UNIVERSITY OF CALIFORNIA SAN DIEGO

Structured Codes for Network Communication

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Electrical Engineering
(Communication Theory and Systems)

by

Pinar Sen

Committee in charge:

Professor Young-Han Kim, Chair
Professor Bhaskar D. Rao
Professor Paul H. Siegel
Professor Alexander Vardy
Professor Geoffrey Voelker

2020

The dissertation of Pinar Sen is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

Chair

University of California San Diego

2020

DEDICATION

To my beloved parents and family

for their unconditional love, endless support, encouragements, and sacrifices

EPIGRAPH

Let everything

happen to you:

beauty and terror.

Just keep going.

No feeling is final.

—Rainer Maria Rilke

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank my advisor and mentor, Young-Han Kim for guiding me in this amazing journey. Since the beginning, he has been an excellent teacher and inspiring researcher to me with his extraordinary talent of converting hard-to-grasp math problems or research questions into meaningful real-world concepts, making them interesting to a greater audience. He always pushes me even beyond my expectations and at the same time gives me courage to aim higher. I am grateful to him for challenging and believing in me.

I am sincerely thankful to the valuable professors in our department, particularly Alexandar Vardy, Alon Orlitsky, Tara Javidi, Bhaskar Rao, and Paul Siegel, for their intellectually challenging and interesting lectures and particularly thankful to my committee members Bhaskar Rao, Paul Siegel, Alexandar Vardy, and Geoffrey Voelker for devoting generously their time for my dissertation. I am also grateful to Michael Gastpar for hosting me during my summer visit in EPFL. It was an incredible opportunity working with him through a process of creating and solving a research problem. The annual dinner with students and professors at EPFL was also memorable for me, I particularly remember pleasant conversation with Emre Teletar. I am also very thankful to Sung Hoon Lim for being an invaluable collaborator with his creative and positive attitude all the times.

I sincerely appreciate the friendship within our group. Thank you Alankrita Bhatt, Shouvik Ganguly, Nadim Ghaddar, Jiunting Huang, and Jongha Ryu for relaxing conversations and stimulating discussions in our group meetings as well as during the season of NSF proposal preparation. I am also grateful to our seniors Lele Wang and Yu Xiang for being role models to us and generously sharing their experiences with us. Erman Köken, Sinan Akyürek, Özge Akyürek, Yonatan Vaizman, and Ran Goldblatt made my transition to San Diego easier. Also, special thanks to my close friends Halime Koca, Gokce Sarar, Mürsel Karadaş, Selim Özgen, and Caner Ünal for lightening the

burden of life with warm conversations.

Last but not least, I thank my family for their unconditional love and support towards me and my sister. My devoted mother and my father, as our first teachers, have a great place in our achievements. I am indebted to Cansu, my little sister, for being the joy of my life, for her relaxing and cheerful personality which has a healing effect on me in my hard times. I thank my partner, Tuğcan Aktaş who is literally always near me under all types of difficulties in both academic and personal life and keep me in countenance believingly throughout my studies. I feel so lucky to have such a supportive family, without whom I would not have been able to complete this dissertation. This dissertation is dedicated to my family.

Chapter 2 and 5 are, in part, a reprint of the material in the papers: Pinar Sen and Young-Han Kim, "Homologous Codes for Multiple Access Channels," in *IEEE Transactions on Information Theory,* vol. 66, no. 3, pp. 1549-1571, March 2020; and Pinar Sen and Young-Han Kim, "Homologous Codes for Multiple Access Channels," *Proceedings of the IEEE International Symposium on Information Theory*, Aachen, Germany, June 2017. The dissertation author was the primary investigator and author of this paper.

Chapter 3 is, in part, a reprint of the material in the papers: Pinar Sen, Sung Hoon Lim, and Young-Han Kim, "On the Optimal Achievable Rates for Linear Computation With Random Homologous Codes," accepted to *IEEE Transactions of Information Theory*, 2020; and Pinar Sen, Sung Hoon Lim, and Young-Han Kim, "Optimal Achievable Rates for Computation With Random Homologous Codes," *Proceedings of IEEE International Symposium on Information Theory*, Vail, Colorado, June 2018. The dissertation author was the primary investigator and author of this paper.

Chapter 4 is, in part, a reprint of the material in the paper: Pinar Sen, Sung Hoon Lim, and Young-Han Kim, "On the Optimal Achievable Rates for Linear Computation With Random Homologous Codes," accepted to *IEEE Transactions of Information Theory*, 2020. The dissertation author was the primary investigator and author of this paper.

Chapters 6 and 7 are, in part, a reprint of the material in the paper: Pinar Sen and Michael Gastpar, "Successive Refinement to Caching for Dynamic Content," *Proceedings of IEEE International Symposium on Information Theory*, Paris, France, June 2019. Chapters 6 and 7 are, in part, currently being prepared for submission for publication of the material in *IEEE Transactions of Information Theory*, 2020 with authors Pinar Sen, Michael Gastpar, and Young-Han Kim. The dissertation author was the primary investigator and author of this paper.

Chapter 8 is, in part, a reprint of the material in the paper: Pinar Sen, Michael Gastpar, and Young-Han Kim, "Successive Refinement to Caching for Dynamic Re-

quests," *Proceedings of IEEE International Symposium on Information Theory*, Los Angeles, California, June 2020. Chapter 8 is, in part, currently being prepared for submission for publication of the material in *IEEE Transactions of Information Theory*, 2020 with authors Pinar Sen, Michael Gastpar, and Young-Han Kim. The dissertation author was the primary investigator and author of this paper.

VITA

2011	Bachelor of Science in Electrical and Electronics Engineering, Middle East Technical University
2011-2014	Graduate Research and Teaching Assistant, Middle East Technical University
2014	Master of Science in Electrical and Electronics Engineering, Middle East Technical University
2014-2020	Graduate Research Assistant, University of California San Diego
2020	Doctor of Philosophy in Electrical Engineering (Communication Theory and Systems), University of California San Diego

PUBLICATIONS

Pinar Sen, Tugcan Aktas, Se Yong Park, Haitong Sun, Naga Bhushan, Tingfang Ji, “Multi-layer rate splitting for wireless communications,” US Patent App. 16/143,337.

Se Yong Park, Pinar Sen, Jay Kumar Sundararajan, Joseph Binamira Soriaga, Tingfang Ji, N. Bhushan, “Sequence generation and assignment,” US Patent App. 16/131,966

Se Yong Park, Pinar Sen, Naga Bhushan, Tingfang Ji, “Modulation Spreading for Wireless Communications,” US Patent App. 16/143,359

Pinar Sen, Michael Gastpar, Young-Han Kim, “Successive Refinement for Dynamic Caching,” in preparation to submit to *IEEE Transactions on Information Theory*, 2020.

Pinar Sen, Sung Hoon Lim, Young-Han Kim, “On the Optimal Achievable Rates for Linear Computation With Random Homologous Codes,” accepted to *IEEE Transactions of Information Theory*, 2020.

Pinar Sen and Young-Han Kim, “Homologous Codes for Multiple Access Channels,” in *IEEE Transactions on Information Theory,* vol. 66, no. 3, pp. 1549-1571, March 2020.

Po-Han Peter Wang, Haowei Jiang, Li Gao, Pinar Sen, Young-Han Kim, Gabriel Rebeiz, Patrick Mercier, Drew Hall, “A Near-Zero-Power Wake-Up Receiver Achieving −69-dBm Sensitivity,” in *IEEE Journal of Solid-State Circuits,* vol. 53, no. 6, pp. 1640-1652, June 2018.

Po-Han Peter Wang, Haowei Jiang, Li Gao, Pinar Sen, Young-Han Kim, Gabriel Rebeiz, Patrick Mercier, Drew Hall, “A 6.1-nW Wake-Up Receiver Achieving −80.5-dBm Sensitivity Via a Passive Pseudo-Balun Envelope Detector,” in *IEEE Journal of Solid-State Circuits Letters,* vol. 1, no. 5, pp. 134-137, May 2018.

Pinar Sen and Ali Ozgur Yilmaz, “A Low-Complexity Graph-Based LMMSE Receiver for MIMO ISI Channels with M-QAM Modulation,” in *IEEE Transactions on Wireless Communications,* vol.16, no.2, pp. 1185-1195, Feb. 2017.

Pinar Sen and Ali Ozgur Yilmaz, "Factor Graph Based LMMSE Filtering for Colored Gaussian Processes," in *IEEE Signal Processing Letters,* vol. 21, no. 10, pp. 1206-1210, Oct. 2014.

Tugcan Aktas and Pinar Sen, "Interleaved Block Coding for Achieving Gaussian Random Access Channel Capacity," *Proceedings of the IEEE International Symposium on Information Theory*, Los Angeles, California, June 2020.

Pinar Sen, Michael Gastpar, Young-Han Kim, "Successive Refinement to Caching for Dynamic Requests," *Proceedings of the IEEE International Symposium on Information Theory*, Los Angeles, California, June 2020.

Pinar Sen and Michael Gastpar, "Successive Refinement to Caching for Dynamic Content," *Proceedings of the IEEE International Symposium on Information Theory*, Paris, France, June 2019.

Alankrita Bhatt, Jiun-Ting Huang, Young-Han Kim, Jongha-John Ryu, Pinar Sen, "Monte Carlo methods for randomized likelihood decoding," *Proceedings of the 56th Annual Allerton Conference on Communication, Control, and Computation*, Monticello, Illinois, September 2018.

Alankrita Bhatt, Jiun-Ting Huang, Young-Han Kim, Jongha-John Ryu, Pinar Sen, "Variations on a Theme by Liu, Cuff, and Verdu: The Power of Posterior Sampling," *IEEE Information Theory Workshop*, 2018.

Pinar Sen, Sung Hoon Lim, and Young-Han Kim, "Optimal Achievable Rates for Computation With Random Homologous Codes," *Proceedings of IEEE International Symposium on Information Theory*, Vail, Colorado, June 2018.

Po-Han Peter Wang, Huawei Jiang, Li Gao, Pinar Sen, Young-Han Kim, Gabriel Rebeiz, Patrick Mercier, Drew Hall, "A 400 MHz 4.5 nW −63.8 dBm sensitivity wake-up receiver employing an active pseudo-balun envelope detector," *Proceedings of the 43rd IEEE European Solid State Circuits Conference*, Leuven, Belgium, 2017.

Huawei Jiang, Po-Han Peter Wang, Li Gao, Pinar Sen, Young-Han Kim, Gabriel Rebeiz, Drew Hall, Patrick Mercier, "24.5 A 4.5 nW wake-up radio with −69 dBm sensitivity," *Proceedings of IEEE International Solid-State Circuits Conference*, San Francisco, CA, 2017.

Pinar Sen and Young-Han Kim, "Homologous codes for multiple access channels," *Proceedings of IEEE International Symposium on Information Theory*, Aachen, Germany, 2017.

Pinar Sen, Tugcan Aktas, Ali Ozgur Yilmaz, "A low-complexity graph-based LMMSE receiver designed for colored noise induced by FTN-signaling," *Proceedings of IEEE Wireless Communications and Networking Conference*, Istanbul, Turkey, 2014.

ABSTRACT OF THE DISSERTATION

Structured Codes for Network Communication

by

Pinar Sen

Doctor of Philosophy in Electrical Engineering
(Communication Theory and Systems)

University of California San Diego, 2020

Professor Young-Han Kim, Chair

Random independently and identically distributed code ensembles play a fundamental role in characterizing the limits of communication rates over different network models, with most existing coding schemes built on them. It has been shown in various problems, on the other hand, these conventional random coding schemes are outperformed by *structured* ones that are well-suited to the problem of interest, resulting in strictly better communication rates. This dissertation investigates the benefits of structured codes for a wider class of network models that can be grouped into two parts. In the first part, a special code structure that is built on linearity shared by multiple senders is studied for the two conflicting canonical problems defined over multiple access channels:

linear computation of codewords and message communication. For linear computation, the optimal decoding performance of such structured codes is analyzed, which yields strictly larger rates than random coding. For message communication, it is shown that the aforementioned family of structured codes can achieve the optimal tradeoff between communication rates. In the second part, a structured transmission scheme, referred to as caching, is studied to reduce the network load between a server that stores a set of file contents and users that request a file from the server. To cope with the unpredictable nature of file contents and user requests, two new caching problems are formulated. As an answer to these caching problems, a successive refinement approach is proposed to store some partial information about file contents in small increments into the memories of end users. These results motivate further research into the potential of structured codes in network communication.

Chapter 1

Introduction

Network communication can be defined as multiple senders trying to convey some information source to multiple receivers via a transmission medium in a reliable manner. At each sender, information source is encoded into a sequence, which is transmitted through the medium. At each receiver, an estimation for the desired sources (or a function of sources) is computed. The goal of network information theory is to characterize the optimal tradeoffs among the encoding rates of information sources for arbitrarily small probability of error in communication. In his ground-breaking paper [1], Shannon established the fundamental limit of reliable communication between one sender and one receiver via a probabilistic method by utilizing independent and identically distributed (i.i.d.) random code ensembles. Following this seminal work, extensive research effort was put into establishing fundamental limits of network communications for various specific scenarios, with most existing coding schemes built on random i.i.d. code ensembles; see, for example, [2–4].

As shown by Körner and Marton [5], on the other hand, for the problem of encoding a modulo-two sum of distributed dependent binary sources, using the *same* random ensemble of linear codes at multiple senders can achieve strictly better rates than using independently generated ensembles of codes. Building on this observation, Nazer and Gastpar [6] developed a channel coding scheme that uses the same random ensemble of lattice codes at multiple encoders and showed that this *structured* coding scheme outperforms conventional random coding schemes for computing a linear combination of the sources over a linear multiple access channel (MAC), even for independent sources. This influential work led to the development of the *compute–forward* strategy for relay networks, which, together with the extensions, was shown to provide higher achievable rates for several communication problems involving relay networks in part.

More recently, *nested coset codes* [7,8] were proposed as more flexible alternatives for achieving the desired linear structure at multiple encoders. In particular, Padakandla and Pradhan [8] developed a fascinating coding scheme for the computation problem over an *arbitrary* MAC. Motivated by the physical meaning of compute–forward and interference alignment, where a linear combination of codewords is to be utilized at the receiver to cancel out the interferer codewords, Lim, Feng, Pastore, Nazer, and Gastpar [9, 10] tackled codeword computation and generalized the nested coset codes constructed with the same generator matrix to asymmetric rate pairs. We referred to this generalized version as *homologous* codes [11–14]. This terminology is motivated from its biological definition, i.e., the structures modified from the same ancestry (underlying linear code) to adapt to different purposes (desired shape).

In the first part of this dissertation, we study the performance of homologous codes for different communication scenarios. In Chapter 2, we start with formal definitions of nested coset codes and homologous codes. In Chapter 3, we concentrate on *linear computation* problem over a multiple access channel with two sender and one receiver, in which the receiver wishes to reliably estimate a linear function of transmitted codewords from the senders. We establish inner and outer bounds on the optimal tradeoff between the communication rates when encoding is restricted to random ensembles of homologous codes but when decoding is optimized with respect to the realization of the encoders. For the special case in which the desired linear combination and the channel structure are "matched" to the structure of the multiple access channel in a natural sense, which is the case in which the benefit of computation can be realized to the fullest extent as indicated by [15], these inner and outer bounds coincide. Generalizing some of the techniques, we provide a single-letter outer bound for the capacity region of the linear computation problem.

Construction of homologous codes has many similarities to Marton's coding scheme, one of the fundamental coding schemes in network information theory. Marton's coding scheme [16] was proposed to provide an inner bound on the optimal tradeoff between the communication rates for a two-receiver broadcast channel, which consists of a sender wishing to convey two separate messages to each receiver reliably. Dated back to 1979, Marton's coding scheme is still the best known inner bound for a general broadcast channel. In Chapter 4, we adapt the proof techniques that we developed for homologous codes to establish an outer bound on the optimal rate region for broadcast channels with Marton's coding scheme. The resulting outer bound coincides with the inner bound that is achieved by *simultaneous nonunique decoding*, thus characterizing the optimal rate region of a two-receiver general broadcast channel achieved by a given random code ensemble.

Returning back to our discussion on the performance of homologous codes, one question remains. Can the benefit of computation be realized to the full extent only in special cases for which desired linear combinations and channel structures are matched, as implied by [13–15]? In the same vein, for a given code distribution, the aforementioned rate region achievable by homologous codes for the linear computation in Chapter 3 turns out to be strictly smaller than the optimal, which is achievable by random i.i.d. codes, when computation is specialized to communication (i.e., the identity function computation). In Chapter 5, we analyze the performance of homologous codes for a multiple access channel, in which the receiver wishes to reliably estimate the transmitted messages themselves. Starting from a two-sender multiple access channel, we show that homologous codes can achieve the optimal tradeoff among communication rates by a careful combination with a *channel transformation* technique, which allows constructing algebraic codes over a larger finite field and mapping them to the channel input alphabet. We then extend this result to multiple access channels with more than two senders and with one or more receivers as well as their Gaussian counterparts. We finalize our discussion on homologous codes by constructing an example of a multi-receiver multiple access channel that requires simultaneous communication and computation, which illustrates the superiority of homologous codes over random i.i.d. codes even in such a competing scenario.

Coding schemes built on a certain *structure* benefits another class of network models as well. Storage networks consists of a server (sender) that stores some file contents and multiple users (receivers) that request a file from the server. Up on users' requests, server maps the requested file contents into a sequence and conveys it to the users via a noiseless link. Due to the ever-growing number of devices in real storage systems, such networks encounter heavy traffic during peak hours of the day. One structured scheme to shifting the network traffic to off-peak hours is to cache partial information about contents on local memories of end users during the off-peak hours for potential future use. After this cache placement phase, user requests are revealed to the server, possibly during the peak hours, and the server broadcasts some other information about the contents. After this content delivery phase, each user recovers its requested content by combining the new information with its cache.

Recently, coding-theoretic approaches were proposed to develop practical close-to-optimal codes for cache placement and content delivery. Breaking off from earlier studies [17,18] that concentrated on optimizing either cache placement or content delivery while the other is fixed, Maddah-Ali and Niesen [19] brought further structure to a coding scheme that optimizes both phases, achieving the optimal tradeoff among communication rates for cache placement and content delivery up to a constant multiplicative factor. In this pioneering work, each file is split into subfiles, where a set of properly chosen subfiles is cached at user devices and a set of linearly encoded subfiles is broadcast in the delivery phase.

Taking an information-theoretic approach, Wang, Lim, and Gastpar [20, 21] formulated a caching problem for a single user and showed a close connection to the Gray–Wyner network [22], a well-known distributed source coding problem in network information theory. Utilizing this connection, they established a single-letter characterization of the optimal tradeoff among communication rates for cache placement and average-case content delivery (for uniformly random requests) as an optimization problem and solved it explicitly when the cache rate is above a well-defined threshold.

In these existing caching problems and extensive research efforts put into improving the results or extending them to other scenarios, cache placement is completed in a single step, which falls short of capturing the unpredictable nature of contents and demands in real networks. In the second part of this dissertation, particularly through Chapters 7 to 8, we formulate new caching problems to address: 1) contents being subject to random modifications during the cache placement phase (*dynamic contents*) and 2) requests arising at any point of time possibly interrupting the cache placement phase (*dynamic requests*). To answer these dynamic caching problems, we propose a successive refinement approach to cache placement.

In Chapter 6, we present a successive version of the Gray–Wyner network (or the *successive Gray–Wyner network* in short) and we establish a single-letter characterization for the optimal rate region of this network. In Chapter 7, we formulate a single-user caching problem for dynamic contents, in which the cache placement phase consists of two successive steps and the second step refines the cache content stored in the first step when the file contents are modified. Taking an information-theoretic approach similar to [20, 21], we relate this problem to the successive Gray–Wyner network and present a single-letter characterization of the optimal tradeoff between communication rates for cache placement and average-case content delivery as an optimization problem. We then derive an explicit characterization of the optimal tradeoff for certain classes of content distributions.

In Chapter 8, we formulate a caching problem for dynamic requests, in which the cache placement phase consists of an arbitrary number of successive steps and each step refines the cache content stored in prior steps for possible requests arising at that moment in time. Taking an information-theoretic approach, we consider a single user and two time points at which the request can arise, and relate this problem to the successive Gray–Wyner network. We characterize the optimal tradeoff between communication rates for cache placement and average-case delivery rates at different request times when the cache rate is above a well-defined threshold. We also consider a coding-theoretic version of the problem with an arbitrary number of users and a finite set of time points at which requests can arise, assuming the class of i.i.d. Bern(1/2) contents. For this setting, we develop a structured successive caching algorithm that benefits from a linear encoding in the delivery phase and achieves average-case delivery rates that are uniformly within a constant multiplicative factor of their respective minima at every request time. Our algorithm is also uniformly near-optimal when the performance criterion is the *worst-case* delivery rates.

Chapter 9 makes concluding remarks and comments on future directions.

Bibliography

[1] Claude E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27(3):379–423, 27(4), 623–656, 1948.

[2] Abbas El Gamal and Young-Han Kim. *Network Information Theory.* Cambridge University Press, Cambridge, 2011.

[3] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory.* Wiley, New York, second edition, 2006.

[4] Gerhard Kramer. Topics in multi-user information theory. *Found. Trends Comm. Inf. Theory*, 4(4/5):265–444, 2007.

[5] János Körner and Katalin Marton. How to encode the modulo-two sum of binary sources. *IEEE Trans. Inf. Theory*, 25(2):219–221, 1979.

[6] Bobak Nazer and Michael Gastpar. Computation over multiple-access channels. *IEEE Trans. Inf. Theory*, 53(10):3498–3516, October 2007.

[7] Shigeki Miyake. *Coding theorems for point-to-point communication systems using sparse matrix codes.* PhD thesis, 2010.

[8] A. Padakandla and S. Sandeep Pradhan. Computing sum of sources over an arbitrary multiple access channel. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2144–2148, July 2013.

[9] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. A joint typicality approach to compute–forward. *IEEE Trans. Inf. Theory*, 64(12):7657–7685, Dec 2018.

[10] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. Towards an algebraic network information theory: Simultaneous joint typicality decoding. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 1818–1822, June 2017.

[11] P. Sen and Y.-H. Kim. Homologous codes for multiple access channels. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 874–878, June 2017.

[12] P. Sen and Y.-H. Kim. Homologous codes for multiple access channels. *IEEE Trans. Inf. Theory*, 66(3):1549–1571, 2020.

[13] P. Sen, S. H. Lim, and Y.-H. Kim. Optimal achievable rates for computation with random homologous codes. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2351–2355, June 2018.

[14] P. Sen, S. H. Lim, and Y.-H. Kim. On the optimal achievable rates for linear computation with random homologous codes. accepted to *IEEE Trans. Inf. Theory*, 2020.

[15] N. Karamchandani, U. Niesen, and S. Diggavi. Computation over mismatched channels. *IEEE J. Sel. Areas Commun.*, 31(4):666–677, April 2013.

[16] Katalin Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, 25(3):306–311, 1979.

[17] Y. Birk and T. Kol. Coding on demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients. *IEEE Trans. Inf. Theory*, 52(6):2825–2830, June 2006.

[18] S. Borst, V. Gupta, and A. Walid. Distributed caching algorithms for content distribution networks. In *Proc. 29th Ann. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, pages 1–9, March 2010.

[19] M. A. Maddah-Ali and U. Niesen. Fundamental limits of caching. *IEEE Trans. Inf. Theory*, 60(5):2856–2867, May 2014.

[20] C. Wang, S. H. Lim, and M. Gastpar. Information-theoretic caching: Sequential coding for computing. *IEEE Transactions on Information Theory*, 62(11):6393–6406, Nov 2016.

[21] Chien-Yi Wang. *Function Computation over Networks Efficient Information Processing for Cache and Sensor Applications*. EPFL, Lausanne, 2015.

[22] R. M. Gray and A. D. Wyner. Source coding for a simple network. *Bell Syst. Tech. J.*, 53(9):1681–1721, 1974.

Chapter 2

Homologous Codes

Nested coset codes, recently developed by Padakandla and Pradhan to preserve the linear structure as well as a desired shape on the codewords, is described. Its construction is based on generating a coset code with a rate higher than the target (message) rate and selecting a codeword of a desired property (such as type or joint type) from a subset of codewords (a coset of a subcode). For multiple senders, a family of nested coset codes that is built on the same linear code and referred to as homologous codes is described. With its common structure shared among senders, homologous codes will be the main interest of the subsequent chapters.

2.1 Introduction

Random independently and identically distributed (i.i.d.) code ensembles play a fundamental role in network information theory, with most existing coding schemes built on them; see, for example, [1–3]. As shown by Körner and Marton [4] for the problem of encoding a modulo-two sum of distributed dependent binary sources, using the *same* random ensemble of linear codes at multiple encoders can achieve strictly better rates than using independently generated ensembles of codes. Building on this observation, Nazer and Gastpar [5] developed a channel coding scheme that uses the same random ensemble of lattice codes at multiple encoders and showed that this *structured* coding scheme outperforms conventional random coding schemes for computing a linear combination of the codewords over a linear multiple access channel (MAC), even for independent sources.

More recently, *nested coset codes* [6,7] were proposed as more flexible alternatives for achieving the desired linear structure at multiple encoders. In particular, Padakandla and Pradhan [7] developed a fascinating coding scheme for the computation problem over an *arbitrary* MAC. In this coding scheme, a coset code with a rate higher than the target (message) rate is first generated randomly. Next, in the *shaping* step, a codeword of a desired property (such as type or joint type) is selected from a subset of codewords (a coset of a subcode). Although reminiscent of the multicoding scheme of Gelfand and Pinsker [8] for channels with state, and Marton's coding scheme [9] for broadcast channels, this construction is more fundamental in some sense, since the scheme is directly applicable even for classical point-to-point communication channels. A similar shaping technique was also developed for lattice codes in [10]. For multiple encoders, the desired common structure is obtained by using coset codes with the same generator matrix. Recent efforts exploited the benefit of such constructions for a broader class of channel models, such as interference channels [11, 12], multiple access channels [13, 14], and multiple access channels with state [15].

Motivated by the physical meaning of compute–forward and interference alignment, where a linear combination of codewords is to be utilized at the receiver to cancel out the interferer codewords, Lim, Feng, Pastore, Nazer, and Gastpar [16, 17] tackled codeword computation and generalized the nested coset codes constructed with the same generator matrix to asymmetric rate pairs. We referred to this generalized version, together with the shaping step, as *homologous* codes [13, 14, 18, 19]. This terminology is motivated from its biological definition, i.e., the structures modified from the same ancestry (underlying linear code) to adapt to different purposes (desired shape).

In the first part of this dissertation, particularly in Chapters 3 and 5, we will study the performance of homologous codes for computing a linear combination of codewords and for communicating messages, respectively. As a preliminary step, in this chapter, we describe homologous codes in details starting from nested coset codes.

We adapt the notation in [1, 2]. The set of integers $\{1, 2, \ldots, n\}$ is denoted by $[n]$. For a length-n sequence (vector) $x^n = (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$, we define its type as $\pi(x|x^n) = |\{i \colon x_i = x\}|/n$ for $x \in \mathcal{X}$. Upper case letters $X, Y, \ldots$ denote random variables. For $\epsilon \in (0, 1)$, we define the ϵ-typical set of length-n sequences (or the typical set in short) as $\mathcal{T}_\epsilon^{(n)}(X) = \{x^n \colon |p(x) - \pi(x|x^n)| \le \epsilon p(x),\, x \in \mathcal{X}\}$.

2.2 For Point-to-point Channels

For the ease of exposition, we start with a discrete memoryless channel, i.e., $k = 1$. For the discrete memoryless channel $p(y|x)$, shaping of the channel input distributions via *nested coset* codes was first proposed in [6] and later appeared in [16, 20]. Following a similar notation to these studies, the nested coset codes can be defined as follows.

Definition 2.2.1 (Nested coset codes). *An $(n, nR, n\hat{R}, \mathbb{F}_q)$ nested coset code consists of a message set $\mathbb{F}_q^{nR}$, a generator matrix $\mathsf{G} \in \mathbb{F}_q^{n(R+\hat{R}) \times n}$, a coset sequence d^n, a shaping function $s : \mathbb{F}_q^{nR} \to \mathbb{F}_q^{n\hat{R}}$, an encoder that assigns a codeword to each message according to the steps below.*

1. *For each $m \in \mathbb{F}_q^{nR}$ and $l \in \mathbb{F}_q^{n\hat{R}}$, compute*

$$u^n(m, l) = [m \;\; l]\, \mathsf{G} \oplus d^n. \tag{2.1}$$

2. *For each message $m \in \mathbb{F}_q^{nR}$, choose $x^n(m) = u^n(m, s(m))$ as the assigned codeword, where $s(m)$ is the specified shaping function.*

Remark 2.2.1. *An $(n, nR, \mathbb{F}_q)$* coset code *is a special case of an $(n, nR, n\hat{R}, \mathbb{F}_q)$ nested coset code with $\hat{R} = 0$ (no shaping). Specializing further, we can view an $(n, nR, \mathbb{F}_q)$* linear code *as an $(n, nR, \mathbb{F}_q)$ coset code with $d^n = \mathbf{0}$.*

The encoding steps of nested coset codes can be interpreted as follows. In Step 1), an $(n, n(R+\hat{R}), \mathbb{F}_q)$ coset code, $\mathcal{C}_1$, of rate $R+\hat{R}$ that is larger than the target rate R is created using a generator matrix G, which includes an $(n, nR, \mathbb{F}_q)$ coset code, $\mathcal{C}_2$, generated by the first nR rows of G, as a subcode. Thus, these two coset codes are *nested*, i.e., $\mathcal{C}_2 \subseteq \mathcal{C}_1$. The intentional redundancy in the size of the code $\mathcal{C}_1$ then allows selecting a subset with the desired properties induced by the shaping function in step 2). By the nested construction of $\mathcal{C}_2 \subseteq \mathcal{C}_1$, any selected codeword in $\mathcal{C}_1$ will be in a coset of $\mathcal{C}_2$.

We now continue with a formal description of a *random ensemble* of nested coset codes that are constructed via a random generator matrix G and a random coset sequence D^n to emulate the behavior of a random (nonlinear) code ensemble drawn from a specified probability mass function (pmf) $p(x)$ on $\mathbb{F}_q$ [20]. For $\epsilon \in (0,1)$, we define the ϵ-typical set of length-n sequences (or the typical set in short) as $\mathcal{T}_\epsilon^{(n)}(X) = \{x^n \colon |p(x) - \pi(x|x^n)| \leq \epsilon p(x),\, x \in \mathcal{X}\}$, where type of sequence x^n, $\pi(x|x^n)$, is defined as $\pi(x|x^n) := |\{i \colon x_i = x\}|/n$ for $x \in \mathcal{X}$.

Definition 2.2.2 (Random nested coset codes)**.** *Given a pmf $p(x)$ on $\mathbb{F}_q$ and $\epsilon > 0$, an $(n, nR, n\hat{R}, \mathbb{F}_q; p(x), \epsilon)$ random nested coset code ensemble consists of a message set $\mathbb{F}_q^{nR}$, a* random *generator matrix $G \in \mathbb{F}_q^{(nR+n\hat{R})\times n}$ and a* random *coset sequence D^n with entries i.i.d.* $\mathrm{Unif}(\mathbb{F}_q)$*, an encoder that assigns a codeword to each message $m \in \mathbb{F}_q^{nR}$ according to the steps below.*

1. *Given the realizations G, and d^n, compute $u^n(m,l)$ for each $m \in \mathbb{F}_q^{nR}$ and $l \in \mathbb{F}_q^{n\hat{R}}$ by (2.1).*

2. *For each message $m \in \mathbb{F}_q^{nR}$, choose an $l \in \mathbb{F}_q^{n\hat{R}}$ such that $u^n(m,l) \in \mathcal{T}_\epsilon^{(n)}(X)$. If there are more than one such l, choose one of them at random; if there is none, choose one in $\mathbb{F}_q^{n\hat{R}}$.*[1] *For the chosen l, Let $x^n(m) = u^n(m,l)$ be the assigned codeword for message m.*

[1] This specific shaping function is referred to as the joint typicality encoding in [20]; see [10] for a similar technique in the context of lattice-based source coding.

Remark 2.2.2. *Encoding error is defined as the event of*

$$\mathcal{E} = \{U^n(M,l) \notin \mathcal{T}_\epsilon^{(n)}(X) \text{ for every } l \in \mathbb{F}_q^{n\hat{R}}\}.$$

When the message is uniformly i.i.d. over its alphabet, the probability $\mathsf{P}(\mathcal{E})$ *tends to zero as* $n \to \infty$ *if*

$$\hat{R} \geq D(p_X||\mathrm{Unif}(\mathbb{F}_q)) + \delta(\epsilon),$$

for some $0 < \delta(\epsilon) < \epsilon$*, where* $D(p(x)||q(x))$ *denotes the KL-divergence*

$$D(p(x)||q(x)) := \mathsf{E}_{X\sim p(x)}\left[\log \frac{p(X)}{q(X)}\right].$$

Intuitively, the redundancy in the auxiliary codeword generation in step 1), the amount of which is determined by $\hat{R}$*, provides the existence of a codeword within the typical set* $\mathcal{T}_\epsilon^{(n)}(X)$ *with high probability.*

Similar to the deterministic setting, we can also consider random coset codes and random linear codes.

Remark 2.2.3. *An* $(n, nR, \mathbb{F}_q)$ random coset code *ensemble is a special case of an* $(n, nR, n\hat{R}, \mathbb{F}_q; p(x), \epsilon)$ *random nested coset code ensemble with* $\hat{R} = 0, p(x) = \mathrm{Unif}(\mathbb{F}_q)$ *and* $\epsilon = 0$*. Specializing further, we can view an* $(n, nR, \mathbb{F}_q)$ random linear code *ensemble as an* $(n, nR, \mathbb{F}_q)$ *random coset code ensemble with* $D^n = \mathbf{0}$*.*

As shown in [16,20], random nested coset code ensembles can achieve the capacity of a discrete memoryless channel $p(y|x)$. When the input alphabet $\mathcal{X}$ is not isomorphic to a finite field, the channel can be transformed into a virtual channel $p(y|v)$ with equal capacity via an appropriately chosen auxiliary input V and symbol-by-symbol mapping $X = \varphi(V)$. This result can be extended to the Gaussian channel [16] (via a quantization argument) to be discussed further in Section 5.6.

