. Based on (3.20), it is concluded that $L(N, K, \boldsymbol{\pi}) \dot{\geq} e^{-NE_r(R)}$.

We know that $L(N, K, \boldsymbol{\pi})$ is a lower-bound on P_E of any code over the symmetric DMC. Moreover, there exists at least one codebook (constructed by random coding) for which $P_E \leq e^{-NE_r(R)}$. Hence, we must have $L(N, K, \boldsymbol{\pi}) \dot{\leq} e^{-NE_r(R)}$. Combining this with the result of the previous paragraph, we get $L(N, K, \boldsymbol{\pi}) \doteq e^{-NE_r(R)}$.

Finally, let us assume there exists another lower-bound $L'(N, K, \boldsymbol{\pi})$ on P_E of any code of size $[N, K]$. For the same reason described in the previous paragraph, we know that $L'(N, K, \boldsymbol{\pi}) \dot{\leq} e^{-NE_r(R)} \doteq L(N, K, \boldsymbol{\pi})$. Therefore, $L(N, K, \boldsymbol{\pi})$ is exponentially the tightest lower-bound we can have in the asymptotic case. ■

Chapter 4

Diversity-Rate Trade-off in Erasure Networks

This chapter addresses a fundamental *trade-off* between rate and *diversity gain* in *erasure networks*. An erasure network is modeled by a directed graph whose links are orthogonal erasure channels. Furthermore, the erasure status of the links is assumed to be fixed during each block of transmission and known only by the destination node. For each link e in the graph, a message transmitted on e is erased with probability $p^{\omega(e)}$. We define the diversity gain as $\lim_{p\to 0} \frac{\log P_E}{\log p}$ where P_E is the probability of error. Intuitively speaking, the diversity gain is the asymptotic slope of P_E versus $\frac{1}{p}$ in logarithmic scale. This definition is similar to the standard definition of diversity gain for the slow Rayleigh fading channel in the wireless communication literature [19] if $\frac{1}{p}$ is interpreted as Signal-to-Noise-Ratio (SNR).

Using diversity gain as a measure of reliability, we show that there is a fundamental trade-off between rate and reliability in erasure networks. Moreover, it is shown that *conventional routing* fails to achieve the optimum trade-off between these two. Instead, linear network coding achieves the optimum trade-off between rate and reliability in all cases.

Unlike the previous works which suggest the potential benefit of linear network coding in the error-free *multicast* scenario (in terms of the achievable rate), our result demonstrates the benefit of linear network coding in the erasure single-source single-destination scenario (in terms of the diversity gain). To the best of our knowledge, this is the first work in the literature which compares conventional routing and linear network coding in *unicast* applications.

Table 4.1: Different Notations for Diversity Gain

Notation	Description	Defined in
$d^{opt}(r)$	maximum diversity gain among all end-to-end connections with rate r	Definition 4.12 in subsection 4.2.5
d^{max}	maximum diversity gain among all end-to-end connections with non-zero rate	Definition 4.13 in subsection 4.2.5
$d^{\star}(r)$	$\min_{d\geq 0, r>\tilde{r}(d)} d$	Definition 4.20 in section 4.4
$d^{MDR}(r)$	diversity gain of MDS coding + Disjoint Routing end-to-end connection with rate r	section 4.3
$d^{MMR}(r)$	diversity gain of MDS coding + Max-Flow Routing end-to-end connection with rate r	subsection 4.5.2
$d^{MMRD}(r)$	diversity gain of MDS coding + Max-Flow Routing with Detours for rate r	subsection 4.5.2

4.1 Notation and Organization

throughout this chapter, capital bold letters represent matrices, while lowercase bold letters and regular letters represent vectors and scalars, respectively. The superscript $'$ stands for the matrix transpose operation, while the operator det(.) denotes the determinant of a matrix. Moreover, all sets are denoted by calligraphic letters. Finally, $f(p) = O\left(g(p)\right)$ *iff* $\exists \epsilon_0, c > 0$ such that $|f(p)| \leq c|g(p)|$ for $\forall\, 0 < p < \epsilon_0$ (the standard big-O notation).

Different notations are used to denote diversity gain in different scenarios throughout the chapter. These notations are listed in table 4.1.

The rest of the chapter is organized as follows. Section 1.3.2 reviews the related work. In section 4.2, the system model is introduced, and the technical terms used in our work are defined in a mathematically accurate way. These definitions include concepts like erasure graph, end-to-end connection, diversity gain, optimum diversity-rate trade-off, conventional routing, and linear network coding. Section 4.3 is dedicated to the analysis of diversity-rate trade-off for homogeneous erasure graphs. In section 4.4, we study the diversity-rate trade-off in the general erasure graphs. Section 4.5 presents the simulation results and compares the performance of linear network coding and conventional routing. Finally, section 4.6 concludes the chapter.

4.2 System Model and Definitions

4.2.1 Network Graph

The network is modeled as an *erasure graph* which is defined as follows.

Definition 4.1. *Erasure Graph*: a graph $G = (\mathcal{V}, \mathcal{E})$ is called an erasure graph if the following conditions are met.

1. G is directed, weakly connected [125], and acyclic.
2. Each link $e \in \mathcal{E}$ has two states: ON and OFF. $\forall\, e \in \mathcal{E}$, e is OFF with the probability $p^{\omega(e)}$ and is ON with the probability $1 - p^{\omega(e)}$.
3. For $\forall\, e \in \mathcal{E}$ connecting $u \in \mathcal{V}$ to $v \in \mathcal{V} - \{u\}$, u transmits a vector of length $\sigma(e)$ consisting of q-ary symbols per time slot on the link e. Then, if e is ON, v receives the transmitted vector correctly during the same time slot. Otherwise (if e is OFF), v receives an erasure symbol, ξ, independent of the transmitted vector.
4. $\sigma(e)$ is a positive integer number, $\sigma(e) \in \mathbb{Z}^+$.
5. For $\forall\, e \in \mathcal{E}$, if e is ON (OFF), it stays ON (OFF) for the whole block of transmission. In other words, links do not change their states in a block.
6. Graph links are *delay-free*. More accurately, the delay on each link is so small that a message transmitted from the source at the time slot $1 \leq t \leq T$ can reach any other node in the graph within the same time slot.

The the rest of this subsection lists some basic definitions which are used in the rest of the chapter.

Definition 4.2. *Head* and *Tail*: for $\forall\, e \in \mathcal{E}$ connecting $u \in \mathcal{V}$ to $v \in \mathcal{V} - \{u\}$, $h(e) = u$ denotes the head of the link and $\tau(e) = v$ denotes its tail.

Definition 4.3. For $\forall\, e \in \mathcal{E}$, $\mathbf{x}_{e,t} \in \mathbb{F}_q^{\sigma(e)}$ denotes the $\sigma(e)$ symbols sent on the link e at the time slot t. $\mathbb{F}_q$ represents the Galois field of size q.

Definition 4.4. For every set $\mathcal{S} \subseteq \mathcal{E}$, $\sigma(\mathcal{S})$ is defined as $\sigma(\mathcal{S}) \triangleq \sum_{e \in \mathcal{S}} \sigma(e)$. Similarly, $\omega(\mathcal{S})$ is defined as $\omega(\mathcal{S}) \triangleq \sum_{e \in \mathcal{S}} \omega(e)$.

Definition 4.5. For $\forall\, v \in \mathcal{V}$, $\mathcal{L}_{in}(v)$ denotes the set of incoming links to v, and $\mathcal{L}_{out}(v)$ denotes the set of outgoing links from v.

Definition 4.6. Consider the nodes $s \in \mathcal{V}$ and $z \in \mathcal{V} - \{s\}$, where there exists at least one directed path from s to z. Any partition of $\mathcal{V}$ to two disjoint sets $\mathcal{V}_1$ and $\mathcal{V}_2$ such that $s \in \mathcal{V}_1$ and $z \in \mathcal{V}_2$ is called an $s - z$ *cut* of the graph $G = (\mathcal{V}, \mathcal{E})$. The set of links from $\mathcal{V}_1$ to $\mathcal{V}_2$ is called an $s - z$ *cutset*, $\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s, z)$. In other words, we define

$$\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s, z) \triangleq \{e \in \mathcal{E} | \tau(e) \in \mathcal{V}_1,\ h(e) \in \mathcal{V}_2\}\,. \tag{4.1}$$

Definition 4.7. *Min-Cardinality-Cut & Min-Cut*: for every pair of end-nodes $s \in \mathcal{V}$ and $z \in \mathcal{V} - \{s\}$, the $s-z$ min-cardinality-cut, $\mathrm{MCC}(s, z)$, is defined as the minimum cardinality of $s - z$ cutsets, i.e. $\mathrm{MCC}(s, z) \triangleq \min_{\mathcal{V}_1,\mathcal{V}_2 \subset \mathcal{V}: s \in \mathcal{V}_1, z \in \mathcal{V}_2, \mathcal{V}_1 \bigcap \mathcal{V}_2 = \emptyset} |\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s, z)|$. Similarly, min-cut, $\mathrm{MC}(s, z)$, is defined as $\mathrm{MC}(s, z) \triangleq \min_{\mathcal{V}_1,\mathcal{V}_2 \subset \mathcal{V}: s \in \mathcal{V}_1, z \in \mathcal{V}_2, \mathcal{V}_1 \bigcap \mathcal{V}_2 = \emptyset} \sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s, z)\right)$.

4.2.2 Justification of the Model

It should be noted that the erasure network model described in Definition 4.1 is an abstraction which captures the essential aspects of many practical networks like: i) wireless mesh networks, ii) the Internet, iii) overlay networks [70, 71, 79]. Overlay networks are virtual networks constructed over the Internet for various purposes and applications. Peer-to-Peer (P2P) networks [14] and Content Delivery Networks (CDN) [79, 101] are examples of overlay networks built over the Internet. The former consists of many end users sharing (music and video) files. The latter is a special overlay network consisting of *Edge Servers* (nodes) responsible for delivery of the contents (e.g. large files or video streams) from an original server to the end users.

Based on the nature of the underlying network, the two assumptions in the erasure network model (Definition 4.1) are justified here.

- *Erasure status of the links does not change in one transmission block*: for wireless mesh networks, this assumption is equivalent to the well-known *slow fading* model [19, 126].

  In case the erasure network models the Internet or an overlay network working over the Internet, this assumption can be justified for many applications, for example, video

transmission. Consider a high-quality video stream (30 frame/sec) with the end-to-end rate of $1-2$ Mbps. According to [127], the average size of video packets is around $500-1500$ Bytes, depending on the type of the packet[1]. This means that video packets are transmitted every $4-12$ ms on the average[2]. Due to the high computational complexity of both *linear network coding* and Forward Error Correction (FEC) across packets, the block length is kept below $100-150$ packets in both coding methods [12, 15, 35, 129]. Thus, the block duration stays well below the ≈ 2 sec limit. On the other hand, many studies have shown that the outage of Internet links or routers typically last for much longer periods (in the order of a few seconds to minutes) [130, 131]. The outage event may arise due to congestion in a router or an automatic update of the Internet path by the Border Gate Protocol (BGP) [130, 131].

- *Delay-free links*: this assumption is added to the model to make the comparison between conventional routing (with the possibility of FEC at the end nodes) and *linear network coding* easier. However, all of the results of the chapter can be extended to erasure networks whose links have non-negligible delay.

  Let us consider linear network coding first. As later described in Definition 4.9 in subsection 4.2.4, each intermediate node generates several linear combinations (weighted sums with different weights) of the received symbols (packets) and transmits them through the outgoing links. Following the setup in [59], we assume that each packet includes a tag (header) which contains the time of transmission from the source node. Since there are multiple paths with different delays from the source to each intermediate node, the symbols (packets) reaching the intermediate node at each instant of time do not correspond to the symbols transmitted by the source at the same time. Thus, the intermediate node has to wait long enough so that it receives all the symbols with the same time tag (generated at the same time) before it generates and transmits their linear combinations on the outgoing links. Obviously, as long as the block duration T is much longer than the maximum end-to-end delay of the erasure graph, the performance of the system is the same as that of a delay-free network.

  Similarly, when conventional routing takes advantage of FEC at the end nodes, the desti-

[1] Video packet size varies depending on the instantaneous rate and the type of frame the packet corresponds to [127, 128].

[2] The term "on the average" is important as the inter-packet time may vary significantly in video applications.

nation node has to wait some extra time until it receives all of the packets routed through different paths (with different delays). Again, as long as the difference between the fastest and slowest end-to-end paths (in terms of the delay) is negligible compared to the block duration, the system can be effectively modeled by a delay-free network. For a more comprehensive discussion about linear network coding and routing in networks with delay, refer to [59, 61, 63]; when each link has a fixed delay of one unit, all of the equations in our work stay valid after multiplying a delay operator D to the entry corresponding to that link in network transfer matrix $\mathbf{F}$. Thus, we can still write the determinants of the end-to-end transfer matrices as polynomials in terms of all the linear coefficients (weights) as well as the delay operator D.

4.2.3 End-to-End Connection

An end-to-end connection from the node $s \in \mathcal{V}$ to the node $z \in \mathcal{V} - \{s\}$ with the normalized rate r over T time slots is denoted by notation $\mathfrak{C}(s, z, r)$ in this work. Such an end-to-end connection consists of the following components.

- *Messages*: a set of equiprobable messages $\mathcal{M} = \{m_1, m_2, \ldots, m_M\}$, where $M = q^{rT}$.
- *Message Vectors*: a one-to-one mapping of the messages to the vectors of size rT with elements in $\mathbb{F}_q$

$$\begin{aligned} \mathbf{w} &= f(m) \\ f &: \mathcal{M} \rightarrow \mathbb{F}_q^{rT} \end{aligned} \tag{4.2}$$

  Therefore, sending the message $m \in \mathcal{M}$ is equivalent to sending the vector $\mathbf{w} \in \mathbb{F}_q^{rT}$.

- *Encoding Strategy*: for $\forall\, e \in \mathcal{L}_{out}(s)$, we consider a set of encoding functions

$$\begin{aligned} \mathbf{x}_{e,t} &= f_{s,e}(t, \mathbf{w}) \\ f_{s,e} &: \{1, \ldots, T\} \times \mathbb{F}_q^{rT} \rightarrow \mathbb{F}_q^{\sigma(e)}. \end{aligned} \tag{4.3}$$

  Therefore, $f_{s,e}(t, \mathbf{w})$ is the vector of symbols the source transmits on the outgoing link e at time t if it tries to send the message vector $\mathbf{w}$.

- *Network Strategy*: for every intermediate node $u \in \mathcal{V} - \{s, z\}$, $\forall\, e \in \mathcal{L}_{out}(u)$, we consider a set of forwarding functions

$$\begin{aligned} \mathbf{x}_{e,t} &= f_{e,t}\left(\mathbf{Y}_{u,t}\right) \\ f_{e,t} &: \mathcal{T}\left(\Sigma, t, \mathbb{F}_q \cup \{\xi\}\right) \rightarrow \mathbb{F}_q^{\sigma(e)} \end{aligned} \tag{4.4}$$

  where $\mathbf{Y}_{u,t}$ is defined as a matrix of size $\sigma\left(\mathcal{L}_{in}(u)\right) \times t$ whose j'th column contains all the symbols u has received in the time slot j. Intuitively speaking, $\mathbf{Y}_{u,t}$ includes all the symbols that the node u has received (on all of its incoming links) up to the time t. Moreover, we define $\Sigma \triangleq \sigma\left(\mathcal{L}_{in}(u)\right)$, and $\mathcal{T}(m, n, \mathcal{A})$ denotes the set of all $m \times n$ matrices with entries in the set $\mathcal{A}$.

