University of California

Los Angeles

Encoding for Degraded Broadcast Channels

and

Resource Allocation for Content Distribution in Peer-to-Peer Networks

A dissertation submitted in partial satisfaction

of the requirements for the degree

Doctor of Philosophy in Electrical Engineering

by

Bike Xie

2010

The dissertation of Bike Xie is approved.

Adnan Darwiche

Lieven Vandenberghe

Mihaela van der Schaar

Richard D. Wesel, Committee Chair

University of California, Los Angeles

2010

Table of Contents

List of Figures

List of Tables

Acknowledgments

My advisor Richard D. Wesel changed my entire life. I still remember the moment when he called me from U.S. to China and finally offered me the Ph.D. admission to UCLA with full fellowship. This offer opened the 5 years of challenging, fulfilling and enjoyable Ph.D. life for me.

Professor Wesel provided me plenary supports to my research in many different aspects. He worked so hard to secure the financial support for the whole research group that I never worried about the living expense in U.S. He fully supports my research interests and provides enough freedom for me to choose my research topics. He teaches me the right approach of the research study and also shows me the conscientious research attitude. He spent a lot of time on discussing research details with me, and reviewing my papers and my dissertation. He even encouraged and supported me to improve my speaking English. I really learned a lot from Professor Wesel in these years. If I had a chance to restart my Ph.D. life, I would definitely want to be Rick's student again.

I was also fortunate to interact with Professor Mihaela van der Schaar, Lieven Vandenberghe, Gregory Pottie, Kung Yao, Alan Laub, Izhak Rubin and Adnan Darwiche. I am grateful for the support and insight which they provided. One of my research topic, P2P network, is inspired, encouraged, and supported by Professor van der Schaar. It is my great pleasure to work with her. I also pressed Professors van der Schaar, Vandenberghe, and Darwiche into service as dissertation readers and members of my orals committee. Thank you for careful reviews you provided for this dissertation. I also want to thank Professor Pottie for being a member of my orals committee. I am so regretful that I cannot have

Professor Pottie as my dissertation reviewer because of the schedule conflict.

Many of my fellow students added substantively to my research through helpful discussions and insightful suggestions. Some especially helpful colleagues are Cong Shen, Wen-Yen Weng, Jun Shi, Andres Vila Casado, Jiadong Wang, Thomas Courtade, Yuan-Mao Chang, Tsung-Yi Chen, Yiyu Shi, Qiyue Zou, Esteban Valles, Miguel Griot, Yi Su, Fangwen Fu, Xinyi Zhang, and Yuxin Han. I had my first journal paper co-authored with Wen-Yen. He provided my many helps and shared with me the surviving strategies at UCLA in my first year. Andres is full of ideas. He was always helpful whenever I had problems. Tom is one of the most brilliant person I have ever met. He is always asking challenge questions which can sharpen my mind and broader my views.

I am also very glad to have many friends at UCLA. Many thanks to Cong Shen who picked me up at LAX and treated me the first dinner in U.S. when I first came to Los Angeles. He also took me to Chinatown every 2 weeks when I didn't know how to drive. Fangwen Fu and Qiyue Zou are golden roommates. I really had a great time with Fangwen at Weyburn and with Qiyue at Mentone. Jiadong Wang is the nicest and most supportive friend. Thank you for helping me to file this dissertation. Jiadong is also a funny-story-talker. I really enjoyed hang out with him no matter where to go.

I also thank some of my friends far from Los Angeles who helps me to pass some lonely days in U.S. I can always find Jiong Chen, Zhenghang Zhu, Lei Yang, Song Mao, Tiantian Huang, Bingqiang Zhu, Zhou Zhou, Yi Ma, Yi Gai, Weiwei Xin, Yi Zhang, Zhen Mao, Hong Xie, Lin Hao, and my cousin, Xiaoqiong Xie, to talk online when I felt lonely.

Specially, I thank Deeona Columbia, who is the director of the Student Affairs Office in the Electrical Engineering department at UCLA. She was extremely helpful to solve all of my requests and questions regarding to school policies and student affairs during these years.

As I write this, I am afraid that several important people are being accidently omitted. I apologize if you deserve to be here, but are not. I hope that you can forgive the oversight.

My parents are a constant source of love and support. Mom, I am sorry that I wasn't be with you when you really needed me. You will always have my love.

Most of all, a big thank you to my wife, Lin. Her love is my happiness and her support is my braveness. She is always a good audience to my practice research presentations even though she has no idea what I am talking about. Lin, thank you for coming into my life. Thank you for coming to U.S. with me. I hope we will always be happy together and both have bright futures. To my wife, I dedicate this dissertation.

Vita

March 18 1983	Born, Shanghai, P. R. China.
2005	B.Eng., Electronic Engineering Tsinghua University Beijing, P. R. China
2006	M.Sc., Electrical Engineering University of California, Los Angeles Los Angeles, California
2006–2010	Research Assistant, Electrical Engineering Department University of California, Los Angeles Los Angeles, California
2008	Intern Software Engineer Google Inc. Mountain View, California
2010	Ph.D., Electrical Engineering University of California, Los Angeles Los Angeles, California

Publications

B. Xie, M. van der Schaar and R. D. Wesel, "Minimizing weighted sum downloading time for one-to-many file transfer in peer-to-peer networks," *In preparation.*

B. Xie and R. D. Wesel, "Optimal encoding schemes for several classes of discrete degraded broadcast channels," *Submitted to IEEE Transactions on Information Theory*, in June 2009.

B. Xie, M. Griot, A. I. Vila Casado and R. D. Wesel, "Optimal transmission strategy and explicit capacity region for broadcast Z channels," *IEEE Transactions on Information Theory*, Vol. 54, No. 9, pp 4296-4304, September 2008.

W.-Y. Weng, C. Kose, **B. Xie** and R. D. Wesel, "Universal serially concatenated trellis coded modulation for space-time channels," *IEEE Transactions on Communications*, Vol. 56, No. 10, pp 1636-1646, October 2008.

T. Courtade, **B. Xie**, and R. D. Wesel, "Optimal exchange of packets for universal recovery in broadcast networks," *Submitted to MILCOM 2010*, in April 2010.

B. Xie and R. D. Wesel,"Minimizing weighted sum delay for one-to-many file transfer in peer-to-peer networks". *IEEE Information Theory and Applications 2010*, San Diego, US, Jan. 31 - Feb. 5, 2010.

B. Xie and R. D. Wesel, "Optimal natural encoding scheme for discrete multiplicative degraded broadcast channels," *IEEE International Symposium on Information Theory 2009*, Seoul, Korea, June 28 - July 3, 2009.

B. Xie and R. D. Wesel,"Optimal independent-encoding schemes for input-symmetric degraded broadcast channels". *IEEE Information Theory and Applications 2009*, San Diego, US, Feb. 8 - Feb. 13, 2009.

B. Xie and R. D. Wesel,"A mutual information invariance approach to symmetry in discrete memoryless channels". *IEEE Information Theory and Applications 2008*, San Diego, US, Jan. 27 - Feb. 1, 2008.

B. Xie, M. Griot, A. I. Vila Casado and R. D. Wesel, "Optimal transmission strategy and capacity region for broadcast Z channels," *IEEE Information Theory Workshop 2007*, Lake Tahoe, CA, US, September 2007.

W.-Y. Weng, **B. Xie** and R. D. Wesel, "Universal space-time serially concatenated trellis coded modulations," *IEEE Global Communications Conference 2006*, San Francisco, US, Nov. 27 - Dec. 1, 2006.

Abstract of the Dissertation

Encoding for Degraded Broadcast Channels and Resource Allocation for Content Distribution in Peer-to-Peer Networks

by

Bike Xie

Doctor of Philosophy in Electrical Engineering

University of California, Los Angeles, 2010

Professor Richard D. Wesel, Chair

The broadcast communication network is a telecommunication network with exactly one source and multiple receivers. This dissertation presents results regarding to two different broadcast communication systems: broadcast channels (BC) and peer-to-peer (P2P) networks. The BC is a single-hop communication network consisting of one transmitter and multiple receivers which observe the transmitted signal through different channels and decode their individual messages. In contrast, the P2P network [1] is a multi-hop broadcast or multi-cast communication network consisting of one source node, possibly some relay nodes, and multiple receivers which download transmitted packages through different routings and decode a common message.

This first part of the dissertation explores encoding schemes for degraded

[1] A general P2P network can simultaneously contain multiple multi-cast communications, and hence have more than one source nodes. In this dissertation, we focus on the simplified model of the P2P network which contains only one broadcast or multi-cast communication.

broadcast channels (DBC) which are BCs with a sequence of receivers, each receiving a degraded version of the signal received by the previous receiver. We are interested in what we call "natural" encoding for the DBC. A natural encoding (NE) scheme is one in which symbols from independent codebooks, each using the same alphabet, are combined using the same single-letter function that adds distortion to the channel. This dissertation shows that NE schemes achieve the boundary of the capacity region for the multi-user broadcast Z channel, the two-user group-additive DBC, and the two-user discrete multiplicative DBC. This dissertation also defines and studies the input-symmetric DBC and introduces a permutation encoding approach for the input-symmetric DBC and proves its optimality.

In addition, this dissertation provides an explicit expression for the capacity region of the two-user broadcast Z channel. Specifically, the NE scheme for the the two-user broadcast Z channel is to encode the information messages corresponding to each user independently and then transmit the binary OR of these two streams. Nonlinear turbo codes that provide a controlled distribution of ones and zeros are used to demonstrate a low-complexity scheme that works close to the optimal boundary.

Inspired by Witsenhausen and Wyner, we define and explore the conditional entropy bound F^* for DBCs. Denote $\boldsymbol{q}$ as the distribution of the channel input X. For any given $\boldsymbol{q}$, and $H(Y|X) \leq s \leq H(Y)$, where $H(Y|X)$ is the conditional entropy of Y given X and $H(Y)$ is the entropy of Y, define the function $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ as the infimum of $H(Z|U)$, the conditional entropy of Z given U with respect to all discrete random variables U such that a) $H(Y|U) = s$, and b) U and Y, Z are conditionally independent given X. This dissertation studies the function F^*, its properties and its calculation. This dissertation then represents the capacity region of the DBC $X \to Y \to Z$ using the function $F^*_{T_{YX},T_{ZX}}$. Finally, this dissertation applies these results to several classes of DBCs and their encoders as discussed above.

The second part of the dissertation investigates the problem of transferring a file from one server to multiple receivers in a peer-to-peer (P2P) network. The objective is to minimize the weighted sum download time (WSDT) for the one-to-many file transfer. Previous work has shown that, given an order at which the receivers finish downloading, the minimum WSDT can be solved in polynomial time by convex optimization, and can be achieved by linear network coding, assuming that node uplinks are the only bottleneck in the network. This dissertation, however, considers heterogeneous peers with both uplink and downlink bandwidth constraints specified. The static scenario is a file-transfer scheme in which the network resource allocation remains static until all receivers finish downloading. This dissertation shows that the static scenario can be optimized in polynomial time by convex optimization, and the associated optimal static WSDT can be achieved by linear network coding. This dissertation also proposes static routing-based and rateless-coding-based schemes that both have almost-optimal empirical performances. The dynamic scenario is a file-transfer scheme which can re-allocate the network resource during the file transfer. This dissertation also proposes a dynamic rateless-coding-based scheme, which provides significantly smaller WSDT than the optimal static scenario does.

CHAPTER 1

Introduction

In the 70's, Cover [1], Bergmans [2] and Gallager [3] established the capacity region for degraded broadcast channels (DBCs), which are broadcast channels (BC) with a sequence of component channels, each being a degraded version of the previous one. A common optimal transmission strategy to achieve the boundary of the capacity region for DBCs is the joint encoding scheme typically referred to as *superposition coding* [4] [1] [2] [3]. Specifically, the data sent to the user with the most degraded channel is encoded first. Given the codeword selected for that user, an appropriate codebook for the user with the second most degraded channel is selected, and so forth.

An independent-encoding scheme can also achieve the capacity of any DBC, as described in Appendix I [5]. This scheme essentially embeds all symbols from all the needed codebooks for the less-degraded user into a single super-symbol (but perhaps with a large alphabet). Then a single-letter function uses the input symbol from the more-degraded user to extract the needed symbol from the super symbol provided by the less-degraded user.

A simple encoding scheme that is optimal for some common DBCs is an independent-encoding approach in which symbols from independent codebooks each with the same alphabet as X are combined using the same single-letter function that adds distortion to the channel. We refer to this encoding scheme as the natural encoding (NE) scheme. As an example, the NE scheme for a two-receiver broadcast Gaussian channel has as each transmitted symbol the real addition of two real symbols from independent codebooks.

The NE scheme is known to achieve the boundary of the capacity region for several broadcast channels including broadcast Gaussian channels [6], broadcast binary-symmetric channels [2] [7] [8] [9], discrete additive degraded broadcast channels [10] and two-user broadcast Z channels [11] [12]. This dissertation shows that NE schemes also achieve the boundary of the capacity region for the multi-user broadcast Z channel, the two-user group-additive DBC, and the two-user discrete multiplicative DBC.

The input-symmetric channel was introduced by Witsenhausen and Wyner [9] and studied in [13] [14] and [15]. We extend the definition of the input-symmetric channel to the definition of the input-symmetric DBC. We introduce an independent-encoding scheme employing permutation functions of independently encoded streams (the permutation encoding approach) for the input-symmetric DBC and proves its optimality. The discrete additive DBC [10] is a special case of the input-symmetric DBC, and the optimal encoding approach for the discrete additive DBC [10] is also a special case of the permutation encoding approach. The group-additive DBC is a class of input-symmetric DBCs whose channel outputs are group additions of the channel input and noise. The permutation encoding approach for the group-additive DBC is the group-addition encoding approach, which is the NE scheme for the group-additive DBC.

A separate question addressed in the dissertation involves content distribution in peer-to-peer (P2P) overlay networks. P2P applications (e.g, [16], [17], [18], [19]) are increasingly popular and represent the majority of the traffic currently transmitted over the Internet. A unique feature of P2P networks is their flexible and distributed nature, where each peer can act as both a server and a client

[20]. Hence, P2P networks provide a cost-effective and easily deployable framework for disseminating large files without relying on a centralized infrastructure [21]. These features of P2P networks have made them popular for a variety of broadcasting and file-distribution applications [21] [22] [23] [24] [25] [26] [27].

In a P2P file transfer application, the key performance metric from an end-user's point of view is the delay, or the time it takes for an end-user to download the file. We consider the problem of minimizing weighted sum downloading time (WSDT) for one-to-many file transfer in a P2P network. Consider a source node s that wants to broadcast a file of size B to a set of N receivers, $\{1, 2, \cdots, N\}$, in a P2P network. We start with a simplified model for the P2P network. It is assumed that node uplinks and downlinks are the only bottlenecks in the network and that every peer can connect to every other peer through routing in the overlay. Most research in P2P consider node uplinks as the only bottlenecks because the uplink capacity is often several times smaller than the downlink capacity for typical residential connections (e.g., DSL and Cable). However, the downlink capacity can still be exceeded when a peer downloads from many other peers simultaneously, as in the routing-based scheme proposed in [28]. For this reason, this dissertation considers heterogeneous peers with both uplink and downlink bandwidth constraints.

The static scenario is a file-transfer scenario in which the network resource allocation keeps static until all the receivers finish downloading. This dissertation shows that the static scenario can be optimized in polynomial time by convex optimization, and the associated optimal static WSDT can be achieved by linear network coding. This dissertation also develops a very tight lower bound to the minimum WSDT, and proposes a static routing-based scheme and a static rateless-coding-based scheme which have almost-optimal empirical performances.

The dynamic scenario is a file-transfer scenario which can re-allocate the network resource during the file transfer. This dissertation also proposes a dynamic rateless-coding-based scheme, which provides significantly smaller WSDT than the optimal static scenario does.

1.1 A Road Map

Chapter 2 introduces a mathematical tool for investigating the encoding schemes for degraded broadcast channels. This mathematical tool provides an closed-form expression of the capacity region and a method to determine the optimal encoding schemes for DBCs.

Chapter 3 applies the mathematical tool developed in Chapter 2 to the multi-user broadcast Z channel, and demonstrates the optimality of the natural encoding scheme for multi-user broadcast Z channels.

Chapter 4 defines and investigates the input-symmetric DBC, which contain most common discrete DBCs. A particular encoding scheme, referred to as permutation encoding scheme, is introduced for IS-DBCs. Chapter 4 also applies the results in Chapter 2 to proves the optimality of the permutation encoding scheme for IS-DBCs.

Chapter 5 combines the results in Chapter 2-4 to demonstrate that the NE scheme also achieves the whole boundary of the capacity region for discrete multiplicative DBCs.

Chapter 6 re-investigates the broadcast Z channel and focuses on the two-user case. An alternative proof without applying the mathematical tool in Chapter 2 is provided for readers who are interested in the two-user broadcast Z channel only. Chapter 6 also provides the details of the optimal encoding scheme for the two-user broadcast Z channel, and provides nonlinear-turbo codes to demonstrate a low-complexity scheme that works close to the optimal boundary.

Chapter 7 investigates the network resource allocation for content distribution in peer-to-peer networks. A simplified model for the P2P network is assumed that node uplinks and downlinks are the only bottlenecks in the network and that every peer can connect to every other peer through routing in the overlay. The static file-distribution scenario and the dynamic scenario are studied separately. For the static scenario, Chapter 7 develops the optimal resource allocation to minimize the weighted sum downloading, an lower bound to the minimum WSDT, and several practical schemes which empirically have almost-optimal performance. For the dynamic scenario, Chapter 7 provides a practical solution to the ordering problem and proposes a rateless-coding-based scheme which provides significantly smaller WSDT than the optimal static scheme does.

Figure 1.1 shows the dependence among chapters. Chapter 2-5 are best read in order. However, Chapter 4 may be read directly after Chapter 2. Reader also may safely go straight to Chapter 6 if the encoding schemes and the practical channel coding design for broadcast Z channels are of primary interest, or Chapter 7 if the resource allocation for content distribution in P2P networks is of primary interest.

1.2 Contributions

The main contributions of this dissertation are the relatively simple encoding schemes for several classes of degraded broadcast channels and the strategies for network resource allocation for content distribution in peer-to-peer networks. The details of the contributions are listed below by chapter.

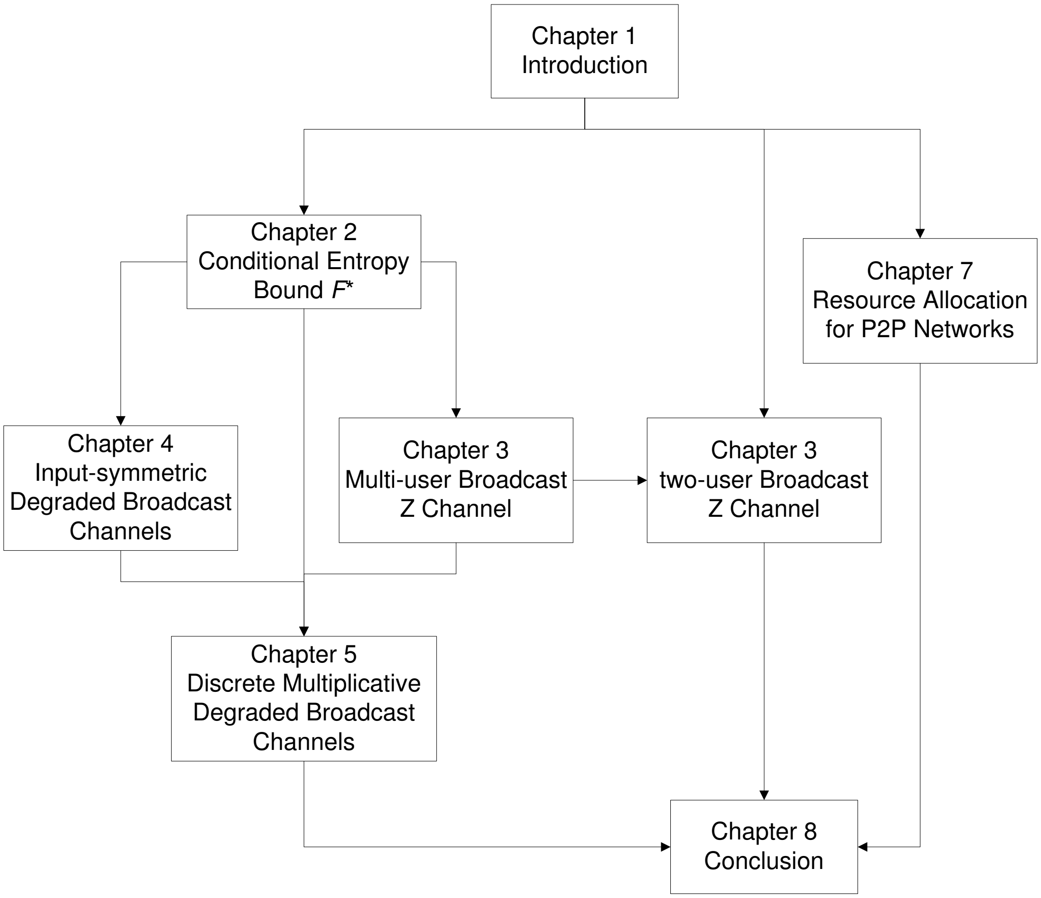


Figure 1.1: Dependence among chapters

Chapter 2) develops a mathematical tool, the conditional entropy bound F^*, for degraded broadcast channels. With the help of this tool, Chapter 2 provides an closed-form expression of the capacity region for DBCs by using F^*, and establishes the relationship between F^* and the optimal encoding schemes for DBCs. These results are applied in Chapter 3-5 to multi-user broadcast Z channels, input-symmetric DBCs, and discrete multiplicative DBCs.

Chapter 3) provides an closed-form expression of the conditional entropy bound F^* to multi-user broadcast Z channels. Based on this result, Chapter 3 applies the results regarding to F^* to multi-user broadcast Z channels and demonstrates that the NE scheme achieves the whole boundary of the capacity region for multi-user DBCs.

Chapter 4) defines the input-symmetric DBCs and introduces the permutation encoding scheme for the IS-DBC. Chapter 4 also applies the conditional entropy bound F^* to prove that the uniform input distribution is optimal, and the permutation encoding scheme achieves the whole boundary of the capacity region for IS-DBCs. As a consequence, the NE scheme for group-additive DBCs achieves the whole boundary of the capacity region.

Chapter 5) combines the results of Chapter 2-4 to prove that the NE scheme also achieves the whole boundary of the capacity region for discrete multiplicative DBCs.

Chapter 6) provides an alternative proof of the optimality of the NE scheme for two-user broadcast Z channels without applying F^*. Chapter 6 also establishes an explicit closed-form expression of the capacity region for two-user broadcast Z channels, develops the details of the optimal encoding scheme, and provides nonlinear-turbo codes to demonstrate a low-complexity scheme that works close to the optimal boundary.

Chapter 7) shows that the static scenario can be optimized in polynomial time by convex optimization, and the associated optimal static WSDT can be achieved by linear network coding. Chapter 7 also proposes a static routing-based scheme and a static rateless-coding-based scheme that have almost-optimal empirical performances. In addition, Chapter 7 provides a practical solution to the ordering problem in dynamic rate allocation and proposes a dynamic rateless-coding-based scheme, which provides significantly smaller WSDT than the optimal static scheme does. The deployment of rateless codes simplifies the mechanism of the file-transfer scenario, enhances the robustness to packet loss in the network, and increases the performance (without considering packet overhead).

CHAPTER 2

A Conditional Entropy Bound for Discrete Degraded Broadcast Channels

Several mathematica tools have been developed to investigate the capacity region and coding scheme for broadcast channels. Shannon's entropy power inequality (EPI) [29] is the first one, which gives a lower bound on the differential entropy of the sum of independent random variables. In Bergmans's remarkable paper [6], he applied EPI to establish a converse showing the optimality of the coding scheme given by [1] [2] (the NE scheme) for broadcast Gaussian channels. "Mrs. Gerber's Lemma" [30] provides a lower bound on the entropy of a sequence of binary-symmetric channel outputs. Wyner and Ziv later developed "Mrs. Gerber's Lemma", which provides a lower bound on the entropy of a sequence of binary-symmetric channel outputs, and applied it to establish a converse showing that the NE scheme for broadcast binary-symmetric channels suggested by Cover [1] and Bergmans [2] achieves the boundary of the capacity region [7]. EPI and "Mrs. Gerber's Lemma" play the same significant role in proving the optimality of the NE schemes for broadcast Gaussian channels and broadcast binary-symmetric channels.

Witsenhausen and Wyner studied a conditional entropy bound for the channel output of a discrete channel and applied the results to establish an outer bound of the capacity region for DBCs [8] [9]. For broadcast binary-symmetric channels, this outer bound coincides with the capacity region.

This chapter extends ideas from Witsenhausen and Wyner [9] to study a conditional entropy bound, F^*, for the channel output of a discrete DBC. We established a number of theorems concerning various properties of this conditional entropy bound and developed two main theorems. The first main theorem represents the capacity region for discrete DBCs with F^*, which bring us a more insight view of the capacity region for DBCs. We apply this theorem in Chapter 2 to prove the optimal input-signal distribution for input-symmetric DBCs. The second main theorem establishes the relationship between the evaluation of F^* and the optimal encoding schemes for the DBC. We later apply this theorem in Chapter 3-5 to prove the optimality of NE scheme for multi-user broadcast Z channels and discrete multiplicative DBCs.

This chapter is organized as follows: Section 2.1 defines the conditional entropy bound $F^*(\cdot)$ for the channel output of a discrete DBC and represents the capacity region of the discrete DBC with the function F^*. Section 2.2 establishes a number of theorems concerning various properties of F^*. Section 2.3 evaluates $F^*(\cdot)$ and indicates the optimal transmission strategy for the discrete DBC. Section **??** delivers the summary.

2.1 The Conditional Entropy Bound $F^*(\cdot)$

Let $X \to Y \to Z$ be a discrete memoryless DBC where $X \in \{1, 2, \cdots, k\}$, $Y \in \{1, 2, \cdots, n\}$ and $Z \in \{1, 2, \cdots, m\}$. Let T_{YX} be an $n \times k$ stochastic matrix with entries $T_{YX}(j, i) = \Pr(Y = j|X = i)$ and T_{ZX} be an $m \times k$ stochastic matrix with entries $T_{ZX}(j, i) = \Pr(Z = j|X = i)$. Thus, T_{YX} and T_{ZX} are the marginal transition probability matrices of the degraded broadcast channel.

Definition 1. *Let vector $\boldsymbol{q}$ in the simplex Δ_k of probability k-vectors be the distribution of the channel input X. Define the function $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ as the infimum of $H(Z|U)$, the conditional entropy of Z given U, with respect to all discrete random variables U such that*

- *a) $H(Y|U) = s$;*
- *b) U and Y, Z are conditionally independent given X, i.e., the sequence U, X, Y, Z forms a Markov chain $U \to X \to Y \to Z$.*

For any fixed vector $\boldsymbol{q}$, the domain of $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ in s is the closed interval $[H(Y|X), H(Y)]$, where $H(Y|X)$ is the conditional entropy of Y given X and $H(Y)$ is the entropy of Y. This will be proved later in Lemma 3. The function $F^*(\cdot)$ is an extension to the function $F(\cdot)$ introduced in [9]. We will use $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$, $F^*(\boldsymbol{q}, s)$ and $F^*(s)$ interchangeably.

Theorem 1. *$F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is monotonically nondecreasing in s and the infimum in its definition is a minimum. Hence, $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ can be taken as the minimum $H(Z|U)$ with respect to all discrete random variables U such that*

- *a) $H(Y|U) \geq s$;*
- *b) U and Y, Z are conditionally independent given X.*

The proof of Theorem 1 will be given in Section 2.2.

Theorem 2. *The capacity region for the discrete memoryless degraded broadcast channel $X \to Y \to Z$ is the closure of the convex hull of all rate pairs (R_1, R_2) satisfying*

$$0 \leq R_1 \leq I(X;Y), \tag{2.1}$$

$$R_2 \leq H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, R_1 + H(Y|X)), \tag{2.2}$$

for some $\boldsymbol{q} \in \Delta_k$, where $I(X;Y)$ is the mutual information of between X and Y, $H(Y|X)$ is the conditional entropy of Y given X, and $H(Z)$ is the entropy of Z resulting from the channel input's distribution $\boldsymbol{q}$. Thus, for a fixed input distribution $\boldsymbol{q}$ and for $\lambda \geq 0$, finding the maximum of $R_2 + \lambda R_1$ is equivalent to finding the minimum of $F^*(\boldsymbol{q}, s) - \lambda s$ as follows:

$$\begin{aligned}
&\max(R_2 + \lambda R_1) \\
&= \max\left(H(Z) - F^*(\boldsymbol{q}, R_1 + H(Y|X)) + \lambda R_1 + \lambda H(Y|X) - \lambda H(Y|X)\right) \\
&= H(Z) - \lambda H(Y|X) + \max\left(-F^*(\boldsymbol{q}, R_1 + H(Y|X)) + \lambda(R_1 + H(Y|X))\right) \\
&= H(Z) - \lambda H(Y|X) - \min\left(F^*(\boldsymbol{q}, s) - \lambda s\right) \qquad (2.3)
\end{aligned}$$

Proof: The capacity region for the DBC is known in [1] [3] [4] as

$$\bar{\text{co}}\left[\bigcup_{p(u),p(x|u)} \{(R_1, R_2) : R_1 \leq I(X;Y|U), R_2 \leq I(U;Z)\}\right], \qquad (2.4)$$

where $\bar{\text{co}}$ denotes the closure of the convex hull operation, and U is the auxiliary random variable which satisfies the Markov chain $U \to X \to Y \to Z$ and $|\mathcal{U}| \leq$

$\min(|\mathcal{X}|, |\mathcal{Y}|, |\mathcal{Z}|)$. Rewrite (2.4) and we have

$$
\begin{aligned}
&\bar{\text{co}}\left[\bigcup_{p(u),p(x|u)} \{(R_1, R_2) : R_1 \le I(X;Y|U), R_2 \le I(U;Z)\}\right] \\
=&\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k} \left\{ \bigcup_{p(u,x) \text{ with } \boldsymbol{p}_X=\boldsymbol{q}} \left\{ (R_1, R_2) : \begin{array}{c} R_1 \le I(X;Y|U) \\ R_2 \le I(U;Z) \end{array} \right\}\right\}\right] \qquad (2.5) \\
=&\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k} \left\{ \bigcup_{p(u,x) \text{ with } \boldsymbol{p}_X=\boldsymbol{q}} \left\{ (R_1, R_2) : \begin{array}{c} R_1 \le H(Y|U) - H(Y|X) \\ R_2 \le H(Z) - H(Z|U) \end{array} \right\}\right\}\right] \qquad (2.6) \\
=&\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k} \left\{ \bigcup_{H(Y|X)\le s\le H(Y)} \left\{ (R_1, R_2) : \begin{array}{c} R_1 \le s - H(Y|X) \\ R_2 \le H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s) \end{array} \right\}\right\}\right] \qquad (2.7) \\
=&\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k} \left\{ (R_1, R_2) : \begin{array}{c} 0 \le R_1 \le I(X;Y) \\ R_2 \le H(Z) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, R_1 + H(Y|X)) \end{array} \right\}\right], \qquad (2.8)
\end{aligned}
$$

where $\boldsymbol{p}_X$ is the vector expression of the distribution of channel input X. Some of these steps are justified as follows:

- (2.5) follows from the equivalence of $\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k} \bigcup_{p(u,x) \text{ with } \boldsymbol{p}_X=\boldsymbol{q}}$ and $\bigcup_{p(u),p(x|u)}$;
- (2.7) follows from the definition of the conditional entropy bound F^*;
- (2.8) follows from the nondecreasing property of $F^*(s)$ in Theorem 1, which allows the substitution $s = R_1 + H(Y|X)$ in the argument of F^*. Q.E.D.

Note that for a fixed distribution $\boldsymbol{p}_X = \boldsymbol{q}$ of the channel input X, the items $I(X;Y)$, $H(Z)$ and $H(Y|X)$ in (2.8) are constants. This theorem provides the relationship between the capacity region and the conditional entropy bound F^* for a discrete degraded broadcast channel. It also motivates the further study of F^*.

2.2 Properties of $F^*(\cdot)$

In this section, we will extend ideas from [9] to establish several properties of the conditional entropy bound $F^*(\cdot)$. In [9], Witsenhausen and Wyner defined a conditional entropy bound $F(\cdot)$ for a pair of discrete random variables and provided some properties of $F(\cdot)$. The definition of $F(\cdot)$ is restated here. Let $X \rightarrow Z$ be a discrete memoryless channel with the $m \times k$ transition probability matrix T, where the entries $T(j, i) = \Pr(Z = j|X = i)$. Let $\boldsymbol{q}$ be the distribution of X. For any $\boldsymbol{q} \in \Delta_k$, and $0 \leq s \leq H(X)$, the function $F_T(\boldsymbol{q}, s)$ is the infimum of $H(Z|U)$ with respect to all discrete random variables U such that $H(X|U) = s$ and the sequence U,X,Z is a Markov chain. By definition, $F_T(\boldsymbol{q}, s) = F^*_{I,T}(\boldsymbol{q}, s)$, where I is an identity matrix. Since $F^*(\cdot)$ is the extension of $F(\cdot)$, most of the properties of $F^*(\cdot)$ in this section are generalizations of properties of $F(\cdot)$ in [9].

For any choice of the integer $l \geq 1$, $\boldsymbol{w} = [w_1, \cdots, w_l]^T \in \Delta_l$ and $\boldsymbol{p}_j \in \Delta_k$ for $j = 1, \cdots, l$, let U be a l-ary random variable with distribution $\boldsymbol{w}$, and let $T_{XU} = [\boldsymbol{p}_1 \cdots \boldsymbol{p}_l]$ be the transition probability matrix from U to X. We can compute

$$\boldsymbol{p} = \boldsymbol{p}_X = T_{XU}\boldsymbol{w} = \sum_{j=1}^{l} w_j \boldsymbol{p}_j \tag{2.9}$$

$$\xi = H(Y|U) = \sum_{j=1}^{l} w_j h_n(T_{YX}\boldsymbol{p}_j) \tag{2.10}$$

$$\eta = H(Z|U) = \sum_{j=1}^{l} w_j h_m(T_{ZX}\boldsymbol{p}_j) \tag{2.11}$$

where $h_n : \Delta_n \to \mathrm{R}$ is the entropy function, i.e., $h_n(p_1, \cdots, p_n) = -\sum p_i \ln p_i$. Thus the choices of U satisfying conditions a) and b) in the definition of $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ corresponds to the choices of l,$\boldsymbol{w}$ and $\boldsymbol{p}_j$ for which (2.9) (2.10) yields $\boldsymbol{p} = \boldsymbol{q}$ and $\xi = s$.

Let $\mathcal{S} = \{(\boldsymbol{p}, h_n(T_{YX}\boldsymbol{p}), h_m(T_{ZX}\boldsymbol{p})) \in \Delta_k \times [0, \ln n] \times [0, \ln n] | \boldsymbol{p} \in \Delta_k\}$. Since Δ_k is $(k-1)$-dimensional, $\Delta_k \times [0, \ln n] \times [0, \ln n]$ is a $(k+1)$-dimensional convex polytope. The mapping $\boldsymbol{p} \to (\boldsymbol{p}, h_n(T_{YX}\boldsymbol{p}), h_m(T_{ZX}\boldsymbol{p}))$ assigns a point in $\mathcal{S}$ for each $\boldsymbol{p} \in \Delta_k$. Because this mapping is continuous and the domain of the mapping, Δ_k, is compact and connected, the image $\mathcal{S}$ is also compact and connected.

Let $\mathcal{C}$ be the set of all $(\boldsymbol{p}, \xi, \eta)$ satisfying (2.9) (2.10) and (2.11) for some choice of l, $\boldsymbol{w}$ and $\boldsymbol{p}_j$. By definition, the set $\mathcal{C}$ is the convex hull of the set $\mathcal{S}$. Thus, $\mathcal{C}$ is compact, connected, and convex.

Lemma 1. *$\mathcal{C}$ is the convex hull of $\mathcal{S}$, and thus $\mathcal{C}$ is compact, connected, and convex.*

Lemma 2. *i) Every point of $\mathcal{C}$ can be obtained by (2.9) (2.10) and (2.11) with $l \leq k+1$. In other words, one only need to consider random variables U taking at most $k+1$ values.*
ii) Every extreme point of the intersection of $\mathcal{C}$ with a two-dimensional plane can

be obtained with $l \leq k$.

The proof of Lemma 2 is the same as the proof of a similar lemma for $F(\cdot)$ in [9]. The details of the proof are given in Appendix II.

Let $\mathcal{C}^* = \{(\xi, \eta) | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\ \}$ be the projection of the set $\mathcal{C}$ onto the (ξ, η)-plane. Let $\mathcal{C}^*_{\boldsymbol{q}} = \{(\xi, \eta) | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\ \}$ be the projection onto the (ξ, η)-plane of the intersection of $\mathcal{C}$ with the two-dimensional plane $\boldsymbol{p} = \boldsymbol{q}$. By definition, $\mathcal{C}^* = \bigcup_{\boldsymbol{q} \in \Delta_k} \mathcal{C}^*_{\boldsymbol{q}}$. Also, $\mathcal{C}^*$ and $\mathcal{C}^*_{\boldsymbol{q}}$ are compact and convex. By definition, $F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s)$ is the infimum of all η, for which $\mathcal{C}^*_{\boldsymbol{q}}$ contains the point (s, η). Thus

$$F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s) = \inf\{\eta | (\boldsymbol{q}, s, \eta) \in \mathcal{C}\} = \inf\{\eta | (s, \eta) \in \mathcal{C}^*_{\boldsymbol{q}}\}. \tag{2.12}$$

Lemma 3. *For any fixed $\boldsymbol{q}$ as the distribution of X, the domain of $F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s)$ in s is the closed interval $[H(Y|X), H(Y)]$, i.e.,$[\sum_{i=1}^k q_i h_n(T_{YX}\boldsymbol{e}_i), h_n(T_{YX}\boldsymbol{q})]$, where $\boldsymbol{e}_i$ is a vector, for which the i^{th} entry is 1 and all other entries are zeros.*

Proof: For any Markov chain $U \rightarrow X \rightarrow Y$, by the Data Processing Theorem [31], $H(Y|U) \geq H(Y|X)$ and the equality is achieved when the random variable $U = X$. One also has $H(Y|U) \leq H(Y)$ and the equality is achieved when U is a constant. Thus, the domain of $F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s)$ in s is $[H(Y|X), H(Y)]$ for a fixed distribution of channel input X. Since $\boldsymbol{q}$ is the distribution of X, $H(Y|X) = \sum_{i=1}^k q_i h_n(T_{YX}\boldsymbol{e}_i)$ and $H(Y) = h_n(T_{YX}\boldsymbol{q})$. Q.E.D.

Theorem 3. *The function $F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s)$ is defined on the compact convex domain $\{(\boldsymbol{q}, s) | \boldsymbol{q} \in \Delta_k, \sum_{i=1}^k q_i h_n(T_{YX}\boldsymbol{e}_i) \leq s \leq h_n(T_{YX}\boldsymbol{q})\}$ and for each $(\boldsymbol{q}, s)$ in this domain, the infimum in its definition is a minimum, attainable with U taking at most $k+1$ values.*

Proof: By Lemma 3, the function F^* is defined on the compact domain

$\{(\boldsymbol{q}, s) | \boldsymbol{q} \in \Delta_k, \sum_{i=1}^{k} q_i h_n(T_{YX}\boldsymbol{e}_i) \leq s \leq h_n(T_{YX}\boldsymbol{q})\}$. This domain is convex because Δ_k is convex, the entropy function $h_n(T_{YX}\boldsymbol{q})$ is concave in $\boldsymbol{q}$ and $\sum_{i=1}^{k} q_i h_n(T_{YX}\boldsymbol{e}_i)$ is linear in $\boldsymbol{q}$. For each $(\boldsymbol{q}, s)$ in this domain, the set $\{\eta | (s, \eta) \in \mathcal{C}_{\boldsymbol{q}}^*\}$ is non-empty. It is in fact a compact interval since $\mathcal{C}_{\boldsymbol{q}}^*$ is compact. Therefore,

$$F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s) = \inf\{\eta | (s, \eta) \in \mathcal{C}_{\boldsymbol{q}}\} = \min\{\eta | (s, \eta) \in \mathcal{C}_{\boldsymbol{q}}\} = \min\{\eta | (\boldsymbol{q}, s, \eta) \in \mathcal{C}\}. \tag{2.13}$$

By Lemma 2 i), this minimum is attained with U taking at most $k + 1$ values. Q.E.D.

By Lemma 2 ii), the extreme points of $\mathcal{C}_{\boldsymbol{q}}^*$ can be attained by convex combinations of at most k points of $\mathcal{S}$. Thus, every linear function of (ξ, η) could attain its minimum with U taking at most k value since every linear function of (ξ, η) achieves its minimum over $\mathcal{C}_{\boldsymbol{q}}^*$ at an extreme point of the compact set $\mathcal{C}_{\boldsymbol{q}}^*$.

Lemma 4. *The function $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is jointly convex in $(\boldsymbol{q}, s)$.*

Proof: $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is jointly convex in $(\boldsymbol{q}, s)$ because $\mathcal{C}$ is a convex set. In particular, the domain of F^* is convex by Theorem 3. For any two points $(\boldsymbol{q_1}, s_1)$ and $(\boldsymbol{q_2}, s_2)$ in the domain, and for any $0 \leq \theta \leq 1$,

$$\begin{aligned}
&F^*_{T_{YX},T_{ZX}}(\theta\boldsymbol{q_1} + (1-\theta)\boldsymbol{q_2}, \theta s_1 + (1-\theta)s_2) \\
=&\min\{\eta | (\theta\boldsymbol{q_1} + (1-\theta)\boldsymbol{q_2}, \theta s_1 + (1-\theta)s_2, \eta) \in \mathcal{C}\} \\
\leq&\min\{\theta\eta_1 + (1-\theta)\eta_2 | (\boldsymbol{q_1}, s_1, \eta_1), (\boldsymbol{q_2}, s_2, \eta_2) \in \mathcal{C}\} \\
=&\theta F^*_{T_{YX},T_{ZX}}(\boldsymbol{q_1}, s_1) + (1-\theta)F^*_{T_{YX},T_{ZX}}(\boldsymbol{q_2}, s_2).
\end{aligned}$$

Therefore, $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is jointly convex in $(\boldsymbol{q}, s)$. Q.E.D.

Now we give the proof of Theorem 1. Since Theorem 3 has shown that the infimum in the definition of F^* is a minimum, it suffices to show that $F^*(s) =$

$F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is monotonically nondecreasing in s. For any fixed $\boldsymbol{q}$, the domain of s is $[H(Y|X), H(Y)]$. On the one hand,

$$\begin{aligned} F^*(\boldsymbol{q}, H(Y|X)) &= \min\{H(Z|U)|\boldsymbol{p}_X = \boldsymbol{q}, H(Y|U) = H(Y|X)\} \\ &\leq \min\{H(Z|U)|\boldsymbol{p}_X = \boldsymbol{q}, U = X\} \\ &= H(Z|X). \end{aligned} \tag{2.14}$$

On the other hand, for any $s \in [H(Y|X), H(Y)]$,

$$\begin{aligned} F^*(\boldsymbol{q}, s) &= \min\{H(Z|U)|\boldsymbol{p}_X = \boldsymbol{q}, H(Y|U) = s\} \\ &\geq \min\{H(Z|U, X)|\boldsymbol{p}_X = \boldsymbol{q}, H(Y|U) = s\} && (2.15) \\ &= H(Z|X), && (2.16) \end{aligned}$$

where (2.15) follows from $H(Z|U) \geq H(Z|U, X)$ and (2.16) follows from the conditional independence between Z and U given X. Inequalities (2.14) and (2.16) imply that for any $s \in [H(Y|X), H(Y)]$,

$$F^*(\boldsymbol{q}, s) \geq F^*(\boldsymbol{q}, H(Y|X)). \tag{2.17}$$

Combining (2.17) and the fact that $F^*(\boldsymbol{q}, s)$ is convex in s for any fixed $\boldsymbol{q}$, we have $F^*(\boldsymbol{q}, s)$ is monotonically nondecreasing in s. Q.E.D.

The proof of Theorem 1 also gives an endpoint of $F^*(s)$,

$$F^*(\boldsymbol{q}, H(Y|X)) = H(Z|X), \tag{2.18}$$

which is achieved when $U = X$. The following theorem will provide the other endpoint,

$$F^*(\boldsymbol{q}, H(Y)) = H(Z), \tag{2.19}$$

which is obtained when U is a constant.

Theorem 4. *For $H(Y|X) \leq s \leq H(Y)$, a lower bound of $F^*(s)$ is*

$$F^*(s) \geq s + H(Z) - H(Y). \tag{2.20}$$

$F^*(s)$ is differentiable at all but at most countably many points. At differentiable points of $F^*(s)$,

$$0 \leq \frac{dF^*(s)}{ds} \leq 1. \tag{2.21}$$

Proof:

$$\begin{aligned} & I(U;Z) \leq I(U;Y) && (2.22)\\ \Rightarrow & H(Z) - H(Z|U) \leq H(Y) - H(Y|U) \\ \Rightarrow & H(Z|U) \geq H(Y|U) + H(Z) - H(Y) \\ \Rightarrow & F^*(s) \geq s + H(Z) - H(Y). && (2.23) \end{aligned}$$

Some of these steps are justified as follows:

- (2.22) follows from the Data Processing Theorem [31];
- (2.23) follows from the definition of $F^*(s)$.