We next consider nested coset codes that preserve a common structure among different senders.

2.3 For Networks with Multiple Senders

Definition 2.3.1 (Homologous codes)**.** *An* $(n, ((nR_j, n\hat{R}_j) : j \in [k]), \mathbb{F}_q)$ homologous code *is a collection of* $(n, nR_j, n\hat{R}_j, \mathbb{F}_q)$ *nested coset codes,* $j \in [k]$*, and consists of* k *message sets* $\mathbb{F}_q^{nR_j}$*, a common generator matrix* $\mathsf{G} \in \mathbb{F}_q^{\kappa \times n}$ *with* $\kappa = \max_j(nR_j + n\hat{R}_j)$*,* k *coset sequences* d_j^n*,* k *shaping functions* $s_j : \mathbb{F}_q^{nR_j} \to \mathbb{F}_q^{n\hat{R}_j}$*,* k *encoders, where encoder* $j \in [k]$ *assigns a codeword to each message according to the steps below.*

1. *For each* $m_j \in \mathbb{F}_q^{nR_j}$ *and* $l_j \in \mathbb{F}_q^{n\hat{R}_j}$*, compute*[2]

$$u_j^n(m_j, l_j) = [m_j \ l_j \ \mathbf{0}_{\kappa - n(R_j + \hat{R}_j)}]\mathsf{G} \oplus d_j^n. \tag{2.2}$$

2. *For each message* $m_j \in \mathbb{F}_q^{nR_j}$*, choose* $x_j^n(m_j) = u_j^n(m_j, s(m_j))$ *as the assigned codeword, where* $s_j(m_j)$ *is the specified shaping function.*

The term "homologous" was first proposed by the well-known biologist Owen [21] and later adopted by Darwin [22] to characterize the structures that have evolved from the same ancestor but differ in detail. In biological analogy, even though homologous codes are constructed from the same generator matrix, the actual "shape" of the codes can be quite different due to individual shaping functions.

We are particularly interested in the performance of a randomly generated homologous code ensemble, which is defined as follows.

Definition 2.3.2 (Random homologous codes)**.** *Given a pmf* $p = \prod_{j=1}^k p(x_j)$ *over* $\mathbb{F}_q$ *and* $\epsilon > 0$*, an* $(n, ((nR_j, n\hat{R}_j) : j \in [k]), \mathbb{F}_q; p, \epsilon)$ random homologous code *ensemble is a collection of* $(n, nR_j, n\hat{R}_j, \mathbb{F}_q; p(x_j), \epsilon)$ *random nested coset code ensembles,* $j \in [k]$*, and consists of* k *message sets* $\mathbb{F}_q^{nR_j}$*, a common* random *generator matrix* $G \in \mathbb{F}_q^{\kappa \times n}$ *with* $\kappa = \max_j(nR_j + n\hat{R}_j)$ *and* k random *coset sequences* D_j^n *with entries i.i.d.* $\mathrm{Unif}(\mathbb{F}_q)$*,* k *encoders, where encoder* $j \in [k]$ *assigns a codeword to each message according to the steps below, and a decoder that assigns an estimate to each received sequence* y^n*.*

[2] Zero padding in (2.2) is because $nR_j + n\hat{R}_j$ may differ for different j.

1. *Given the realizations* G, *and* d^n, *compute* $u_j^n(m_j, l_j)$ *for each* $m_j \in \mathbb{F}_q^{nR_j}$ *and* $l_j \in \mathbb{F}_q^{n\hat{R}_j}$ *by (2.2).*

2. *For each message* $m_j \in \mathbb{F}_q^{nR_j}$, *choose an* $l_j \in \mathbb{F}_q^{n\hat{R}_j}$ *such that* $u_j^n(m_j, l_j) \in \mathcal{T}_\epsilon^{(n)}(X_j)$. *If there are more than one such* l_j, *choose one of them at random; if there is none, choose one in* $\mathbb{F}_q^{n\hat{R}_j}$. *For the chosen* l_j, *Let* $x_j^n(m_j) = u_j^n(m_j, l_j)$ *be the assigned codeword for message* m_j.

Remark 2.3.1. *In the construction of homologous codes, the codewords of different senders are build from the same underlying linear code and thus a linear combination of codewords is a codeword from a coset of the same underlying linear code. This property benefits linear computation over multiple access channels to be discussed in Chapter 3, where decoder wishes to recover a linear combination of codewords.*

2.4 Discussion

We have described how to construct random ensembles of homologous codes. The underlying linearity shared by multiple encoders benefits linear computation problem, in which a decoder wishes to recover a linear combination of codewords transmitted from multiple encoders. In the next chapter, we will analyze the optimal performance of random ensembles of homologous codes for such a linear computation problem when the decoder applies the optimal maximum likelihood decoding rule.

Acknowledgment

This chapter is, in part, a reprint of the material in the papers: Pinar Sen and Young-Han Kim, "Homologous Codes for Multiple Access Channels," in *IEEE Transactions on Information Theory,* vol. 66, no. 3, pp. 1549-1571, March 2020; and Pinar Sen and Young-Han Kim, "Homologous Codes for Multiple Access Channels," *Proceedings of the IEEE International Symposium on Information Theory*, Aachen, Germany, June

2017. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] Abbas El Gamal and Young-Han Kim. *Network Information Theory*. Cambridge University Press, Cambridge, 2011.

[2] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, New York, second edition, 2006.

[3] Gerhard Kramer. Topics in multi-user information theory. *Found. Trends Comm. Inf. Theory*, 4(4/5):265–444, 2007.

[4] János Körner and Katalin Marton. How to encode the modulo-two sum of binary sources. *IEEE Trans. Inf. Theory*, 25(2):219–221, 1979.

[5] Bobak Nazer and Michael Gastpar. Computation over multiple-access channels. *IEEE Trans. Inf. Theory*, 53(10):3498–3516, October 2007.

[6] Shigeki Miyake. *Coding theorems for point-to-point communication systems using sparse matrix codes*. PhD thesis, 2010.

[7] A. Padakandla and S. Sandeep Pradhan. Computing sum of sources over an arbitrary multiple access channel. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2144–2148, July 2013.

[8] S. I. Gelfand and M. S. Pinsker. Coding for channel with random parameters. *Probl. Control Inf. Theory*, 9(1):19–31, 1980.

[9] Katalin Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, 25(3):306–311, 1979.

[10] T. Gariby and U. Erez. On general lattice quantization noise. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2717–2721, July 2008.

[11] A. Padakandla, A. G. Sahebi, and S. S. Pradhan. A new achievable rate region for the 3-user discrete memoryless interference channel. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2256–2260, July 2012.

[12] A. Padakandla, A. G. Sahebi, and S. S. Pradhan. An achievable rate region for the three-user interference channel based on coset codes. *IEEE Trans. Inf. Theory*, 62(3):1250–1279, March 2016.

[13] P. Sen and Y.-H. Kim. Homologous codes for multiple access channels. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 874–878, June 2017.

[14] P. Sen and Y.-H. Kim. Homologous codes for multiple access channels. *IEEE Trans. Inf. Theory*, 66(3):1549–1571, 2020.

[15] A. Padakandla and S. S. Pradhan. Achievable rate region based on coset codes for multiple access channel with states. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2641–2645, July 2013.

[16] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. A joint typicality approach to compute–forward. *IEEE Trans. Inf. Theory*, 64(12):7657–7685, Dec 2018.

[17] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. Towards an algebraic network information theory: Simultaneous joint typicality decoding. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 1818–1822, June 2017.

[18] P. Sen, S. H. Lim, and Y.-H. Kim. Optimal achievable rates for computation with random homologous codes. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2351–2355, June 2018.

[19] P. Sen, S. H. Lim, and Y.-H. Kim. On the optimal achievable rates for linear computation with random homologous codes. accepted to *IEEE Trans. Inf. Theory*, 2020.

[20] A. Padakandla and S. S. Pradhan. An achievable rate region based on coset codes for multiple access channel with states. *IEEE Trans. Inf. Theory*, 63(10):6393–6415, Oct 2017.

[21] Richard Owen. *Lectures on the Compara- tive Anatomy and Physiology of the Invertebrate Animals.* Longman, Brown, Green, Longmans, London, 1843.

[22] Charles Robert Darwin. *On the Origins of Species.* John Murray, London, 1859.

Chapter 3

Linear Computation Over Multiple Access Channels with Homologous Codes

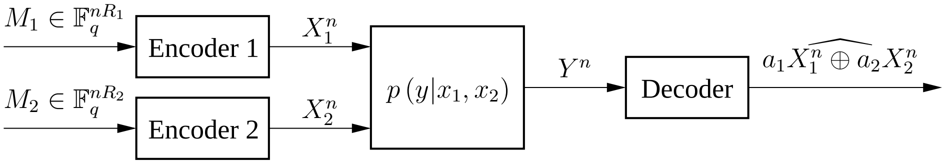
The problem of computing a linear combination of sources over a multiple access channel is studied. Inner and outer bounds on the optimal tradeoff between the communication rates are established when encoding is restricted to random ensembles of *homologous codes*, namely, structured nested coset codes from the same generator matrix and individual shaping functions, but when decoding is optimized with respect to the realization of the encoders. For the special case in which the desired linear combination is "matched" to the structure of the multiple access channel in a natural sense, these inner and outer bounds coincide. This result indicates that most, if not all, coding schemes for computation in the literature that rely on random construction of nested coset codes cannot be improved by using more powerful decoders, such as the maximum likelihood decoder. Generalizing some of the techniques, a single letter outer bound for the capacity region of the computation problem is presented and compared with the inner bound achieved by homologous codes.

3.1 Formal Statement of the Problem

Consider the two-sender finite-field input memoryless multiple access channel (MAC)

$$(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1,x_2), \mathcal{Y})$$

in Figure 3.1, which consists of two sender alphabets $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{F}_q$ for a finite-field $\mathbb{F}_q$, a receiver alphabet $\mathcal{Y}$, and a collection of conditional probability distributions $p_{Y|X_1,X_2}(y|x_1,x_2)$. Each sender $j = 1,2$ encodes a message $M_j \in \mathbb{F}_q^{nR_j}$ into a codeword $X_j^n = x_j^n(M_j) \in \mathbb{F}_q^n$ and transmits X_j^n over the channel. Message M_j is said to be *confusable* if $x_j^n(M_j) = x_j^n(m_j)$ for some $m_j \neq M_j \in \mathbb{F}_q^{nR_j}$. Here and henceforth, we assume without loss of generality that nR_1 and nR_2 are integers. The goal of communication is to convey a linear combination of the codewords. Hence, the receiver finds an estimate $\hat{W}_{\mathbf{a}}^n = \hat{w}_{\mathbf{a}}^n(Y^n) \in \mathbb{F}_q^n$ of



$M_1 \in \mathbb{F}_q^{nR_1}$
Encoder 1
X_1^n
$M_2 \in \mathbb{F}_q^{nR_2}$
Encoder 2
X_2^n
$p\,(y|x_1,x_2)$
Y^n
Decoder
$\widehat{a_1X_1^n \oplus a_2X_2^n}$

Figure 3.1. Linear computation over two-sender multiple access channel.

$$W_{\mathbf{a}}^n := a_1X_1^n \oplus a_2X_2^n$$

for a desired (nonzero) vector $\mathbf{a} = [a_1\ a_2]$ over $\mathbb{F}_q$, where the operator $\oplus$ denotes the q-ary addition. Formally, an (n, nR_1, nR_2) *computation code* for the multiple access channel consists of two encoders that map $x_j^n(m_j)$, $j = 1,2$.

Remark 3.1.1. *For simplicity of presentation, we consider the case $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{F}_q$, but our arguments can be extended to arbitrary $\mathcal{X}_1$ and $\mathcal{X}_2$ through the channel transformation technique by Gallager [1, Sec. 6.2]. More specifically, given a pair of symbol-by-symbol mappings $\varphi_j : \mathbb{F}_q \to \mathcal{X}_j$, $j = 1,2$, consider the* virtual channel *with finite field inputs, $p(y|v_1,v_2) = p_{Y|X_1,X_2}(y|\varphi_1(v_1),\varphi_2(v_2))$, for which a computation code is to be defined. The goal of the communication is to convey $W_{\mathbf{a}} := a_1V_1^n \oplus a_2V_2^n$, where $V_j^n = v_j^n(M_j) \in$*

$\mathbb{F}_q^n$ *is the virtual codeword mapped to message* M_j *at sender* $j = 1, 2$. *Our results can be readily applied to this computation problem defined on the virtual channel.*

The performance of a given computation code $\mathcal{C}_n$ that is paired with a decoding map $\hat{w}_{\mathbf{a}}^n(y^n)$ for a fixed desired vector $\mathbf{a}$ is measured by the average probability of error

$$P_e^{(n)}(\mathcal{C}_n) = \mathsf{P}(\hat{W}_{\mathbf{a}}^n \neq W_{\mathbf{a}}^n | \mathcal{C}_n),$$

when M_1 and M_2 are independent and uniformly distributed. A rate pair (R_1, R_2) is said to be *achievable for* $\mathbf{a}$*-computation* if there exists a sequence of (n, nR_1, nR_2) computation codes along with a decoding map $\hat{w}_{\mathbf{a}}^n(y^n)$ such that

$$\lim_{n\to\infty} P_e^{(n)}(\mathcal{C}_n) = 0$$

and

$$\lim_{n\to\infty} \mathsf{P}(M_j \text{ is confusable}|\mathcal{C}_n) = 0, \quad \forall j \in \{1, 2\} \text{ with } a_j \neq 0. \tag{3.1}$$

Note that without the condition in (3.1), the problem is trivial and an arbitrarily large rate pair is achievable.

We concentrate on the random homologous code ensembles described in Definition 2.3.2 in Chapter 2. Given an input pmf $p = p(x_1)p(x_2)$ on $\mathbb{F}_q \times \mathbb{F}_q$ and parameter $\epsilon > 0$, consider an $(n, nR_1, n\hat{R}_1, nR_2, n\hat{R}_2, \mathbb{F}_q; p, \epsilon)$ random homologous code ensemble with

$$\hat{R}_j = D(p_{X_j}||\text{Unif}(\mathbb{F}_q)) + \epsilon, \text{ for } j = 1, 2, ^1$$

where $D(p_X||\text{Unif}(\mathbb{F}_q))$ denotes the KL-divergence. Since the underlying finite field $\mathbb{F}_q$ and the rates $\hat{R}_1$ and $\hat{R}_2$ are fixed, for the simplicity of the notation, we drop them throughout this chapter and continue with the term of $(n, nR_1, nR_2; p, \epsilon)$ random homologous code ensemble. With a slight abuse of terminology, we refer to the random tuple $\mathcal{C}_n := (G, D_1^n, D_2^n, (L_1(m_1) : m_1 \in \mathbb{F}_q^{nR_1}), (L_2(m_2) : m_2 \in \mathbb{F}_q^{nR_2}))$ as the *random*

[1] Please refer to Remark 2.2.2 in Chapter 2 for the choice of $\hat{R}_j$.

homologous code. Each realization of the random homologous code results in one instance $\{(x_1^n(m_1), x_2^n(m_2)) : (m_1, m_2) \in \mathbb{F}_q^{nR_1} \times \mathbb{F}_q^{nR_2}\}$ of such generated codewords. A rate pair (R_1, R_2) is said to be *achievable for* $\mathbf{a}$*-computation by the* (p, ϵ)*-distributed random homologous code ensemble* if there exits a sequence of $(n, nR_1, nR_2; p, \epsilon)$ random homologous code ensembles along with the optimal decoding map such that

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)] = 0 \tag{3.2}$$

and

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n}[\mathsf{P}(M_j \text{ is confusable}|\mathcal{C}_n)] = 0, \quad \forall j \in \{1, 2\} \text{ with } a_j \neq 0. \tag{3.3}$$

Here the expectations are with respect to the random homologous code $\mathcal{C}_n$, i.e.,

$$(G, D_1^n, D_2^n, (L_1(m_1) : m_1 \in \mathbb{F}_q^{nR_1}), (L_2(m_2) : m_2 \in \mathbb{F}_q^{nR_2})).$$

Given $(p, \epsilon, \mathbf{a})$, let $\mathscr{R}^*(p, \epsilon, \mathbf{a})$ be the set of all rate pairs achievable for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble. Given the input pmf p and the desired vector $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$, the optimal rate region $\mathscr{R}^*(p, \mathbf{a})$, when it exists, is defined as

$$\mathscr{R}^*(p, \mathbf{a}) := \mathrm{cl}\left[\lim_{\epsilon\to 0} \mathscr{R}^*(p, \epsilon, \mathbf{a})\right].$$

Remark 3.1.2. *Given a pmf $p(x)$, its entropy, $H(X)$, is defined by*

$$H(X) := \mathsf{E}\left[\frac{1}{\log p(X)}\right].$$

Instead of (3.3), one may consider alternative notions for the confusability *of the transmitted message, such as*

$$\lim_{n\to\infty} \frac{H(M_j|X_j^n(M_j), \mathcal{C}_n)}{n} = 0, \tag{3.4}$$

or

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n}[\mathsf{P}(G \text{ is rank deficient}|\mathcal{C}_n)] = 0. \tag{3.5}$$

It is easy to show that our results for the optimal rate region $\mathscr{R}^*(p, \mathbf{a})$ under (3.3) still apply if we change the confusability notion with (3.4) or (3.5).

3.2 Main Result

In this section, we present a single-letter characterization of the optimal rate region when the target linear combination is in the following class.

Definition 3.2.1. *A linear combination $W_{\mathbf{a}} = a_1X_1 \oplus a_2X_2$ for some $\mathbf{a} = [a_1\ a_2] \in \mathbb{F}_q^2 \setminus \{\mathbf{0}\}$ is said to be* natural *if*

$$H(W_{\mathbf{a}}|Y) = \min_{\mathbf{b}\neq\mathbf{0}} H(W_{\mathbf{b}}|Y), \tag{3.6}$$

where $\mathbf{b} = [b_1\ b_2]$ and $W_{\mathbf{b}} = b_1X_1 \oplus b_2X_2$ are over $\mathbb{F}_q$.

In words, a natural combination $W_{\mathbf{a}}$ is the easiest to recover at the receiver and thus, in some sense, is the best linear combination that is matched to the channel structure.

We are now ready to present the optimal rate region for computing natural linear combinations.

Theorem 3.2.1. *Given an input pmf $p = p(x_1)p(x_2)$ and a vector $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$ such that $W_{\mathbf{a}}$ is a natural combination, the optimal rate region $\mathscr{R}^*(p, \mathbf{a})$ is the set of rate pairs (R_1, R_2) such that*

$$R_j \leq I(X_j; Y|X_{j^c}), \tag{3.7a}$$

$$R_j \leq I(X_1, X_2; Y) - \min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} \tag{3.7b}$$

for every $j \in \{1,2\}$ *with* $a_j \neq 0$*, where* $j^c = \{1,2\} \setminus \{j\}$*.*[2]

The rate region in (3.7) in Theorem 3.2.1, which we will denote as $\mathscr{R}^{**}(p, \mathbf{a})$, can be equivalently characterized in terms of well-known rate regions for compute–forward and message communication. Let $\mathscr{R}_{\mathrm{CF}}(p, \mathbf{a})$ be the set of rate pairs (R_1, R_2) such that

$$R_j \leq H(X_j) - H(W_{\mathbf{a}}|Y), \quad \forall j \in \{1,2\} \text{ with } a_j \neq 0. \tag{3.8}$$

Let $\mathscr{R}_{\mathrm{MAC}}(p)$ be the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y|X_2), \tag{3.9}$$

$$R_2 \leq I(X_2; Y|X_1), \tag{3.10}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y). \tag{3.11}$$

Proposition 3.2.1. *For any input pmf* $p = p(x_1)p(x_2)$ *and any linear combination* $W_{\mathbf{a}}$*,*

$$\mathscr{R}^{**}(p, \mathbf{a}) = \mathscr{R}_{\mathrm{CF}}(p, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p).$$

The proof of Proposition 3.2.1 is relegated to Appendix 3.A.

We prove Theorem 3.2.1 in three steps: 1) we first present a general (not necessarily for natural combinations) inner bound on the optimal rate region in Section 3.3, where we follow the results in [2,3] that studied the rate region achievable by random homologous code ensembles using a suboptimal joint typicality decoding rule, 2) we then show by Lemma 3.3.1 in Section 3.3 that this inner bound is equivalent to $\mathscr{R}^{**}(p, \mathbf{a})$ in Proposition 3.2.1 if $W_{\mathbf{a}}$ is a natural combination, and 3) we present a general (not necessarily for natural combinations) outer bound on the optimal rate region in Section 3.4 by showing that if a rate pair (R_1, R_2) is achievable for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble for arbitrarily small ϵ, then (R_1, R_2)

[2] Mutual information $I(X;Y) := D(p(x,y)||p(x)p(y))$ and conditional mutual information $I(X;Y|Z) := \mathsf{E}_Z[D(p(x,y|z)||p(x|z)p(y|z))]$, where $D(\cdot||\cdot)$ denotes the KL divergence.

must lie in $\mathscr{R}^{**}(p, \mathbf{a})$ in Theorem 3.2.1.

Remark 3.2.1. *Due to the underlying linearity shared between different users' code, the computation problem defined in Section 3.1 is closely related to the* message computation. *Indeed, one may redefine the computation problem over messages where the goal of transmission is to convey a linear combination $a_1 M_1 \oplus a_2 M_2$ of messages for $R_1 = R_2$ and redefine the achievability for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble and optimal symmetric rate $R^*(p, \mathbf{a})$ in a similar manner but based on condition (3.2) only, then $R^*(p, \mathbf{a})$ is equal to the largest symmetric rate satisfying (3.7) in Theorem 3.2.1. The achievability simply follows from the inner bound in Section 3.3. To see this, note that a linear combination of codewords is of the form*

$$\begin{aligned} &a_1 X_1^n(M_1) \oplus a_2 X_2^n(M_2) \\ &\qquad = \big(a_1[M_1\ L_1\ \mathbf{0}_{\kappa - n(R_1 + \hat{R}_1)}] \oplus a_2[M_2\ L_1\ \mathbf{0}_{\kappa - n(R_2 + \hat{R}_2)}]\big) G \oplus a_1 D_1^n \oplus a_2 D_2^n. \end{aligned}$$

Since the generator matrix G is full rank almost surely as $n \to \infty$ by Lemma 3.B.1 under the rate constraints in Theorem 3.2.1, $\big(a_1[M_1\ L_1\ \mathbf{0}] \oplus a_2[M_2\ L_1\ \mathbf{0}]\big)$ can be recovered from $a_1 X_1^n(M_1, L_1) \oplus a_2 X_2^n(M_2, L_2)$ almost surely. When $R_1 = R_2 = R$, the first nR bits of $\big(a_1[M_1\ L_1\ \mathbf{0}] \oplus a_2[M_2\ L_1\ \mathbf{0}]\big)$ would give $a_1 M_1 \oplus a_2 M_2$ as desired. To prove the optimality, an outer bound can be obtained by following similar steps with Section 3.4.

3.3 An Inner Bound

The computation performance of random homologous code ensembles was studied using a suboptimal *joint typicality* decoder in [2, 3]. For completeness, we first describe the joint typicality decoding rule and then characterize the rate region achievable for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble *under this joint typicality decoding rule.* We then concentrate on an arbitrarily small ϵ to provide an inner bound on the optimal rate region $\mathscr{R}^*(p, \mathbf{a})$. We will omit the steps that were already established in [2,3] and instead provide detailed references.

Upon receiving y^n, the ϵ'-joint typicality decoder, $\epsilon' > 0$, looks for a unique vector $s \in \mathbb{F}_q^\kappa$ such that

$$s = a_1[m_1 \; l_1 \; \mathbf{0}_{\kappa-n(R_1+\hat{R}_1)}] \oplus a_2[m_2 \; l_2 \; \mathbf{0}_{\kappa-n(R_2+\hat{R}_2)}],$$

for some $(m_1, l_1, m_2, l_2) \in \mathbb{F}_q^{nR_1} \times \mathbb{F}_q^{n\hat{R}_1} \times \mathbb{F}_q^{nR_2} \times \mathbb{F}_q^{n\hat{R}_2}$ that satisfies

$$(u_1^n(m_1, l_1), u_2^n(m_2, l_2), y^n) \in \mathcal{T}_{\epsilon'}^{(n)}(X_1, X_2, Y),$$

where $u_j^n(m_j, l_j) = [m_j \; l_j \; \mathbf{0}_{\kappa-n(R_j+\hat{R}_j)}]\mathsf{G} \oplus d_j^n$ is the auxiliary codeword defined in step 2) of the code construction in Definition 2.3.2. If the decoder finds such s, then it declares $\hat{w}_{\mathbf{a}}^n = s\mathsf{G} \oplus a_1 d_1^n \oplus a_2 d_2^n$ as an estimate; otherwise, it declares an error.

To describe the performance of the joint typicality decoder, we define $\mathscr{R}_{\mathrm{CF}}(p, \delta, \mathbf{a})$ for a given input pmf p, $\delta \geq 0$, and nonzero vector $\mathbf{a} \in \mathbb{F}_q^2$ as the set of rate pairs (R_1, R_2) such that

$$R_j \leq H(X_j) - H(W_{\mathbf{a}}|Y) - \delta, \quad \forall j \in \{1,2\} \text{ with } a_j \neq 0.$$

Similarly, we define $\mathscr{R}_1(p, \delta)$ as the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y|X_2) - \delta, \tag{3.12a}$$

$$R_2 \leq I(X_2; Y|X_1) - \delta, \tag{3.12b}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) - \delta, \tag{3.12c}$$

$$R_1 \leq I(X_1, X_2; Y) - H(X_2) + \min_{b_1, b_2 \in \mathbb{F}_q^*} H(W_{\mathbf{b}}|Y) - \delta, \tag{3.12d}$$

and $\mathscr{R}_2(p, \delta)$ as the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y|X_2) - \delta, \tag{3.13a}$$

$$R_2 \leq I(X_2; Y|X_1) - \delta, \tag{3.13b}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) - \delta, \tag{3.13c}$$

$$R_2 \leq I(X_1, X_2; Y) - H(X_1) + \min_{b_1, b_2 \in \mathbb{F}_q^*} H(W_{\mathbf{b}}|Y) - \delta, \tag{3.13d}$$

where $\mathbf{b} = [b_1 \; b_2]$ and $W_{\mathbf{b}} = b_1 X_1 \oplus b_2 X_2$ are over $\mathbb{F}_q$. Note that the region $\mathscr{R}_{\text{CF}}(p, \mathbf{a}) = \mathscr{R}_{\text{CF}}(p, \delta = 0, \mathbf{a})$, as defined in (3.8) in Section 5.3. Similarly, let $\mathscr{R}_j(p)$ denote the region $\mathscr{R}_j(p, \delta = 0)$ for $j = 1, 2$ in (3.12) and (3.13).

We are now ready to state the rate region achievable by the random homologous code ensembles that combines the inner bounds in [3, Theorem 1] and [2, Corollary 1].

Theorem 3.3.1. *Let $p = p(x_1)p(x_2)$ be an input pmf, $\delta > 0$, and $\mathbf{a} \in \mathbb{F}_q^2$ be a nonzero vector. Then, there exists $\epsilon' < \delta$ such that for every $\epsilon < \epsilon'$ sufficiently small, a rate pair*

$$(R_1, R_2) \in \mathscr{R}_{CF}(p, \delta, \mathbf{a}) \cup \mathscr{R}_1(p, \delta) \cup \mathscr{R}_2(p, \delta) \tag{3.14}$$

is achievable for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble along with the ϵ'-joint typicality decoder. In particular,

$$[\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p)] \subseteq \mathscr{R}^*(p, \mathbf{a}). \tag{3.15}$$

Proof. The proof of [3, Theorem 1] analyzes the average probability of error for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble paired with the ϵ'-joint typicality decoder for $\epsilon' > \epsilon > 0$. Two upper bounds on the average probability of error were given. The first one, direct decoding bound, captures the error event that incorrect linear combinations are confused with the correct one and shows that for sufficiently small $\epsilon < \epsilon' < \delta$, the average probability of error tends to zero as $n \to \infty$ if

$$(R_1, R_2) \in \mathscr{R}_{CF}(p, \delta, \mathbf{a}). \tag{3.16}$$

The second one, multiple access bound, captures the error event that incorrect message pairs (codeword pairs) are confused with the correct one. This bound was later improved in the proof of [2, Corollary 1]. The improved version shows that for every $\mathbf{a} \in \mathbb{F}_q^2$, the average probability of error for $\mathbf{a}$-computation tends to zero as $n \to \infty$ if

$$(R_1, R_2) \in \mathscr{R}_1(p, \delta) \cup \mathscr{R}_2(p, \delta). \tag{3.17}$$

Combining (3.16) and (3.17) establishes (3.14).

We still need to show that the condition in (3.3) holds. Suppose that $a_j \neq 0$. For a given code $\mathcal{C}_n$, let G_j denote the submatrix that consists of the first $(nR_j + n\hat{R}_j)$ rows of G within $\mathcal{C}_n$ and $s_j(\mathsf{G})$ be the indicator variable such that $s_j = 1$ if G_j is full rank. Then,

$$\begin{aligned}
\mathsf{E}_{\mathcal{C}_n}[\mathsf{P}(M_j \text{ is confusable}|\mathcal{C}_n)] &= \sum_{\mathcal{C}_n} \mathsf{P}(\mathcal{C}_n = \mathcal{C}_n)\, \mathsf{P}(M_j \text{ is confusable}|\mathcal{C}_n = \mathcal{C}_n) \\
&= \sum_{\substack{\mathcal{C}_n: \\ s_j(\mathsf{G})=0}} \mathsf{P}(\mathcal{C}_n = \mathcal{C}_n)\, \mathsf{P}(M_j \text{ is confusable}|\mathcal{C}_n = \mathcal{C}_n) \\
&\leq \sum_{\substack{\mathcal{C}_n: \\ s_j(\mathsf{G})=0}} \mathsf{P}(\mathcal{C}_n = \mathcal{C}_n) \\
&= \mathsf{P}(S_j(G) = 0).
\end{aligned}$$

Now, by Lemma 3.B.1 in Appendix 3.B (with $R \leftarrow R_j + \hat{R}_j$), the term $\mathsf{P}(S_j(G) = 0)$ tends to zero as $n \to \infty$ if $R_j + \hat{R}_j < 1$. By definition, $\hat{R}_j = D(p_{X_j} \| \mathrm{Unif}(\mathbb{F}_q)) + \epsilon$, which reduces the constraint to the form of $R_j < H(X_j) - \epsilon$. Since this condition is satisfied if (3.14) holds, the proof of (3.14) follows.

The proof of (3.15) follows by taking the closure of the union of (3.14) over all $\delta > 0$, which completes the proof of Theorem 3.2.1. □

The inner bound (3.15) in Theorem 3.2.1 is valid for computing an arbitrary linear combination, which may not be equal to the rate region $\mathscr{R}^{**}(p, \mathbf{a})$ in Theorem 3.2.1 for every $\mathbf{a} \in \mathbb{F}_q^2$, in general. For computing a *natural* linear combination, however, the following lemma shows that the equivalent rate region in Proposition 3.2.1 is achievable.

Lemma 3.3.1. *If the desired linear combination $W_{\mathbf{a}} = a_1X_1 \oplus a_2X_2$ for $(a_1, a_2) \neq (0, 0)$ is natural, then*

$$[\mathscr{R}_{\mathrm{CF}}(p, \mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p)] = [\mathscr{R}_{\mathrm{CF}}(p, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p)].$$

The proof of Lemma 3.3.1 is relegated to Appendix 3.C.

3.4 An Outer Bound

We first present an outer bound on the rate region $\mathscr{R}^*(p, \epsilon, \mathbf{a})$ for a fixed input pmf p, $\epsilon > 0$, and nonzero vector $\mathbf{a} \in \mathbb{F}_q^2$. We then discuss the limit of this outer bound as $\epsilon \to 0$ to establish an outer bound on the rate region $\mathscr{R}^*(p, \mathbf{a})$. Given an input pmf p, $\delta > 0$, and nonzero vector $\mathbf{a} \in \mathbb{F}_q^2$, we define the rate region $\mathscr{R}^{**}(p, \delta, \mathbf{a})$ as the set of rate pairs (R_1, R_2) such that

$$R_j \leq I(X_j; Y | X_{j^c}) + \delta, \tag{3.18a}$$

$$R_j \leq I(X_1, X_2; Y) - \min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} + \delta, \tag{3.18b}$$

for every $j \in \{1, 2\}$ with $a_j \neq 0$, where $j^c = \{1, 2\} \setminus \{j\}$. Note that $\mathscr{R}^{**}(p, \delta = 0, \mathbf{a})$ is equal to $\mathscr{R}^{**}(p, \mathbf{a})$ as defined in (3.7).

We are now ready to state the outer bound on the optimal rate region for computing an *arbitrary* linear combination, which is also an outer bound on $\mathscr{R}^*(p, \mathbf{a})$ in Theorem 3.2.1 for computing a *natural* combination.