- *Decoding Strategy*: we consider a decoding function at the end node

$$\begin{aligned} \hat{\mathbf{w}} &= f_z\left(\mathbf{Y}_{z,T}\right) \\ f_z &: \mathcal{T}\left(\sigma\left(\mathcal{L}_{in}(z)\right), T, \mathbb{F}_q \cup \{\xi\}\right) \rightarrow \mathbb{F}_q^{rT} \end{aligned} \tag{4.5}$$

  where $\mathbf{Y}_{z,T}$ is defined similar to $\mathbf{Y}_{u,t}$ in the previous bullet. $\hat{\mathbf{w}}$ is the estimate of the transmitted message vector at the receiver side. The receiver decodes the message as $\hat{m} = f^{-1}(\hat{\mathbf{w}})$ where $f()$ is defined in (4.2).

4.2.4 Conventional Routing & Linear Network Coding

Definition 4.8. *Conventional Routing*: an end-to-end connection $\mathfrak{C}(s, z, r)$ uses conventional routing if the following conditions are satisfied.

1. For $\forall\, e \in \mathcal{L}_{out}(s)$ and $1 \leq t \leq T$, we should have $\mathbf{x}_{e,t} \in \mathcal{W}^{\sigma(e)}$ where $\mathcal{W}$ is the set of all elements in the message vector $\mathbf{w}$.

2. For $\forall\, u \in \mathcal{V} - \{s, z\}$ and $\forall\, e \in \mathcal{L}_{out}(u)$ and $1 \leq t \leq T$, we should have $\mathbf{x}_{e,t} \in \mathcal{Y}_{u,t}^{\sigma(e)}$ where $\mathcal{Y}_{u,t}$ denotes the set of all the elements in the matrix $\mathbf{Y}_{u,t}$. Moreover, the routing function which selects the elements of $\mathbf{x}_{e,t}$ out of the elements in $\mathbf{Y}_{u,t}$ can only depend on the state (ON or OFF) of the incoming edges to u. In other words, the set of outgoing links on which a specific incoming symbol is forwarded is independent of the incoming symbols. Instead, it only depends on the ON-OFF states of the incoming links.

The above definition describes the routing schemes used in the conventional packet switched networks. A set of symbols (packets) are generated at the source and are conveyed to the destination through the network. The intermediate nodes do not perform any algebraic computation on the symbols (packets); they either simply forward or copy-and-forward the packets received through the incoming links to the outgoing links.

Definition 4.9. *Linear Network Coding*: for an integer value of r, an end-to-end connection $\mathfrak{C}(s, z, r)$ uses linear network coding if the following conditions are satisfied.

1. At the source side: for $\forall\, e \in \mathcal{L}_{out}(s)$ and $1 \leq t \leq T$, we have

$$\mathbf{x}_{e,t} = \mathbf{\Gamma}_e \ \mathbf{w}^t \tag{4.6}$$

   where $\mathbf{w}^t \triangleq \left[w_{(t-1)r+1}, w_{(t-1)r+2}, \ldots, w_{tr}\right]'$ and Γ_e is a matrix of size $\sigma(e) \times r$ relating the input message vector to the inputs for the edge e.

2. At the intermediate nodes: for $\forall\, u \in \mathcal{V} - \{s, z\}$ and $\forall\, e \in \mathcal{L}_{out}(u)$ and $1 \leq t \leq T$, we have

$$\mathbf{x}_{e,t} = \sum_{e' \in \mathcal{L}_{in}(u), e' \text{is ON}} \mathbf{B}_{e,e'} \mathbf{x}_{e',t} \tag{4.7}$$

   where $B_{e,e'}$ is a matrix of size $\sigma(e) \times \sigma(e')$ relating the output vector on edge e to the input vector on edge e'. It should be noted that the linear operator here is performed only on the inputs of the edges which are ON. In other words, whenever we have $\mathbf{x}_{e',t} = [\xi, \xi, \ldots, \xi]'$ (a vector of length $\sigma(e')$ consisting of erasure symbols), $\mathbf{x}_{e',t}$ is just discarded.

3. At the destination side: for $1 \leq t \leq T$, we have

$$\hat{\mathbf{w}}^t = \sum_{e \in \mathcal{L}_{in}(z), e \text{ is ON}} \Lambda_e \mathbf{x}_{e,t} \tag{4.8}$$

   where $\hat{\mathbf{w}}^t$ is defined similar to $\mathbf{w}^t$ and Λ_e is a matrix of size $r \times \sigma(e)$ relating the inputs on edge e to the estimated message. It should be noted that the linear operator here is performed only on the inputs of the edges which are ON.

The above definition means that the source transmits multiple linear combinations of r message symbols in each time slot. The intermediate nodes also produce multiple linear

combinations of the received symbols and transmit them on the outgoing links. The end node should be able to reconstruct the r message symbols transmitted in each time slot by computing linear combinations of the received symbols.

Note that the described linear network code is defined for integer values of r. However, any non-integer rate can be achieved by time-sharing between two linear network codes with different integer rates.

4.2.5 Diversity Gain

In section 1.3 of chapter 1, we introduced the diversity gain of an end-to-end connection over an erasure graph as the (decaying) slope of P_E versus p in the logarithmic scale as $p \to 0$. We also stated that this definition is compatible with the concept of diversity gain in the wireless communication literature if $\frac{1}{p}$ is interpreted as the SNR. In this subsection, we accurately define the previously introduced concepts.

Definition 4.10. *Probability of Error*: for an end-to-end connection from s to z with the normalized rate r over T time slots, the probability of error is defined as

$$P_E \triangleq \mathbb{P}\{\hat{m} \neq m\} \stackrel{(a)}{=} \mathbb{P}\{\hat{\mathbf{w}} \neq \mathbf{w}\} \tag{4.9}$$

where $\mathbb{P}\{.\}$ denotes the probability of an event, and (a) follows from the fact that the function $f()$ in (4.2) is one-to-one.

Remark 4.1. For each block, let us define the binary random variable $\mathfrak{E}$, where $\mathfrak{E} = 1$ if $\hat{m} \neq m$, and $\mathfrak{E} = 0$, otherwise. Then, we clearly have $P_E = \mathbb{E}\{\mathfrak{E}\}$. In other words, P_E represents the statistical average of $\mathfrak{E}$ in each block. In case we have a very long data stream composing a large number of blocks, time average of $\mathfrak{E}$ converges to the statistical average of $\mathfrak{E}$ (due to ergodicity). Intuitively speaking, the observed percentage of error converges to the probability of error.

Definition 4.11. *Diversity Gain*: for an end-to-end connection from s to z with the normalized rate r, $\mathfrak{C}(s, z, r)$, we define the diversity gain as

$$d^{\mathfrak{C}} \triangleq \lim_{p \to 0} \lim_{T \to \infty} \frac{\log P_E}{\log p}. \tag{4.10}$$

Definition 4.12. *Optimum Diversity Gain*: for a rate r and end nodes s and z, the optimum diversity gain is defined as the maximum diversity gain over all possible end-to-end connections between s and z with rate r

$$d^{opt}(r) \triangleq \max_{\mathfrak{C}(s,z,r)} d^{\mathfrak{C}}. \tag{4.11}$$

Remark 4.2. We will later show that $d^{opt}(r)$ is a decreasing function of r. More accurately, there is a trade-off between $d^{opt}(r)$ and r.

Definition 4.13. *Maximum Diversity Gain*: for the end nodes s and z, the maximum diversity gain is defined as

$$d^{max} \triangleq \max_{r>0} d^{opt}(r). \tag{4.12}$$

Definition 4.14. *Strategy Factor*: for an end-to-end connection $\mathfrak{C}(s,z,r)$, we define the *strategy factor* as

$$A^{\mathfrak{C}} \triangleq \lim_{p\to 0} \lim_{T\to\infty} \frac{P_E}{p^{d^{\mathfrak{C}}}}. \tag{4.13}$$

Example 4.1. Consider the network of Example 1.1 with the number of links $n = 5$ and rate $r = 3$. The following end-to-end connection is denoted by $\mathfrak{C}(s,z,r)$: every r packets are coded into an MDS code of length n and then transmitted over the n links (as described in Example 1.1). Figure 4.1 depicts the plot of P_E versus $\frac{1}{p}$ in the log-log scale for $\mathfrak{C}(s,z,r)$. $d^{\mathfrak{C}} = 3$ is the slope of the tangential line at $\frac{1}{p} \to \infty$. The strategy factor $A^{\mathfrak{C}}$ can be found at the intersection of this tangential line with the vertical line $\frac{1}{p} = 1$.

4.3 Homogeneous Erasure Graphs

In this section, we analyze the diversity-rate trade-off over erasure graphs with *homogeneous* links defined as follows.

Definition 4.15. An erasure graph $G = (\mathcal{V}, \mathcal{E})$ is called a *Homogeneous Erasure Graph* (HEG) if all the links have the same capacity and the same erasure probability. In other words, $\forall e \in \mathcal{E}$, we have $\sigma(e) = \omega(e) = 1$.

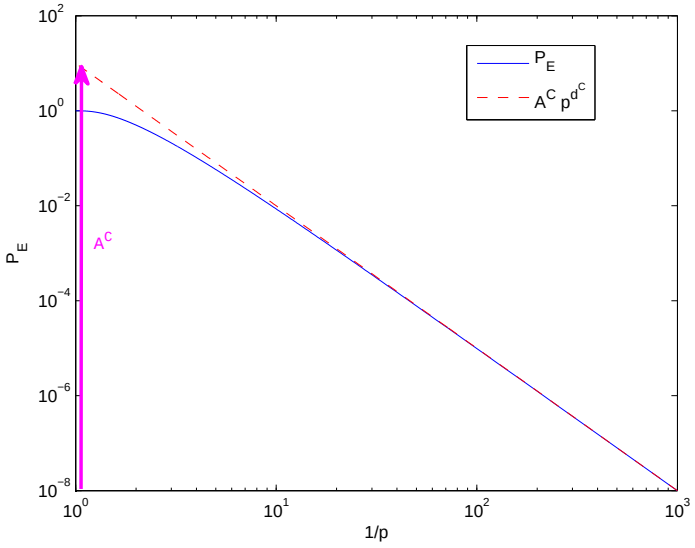


Figure 4.1: P_E vs. $\frac{1}{p}$ in the log-log scale for the network of Fig. 1.1 with $n = 5$ and $r = 3$. The diversity gain is $d^{\mathfrak{C}} = 3$ and the strategy factor $A^{\mathfrak{C}}$ is indicated in the plot.

Remark 4.3. In this work, to keep the analysis simple, we have defined an HEG such that $\sigma(e) = \omega(e) = 1$ for all $e \in \mathcal{E}$. However, the results stay valid (with some scaling factors) if $\forall e \in \mathcal{E}$, we have $\omega(e) = \omega_0$ and $\sigma(e) = \sigma_0$ for some constants ω_0 and σ_0. We can still apply the results of this subsection using the scaled rate $r' = \frac{r}{\sigma_0}$ and substituting p with $p' = p^{\omega_0}$. Thus, the diversity gain $d = \lim_{p\to 0} \frac{\log P_E}{\log p}$ gets scaled by the factor $\frac{1}{\omega_0}$.

Furthermore, we define *deterministic erasure graph* to proceed with our analysis.

Definition 4.16. An erasure graph, in the sense of Definition 4.1, is called deterministic if we have $p = 0$.

Lemma 4.1. *Consider a deterministic erasure graph $G = (\mathcal{V}, \mathcal{E})$ with the end nodes $s \in \mathcal{V}$ and $z \in \mathcal{V} - \{s\}$. If there exists an $s - z$ cutset $\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s, z)$ with $\sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s, z)\right) < r$, then for any end-to-end connection $\mathfrak{C}(s, z, r)$, we have $\lim_{T\to\infty} P_E = 1$.*

Proof See appendix 4.7.1. ■

Lemma 4.2. *In a HEG with the $s - z$ min-cardinality-cut $\mathrm{MCC}(s, z)$, we have*

$$\lim_{T\to\infty} P_E \geq n\left(s, z, \mathrm{MCC}(s, z) - \lceil r \rceil + 1\right) p^{\mathrm{MCC}(s,z)-\lceil r\rceil+1} \left(1 + O(p)\right)$$

for any end-to-end connection $\mathfrak{C}(s,z,r)$*. Here,* $n(s,z,\alpha)$ *denotes the number of sets* $\mathcal{S}\subseteq\mathcal{E}$ *of cardinality* α *such that there exists a* $s-z$ *cut of minimum cardinality,* $\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)$*, for which* $\mathcal{S}\subseteq\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)$*. Thus, we have* $d^{opt}(r)\leq \mathrm{MCC}(s,z)-\lceil r\rceil+1$*.* $\mathrm{MCC}(s,z)$ *is defined in Definition 4.7.*

Proof See appendix 4.7.2. ■

Lemma 4.3. *In a HEG with the* $s-z$ *min-cardinality-cut* $\mathrm{MCC}(s,z)$*, there exist* $\mathrm{MCC}(s,z)$ *link-disjoint paths from* s *to* z*.*

Proof This lemma is direct result of the *Ford-Fulkerson Theorem* and the fact that $\sigma(e)=1$ for $\forall\, e\in\mathcal{E}$ in a HEG. ■

Definition 4.17. *MDS Coding + Disjoint Routing* (MDR): in a HEG with the $s-z$ min-cardinality-cut $\mathrm{MCC}(s,z)$, an MDR end-to-end connection with the integer normalized rate $r\leq\mathrm{MCC}(s,z)$ is defined as follows:

1. At any time slot t, the node s encodes $w_{(t-1)r+1},\ldots,w_{tr}$ to $\mathrm{MCC}(s,z)$ q-ary symbols using an MDS code.
2. Then, s transmits the $\mathrm{MCC}(s,z)$ q-ary symbols along the $\mathrm{MCC}(s,z)$ link-disjoint paths to z, one symbol per path.
3. If r or more symbols are received correctly by z, it can reconstruct $w_{(t-1)r+1},\ldots,w_{tr}$. Otherwise, an error is declared.

For non-integer values of r, an MDR end-to-end connection is achieved by time sharing. s uses an MDR connection with the rate $\lfloor r\rfloor$ for $\lceil r\rceil-r$ percent of the time and an MDR connection with the rate $\lceil r\rceil$ for the rest of time.

Remark 4.4. According to Definition 4.17, it is obvious that MDR is a special case of conventional routing.

Remark 4.5. For any MDS code of size $[n,r]$, we know that the receiver can decode the original r data symbols if out of the n transmitted symbols, at least r of them are received correctly [56].

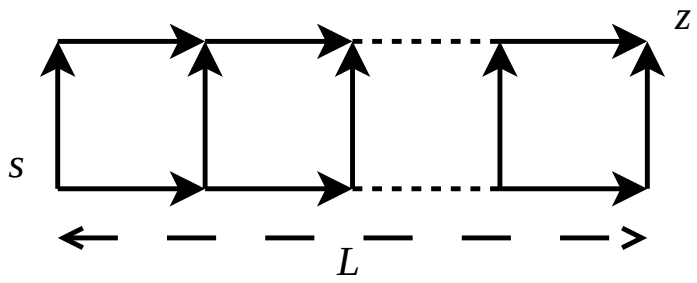


Figure 4.2: Ladder-shaped HEG

Theorem 4.1. *Consider a homogeneous erasure graph $G = (\mathcal{V}, \mathcal{E})$ and a MDS coding+disjoint routing end-to-end connection which transmits messages over* $\mathrm{MCC}(s,z)$ *link-disjoint paths from s to z where* $\mathrm{MCC}(s,z)$ *is the min-cardinality-cut between s and z. Assume the length of the i'th path is l_i, for $1 \leq i \leq \mathrm{MCC}(s,z)$. Then, for every rate $r \geq 0$, the end-to-end connection achieves the diversity gain $d^{MDR} = (\mathrm{MCC}(s,z) - \lceil r \rceil + 1)^+$ and the strategy factor*[3]

$$A^{MDR} = \sum_{\substack{\mathcal{I} \subseteq \mathcal{P} \\ |\mathcal{I}| = d^{MDR}}} \prod_{x \in \mathcal{I}} l_x \tag{4.14}$$

where $\mathcal{P} \triangleq \{1, 2, \ldots, \mathrm{MCC}(s,z)\}$, and we define $x^+ \triangleq \frac{x+|x|}{2}$.