When the random variable U is a constant, $H(Y|U) = H(Y)$ and $H(Z|U) = H(Z)$. Thus, equality in (2.23) is attained when $s = H(Y)$. Since $F^*(s)$ is convex in s, it is differentiable at all but at most countably many points. If $F^*(s)$ is differentiable at $s = H(Y)$, then $\left.\frac{dF^*(s)}{ds}\right|_{s=H(Y)} \leq 1$ because the line $s + H(Z) -$

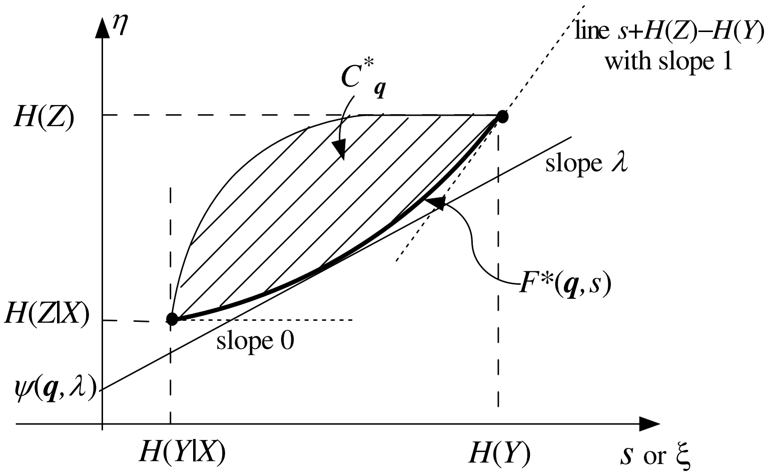


Figure 2.1: Illustrations of the curve $F^*(\boldsymbol{q},s) = F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)$ shown in bold, the region $\mathcal{C}^*_{\boldsymbol{q}}$, and the point $(0,\psi(\boldsymbol{q},\lambda))$.

$H(Y)$ with slope 1 supports the curve $F^*(s)$ at its end point $(H(Y),F^*(H(Y)))$. For any $H(Y|X) \le s < H(Y)$ where $F^*(s)$ is differentiable, since $F^*(s)$ is convex, the slope of the supporting line at the point $(s,F^*(s))$ is less than or equal to the slope of the supporting line $s+H(Z)-H(Y)$ at the point $(H(Y),F^*(H(Y)))$. Thus, for any $H(Y|X) \le s \le H(Y)$ where $F^*(s)$ is differentiable

$$\frac{dF^*(s)}{ds} \le 1. \tag{2.24}$$

$\frac{dF^*(s)}{ds} \ge 0$ because $F^*(s)$ is monotonically nondecreasing. The illustrations of the function $F^*(s) = F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)$ and $\mathcal{C}^*_{\boldsymbol{q}}$ are shown in Fig. 2.1. Q.E.D.

For $X \sim \boldsymbol{q}$, where $\boldsymbol{q}$ is a fixed vector, by Theorem 2, finding the maximum of $R_2+\lambda R_1$ is equivalent to finding the minimum of $F^*(\boldsymbol{q},s)-\lambda s$. Theorem 4 indicates that for every $\lambda > 1$, the minimum of $F^*(\boldsymbol{q},s)-\lambda s$ is attained when $s = H(Y)$ and $F^*(s) = H(Z)$, i.e., U is a constant. Thus, the non-trivial range of λ is $0 \le \lambda \le 1$.

The following theorem is the key to the applications in Section 6.1 and is an extension and generalization of Theorem 2.4 in [9]. Let $\boldsymbol{X} = (X_1, \cdots, X_N)$ be a sequence of channel inputs to the degraded broadcast channel $X \rightarrow Y \rightarrow Z$. The corresponding channel outputs are $\boldsymbol{Y} = (Y_1, \cdots, Y_N)$ and $\boldsymbol{Z} = (Z_1, \cdots, Z_N)$. Thus, the sequence of the channel outputs (Y_i, Z_i), $i = 1, \cdots, N$, are conditionally independent of each other given the channel inputs $\boldsymbol{X}$. Note that the channel outputs (Y_i, Z_i) do *not* have to be identically or independently distributed since $X_1, \cdots, X_N$ could be correlated and have different distributions. Denote $\boldsymbol{q_i}$ as the distribution of X_i for $i = 1, \cdots, N$. Thus, $\boldsymbol{q} = \sum \boldsymbol{q_i}/N$ is the average of the distribution of the channel inputs. For any $\boldsymbol{q} \in \Delta_k$, define $F^*_{T^{(N)}_{YX}, T^{(N)}_{ZX}}(\boldsymbol{q}, Ns)$ be the infimum of $H(\boldsymbol{Z}|U)$ with respect to all random variables U and all possible channel inputs $\boldsymbol{X}$ such that $H(\boldsymbol{Y}|U) = Ns$, the average of the distribution of the channel inputs is $\boldsymbol{q}$ and $U \rightarrow \boldsymbol{X} \rightarrow \boldsymbol{Y} \rightarrow \boldsymbol{Z}$ is a Markov chain.

Theorem 5. *For all $N = 1, 2, \cdots$, and all T_{YX},T_{ZX}, $\boldsymbol{q}$, and $H(Y|X) \leq s \leq H(Y)$, one has*

$$F^*_{T^{(N)}_{YX}, T^{(N)}_{ZX}}(\boldsymbol{q}, Ns) = N F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s). \tag{2.25}$$

Proof: We first prove that $F^*_{T^{(N)}_{YX}, T^{(N)}_{ZX}}(\boldsymbol{q}, Ns) \geq N F^*_{T_{YX}, T_{ZX}}(\boldsymbol{q}, s)$. Since

$$Ns = H(\boldsymbol{Y}|U) = \sum_{i=1}^{N} H(Y_i|Y_1, \cdots, Y_{i-1}, U) \tag{2.26}$$

$$= \sum_{i=1}^{N} s_i, \tag{2.27}$$

where $s_i = H(Y_i|Y_1, \cdots, Y_{i-1}, U)$ and (2.26) follows from the chain rule of entropy

[4],

$$
\begin{aligned}
H(\boldsymbol{Z}|U) &= \sum_{i=1}^{N} H(Z_i|Z_1,\cdots,Z_{i-1},U) && (2.28)\\
&\geq \sum_{i=1}^{N} H(Z_i|Z_1,\cdots,Z_{i-1},Y_1,\cdots,Y_{i-1},U) && (2.29)\\
&= \sum_{i=1}^{N} H(Z_i|Y_1,\cdots,Y_{i-1},U) && (2.30)\\
&\geq \sum_{i=1}^{N} F^*_{T_{YX},T_{ZX}}(\boldsymbol{q_i},s_i) && (2.31)\\
&\geq NF^*_{T_{YX},T_{ZX}}(\sum_{i=1}^{N}\boldsymbol{q_i}/N,\sum_{i=1}^{N}s_i/N) && (2.32)\\
&= NF^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s). && (2.33)
\end{aligned}
$$

Some of these steps are justified as follows:

- (2.28) follows from the chain rule of entropy [4];
- (2.29) holds because conditional entropy decreases when the conditioning increases;
- (2.30) follows from the fact that Z_i and $Z_1,\cdots,Z_{i-1}$ are conditionally independent given $Y_1,\cdots,Y_{i-1}$;
- (2.31) follows from the definition of F^* if considering the Markov chain $(U,Y_1,\cdots,Y_{i-1})\rightarrow X_i\rightarrow Y_i\rightarrow Z_i$;
- (2.32) results from applying Jensen's inequality to the convex function F^*.

By the definition of $F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}(\boldsymbol{q},Ns)$, Equation (2.33) implies that

$$F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}(\boldsymbol{q},Ns)\geq NF^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s). \tag{2.34}$$

On the other hand, in the case that U is composed of N independently identically distributed (i.i.d.) random variables $(U_1, \cdots, U_N)$, and each $U_i \to X_i$ achieves $\boldsymbol{p}_{X_i} = \boldsymbol{q}$, $H(Y_i|U_i) = s$ and $H(Z_i|U_i) = F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$, one has $H(\boldsymbol{Y}|U) = Ns$ and $H(\boldsymbol{Z}|U) = NF^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$. Since $F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}$ is defined by taking the minimum,

$$F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}(\boldsymbol{q}, Ns) \leq NF^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s). \tag{2.35}$$

Combining (2.34) and (2.35), one has $F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}(\boldsymbol{q}, Ns) = NF^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$. Q.E.D.

Theorem 5 indicates that if using the degraded broadcast channel $X \to Y \to Z$ for N times, and for a fixed $\boldsymbol{q}$ as the average of the distribution of the channel inputs, the conditional entropy bound $F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}(\boldsymbol{q}, Ns)$ is achieved when the channel is used independently and identically for N times, and single use of the channel at each time achieves the conditional entropy bound $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$.

2.3 Evaluation of $F^*(\cdot)$

In this section, we evaluate $F^*(s) = F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ via a duality technique, which is also used for evaluating $F(\cdot)$ in [9]. This duality technique also provides the optimal transmission strategy for the DBC $X \to Y \to Z$ to achieve the maximum of $R_2 + \lambda R_1$ for any $\lambda \geq 0$.

Theorem 3 shows that

$$F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s) = \min\{\eta | (s, \eta) \in \mathcal{C}_{\boldsymbol{q}}\} = \min\{\eta | (\boldsymbol{q}, s, \eta) \in \mathcal{C}\}. \tag{2.36}$$

Thus, the function $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ is determined by the lower boundary of $\mathcal{C}^*_{\boldsymbol{q}}$. Since $\mathcal{C}^*_{\boldsymbol{q}}$ is convex, its lower boundary can be described by the lines supporting its graph from the below. The line with slope λ in the (ξ, η)-plane supporting $\mathcal{C}^*_{\boldsymbol{q}}$

as shown in Fig. 2.1 has the equation

$$\eta = \lambda\xi + \psi(\boldsymbol{q}, \lambda), \tag{2.37}$$

where $\psi(\boldsymbol{q}, \lambda)$ is the η-intercept of the tangent line with slope λ for the function $F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$. Thus,

$$\psi(\boldsymbol{q}, \lambda) = \min\{F^*(\boldsymbol{q}, \xi) - \lambda\xi | H(Y|X) \leq \xi \leq H(Y)\} \tag{2.38}$$

$$= \min\{\eta - \lambda\xi | (\xi, \eta) \in \mathcal{C}_{\boldsymbol{q}}\} \tag{2.39}$$

$$= \min\{\eta - \lambda\xi | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\}. \tag{2.40}$$

For $H(Y|X) \leq s \leq H(Y)$, the function $F^*(s) = F^*_{T_{YX},T_{ZX}}(\boldsymbol{q}, s)$ can be represented as

$$F^*(s) = \max\{\psi(\boldsymbol{q}, \lambda) + \lambda s | -\infty < \lambda < \infty\}. \tag{2.41}$$

Theorem 1 shows that the graph of $F^*(s)$ is supported at $s = H(Y|X)$ by a line of slope 0, and Theorem 4 shows that the graph of $F^*(s)$ is supported at $s = H(Y)$ by a line of slope 1. Thus, for $H(Y|X) \leq s \leq H(Y)$,

$$F^*(s) = \max\{\psi(\boldsymbol{q}, \lambda) + \lambda s | 0 \leq \lambda \leq 1\}. \tag{2.42}$$

Let L_λ be a linear transformation $(\boldsymbol{q}, \xi, \eta) \to (\boldsymbol{q}, \eta - \lambda\xi)$. It maps $\mathcal{C}$ and $\mathcal{S}$ onto the sets

$$\mathcal{C}_\lambda = \{(\boldsymbol{q}, \eta - \lambda\xi) | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\}, \tag{2.43}$$

and

$$\mathcal{S}_\lambda = \{(\boldsymbol{q}, h_m(T_{ZX}\boldsymbol{q}) - \lambda h_n(T_{YX}\boldsymbol{q})) | \boldsymbol{q} \in \Delta_k\}. \tag{2.44}$$

The lower boundaries of $\mathcal{C}_\lambda$ and $\mathcal{S}_\lambda$ are the graphs of $\psi(\boldsymbol{q}, \lambda)$ and $\phi(\boldsymbol{q}, \lambda) =$

$h_m(T_{ZX}\boldsymbol{q}) - \lambda h_n(T_{YX}\boldsymbol{q})$ respectively. Since $\mathcal{C}$ is the convex hull of $\mathcal{S}$, and thus $\mathcal{C}_\lambda$ is the convex hull of $\mathcal{S}_\lambda$, $\psi(\boldsymbol{q}, \lambda)$ is the lower convex envelope of $\phi(\boldsymbol{q}, \lambda)$ on Δ_k.

In conclusion, $\psi(\cdot, \lambda)$ can be obtained by forming the lower convex envelope of $\phi(\cdot, \lambda)$ for each λ and $F^*(\boldsymbol{q}, s)$ can be reconstructed from $\psi(\boldsymbol{q}, \lambda)$ by (2.42). This is the dual approach to the evaluation of F^*.

Theorem 2 represents the capacity region for a DBC by the function $F^*(\boldsymbol{q}, s)$. Since $\psi(\boldsymbol{q}, \lambda)$ and $F^*(\boldsymbol{q}, s)$ can be constructed by each other from (2.38) and (2.42), for any $\lambda \geq 0$, the associated point on the boundary of the capacity region may be found (from its unique value of $R_2 + \lambda R_1$) as follows

$$\begin{aligned}
&\max_{\boldsymbol{q} \in \Delta_k} \max\{R_2 + \lambda R_1 | \boldsymbol{p}_X = \boldsymbol{q}\} \\
=&\max_{\boldsymbol{q} \in \Delta_k} \max\{H(Z) - F^*(\boldsymbol{q}, s) + \lambda s - \lambda H(Y|X)\} \\
=&\max_{\boldsymbol{q} \in \Delta_k} (H(Z) - \lambda H(Y|X) - \min\{F^*(\boldsymbol{q}, s) - \lambda s\}) \\
=&\max_{\boldsymbol{q} \in \Delta_k} (H(Z) - \lambda H(Y|X) - \psi(\boldsymbol{q}, \lambda)). \qquad (2.45)
\end{aligned}$$

We have shown the relationship among F^*, ψ and the capacity region for the DBC. Now we state a theorem which provides the relationship among $F^*(\boldsymbol{q}, s)$, $\psi(\boldsymbol{q}, \lambda)$, $\phi(\boldsymbol{q}, \lambda)$, and the optimal transmission strategies for the DBC.

Theorem 6. *i) For any $0 \leq \lambda \leq 1$, if a point of the graph of $\psi(\cdot, \lambda)$ is the convex combination of l points of the graph of $\phi(\cdot, \lambda)$ with arguments $\boldsymbol{p}_j$ and weights w_λ, $j = 1, \cdots, l$, then*

$$F^*_{T_{YX}, T_{ZX}}\left(\sum_j w_j \boldsymbol{p}_j, \sum_j w_j h_n(T_{YX}\boldsymbol{p}_j)\right) = \sum_j w_j h_m(T_{ZX}\boldsymbol{p}_j). \qquad (2.46)$$

Furthermore, for a fixed channel input distribution $\boldsymbol{q} = \sum_j w_j \boldsymbol{p}_j$, the optimal *transmission strategy to achieve the maximum of $R_2 + \lambda R_1$ is determined by l,w_j and $\boldsymbol{p}_j$. In particular, an optimal transmission strategy has $|\mathcal{U}| = l$, $Pr(U = j) = w_j$ and $\boldsymbol{p}_{X|U=j} = \boldsymbol{p}_j$, where $\boldsymbol{p}_{X|U=j}$ denotes the conditional distribution of X given $U = j$.*

ii)For a predetermined channel input distribution $\boldsymbol{q}$, if the transmission strategy $|\mathcal{U}| = l$, $Pr(U = j) = w_j$ and $\boldsymbol{p}_{X|U=j} = \boldsymbol{p}_j$ achieves $\max\{R_2+\lambda R_1 | \sum_j w_j \boldsymbol{p}_j = \boldsymbol{q}\}$, then the point $(\boldsymbol{q}, \psi(\boldsymbol{q}, \lambda))$ is the convex combination of l points of the graph of $\phi(\cdot, \lambda)$ with arguments $\boldsymbol{p}_j$ and weights w_λ, $j = 1, \cdots, l$.

The proof is given in Appendix III.

Note that if for some pair $(\boldsymbol{q}, \lambda)$, $\psi(\boldsymbol{q}, \lambda) = \phi(\boldsymbol{q}, \lambda)$, then the corresponding optimal transmission strategy has $l = 1$, which means U is a constant. Thus, the line $\eta = \lambda\xi + \psi(\boldsymbol{q}, \lambda)$ supports the graph of $F^*(\boldsymbol{q}, \cdot)$ at its endpoint $(H(Y), H(Z)) = (h_n(T_{YX}\boldsymbol{q}), h_m(T_{ZX}\boldsymbol{q}))$.

2.3.1 Example: broadcast binary-symmetric channel

For the broadcast binary-symmetric channel $X \to Y \to Z$ with

$$T_{YX} = \begin{bmatrix} 1-\alpha_1 & \alpha_1 \\ \alpha_1 & 1-\alpha_1 \end{bmatrix}, T_{ZX} = \begin{bmatrix} 1-\alpha_2 & \alpha_2 \\ \alpha_2 & 1-\alpha_2 \end{bmatrix}, \tag{2.47}$$

where $0 < \alpha_1 < \alpha_2 < 1/2$, one has

$$\begin{aligned} \phi(p, \lambda) &\triangleq \phi((p, 1-p)^T, \lambda) \\ &= h_m(T_{ZX}\boldsymbol{q}) - \lambda h_n(T_{YX}\boldsymbol{q}) \\ &= h((1-\alpha_2)p + \alpha_2(1-p)) - \lambda h((1-\alpha_1)p + \alpha_1(1-p)), \end{aligned} \tag{2.48}$$

where $h(x) = -x \ln x - (1-x)\ln(1-x)$ is the binary entropy function. Taking the second derivative of $\phi(p, \lambda)$ with respect to p, we have

$$\begin{aligned}\phi''(p,\lambda) = & \frac{-(1-2\alpha_2)^2}{(\alpha_2 p + (1-\alpha_2)(1-p))((1-\alpha_2)p + \alpha_2(1-p))} \\ & + \frac{\lambda(1-2\alpha_1)^2}{(\alpha_1 p + (1-\alpha_1)(1-p))((1-\alpha_1)p + \alpha_1(1-p))},\end{aligned} \tag{2.49}$$

which has the sign of

$$\rho(p,\lambda) = -(\frac{1-\alpha_1}{1-2\alpha_1} - p)(\frac{1-\alpha_1}{1-2\alpha_1} + p) + \lambda(\frac{1-\alpha_2}{1-2\alpha_2} - p)(\frac{1-\alpha_2}{1-2\alpha_2} + p). \tag{2.50}$$

For any $0 \le \lambda \le 1$,

$$\min_p \rho(p,\lambda) = \frac{\lambda}{4(1-2\alpha_2)^2} - \frac{1}{4(1-2\alpha_1)^2}. \tag{2.51}$$

Thus, for $\lambda \ge (1-2\alpha_2)^2/(1-2\alpha_1)^2$, $\phi''(p,\lambda) \ge 0$ for all $0 \le p \le 1$, and so $\psi(p,\lambda) = \phi(p,\lambda)$. In this case, the optimal transmission strategy achieving the maximum of R_1 also achieves the maximum of $R_2 + \lambda R_1$, and thus the optimal transmission strategy has $l = 1$, which means U is a constant.

Note that $\phi(1/2 + p, \lambda) = \phi(1/2 - p, \lambda)$. For $\lambda < (1-2\alpha_2)^2/(1-2\alpha_1)^2$, $\phi(p,\lambda)$ has negative second derivative on an interval symmetric about $p = 1/2$. Let $p_\lambda = \arg\min_p \phi(p,\lambda)$ with $p_\lambda \le 1/2$. Thus p_λ satisfies $\phi'_p(p_\lambda, \lambda) = 0$.

By symmetry, the envelope $\psi(\cdot, \lambda)$ is obtained by replacing $\phi(p,\lambda)$ on the interval $(p_\lambda, 1-p_\lambda)$ by its minimum over p, which is shown in Fig. 2.2. Therefore, the lower envelope of $\phi(p,\lambda)$ is

$$\psi(p,\lambda) = \begin{cases} \phi(p_\lambda, \lambda), & \text{for } p_\lambda \le p \le 1 - p_\lambda \\ \phi(p,\lambda), & \text{otherwise.} \end{cases} \tag{2.52}$$

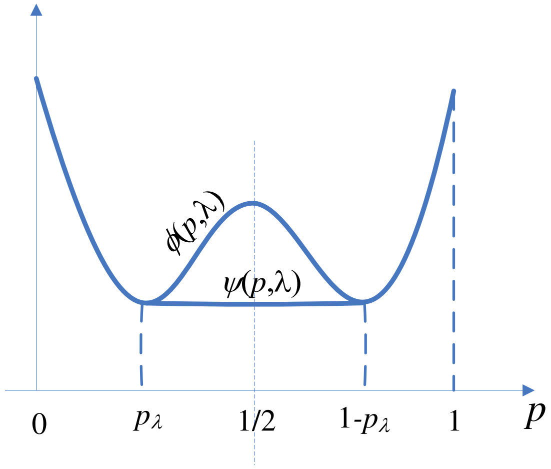


Figure 2.2: Illustration of ϕ and ψ function for the broadcast binary-symmetric channel.

For the predetermined distribution of X, $\boldsymbol{p}_X = \boldsymbol{q} = (q, 1-q)^T$ with $p_\lambda < q < 1-p_\lambda$, $(q, \psi(q,\lambda))$ is the convex combination of the points $(p_\lambda, \psi(p_\lambda,\lambda))$ and $(1-p_\lambda, \psi(1-p_\lambda,\lambda))$. Therefore, by Theorem 6, $F^*(q,s) = h_2(T_{ZX} \cdot (p_\lambda, 1-p_\lambda)^T) = h(\alpha_2 + (1-2\alpha_2)p_\lambda)$ for $s = h_2(T_{YX} \cdot (p_\lambda, 1-p_\lambda)^T) = h(\alpha_1 + (1-2\alpha_1)p_\lambda)$, and $0 \leq p_\lambda \leq q$ or $1-q \leq p_\lambda \leq 1$. This defines $F^*(q,\cdot)$ on its entire domain $[h(\alpha_1), h(\alpha_1 + (1-2\alpha_1)q)]$, i.e., $[H(Y|X), H(Y)]$. For the predetermined distribution of X, $\boldsymbol{q} = (q, 1-q)^T$ with $q < p_\lambda$ or $q > 1-p_\lambda$, one has $\phi(q,\lambda) = \psi(q,\lambda)$, which means that a line with slope λ supports $F^*(q,\cdot)$ at point $s = H(Y) = h(\alpha_1 + (1-2\alpha_1)q$, and thus the optimal transmission strategy has $l = 1$, which means U is a constant.

2.4 Summary

This chapter defines and explores the conditional entropy bound F^* for discrete DBCs. $F^*(\boldsymbol{q}, s)$ is the infimum of $H(Z|U)$ with respect to all auxiliary random variables U given that the input-signal distribution is $\boldsymbol{q}$ and $H(Y|U) = s$. Two main theorems regarding to F^* in this chapter establish the relationship among

F^*, the capacity region, and optimal encoding schemes for DBCs. The first main theorem represents the capacity region for discrete DBCs with F^*, which bring us a more insight view of the capacity region for DBCs. We apply this theorem in Chapter 2 to prove the optimal input-signal distribution for input-symmetric DBCs. The second main theorem establishes the relationship between the evaluation of F^* and the optimal encoding schemes for the DBC. We later apply this theorem in Chapter 3-5 to prove the optimality of NE scheme for multi-user broadcast Z channels and discrete multiplicative DBCs.

CHAPTER 3

Natural Encoding for Multi-User Broadcast Z Channels

3.1 Definition of the Broadcast Z Channel

The Z channel, shown in Fig. 3.1(a), is a binary asymmetric channel which is noiseless when symbol 1 is transmitted but noisy when symbol 0 is transmitted. The channel output Y is the binary OR of the channel input X and Bernoulli distributed noise with parameter α. The capacity of the Z channel was studied in [32]. The Broadcast Z channel is a class of discrete memoryless broadcast channels whose component channels are Z channels. A two-user broadcast Z channel with marginal transition probability matrices

$$T_{YX} = \begin{bmatrix} 1 & \alpha_1 \\ 0 & 1-\alpha_1 \end{bmatrix}, T_{ZX} = \begin{bmatrix} 1 & \alpha_2 \\ 0 & 1-\alpha_2 \end{bmatrix}, \tag{3.1}$$

where $0 < \alpha_1 \leq \alpha_2 < 1$, is shown in Fig 3.1(b). The two-user broadcast Z channel is stochastically degraded and can be modeled as a physically degraded broadcast channel as shown in Fig. 6.4, where $\alpha_\Delta = (\alpha_2 - \alpha_1)/(1-\alpha_1)$ [11]. In the NE scheme for broadcast Z channels, the transmitter first independently encodes users' information messages into binary codewords and then broadcasts the binary OR of these encoded codewords. The NE scheme achieves the whole

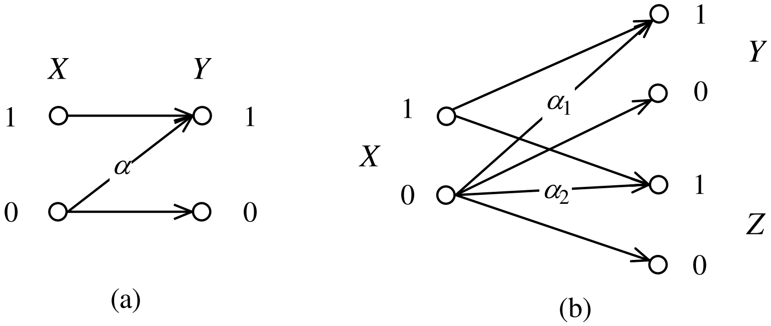


Figure 3.1: The broadcast Z channel

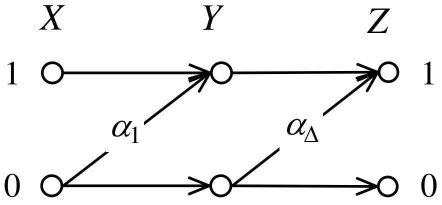


Figure 3.2: The degraded version of the broadcast Z channel

boundary of the capacity region for the two-user broadcast Z channel [11] [12]. In this section, we will show that the NE scheme also achieves the boundary of the capacity region for multi-user broadcast Z channels.

3.2 F^* for the broadcast Z channel

For the broadcast Z channel $X \to Y \to Z$ shown in Fig. 3.1(b) and Fig. 6.4 with

$$T_{YX} = \begin{bmatrix} 1 & \alpha_1 \\ 0 & \beta_1 \end{bmatrix}, T_{ZX} = \begin{bmatrix} 1 & \alpha_2 \\ 0 & \beta_2 \end{bmatrix}, \tag{3.2}$$

where $0 < \alpha_1 \leq \alpha_2 < 1$, $\beta_1 = 1 - \alpha_1$, and $\beta_2 = 1 - \alpha_2$, one has

$$\phi(p, \lambda) \stackrel{\Delta}{=} \phi((1-p, p)^T, \lambda) = h(p\beta_2) - \lambda h(p\beta_1). \tag{3.3}$$

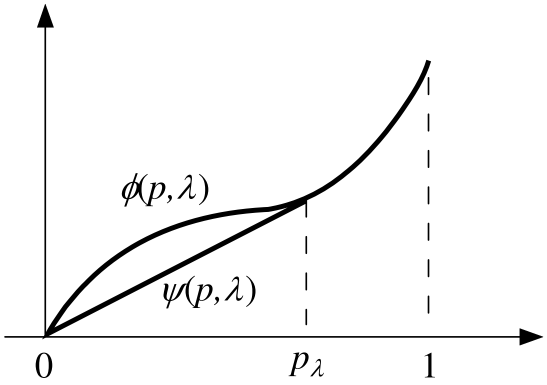


Figure 3.3: Illustrations of $\phi(\cdot,\lambda)$ and $\psi(\cdot,\lambda)$ for the broadcast Z channel

Taking the second derivative of $\phi(p,\lambda)$ with respect to p, we have

$$\phi''(p,\lambda) = \frac{-\beta_2^2}{(1-p\beta_2)p\beta_2} - \frac{-\lambda\beta_1^2}{(1-p\beta_1)p\beta_1}, \tag{3.4}$$

which has the sign of

$$\rho(p,\lambda) = p\beta_1\beta_2(1-\lambda) + \lambda\beta_1 - \beta_2. \tag{3.5}$$

Let $\beta_\Delta \triangleq \beta_2/\beta_1$. For the case of $\beta_\Delta \leq \lambda \leq 1$, $\phi''(p,\lambda) \geq 0$ for all $0 \leq p \leq 1$. Hence, $\phi(p,\lambda)$ is convex in p and thus $\phi(p,\lambda) = \psi(p,\lambda)$ for all $0 \leq p \leq 1$. In this case, the optimal transmission strategy achieving the maximum of R_1 also achieves the maximum of $R_2 + \lambda R_1$, and the optimal transmission strategy has $l = 1$, i.e., U is a constant. Note that the transmission strategy with $l = 1$ is a special case of the NE scheme in which the only codeword for the second user is an all-ones codeword.

For the case of $0 \leq \lambda < \beta_\Delta$, $\phi(p,\lambda)$ is concave in p on $[0, \frac{\beta_2-\lambda\beta_1}{\beta_1\beta_2(1-\lambda)}]$ and convex on $[\frac{\beta_2-\lambda\beta_1}{\beta_1\beta_2(1-\lambda)}, 1]$. The graph of $\phi(\cdot,\lambda)$ in this case is shown in Fig. 3.3. Since $\phi(0,\lambda) = 0$, $\psi(\cdot,\lambda)$, the lower convex envelope of $\phi(\cdot,\lambda)$, is constructed by drawing the tangent through the origin. Let $(p_\lambda, \phi(p_\lambda,\lambda))$ be the point of contact.

The value of p_λ is determined by $\phi'_p(p_\lambda, \lambda) = \phi(p_\lambda, \lambda)/p_\lambda$, i.e.,

$$\ln(1 - \beta_2 p_\lambda) = \lambda \ln(1 - \beta_1 p_\lambda). \tag{3.6}$$

Let $\boldsymbol{q} = (1 - q, q)^T$ be the distribution of the channel input X. For $q \leq p_\lambda$, $\psi(q, \lambda)$ is obtained as a convex combination of points $(0, 0)$ and $(p_\lambda, \phi(p_\lambda, \lambda))$ with weights $(p_\lambda - q)/p_\lambda$ and q/p_λ. By Theorem 6, it corresponds to $s = [(p_\lambda - q)/p_\lambda]0 + [q/p_\lambda]h(\beta_1 p_\lambda) = qh(\beta_1 p_\lambda)/p_\lambda$ and $F^*(q, s) = q/p_\lambda \cdot h(\beta_2 p_\lambda)$. Hence, for the broadcast Z channel,

$$F^*_{T_{YX},T_{ZX}}(q, qh(\beta_1 p)/p) = qh(\beta_2 p)/p \tag{3.7}$$

for $p \in [q, 1]$, which defines $F^*_{T_{YX},T_{ZX}}(q, \cdot)$ on its entire domain $[qh(\beta_1), h(q\beta_1)]$. Also by Theorem 6, the optimal transmission strategy $U \to X$ achieving $\max\{R_2 + \lambda R_1 | \sum_j w_j \boldsymbol{p}_j = \boldsymbol{q}\}$ is determined by $l = 2$, $w_1 = (p_\lambda - q)/p_\lambda$, $w_2 = q/p_\lambda$, $\boldsymbol{p}_1 = (1, 0)^T$ and $\boldsymbol{p}_2 = (1 - p_\lambda, p_\lambda)^T$. Since the optimal transmission strategy $U \to X$ is a Z channel as shown in Fig. 3.4, the random variable X could also be constructed as the OR operation of two Bernoulli random variables with parameters $(p_\lambda - q)/p_\lambda$ and $1 - p_\lambda$ respectively. Hence, the optimal transmission strategy for the broadcast Z channel is still the NE scheme in this case. For $q > p_\lambda$, $\psi(q, \lambda) = \phi(q, \lambda)$ and so the optimal transmission strategy has $l = 1$, i.e., U is a constant. Therefore, we provide an alternative proof to show that the NE scheme achieves the whole boundary of the two-user broadcast Z channel.

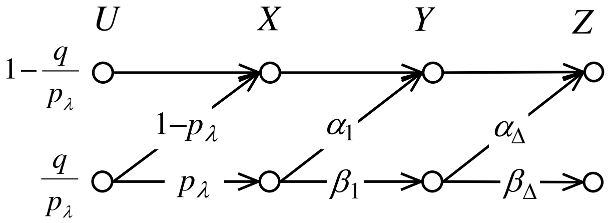


Figure 3.4: The optimal transmission strategy for the two-user broadcast Z channel

3.3 Natural Encoding for Multi-user broadcast Z channel

Let $\boldsymbol{X} = (X_1, \cdots, X_N)$ be a sequence of channel inputs to the broadcast Z channel $X \to Y \to Z$ satisfying (3.2). The corresponding channel outputs are $\boldsymbol{Y} = (Y_1, \cdots, Y_N)$ and $\boldsymbol{Z} = (Z_1, \cdots, Z_N)$. Thus, the sequence of the channel outputs (Y_i, Z_i), $i = 1, \cdots, N$, are conditionally independent with each other given the channel inputs $\boldsymbol{X}$. Note that the channel outputs (Y_i, Z_i) do *not* have to be identically or independently distributed since $X_1, \cdots, X_N$ could be correlated and have different distributions.

Lemma 5. *Consider the Markov chain $U \to \boldsymbol{X} \to \boldsymbol{Y} \to \boldsymbol{Z}$ with $\sum_i Pr(X_i = 0)/N = q$, if*

$$H(\boldsymbol{Y}|U) \geq N \cdot \frac{q}{p} \cdot h(\beta_1 p), \tag{3.8}$$

for some $p \in [q, 1]$, then

$$\begin{aligned} H(\boldsymbol{Z}|U) &\geq N \cdot \frac{q}{p} \cdot h(\beta_2 p) && (3.9) \\ &= N \cdot \frac{q}{p} \cdot h(\beta_1 p \beta_\Delta), && (3.10) \end{aligned}$$

The proof is given in Appendix IV.

Consider a K-user broadcast Z channel with marginal transition probability

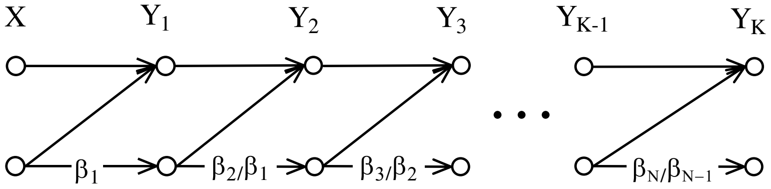


Figure 3.5: The K-user broadcast Z channel

matrices

$$T_{Y_jX} = \begin{bmatrix} 1 & \alpha_j \\ 0 & \beta_j \end{bmatrix}, \tag{3.11}$$

where $0 < \alpha_1 \leq \cdots \leq \alpha_K < 1$, and $\beta_j = 1 - \alpha_j$ for $j = 1, \cdots, K$. The K-user broadcast Z channel is stochastically degraded and can be modeled as a physically DBC as shown in Fig. 3.5. The NE scheme for the K-user broadcast Z channel is to independently encode the K users' information messages into K binary codewords and broadcast the binary OR of these K encoded codewords. The j^{th} user then successively decodes the messages for User K, User $K-1$, $\cdots$, and finally for User j. The codebook for the j^{th} user is designed by random coding technique according to the binary random variable $X^{(j)}$ with $\Pr\{X^{(j)} = 0\} = q^{(j)}$. Denote $X^{(i)} \circ X^{(j)}$ as the OR of $X^{(i)}$ and $X^{(j)}$. Hence, the channel input X is the OR of $X^{(j)}$ for all $1 \leq j \leq K$, i.e., $X = X^{(1)} \circ \cdots \circ X^{(K)}$. From the coding theorem for DBCs [2] [3], the achievable region of the NE scheme for the K-user broadcast Z channel is determined by

$$\begin{aligned}
R_j &\leq I(Y_j, X^{(j)} | X^{(j+1)}, \cdots, X^{(K)}) && (3.12)\\
&= H(Y_j | X^{(j+1)}, \cdots, X^{(K)}) - H(Y_j | X^{(j)}, X^{(j+1)}, \cdots, X^{(K)}) && (3.13)\\
&= \left(\prod_{i=j+1}^{K} q^{(i)} \right) \cdot h(\beta_j \prod_{i=1}^{j} q^{(i)}) - \left(\prod_{i=j}^{K} q^{(i)} \right) \cdot h(\beta_j \prod_{i=1}^{j-1} q^{(i)}) && (3.14)\\
&= \frac{q}{t_j} h(\beta_j t_j) - \frac{q}{t_{j-1}} h(\beta_j t_{j-1}) && (3.15)
\end{aligned}$$

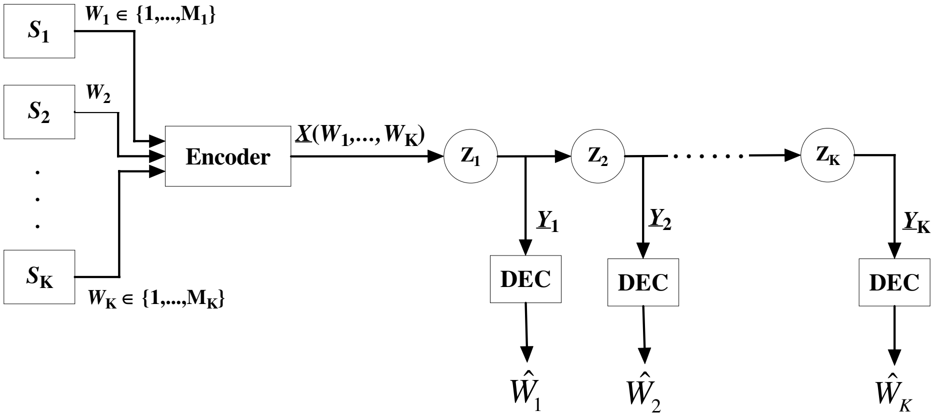


Figure 3.6: The communication system for the multi-user broadcast Z channel

where $t_j = \prod_{i=1}^{j} q^{(i)}$ for $j = 1, \cdots, K$, and $q = \Pr(X = 0) = \prod_{i=1}^{K} q^{(i)}$. Denote $t_0 = 1$. Since $0 \leq q^{(1)}, \cdots, q^{(K)} \leq 1$, one has

$$1 = t_0 \geq t_1 \geq \cdots \geq t_K = q. \tag{3.16}$$

We now state and prove that the achievable region of the NE scheme is the capacity region for the multi-user broadcast Z channel. Fig. 3.6 shows the communication system for the K-user broadcast Z channel. $\boldsymbol{X} = (X_1, \cdots, X_N)$ is a length-N codeword determined by the messages $W_1, \cdots, W_K$. $\boldsymbol{Y_1}, \cdots, \boldsymbol{Y_K}$ are the channel outputs corresponding to the channel input $\boldsymbol{X}$.

Theorem 7. *If $\sum_{i=1}^{N} Pr\{X_i = 0\}/N = q$, then no point $(R_1, \cdots, R_K)$ such that*

$$\begin{cases} R_j \geq \frac{q}{t_j} h(\beta_j t_j) - \frac{q}{t_{j-1}} h(\beta_j t_{j-1}), & j = 1, \cdots, K \\ R_d = \frac{q}{t_d} h(\beta_d t_d) - \frac{q}{t_{d-1}} h(\beta_d t_{d-1}) + \delta, & \textit{for some } d \in \{1, \cdots, K\}, \delta > 0 \end{cases} \tag{3.17}$$

is achievable, where the t_j are as in (3.15) and (3.16).

Proof (by contradiction): This proof borrows the idea of proving the converse of the coding theorem for broadcast Gaussian channels [2]. Lemma 5 plays the same role in this proof as the entropy power inequality does in the proof for broadcast Gaussian channels.

We suppose that the rates of (3.17) are achievable, which means that the probability of decoding error for each receiver can be upper bounded by an arbitrarily small ϵ for sufficiently large N

$$\Pr\{\hat{W}_j \neq W_j | \boldsymbol{Y_j}\} < \epsilon, \quad j = 1, \cdots, K. \tag{3.18}$$

By Fano's inequality, this implies that

$$H(W_j|\boldsymbol{Y_j}) \leq h(\epsilon) + \epsilon \ln(M_j - 1), \quad j = 1, \cdots, K. \tag{3.19}$$

Let $o(\epsilon)$ represent any function of ϵ such that $o(\epsilon) \geq 0$ and $o(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$. Equation (3.19) implies that $H(W_j|\boldsymbol{Y_j})$, $j = 1, \cdots, K$, are all $o(\epsilon)$. Therefore,

$$\begin{aligned}
H(W_j) &= H(W_j|W_{j+1}, \cdots, W_K) && (3.20)\\
&= I(W_j; \boldsymbol{Y_j}|W_{j+1}, \cdots, W_K) + H(W_j|\boldsymbol{Y_j}, W_{j+1}, \cdots, W_K) && (3.21)\\
&\leq I(W_j; \boldsymbol{Y_j}|W_{j+1}, \cdots, W_K) + H(W_j|\boldsymbol{Y_j}) && (3.22)\\
&= H(\boldsymbol{Y_j}|W_{j+1}, \cdots, W_K) - H(\boldsymbol{Y_j}|W_j, W_{j+1}, \cdots, W_K) + o(\epsilon), && (3.23)
\end{aligned}$$

where (3.20) follows from the independence of the W_j, $j = 1, \cdots, K$. From (3.17), (3.23) and the fact that $NR_j \leq H(W_j)$,

$$\begin{aligned}
&H(\boldsymbol{Y_j}|W_{j+1}, \cdots, W_K) - H(\boldsymbol{Y_j}|W_j, W_{j+1}, \cdots, W_K)\\
\geq &N\frac{q}{t_j}h(\beta_j t_j) - N\frac{q}{t_{j-1}}h(\beta_j t_{j-1}) - o(\epsilon).
\end{aligned} \tag{3.24}$$

Next, using Lemma 5 and (3.24), we show in the Appendix V that

$$H(\boldsymbol{Y_K}) \geq Nh(\beta_K q) + N\delta - o(\epsilon), \tag{3.25}$$

where $q = t_K = \sum_{i=1}^{N} \Pr(X_i = 0)/N$. Since ϵ can be arbitrarily small for sufficient large N, $o(\epsilon) \to 0$ as $N \to \infty$. For sufficiently large N, $H(\boldsymbol{Y_K}) \geq Nh(\beta_K q) + N\delta/2$. However, it contradicts

$$\begin{aligned} H(\boldsymbol{Y_K}) &\leq \sum_{i=1}^{N} H(Y_{K,i}) && (3.26)\\ &= \sum_{i=1}^{N} h(\beta_K \cdot \Pr(X_i = 0)) && (3.27)\\ &\leq Nh(\beta_K \cdot \sum_{i=1}^{N} \Pr(X_i = 0)/N) && (3.28)\\ &= Nh(\beta_K q). && (3.29) \end{aligned}$$

Some of these steps are justified as follows:

- (3.26) follows from $\boldsymbol{Y_K} = (Y_{K,1}, \cdots, Y_{K,N})$;
- (3.28) is obtained by applying Jensen's inequality to the concave function $h(\cdot)$;
- (3.29) follows from $q = \sum_{i=1}^{N} \Pr(X_i = 0)/N$.

The desired contradiction has been obtained, so the theorem is proved.

3.4 Summary

This chapter applies the conditional entropy bound F^* to prove that the NE scheme achieves the whole boundary of the capacity region of multi-user DBCs.

As an example of the application of F^*, this chapter shows the power of the mathematica tool of this conditional entropy bound for DBCs.

CHAPTER 4

Permutation Encoding for Input Symmetric Degraded Broadcast Channels

The input-symmetric channel was introduced by Witsenhausen and Wyner [9] and studied in [13] [14] and [15]. We extend the definition of the input-symmetric channel to the definition of the input-symmetric DBC. This chapter introduces an independent-encoding scheme employing permutation functions of independently encoded streams (the permutation encoding approach) for the input-symmetric DBC and proves its optimality. The discrete additive DBC [10] is a special case of the input-symmetric DBC, and the optimal encoding approach for the discrete additive DBC [10] is also a special case of the permutation encoding approach. The group-additive DBC is a class of input-symmetric DBCs whose channel outputs are group additions of the channel input and noise. The permutation encoding approach for the group-additive DBC is the group-addition encoding approach, which is the NE scheme for the group-additive DBC.