Theorem 3.4.1. *Let $p = p(x_1)p(x_2)$ be an input pmf, $\epsilon > 0$, and $\mathbf{a} \in \mathbb{F}_q^2$ be a nonzero vector. If a rate pair (R_1, R_2) is achievable for $\mathbf{a}$-computation by the (p, ϵ)-distributed random homologous code ensemble, then there exists a continuous $\delta'(\epsilon)$ that tends to zero monotonically as $\epsilon \to 0$ such that*

$$(R_1, R_2) \in \mathscr{R}^{**}(p, \delta'(\epsilon), \mathbf{a}). \tag{3.19}$$

In particular,

$$\mathscr{R}^*(p, \mathbf{a}) \subseteq \mathscr{R}^{**}(p, \mathbf{a}). \tag{3.20}$$

Proof. We first start with an averaged version of Fano's inequality for a random homologous code ensemble $\mathcal{C}_n$ (recall the notation in Section 3.1).

Lemma 3.4.1. *If*

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)] = 0$$

and

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n}[\mathsf{P}(M_j \textit{ is confusable}|\mathcal{C}_n)] = 0 \tag{3.21}$$

for every $j \in \{1,2\}$ with $a_j \neq 0$, then for every $j \in \{1,2\}$ with $a_j \neq 0$

$$H(M_j|Y^n, M_{j^c}, \mathcal{C}_n) \leq n\epsilon_n$$

for some $\epsilon_n \to 0$ as $n \to \infty$.

The proof of Lemma 3.4.1 is relegated to Appendix 3.D.

We next define the indicator random variable

$$E_n = \mathbb{1}_{\{(X_1^n(M_1), X_2^n(M_2)) \in \mathcal{T}_{\epsilon'}^{(n)}(X_1, X_2)\}} \tag{3.22}$$

for $\epsilon' > 0$. Since $\hat{R}_i = D(p_{X_i} \| \mathrm{Unif}(\mathbb{F}_q)) + \epsilon$, $i = 1, 2$, by the Markov lemma [3, Lemma 12] for homologous codes, $\mathsf{P}(E_n = 0)$ tends to zero as $n \to \infty$ if ϵ' is sufficiently large compared to ϵ. Let $\epsilon' = \delta_1(\epsilon)$, which still tends to zero as $\epsilon \to 0$. Suppose that $a_j \neq 0$. Then, for n sufficiently large,

$$\begin{aligned} nR_j &= H(M_j|M_{j^c}, \mathcal{C}_n) \\ &\overset{(a)}{\leq} I(M_j; Y^n|M_{j^c}, \mathcal{C}_n) + n\epsilon_n \\ &\leq I(M_j, E_n; Y^n|M_{j^c}, \mathcal{C}_n) + n\epsilon_n \end{aligned}$$

$$
\begin{aligned}
&\overset{(b)}{\leq} \log_q 2 + I(M_j; Y^n | M_{j^c}, \mathcal{C}_n, E_n) + n\epsilon_n \\
&\leq \log_q 2 + I(M_j; Y^n | M_{j^c}, \mathcal{C}_n, E_n = 0)\, \mathsf{P}(E_n = 0) \\
&\qquad\qquad + I(M_j; Y^n | M_{j^c}, \mathcal{C}_n, E = 1)\, \mathsf{P}(E_n = 1) + n\epsilon_n \qquad (3.23) \\
&\leq \log_q 2 + nR_j\, \mathsf{P}(E_n = 0) + I(M_j; Y^n | M_{j^c}, \mathcal{C}_n, E_n = 1) + n\epsilon_n \\
&= \log_q 2 + nR_j\, \mathsf{P}(E_n = 0) + \sum_{i=1}^{n} I(M_j; Y_i | Y^{i-1}, M_{j^c}, \mathcal{C}_n, X_{j^c i}, E_n = 1) + n\epsilon_n \\
&\leq \log_q 2 + nR_j\, \mathsf{P}(E_n = 0) + \sum_{i=1}^{n} I(M_j, X_{ji}, Y^{i-1}, M_{j^c}, \mathcal{C}_n; Y_i | X_{j^c i}, E_n = 1) + n\epsilon_n \\
&\overset{(c)}{=} \log_q 2 + nR_j\, \mathsf{P}(E_n = 0) + \sum_{i=1}^{n} I(X_{ji}; Y_i | X_{j^c i}, E_n = 1) + n\epsilon_n, \qquad (3.24)
\end{aligned}
$$

where (a) follows by Lemma 3.4.1, (b) follows since E_n is a binary random variable, and (c) follows since $(M_1, M_2, Y^{i-1}, \mathcal{C}_n, E_n) \to (X_{1i}, X_{2i}) \to Y_i$ form a Markov chain for every $i \in [n]$. To further upper bound (3.24), we make a connection between the distribution of the random homologous code and the input pmf p as follows.

Lemma 3.4.2. *Let $(X_1, X_2, Y) \sim p(x_1)p(x_2)p(y|x_1, x_2)$ on $\mathbb{F}_q \times \mathbb{F}_q \times \mathcal{Y}$ and $\epsilon, \epsilon' > 0$. Let $(X_1^n(m_1), X_2^n(m_2))$ be the random codeword pair assigned to message pair $(m_1, m_2) \in \mathbb{F}_q^{nR_1} \times \mathbb{F}_q^{nR_2}$ by an $(n, nR_1, nR_2; p, \epsilon)$ random homologous code ensemble, where $p = p(x_1)p(x_2)$ is the input pmf. Further let Y^n be a random sequence distributed according to $\prod_{i=1}^n p_{Y|X_1,X_2}(y_i|x_{1i}, x_{2i})$. Then, for every $(x_1, x_2, y) \in \mathbb{F}_q \times \mathbb{F}_q \times \mathcal{Y}$ and for every $i = 1, 2, \ldots, n$,*

$$
\begin{aligned}
(1-\epsilon')p(x_1, x_2, y) &\leq P(X_{1i} = x_1, X_{2i} = x_2, Y_i = y | (X_1^n, X_2^n) \in \mathcal{T}_{\epsilon'}^{(n)}(X_1, X_2)) \\
&\leq (1+\epsilon')p(x_1, x_2, y).
\end{aligned}
$$

The proof of Lemma 3.4.2 is relegated to Appendix 3.E.

Back to the proof of Theorem 3.4.1, we are now ready to establish (3.18a). By Lemma 3.4.2, each term $I(X_{ji}; Y_i | X_{j^c i}, E_n = 1)$ is close to $I(X_j; Y | X_{j^c})$ upto a function of ϵ' that vanishes as $\epsilon' \to 0$. Therefore, combining (3.24) with Lemma 3.4.2, we have

$$\begin{aligned} nR_j &\le \log_q 2 + nR_j \,\mathsf{P}(E_n = 0) + n(I(X_j; Y | X_{j^c}) + \delta_2(\epsilon')) + n\epsilon_n \\ &\overset{(d)}{\le} n(I(X_j; Y | X_{j^c}) + \delta_2(\epsilon')) + 2n\epsilon_n \\ &\overset{(e)}{\le} n(I(X_j; Y | X_{j^c}) + \delta_3(\epsilon)) + 2n\epsilon_n, \end{aligned} \tag{3.25}$$

where (d) follows since $\mathsf{P}(E_n = 0)$ tends to zero as $n \to \infty$ and (e) follows since $\epsilon' = \delta_1(\epsilon)$.

For the proof of (3.18b), we start with

$$\begin{aligned} nR_j &= H(M_j | M_{j^c}, \mathcal{C}_n) \\ &\overset{(a)}{\le} I(M_j; Y^n | M_{j^c}, \mathcal{C}_n) + n\epsilon_n \\ &= I(M_1, M_2; Y^n | \mathcal{C}_n) - I(M_{j^c}; Y^n | \mathcal{C}_n) + n\epsilon_n, \end{aligned} \tag{3.26}$$

where (a) follows by Lemma 3.4.1. Following arguments similar to (3.25), the first term in (3.26) can be bounded as

$$\begin{aligned} &I(M_1, M_2; Y^n | \mathcal{C}_n) \\ &\quad\le \log_q 2 + n(R_1 + R_2) \,\mathsf{P}(E_n = 0) + \sum_{i=1}^{n} I(M_1, M_2; Y_i | \mathcal{C}_n, Y^{i-1}, E_n = 1) \\ &\quad\le n\epsilon_n + \sum_{i=1}^{n} I(M_1, M_2, \mathcal{C}_n, Y^{i-1}; Y_i | E_n = 1) \\ &\quad= n\epsilon_n + \sum_{i=1}^{n} I(M_1, M_2, \mathcal{C}_n, Y^{i-1}, X_{1i}, X_{2i}; Y_i | E_n = 1) \\ &\quad= n\epsilon_n + \sum_{i=1}^{n} I(X_{1i}, X_{2i}; Y_i | E_n = 1) \\ &\quad\le n\epsilon_n + n(I(X_1, X_2; Y) + \delta_4(\epsilon)). \end{aligned} \tag{3.27}$$

To bound the second term in (3.26), we need the following lemma, which is proved in Appendix 3.F.

Lemma 3.4.3. *For every $\epsilon'' > \epsilon'$ and for n sufficiently large,*

$$I(M_{j^c}; Y^n | \mathcal{C}_n) \geq n[\min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} - \delta_5(\epsilon'')] - n\epsilon_n.$$

Combining (3.26), (3.27), and Lemma 3.4.3 with $\epsilon'' = 2\delta_1(\epsilon)$, we have

$$nR_j \leq n(I(X_1, X_2; Y) + \delta_4(\epsilon)) - n[\min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} - \delta_6(\epsilon)] + 2n\epsilon_n \tag{3.28}$$

for n sufficiently large. Letting $n \to \infty$ in (3.25) and (3.28) establishes

$$\begin{aligned} R_j &\leq I(X_j; Y | X_{j^c}) + \delta_3(\epsilon), \\ R_j &\leq I(X_1, X_2; Y) - \min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} + \delta_7(\epsilon). \end{aligned}$$

The proof of (3.19) follows by taking a continuous monotonic function

$$\delta'(\epsilon) \geq \max\{\delta_3(\epsilon), \delta_7(\epsilon)\}$$

that tends to zero as $\epsilon \to 0$. Letting $\epsilon \to 0$ in (3.19) establishes (3.20), which completes the proof of Theorem 3.4.1. □

The arguments used in the proof of (3.18a) starting from Fano's inequality can be generalized for a fixed (n, nR_1, nR_2) computation code to provide a general outer bound on the achievable rate pairs for **a**-computation. It seems, however, difficult to generalize the arguments used in the proof of (3.18b). In particular, it is unclear whether Lemma 3.4.3 can be generalized to a fixed computation code. In Section 3.6, we present a single letter outer bound on the achievable rate pairs for **a**-computation and compare that with the inner bound implied by Theorem 3.3.1. Before our discussion on a general outer bound, we next present the optimal rate region achievable by conventional unstructured random coding arguments for the linear computation problem.

3.5 An Achievable Rate Region for Linear Computation with Conventional Random Codes

We now concentrate on conventional random i.i.d. code ensembles for the linear computation problem illustrated in Figure 3.1. Given an input pmf $p = p(x_1)p(x_2)$ on $\mathbb{F}_q \times \mathbb{F}_q$, an $(n, nR_1, nR_2; p)$ *random i.i.d. code ensemble* consists of two message sets $\mathbb{F}_q^{nR_1}$ and $\mathbb{F}_q^{nR_2}$, two encoders where encoder $j = 1, 2$ assigns randomly generated codewords $X_j^n(m_j)$ that are drawn i.i.d. from $\prod_{i=1}^n p_{X_j}(x_{ji})$ to each message $m_j \in \mathbb{F}_q^{nR_j}$. Similar to section 3.1, we refer to the random tuple $\mathcal{C}_n^{\text{IID}} := ((X_1(m_1), X_2^n(m_2)) : m_1 \in \mathbb{F}_q^{nR_1}), m_2 \in \mathbb{F}_q^{nR_2}))$ as the *random i.i.d. code.* Each realization of the random i.i.d. code results in one instance $\{(x_1^n(m_1), x_2^n(m_2)) : (m_1, m_2) \in \mathbb{F}_q^{nR_1} \times \mathbb{F}_q^{nR_2}\}$ of such generated codewords. A rate pair (R_1, R_2) is said to be *achievable for* $\mathbf{a}$*-computation by the p-distributed random i.i.d. code ensemble* if there exits a sequence of $(n, nR_1, nR_2; p)$ random i.i.d. code ensembles along with the optimal decoding map such that

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n^{\text{IID}}}[P_e^{(n)}(\mathcal{C}_n^{\text{IID}})] = 0 \tag{3.29}$$

and

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n^{\text{IID}}}[\mathsf{P}(M_j \text{ is confusable}|\mathcal{C}_n^{\text{IID}})] = 0, \quad \forall j \in \{1,2\} \text{ with } a_j \neq 0. \tag{3.30}$$

Here the expectations are with respect to the random i.i.d. code $\mathcal{C}_n^{\text{IID}}$.

Given a pmf $p = p(x_1)p(x_2)$ and vector $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$, define the rate region $\mathscr{R}_{\text{TIN}}(p, \mathbf{a})$ as the set of rate pairs (R_1, R_2) such that

$$R_j \leq I(X_j; Y), \quad \forall j \in \{1,2\} \text{ with } a_j \neq 0. \tag{3.31}$$

We are now ready to present an achievable rate region by random i.i.d. code ensembles, the proof of which simply follows from standard arguments by first estimating the message M_j for all $j \in \{1, 2\}$ with $a_j \neq 0$ and then computing the desired linear combination of codewords.

Proposition 3.5.1 (i.i.d. codes for computation)**.** *Given an input pmf* $p = p(x_1)p(x_2)$ *and a vector* $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$*, a rate pair* (R_1, R_2) *is achievable by random i.i.d. code ensembles if*

$$(R_1, R_2) \in [\mathscr{R}_{TIN}(p, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p)].$$

Note that the achievable rate region in Proposition 3.5.1 is included in the optimal rate region in Theorem 3.2.1 that is achievable by random homologous codes when the channel is matched to the desired linear combination.

3.6 Discussion on the Capacity Region of the Linear Computation Problem

For the linear computation problem, the outer bound on the optimal rate region presented in Section 3.4 is valid for *any* computation, not only for natural computation. The inner bound presented in Theorem 3.3.1, however, matches with this outer bound only for *natural* computation. It is an interesting but difficult problem to characterize the optimal rate region for an arbitrary linear computation problem. At this point, it is unclear whether it is the inner or the outer bound that is loose. The extension of the results in this paper to more than two senders is also a challenging question.

A more fundamental question is to establish a general outer bound on the *capacity region* of the linear computation problem. The following presents an outer bound on the rate pairs (R_1, R_2) that is achievable for $\mathbf{a}$-computation. The proof is deferred to Appendix 3.G.

Proposition 3.6.1 (A general outer bound)**.** *Given a vector* $\mathbf{a} = [a_1\ a_2] \in \mathbb{F}_q^2$ *with*

$a_1, a_2 \neq 0$, if a rate pair (R_1, R_2) is achievable for **a***-computation, then it must satisfy*

$$R_1 \leq \min\{I(X_1; Y|X_2, Q), I(X_1, X_2; Y|Q) - I(X_2; W_{\mathbf{a}}, Y|T, Q)\}, \tag{3.32a}$$

$$R_2 \leq \min\{I(X_2; Y|X_1, Q), I(X_1, X_2; Y|Q) - I(X_1; W_{\mathbf{a}}, Y|T, Q)\}, \tag{3.32b}$$

$$\begin{aligned} R_1 + R_2 \leq\ & I(X_1, X_2; Y|Q) + I(X_1, X_2; W_{\mathbf{a}}, Y|T, Q) \\ & - I(X_1; W_{\mathbf{a}}, Y|T, Q) - I(X_2; W_{\mathbf{a}}, Y|T, Q), \end{aligned} \tag{3.32c}$$

for some $p(q)p(x_1|q)p(x_2|q)p(t|x_1, x_2, q)$ such that

$$(T, Q) \to (X_1, X_2) \to W_{\mathbf{a}}$$

and

$$(T, Q, W_{\mathbf{a}}) \to (X_1, X_2) \to Y$$

each form a Markov chain, and

$$I(X_1; W_{\mathbf{a}}, Y|T, Q) + I(X_2; W_{\mathbf{a}}, Y|T, Q) \leq I(X_1, X_2; W_{\mathbf{a}}, Y|T, Q). \tag{3.33}$$

Note that (3.33) is equivalent to

$$I(X_1; X_2|T, Q) \leq I(X_1; X_2|W_{\mathbf{a}}, Y, T, Q),$$

which is a variation of dependence-balance condition reminiscent from two-way channels [4].

We next take a closer look at the achievability. First, note that by Theorem 3.3.1, there exists a sequence of (fixed) (n, nR_1, nR_2) computation codes that have vanishing error probability and satisfy (3.1) if

$$(R_1, R_2) \in \mathscr{R}_{\text{CF}}(p, \mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p)$$

for some input pmf $p = p(x_1)p(x_2)$. We now convexify this achievable rate region to get the following general inner bound on the capacity region for $\mathbf{a}$-computation.

Proposition 3.6.2 (A general inner bound)**.** *Given a vector* $\mathbf{a} = [a_1\ a_2] \in \mathbb{F}_q^2$ *with* $a_1, a_2 \neq 0$*, a rate pair* (R_1, R_2) *is achievable for* $\mathbf{a}$*-computation if*

$$R_1 \leq \min\{I(X_1;Y|X_2,Q), I(X_1,X_2;Y|Q) - I(X_2;W_{\mathbf{a}},Y|T,Q)\}, \tag{3.34a}$$

$$R_2 \leq \min\{I(X_2;Y|X_1,Q), I(X_1,X_2;Y|Q) - I(X_1;W_{\mathbf{a}},Y|T,Q)\}, \tag{3.34b}$$

$$\begin{aligned} R_1 + R_2 \leq{}& I(X_1,X_2;Y|Q) + I(X_1,X_2;W_{\mathbf{a}},Y|T,Q) \\ &- I(X_1;W_{\mathbf{a}},Y|T,Q) - I(X_2;W_{\mathbf{a}},Y|T,Q), \end{aligned} \tag{3.34c}$$

for some $p(q)p(x_1|q)p(x_2|q)p(t|x_1,x_2,q)$ *such that*

$$T|x_1,x_2,q \sim \begin{cases} (x_1,x_2) & \textit{with probability } \beta \\ \emptyset & \textit{with probability } 1-\beta \end{cases}$$

for some $\beta \in [0,1]$.

Proof. Taking the convex hull of the rate region in Theorem 3.3.1, we know that the rate region

$$\begin{aligned} &\operatorname{conv}\left(\bigcup_{p=p(x_1)p(x_2)} [\mathscr{R}_{\mathrm{CF}}(p,\mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p)]\right) \\ &\qquad = \operatorname{conv}\left(\bigcup_{p=p(x_1)p(x_2)} \operatorname{conv}\big[\mathscr{R}_{\mathrm{CF}}(p,\mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p)\big]\right) \\ &\qquad \overset{(a)}{=} \operatorname{conv}\left(\bigcup_{p=p(x_1)p(x_2)} \operatorname{conv}\big[\mathscr{R}_{\mathrm{CF}}(p,\mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p)\big]\right) \end{aligned}$$

is achievable, where (a) follows since for every $p = p(x_1)p(x_2)$, $\operatorname{conv}\big(\mathscr{R}_1(p) \cup \mathscr{R}_2(p)\big) = \mathscr{R}_{\mathrm{MAC}}(p)$. We now prove that this achievable rate region is equivalent to the rate region in Proposition 3.6.2. Consider a fixed $Q = q$ and let $p_q := p(x_1|q)p(x_2|q)$ and $(X_{1q}, X_{2q}) \sim$

p_q. It suffices to show that the rate region defined by (3.34) evaluated for $Q = q$ and p_q is equivalent to

$$\operatorname{conv}\big[\mathscr{R}_{\mathrm{CF}}(p_q, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p_q)\big].$$

To see this, note that when $T = (X_{1q}, X_{2q})$, the rate region defined by (3.34) reduces to $\mathscr{R}_{\mathrm{MAC}}(p_q)$. Similarly, when $T = \emptyset$, the rate region defined by (3.34) reduces to $\mathscr{R}_{\mathrm{CF}}(p_q, \mathbf{a})$. In words, the random variable T for different $\beta \in [0,1]$ values plays the role of time-sharing between the rate regions $\mathscr{R}_{\mathrm{MAC}}(p_q)$ and $\mathscr{R}_{\mathrm{CF}}(p_q, \mathbf{a})$. Therefore, taking the union over $\beta \in [0,1]$ results in $\operatorname{conv}\big[\mathscr{R}_{\mathrm{CF}}(p_q, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p_q)\big]$, which completes the proof. □

3.A Proof of Proposition 3.2.1

Fix pmf $p = p(x_1)p(x_2)$ and nonzero vector $\mathbf{a} \in \mathbb{F}_q^2$. We first show that

$$[\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p)] \subseteq \mathscr{R}^*(p, \mathbf{a}).$$

Suppose that the rate pair $(R_1, R_2) \in \mathscr{R}_{CF}(p, \mathbf{a})$. Then, for every $j \in \{1,2\}$ with $a_j \neq 0$, the rate pair (R_1, R_2) satisfies

$$\begin{aligned} R_j &\le H(X_j) - H(W_{\mathbf{a}}|Y) \\ &\le H(X_j) - H(W_{\mathbf{a}}|Y, X_{j^c}) \\ &= I(X_j; Y|X_{j^c}), \end{aligned}$$

and

$$\begin{aligned} R_j &\le H(X_j) - H(W_{\mathbf{a}}|Y) \\ &= I(X_1, X_2; Y) - I(X_{j^c}; W_{\mathbf{a}}, Y) \\ &\le I(X_1, X_2; Y) - \min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\}, \end{aligned}$$

which implies that $(R_1, R_2) \in \mathscr{R}^*(p, \mathbf{a})$. It follows that $\mathscr{R}_{CF}(p, \mathbf{a}) \subseteq \mathscr{R}^*(p, \mathbf{a})$. Similarly, suppose that the rate pair $(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(p)$. Then, for every $j \in \{1, 2\}$ with $a_j \neq 0$, the rate pair (R_1, R_2) satisfies

$$R_j \leq I(X_j; Y | X_{j^c}),$$

and

$$\begin{aligned} R_j &\leq I(X_1, X_2; Y) - R_{j^c} \\ &\leq I(X_1, X_2; Y) - \min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\}, \end{aligned}$$

which implies that $(R_1, R_2) \in \mathscr{R}^*(p, \mathbf{a})$. Therefore, $\mathscr{R}_{\text{MAC}}(p) \subseteq \mathscr{R}^*(p, \mathbf{a})$.

Next, we show that $\mathscr{R}^*(p, \mathbf{a}) \subseteq [\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_{\text{MAC}}(p)]$. Suppose that the rate pair $(R_1, R_2) \in \mathscr{R}^*(p, \mathbf{a})$ such that $R_{j^c} > I(X_{j^c}; W_{\mathbf{a}}, Y)$ for every $j \in \{1, 2\}$ with $a_j \neq 0$. Then, (R_1, R_2) satisfies

$$\begin{aligned} R_j &\leq I(X_1, X_2; Y) - I(X_{j^c}; W_{\mathbf{a}}, Y) \\ &= H(X_j) - H(W_{\mathbf{a}} | Y), \end{aligned}$$

for every $j \in \{1, 2\}$ with $a_j \neq 0$. Then, $(R_1, R_2) \in \mathscr{R}_{CF}(p, \mathbf{a})$. It is easy to see that the rate pair $(R_1, R_2) \in \mathscr{R}^*(p, \mathbf{a})$ that satisfies $R_{j^c} \leq I(X_{j^c}; W_{\mathbf{a}}, Y)$ for some $j \in \{1, 2\}$ with $a_j \neq 0$, is included in $\mathscr{R}_{\text{MAC}}(p)$. Thus, $\mathscr{R}^*(p, \mathbf{a}) \subseteq [\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_{\text{MAC}}(p)]$, which completes the proof.

3.B A Lemma on the Rank of a Random Matrix

Lemma 3.B.1. *Let G be an $nR \times n$ random matrix over $\mathbb{F}_q$ with $R < 1$ where each element is drawn i.i.d.* $\mathrm{Unif}(\mathbb{F}_q)$*. Then,*

$$\mathsf{P}(G \textit{ is not full rank}) \leq q^{-n(1-R-\epsilon_n)},$$

for some $\epsilon_n \to 0$ as $n \to \infty$.

Proof. Probability of choosing nR linearly independent rows can be written as

$$\begin{aligned}\mathsf{P}(G \text{ is full rank}) &= \frac{\prod_{j=1}^{nR}(q^n - q^{j-1})}{(q^n)^{nR}} \\ &= \prod_{j=1}^{nR}(1 - q^{j-1-n}) \\ &\geq (1 - q^{-n(1-R)})^{nR} \\ &\overset{(a)}{\geq} 1 - nRq^{-n(1-R)},\end{aligned}$$

where (a) follows by Bernoulli's inequality for n large enough since $R < 1$. Using this relation, we have

$$\begin{aligned}\mathsf{P}(G \text{ is not full rank}) &= 1 - \mathsf{P}(G \text{ is full rank}) \\ &\leq nRq^{-n(1-R)}.\end{aligned}$$

Defining $\epsilon_n = \frac{\log_q(nR)}{n}$ completes the proof. □

3.C Proof of Lemma 3.3.1

Fix pmf $p = p(x_1)p(x_2)$ and nonzero vector $\mathbf{a} \in \mathbb{F}_q^2$. We will show that if the condition in (3.6) holds, then $\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p) = \mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p)$. To start with, note that the rate regions $\mathscr{R}_1(p)$ and $\mathscr{R}_2(p)$ have one additional rate constraint compared to $\mathscr{R}_{\mathrm{MAC}}(p)$. Therefore, $\mathscr{R}_j(p) \subseteq \mathscr{R}_{\mathrm{MAC}}(p)$ for $j = 1, 2$ and it follows that $\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p) \subseteq \mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_{\mathrm{MAC}}(p)$ holds in general. Then, it suffices to show that if the condition in (3.6) holds, then $\mathscr{R}_{\mathrm{MAC}}(p) \subseteq [\mathscr{R}_{CF}(p, \mathbf{a}) \cup \mathscr{R}_1(p) \cup \mathscr{R}_2(p)]$. Suppose that the condition in (3.6) is satisfied. Let the rate pair $(R_1, R_2) \in \mathscr{R}_{\mathrm{MAC}}(p)$ be such that $R_{j^c} > I(X_{j^c}; W_{\mathbf{a}}, Y)$ for every $j \in \{1, 2\}$ with $a_j \neq 0$. Then, (R_1, R_2) satisfies

$$\begin{aligned} R_j &\leq I(X_1, X_2; Y) - I(X_{j^c}; W_{\mathbf{a}}, Y) \\ &= H(X_j) - H(W_{\mathbf{a}}|Y), \end{aligned}$$

for every $j \in \{1, 2\}$ with $a_j \neq 0$, implying that $(R_1, R_2) \in \mathscr{R}_{CF}(p, \mathbf{a})$. Now, let the rate pair $(R_1, R_2) \in \mathscr{R}_{\mathrm{MAC}}(p)$ be such that $R_{j^c} \leq I(X_{j^c}; W_{\mathbf{a}}, Y)$ for some $j \in \{1, 2\}$ with $a_j \neq 0$. By condition (3.6), we have

$$\begin{aligned} I(X_{j^c}; W_{\mathbf{a}}, Y) &= I(X_1, X_2; Y) - H(X_j) + H(W_{\mathbf{a}}|Y) \\ &= I(X_1, X_2; Y) - H(X_j) + \min_{\mathbf{b} \neq \mathbf{0}} H(W_{\mathbf{b}}|Y) \\ &\leq I(X_1, X_2; Y) - H(X_j) + \min_{b_1, b_2 \in \mathbb{F}_q^*} H(W_{\mathbf{b}}|Y). \end{aligned}$$

Then, the rate pair $(R_1, R_2) \in \mathscr{R}_1(p) \cup \mathscr{R}_2(p)$, which completes the proof.

3.D Proof of Lemma 3.4.1

Note that for $j = 1, 2$,

$$\begin{aligned} H(M_j|Y^n, M_{j^c}, \mathcal{C}_n) &= I(M_j; W_{\mathbf{a}}^n|Y^n, M_{j^c}, \mathcal{C}_n) + H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}, \mathcal{C}_n) \\ &\leq H(W_{\mathbf{a}}^n|Y^n, \mathcal{C}_n) + H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}, \mathcal{C}_n). \end{aligned} \tag{3.35}$$

To bound the first term in (3.35), we need a version of Fano's inequality for computation.

Lemma 3.D.1. *If the average probability of error $\mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)]$ tends to zero as $n \to \infty$,* *then*

$$H(W_{\mathbf{a}}^n|Y^n, \mathcal{C}_n) \leq n\epsilon_n$$

for some $\epsilon_n \to 0$ *as* $n \to \infty$.

Proof. For fixed code $\mathcal{C}_n = \mathcal{c}_n$, by Fano's inequality

$$H(W_{\mathbf{a}}^n|Y^n, \mathcal{C}_n = \mathcal{c}_n) \leq 1 + nP_e^{(n)}(\mathcal{c}_n).$$

Taking the expectation over the random homologous code $\mathcal{C}_n$, we have

$$H(W_{\mathbf{a}}^n|Y^n, \mathcal{C}_n) \leq 1 + nE_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)] \overset{(a)}{\leq} n\epsilon_n,$$

where (a) follows since $\mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)]$ tends to zero as $n \to \infty$. □

Suppose that $a_j \neq 0$. Define indicator variable θ_j, $j = 1, 2$, such that $\theta_j = 1$ if M_j is confusable. Combining (3.35) with Lemma 3.D.1, we have

$$\begin{aligned}
H(M_j|Y^n, M_{j^c}, \mathcal{C}_n) &\leq n\epsilon_n + H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}, \mathcal{C}_n) \\
&\overset{(a)}{=} n\epsilon_n + H(M_j|W_{\mathbf{a}}^n, X_{j^c}^n(M_{j^c}), Y^n, M_{j^c}, \mathcal{C}_n) \\
&\overset{(b)}{=} n\epsilon_n + H(M_j|W_{\mathbf{a}}^n, X_j^n(M_j), X_{j^c}^n(M_{j^c}), Y^n, M_{j^c}, \mathcal{C}_n) \\
&\leq n\epsilon_n + H(M_j|X_j^n(M_j), \mathcal{C}_n) \\
&\leq n\epsilon_n + H(M_j, \theta_j|X_j^n(M_j), \mathcal{C}_n) \\
&\overset{(c)}{\leq} n\epsilon_n + \log_q 2 + H(M_j|X_j^n(M_j), \mathcal{C}_n, \theta_j) \\
&= n\epsilon_n + \log_q 2 + H(M_j|X_j^n(M_j), \mathcal{C}_n, \theta_j = 1)\,\mathsf{P}(\theta_j = 1) \\
&\leq n\epsilon_n + \log_q 2 + nR_j\,\mathsf{P}(\theta_j = 1) \\
&\overset{(d)}{\leq} n\epsilon_n + \log_q 2 + nR_j\epsilon_n \\
&= n(\epsilon_n + \frac{\log_q 2}{n} + R_j\epsilon_n),
\end{aligned}$$

where (a) follows since $X^n_{j^c}(M_{j^c})$ is a function of $(M_{j^c}, \mathcal{C}_n)$, (b) follows since $X^n_j(M_j)$ is a function of $(X^n_{j^c}(M_{j^c}), W^n_{\mathbf{a}})$ when $a_j \neq 0$, (c) follows since θ_j is a binary random variable, and (d) follows by the assumption in (3.21) in Lemma 3.4.1.

3.E Proof of Lemma 3.4.2

For the simplicity of the exposition without loss of generality, we provide a proof from a single sender perspective and the memoryless point-to-point channel $p_{Y|X}(y|x)$ with $\mathcal{X} = \mathbb{F}_q$. Let $\epsilon > 0$ and $p = p(x)$ be a pmf on $\mathbb{F}_q$. Define an $(n, nR; p_X, \epsilon)$ random nested coset code ensemble following steps 1)-3) for a single sender. Let X^n be the codeword sent through the channel, $\epsilon' > 0$, $i \in [n]$, and $(x, y) \in \mathbb{F}_q \times \mathcal{Y}$. Then,

$$\begin{aligned}
&\mathsf{P}(X_i = x, Y_i = y | X^n \in \mathcal{T}^{(n)}_{\epsilon'}(X)) \\
&\qquad\qquad = \mathsf{P}(X_i = x | X^n \in \mathcal{T}^{(n)}_{\epsilon'}(X))\, \mathsf{P}(Y_i = y | X_i = x, X^n \in \mathcal{T}^{(n)}_{\epsilon'}(X)) \\
&\qquad\qquad = \mathsf{P}(X_i = x | X^n \in \mathcal{T}^{(n)}_{\epsilon'}(X)) p_{Y|X}(y|x). \qquad (3.36)
\end{aligned}$$

We make a connection between the conditional distribution of X_i given $\{X^n \in \mathcal{T}^{(n)}_{\epsilon'}(X)\}$ and the input pmf $p(x)$. Therefore, we start with exploring the conditional distribution of X_i given $\{X^n \in \mathcal{T}^{(n)}_{\epsilon'}(X)\}$.

Lemma 3.E.1. *Let $p(x)$ be a pmf on $\mathbb{F}_q$, and $\epsilon, \epsilon' > 0$. Define $\mathcal{T}^{(n)}_{\epsilon'}(X, \Theta)$ as the set of elements in $\mathcal{T}^{(n)}_{\epsilon'}(X)$ with type Θ. Suppose $X^n(m) = U^n(m, L(m))$ denote the random codeword assigned to message m by $(n, nR; p(x), \epsilon)$ random nested coset code ensemble. Then,*

$$U^n(m, L) | \{U^n(m, L) \in \mathcal{T}^{(n)}_{\epsilon'}(X, \Theta)\} \sim \mathrm{Unif}(\mathcal{T}^{(n)}_{\epsilon'}(X, \Theta)),$$

for every $m \in \mathbb{F}_q^{nR}$.