Proof See appendix 4.7.3. ■

Remark 4.6. According to Theorem 4.1, for an MDR end-to-end connection with the normalized rate $r \leq 1$, the strategy factor is equal to $A^{MDR} = \prod_{i=1}^{\mathrm{MCC}(s,z)} l_i$.

Theorem 4.2. *Consider a homogeneous erasure graph $G = (\mathcal{V}, \mathcal{E})$ and a pair of source and destination nodes, $s, z \in \mathcal{V}$. For every rate $r \geq 0$, the optimum diversity gain is equal to $d^{opt}(r) = (\mathrm{MCC}(s,z) - \lceil r \rceil + 1)^+$ where* $\mathrm{MCC}(s,z)$ *is the min-cardinality-cut between s and z and $x^+ \triangleq \frac{x+|x|}{2}$. Furthermore, there exists a MDS coding+disjoint routing end-to-end connection which achieves the optimum diversity-rate trade-off.*

Proof Combining Theorem 4.1 and Lemma 4.2, the proof becomes obvious. ■

[3]Strategy factor is defined in Definition 4.14 in subsection 4.2.5.

Definition 4.18. *Flooding*: an end-to-end connection with the rate $r = 1$ over a HEG is called *flooding* if the following conditions are satisfied:

1. For $\forall\, e \in \mathcal{L}_{out}(s)$ and $1 \leq t \leq T$, we should have $\mathbf{x}_{e,t} = w_t$.
2. For $\forall\, u \in \mathcal{V} - \{s, z\}$ and $\forall\, e \in \mathcal{L}_{out}(u)$ and $1 \leq t \leq T$, we should have

$$\mathbf{x}_{e,t} = \begin{cases} 0 & \text{if } \mathcal{X} \subseteq \{0, \xi\} \\ w_t & \text{otherwise} \end{cases} \tag{4.15}$$

where $\mathcal{X}$ is the set of all elements in the t'th column of $\mathbf{Y}_{u,t}$, i.e. all of the symbols u has received in at time slot t. The matrix $\mathbf{Y}_{u,t}$ is defined in (4.4). Since in each time slot t only one symbol w_t is being broadcast, it is easy to verify that $\mathcal{X}$ can consist of at most 3 elements: 0, ξ, and w_t. The above equation simply states that if $w_t \in \mathcal{X}$, the node broadcasts it at all of the outgoing edges. Otherwise, it broadcasts 0.

Intuitively speaking, flooding works by each intermediate node broadcasting the same packet on all of the outgoing links.

Theorem 4.3. *Consider a homogeneous erasure graph $G = (\mathcal{V}, \mathcal{E})$ and a pair of source and destination nodes, $s, z \in \mathcal{V}$. A flooding end-to-end connection from s to z achieves the maximum diversity gain $d^{fl} = d^{max} = \mathrm{MCC}(s, z)$ with the minimum possible strategy factor of $A^{fl} = N(s, z)$ where $N(s, z)$ is the number of min-cardinality-cuts between s and z.*

Proof See appendix 4.7.4. ■

Example 4.2. *Ladder Grid*: consider the ladder-shaped HEG of Fig. 4.2. Clearly, we have $\mathrm{MCC}(s, z) = 2$ in this graph. An MDR end-to-end connection with the rate $r = 1$ consists of two disjoint paths from s to z. Each path has the length of $L+1$ links. Thus, according to Theorem 4.1 and Remark 4.6, such an MDR end-to-end connection has the diversity gain of $d^{MDR} = 2$ and the strategy factor of $A^{MDR} = (L+1)^2$.

On the other hand, flooding provides us with the same diversity gain, $d^{fl} = 2$, and a better (lower) strategy factor. According to Theorem 4.3, $A^{fl} = N(s, z)$ where $N(s, z)$ denotes the number of min-cardinality-cuts between s and z. In the graph of Fig. 4.2, there are $L + 2$ cuts of cardinality 2. L of them correspond to the L steps on the ladder.

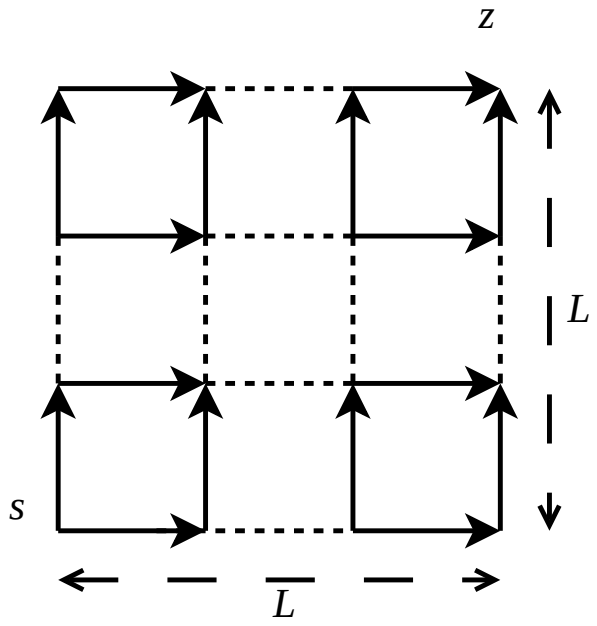


Figure 4.3: Square-shaped HEG

The last two cuts disconnect the end point (s and z) from the rest of the graph. Hence, we have $A^{fl} = N(s,z) = L+2$ which is much less than $A^{MDR} = (L+1)^2$.

Example 4.3. *Square Grid*: consider the square-shaped HEG of Fig. 4.3. Again, we have $\mathrm{MCC}(s,z) = 2$ in this graph. Any MDR end-to-end connection with the rate $r = 1$ consists of two paths of length $2L$ links each. Thus, according to Theorem 4.1 and Remark 4.6, it has the diversity gain of $d^{MDR} = 2$ and the strategy factor of $A^{MDR} = 4L^2$. Flooding provides us with the same diversity gain, $d^{fl} = 2$, and a much better (lower) strategy factor, $A^{fl} = 2$. The reason is that there are only two cuts of cardinality 2 in the graph, the ones disconnecting s and z from the rest of the graph.

4.4 General Erasure Graphs

In this section, we analyze the diversity-rate trade-off for the general erasure graphs, meaning that $\sigma(e)$'s and $\omega(e)$'s can take different values. As we will observe, in the general case, conventional routing fails to achieve the optimum diversity-rate trade-off. However, we show that linear network coding in the intermediate nodes can achieve the optimum

diversity-rate trade-off. First, we define the following notations.

Definition 4.19. Consider an erasure graph $G = (\mathcal{V}, \mathcal{E})$. For a pair of end nodes $s, z \in \mathcal{V}$ and any value of $d \geq 0$, $\tilde{r}(d)$ is defined as the minimum value of $\mathrm{MC}(s, z)$ over all graphs $G' = (\mathcal{V}, \mathcal{E}')$ such that $\mathcal{E}' \subseteq \mathcal{E}$ and $\omega(\mathcal{E} - \mathcal{E}') \leq d$. Equivalently,

$$\tilde{r}(d) = \min_{\mathcal{V}_1, \mathcal{V}_2} \min_{\substack{\mathcal{S} \subseteq \mathcal{C}_{\mathcal{V}_1, \mathcal{V}_2}(s,z) \\ \omega(\mathcal{S}) \leq d}} \sigma\left(\mathcal{C}_{\mathcal{V}_1, \mathcal{V}_2}(s, z) - \mathcal{S}\right), \tag{4.16}$$

where $\mathcal{C}_{\mathcal{V}_1, \mathcal{V}_2}(s, z)$ is an $s - z$ cutset in G, such that $\mathcal{V}_1, \mathcal{V}_2 \subset \mathcal{V}; s \in \mathcal{V}_1; z \in \mathcal{V}_2; \mathcal{V}_1 \bigcap \mathcal{V}_2 = \emptyset$.

Definition 4.20. Consider an erasure graph $G = (\mathcal{V}, \mathcal{E})$. For a pair of end nodes $s, z \in \mathcal{V}$ and any rate $r \geq 0$, $d^\star(r)$ is defined as

$$d^\star(r) \triangleq \min_{d \geq 0, r > \tilde{r}(d)} d,$$

Lemma 4.4. *$\tilde{r}(d)$ and $d^\star(r)$ are both decreasing functions.*

Proof See appendix 4.7.5. ■

Lemma 4.5. *Consider an erasure graph $G = (\mathcal{V}, \mathcal{E})$ and a pair of end nodes $s, z \in \mathcal{V}$. For any end-to-end connection $\mathfrak{C}(s, z, r)$ with rate $r \geq 0$, we have $\lim_{T \to \infty} P_E \geq p^d$ if $r > \tilde{r}(d)$. Equivalently, we have $\lim_{T \to \infty} P_E \geq p^{d^\star(r)}$.*

Proof See appendix 4.7.6. ■

Lemma 4.6. *Consider an erasure graph $G = (\mathcal{V}, \mathcal{E})$, end nodes $s, z \in \mathcal{V}$, $d \geq 0$, and any rate $r \leq \tilde{r}(d)$. The symbols transmitted on the links of G are assumed to be in $\mathbb{F}_q$ as explained in Definition 4.3. Let $\mathcal{E}_{\mathrm{OFF}}$ denote the set of OFF edges. For sufficiently large values of q, there exists a linear network coding[4] strategy $\mathfrak{C}^{NC}(s, z, r)$ such that $\mathbb{P}\left\{error | \omega\left(\mathcal{E}_{\mathrm{OFF}}\right) \leq d\right\} = 0$.*

Proof See appendix 4.7.7. ■

[4]Linear network coding is defined in Definition 4.9.

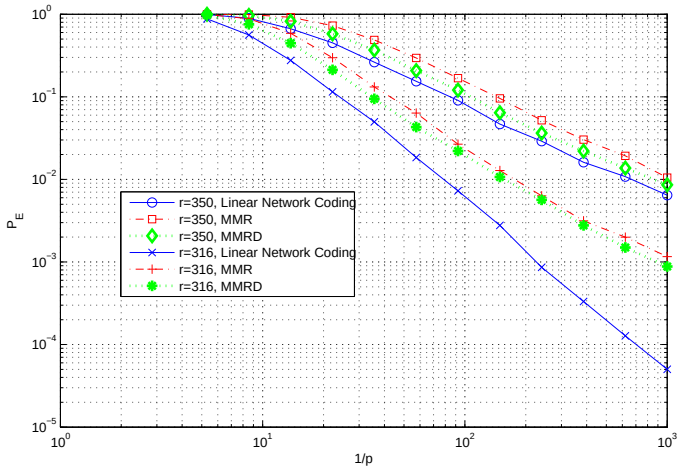


Figure 4.4: P_E of linear network coding, MDS Max-Flow Routing (MMR), and MDS Max-Flow Routing with Detours (MMRD) vs. $\frac{1}{p}$ in logarithmic scale for different rates $r = 350$ and $r = 316$. The network parameters are $|\mathcal{V}| = 40$, $m = 5$, and $10 < \sigma(e) < 100$.

Theorem 4.4. *Consider a general erasure graph $G = (\mathcal{V}, \mathcal{E})$ and a pair of end nodes $s, z \in \mathcal{V}$. The symbols transmitted on the links of G are assumed to be in $\mathbb{F}_q$ as explained in Definition 4.3. For sufficiently large values of q, there exists a linear network coding end-to-end connection which achieves the optimum diversity-rate trade-off. Moreover, the optimum diversity-rate trade-off is equal to $d^\star(r)$ as defined in Definition 4.20.*

Proof See appendix 4.7.8. ■

Theorem 4.5. *There exists an erasure graph $G = (\mathcal{V}, \mathcal{E})$ and end nodes $s, z \in \mathcal{V}$ such that no conventional routing end-to-end connection from s to z can achieve the optimum diversity-rate trade-off, $d^\star(r)$. Conventional routing is defined in Definition 4.8.*

Proof See appendix 4.7.9.

Remark 4.7. Theorem 4.5 shows a sharp distinction between HEG's and general erasure graphs. In a HEG, according to Theorem 4.1, it is possible to achieve the optimum diversity gain for any rate using conventional routing (MDS Coding + Disjoint Routing). On the other hand, in the general erasure graphs, there are cases where any conventional routing strategy fails to achieve the optimum diversity gain. In such cases, the intermediate nodes

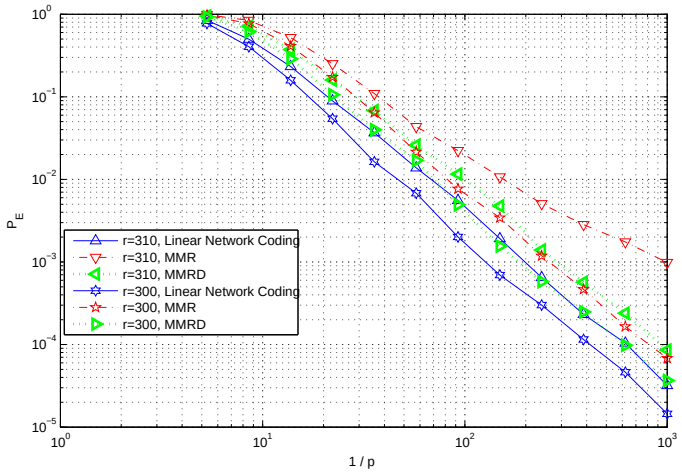


Figure 4.5: P_E of linear network coding, MDS Max-Flow Routing (MMR), and MDS Max-Flow Routing with Detours (MMRD) vs. $\frac{1}{p}$ in logarithmic scale for different rates $r = 310$ and $r = 300$. The network parameters are $|\mathcal{V}| = 40$, $m = 5$, and $10 < \sigma(e) < 100$.

have to perform algebraic operation (instead of simple forwarding) on the incoming symbols (packets) to achieve $d^{opt}(r)$.

4.5 Numerical Results

This section utilizes numerical evaluation to compare the performance of linear network coding and conventional routing over erasure networks with random topologies. The network topology is generated based on the random models explained in the next subsection.