Witsenhausen and Wyner made two seminal contributions in [8] and [9]: the notion of minimizing one entropy under the constraint that another related entropy is fixed and the use of input symmetry as a way of solving an entire class of channels with a single unifying approach. Benzel [10] used the first idea to study discrete additive degraded broadcast channels. Recently Liu and Ulukus [13] [14] used both ideas together to extend Benzels results to include the larger class of discrete degraded interference channels (DDIC). This chapter defines what it means for a degraded broadcast channel to be input-symmetric (IS) and provides an independent-encoding scheme which achieves the capacity region of all input-symmetric DBCs.

4.1 Input-Symmetric Degraded Broadcast Channels

The input-symmetric channel was first introduced in [9] and studied further in [13] [14] [15]. The definition of the input-symmetric channel is as follows: Let Φ_n denote the symmetric group of permutations of n objects by the $n \times n$ permutation matrices. An n-input m-output channel with transition probability matrix $T_{m\times n}$ is input-symmetric if the set

$$\mathcal{G}_T = \{G \in \Phi_n | \exists \Pi \in \Phi_m, \text{ s.t. } TG = \Pi T\} \tag{4.1}$$

is transitive, which means each element of $\{1, \cdots, n\}$ can be mapped to every other element of $\{1, \cdots, n\}$ by some permutation matrix in $\mathcal{G}_T$ [9]. An important property of input-symmetric channel is that the uniform distribution achieves capacity.

Extend the definition of the input-symmetric channel to the input-symmetric DBC as follows:

Definition 2. *Input-Symmetric Degraded Broadcast Channel: A discrete memoryless DBC $X \to Y \to Z$ with $|\mathcal{X}| = k$, $|\mathcal{Y}| = n$ and $|\mathcal{Z}| = m$ is input-symmetric* *if the set*

$$\begin{aligned}\mathcal{G}_{T_{YX},T_{ZX}} &\triangleq \mathcal{G}_{T_{YX}} \cap \mathcal{G}_{T_{ZX}} && (4.2)\\ &= \{G \in \Phi_k | \exists \Pi_{YX} \in \Phi_n, \Pi_{ZX} \in \Phi_m,\\ &\quad s.t.\ T_{YX}G = \Pi_{YX}T_{YX}, T_{ZX}G = \Pi_{ZX}T_{ZX}\} && (4.3)\end{aligned}$$

is transitive.

Lemma 6. $\mathcal{G}_{T_{YX},T_{ZX}}$ *is a group under matrix multiplication.*

Proof: Every closed subset of a group is a group. Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a subset of Φ_k, which is a group under matrix multiplication, it suffices to show that $\mathcal{G}_{T_{YX},T_{ZX}}$ is closed under matrix multiplication. Suppose $G_1, G_2 \in \mathcal{G}_{T_{YX},T_{ZX}}$ such that $T_{YX}G_1 = \Pi_{YX,1}T_{YX}$, $T_{ZX}G_1 = \Pi_{ZX,1}T_{ZX}$, $T_{YX}G_2 = \Pi_{YX,2}T_{YX}$ and $T_{ZX}G_2 = \Pi_{ZX,2}T_{ZX}$. Thus,

$$T_{YX}G_1G_2 = \Pi_{YX,1}\Pi_{YX,2}T_{YX}, \tag{4.4}$$

and

$$T_{ZX}G_1G_2 = \Pi_{ZX,1}\Pi_{ZX,2}T_{ZX}. \tag{4.5}$$

Therefore, $G_1G_2 \in \mathcal{G}_{T_{YX},T_{ZX}}$. Q.E.D.

Let $l = |\mathcal{G}_{T_{YX},T_{ZX}}|$ and $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$.

Lemma 7. $\sum_{i=1}^{l} G_i = \frac{l}{k}\mathbf{1}\mathbf{1}^T$, *where* $\frac{l}{k}$ *is an integer and* $\mathbf{1}$ *is an all-ones vector.*

Proof: Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a group, for all $j = 1, \cdots, l$,

$$G_j \left(\sum_{i=1}^{l} G_i \right) = \sum_{i=1}^{l} G_j G_i = \sum_{i=1}^{l} G_i. \tag{4.6}$$

Hence, $\sum_{i=1}^{l} G_i$ has k identical columns and k identical rows since $\mathcal{G}_{T_{YX},T_{ZX}}$ is transitive. Therefore, $\sum_{i=1}^{l} G_i = \frac{l}{k}\mathbf{1}\mathbf{1}^T$. Q.E.D.

Definition 3. *A subset of* $\mathcal{G}_{T_{YX},T_{ZX}}$*:* $\{G_{i_1}, \cdots, G_{i_{l_s}}\}$ *is a smallest transitive subset of* $\mathcal{G}_{T_{YX},T_{ZX}}$ *if*

$$\sum_{j=1}^{l_s} G_{i_j} = \frac{l_s}{k}\mathbf{1}\mathbf{1}^T, \tag{4.7}$$

where $\frac{l_s}{k}$ *is the smallest possible integer for which (4.7) is satisfied.*

4.2 Examples: broadcast binary-symmetric channels and broadcast binary-erasure channels

The class of input-symmetric DBCs includes most of the common discrete memoryless DBCs. For example, the broadcast binary-symmetric channel $X \to Y \to Z$ with marginal transition probability matrices

$$T_{YX} = \begin{bmatrix} 1-\alpha_1 & \alpha_1 \\ \alpha_1 & 1-\alpha_1 \end{bmatrix} \text{ and } T_{ZX} = \begin{bmatrix} 1-\alpha_2 & \alpha_2 \\ \alpha_2 & 1-\alpha_2 \end{bmatrix},$$

where $0 \leq \alpha_1 \leq \alpha_2 \leq 1/2$, is input-symmetric since

$$\mathcal{G}_{T_{YX},T_{ZX}} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \tag{4.8}$$

is transitive.

Another interesting example is the broadcast binary-erasure channel with

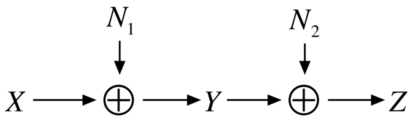


Figure 4.1: The group-additive degraded broadcast channel.

marginal transition probability matrices

$$T_{YX} = \begin{bmatrix} 1-a_1 & 0 \\ a_1 & a_1 \\ 0 & 1-a_1 \end{bmatrix} \text{ and } T_{ZX} = \begin{bmatrix} 1-a_2 & 0 \\ a_2 & a_2 \\ 0 & 1-a_2 \end{bmatrix},$$

where $0 \leq a_1 \leq a_2 \leq 1$. It is input-symmetric since its $\mathcal{G}_{T_{YX},T_{ZX}}$ is the same as that of the broadcast binary-symmetric channel shown in (4.8).

4.3 Group-additive DBC

Definition 4. *Group-additive Degraded Broadcast Channel: A degraded broadcast channel $X \to Y \to Z$ with $X, Y, Z \in \{1, \cdots, n\}$ is a group-additive degraded broadcast channel if there exist two n-ary random variables N_1 and N_2 such that $Y \sim X \oplus N_1$ and $Z \sim Y \oplus N_2$ as shown in Fig. 4.1, where $\sim$ denotes identical distribution and $\oplus$ denotes group addition.*

The class of group-additive DBCs includes the broadcast binary-symmetric channel and the discrete additive DBC [10] as special cases.

Theorem 8. *Group-additive DBCs are input-symmetric.*

Proof: For the group-additive DBC $X \to Y \to Z$ with $X, Y, Z \in \{1, \cdots, n\}$, let G_x for $x = 1, \cdots, n$, be 0-1 matrices with entries

$$G_x(i,j) = \begin{cases} 1 & \text{if } j \oplus x = i \\ \\ 0 & \text{otherwise} \end{cases} \text{ for } i,j = 1, \cdots, n. \tag{4.9}$$

G_x for $x = 1, \cdots, n$, are actually permutation matrices and have the property that $G_{x_1} \cdot G_{x_2} = G_{x_2} \cdot G_{x_1} = G_{x_1 \oplus x_2}$. Let $(\gamma_0, \cdots, \gamma_{n-1})^T$ be the distribution of N_1. Since Y has the same distribution as $X \oplus N_1$, one has

$$T_{YX} = \sum_{x=1}^{n} \gamma_x G_x. \tag{4.10}$$

Hence, $T_{YX} G_x = G_x T_{YX}$ for all $x = 1, \cdots, n$. Similarly, we have $T_{ZX} G_x = G_x T_{ZX}$ for all $x = 1, \cdots, n$, and so

$$\{G_1, \cdots, G_n\} \subseteq \mathcal{G}_{T_{YX}, T_{ZX}}. \tag{4.11}$$

Since the set $\{G_1, \cdots, G_n\}$ is transitive by definition, $\mathcal{G}_{T_{YX}, T_{ZX}}$ is also transitive and hence the group-additive degraded broadcast channel is input-symmetric. Q.E.D.

By definition, $\sum_{j=1}^{n} G_j = \mathbf{1}\mathbf{1}^T$, and hence, $\{G_1, \cdots, G_n\}$ is a smallest transitive subset of $\mathcal{G}_{T_{YX}, T_{ZX}}$ for the group-additive DBC.

4.4 Example: IS-DBC not covered in [13] [14]

The class of DDICs and the corresponding DBCs studied in [13] [14] have to satisfy the condition that the transition probability matrix T_{ZY} is input-symmetric, i.e., $\mathcal{G}_{T_{ZY}}$ is transitive. The input-symmetric DBC, however, does not have to satisfy this condition. The following example provides an IS-DBC which is not covered in [13] [14]. Consider a DBC $X \to Y \to Z$ with transition probability matrices

$$T_{YX} = \begin{bmatrix} a & c \\ b & d \\ c & a \\ d & b \end{bmatrix}, T_{ZY} = \begin{bmatrix} e & f & g & h \\ g & h & e & f \end{bmatrix},$$

and

$$T_{ZX} = T_{ZY}T_{YX} = \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}, \tag{4.12}$$

where $a + c = b + d = 1$, $e + f + g + h = 1$, $\alpha = ae + bf + cg + dh$ and $\beta = ag + bh + ce + df$. This DBC is input-symmetric since its $\mathcal{G}_{T_{YX},T_{ZX}}$ is the same as that of the broadcast binary-symmetric channel shown in (4.8). It is not covered in [13] [14] because

$$\mathcal{G}_{T_{ZY}} = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right\} \tag{4.13}$$

is *not* transitive.

4.5 Optimal input distribution and capacity region

Consider the input-symmetric DBC $X \to Y \to Z$ with the marginal transition probability matrices T_{YX} and T_{ZX}. Recall that the set $\mathcal{C}$ is the set of all $(\boldsymbol{p}, \xi, \eta)$ satisfying (2.9) (2.10) and (2.11) for some choice of l, $\boldsymbol{w}$ and $\boldsymbol{p}_j$, $j = 1, \cdots, l$, the set $\mathcal{C}^* = \{(\xi, \eta) | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\ \}$ is the projection of the set $\mathcal{C}$ on the (ξ, η)-plane, and the set $\mathcal{C}^*_{\boldsymbol{q}} = \{(\xi, \eta) | (\boldsymbol{q}, \xi, \eta) \in \mathcal{C}\ \}$ is the projection on the (ξ, η)-plane of the intersection of $\mathcal{C}$ with the two-dimensional plane $\boldsymbol{p} = \boldsymbol{q}$.

Lemma 8. *For any permutation matrix* $G \in \mathcal{G}_{T_{YX},T_{ZX}}$ *and* $(\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$*, one has* $(G\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$*.*

Proof: Since $(\boldsymbol{p}, \xi, \eta)$ satisfying (2.9) (2.10) and (2.11) for some choice of l, $\boldsymbol{w}$ and $\boldsymbol{p}_j$,

$$\sum_{j=1}^{l} w_j G\boldsymbol{p}_j = G\boldsymbol{p} \tag{4.14}$$

$$\sum_{j=1}^{l} w_j h_n(T_{YX} G\boldsymbol{p}_j) = \sum_{j=1}^{l} w_j h_n(\Pi_{YX} T_{YX} \boldsymbol{p}_j) = \xi \tag{4.15}$$

$$\sum_{j=1}^{l} w_j h_m(T_{ZX} G\boldsymbol{p}_j) = \sum_{j=1}^{l} w_j h_m(\Pi_{YX} T_{ZX} \boldsymbol{p}_j) = \eta. \tag{4.16}$$

Hence, $(G\boldsymbol{p}, \xi, \eta)$ satisfying (2.9) (2.10) and (2.11) for the choice of l, $\boldsymbol{w}$ and $G\boldsymbol{p}_j$,$j = 1, \cdots, l$. Q.E.D.

Corollary 1. $\forall \boldsymbol{p} \in \Delta_k$ *and* $G \in \mathcal{G}_{T_{YX},T_{ZX}}$*, one has* $\mathcal{C}^*_{G\boldsymbol{p}} = \mathcal{C}^*_{\boldsymbol{p}}$*, and so* $F^*(G\boldsymbol{p}, s) = F^*(\boldsymbol{p}, s)$ *for any* $H(Y|X) \le s \le H(Y)$*.*

Lemma 9. *For any input-symmetric DBC,* $\mathcal{C}^* = \mathcal{C}^*_{\boldsymbol{u}}$*, where* $\boldsymbol{u}$ *denotes the uniform distribution.*

Proof: For any $(\xi, \eta) \in \mathcal{C}^*$, there exits a distribution $\boldsymbol{p}$ such that $(\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$. Let $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$. By Corollary 1, $(G_j\boldsymbol{p}, \xi, \eta) \in \mathcal{C}$ for all $j = 1, \cdots, l$. By the convexity of the set $\mathcal{C}$,

$$(\boldsymbol{q}, \xi, \eta) = (\sum_{j=1}^{l} G_j\boldsymbol{p}\ , \xi, \eta) \in \mathcal{C}, \tag{4.17}$$

where $\boldsymbol{q} = \sum_{j=1}^{l} G_j \boldsymbol{p}$. Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a group , for any permutation matrix $G' \in \mathcal{G}_{T_{YX},T_{ZX}}$,

$$G'\boldsymbol{q} = \sum_{j=1}^{l} G' G_j \boldsymbol{p} = \sum_{j=1}^{l} G_j \boldsymbol{p} = \boldsymbol{q}. \tag{4.18}$$

Since $G'\boldsymbol{q} = \boldsymbol{q}$, the i^{th} entry and the j^{th} entry of $\boldsymbol{q}$ are the same if G' permutes the i^{th} row to the j^{th} row. Since the set $\mathcal{G}_{T_{YX},T_{ZX}}$ for an input-symmetric DBC is transitive, all the entries of $\boldsymbol{q}$ are the same, and so $\boldsymbol{q} = \boldsymbol{u}$. This implies that $(\xi, \eta) \in \mathcal{C}^*_{\boldsymbol{u}}$. Since (ξ, η) is arbitrarily taken from $\mathcal{C}^*$, one has $\mathcal{C}^* \subseteq \mathcal{C}^*_{\boldsymbol{u}}$. On the other hand, by definition, $\mathcal{C}^* \supseteq \mathcal{C}^*_{\boldsymbol{u}}$. Therefore, $\mathcal{C}^* = \mathcal{C}^*_{\boldsymbol{u}}$. Q.E.D.

Now we state and prove that the uniformly distributed X is optimal for input-symmetric DBCs.

Theorem 9. *For any input-symmetric DBC, its capacity region can be achieved by using the transmission strategies such that the broadcast signal X is uniformly distributed. As a consequence, the capacity region is*

$$\bar{co} \left\{ (R_1, R_2) : \begin{array}{c} R_1 \leq s - h_n(T_{YX}\boldsymbol{e_1}), \\ R_2 \leq h_m(T_{ZX}\boldsymbol{u}) - F^*_{T_{YX},T_{ZX}}(\boldsymbol{u}, s), \end{array} \quad h_n(T_{YX}\boldsymbol{e_1}) \leq s \leq \ln(n) \right\}, \tag{4.19}$$

where $\boldsymbol{e_1} = (1, 0, \cdots, 0)^T$, $n = |\mathcal{Y}|$, and $m = |\mathcal{Z}|$.

Proof: Let $\boldsymbol{q} = (q_1, \cdots, q_k)^T$ be the distribution of the channel input X for the input-symmetric DBC $X \to Y \to Z$. Since $\mathcal{G}_{T_{YX}}$ is transitive, the columns of T_{YX} are permutations of each other.

$$\begin{aligned}
H(Y|X) &= \sum_{i=1}^{k} H(Y|X=i) && (4.20)\\
&= \sum_{i=1}^{k} q_i h_n(T_{YX}\boldsymbol{e_i}) && (4.21)\\
&= \sum_{i=1}^{k} q_i h_n(T_{YX}\boldsymbol{e_1}) && (4.22)\\
&= h_n(T_{YX}\boldsymbol{e_1}), && (4.23)
\end{aligned}$$

which is independent of $\boldsymbol{q}$. Let $l = |\mathcal{G}_{T_{YX},T_{ZX}}|$ and $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$.

$$\begin{aligned}
H(Z) &= h_m(T_{ZX}\boldsymbol{q}) && (4.24)\\
&= h_m(T_{ZX}\boldsymbol{q}) && (4.25)\\
&= \frac{1}{l}\sum_{i=1}^{l} h_m(T_{ZX}G_i\boldsymbol{q}) && (4.26)\\
&\le h_m(T_{ZX}\frac{1}{l}\sum_{i=1}^{l} G_i\boldsymbol{q}) && (4.27)\\
&= h_m(T_{ZX}\boldsymbol{u}), && (4.28)
\end{aligned}$$

where (4.27) follows from Jensen's inequality. Since $\mathcal{C}^* = \mathcal{C}^*_{\boldsymbol{u}}$ for the input-symmetric DBC,

$$F^*(\boldsymbol{q}, s) \ge F^*(\boldsymbol{u}, s). \qquad (4.29)$$

Plugging (4.23), (4.28) and (4.29) into (2.7), the expression of the capacity region for the DBC, the capacity region for input-symmetric DBCs is

$$\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k}\left\{(R_1,R_2):R_1\le s-H(Y|X),R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\right\}\right] \tag{4.30}$$

$$\subseteq\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k}\left\{(R_1,R_2):\begin{array}{c}R_1\le s-h_n(T_{YX}\boldsymbol{e_1})\\ R_2\le h_m(T_{ZX}\boldsymbol{u})-F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s)\end{array}\right\}\right] \tag{4.31}$$

$$=\bar{\text{co}}\left\{(R_1,R_2):\begin{array}{c}R_1\le s-h_n(T_{YX}\boldsymbol{e_1})\\ R_2\le h_m(T_{ZX}\boldsymbol{u})-F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s)\end{array}\right\} \tag{4.32}$$

$$=\bar{\text{co}}\left\{(R_1,R_2):\boldsymbol{p}_X=\boldsymbol{u},R_1\le s-H(Y|X),R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{u},s)\right\} \tag{4.33}$$

$$\subseteq\bar{\text{co}}\left[\bigcup_{\boldsymbol{p}_X=\boldsymbol{q}\in\Delta_k}\left\{(R_1,R_2):R_1\le s-H(Y|X),R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\right\}\right], \tag{4.34}$$

Note that (4.30) and (4.34) are identical expressions, hence (4.30 - 4.34) are all equal. Therefore, (4.19) and (4.32) express the capacity region for the input-symmetric DBC, which also means that the capacity region can be achieved by using transmission strategies where the broadcast signal X is uniformly distributed. Q.E.D.

4.6 Permutation encoding approach and its optimality

The permutation encoding approach is an independent-encoding scheme which achieves the capacity region for input-symmetric DBCs. The block diagram of this approach is shown in Fig. 4.2. In Fig. 4.2, W_1 is the message for User 1, which sees the better channel T_{YX}, and W_2 is the message for User 2, which sees the

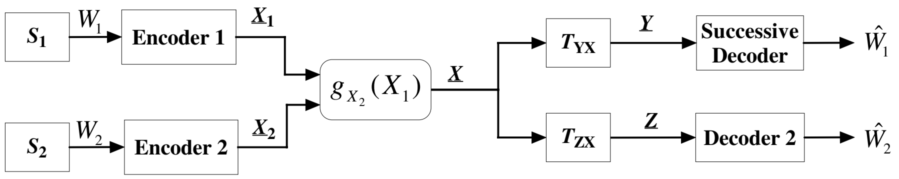


Figure 4.2: The block diagram of the permutation encoding approach

worse channel T_{ZX}. The permutation encoding approach is first to independently encode these two messages into two codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$, and then to combine these two independent codewords using a single-letter operation.

Let $\mathcal{G}_s$ be a smallest transitive subset of $\mathcal{G}_{T_{YX},T_{ZX}}$. Denote $k = |\mathcal{X}|$ and $l_s = |\mathcal{G}_s|$. Use a random coding technique to design the codebook for User 1 according to the k-ary random variable X_1 with distribution $\boldsymbol{p_1}$ and the codebook for User 2 according to the l-ary random variable X_2 with uniform distribution. Let $\mathcal{G}_s = \{G_1, \cdots, G_{l_s}\}$. Define the permutation function $g_{x_2}(x_1) = x$ if the permutation matrix G_{x_2} maps the x_1^{th} column to the x^{th} column, where $x_2 \in \{1, \cdots, l_s\}$ and $x, x_1 \in \{1, \cdots, k\}$. Hence, $g_{x_2}(x_1) = x$ if and only if the x_1^{th} row, x^{th} column entry of G_{x_2} is 1. The permutation encoding approach is then to broadcast $\boldsymbol{X}$ which is obtained by applying the single-letter permutation function $X = g_{X_2}(X_1)$ on symbols of codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$. Since X_2 is uniformly distributed and $\sum_{j=1}^{l_s} G_j = \frac{l_s}{k}\mathbf{1}\mathbf{1}^T$, the broadcast signal X is also uniformly distributed.

User 2 receives $\boldsymbol{Z}$ and decodes the desired message directly. User 1 receives $\boldsymbol{Y}$ and successively decodes the message for User 2 and then for User 1. The structure of the successive decoder is shown in Fig. 4.3. Note that Decoder 1 in Fig. 4.3 is *not* a joint decoder even though it has two inputs $\boldsymbol{Y}$ and $\boldsymbol{\hat{X}_2}$.

In particular, for the group-additive DBC with $Y \sim X \oplus N_1$ and $Z \sim Y \oplus N_2$, the permutation function $g_{x_2}(x_1)$ is the group addition $x_2 \oplus x_1$. Hence the permutation encoding approach for the group-additive DBC is the NE scheme

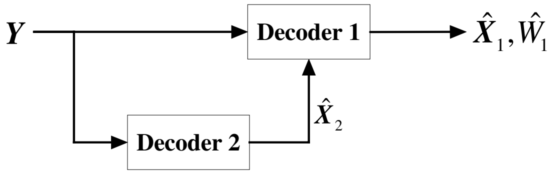


Figure 4.3: The structure of the successive decoder for input-symmetric DBCs

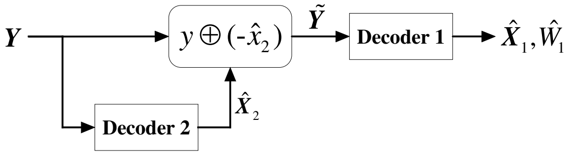


Figure 4.4: The structure of the successive decoder for degraded group-addition channels

for the group-additive DBC. The successive decoder for the group-additive DBC is shown in Fig. 4.4, where

$$\tilde{y} = y \oplus (-\hat{x}_2). \tag{4.35}$$

From the coding theorem for DBCs [2] [3], the achievable region of the permutation encoding approach for the input-symmetric DBC is determined by

$$\begin{aligned}
R_1 &\leq I(X;Y|X_2) && (4.36)\\
&= H(Y|X_2) - H(Y|X) && (4.37)\\
&= \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) H(Y|X_2 = x_2) - \sum_{x=1}^{k} \Pr(X = x) H(Y|X = x) && (4.38)\\
&= \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_n(T_{YX} G_{x_2} \boldsymbol{p_1}) - \sum_{x=1}^{k} \Pr(X = x) h_n(T_{YX} \boldsymbol{e}_x) && (4.39)\\
&= \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_n(\Pi_{YX,x_2} T_{YX} \boldsymbol{p_1}) - \sum_{x=1}^{k} \Pr(X = x) h_n(T_{YX} \boldsymbol{e}_1) && (4.40)\\
&= h_n(T_{YX} \boldsymbol{p_1}) - h_n(T_{YX} \boldsymbol{e}_1), && (4.41)
\end{aligned}$$

and

$$
\begin{aligned}
R_2 &\leq I(X_2; Z) && (4.42)\\
&= H(Z) - H(Z|X_2) && (4.43)\\
&= h_m(T_{ZX}\boldsymbol{u}) - \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_m(T_{ZX} G_{x_2} \boldsymbol{p_1}) && (4.44)\\
&= h_m(T_{ZX}\boldsymbol{u}) - \sum_{x_2=1}^{l_s} \Pr(X_2 = x_2) h_m(\Pi_{ZX,x_2} T_{ZX} \boldsymbol{p_1}) && (4.45)\\
&= h_m(T_{ZX}\boldsymbol{u}) - h_m(T_{ZX}\boldsymbol{p_1}), && (4.46)\\
& && (4.47)
\end{aligned}
$$

where $\boldsymbol{u}$ is the k-ary uniform distribution, $\boldsymbol{p}_1$ is the distribution of X_1, and $\boldsymbol{e}_x$ is a 0-1 vector such that the x^{th} entry is 1 and all other entries are 0. Hence, the achievable region is

$$
\bar{\text{co}} \left[\bigcup_{\boldsymbol{p_1} \in \Delta_k} \left\{ (R_1, R_2) : \begin{array}{c} R_1 \leq h_n(T_{YX}\boldsymbol{p_1}) - h_n(T_{YX}\boldsymbol{e_1}) \\ R_2 \leq h_m(T_{ZX}\boldsymbol{u}) - h_m(T_{ZX}\boldsymbol{p_1}) \end{array} \right\} \right] \tag{4.48}
$$

Define $\tilde{F}(s)$ as the infimum of $h_m(T_{ZX}\boldsymbol{p_1})$ with respect to all distributions $\boldsymbol{p_1}$ such that $h_n(T_{YX}\boldsymbol{p_1}) = s$. Hence the achievable region (4.48) can be expressed as

$$
\left\{ (R_1, R_2) : \begin{array}{c} R_1 \leq s - h_n(T_{YX}\boldsymbol{e_1}), \\ R_2 \leq h_m(T_{ZX}\boldsymbol{u}) - \underline{\text{env}}\tilde{F}(s), \end{array} \quad h_n(T_{YX}\boldsymbol{e_1}) \leq s \leq h_n(T_{YX}\boldsymbol{u}) \right\}, \tag{4.49}
$$

where $\underline{\text{env}}\tilde{F}(s)$ denotes the lower convex envelope of $\tilde{F}(s)$. In order to show that the achievable region (4.49) is the same as the capacity region (4.19) for the input-symmetric DBC, it suffices to show that

$$\underline{\mathrm{env}}\tilde{F}(s) \leq F^*(\boldsymbol{u}, s) \tag{4.50}$$

For any $U \to X$ with uniformly distributed X,

$$\begin{aligned}
H(Z|U) &= \sum_u \Pr(U = u) H(Z|U = u) && (4.51)\\
&= \sum_u \Pr(U = u) h_m(T_{ZX}\boldsymbol{p}_{X|U=u}) && (4.52)\\
&\geq \sum_u \Pr(U = u) \tilde{F}(h_n(T_{YX}\boldsymbol{p}_{X|U=u})) && (4.53)\\
&\geq \sum_u \Pr(U = u) \underline{\mathrm{env}}\tilde{F}(h_n(T_{YX}\boldsymbol{p}_{X|U=u})) && (4.54)\\
&\geq \underline{\mathrm{env}}\tilde{F}(\sum_u \Pr(U = u) h_n(T_{YX}\boldsymbol{p}_{X|U=u})) && (4.55)\\
&= \underline{\mathrm{env}}\tilde{F}(H(Y|U)), && (4.56)
\end{aligned}$$

where $\boldsymbol{p}_{X|U=u}$ is the conditional distribution of X given $U = u$. Some of these steps are justified as follows:

- (4.53) follows from the definition of $\tilde{F}(s)$;
- (4.55) follows from Jensen's inequality.

Therefore, by definition, $\underline{\mathrm{env}}\tilde{F}(s) \leq F^*(\boldsymbol{u}, s)$.

The results of this subsection may be summarized in the following theorem.

Theorem 10. *The permutation encoding approach achieves the capacity region for input-symmetric DBCs, which is expressed in (4.48) (4.49) and (4.19).*

Corollary 2. *The group-addition encoding approach achieves the capacity region for group-additive degraded broadcast channels.*

Conjecture 1. *The alphabet size of the code for User 2, l_s, is equal to the alphabet size of the channel input, k, in a permutation encoding approach for any input-symmetric DBC. In other words, a smallest transitive subset $\{G_1, \cdots, G_{l_s}\}$ of $\mathcal{G}_{T_{YX}, T_{ZX}}$ for any input-symmetric DBC has*

$$\sum_{j=1}^{l_s} G_j = \mathbf{1}\mathbf{1}^T. \tag{4.57}$$

4.7 Summary

The input-symmetric DBC is a class of discrete DBCs, which contains most commonly studied DBCs including broadcast binary-symmetric channels, broadcast binary-erasure channels, and group-additive DBCs. This chapter defines the input symmetry for DBCs and introduces the permutation encoding scheme which employs permutation functions of independently encoded streams for the input-symmetric DBC. We apply the results regarding to F^* in Chapter 2 to prove that the uniform input distribution is optimal for IS-DBCs and then the permutation encoding scheme achieves the whole capacity region for IS-DBCs. As a consequence, the NE scheme (also the permuatation encoding scheme) for group-additive DBCs achieves the whole capacity region.

CHAPTER 5

Natural Encoding for Discrete Multiplicative Degraded Broadcast Channels

The discrete multiplicative DBC is a discrete DBC whose channel outputs are discrete multiplications (multiplications in a finite field) of the channel input and noise. This chapter combines the results of Chapter 3, Chapter 4, and the results of the conditional entropy bound to prove that the NE scheme achieves the whole boundary of the capacity region for discrete multiplicative DBC.

5.1 Discrete Multiplicative Degraded Broadcast Channels

Definition 5. *Discrete Multiplicative Degraded Broadcast Channel: A discrete DBC $X \rightarrow Y \rightarrow Z$ with $X, Y, Z \in \{0, 1, \cdots, n\}$ is a discrete multiplicative degraded broadcast channel if there exist two $(n+1)$-ary random variables N_1 and N_2 such that $Y \sim X \otimes N_1$ and $Z \sim Y \otimes N_2$ as shown in Fig. 5.1, where $\otimes$ denotes discrete multiplication.*

By the definition of discrete multiplication and group addition, the multiplication of zero and any element in $\{0, 1, \cdots, n\}$ is always zero and $\{1, \cdots, n\}$ under the discrete multiplication operation forms a group. Hence, the discrete DBC $X \rightarrow Y \rightarrow Z$ has the channel structure as shown in Fig. 5.2. The subchannel $\tilde{X} \rightarrow \tilde{Y} \rightarrow \tilde{Z}$ is a group-additive DBC with marginal distributions $T_{\tilde{Y}\tilde{X}}$

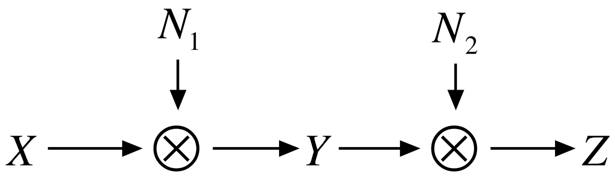


Figure 5.1: The discrete degraded broadcast multiplication channel.

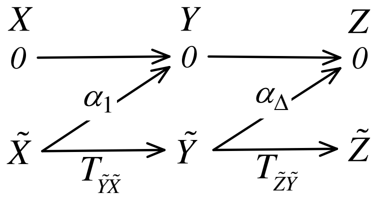


Figure 5.2: The channel structure of a DBC with erasures.

and $T_{\tilde{Z}\tilde{X}} = T_{\tilde{Z}\tilde{Y}} T_{\tilde{Y}\tilde{X}}$, where $\tilde{\mathcal{X}}$, $\tilde{\mathcal{Y}}$, $\tilde{\mathcal{Z}} = \{1, \cdots, n\}$. For the discrete multiplicative DBC $X \to Y \to Z$, if the channel input X is zero, the channel outputs Y and Z are zeros for sure. If the channel input is a non-zero symbol, the channel output Y is zero with probability α_1 and Z is zero with probability α_2, where $\alpha_2 = \alpha_1 + (1 - \alpha_1)\alpha_\Delta$. Therefore, the marginal transmission probability matrices for $X \to Y \to Z$ are

$$T_{YX} = \begin{bmatrix} 1 & \alpha_1 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_1) T_{\tilde{Y}\tilde{X}} \end{bmatrix}, T_{ZY} = \begin{bmatrix} 1 & \alpha_\Delta \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_\Delta) T_{\tilde{Z}\tilde{Y}} \end{bmatrix}, \tag{5.1}$$

and

$$T_{ZX} = T_{ZY} T_{YX} = \begin{bmatrix} 1 & \alpha_1 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_1) T_{\tilde{Y}\tilde{X}} \end{bmatrix} \begin{bmatrix} 1 & \alpha_\Delta \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_\Delta) T_{\tilde{Z}\tilde{Y}} \end{bmatrix} = \begin{bmatrix} 1 & \alpha_2 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_2) T_{\tilde{Z}\tilde{Y}} \end{bmatrix}, \tag{5.2}$$

where $\mathbf{1}$ is an all-ones vector and $\mathbf{0}$ is an all-zeros vector.

5.2 Optimal input distribution

The sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$ is a group-additive DBC, and hence, $\mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}}$ is transitive. For any $n \times n$ permutation matrix $\tilde{G} \in \mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}}$ with $T_{\tilde{Y}\tilde{X}}\tilde{G} = \Pi_{\tilde{Y}\tilde{X}}T_{\tilde{Y}\tilde{X}}$ and $T_{\tilde{Z}\tilde{X}}\tilde{G} = \Pi_{\tilde{Z}\tilde{X}}T_{\tilde{Z}\tilde{X}}$, the $(n+1) \times (n+1)$ permutation matrix

$$G = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G} \end{bmatrix} \tag{5.3}$$

has

$$T_{YX}G = \begin{bmatrix} 1 & \alpha_1 \mathbf{1}^T \\ \mathbf{0} & (1-\alpha_1)T_{\tilde{Y}\tilde{X}} \end{bmatrix} \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G} \end{bmatrix} = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \Pi_{\tilde{Y}\tilde{X}} \end{bmatrix} T_{YX}, \tag{5.4}$$

and so $G \in \mathcal{G}_{T_{YX}}$. Similarly, $G \in \mathcal{G}_{T_{ZX}}$, and hence $G \in \mathcal{G}_{T_{YX},T_{ZX}}$. Therefore, any non-zero element in $\{0, 1, \cdots, n\}$ can be mapped to any other non-zero element in $\{0, 1, \cdots, n\}$ by some permutation matrix in $\mathcal{G}_{T_{YX},T_{ZX}}$, however, no matrix in $\mathcal{G}_{T_{YX},T_{ZX}}$ maps zero to non-zero element or non-zero element to zero. Hence, any permutation matrix $G \in \mathcal{G}_{T_{YX},T_{ZX}}$ has

$$G = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G} \end{bmatrix}, \tag{5.5}$$

for some $\tilde{G} \in \mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}}$. These results may be summarized in the following Lemma:

Lemma 10. *Let* $\mathcal{G}_{T_{\tilde{Y}\tilde{X}},T_{\tilde{Z}\tilde{X}}} = \{\tilde{G}_1, \cdots, \tilde{G}_l\}$. *Hence,* $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$, *where*

$$G_j = \begin{bmatrix} 1 & \mathbf{0}^T \\ \mathbf{0} & \tilde{G}_j \end{bmatrix}, \tag{5.6}$$

for $j = 1, \ldots, l$.

Now we state and prove that the uniformly distributed $\tilde{X}$ is optimal for the discrete degraded broadcast multiplication channel.

Lemma 11. *Let $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}_{\tilde{X}}^T)^T \in \Delta_{n+1}$ be the distribution of channel input X, where $\boldsymbol{p}_{\tilde{X}}$ is the distribution of $\tilde{X}$. For any discrete multiplicative DBC, $\mathcal{C}^*_{\boldsymbol{p}_X} \subseteq \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$ and $\mathcal{C}^* = \bigcup_{q\in[0,1]} \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$, where $\boldsymbol{u} \in \Delta_n$ denotes the uniform distribution.*

The proof of Lemma 11 is similar to that of Lemma 9 and the details are given in Appendix VI.

Theorem 11. *The capacity region of the discrete multiplicative degraded broadcast channel can be achieved by using transmission strategies where $\tilde{X}$ is uniformly distributed, i.e., the distribution of X has $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$. As a consequence, the capacity region is*

$$\bar{co}\Big[\bigcup_{q\in[0,1]} \big\{(R_1,R_2) : R_1 \le s - qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}),$$

$$R_2 \le h((1-\alpha_2)q) + (1-\alpha_2)q\ln(n) - F^*_{T_{YX},T_{ZX}}((1-q,q\boldsymbol{u}^T)^T, s)\big\}\Big]. \qquad (5.7)$$

Proof: Let $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}_{\tilde{X}})^T$ be the distribution of the channel input X, where $\boldsymbol{p}_{\tilde{X}} = (p_1, \cdots, p_n)^T$. Since $\mathcal{G}_{T_{\tilde{Y}\tilde{X}}}$ is transitive and the columns of $T_{\tilde{Y}\tilde{X}}$ are permutations of each other.

$$
\begin{aligned}
H(Y|X) &= \sum_{i=0}^{n} H(Y|X=i) && (5.8)\\
&= (1-q)H(Y|X=0) + \sum_{i=1}^{n} qp_i h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_i}) && (5.9)\\
&= \sum_{i=1}^{n} qp_i h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}) && (5.10)\\
&= qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}), && (5.11)
\end{aligned}
$$

which is independent of $\boldsymbol{p}_X$. Let $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$.

$$
\begin{aligned}
H(Z) &= h_{n+1}(T_{ZX}\boldsymbol{p}_X) && (5.12)\\
&= \frac{1}{l}\sum_{i=1}^{l} h_{n+1}(T_{ZX}G_i\boldsymbol{p}_X) && (5.13)\\
&\leq h_{n+1}(T_{ZX}\frac{1}{l}\sum_{i=1}^{l} G_i\boldsymbol{p}_X) && (5.14)\\
&= h_{n+1}\left(T_{ZX}(1-q, q\boldsymbol{u}^T)^T\right) && (5.15)\\
&= h((1-\alpha_2)q) + (1-\alpha_2)q\ln(n) && (5.16)
\end{aligned}
$$

where (5.14) follows from Jensen's inequality. Since $\mathcal{C}^*_{\boldsymbol{p}_X} \subseteq \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$ for the discrete multiplicative DBC,

$$F^*(\boldsymbol{p}_X, s) \geq F^*((1-q, q\boldsymbol{u}^T)^T, s). \tag{5.17}$$

Plugging (5.11), (5.16) and (5.17) into (2.7), the capacity region for discrete multiplicative DBCs is

$$\begin{aligned}
&\bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X\in\Delta_k}\big\{(R_1,R_2):R_1\le s-H(Y|X),\\
&\qquad\qquad R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\big\}\Big] && (5.18)\\
\subseteq\ &\bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X\in\Delta_k}\big\{(R_1,R_2):R_1\le s-h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}),\\
&\qquad\qquad R_2\le h((1-\alpha_2)q)+(1-\alpha_2)q\ln(n)\\
&\qquad\qquad\qquad -F^*_{T_{YX},T_{ZX}}((1-q,q\boldsymbol{u}^T)^T,s)\big\}\Big] && (5.19)\\
=\ &\bar{\text{co}}\Big[\bigcup_{q\in[0,1]}\big\{(R_1,R_2):R_1\le s-qh_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{e_1}),\\
&\qquad\qquad R_2\le h((1-\alpha_2)q)+(1-\alpha_2)q\ln(n)\\
&\qquad\qquad\qquad -F^*_{T_{YX},T_{ZX}}((1-q,q\boldsymbol{u}^T)^T,s)\big\}\Big] && (5.20)\\
=&\bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X=(1-q,q\boldsymbol{u}^T)^T}\big\{(R_1,R_2):R_1\le s-H(Y|X),\\
&\qquad\qquad R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\big\}\Big] && (5.21)\\
\subseteq&\bar{\text{co}}\Big[\bigcup_{\boldsymbol{p}_X\in\Delta_k}\big\{(R_1,R_2):R_1\le s-H(Y|X),\\
&\qquad\qquad R_2\le H(Z)-F^*_{T_{YX},T_{ZX}}(\boldsymbol{q},s)\big\}\Big], && (5.22)
\end{aligned}$$

where $\bar{\text{co}}$ denotes the convex hull of the closure. Note that (5.18) and (5.22) are identical expressions, hence (5.18 - 5.22) are all equal. Therefore, (5.20) expresses the capacity region for the DM-DBC, which also means that the capacity region can be achieved by using transmission strategies where the broadcast signal X has distribution $\boldsymbol{p}_X=(1-q,q\boldsymbol{u}^T)^T$ for some $q\in[0,1]$. Q.E.D.

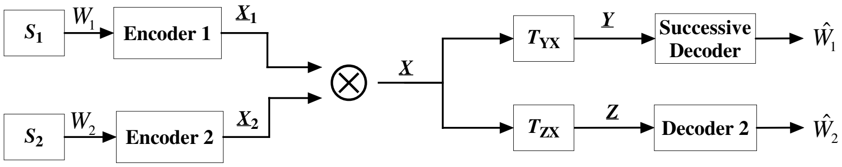


Figure 5.3: The block diagram of the NE scheme for the discrete multiplicative DBC.

5.3 Optimality of the NE scheme for DM-DBCs

The NE scheme for the discrete multiplicative DBC is shown in Fig. 5.3. W_1 is the message for User 1 who sees the better channel T_{YX} and W_2 is the message for User 2 who sees the worse channel T_{ZX}. The NE scheme is first to independently encode these two messages into two codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$ respectively, and then to broadcast $\boldsymbol{X}$ which is obtained by applying the single-letter multiplication function $X = X_2 \otimes X_1$ on symbols of codewords $\boldsymbol{X_1}$ and $\boldsymbol{X_2}$. The distribution of X_2 is constrained to be $\boldsymbol{p}_{X_2} = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$ and hence the distribution of the broadcast signal X also has $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ for some $q \in [0,1]$, which was proved to be the optimal input distribution for the discrete multiplicative DBC. User 2 receives $\boldsymbol{Z}$ and decodes the desired message directly. User 1 receives $\boldsymbol{Y}$ and successively decodes the message for User 2 and then for User 1.

Let $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}_{\tilde{X}})^T$ be the distribution of the channel input X, where $\boldsymbol{p}_{\tilde{X}}$ is the distribution of sub-channel input $\tilde{X}$. For the discrete multiplicative DBC

$X \to Y \to Z$,

$$
\begin{aligned}
\phi(\boldsymbol{p}_X, \lambda) &= h_{n+1}(T_{ZX}\boldsymbol{p}_X) - \lambda h_{n+1}(T_{YX}\boldsymbol{p}_X) && (5.23)\\
&= h_{n+1}(\begin{bmatrix} 1-q+q\alpha_2 \\ q(1-\alpha_2)T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}} \end{bmatrix}) - \lambda h_{n+1}(\begin{bmatrix} 1-q+q\alpha_1 \\ q(1-\alpha_1)T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}} \end{bmatrix}) && (5.24)\\
&= h(q(1-\alpha_2)) - q(1-\alpha_2)h_n(T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}})\\
&- \lambda\left(h(q(1-\alpha_1)) - q(1-\alpha_1)h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}})\right) && (5.25)\\
&= h(q\beta_2) - \lambda h(q\beta_1) + q\beta_2(h_n(T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}}) - \frac{\lambda}{1-\alpha_\Delta}h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}})), && (5.26)
\end{aligned}
$$

where $\beta_1 = 1-\alpha_1$ and $\beta_2 = 1-\alpha_2$.

For the sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$, define $\tilde{\phi}(\boldsymbol{p}_{\tilde{X}}, \frac{\lambda}{1-\alpha_\Delta}) = h_n(T_{\tilde{Z}\tilde{X}}\boldsymbol{p}_{\tilde{X}}) - \frac{\lambda}{1-\alpha_\Delta}h_n(T_{\tilde{Y}\tilde{X}}\boldsymbol{p}_{\tilde{X}})$. Define $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$ as follows:

$$
\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda) = h(q\beta_2) - \lambda h(q\beta_1) + q\beta_2\tilde{\psi}(\boldsymbol{p}_{\tilde{X}}, \frac{\lambda}{1-\alpha_\Delta}), \qquad (5.27)
$$

where $\tilde{\psi}$ is the lower envelope of $\tilde{\phi}(\boldsymbol{p}_{\tilde{X}}, \frac{\lambda}{1-\alpha_\Delta})$ in $\boldsymbol{p}_{\tilde{X}}$. With this definition, note that $\psi(\boldsymbol{p}_X, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$, is also the lower envelope of $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$.