Proof. Without loss of generality, we drop index m. It suffices to show that the distribution of $U^n(L)$ is permutation invariant. Let u^n, v^n have the same type (typical or not) and let $v^n = \sigma(u^n)$ for some permutation σ. Then, we have

$$\begin{aligned}\mathsf{P}(U^n(L) = u^n) &= \sum_l \sum_{\mathsf{G}} \mathsf{P}(L = l, G = \mathsf{G}, D^n = u^n \ominus l\mathsf{G}) \\ &\overset{(a)}{=} \sum_l \sum_{\mathsf{G}} \mathsf{P}(L = l, G = \sigma(\mathsf{G}), D^n = v^n \ominus l\sigma(\mathsf{G})) \\ &= \mathsf{P}(U^n(L) = v^n),\end{aligned}$$

where $\sigma(\mathsf{G})$ is the matrix constructed by applying permutation σ to the columns of G and (a) follows since a permutation applied to a coset code preserves the type of each codeword. □

Building on top of Lemma 3.E.1, we next establish that the conditional distribution of X_i given $\{X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)\}$ is *close* to the input pmf $p(x)$.

Lemma 3.E.2. *Let $\epsilon' > 0$. Define $\mathcal{T}_{\epsilon'}^{(n)}(X, \Theta)$ in a similar way to Lemma 3.E.1. Suppose that the distribution of X^n is uniform within $\mathcal{T}_{\epsilon'}^{(n)}(X, \Theta)$, namely,*

$$X^n | \{X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X, \Theta)\} \sim \mathrm{Unif}(\mathcal{T}_{\epsilon'}^{(n)}(X, \Theta)) \tag{3.37}$$

for every type Θ such that $\mathcal{T}_{\epsilon'}^{(n)}(X, \Theta) \neq \emptyset$. Then, conditioned on the typical set, X_i's have identical distribution that satisfies

$$(1 - \epsilon')p(x) \leq P(X_i = x | X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)) \leq (1 + \epsilon')p(x), \quad \forall x \in \mathcal{X}.$$

Proof. Let $x \in \mathcal{X}$. For a type Θ, let Θ_x denote the empirical mode of x within type Θ. Then, for every type Θ such that $\mathcal{T}_{\epsilon'}^{(n)}(X, \Theta) \neq \emptyset$, we have

$$\mathsf{P}(X_i = x | X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X, \Theta)) = \sum_{\substack{x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X, \Theta) \\ \text{s.t. } x_i = x}} \mathsf{P}(X^n = x^n | X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X, \Theta))$$

$$
\begin{aligned}
&\overset{(a)}{=} \sum_{\substack{x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)\\ x_i = x}} \frac{1}{|\mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)|} \\
&\overset{(b)}{=} \Theta_x |\mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)| \frac{1}{|\mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)|} \\
&= \Theta_x,
\end{aligned}
$$

where (a) follows since X^n is conditionally uniform over $\mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)$, and (b) follows since $\mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)$ is closed under permutation. Combining this observation with the fact that Θ is the type of a typical sequence, we get

$$
(1-\epsilon')p(x) \le \mathsf{P}(X_i = x | X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)) \le (1+\epsilon')p(x), \quad \forall x \in \mathcal{X}.
$$

Since $\mathcal{T}_{\epsilon'}^{(n)}(X)$ is the disjoint union of $\mathcal{T}_{\epsilon'}^{(n)}(X,\Theta)$ over all types, multiplying each side with $\mathsf{P}(X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X,\Theta))$ and then summing over Θ gives

$$
\begin{aligned}
&(1-\epsilon')p(x)\, \mathsf{P}(X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)) \\
&\qquad \le \mathsf{P}(X_i = x, X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)) \le (1+\epsilon')p(x)\, \mathsf{P}(X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)),
\end{aligned}
$$

for all $x \in \mathcal{X}$. The claim follows from dividing each side by $\mathsf{P}(X^n \in \mathcal{T}_{\epsilon'}^{(n)}(X))$. □

Back to the proof of Lemma 3.4.2, we have by Lemma 3.E.1 that the distribution of X^n (codeword from an $(n, nR; p(x), \epsilon)$ random nested coset code ensemble) satisfies the condition in (3.37) in Lemma 3.E.2. Therefore, combining (3.36) with Lemma 3.E.2 completes the proof.

3.F Proof of Lemma 3.4.3

Let $\epsilon'' > \epsilon'$. Suppose that $a_j \neq 0$, and $j^c = \{1,2\} \setminus \{j\}$. First, by Lemma 3.D.1, we have

$$
I(M_{j^c}; Y^n | \mathcal{C}_n) \ge I(M_{j^c}; W_{\mathbf{a}}^n, Y^n | \mathcal{C}_n) - n\epsilon_n.
$$

Therefore, it suffices to prove that for n sufficiently large,

$$I(M_{j^c}; W_{\mathbf{a}}^n, Y^n | \mathcal{C}_n) \geq n[\min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} - \delta_5(\epsilon'') - \epsilon_n].$$

Similar to [5], we will show that given $W_{\mathbf{a}}^n, Y^n$, and $\mathcal{C}_n$, a relatively short list $\mathcal{L} \subseteq \mathbb{F}_q^{nR_{j^c}}$ can be constructed that contains M_{j^c} with high probability. Define a random set

$$\mathcal{L} = \{m \in \mathbb{F}_q^{nR_{j^c}} : (X_{j^c}^n(m), W_{\mathbf{a}}^n, Y^n) \in \mathcal{T}_{\epsilon''}^{(n)}(X_{j^c}, W_{\mathbf{a}}, Y)\}.$$

Note that the set $\mathcal{L}$ is random with the underlying distribution on $(W_{\mathbf{a}}^n, Y^n, \mathcal{C}_n)$, which is induced by drawing a random homologous code $\mathcal{C}_n$ and using this code to encode $X_1^n(M_1)$ and $X_2^n(M_2)$ that lead to $W_{\mathbf{a}}^n = a_1 X_1^n(M_1) \oplus a_2 X_2^n(M_2)$ and Y^n through the finite-field input memoryless MAC $p(y|x_1, x_2)$. We first bound the probability that an incorrect message is in the random set $\mathcal{L}$. Define two events $\mathcal{M}_1 = \{M_1 = M_2 = \mathbf{0}\}$ and $\mathcal{M}_2 = \{L_1(M_1) = L_2(M_2) = \mathbf{0}\}$. The indicator random variable E_n is as defined in (3.22). By the symmetry of the code generation, for every $m \neq \mathbf{0} \in \mathbb{F}_q^{nR_{j^c}}$, we have

$$\mathsf{P}(m \oplus M_{j^c} \in \mathcal{L},\, E_n = 1) = \mathsf{P}(m \in \mathcal{L}, E_n = 1 | \mathcal{M}_1, \mathcal{M}_2). \tag{3.38}$$

To see this, we start with

$$\begin{aligned}
&\mathsf{P}(m \oplus M_{j^c} \in \mathcal{L},\, E_n = 1) \\
&= \mathsf{P}((X_{j^c}^n(m \oplus M_{j^c}), W_{\mathbf{a}}^n, Y^n) \in \mathcal{T}_{\epsilon''}^{(n)}(X_{j^c}, W_{\mathbf{a}}, Y), (X_1^n(M_1), X_2(M_2)) \in \mathcal{T}_{\epsilon'}^{(n)}(X_1, X_2)) \\
&= \sum_{\substack{m_1, l_1, \\ m_2, l_2}} \sum_{\substack{\mathsf{G}, \\ d_1^n, d_2^n}} \mathsf{P}\left(\begin{array}{c} (M_1, M_2) = (m_1, m_2), (L_1(M_1), L_2(M_2)) = (l_1, l_2), G = \mathsf{G}, \\ D_1^n = d_1^n, D_2^n = d_2^n, (X_{j^c}^n(m \oplus m_{j^c}), W_{\mathbf{a}}^n, Y^n) \in \mathcal{T}_{\epsilon''}^{(n)}(X_{j^c}, W_{\mathbf{a}}, Y), \\ (X_1^n(m_1), X_2^n(m_2)) \in \mathcal{T}_{\epsilon'}^{(n)}(X_1, X_2) \end{array} \right) \\
&= \sum_{\substack{m_1, l_1, \\ m_2, l_2}} \sum_{\substack{\mathsf{G}, \\ d_1^n, d_2^n}} \mathsf{P}(M_1 = m_1, M_2 = m_2)\, \mathsf{P}(G = \mathsf{G}, D_1^n = d_1^n, D_2^n = d_2^n)
\end{aligned}$$

$$\mathsf{P}\left(\begin{array}{c|c} L_1(M_1) = l_1, L_2(M_2) = l_2, & (M_1, M_2) = (m_1, m_2), \\ (X^n_{j^c}(m \oplus m_{j^c}), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), & G = \mathsf{G}, \\ (X^n_1(m_1), X^n_2(m_2)) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) & D^n_1 = d^n_1, D^n_2 = d^n_2 \end{array}\right) \tag{3.39}$$

$$= \sum_{\substack{m_1,l_1,\\ m_2,l_2}} \sum_{\substack{\mathsf{G},\\ d^n_1,d^n_2}} \mathsf{P}(M_1 = \mathbf{0}, M_2 = \mathbf{0})\, \mathsf{P}\left(\begin{array}{c} G = \mathsf{G}, D^n_1 = [m_1\ l_1\ \mathbf{0}]\mathsf{G} \oplus d^n_1, \\ D^n_2 = [m_2\ l_2\ \mathbf{0}]\mathsf{G} \oplus d^n_2 \end{array}\right)$$

$$\mathsf{P}\left(\begin{array}{c|c} L_1(M_1) = \mathbf{0}, L_2(M_1) = \mathbf{0}, & (M_1, M_2) = (\mathbf{0}, \mathbf{0}), \\ (X^n_{j^c}(m), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), & G = \mathsf{G}, D^n_1 = [m_1\ l_1\ \mathbf{0}]\mathsf{G} \oplus d^n_1, \\ (X^n_1(\mathbf{0}), X^n_2(\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) & D^n_2 = [m_2\ l_2\ \mathbf{0}]\mathsf{G} \oplus d^n_2 \end{array}\right) \tag{3.40}$$

$$= \sum_{\substack{m_1,l_1,\\ m_2,l_2}} \sum_{\substack{\mathsf{G},\\ d^n_1,d^n_2}} \mathsf{P}\left(\begin{array}{c} (M_1, M_2) = (\mathbf{0}, \mathbf{0}), (L_1(M_1), L_2(M_2)) = (\mathbf{0}, \mathbf{0}), \\ G = \mathsf{G}, D^n_1 = [m_1\ l_1\ \mathbf{0}]\mathsf{G} \oplus d^n_1, D^n_2 = [m_2\ l_2\ \mathbf{0}]\mathsf{G} \oplus d^n_2, \\ (X^n_{j^c}(m), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), \\ (X^n_1(\mathbf{0}), X^n_2(\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) \end{array}\right)$$

$$= \sum_{\substack{m_1,l_1,\\ m_2,l_2}} \mathsf{P}\left(\begin{array}{c} (M_1, M_2) = (\mathbf{0}, \mathbf{0}), (L_1(M_1), L_2(M_2)) = (\mathbf{0}, \mathbf{0}), \\ (X^n_{j^c}(m), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), (X^n_1(\mathbf{0}), X^n_2(\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) \end{array}\right)$$

$$= \sum_{\substack{m_1,l_1,\\ m_2,l_2}} \mathsf{P}(\mathcal{M}_1, \mathcal{M}_2)\, \mathsf{P}\left(\begin{array}{c|c} (X^n_{j^c}(m), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), & \mathcal{M}_1, \\ (X^n_1(\mathbf{0}), X^n_2(\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) & \mathcal{M}_2 \end{array}\right)$$

$$= \mathsf{P}((X^n_{j^c}(m), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), (X^n_1(\mathbf{0}), X^n_2(\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) | \mathcal{M}_1, \mathcal{M}_2), \tag{3.41}$$

where (3.39) follows since (M_1, M_2) is independent from (G, D^n_1, D^n_2), (3.40) follows since (M_1, M_2) is uniformly distributed and

$$(G, D^n_1, D^n_2) \overset{d}{=} (G, [m_1\ l_1\ \mathbf{0}]G \oplus D^n_1, [m_2\ l_2\ \mathbf{0}]G \oplus D^n_2)$$

result in two equivalent codes (i.e., the same set of codewords with permuted mappings from messages to codewords), and (3.41) follows by the fact proved in [3, Lemma 11] that (M_1, L_1, M_2, L_2) is uniformly distributed over its support.

To bound the probability in (3.38), we continue from (3.41) as follows.

$$
\begin{aligned}
&\mathsf{P}(m \in \mathcal{L},\, E_n = 1 | \mathcal{M}_1, \mathcal{M}_2) \\
&\quad = \mathsf{P}((X^n_{j^c}(m), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y)(X^n_1(\mathbf{0}), X_2(\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) | \mathcal{M}_1, \mathcal{M}_2) \\
&\quad \le \mathsf{P}\left(\begin{array}{c|c} (U^n_{j^c}(m,l), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y) \text{ for some } l \in \mathbb{F}_q^{n\hat{R}_{j^c}}, & \mathcal{M}_1, \\ (U^n_1(\mathbf{0},\mathbf{0}), U_2(\mathbf{0},\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon'}(X_1, X_2) & \mathcal{M}_2 \end{array} \right) \\
&\quad \overset{(a)}{\le} \mathsf{P}\left(\begin{array}{c|c} (U^n_{j^c}(m,l), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y) \text{ for some } l \in \mathbb{F}_q^{n\hat{R}_{j^c}}, & \mathcal{M}_1, \\ (U^n_1(\mathbf{0},\mathbf{0}), U_2(\mathbf{0},\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon''}(X_1, X_2) & \mathcal{M}_2 \end{array} \right) \\
&\quad \le \sum_l \mathsf{P}\left(\begin{array}{c|c} (U^n_{j^c}(m,l), W^n_{\mathbf{a}}, Y^n) \in \mathcal{T}^{(n)}_{\epsilon''}(X_{j^c}, W_{\mathbf{a}}, Y), & \mathcal{M}_1, \\ (U^n_1(\mathbf{0},\mathbf{0}), U_2(\mathbf{0},\mathbf{0})) \in \mathcal{T}^{(n)}_{\epsilon''}(X_1, X_2) & \mathcal{M}_2 \end{array} \right) \\
&\quad \le \sum_l \sum_{\substack{(x^n_1, x^n_2) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_1, X_2)}} \sum_{\substack{(u^n, w^n, y^n) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_{jc}, W_{\mathbf{a}}, Y)}} \mathsf{P}\left(\begin{array}{c|c} U^n_{j^c}(m,l) = u^n, W^n_{\mathbf{a}} = w^n, Y^n = y^n, & \mathcal{M}_1, \\ U^n_1(\mathbf{0},\mathbf{0}) = x^n_1, U^n_2(\mathbf{0},\mathbf{0}) = x^n_2 & \mathcal{M}_2 \end{array} \right) \\
&\quad = \sum_l \sum_{\substack{(x^n_1, x^n_2) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_1, X_2)}} \sum_{\substack{(u^n, w^n, y^n) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_{jc}, W_{\mathbf{a}}, Y)}} \mathsf{P}\left(\begin{array}{c|c} U^n_{j^c}(m,l) = u^n, a_1 D^n_1 \oplus a_2 D^n_2 = w^n, & \mathcal{M}_1, \\ Y^n = y^n, D^n_1 = x^n_1, D^n_2 = x^n_2 & \mathcal{M}_2 \end{array} \right) \\
&\quad \overset{(b)}{=} \sum_l \sum_{\substack{(x^n_1, x^n_2) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_1, X_2)}} \sum_{\substack{(u^n, w^n, y^n) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_{jc}, W_{\mathbf{a}}, Y)}} \mathsf{P}\left(\begin{array}{c|c} U^n_{j^c}(m,l) = u^n, & \\ a_1 D^n_1 \oplus a_2 D^n_2 = w^n, & \begin{array}{c} \mathcal{M}_1, \\ \mathcal{M}_2 \end{array} \\ D^n_1 = x^n_1, D^n_2 = x^n_2 & \end{array} \right) p(y^n | x^n_1, x^n_2) \\
&\quad \overset{(c)}{\le} q^{n(\hat{R}_1 + \hat{R}_2)} \sum_l \sum_{\substack{(x^n_1, x^n_2) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_1, X_2)}} \\
&\qquad\qquad \sum_{\substack{(u^n, w^n, y^n) \in \\ \mathcal{T}^{(n)}_{\epsilon''}(X_{jc}, W_{\mathbf{a}}, Y)}} \mathsf{P}\left(\begin{array}{c} U^n_{j^c}(m,l) = u^n, a_1 D^n_1 \oplus a_2 D^n_2 = w^n, \\ D^n_1 = x^n_1, D^n_2 = x^n_2 \end{array} \right) p(y^n | x^n_1, x^n_2)
\end{aligned}
$$

$$
\begin{aligned}
&= q^{n(\hat{R}_1+\hat{R}_2)} \sum_{l} \sum_{\substack{(x_1^n,x_2^n)\in\\ \mathcal{T}_{\epsilon''}^{(n)}(X_1,X_2)}} \\
&\qquad \sum_{\substack{(u^n,w^n,y^n)\in\\ \mathcal{T}_{\epsilon''}^{(n)}(X_{j^c},W_{\mathbf{a}},Y)}} \mathsf{P}\begin{pmatrix} [m\ l]G\oplus D_{j^c}^n = u^n, \\ D_1^n = x_1^n, D_2^n = x_2^n \end{pmatrix} p(y^n|x_1^n,x_2^n)\,\mathbb{1}_{\{w^n=a_1x_1^n\oplus a_2x_2^n\}} \\
&= q^{n(\hat{R}_1+\hat{R}_2)} \sum_{l} \sum_{\substack{(x_1^n,x_2^n)\in\\ \mathcal{T}_{\epsilon''}^{(n)}(X_1,X_2)}} \sum_{\substack{(w^n,y^n)\in\\ \mathcal{T}_{\epsilon''}^{(n)}(W_{\mathbf{a}},Y)}} \sum_{\substack{u^n\in\\ \mathcal{T}_{\epsilon''}^{(n)}(X_{j^c}|w^n,y^n)}} q^{-3n}\, p(y^n|x_1^n,x_2^n)\,\mathbb{1}_{\{w^n=a_1x_1^n\oplus a_2x_2^n\}} \\
&\le q^{n(\hat{R}_1+\hat{R}_2+\hat{R}_{j^c})}\, q^{-3n}\, q^{n(H(X_{j^c}|W_{\mathbf{a}},Y)+H(X_1,X_2)+\delta(\epsilon''))} \\
&\overset{(d)}{\le} q^{-n(I(X_{j^c};W_{\mathbf{a}},Y)-\delta(\epsilon'')-3\epsilon)}, \\
&\le q^{-n(I(X_{j^c};W_{\mathbf{a}},Y)-\delta_5(\epsilon''))},
\end{aligned}
$$

where (a) follows since $\epsilon'' > \epsilon'$, (b) follows since conditioned on $\mathcal{M}_1$ and $\mathcal{M}_2$, $U_{j^c}^n \to (D_1^n, D_2^n) \to Y^n$ form a Markov chain, (c) follows by [3, Lemma 11] since (G, D_1^n, D_2^n) is independent from (M_1, M_2), and (d) follows by the construction of the random homologous code $\mathcal{C}_n$ with $\hat{R}_i = D(p_{X_i}\|\mathrm{Unif}(\mathbb{F}_q)) + \epsilon$. Since $\mathsf{P}(E_n = 1)$ tends to one as $n \to \infty$, for n sufficiently large we have $\mathsf{P}(E_n = 1) \ge q^{-\epsilon}$. Therefore, for n sufficiently large, the conditional probability is bounded as follows

$$
\begin{aligned}
\mathsf{P}(m \oplus M_{j^c} \in \mathcal{L} | E_n = 1) &= \frac{\mathsf{P}(m \oplus M_{j^c} \in \mathcal{L}, E_n = 1)}{\mathsf{P}(E_n = 1)} \\
&\le \mathsf{P}(m \oplus M_{j^c} \in \mathcal{L}, E_n = 1) q^{\epsilon}.
\end{aligned}
$$

The expected cardinality of $\mathcal{L}$ given $\{E_n = 1\}$ is then bounded as

$$
\begin{aligned}
\mathsf{E}(|\mathcal{L}||E_n = 1) &\le 1 + \sum_{m\neq\mathbf{0}} \mathsf{P}(m \oplus M_{j^c} \in \mathcal{L} | E_n = 1) \\
&\le 1 + q^{n(R_{j^c} - I(X_{j^c};W_{\mathbf{a}},Y) + \delta_5(\epsilon'') + \frac{\epsilon}{n})} \qquad (3.42) \\
&= 1 + q^{n(R_{j^c} - I(X_{j^c};W_{\mathbf{a}},Y) + \delta_5(\epsilon'') + \epsilon_n)}, \qquad (3.43)
\end{aligned}
$$

for n sufficiently large. Define another indicator random variable $F_n = \mathbb{1}_{\{M_{j^c} \in \mathcal{L}\}}$. Since $\epsilon'' > \epsilon'$ and $\mathsf{P}(E_n = 1)$ tends to one as $n \to \infty$, by the conditional typicality lemma in [6, p. 27], $\mathsf{P}(F_n = 1)$ tends to one as $n \to \infty$. Then, for n sufficiently large, we have

$$\begin{aligned}
&H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n) \\
&\qquad = H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, E_n, F_n) + I(M_{j^c}; E_n, F_n|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n) \\
&\qquad \le H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, E_n, F_n) + 2\log_q 2 \\
&\qquad \le 2\log_q 2 + \mathsf{P}(F_n = 0) H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, F_n = 0, E_n) \\
&\qquad\qquad + \mathsf{P}(F_n = 1) H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, F_n = 1, E_n) \\
&\qquad \le 2\log_q 2 + nR_{j^c}\,\mathsf{P}(F_n = 0) + H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, F_n = 1, E_n). \qquad (3.44)
\end{aligned}$$

For the last term in (3.44), we use the fact that if $M_{j^c} \in \mathcal{L}$, then the conditional entropy cannot exceed $\log(|\mathcal{L}|)$:

$$\begin{aligned}
&H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, F_n = 1, E_n) \\
&\qquad \overset{(a)}{=} H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, F_n = 1, E_n, \mathcal{L}, |\mathcal{L}|) \\
&\qquad \le H(M_{j^c}|F_n = 1, E_n, \mathcal{L}, |\mathcal{L}|) \\
&\qquad = \sum_{l=0}^{q^{nR_{j^c}}} \mathsf{P}(|\mathcal{L}| = l, E_n = 1) H(M_{j^c}|E_n = 1, F_n = 1, \mathcal{L}, |\mathcal{L}| = l) \\
&\qquad\quad + \sum_{l=0}^{q^{nR_{j^c}}} \mathsf{P}(|\mathcal{L}| = l, E_n = 0) H(M_{j^c}|E_n = 0, F_n = 1, \mathcal{L}, |\mathcal{L}| = l) \\
&\qquad \le \sum_{l=0}^{q^{nR_{j^c}}} \mathsf{P}(|\mathcal{L}| = l, E_n = 1) H(M_{j^c}|E_n = 1, F_n = 1, \mathcal{L}, |\mathcal{L}| = l) + \mathsf{P}(E_n = 0) nR_{j^c} \\
&\qquad \le \sum_{l=0}^{q^{nR_{j^c}}} \mathsf{P}(|\mathcal{L}| = l, E_n = 1) \log_q(l) + nR_{j^c}\,\mathsf{P}(E_n = 0) \\
&\qquad \le \sum_{l=0}^{q^{nR_{j^c}}} \mathsf{P}(|\mathcal{L}| = l|E_n = 1) \log_q(l) + nR_{j^c}\,\mathsf{P}(E_n = 0) \\
&\qquad = \mathsf{E}[\log_q(|\mathcal{L}|)|E_n = 1] + nR_{j^c}\,\mathsf{P}(E_n = 0)
\end{aligned}$$

$$
\begin{aligned}
&\overset{(b)}{\leq} \log_q(\mathsf{E}[|\mathcal{L}||E_n = 1]) + nR_{j^c}\,\mathsf{P}(E_n = 0) \\
&\overset{(c)}{\leq} \log_q 2 + \max\{0, n(R_{j^c} - I(X_{j^c}; W_{\mathbf{a}}, Y) + \delta_5(\epsilon'') + \epsilon_n)\} + nR_{j^c}\,\mathsf{P}(E_n = 0) \\
&\leq \log_q 2 + \max\{0, n(R_{j^c} - I(X_{j^c}; W_{\mathbf{a}}, Y))\} + n\delta_5(\epsilon'') + n\epsilon_n + nR_{j^c}\,\mathsf{P}(E_n = 0)
\end{aligned}
$$

where (a) follows since the set $\mathcal{L}$ and its cardinality $|\mathcal{L}|$ are functions of $(\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n)$, (b) follows by Jensen's inequality, and (c) follows by (3.43) and the soft-max interpretation of the log-sum-exp function [7, p. 72]. Substituting back gives

$$
\begin{aligned}
&I(M_{j^c}; W_{\mathbf{a}}^n, Y^n|\mathcal{C}_n) \\
&= H(M_{j^c}|\mathcal{C}_n) - H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n) \\
&= nR_{j^c} - H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n) \\
&\geq nR_{j^c} - 2\log_q 2 - nR_{j^c}\,\mathsf{P}(F_n = 0) - H(M_{j^c}|\mathcal{C}_n, W_{\mathbf{a}}^n, Y^n, F_n = 1, E_n) \\
&\geq nR_{j^c} - 3\log_q 2 - nR_{j^c}(\mathsf{P}(E_n = 0) + \mathsf{P}(F_n = 0)) \\
&\qquad\quad - \max\{0, n(R_{j^c} - I(X_{j^c}; W_{\mathbf{a}}, Y))\} - n\delta_5(\epsilon'') - n\epsilon_n \\
&= n[\min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} - \delta_5(\epsilon'') - \epsilon_n] - 3 - nR_{j^c}(\mathsf{P}(E = 0) + \mathsf{P}(F = 0)) \\
&\overset{(a)}{=} n[\min\{R_{j^c}, I(X_{j^c}; W_{\mathbf{a}}, Y)\} - \delta_5(\epsilon'') - 2\epsilon_n],
\end{aligned}
$$

where (a) follows for large n since both probabilities $\mathsf{P}(E_n = 0)$ and $\mathsf{P}(F_n = 0)$ tend to zero as $n \to \infty$.

3.G Proof of Proposition 3.6.1

We start with another version of Fano's inequality for computation, similar to Lemma 3.4.1 but for a fixed code this time.

Lemma 3.G.1. *If*

$$\lim_{n\to\infty} P_e^{(n)} = 0$$

and

$$\lim_{n\to\infty} \mathsf{P}(M_j \textit{ is confusable}) = 0,$$

for every $j \in \{1,2\}$ *with* $a_j \neq 0$*, then for every* $j \in \{1,2\}$ *with* $a_j \neq 0$

$$H(M_j|Y^n, M_{j^c}) \leq n\epsilon_n$$

for some $\epsilon_n \to 0$ *as* $n \to \infty$*.*

Proof. First note that for every $j \in \{1,2\}$, we have

$$\begin{aligned}
H(M_j|Y^n, M_{j^c}) &\leq H(M_j, W_{\mathbf{a}}^n|Y^n, M_{j^c}) \\
&= H(W_{\mathbf{a}}^n|Y^n, M_{j^c}) + H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}) \\
&\overset{(a)}{\leq} n\epsilon_n + H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}),
\end{aligned}$$

where (a) follows by Fano's inequality. To bound the second term in (a), let j be such that $a_j \neq 0$ and let θ_j be an indicator random variable which is 1 if M_j is confusable. Then, we get

$$\begin{aligned}
H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}) &\overset{(b)}{=} H(M_j|W_{\mathbf{a}}^n, Y^n, M_{j^c}, X_1^n, X_2^n) \\
&\leq H(M_j|X_j^n) \\
&\leq H(M_j, \theta_j|X_j^n) \\
&\overset{(c)}{\leq} \log_q 2 + H(M_j|\theta_j, X_j^n) \\
&= \log_q 2 + H(M_j|\theta_j = 1, X_j^n)\, \mathsf{P}(\theta_j = 1) \\
&\leq \log_q 2 + nR_j\, \mathsf{P}(\theta_j = 1) \\
&\overset{(d)}{\leq} n\epsilon_n,
\end{aligned}$$

where (b) follows since (X_1^n, X_2^n) is a function of $(M_{j^c}, W_{\mathbf{a}}^n)$ when $a_j \neq 0$, (c) follows since θ_j is a binary random variable, and (d) follows since $\mathsf{P}(\theta_j = 1)$ tends to zero as

$n \to \infty$. □

Suppose now that a rate pair (R_1, R_2) is achievable. Let j is such that $a_j \neq 0$. Then,

$$\begin{aligned}
nR_j &= H(M_j|M_{j^c}) \\
&\overset{(a)}{\leq} I(M_j; Y^n|M_{j^c}) + n\epsilon_n \\
&= \sum_{i=1}^{n} I(M_j; Y_i|Y^{i-1}, M_{j^c}) + n\epsilon_n \\
&= \sum_{i=1}^{n} I(M_j, X_{ji}; Y_i|Y^{i-1}, M_{j^c}, X_{j^c i}) + n\epsilon_n \\
&\leq \sum_{i=1}^{n} I(M_j, Y^{i-1}, M_{j^c}, X_{ji}; Y_i|X_{j^c i}) + n\epsilon_n \\
&\overset{(b)}{=} \sum_{i=1}^{n} I(X_{ji}; Y_i|X_{j^c i}) + n\epsilon_n \\
&\overset{(c)}{=} nI(X_{jQ}; Y_Q|X_{j^c Q}, Q) + n\epsilon_n,
\end{aligned}$$

where (a) follows by Lemma 3.G.1, (b) follows since $(M_1, M_2, Y^{i-1}) \to (X_{1i}, X_{2i}) \to Y_i$ form a Markov chain, and (c) follows by defining a time sharing random variable Q that is uniform on $[n]$ and independent from (X_1^n, X_2^n, Y^n).

We can continue from (a) above to provide another bound on nR_j as follows.

$$\begin{aligned}
nR_j &\leq I(M_j; Y^n|M_{j^c}) + n\epsilon_n \\
&= I(M_1, M_2; Y^n) - I(M_{j^c}; Y^n) + n\epsilon_n \\
&\overset{(d)}{\leq} I(M_1, M_2; Y^n) - I(M_{j^c}; W_{\mathbf{a}}^n, Y^n) + 2n\epsilon_n \\
&= \sum_{i=1}^{n} I(M_1, M_2; Y_i|Y^{i-1}) - \sum_{i=1}^{n} I(M_{j^c}; W_{\mathbf{a},i}, Y_i|W_{\mathbf{a}}^{i-1}, Y^{i-1}) + 2n\epsilon_n \\
&= \sum_{i=1}^{n} I(M_1, M_2, X_{1i}, X_{2i}; Y_i|Y^{i-1}) - \sum_{i=1}^{n} I(M_{j^c}, X_{j^c i}; W_{\mathbf{a},i}, Y_i|W_{\mathbf{a}}^{i-1}, Y^{i-1}) + 2n\epsilon_n \\
&\overset{(e)}{=} \sum_{i=1}^{n} I(M_1, M_2, X_{1i}, X_{2i}; Y_i|Y^{i-1}) - \sum_{i=1}^{n} I(M_{j^c}, X_{j^c i}; W_{\mathbf{a},i}, Y_i|T_i) + 2n\epsilon_n
\end{aligned}$$

$$
\begin{aligned}
&\le \sum_{i=1}^{n} I(M_1, M_2, Y^{i-1}, X_{1i}, X_{2i}; Y_i) - \sum_{i=1}^{n} I(X_{j^c i}; W_{\mathbf{a},i}, Y_i | T_i) + 2n\epsilon_n \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(X_{1i}, X_{2i}; Y_i) - \sum_{i=1}^{n} I(X_{j^c i}; W_{\mathbf{a},i}, Y_i | T_i) + 2n\epsilon_n \\
&= n\big(I(X_{1Q}, X_{2Q}; Y_Q | Q) - I(X_{j^c Q}; W_{\mathbf{a},Q}, Y_Q | T_Q, Q)\big) + 2n\epsilon_n,
\end{aligned}
$$

where (d) follows by Fano's inequality, (e) follows by defining $T_i := (W_{\mathbf{a}}^{i-1}, Y^{i-1})$, and (f) follows since $(M_1, M_2, Y^{i-1}) \to (X_{1i}, X_{2i}) \to Y_i$ form a Markov chain. Note that $T_i \to (X_{1i}, X_{2i}) \to W_{\mathbf{a},i}$ and $(T_i, W_{\mathbf{a},i}) \to (X_{1i}, X_{2i}) \to Y_i$ each form a Markov chain.