4.5.1 Network Topology

To model the topology of practical networks realistically, we use the well-known Boston university Representative Internet Topology gEnerator (BRITE) [132, 133]. BRITE has the ability to construct random network topologies based on the Barabasi-Albert (BA) model [134] and Waxman model [135]. The BA model is able to capture the scale-free and power-law degree distribution phenomena which are observed in many networks like the IP routers, World Wide Web, social networks (Facebook, Orkut), scientific paper citations, etc [136]. This model is based on two principles: incremental growth and preferential

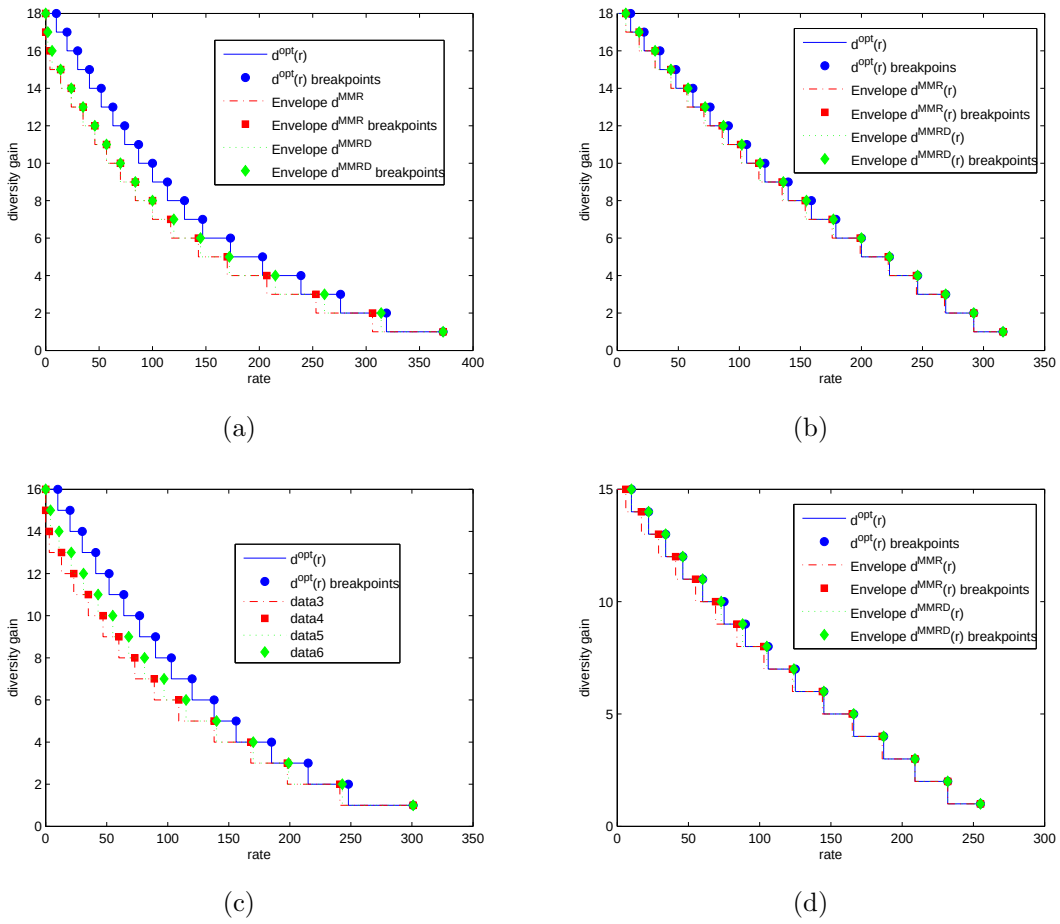


Figure 4.6: $d^{opt}(r)$ is compared with the envelope of MMR and MMRD diversity gain for 100 random routing schemes. MMR and MMRD stand for MDS Max-Flow Routing and MDS Max-Flow Routing with Detours, respectively (see subsection 4.5.2). Subfigures (a) to (d) correspond to the four network topologies described in subsection 4.5.1. The topologies are generated based on the BA model.

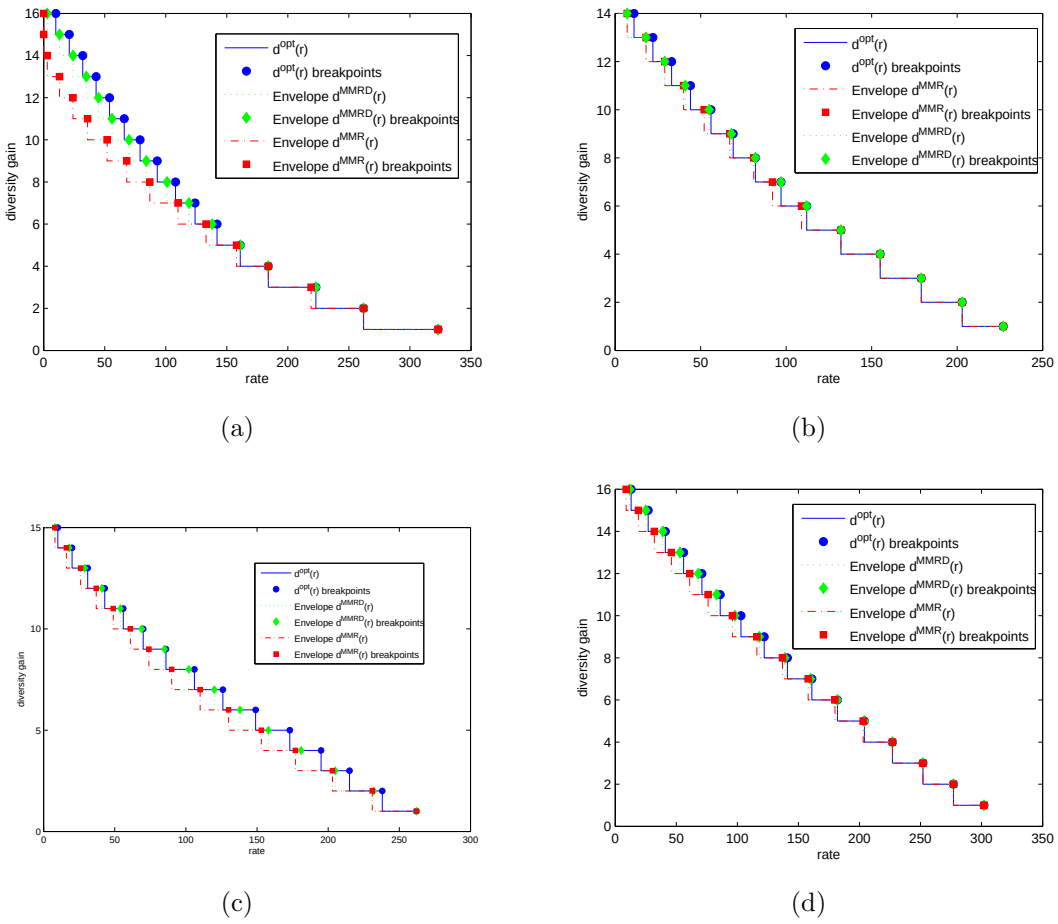


Figure 4.7: $d^{opt}(r)$ is compared with the envelope of MMR and MMRD diversity gain for 100 random routing schemes. MMR and MMRD stand for MDS Max-Flow Routing and MDS Max-Flow Routing with Detours, respectively (see subsection 4.5.2). Subfigures (a) to (d) correspond to the four network topologies described in subsection 4.5.1. The topologies are generated based on Waxman model.

connectivity [134]. The BRITE topology generator identifies the BA model with two parameters: the number of nodes ($|\mathcal{V}|$) and the connectivity parameter m. During the incremental growth phase, once a new node joins the network, it selects m old nodes and connects to them. Due to the principle of preferential connectivity, the old nodes which already have higher degrees are more likely to be selected. In other words, the probability that an old node is selected by the new node is proportional to its degree [134].

The number of edges in a random graph with $|\mathcal{V}|$ nodes generated by the BA model can be computed as follows. The first node has no other nodes to connect to and forms zero new links. The second node forms one new link. Similarly, for $1 \leq i \leq m$, the i'th node added to the network forms $i-1$ new links. The nodes after the m'th node each form exactly m new links. Adding all of the links together gives us the total number of edges $|\mathcal{E}| = m|\mathcal{V}| - \frac{m(m+1)}{2}$.

On the other hand, Waxman model is based on the simple assumption that two close nodes are exponentially more likely to connect (and form a link) than two far apart nodes [135]. This property is called *local preference*. In the original Waxman model [135], the nodes are uniformly distributed in a square of size $Z_1 \times Z_2$. The probability that two nodes u and v with the distance $l(u,v)$ of each other are connected is equal to $P(u,v) = \alpha e^{-\frac{l(u,v)}{\beta Z}}$ where $Z = \sqrt{Z_1^2 + Z_2^2}$ is the largest Euclidean distance between any two points in the area. The parameter α controls the total number of edges in the graph, while β determines the ratio of long edges to the short ones. Unfortunately, according to this model, the average degree of a node grows infinitely large as the total number of nodes in the graph ($|\mathcal{V}|$) grows. This trend is in contrast with the observations in most practical networks like the Internet where the average degree stays limited as the network grows [137]. Therefore, BRITE applies a variation of Waxman model in which each node connects to m other nodes. Thus, the number of edges would be $|\mathcal{E}| = m|\mathcal{V}|$. When adding a link whose tail is the node u_i, there are $|\mathcal{V}| - 1$ candidates for the head. Modified Waxman model picks the closer nodes with higher probability, i.e. the probability of u_j being selected is [138]

$$P(u_i, u_j) = \frac{e^{-\frac{l(u_i,u_j)}{\beta Z}}}{\sum_{j'=1, j' \neq i}^{j'=|\mathcal{V}|} e^{-\frac{l(u_i,u_{j'})}{\beta Z}}}.$$

Unlike the BA model, Waxman model results in a degree distribution which decays exponentially at large degrees [139]. Although this is in contrast with the scale-free property

observed in the Internet [136], Waxman model is widely used to generate small-size networks due to its simplicity and local preference property [140]. We apply the modified Waxman model with $\beta = 0.2$ (the default value in BRITE software [138]).

As stated, the BA model emulates the behavior of the real networks in the asymptotic case where the number of nodes (and edges) in the graph is very large [136]. However, due to the high complexity of computing $d^{opt}(r)$, we do not grow the number of nodes more than ≈ 50 and the number of edges more than ≈ 250 in the simulations. Therefore, we also test graphs constructed based on the Waxman model which is more suitable for small-size networks.

BRITE topology generator assigns a random capacity value $\sigma(e)$ to any edge $e \in \mathcal{E}$. $\sigma(e)$ follows the heavy-tailed Pareto distribution [141] with the shape factor $\gamma = 1.2$ (the default value in BRITE software [138]), the minimum value set at BW_{min}, and the maximum at BW_{max}. $\omega(e)$ is set to one for all $e \in \mathcal{E}$, i.e. each link in the graph may be OFF with the probability p. We run the simulations for 4 BA topologies and 4 Waxman topologies:

- (a) $|\mathcal{V}| = 40$, $m = 5$, and $10 < \sigma(e) < 100$,
- (b) $|\mathcal{V}| = 40$, $m = 5$, and $10 < \sigma(e) < 15$,
- (c) $|\mathcal{V}| = 30$, $m = 4$, and $10 < \sigma(e) < 100$,
- (d) $|\mathcal{V}| = 30$, $m = 4$, and $10 < \sigma(e) < 15$.

As explained before, the number of nodes and edges in the network is kept small due to high complexity of computing $d^{opt}(r)$. The reason we adopted the connectivity parameter m equal to 4 or 5 is that for smaller values of m, the network becomes too sparse (and in some cases unconnected). Even if the network stays connected, the min-cut (bottleneck) between most of source-destination pairs is composed of the edges connecting one of the end-nodes to the rest of the network. In such cases, there is not much of difference between the performance of conventional routing and linear network coding.

The distribution of the links's capacity ($\sigma(e)$) is selected such that networks (a) and (c) become *very heterogeneous*, in the sense that capacity of their links vary significantly. On the other hand, networks (b) and (d) can be viewed as *almost-homogeneous* erasure networks. The reason is that capacity of the links in these graphs do not vary significantly.

4.5.2 Random Routing vs. Linear Network Coding

To have a fair comparison between conventional routing and linear network coding, we measure the performance of three different end-to-end connections:

- Linear Network Coding: according to theorem 4.4, we know that there exists at least one linear network coding scheme which achieves the maximum diversity gain for any rate r, denoted by $d^{opt}(r)$.

- MDS Max-Flow Routing (MMR): for any $0 < r < \mathrm{MC}(s, z)$, the source node, s, encodes every r symbols (packets) into $\mathrm{MC}(s, z)$ symbols using an MDS code. Then, we find a flow with the rate of $\mathrm{MC}(s, z)$ (max-flow) from s to the destination, z. Finally, the state of each link is set to $\{\mathrm{ON,OFF}\}$ with the probabilities $\{1-p, p\}$. If less than r symbols reach the destination, an error is declared.

- MDS Max-Flow Routing with Detours (MMRD): this scheme is exactly the same as MMR, except that the max-flow found by MMR is *enhanced* by adding random extra detours to the path of each symbol from s to z. This is done until all links are saturated and no detour can be found.

It is easily seen that both MMR and MMRD schemes can be categorized as conventional routing end-to-end connections. Intuitively speaking, we expect MMRD to have a better performance than MMR ($d^{MMRD}(r) > d^{MMR}(r)$). The reason is that MMRD takes advantage of the unused links in the graph to send extra copies of the symbols to the destination. This increases resilience of the end-to-end connection to link breakdowns.

The last two schemes have a random nature. Therefore, we generate up to 100 MMR and MMRD schemes. Then for each rate, we select the MMR and MMRD schemes with maximum diversity gain. This gives us the *envelope* of $d^{MMR}(r)$ and $d^{MMRD}(r)$. Our simulation results show little variation in the the diversity gains of 100 randomly generated MMR (and MMRD) schemes for each rate. In the cases where more than 100 (say 1000) random MMR and MMRD schemes were generated, the maximum diversity gain of MMR and MMRD schemes for each rate (envelope of $d^{MMR}(r)$ and $d^{MMRD}(r)$) did not change. Therefore, there is no need to test more than 100 MMR and MMRD schemes.

Figure 4.4 and Fig. 4.5 depict P_E of linear network coding, MMR, and MMRD versus $\frac{1}{p}$ for different rates over the BA network with topology (a) described in the previous subsection. The graph has the max-flow of $\mathrm{MC}(s, z) = 372$. The diversity gains can be computed

based on the decaying slope of P_E vs. $\frac{1}{p}$ (in logarithmic scale). It is observed that the slope increases as the rate decreases. Moreover, the diversity gain (slope) of linear network coding is always larger than or equal to that of conventional routing (MMR and MMRD) for the same rate. Figure 4.6 compares $d^{opt}(r)$ with the envelope of MMR and MMRD diversity gain ($d^{MMR}(r)$ and $d^{MMRD}(r)$) for 100 random routing schemes. Subfigures (a) to (d) correspond to the four network topologies described in the previous subsection. All of the topologies are generated based on the BA model. In all cases, the diversity gains take integer values only and have stepwise shapes. This is an obvious result of the assumption that $\omega(e) = 1$ for all $e \in \mathcal{E}$. Comparing subfigure (a) with (b) and (c) with (d) reveals that the gap between $d^{opt}(r)$ and conventional routing diversity gain ($d^{MMR}(r)$ and $d^{MMRD}(r)$) is significantly smaller in almost-homogeneous networks (graphs (b) and (d)). In both almost-homogeneous networks (graphs (b) and (d)), the envelope of $d^{MMRD}(r)$ is barely distinguishable from $d^{opt}(r)$ (optimal diversity gain) at all rates. This observation verifies Theorem 4.2 which states that proper conventional routing can achieve the optimum diversity-rate trade-off in homogeneous erasure networks. In topologies (a) and (c), however, the envelope of $d^{MMRD}(r)$ stays considerably smaller than $d^{opt}(r)$. The reason is that in such cases, the capacity of different links vary significantly, and conventional routing fails to achieve the optimum diversity-rate trade-off.

Figure 4.7 depicts $d^{opt}(r)$ and the envelope of MMR and MMRD diversity gain for the scenarios (a) to (d) with the Waxman model. It is observed that the general trend is similar to Fig. 4.6 (the BA model), i.e. the gap between $d^{opt}(r)$ and $d^{MMRD}(r)$ is significantly larger in heterogeneous networks (subfigures (a) and (c)) than in the almost-homogeneous ones (subfigures (b) and (d)). However, this gap is slightly smaller in subfigures 4.7(a) and 4.7(c) than in subfigures 4.6(a) and 4.6(c). This observation can be attributed to the fact that in the BA model, the degree distribution is more non-uniform than in the Waxman model. In other words, a small percentage of the nodes are highly connected, while the rest of the nodes have low connectivity. Therefore, the advantage of linear network coding over conventional routing is more significant in the BA model.