Lemma 12. *$\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_X$ at $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ is on the lower envelope of $\varphi(q, \boldsymbol{u}, \lambda)$ in q.*

The proof is given in Appendix VII. Lemma 12 indicates that the lower envelope of $\phi(\cdot, \lambda)$ at $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$ can be decomposed into two steps. First, for any fixed q, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_{\tilde{X}}$ is $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$. Second, for $\boldsymbol{p}_{\tilde{X}} = \boldsymbol{u}$, the lower envelope of $\varphi(q, \boldsymbol{u}, \lambda)$ in q coincides with $\psi(\boldsymbol{p}_X, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_X$.

Now we state and prove that the NE scheme is optimal for the discrete multiplicative DBC.

Theorem 12. *The NE scheme with time sharing achieves the boundary of the capacity region for the discrete multiplicative degraded broadcast channel.*

Proof : Theorem 11 shows that the boundary of the capacity region for the discrete multiplicative DBC can be achieved by using transmission strategies with uniformly distributed $\tilde{X}$, i.e., the input distribution $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$. For $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$, $\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$ can be attained by the convex combination of points on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$. Since

$$\varphi(q, \boldsymbol{u}, \lambda) = h(q\beta_2) - \lambda h(q\beta_1) + q\beta_2\tilde{\psi}(\boldsymbol{u}, \frac{\lambda}{1-\alpha_\Delta}), \tag{5.28}$$

which is the sum of $\phi(q, \lambda)$ for the broadcast Z channel and q times the constant $\beta_2\tilde{\psi}(\boldsymbol{u}, \frac{\lambda}{1-\alpha_\Delta})$. Hence, by a discussion analogous to Section 6.1, $\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$ can be attained by the convex combination of 2 points on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$. One point is at $q = 0$ and $\varphi(0, \boldsymbol{u}, \lambda) = 0$. The other point is at $q = p_\lambda$, where p_λ is determined by $\ln(1 - \beta_2 p_\lambda) = \lambda \ln(1 - \beta_1 p_\lambda)$.

Note that the point (0,0) on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$ is also on the graph of $\phi(\boldsymbol{p}_X, \lambda)$. By Theorem 6, the point $(p_\lambda, \varphi(p_\lambda, \boldsymbol{u}, \lambda))$ is the convex combination of n points on the graph of $\phi(\boldsymbol{p}_X, \lambda)$, which corresponds to the group-addition encoding approach for the sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$ because the group-addition encoding approach is the optimal NE scheme for the group-additive DBC $\tilde{X} \to \tilde{Y} \to \tilde{Z}$. Therefore, by Theorem 6, an optimal transmission strategy for the discrete multiplicative DBC $X \to Y \to Z$ has the NE structure as shown in Fig. 5.4. Q.E.D.

If the auxiliary random variable $U = 0$, then the channel input $X = 0$. If U is a non-zero symbol, then $X = 0$ with probability $1 - p_\lambda$. In the case where U

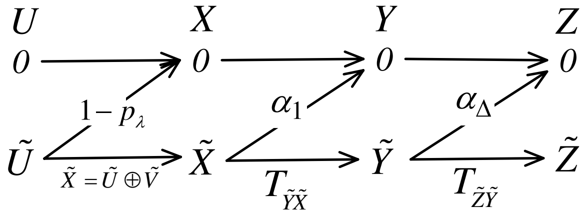


Figure 5.4: The optimal transmission strategy for the discrete multiplicative degraded broadcast channel

and X are both non-zero, $\tilde{X}$ can be obtained as $\tilde{X} = \tilde{U} \oplus \tilde{V}$, where $\oplus$ is a group operation equivalent to group addition in the group-additive degraded broadcast sub-channel $\tilde{X} \to \tilde{Y} \to \tilde{Z}$, $\tilde{U}$ is uniformly distributed and $\tilde{V}$ is an n-ary random variable.

Since the NE scheme is optimal for discrete multiplicative DBCs, its achievable rate region is the capacity region for discrete multiplicative DBCs. Hence, the capacity region for the discrete multiplicative DBC in Fig. 5.1 is

$$\bar{\text{co}}\Big[\bigcup_{p_U=(1-q,q\boldsymbol{u}^T)^T, p_V\in\Delta_{n+1}} \big\{(R_1,R_2): R_2 \le H(U\otimes V\otimes N_2) - H(U\otimes V\otimes N_2|U)$$

$$R_1 \le H(U\otimes V\otimes N_1|U) - H(U\otimes V\otimes N_1|U\otimes V)\big\}\Big]. \tag{5.29}$$

5.4 Summary

This chapter combines the results of Chapter 3, Chapter 4, and the results of the conditional entropy bound to prove that the NE scheme achieves the whole boundary of the capacity region for discrete multiplicative DBC.

CHAPTER 6

Explicit Capacity Region and Nonlinear Turbo Coding for Two-User Broadcast Z Channels

The Z channel is the binary-asymmetric channel shown in Fig. 6.1(a). The capacity of the Z channel was studied in [32]. Nonlinear trellis codes were designed to maintain a low ones density for the Z channel in [33] and parallel concatenated nonlinear turbo codes were designed for the Z channel in [34]. Fig. 6.1(b) shows a two-user broadcast Z channel.

Chapter 3 has already shown that the NE scheme achieves the whole boundary of the capacity region for multi-user broadcast Z channels. This chapter, however, provides an alternative proof without applying the conditional entropy bound F^* to show the optimality of the NE scheme for two-user broadcast Z channels. This chapter also establishes an explicit expression of the capacity region for two-user broadcast Z channels, and provides nonlinear-turbo codes that demonstrate a

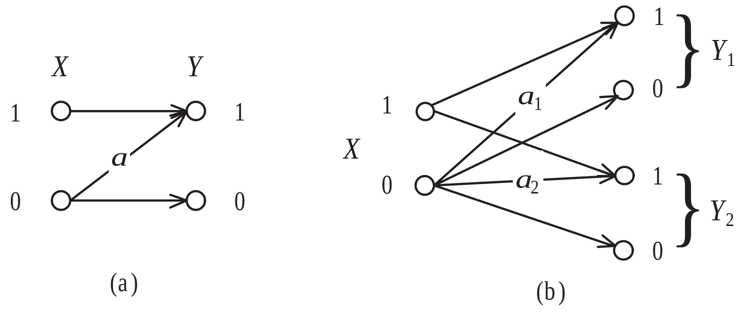


Figure 6.1: (a) Z channel. (b) Broadcast Z channel.

low-complexity scheme that works close to the optimal boundary.

This chapter is organized as follows. Section 6.1 introduced definitions and notation for broadcast channels. Section 6.2 provides the explicit expression of the capacity region for the two-user broadcast Z channel and the proof that independent encoding can achieve the optimal boundary of the capacity region. Section 6.3 presents nonlinear-turbo codes, designed to achieve the optimal boundary, and Section 6.4 provides the simulation results. Section 7.8 delivers the summaries.

6.1 Definitions and Preliminaries

6.1.1 Degraded broadcast channels

The general representation of a discrete memoryless broadcast channel is given in Fig. 6.2. A single signal X is broadcast to M users through M different channels. Channel A_2 is a physically degraded version of channel A_1 and broadcast channel $X \rightarrow Y_1, Y_2$ is physically degraded if $p(y_1, y_2|x) = p(y_1|x)p(y_2|y_1)$ [35]. A physically degraded broadcast channel with M users is shown in Fig. 6.3. Since each user decodes its received signal without collaboration, we only need to consider the marginal transition probabilities $p(y_1|x), p(y_2|x), \cdots, p(y_M|x)$ of the component channels $A_1, A_2, \cdots, A_M$. Since only the marginal distributions affect receiver performance, the *stochastically* degraded broadcast channel is defined in [2] and [35].

Let A_1 be a channel with input alphabet $\mathcal{X}$, output alphabet $\mathcal{Y}_1$, and transition probability $p_1(y_1|x)$. Let A_2 be another channel with the same input alphabet $\mathcal{X}$, output alphabet $\mathcal{Y}_2$, and transition probability $p_2(y_2|x)$. A_2 is a stochastically

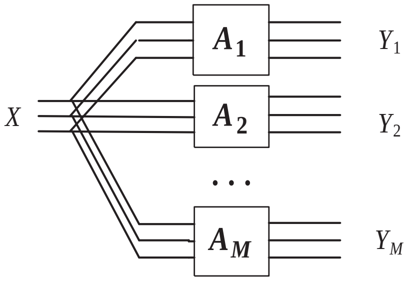


Figure 6.2: Broadcast channel.

degraded version of A_1 if there exists a transition probability $q(y_2|y_1)$ such that

$$p_2(y_2|x) = \sum_{y_1 \in \mathcal{Y}_1} q(y_2|y_1)p_1(y_1|x). \tag{6.1}$$

A broadcast channel with receivers $Y_1, Y_2 \cdots, Y_M$ is a stochastically degraded broadcast channel if every component channel A_i is a stochastically degraded version of A_{i-1} for all $i = 2, \cdots, M$ [2]. Since the marginal transition probabilities $p(y_1|x), p(y_2|x), \cdots, p(y_M|x)$ completely determine a stochastically degraded broadcast channel, we can model any stochastically degraded broadcast channel as a physically degraded broadcast channel with the same marginal transition probabilities.

Theorem 1 ([2] [3]). *The capacity region for the two-user stochastically degraded broadcast channel $X \rightarrow Y_1 \rightarrow Y_2$ is the convex hull of the closure of all (R_1, R_2) satisfying*

$$R_2 \leq I(X_2; Y_2) \qquad R_1 \leq I(X; Y_1|X_2), \tag{6.2}$$

for some joint distribution $p(x_2)p(x|x_2)p(y_1, y_2|x)$, where the auxiliary random variable X_2 has cardinality bounded by $|\mathcal{X}_2| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$.

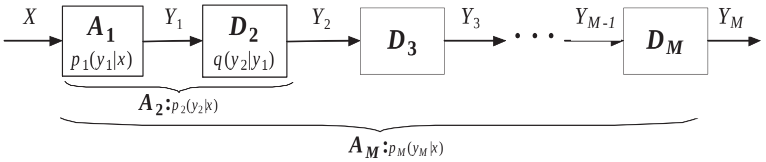


Figure 6.3: Physically degraded broadcast channel.

6.1.2 The broadcast Z channel

The Z channel is a binary-asymmetric channel with $\Pr\{y = 0|x = 1\} = 0$ (see Fig. 6.1(a)). If symbol 1 is transmitted, symbol 1 is received with probability 1. If symbol 0 is transmitted, symbol 1 is received with probability α and symbol 0 is received with probability $1 - \alpha$. We can consider a Z channel as the OR operation of the channel input X and Bernoulli noise N with parameter α (see Fig. 6.4(a)) and vice versa. In an OR Multiple Access Channel, each user equivalently transmits over a Z channel when the other users are treated as noise [34]. Thus, in an OR network with multiple transmitters and multiple receivers, each transmitter associated with more than one receivers sees a broadcast Z channel if the other transmitters are treated as noise. The diagram of a two-user broadcast Z channel is shown in Fig. 6.1(b), where $\alpha_2 \geq \alpha_1$. Because broadcast Z channels are stochastically degraded, we can model any broadcast Z channel as a physically degraded broadcast Z channel as shown in Fig. 6.4(b), where

$$\alpha_{\Delta} = \frac{\alpha_2 - \alpha_1}{1 - \alpha_1}. \tag{6.3}$$

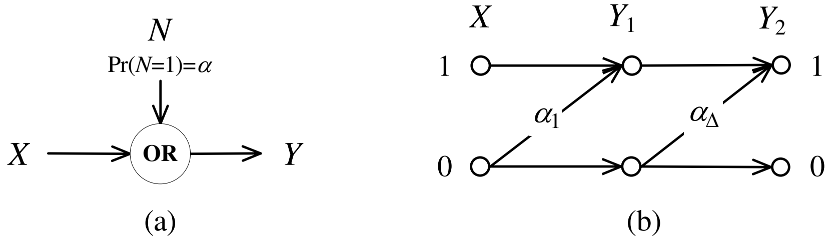


Figure 6.4: (a) OR operation view of Z channel. (b) Physically degraded broadcast Z channel.

6.2 Optimal Transmission Strategy for the 2-User Broadcast Z Channel

Since the broadcast Z channel is stochastically degraded, its capacity region can be found directly from Theorem 1. The capacity region for the broadcast Z channel $X \to Y_1 \to Y_2$ (see Fig. 6.5) is the convex hull of the closure of all (R_1, R_2) satisfying

$$\begin{aligned} R_2 &\leq I_2 = I(X_2;Y_2) \\ &= H\big((p_2\gamma + q_2q_1)(1-\alpha_2)\big) - p_2H\big(\gamma(1-\alpha_2)\big) - q_2H\big(q_1(1-\alpha_2)\big), \qquad (6.4) \\ R_1 &\leq I_1 = I(X;Y_1|X_2) \\ &= p_2\big(H(\gamma(1-\alpha_1)) - \gamma H(1-\alpha_1)\big) + q_2\big(H(q_1(1-\alpha_1)) - q_1H(1-\alpha_1)\big), \\ & \qquad (6.5) \end{aligned}$$

for some probabilities q_1, q_2, γ, where $q_1 = p(x=0|x_2=0)$, $q_2 = p(x_2=0)$, $\gamma = p(x=0|x_2=1)$, $H(p)$ is the binary entropy function, $p_1 = 1-q_1$, $p_2 = 1-q_2$ and

$$\alpha_2 = \Pr\{y_2 = 1|x=0\} = 1-(1-\alpha_1)(1-\alpha_\Delta). \qquad (6.6)$$

Each particular choice of (q_1, q_2, γ) in Fig. 6.5 specifies a particular transmis-

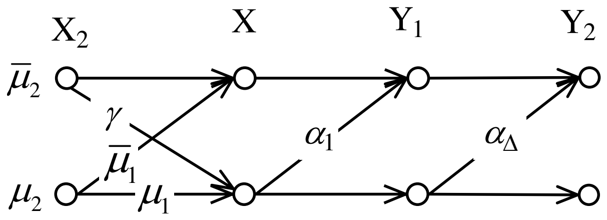


Figure 6.5: Information theoretic diagram of the system.

sion strategy and a rate pair (I_1, I_2). We say that the optimal boundary of a capacity region is the set of all Pareto optimal points (I_1, I_2), which are points for which it is impossible to increase rate I_1 without decreasing rate I_2 or vice versa. A transmission strategy is optimal if and only if it achieves a rate pair on the optimal boundary. We say a set of transmission strategies is sufficient if all rate pairs on the optimal boundary can be achieved by using these strategies and time sharing. Furthermore, a set of transmission strategies is strongly sufficient if these strategies can achieve all rate pairs on the optimal boundary without using time sharing. (6.4) and (6.5) give a set of pentagons that yield the capacity region through their convex hull, but do not explicitly show the optimal transmission strategies or derive the boundary of the rate region.

6.2.1 Optimal transmission strategies

Theorem 2 identifies a set of optimal transmission strategies and provides an explicit description of the boundary of the capacity region.

Theorem 2. *For a broadcast Z channel with* $0 < \alpha_1 < \alpha_2 < 1$*, the set of the optimal transmission strategies* (q_1, q_2, γ)*, which satisfy*

$$\gamma = 0, \tag{6.7}$$

$$\frac{1}{(1-\alpha_1)(e^{H(1-\alpha_1)/(1-\alpha_1)}+1)} \leq q_1 \leq 1, \tag{6.8}$$

and

$$\begin{aligned}&\log(1-q_1(1-\alpha_1))\big(H(q_1(1-\alpha_2)) - q_1(1-\alpha_2)\log\frac{1-q_2q_1(1-\alpha_2)}{q_2q_1(1-\alpha_2)}\big)\\ &= \log(1-q_1(1-\alpha_2))\big(H(q_1(1-\alpha_1)) - q_1H(1-\alpha_1)\big),\end{aligned} \tag{6.9}$$

are strongly sufficient. In other words, all rate pairs on the optimal boundary of the capacity region can be achieved by using exactly the transmission strategies, described in (6.7-6.8), without the need for time sharing. Furthermore, applying (6.7-6.9) to (6.4) and (6.5) yields an explicit expression of the optimal boundary of the capacity region.

Before proving Theorem 2, we present and prove some preliminary results. From (6.4) and (6.5), we can see that the transmission strategies (q_1, q_2, γ) and $(\gamma, 1-q_2, q_1)$ have the same transmission rate pairs. So we can assume $\gamma \leq q_1$ in the rest of the section without loss of generality.

Theorem 3. *For a broadcast Z channel with* $0 < \alpha_1 < \alpha_2 < 1$*, any transmission strategy* (q_1, q_2, γ) *with* $0 < q_2 < 1, 0 < \gamma < q_1$ *is not optimal.*

The proof is given in Appendix VIII.

Corollary 1. *The set of all the transmission strategies with* $\gamma = 0$ *is sufficient for any broadcast Z channel with* $0 < \alpha_1 < \alpha_2 < 1$.

Proof: From Theorem 3, we know that the transmission strategy (q_1, q_2, γ) is optimal only if at least one of these four equations $q_2 = 0$, $q_2 = 1$, $\gamma = q_1$, $\gamma = 0$ is true. Hence the set of all the transmission strategies with $q_2 = 0$, $q_2 = 1$, $\gamma = q_1$ or $\gamma = 0$ is sufficient. When $q_2 = 0$, $q_2 = 1$ or $\gamma = q_1$, the transmission rate for the second user, I_2 in equation (6.4), is zero. (This optimal rate pair is the point B in Fig. 6.6(a), which will see later.) Since this point can also be achieved by the transmission strategy with $\gamma = 0$, $q_2 = 1$ and $q_1 = \arg\max(H(x(1-\alpha_1)) - xH(1-\alpha_1))$, all the optimal rate pairs on the optimal boundary of the capacity region can be achieved by using the transmission strategies with $\gamma = 0$ and time sharing. Thus, the set of all the transmission strategies with $\gamma = 0$ is sufficient.

From Corollary 1, we can set $\gamma = 0$ in Fig. 6.5 without losing any part of the capacity region and so the designed virtual channel $X_2 \to X$ is a Z channel. Since we can consider the output of a Z channel as the OR operation of two Bernoulli random variables, an independent encoding scheme that works well for the broadcast Z channel will be introduced later in this chapter.

Applying $\gamma = 0$ to (6.4) and (6.5) yields

$$R_2 \le I_2 = H(q_2q_1(1-\alpha_2)) - q_2H(q_1(1-\alpha_2)), \tag{6.10}$$

$$R_1 \le I_1 = q_2H(q_1(1-\alpha_1)) - q_2q_1H(1-\alpha_1). \tag{6.11}$$

according to Corollary 1, the capacity region is the convex hull of the closure of all rate pairs (R_1, R_2) satisfying (6.10) and (6.11) for some probability q_1, q_2. Any optimal transmission strategy maximizes $I_1 + \lambda I_2$ for some nonnegative λ. In order to find the constraints on q_1 and q_2 for optimal transmission strategies, we consider the following optimization problem: maximize $I_1 + \lambda I_2$ for any fixed $\lambda \ge 0$. Theorem 4 provides the solution to this maximization.

Theorem 4. *The optimal solution to the maximization problem*

$$\begin{aligned} &\textit{maximize} && I_1 + \lambda I_2 \\ &\textit{subject to} && I_2 = H(q_2 q_1(1-\alpha_2)) - q_2 H(q_1(1-\alpha_2)) \\ &&& I_1 = q_2 H(q_1(1-\alpha_1)) - q_2 q_1 H(1-\alpha_1) \\ &&& 0 \leq q_2 \leq 1, 0 \leq q_1 \leq 1, \end{aligned} \tag{6.12}$$

is unique and it is given below for any fixed $\lambda \geq 0$.

Define

$$\varphi(x) = \frac{\log(1-(1-\alpha_1)x)}{\log(1-(1-\alpha_2)x)}, \tag{6.13}$$

$$\psi(x) = \frac{1}{xe^{H(x)/x} + x}. \tag{6.14}$$

Case 1: *if $0 \leq \lambda \leq \varphi(\psi(1-\alpha_1))$, then the optimal solution is $q_2^* = 1, q_1^* = \psi(1-\alpha_1)$, which satisfies (6.9), and the corresponding rate pair is $I_1^* = H(q_1^*(1-\alpha_1)) - q_1^* H(1-\alpha_1), I_2^* = 0$.*

Case 2: *if $\lambda \geq \varphi(1)$, then the optimal solution is $q_2^* = \psi(1-\alpha_2), q_1^* = 1$, which satisfies (6.9), and the corresponding rate pair is $I_1^* = 0, I_2^* = H(q_2^*(1-\alpha_2)) - q_2^* H(1-\alpha_2)$.*

Case 3: *if $\varphi(\psi(1-\alpha_1)) < \lambda < \varphi(1)$, then the optimal solution satisfies (6.15)-(6.16):*

$$q_1^* = \varphi^{-1}(\lambda) = \frac{e^\lambda - 1}{e^\lambda(1-\alpha_2) - (1-\alpha_1)}, \tag{6.15}$$

$$\begin{aligned} &\log(1-q_1^*(1-\alpha_1))\big(H(q_1^*(1-\alpha_2)) - q_1^*(1-\alpha_2)\log\frac{1-q_2^*q_1^*(1-\alpha_2)}{q_2^*q_1^*(1-\alpha_2)}\big) \\ &= \log(1-q_1^*(1-\alpha_2))\big(H(q_1^*(1-\alpha_1)) - q_1^* H(1-\alpha_1)\big). \end{aligned} \tag{6.16}$$

The proof is given in Appendix IX. From cases 1,2 and 3, (q_1, q_2) is a maximizer of (6.12) if and only if the pair (q_1, q_2) satisfies (6.8) and (6.9). In other words, if (q_1, q_2) doesn't satisfy (6.8) or (6.9), (q_1, q_2) can not be a maximizer of (6.12) and hence the transmission strategy $(q_1, q_2, \gamma = 0)$ is not optimal. Since we have proved Corollary 1, the set of all the transmission strategies which satisfy (6.7-6.9) is also sufficient. Therefore the capacity region is the convex hull of the closure of all rate pairs (R_1, R_2) satisfying (6.10) and (6.11) for some q_1, q_2 which satisfy (6.8) and (6.9).

A sketch of a capacity region is shown with two upper bounds in Fig. 6.6(a). From case 1 in Theorem 4, we can see that point B corresponds to the largest transmission rate for the first user. The first upper bound is the tangent of the achievable region in point B, and its slope is $-1/\varphi(\psi(1-\alpha_1))$. From case 2, we show that point A provides the largest transmission rate for the second user. The second upper bound is the tangent of the achievable region in point A, and its slope is $-1/\varphi(1)$. Case 3 gives us the optimal boundary of the achievable region except points A and B.

Given α_1 and α_2, which completely describe a two-user degraded broadcast Z channel, the optimal boundary of the capacity region can be explicitly described using (6.8-6.11). The curve of the capacity region is described by the range of q_1 from (6.8). The associated q_2 values follow from (6.9). The curve of the capacity region boundary is the set of (I_1, I_2) pairs resulting from using these q_1 and q_2 values in (6.10) and (6.11). For example, for $\alpha_1 = 0.15$ and $\alpha_2 = 0.6$, the range of q_1 values is $0.445 < q_1 < 1$ and the associated capacity region boundary is plotted in Fig. 6.12.

Finally, we prove Theorem 2. Since we have proved that the set of all the transmission strategies satisfying (6.7-6.9) is sufficient, we only need to show that any rate pair on the optimal boundary of the capacity region can be achieved

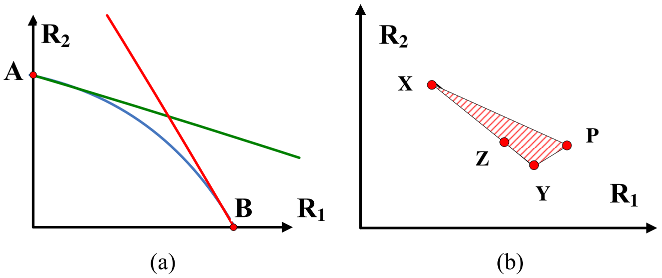


Figure 6.6: (a) The capacity region and two upper bounds. (b) Point Z can not be on the boundary of the capacity region.

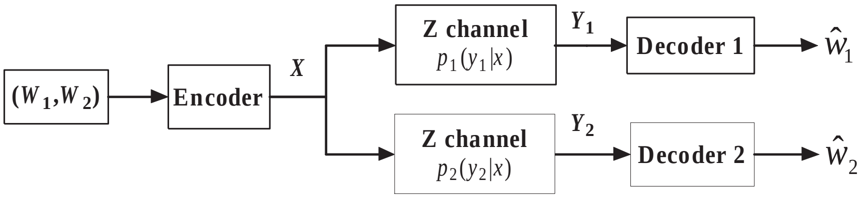


Figure 6.7: Communication system for 2-user broadcast Z channel.

without using time sharing.

Proof by contradiction: Suppose the point Z in Fig. 6.6(b) is on the optimal boundary of the capacity region for the broadcast Z channel and only can be achieved by time sharing of points X and Y, which can be directly achieved by using transmission strategies satisfying (6.7-6.9). Clearly, The slope of the line segment XY is neither zero nor infinity. Suppose the slope of XY is $-k, 0 < k < \infty$, so points X and Y provide the same value of $I_1 + \frac{1}{k}I_2$. From Theorem 4, the optimal solution to the maximization problem $\max(I_1 + \lambda I_2)$ is unique, therefore neither X nor Y maximizes $(I_1 + \frac{1}{k}I_2)$. Thus, there exists an achievable point P on the right upper side of the line XY and the triangle $\triangle XYP$ is in the capacity region. So the point Z must not be on the optimal boundary of the capacity region (contradiction).

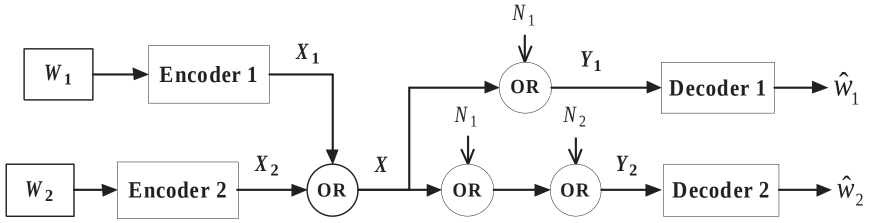


Figure 6.8: Optimal transmission strategy for broadcast Z channels.

6.2.2 Independent encoding scheme

The communication system for the two-user broadcast Z channel is shown in Fig. 6.7. In a general scheme, the transmitter jointly encodes the independent messages W_1 and W_2, which is potentially quite complex. Theorem 2 demonstrates that an independent encoding scheme can achieve the optimal boundary of the capacity region. Since $\gamma = 0$ is strongly sufficient, the virtual channel $X_2 \rightarrow X$ is a Z channel. Thus, the broadcast signal X is the OR of two Bernoulli random variable X_1 and X_2, which is an independently encoding scheme. The system diagram of the independent encoding scheme is shown in Fig. 6.8. First the messages W_1 and W_2 are encoded separately and independently. X_1 and X_2 are two binary random variables with $\Pr\{X_j = 1\} = p_j$ and $\Pr\{X_j = 0\} = q_j$. Thus $p_j + q_j = 1, j = 1, 2$. The transmitter broadcasts X, which is the OR of X_1 and X_2. From Theorem 2, this independent encoding scheme with any choice of (q_1, q_2) satisfying (6.8) and (6.9) can achieve a rate pair (I_1, I_2) on the optimal boundary of the capacity region.

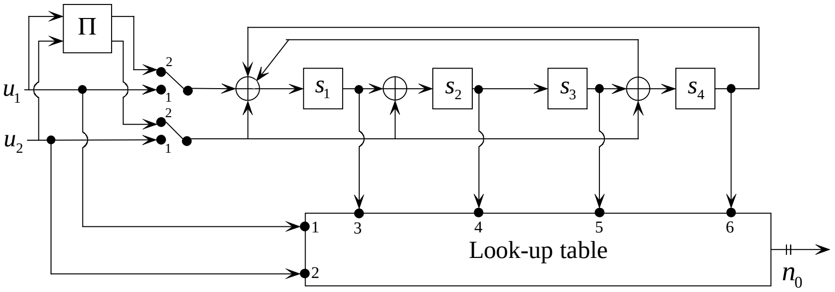


Figure 6.9: 16-state nonlinear turbo code structure, with $k_0 = 2$ input bits per trellis section.

6.3 Nonlinear-Turbo Codes for the Two-User Broadcast Z Channel

In this section we show a practical implementation of the transmission strategy for the two-user broadcast Z channel. As proved in Section 6.2, the optimal boundary is achieved by transmitting the OR of the encoded data of each user, provided that the density of ones of each of these encoded streams is chosen properly. Hence, a family of codes that provides a controlled density of ones is required. We use the nonlinear turbo codes, introduced in [34], to provide the needed controlled density of ones. Nonlinear turbo codes are parallel concatenated trellis codes with k_0 input bits and n_0 output bits per trellis section. A look-up table assigns the output label for each branch of the trellis so that the required ones density is achieved. Each constituent encoder for the turbo code in this chapter is a 16-state trellis code with $k_0 = 2$ and the trellis structure shown in Fig. 6.9. The output labels are assigned via a constrained search that provides the required ones density for each case, using the tools presented in [34] for the Z Channel. The output labels for the codes with rate pair $(R_1 = 1/6, R_2 = 1/6)$, which is simulated on a broadcast Z channel with $\alpha_1 = 0.15, \alpha_2 = 0.6$, are listed in Table 6.1.

Table 6.1: Labeling for constituent trellis codes. Rates $R_1 = 1/6, R_2 = 1/6$. Rows represent the state $s_1 s_2 s_3 s_4$, columns represent the input $u_1 u_2$. Labeling in octal notation.

User 1				
state	input			
	00	01	10	11
0000	40	20	10	04
0001	20	40	04	10
0010	10	04	02	01
0011	04	10	01	02
0100	02	01	40	20
0101	01	02	20	40
0110	42	21	14	05
0111	21	42	05	14
1000	01	02	04	10
1001	02	01	10	04
1010	04	10	20	40
1011	10	04	40	20
1100	05	14	21	42
1101	14	05	42	21
1110	20	40	01	02
1111	40	20	02	01

User 2				
state	input			
	00	01	10	11
0000	07	34	62	51
0001	34	07	51	62
0010	25	16	43	70
0011	16	25	70	43
0100	61	13	54	26
0101	13	61	26	54
0110	23	15	52	64
0111	15	23	64	52
1000	70	43	16	25
1001	43	70	25	16
1010	51	62	34	07
1011	62	51	07	34
1100	64	52	15	23
1101	52	64	23	15
1110	26	54	13	61
1111	54	26	61	13

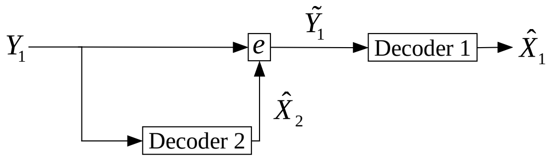
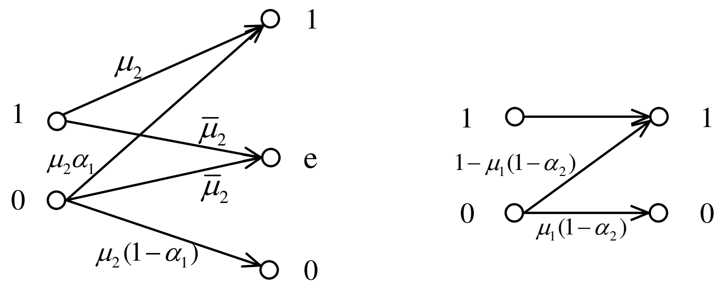


Figure 6.10: Decoder structure for user 1.



(a) User 1: Z channel with erasures (b) User 2: Z channel

Figure 6.11: Perceived channel by each decoder.

Receiver 1 uses successive decoding as shown in Fig. 6.10. Denote as $\hat{X}_2$ the decoded stream corresponding to user 2. Since the transmitted data is $x = x_1(\text{OR})x_2$, whenever a bit $x_2 = 1$, there is no information about x_1, and x_1 can be considered an erasure. Hence, the input stream to Decoder 1 is

$$\hat{y}_1 = e(y_1, \hat{x}_2) = \begin{cases} y_1 & \text{if} \quad \hat{x}_2 = 0, \\ e & \text{if} \quad \hat{x}_2 = 1. \end{cases} \tag{6.17}$$

Therefore, Decoder 2 sees a Z Channel with erasures as shown in Fig. 6.11. The tools presented in [34] were general enough to be applied to the Z Channel with erasures. Note that if α_1 is much smaller than α_2 we can use hard decoding in Decoder 2 instead of soft decoding without any loss in performance. Since the code for user 2 is designed for a Z Channel with 0-to-1 crossover probability $1 - (1 - \alpha_2)q_1$, and the channel perceived by Decoder 2 in user 1 is a Z-Channel with crossover probability $1 - (1 - \alpha_1)q_1 < 1 - (1 - \alpha_2)q_1$, the bit error rate of $\hat{x}_2$ is negligible compared to the bit error rate of Decoder 1. In fact, in all the simulations shown in Section 6.4, which include 100 frame errors of user 1, none of the errors were produced by Decoder 2.

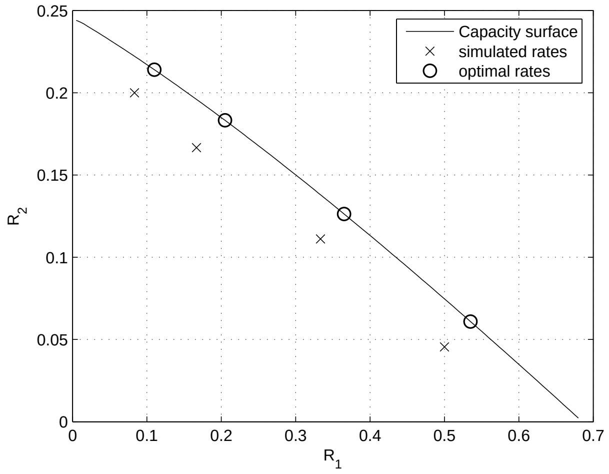


Figure 6.12: Broadcast Z channel with crossover probabilities $\alpha_1 = 0.15$ and $\alpha_2 = 0.6$ for receiver 1 and 2 respectively: achievable capacity region, simulated rate pairs (R_1, R_2) and their corresponding optimal rates.

6.4 Results

We have simulated the transmission strategy for the two-user broadcast Z channel with crossover probabilities $\alpha_1 = 0.15$ and $\alpha_2 = 0.6$, using nonlinear turbo codes, with the structure shown in Fig. 6.9. Fig. 6.12 shows the achievable region of the rate pairs (R_1, R_2) on this channel, and the simulated rate pairs. It also shows the optimal rate pairs used to compute the ones densities of each code. For each of these four simulated rate pairs, the loss in mutual information from the associated optimal rate is only 0.04 bits or less in R_1 and only 0.02 bits or less in R_2. Table 6.2 shows bit error rates for each rate pair, the ones densities p_1 and p_2, and the interleaver lengths K_1 and K_2 used for each code. For simplicity, we chose K_1 and K_2 so that the codeword length n would be the same for user 1 and user 2, except for rate pairs $R_1 = 1/2$ and $R_2 = 1/22$, where one codeword length of user 2 is twice the length of user 1.

Table 6.2: BER for two-user broadcast Z channel with crossover probabilities $\alpha_1 = 0.15$ and $\alpha_2 = 0.6$.

R_1	R_2	p_1	p_2	K_1	K_2	BER_1	BER_2
1/12	1/5	0.106	0.56	4800	1700	2.54×10^{-5}	1.24×10^{-5}
1/6	1/6	0.196	0.5	2048	2048	7.01×10^{-6}	5.33×10^{-6}
1/3	1/9	0.336	0.3739	4608	1536	7.13×10^{-6}	6.70×10^{-6}
1/2	1/22	0.463	0.1979	5632	1024	9.27×10^{-7}	3.27×10^{-6}

6.5 Summary

This chapter proves that the NE scheme achieves the whole boundary of the capacity region for two-user broadcast Z channels without applying results of the conditional entropy bound F^*. In particular, the NE scheme for two-user broadcast Z channels is to independently encode the message corresponding to each user and transmit the binary OR of the encoded signals. This chapter also establishes an explicit expression of the capacity region for two-user broadcast Z channels, and provides the distributions of the outputs of each encoder that achieve the optimal boundary. Nonlinear-turbo codes that provide a controlled distribution of ones and zeros in their codewords were used to demonstrate a low-complexity scheme that works close to the optimal boundary.

CHAPTER 7

Minimizing Weighted Sum Download Time for One-to-Many File Transfer in Peer-to-Peer Networks

7.1 Background

Consider a scenario where millions of peers would like to download content from a source node in the Internet. The source node has sufficient bandwidth to serve tens or hundreds of receivers, but not millions. In the absence of IP multicast, one solution is to form the source node and the peers into a P2P overlay network and distribute the content using application layer multicast [36] [37]. In this scenario, the content in the source node is partitioned into chunks. Peers not only download chunks or coded chunks (e.g. a linear combination of multiple chunks) from the source node and other peers but also upload to some other peers that are interested in the content.

This chapter focuses on content distribution applications (e.g, BitTorrent [16], Overcast [27]) in which peers are only interested in content at full fidelity, even if it means that the content does not become available to all peers at the same time. The key issue for these P2P applications is to minimize download times (delays) to receivers. Since it usually takes several hours or days for a peer to download content in full fidelity, our work is less concerned with interactive response times and transmission delays in buffers and in the network.

In order to understand the fundamental performance limit for one-to-many file transfer in P2P networks, it is assumed that all nodes are cooperative, and a centralized algorithm provides the file-transfer scenario with the full knowledge of the P2P network including the source node's uplink capacity , and the weights, downlink capacities, and uplink capacities of peers. The cooperative assumption holds in many practical applications, for example, in closed content distribution systems where the programs are managed by a single authority.

P2P applications (e.g, [16], [17], [18], [19]) are increasingly popular and represent the majority of the traffic currently transmitted over the Internet. A unique feature of P2P networks is their flexible and distributed nature, where each peer can act as both a server and a client [20]. Hence, P2P networks provide a cost-effective and easily deployable framework for disseminating large files without relying on a centralized infrastructure [21]. These features of P2P networks have made them popular for a variety of broadcasting and file-distribution applications [21] [22] [23] [24] [25] [26] [27].

Specifically, chunk-based and data-driven P2P broadcasting systems such as CoolStreaming [22] and Chainsaw [23] have been developed, which adopt pull-based techniques [22], [23]. In these P2P systems, the peers possess several chunks and these chunks are shared by peers that are interested in the same content. An important problem in such P2P systems is how to transmit the chunks to the various peers and create reliable and efficient connections between peers. For this, various approaches have been proposed including tree-based and data-driven approaches (e.g. [25] [38] [39] [40] [41] [42] [43]).

Besides these practical approaches, some research has begun to analyze P2P networks from a theoretic perspective to quantify the achievable performance.

The performance, scalability and robustness of P2P networks using network coding are studied in [36] [44]. In these investigations, each peer in a P2P network randomly chooses several peers including the server as its parents, and also transmits to its children a random linear combination of all packets the peer has received. Random linear network coding [45] [46] [47], working as a perfect chunk selection algorithm, makes elegant theoretical analysis possible. Some other research investigates the steady-state behavior of P2P networks with homogenous peers by using fluid models [48] [49] [50].

In a P2P file transfer application, the key performance metric from an end-user's point of view is the delay, or the time it takes for an end-user to download the file. In [24], Li, Chou, and Zhang explore the problem of delivering the file to all receivers in minimum amount of time (equivalently, minimizing the maximum delay to the receivers) assuming node uplinks are the only bottleneck in the network. They introduce a routing-based scheme, referred to as Mutualcast, which minimizes the maximum delay to all receivers with or without helpers.

The uplink and downlink capacities of each peer are usually determined at the application layer instead of the physical layer, because an Internet user can have several applications that share the physical downlink and uplink capacities. The peer weights depend on the applications. For broadcast applications such as CoolStreaming [22] and Overcast [27]in which all peers in the P2P network are interested in the same content, all peer weights in the content distribution system can be set to 1. In multicast applications such as "Tribler" [51] peers called helpers, who are not interested in any particular content, store part of the content and share it with other peers. Assign weight zero to helpers, and weight 1 to receivers. In some applications, P2P systems partition peers into several classes and assign different weights to peers in different classes.

7.2 Introduction

This chapter considers the problem of minimizing weighted sum download time (WSDT) for one-to-many file transfer in a peer-to-peer (P2P) network. Consider a source node s that wants to broadcast a file of size B to a set of N receivers $i \in \{1, 2, \cdots, N\}$ in a P2P network. Our model assumes that the source uplink bandwidth constraint U_s, the peer uplink bandwidth constraints U_i, and the peer downlink bandwidth constraints D_i are the only bottlenecks in the network. Limited only by these constraints, every peer can connect to every other peer through routing in the overlay network.

The general problem of minimizing WSDT divides into an exhaustive set of cases according to three attributes. The first attribute is whether the allocation of network resources is static or dynamic. In the static scenario, the network resource allocation remains unchanged from the beginning of the file transfer until all receivers finish downloading. The dynamic scenario allows the network resource allocation to change as often as desired during the file transfer.

The second attribute is whether downlink bandwidth constraints are considered to be unlimited (i.e. $D_i = \infty$) or not (i.e.$D_i \leq \infty$). Most research in P2P considers the download bandwidth constraints to be unlimited because the uplink capacity is often several times smaller than the downlink capacity for typical residential connections (e.g., DSL and Cable). However, consideration of downlink bandwidth constraints can be important. The downlink capacity can still be exceeded when a peer downloads from many other peers simultaneously, as in the routing-based scheme proposed in [28].

The third attribute is whether we consider the special case of sum download time (i.e. $W_i = 1$ for all i) or the general case of weighted sum download time which allows any values of the weights W_i.

With these cases in mind, here is an overview of the results presented in this chapter. For the static scenario that considers download bandwidth constraints $D_i \leq \infty$ and allows any values of W_i Section 7.3 uses a time-expanded graph and linear network coding to show that the minimum WSDT and the corresponding allocation of network resources may be found in polynomial time by solving a convex optimization problem. We also present a lower bound on minimum WSDT that is easily computed and turns out to be tight across a wide range of parameterizations of the problem.

While the minimum WSDT for the static scenario may be found in polynomial time using the approach of Section 7.3, that approach is sufficiently computationally intensive that Sections 7.4 and 7.5 provide lower complexity alternatives. In some cases, the lower complexity approaches are exactly optimal. For the remaining cases, the lower bound of Section 7.3 shows that their performance is indistinguishable from the lower bound and hence closely approach optimality across a wide range of parameterizations.

Sections 7.4 and 7.5 build on the foundation of the Mutualcast algorithm [24]. Mutualcast is a static rate allocation algorithm designed to minimize the maximum delay to all peers in the case where $D_i = \infty$. Section 7.3 concludes by showing that Mutualcast achieves that section's lower bound when $W_i = 1$ for all i and therefore minimizes sum download time as well as maximum download time.

Inspired by this result, Section 7.4 proposes a generalization of this algorithm, Extended Mutualcast, that minimizes sum download time even when the download bandwidth constraints D_i are finite and distinct from each other. When uplink bandwidth resources are plentiful, Extended Mutualcast also minimizes weighted sum download time regardless of weights because each receiver is downloading content as quickly as possible given its download bandwidth constraint and the upload bandwidth constraint of the source.

It is notable that Mutualcast and Extended Mutualcast achieve their optimal results while utilizing only depth-1 and depth-2 trees. Inspired by this fact and the technique of rateless coding, Section 7.5 attacks the general problem of minimizing weighted sum download time(WSDT) by proposing a convex optimization approach that assumes only trees of depth one or two. Then, Section 7.5 proposes a simple water-filling approach using only depth-1 and depth-2 trees. While the optimality of this approach is not proven, Section 7.5.5 shows that its performance matches that of the lower bound of 7.3 for a wide variety of parameterizations. Thus this water-filling approach provides a simple algorithm that empirically achieves the lower bound on WSDT for all cases of the static scenario across a wide range of parameterizations.

Turning our attention to the dynamic scenario, Wu et al. [28] demonstrate that given an order in which the receivers finish downloading, the dynamic allocation (neglecting downlink bandwidth constraints) that minimizes WSDT can be obtained in polynomial time by convex optimization and can be achieved through linear network coding. They also propose a routing-based scheme which has almost-optimal empirical performance and demonstrate how to significantly reduce the sum download time at the expense of a slight increase in the maximum download time.

Dynamic schemes can reduce the minimum sum download time to approximately half that of the static case, at least when downlink capacities are considered to be infinite [28]. Essentially, [28] shows that to optimize WSDT the network resource allocation should remain constant during any “epoch”, a period of time between when one receiver finishes downloading and another finishes downloading. Thus, one optimal solution for the dynamic scenario is "piecewise static". However, [28] leaves the proper selection of the ordering as an open problem and does not address the finite downlink capacities $D_i < \infty$ or the general case of weighted sum download time which allows any values of the weights W_i.