We next bound the sum rate using the fact that $a_1, a_2 \neq 0$ as follows.

$$
\begin{aligned}
n(R_1 + R_2) &= H(M_1, M_2) \\
&= I(M_1, M_2; Y^n) + H(M_1, M_2, W_{\mathbf{a}}^n | Y^n) \\
&\overset{(g)}{\le} I(M_1, M_2; Y^n) + H(M_1, M_2 | W_{\mathbf{a}}^n, Y^n) + n\epsilon_n \\
&= I(M_1, M_2; Y^n) + H(M_1 | W_{\mathbf{a}}^n, Y^n) + H(M_2 | M_1, W_{\mathbf{a}}^n, Y^n) + n\epsilon_n \\
&\overset{(h)}{\le} I(M_1, M_2; Y^n) + H(M_1 | W_{\mathbf{a}}^n, Y^n) + 2n\epsilon_n \\
&= I(M_1, M_2; Y^n) + H(M_1 | W_{\mathbf{a}}^n, Y^n) + H(M_2 | W_{\mathbf{a}}^n, Y^n) \\
&\qquad - H(M_1, M_2 | W_{\mathbf{a}}^n, Y^n) + H(M_1 | W_{\mathbf{a}}^n, Y^n, M_2) + 2n\epsilon_n, \qquad (3.45)
\end{aligned}
$$

where (g) follows by Fano's inequality and (h) follows by Lemma 3.G.1 since $a_2 \neq 0$. Note that since $a_1 \neq 0$, by Lemma 3.G.1, we also have

$$
H(M_1 | W_{\mathbf{a}}^n, Y^n, M_2) \le n\epsilon_n.
$$

Utilizing this observation in (3.45), we continue with

$$
\begin{aligned}
&n(R_1 + R_2) \\
&\le I(M_1, M_2; Y^n) + H(M_1 | W_{\mathbf{a}}^n, Y^n) + H(M_2 | W_{\mathbf{a}}^n, Y^n) - H(M_1, M_2 | W_{\mathbf{a}}^n, Y^n) + 3n\epsilon_n
\end{aligned}
$$

$$
\begin{aligned}
&\leq I(M_1,M_2;Y^n)+I(M_1,M_2;W_{\mathbf{a}}^n,Y^n)-I(M_1;W_{\mathbf{a}}^n,Y^n)-I(M_2;W_{\mathbf{a}}^n,Y^n)+3n\epsilon_n\\
&=\sum_{i=1}^n I(M_1,M_2;Y_i|Y^{i-1})+\sum_{i=1}^n I(M_1,M_2;W_{\mathbf{a},i},Y_i|W_{\mathbf{a}}^{i-1},Y^{i-1})\\
&\qquad -\sum_{i=1}^n I(M_1;W_{\mathbf{a},i},Y_i|W_{\mathbf{a}}^{i-1},Y^{i-1})-\sum_{i=1}^n I(M_2;W_{\mathbf{a},i},Y_i|W_{\mathbf{a}}^{i-1},Y^{i-1})+3n\epsilon_n\\
&=\sum_{i=1}^n I(M_1,M_2,X_{1i},X_{2i};Y_i|Y^{i-1})+\sum_{i=1}^n I(M_1,M_2,X_{1i},X_{2i};W_{\mathbf{a},i},Y_i|T_i)\\
&\qquad -\sum_{i=1}^n I(M_1,X_{1i};W_{\mathbf{a},i},Y_i|T_i)-\sum_{i=1}^n I(M_2,X_{2i};W_{\mathbf{a},i},Y_i|T_i)+3n\epsilon_n\\
&\leq\sum_{i=1}^n I(M_1,M_2,Y^{i-1},X_{1i},X_{2i};Y_i)+\sum_{i=1}^n I(M_1,M_2,X_{1i},X_{2i};W_{\mathbf{a},i},Y_i|T_i)\\
&\qquad -\sum_{i=1}^n I(X_{1i};W_{\mathbf{a},i},Y_i|T_i)-\sum_{i=1}^n I(X_{2i};W_{\mathbf{a},i},Y_i|T_i)+3n\epsilon_n\\
&\overset{(k)}{=}\sum_{i=1}^n I(X_{1i},X_{2i};Y_i)+\sum_{i=1}^n I(X_{1i},X_{2i};W_{\mathbf{a},i},Y_i|T_i)\\
&\qquad -\sum_{i=1}^n I(X_{1i};W_{\mathbf{a},i},Y_i|T_i)-\sum_{i=1}^n I(X_{2i};W_{\mathbf{a},i},Y_i|T_i)+3n\epsilon_n\\
&=n\big(I(X_{1Q},X_{2Q};Y_Q|Q)+I(X_{1Q},X_{2Q};W_{\mathbf{a},Q},Y_Q|T_Q,Q)\\
&\qquad -I(X_{1Q};W_{\mathbf{a},Q},Y_Q|T_Q,Q)-I(X_{2Q};W_{\mathbf{a},Q},Y_Q|T_Q,Q)\big)+3n\epsilon_n,
\end{aligned}
$$

where (k) follows since $(M_1,M_2,W_{\mathbf{a}}^{i-1},Y^{i-1})\to(X_{1i},X_{2i})\to(W_{\mathbf{a},i},Y_i)$ form a Markov chain.

It remains to show the dependence balance condition in (3.33).

$$
\begin{aligned}
0&\leq I(M_1;M_2|W_{\mathbf{a}}^n,Y^n)\\
&\overset{(a)}{=} I(M_1;M_2|W_{\mathbf{a}}^n,Y^n)-I(M_1;M_2)\\
&=H(M_1|W_{\mathbf{a}}^n,Y^n)-H(M_1|M_2,W_{\mathbf{a}}^n,Y^n)-H(M_1)+H(M_1|M_2)\\
&=I(M_1;W_{\mathbf{a}}^n,Y^n|M_2)-I(M_1;W_{\mathbf{a}}^n,Y^n)\\
&=\sum_{i=1}^n I(M_1;W_{\mathbf{a},i},Y_i|M_2,W_{\mathbf{a}}^{i-1},Y^{i-1})-\sum_{i=1}^n I(M_1;W_{\mathbf{a},i},Y_i|W_{\mathbf{a}}^{i-1},Y^{i-1})
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} I(M_1, X_{1i}; W_{\mathbf{a},i}, Y_i | M_2, X_{2i}, W_{\mathbf{a}}^{i-1}, Y^{i-1}) - \sum_{i=1}^{n} I(M_1, X_{1i}; W_{\mathbf{a},i}, Y_i | W_{\mathbf{a}}^{i-1}, Y^{i-1}) \\
&\leq \sum_{i=1}^{n} I(M_1, M_2, X_{1i}; W_{\mathbf{a},i}, Y_i | X_{2i}, W_{\mathbf{a}}^{i-1}, Y^{i-1}) - \sum_{i=1}^{n} I(X_{1i}; W_{\mathbf{a},i}, Y_i | W_{\mathbf{a}}^{i-1}, Y^{i-1}) \\
&\overset{(b)}{=} \sum_{i=1}^{n} I(X_{1i}; W_{\mathbf{a},i}, Y_i | X_{2i}, W_{\mathbf{a}}^{i-1}, Y^{i-1}) - \sum_{i=1}^{n} I(X_{1i}; W_{\mathbf{a},i}, Y_i | W_{\mathbf{a}}^{i-1}, Y^{i-1}) \\
&= \sum_{i=1}^{n} I(X_{1i}; W_{\mathbf{a},i}, Y_i | X_{2i}, T_i) - \sum_{i=1}^{n} I(X_{1i}; W_{\mathbf{a},i}, Y_i | T_i), \\
&= n\big(I(X_{1Q}; W_{\mathbf{a},Q}, Y_Q | X_{2Q}, T_Q, Q) - I(X_{1Q}; W_{\mathbf{a},Q}, Y_Q | T_Q, Q)\big),
\end{aligned}
$$

where (a) follows since M_1 and M_2 are independent and (b) follows since

$$(M_1, M_2, W^{i-1}, Y^{i-1}) \to (X_{1i}, X_{2i}) \to (W_i, Y_i)$$

form a Markov chain.

Letting $X_1 = X_{1Q}, X_2 = X_{2Q}, W_{\mathbf{a}} = W_{\mathbf{a},Q}, Y = Y_Q$, and $T = T_Q$ and $n \to \infty$ completes the proof.

Acknowledgment

This chapter is, in part, a reprint of the material in the papers: Pinar Sen, Sung Hoon Lim, and Young-Han Kim, “On the Optimal Achievable Rates for Linear Computation With Random Homologous Codes,” accepted to *IEEE Transactions of Information Theory*, 2020; and Pinar Sen, Sung Hoon Lim, and Young-Han Kim, “Optimal Achievable Rates for Computation With Random Homologous Codes,” *Proceedings of IEEE International Symposium on Information Theory*, Vail, Colorado, June 2018. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] R. G. Gallager. *Information Theory and Reliable Communication.* Wiley, New York, 1968.

[2] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. Towards an algebraic network information theory: Simultaneous joint typicality decoding. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 1818–1822, June 2017.

[3] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. A joint typicality approach to compute–forward. *IEEE Trans. Inf. Theory*, 64(12):7657–7685, Dec 2018.

[4] Andries P. Hekstra and Frans M. J. Willems. Dependence balance bounds for single-output two-way channels. *IEEE Trans. Inf. Theory*, 35(1):44–53, 1989.

[5] B. Bandemer, A. El Gamal, and Y.-H. Kim. Optimal achievable rates for interference networks with random codes. *IEEE Trans. Inf. Theory*, 61(12):6536–6549, Dec 2015.

[6] Abbas El Gamal and Young-Han Kim. *Network Information Theory.* Cambridge University Press, Cambridge, 2011.

[7] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization.* Cambridge University Press, Cambridge, 2004.

Chapter 4

Optimal Achievable Rates for Broadcast Channels with Marton Coding

The techniques developed in Chapter 3 are applied to broadcast channels to establish the optimal tradeoff between the communication rates when encoding is restricted to random ensembles of Marton codes. This result indicates that Marton coding scheme, which was only analyzed along with suboptimal decoders in the literature resulting in the best known inner bound on the capacity region, cannot be improved by using more powerful decoders, such as the maximum likelihood decoder.

4.1 Formal Statement of the Problem

Consider the two-receiver discrete memoryless broadcast channel (DM-BC)

$$(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$$

in Fig. 4.1, which consists of one sender alphabet $\mathcal{X}$, two receiver alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$, and a collection of conditional probability distributions $p_{Y_1,Y_2|X}(y_1, y_2|x)$.

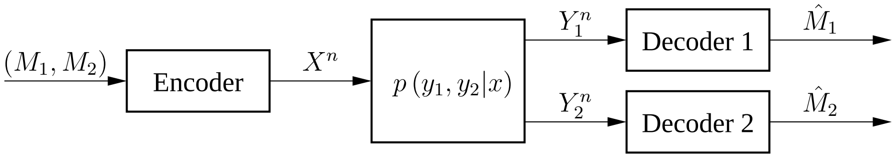


Figure 4.1. Two-receiver broadcast channel.

An (n, nR_1, nR_2) code for the two-receiver broadcast channel consists of two message sets[1], $[2^{nR_j}], j \in \{1, 2\}$ and an encoder that assigns a codeword $x^n(m_1, m_2) \in \mathcal{X}^n$ to each message pair $(m_1, m_2) \in [2^{nR_1}] \times [2^{nR_2}]$. The performance of a given code that is paired with two decoders where decoder $j \in \{1, 2\}$ assigns an estimate $\hat{m}_j$ to each received sequence y_j^n is measured by the probability of error

$$P_e^{(n)} = \mathsf{P}((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)),$$

where the message pair (M_1, M_2) is assumed to be independent and uniformly distributed. A rate pair (R_1, R_2) is said to be *achievable* if there exists a sequence of (n, nR_1, nR_2) codes for the two-receiver broadcast channel along with two decoders such that $\lim_{n\to\infty} P_e^{(n)} = 0$. The capacity region is defined as the closure of the set of achievable rate tuples.

This problem was first studied by [1–3], where the well-known Marton coding due to [3] is still the best known inner bound on the capacity region in the literature. Our main goal in this section is to investigate the optimal tradeoff between the communication rates when encoding is restricted to random ensembles of Marton codes, which is formally defined as follows.

Let $p = p(u_1, u_2)$ be a given pmf on some finite set $\mathcal{U}_1 \times \mathcal{U}_2$, and $x = x(u_1, u_2)$ be a function from $\mathcal{U}_1 \times \mathcal{U}_2$ to $\mathcal{X}$, and let $\epsilon > 0$ and $\alpha \in [0\ 1]$. The random ensemble of

[1] Throughout this section, information measures are in log base 2 to follow a similar notation with the existing literature.

Marton codes [3] is generated according to the following steps:

1. Let $\hat{R}_1 = \alpha(I(U_1;U_2) + 10\epsilon H(U_1,U_2))$ and $\hat{R}_2 = \overline{\alpha}(I(U_1;U_2) + 10\epsilon H(U_1,U_2))$, where $\overline{\alpha} := (1-\alpha)$.

2. For each $m_1 \in [2^{nR_1}]$, generate *auxiliary* codewords $u_1^n(m_1,l_1), l_1 \in [2^{n\hat{R}_1}]$, each drawn i.i.d. from $p(u_1)$. Similarly, for each $m_2 \in [2^{nR_2}]$, generate *auxiliary* codewords $u_2^n(m_2,l_2), l_2 \in [2^{n\hat{R}_2}]$, each drawn i.i.d. from $p(u_2)$.

3. At the sender, for each message pair, $(m_1,m_2) \in [2^{nR_1}] \times [2^{nR_2}]$, find an index pair $(l_1,l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]$ such that

$$(u_1^n(m_1,l_1), u_2^n(m_2,l_2)) \in \mathcal{T}_\epsilon^{(n)}(U_1,U_2),$$

and assign the codeword $x^n(m_1,m_2)$ as $x_i(m_1,m_2) = x(u_{1i}(m_1,l_1), u_{2i}(m_2,l_2)), i \in [n]$. If there are more than one such pair of (l_1,l_2), choose one of them uniformly at random; otherwise, choose one uniformly at random from $[2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]$.

We refer to the random tuple $\mathcal{C}_n := ((U_1^n(m_1,l_1) : m_1 \in [2^{nR_1}], l_1 \in [2^{n\hat{R}_1}]), (U_2^n(m_2,l_2) : m_2 \in [2^{nR_2}], l_2 \in [2^{n\hat{R}_2}]), ((L_1,L_2,x)(m_1,m_2) : m_1 \in [2^{nR_1}], m_2 \in [2^{nR_2}]))$ as the *Marton random code.* Each realization of the Marton random code $\mathcal{C}_n$ results in one instance $\{x^n(m_1,m_2) : (m_1,m_2) \in [2^{nR_1}] \times [2^{nR_2}]\}$ of such generated codewords. The random code ensemble generated in this manner is referred to as an $(n, nR_1, nR_2; p, x, \alpha, \epsilon)$ *Marton random code ensemble*, where $p = p(u_1,u_2)$ is the given pmf, $x = x(u_1,u_2)$ is the given function from $\mathcal{U}_1 \times \mathcal{U}_2$ to $\mathcal{X}$, $\alpha \in [0\ 1]$ is the parameter used in step (1), and $\epsilon > 0$ is the parameter used in steps (1) and (3). A rate pair (R_1,R_2) is said to be *achievable by the* (p,x,α,ϵ)*-distributed Marton random code ensemble* if there exits a sequence of $(n, nR_1, nR_2; p, x, \alpha, \epsilon)$ Marton random code ensembles along with the optimal decoders such that

$$\lim_{n\to\infty} \mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)] = 0,$$

where the expectation is with respect to the Marton random code $\mathcal{C}_n$. Given (p,x,α,ϵ), let $\mathscr{R}^*_{\text{BC}}(p, x, \alpha, \epsilon)$ be the set of all rate pairs achievable by the (p, x, α, ϵ)-distributed Marton random code ensemble. Given pmf $p = p(u_1, u_2)$ and function $x = x(u_1, u_2)$, the optimal rate region $\mathscr{R}^*_{\text{BC}}(p, x)$, when it exists, is defined as

$$\mathscr{R}^*_{\text{BC}}(p, x) := \text{cl}\left[\bigcup_{\alpha\in[0\ 1]} \lim_{\epsilon\to 0} \mathscr{R}^*_{\text{BC}}(p, x, \alpha, \epsilon)\right].$$

4.2 Main Result

In this section, we present a single-letter characterization of the optimal rate region.

Theorem 4.2.1. *Given a pmf $p(u_1, u_2)$ and a function $x = x(u_1, u_2)$, the optimal rate region $\mathscr{R}^*_{\text{BC}}(p, x)$ for the broadcast channel $p(y_1, y_2|x)$ is the closure of the set of rate pairs (R_1, R_2) satisfying*

$$R_1 \le I(U_1; Y_1, U_2) - \alpha I(U_1; U_2), \tag{4.1a}$$

$$R_1 \le I(U_1, U_2; Y_1) - \min\{R_2; I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\}, \tag{4.1b}$$

$$R_2 \le I(U_2; Y_2, U_1) - \overline{\alpha} I(U_1; U_2), \tag{4.1c}$$

$$R_2 \le I(U_1, U_2; Y_2) - \min\{R_1; I(U_1; Y_2, U_2) - \alpha I(U_1; U_2), I(U_1, U_2; Y_2)\}, \tag{4.1d}$$

for some $\alpha \in [0\ 1]$.

We prove Theorem 4.2.1 by showing that given a pmf $p(u_1, u_2)$, a function $x(u_1, u_2)$, and $\alpha \in [0\ 1]$, the rate region $\mathscr{R}^*_{\text{BC}}(p, x, \alpha) := \text{cl}\,[\lim_{\epsilon\to 0} \mathscr{R}^*_{\text{BC}}(p, x, \alpha, \epsilon)]$ is equal to the rate region characterized by (4.1), which we will denote as $\mathscr{R}^{**}_{\text{BC}}(p, x, \alpha)$. We take a two-step approach similar to Sections 3.3 and 3.4, and establish the inner and the outer bounds on the rate region $\mathscr{R}^*_{\text{BC}}(p, x, \alpha)$, respectively.

The inner bound is relegated to Appendix 4.A. For the outer bound, given a fixed pmf $p = p(u_1, u_2)$, a function $x = x(u_1, u_2)$ from $\mathcal{U}_1 \times \mathcal{U}_2$ to $\mathcal{X}$, $\alpha \in [0\ 1]$, and

$\delta > 0$, we define the rate region $\mathscr{R}^{**}_{\mathrm{BC}}(p, x, \alpha, \delta)$ as the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(U_1; Y_1, U_2) - \alpha I(U_1; U_2) + \delta, \tag{4.2a}$$

$$R_1 \leq I(U_1, U_2; Y_1) - \min\{R_2; I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\} + \delta, \tag{4.2b}$$

$$R_2 \leq I(U_2; Y_2, U_1) - \overline{\alpha} I(U_1; U_2) + \delta, \tag{4.2c}$$

$$R_2 \leq I(U_1, U_2; Y_2) - \min\{R_1; I(U_1; Y_2, U_2) - \alpha I(U_1; U_2), I(U_1, U_2; Y_2)\} + \delta. \tag{4.2d}$$

Note that the region $\mathscr{R}^{**}_{\mathrm{BC}}(p, x, \alpha, \delta = 0)$ is equal to $\mathscr{R}^{**}_{\mathrm{BC}}(p, x, \alpha)$ as defined in (4.1).

Proposition 4.2.1. *Let $p = p(u_1, u_2)$ be a pmf, $x = x(u_1, u_2)$ be a function, $\alpha \in [0\ 1]$, and $\epsilon > 0$. If a rate pair (R_1, R_2) is achievable by the (p, x, α, ϵ)-distributed Marton random code ensemble, then there exists a continuous $\delta'(\epsilon)$ that tends to zero monotonically as $\epsilon \to 0$ such that*

$$(R_1, R_2) \in \mathscr{R}^{**}_{\mathrm{BC}}(p, x, \alpha, \delta'(\epsilon)). \tag{4.3}$$

In particular,

$$\mathscr{R}^{*}_{\mathrm{BC}}(p, x, \alpha) \subseteq \mathscr{R}^{**}_{\mathrm{BC}}(p, x, \alpha). \tag{4.4}$$

Proof. We first start with an averaged version of Fano's inequality for a Marton random code ensemble $\mathcal{C}_n$. Consider a fixed code $\mathcal{C}_n = \mathcal{c}_n$. By Fano's inequality,

$$H(M_j | Y_j^n, \mathcal{C}_n = \mathcal{c}_n) \leq 1 + nR_j P_e^{(n)}(\mathcal{c}_n) \quad j = 1, 2.$$

Taking the expectation over Marton random code $\mathcal{C}_n$, it follows that

$$H(M_j | Y_j^n, \mathcal{C}_n) \leq 1 + nR_j \, \mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)] \leq n\epsilon_n, \quad j = 1, 2 \tag{4.5}$$

for some $\epsilon_n \to 0$ as $n \to \infty$ since $\mathsf{E}_{\mathcal{C}_n}[P_e^{(n)}(\mathcal{C}_n)] \to 0$.

We next define the indicator random variable

$$\tilde{E}_n = \mathbb{1}_{\{(U_1^n(M_1,L_1),U_2^n(M_2,L_2))\in\mathcal{T}_\epsilon^{(n)}(U_1,U_2)\}}. \tag{4.6}$$

Since $\hat{R}_1 + \hat{R}_2 = I(U_1;U_2) + 10\epsilon H(U_1,U_2)$, $\mathsf{P}(\tilde{E}_n = 0)$ tends to zero as $n \to \infty$ by the mutual covering lemma in [4, p. 208].

We are now ready to establish (4.2a). For n sufficiently large, we have

$$\begin{aligned}
&nR_1 \\
&= H(M_1|M_2,\mathcal{C}_n) \\
&\overset{(a)}{\leq} I(M_1;Y_1^n|M_2,\mathcal{C}_n) + n\epsilon_n \\
&\leq I(M_1,\tilde{E}_n;Y_1^n|M_2,\mathcal{C}_n) + n\epsilon_n \\
&\overset{(b)}{\leq} 1 + I(M_1;Y_1^n|M_2,\mathcal{C}_n,\tilde{E}_n) + n\epsilon_n \\
&\leq 1 + I(M_1;Y_1^n|M_2,\mathcal{C}_n,\tilde{E}_n = 0)\,\mathsf{P}(\tilde{E}_n = 0) \\
&\qquad\qquad + I(M_1;Y_1^n|M_2,\mathcal{C}_n,\tilde{E}_n = 1)\,\mathsf{P}(\tilde{E}_n = 1) + n\epsilon_n \\
&\leq 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + I(M_1;Y_1^n|M_2,\mathcal{C}_n,\tilde{E}_n = 1) + n\epsilon_n \\
&\leq 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + I(M_1,L_2;Y_1^n|M_2,\mathcal{C}_n,\tilde{E}_n = 1) + n\epsilon_n \\
&\leq 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + n\hat{R}_2 + I(M_1;Y_1^n|M_2,L_2,\mathcal{C}_n,\tilde{E}_n = 1) + n\epsilon_n \\
&= 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + n\hat{R}_2 + \sum_{i=1}^n I(M_1;Y_{1i}|Y_1^{i-1},M_2,L_2,\mathcal{C}_n,U_{2i},\tilde{E}_n = 1) + n\epsilon_n \\
&\leq 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + n\hat{R}_2 + \sum_{i=1}^n I(M_1,U_{1i},Y_1^{i-1},M_2,L_2,\mathcal{C}_n;Y_{1i}|U_{2i},\tilde{E}_n = 1) + n\epsilon_n \\
&\overset{(c)}{=} 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + n\hat{R}_2 + \sum_{i=1}^n I(U_{1i};Y_{1i}|U_{2i},\tilde{E}_n = 1) + n\epsilon_n \\
&\overset{(d)}{\leq} 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + n\hat{R}_2 + n(I(U_1;Y_1|U_2) + \delta_1(\epsilon)) + n\epsilon_n, \\
&\leq 1 + nR_1\,\mathsf{P}(\tilde{E}_n = 0) + n\overline{\alpha}(I(U_1;U_2) + \delta_2(\epsilon)) + n(I(U_1;Y_1|U_2) + \delta_1(\epsilon)) + n\epsilon_n, \\
&\overset{(e)}{\leq} n(I(U_1;Y_1,U_2) - \alpha I(U_1;U_2) + \delta_3(\epsilon)) + 2n\epsilon_n,
\end{aligned} \tag{4.7}$$

where (a) follows by (the averaged version of) Fano's inequality in (4.5), (b) follows since $\tilde{E}_n$ is a binary random variable, (c) follows since

$$(M_1, M_2, Y_1^{i-1}, \mathcal{C}_n, \tilde{E}_n) \to (U_{1i}, U_{2i}) \to Y_{1i}$$

form a Markov chain for every $i \in [n]$, (d) follows by the memoryless property of the channel and by Lemma 3.E.2 in Appendix 3.E since the distribution of the pair of random variables $(U_1^n(M_1, L_1), U_2^n(M_2, L_2))$ is permutation invariant by construction, and (e) follows since $\mathsf{P}(\tilde{E}_n = 0)$ tends to zero as $n \to \infty$.

For the proof of (4.2b), we start with

$$\begin{aligned} nR_1 &= H(M_1 | M_2, \mathcal{C}_n) \\ &\overset{(a)}{\leq} I(M_1; Y_1^n | M_2, \mathcal{C}_n) + n\epsilon_n \\ &= I(M_1, M_2; Y_1^n | \mathcal{C}_n) - I(M_2; Y_1^n | \mathcal{C}_n) + n\epsilon_n, \end{aligned} \tag{4.8}$$

where (a) follows by (the averaged version of) Fano's inequality in (4.5). Following arguments similar to (4.7), the first term in (4.8) can be bounded as

$$\begin{aligned} I(M_1, M_2; Y_1^n | \mathcal{C}_n) &\leq 1 + n(R_1 + R_2)\, \mathsf{P}(\tilde{E}_n = 0) + \sum_{i=1}^n I(M_1, M_2; Y_{1i} | \mathcal{C}_n, Y_1^{i-1}, \tilde{E}_n = 1) \\ &\leq n\epsilon_n + \sum_{i=1}^n I(M_1, M_2, \mathcal{C}_n, Y_1^{i-1}; Y_{1i} | \tilde{E}_n = 1) \\ &= n\epsilon_n + \sum_{i=1}^n I(M_1, M_2, \mathcal{C}_n, Y_1^{i-1}, U_{1i}, U_{2i}; Y_{1i} | \tilde{E}_n = 1) \\ &= n\epsilon_n + \sum_{i=1}^n I(U_{1i}, U_{2i}; Y_{1i} | \tilde{E}_n = 1), \\ &\leq n\epsilon_n + n(I(U_1, U_2; Y_1) + \delta_4(\epsilon)). \end{aligned} \tag{4.9}$$

For the second term in (4.8), we need the following lemma, which is proved in Appendix 4.B. This lemma is a version of Lemma 3.4.3 for Marton random code ensembles.

Lemma 4.2.1. *For every $\epsilon' > \epsilon$ and for n sufficiently large,*

$$I(M_2; Y_1^n | \mathcal{C}_n) \geq n[\min\{R_2, I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\} - \delta_5(\epsilon')] - n\epsilon_n.$$

Combining (4.8), (4.9), and Lemma 4.2.1 with $\epsilon' = 2\epsilon$, we have

$$\begin{aligned} &nR_1 \\ &\leq n[I(U_1, U_2; Y_1) - \min\{R_2, I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\} + \delta_6(\epsilon)] + 2n\epsilon_n \end{aligned} \tag{4.10}$$

for n sufficiently large.

For (4.2c) and (4.2d), we can similarly establish for receiver 2

$$nR_2 \leq n(I(U_2; Y_2, U_1) - \overline{\alpha} I(U_1; U_2) + \delta_7(\epsilon)) + 2n\epsilon_n \tag{4.11}$$

and

$$\begin{aligned} &nR_2 \\ &\leq n[I(U_1, U_2; Y_2) - \min\{R_1, I(U_1; Y_2, U_2) - \alpha I(U_1; U_2), I(U_1, U_2; Y_2)\} + \delta_8(\epsilon)] + 2n\epsilon_n \end{aligned} \tag{4.12}$$

for n sufficiently large. The proof of (4.3) follows by letting $n \to \infty$ in (4.7), (4.10), (4.11), and (4.12) and taking a continuous monotonic function

$$\delta'(\epsilon) \geq \max\{\delta_3(\epsilon), \delta_6(\epsilon), \delta_7(\epsilon), \delta_8(\epsilon)\}$$

that tends to zero as $\epsilon \to 0$. Letting $\epsilon \to 0$ in (4.3) establishes (4.4), which completes the proof of Proposition 4.2.1. □

Remark 4.2.1. *Marton coding we have analyzed involves two codewords. Marton's original coding scheme [3] uses rate splitting and superposition coding, and involves an additional codeword that carries messages for both receivers (see also [4, Proposition 8.1]). Our technique can be similarly adapted to this general version of Marton coding.*

4.3 Discussion

In this chapter, we have established a single-letter characterization for the optimal rate region of broadcast channels when the encoding is restricted to random ensembles of Marton codes. The results implies that the performance of Marton coding scheme cannot be improved by using the maximum likelihood decoder. Therefore, the gap between the achievable rate region of Marton coding scheme and the best known outer bound on the capacity region of broadcast channels is due to the lack of either a more powerful encoding scheme or a better outer bound.

4.A Proof of Achievability for Theorem 4.2.1

Let $\alpha \in [0\ 1]$ and $\epsilon > 0$. Consider an $(n, nR_1, nR_2; p, x, \alpha, \epsilon)$ Marton random code ensemble. We use the nonunique simultaneous joint typicality decoding rule in [5] to establish the achievability. Let $\epsilon' > \epsilon$. Upon receiving y_j^n at receiver $j = 1, 2$, the ϵ'-joint typicality decoder j looks for a unique $m_j \in [2^{nR_j}]$ such that

$$(u_1^n(m_1, l_1), u_2^n(m_2, l_2), y_j^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_j),$$

for some $l_1 \in [2^{n\hat{R}_1}]$, $l_2 \in [2^{n\hat{R}_2}]$ and $m_{j^c} \in [2^{nR_{j^c}}]$, where j^c denotes $\{1, 2\} \setminus j$. If the decoder $j = 1, 2$ finds such m_j, then it declares m_j as an estimate; otherwise, it declares an error.

We analyze the probability of error. It suffices to consider decoder 1, which declares an error if one or more of the following events occur

$$\begin{aligned}
\mathcal{E}_0 &= \{(U_1^n(M_1,l_1), U_2^n(M_2,l_2)) \notin \mathcal{T}_\epsilon^{(n)}(U_1,U_2) \text{ for every } (l_1,l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]\},\\
\mathcal{E}_1 &= \{(U_1^n(M_1,L_1), U_2^n(M_2,L_2), Y_1^n) \notin \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y_1)\},\\
\mathcal{E}_2 &= \{(U_1^n(m_1,l_1), U_2^n(m_2,l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y_1) \text{ for some } m_1 \neq M_1,\\
&\qquad\qquad \text{for some } (m_2,l_1,l_2) \in [2^{nR_2}] \times [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]\}.
\end{aligned}$$

By the union of events bound, $\mathsf{P}_e^{(n)}(\mathcal{C}_n) \le \mathsf{P}(\mathcal{E}_0) + \mathsf{P}(\mathcal{E}_1 \cap \mathcal{E}_0^c) + \mathsf{P}(\mathcal{E}_2 \cap \mathcal{E}_0^c)$. Since $\hat{R}_1 + \hat{R}_2 = I(U_1;U_2) + 10\epsilon H(U_1,U_2)$, by the mutual covering lemma in [4, p. 208], the probability $\mathsf{P}(\mathcal{E}_0)$ tends to zero as $n \to \infty$. By the conditional typicality lemma in [4, p. 27], the probability $\mathsf{P}(\mathcal{E}_1 \cap \mathcal{E}_0^c)$ tends to zero as $n \to \infty$. The last term can be bounded by two ways. First, by the symmetric code generation,

$$\begin{aligned}
&\mathsf{P}(\mathcal{E}_2 \cap \mathcal{E}_0^c)\\
&\le \mathsf{P}(\mathcal{E}_2)\\
&= \mathsf{P}(\mathcal{E}_2 | M_1 = M_2 = 1)\\
&\le \mathsf{P}((U_1^n(m_1,l_1), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,Y_1) \text{ for some } m_1 \neq 1, \text{ for some } l_1 \in [2^{n\hat{R}_1}] | M_1 = 1),
\end{aligned}$$

which tends to zero as $n \to \infty$ if $R_1 + \hat{R}_1 \le I(U_1;Y_1) - \delta(\epsilon')$ by the packing lemma in [4]. Letting $\hat{R}_1 = \alpha(I(U_1;U_2) + 10\epsilon H(U_1,U_2))$, we have

$$R_1 \le \max\{0, I(U_1;Y_1) - \alpha I(U_1;U_2) - 2\delta(\epsilon')\}. \tag{4.13}$$

Secondly, we can decompose the event $\mathcal{E}_2 = \mathcal{E}_{21} \cup \mathcal{E}_{22}$ such that

$$\begin{aligned}
\mathcal{E}_{21} &= \{(U_1^n(m_1,l_1), U_2^n(M_2,l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y_1) \text{ for some } m_1 \neq M_1,\\
&\qquad\qquad \text{for some } (l_1,l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]\},\\
\mathcal{E}_{22} &= \{(U_1^n(m_1,l_1), U_2^n(m_2,l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y_1) \text{ for some } m_1 \neq M_1,
\end{aligned}$$

$$\text{for some } m_2 \neq M_2, \text{ for some } (l_1, l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]\}.$$

We start with bounding $\mathsf{P}(\mathcal{E}_{22})$ as follows:

$$\begin{aligned}
&\mathsf{P}(\mathcal{E}_{22}) \\
&= \mathsf{P}(\mathcal{E}_{22} | M_1 = M_2 = 1) \\
&= \mathsf{P}((U_1^n(m_1, l_1), U_2^n(m_2, l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) \text{ for some } m_1 \neq 1, \\
&\qquad\qquad \text{for some } m_2 \neq 1, \text{ for some } (l_1, l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}] | M_1 = M_2 = 1) \\
&\leq \sum_{\substack{m_1 \neq 1, \\ m_2 \neq 2}} \sum_{l_1, l_2} \mathsf{P}((U_1^n(m_1, l_1), U_2^n(m_2, l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) | M_1 = M_2 = 1) \\
&\leq \sum_{\substack{m_1 \neq 1, \\ m_2 \neq 2}} \sum_{l_1, l_2} \sum_{\substack{(u_1^n, u_2^n, y_1^n) \in \\ \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1)}} \mathsf{P}(U_1^n(m_1, l_1) = u_1^n, U_2^n(m_2, l_2) = u_2^n, Y_1^n = y_1^n | M_1 = M_2 = 1) \\
&\overset{(a)}{=} \sum_{\substack{m_1 \neq 1, \\ m_2 \neq 2}} \sum_{l_1, l_2} \sum_{\substack{(u_1^n, u_2^n, y_1^n) \in \\ \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1)}} p(y_1^n | M_1 = M_2 = 1) \prod_{i=1}^{n} p_{U_1}(u_{1i}) p_{U_2}(u_{2i}) \\
&\leq \sum_{\substack{m_1 \neq 1, \\ m_2 \neq 2}} \sum_{l_1, l_2} \sum_{\substack{(u_1^n, u_2^n, y_1^n) \in \\ \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1)}} p(y_1^n | M_1 = M_2 = 1) 2^{-n(H(U_1) + H(U_2) - \delta(\epsilon'))} \\
&\leq \sum_{\substack{m_1 \neq 1, \\ m_2 \neq 2}} \sum_{l_1, l_2} 2^{-n(H(U_1) + H(U_2) - H(U_1, U_2 | Y_1) - 2\delta(\epsilon'))} \\
&\leq 2^{n(R_1 + R_2 + \hat{R}_1 + \hat{R}_2)} 2^{-n(H(U_1) + H(U_2) - H(U_1, U_2 | Y_1) - 2\delta(\epsilon'))},
\end{aligned}$$

where (a) follows since given $\{M_1 = M_2 = 1\}$, the pair $(U_1^n(m_1, l_1), U_2^n(m_2, l_2))$ for $m_1 \neq 1, m_2 \neq 1$ is i.i.d. with respect to the product pmf $p(u_1)p(u_2)$ and is independent from Y_1^n. Substituting $\hat{R}_1 + \hat{R}_2 = I(U_1; U_2) + 10\epsilon H(U_1, U_2)$, it follows that $\mathsf{P}(\mathcal{E}_{22})$ tends to zero as $n \to \infty$ if $R_1 + R_2 \leq I(U_1, U_2; Y_1) - 3\delta(\epsilon')$.