4.6 Conclusion

We have studied a fundamental trade-off between rate and diversity gain over an erasure network. The erasure network is modeled as a directed acyclic graph whose links are

orthogonal erasure channels. The erasure status of the links is assumed to be known only by the destination node. First, we focused on the homogeneous erasure networks whose links have the same erasure probability and capacity. The optimum diversity-rate trade-off was derived for homogeneous erasure networks and was shown to be achievable by MDS coding at the source node and disjoint routing in the intermediate nodes (a variant of conventional routing). Next, we analyzed the general erasure networks whose links may have different capacity and erasure probability values. It was proved that in general erasure graphs, conventional routing strategies fail to achieve the optimum diversity-rate trade-off. However, the optimum trade-off is always achievable by linear network coding. Finally, we studied the diversity-rate trade-off through simulations over graphs constructed based on the Barabasi-Albert and Waxman random models. The diversity gain of linear network coding strategy was plotted versus the rate and was compared with that of different conventional routing schemes. It was observed that linear network coding outperforms all conventional routing strategies in terms of the diversity gain.

4.7 Appendices

4.7.1 Proof of Lemma 4.1

Let us denote the vector of symbols transmitted on the cut edges by $\mathbf{x}(\mathcal{C})$. Then $\mathbf{w} \leftrightarrow \mathbf{x}(\mathcal{C}) \leftrightarrow \hat{\mathbf{w}}$ form a Markov chain. Thus, the capacity of the end-to-end-channel from s to z can be bounded as

$$\begin{aligned} C &= \lim_{T\to\infty} \frac{1}{T}\, I(\mathbf{w};\hat{\mathbf{w}}) \\ &\overset{(a)}{\leq} \lim_{T\to\infty} \frac{1}{T}\, I(\mathbf{w};\mathbf{x}(\mathcal{C})) \\ &\leq \lim_{T\to\infty} \frac{1}{T}\, H(\mathbf{x}(\mathcal{C})) \\ &\overset{(b)}{\leq} \lim_{T\to\infty} \frac{1}{T}\, \log_2 q^{T\sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)\right)} \\ &= \sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)\right) \log_2 q \\ &< r \log_2 q \end{aligned}$$

where (a) follows from the data processing inequality and (b) from the fact that $\mathbf{x}(\mathcal{C})$ takes at most $q^{T\sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)\right)}$ different values. $r\log_2 q$ equals the non-normalized end-to-end rate in bits. Using the strong version of the converse of the *noisy channel (Shannon) theorem*, we know that $\lim_{T\to\infty} P_E = 1$ for rates above the capacity. This proves the lemma. ■

4.7.2 Proof of Lemma 4.2

Let us denote all the $s-z$ cutsets with the minimum cardinality as $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{N(s,z)}$. Furthermore, we define $\mathcal{E}_{\mathcal{S}}$ as the event[5] that the edges in the subset $\mathcal{S} \subseteq \mathcal{E}$ are OFF and $\alpha \triangleq \mathrm{MCC}(s,z) - \lceil r \rceil + 1$. Then, $\lim_{T\to\infty} P_E$ can be lower-bounded as

$$\begin{aligned}
\lim_{T\to\infty} P_E &\geq \lim_{T\to\infty} \mathbb{P}\left\{ \text{error} \bigcap \left(\bigcup_i \bigcup_{\substack{\mathcal{S}\subseteq\mathcal{C}_i \\ |\mathcal{S}|=\alpha}} \mathcal{E}_{\mathcal{S}} \right) \right\} \\
&= \lim_{T\to\infty} \mathbb{P}\left\{ \bigcup_{\substack{\mathcal{S},|\mathcal{S}|=\alpha \\ \exists i:\mathcal{S}\subseteq\mathcal{C}_i}} \left(\text{error} \bigcap \mathcal{E}_{\mathcal{S}} \right) \right\}
\end{aligned}$$

$$\begin{aligned}
&\overset{(a)}{\geq} \lim_{T\to\infty} \sum_{\substack{\mathcal{S},|\mathcal{S}|=\alpha \\ \exists i:\mathcal{S}\subseteq\mathcal{C}_i}} \mathbb{P}\left\{\mathcal{E}_{\mathcal{S}}\right\} \mathbb{P}\left\{\text{error } | \mathcal{E}_{\mathcal{S}}\right\} - \\
&\quad \sum_{\substack{\mathcal{S}\neq\mathcal{S}',|\mathcal{S}|=|\mathcal{S}'|=\alpha, \\ \exists i,j:\mathcal{S}\subseteq\mathcal{C}_i,\mathcal{S}'\subseteq\mathcal{C}_j}} \mathbb{P}\left\{\mathcal{E}_{\mathcal{S}}\cap\mathcal{E}_{\mathcal{S}'}\right\} \mathbb{P}\left\{\text{error } | \mathcal{E}_{\mathcal{S}}\cap\mathcal{E}_{\mathcal{S}'}\right\} \\
&\overset{(b)}{\geq} n(s,z,\alpha)p^{\alpha} - N(s,z)^2 \binom{MCC(s,z)}{\alpha}^2 p^{\alpha+1} \\
&= n(s,z,\alpha)p^{\alpha}\left(1+O(p)\right). \qquad (4.17)
\end{aligned}$$

Here, (a) follows from the principle of inclusion-exclusion [142] and (b) follows from i) Lemma 4.1, ii) the facts that $\mathbb{P}\left\{\mathcal{E}_{\mathcal{S}}\right\} = p^{\alpha}$ and $\mathbb{P}\left\{\mathcal{E}_{\mathcal{S}}\cap\mathcal{E}_{\mathcal{S}'}\right\} \leq p^{\alpha+1}$, and iii) the fact that the number of subsets $\mathcal{S}$ for which we have $\exists i : \mathcal{S}\subseteq\mathcal{C}_i$, can be upper-bounded by $N(s,z)\binom{MCC(s,z)}{\alpha}$. Therefore, for any end-to-end connection $\mathfrak{C}(s,z,r)$, the above inequality

[5] In the axiomatic probability theory, an event is interpreted as a set. Thus, following the convention of this thesis, we denote all events by calligraphic letters.

results in $d^{\mathfrak{C}} \leq \mathrm{MCC}(s,z) - \lceil r \rceil + 1$. ■

4.7.3 Proof of Theorem 4.1

First, let us prove the theorem for integer values of r. A path from s to z is called *broken* if at least one of the links in the path is OFF. For each i, $i \in \mathcal{P}$, the probability of path i being broken is $p_i = 1-(1-p)^{l_i}$, where l_i is the number of links the path consists of. It is easy to see that $p_i = l_i p(1+O(p))$. In an MDR end-to-end connection with the normalized rate r, the r packets at the source are coded into $\mathrm{MCC}(s,z)$ packets using an MDS block code of size $[\mathrm{MCC}(s,z), r]$. An error occurs iff more than $\mathrm{MCC}(s,z)-r$ packets are lost. This is equivalent of $\mathrm{MCC}(s,z)-r+1$ or more paths being broken (out of the total $\mathrm{MCC}(s,z)$ paths). Therefore, P_E can be written as

$$\begin{aligned} P_E &= \sum_{d=\mathrm{MCC}(s,z)-r+1}^{\mathrm{MCC}(s,z)} \sum_{\substack{\mathcal{I}\subseteq\mathcal{P} \\ |\mathcal{I}|=d}} \prod_{x\in\mathcal{I}} p_x \\ &= \sum_{d=\mathrm{MCC}(s,z)-r+1}^{\mathrm{MCC}(s,z)} \sum_{\substack{\mathcal{I}\subseteq\mathcal{P} \\ |\mathcal{I}|=d}} p^d(1+O(p)) \prod_{x\in\mathcal{I}} l_x \\ &= p^{\mathrm{MCC}(s,z)-r+1}(1+O(p)) \sum_{\substack{\mathcal{I}\subseteq\mathcal{P} \\ |\mathcal{I}|=\mathrm{MCC}(s,z)-r+1}} \prod_{x\in\mathcal{I}} l_x. \end{aligned}$$

The above result proves the theorem for integer values of r.

As explained in Definition 4.17, non-integer rates are achieved by time sharing between two MDR connection of rates $\lceil r \rceil$ and $\lfloor r \rfloor$. According to the above result, it can be seen that the diversity gain corresponding to the higher rate ($\lceil r \rceil$) is smaller and therefore dominates. Hence, the overall diversity gain and strategy factor are identical to those of a connection with the rate $\lceil r \rceil$. This completes the proof. ■

4.7.4 Proof of Theorem 4.3

A cutset is called *broken* if all of the links in the cutset are OFF. Let us denote $\mathcal{E}_i$ as the event where the i'th $s-z$ cutset of minimum cardinality is broken, $1 \leq i \leq N(s,z)$.

Obviously, an error occurs *iff* at least one of the cutsets is broken. Hence, we have

$$\begin{aligned} P_E &= \mathbb{P}\left\{\bigcup_{i=1}^{n(s,z)} \mathcal{E}_i\right\} \\ &\leq \sum_{i=1}^{n(s,z)} \mathbb{P}\left\{\mathcal{E}_i\right\} \\ &= N(s,z)p^{\mathrm{MCC}(s,z)}. \end{aligned} \tag{4.18}$$

On the other hand, from Lemma 4.2, we know that $\lim_{T\to\infty} P_E \geq n(s,z,\mathrm{MCC}(s,z))p^{\mathrm{MCC}(s,z)}$. According to the definition, we conclude that $n(s,z,\mathrm{MCC}(s,z)) = N(s,z)$. Hence, the flooding end-to-end connection achieves the optimum diversity gain of $\mathrm{MCC}(s,z)$ and the minimum strategy factor of $N(s,z)$. This completes the proof. ■

4.7.5 Proof of Lemma 4.4

Let us consider $d \leq d'$. We have

$$\begin{aligned} \tilde{r}(d) &= \min_{\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)} \min_{\substack{\mathcal{S}\subseteq\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) \\ \omega(\mathcal{S})\leq d}} \sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) - \mathcal{S}\right) \\ &\geq \min_{\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)} \min_{\substack{\mathcal{S}\subseteq\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) \\ \omega(\mathcal{S})\leq d'}} \sigma\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) - \mathcal{S}\right) = \tilde{r}(d'), \end{aligned} \tag{4.19}$$

where $\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)$ is defined in Definition 4.6. This proves that $\tilde{r}(d)$ is decreasing.

Next, let us consider $r \leq r'$. We have

$$\begin{aligned} d^\star(r) &= \min_{d\geq 0, r>\tilde{r}(d)} d \\ &\geq \min_{d\geq 0, r'>\tilde{r}(d)} d = d^\star(r'). \end{aligned} \tag{4.20}$$

This proves that $\tilde{r}(d)$ is decreasing with respect to d. ■

4.7.6 Proof of Lemma 4.5

Let us consider a value of d such that $r > \tilde{r}(d)$. According to the definition, there exists a set $\mathcal{E}' \subseteq \mathcal{E}$ such that $\omega(\mathcal{E} - \mathcal{E}') \leq d$ and $\mathrm{MC}(s,z) = \tilde{r}(d) < r$ over the graph $G' = (\mathcal{V}, \mathcal{E}')$.

Furthermore, let us define $\mathcal{D}$ as the event where all edges in $\mathcal{E}-\mathcal{E}'$ are OFF. Then, we have

$$\begin{aligned}\lim_{T\to\infty} P_E &\geq \lim_{T\to\infty} \mathbb{P}\{\text{error } \cap \mathcal{D}\} \\ &= \lim_{T\to\infty} \mathbb{P}\{\text{error } |\mathcal{D}\}\mathbb{P}\{\mathcal{D}\} \\ &\overset{(a)}{=} \mathbb{P}\{\mathcal{D}\} = p^{\omega(\mathcal{E}-\mathcal{E}')} \geq p^{d} \end{aligned} \tag{4.21}$$

where (a) follows from Lemma 4.1 and the fact that $\mathrm{MC}(s,z) < r$ for the graph G'.

Next, we prove $\lim_{T\to\infty} P_E \geq p^{d^\star(r)}$. According to Definition 4.20, it is obvious that $r > \tilde{r}(d^\star(r))$. Thus, setting $d = d^\star(r)$ in (4.21) proves the lemma. ■

4.7.7 Proof of Lemma 4.6

Sketch of the Proof: the proof is similar to the proof for capacity achievability of linear network coding presented in [61]. Here, we have to show that there exists a linear network code such that for any subgraph $\hat{G} = (\mathcal{V}, \hat{\mathcal{E}})$ of G for which $\omega\left(\mathcal{E}-\hat{\mathcal{E}}\right) \leq d$, it achieves the deterministic capacity of $\hat{G}$. To ensure this, we have to consider the multi-variate polynomial obtained by multiplying the determinant of the transfer matrices corresponding to each subgraph $\hat{G}$ and show that providing a Galois Field $\mathbb{F}_q$ large enough, the corresponding multi-variate polynomial is not equal to zero. This method is very similar to the algebraic anlaysis of network coding in [61, 63].

Proof: let us consider an arbitrary labeling $\ell : \{1, 2, \ldots, \sigma(\mathcal{E})\} \to \mathcal{E}$ such that for every edge e, we have $|\{x\,|\ell(x) = e\}| = \sigma(e)$. Now, we define the multivariate matrix $\mathbf{F}$ of size $\sigma(\mathcal{E}) \times \sigma(\mathcal{E})$ over $\mathbb{F}_q$ as follows. For any $1 \leq i, j \leq \sigma(\mathcal{E})$, we have $F_{i,j} = 0$ if $h(\ell(j)) \neq \tau(\ell(i))$. Otherwise, $F_{i,j} = \beta_{i,j}$ where $\beta_{i,j}$ is a variable in $\mathbb{F}_q$. $\beta_{i,j}$ denotes the coefficient used at the node $h(\ell(j))$ to compute the effect of the corresponding input symbol over $\ell(j)$ on the corresponding output symbol over $\ell(i)$. Hence, for any two edges e, e' with $h(e') = \tau(e)$, every realization of $\{\beta_{i,j}\}_{\ell(i)=e,\ell(j)=e'}$ corresponds to $\mathbf{B}_{e,e'}$ defined in Definition 4.9. Accordingly, every realization of the multivariate matrix $\mathbf{F}$ determines the linear network operations in all intermediate nodes.

Similarly, we define the multivariate matrices $\mathbf{A}$ and $\mathbf{C}$ over $\mathbb{F}_q$ with sizes $r \times \sigma(\mathcal{E})$ and $\sigma(\mathcal{E}) \times r$, respectively. $\mathbf{A}$ and $\mathbf{C}$ correspond to the linear network operations performed at the destination and source nodes, respectively. More precisely, $\mathbf{A}_{i,j} = 0$ if $h(\ell(j)) \neq z$.

Otherwise, $\mathbf{A}_{i,j} = \alpha_{i,j}$ where $\alpha_{i,j}$ is a variable in $\mathbb{F}_q$ denoting the coefficient used at the destination node to compute the effect of the corresponding input symbol over edge $\ell(j)$ on the i'th element of the output vector, $\mathbf{y}^t$. Similarly, $\mathbf{C}_{i,j} = 0$ if $\tau(\ell(i)) \neq s$. Otherwise, $\mathbf{C}_{i,j} = \zeta_{i,j}$ where $\zeta_{i,j}$ is a variable in $\mathbb{F}_q$ denoting the coefficient used at the source node to compute the effect of the j'th element of the message vector, $\mathbf{w}^t$, on the corresponding symbol over edge $\ell(i)$.

In the case where all the edges in the network are ON, using the same argument introduced in [61], the input and output vectors at time t are related as $\mathbf{y}^t = \mathbf{A}\left(\mathbf{I} - \mathbf{F}\right)^{-1}\mathbf{C}\mathbf{w}^t$. This is due to the facts that the network is delay-free and the underlying graph is directed acyclic. Hence, the receiver can successfully decode the transmitted message if $\det\left(\mathbf{A}\left(\mathbf{I} - \mathbf{F}\right)^{-1}\mathbf{C}\right) \neq 0$.