Section 7.6 provides a practical solution for the dynamic scenario. Specifically, it provides an approach the ordering problem left open by [28] by reformulating the problem as that of determining the weights that should be assigned during each static epoch so as to produce the piecewise static solution that minimizes the WSTD (according to the original weights). This approach handles both finite downlink capacities $D_i < \infty$ and the general case of weighted sum download time which allows any values of the weights W_i. A key result of this section is that, regardless of how the overall weights W_i are set, the "piecewise static" solution may be obtained by finding the appropriate weights for each epoch and solving the static problem for that epoch. Furthermore, during any epoch the appropriate weights of all peers are either 1 or zero with the exception of at most one "transitional" peer whose weight can be anywhere between zero and 1. Neglecting the "transitional" node, the ordering problem becomes approximately one of choosing which peers should be served during each epoch. Having resolved the ordering problem in this way, the simple water-filling approach of Section 7.5 provides the rate allocations for the source and for each peer during each of the piecewise-static epochs. Thus this section provides a complete solution for the dynamic scenario. Because the selection of the ordering and the rate allocation are both close to optimal, we conjecture that the overall performance of this solution is close to optimal across a wide range of parameterizations.

Section 7.8 delivers the conclusions of this chapter.

7.3 Convex Optimization of WSDT in the Static Case

This section considers static P2P network in which the source node with uplink bandwidth U_s seeks to distribute a file of size B so as to minimize the weighted sum of download times given a static allocation of resources. No peer leaves or joins during the file transfer. There are N peers who want to download the file that the source node has. Each peer has weight W_i, downlink capacity D_i and uplink capacity U_i, for $i = 1, 2, \cdots, N$. It is reasonable to assume that $D_i \geq U_i$ for each $i = 1, \cdots, N$ since it holds for typical residential connections (e.g., Fiber, DSL and Cable). In case of $D_i < U_i$ for some i, we just use peer i's part of the uplink capacity which equals to its downlink capacity and leave the rest of the uplink capacity unused.

Denote the transmission rate from the source node to peer j as $r_{s\to j}$ and the transmission rate from peer i to peer j as $r_{i\to j}$. The total download rate of peer j, denoted as d_j, is the summation of $r_{s\to j}$ and $r_{i\to j}$ for all $i \neq j$. Since the total download rate is constrained by the downlink capacity, we have

$$d_j = r_{s\to j} + \sum_{i\neq j} r_{i\to j} \leq D_j \tag{7.1}$$

for all $j = 1, \cdots, N$. As a notational convenience, we also denote $r_{j\to j}$ as the transmission rate from the source node to peer j so that

$$d_j = \sum_{i=1}^{N} r_{i\to j} \leq D_j \tag{7.2}$$

for all $j = 1, \cdots, N$. The total upload rate, denoted as u_j, is constrained by the uplink capacity. Hence, we also have $u_j = \sum_{i\neq j} r_{j\to i} \leq U_j$ for all $j = 1, \cdots, N$.

One example of the peer model is shown in Fig. 7.1. The downlink capacity

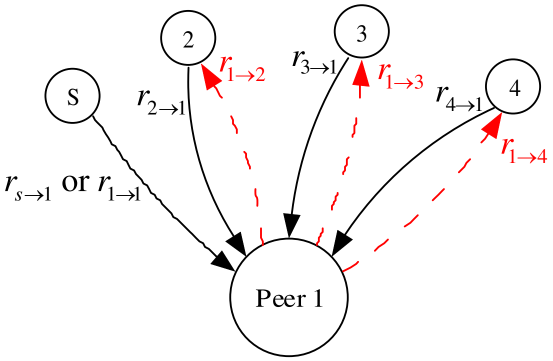


Figure 7.1: The peer model

and uplink capacity of peer 1 are D_1 and U_1 respectively. Thus, the total download rate $r_{s\to1} + \sum_{i=2}^{4} r_{i\to1} = \sum_{i=1}^{4} r_{i\to1}$ has to be less than or equal to D_1, and the total upload rate $\sum_{i=2}^{4} r_{1\to i}$ has to be less than or equal to U_1.

7.3.1 The Time-Expanded Graph

As one of the key contributions of [28], Wu *et al.* used a time-expanded graph to show how the dynamic scenario decomposes into epochs. This section applies the time-expanded graph approach provided in [28] to the *static* case.

To obtain the time-expanded graph for a P2P network with N peers, we need to divide the time into N *epochs* according to the finishing times of the peers. One peer finishes downloading at the end of each epoch so that the number of epochs is always equal to the number of peers. Let Δt_i denote the duration of the i-th epoch. Hence, i receivers finish downloading by time $t_i = \sum_{k=1}^{i} \Delta t_k$. If peers i and $i+1$ finish downloading at the same time, $\Delta t_{i+1} = 0$.

Each vertex in the original graph G corresponds to N vertices, one for each epoch, in the time-expanded graph $G^{(N)}$ as follows: We begin with the original P2P graph G with node set $V = \{s, 1, \cdots, N\}$ and allowed edge set E. For each $v \in V$ and each $n \in \{1, \cdots, N\}$, $G^{(N)}$ includes a vertex $v^{(n)}$ corresponding to the associated physical node v in the n-th epoch. For each $e \in E$ going from u to v and each $n \in \{1, \cdots, N\}$, $G^{(N)}$ includes an edge $e^{(n)}$ going from $u^{(n)}$ to $v^{(n)}$ corresponding to the transmission from u to v during the n-th epoch.

The subgraph $G^{(n)} = (V^{(n)}, E^{(n)})$ for $n = 1, \cdots, N$ characterizes the network resource allocation in the n-th epoch. To describe a rate allocation in the original graph G, edges are typically labeled with the *rate* of information flow. However, since each epoch in the time-expanded graph $G^{(N)}$ has a specified duration, each of the N edges in the time-expanded graph corresponding to an edge in G is labeled with the total amount of information flow across the edge during its epoch. This is the product of the flow rate labeling that edge in the original graph G and the duration of the epoch.

The time-expanded graph also includes memory edges. For each $v \in V$ and each $n \in \{1, \cdots, N-1\}$, there is an edge with infinite capacity from $v^{(n)}$ to $v^{(n+1)}$. These memory edges reflect the accumulation of received information by node v over time.

As just described, the time-expanded graph not only describes the network topology, but also characterizes the network resource allocation over time until all peers finish downloading in a P2P network. As shown in [28] by Wu et al., even in the dynamic scenario the network resource allocation can remain static throughout each epoch without loss of optimality. In this section, we apply the time-expanded graph to the static scenario in which the rate allocation remains fixed for the entire file transfer.

As an example, consider the following scenario. A P2P network contains a source node seeking to disseminate a file of unit size ($B = 1$). Its upload capacity is $U_S = 2$. There are three peers $\{1, 2, 3\}$ with upload capacities $U_1 = U_2 = U_3 = 1$ and download capacities $D_1 = D_2 = D_3 = \infty$.

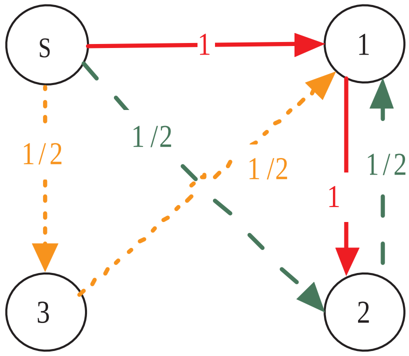


Figure 7.2: An example P2P graph G. Edges are labeled with one possible rate allocation $r_{i\to j}$.

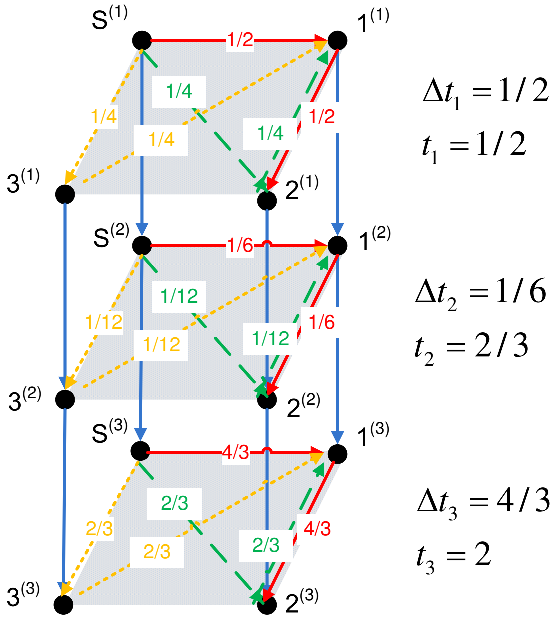


Figure 7.3: The time-expanded $G^{(3)}$ for the P2P graph G shown in Fig. 7.2. Edges are labeled with the total information flow along the edge during the epoch. This is the product of the rate allocation along the edge (from the graph in Fig. 7.2) and the duration of the epoch. Edges with zero flow are not shown.

Fig. 7.2 gives one possible static rate allocation, showing the allocated rate for each edge of the original P2P graph G. (Edges with zero allocated rate are not shown.) The source node transmits with a rate of 1 to peer 1 and with rate 1/2 to peers 3 and 4. Peer 1 transmits with rate 1 to peer 2 but does not transmit to any other peers. Peers 2 and 3 transmit with rate 1/2 to Peer 1, but do not transmit to any other peers.

Fig. 7.3 shows the time-expanded graph induced by the static rate allocation shown in Fig. 7.2. Because there are three peers, this time-expanded graph has 3 epochs. The peers are numbered in the order they finish downloading; peer 1 finishes first followed by peer 2 and then peer 3. The first epoch lasts $\Delta t_1 = 1/2$ time units, the second epoch lasts $\Delta t_2 = 1/6$ time units, and the third epoch lasts $\Delta t_3 = 4/3$ time units.

Peer 1 finishes first because it sees the full upload capacity of the source. As shown in Fig. 7.2 it sees rate 1 directly from the source. The other half of the source upload capacity is relayed to peer 1 by peers 2 and 3 immediately after they receive it. Hence peer 1 receives information with an overall rate of $r_1 = 2$ and finishes downloading the entire file, which has size $B = 1$ at time $t_1 = 1/2$. As a result, the duration of the first epoch is $\Delta t_1 = 1/2$.

Peer 2 sees rate 1/2 directly from the source and rate 1 relayed to peer 2 by peer 1. Hence it sees an overall upload capacity of $r_2 = 3/2$ and finishes downloading the entire file at time $t_2 = 2/3$. The duration of the second epoch can be computed as $t_2 - t_1 = 1/6$.

Because it receives no help from the other two peers, peer 3 sees an overall upload rate of only $r_3 = 1/2$, which it receives directly from the source. It finishes downloading the entire file at time $t_3 = 2$. The duration of the third epoch can be computed as $t_3 - t_2 = 4/3$.

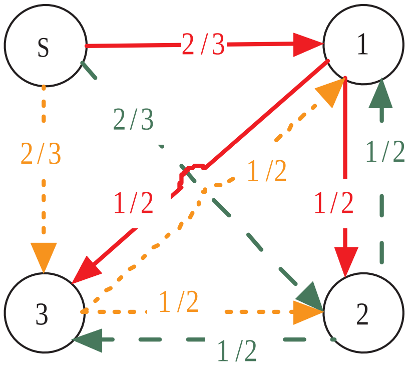


Figure 7.4: An example P2P graph G. Edges are labeled with the rate allocation $r_{i \to j}$ that minimizes the sum of the download times.

The sum of the download times for the example of Figs. 7.2 and 7.3 is $1/2 + 2/3 + 2 = 3\ 1/6$. Now let's consider an example that minimizes the sum of the download times and in which peers finish at the same time.

Fig. 7.4 shows the rate allocation that achieves the minimum possible sum of download times for a static allocation in this scenario, which turns out to be 1 4/5. The allocation shown in Fig. 7.4 is perfectly symmetric. Each peer receives rate 2/3 directly from the source and rate 1/2 from each of the two other peers. Each peer receives an overall rate of 5/3. Hence all three peers finish downloading simultaneously at $t = 3/5$ and the second and third epochs have zero duration.

7.3.2 Transmission Flow Vectors and a Basic Network Coding Result

In Subsection 7.3.1 there was a tacit assumption that all of the information received by a peer is *useful*. For example, we assumed that the information relayed from peer 2 to peer 1 did not repeat information sent from the source to peer 1. In the examples of Subsection 7.3.1, one can quickly construct simple protocols that ensure that no critical flows are redundant. In this subsection, we review a general result that uses network coding theory to show that there is

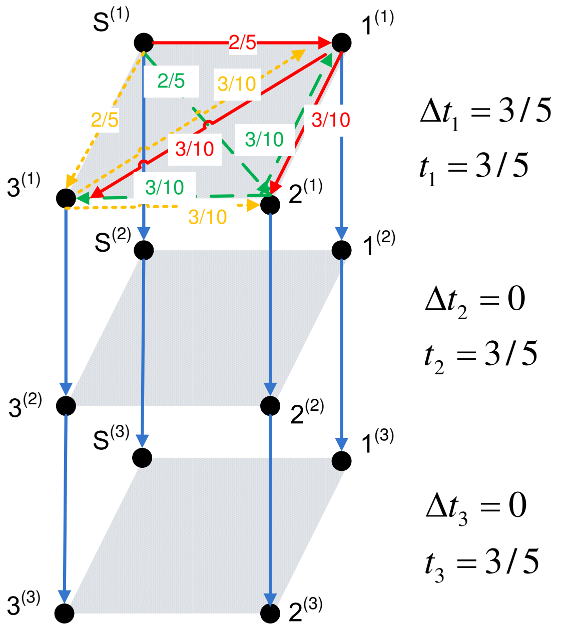


Figure 7.5: The time-expanded G^3 for the P2P graph G shown in Fig. 7.4. Edges are labeled with the total information flow along the edge during the epoch. This is the product of the rate allocation along the edge (from the graph in Fig. 7.4)and the duration of the epoch. Edges with zero flow are not shown.

always a way to ensure that no critical flows are redundant.

Consider a general graph $G = (V, E)$, which could be either a rate-allocation graph G such as Figs. 7.2 or 7.4 or a time-expanded graph such as G^3 described in Figs. 7.3 and 7.5. Denote $c(e)$ as the capacity of the edge $e \in E$. A transmission flow from the source node s to a destination node i is a nonnegative vector $\boldsymbol{f}$ of length $|E|$ satisfying the flow conservation constraint: $\text{excess}_v(\boldsymbol{f}) = 0, \forall v \in V \backslash \{s, i\}$,where

$$\text{excess}_v(\boldsymbol{f}) = \sum_{e \in In(v)} f(e) - \sum_{e \in Out(v)} f(e). \tag{7.3}$$

The total flow supported by $\boldsymbol{f}$ is $\sum_{e \in Out(s)} f(e)$. This "flow" could be a flow *rate* with units of bits per unit time if we are considering a rate allocation graph such as Fig. 7.2 or it could be a total flow with units of bits or packets or files if we are considering a time-expanded graph such as Fig. 7.3.

As an example, the flow vector $\boldsymbol{f}$ describing the flow in Fig. 7.3 from $S^{(1)}$ (the source in the first epoch) to destination node $2^{(2)}$ (peer 2 in the second epoch, when peer 2 finishes downloading) has the nonzero elements $f(e)$ shown in Table 7.1. Examining Table 7.1 verifies that the flow conservation constraint (7.3) is satisfied and that the total flow supported is equal to 1 file.

Table 7.1: Table showing nonzero elements $f(e)$ for the flow vector $\boldsymbol{f}$ from $S^{(1)}$ to $2^{(2)}$ in Fig. 7.3.

e	$f(e)$
$S^{(1)} \rightarrow 2^{(1)}$	1/4
$S^{(1)} \rightarrow 1^{(1)}$	1/2
$1^{(1)} \rightarrow 2^{(1)}$	1/2
$2^{(1)} \rightarrow 2^{(2)}$	3/4
$S^{(1)} \rightarrow S^{(2)}$	1/4
$S^{(2)} \rightarrow 2^{(2)}$	1/12
$S^{(2)} \rightarrow 1^{(2)}$	1/6
$1^{(2)} \rightarrow 2^{(2)}$	1/6

The following lemma states that a given fixed flow (or flow rate) can be achieved from the source to all destinations as long as there is a feasible flow vector supporting the desired flow from the source to each destination. i.e. We can achieve this flow to all destinations with network coding without worrying about possible interactions of the various flows..

Lemma 1. ***(Network Coding for Multicasting [45] [46])*** *In a directed graph $G = (V, E)$ with edge capacity specified by a vector* $\mathbf{c}$ *, a multicast session from the source node s to a set of receivers $i \in \{1, \ldots, N\}$ can achieve the same flow r for each $i \in \{1, \ldots, N\}$ if and only if there exits a set of flows $\{\boldsymbol{f}_i\}$ such that*

$$\boldsymbol{c} \geq \max_i \boldsymbol{f}_i \tag{7.4}$$

where $\boldsymbol{f}_i$ is a flow from s to i with flow r. Furthermore, if (7.4) holds, there exists a linear network coding solution.

7.3.3 A Convex Optimization

Given an order in which the peers will finish downloading, say peer i finishes at the end of the k_i-th epoch, applying Lemma 1 to the time-expanded graph $G^{(N)}$ with the set of destination nodes $i \in \{1, \ldots, N\}$ gives a characterization of all feasible downloading times, as concluded in the following lemma.

Lemma 2. ***Lemma: (Feasible Downloading Times with Given Order [28])*** *Consider a P2P network in which node $D_i = \infty$. Given an order in which the nodes will finish downloading a file with size B, say node i finishes at epoch k_i, a set of epoch durations Δt_i is feasible if and only if the following system of linear inequalities has a feasible solution:*

$$\Delta t_i \geq 0, \quad i = 1, \cdots, N, \tag{7.5}$$

$$\boldsymbol{g} \geq \boldsymbol{f}_i, \quad i = 1, \cdots, N, \tag{7.6}$$

$$\sum_{v:u^{(i)} \rightarrow v^{(i)}} g_{u^{(i)} \rightarrow v^{(i)}} \leq c_u \Delta t_i, \quad \forall u \in V, i = 1, \cdots, N, \tag{7.7}$$

where c_u is the uplink capacity of peer u, and $\boldsymbol{f}_i$ is a flow from first-epoch source node $s^{(1)}$ to node i's termination-epoch node $i^{(k_i)}$ with flow rate B.

As an example, the epoch durations of Fig. 7.3 are feasible because each of the flow vectors (one example was given in Table 7.1) satisfy the feasibility constraints of Lemma 2.

Let t_j denote the delay to peer j for $j = 1, \cdots, N$. Given a static network resource allocation $r_{i \rightarrow j}$, $(i, j \in \{1, \cdots, N\})$ as shown for example in Fig. 7.2, the maximum flow to peer j, denoted as r_j, is equal to the minimum cut between source node s and peer j in the rate-allocation graph (i.e. a graph such as Fig. 7.2, not the time-expanded graph). This follows from the Max-Flow-Min-

Cut Theorem. Hence, $t_j \geq \frac{B}{r_j}, \forall j$.

From applying network coding results such as Lemma 1 to the rate allocation graph alone, we cannot conclude much about feasible download times since Lemma 1 addresses only the feasibility of the same flow to all destinations. However, by applying Lemma 1 to the *time-expanded graph* we can show that $t_j = \frac{B}{r_j}$ can be achieved simultaneously for all $j = 1, \cdots, N$. Lemma 3 below states this result.

Lemma 3. *Given a static network resource allocation $r_{i \to j}$, $(i, j = 1, \cdots, N)$, for a P2P network, the only Pareto optimal (smallest) delay vector is $t_j = \frac{B}{r_j}$ for $j = 1, \cdots, N$, where r_j is the minimum cut from the source node s to peer j.*

Proof. It has been shown that $t_j \geq \frac{B}{r_j}$ for $j = 1, \cdots, N$. Hence, it is sufficient to show that $t_j = \frac{B}{r_j}$ for $j = 1, \cdots, N$ is achievable. Without loss of generality, assume that $r_1 \geq r_2 \geq \cdots \geq r_N > 0$. Construct a static scheme (i.e. a time-expanded graph $G^{(N)}$) as follows:

(1) $\Delta t_i = \frac{B}{r_i} - \frac{B}{r_{i-1}}$, where $r_0 \triangleq \infty$;

(2) Flow capacity of edge $i^{(k)} \to j^{(k)}$ is $r_{i \to j} \Delta t_k$ for $1 \leq i \neq j \leq N$ and $k = 1, \cdots, N$;

(3) Flow capacity of edge $s^{(k)} \to j^{(k)}$ is $r_{s \to j} \Delta t_k$ for $j, k = 1, \cdots, N$;

(4) Flow capacity of edge $j^{(k)} \to j^{(k+1)}$ is infinity for $j = 1, \cdot, N$ and $k = 1, \cdots, N-1$;

(5) The destination nodes in the time-expanded graph are node $i^{(i)}$ for $i = 1, \cdots, N$. In other words, peer i finishes at the end of i-th epoch.

According to the constructions (1) and (5), the delay to peer i is $t_i = \sum_{k=1}^{i} \Delta t_k = \frac{B}{r_i}$. According to the constructions (2) and (3), in the subgraph $G^{(k)}$, the maximum flow from $s^{(k)}$ to $i^{(k)}$ is equal to $r_i \Delta t_k$ for all $i, k = 1, \cdots, N$. Therefore, in this time-expanded graph $G^{(N)}$, the maximum flow from source node s to node

$i^{(i)}$ is greater than or equal to

$$\sum_{k=1}^{i} r_i \Delta t_k = B.$$

Therefore, by Lemma 1 and Lemma 2, there exists a linear network coding solution to multicast a file with size B from the source node s to peer i within delay $t_i = \frac{B}{r_i}$ for all $i = 1, \cdots, N$. □

The maximum flow r_i can be found by solving a linear optimization. Specifically, a set of flow rates $\{r_i\}_{i=1}^{N}$ is feasible if and only if there exists a solution to the following system of linear inequalities:

$$r_{i \to j} \geq 0, \quad \forall i, j = 1, \cdots, N; \tag{7.8}$$

$$\sum_{i=1}^{N} r_{i \to i} \leq U_s; \quad \text{(recall that } r_{i \to i} \triangleq r_{s \to i}\text{)} \tag{7.9}$$

$$\sum_{j=1, j \neq i}^{N} r_{i \to j} \leq U_i, \quad \forall i = 1, \cdots, N; \tag{7.10}$$

$$\sum_{j=1}^{N} r_{j \to i} \leq D_i, \quad \forall i = 1, \cdots, N; \tag{7.11}$$

$$0 \leq f_{i \to j}^{(k)} \leq r_{i \to j}, \forall i, j, k = 1, \cdots, N; \tag{7.12}$$

$$f_{k \to j}^{(k)} = 0, \quad \forall j \neq k; \tag{7.13}$$

$$\sum_{j=1}^{N} f_{j \to i}^{(k)} = \sum_{j=1, j \neq i}^{N} f_{i \to j}^{(k)}, \quad \forall i \neq k; \tag{7.14}$$

$$\sum_{i=1}^{N} f_{i \to k}^{(k)} \geq r_k, \quad \forall k = 1, \cdots, N, \tag{7.15}$$

where $r_{i \to j}$ $(i, j = 1, \cdots, N)$ represents the network resource allocation and $f_{i \to j}^{(k)}$

$(i, j = 1, \cdots, N)$ is a flow from the source node s to peer k.

By Lemma 3, the minimum WSDT is the solution to the convex optimization of minimizing $\sum_{i=1}^{N} W_i B / r_i$ subject to (7.8-7.15). Thus, we can conclude the following theorem:

Theorem 1. *Consider multicasting a file with size B from a source node s to peers $\{1, \cdots, N\}$ in a P2P network with both uplink and downlink capacity limits. The minimum weighted sum downloading time for the static scenario and the corresponding optimal static allocation can be found in polynomial time by solving the convex optimization of minimizing $\sum_{k=1}^{N} W_k B / r_i$ subject to the constraints (7.8-7.15).*

Theorem 1 gives a solution to the most general static case that we are considering in this chapter. However, it can be extended further by adding other linear network constraints (e.g. edge capacity constraints), which are not a concern of this chapter.

7.3.4 The Uplink-Bandwidth-Sum Bound

For a P2P network with a source node and N peers, the convex optimization in Theorem 1 has $N^3 + N^2 + N$ variables and $2N^3 + 3N^2 + N + 1$ linear constraints. The complexity for the interior point method to solve this convex optimization is $O((N^3)^{3.5})$ [52].

Even though the convex optimization can be solved in polynomial time, its complexity is still too high for practical applications when N is large. Hence, bounds on the minimum WSDT and static schemes having network resource allocations that may be computed with low complexity are desired. In this subsection, we provide an analytical lower bound to the minimum WSDT with $O(N^2)$

complexity for computing both the bound itself and the associated rate allocations.

Consider the cut of $\{V \setminus i\} \rightarrow \{i\}$ for any static allocation $r_{i \to j}$ $i, j \in \{1, \cdots, N\}$, the maximum flow rate from the source node s to peer i, r_i, is limited by

$$r_i \leq \sum_{j=1}^{N} r_{j \to i} \leq D_i, \tag{7.16}$$

and

$$\begin{aligned} \sum_{i=1}^{N} r_i &\leq \sum_{i=1}^{N} \sum_{j=1}^{N} r_{j \to i} && (7.17) \\ &= \sum_{j=1}^{N} r_{j \to j} + \sum_{j=1}^{N} \sum_{i=1, i \neq j}^{N} r_{j \to i} && (7.18) \\ &\leq U_s + \sum_{j=1}^{N} U_j. && (7.19) \end{aligned}$$

Consider the cut of $\{s\} \rightarrow \{1, \cdots, N\}$, r_i is also bounded by

$$r_i \leq \sum_{j=1}^{N} r_{j \to j} \leq U_s. \tag{7.20}$$

Inequalities (7.16) and (7.20) indicate that the downloading flow rate for peer i is limited by peer i's downlink capacity and the source node's uplink capacity respectively. These two constraints are not only valid for the static scenario but also for dynamic scenarios.

Inequality (7.19) shows that the sum of the downloading flow rates for all peers is bounded by the total amount of the network uplink resource. Again, this constraint holds in both the static and dynamic cases.

These three constraints characterize an outer bound to the region of all feasible sets of $\{r_i\}_{i=1}^N$ satisfying (7.8 - 7.15). Therefore, for any static scheme, every set of feasible flow rates $\{r_i\}_{i=1}^N$ must satisfy (7.16), (7.19) and (7.20). However, not all $\{r_i\}_{i=1}^N$ satisfying (7.16), (7.19) and (7.20) are feasible.

Consider the following example: Let $B = 1$, $U_S = 3$, and $U_1 = U_2 = U_3 = 1$ (with $D_1 = D_2 = D_3 = \infty$), the downloading flow rates $r_1 = r_2 = 3, r_3 = 0$ satisfies the constraints (7.16), (7.19) and (7.20), but are not feasible because there is no solution to (7.8 - 7.15) with $r_1 = r_2 = 3, r_3 = 0$, i.e., no static scenario to support $r_1 = r_2 = 3, r_3 = 0$ simultaneously. Specifically, for $r_1 + r_2 = 6$, all upload capability must be deployed, including that of peer 3. However, since $r_3 = 0$, any transmission by peer 3 would violate the conservation-of-flow constraint.

Because all feasible sets of $\{r_i\}_{i=1}^N$ satisfy (7.16) (7.19) and (7.20), the solution to the following minimization problem provides a lower bound to the minimum WSDT for the static scenario:

$$\begin{array}{cc} \min & \sum_{i=1}^N W_i \frac{B}{r_i} \\ \text{subject to} & \sum_{i=1}^N r_i \le U_s + \sum_{i=1}^N U_i \\ & 0 \le r_i \le \tilde{D}_i \triangleq \min(D_i, U_s), \forall i = 1, \cdots, N, \end{array} \tag{7.21}$$

where only r_i $(i = 1, \cdots, N)$ are the variables. Empirical experiments presented in Section 7.5.5 show that this lower bound is tight for most P2P networks.

The minimization problem (7.21) is a convex optimization. Its optimal solutions are also the solutions to the associated Karush−Kuhn−Tucker (KKT) conditions [52]. The KKT conditions for problem (7.21) are

$$-W_i \cdot \frac{1}{r_i^2} + \lambda + \mu_i = 0, \quad i = 1, \cdots, N; \tag{7.22}$$

$$\sum_{i=1}^{N} r_i - U_s - \sum_{i=1}^{N} U_i \leq 0, \quad \lambda \geq 0; \tag{7.23}$$

$$r_i - \tilde{D}_i \leq 0, \quad \mu_i \geq 0; \tag{7.24}$$

$$\lambda(\sum_{i=1}^{N} r_i - U_s - \sum_{i=1}^{N} U_i) = 0; \tag{7.25}$$

$$\mu_i(r_i - \tilde{D}_i) = 0, \quad i = 1, \cdots, N. \tag{7.26}$$

Solving the KKT conditions yields the following optimal solution for $\{r_i\}$:

$$r_i^* = \begin{cases} \sqrt{W_i} \cdot R, & \text{if } \sqrt{W_i} \cdot R < \tilde{D}_i \\ \tilde{D}_i & \text{if } \sqrt{W_i} \cdot R \geq \tilde{D}_i \end{cases}, \tag{7.27}$$

where R is chosen such that

$$\sum_{i=1}^{N} r_i^* = \min(U_s + \sum_{i=1}^{N} U_i, \sum_{i=1}^{N} \tilde{D}_i). \tag{7.28}$$

The lower bound to the WSDT for the static scenario is then

$$\sum_{i=1}^{N} W_i t_i \geq \sum_{i=1}^{N} W_i \frac{B}{r_i^*}, \tag{7.29}$$

with r_i^* as specified in 7.27.

For the special case where $W_i = 1$ and $D_i = \infty$ ($i = 1, \cdots, N$), the solution given in (7.27) becomes

$$r_i^* = \min(U_s, \frac{U_s + \sum_{i=1}^{N} U_i}{N}), \tag{7.30}$$

and the lower bound to the minimum WSDT is

$$\sum_{i=1}^{N} t_i \geq \frac{NB}{\min(U_s, \frac{U_s+\sum_{i=1}^{N} U_i}{N})}. \tag{7.31}$$

Mutualcast [24] was designed to minimize the maximum download time for the case where $D_i = \infty$. However, since Mutualcast can achieve the download time of $\frac{B}{\min(U_s, \frac{U_s+\sum_{i=1}^{N} U_i}{N})}$ for all peers, it achieves the lower bound of (7.29) for the $W_i = 1$ case. This fact shows both that the lower bound of (7.29) is tight when $W_i = 1$ and $D_i = \infty$ and that Mutualcast minimizes sum download time as well as the maximum download time when $D_i = \infty$.

7.4 Mutualcast and Extended Mutualcast for the Equal-Weight Static Case

The concluding paragraph of Section 7.3.4 stated that Mutualcast minimizes the sum download time for the case where $D_i = \infty$. In this section we extend Mutualcast to provide an algorithm we call Extended Mutualcast that handles finite constraints on D_i (possibly delivering different rates to different peers) while still minimizing the sum download time.

7.4.1 Mutualcast

Mutualcast delivers the same rate to every peer. Assuming $D_i = \infty$, Mutualcast can support peers with any rate $R \leq \min(U_s, \frac{U_s+\sum_{i=1}^{N} U_i}{N})$. The key aspect of Mutualcast is that the source first delivers bandwidth to each node according to how much that node can share with all other peers. After that, if the source has any upload bandwidth left over, it is divided evenly among all peers. This leftover rate goes serves only one peer; it is not relayed to any other peers. Thus Mutualcast first forms a series of depth-two trees from the source to all nodes. Then, if there is any source upload bandwidth left over, it is used to form a series of depth-one trees. Here is a specification of the Mutualcast algorithm (without considering helper nodes):

Algorithm 1 The Mutualcast Algorithm for Network Resource Allocation

```
Given broadcast rate $R \leq \min(U_s, \frac{U_s+\sum_{i=1}^{N} U_i}{N})$.
Given an ordering of the peers. (Without loss of generality, assume the order is $1, \cdots, N$.)
for $i = 1$ to $N$ do
    $r_{s\to i} \leftarrow \min(R, U_i/(N-1))$.
    $r_{i\to j} \leftarrow r_{s\to i}$ for $j \neq i$.
    $R \leftarrow R - r_{s\to i}$.
    $U_s \leftarrow U_s - r_{s\to i}$.
end for
$r_{s\to i} \leftarrow r_{s\to i} + R$.
```

Mutualcast delivers information to all peers at the same rate. As described in Algorithm 1 the highest rate that Mutualcast can deliver is

$$R = \min(U_s, \frac{U_s + \sum_{i=1}^{N} U_i}{N}). \tag{7.32}$$

Consider two examples with ten peers, one in which $R = U_s$ and one in which $R = \frac{U_s+\sum_{i=1}^{N} U_i}{N}$.

First an example where $R = U_s$. Note that in general it is not possible for any peer to receive information at a rate higher than U_s. Let $U_s = 1$, $U_i = 1$ for all ten peers, and $D_i = \infty$ for all ten peers. Mutualcast achieves $R = U_s = 1$ by having nine peers receive rate 1/9 from the source and forward at that rate to the nine other peers. One peer receives no information directly from the source because by the time the Mutualcast algorithm gets to that peer, the source upload bandwith has been used up.

For an example where $R = \frac{U_s + \sum_{i=1}^{N} U_i}{N}$ a larger U_s is necessary. Let $U_s = 10$, $U_i = 1$ for all ten peers and $D_i = \infty$ for all ten peers. Mutualcast achieves $R = \frac{U_s + \sum_{i=1}^{N} U_i}{N} = 2$. In the first part of the Mutualcast algorithm, all ten peers receive rate 1/9 from the source and relay at that rate to the nine other peers. At this point there remains 80/9 of source upload bandwidth, which is distributed evenly so that each peer receives a rate of 8/9 directly from the source that it does not relay. In total, each peer receives rate 2 which is comprised of rate 1 from other peers, rate 1/9 from the source that it relays to the other peers, and rate 8/9 from the source that it does not relay.

The basic Mutualcast algorithm does not consider download constraints. The slight modification of Mutualcast given below includes download bandwidth constraints D_i in the simplest possible way. Note that if all peers are to receive at the same rate, that rate must be less than the smallest download constraint. This is reflected in line 1 of Algorithm 2.

Algorithm 2 The Mutualcast Algorithm with Download Bandwidth Constraints

```
 1: Given broadcast rate $R \leq \min\left(U_s, \frac{U_s + \sum_{i=1}^{N} U_i}{N}, \min_{j \in \{1,\ldots,N\}}(D_j)\right)$.
 2: Given an order of peers. (Without loss of generality, assume the order is
    $1, \cdots, N$.)
 3: for $i = 1$ to $N$ do
 4:     $r_{s \to i} \leftarrow \min(R, D_i, U_i/(N-1))$.
 5:     $r_{i \to j} \leftarrow r_{s \to i}$ for $j \neq i$.
 6:     $R \leftarrow R - r_{s \to i}$.
 7:     $U_s \leftarrow U_s - r_{s \to i}$.
 8:     $D_j \leftarrow D_j - r_{s \to i}$ for $j = 1, \cdots, N$.
 9: end for
10: $r_{s \to i} \leftarrow r_{s \to i} + R$.
```

As with the original Mutualcast, Algorithm 2 delivers the same rate to every peer. This alone is enough to prevent it from minimizes the sum download time in general when there are download constraints. However, it will turn out to be an important component of Extended Mutualcast, which is an algorithm that does minimize the sum download time under general download constraints.

7.4.2 Extended Mutualcast

Setting $W_i = 1$ for all i in (7.27) produces the following lower bound on the sum download time when both upload and download constraints are considered:

$$\sum_{i=1}^{N} \frac{B}{r_i^*}, \tag{7.33}$$

where

$$r_i^* = \begin{cases} R, & \text{if } R < \tilde{D}_i \\ \tilde{D}_i & \text{if } R \geq \tilde{D}_i \end{cases} \tag{7.34}$$

$$= \min(R, D_i, U_s), \tag{7.35}$$

where R is chosen such that

$$\sum_{i=1}^{N} r_i^* = \min(U_s + \sum_{i=1}^{N} U_i, \sum_{i=1}^{N} \tilde{D}_i). \tag{7.36}$$

This lower bound can be achieved by a routing-based scheme that we call Extended Mutualcast.

Consider a P2P network with constraints on peer uplink bandwidth and peer downlink bandwidth. Without loss of generality, assume that $D_1 \leq \cdots \leq D_N$. Hence, $\tilde{D}_i \leq \cdots \leq \tilde{D}_N \leq U_s$ and $r_1^* \leq \cdots \leq r_N^*$. The network resource allocation and the routing for Extended Mutualcast are provided in Algorithms 3 and 4 respectively.

Algorithm 3 Network Resource Allocation for Extended Mutualcast

```
Calculate $R$ and $r_i^*$ $(i = 1, \cdots, N)$ from (7.33-7.36).
Initialize network resource allocation $r_{i \to j} \leftarrow 0$.
if $R \leq \tilde{D}_1$ then
    $r_i^* = R$ for all $i = 1, \cdots, N$.
    Apply Algorithm 2 with rate $R$ to the network.
else if $\tilde{D}_j < R \leq \tilde{D}_{j+1}$ for $j \in \{1, \cdots, N-1\}$ then
    $r_i^* = \tilde{D}_i$ for $i \in \{1, \cdots, j\}$.
    $r_i^* = R$ for $i \in \{j+1, \cdots, N\}$.
    for Step $i = 1$ to $j$ do
        Successively apply Algorithm 2 with rate $\tilde{D}_i - \tilde{D}_{i-1}$ $(\tilde{D}_0 \triangleq 0)$ to the
        network with the source node $s$ and the ordered peers $\{i, \cdots, N\}$. Note
        that with each successive application of Algorithm 2, the values of $r_{i \to j}$
        accumulate.
    end for
    Step $j+1$: Apply Algorithm 2 one final time with rate $R - \tilde{D}_j$ to the
    network with the source node $s$ and the ordered peers $\{j+1, \cdots, N\}$.
    Again, the values of $r_{i \to j}$ accumulate.
else if $R \geq \tilde{D}_N$ then
    $r_i^* = \tilde{D}_i = D_i$ for $i = 1, \cdots, N$.
    for Step $i = 1$ to $N$ do
        Successively apply Algorithm 2 with supporting rate $\tilde{D}_i - \tilde{D}_{i-1}$ to the
        network with the source node $s$ and the ordered peers $\{i, \cdots, N\}$. Note
        that with each successive application of Algorithm 2, the values of $r_{i \to j}$
        accumulate.
    end for
end if
```

Algorithm 4 Routing Scheme for Extended Mutualcast

```
Given $R$ and $r_i^*$ $(i = 1, \cdots, N)$ from (7.33-7.36).
Given the network resource allocation $r_{i \to j}$ $(i, j = 1, \cdots, N)$ by Algorithm 3
where $r_{i \to i} \triangleq r_{s \to i} \geq r_{i \to j}$. (This routing scheme is based on that network
resource allocation.)
Partition the whole file into many chunks.
**if** $R \leq \tilde{D}_1$ **then**
  Apply the routing scheme of Mutualcast [24]. That is, for each $i = 1, \cdots, N$
  and some $j \neq i$, accumulatively route $\frac{r_{i \to j}}{R}$ fraction of all chunks from the
  source node to peer $i$, and then copy and route them from peer $i$ to other
  peers. Accumulatively route the rest of the chunks are from the source
  node to all peers directly.
**else if** $\tilde{D}_j < R \leq \tilde{D}_{j+1}$ for $j = 1, \cdots, N-1$. **then**
  For $k = 1, \cdots, j$, broadcast $\frac{\tilde{D}_k - \tilde{D}_{k-1}}{R}$ fraction of all chunks to peers
  $\{k, \cdots, N\}$ by Mutualcast. Broadcast the rest of the chunks to peers
  $\{j+1, \cdots, N\}$ by Mutualcast.
  Until peers $\{j+1, \cdots, N\}$ finish downloading.
  **for** Step $i = j$ to 1 **do**
    In Step $i$, the interesting chunks are those peer $i$ hasn't received.
    For $k = 1, \cdots, i$, accumulatively broadcast $\frac{\tilde{D}_k - \tilde{D}_{k-1}}{\tilde{D}_i}$ fraction of the in-
    teresting chunks to peers $k, \cdots, i$ by Mutualcast.
    Until peer $i$ finishes downloading.
    Note that peers $i+1, \cdots, N$ finish downloading before Step $i$.
    Note that prior to Step $i$, none of the peers $1, \cdots, i$ contain the interesting
    chunks broadcast during Step $i$.
  **end for**
**else if** $R \geq \tilde{D}_N$ **then**
  **for** Step $i = N$ to 1 **do**
    In Step $i$, the interesting chunks are those peer $i$ hasn't received.
    For $k = 1, \cdots, i$, accumulatively broadcast $\frac{\tilde{D}_k - \tilde{D}_{k-1}}{\tilde{D}_i}$ fraction of the in-
    teresting chunks to peers $k, \cdots, i$ by Mutualcast.
    Until peer $i$ finishes downloading.
  **end for**
**end if**
```

The network resource allocation for Extended Mutualcast (Algorithm 3) is obtained by successively applying Algorithm 2 to the P2P network or part of the P2P network. The network resource allocation by Algorithm 3 has $r_{s\to i} \geq r_{i\to j}$ for all i, j. The flow rate to peer i, r_i, is then equal to its download rate $\sum_{j=1}^{N} r_{j\to i}$. The routing scheme for Extended Mutualcast (Algorithm 4) guarantees that the entire flow rate r_i is *useful*. For the Extended Mutualcast rate allocation, $r_i = \min(R, \tilde{D}_i)$ so that the lower bound (7.33-7.36) on sum download time is achieved. Theorem 2 formally states and proves this fact.

Theorem 2. ***(Minimum Sum Delay)*** *Consider multicasting a file with size B from a source node s to peers $\{1, \cdots, N\}$ in a P2P network with constraints on peer uplink bandwidth and peer downlink bandwidth. The minimum sum download time for the static scenario is $\sum_{i=1}^{N} \frac{B}{r_i^*}$, where r_i^*, the flow rate to peer i, follows from (7.33-7.36).*

Proof. (**Converse**) From (7.33-7.36), $\sum_{i=1}^{N} \frac{B}{r_i^*}$ is a lower bound on the minimum sum download time. Hence, any sum download time less than $\sum_{i=1}^{N} \frac{B}{r_i^*}$ is not achievable.

(**Achievability**) It is sufficient to show that (a) Extended Mutualcast is applicable to any P2P network, and (b) Extended Mutualcast provides a static scenario in which the flow rate from the source node to peer i is r_i^* of (7.33-7.36).

(**To Show (a)**) It is sufficient to show that in Algorithm 3, the rate for each applied Algorithms 2 is attainable. In other words, each rate for the applied network is less than or equal to the minimum of the source node's uplink capacity and the total uplink resource over all of the peers.

- If $R \leq \tilde{D}_1$, then $R \leq U_s$ and $R \leq \frac{U_s + \sum_{i=1}^{N} U_i}{N}$. Hence, the rate R is attainable for Algorithm 2 in Line 4, Algorithm 3.

- If $\tilde{D}_j < R \leq \tilde{D}_{j+1}$, consider the worst case of $D_i = R$ for $i = j+1, \cdots, N$ and $U_s = R$. In this case, we have

$$r_i^* = \tilde{D}_i, \quad i = 1, \cdots, N; \tag{7.37}$$

$$U_i \leq D_i = \tilde{D}_i, \quad i = 1, \cdots, j; \tag{7.38}$$

$$\tilde{D}_1 \leq \cdots \leq \tilde{D}_j < R = \tilde{D}_{j+1} = \cdots = \tilde{D}_N = U_s; \tag{7.39}$$

$$\sum_{i=1}^{N} \tilde{D}_i = U_s + \sum_{i=1}^{N} U_i. \tag{7.40}$$

Denote $U_p^{(i)}$ as the total amount of the peers' uplink resource used after Step i, and $U_s^{(i)}$ as the total amount of the source node's uplink resource used after Step i. For Step 1, $\tilde{D}_1 \leq U_s$ and $\tilde{D}_1 \leq \frac{\sum_{i=1}^{N} \tilde{D}_i}{N} = \frac{U_s + \sum_{i=1}^{N} U_i}{N}$. Hence, Algorithm 2 in Step 1 is feasible. Suppose Algorithm 2 is feasible for Step 1 to Step n $(1 \leq n \leq j)$. Then $U_s^{(i)} = \tilde{D}_i$ and $U_p^{(i)} = \sum_{k=1}^{i} \tilde{D}_k + (N-i-1)\tilde{D}_i$. Hence,

$$U_p^{(i)} \geq \sum_{k=1}^{i} \tilde{D}_k = \sum_{k=1}^{i} D_k \geq \sum_{k=1}^{i} U_k, \tag{7.41}$$

which indicates that Algorithm 2 for Step 1 to Step i fully deploys the uplink resources of peers $1, \cdots, i$.