We next bound the probability $\mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c)$. Define the events $\mathcal{M}_1 := \{M_1 =$

$M_2 = 1\}$ and $\mathcal{M}_2 := \{L_1 = L_2 = 1\}$. By the symmetry of the code generation,

$$\mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c) = \mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c | \mathcal{M}_1, \mathcal{M}_2). \tag{4.14}$$

To see this, define the tuple of auxiliary codewords for sender $j = 1, 2$ as $\tilde{\mathcal{C}}_n(j) := (U_j^n(m_j, l_j) : m_j \in [2^{nR_j}], l_j \in [2^{n\hat{R}_j}])$. We first show that (M_1, M_2, L_1, L_2) is uniformly distributed over its support. It suffices to show that for every $(m_1, m_2, l_1, l_2) \in [2^{nR_1}] \times [2^{nR_2}] \times [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]$,

$$\mathsf{P}(M_1 = m_1, M_2 = m_2, L_1 = l_1, L_2 = l_2) = \mathsf{P}(M_1 = 1, M_2 = 1, L_1 = 1, L_2 = 1).$$

Fix a tuple $(m_1, m_2, l_1, l_2) \in [2^{nR_1}] \times [2^{nR_2}] \times [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]$. Given $\tilde{\mathcal{C}}_n(j) = \mathcal{C}_j$, let $\sigma_j(\mathcal{C}_j)$ denote the permuted version of $\mathcal{C}_j$ such that

$$\{u_j^n(m_j, l_j') \in \mathcal{C}_j : l_j' \in [2^{n\hat{R}_j}]\} = \{\tilde{u}_j^n(1, l_j') \in \sigma_j(\mathcal{C}_j) : l_j' \in [2^{n\hat{R}_j}]\}$$

and $u_j^n(m_j, l_j) \in \mathcal{C}_j$ and $\tilde{u}_j^n(1,1) \in \sigma_j(\mathcal{C}_j)$ satisfy

$$u_j^n(m_j, l_j) = \tilde{u}_j^n(1, 1).$$

Then, we have

$$\begin{aligned}
&\mathsf{P}(M_1 = m_1, M_2 = m_2, L_1 = l_1, L_2 = l_2) \\
&= \sum_{\mathcal{C}_1, \mathcal{C}_2} \mathsf{P}(M_1 = m_1, M_2 = m_2, L_1 = l_1, L_2 = l_2, \tilde{\mathcal{C}}_n(1) = \mathcal{C}_1, \tilde{\mathcal{C}}_n(2) = \mathcal{C}_2) \\
&\overset{(a)}{=} \sum_{\mathcal{C}_1, \mathcal{C}_2} \mathsf{P}(M_1 = m_1, M_2 = m_2)\, \mathsf{P}(\tilde{\mathcal{C}}_n(1) = \mathcal{C}_1)\, \mathsf{P}(\tilde{\mathcal{C}}_n(2) = \mathcal{C}_2) \\
&\qquad\qquad \mathsf{P}(L_1 = l_1, L_2 = l_2 | M_1 = m_1, M_2 = m_2, \tilde{\mathcal{C}}_n(1) = \mathcal{C}_1, \tilde{\mathcal{C}}_n(2) = \mathcal{C}_2) \\
&\overset{(b)}{=} \sum_{\mathcal{C}_1, \mathcal{C}_2} \mathsf{P}(M_1 = 1, M_2 = 1)\, \mathsf{P}(\tilde{\mathcal{C}}_n(1) = \sigma_1(\mathcal{C}_1))\, \mathsf{P}(\tilde{\mathcal{C}}_n(2) = \sigma_2(\mathcal{C}_2)) \\
&\qquad\qquad \mathsf{P}(L_1 = 1, L_2 = 1 | M_1 = 1, M_2 = 1, \tilde{\mathcal{C}}_n(1) = \sigma_1(\mathcal{C}_1) \tilde{\mathcal{C}}_n(2) = \sigma_2(\mathcal{C}_2))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\mathcal{C}_1,\mathcal{C}_2} \mathsf{P}(M_1 = 1, M_2 = 1, L_1 = 1, L_2 = 1, \tilde{\mathcal{C}}_n(1) = \sigma_1(\mathcal{C}_1), \tilde{\mathcal{C}}_n(2) = \sigma_2(\mathcal{C}_2)) \\
&= \mathsf{P}(M_1 = 1, M_2 = 1, L_1 = 1, L_2 = 1),
\end{aligned}
$$

where (a) follows since $(M_1, M_2, \tilde{\mathcal{C}}_n(1), \tilde{\mathcal{C}}_n(2))$ are independent, (b) follows since (M_1, M_2) is uniformly distributed and $\tilde{\mathcal{C}}_n(j) \overset{d}{=} \sigma_j(\tilde{\mathcal{C}}_n(j))$, $j = 1, 2$.

Following similar arguments, we can now prove the claim in (4.14).

$$
\begin{aligned}
&\mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c) \\
&= \mathsf{P}((U_1^n(m_1', l_1'), U_2^n(M_2, l_2'), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) \text{ for some } m_1' \neq M_1, \\
&\qquad\qquad \text{for some } (l_1', l_2') \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}], (U_1^n(M_1, L_1), U_2^n(M_2, L_2)) \in \mathcal{T}_{\epsilon}^{(n)}(U_1, U_2)) \\
&= \sum_{\substack{m_1, m_2, \\ l_1, l_2}} \sum_{\mathcal{C}_1, \mathcal{C}_2} \mathsf{P}\left(\begin{array}{c}
(U_1^n(m_1', l_1'), U_2^n(M_2, l_2'), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) \\
\text{for some } m_1' \neq M_1, \ \text{for some } (l_1', l_2') \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}], \\
(U_1^n(M_1, L_1), U_2^n(M_2, L_2)) \in \mathcal{T}_{\epsilon}^{(n)}(U_1, U_2), \\
(M_1, M_2, L_1, L_2) = (m_1, m_2, l_1, l_2), (\tilde{\mathcal{C}}_n(1), \tilde{\mathcal{C}}_n(2)) = (\mathcal{C}_1, \mathcal{C}_2)
\end{array}\right) \\
&= \sum_{\substack{m_1, m_2, \\ l_1, l_2}} \sum_{\mathcal{C}_1, \mathcal{C}_2} \mathsf{P}(M_1 = m_1, M_2 = m_2)\, \mathsf{P}\left((\tilde{\mathcal{C}}_n(1), \tilde{\mathcal{C}}_n(2)) = (\mathcal{C}_1, \mathcal{C}_2)\right) \\
&\quad \mathsf{P}\left(\begin{array}{c|c}
(U_1^n(m_1', l_1'), U_2^n(M_2, l_2'), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) & M_1 = m_1, \\
\text{for some } m_1' \neq M_1, \ \text{for some } (l_1', l_2') \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}], & M_2 = m_2, \\
(U_1^n(M_1, L_1), U_2^n(M_2, L_2)) \in \mathcal{T}_{\epsilon}^{(n)}(U_1, U_2), & \tilde{\mathcal{C}}_n(1) = \mathcal{C}_1, \\
(L_1, L_2) = (l_1, l_2)) & \tilde{\mathcal{C}}_n(2) = \mathcal{C}_2
\end{array}\right) \\
&= \sum_{\substack{m_1, m_2, \\ l_1, l_2}} \sum_{\mathcal{C}_1, \mathcal{C}_2} \mathsf{P}(M_1 = 1, M_2 = 1)\, \mathsf{P}\Big((\tilde{\mathcal{C}}_n(1), \tilde{\mathcal{C}}_n(2)) = \big(\sigma_1(\mathcal{C}_1), \sigma_2(\mathcal{C}_2)\big)\Big) \\
&\quad \mathsf{P}\left(\begin{array}{c|c}
(U_1^n(m_1', l_1'), U_2^n(M_2, l_2'), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) & M_1 = 1, \\
\text{for some } m_1' \neq M_1, \ \text{for some } (l_1', l_2') \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}], & M_2 = 1, \\
(U_1^n(M_1, L_1), U_2^n(M_2, L_2)) \in \mathcal{T}_{\epsilon}^{(n)}(U_1, U_2), & \tilde{\mathcal{C}}_n(1) = \sigma_1(\mathcal{C}_1), \\
(L_1, L_2) = (1, 1)) & \tilde{\mathcal{C}}_n(2) = \sigma_2(\mathcal{C}_2)
\end{array}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{\substack{m_1,m_2,\\ l_1,l_2}} \sum_{\mathcal{C}_1,\mathcal{C}_2} \mathsf{P}\left(\begin{array}{c} (U_1^n(m_1',l_1'),U_2^n(M_2,l_2'),Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y_1) \\ \text{for some } m_1' \neq M_1, \text{ for some } (l_1',l_2') \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}], \\ (U_1^n(M_1,L_1),U_2^n(M_2,L_2)) \in \mathcal{T}_{\epsilon}^{(n)}(U_1,U_2), \\ (M_1,M_2,L_1,L_2) = (1,1,1,1), (\tilde{\mathcal{C}}_n(1),\tilde{\mathcal{C}}_n(2)) = \big(\sigma_1(\mathcal{C}_1),\sigma_2(\mathcal{C}_2)\big) \end{array}\right) \\
&= \sum_{\substack{m_1,m_2,\\ l_1,l_2}} \mathsf{P}\left(\mathcal{E}_{21} \cap \mathcal{E}_0^c, (M_1,M_2,L_1,L_2) = (1,1,1,1)\right) \\
&= \sum_{\substack{m_1,m_2,\\ l_1,l_2}} \mathsf{P}\left((M_1,M_2,L_1,L_2) = (1,1,1,1)\right) \mathsf{P}\left(\mathcal{E}_{21} \cap \mathcal{E}_0^c | \mathcal{M}_1,\mathcal{M}_2\right) \\
&\overset{(a)}{=} \mathsf{P}\left(\mathcal{E}_{21} \cap \mathcal{E}_0^c | \mathcal{M}_1,\mathcal{M}_2\right),
\end{aligned}
$$

where (a) follows since (M_1,M_2,L_1,L_2) is uniformly distributed.

To bound $\mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c)$, we continue from (4.14) as follows.

$$
\begin{aligned}
&\mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c | \mathcal{M}_1,\mathcal{M}_2) \\
&\leq \sum_{m_1 \neq 1} \sum_{l_1,l_2} \mathsf{P}\left(\begin{array}{c|c} (U_1^n(m_1,l_1),U_2^n(1,l_2),Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y), & \mathcal{M}_1, \\ (U_1^n(1,1),U_2^n(1,1)) \in \mathcal{T}_{\epsilon}^{(n)}(U_1,U_2) & \mathcal{M}_2 \end{array}\right) \\
&\overset{(a)}{\leq} \sum_{m_1 \neq 1} \sum_{l_1,l_2} \mathsf{P}\left(\begin{array}{c|c} (U_1^n(m_1,l_1),U_2^n(1,l_2),Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y), & \mathcal{M}_1, \\ (U_1^n(1,1),U_2^n(1,1)) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2) & \mathcal{M}_2 \end{array}\right) \\
&\leq \sum_{m_1 \neq 1} \sum_{l_1} \mathsf{P}\left(\begin{array}{c|c} (U_1^n(m_1,l_1),U_2^n(1,1),Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y), & \mathcal{M}_1, \\ (U_1^n(1,1),U_2^n(1,1)) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2) & \mathcal{M}_2 \end{array}\right) + \qquad (4.15) \\
&\qquad \sum_{m_1 \neq 1} \sum_{l_1} \sum_{l_2 \neq 1} \mathsf{P}\left(\begin{array}{c|c} (U_1^n(m_1,l_1),U_2^n(1,l_2),Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y), & \mathcal{M}_1, \\ (U_1^n(1,1),U_2^n(1,1)) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2) & \mathcal{M}_2 \end{array}\right), \qquad (4.16)
\end{aligned}
$$

where (a) follows since $\epsilon' > \epsilon$. The summation term in (4.15) can be bounded as

$$
\sum_{m_1 \neq 1} \sum_{l_1} \mathsf{P}\left(\begin{array}{c|c} (U_1^n(m_1,l_1),U_2^n(1,1),Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2,Y), & \mathcal{M}_1, \\ (U_1^n(1,1),U_2^n(1,1)) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1,U_2) & \mathcal{M}_2 \end{array}\right)
$$

$$
\leq \sum_{m_1 \neq 1} \sum_{l_1} \sum_{\substack{(u_1^n, u_2^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2)}} \sum_{\substack{(\tilde{u}_1^n, y_1^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, Y_1 | u_2^n)}} \mathsf{P} \left(\begin{array}{c|c} U_1^n(m_1, l_1) = \tilde{u}_1^n, U_1^n(1,1) = u_1^n, & \mathcal{M}_1, \\ U_2^n(1,1) = u_2^n, Y_1^n = y_1^n & \mathcal{M}_2 \end{array} \right)
$$

$$
\overset{(a)}{=} \sum_{m_1 \neq 1} \sum_{l_1}
$$

$$
\sum_{\substack{(u_1^n, u_2^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2)}} \sum_{\substack{(\tilde{u}_1^n, y_1^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, Y_1 | u_2^n)}} \mathsf{P} \left(\begin{array}{c|c} U_1^n(m_1, l_1) = \tilde{u}_1^n, & \mathcal{M}_1, \\ U_1^n(1,1) = u_1^n, U_2^n(1,1) = u_2^n & \mathcal{M}_2 \end{array} \right) p(y_1^n | u_1^n, u_2^n)
$$

$$
\overset{(b)}{\leq} 2^{n(\hat{R}_1 + \hat{R}_2)} \sum_{m_1 \neq 1} \sum_{l_1}
$$

$$
\sum_{\substack{(u_1^n, u_2^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2)}} \sum_{\substack{(\tilde{u}_1^n, y_1^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, Y_1 | u_2^n)}} \mathsf{P} \left(\begin{array}{c} U_1^n(m_1, l_1) = \tilde{u}_1^n, \\ U_1^n(1,1) = u_1^n, U_2^n(1,1) = u_2^n \end{array} \right) p(y_1^n | u_1^n, u_2^n)
$$

$$
\overset{(c)}{\leq} 2^{n(\hat{R}_1 + \hat{R}_2)} \sum_{m_1 \neq 1} \sum_{l_1} \sum_{\substack{(u_1^n, u_2^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2)}} \sum_{\substack{(\tilde{u}_1^n, y_1^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, Y_1 | u_2^n)}} p(y_1^n | u_1^n, u_2^n) 2^{-n(2H(U_1) + H(U_2) - \delta(\epsilon'))}
$$

$$
\leq 2^{n(\hat{R}_1 + \hat{R}_2)} \sum_{m_1 \neq 1} \sum_{l_1} \sum_{\substack{(u_1^n, u_2^n) \\ \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2)}} 2^{n(H(U_1 | Y_1, U_2) + \delta(\epsilon'))} 2^{-n(2H(U_1) + H(U_2) - \delta(\epsilon'))}
$$

$$
\leq 2^{n(\hat{R}_1 + \hat{R}_2)} \sum_{m_1 \neq 1} \sum_{l_1} 2^{n(H(U_1, U_2) + \delta(\epsilon'))} 2^{n(H(U_1 | Y_1, U_2) + \delta(\epsilon'))} 2^{-n(2H(U_1) + H(U_2) - \delta(\epsilon'))}
$$

$$
\leq 2^{n(R_1 + 2\hat{R}_1 + \hat{R}_2 + H(U_1, U_2) + H(U_1 | Y_1, U_2) - 2H(U_1) - H(U_2) + 3\delta(\epsilon'))}
$$

$$
= 2^{n(R_1 + 2\hat{R}_1 + \hat{R}_2 - I(U_1; U_2) - I(U_1; Y_1, U_2) + 3\delta(\epsilon'))},
$$

where (a) follows since given $(\mathcal{M}_1, \mathcal{M}_2)$ the tuple

$$
U_1^n(m_1, l_1) \to (U_1^n(1,1), U_2^n(1,1)) \to Y_1^n
$$

form a Markov chain, (b) follows by [6, Lemma 11] since the tuple

$$
(U_1^n(m_1, l_1), U_1^n(1,1), U_2^n(1,1))
$$

is independent of the event $\mathcal{M}_1$ and (M_1, M_2, L_1, L_2) is uniformly distributed, and (c) follows since the tuple $(U_1^n(m_1, l_1), U_1^n(1,1), U_2^n(1,1))$ is i.i.d. with respect to the product pmf $p(u_1)p(u_1)p(u_2)$.

Similarly, the summation term in (4.16) can be bounded as

$$\sum_{m_1 \neq 1} \sum_{l_1} \sum_{l_2 \neq 1} \mathsf{P} \left(\begin{array}{c|l} (U_1^n(m_1, l_1), U_2^n(1, l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y), & \mathcal{M}_1, \\ (U_1^n(1,1), U_2^n(1,1)) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2) & \mathcal{M}_2) \end{array} \right)$$
$$\leq 2^{n(R_1 + 2\hat{R}_1 + 2\hat{R}_2 - 2I(U_1;U_2) - I(U_1,U_2;Y_1) + 3\delta(\epsilon'))}.$$

Therefore, $\mathsf{P}(\mathcal{E}_{21} \cap \mathcal{E}_0^c)$ tends to zero as $n \to \infty$ if $R_1 + 2\hat{R}_1 + \hat{R}_2 \leq I(U_1;U_2) + I(U_1;Y_1,U_2) - 3\delta(\epsilon')$ and $R_1 + 2\hat{R}_1 + 2\hat{R}_2 \leq 2I(U_1;U_2) + I(U_1,U_2;Y_1) - 3\delta(\epsilon')$. Letting $\hat{R}_1 = \alpha(I(U_1;U_2) + 10\epsilon H(U_1,U_2))$ and $\hat{R}_2 = \overline{\alpha}(I(U_1;U_2) + 10\epsilon H(U_1,U_2))$ results in $R_1 \leq I(U_1;Y_1,U_2) - \alpha I(U_1;U_2) - 4\delta(\epsilon')$ and $R_1 \leq I(U_1,U_2;Y_1) - 4\delta(\epsilon')$.

Combining with (4.13), the probability of error at Decoder 1 tends to zero as $n \to \infty$ if

$$R_1 \leq \max\{0, I(U_1;Y_1) - \alpha I(U_1;U_2) - 4\delta(\epsilon')\}, \tag{4.17}$$

or

$$R_1 \leq I(U_1;Y_1,U_2) - \alpha I(U_1;U_2) - 4\delta(\epsilon'), \tag{4.18a}$$
$$R_1 + R_2 \leq I(U_1,U_2;Y_1) - 4\delta(\epsilon'). \tag{4.18b}$$

Repeating similar steps, the probability of error at Decoder 2 tends to zero as $n \to \infty$ if

$$R_2 \leq \max\{0, I(U_2;Y_2) - \overline{\alpha} I(U_1;U_2) - 4\delta(\epsilon')\}, \tag{4.19}$$

or

$$R_2 \leq I(U_2;Y_2,U_1) - \overline{\alpha} I(U_1;U_2) - 4\delta(\epsilon'), \tag{4.20a}$$

$$R_1 + R_2 \leq I(U_1, U_2; Y_2) - 4\delta(\epsilon'). \tag{4.20b}$$

If we denote the set of rate pairs satisfying (4.17) or (4.18) as $\mathscr{R}_{\mathrm{BC},1}(p, x, \alpha, \delta(\epsilon'))$, and denote the set of rate pairs satisfying (4.19) or (4.20) as $\mathscr{R}_{\mathrm{BC},2}(p, x, \alpha, \delta(\epsilon'))$, then the rate region $\mathscr{R}_{\mathrm{BC},1}(p, x, \alpha, \delta(\epsilon')) \cap \mathscr{R}_{\mathrm{BC},2}(p, x, \alpha, \delta(\epsilon'))$ is achievable by the ϵ'-typicality decoders. Define the rate regions $\mathscr{R}_{\mathrm{BC},j}(p, x, \alpha) := \mathscr{R}_{\mathrm{BC},j}(p, x, \alpha, \delta(\epsilon') = 0)$, $j = 1, 2$. Let $\epsilon' = 2\epsilon$. Taking $\epsilon \to 0$ and then taking the closure implies

$$\mathscr{R}_{\mathrm{BC},1}(p, x, \alpha) \cap \mathscr{R}_{\mathrm{BC},2}(p, x, \alpha) \ \subseteq\ \mathscr{R}^{*}_{\mathrm{BC}}(p, x, \alpha).$$

The achievability proof follows from the next lemma that provides an equivalent characterization for the rate region in Theorem 4.2.1.

Lemma 4.A.1. *For any input pmf $p = p(u_1, u_2)$, function $x = x(u_1, u_2)$, and $\alpha \in [0\ 1]$,*

$$\mathscr{R}^{**}_{\mathrm{BC}}(p, x, \alpha) = \mathscr{R}_{\mathrm{BC},1}(p, x, \alpha) \cap \mathscr{R}_{\mathrm{BC},2}(p, x, \alpha).$$

Proof. Fix pmf $p = p(u_1, u_2)$, function $x = x(u_1, u_2)$ and $\alpha \in [0\ 1]$. It suffices to show that the rate region $\mathscr{R}_{\mathrm{BC},1}(p, x, \alpha)$ is equivalent to the set of rate pairs (R_1, R_2) that satisfy (4.1a)-(4.1b). We first show that any rate pair in $\mathscr{R}_{\mathrm{BC},1}(p, x, \alpha)$ satisfies (4.1a)-(4.1b). Suppose that the rate pair $(R_1, R_2) \in \mathscr{R}_{\mathrm{BC},1}(p, x, \alpha)$, which implies that

$$R_1 \leq I(U_1; Y_1, U_2) - \alpha I(U_1; U_2),$$

and

$$\begin{aligned} R_1 &\leq \max\{0, I(U_1; Y_1) - \alpha I(U_1; U_2), I(U_1, U_2; Y_1) - R_2\} \\ &= I(U_1, U_2; Y_1) - \min\{I(U_1, U_2; Y_1), I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), R_2\}. \end{aligned}$$

Therefore, (R_1, R_2) satisfies (4.1a)-(4.1b).

For the other direction, suppose that the rate pair (R_1, R_2) satisfies (4.1a)-(4.1b). Assume also that

$$R_2 < \min\{I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\}.$$

It then follows that

$$\begin{aligned} R_1 &\leq I(U_1; Y_1, U_2) - \alpha I(U_1; U_2), \\ R_1 &\leq I(U_1, U_2; Y_1) - R_2. \end{aligned}$$

So, $(R_1, R_2) \in \mathscr{R}_{\mathrm{BC},1}(p, x, \alpha)$. If instead

$$R_2 \geq \min\{I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\},$$

then

$$\begin{aligned} R_1 &\leq I(U_1; Y_1, U_2) - \alpha I(U_1; U_2), \\ R_1 &\leq I(U_1, U_2; Y_1) - \min\{I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\} \\ &= \max\{0, I(U_1; Y_1) - \alpha I(U_1; U_2)\}. \end{aligned}$$

Therefore, $(R_1, R_2) \in \mathscr{R}_{\mathrm{BC},1}(p, x, \alpha)$, which completes the proof of the lemma. □

4.B Proof of Lemma 4.2.1

Let $\epsilon' > \epsilon$. First, by (the averaged version of) Fano's lemma in (4.5), we have

$$I(M_2; Y_1^n | \mathcal{C}_n) \geq I(M_2; M_1, Y_1^n | \mathcal{C}_n) - n\epsilon_n.$$

Therefore, it suffices to prove that for n sufficiently large,

$$I(M_2; M_1, Y_1^n|\mathcal{C}_n) \geq n[\min\{R_2, I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\} - \delta(\epsilon') - 2\epsilon_n],$$

for some $\delta(\epsilon')$ that tends to zero as $\epsilon' \to 0$.

Similar to [7], we will show that given M_1, Y_1^n and $\mathcal{C}_n$, a relatively short list $\mathcal{L} \subseteq [2^{nR_2}]$ can be constructed that contains M_2 with high probability. Define a random set

$$\begin{aligned}\mathcal{L} = \{m_2 \in [2^{nR_2}] : (U_1^n(M_1, l_1), &U_2^n(m_2, l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1) \\ &\text{for some } (l_1, l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}]\}.\end{aligned}$$

Note that the set $\mathcal{L}$ is random with the underlying distribution on $(M_1, Y_1^n, \mathcal{C}_n)$, which is induced by drawing a Marton random code $\mathcal{C}_n$ and using this code to encode $U_1^n(M_1, L_1)$ and $U_2^n(M_2, L_2)$ into $X^n(M_1, M_2)$ that lead to Y_1^n through the DM-BC $p(y_1, y_2|x)$. We first bound the probability that an incorrect message is in the random set $\mathcal{L}$. Define the events $\mathcal{M}_1 = \{M_1 = M_2 = 1\}$ and $\mathcal{M}_2 = \{L_1 = L_2 = 1\}$. The indicator random variable $\tilde{E}_n$ is as defined in (4.6). By the symmetry of the code generation discussed in Appendix 4.A, for every $m_2 \neq M_2 \in [2^{nR_2}]$

$$\mathsf{P}(m_2 \in \mathcal{L}, \tilde{E}_n = 1) = \mathsf{P}(m_2 \in \mathcal{L}, \tilde{E}_n = 1|\mathcal{M}_1, \mathcal{M}_2), \tag{4.21}$$

which is easy to see following similar steps to the proof of (4.14). We will use the conditioned version to bound the probability term in (4.21). For every $m_2 \neq 1 \in [2^{nR_2}]$,

$$\begin{aligned}&\mathsf{P}(m_2 \in \mathcal{L}, \tilde{E}_n = 1|\mathcal{M}_1, \mathcal{M}_2) \\ &\overset{(a)}{=} \mathsf{P}((U_1^n(1, l_1), U_2^n(m_2, l_2), Y_1^n) \in \mathcal{T}_{\epsilon'}^{(n)} \text{ for some } (l_1, l_2) \in [2^{n\hat{R}_1}] \times [2^{n\hat{R}_2}], \\ &\qquad\qquad (U_1^n(1,1), U_2^n(1,1)) \in \mathcal{T}_{\epsilon}^{(n)}|\mathcal{M}_1, \mathcal{M}_2)\end{aligned}$$

$$\overset{(b)}{\leq} \sum_{l_2} \sum_{\substack{(u_1^n, u_2^n) \in \\ \mathcal{T}_{\epsilon}^{(n)}(U_1, U_2)}} \sum_{\substack{(\tilde{u}_2^n, y_1^n) \in \\ \mathcal{T}_{\epsilon'}^{(n)}(U_2, Y_1 | u_1^n)}} \mathsf{P}\left(\begin{array}{c|c} U_1^n(1,1) = u_1^n, U_2^n(1,1) = u_2^n, & \mathcal{M}_1, \\ U_2^n(m_2, l_2) = \tilde{u}_2^n, Y_1^n = y_1^n & \mathcal{M}_2 \end{array} \right)$$

$$+ \sum_{l_1 \neq 1} \sum_{l_2} \sum_{\substack{(u_1^n, u_2^n) \in \\ \mathcal{T}_{\epsilon}^{(n)}(U_1, U_2)}} \sum_{\substack{(\tilde{u}_1^n, \tilde{u}_2^n, y_1^n) \in \\ \mathcal{T}_{\epsilon'}^{(n)}(U_1, U_2, Y_1)}} \mathsf{P}\left(\begin{array}{c|c} U_1^n(1,1) = u_1^n, U_2^n(1,1) = u_2^n, Y_1^n = y_1^n, & \mathcal{M}_1, \\ U_1^n(m_1, l_1) = \tilde{u}_1^n, U_2^n(m_2, l_2) = \tilde{u}_2^n & \mathcal{M}_2 \end{array} \right) \tag{4.22}$$

where (b) follows by the union of events bound and by decomposing the event in (a) onto two sets: $\{l_1 = 1\}$ and $\{l_1 \neq 1\}$. Two summation terms on the right hand side of (4.22) can be bounded by using similar arguments to the proof of the inner bound for Theorem 4.2.1 (refer to the bounds on (4.15) and (4.16) in Appendix 4.A) to get

$$\mathsf{P}(m_2 \in \mathcal{L}, \tilde{E}_n = 1) \leq 2^{-n(I(U_2;Y_1,U_1) - \overline{\alpha} I(U_1;U_2) - 4\delta(\epsilon'))} + 2^{-n(I(U_1,U_2;Y_1) - 4\delta(\epsilon'))}.$$

Since $\mathsf{P}(\tilde{E}_n = 1)$ tends to one as $n \to \infty$, for n sufficiently large, $\mathsf{P}(m_2 \in \mathcal{L} | \tilde{E}_n = 1) \leq \mathsf{P}(m_2 \in \mathcal{L}, \tilde{E}_n = 1) 2^{\epsilon}$. The expected cardinality of $\mathcal{L}$ given $\{\tilde{E}_n = 1\}$ is then bounded as

$$\begin{aligned} \mathsf{E}(|\mathcal{L}| | \tilde{E}_n = 1) &\leq 1 + \sum_{m_2 \neq M_2} \mathsf{P}(m_2 \in \mathcal{L} | \tilde{E}_n = 1) \\ &\leq 1 + 2^{n(R_2 - I(U_2;Y_1,U_1) + \overline{\alpha} I(U_1;U_2) + 4\delta(\epsilon') + \frac{\epsilon}{n})} + 2^{n(R_2 - I(U_1,U_2;Y_1) + 4\delta(\epsilon') + \frac{\epsilon}{n})} \\ &= 1 + 2^{n(R_2 - I(U_2;Y_1,U_1) + \overline{\alpha} I(U_1;U_2) + 4\delta(\epsilon') + \epsilon_n)} + 2^{n(R_2 - I(U_1,U_2;Y_1) + 4\delta(\epsilon') + \epsilon_n)} \end{aligned} \tag{4.23}$$

for n sufficiently large.