However, according to the network model, each link in the graph can be in the ON or OFF state. The state of the graph G is defined as the vector of the states of all the links in the graph. Consider all states of the graph for which $\omega\left(\mathcal{E}_{\text{OFF}}\right) \leq d$. Let us denote the number of such states by Ψ (obviously, $\Psi \leq 2^{|\mathcal{E}|}$), and label them from 1 to Ψ. Corresponding to the i'th state, $1 \leq i \leq \Psi$, we define the graph $\hat{G}^i = (\mathcal{V}, \hat{\mathcal{E}}^i)$ where $\hat{\mathcal{E}}^i \triangleq \mathcal{E} - \mathcal{E}_{\text{OFF}}$, and the operator '$-$' is defined as $\mathcal{A} - \mathcal{B} \triangleq \{x \in \mathcal{A} |\ x \notin \mathcal{B}\}$ for any two sets $\mathcal{A}$ and $\mathcal{B}$. Let us assume the i'th state occurs. According to the definition of linear network coding (Definition 4.9), the intermediate nodes disregard the symbols received from the OFF edges. Thus, the input and output vectors at time t are related as $\mathbf{y}^t = \hat{\mathbf{A}}^i\left(\mathbf{I} - \hat{\mathbf{F}}^i\right)^{-1}\mathbf{C}\mathbf{w}^t$ where

$$\begin{aligned}
\hat{F}^i_{j,k} &= \begin{cases} 0 & \ell(k) \in \mathcal{E} - \hat{\mathcal{E}}_i \\ F_{j,k} & \text{otherwise} \end{cases} \\
\hat{A}^i_{j,k} &= \begin{cases} 0 & \ell(k) \in \mathcal{E} - \hat{\mathcal{E}}_i \\ A_{j,k} & \text{otherwise} \end{cases} .
\end{aligned}$$

Let us consider an arbitrary cut $\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)$ in G. The projection of this cut on $\hat{G}^i$, $\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) \cap \hat{\mathcal{E}}^i$, corresponds to a cut in $\hat{G}^i$ which is denoted by $\mathcal{C}^{\mathcal{V}_1,\mathcal{V}_2}_{\hat{G}^i}(s,z) \triangleq \mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) \cap \hat{\mathcal{E}}^i$. Since $\omega\left(\mathcal{E} - \hat{\mathcal{E}}_i\right) \leq d$, we conclude that $\omega\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) - \mathcal{C}^{\mathcal{V}_1,\mathcal{V}_2}_{\hat{G}^i}(s,z)\right) \leq d$. Thus, we have

$$\sigma\left(\mathcal{C}^{\mathcal{V}_1,\mathcal{V}_2}_{\hat{G}^i}(s,z)\right) \overset{(a)}{\geq} \tilde{r}(d) \overset{(b)}{\geq} r. \tag{4.22}$$

Here, (a) results from Definition 4.19 and the facts that $\mathcal{C}_{\hat{G}^i}^{\mathcal{V}_1,\mathcal{V}_2}(s,z) \subseteq \mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z)$ and

$$\omega\left(\mathcal{C}_{\mathcal{V}_1,\mathcal{V}_2}(s,z) - \mathcal{C}_{\hat{G}^i}^{\mathcal{V}_1,\mathcal{V}_2}(s,z)\right) \leq d,$$

and (b) results from the assumption of the Lemma.

The above inequality implies that the min-cut of graph $\hat{G}_i$ is greater than or equal to r, for all $1 \leq i \leq \Psi$. Hence, according to the Ford-Fulkerson Theorem, a routing algorithm with the rate r exists for every $\hat{G}_i$. Any routing algorithm with rate r over $\hat{G}_i$ can be interpreted as a realization of $\hat{\mathbf{A}}^i, \hat{\mathbf{F}}^i, \mathbf{C}$ for which the matrix $\hat{\mathbf{A}}^i\left(\mathbf{I}-\hat{\mathbf{F}}^i\right)^{-1}\mathbf{C}$ is non-singular. Accordingly, by defining the multivariate polynomial δ_i as $\delta_i \triangleq \det\left(\hat{\mathbf{A}}^i\left(\mathbf{I}-\hat{\mathbf{F}}^i\right)^{-1}\mathbf{C}\right)$, we conclude that δ_i is a non-zero polynomial of $\{\alpha_{j,k}, \beta_{j,k}, \zeta_{j,k}\}$ over $\mathbb{F}_q$. Let us denote the length of the longest path over G by L_G. Hence, the entries of $\left(\mathbf{I}-\hat{\mathbf{F}}^i\right)^{-1}$ are polynomials with the degree of at most $L_G - 1$. Knowing that the entries of $\hat{\mathbf{A}}^i$ and $\mathbf{C}$ are polynomials with degree 1, we conclude δ_i is a polynomial of degree $(L_G+1)r$.

Let us define the multivariate polynomial $\delta \triangleq \prod_{i=1}^{\Psi}\delta_i$. Since δ_i's are non-zero polynomials of degree at most $(L_G+1)r$, δ is also a non-zero polynomial of degree at most $\Psi(L_G+1)r$. Let us assume q is large enough such that $q > \Psi(L_G+1)r$. Applying Schwartz-Zippel Theorem [143], we have

$$\mathbb{P}\left\{\delta\left(\alpha_{j,k}, \beta_{j,k}, \zeta_{j,k}\right) = 0\right\} \leq \frac{\deg\left(\delta\right)}{q} \leq \frac{(L_G+1)r}{q} < 1. \tag{4.23}$$

Here, it is assumed that the variables are chosen independently and equiprobably from $\mathbb{F}_q$. (4.23) implies that there exists a realization such that $\delta \neq 0$. Equivalently, there exists a linear network code such that for all states of the network, the matrix $\hat{\mathbf{A}}^i\left(\mathbf{I}-\hat{\mathbf{F}}^i\right)^{-1}\mathbf{C}$ is non-singular and the message vector can be decoded with zero error probability, $P_E = 0$. This completes the proof of the lemma.

4.7.8 Proof of Theorem 4.4

Similar to the proof in appendix 4.7.7, we can define $2^{|\mathcal{E}|}$ different states for the graph G labeled arbitrarily from 1 to $2^{|\mathcal{E}|}$. Similarly, corresponding to the i'th state, we can define the graph $\hat{G}^i = \left(\mathcal{V}, \hat{\mathcal{E}}^i\right)$ where $\hat{\mathcal{E}}^i$ denotes the set of ON edges. Moreover, let us define $\mathcal{D}_i$ as the event that the i'th state occurs. Since $\mathcal{D}_i$'s are disjoint and cover all the possibilities,

P_E can be upper-bounded as

$$\begin{aligned} P_E &= \sum_{i=1}^{2^{|\mathcal{E}|}} \mathbb{P}\{\text{error } |\mathcal{D}_i\}\mathbb{P}\{\mathcal{D}_i\} \\ &\overset{(a)}{=} \sum_{\substack{i=1 \\ \omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)\geq d^\star(r)}}^{2^{|\mathcal{E}|}} \mathbb{P}\{\text{error } |\mathcal{D}_i\}\mathbb{P}\{\mathcal{D}_i\} \\ &\overset{(b)}{=} \sum_{\substack{i=1 \\ \omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)\geq d^\star(r)}}^{2^{|\mathcal{E}|}} \mathbb{P}\{\text{error } |\mathcal{D}_i\}p^{\omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)}(1-p)^{\omega\left(\hat{\mathcal{E}}^i\right)} \\ &\leq \sum_{\substack{i=1 \\ \omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)\geq d^\star(r)}}^{2^{|\mathcal{E}|}} p^{\omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)}(1-p)^{\omega\left(\hat{\mathcal{E}}^i\right)} \\ &\leq 2^{|\mathcal{E}|}p^{d^\star(r)}. \end{aligned} \tag{4.24}$$

Here, (a) follows from Lemma 4.6 by setting

$$d = \max_{\substack{1\leq i\leq 2^{|\mathcal{E}|} \\ \omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)<d^\star(r)}} \omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)$$

and the facts that: i) for all states in which $\omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right) < d^\star(r)$, we have $\omega(\mathcal{E}_{OFF}) \leq d$, and ii) $d < d^\star(r)$ which results in $r \leq \tilde{r}(d)$. (b) results knowing $\mathbb{P}\{\mathcal{D}_i\} = p^{\omega\left(\mathcal{E}-\hat{\mathcal{E}}^i\right)}(1-p)^{\omega\left(\hat{\mathcal{E}}^i\right)}$. Combining (4.24) and the lower-bound of P_E obtained in Lemma 4.5 completes the proof of the theorem. ■

4.7.9 Proof of Theorem 4.5

Since the theorem is an existential one, providing a constructive example is sufficient for the proof. Thus, we prove the theorem by presenting a graph for which no conventional routing scheme can achieve the optimum diversity-rate trade-off.

Consider the erasure graph in Fig. 4.8. All links have the same erasure probability, i.e. $\omega(e) = 1$ for all edges. Furthermore, all links have unit capacity except the three links from u to z which have the capacity of 5 symbols per time slot each. We label these links

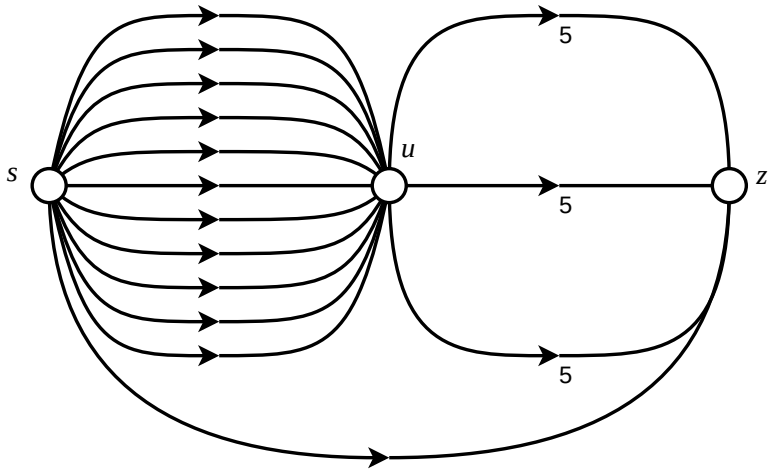


Figure 4.8: An example of conventional routing failing to achieve $d^{opt}(r)$

as e_1, e_2, and e_3. Moreover, e_4 denotes the only direct link from s to z.

Consider an end-to-end connection $\mathfrak{C}(s, z, r)$ with $r = 11$ which uses conventional routing during T time-slots. Let the vectors $\mathbf{s}$ of size $12T$ denote the vector of the symbols sent by the source on its outgoing links. Since, the intermediate node applies conventional routing, the information symbols on the links $e_1, \ldots, e_4$ correspond to specific indices of the vector $\mathbf{s}$. For $i = 1 \ldots 4$, let $\mathcal{A}_i$ denote the set of all indices of $\mathbf{s}$ which correspond to the symbols sent on link e_i during time slot 1 to T.

We define $\mathcal{C}_1(s, z)$ as the $s - z$ cutset consisting of $e_1, \ldots, e_4$. According to Lemma 4.1, if any two links in $\mathcal{C}_1(s, z)$ are OFF, we have $\lim_{T\to\infty} P_E = 1$. This implies that $d^{\mathfrak{C}} \leq 2$, i.e. we have $d^{\mathfrak{C}} = 1$ or $d^{\mathfrak{C}} = 2$. Next, we show that $d^{\mathfrak{C}} = 2$ leads to contradiction, proving that we must have $d^{\mathfrak{C}} = 1$.

Let us assume that $d^{\mathfrak{C}} = 2$. This implies that even if e_3 is OFF, the end node z should be able to decode the transmitted data from s based on the symbols conveyed through e_1, e_2, and e_4 with the error probability of $O(p)$. Thus, we can write

$$\begin{aligned} rT &= 11T \\ &\overset{(a)}{\leq} |\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_4| \\ &\overset{(b)}{=} |\mathcal{A}_1 \cup \mathcal{A}_2| + |\mathcal{A}_4| \\ &= |\mathcal{A}_1 \cup \mathcal{A}_2| + T, \end{aligned}$$

where operator $||$ denotes the cardinality of the set. Here, (a) follows from the fact that any code with the rate greater than 1 has a strictly positive probability of error (constant with p), and (b) follows from the fact that $\mathcal{A}_4$ and $\mathcal{A}_1 \cup \mathcal{A}_2 \cup \mathcal{A}_3$ are disjoint sets. The above result is equivalent to

$$|\mathcal{A}_1| + |\mathcal{A}_2| - |\mathcal{A}_1 \cap \mathcal{A}_2| \geq 10T \tag{4.25}$$

Based on similar arguments for the cases where e_2 or e_3 are OFF, we can write

$$\begin{aligned} |\mathcal{A}_1| + |\mathcal{A}_3| - |\mathcal{A}_1 \cap \mathcal{A}_3| &\geq 10T \\ |\mathcal{A}_2| + |\mathcal{A}_3| - |\mathcal{A}_2 \cap \mathcal{A}_3| &\geq 10T \end{aligned} \tag{4.26}$$

Now, we have

$$\begin{aligned} 11T &\overset{(a)}{\geq} |\mathcal{A}_1 \cup \mathcal{A}_2 \cup A_3| \\ &\geq \sum_{i=1}^{3} |\mathcal{A}_i| - \sum_{i=1}^{3} \sum_{\substack{j=1 \\ j>i}}^{3} |\mathcal{A}_i \cap \mathcal{A}_j| \\ &\overset{(b)}{\geq} 30T - \sum_{i=1}^{3} |\mathcal{A}_i| \\ &\overset{(c)}{\geq} 15T \end{aligned} \tag{4.27}$$

Since u uses conventional routing, $\mathcal{A}_1 \cup \mathcal{A}_2 \cup A_3$ is a subset of the symbol indices on its incoming links. This results in (a). (b) can be justified by adding the inequalities in (4.25) and (4.26). (c) results from $|\mathcal{A}_i| \leq 5T$. (4.27) is an obvious contradiction. This contradiction proves that for $r = 11$ and any conventional routing end-to-end connection $\mathfrak{C}(s, z, r)$, we have $d^{\mathfrak{C}} \leq 1$.

However, according to Theorem 4.4, for $r = 11$, we have $d^{opt}(r) = d^{\star}(r) = 2$. Therefore, for this graph, the diversity gain of any conventional routing end-to-end connection is strictly smaller than $d^{opt}(r)$. This completes the proof. ■

Chapter 5

Conclusion

5.1 Contributions

In this thesis, we studied the issue of diversity and reliability over erasure networks from three different (but inter-connected) angles: rate allocation (RA) problem, coding, and diversity-rate trade-off (DRT) over erasure networks. The next three subsections review our contributions on each topic.

5.1.1 Rate Allocation Across Multiple Paths

In chapter 2, we focused on analyzing the probability of irrecoverable loss (P_E) for a block of packets sent through multiple independent paths between two end-points. The end-nodes apply Forward Error Correction (FEC) to overcome temporary packet loss on the paths. Based on the results of chapter 3, we adopt an MDS code for FEC. We show that P_E decays exponentially as the number of paths increases. We are also able to analytically solve the RA problem for the asymptotic case (large number of paths). It is shown that in the asymptotically optimal RA, each path should be included in RA *iff* its *quality* is above a certain threshold; otherwise, it is assigned the rate zero. Finally, we propose a heuristic suboptimal RA algorithm for practical (limited) number of paths. It is proved that this suboptimal RA algorithm converges to the asymptotically optimal one as the number of paths increases. Unlike the optimal RA algorithm, the suboptimal one has polynomial time complexity. Simulation results confirm the near-optimal performance of the suboptimal RA in practical scenarios.