Now consider Algorithm 2 for Step $n+1$, the supporting rate is $\tilde{D}_{n+1} - \tilde{D}_n$.

The source node's uplink is $R - \tilde{D}_n$. The total uplink resource is

$$U_s + \sum_{i=1}^{N} U_i - (U_s^{(n)} + U_p^{(n)}) \tag{7.42}$$

$$= \sum_{i=1}^{N} \tilde{D}_i - (\sum_{k=1}^{n} \tilde{D}_k + (N-n)\tilde{D}_n) \tag{7.43}$$

$$= \sum_{k=n+1}^{N} (\tilde{D}_i - \tilde{D}_n) \tag{7.44}$$

$$\geq (N-n)(\tilde{D}_{n+1} - \tilde{D}_n), \tag{7.45}$$

where (7.43) follows from (7.40), and (7.45) follows from (7.39). Hence, the rate $\tilde{D}_{n+1} - \tilde{D}_n$ is less than or equal to the total available uplink resource (7.42) divided by the number of peers, $N - n$. We also can see that $\tilde{D}_{n+1} - \tilde{D}_n$ is less than or equal to the available source node's uplink bandwidth, $R - \tilde{D}_n$. Therefore, Algorithm 2 for Step $n+1$ is also feasible. By induction, Algorithm 2 is feasible for every step.

- If $R \geq \tilde{D}_N$, then

$$D_1 \leq \cdots \leq D_N \leq R \leq U_s; \tag{7.46}$$

$$r_i^* = D_i = \tilde{D}_i, \quad i = 1, \cdots, N; \tag{7.47}$$

$$\sum_{i=1}^{N} r_i^* = \sum_{i=1}^{N} D_i \leq \sum_{i=1}^{N} U_i + U_s. \tag{7.48}$$

Consider the worst case of $\sum_{i=1}^{N} D_i = \sum_{i=1}^{N} U_i + U_s$. For this worst case, Algorithm 2 in Line 14 is feasible following an argument similar to that for the case of $\tilde{D}_j < R \leq \tilde{D}_{j+1}$.

Therefore, Extended Mutualcast in Algorithm 3 is applicable to any P2P network.

(**To Show (b)**) From Algorithms 2 and 3, Extended Mutualcast constructs a static scenario with $r_{s\to i} \triangleq r_{i\to i} \geq r_{i\to j}$ for $i, j = 1, \cdots, N$, and $\sum_{j=1}^{N} r_{j\to i} \geq \min(R, \tilde{D}_i) = r_i^*$. Hence, the maximum flow from the source node to peer i is larger than or equal to

$$\sum_{j=1, j\neq i}^{N} \min(r_{s\to j}, r_{j\to i}) + r_{s\to i} \tag{7.49}$$

$$= \sum_{j=1, j\neq i}^{N} r_{j\to i} + r_{s\to i} \tag{7.50}$$

$$\geq r_i^*. \tag{7.51}$$

Therefore, Extended Mutualcast provides a static scenario in which the flow rate from the source node to peer i is r_i^* of (7.33-7.36). □

Theorem 2 showed that Extended Mutualcast minimizes the sum download time for any static P2P network. When the total uplink bandwidth resource is sufficiently abundant, Extended Mutualcast also minimizes the weighted sum download time for any set of weights because all peers are downloading at their limit of $\tilde{D}_i$. Corollary 1 formally states and proves this fact.

Corollary 1. *Consider multicasting a file with size B from a source node s to peers $\{1, \cdots, N\}$ in a P2P network with constraints on peer uplink bandwidth and peer downlink bandwidth. If $U_s + \sum_{i=1}^{N} U_i \geq \sum_{i=1}^{N} \tilde{D}_i$, the set of the flow rates $r_i = \tilde{D}_i$ $(i = 1, \cdots, N)$ is attainable. Hence, the minimum weighted sum download time for the static scenario is $\sum_{i=1}^{N} W_i \frac{B}{\tilde{D}_i}$ for any given weights W_i.*

Proof. (**Achievability**) Note that when $U_s + \sum_{i=1}^{N} U_i \geq \sum_{i=1}^{N} \tilde{D}_i$, r_i^* of (7.33-7.36) is equal to $\tilde{D}_i$. By Theorem 2, Extended Mutualcast can achieve the download rates $r_i^* = \tilde{D}_i$.

(**Converse**) By Max-Flow Min-Cut Theorem, the maximum flow from source node to peer i is limited by $\tilde{D}_i = \min(D_i, U_s)$. Hence, any weighted sum downloading time less than $\sum_{i=1}^{N} W_i \frac{B}{\tilde{D}_i}$ is not achievable. □

7.5 A Depth-2 Approach for the Minimizing Weighted Sum Download Time

Section 7.4 provided a complete solution (Extended Mutualcast) for achieving the minimum sum download time with constraints on both peer uplink bandwidth and peer downlink bandwidth. That section concluded by showing that if the total uplink resource is sufficiently abundant, Extended Mutualcast minimizes WSDT for any set of weights. This section attacks the minimization of WSDT more broadly.

Mutualcast and Extended Mutualcast construct only two types of trees to distribute content. The first type is a depth-1 tree as shown in Fig. 7.6(a). The source node s broadcasts content to all peers directly with rate $r^{(1)}_{s\to i}$, $i = 1, \cdots, N$. The second type is a depth-2 tree as shown in Fig. 7.6(b). The source node distributes content to peer i with rate $r^{(2)}_{s\to i}$, and then peer i relays this content to all other peers.

In Mutualcast, the rates $r^{(1)}_{s\to i}$ are constrained to be equal for all i. Also, for a fixed i, $r^{(2)}_{s\to i} = r_{i\to j}$ for all $j \in \{1, \cdots, N\}$; $\quad j \neq i$. These constraints on the network resource allocation simplify the mechanism design and allow a simple routing-based scheme. These two constraints together ensure that each peer downloads content at the same rate. However, to optimize WSDT peers surely need to download content and different rates.

In Section 7.4 we saw that peers needed to download content at different rates

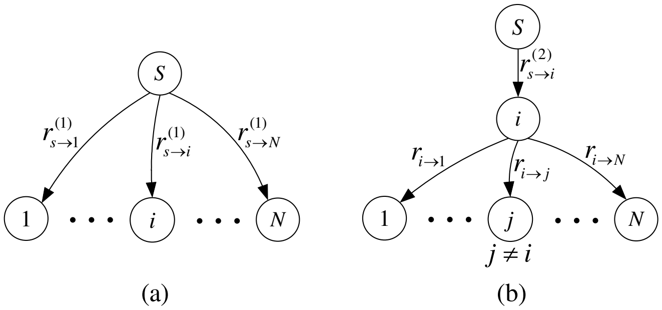


Figure 7.6: The two tree sturctures used by Mutualcast and Extended Mutualcast: (a) Depth-1 tree; (b) Depth-2 tree.

to minimize the sum download time with peer downlink bandwidth constraints. The Extended Mutualcast algorithm provided a way to serve the peers at different rates corresponding to their download bandwidth constraints so as to minimize the sum download time. However, Extended Mutualcast required successive applications of Mutualcast which led to a complicated routing protocol.

In order to serve peers at different rates to minimize WSDT and still maintain a simple mechanism design, we apply the technique of rateless coding at the source node. A rateless code is an erasure correcting code. It is rateless in the sense that the number of encoded packets that can be generated from the source message is potentially limitless [53]. Suppose the original file size is B packets, once the receiver has received any B' packets, where B' is just slightly greater than B, the whole file can be recovered.

Fountain codes [53], LT codes [54], and raptor codes [55] are rateless erasure codes. LT codes have linear encoding complexity and sub-linear decoding complexity. Raptor codes have linear encoding and decoding complexities. The percentage of the overhead packets goes to zero as B goes to infinity. In practice, the overhead is about 5% for LT codes with file size $B \simeq 10000$ [53]. This subsection focuses on applying rateless erasure codes for P2P file transfer instead of designing rateless erasure codes. Hence, we assume the overhead of the applied rateless erasure code is zero for simplicity. We note that if redundancy does not need to be limitless, there are solutions that provide zero overhead [56].

7.5.1 The Rateless-Coding-Based Scheme

We propose a rateless-coding-based scheme that constructs the two types of trees in Fig. 7.6 to distribute the content as did Mutualcast and Extended Mutualcast. The source node first partitions the whole file into B chunks and applies a rateless erasure code to these B chunks producing a potentially limitless number of chunks.

For the depth-1 tree, the source node broadcasts different rateless-coded chunks directly to each peer. For the depth-2 trees, The source node sends different rateless-coded chunks to each peer, and then that peer relays some or all of those chunks to other some or all of the other peers. A key point is that every chunk transmitted by the source is different from every other chunk transmitted by the source. This condition guarantees that all chunks received by a peer are useful (because they are not a repetition of a previously received chunk). Hence, a peer can decode the whole file as long as it receives B coded chunks.

The rateless-coding-based scheme allows peers to download content at different rates with a simpler mechanism than the routing-based approach of Extended Mutualcast. Peers don't have to receive exactly the same chunks to decode the whole file. Hence, the two types of tree structures can be combined as one tree structure with depth 2, but without the constraint that the rate from the peer to its neighbors has to equal the rate from the source to the peer.

The source node sends coded chunks to peer i with rate $r_{s\to i} = r^{(1)}_{s\to i} + r^{(2)}_{s\to i}$, and peer i relays some of them to peer j ($j \neq i$) with rate $r_{i\to j} \leq r_{s\to i}$. Note that the values of $r_{i\to j}$ do not even need to be the same for a fixed value of i and different values of j.

Another benefit of applying a rateless coding approach is that it is robust to packet loss in the Internet if we allow some extra rate for each user.

Assuming rateless coding at the source node and constraining the P2P network to include only depth-2 trees as discussed above, the network resource allocation that minimizes WSDT can be obtained by solving the following convex optimization problem.

$$\begin{array}{cc} \min & \sum_{i=1}^{N} W_i \frac{B}{r_i} \\ \text{subject to} & 0 \le r_{i\to j} \le r_{i\to i}, \forall i, j = 1, \cdots, N, \\ & \sum_{i=1}^{N} r_{i\to i} \le U_s, \\ & \sum_{j=1, j\neq i}^{N} r_{i\to j} \le U_i, \forall i = 1, \cdots, N, \\ & r_i = \sum_{j=1}^{N} r_{j\to i} \le D_i, \forall i = 1, \cdots, N, \end{array} \tag{7.52}$$

where $r_{i\to i} \triangleq r_{s\to i}$. The complexity for the interior point method to solve this convex optimization is $O((N^2)^{3.5})$ [52].

For the case of $W_i = 1, D_i = \infty$, the optimal resource allocation is, of course, the same as that of Mutualcast.

For the case of $W_i = 1$ and finite values of D_i, Algorithm 3 provides an optimal network resource allocation that certainly also solves 7.52. A key point is that the routing of Algorithm 4 becomes unnecessary if the source employs rateless coding. Peers need only relay the appropriate number of chunks to the appropriate neighbors without worrying about *which* chunks are relayed.

For other cases, we provide a network resource allocation that we have not proven to be optimal. We will see in Section 7.5.5 that its performance achieves the lower bound (7.29) across a wide range of parameterizations.

7.5.2 Resource Allocation for Networks with $D_i = \infty$

Consider a P2P network in which peer uplink bandwidth is constrained but $D_i = \infty$ for $i = 1, \cdots, N$. If $\sum_{i=1}^{N} U_i \geq (N-1)U_s$, then the resource allocation of $r_{i \to j} = \frac{U_s U_i}{\sum_{i=1}^{N} U_i}$ achieves the minimum WSDT with flow rates $r_i = U_s$ for all $i = 1, \cdots, N$. (This is the case discussed at the end of Section 7.4.) Otherwise, consider the following water-filling-type solution:

$$\tilde{r}_i = \begin{cases} \sqrt{W_i} \cdot R, & \text{if } \sqrt{W_i} \cdot R < U_s, \\ U_s & \text{if } \sqrt{W_i} \cdot R \geq U_s, \end{cases} \tag{7.53}$$

where R is chosen such that

$$\sum_{i=1}^{N} \tilde{r}_i = U_s + \sum_{i=1}^{N} U_i - \max_k(\tilde{r}_k). \tag{7.54}$$

The potential suboptimality of this approach comes from the subtraction of $\max_k(\tilde{r}_k)$ on the right side of (7.54) which does not appear in (eq:ratesumforbound). Note that when $\max(\tilde{r}_k) \ll U_s + \sum_{i=1}^{N} U_i$ (this is true for large N), $\tilde{r}_i$ is close to r_i^* corresponding to the lower bound (7.27).

We now show that the proposed suboptimal network resource allocation ensures that the flow rate to peer i is larger than or equal to $\tilde{r}_i$ of (7.53). Hence, the WSDT for the proposed suboptimal resource allocation is very close to the lower bound to the minimum WSDT for large networks.

First assign the rates for the depth-2 trees with

$$r^{(2)}_{s\to i} = c\frac{U_i \max(\tilde{r}_k)}{\sum_{k=1}^N \tilde{r}_k - \tilde{r}_i} \tag{7.55}$$

and

$$r_{i\to j} = c\frac{U_i \tilde{r}_j}{\sum_{k=1}^N \tilde{r}_k - \tilde{r}_i}, \tag{7.56}$$

where c is chosen to be the largest possible value satisfying

$$\sum_{i=1}^N r^{(2)}_{s\to i} \leq U_s \tag{7.57}$$

$$\sum_{j=1, j\neq i}^N r_{i\to j} \leq U_i. \tag{7.58}$$

Plugging (7.55) (7.56) into (7.57) (7.58), and obtain

$$c = \min(1, \frac{U_s}{\max(\tilde{r}_k)\alpha}), \tag{7.59}$$

where $\alpha = \sum_{i=1}^N \frac{U_i}{\sum_{k=1}^N \tilde{r}_k - \tilde{r}_i}$.

If $c = \frac{U_s}{\alpha \max(\tilde{r}_k)}$, then the depth-2 trees have already fully deployed the source node's uplink. The rate assignment for depth-2 trees is the network resource allocation for the rateless-coding-based scheme.

If $c = 1$, then the depth-2 trees have fully deployed all peers' uplinks, but not the source node's uplink. Hence, we can further deploy the rest of the source node's uplink to construct the depth-1 tree. After constructing the depth-2 trees, the flow rate to peer i is

$$\beta_i \triangleq r^{(2)}_{s\to i} + \sum_{j=1, j\neq i}^N r_{j\to i} = \alpha\tilde{r}_i + \frac{(\max_k(\tilde{r}_k) - \tilde{r}_i)U_i}{\sum_{k=1}^N \tilde{r}_k - \tilde{r}_i}.$$

The rest of the source node's uplink is

$$U_s - \sum_{i=1}^{N} r_{s\to i}^{(2)} = U_s - \alpha \max(\tilde{r}_k).$$

The optimal depth-1 tree can be obtained by the convex optimization

$$\begin{array}{cc} \min & \sum_{i=1}^{N} W_i \frac{B}{r_i} \\ \text{subject to} & r_i = \beta_i + r_{s\to i}^{(1)}, \\ & r_{s\to i}^{(1)} \geq 0, \forall i = 1 \cdots, N, \\ & \sum_{i=1}^{N} r_{s\to i}^{(1)} \leq U_s - \alpha \max(\tilde{r}_k). \end{array} \tag{7.60}$$

The optimal solution to the problem (7.60) is

$$r_i = \begin{cases} \sqrt{W_i} \cdot R, & \text{if } \sqrt{W_i} \cdot R \geq \beta_i, \\ \beta_i & \text{if } \sqrt{W_i} \cdot R < \beta_i, \end{cases} \tag{7.61}$$

and

$$r_{s\to i}^{(1)} = \begin{cases} \sqrt{W_i} \cdot R - \beta_i, & \text{if } \sqrt{W_i} \cdot R \geq \beta_i, \\ 0 & \text{if } \sqrt{W_i} \cdot R < \beta_i, \end{cases} \tag{7.62}$$

where R is chosen such that $\sum_{i=1}^{N} r_{s\to i}^{(1)} = U_s - \alpha \max(\tilde{r}_k)$ (also $\sum_{i=1}^{N} r_i = U_s + \sum_{i=1}^{N} U_i$).

The complexity of calculating this suboptimal network resource allocation is $O(N^2)$. Note that when $W_i = 1$ for all $i = 1, \cdots, N$, this suboptimal network resource allocation is the same as that of Mutualcast, and hence, this network resource allocation is optimal for this case. For general weight settings, this network resource allocation guarantees that the flow rate to peer i is larger than or equal to $\tilde{r}_i$, which is stated in the following theorem.

Theorem 3. *For P2P networks with peer uplink constraints but no peer downlink* *constraints (i.e. $D_i = \infty$), the network resource allocation determined by (7.55) (7.56) (7.59) (7.61) and (7.62) ensures that the WSDT $\sum_{i=1}^{N} W_i B / r_i$ is less than or equal to the WSDT associated to (7.53), i.e., $\sum_{i=1}^{N} W_i B / \tilde{r}_i$.*

Proof. If $c = \frac{U_s}{\alpha \max(\tilde{r}_k)}$, the flow rate to peer i is

$$
\begin{aligned}
r_i &= r_{s\to i}^{(2)} + \sum_{j=1, j\neq i}^{N} r_{j\to i} && (7.63)\\
&= c\alpha\tilde{r}_i + c\frac{(\max_k(\tilde{r}_k) - \tilde{r}_i)U_i}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i} && (7.64)\\
&\geq c\alpha\tilde{r}_i && (7.65)\\
&= \frac{U_s}{\max(\tilde{r}_k)}\tilde{r}_i && (7.66)\\
&\geq \tilde{r}_i, && (7.67)
\end{aligned}
$$

where (7.67) follows from $\tilde{r}_k \leq \tilde{D}_k \leq U_s$. If $c = 1$, a feasible solution to problem (7.60) is

$$
r_{s\to i}^{(1)} = (U_s - \alpha \max(\tilde{r}_k)) \frac{\tilde{r}_i}{\sum_{k=1}^{N} \tilde{r}_k}.
$$

For this feasible solution, the total flow rate to peer i with the depth-1 tree and the depth-2 trees is

$$
\begin{aligned}
r_i &= \beta_i + (U_s - \alpha \max(\tilde{r}_k)) \frac{\tilde{r}_i}{\sum_{k=1}^{N} \tilde{r}_k} && (7.68)\\
&= (\alpha + (U_s - \alpha \max(\tilde{r}_k)) \frac{1}{\sum_{k=1}^{N} \tilde{r}_k})\tilde{r}_i + \frac{(\max(\tilde{r}_k) - \tilde{r}_i)U_i}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i}. && (7.69)
\end{aligned}
$$

Denote $\gamma = \alpha + (U_s - \alpha \max(\tilde{r}_k))\frac{1}{\sum_{k=1}^{N} \tilde{r}_k}$. We have

$$\begin{aligned}
U_s + \sum_{i=1}^{N} U_i &= \sum_{i=1}^{N} r_i && (7.70)\\
&= \gamma \sum_{i=1}^{N} \tilde{r}_i + \sum_{i=1}^{N} \frac{(\max(\tilde{r}_k) - \tilde{r}_i)U_i}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i} && (7.71)\\
&\leq \gamma \sum_{i=1}^{N} \tilde{r}_i + \sum_{i=1}^{N} \frac{\max(\tilde{r}_k)U_i}{\sum_{k=1}^{N} \tilde{r}_k} && (7.72)\\
&\leq \gamma \sum_{i=1}^{N} \tilde{r}_i + \max(\tilde{r}_k) && (7.73)\\
&= \gamma(U_s + \sum_{i=1}^{N} U_i - \max(\tilde{r}_k)) + \max(\tilde{r}_k). && (7.74)
\end{aligned}$$

Some of these steps are justified as follows:

- (7.70) follows from the fact that all uplink resource is deployed;
- (7.72) follows from the inequality $\frac{b-d}{a-d} \leq \frac{b}{a}$ when $a \geq b \geq d \geq 0$;
- (7.73) follows from $\sum_{k=1}^{N} \tilde{r}_k = U_s - \max \tilde{r}_k + \sum_{i=1}^{N} U_i \geq \sum_{i=1}^{N} U_i \geq U_i$.

Therefore, $\gamma \geq 1$. Hence,

$$r_i = \gamma \tilde{r}_i + \frac{(\max(\tilde{r}_k) - \tilde{r}_i)U_i}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i} \geq \tilde{r}_i, \qquad (7.75)$$

which indicates that this feasible solution r_i to the problem (7.60) provides a WSDT less than or equal to $\sum_{i=1}^{N} W_i B/\tilde{r}_i$. Hence, the network resource allocation determined by (7.55) (7.56) (7.59) (7.61) and (7.62) also provides a WSDT less than or equal to $\sum_{i=1}^{N} W_i B/\tilde{r}_i$. □

7.5.3 Resource Allocation with Peer Downlink Constraints

Now we consider P2P networks with both peer uplink bandwidth constraints and peer downlink bandwidth constraints. The idea of the resource allocation for these P2P networks is the same as that for P2P networks without downlink constraints. The details are provided as follows:

If $U_s+\sum_{i=1}^N U_i \geq \sum_{i=1}^N \tilde{D}_i$, from Corollary 1, Algorithm 3 provides the optimal network resource allocation.

If $U_s + \sum_{i=1}^N U_i < \sum_{i=1}^N \tilde{D}_i$, consider a water-filling-type solution

$$\tilde{r}_i = \begin{cases} \sqrt{W_i} \cdot R, & \text{if } \sqrt{W_i} \cdot R < \tilde{D}_i, \\ \tilde{D}_i & \text{if } \sqrt{W_i} \cdot R \geq \tilde{D}_i, \end{cases} \tag{7.76}$$

where R is chosen such that $\sum_{i=1}^N \tilde{r}_i = U_s + \sum_{i=1}^N U_i - \max(\tilde{r}_k)$.

First construct the depth-2 trees with rates in (7.55) and (7.56), where c is still chosen to be the largest possible value. However, for general P2P networks, the constraints on c are not only (7.57) (7.58), but also

$$\beta_i \triangleq r_{s\to i}^{(2)} + \sum_{j=1, j\neq i}^{N} r_{j\to i} \leq \tilde{D}_i. \tag{7.77}$$

After constructing the depth-2 trees, the flow rate to peer i is β_i. The used source node's uplink is $c\alpha \max(\tilde{r}_k)$. If $c\alpha \max(\tilde{r}_k) < U_s$, we can further use the rest of the source node's uplink to distribute content through the depth-1 tree. The optimal resource allocation for the depth-1 tree can be obtained by the convex optimization

$$\begin{array}{cc} \min & \sum_{i=1}^{N} W_i \frac{B}{r_i} \\ \text{subject to} & r_i = \beta_i + r_{s\to i}^{(1)}, \\ & r_{s\to i}^{(1)} \geq 0, \forall i = 1 \cdots, N, \\ & r_i \leq \tilde{D}_i, \forall i = 1 \cdots, N, \\ & \sum_{i=1}^{N} r_{s\to i}^{(1)} \leq U_s - c\alpha \max(\tilde{r}_k). \end{array} \tag{7.78}$$

The optimal solution to the problem (7.78) is

$$r_i = \begin{cases} \sqrt{W_i} \cdot R, & \text{if } \beta_i \leq \sqrt{W_i} \cdot R \leq \tilde{D}_i, \\ \beta_i & \text{if } \sqrt{W_i} \cdot R < \beta_i, \\ \tilde{D}_i, & \text{if } \sqrt{W_i} \cdot R > \tilde{D}_i, \end{cases} \tag{7.79}$$

and

$$\tilde{r}_{s\to i}^{(1)} = r_i - \beta_i, \tag{7.80}$$

where R is chosen such that

$$\sum_{i=1}^{N} r_i = U_s + c \sum_{i=1}^{N} U_i.$$

The complexity of calculating this resource allocation is $O(N^2)$.

7.5.4 Routing-Based Depth-2 Scheme

So far, this section has provided a family of rateless-coding-based schemes for P2P file-transfer applications. In this subsection, we introduce a routing-based scheme. This routing-based scheme is a further extension to Extended Mutualcast. This scheme also applies the tree structures in Fig. 7.6 to distribute content.

The constraints on the network resource allocation for this scheme are

$$r^{(1)}_{s\to k_1} \geq \cdots \geq r^{(1)}_{s\to k_N} \geq 0, \tag{7.81}$$

and

$$\begin{aligned} & r^{(2)}_{s\to k_i} \geq r_{k_i\to k_1} \geq \cdots \geq r_{k_i\to k_{i-1}} \\ & \geq r_{k_i\to k_{i+1}} \geq \cdots \geq r_{k_i\to k_N}, \forall i = 1, \cdots, N, \end{aligned} \tag{7.82}$$

where $(k_1, \cdots, k_N)$ is the order in which the peers finish downloading. In the rest of this section, we assume the order is $(1, \cdots, N)$ for simplicity. These constraints are stricter than those of the rateless-coding-based scheme, and they are introduced to simplify the routing scheme. In particular, given the order of $(1, \cdots, N)$ in which peers finish downloading, the proposed routing-based scheme ensures that at any time in the scheme, peer i has all packets received by peers $i+1, \cdots, N$ for all $i = 1, \cdots, N-1$. This condition is achievable if the network resource allocation satisfies (7.81) and (7.82). For the routing-based scheme, when peer i finishes downloading, the scheme starts to only broadcast the chunks which peer $i+1$ hasn't received, called interesting chunks. With this condition, the interesting chunks are also new to peers $i+2, \cdots, N$. The details of the routing-based scheme is given in Algorithm 5.

The optimal network resource allocation for this routing-based scheme can be obtained by the convex optimization of minimizing $\sum_{i=1}^{N} W_i B / r_i$ subject to the constraints (7.81) (7.82), nodes' uplink and downlink constraints, and the flow rate expression

$$r_i = \sum_{j=1, j\neq i}^{N} r_{j\to i} + r^{(1)}_{s\to i} + r_{i\to i-1}, \quad i = 1, \cdots, N,$$

Algorithm 5 Routing-Based Scheme

```
Given the order in which the peers finish downloading. Assume the order is $(1, \cdots, N)$ for simplicity.
Given the network resource allocation $\{r_{i \to j}, r^{(1)}_{s \to i}, r^{(2)}_{s \to i}\}$ for $i, j = 1, \cdots, N$, which satisfies the constraints (7.81) and (7.82).
Partition the whole file into many chunks.
for Step $i = 1$ to $N$ do
    At the beginning of Step $i$, peer $1, \cdots, i$ finish downloading.
    In Step $i$, only broadcast the chunks which peer $i$ doesn't have, called interesting chunks. Note that all peers $i, \cdots, N$ don't contain the interesting chunks.
    Distribute interesting chunks along the depth-1 tree and the depth-2 trees according to the network resource allocation.
    For the depth-1 tree , the set of chunks sent to peer $i$ contains the set of chunks sent to peer $j$ for $i < j$.
    For the depth-2 tree in Fig. 7.6(b), the set of chunks from peer $i$ to peer $k$ contains the set of chunks from peer $i$ to peer $j$ for $k > j$. Peer $i$ only keeps the set of chunks sent to peer $i - 1$ for $i = 2, \cdots, N$.
    The above two chunk selection constraints guarantee that peers $i, \cdots, N$ don't contain the interesting chunks in Step $i$ for $i = 1, \cdots, N$.
    Until peer $i$ receives all interesting chunks and finishes downloading.
end for
```

where $r_{1\to 0} = r_{s\to 1}^{(2)}$. The complexity for the interior point method to solve the problem is $O((N^2)^{3.5})$. For Case I in which $W_i = 1$ and $D_i = \infty$, the optimal network resource allocation is the same as that of Mutualcast. For the case of $W_i = 1$ or $U_s + \sum_{i=1}^{N} U_i \geq \sum_{i=1}^{N} \tilde{D}_i$, by Theorem 2 and Corollary 1, Algorithm 3 provides the optimal network resource allocation.

For general cases with $U_s + \sum_{i=1}^{N} U_i < \sum_{i=1}^{N} \tilde{D}_i$, we provide a suboptimal network resource allocation for this routing-based scheme. Consider the water-filling-type solution in (7.76). Without loss of generality, assume that $\tilde{r}_1 \geq \cdots \geq \tilde{r}_N$, and give the ordering $(1, \cdots, N)$ in which the peers finish downloading. First construct the depth-2 trees with rates in (7.55) and (7.56), where c is still chosen to be the largest possible value satisfying (7.57) (7.58) and (7.77). After constructing the depth-2 trees, the effective flow rate to peer i is

$$\beta_i = \sum_{j=1, j\neq i}^{N} r_{j\to i} + r_{i\to i-1} \tag{7.83}$$

$$= c(\alpha\tilde{r}_i + \frac{\tilde{r}_{i-1} - \tilde{r}_i}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i} U_i), \tag{7.84}$$

where $\tilde{r}_0 \triangleq \tilde{r}_1$. The download rate (used downlink) for peer i is $c(\alpha\tilde{r}_i + \frac{\tilde{r}_1 - \tilde{r}_i}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i} U_i)$. Note that the effective flow rate is smaller than the download rate for peer i. This is because peer i only keeps a subset of chunks received from the source node. For this reason, parts of peer i's downlink and the source node's uplink are wasted. The total amount of the wasted uplink is

$$U_w = c \sum_{i=1}^{N} \frac{\tilde{r}_1 - \tilde{r}_{i-1}}{\sum_{k=1}^{N} \tilde{r}_k - \tilde{r}_i} U_i. \tag{7.85}$$

The used source node's uplink is $c\alpha\tilde{r}_1$. If $c\alpha\tilde{r}_1 < U_s$, we can further use the rest of the source node's uplink to distribute content through the depth-1 tree. The constraints on the resource allocation for the depth-1 tree are (7.81),

$$r^{(1)}_{s\to i} \leq D_i - \beta_i, \forall i = 1, \cdots, N, \tag{7.86}$$

and

$$\sum_{i=1}^{N} r^{(1)}_{s\to i} \leq U_s - c\alpha\tilde{r}_1. \tag{7.87}$$

Let $\hat{W}_i = \min_{k\leq i}(W_k)$. Let $\hat{D}_i = \min_{k\leq i}(D_k - \beta_k)$. A sub-optimal network resource allocation for the depth-1 tree is

$$r^{(1)}_{s\to i} = \begin{cases} \sqrt{\tilde{W}_i}\cdot R - \beta_i, & \text{if } \beta_i \leq \sqrt{W_i}\cdot R \leq \hat{D}_i, \\ 0 & \text{if } \sqrt{\tilde{W}_i}\cdot R < \beta_i, \\ \hat{D}_i - \beta_i, & \text{if } \sqrt{\tilde{W}_i}\cdot R > \tilde{D}_i, \end{cases} \tag{7.88}$$

and $r_i = r^{(1)}_{s\to i} + \beta_i$, where R is chosen such that

$$\sum_{i=1}^{N} r^{(1)}_{s\to i} = U_s - c\alpha\tilde{r}_1$$

and also

$$\sum_{i=1}^{N} r_i = U_s + c\sum_{i=1}^{N} U_i - U_w.$$

The complexity of calculating the suboptimal resource allocation for the routing-based scheme is $O(N^2)$.

7.5.5 Simulations for the Static Scenario

This section provides the empirical WSDT performances of the rateless-coding-based scheme, the routing-based scheme, and compares them with the lower bound to the WSDT. In all simulations, the file size B is normalized to be 1.

This section shows simulations for 6 cases of network settings as follows:

- Case I: $U_i = 1$, $D_i = \infty$ for $i = 1, \cdots, N$;
- Case II: $U_i = 1$, $D_i = 8$ for $i = 1, \cdots, N$;
- Case III: $U_i = i/N$, $D_i = \infty$ for $i = 1, \cdots, N$;
- Case IV: $U_i = i/N$, $D_i = 8i/N$ for $i = 1, \cdots, N$;
- Case V: $U_i = 1 + 9\delta(i > N/2)$, $D_i = \infty$ for $i = 1, \cdots, N$;
- Case VI: $U_i = 1 + 9\delta(i > N/2)$, $D_i = 8i/N$, $i = 1, \cdots, N$;

where $\delta(\cdot)$ is the indicate function.

Consider small P2P networks with $N = 10$ peers. The performances of sum download time versus U_s for these 6 cases are shown in Fig. 7.7. The performances of WSDT versus U_s with weight $W_i = i/N$ ($i = 1, \cdots, N$) are shown in Fig. 7.8. The performances of WSDT versus U_s with weight $W_i = 1 + \delta(i > N/2)$ ($i = 1, \cdots, N$) are shown in Fig. 7.9. In all these simulations, the weighted sum download times of the rateless-coding-based scheme and the routing-based scheme achieve or almost achieve the lower bound.

Consider large P2P networks with $N = 1000$ peers. The performances of sum download time versus U_s for these 6 cases are shown in Fig. 7.10. The performances of WSDT versus U_s with weight $W_i = i/N$ ($i = 1, \cdots, N$) are shown in Fig. 7.11. The performances of WSDT versus U_s with weight $W_i = 1 + \delta(i > N/2)$ ($i = 1, \cdots, N$) are shown in Fig. 7.12. In all these simulations, the weighted sum download times of the rateless-coding-based scheme and the routing-based scheme also achieve or almost achieve the lower bound.

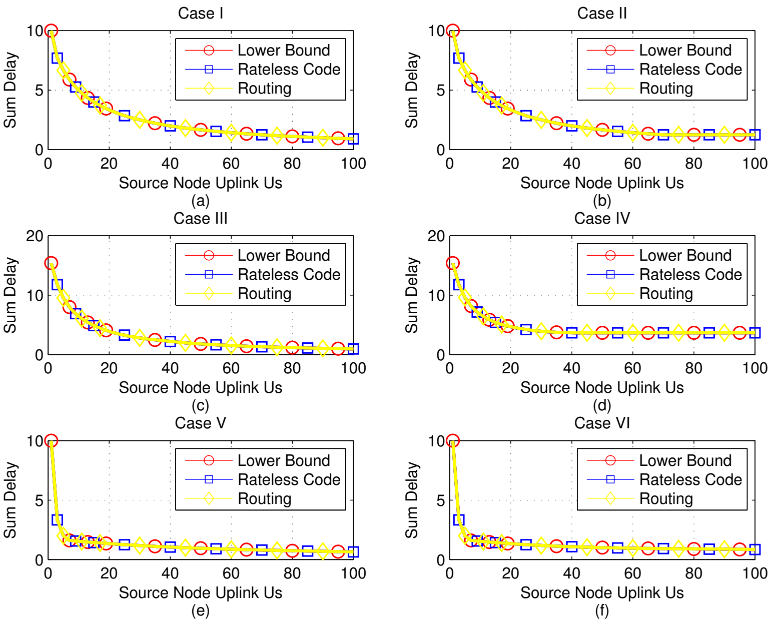


Figure 7.7: Sum download time versus U_s for small P2P networks with $N = 10$ peers.

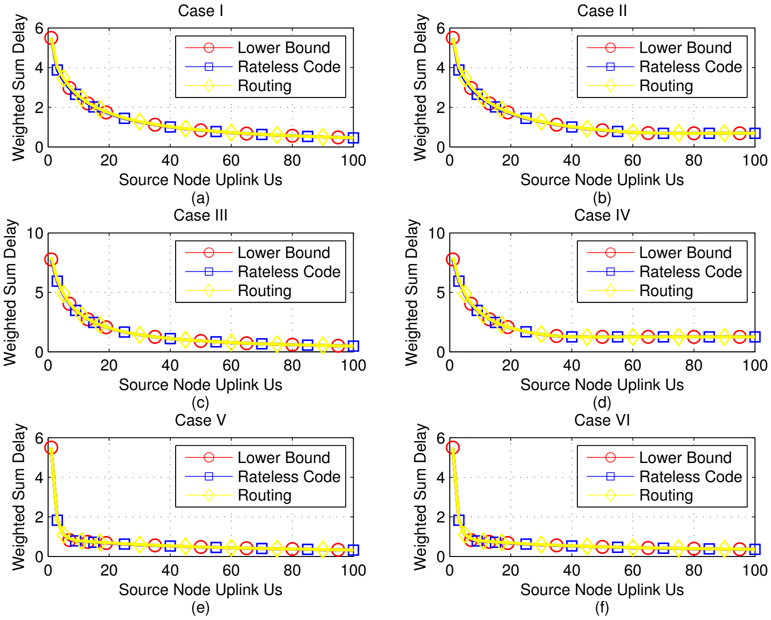


Figure 7.8: Weighted sum downloading time versus U_s for small P2P networks with $N = 10$ peers and weight $W_i = i/N$.

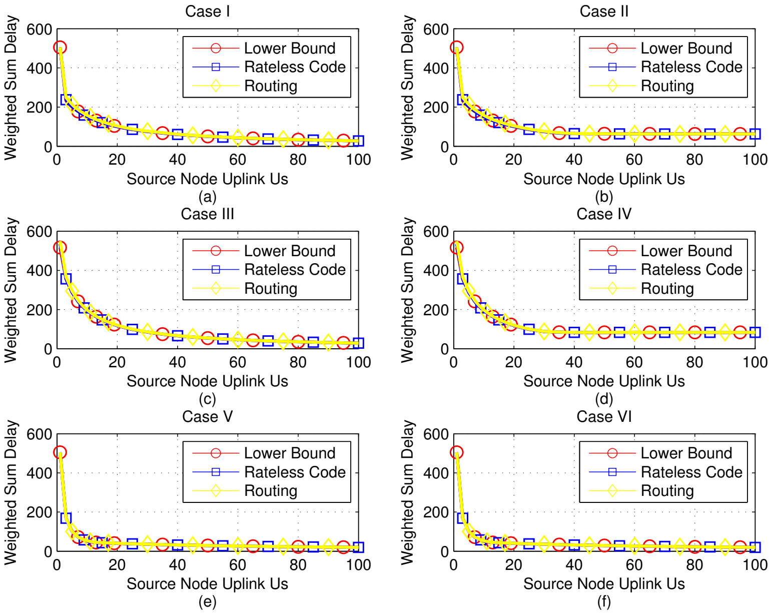


Figure 7.9: Weighted sum downloading time versus U_s for small P2P networks with $N = 10$ peers and weight $W_i = 1 + 99\delta(i > N/2)$.

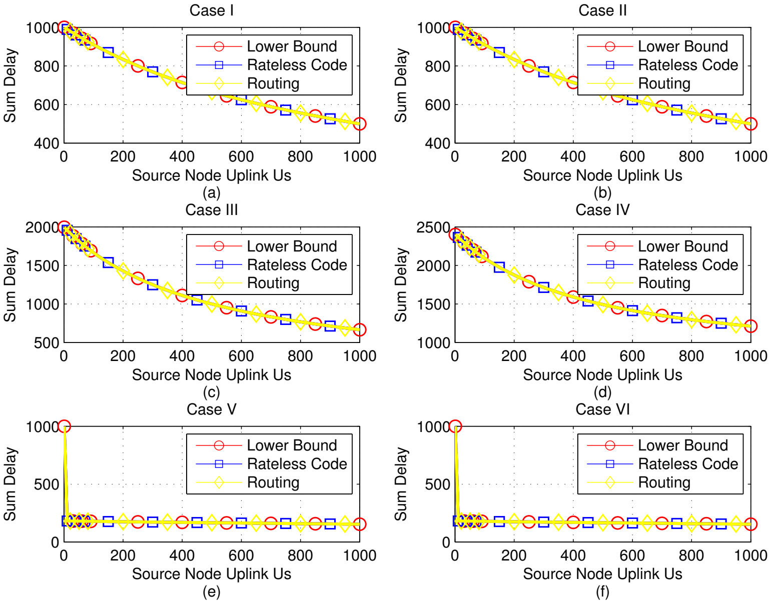


Figure 7.10: Sum download time versus U_s for large P2P networks with $N = 1000$ peers.

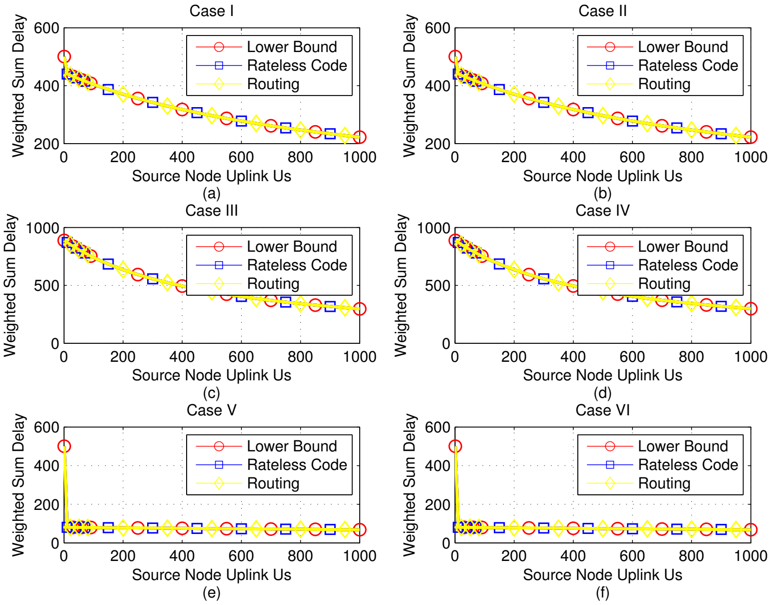


Figure 7.11: Weighted sum downloading time versus U_s for large P2P networks with $N = 1000$ peers and weight $W_i = i/N$.

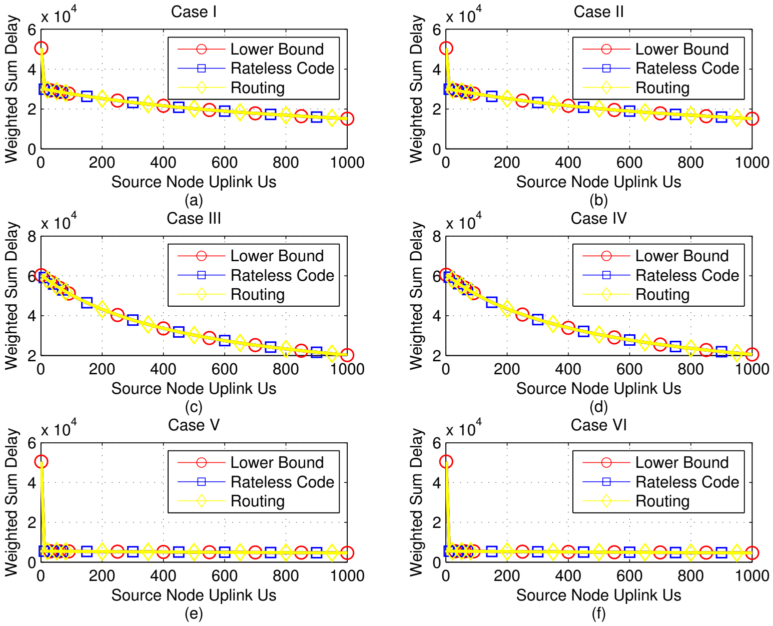


Figure 7.12: Weighted sum downloading time versus U_s for large P2P networks with $N = 1000$ peers and weight $W_i = 1 + 99\delta(i > N/2)$.

We also simulated for many other network settings and weight settings. In all these simulations, the rateless-coding-based scheme achieves or almost achieves the lower bound to the WSDT. Hence, the lower bound to the WSDT is empirically tight, and the rateless-coding-based scheme has almost-optimal empirical performance. The routing-based scheme also has near-optimal empirical performance. However, for few cases there are clear differences between the performance of the routing-based scheme and the lower bound.

7.6 The Dynamic Scenario

The dynamic scenario is allowed to re-allocate the network resource during the file transfer, in particular, whenever a peer finishes downloading, joins into the network, or leaves from the network.

7.6.1 A Piece-wise Static Approach to the General Dynamic Case

Wu et al. [28] show that to optimize WSDT the network resource allocation should be dynamic, but may remain constant during any "epoch", a period of time between when one receiver finishes downloading and another finishes downloading. Thus, one optimal solution for the dynamic scenario is "piecewise static".