Define another indicator random variable $\tilde{F}_n = \mathbb{1}_{\{M_2 \in \mathcal{L}\}}$. Since $\epsilon' > \epsilon$ and $\mathsf{P}(\tilde{E}_n = 1)$ tends to one as $n \to \infty$, by the conditional typicality lemma in [4, p. 27], $\mathsf{P}(\tilde{F}_n = 1)$

tends to one as $n \to \infty$. Then, for n sufficiently large, we have

$$\begin{aligned}
&H(M_2|\mathcal{C}_n, M_1, Y_1^n) \\
&= H(M_2|\mathcal{C}_n, M_1, Y_1^n, \tilde{E}_n, \tilde{F}_n) + I(M_2; \tilde{E}_n, \tilde{F}_n|\mathcal{C}_n, M_1, Y_1^n) \\
&\leq H(M_2|\mathcal{C}_n, M_1, Y_1^n, \tilde{E}_n, \tilde{F}_n) + 2 \\
&\leq 2 + \mathsf{P}(\tilde{F}_n = 0) H(M_2|\mathcal{C}_n, M_1, Y_1^n, \tilde{E}_n, \tilde{F}_n = 0) + H(M_2|\mathcal{C}_n, M_1, Y_1^n, \tilde{E}_n, \tilde{F}_n = 1) \\
&\leq 2 + nR_2 \, \mathsf{P}(\tilde{F}_n = 0) + H(M_2|\mathcal{C}_n, M_1^n, Y_1^n, \tilde{E}_n, \tilde{F}_n = 1).
\end{aligned}$$

For the last term, we use the fact that if $M_2 \in \mathcal{L}$, then the conditional entropy cannot exceed $\log(|\mathcal{L}|)$:

$$\begin{aligned}
&H(M_2|\mathcal{C}_n, M_1, Y_1^n, \tilde{E}_n, \tilde{F}_n = 1) \\
&\overset{(a)}{=} H(M_2|\mathcal{C}_n, M_1, Y_1^n, \tilde{E}_n, \tilde{F}_n = 1, \mathcal{L}, |\mathcal{L}|) \\
&\leq H(M_2|\tilde{E}_n, \tilde{F}_n = 1, \mathcal{L}, |\mathcal{L}|) \\
&= \sum_{l=0}^{2^{nR_2}} \mathsf{P}(|\mathcal{L}| = l, \tilde{E}_n = 1) H(M_2|\tilde{E}_n = 1, \tilde{F}_n = 1, \mathcal{L}, |\mathcal{L}| = l) \\
&\qquad + \sum_{l=0}^{2^{nR_2}} \mathsf{P}(|\mathcal{L}| = l, \tilde{E}_n = 0) H(M_2|\tilde{E}_n = 0, \tilde{F}_n = 1, \mathcal{L}, |\mathcal{L}| = l) \\
&\leq \sum_{l=0}^{2^{nR_2}} \mathsf{P}(|\mathcal{L}| = l, \tilde{E}_n = 1) H(M_2|\tilde{E}_n = 1, \tilde{F}_n = 1, \mathcal{L}, |\mathcal{L}| = l) + nR_2 \, \mathsf{P}(\tilde{E}_n = 0) \\
&\leq \sum_{l=0}^{2^{nR_2}} \mathsf{P}(|\mathcal{L}| = l, \tilde{E}_n = 1) \log(l) + nR_2 \, \mathsf{P}(\tilde{E}_n = 0) \\
&\leq \sum_{l=0}^{2^{nR_2}} \mathsf{P}(|\mathcal{L}| = l|\tilde{E}_n = 1) \log(l) + nR_2 \, \mathsf{P}(\tilde{E}_n = 0) \\
&= \mathsf{E}[\log(|\mathcal{L}|)|\tilde{E}_n = 1] + nR_2 \, \mathsf{P}(\tilde{E}_n = 0) \\
&\overset{(b)}{\leq} \log(\mathsf{E}[|\mathcal{L}||\tilde{E}_n = 1]) + nR_2 \, \mathsf{P}(\tilde{E}_n = 0) \\
&\overset{(c)}{\leq} \max\big\{0, n(R_2 - I(U_2; Y_1, U_1) + \overline{\alpha} I(U_1; U_2) + 4\delta(\epsilon') + \epsilon_n), \\
&\qquad\qquad n(R_2 - I(U_1, U_2; Y_1) + 4\delta(\epsilon') + \epsilon_n)\big\} + nR_2 \, \mathsf{P}(\tilde{E}_n = 0)
\end{aligned}$$

$$\begin{aligned}&\le n \cdot \max\{0, R_2 - I(U_2; Y_1, U_1) + \overline{\alpha} I(U_1; U_2), R_2 - I(U_1, U_2; Y_1)\} \\ &\qquad\qquad + n4\delta(\epsilon') + n\epsilon_n + nR_2\, \mathsf{P}(\tilde{E}_n = 0),\end{aligned}$$

where (a) follows since the set $\mathcal{L}$ and its cardinality $|\mathcal{L}|$ are functions of $(\mathcal{C}_n, M_1, Y_1^n)$, (b) follows by Jensen's inequality, and (c) follows by (4.23) and the soft-max interpretation of the log-sum-exp function [8, p. 72]. Substituting back gives

$$\begin{aligned}&I(M_2; M_1, Y_1^n | \mathcal{C}_n) \\ &= H(M_2|\mathcal{C}_n) - H(M_2|\mathcal{C}_n, M_1, Y_1^n) \\ &= nR_2 - H(M_2|\mathcal{C}_n, M_1, Y_1^n) \\ &\ge nR_2 - 2 - nR_2\, \mathsf{P}(\tilde{F}_n = 0) - H(M_2|\mathcal{C}_n, M_1^n, Y_1^n, \tilde{E}_n, \tilde{F}_n = 1) \\ &\ge nR_2 - 2 - nR_2\, \mathsf{P}(\tilde{F}_n = 0) - n4\delta(\epsilon') - n\epsilon_n - nR_2\, \mathsf{P}(\tilde{E}_n = 0) \\ &\qquad - n \cdot \max\{0, R_2 - I(U_2; Y_1, U_1) + \overline{\alpha} I(U_1; U_2), R_2 - I(U_1, U_2; Y_1)\} \\ &\overset{(a)}{=} n[\min\{R_2, I(U_2; Y_1, U_1) - \overline{\alpha} I(U_1; U_2), I(U_1, U_2; Y_1)\} - 4\delta(\epsilon') - 2\epsilon_n],\end{aligned}$$

where (a) follows since both of the probabilities $\mathsf{P}(\tilde{E}_n = 0)$ and $\mathsf{P}(\tilde{F}_n = 0)$ tend to zero as $n \to \infty$.

Acknowledgment

This chapter is, in part, a reprint of the material in the papers: Pinar Sen, Sung Hoon Lim, and Young-Han Kim, “On the Optimal Achievable Rates for Linear Computation With Random Homologous Codes,” accepted to *IEEE Transactions of Information Theory*, 2020. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] Thomas M. Cover. Broadcast channels. *IEEE Trans. Inf. Theory*, 18(1):2–14, January 1972.

[2] Thomas M. Cover. Comments on broadcast channels. *IEEE Trans. Inf. Theory*, 44(6):2524–2530, 1998.

[3] Katalin Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, 25(3):306–311, 1979.

[4] Abbas El Gamal and Young-Han Kim. *Network Information Theory.* Cambridge University Press, Cambridge, 2011.

[5] L. Wang, E. Sasoglu, B. Bandemer, and Y.-Kim. A comparison of superposition coding schemes. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2970–2974, July 2013.

[6] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. A joint typicality approach to compute–forward. *IEEE Trans. Inf. Theory*, 64(12):7657–7685, Dec 2018.

[7] B. Bandemer, A. El Gamal, and Y.-H. Kim. Optimal achievable rates for interference networks with random codes. *IEEE Trans. Inf. Theory*, 61(12):6536–6549, Dec 2015.

[8] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization.* Cambridge University Press, Cambridge, 2004.

Chapter 5

Message Communication Over Multiple Access Channels with Homologous Codes

The roles of two techniques used in coset coding to generate nonuniform codewords, namely, shaping and channel transformation, are clarified and illustrated via the simple example of the two-sender multiple access channel. While individually deficient, the optimal combination of shaping via nested coset codes of the same generator matrix (which we refer to as homologous codes) and channel transformation is shown to achieve the same performance as traditional random codes for the general two-sender multiple access channel. The achievability proof of the capacity region is extended to multiple access channels with more than two senders, and with one or more receivers. A quantization argument adapted to the proposed combination of two techniques is presented to establish the achievability proof for their Gaussian counterparts.

5.1 Problem Formulation

Consider the k-sender discrete memoryless (DM) multiple access channel (MAC)

$$(\mathcal{X}_1 \times \mathcal{X}_2 \times \ldots \times \mathcal{X}_k, p(y|x_1, x_2, \ldots, x_k), \mathcal{Y})$$

in Fig. 5.1, which consists of k sender alphabets $\mathcal{X}_j, j \in [k]$, a receiver alphabet $\mathcal{Y}$, and a collection of conditional probability distributions $p_{Y|X^k}(y|x_1, x_2, \ldots, x_k)$.

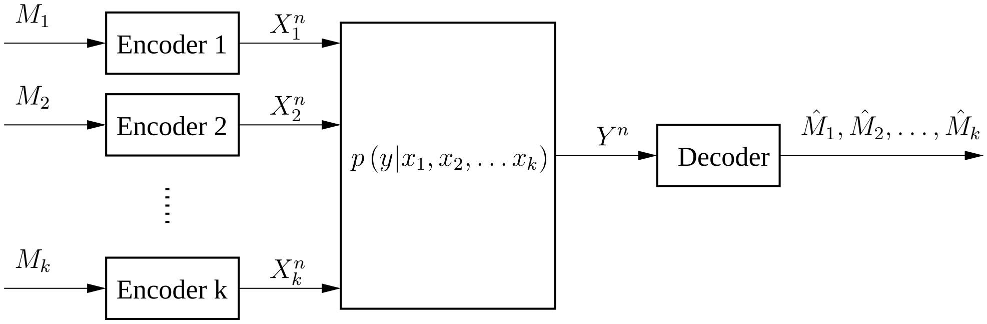


Figure 5.1. k-sender multiple access channel.

An $(n, nR_1, nR_2, \ldots, nR_k)$ code for the multiple access channel consists of k message sets, $\mathbb{F}_q^{nR_j}, j \in [k]$ and k encoders where encoder $j \in [k]$ assigns a codeword $x_j^n(m_j) \in \mathcal{X}_j^n$ to each message $m_j \in \mathbb{F}_q^{nR_j}$. The performance of a given code paired with a decoder that assigns an estimate $(\hat{m}_1, \ldots, \hat{m}_k)$ to each received sequence y^n is measured by the average probability of error

$$P_e^{(n)} = \mathsf{P}((\hat{M}_1, \ldots, \hat{M}_k) \neq (M_1, \ldots, M_k)),$$

where message tuple $(M_1, \ldots, M_k)$ is assumed to be independent and uniformly distributed. A rate tuple $(R_1, R_2, \ldots, R_k)$ is said to be *achievable* if there exists a sequence of $(n, nR_1, nR_2, \ldots, nR_k)$ codes along with a decoder such that $\lim_{n\to\infty} P_e^{(n)} = 0$. The capacity region is defined as the closure of the set of achievable rate tuples. Single letter characterization of this capacity region was derived in [1, 2] using random i.i.d. coding arguments. For a given pmf $p(x^k)$, define $\mathscr{R}_{\text{MAC}}(X^k)$ as the set of rate tuples

$(R_1, R_2, \ldots, R_k)$ such that

$$\sum_{i \in \mathcal{J}} R_i < I(X(\mathcal{J}); Y | X(\mathcal{J}^c)), \quad \forall \mathcal{J} \subseteq [k], \tag{5.1}$$

where $X(\mathcal{J}) = (X_i : i \in \mathcal{J})$. In (5.1), by the q-ary code construction, the information rates are in terms of q-ary symbols and the information measures are in log base q. One can divide both sides of the inequalities in (5.1) by $\log_2 q$ to obtain a set of rate constraints in terms of *bits*. Henceforth, we present all the achievability results in this chapter in terms of bits by assuming this q-ary to bit conversion is performed. The capacity region is then defined as the convex closure of $\bigcup_{p(x^k)} \mathscr{R}_{\text{MAC}}(X^k)$.

Achievability for the random homologous codes described in Chapter 2 is defined in a similar manner. A rate tuple $(R_1, R_2, \ldots, R_k)$ is said to be *achievable by random homologous codes* in $\mathbb{F}_q$ for the multiple access channel $p(y|x_1, \ldots, x_k)$ if there exists a sequence of $(n, ((nR_j, n\hat{R}_j) : j \in [k]), \mathbb{F}_q; p(x^k), \epsilon)$ random homologous code ensembles along with a decoder such that $\lim_{n\to\infty} \mathsf{E}[P_e^{(n)}] = 0$ for some pmf $p(x^k)$ and for some $\epsilon > 0$, where the expectation is taken with respect to the randomness in the common generator matrix and individual coset sequences.

Note that for the k-sender DM-MAC $p(y|x_1, x_2, \ldots, x_k)$ and the input pmfs $p(x_1), p(x_2), \ldots, p(x_k)$, each sender can use a random nested coset code ensemble (with individual generator matrices $G_1, G_2, \ldots, G_k$) to achieve the region $\mathscr{R}_{\text{MAC}}(X^k)$ characterized in (5.1). Thus, the corresponding *heterologous* nested coset codes can emulate the performance of typically nonlinear random code ensembles for MACs.[1] On the other hand, due to the use of a common generator matrix, homologous codes can achieve high rates when the goal of communication is to recover a linear combination of codewords as discussed in Chapter 3. For a 2-sender DM-MAC, an achievable rate region is characterized in [4] for recovering linear combinations of codewords from random homologous code ensembles. When recovering both messages, however, this achievable rate region

[1] Indeed, for $k = 2$, by controlling the structure of G_1 and G_2 more carefully, larger rates than random codes can be achieved for channels with state [3].

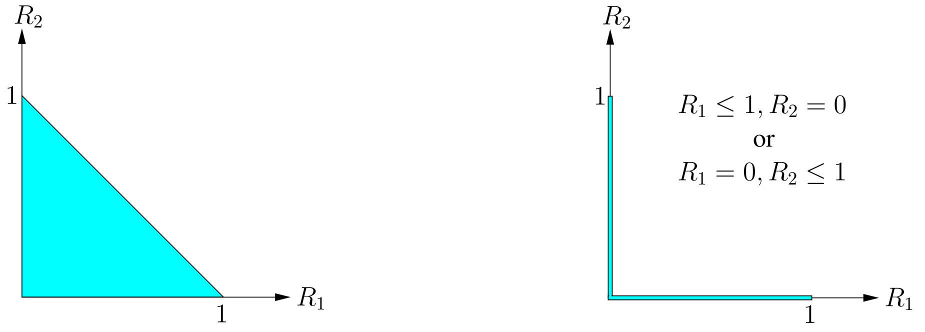
computed for a given input pmf is in general smaller than the region in (5.1). Even a tighter probability of error analysis discussed in [5] does not guarantee the achievability of the region in (5.1). This raises the question of whether random homologous codes are useful only for communicating the sum of the codewords (or equivalently, the sum of the messages) and fundamentally deficient compared to heterologous ones in communicating the messages themselves.

5.2 Motivating Examples

We present two toy examples that illustrate the performance of homologous codes and motivate our main result in Section 5.3.

Example 5.2.1 (Binary adder MAC). *Let $Y = X_1 \oplus X_2$, where $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \{0,1\}$ and the addition operation $\oplus$ is over $\mathbb{F}_2$. The capacity region of this channel is achieved by random coding with i.i.d.* Bern(1/2) *inputs X_1 and X_2, and is depicted in Fig. 5.2a. No binary linear or coset codes of the same generator matrix, however, can achieve this region. As a matter of fact, binary linear or coset codes of the same generator matrix can only achieve the rate region depicted in Fig. 5.2b. The achievability of $(R_1, R_2) = (1, 0)$ follows by using a pair of $(n, n, \mathbb{F}_2)$ and $(n, 0, \mathbb{F}_2)$ coset (or linear) codes with the generator matrix $\mathsf{G} = I$, arbitrarily chosen coset sequences d_1^n and d_2^n, and the decoder that estimates $\hat{m}_1 = y^n \ominus d_1^n$. Exchanging the roles of encoder 1 and 2 implies the achievability of $(R_1, R_2) = (0, 1)$. For the converse, suppose without loss of generality that $R_1 \geq R_2 > 0$. Any message pair $(m_1, m_2) \in \mathbb{F}_2^{nR_1} \times \mathbb{F}_2^{nR_2}$ results in the same output as the message pair $(m_1 \oplus [m\ \mathbf{0}], m_2 \oplus m)$ for some $m \neq \mathbf{0} \in \mathbb{F}_2^{nR_2}$, which implies the converse.*

By using homologous *codes, however, the capacity region can be achieved as follows. Suppose without loss of generality that $R_1 \geq R_2$ where $R_1 + R_2 \leq 1$. Consider the $(n, nR_1, 0, nR_2, n(1-R_2), \mathbb{F}_2)$ homologous code constructed using the generator matrix $G = I$ and the coset sequences $d_1^n = d_2^n = \mathbf{0}$, where the shaping function for encoder 2*



(a) The capacity region. **(b)** An achievable rate region by coset codes.

Figure 5.2. The binary adder MAC in Example 5.2.1.

is specified as $s_2 : \mathbb{F}_2^{nR_2} \to \mathbb{F}_2^{n(1-R_2)}, s_2(m_2) = [\mathbf{0}\ m_2]$. *It follows that the codeword pair assigned to* $(m_1, m_2) \in \mathbb{F}_2^{nR_1 \times nR_2}$ *is*

$$x_1^n(m_1) = [m_1\ \ \mathbf{0}],$$
$$x_2^n(m_2) = [m_2\ s_2(m_2)] = [m_2\ \ \mathbf{0}\ \ m_2].$$

Given the channel output y^n, *the decoding rule that declares the estimates* $\hat{m}_1$ *and* $\hat{m}_2$ *according to*

$$\hat{m}_2 = y_{n-nR_2+1}^n \quad \textit{and} \quad \hat{m}_1 = y_1^{nR_1} \ominus [\hat{m}_2\ \mathbf{0}]$$

can recover the messages m_1 *and* m_2 *without any errors.*

In Example 5.2.1, homologous codes benefit from the algebraic structure of the channel and emulate time division via the concatenation of two codes. The next example has an underlying channel structure that is not fully compatible with the algebraic structure of codes.

Example 5.2.2 (Binary erasure MAC)**.** *Let* $Y = X_1 + X_2$, *where* $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$, $\mathcal{Y} = \{0, 1, 2\}$, *and the addition operation* $+$ *is over* $\mathbb{R}$. *The capacity region of the channel is achieved by random coding with i.i.d.* Bern(1/2) *inputs* X_1 *and* X_2, *and is depicted in Fig. 5.3a. In contrast, no pair of binary coset codes with the same generator matrix can achieve the rate pair* $(1/2 + \epsilon, 1/2 + \epsilon)$ *for* $\epsilon > 0$. *The proof of this proposition is given* *in Appendix 5.A.*

This limitation of coset codes can be once again overcome by using homologous codes. We first present the achievability of the rate pair $(R, 1)$ for $R < 1/2$ with linear codes. Let $A_{nR\times n}$ be a full-rank binary generator matrix of a linear code that can reliably communicate $R < 1/2$ bits over the point-to-point DM binary erasure channel of erasure probability $1/2$.[2] *Let*

$$B = \begin{bmatrix} A \\ A^{\perp} \end{bmatrix},$$

where $A^{\perp}$ is an $(n-nR)\times n$ matrix whose rows are orthogonal to the rows of A. Consider now a pair of $(n, nR, \mathbb{F}_2)$ and $(n, n, \mathbb{F}_2)$ linear codes with generator matrices A and B respectively. Each message pair $(m_1, m_2) \in \mathbb{F}_2^{nR\times n}$ is assigned codewords $x_1^n(m_1) = [m_1\, \mathbf{0}_{n(1-R)}]\, B$ and $x_2^n(m_2) = m_2\, B$, respectively. Notice that since messages M_1 and M_2 are chosen independently, the codeword $x_1^n(M_1)$ is independent from the codeword $x_2^n(M_2)$. Moreover, since B is a full-rank square matrix and M_2 is chosen uniformly at random among $\mathbb{F}_2^n$, entries of $x_2^n(M_2)$ are i.i.d. $\mathrm{Bern}(1/2)$. *Therefore, the channel from the perspective of sender 1, $p(y^n|x_1^n(M_1))$, is equivalent to the point-to-point DM binary erasure channel with erasure probability $1/2$, which is illustrated in Fig. 5.3b. Upon receiving y^n, the decoder first declares the maximum likelihood estimate $\hat{m}_1$ by treating x_2^n as noise and then declares the estimate $\hat{m}_2$ by successive cancellation $x_2^n(\hat{m}_2) = y^n - x_1^n(\hat{m}_1)$. The reliable communication of M_1 and M_2 depends on the probability of error of the first decoding step, which vanishes asymptotically as $n \to \infty$ under the described matrix A.*

Consider now the $(2n, n+nR, 0, n+nR, n-nR, \mathbb{F}_2)$ homologous code constructed

[2] The existence of such a linear code follows from [6, Section 3.1.3].

using the generator matrix

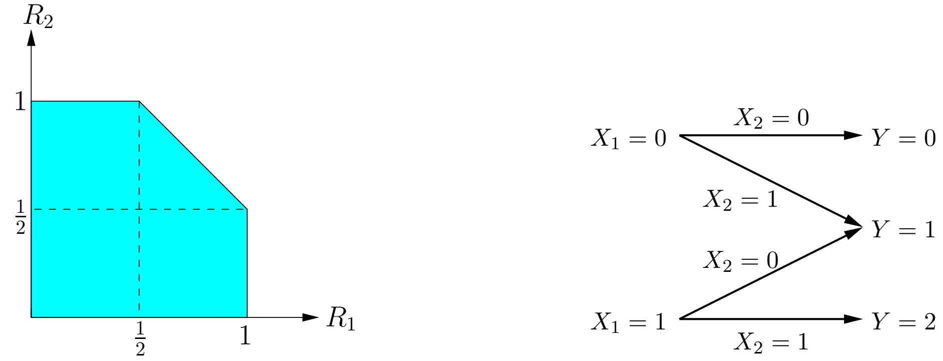
$$\mathsf{G} = \left[\begin{array}{c|c} B & O_{n\times n} \\ \hline O_{nR\times n} & \\ & B \\ A^{\perp} & \end{array}\right],$$

the coset sequences $d_1^n = d_2^n = \mathbf{0}$, where the shaping function for encoder 2 is specified as $s_2 : \mathbb{F}_2^{n+nR} \to \mathbb{F}_2^{n-nR}$, $s_2(m_2) = (m_{2,i})_{i=nR+1}^{n}$. If each message $m_1 \in \mathbb{F}_2^{n+nR}$ is divided into two sub-vectors as $m_1 = [m_{11} \mid m_{12}]$, where $m_{11} \in \mathbb{F}_2^n$ and $m_{12} \in \mathbb{F}_2^{nR}$, and similarly each message $m_2 \in \mathbb{F}_2^{n+nR}$ is divided into three sub-vectors as $m_2 = [m_{21} \mid m_{22} \mid m_{23}]$, where $m_{21}, m_{23} \in \mathbb{F}_2^{nR}$ and $m_{22} \in \mathbb{F}_2^{n-nR}$, then the assigned codewords can be written as

$$\begin{aligned} x_1^{2n}(m_1) &= \big[m_{11}B \quad \big| \quad m_{12}A\big], \\ x_2^{2n}(m_2) &= \big[m_{21}A \quad \big| \quad [m_{23}\; m_{22}]B\big]. \end{aligned}$$

Upon receiving the first half of the sequence y^{2n}, the decoder first declares the maximum likelihood estimate $\hat{m}_{21}$ by treating the first half of x_1^{2n} as noise and then declares the estimate $\hat{m}_{11}$ by successive cancellation. Similarly after receiving the second half of the sequence y^{2n}, it declares the maximum likelihood estimate $\hat{m}_{12}$ by treating the second half of x_2^{2n} as noise and then declares the estimates $\hat{m}_{22}$ and $\hat{m}_{23}$ by successive cancellation. By the construction of the matrix A, the first and second halves of codewords are reliably communicated at rates $(1, R)$ and $(R, 1)$, which, combined together, can be arbitrarily close to $(3/4, 3/4)$. The resulting transmission corresponds to time sharing via the concatenation of two codes. A similar argument can be extended to the entire capacity region.

The constructions of homologous codes for the binary adder and erasure MACs respectively emulate time division and time sharing in disguise via the concatenation of two codes. Consequently, these codes do not scale to more complicated problems (such as interference channels) in a satisfactory manner. As we will illustrate shortly, however,



(a) The capacity region.

(b) The channel from the perspective of sender 1.

Figure 5.3. The binary erasure MAC in Example 5.2.2.

most (random) homologous codes are sufficient to achieve the capacity region, provided that they are constructed according to appropriate distributions.

5.3 Achievable Rate Regions for Two Senders by Random Homologous Codes

We now investigate the performance of random homologous codes described in Chapter 2 for the two sender DM-MAC $p(y|x_1, x_2)$. We take a gradual approach to presenting the main result and first discuss the key technical ingredients of the proof one by one.

5.3.1 Shaping

Symbols in an $(n, nR, \mathbb{F}_q)$ random coset code ensemble are uniformly distributed over $\mathbb{F}_q$. By the shaping step inherent in the nested coset codes, random homologous code ensembles emulate the statistical behavior of a random (nonlinear) code ensemble drawn from the desired distribution while maintaining a common algebraic structure across users. To separate the benefit from channel transformation, in this section, we are particularly interested in the finite-field input DM-MAC $p(y|x_1, x_2)$, where $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{F}_q$, and random homologous codes designed over $\mathbb{F}_q$ for this channel. The block diagram of this scheme is depicted in Fig. 5.4.

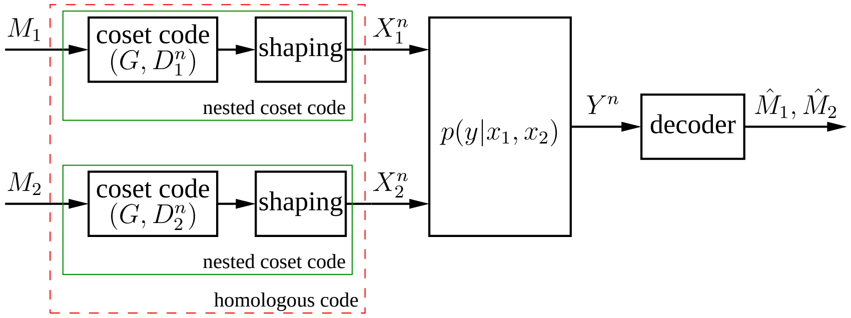


Figure 5.4. Block diagram for shaping.

We describe the rate region achievable by random homologous codes. For given input pmfs $p(x_1)$ and $p(x_2)$, we refer to the rate region in (5.1) as $\mathscr{R}_{\text{MAC}}(X_1, X_2)$, i.e., the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y | X_2), \\ R_2 &< I(X_2; Y | X_1), \\ R_1 + R_2 &< I(X_1, X_2; Y), \end{aligned}$$

and define $\mathscr{R}_{\text{L}}(X_1, X_2)$ as the set of rate pairs (R_1, R_2) such that

$$R_1 < \max\{I(X_1; Y),\, H(X_1) - H(X_2) + I(X_2; Y)\}, \tag{5.2}$$

or

$$R_2 < \max\{I(X_2; Y),\, H(X_2) - H(X_1) + I(X_1; Y)\}. \tag{5.3}$$

Proposition 5.3.1 (Shaping)**.** *A rate pair (R_1, R_2) is achievable by random homologous codes in $\mathbb{F}_q$ for the finite-field input DM-MAC $p(y|x_1, x_2)$ if*

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}_{\text{L}}(X_1, X_2)$$

for some input pmfs $p(x_1)$ and $p(x_2)$.

Proof. Our proof steps follow [4, Sec. VI] essentially line by line, except the analysis of one error event. Fix an input pmf $p = p(x_1)p(x_2)$ and let paramter $\epsilon' > 0$. We use an $(n, nR_1, n\hat{R}_1, nR_2, n\hat{R}_2, \mathbb{F}_q; p, \epsilon')$ random homologous code ensemble constructed in Definition 2.3.2. The decoder first fixes a sufficiently large $\epsilon > \epsilon'$ and then searches a unique pair of $(\hat{m}_1, \hat{m}_2)$ such that $(u_1^n(\hat{m}_1, l_1), u_2^n(\hat{m}_2, l_2), y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y)$ for some (l_1, l_2), where $u_j^n(\hat{m}_j, l_j)$ is the auxiliary codeword generated in step 1) of random homologous code construction in Definition 2.3.2. If the decoder finds the unique pair, then it declares that $(\hat{m}_1, \hat{m}_2)$ was transmitted. Otherwise, it declares error. Assume that (M_1, M_2) is the transmitted message pair and (L_1, L_2) is the auxiliary index pair chosen by the shaping functions. We bound the probability of error averaged over code ensembles. As in [4], the decoder makes an error only if one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_1 &= \{U_j^n(M_j, l_j) \notin \mathcal{T}_{\epsilon'}^{(n)}(X_j) \text{ for all } l_j,\ j = 1 \text{ or } 2\},\\
\mathcal{E}_2 &= \{(U_1^n(M_1, L_1), U_2^n(M_2, L_2), Y^n) \notin \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y)\},\\
\mathcal{E}_3 &= \{(U_1^n(M_1, L_1), U_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y) \text{ for some } (m_2, l_2) \neq (M_2, L_2)\},\\
\mathcal{E}_4 &= \{(U_1^n(m_1, l_1), U_2^n(M_2, L_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y) \text{ for some } (m_1, l_1) \neq (M_1, L_1)\},\\
\mathcal{E}_5 &= \{(U_1^n(m_1, l_1), U_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y) \text{ for some } (m_1, l_1) \neq (M_1, L_1)\\
&\qquad \text{and } (m_2, l_2) \neq (M_2, L_2) \text{ such that } [m_1\ l_1\ \mathbf{0}] \ominus [M_1\ L_1\ \mathbf{0}] \text{ and } [m_2\ l_2\ \mathbf{0}] \ominus [M_2\ L_2\ \mathbf{0}]\\
&\qquad \text{are linearly independent}\},\\
\mathcal{E}_6 &= \{(U_1^n(m_1, l_1), U_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y) \text{ for some } (m_1, l_1) \neq (M_1, L_1)\\
&\qquad \text{and } (m_2, l_2) \neq (M_2, L_2) \text{ such that } [m_1\ l_1\ \mathbf{0}] \ominus [M_1\ L_1\ \mathbf{0}] \text{ and } [m_2\ l_2\ \mathbf{0}] \ominus [M_2\ L_2\ \mathbf{0}]\\
&\qquad \text{are linearly dependent}\}.
\end{aligned}$$

Thus, by the union of events bound, $\mathsf{E}[P_e^{(n)}] \leq \mathsf{P}(\mathcal{E}_1) + \sum_{k \neq 1} \mathsf{P}(\mathcal{E}_k \cap \mathcal{E}_1^c)$. By [4], the first five terms tend to 0 as $n \to \infty$ if

$$
\begin{aligned}
\hat{R}_j &> \mathrm{D}_j^{\mathrm{KL}} + \delta(\epsilon'),\ j = 1, 2 \\
R_1 + 2\hat{R}_1 + \hat{R}_2 &< I(X_1; Y|X_2) + 2\mathrm{D}_1^{\mathrm{KL}} + \mathrm{D}_2^{\mathrm{KL}} - \delta(\epsilon), \\
R_2 + \hat{R}_1 + 2\hat{R}_2 &< I(X_2; Y|X_1) + \mathrm{D}_1^{\mathrm{KL}} + 2\mathrm{D}_2^{\mathrm{KL}} - \delta(\epsilon), \\
R_1 + R_2 + 2\sum_{i=1}^{2} \hat{R}_i &< I(X_1, X_2; Y) + 2\sum_{i=1}^{2} \mathrm{D}_i^{\mathrm{KL}} - \delta(\epsilon),
\end{aligned}
$$

where $\mathrm{D}_j^{\mathrm{KL}} := D(p_{X_j}||\mathrm{Unif}(\mathbb{F}_q))$ denotes the KL-divergence between the input pmf $p(x_j)$ and $\mathrm{Unif}(\mathbb{F}_q)$ for $j = 1, 2$. For the last term, one can use the analysis in [4] that is originally conducted for decoding of two linearly independent combinations of X_1 and X_2, namely, $W_1 = a_1 X_1 \oplus a_2 X_2$ and $W_2 = b_1 X_1 \oplus b_2 X_2$. Even for fixed W_1 and W_2, however, the resulting upper bound on R_1 and R_2 includes a max-min optimization over all linear combinations of W_1 and W_2, which is difficult to compute in general. Therefore, we present a new upper bound resulting in an achievable rate region that is easier to compute than the optimized rate region provided by [4]. Moreover, it can be shown that our achievable rate region is larger than the one in [4] for some channels, such as the on–off erasure MAC with $p = 1/2$ to be defined in Example 3.

Lemma 5.3.1. *The probability $\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c)$ can be bounded by two different expressions:*

$$
\begin{aligned}
\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) &\le (q-1) q^{n(\hat{R}_1 + \hat{R}_2 + \min\{R_1 + \hat{R}_1, R_2 + \hat{R}_2\})} q^{n(H(X_1) + H(X_2) + H(X_2|Y) - 3 + \delta(\epsilon))}, \\
\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) &\le (q-1) q^{n(\hat{R}_1 + \hat{R}_2 + \min\{R_1 + \hat{R}_1, R_2 + \hat{R}_2\})} q^{n(H(X_1) + H(X_2) + H(X_1|Y) - 3 + \delta(\epsilon))}.
\end{aligned}
$$

Proof. Define the rate $R = \min\{R_1 + \hat{R}_1, R_2 + \hat{R}_2\}$, and the events $\mathcal{M} = \{M_1 = \mathbf{0}, M_2 = \mathbf{0}\}$ and $\mathcal{L} = \{L_1 = \mathbf{0}, L_2 = \mathbf{0}\}$. Define the set

$$
\begin{aligned}
\mathcal{D} = \{(m_1, l_1, m_2, l_2) \in \mathbb{F}_q^{nR_1} \times \mathbb{F}_q^{n\hat{R}_1} \times \mathbb{F}_q^{nR_2} \times \mathbb{F}_q^{n\hat{R}_2} :& \\
[m_1\ l_1\ \mathbf{0}] \ne \mathbf{0}, [m_2\ l_2\ \mathbf{0}] \ne \mathbf{0} \text{ are linearly dependent}\}.&
\end{aligned}
$$

By the symmetry of code generation, $\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) = \mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c | \mathcal{M}, \mathcal{L})$. To see this, we start with marginalization over some random variables as follows.

$$\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) = \sum_{m_1,l_1} \sum_{m_2,l_2} \sum_{G} \sum_{d_1^n,d_2^n} \mathsf{P} \begin{pmatrix} \mathcal{E}_6 \cap \mathcal{E}_1^c, (M_1, M_2) = (m_1, m_2), \\ (L_1, L_2) = (l_1, l_2), G = G, \\ D_1^n = d_1^n, D_2^n = d_2^n \end{pmatrix}. \tag{5.4}$$

Continuing from (5.4), we have

$$\begin{aligned} \mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) &\overset{(a)}{=} \sum_{m_1,l_1} \sum_{m_2,l_2} \sum_{G} \sum_{d_1^n,d_2^n} \mathsf{P} \begin{pmatrix} \mathcal{E}_6 \cap \mathcal{E}_1^c, (M_1, M_2) = (\mathbf{0}, \mathbf{0}), \\ (L_1, L_2) = (\mathbf{0}, \mathbf{0}), G = G, \\ D_1^n = [m_1 \ l_1 \ \mathbf{0}]G \oplus d_1^n, \\ D_2^n = [m_2 \ l_2 \ \mathbf{0}]G \oplus d_2^n \end{pmatrix} \\ &= \sum_{m_1,l_1} \sum_{m_2,l_2} \mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c, (M_1, L_1, M_2, L_2) = (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0})) \\ &\overset{(b)}{=} \mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c | (M_1, L_1, M_2, L_2) = (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0})), \end{aligned}$$

where (a) follows since $(G, [m_1 \ l_1 \ \mathbf{0}]G \oplus D_1^n, [m_2 \ l_2 \ \mathbf{0}]G \oplus D_2^n) \overset{d}{=} (G, D_1^n, D_2^n)$ results in a permuted code and (b) follows by the fact proved in [4, Lemma 11] that (M_1, L_1, M_2, L_2) is uniformly distributed over its support.