5.1.2 Coding

Although we are mainly interested in the erasure channel, we generalize our analysis into a more broad class of channels called input-independent channels in chapter 3. Symmetric discrete memoryless channel (DMC) and erasure channels with memory extended over a block of symbols are all special cases of input-independent channel. We derive a lower-bound on P_E of any code (with limited length) over a general input-independent channel. Next, we apply this lower-bound on three special input-independent channels: erasure channel, super-symmetric DMC, and q-ary symmetric DMC. We show that *Maximum Distance Separable* (MDS) codes are optimal over erasure channels (with or without memory) in the sense that they achieve the minimum probability of error among all block codes of the same size. Moreover, we prove that *perfect* codes achieve the minimum probability of error over a super-symmetric channel. Finally, using the *method of types*, we simplify our lower-bound for P_E of any block code over symmetric DMC and show that this bound is exponentially tight. For ternary and 4-ary symmetric channels, the proposed lower-bound is compared with the previous lower-bounds in moderate to short block lengths. It is shown that our lower-bound by far outperforms the previous bounds, especially for shorter block lengths.

5.1.3 Diversity-Rate Trade-off over Erasure Networks

In chapter 4, we address a fundamental trade-off between rate and diversity gain for any end-to-end connection in an erasure network. The erasure network is modeled as a directed acyclic graph whose links are orthogonal erasure channels. First, we consider homogeneous erasure networks whose links have the same erasure probability and capacity. It is shown that a special form of FEC (MDS coding at the source node and disjoint routing) achieves the optimum diversity-rate trade-off. This is obviously an example of *conventional routing*.

Next, we study general erasure networks in which links can have different capacity and erasure probabilities. It is proved that linear network coding can always achieve the optimum trade-off between rate and diversity gain. More importantly, there exist networks for which any conventional routing scheme fails to achieve this optimum trade-off. Finally, we construct networks using the standard random graph generation models and show that the cases where conventional routing fails are indeed very prevalent. However, linear network coding always achieves the optimum diversity-rate trade-off.

5.2 Future Directions

Here, we list the directions in which our work can be extended. We categorize the future work based on the chapter (i.e topic) they correspond to.

5.2.1 FEC Rate Allocation

- Correlated paths: in chapter 2, we study the problem of Rate Allocation (RA) for a block of packets sent through multiple independent paths between two end-points. In other words, it is assumed the L given paths are completely independent. In many networks, it is not easy to find more than very few completely independent paths between most two nodes. However, it is reasonable to assume that we can easily find multiple partially correlated paths between the end-nodes.

  Intuitively speaking, we expect to get less improvement from RA over multiple partially correlated paths (compared to the case where the paths are independent). For partially correlated paths, the question is that whether P_E drops exponentially with the number of paths (L) or not? If yes, what is the exponent of P_E versus L? This would be a measure of how much of the improvement is lost because of the dependency between the paths.

5.2.2 Coding

- Lower-bounding P_E for non-block codes: the main lower-bound which is the basis for all of the results in chapter 3 is valid for block codes only. An important generalization of this work would include extending this lower-bound such that it is valid for convolutional codes, etc.

- Complexity of the lower-bound for symmetric DMC's: in section 3.4, we introduce an algorithm for computing the general lower-bound (previously introduced in section 3.1). This algorithm is based on he method of types in information theory [18] and has the complexity of $O(N^q)$, i.e. it is polynomial in terms of the block length N and exponential in terms of the alphabet size q. This imposes a serious restriction on practicality of the algorithm and limits its application to short to moderate block codes.

This work can be improved significantly by introducing an algorithm which computes (or approximates) the lower-bound on P_E of block codes over symmetric DMC's (noted by $L(N, K, \boldsymbol{\pi})$) with polynomial complexity in terms of both block length N and alphabet size q. It should be noted that such an algorithm does not need to compute $L(N, K, \boldsymbol{\pi})$ precisely; even an approximation (a lower-bound) to $L(N, K, \boldsymbol{\pi})$ suffices for our purpose, as long as the lower-bound to $L(N, K, \boldsymbol{\pi})$ is tight enough such that the overall lower-bound remains stronger than previously known lower-bounds.

- Symmetric DMC's with soft decoding: the introduced lower-bound in section 3.4, denoted by $L(N, K, \boldsymbol{\pi})$, works for channels with limited alphabet size. This imposes another restriction on the applicability of this bound. Unlike some previously known lower-bounds [44, 45, 53], it can not be used for limiting P_E of soft-decoding over AWGN channel with symmetric constellations.

5.2.3 Diversity-Rate Trade-off

- General models for network graph: the network model studied in chapter 4 is identified by an *erasure graph*. An erasure graph is defined as an acyclic directed graph $G = (\mathcal{V}, \mathcal{E})$ whose links are orthogonal erasure channels. Each link $e \in \mathcal{E}$ has the maximum rate of $\sigma(e)$ and the erasure probability of $p^{\omega(e)}$. The probability of a link being OFF (in erasure state) is independent from the status of other links.

  In the real networks modeled as erasure networks (the Internet, wireless mesh networks, etc), the erasure status of the links can have significant correlation with each other. Moreover, the erasure status of each link may have a memory and depend on the link status in the previous blocks. The fundamental trade-off we derived between diversity and trade-off for the erasure graph model (described in the previous paragraph) may not necessarily be valid for more general (and more practical) network models.

- Complexity of computing the optimal diversity-rate trade-off: for any erasure graph, we show that there exists a *linear network coding* strategy which achieves the optimum diversity-rate trade-off, $d^{opt}(r)$. However unfortunately, this optimum diversity gain for a given rate r is not easy to compute. In other to find $d^{opt}(r)$, we have to compute a rather simple function over all cuts between the source and destination

nodes. This obviously has an exponential complexity in terms of the network size. It would be of great practical value if we can compute (or estimate) $d^{opt}(r)$ with lower complexity.

- Optimum diversity-rate trade-off achieved by conventional routing: in general erasure graphs, it is proved that conventional routing is not optimum in terms of diversity-rate trade-off. More accurately, there exist general erasure graphs for which any conventional routing strategy fails to achieve the optimum diversity-rate trade-off. Since conventional routing strategies still dominate the sphere of routing in packet-switched networks, one important question which arises is this: for a given network and a given rate, what is the maximum diversity gain achieved by conventional routing schemes? How different is this maximum from $d^{opt}(r)$?

Bibliography

[1] A. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *Information Theory, IEEE Transactions on*, vol. 52, no. 3, pp. 789–804, 2006.

[2] B. Smith, P. Gupta, and S. Vishwanath, "Routing is Order-optimal in Broadcast Erasure Networks with Interference," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, 2007, pp. 141–145.

[3] N. Ratnakar and G. Kramer, "The multicast capacity of deterministic relay networks with no interference," *IEEE/ACM Transactions on Networking (TON)*, vol. 14, pp. 2425–2432, 2006.

[4] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow," in *45th Allerton Conference on Communication, Control, and Computing*, 2007.

[5] R. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19–36, 2006.

[6] N. Cai and R. Yeung, "Network error correction, Part II: Lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 37–54, 2006.

[7] R. Koetter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *Information Theory, IEEE Transactions on*, vol. 54, no. 8, pp. 3579–3591, 2008.

[8] W.H. Tarn and Y.C. Tseng, "Joint Multi-Channel Link Layer and Multi-Path Routing Design for Wireless Mesh Networks," in *INFOCOM*, 2007, pp. 2081–2089.

[9] N.S. Nandiraju, D.S. Nandiraju, and D.P. Agrawal, "Multipath Routing in Wireless Mesh Networks," in *IEEE International Conference on Mobile Adhoc and Sensor Systems*, 2006, pp. 741–746.

[10] P. Djukic and S. Valaee, "Reliable Packet Transmissions in Multipath Routed Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 548– 559, 2006.

[11] H. Han, S. Shakkottai, C.V. Hollot, R. Srikant, and D. Towsley, "Multi-Path TCP: A Joint Congestion Control and Routing Scheme to Exploit Path Diversity in the Internet," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, pp. 1260 – 1271, 2006.

[12] T. Nguyen and A. Zakhor , "Path diversity with forward error correction (pdf) system for packet switched networks," in *IEEE INFOCOM Proc. IEEE Vol. 1*, 2003, pp. 663– 672.

[13] A. Akella, J. Pang, B. Maggs, S. Seshan, and A. Shaikh, "A Comparison of Overlay Routing and Multihoming Route Control," in *ACM SIGCOMM*, 2004, pp. 93 – 106.

[14] V.N. Padmanabhan, H.J. Wang, P.A. Chou, "Resilient Peer-to-peer Streaming," in *IEEE International Conference on Network Protocols*, 2003, pp. 16–27.

[15] S. Fashandi, S. Oveisgharan, and A.K. Khandani, "Path Diversity Over Packet Switched Networks: Performance Analysis and Rate Allocation," *IEEE/ACM Transactions on Networking*, vol. 18, no. 5, pp. 1373 – 1386, 2010.

[16] ——, "Path Diversity in Packet Switched Networks: Performance Analysis and Rate Allocation," in *IEEE Global Telecommunications Conference, GLOBECOM '07*, 2007, pp. 1840–1844.

[17] T. Nguyen and A. Zakhor, "Multiple Sender Distributed Video Streaming," *IEEE transactions on multimedia*, vol. 6, no. 2, pp. 315– 326, 2004.

[18] T. Cover and J. Thomas, *Elements of Information Theory*, 1st ed. New York: Wiley, 2006, pp. 284–285.

[19] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1073– 1096, May 2003.

[20] S. Oveisgharan, S. Fashandi, and A.K. Khandani, "Diversity-Rate Trade-off in Erasure Networks," in *IEEE INFOCOM*, 2010, pp. 1–9.

[21] S. Fashandi, S. Oveisgharan, and A.K. Khandani, "Coding over an Erasure Channel with a Large Alphabet Size," in *IEEE International Symposium on Information Theory*, 2008, pp. 1053–1057.

[22] S. Feng, Z. Liang, and D. Zhao, "Providing Telemedicine Services in an Infrastructure-based Cognitive Radio Network," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 96–103, 2010.

[23] V.S. Shukla, "Optical Core Networks: Architecture and Challenges," in *OptoeElectronics and Communications Conference (OECC)*, 2010, pp. 86–87.

[24] J.S. Park, M. Gerla, D.S. Lun, Y. Yi, and M. Medard, "CodeCast: A Network-Coding-Based Ad hoc Multicast Protocol," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 76–81, 2006.

[25] N. Gogate, D.M. Chung, S.S. Panwar, Yao Wang, "Supporting Image and Video Applications in a Multihop Radio Environment Using Path Diversity and Multiple Description Coding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12, no. 9, pp. 777–792, 2002.

[26] Wei Wei and A. Zakhor, "Interference Aware Multipath Selection for Video Streaming in Wireless Ad Hoc Networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 165 – 178, 2009.

[27] S. Mao, S.S. Panwar, and Y.T. Hou, "On optimal partitioning of realtime traffic over multiple paths," in *INFOCOM 2005, Proc. IEEE Vol. 4*, 2005, pp. 2325–2336.

[28] S.J. Lee and M. Gerla, "SMR: Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks," in *IEEE Interneational Conference on Communications*, 2001, pp. 3201–3205.

[29] ——, "AODV-BR: Backup Routing in Ad Hoc Networks," in *Wireless Communications and Networking Conference*, 2000, pp. 1311–1316.

[30] M.K. Marina and S.R. Das, "On-Demand Multipath Distance Vector Routing for Ad Hoc Networks," in *IEEE International Conference on Network Protocols*, 2001, pp. 14–23.

[31] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks," in *INFOCOM*, 2003, pp. 270– 280.

[32] S. Mao, Y.T. Hou, X. Cheng, H.D. Sherali, S.F. Midkiff, and Y.Q. Zhang, "On Routing for Multiple Description Video Over Wireless Ad Hoc Networks," *IEEE Transactions on Multimedia*, vol. 8, no. 5, pp. 1063–1074, 2006.

[33] R. Leung, J. Liu, E. Poon, A.L.C. Chan, and Baochun Li, "MP-DSR: A QoS-aware Multi-path Dynamic Source Routing Protocol For Wireless Ad-hoc Networks," in *IEEE International Conference on Local Computer Networks*, 2001, pp. 132–141.

[34] L. Wang, Y. Shu, O. Yang, M. Dong, and L. Zhang, "Adaptive Multipath Source Routing in Ad Hoc Networks,," in *IEEE International Conference on Communications*, 2001, pp. 867–871.

[35] Yi Li, Yin Zhang, Li Li Qiu, and S. Lam, "SmartTunnel: Achieving Reliability in the Internet," in *IEEE INFOCOM*, 2007, pp. 830–838.

[36] A. Populis and S. Pillai, *Probability, Random Variables and Stochastic Processes*. McGraw Hill, 2002.

[37] H. Sanneck, G. Carle, "A Framework Model for Packet Loss Metrics Based on Loss Runlengths," in *ACM SIGMM Multimedia Computing and Networking Conference*, 2000.

[38] J. C. Bolot, "End-to-end Packet Delay and Loss Behavior in the Internet," in *ACM SIGCOMM Conference on Communication Architectures, Protocols and Applications*, 1993, pp. 289 – 298.

[39] J.C. Bolot, S. Fosse-Parisis, and D. Towsley, "Adaptive FEC-based error control for Internet telephony," in *IEEE INFOCOM, Proc. IEEE Vol. 3*, 1999, pp. 1453–1460.

[40] J.C. Bolot and T. Turletti, "Adaptive Error Control For Packet Video In The Internet," in *Proc. IEEE International Conference on Image Processing*, 1996, pp. 25 – 28.

[41] F. L. Leannec, F. Toutain, and C. Guillemot, "Packet Loss Resilient MPEG-4 Compliant Video Coding for the Internet," *Journal of Image Communication, Special Issue on Real-time video over the Internet*, no. 15, pp. 35–56, 1999.

[42] Y. Polyanskiy, H.V. Poor, and S. Verdu, "Channel Coding Rate in Finite Blocklength Regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[43] R. G. Gallager, *Information Theory and Reliable Communication*, 1st ed. New York, NY, USA: John Wiley & Sons, 1968, pp. 157–158.

[44] A. Velambois and P. C. Fossorier, "Sphere-packing Bounds Revisited for Moderate Block Lengths," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 2998–3014, 2004.

[45] G. Wiechman and I. Sason, "An Improved Sphere-packing Bound for Finite-length Codes over Symmetric Memoryless Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 1962–1990, 2008.

[46] C. E. Shannon, "A Mathematical Theory of Communications," *Bell Systems Technical Journal*, vol. 27, pp. 379–423,623–656, 1948.

[47] A. Feinstein, "A New Basic Theorem of Information Theory," *IRE Professional Group on Information Theory*, vol. 4, no. 4, pp. 2–22, 1954.

[48] P. Elias, "Coding for Noisy Channels," *IRE Convention Record*, vol. 4, pp. 37–46, 1955.

[49] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to Error Probability for Coding on Discrete Memoryless Channels," *Information and Control*, vol. 10, pp. 65–103,522–552, 1967.

[50] R. G. Gallager, *Information Theory and Reliable Communication*, 1st ed. New York, NY, USA: John Wiley & Sons, 1968, pp. 135–144.

[51] G. Forney, "Exponential Error Bounds for Erasure, List, and Decision Feedback Schemes," *IEEE Transactions on Information Theory*, vol. 14, no. 2, pp. 206–220, 1968.

[52] R. Gallager, "The Random Coding Bound is Tight for the Average Code," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 244–246, 1973.

[53] C. E. Shannon, "Probability of Error for Optimal Codes in a Gaussian Channel," *Bell Systems Technical Journal*, vol. 38, pp. 611–656, 1959.

[54] Ron M. Roth, *Introduction to Coding Theory*, 1st ed. Cambridge University Press, 2006, pp. 333–351.

[55] ——, *Introduction to Coding Theory*, 1st ed. Cambridge University Press, 2006, pp. 183–204.