As an example of how a "piecewise static" dynamic allocation can reduce the WSDT, consider the example for which we studied static allocations in Section 7.3.1. Recall that the example was for a P2P network with $U_S = 2$, $B = 1$ and three peers $\{1, 2, 3\}$ with $U_1 = U_2 = U_3 = 1$ and $D_1 = D_2 = D_3 = \infty$. Fig. 7.13 shows the time-expanded graph corresponding to the optimal dynamic rate allocation for this example. Because there are three peers, this time-expanded graph describes a file transfer scenario with 3 epochs. The first epoch lasts 0.5 unit

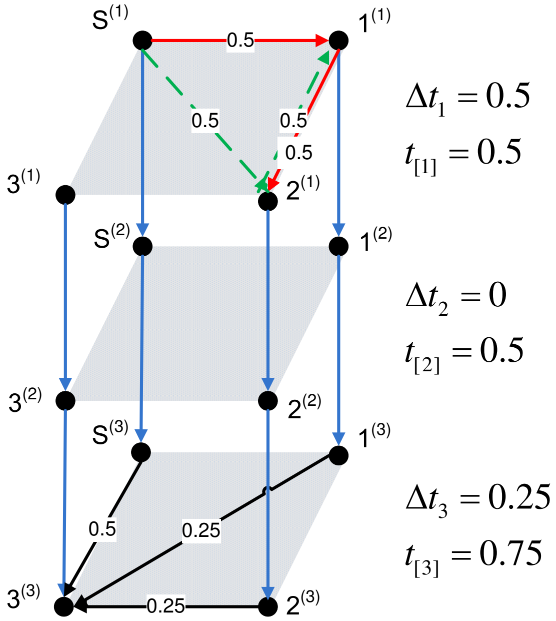


Figure 7.13: A time-expanded graph for a P2P network with three peers where $U_S = 2$, $B = 1$, $U_1 = U_2 = U_3 = 1$ and $D_1 = D_2 = D_3 = \infty$. Edges are labeled with the total information flow along the edge during the epoch. This is the product of the rate allocation along the edge during the epoch and the duration of the epoch.

time. In the first epoch, the source node sends half of the file to peer 1 and the other half to peer 2. Peer 1 and peer 2 exchange their received content, and hence, both peer 1 and peer 2 finish downloading at the same time. Hence, the second epoch lasts 0 time units (since $t_2 - t - 1 = 0$). The third epoch lasts 0.25 unit time, in which the source node, peer 1 and peer 2 transmits to peer 3 simultaneously. Peer 1 sends a quarter of the file. Peer 2 sends another quarter. The source node sends the other two quarters.

This dynamic solution turns out to achieve the minimum possible sum download time for this example which is 1.75. For comparison, the optimal static solution, which we saw in Section 7.3.1 had an only slightly larger sum download time of 1.8. This simple example shows that a dynamic rate allocation can reduce WSDT. In certain cases the benefit can be significant. Dynamic schemes can reduce the minimum sum download time to approximately half that of the static case, at least when downlink capacities are considered to be infinite [28].

7.6.2 A Rateless-coding Approach to Dynamic Allocation

Wu et al. [28] propose a dynamic routing-based scheme. This scheme first deploys all uplink resource to fully support the first K peers until they finish downloading, where K is appropriately chosen. After that, the scheme deploys all uplink resource to fully support the next peer until it finishes downloading, an so forth. Inspired by the work [28], we propose a dynamic rateless-coding-based scheme for P2P networks with both peer uplink bandwidth constraints and peer downlink bandwidth constraints. This scheme is applicable for dynamic P2P networks in which peers may even join or leave the network.

The key idea of this dynamic rateless-coding-based scheme is similar to that of the dynamic routing-based scheme in [28]. In particular, in each epoch, the scheme deploys all uplink resource to fully support several chosen peers. The details of the dynamic rateless-coding-based scheme are provided in Algorithm 6.

Algorithm 6 Dynamic Rateless-Coding-Based Scheme

```
Initiate the P2P network. Peers join into the network.
while A peer finishes downloading, joins into the network or leaves from the network do
    Select a set of peers and reset peers' weights. (The peer selection algorithm and the weight setting are addressed in Section 7.6.3)
    Apply the static rateless-coding-based scheme based on the new weights until a peer finishes downloading, joins into the network or leaves from the network.
end while
```

Algorithm 6 provides the structure of the dynamic rateless-coding-based scheme.

Because the peers always receive independently generated rateless coded chunks in the static rateless-code scheme, the dynamic rateless-coding-based scheme is also applicable for dynamic P2P network. As long as a peer receives enough rateless coded chunks [1], it can decode the whole file. The key issue is how to set the peers' weights in each epoch. Since the weight setting and the static rateless-coding-based scheme in the current epoch will influence the dynamic scheme in the following epoches, the problem of setting weights is very complicated. We will address this problem in Section 7.6.3 and show that this problem is approximately equivalent to selecting a set of peers to fully support.

7.6.3 A Solution to the Ordering Problem

Wu et al. [28] demonstrate that given an order in which the receivers finish downloading, the dynamic allocation (neglecting downlink bandwidth constraints) that minimizes WSDT can be obtained in polynomial time by convex optimization and can be achieved through linear network coding. However, [28] leaves the proper selection of the ordering as an open problem and does not address the finite downlink capacities $D_i < \infty$ or the general case of weighted sum download time which allows any values of the weights W_i.

The simulations for the static scenario in Section 7.5.5 show that the WSDT of static rateless-coding-based schemes are very close to that of the lower bound (7.27, 7.29). Hence, the flow rates r_i in (7.27) are achievable or almost achievable by the static rateless-coding-based scheme. Recall that the constraints on the rate r_i in (7.27) are

$$0 \leq r_i \leq \tilde{D}_i, \quad \forall i = 1, \cdots, N,$$

[1] The number of coded chunks needed to decode the whole file is only slightly larger than the total number of the original chunks.

and

$$\sum_{i=1}^{N} r_i \leq U_s + \sum_{i=1}^{N} U_i.$$

In the following discussion, we assume that any set of flow rates r_i $(i = 1, \cdots, N)$ satisfying the above constraints is achievable by the static rateless-coding-based scheme.

Consider one epoch of the dynamic rateless-coding-based scheme. Suppose there are N peers in the network in the current epoch. Peer i $(i = 1, \cdots, N)$ has uplink capacity U_i, downlink capacity D_i and $B - q_i B$ received rateless-coded chunks. Suppose the static rateless-coding-based scheme supports peer i with flow rate r_i $(i = 1, \cdots, N)$ based on a weight setting. In order to find the optimal weight setting for the current epoch, we study the necessary conditions for the flow rates r_i $(i = 1, \cdot, N)$ to be optimal.

Let us first focus on two peers in the network, say peer 1 and peer 2. The total amount of the uplink resource supporting peer 1 and peer 2 is $s = r_1 + r_2$. If the flow rates r_i for $i = 1, \cdots, N$ is optimal, then the flow rates r_1 and r_2 are also the optimal resource allocation for peers 1 and 2 given that the flow rates r_i for $i = 3, \cdots, N$ are fixed. Now consider a suboptimal scenario in which the uplink resource with the amount of s serves peers 1 and 2, and the rest of the uplink serves other peers in all of the following epoches. This suboptimal scenario provides a WSDT close to the minimum WSDT if $s \ll U_s + \sum_{i=1}^{N} U_i$ (this is true for large N). Hence, we consider this suboptimal scenario and address the necessary conditions for r_1 and r_2 to be the optimal resource allocation for peers 1 and 2.

If $\frac{q_1 B}{r_1} \leq \frac{q_2 B}{r_2}$, then peer 1 finishes downloading before peer 2 does. After peer 1 finishes downloading, peer 1 acts as a source node and hence the total amount of the source nodes' uplink is $U_s + U_1$, and peer 2 is supported by the uplink resource with the amount of s. Hence, the WSDT for peers 1 and 2 is

$$\Delta_1 = W_1 \frac{q_1 B}{r_1} + W_2 (\frac{q_1 B}{r_1} + \frac{q_2 B - \frac{q_1 B}{r_1} r_2}{\min(s, D_2, U_s + U_1)}), \tag{7.89}$$

and

$$\frac{\Delta_1}{r_1} = \frac{q_1 B}{r_1^2} (-W_1 - W_2 + \frac{sW_2}{\min(s, D_2, U_s + U_1)}). \tag{7.90}$$

Note that the sign of $\frac{\Delta_1}{r_1}$ does not depend on r_1. Hence, the optimal solution to r_1 is either $r_1 = r_2 q_1 / q_2$ (peer 1 and peer 2 finish at the same time) if $-W_1 - W_2 + \frac{sW_2}{\min(s, D_2, U_s + U_1)} \geq 0$, or $r_1 = \min(s, \tilde{D}_1)$ (peer 1 is fully supported) if $-W_1 - W_2 + \frac{sW_2}{\min(s, D_2, U_s + U_1)} < 0$. Similarly, if $\frac{q_1 B}{r_1} \geq \frac{q_2 B}{r_2}$, then peer 2 finishes downloading before peer 1 does. The WSDT for peers 1 and 2 is

$$\Delta_2 = W_2 \frac{q_2 B}{r_2} + W_1 (\frac{q_2 B}{r_2} + \frac{q_1 B - \frac{q_2 B}{r_2} r_1}{\min(s, D_1, U_s + U_2)}), \tag{7.91}$$

and

$$\frac{\Delta_2}{r_2} = \frac{q_2 B}{r_2^2} (-W_2 - W_1 + \frac{sW_1}{\min(s, D_1, U_s + U_2)}). \tag{7.92}$$

Note that the sign of $\frac{\Delta_2}{r_2}$ does not depend on r_2 eithter. Hence, the optimal solution to r_2 is either $r_2 = r_1 q_2 / q_1$ (peer 1 and peer 2 finish at the same time) if $-W_2 - W_1 + \frac{sW_1}{\min(s, D_1, U_s + U_2)} \geq 0$, or $r_2 = \min(s, \tilde{D}_2)$ (peer 2 is fully supported) if $-W_2 - W_1 + \frac{sW_1}{\min(s, D_1, U_s + U_2)} < 0$. Therefore, the optimal resource allocation for peer 1 and peer 2 is achieved when one of the peers is fully supported, or they finish at the same time.

Lemma 4. *Given that the flow rates to peer i for $i = 3, \cdots, N$ are fixed, and the amount of uplink resource supporting peer 1 and peer 2 is s. If the optimal resource allocation for peer 1 and peer 2 is achieved when they finish at the same time, then both peer 1 and peer 2 are fully supported.*

Proof. Let $\tilde{D}_1^+ = \min(s, D_1, U_s + U_2)$ and $\tilde{D}_2^+ = \min(s, D_2, U_s + U_1)$. According to the above discussion, the optimal resource allocation for peer 1 and peer 2 is achieved when they finish at the same time if and only if $s \geq \tilde{D}_1 + \tilde{D}_2$, or $\frac{\Delta_1}{r_1} \geq 0$ and $\frac{\Delta_2}{r_2} \geq 0$.

If $s \geq \tilde{D}_1 + \tilde{D}_2$, then $r_1 = \tilde{D}_1$, $r_2 = \tilde{D}_2$, and hence, peers 1 and 2 are fully supported.

If $\frac{\Delta_1}{r_1} \geq 0$ and $\frac{\Delta_2}{r_2} \geq 0$, then

$$-W_1 - W_2 + \frac{sW_2}{\tilde{D}_2^+} \geq 0,$$

and

$$-W_2 - W_1 + \frac{sW_1}{\tilde{D}_1^+} \geq 0$$

. Hence, $0 \leq W_1 \leq \frac{s-\tilde{D}_2^+}{\tilde{D}_2^+} W_2$ and $0 \leq W_2 \leq \frac{s-\tilde{D}_1^+}{\tilde{D}_1^+} W_1$. Multiply the above two inequalities and obtain

$$s \geq \tilde{D}_1^+ + \tilde{D}_2^+ \geq \tilde{D}_1 + \tilde{D}_2.$$

Therefor, peer 1 and peer 2 are also fully supported. □

Corollary 2. *Given that the flow rates to peer i for $i = 3, \cdots, N$ are fixed, and the amount of uplink resource supporting peer 1 and peer 2 is s. The optimal resource allocation for peer 1 and peer 2 is achieved when one of them is fully supported or both of them are fully supported.*

Corollary 3. *The optimal network resource allocation in each epoch of a dynamic scenario is only obtained when some peers are fully supported, one or zero peer is partly supported, and the other peers are not supported.*

Proof. (**proof by contradiction**) If two peers are partly supported, say peer 1 and peer 2 are partly supported, then the resource allocation for peer 1 and peer 2 is not optimal by Corollary 2. □

By Corollary 3, the optimal weight setting in each epoch is $W = 1$ for the fully supported peers, $0 \leq W \leq 1$ for the partly supported peer, and $W = 0$ for other peers. Hence, the problem of optimizing the weight setting is approximately equivalent to selecting a set of peers to fully support.

Now study the necessary conditions for a peer selection to be optimal in a similar way. Suppose that the amount of uplink resource supporting peer 1 and peer 2 is s, and the flow rates to peer i for $i = 3, \cdots, N$ are fixed.
If $s < \frac{q_1+q_2}{q_1}\tilde{D}_1$ and $s < \frac{q_1+q_2}{q_2}\tilde{D}_2$, then peer 1 finishes downloading if peer 1 is fully supported, or peer 2 finishes downloading if peer 2 is fully supported. When peer 1 is fully supported, the WSDT for peer 1 and peer 2 is Δ_1 in (7.89) with $r_1 = \tilde{D}_1$. When peer 2 is fully supported, the WSDT for these two peers is Δ_2 in (7.91) with $r_2 = \tilde{D}_2$. Hence, we have

$$\begin{aligned}
\Delta_1 - \Delta_2 = {} & W_1\frac{q_1 B}{\tilde{D}_1} + W_2\left(\frac{q_1 B}{\tilde{D}_1} + \frac{q_2 B - \frac{q_1 B}{\tilde{D}_1} r_2}{\min(s, D_2, U_s + U_1)}\right) \\
& - \left(W_2\frac{q_2 B}{\tilde{D}_2} + W_1\left(\frac{q_2 B}{\tilde{D}_2} + \frac{q_1 B - \frac{q_2 B}{\tilde{D}_2} r_1}{\min(s, D_1, U_s + U_2)}\right)\right) \qquad (7.93) \\
= {} & q_1 B W_1\left(\frac{1}{\tilde{D}_1} - \frac{1}{\tilde{D}_1^+}\right) - q_2 B W_2\left(\frac{1}{\tilde{D}_2} - \frac{1}{\tilde{D}_2^+}\right) \\
& + q_1 B W_2\left(\frac{1}{\tilde{D}_2^+} - \frac{1}{\tilde{D}_2}\right)\left(1 - \frac{s}{\tilde{D}_1}\right) \\
& - q_2 B W_1\left(\frac{1}{\tilde{D}_1^+} - \frac{1}{\tilde{D}_1}\right)\left(1 - \frac{s}{\tilde{D}_1}\right) \\
& + (q_1 B W_2 - q_2 B W_1)\left(\frac{1}{\tilde{D}_1} + \frac{1}{\tilde{D}_2} - \frac{s}{\tilde{D}_1 \tilde{D}_2}\right) \qquad (7.94) \\
\approx {} & \left(\frac{W_2}{q_2} - \frac{W_1}{q_1}\right)\frac{q_1 q_2 B(\tilde{D}_1 + \tilde{D}_2 - s)}{\tilde{D}_1 \tilde{D}_2}. \qquad (7.95)
\end{aligned}$$

Therefore, it is better to first fully support peer 1 if $\frac{W_2}{q_2} < \frac{W_1}{q_1}$ when $s < \frac{q_1+q_2}{q_1}\tilde{D}_1$ and $s < \frac{q_1+q_2}{q_2}\tilde{D}_2$.

If $\frac{q_1}{\tilde{D}_1} > \frac{q_2}{\tilde{D}_2}$ and $\frac{q_1+q_2}{q_1}\tilde{D}_1 < s < \frac{q_1+q_2}{q_2}\tilde{D}_2$, then peer 2 always finishes downloading before peer 1 does. In this case, it is better to first fully support peer 1 if $\frac{\Delta_2}{r_2} > 0$, i.e.,

$$\frac{W_1}{W_2} > \frac{\tilde{D}_1^+}{s - \tilde{D}_1^+},$$

or approximately

$$\frac{W_1}{W_2} > \frac{\tilde{D}_1}{s - \tilde{D}_1}.$$

If $\frac{q_1}{\tilde{D}_1} < \frac{q_2}{\tilde{D}_2}$ and $\frac{q_1+q_2}{q_2}\tilde{D}_2 < s < \frac{q_1+q_2}{q_1}\tilde{D}_1$, then peer 1 always finishes downloading before peer 2 does. In this case, it is better to first fully support peer 1 if $\frac{\Delta_1}{r_1} < 0$, i.e.,

$$\frac{W_1}{W_2} > \frac{\tilde{D}_2^+}{s - \tilde{D}_2^+},$$

or approximately

$$\frac{W_1}{W_2} > \frac{\tilde{D}_2}{s - \tilde{D}_2}.$$

These discussions are concluded in the following theorem.

Theorem 4. *Given that the amount of uplink resource supporting peer i and peer j is s, and the flow rates to peer k for $k \neq i, j$ are fixed. The optimal resource allocation for peer i and peer j is to fully support peer i (i.e., $r_i = \tilde{D}_i$) if*

$$\frac{W_i}{W_j} > \begin{cases} \max(\frac{q_i}{q_j}, \frac{s-\tilde{D}_j}{\tilde{D}_j}) & \textit{when } \frac{q_i}{\tilde{D}_i} < \frac{q_j}{\tilde{D}_j}, \\ \frac{1}{\max(\frac{q_j}{q_i}, \frac{s-\tilde{D}_i}{\tilde{D}_i})} & \textit{when } \frac{q_i}{\tilde{D}_i} > \frac{q_j}{\tilde{D}_j}. \end{cases} \tag{7.96}$$

Corollary 4. *Consider a peer selection for a dynamic scenario which select peer* *i to fully support and peer j to not support. This peer selection is optimal only if*

$$\frac{W_i}{W_j} > \begin{cases} \max(\frac{q_i}{q_j}, \frac{\tilde{D}_i - \tilde{D}_j}{\tilde{D}_j}) & when\ \frac{q_i}{\tilde{D}_i} < \frac{q_j}{\tilde{D}_j}, \\ \frac{q_i}{q_j} & when\ \frac{q_i}{\tilde{D}_i} > \frac{q_j}{\tilde{D}_j}. \end{cases} \tag{7.97}$$

Proof. When peer i is fully supported and peer j is not supported, $s = r_i + r_j = \tilde{D}_i$. Plugging $s = \tilde{D}_i$ into (7.96) and obtain (7.97). □

Define the binary relation $\succ$ on $\{1, \cdots, N\}$ as $i \succ j$ if (7.97) is satisfied. Denote a peer selection as (I, J) where I is the set of fully supported peers and J is the set of unsupported peers. (I, J) is optimal only if $i \succ j$ for any $i \in I$ and $j \in J$. For general P2P networks, finding the optimal (I, J) is computational impossible because the binary relation $\succ$ is not transitive, which means

$$i \succ j; j \succ k \nRightarrow i \succ k.$$

Define the binary relation $\gtrapprox$ on $\{1, \cdots, N\}$ as $i \gtrapprox j$ if $\frac{W_i}{q_i} \geq \frac{W_j}{q_j}$. The binary relation $\gtrapprox$ is an approximation to the binary relation $\succ$. $i \gtrapprox j$ is equivalent to $i \succ j$ when

$$\frac{q_i}{q_j} > \frac{\tilde{D}_i - \tilde{D}_j}{\tilde{D}_j}. \tag{7.98}$$

It can be seen by plugging (7.98) into (7.97). The approximated binary relation $\gtrapprox$ has the transitive property, and hence, the peers can be ordered with respect to $\gtrapprox$. Based on this ordering, a suboptimal peer selection algorithm and the corresponding weight setting is constructed as shown in Algorithm 7.

Algorithm 7 Peer Selection and Weight Setting

```
Suppose $N$ peers are downloading in the current epoch.
Let $B - q_iB$ $(0 < q_i \leq 1)$be the number of chunks that peer $i$ has received for $i = 1, \cdots, N$.
Sort $\{\frac{W_i}{q_i}\}_{i=1}^{N}$ in descending order and get $(k_1, \cdots, k_N)$.
Find the smallest $M$ such that $\sum_{i=1}^{M} \tilde{D}_{k_i} \geq U_s + \sum_{i=1}^{N} U_i$.
Select peers $\{k_i\}_{i=1}^{M}$ to fully support.
Set $W_j = 1$ if $j \in \{k_i\}_{i=1}^{M}$, or $W_j = 0$ otherwise.
```

7.7 Simulations of the Dynamic Scenario

The dynamic rateless-coding-based scheme is feasible to both static P2P networks and dynamic P2P networks. Consider a type of dynamic P2P networks which any peer leaves from as it finishes downloading, and no peer joins into. This section provides the empirical WSDT performances of the dynamic rateless-coding-based scheme for static P2P networks and dynamic P2P networks with peer leaving, and compares them with those of the the static scenario for static P2P networks. In all simulations, the file size B is normalized to be 1. This section shows simulations for Cases I,II,IV, and VI investigated in 7.5.5.

Consider median-size P2P networks with $N = 100$ peers. The performances of sum download time versus U_s for the 4 cases are shown in Fig. 7.14. Fig. 7.15 shows the relative value of the sum download time by normalizing the lower bound to be 1 in order to explicitly compare the performances of the dynamic rateless-coding-based scheme and the static scenario. For Case I where peers have infinite downlink capacities, the sum download time of the dynamic rateless-coding-based scheme is almost half of the minimum sum download time for the static scenario for a broad range of the source node uplink U_s. This result matches the results in the previous work [28], which says that the minimum sum download time of dynamic scenarios is almost half of the minimum sum download time of

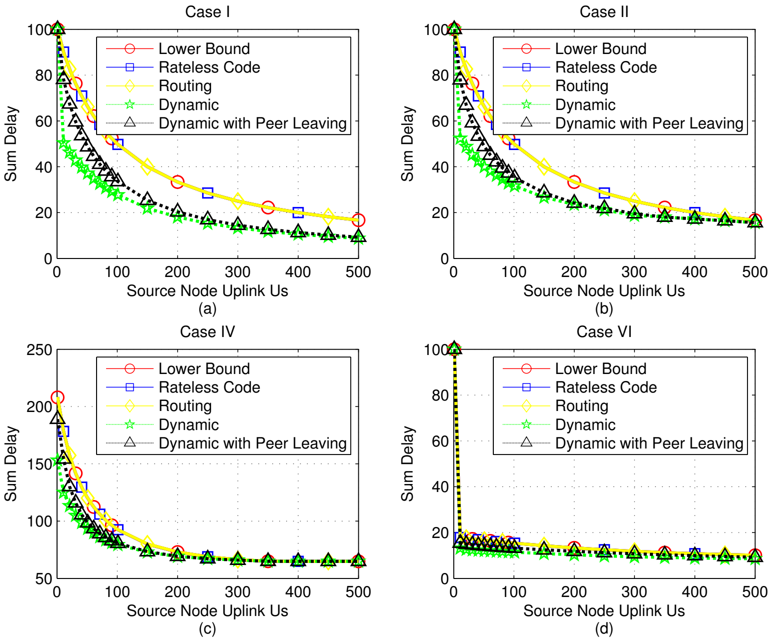


Figure 7.14: Sum download time versus U_s for large P2P networks with $N = 100$ peers.

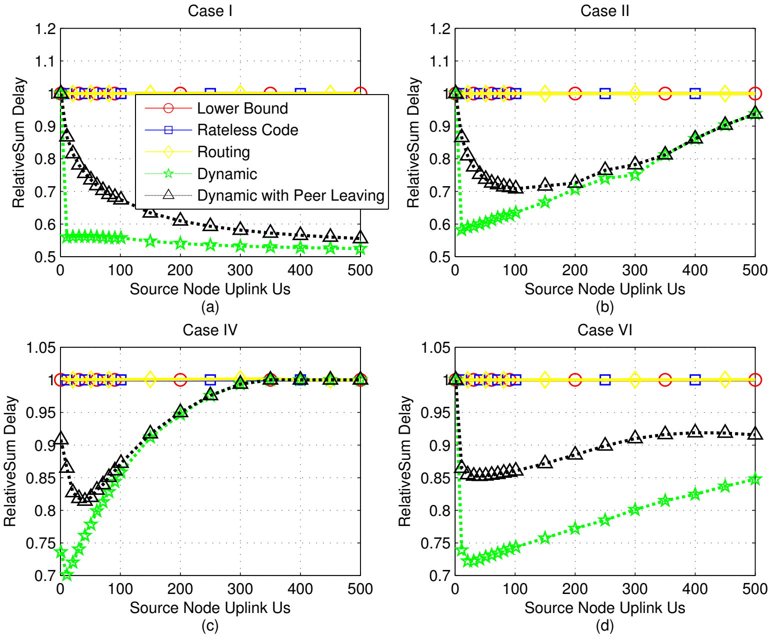


Figure 7.15: Relative sum download time versus U_s for large P2P networks with $N = 100$ peers.

static scenarios when node uplinks are the only bottleneck in the network. Our results also show that the sum download time of the dynamic rateless-coding-based scheme with peer leaving decreases to almost half of the minimum sum download time for the static scenario as U_s increases. For Cases II, IV, and VI, the WSDs of the dynamic scheme and the dynamic scheme with peer leaving are also always smaller than the minimum WSDT for the static scenario. In particular, the WSDT of the dynamic scheme can be as small as 0.59, 0.70, and 0.73 of the minimum WSDT for the static scenario for Cases II, IV and VI, respectively. The WSDT of the dynamic scheme with peer leaving can be as small as 0.71, 0.82, and 0.86 of the minimum WSDT for static scenarios for Cases II, IV and VI, respectively. These largest improvements in percentage of deploying the dynamic scheme is obtained when the source node can directly support tens of the peers.

The performances of WSDT versus U_s with weight $W_i = i/N$ $(i = 1, \cdots, N)$ are shown in Fig. 7.16. Fig. 7.17 shows the relative value of the WSDT. For Case I, the sum download times of the dynamic rateless-coding-based scheme and the dynamic scheme with peer leaving can be even less than half of the minimum sum download time for the static scenario for a broad range of the source node uplink U_s. This is because the peers with largest weight finish downloading first in the dynamic scheme. The WSDT of the dynamic scheme can be as small as 0.48, 0.49, and 0.58 of the minimum WSDT for the static scenario for Cases II, IV and VI, respectively. The WSDT of the dynamic scheme with peer leaving can be as small as 0.56, 0.62, and 0.77 of the minimum WSDT for the static scenario for Cases II, IV and VI, respectively. Note that for Case VI, the WSDT of the dynamic scheme with peer leaving is larger than that of the static scenario for small U_s. This is because the peers with larger uplink resource also have larger weight, and they finish downloading and leave from the network first.

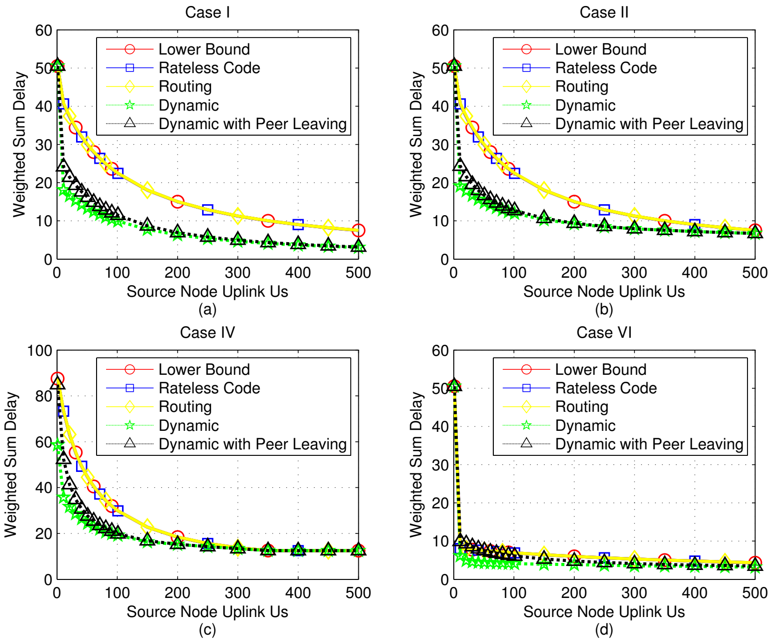


Figure 7.16: Weighted sum downloading time versus U_s for large P2P networks with $N = 100$ peers and weight $W_i = i/N$.

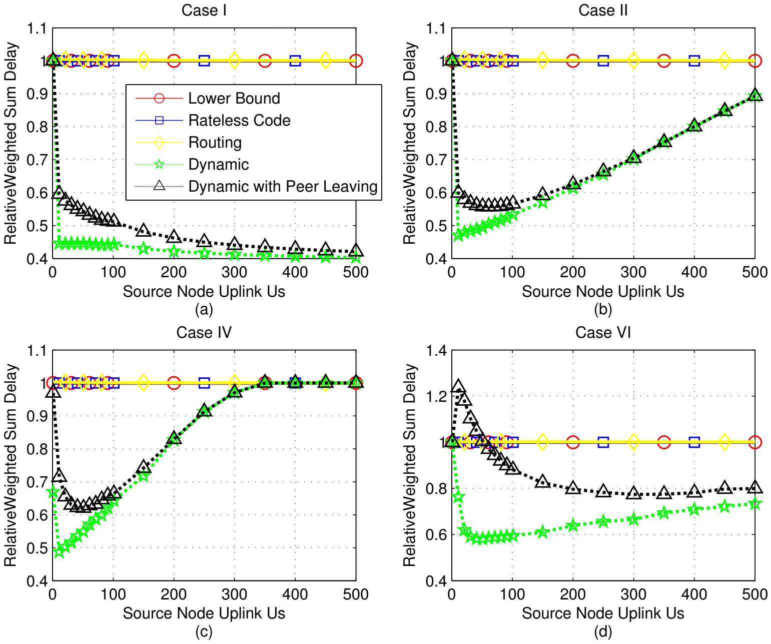


Figure 7.17: Relative weighted sum downloading time versus U_s for large P2P networks with $N = 100$ peers and weight $W_i = i/N$.

The performances of WSDT versus U_s with weight $W_i = 1 + 99\delta(i > N/2)$ $(i = 1, \cdots, N)$ are shown in Fig. 7.18. Fig. 7.19 shows the relative value of the WSDT. For Case I, the sum download times of the dynamic rateless-coding-based scheme and the dynamic scheme with peer leaving is around half of the minimum sum download time for the static scenario for a broad range of the source node uplink U_s. The WSDT of the dynamic scheme can be as small as 0.58, 0.55, and 0.52 of the minimum WSDT for static scenarios for Cases II, IV and VI, respectively. The WSDT of the dynamic scheme with peer leaving can be as small as 0.64, 0.64, and 0.63 of the minimum WSDT for the static scenario for Cases II, IV and VI, respectively. Note that for this weight setting, the WSDT of the dynamic scheme with peer leaving is always smaller than that of the static scenario for Case VI. This is because the gain by finishing peers with larger weight is more than than the loss by the peers with larger uplink resource leaving from the network.

Consider large P2P networks with $N = 1000$ peers. The performances of sum download time versus U_s for the 4 cases are shown in Fig. 7.14. Fig. 7.15 shows the relative value of the sum download time. For Case I, the sum download time of the dynamic rateless-coding-based scheme is around 0.55 of the minimum sum download time for the static scenario for a broad range of the source node uplink U_s. The sum download time of the dynamic rateless-coding-based scheme with peer leaving decreases to 0.70 of the minimum sum download time for the static scenario as U_s increases to 1000. The WSDT of the dynamic scheme can be as small as 0.57, 0.70, and 0.70 of the minimum WSDT for the static scenario for Cases II, IV and VI, respectively.

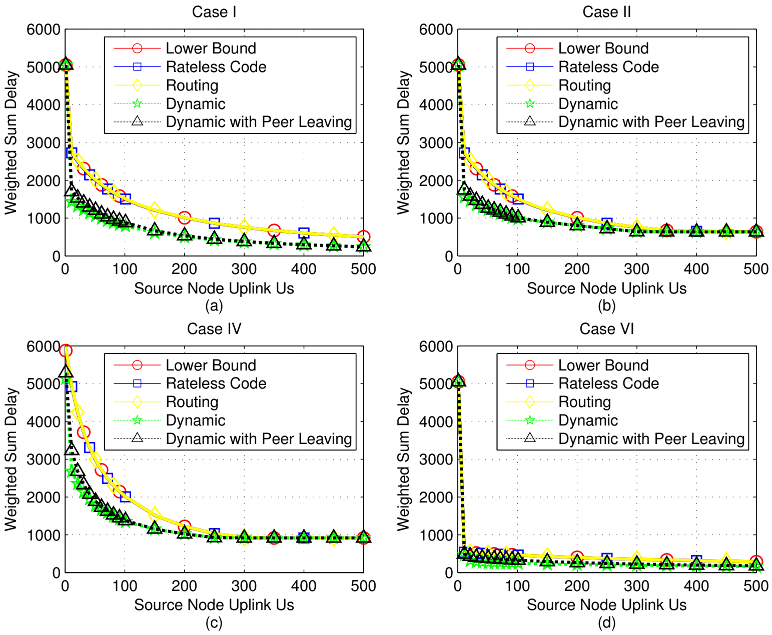


Figure 7.18: Weighted sum downloading time versus U_s for large P2P networks with $N = 100$ peers and weight $W_i = 1 + 99\delta(i > N/2)$.

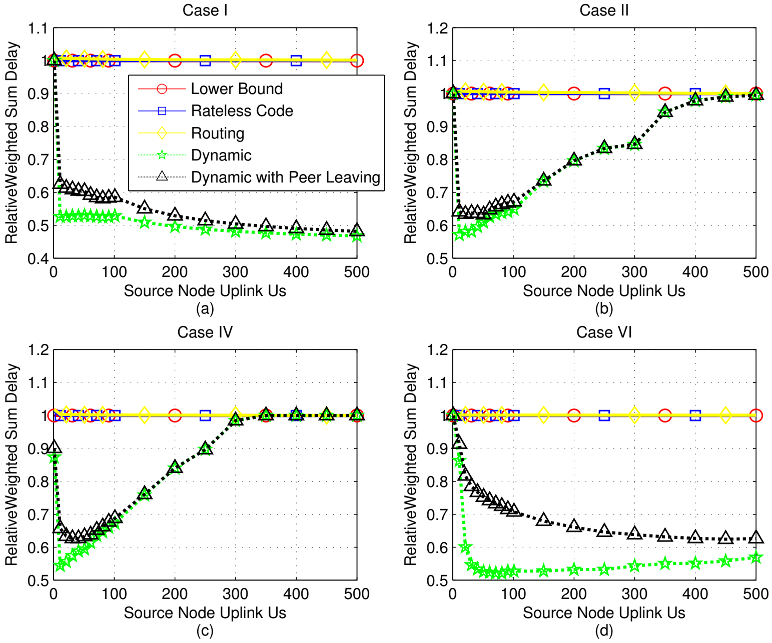


Figure 7.19: Relative weighted sum downloading time versus U_s for large P2P networks with $N = 100$ peers and weight $W_i = 1 + 99\delta(i > N/2)$.

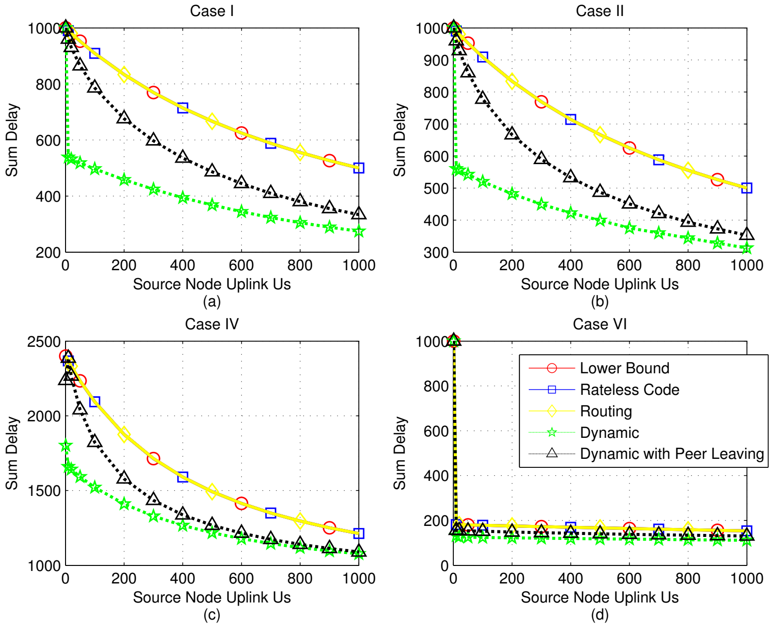


Figure 7.20: Sum download time versus U_s for large P2P networks with $N = 1000$ peers.

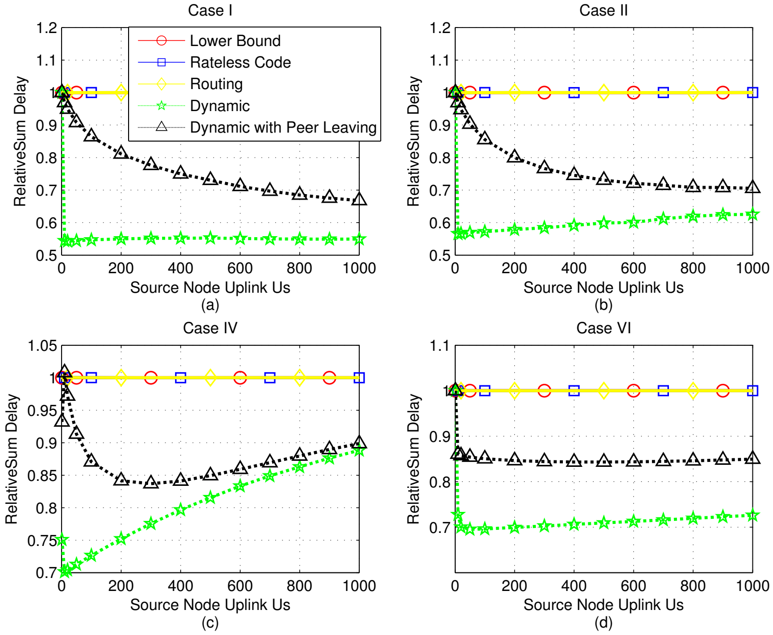


Figure 7.21: Relative sum download time versus U_s for large P2P networks with $N = 1000$ peers.

7.8 Summary

This chapter considers the problem of transferring a file from one server to multiple receivers in a P2P network with both peer uplink bandwidth constraints and peer downlink bandwidth constraints. This chapter shows that the static scenario can be optimized in polynomial time by convex optimization, and the associated optimal static WSDT can be achieved by linear network coding. Furthermore, this chapter proposes static routing-based and rateless-coding-based schemes that closely approach a new lower bound on performance derived in this chapter.

This chapter also proposes a dynamic rateless-coding-based scheme, which provides significantly smaller WSDT than the optimal static scheme does. A key contribution for the dynamic scenario is a practical solution to the ordering problem left open by Wu. Our solution is to recast this problem as the problem of identifying the peer weights for each epoch of the "piecewise static" rate allocation.

The deployment of rateless codes simplifies the mechanism of the file-transfer scenario, enhances the robustness to packet loss in the network, and increases the performance (without considering packet overhead). However, there still exist several issues for rateless-coding-based scheme such as high source node encoding complexity, packet overhead, and fast peer selection algorithm for the dynamic scenario. The results of this chapter open interesting problems in applying rateless codes for P2P applications.

The optimal delay region (set of optimal download times) for one-to-many file transfer in a P2P network can be characterized by a system of linear inequalities. Hence, minimizing the WSDT for all sets of peer weights leads to the delay region.

The set of peer weights can also be assigned according to the applications. For instances, for a file transfer application with multiple classes of users, assign a weight to each class of users. For an application with both receivers and helpers, assign weight zero to helpers and positive weights to receivers. Hence, the results of this chapter in fact apply directly to one-to-many file transfer applications both with and without helpers.

CHAPTER 8

Conclusion

8.1 Thesis Summary

Chapter 2-6 explore relatively simple optimal encoders for the degraded broadcast channel. Chapter 7 investigates the optimal resource allocation for content distribution in peer-to-peer networks.

Chapter 2 defines and explores the conditional entropy bound F^* for discrete DBCs. $F^*(\boldsymbol{q}, s)$ is the infimum of $H(Z|U)$ with respect to all auxiliary random variables U given that the input-signal distribution is $\boldsymbol{q}$ and $H(Y|U) = s$. Two main theorems regarding to F^* were established to show the relationship among F^*, the capacity region, and optimal encoding schemes for DBCs. The first main theorem represents the capacity region for discrete DBCs with F^*, which bring us a more insight view of the capacity region for DBCs. We apply this theorem in Chapter 2 to prove the optimal input-signal distribution for input-symmetric DBCs. The second main theorem establishes the relationship between the evaluation of F^* and the optimal encoding schemes for the DBC. We later apply this theorem in Chapter 3-5 to prove the optimality of NE scheme for multi-user broadcast Z channels and discrete multiplicative DBCs.

Chapter 3 applies the results of the conditional entropy bound F^* to prove that the NE scheme achieves the whole boundary of the capacity region of multi-user DBCs. As an example of the application of F^*, Chapter 3 shows the power of this conditional entropy bound for DBCs.

The input-symmetric DBC is a class of discrete DBCs, which contains most commonly studied DBCs including broadcast binary-symmetric channels, broadcast binary-erasure channels, and group-additive DBCs. By extending the input-symmetry and $F(\cdot)$ ideas of Wyner and Witsenhausen, Chapter 4 defines the input symmetry for DBCs and introduces the permutation encoding scheme which employs permutation functions of independently encoded streams for the input-symmetric DBC. We apply the results regarding to F^* in Chapter 2 to prove that the uniform input distribution is optimal for IS-DBCs and then the permutation encoding scheme achieves the whole capacity region for IS-DBCs. As a consequence, the NE scheme (also the permuatation encoding scheme) for group-additive DBCs achieves the whole capacity region.

Chapter 5 combines the results of Chapter 3, Chapter 4, and the results of the conditional entropy bound to prove that the NE scheme achieves the whole boundary of the capacity region for discrete multiplicative DBC.

Chapter 6 proves that the NE scheme achieves the whole boundary of the capacity region for two-user broadcast Z channels without applying results of the conditional entropy bound F^*. In particular, the NE scheme for two-user broadcast Z channels is to independently encode the message corresponding to each user and transmit the binary OR of the encoded signals. Chapter 6 also establishes an explicit expression of the capacity region for two-user broadcast Z channels, and provides the distributions of the outputs of each encoder that achieve the optimal boundary. Nonlinear-turbo codes that provide a controlled distribution of ones and zeros in their codewords were used to demonstrate a low-complexity scheme that works close to the optimal boundary.

In conclusion, natural encoding achieves the capacity region of DBCs much more often that has been previously known. In fact, it would seem that there are more such cases where natural encoding achieves the DBC capacity region waiting to be identified. It remains an open problem to prove a general theorem establishing the optimality of natural encoding over a suitably large class of DBCs. The results of this chapter also open interesting problems in channel coding to find practical channel codes for the DBCs examined in this chapter.

Chapter 7 considers the problem of transferring a file from one server to multiple receivers in a P2P network in which node uplinks and downlinks are the only bottleneck. Chapter 7 shows that the static scenario can be optimized in polynomial time by convex optimization, and the associated optimal static WSDT can be achieved by linear network coding. We also propose a static routing-based scheme and a static rateless-coding-based scheme that have almost-optimal empirical performance. Chapter 7 also provides a practical solution for the ordering problem in dynamic rate allocation and proposes a dynamic rateless-coding-based scheme, which provides significantly smaller WSDT than the optimal static scheme does.

The deployment of rateless codes simplifies the mechanism of the file-transfer scenario, enhances the robustness to packet loss in the network, and increases the performance (without considering packet overhead). However, there still exist several issues for rateless-coding-based scheme such as high source node's encoding complexity, packet overhead, and fast peer selection algorithm for the dynamic scenario. The results of Chapter 7 open interesting problems in applying rateless codes to P2P applications.

APPENDIX A

Appendices

A.1 Appendix I: Independent Encoding Scheme for Degraded Broadcast Channels

The appendix presents a simple independent encoding scheme made known to us by Telatar [5] which achieves the capacity region for DBCs. The scheme generalizes to any number of receivers, but showing the two-user case suffices to explain the approach. It indicates that any achievable rate pair (R_1, R_2) for a DBC can be achieved by combining symbols from independent encoders with a single-letter function. The independent encoders operate using two codebooks $\{v^n(i) : i = 1, \cdots, 2^{nR_1}\}$, $\{u^n(j) : j = 1, \cdots, 2^{nR_2}\}$ and a single-letter function $f(v, u)$. In order to transmit the message pair (i, j), the transmitter sends the sequence $f(v_1(i), u_1(j)), \cdots, f(v_n(i), u_n(j))$. The scheme is described below:

Lemma 13. *Suppose U and X are discrete random variables with joint distribution p_{UX}. There exist V independent of U and a deterministic function f such that the pair $(U, f(V, U))$ has joint distribution p_{UX}. [5]*

Proof: Suppose U and X take values in $\{1, \cdots, l\}$ and $\{1, \cdots, k\}$ respectively. Let $V = (V_1, \cdots, V_l)$, independent of U, be a random variable taking values in $\{1, \cdots, k\}^l$ with $\Pr(V_j = i) = p_{X|U}(i|j)$. Set $f((v_1, \cdots, v_l), u) = v_u$. Then we have

$$\begin{aligned}\Pr(U=u, f(V,U)=x) &= \Pr(U=u, V_u=x)\\ &= \Pr(U=u)Pr(V_u=x)\\ &= p_U(u)p_{X|U}(x|u)\\ &= p_{UX}(u,x). \qquad \text{(A.1)}\end{aligned}$$

Q.E.D.