[56] ——, *Introduction to Coding Theory*, 1st ed. Cambridge University Press, 2006, pp. 16–17.

[57] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed. McGraw-Hill, 1976.

[58] R. Diestel, *Graph Theory*. Springer, 2006.

[59] Y. R. W. Li S.-Y.R. and N. Cai, "Linear network coding," *Information Theory, IEEE Transactions on*, vol. 49, no. 2, pp. 371–381, 2003.

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

[61] R. Koetter and M. Medard , "An algebraic approach to network coding," *IEEE transactions on Networking*, vol. 11, no. 5, pp. 782– 795, 2003.

[62] T. Ho, M. Medard, and R. Koetter, "An Information-theoretic View of Network Management," *Information Theory, IEEE Transactions on*, vol. 51, no. 4, pp. 1295–1312, 2005.

[63] T. Ho, M. Medard, and R. Koetter, D.R. Karger, M. Effros, Jun Shi, and B. Leong, "A Random Linear Network Coding Approach to Multicast," *Information Theory, IEEE Transactions on*, vol. 52, no. 10, pp. 4413–4430, 2006.

[64] I. Csiszar, "Linear Codes for Sources and Source Networks: Error Exponents, Universal Coding," *Information Theory, IEEE Transactions on*, vol. 28, no. 4, pp. 585–592, 1982.

[65] K. Rojviboonchai, F. Yang, Q. Zhang, H. Aida1, and W. Zhu, "AMTP: A Multipath Multimedia Streaming Protocol for Mobile Ad Hoc Networks," in *IEEE International Conference on Communications*, 2005, pp. 1246–1250.

[66] Wei Wei and A. Zakhor, "Robust Multipath Source Routing Protocol (RMPSR) for Video Communication over Wireless Ad Hoc Networks," in *International Conference on Multimedia*, 2004, p. 13791382.

[67] Y. J. Liang, E. G. Steinbach, and B. Girod , "Multi-stream Voice over IP using Packet Path Diversity," in *IEEE Fourth Workshop on Multimedia Signal Processing*, 2001, pp. 555–560.

[68] S. Nelakuditi, Z. Zhang, and D. H. C. Du, "On Selection of Candidate Paths for Proportional Routing," *Elsevier Computer Networks*, vol. 44, no. 1, pp. 79–102, 2004.

[69] J. Han and F. Jahanian, "Impact of Path Diversity on Multi-homed and Overlay Networks," in *International Conference on Dependable Systems and Networks*, 2004, pp. 29–38.

[70] David G. Andersen, *Resilient Overlay Networks*. Master's Thesis, Massachusetts Institute of Technology, 2001.

[71] D. G. Andersen, A. C. Snoeren, and H. Balakrishnan, "Best-path vs. Multi-path Overlay Routing," in *Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement*, 2003, pp. 91 – 100.

[72] R. Teixeira, K. Marzullo, S. Savage, and G. M. Voelker, "In Search of Path Diversity in ISP Networks," in *Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement*, 2003, pp. 313 – 318.

[73] D. Rubenstein, J. Kurose, and D. Towsley, "Detecting Shared Congestion of Flows via End-to-end Measurement," *IEEE/ACM Transactions on Networking*, vol. 10, no. 3, p. 381395, 2002.

[74] D. Katabi, I. Bazzi, and Xiaowei Yang, "A Passive Approach for Detecting Shared Bottlenecks," in *IEEE International Conference on Computer Communications and Networks*, 2001, pp. 174–181.

[75] M. S. Kim, T. Kim, Y. J. Shin, S. S. Lam, E.J. Powers, "A Wavelet-Based Approach to Detect Shared Congestion," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 763–776, 2008.

[76] C.E. Perkins, E.M. Royer, S.R. Das, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," *IEEE Personal Communications*, vol. 8, no. 1, pp. 16–28, 2001.

[77] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, p. 153181, 1996.

[78] Wei Wei and A. Zakhor, "Multiple Tree Video Multicast over Wireless Ad Hoc Networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 1, pp. 2–15, 2007.

[79] D. Clark, W. Lehr, S. Bauer, P. Faratin, R. Sami, and J. Wroclawski, "Overlay Networks and Future of the Internet," *Journal of Communications and Strategies*, vol. 3, no. 63, pp. 1–21, 2006.

[80] M. Guo, Q. Zhang, and W. Zhu , "Selecting Path-diversified Servers in Content Distribution Networks," in *IEEE Global Telecommunications Conference*, vol. 6, 2003, pp. 3181–3185.

[81] M. Cha, S. Moon, C. D. Park, and A. Shaikh, "Placing Relay Nodes for Intra-Domain Path Diversity," in *IEEE INFOCOM*, 2006, pp. 1–12.

[82] S. Srinivasan, *Design and Use of Managed Overlay Networks.* PhD Dissertation, Georgia Institute of Technology, 2007.

[83] J. Han, D. Watson, and F. Jahanian, "Enhancing End-to-End Availability and Performance via Topology-aware Overlay Networks," *Elsevier Computer Networks*, vol. 52, no. 16, pp. 3029–3046, 2008.

[84] S. Ratnasamy, M. Handley, R. Karp, and S. Shenker, "Topologically-aware Overlay Construction and Server Selection," in *IEEE INFOCOM*, 2002, pp. 1190–1199.

[85] M. Castro, P. Druschel, Y. C. Hu, and A. Rowstron, "Topology-aware Routing in Structured Peer-to-peer Overlay Networks."

[86] Zhi Li and P. Mohapatra, "QRON: QoS-aware Routing in Overlay Networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 1, pp. 29–40, 2004.

[87] ——, "The Impact of Topology on Overlay Routing Service," in *IEEE INFOCOM*, 2004, pp. 408–418.

[88] A. Nakao, L. Peterson, and A. Bavier, "A Routing Underlay for Overlay Networks," in *Proceedings of ACM SIGCOMM*, 2003, pp. 11–18.

[89] J. Touch, Y. Wang, V. Pingali, L. Eggert, R. Zhou, and G. Finn, "A Routing Underlay for Overlay Networks," in *Proc. IEEE Tridentcom*, 2005, pp. 194–203.

[90] B-G Chun, R. Fonseca, I. Stoica, and J. Kubiatowicz, "Characterizing Selfishly Constructed Overlay Routing Networks," in *IEEE INFOCOM*, 2004, pp. 1329–1339.

[91] Z. Li, L. Yuan, P. Mohapatra, and C-N. Chuah, "On the Analysis of Overlay Failure Detection and Recovery," *Computer Networks Journal*, vol. 51, no. 13, pp. 3838–3843, 2007.

[92] A. Akella, B. Maggs, S. Seshan, and A. Shaikh, "On the Performance Benefits of Multihoming Route Control," *IEEE/ACM Transactions on Networking*, vol. 16, no. 1, pp. 91–104, 2008.

[93] Y.H. Wang and H.Z. Lin, "Multipath QoS Routing with Interference Provision in Ad Hoc Wireless Network," *IEEE Transactions on Multimedia*, vol. 22, no. 6, pp. 1325–1338, 2006.

[94] Roger Karrer, and Thomas Gross, "Multipath Streaming in Best-Effort Networks," in *Proc. of the IEEE International Conference on Communications (ICC'03)*, 2003.

[95] J.G. Apostolopoulos, T. Wong, W. Tan, and S.J. Wee, "On Multiple Description Streaming with Content Delivery Networks," in *IEEE INFOCOM, Proc. IEEE Vol. 3*, 2002, pp. 1736 – 1745.

[96] "Akamai sureroute," akamai.com/dl/feature_sheets/fs_edge_suite_sureroute.pdf.

[97] M. Ghanassi and P. Kabal, "Optimizing Voice-over-IP Speech Quality Using Path Diversity," in *IEEE 8th Workshop on Multimedia Signal Processing*, 2006, pp. 155–160.

[98] J. Chakareski and B. Girod, "Rate-distortion optimized packet scheduling and routing for media streaming with path diversity," in *Proc. IEEE Data Compression Conference*, 2003, pp. 203– 212.

[99] E. Setton, X. Zhu, and B. Girod, "Congestion-optimized Multi-path Streaming of Video over Ad Hoc Wireless Networks," in *IEEE International Conference on Multimedia*, 2004, pp. 1619– 1622.

[100] S. Mao, D. Bushmitch, S. Narayanan, and S.S. Panwar, "MRTP: A Multiflow Real-Time Transport Protocol for Ad Hoc Networks," *IEEE Transactions on Multimedia*, vol. 8, no. 2, pp. 356–369, 2006.

[101] M. Afergan, J. Wein, and A. LaMeyer, "Experience with some Principles for Building an Internet-Scale Reliable System," in *Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, 2006, p. 3.

[102] M. Yajnik, S.B. Moon, J.F. Kurose, and D.F. Towsley , "Measurement and Modeling of the Temporal Dependence in Packet Loss," in *IEEE INFOCOM Proc. IEEE Vol. 1*, 1999, pp. 345–352.

[103] Wenyu Jiang and Henning Schulzrinne, "Modeling of Packet Loss and Delay and their Effect on Real-Time Multimedia Service Quality," in *Proc. Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, 2000.

[104] Yin Zhang and Nick Duffield, "On the Constancy of Internet Path Properties," in *ACM SIGCOMM Workshop on Internet Measurement*, 2001, pp. 197 – 211.

[105] P. Rossi, G. Romano, F. Palmieri, and G. Iannello , "A Hidden Markov Model for Internet Channels," in *IEEE International Symposium on Signal Processing and Information Technology*, 2003.

[106] K. Salamatian and Vaton, "Hidden Markov Modeling for Network Communication Channels," in *Proc. ACM SIGMETRICS*, 2001, pp. 92 – 101.

[107] D. Wu, Y.T. Hou, and Y-Q Zhang , "Transporting Real-time Video over the Internet: Challenges and Approaches," *Proceedings of the IEEE*, vol. 88, no. 12, pp. 1855–1877, 2000.

[108] M. Podolsky, C. Romer, and S. McCanne, "Simulation of FEC-based Error Control for Packet Audio on the Internet," in *IEEE INFOCOM*, 1998, pp. 505–515.

[109] R. Puri, K. Ramchandran, K.W. Lee, and V. Bharghavan, "Forward Error Correction (FEC) Codes Based Multiple Description Coding for Internet Video Streaming and Multicast," *Elsevier Signal Processing: Image Communication*, vol. 16, no. 8, pp. 745–762, 2001.

[110] W. T. Tan and A. Zakhor, "Video Multicast Using Layered FEC and Scalable Compression," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 11, no. 3, pp. 373–386, 2001.

[111] L. Dairaine, L. Lancrica, J. Lacan, and J. Fimes, "Content-Access QoS in Peer-to-Peer Networks Using a Fast MDS Erasure Code," *Elsevier Computer Communications*, vol. 28, no. 15, pp. 1778–1790, 2005.

[112] X. H. Peng, "Erasure-control Coding for Distributed Networks," *IEE Proceedings on Communications*, vol. 152, pp. 1075 – 1080, 2005.

[113] Amir Dembo and Ofer Zeitouni, *Large Deviations Techniques and Applications*, 2nd ed. New York: Springer, 1998, pp. 11–43.

[114] ISO/IEC JTC 1/SC 29, *Information technology – Generic Coding of Moving Pictures and Associated Audio Information: Systems*, ISO/IEC 13818-1, International Standard, October 2007.

[115] ——, *Information Technology – Coding of Audio-Visual Objects – Part 10: Advanced Video Coding*, ISO/IEC 14496-10, International Standard, November 2008.

[116] K.H. Goh, D.J. Wu, J.Y. Tham, T.K. Chiew and W.S. Lee, "Real-time Software MPEG-2 TO H.264 Video Transcoding," in *IEEE International Conference on Multimedia and Expo*, 2008, pp. 165–168.

[117] B. Bing, "Real-time Software MPEG-2 TO H.264 Video Transcoding," in *Communication Networks and Services Research Conference*, 2008, pp. 13–17.

[118] T. Yamaguchi, T. Kanekiyo, M. Horii, K. Kawazoe and F. Kishino, "Highly Efficient Transmission System for Digital Broadcasting Redistribution Services over IP Multicast Networks," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 2, pp. 920–924, 2008.

[119] J. L. Kelley, *General Topology.* Springer, 1975, pp. 40–43.

[120] C. H. Papadimitriou, *Computational Complexity*, 1st ed. New York: Addison Wesley, 1994.

[121] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. MIT Press, 2001, pp. 347–349.

[122] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed. Cambridge, UK: Cambridge University Press, 2004, pp. 243–245.

[123] T. Cover and J. Thomas, *Elements of Information Theory*, 1st ed. New York: Wiley, 1991, pp. 291–294.

[124] ——, *Elements of Information Theory*, 1st ed. New York: Wiley, 1991, pp. 30–31.

[125] R. Diestel, *Graph Theory.* Springer, 2006, pp. 10–12.

[126] J.C. Guey, M.P. Fitz, M.R. Bell, and W.Y. Kuo, "Signal Design for Transmitter Diversity Wireless Communication Systems over Rayleigh Fading Channels," *IEEE Transactions on Communications*, vol. 47, no. 4, pp. 527–537, 1999.

[127] J.M. Boyce and R.D. Gaglianello, "Packet Loss Effects on MPEG Video Sent over the Public Internet," in *Proceedings of ACM International Conference on Multimedia*, 1998, pp. 181 – 190.

[128] M.P. Farrera, *Packet-by-Packet Analysis of Video Traffic Dynamics on IP Networks.* PhD Dissertation, University of Essex, 2005.

[129] C. Gkantsidis and P. R. Rodriguez, "Network coding for large scale content distribution," in *IEEE INFOCOM, Proc. IEEE Vol. 4*, 2005, pp. 2235–2245.

[130] V. Paxson, "End-to-end Routing Behavior in the Internet," *IEEE/ACM Transactions on Networking*, vol. 5, no. 5, pp. 601 – 615, 1997.

[131] C. Labovitz, A. Ahuja, F. Jahanian, "Experimental Study of Internet Stability and Backbone Failures," in *Proceedings of ACM International Conference on Multimedia*, 1999, pp. 278 – 285.

[132] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: Boston university Representative Internet Topology gEnerator," http://www.cs.bu.edu/brite.

[133] ——, "BRITE: an approach to universal topology generation," in *Ninth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, 2001, pp. 346–353.

[134] A.L. Barabsi and R. Albert, "Emergence of Scaling in Random Networks," *Science Magazine*, vol. 286, no. 5439, pp. 509 – 512, 1999.

[135] B.M. Waxman, "Routing of Multipoint Connections," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 9, pp. 1617–1622, 1988.

[136] R. Albert and A.L. Barabsi, "Statistical Mechanics of Complex Networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47–97, 2002.

[137] E.W. Zegura, K.L. Calvert, and S. Bhattacharjee, "How to Model an Internetwork," in *IEEE INFOCOM*, 1996, pp. 594 – 602.

[138] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: Universal Topology Generation from a User's Perspective," 2001, Boston University Technical Report # BUCS-TR-2001-003.

[139] S.S. Manna1 and P. Sen, "Modulated Scale-free Network in Euclidean Space," *Physical Review E*, vol. 66, no. 6, pp. 1–4, 2002.

[140] S-H Yook, H. Jeong, and A.L. Barabasi, "Modeling the Internet's Large-Scale Topology," *Proceeding National Academic Science USA*, vol. 99, no. 21, pp. 13 382 – 13 386, 2002.

[141] W.J. Reed, "The Pareto, Zipf and Other Power Laws," *Economics Letters*, vol. 74, no. 1, pp. 15–19, 2001.

[142] M. Erickson, *Introduction to combinatorics*. Wiley-Interscience, 1996.

[143] R. Zippel, *Effective polynomial computation*. Kluwer Academic Pub, 1993.