If the rate pair (R_1, R_2) is achievable for a degraded broadcast channel $X \to Y \to Z$, there exists an auxiliary random variable U such that

$$\begin{aligned}&\text{(a) } U \to X \to Y \to Z;\\ &\text{(b) } I(X;Y|U) \geq R_1;\\ &\text{(c) } I(U;Z) \geq R_2. \qquad \text{(A.2)}\end{aligned}$$

Use Lemma 13 to find V independent of U and the deterministic function $f(v,u)$ such that the pair $(U, f(V,U))$ has the same joint distribution as that of (U,X). Randomly and independently choose codewords $\left\{v^n(1), \cdots, v^n(2^{nR_1})\right\}$ according to $p(v^n) = p_V(v_1)\cdots, p_V(v_n)$, and choose codewords $\left\{u^n(1), \cdots, u^n(2^{nR_2})\right\}$ according to $p(u^n) = p_U(u_1)\cdots, p_U(u_n)$. To send message pair (i,j), the encoder transmits $f(v_1(i), u_1(j)), \cdots, f(v_n(i), u_n(j))$.

Using a typical-set-decoding random-coding argument, the weak decoder, given z^n, searches for the unique j' such that $(z^n, u^n(j'))$ is jointly typical. The error probability converges to zero as n goes to infinity since $R_2 \leq I(U;Z)$. The strong decoder, given y^n, also searches for the unique j' such that $(y^n, u^n(j'))$ is jointly typical, and then searches for the unique i' such that $(y^n, v^n(i'))$ is jointly typical given $u^n(j')$. The error probability converges to zero as n goes to infinity since

$$R_2 \leq I(U;Z) \leq I(U;Y), \tag{A.3}$$

and

$$\begin{aligned} R_1 &\leq I(X;Y|U) \\ &= H(Y|U) - H(Y|f(V,U),U) \\ &\leq H(Y|U) - H(Y|f(V,U),U,V) \\ &= H(Y|U) - H(Y|U,V) \\ &= I(V;Y|U). \end{aligned} \tag{A.4}$$

A.2 Appendix II: Proof of Lemma 2

Proof of Lemma 2: Part i) is a consequence of Lemma 1 by applying the Fenchel-Eggleston strengthening of Caratheodory's Theorem [57] (Theorem 18(i)(ii), p. 35). If a compact set $\tilde{\mathcal{S}}$ has d or fewer connected components, and the set $\tilde{\mathcal{C}}$ with dimension d is the convex hull of $\tilde{\mathcal{S}}$, then the Fenchel-Eggleston Theorem shows that every point in $\tilde{\mathcal{C}}$ is a convex combination of d or few points of $\tilde{\mathcal{S}}$. Since the dimension of $\mathcal{C}$ in this chapter is $d = k+1$, every point of $\mathcal{C}$ can be achieved by (2.9) (2.10) and (2.11) with $l \leq k+1$.

ii) Dubins' Theorem [31] (Theorem 3.6.20, p.116) shows that if a set $\tilde{\mathcal{C}}$ is convex and compact, then every extreme point of the intersection of $\tilde{\mathcal{C}}$ with d hyperplanes is a convex combination of $d+1$ or fewer extreme points of $\tilde{\mathcal{C}}$. A two-dimensional plane in $(k+1)$ dimensions can be considered as the intersection of $(k+1)-2 = k-1$ hyperplanes. Thus every extreme point of the intersection of $\mathcal{C}$ with a two-dimensional plane is a convex combination of $l \leq k$ extreme points of $\mathcal{C}$. Part ii) is then proved by the fact that every extreme point of $\mathcal{C}$ belongs to $\mathcal{S}$. Q.E.D.

A.3 Appendix III: Proof of Theorem 6

Proof of Theorem 6: i) The point $(\boldsymbol{q}, \psi(\boldsymbol{q}, \lambda))$ is a point on the lower boundary of $\mathcal{C}_\lambda$ which is obtained as a convex combination of the points $(\boldsymbol{p}_j, \phi(\boldsymbol{p}_j, \lambda))$ of $\mathcal{S}_\lambda$ with weights w_j. By (2.45), the transmission strategy $U \rightarrow X$ determined by $|\mathcal{U}| = l$, $\Pr(U = j) = w_j$ and $\boldsymbol{p}_{X|U=j} = \boldsymbol{p}_j$, $j = 1, \cdots, l$ achieves the maximum of $R_2 + \lambda R_1$ subject to the constraint $\boldsymbol{p}_X = \boldsymbol{q}$. Thus, the point $(\boldsymbol{q}, \sum_j w_j h_n(T_{YX}\boldsymbol{p}_j), \sum_j w_j h_m(T_{ZX}\boldsymbol{p}_j))$ is on the lower boundary of $\mathcal{C}$, and hence of $\mathcal{C}^*_{\boldsymbol{q}}$. It implies that the graph of $F^*(\boldsymbol{q}, \cdot)$ is supported by a line of slope λ at that point, and thus (2.46) holds. For Part ii), if the transmission strategy $U \rightarrow X$ determined by $|\mathcal{U}| = l$, $\Pr(U = j) = w_j$ and $\boldsymbol{p}_{X|U=j} = \boldsymbol{p}_j$, $j = 1, \cdots, l$ achieves the maximum of $R_2 + \lambda R_1$ subject to the constraint $\boldsymbol{p}_X = \boldsymbol{q}$, the point $(\boldsymbol{q}, \sum_j w_j h_n(T_{YX}\boldsymbol{p}_j), \sum_j w_j h_m(T_{ZX}\boldsymbol{p}_j))$ is on the lower boundary of $\mathcal{C}^*_{\boldsymbol{q}}$, and at this point the graph of $F^*(\boldsymbol{q}, \cdot)$ is supported by a line of slope λ. Thus, the point $(\boldsymbol{q}, \psi(\boldsymbol{q}, \lambda))$ is the convex combination of l points of the graph of $\phi(\cdot, \lambda)$ with arguments $\boldsymbol{p}_j$ and weights w_j, $j = 1, \cdots, l$. Q.E.D.

A.4 Appendix IV: Proof of Lemma 5

Proof of Lemma 5: Lemma 5 is the consequence of Theorem 5 for the broadcast Z channel. Since $H(\boldsymbol{Y}|U) \geq N \cdot q/p \cdot h(\beta_1 p)$,

$$\begin{aligned} H(\boldsymbol{Z}|U) &\geq F^*_{T^{(N)}_{YX},T^{(N)}_{ZX}}(q, N \cdot q/p \cdot h(\beta_1 p)) & \text{(A.5)} \\ &= N \cdot F^*_{T_{YX},T_{ZX}}(q, q/p \cdot h(\beta_1 p)) & \text{(A.6)} \\ &= N \cdot \frac{q}{p} \cdot h(\beta_2 p) & \text{(A.7)} \\ &= N \cdot \frac{q}{p} \cdot h(\beta_1 p \beta_\Delta). & \text{(A.8)} \end{aligned}$$

These steps are justified as follows:

- (A.5) follows from the definition of F^*;
- (A.6) follows from Theorem 5;
- (A.7) follows from the expression of the function F^* for the broadcast Z channel in (3.7);
- (A.8) follows from $\beta_\Delta = \Pr\{Z = 0|Y = 0\} = \beta_2/\beta_1$.

A.5 Appendix V: Proof of (3.25)

Proof of (3.25): Plugging $j = 1$ in (3.24), we have

$$H(\mathbf{Y_1}|W_2, \cdots, W_K) - H(\mathbf{Y_1}|W_1, \cdots, W_K) \geq N\frac{q}{t_1}h(\beta_1 t_1) - Nqh(\beta_1) - o(\epsilon) \quad \text{(A.9)}$$

or

$$H(\mathbf{Y_1}|W_2, \cdots, W_K) \geq N\frac{q}{t_1}h(\beta_1 t_1) - o(\epsilon), \quad \text{(A.10)}$$

since

$$
\begin{aligned}
H(\mathbf{Y_1}|W_1,\cdots,W_K) &= H(\mathbf{Y_1}|\boldsymbol{X}) && \text{(A.11)}\\
&= \sum_{i=1}^{N} H(Y_{1,i}|\boldsymbol{X}) && \text{(A.12)}\\
&= \sum_{i=1}^{N} H(Y_{1,i}|X_i) && \text{(A.13)}\\
&= \sum_{i=1}^{N} \Pr(X_i=0)h(\beta_1) && \text{(A.14)}\\
&= Nqh(\beta_1). && \text{(A.15)}
\end{aligned}
$$

Some of these steps are justified as follows:

- (A.11) follows from the fact that $\boldsymbol{X}$ is a function of $(W_1,\cdots,W_K)$;
- (A.12) follows from the conditional independence of $Y_{1,i}$,$i=1,\cdots,N$, given $\boldsymbol{X}$;
- (A.13) follows from the conditional independence of $Y_{1,i}$ and $(X_1,\cdots,X_{i-1},X_{i+1},\cdots,X_N)$ given X_i.

Inequality (A.10) indicates that

$$
H(\mathbf{Y_j}|W_{j+1},\cdots,W_K) \geq N\frac{q}{t_j}h(\beta_j t_j) - o(\epsilon), \qquad \text{(A.16)}
$$

is true for $j = 1$. The rest of the proof is by induction. We assume that (A.16) is true for j, which means

$$H(\boldsymbol{Y_j}|W_{j+1}, \cdots, W_K) \geq N\left[\frac{q}{t_j}h(\beta_j t_j) - \frac{o(\epsilon)}{N}\right] \tag{A.17}$$

$$= N\frac{q}{t_j + \frac{\tau(\epsilon)}{N}}h(\beta_j(t_j + \frac{\tau(\epsilon)}{N})), \tag{A.18}$$

where the function $\tau(\epsilon) \to 0$ as $\epsilon \to 0$, since $\frac{q}{t_j}h(\beta_j t_j)$ is continuous in t_j. Applying Lemma 5 to the Markov chain $(W_{j+1}, \cdots, W_N) \to \boldsymbol{X} \to \boldsymbol{Y_j} \to \boldsymbol{Y_{j+1}}$, we have

$$H(\boldsymbol{Y_{j+1}}|W_{j+1}, \cdots, W_N) \geq N\frac{q}{t_j + \frac{\tau(\epsilon)}{N}}h(\beta_{j+1}(t_j + \frac{\tau(\epsilon)}{N})) \tag{A.19}$$

$$= N\frac{q}{t_j}h(\beta_{j+1}t_j) + o(\epsilon). \tag{A.20}$$

Considering (3.24) for $j + 1$, we have

$$\begin{aligned} &H(\boldsymbol{Y_{j+1}}|W_{j+2}, \cdots, W_K) - H(\boldsymbol{Y_{j+1}}|W_{j+1}, \cdots, W_K) \\ \geq &N\frac{q}{t_{j+1}}h(\beta_{j+1}t_{j+1}) - N\frac{q}{t_j}h(\beta_{j+1}t_j) - o(\epsilon). \end{aligned} \tag{A.21}$$

Substitution of (A.20) in (A.21) yields

$$H(\boldsymbol{Y_{j+1}}|W_{j+2}, \cdots, W_K) \geq N\frac{q}{t_{j+1}}h(\beta_{j+1}t_{j+1}) - o(\epsilon), \tag{A.22}$$

which establishes the induction. Finally, for $j \geq d$, $N\delta$ should be added to the right side of (A.17) because of the presence of δ in (3.17) for $j = d$, and hence, of $N\delta$ in (3.24).

A.6 Appendix VI: Proof of Lemma 11

Proof of Lemma 11: Let $\mathcal{G}_{T_{YX},T_{ZX}} = \{G_1, \cdots, G_l\}$. For any $(\xi, \eta) \in \mathcal{C}^*_{\boldsymbol{p}_X}$, where $\boldsymbol{p}_X = (1-q, q\boldsymbol{p}^T_{\tilde{X}})^T$, one has $(\boldsymbol{p}_X, \xi, \eta) \in \mathcal{C}$. Since Lemma 8 and Corollary 1 also hold for the discrete multiplicative DBC, $(G_j\boldsymbol{p}_X, \xi, \eta) \in \mathcal{C}$ for all $j = 1, \cdots, l$. By the convexity of the set $\mathcal{C}$,

$$(\boldsymbol{q}, \xi, \eta) = (\sum_{j=1}^{l} G_j\boldsymbol{p}_X \ , \xi, \eta) \in \mathcal{C}, \tag{A.23}$$

where $\boldsymbol{q} = \sum_{j=1}^{l} G_j\boldsymbol{p}_X$. Since $\mathcal{G}_{T_{YX},T_{ZX}}$ is a group, for any permutation matrix $G' \in \mathcal{G}_{T_{YX},T_{ZX}}$,

$$G'\boldsymbol{q} \ = \sum_{j=1}^{l} G'G_j\boldsymbol{p}_X \ = \sum_{j=1}^{l} G_j\boldsymbol{p}_X \ = \ \boldsymbol{q}. \tag{A.24}$$

Hence, the i^{th} entry and the j^{th} entry of $\boldsymbol{q}$ are the same if G' permutes the i^{th} row to the j^{th} row. Since, for any discrete multiplicative DBC, the set $\mathcal{G}_{T_{YX},T_{ZX}}$ maps any non-zero element in $\{0, 1, \cdots, n\}$ to any other non-zero element, all entries except the first entry of $\boldsymbol{q}$ are the same as each other. Furthermore, no matrix in $\mathcal{G}_{T_{YX},T_{ZX}}$ maps the zero element to a non-zero element, hence the first entry of $\boldsymbol{q}$ is the same as the first entry of $\boldsymbol{p}_X$. Therefore, $\boldsymbol{q} = (1-q, q\boldsymbol{u}^T)^T$. This implies that $(\xi, \eta) \in \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$, and hence $\mathcal{C}^*_{\boldsymbol{p}_X} \subseteq \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$. Therefore, $\mathcal{C}^* = \bigcup_{q\in[0,1]} \mathcal{C}^*_{(1-q,q\boldsymbol{u}^T)^T}$. Q.E.D.

A.7 Appendix VII: Proof of Lemma 12

Proof of Lemma 12: $\psi(\boldsymbol{p}_X, \lambda)$ is the lower envelope of $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$ in $\boldsymbol{p}_X$. For $\boldsymbol{p}_X = (1-q, q\boldsymbol{u}^T)^T$, suppose the point $(\boldsymbol{p}_X, \psi(\boldsymbol{p}_X, \lambda))$ is the convex combination of $n+1$ points $((q_i, \boldsymbol{p}_i), \varphi(q_i, \boldsymbol{p}_i, \lambda))$ on the graph of $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$ with weights w_i

for $i = 1, \cdots, n+1$. Therefore,

$$q = \sum_{i=1}^{n+1} w_i q_i, \tag{A.25}$$

$$\boldsymbol{u} = \sum_{i=1}^{n+1} w_i \boldsymbol{p}_i, \tag{A.26}$$

$$\psi(\boldsymbol{p}_X, \lambda) = \sum_{i=1}^{n+1} w_i \varphi(q_i, \boldsymbol{p}_i, \lambda). \tag{A.27}$$

Since $\tilde{\psi}(\boldsymbol{p}, \lambda) \geq \tilde{\psi}(\boldsymbol{u}, \lambda)$ for the group-additive degraded broadcast sub-channel,

$$\varphi(q_i, \boldsymbol{p}_i, \lambda) \geq \varphi(q_i, \boldsymbol{u}, \lambda). \tag{A.28}$$

Therefore, the convex combination of $n+1$ points $((q_i, \boldsymbol{u}), \varphi(q_i, \boldsymbol{u}, \lambda))$ with weights w_i has

$$\sum_{i=1}^{n+1} w_i q_i = q, \tag{A.29}$$

and

$$\sum_{i=1}^{n+1} w_i \varphi(q_i, \boldsymbol{u}, \lambda) \leq \sum_{i=1}^{n+1} w_i \varphi(q_i, \boldsymbol{p}_i, \lambda) = \psi(\boldsymbol{p}_X, \lambda). \tag{A.30}$$

On the other hand, since $\psi(\boldsymbol{p}_X, \lambda)$ is the lower envelope of $\varphi(q, \boldsymbol{p}_{\tilde{X}}, \lambda)$ in $\boldsymbol{p}_X$, $\sum_{i=1}^{n+1} w_i \varphi(q_i, \boldsymbol{u}, \lambda) \geq \psi(\boldsymbol{p}_X, \lambda)$ and hence $\sum_{i=1}^{n+1} w_i \varphi(q_i, \boldsymbol{u}, \lambda) = \psi(\boldsymbol{p}_X, \lambda)$. Therefore, $\psi((1-q, q\boldsymbol{u}^T)^T, \lambda)$, the lower envelope of $\phi(\boldsymbol{p}_X, \lambda)$ in $\boldsymbol{p}_X$ at $\boldsymbol{p}_X = (1 - q, q\boldsymbol{u}^T)^T$ can be attained as the convex combination of points on the graph of $\varphi(q, \boldsymbol{u}, \lambda)$ in the dimension of q. Q.E.D.

A.8 Appendix VIII: Proof of Theorem 3

Here we prove Theorem 3. In (6.4) and (6.5), denote

$$I_1(q_1,q_2,\gamma) = I(X;Y_1|X_2)\Big|_{q_1,q_2,\gamma} \tag{A.31}$$

$$I_2(q_1,q_2,\gamma) = I(X_2;Y_2)\Big|_{q_1,q_2,\gamma} \tag{A.32}$$

$$I_{1,2}(q_1,q_2,\gamma) = (I_1,I_2)\Big|_{q_1,q_2,\gamma}. \tag{A.33}$$

The strategy (q_1,q_2,γ) has the rate pair $I_{1,2}(q_1,q_2,\gamma)$. The theorem is true if we can increase both I_1 and I_2 when $0 < q_2 < 1, 0 < \gamma < q_1$.

Firstly we compare the strategies (q_1,q_2,γ) and $(q_1+p_2\delta_1, q_2, \gamma - q_2\delta_1)$ for a small positive number $\delta_1 > 0$.

$$\begin{aligned}\Delta_1 I_1 &= I_1(q_1+p_2\delta_1,q_2,\gamma-q_2\delta_1) - I_1(q_1,q_2,\gamma)\\ &\simeq \frac{\partial I_1(q_1+p_2\delta_1,q_2,\gamma-q_2\delta_1)}{\partial\delta_1}\Big|_{\delta_1=0}\delta_1\\ &= -q_2p_2(1-\alpha_1)\big(\log\frac{1-\gamma(1-\alpha_1)}{\gamma(1-\alpha_1)} + \log\frac{q_1(1-\alpha_1)}{1-q_1(1-\alpha_1)}\big)\delta_1\\ &< 0,\end{aligned} \tag{A.34}$$

$$\begin{aligned}\Delta_1 I_2 &= I_2(q_1+p_2\delta_1,q_2,\gamma-q_2\delta_1) - I_2(q_1,q_2,\gamma)\\ &\simeq \frac{\partial I_2(q_1+p_2\delta_1,q_2,\gamma-q_2\delta_1)}{\partial\delta_1}\Big|_{\delta_1=0}\delta_1\\ &= q_2p_2(1-\alpha_2)\big(\log\frac{1-\gamma(1-\alpha_2)}{\gamma(1-\alpha_2)} + \log\frac{q_1(1-\alpha_2)}{1-q_1(1-\alpha_2)}\big)\delta_1\\ &> 0.\end{aligned} \tag{A.35}$$

The small change of the rate pair $(\Delta_1 I_1, \Delta_1 I_2)$ is shown Fig. A.1. Point A is the rate pair of the transmission strategy (q_1, q_2, γ), the arrow Δ_1 shows the small movement of the rate pair $(\Delta_1 I_1, \Delta_1 I_2)$.

Secondly we compare the strategies (q_1, q_2, γ) and $(q_1 + (\gamma - q_1)\delta_2, q_2 + q_2\delta_2, \gamma)$ for a small positive number $\delta_2 > 0$.

$$\begin{aligned}\Delta_2 I_1 &= I_1(q_1 + (\gamma - q_1)\delta_2, q_2 + q_2\delta_2, \gamma) - I_1(q_1, q_2, \gamma)\\ &\simeq \frac{\partial I_1(q_1 + (\gamma - q_1)\delta_2, q_2 + q_2\delta_2, \gamma)}{\partial \delta_2}\Big|_{\delta_2=0}\delta_2\\ &= -q_2\delta_2\{\gamma(1-\alpha_1)\log\frac{q_1}{\gamma} + (1-\gamma(1-\alpha_1))\log\frac{1-q_1(1-\alpha_1)}{1-\gamma(1-\alpha_1)}\}\\ &= q_2\delta_2 D(\gamma(1-\alpha_1) \parallel q_1(1-\alpha_1))\\ &> 0, \end{aligned} \tag{A.36}$$

$$\begin{aligned}\Delta_2 I_2 &= I_2(q_1 + (\gamma - q_1)\delta_2, q_2 + q_2\delta_2, \gamma) - I_2(q_1, q_2, \gamma)\\ &\simeq \frac{\partial I_2(q_1 + (\gamma - q_1)\delta_2, q_2 + q_2\delta_2, \gamma)}{\partial \delta_2}\Big|_{\delta_2=0}\delta_2\\ &= q_2\delta_2\{\gamma(1-\alpha_2)\log\frac{q_1}{\gamma} + (1-\gamma(1-\alpha_2))\log\frac{1-q_1(1-\alpha_2)}{1-\gamma(1-\alpha_2)}\}\\ &= -q_2\delta_2 D(\gamma(1-\alpha_2) \parallel q_1(1-\alpha_2))\\ &< 0. \end{aligned} \tag{A.37}$$

where $D(p \parallel q)$ is the relative entropy between distribution p and q. The arrow Δ_2 in Fig. A.1 shows the small movement of the rate pair $(\Delta_2 I_1, \Delta_2 I_2)$.

Now we show that

$$\frac{\Delta_1 I_2}{\Delta_1 I_1} < \frac{\Delta_2 I_2}{\Delta_2 I_1} < 0. \tag{A.38}$$

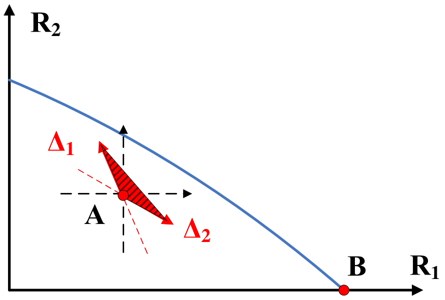


Figure A.1: Capacity region and the changes of rate pairs.

$$
\begin{aligned}
&\frac{\Delta_1 I_2}{\Delta_1 I_1} < \frac{\Delta_2 I_2}{\Delta_2 I_1} \\
&\Leftrightarrow \frac{D(\gamma(1-\alpha_2) \parallel q_1(1-\alpha_2)) + \log\frac{1-\gamma(1-\alpha_2)}{1-q_1(1-\alpha_2)}}{D(\gamma(1-\alpha_1) \parallel q_1(1-\alpha_1)) + \log\frac{1-\gamma(1-\alpha_1)}{1-q_1(1-\alpha_1)}} > \frac{D(\gamma(1-\alpha_2) \parallel q_1(1-\alpha_2))}{D(\gamma(1-\alpha_1) \parallel q_1(1-\alpha_1))} \\
&\Leftrightarrow \frac{D(\gamma(1-\alpha_1) \parallel q_1(1-\alpha_1))}{\log\frac{1-\gamma(1-\alpha_1)}{1-q_1(1-\alpha_1)}} > \frac{D(\gamma(1-\alpha_2) \parallel q_1(1-\alpha_2))}{\log\frac{1-\gamma(1-\alpha_2)}{1-q_1(1-\alpha_2)}} \\
&\Leftrightarrow f(x) = \frac{D(\gamma x \parallel q_1 x)}{\log\frac{1-\gamma x}{1-q_1 x}} \text{is monotonically increasing in } \{x|0<x<1\} \\
&\Leftrightarrow f'(x) = \big(\log\frac{\gamma x}{q_1 x}\log\frac{1-\gamma x}{1-q_1 x} - (\log\frac{1-\gamma x}{1-q_1 x})^2 + \log\frac{\gamma x}{q_1 x}(\frac{1}{1-\gamma x} - \frac{1}{1-q_1 x})\big) \\
&\cdot \gamma(\log\frac{1-\gamma x}{1-q_1 x})^{-2} > 0. \qquad \text{(A.39)}
\end{aligned}
$$

Let $u = 1-\gamma x$ and $v = 1-q_1 x$. So we have $0 < v < u < 1$ and need to prove that

$$g(u,v) = \log\frac{u}{v}\log\frac{1-u}{1-v} - (\log\frac{u}{v})^2 + \log\frac{1-u}{1-v}(\frac{1}{u} - \frac{1}{v}) > 0. \qquad \text{(A.40)}$$

Since

$$\frac{\partial^2 g(u,v)}{\partial u \partial v} = -\frac{(u-v)^2}{u^2 v^2 (1-u)(1-v)} < 0, \qquad \text{(A.41)}$$

and

$$\frac{\partial g(u,v)}{\partial u}\Big|_{v=u} = 0 \quad \forall 0 < u < 1, \tag{A.42}$$

it is true that

$$\frac{\partial g(u,v)}{\partial u} > 0 \quad \forall 0 < v < u < 1. \tag{A.43}$$

Considering (A.43) and $g(v,v) = 0, \forall 0 < v < 1$, we can get $g(u,v) > 0, \forall 0 < v < u < 1$. Thus, the inequality (A.38) is true, which means that the slope of Δ_1 is smaller than that of Δ_2 in Fig. A.1. The achievable shaded region is on the upper right side of point A. Therefore, we can increase the rate pair $I_{1,2}(q_1, q_2, \gamma)$ together and the strategy (q_1, q_2, γ) is not optimal when $0 < q_2 < 1$ and $0 < \gamma < q_1$.

A.9 Appendix IX: Proof of Theorem 4

Here we prove Theorem 4. In problem (6.12), the objective function $I_1 + \lambda I_2$ is bounded and the domain $0 \leq q_1, q_2 \leq 1$ is closed, so the maximum exists and can be attained. First we discuss some possible optimal solutions and then we show that only one of them is the optimum for any fixed $\lambda \geq 0$.

Case 0: If $q_1 = 0$ or $q_2 = 0$ or $q_1 = q_2 = 1$, then $I_1 = I_2 = 0$ and so it can not be the optimum.

Case 1: If $q_2 = 1$ and $0 < q_1 < 1$, then $I_2 = 0$ and

$$\frac{\partial I_1}{\partial q_1} = (1-\alpha_1)\log\frac{1-q_1(1-\alpha_1)}{q_1(1-\alpha_1)} - H(1-\alpha_1) = 0 \tag{A.44}$$

$$\Rightarrow q_1^* = \frac{1}{(1-\alpha_1)(e^{H(1-\alpha_1)/(1-\alpha_1)}+1)}. \tag{A.45}$$

Case 2: If $q_1 = 1$ and $0 < q_2 < 1$, then $I_1 = 0$ and

$$\frac{\partial I_2}{\partial q_2} = (1-\alpha_2)\log\frac{1-q_2(1-\alpha_2)}{q_2(1-\alpha_2)} - H(1-\alpha_2) = 0 \tag{A.46}$$

$$\Rightarrow q_2^* = \frac{1}{(1-\alpha_2)(e^{H(1-\alpha_2)/(1-\alpha_2)}+1)}. \tag{A.47}$$

Case 3: If $0 < q_1, q_2 < 1$, then the optimum is attained when

$$q_2\frac{\partial(I_1+\lambda I_2)}{\partial q_2} + q_1\frac{\partial(I_1+\lambda I_2)}{\partial q_1} = 0$$

$$\Rightarrow \log(1-q_1^*(1-\alpha_1)) = \lambda\log(1-q_1^*(1-\alpha_2)), \tag{A.48}$$

and

$$\begin{aligned}
&\frac{\partial(I_1+\lambda I_2)}{\partial q_2} = 0\\
\Rightarrow &\lambda\big(H(q_1^*(1-\alpha_2)) - q_1^*(1-\alpha_2)\log\frac{1-q_2^*q_1^*(1-\alpha_2)}{q_2^*q_1^*(1-\alpha_2)}\big)\\
&= \big(H(q_1^*(1-\alpha_1)) - q_1^*H(1-\alpha_1)\big)\\
\Rightarrow &\log(1-q_1^*(1-\alpha_1))\big(H(q_1^*(1-\alpha_2)) - q_1^*(1-\alpha_2)\log\frac{1-q_2^*q_1^*(1-\alpha_2)}{q_2^*q_1^*(1-\alpha_2)}\big)\\
&= \log(1-q_1^*(1-\alpha_2))\big(H(q_1^*(1-\alpha_1)) - q_1^*H(1-\alpha_1)\big).
\end{aligned} \tag{A.49}$$

For any fixed $\lambda \geq 0$, the optimal solution is in Case 1,2 or 3.

Lemma 1. *Function* $\varphi(x) = \frac{\log(1-(1-\alpha_1)x)}{\log(1-(1-\alpha_2)x)}$ *is monotonically increasing in the domain of* $0 \leq x \leq 1$ *when* $\alpha_1 < \alpha_2$.

Lemma 2. *The solution in Case 1 can not be the optimum when* $\lambda > \varphi(\psi(1-\alpha_1))$.

proof: When $q_2 = 1$ and $q_1 = \psi(1-\alpha_1)$, $\frac{\partial I_2}{\partial q_1} = 0$ and $\frac{\partial I_1}{\partial q_1} = 0$. Therefore, for any fixed λ, $\frac{\partial(I_1+\lambda I_2)}{\partial q_1} = 0$. When $\lambda = \varphi(q_1) = \varphi(\psi(1-\alpha_1))$, (A.48) holds, and so $\frac{\partial(I_1+\lambda I_2)}{\partial q_2} = 0$.

Since $\frac{\partial(I_2)}{\partial q_2}\Big|_{q_2=1,q_1=\psi(1-\alpha_1)} = \log(1-\psi(1-\alpha_1)\cdot(1-\alpha_2)) < 0$, when $\lambda > \varphi(\psi(1-\alpha_1))$,

$$\begin{aligned} & \frac{\partial(I_1+\lambda I_2)}{\partial q_2}\Big|_{q_2=1,q_1=\psi(1-\alpha_1)} \\ & = \frac{\partial(I_1)}{\partial q_2}\Big|_{q_2=1,q_1=\psi(1-\alpha_1)} + \lambda\frac{\partial(I_2)}{\partial q_2}\Big|_{q_2=1,q_1=\psi(1-\alpha_1)} \\ & < 0. \end{aligned} \tag{A.50}$$

Therefore, Case 1 can not be the optimum when $\lambda > \varphi(\psi(1-\alpha_1))$.

Lemma 3. *The solution in Case 2 can not be the optimum when* $\lambda < \varphi(1)$*.*

proof: When $q_2 = \psi(1-\alpha_2)$ and $q_1 = 1$, $\frac{\partial I_2}{\partial q_2} = 0$ and $\frac{\partial I_1}{\partial q_2} = 0$. Therefore, for any fixed λ, $\frac{\partial(I_1+\lambda I_2)}{\partial q_2} = 0$. When $\lambda = \varphi(q_1) = \varphi(1)$, (A.48) holds, and so $\frac{\partial(I_1+\lambda I_2)}{\partial q_1} = 0$.

Since $\frac{\partial(I_2)}{\partial q_1}\Big|_{q_2=\psi(1-\alpha_2),q_1=1} = q_2(1-\alpha_2)\log\frac{1-q_2+q_2\alpha_2}{q_2\alpha_2}\Big|_{q_2=\psi(1-\alpha_2)} > 0$, when $\lambda < \varphi(1)$,

$$\begin{aligned} & \frac{\partial(I_1+\lambda I_2)}{\partial q_1}\Big|_{q_2=\psi(1-\alpha_2),q_1=1} \\ & = \frac{\partial(I_1)}{\partial q_2}\Big|_{q_2=\psi(1-\alpha_2),q_1=1} + \lambda\frac{\partial(I_2)}{\partial q_2}\Big|_{q_2=\psi(1-\alpha_2),q_1=1} \\ & < 0. \end{aligned} \tag{A.51}$$

Therefore, Case 2 can not be the optimum when $\lambda < \varphi(1)$.

Lemma 4. *The solution to equation (A.48) exists in* $(0, 1)$ *and is unique for any* λ *in the range of* $\varphi(0) < \lambda < \varphi(1)$*.*

Proof: Equation (A.48) is equivalent to $\varphi(q_1^*) = \lambda$. From Lemma 1, $\varphi(q_1)$ is monotonically increasing. Therefore, when $\varphi(0) < \lambda < \varphi(1)$, the solution $q_1^*$is unique and $q_1^* \in (0, 1)$.

Lemma 5. *The unique solution (q_1^*, q_2^*) to equation (A.48) and (A.49) in case 3 is the optimum if $\varphi(\psi(1 - \alpha_1)) < \lambda < \varphi(1)$.*

Proof: From Lemma 4, the solution q_1^* to equation (A.48) is unique if $\varphi(\psi(1 - \alpha_1)) < \lambda < \varphi(1)$. From (A.49),

$$\begin{aligned} m(q_2) = &\big(H(q_1^*(1-\alpha_2)) - q_1^*(1-\alpha_2)\log\frac{1 - q_2 q_1^*(1-\alpha_2)}{q_2 q_1^*(1-\alpha_2)}\big)\log(1 - q_1^*(1-\alpha_1)) \\ &- \big(H(q_1^*(1-\alpha_1)) - q_1^* H(1-\alpha_1)\big)\log(1 - q_1^*(1-\alpha_2)) \\ &= 0. \end{aligned} \tag{A.52}$$

Clearly, $m(q_2)$ is monotonically increasing,

$$\lim_{q_2 \to 0} m(q_2) = -\infty < 0, \tag{A.53}$$

and

$$\begin{aligned} &\varphi(\psi(1-\alpha_1)) < \lambda < \varphi(1) \\ \Rightarrow &q_1^* > \psi(1-\alpha_1) \\ \Rightarrow &m(1) > 0. \end{aligned} \tag{A.54}$$

That means the unique solution q_2^* to equation (A.49) is in the domain of $0 \leq q_2 \leq 1$. Furthermore, when $\varphi(\psi(1-\alpha_1)) < \lambda < \varphi(1)$, from Lemma 2 and Lemma

3, case 1 or case 2 can not be the optimum because

$$\frac{\partial(\lambda I_1 + (1-\lambda)I_2)}{\partial q_2}\Big|_{q_2=1, q_1=\psi(1-\alpha_1)} < 0, \tag{A.55}$$

$$\frac{\partial(\lambda I_1 + (1-\lambda)I_2)}{\partial q_1}\Big|_{q_1=1, q_2=\psi(1-\alpha_2)} < 0. \tag{A.56}$$

Therefore, case 3 is the optimum.

Lemma 6. *The unique solution* $(q_2^* = 1, q_1^* = \psi(1-\alpha_1))$ *in case 1 is the optimum if* $0 \leq \lambda \leq \varphi(\psi(1-\alpha_1))$.

Proof: When $0 \leq \lambda \leq \varphi(\psi(1-\alpha_1))$, Case 3 is not optimal because there is no solution $q_1 \in (0,1)$ to equation (A.48). Case 2 is not optimal from Lemma 3. So Case 1 is the optimum.

Lemma 7. *The unique solution* $(q_2^* = \psi(1-\alpha_2), q_1^* = 1)$ *in Case 2 is the optimum if* $\lambda \geq \varphi(1)$.

Proof: When $\lambda \geq \varphi(1)$, Case 3 is not optimal because there is no solution $q_2 \in (0,1)$ to equation (A.49). Case 1 is not optimal from Lemma 2. So Case 2 is the optimum.

From Lemma 5,6 and 7, Theorem 4 is immediately proved.

References

[1] T. M. Cover. Broadcast channels. *IEEE Trans. Inform. Theory*, IT-18:2–14, January 1972.

[2] P. P. Bergmans. Random coding theorem for broadcast channels with degraded components. *IEEE Trans. Inform. Theory*, IT-19:197–207, March 1973.

[3] R. G. Gallager. Capacity and coding for degraded broadcast channels. *Probl. Pered. Inform.*, 10:3–14, July–Sept. 1974.

[4] T. M. Cover and J. A. Thomas. *Elements of information theory.* Wiley-Interscience, 1991.

[5] E. Telatar. *Private Communication.*

[6] P. P. Bergmans. A simple converse for broadcast channels with additive white Gaussian noise. *IEEE Trans. Inform. Theory*, IT-20:279–280, March 1974.

[7] A. D. Wyner. A theorem on the entropy of certain binary sequences and applications: Part II. *IEEE Trans. Inform. Theory*, IT-19:772–777, Nov 1973.

[8] H. Witsenhausen. Entropy inequalities for discrete channels. *IEEE Trans. Inform. Theory*, IT-20(5):610–616, Sep 1974.

[9] H. Witsenhausen and A. Wyner. A conditional entropy bound for a pair of discrete random variables. *IEEE Trans. Inform. Theory*, IT-21(5):493–501, Sep 1975.

[10] R. Benzel. The capacity region of a class of discrete additive degraded interference channels. *IEEE Trans. on Info. Theo.*, IT-25:228–231, 1979.

[11] B. Xie, M. Griot, A. I. Vila Casado and R. D. Wesel. Optimal transmission strategy and capacity region for broadcast Z channels. In *IEEE Information Theory Workshop 2007*, Lake Tahoe, USA, Sep 2007.

[12] B. Xie, M. Griot, A. I. Vila Casado and R. D. Wesel. Optimal transmission strategy and explicit capacity region for broadcast Z channels.

[13] N. Liu and S. Ulukus. The capacity region of a class of discrete degraded interference channels. In *Information Theory and Applications 2007*, UCSD, San Diego, USA, Jan 29-Feb 2 2007.

[14] N. Liu and S. Ulukus. The capacity region of a class of discrete degraded interference channels. *IEEE Trans. Inform. Theory*, 54(9):4372–4378, Sep 2008.

[15] B. Xie and R. D. Wesel. A mutual information invariance approach to symmetry in discrete memoryless channels. In *Information Theory and Application 2008*, UCSD, San Diego, USA, Jan. 27-Feb. 1 2008.

[16] "BitTorrent.". *[Online]. Available: http://www.bittorrent.com.*

[17] "Napster.". *[Online]. Available: http://www.napster.com.*

[18] "Gnutella.". *[Online]. Available: http://www.gnutella.com.*

[19] "KaZaA.". *[Online]. Available: http://www.kazaa.com.*

[20] S. Androutsellis-Theotokis and D. Spinellis. "A survey of peer-to-peer content distribution technologies". *ACM Compl Surveys*, 36(4):335–371, Dec. 2004.

[21] J. Liu, S. G. Rao, B. Li, and H. Zhang. "Opportunities and challenges of peer-to-peer internet video broadcast". *Proceedings of the IEEE, Special Issue on Recent Advances in Distributed Multimedia Communications*, 2007.

[22] X. Zhang, J. Liu, B. Li, and T. S. P. Yum. "Coolstreaming/donet: A data-driven overlay network for efficient live media streaming". *in Proc. INFOCOM'05*, 2005.

[23] V. Pai, K. Kumar, K. Tamilmani, V. Sambamurthy, and A. E. Mohr. "Chainsaw: Eliminating trees from overlay multicast". *in Proc. 4th Int. Workshop on Peer-to-Peer Systems (IPTPS)*, Feb. 2005.

[24] J. Li, P. A. Chou, and C. Zhang. "Mutualcast: An efficient mechanism for content distribution in a peer-to-peer (P2P) network". *Microsoft Research, MSR-TR-2004-100*, 2004.

[25] J. Li. "PeerStreaming: A practical receiver-driven peer-to-peer media streaming system". *Microsoft, Tech. Rep. MSR-TR-2004-101*, Sep. 2004.

[26] Z. Xiang, Q. Zhang, W. Zhu, Z. Zhang, and Y.-Q. Zhang. "Peer-to-peer based multimedia distribution service". *IEEE Trans. Multimedia*, 6(2):343–355, Apr. 2004.

[27] J. Jannotti, D. K. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole. "Overcast: Reliable multicasting with an overlay network". *in Proc. of the Fourth Symposium of Operating System Design and Implementation (OSDI)*, pages 197–212, Oct. 2000.

[28] Y. Wu, Y. C. Hu, J. Li, and P. A. Chou. "The delay region for P2P file transfer". *in International Symposium of Information Theory 2009, Seoul Korea*, July 2009.

[29] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:623–656, Oct 1948.

[30] A. D. Wyner and J. Ziv. A theorem on the entropy of certain binary sequences and applications: Part I. *IEEE Trans. Inform. Theory*, IT-19:769–772, Nov 1973.

[31] R. G. Gallager. *Information theory and reliable communication.* New York: Wiley, 1968.

[32] S. W. Golomb. The limiting behavior of the Z-channel. *IEEE Trans. Inform. Theory*, IT-26:372, May 1980.

[33] M. Griot, A.I. Vila Casado, W-Y. Weng, H. Chan, J. Basak, E. Yablanovitch, I. Verbauwhede, B. Jalali and R. D. Wesel. Trellis codes with low ones density for the OR multiple access channel. In *IEEE ISIT 2006*, July 2006.

[34] M. Griot, A.I. Vila Casado, and R.D. Wesel. Non-linear turbo codes for interleaver-division multiple access on the OR channel. In *GLOBECOM '06. IEEE Global Telecomm. Conf.*, 27 Nov. - 1 Dec. 2006.

[35] T. M. Cover. Comments on broadcast channels. *IEEE Trans. Inform. Theory*, 44:2524–2530, October 1998.

[36] K. Jain, L. Lovasz, and P. A. Chou. "Building scalable and robust peer-to-peer overlay networks for broadcasting using network coding". *Microsoft Research Technical Report MSR-TR-2004-135*, Dec. 2004.

[37] Y. Chu, S. G. Rao, and H. Zhang. "A case of end system multicast". *in Joint Int'l Conf. Measurement and Modeling of Computer Systems (SIGMETRICS)*, Jun. 2000.

[38] Y. Chu, A. Ganjam, T. S. E. Ng, S. G. Rao, K. Sripanidkulchai, J. Zhan, and H. Zhang. "Early experience with an internet broadcast system based on overlay multicast". *in Proc. of USENIX*, 2004.

[39] H. Deshpande, M. Bawa, and H. Garcia-Molina. “Streaming live media over a peer-to-peer network”. *Stanford Univ. Comput. Sci. Dept., Tech. Rep.*, Jun. 2001.

[40] X. Jiang, Y. Dong, D. Xu, and B. Bhargava. “GnuStream: A P2P media streaming system prototype”. *in Proc. of 4th International Conference on Multimedia and Expo*, Jul. 2003.

[41] Y. Cui, B. Li, and K. Nahrstedt. “oStream: asynchronous streaming multicast in application-layer overlay networks”. *IEEE J. Select. Areas Commun.*, 22(1):91–106, Jan. 2004.

[42] V. N. Padmanabhan, H. J. Wang, and P. A. Chou. “Resilient peer-to-peer streaming”. *Microsoft, Tech. Rep. MSR-TR-2003-11*, Mar. 2003.

[43] V. N. Padmanabhan, H. J. Wang, P. A. Chou, and K. Sripanidkulchai. “Distributing streaming media content using cooperative networking”. *in Proc. NOSSDAV’02*, May 2002.

[44] S. Accendanski, S. Deb, M. Medard, and R. Koetter. “How good is random linear coding based distributed networked storage?”. *in Proc. 1st Workshop on Network Coding, WiOpt 2005, Riva del Garda, Italy*, Apr. 2005.

[45] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung. “Network information flow”. *IEEE Trans. on Information Theory*, 2000.

[46] S.-Y. R. Li, R. W. Yeung, and N. Cai. “Linear network coding”. *IEEE Trans. on Information Theory*, 2003.

[47] R. Koetter, M. Medard. “An algebraic approach to network coding”. *IEEE Trans. on Networking*, 2003.

[48] D. Qiu and R. Srikant. “Modeling and performance analysis of BitTorrent-like peer-to-peer netowks”. *In Proc. of SIGCOMM04, Portland, OR*, Aug. 30 - Sep. 3 2004.

[49] Z. Ge, D. R. Figueiredo, S. Jaiswal, J. Kurose, and D. Towsley. “Modeling peer-peer file sharing systems”. *In Article of IEEE INFOCOM*, 2003.

[50] F. Clevenot and P. Nain. “A simple fluid model for the analysis of the squirrel peer-to-peer caching system”. *In Article of IEEE INFOCOM*, 2004.

[51] J. Pouwelse, P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D. Epema, M. Reinders, M. van Steen, and H. Sips. “Tribler: A social-based peer-to-peer system”. *The 5th International Workshop on Peer-to-Peer Systems*, 2006.

[52] S. Boyd and L. Vandenberghe. *Convex optimization.* Cambridge Univ. Press, 2004.

[53] D.J.C. MacKay. "Fountain codes". *in IEEE Proc.-Commun.*, (6), 2005.

[54] M. Luby. "LT codes". *in 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 271–282, 2002.

[55] A. Shokrollahi. "Raptor codes". *"Technical report, Laboratoire dalgorithmique, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland"*, 2003, Available from algo.epfl.ch/.

[56] T. Courtade and R. D. Wesel. "A deterministic approach to rate-compatible fountain communication". *IEEE Information Theory and Applications*, 2010.

[57] H. G. Eggleston. *Convexity.* New York: Cambridge Univ., 1963.