By this observation, it suffices to bound the conditional probability as follows.

$$\begin{aligned} &\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c | \mathcal{M}, \mathcal{L}) \\ &= \mathsf{P}\big((U_1^n(m_1, l_1), U_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y) \\ &\qquad \text{for some } (m_1, l_1, m_2, l_2) \in \mathcal{D}, U_j^n(\mathbf{0}, \mathbf{0}) \in \mathcal{T}_{\epsilon'}^{(n)}(X_j) \ j = 1, 2 | \mathcal{M}, \mathcal{L}\big) \\ &\overset{(a)}{\leq} \sum_{(m_1,l_1,m_2,l_2) \in \mathcal{D}} \mathsf{P} \left(\begin{matrix} (U_1^n(m_1, l_1), U_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, Y), \\ U_j^n(\mathbf{0}, \mathbf{0}) \in \mathcal{T}_{\epsilon'}^{(n)}(X_j) \ j = 1, 2 \end{matrix} \middle| \mathcal{M}, \mathcal{L} \right) \\ &\leq \sum_{(m_1,l_1,m_2,l_2) \in \mathcal{D}} \mathsf{P} \left(\begin{matrix} U_2^n(m_2, l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_2, Y), \\ U_j^n(\mathbf{0}, \mathbf{0}) \in \mathcal{T}_{\epsilon'}^{(n)}(X_j) \ j = 1, 2 \end{matrix} \middle| \mathcal{M}, \mathcal{L} \right) \end{aligned}$$

$$
\begin{aligned}
&\overset{(b)}{\leq} \sum_{(m_1,l_1,m_2,l_2)\in\mathcal{D}} \mathsf{P}\left(\begin{array}{c} U_2^n(m_2,l_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X_2,Y), \\ U_j^n(\mathbf{0},\mathbf{0}) \in \mathcal{T}_\epsilon^{(n)}(X_j)\, j=1,2 \end{array} \middle| \mathcal{M},\mathcal{L} \right), \\
&= \sum_{(m_1,l_1,m_2,l_2)\in\mathcal{D}} \sum_{\substack{x_1^n\in\mathcal{T}_\epsilon^{(n)}(X_1),\\ x_2^n\in\mathcal{T}_\epsilon^{(n)}(X_2)}} \sum_{(\tilde{x}_2^n,y^n)\in\mathcal{T}_\epsilon^{(n)}(X_2,Y)} \mathsf{P}\left(\begin{array}{c} [m_2\ l_2\ \mathbf{0}]G \oplus D_2^n = \tilde{x}_2^n, \\ D_1^n = x_1^n, D_2^n = x_2^n, Y^n = y^n \end{array} \middle| \mathcal{M},\mathcal{L} \right) \\
&\overset{(c)}{=} \sum_{(m_1,l_1,m_2,l_2)\in\mathcal{D}} \\
&\qquad \sum_{\substack{x_1^n\in\mathcal{T}_\epsilon^{(n)}(X_1),\\ x_2^n\in\mathcal{T}_\epsilon^{(n)}(X_2)}} \sum_{(\tilde{x}_2^n,y^n)\in\mathcal{T}_\epsilon^{(n)}(X_2,Y)} \mathsf{P}\left(\begin{array}{c} [m_2\ l_2\ \mathbf{0}]G \oplus D_2^n = \tilde{x}_2^n, \\ D_1^n = x_1^n, D_2^n = x_2^n \end{array} \middle| \mathcal{M},\mathcal{L} \right) p(y^n|x_1^n,x_2^n) \\
&\overset{(d)}{\leq} \sum_{(m_1,l_1,m_2,l_2)\in\mathcal{D}} \sum_{\substack{x_1^n\in\mathcal{T}_\epsilon^{(n)}(X_1),\\ x_2^n\in\mathcal{T}_\epsilon^{(n)}(X_2)}} \\
&\qquad \sum_{y^n\in\mathcal{T}_\epsilon^{(n)}(Y)} p(y^n|x_1^n,x_2^n) \sum_{\tilde{x}_2^n\in\mathcal{T}_\epsilon^{(n)}(X_2|y^n)} q^{n(\hat{R}_1+\hat{R}_2)} \mathsf{P}\left(\begin{array}{c} [m_2\ l_2\ \mathbf{0}]G \oplus D_2^n = \tilde{x}_2^n, \\ D_1^n = x_1^n, D_2^n = x_2^n \end{array} \right) \\
&= \sum_{(m_1,l_1,m_2,l_2)\in\mathcal{D}} \sum_{\substack{x_1^n\in\mathcal{T}_\epsilon^{(n)}(X_1),\\ x_2^n\in\mathcal{T}_\epsilon^{(n)}(X_2)}} \sum_{y^n\in\mathcal{T}_\epsilon^{(n)}(Y)} p(y^n|x_1^n,x_2^n) \sum_{\tilde{x}_2^n\in\mathcal{T}_\epsilon^{(n)}(X_2|y^n)} q^{n(\hat{R}_1+\hat{R}_2)} q^{-3n} \\
&\leq q^{n(\hat{R}_1+\hat{R}_2)} q^{-3n} q^{n(H(X_1)+H(X_2)+H(X_2|Y)+\delta(\epsilon))} |\mathcal{D}| \\
&\leq q^{n(\hat{R}_1+\hat{R}_2)} q^{-3n} q^{n(H(X_1)+H(X_2)+H(X_2|Y)+\delta(\epsilon))} q^{nR}(q-1),
\end{aligned}
$$

where (a) follows by the union of events bound, (b) follows since $\epsilon > \epsilon'$, (c) follows since, conditioned on $(\mathcal{M},\mathcal{L})$, the triple $G \to (D_1^n, D_2^n) \to Y^n$ form a Markov chain, and (d) follows by [4, Lemma 11]. By changing the order of X_1^n and X_2^n, we obtain the second bound on $\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c)$. □

By Lemma 5.3.1 and using the relation $\mathrm{D}_j^{\mathrm{KL}} = 1 - H(X_j)$, we have $\mathsf{P}(\mathcal{E}_6 \cap \mathcal{E}_1^c) \to 0$ as $n \to \infty$ if $\min\{R_1 + 2\hat{R}_1 + \hat{R}_2, R_2 + \hat{R}_1 + 2\hat{R}_2\} < H(X_1) + 2\mathrm{D}_1^{\mathrm{KL}} + \mathrm{D}_2^{\mathrm{KL}} - \min\{H(X_1|Y), H(X_2|Y)\} - \delta(\epsilon)$. Choosing $\hat{R}_1 = \mathrm{D}_1^{\mathrm{KL}} + 2\delta(\epsilon'), \hat{R}_2 = \mathrm{D}_2^{\mathrm{KL}} + 2\delta(\epsilon')$ and letting $\epsilon \to 0$ yield that the rate pairs (R_1, R_2) is achievable if

$$\begin{aligned} R_1 &< I(X_1; Y | X_2), \\ R_2 &< I(X_2; Y | X_1), \\ R_1 + R_2 &< I(X_1, X_2; Y), \\ \min\{R_1 + H(X_2), R_2 + H(X_1)\} &< H(X_1) + H(X_2) - \min\{H(X_1|Y), H(X_2|Y)\}. \end{aligned} \tag{5.5}$$

The rate region defined by (5.5) is equivalent to the region $\mathscr{R}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}_{\text{L}}(X_1, X_2)$, as will be proved in Appendix 5.B. Taking the union over input pmfs $p(x_1)$ and $p(x_2)$ completes the proof. □

For the **binary adder MAC**, the achievable rate region in Proposition 5.3.1 is indeed equivalent to the capacity region, which is proved in Appendix 5.C.

For the **binary erasure MAC**, however, the rate region in Proposition 5.3.1 is *strictly smaller* than the capacity region, as sketched in Fig. 5.5. In particular, the largest achievable symmetric rate is 2/3 (see Appendix 5.D).

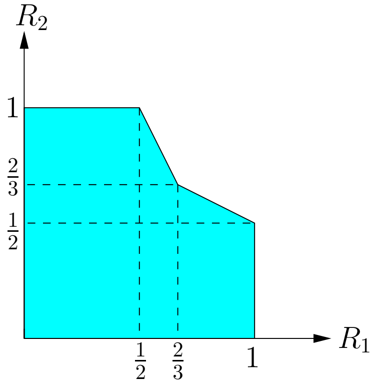
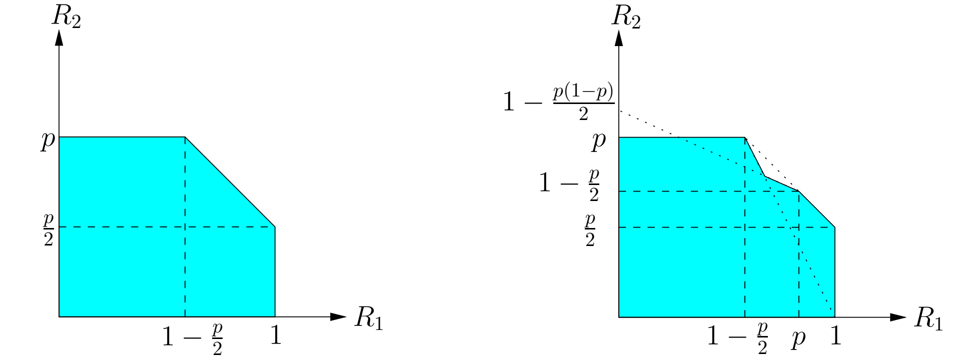


Figure 5.5. The achievable rate region in Proposition 5.3.1 for the binary erasure MAC in Example 5.2.2.

We now introduce another simple example, which will be used again in Section 5.5 when we deal with multiple-receiver MACs.

Example 5.3.1 (On–off erasure MAC). *Let* $Y = (2X_1 - 1) + Z(2X_2 - 1)$, *where* $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$, $\mathcal{Z} = \{0, 1\}$, *and* $\mathcal{Y} = \{0, \pm 1, \pm 2\}$, *where the random variable* $Z \sim \text{Bern}(p)$



(a) The capacity region for $0 < p \leq 1$.

(b) The achievable rate region in Proposition 5.3.1 for $2/3 < p \leq 1$.

Figure 5.6. The on–off erasure MAC in Example 5.3.1.

is independent from X_1 and X_2. If $Z = 1$, the channel is equivalent to the binary erasure MAC. If $Z = 0$, the output Y is only dependent on X_1. That is why this channel is called the on–off erasure MAC*.*

For any $p \in (0, 1]$, the capacity region of the on–off erasure MAC is achieved by random coding with i.i.d. Bern(1/2) *inputs X_1 and X_2, and is shown in Fig. 5.6a (in terms of p). If $p \leq 2/3$, the achievable rate region in Proposition 5.3.1 is equivalent to the capacity region. If $p > 2/3$, however, it reduces to the rate region depicted in Fig. 5.6b that is strictly smaller than the capacity region (see Appendix 5.E). Note that for $p = 1$, the rate region in Fig. 5.6b is equivalent to the achievable rate region for the binary erasure MAC sketched in Fig. 5.5, since the on–off erasure MAC is equivalent to the binary erasure MAC when $p = 1$.*

Remark 5.3.1. *As shown by [5], the achievable rate region in Proposition 5.3.1 can be improved by stronger analysis tools, which we will discuss later in Section 5.4.1 and Proposition 5.4.1. For Examples 5.2.1–5.3.1, however, the achievable rate region in [5] reduces to that of Proposition 5.3.1.*

5.3.2 Channel Transformation

Instead of choosing an appropriate shaping function within a nested coset code, there is a simpler way of achieving the performance of nonuniformly distributed codes.

Following the basic idea in [7, Sec. 6.2], we can simply transform the channel $p(y|x_1, x_2)$ into a *virtual channel* with finite-field inputs

$$p(y|v_1, v_2) = p_{Y|V_1,V_2}(y|\varphi_1(v_1), \varphi_2(v_2)) \tag{5.6}$$

for some symbol-by-symbol mappings $\varphi_1 : \mathbb{F}_q \to \mathscr{X}_1$ and $\varphi_2 : \mathbb{F}_q \to \mathscr{X}_2$, as illustrated in Fig. 5.7. Note that this transformation can be applied to any DM-MAC $p(y|x_1, x_2)$ of arbitrary (not necessarily the same finite-field) input alphabets.

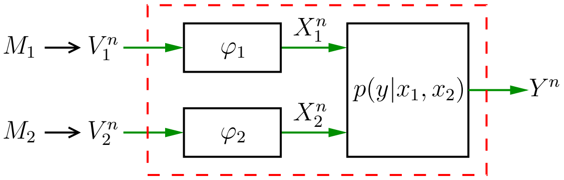


Figure 5.7. The virtual DM-MAC $p(y|v_1, v_2)$ with virtual inputs V_1 and V_2.

We now consider a pair of $(n, nR_1, \mathbb{F}_q)$ and $(n, nR_2, \mathbb{F}_q)$ random coset code ensembles with the same generator matrix for the virtual channel, which is equivalent to random homologous codes with $\hat{R}_1 = \hat{R}_2 = 0$. The block diagram of this scheme is depicted in Fig. 5.8. For a given pair of symbol-by-symbol mappings φ_1 and φ_2, we can establish the following whose proof is deferred to Appendix 5.F.

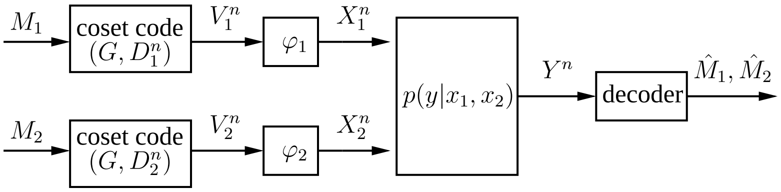


Figure 5.8. Block diagram for channel transformation.

Proposition 5.3.2. *A rate pair (R_1, R_2) is achievable by random coset codes in $\mathbb{F}_q$ with the same generator matrix for the DM-MAC $p(y|x_1, x_2)$, if*

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(V_1, V_2) \cap \mathscr{R}_{\text{L}}(V_1, V_2),$$

where $\mathscr{R}_{\text{MAC}}(V_1, V_2)$ *is defined as in* (5.1) *for the virtual channel* $p(y|v_1, v_2)$ *in* (5.6) *and for the inputs* V_1 *and* V_2 *drawn independently according to* $\text{Unif}(\mathbb{F}_q)$*, and* $\mathscr{R}_{\text{L}}(V_1, V_2)$ *is the set of* (R_1, R_2) *such that*

$$\min(R_1, R_2) < \max\{I(V_1; Y),\, I(V_2; Y)\}. \tag{5.7}$$

Note that (5.7) is equivalent to (5.2) and (5.3) with (V_1, V_2) in place of (X_1, X_2) since V_1 and V_2 are uniform on $\mathbb{F}_q$.

Proposition 5.3.2 was stated for a fixed channel transformation specified by a given pair of symbol-by-symbol mappings $\varphi_1(v_1)$ and $\varphi_2(v_2)$ on a finite field $\mathbb{F}_q$. We now consider all such channel transformations, which results in a simpler achievable rate region.

Corollary 5.3.1 (Channel transformation)**.** *A rate pair* (R_1, R_2) *is achievable by random coset codes generated in some finite field with the same generator matrix for the DM-MAC* $p(y|x_1, x_2)$*, if*

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}'_{\text{L}}(X_1, X_2)$$

for some input pmfs $p(x_1)$ *and* $p(x_2)$*, where* $\mathscr{R}'_{\text{L}}(X_1, X_2)$ *is the set of* (R_1, R_2) *such that*

$$\min(R_1, R_2) < \max\{I(X_1; Y),\, I(X_2; Y)\}.$$

Proof. First suppose that $p(x_1)$ and $p(x_2)$ are of the form

$$\frac{i}{\rho^m} \tag{5.8}$$

for some prime ρ and $i, m \in \mathbb{Z}^+$ for all x_1 and x_2. Then there exist $\varphi_1(v_1)$ and $\varphi_2(v_2)$ on $\mathbb{F}_q$ such that $X_j \overset{d}{=} \varphi_j(V_j)$ with $V_j \sim \text{Unif}(\mathbb{F}_q)$, where $q = \rho^m$. Hence, we can transform the channel $p(y|x_1, x_2)$ into a virtual channel $p(y|v_1, v_2)$ and achieve the rate region in Proposition 5.3.2. Now, since $(V_1, V_2) \to (X_1, X_2) \to Y$ form a Markov chain and (V_1, X_1) and (V_2, X_2) are independent, the rate region $\mathscr{R}_{\text{MAC}}(V_1, V_2) \cap \mathscr{R}_{\text{L}}(V_1, V_2)$ in Proposition 5.3.2 can be simplified as $\mathscr{R}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}'_{\text{L}}(X_1, X_2)$. Finally, the earlier restrictions on the input pmfs can be removed since the set of pmfs of the form (5.8) is dense. This completes the proof. □

We now revisit the previous examples to evaluate the achievable rate region in Corollary 5.3.1.

- **Binary adder MAC**: The achievable rate region in Corollary 5.3.1 is equivalent to the capacity region. To see this, note that for the binary adder MAC, $\mathscr{R}_{\text{L}}(X_1, X_2) \subseteq \mathscr{R}'_{\text{L}}(X_1, X_2)$ for any $p(x_1)$ and $p(x_2)$, and the former region achieved by the shaping (with the intersection with $\mathscr{R}_{\text{MAC}}(X_1, X_2)$) reduces to the capacity region as proved in Appendix 5.C. Therefore, the capacity region of the binary adder MAC is achievable by using coset codes over the virtual channel. This does not contradict the fact that no coset code on the *binary field* can achieve a positive symmetric rate pair, since channel transformation allows the use of linear (or coset) codes over larger finite fields.

- **Binary erasure MAC**: The achievable rate region in Corollary 5.3.1 reduces to the one in Proposition 5.3.1 sketched in Fig. 5.5, although $\mathscr{R}'_{\text{L}}(X_1, X_2)$ is in general different than $\mathscr{R}_{\text{L}}(X_1, X_2)$ for fixed pmfs $p(x_1)$ and $p(x_2)$. The proof is given in Appendix 5.D.

- **On–off erasure MAC**: If $p \leq 2/3$, the achievable rate region in Corollary 5.3.1 reduces to the capacity region sketched in Fig. 5.6a. If $p > 2/3$, however, it reduces to the rate region sketched in Fig. 5.9. While larger than what is achieved by the shaping (cf. Fig. 5.6b), the achievable rate region by channel transformation in Corollary 5.3.1 is still strictly smaller than the capacity region. The details are given in Appendix 5.E.

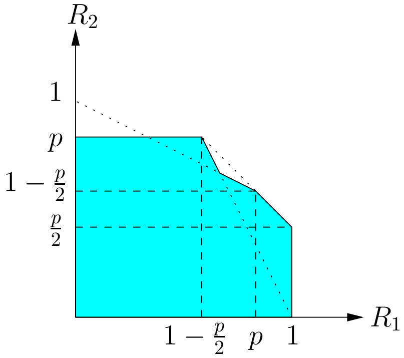


Figure 5.9. The achievable rate region in Corollary 5.3.1 for the on–off erasure MAC in Example 5.3.1 when $2/3 < p \leq 1$.

Remark 5.3.2. *The achievable rate region for the channel transformation technique in Corollary 5.3.1 can be easily evaluated for fixed input pmfs $p(x_1)$ and $p(x_2)$. Using the analysis tools developed in [5], Proposition 5.3.2 and Corollary 5.3.1 can be potentially strengthened. Given a virtual channel $p(y|v_1, v_2)$ with input pmfs $p(v_1)$ and $p(v_2)$ on some $\mathbb{F}_q$, the resulting achievable rate region would depend on the distribution of $(a_1V_1 \oplus a_2V_2, Y)$ for every $a_1, a_2 \neq 0 \in \mathbb{F}_q$. The union of these rate regions over all channel transformations, however, is not computable. Therefore, it is unclear whether the insufficiency of the channel transformation technique for Examples 5.2.2–5.3.1 (binary erasure MAC and on–off erasure MAC) is fundamental or due to the deficiency of our analysis tools.*

5.3.3 Combination

As shown for the binary erasure MAC and on–off erasure MAC examples, shaping (with homologous codes) and channel transformation (with coset codes of the same generator matrix) seemingly cannot achieve the capacity region. When combined together, these techniques can achieve the pentagonal region $\mathscr{R}_{\text{MAC}}(X_1, X_2)$ for any $p(x_1)$ and $p(x_2)$ while maintaining the algebraic structure of the code. Consider the virtual channel in (5.6) and random homologous codes for this channel, a block diagram for which is depicted in Fig. 5.10. Then, Proposition 5.3.1 implies the following.

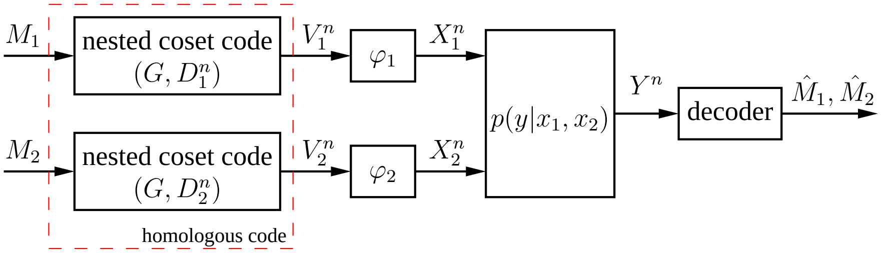


Figure 5.10. Block diagram for homologous codes over the virtual channel.

Proposition 5.3.3. *A rate pair (R_1, R_2) is achievable by random homologous codes in $\mathbb{F}_q$ for the DM-MAC $p(y|x_1, x_2)$, if*

$$(R_1, R_2) \in \mathscr{R}_{\mathrm{MAC}}(X_1, X_2) \cap \mathscr{R}_{\mathrm{L}}(V_1, V_2)$$

for some pmfs $p(v_1)$ and $p(v_2)$ on $\mathbb{F}_q$, and some mappings $x_1 = \varphi_1(v_1)$ and $x_2 = \varphi_2(v_2)$, where $\mathscr{R}_{\mathrm{L}}(V_1, V_2)$ is the set of rate pairs (R_1, R_2) satisfying (5.2) or (5.3).

Proof. Given pmfs $p(v_1)$ and $p(v_2)$ on $\mathbb{F}_q$, and mappings $x_1 = \varphi_1(v_1)$ and $x_2 = \varphi_2(v_2)$, by Proposition 5.3.1, the rate region $\mathscr{R}_{\mathrm{MAC}}(V_1, V_2) \cap \mathscr{R}_{\mathrm{L}}(V_1, V_2)$ is achievable by random homologous codes in $\mathbb{F}_q$ for the virtual channel $p(y|v_1, v_2)$. Now, since $(V_1, V_2) \to (X_1, X_2) \to Y$ form a Markov chain and (V_1, X_1) and (V_2, X_2) are independent, the rate region $\mathscr{R}_{\mathrm{MAC}}(V_1, V_2) \cap \mathscr{R}_{\mathrm{L}}(V_1, V_2)$ simplifies to $\mathscr{R}_{\mathrm{MAC}}(X_1, X_2) \cap \mathscr{R}_{\mathrm{L}}(V_1, V_2)$. The proof follows by taking the union over pmfs $p(v_1)$ and $p(v_2)$ on $\mathbb{F}_q$, and mappings $x_1 = \varphi_1(v_1)$ and $x_2 = \varphi_2(v_2)$. □

We are now ready to state one of the main technical results of this paper, which follows from Proposition 5.3.3 by optimizing over all channel transformations.

Theorem 5.3.1 (Combination)**.** *A rate pair (R_1, R_2) is achievable by random homologous codes in some finite field for the DM-MAC $p(y|x_1, x_2)$, if $(R_1, R_2) \in \mathscr{R}_{\mathrm{MAC}}(X_1, X_2)$ for some $p(x_1)$ and $p(x_2)$.*

Proof. Our argument is similar to the proof of Corollary 5.3.1, except that the choice of channel transformation needs more care. First suppose that $p(x_1)$ and $p(x_2)$ are of the form (5.8) for some prime ρ. We will show that there exist a finite field $\mathbb{F}_q$, pmfs $p(v_1)$ and $p(v_2)$ on $\mathbb{F}_q$, and mappings $x_1 = \varphi_1(v_1)$ and $x_2 = \varphi_2(v_2)$ such that $\mathscr{R}_{\text{MAC}}(X_1, X_2) \subseteq \mathscr{R}_{\text{L}}(V_1, V_2)$. Consider random homologous codes over $\mathbb{F}_q$ with $q = \rho^{2m}$. Choose V_1 and φ_1 such that V_1 and $\varphi_1(V_1) \overset{d}{=} X_1$ are one-to-one on the support of V_1 (this is always possible since $q \geq \rho^m$). Also choose $V_2 \sim \text{Unif}(\mathbb{F}_q)$ and φ_2 such that $\varphi_2(V_2) \overset{d}{=} X_2$ (this is possible due to the form of $p(x_2)$). Let $(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(X_1, X_2)$. Then, (R_1, R_2) satisfies

$$\begin{aligned} R_2 &< I(X_2; Y | X_1) \\ &\leq H(X_2) \\ &\leq \log \rho^m \\ &\leq H(V_2) - H(V_1) \\ &\leq H(V_2) - H(V_1) + I(V_1; Y), \end{aligned}$$

which implies that $(R_1, R_2) \in \mathscr{R}_{\text{L}}(V_1, V_2)$. Finally, the restrictions on the input pmfs can be removed again by the denseness argument. □

Remark 5.3.3. *Theorem 5.3.1 can be strengthened by putting a cardinality bound on the underlying finite field. We need a different construction. By Bertrand's postulate, there exists a prime q such that $|\mathcal{X}_1||\mathcal{X}_2| < q < 2|\mathcal{X}_1||\mathcal{X}_2|$. For a given input pmf $p(x_1)$ and $p(x_2)$, consider a random homologous code ensemble over $\mathbb{F}_q$. Choose V_1 and φ_1 such that V_1 and $\varphi_1(V_1) \overset{d}{=} X_1$ are one-to-one on the support of V_1, which is always possible since $q \geq |\mathcal{X}_1|$. Also choose V_2 and φ_2 such that V_2 and (X_1, X_2) are one-to-one on the support of V_2 and that $\varphi_2(V_2) \overset{d}{=} X_2$, which is always possible since $q \geq |\mathcal{X}_1||\mathcal{X}_2|$. The claim is that $\mathscr{R}_{\text{MAC}}(X_1, X_2) \subseteq \mathscr{R}_{\text{L}}(V_1, V_2)$. To see this, let $(R_1, R_2) \in \mathscr{R}_{\text{MAC}}(X_1, X_2)$. Then, (R_1, R_2) satisfies*

$$R_2 < I(X_2; Y | X_1)$$

$$
\begin{aligned}
&\leq H(X_2) \\
&= H(X_1, X_2) - H(X_1) \\
&= H(V_2) - H(V_1) \\
&\leq H(V_2) - H(V_1) + I(V_1; Y),
\end{aligned}
$$

which implies that $(R_1, R_2) \in \mathscr{R}_{\mathrm{L}}(V_1, V_2)$. *Therefore, for any pmfs* $p(x_1)$ *and* $p(x_2)$*, the rate region* $\mathscr{R}_{\mathrm{MAC}}(X_1, X_2)$ *is achievable by random homologous codes in some finite field* $\mathbb{F}_q$ *such that* $q \leq 2|\mathcal{X}_1||\mathcal{X}_2|$ *for the DM-MAC* $p(y|x_1, x_2)$.

5.4 Extension to More Than Two Senders

The achievable rate region by random homologous codes for the 2-sender DM-MAC can be extended to DM-MACs with more senders. In this section, we present the performance of random homologous code ensembles for the k-sender DM-MAC $p(y|x_1, x_2, \ldots, x_k)$. Similar to Section 5.3, we first discuss the performance of random homologous codes under the fixed channel alphabets, following the recent work in [5]. We then generalize the result by incorporating channel transformation.

5.4.1 Shaping

The achievable rate region for the finite-field input DM-MAC $p(y|x_1, x_2, \ldots, x_k)$, $\mathcal{X}_1 = \mathcal{X}_2 = \cdots = \mathcal{X}_k = \mathbb{F}_q$, by random homologous code ensembles was studied in [5]. For the sake of completeness, we review the main result in [5] on which we build the achievability of the capacity region for the k-sender DM-MAC. Let $\mathcal{A}$ denote the set of rank deficient $k \times k$ matrices over $\mathbb{F}_q$. For a given matrix $A \in \mathcal{A}$, we define the collection

$$\mathscr{D}(A) = \{\mathcal{J} \subseteq [k] : |\mathcal{J}| = k - \mathrm{rank}(A),\ \mathrm{rank}[A^T\ e(\mathcal{J})^T]^T = k\},$$

where $e(\mathcal{J}) \in \mathbb{F}_q^{|\mathcal{J}| \times k}$ denotes the matrix whose rows are the standard basis vectors e_j for $j \in \mathcal{J}$. For a given set $\mathcal{J} \in \mathscr{D}(A)$ and input pmfs $p(x_1), p(x_2), \ldots, p(x_k)$, we define the rate region $\mathscr{R}(A, \mathcal{J}, X^k)$ as the set of rate tuples $(R_1, R_2, \ldots, R_k)$ such that

$$\sum_{j \in \mathcal{J}} R_j < I(X(\mathcal{J}); Y, W_A),$$

where

$$W_A = A\, [X_1 \; X_2 \; \ldots \; X_k]^T.$$

We are now ready to state the main result of [5].

Proposition 5.4.1 ([5, Theorem 1])**.** *A rate tuple $(R_1, R_2, \ldots, R_k)$ is achievable by random homologous codes in $\mathbb{F}_q$ for the finite-field input DM-MAC $p(y|x_1, x_2, \ldots, x_k)$, if*

$$(R_1, R_2, \ldots, R_k) \in \bigcap_{A \in \mathcal{A}} \bigcup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X^k)$$

for some input pmfs $p(x_1), p(x_2), \ldots, p(x_k)$.

Remark 5.4.1 (Revisit of the 2-sender DM-MAC)**.** *Consider the 2-sender DM-MAC $p(y|x_1, x_2)$ with given input pmfs $p(x_1)$ and $p(x_2)$. To compute the achievable rate region in Proposition 5.4.1, it suffices to consider the set of rank deficient 2×2 matrices with different spans. There are four types of such matrices:*

- $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$*:*

  $\mathscr{D}(A) = \{\{1, 2\}\}$ and $\cup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X_1, X_2)$ reduces to the set of rate pairs satisfying

  $$R_1 + R_2 < I(X_1, X_2; Y),$$

- $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$*:*

$\mathscr{D}(A) = \{\{1\}\}$ and $\cup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X_1, X_2)$ is the set of rate pairs satisfying

$$R_1 < I(X_1; Y | X_2),$$

- $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$*:*

  $\mathscr{D}(A) = \{\{2\}\}$ and $\cup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X_1, X_2)$ is the set of rate pairs satisfying

$$R_2 < I(X_2; Y | X_1),$$

- $A = \begin{bmatrix} 1 & a \\ 0 & 0 \end{bmatrix}$ *for some nonzero $a \in \mathbb{F}_q$:*

  $\mathscr{D}(A) = \{\{1\}, \{2\}\}$ and $\cup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X_1, X_2)$ is the set of rate pairs satisfying

$$R_1 < I(X_1; Y, W_a),$$

  or

$$R_2 < I(X_2; Y, W_a),$$

  where $W_a = X_1 \oplus aX_2$.

The achievable rate region in Proposition 5.4.1 is then equivalent to $\mathscr{R}_{\mathrm{MAC}}(X_1, X_2) \cap \tilde{\mathscr{R}}_{\mathrm{L}}(X_1, X_2)$ where $\tilde{\mathscr{R}}_{\mathrm{L}}(X_1, X_2)$ is the set of rate pairs (R_1, R_2) such that for every nonzero $a \in \mathbb{F}_q$

$$R_1 < I(X_1; Y, X_1 \oplus aX_2) \tag{5.9}$$

or

$$R_2 < I(X_2; Y, X_1 \oplus aX_2). \tag{5.10}$$

One may notice that for every nonzero a over $\mathbb{F}_q$

$$H(X_1 | Y, X_1 \oplus aX_2) = H(X_2 | Y, X_1 \oplus aX_2)$$

$$\leq \min\{H(X_1|Y), H(X_2|Y)\},$$

which implies that $\tilde{\mathscr{R}}_{\mathrm{L}}(X_1, X_2)$ is in general larger than $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$ defined in Proposition 5.3.1 in Section 5.3.1. Indeed, the error analysis in the proof of Proposition 5.3.1 can be modified to account for the larger $\tilde{\mathscr{R}}_{\mathrm{L}}(X_1, X_2)$ region.

Remark 5.4.2. *The achievable rate region in Proposition 5.4.1 is the largest region thus far established with homologous codes in the literature. As a matter of fact, there is some indication that this region is optimal in the sense that it cannot be improved by using maximum likelihood decoding [8, 9]. Still, it is in general strictly smaller than the capacity region of the k-sender DM-MAC. In particular, for the channels defined in Examples 5.2.1–5.3.1, the achievable rate region in Propositon 5.4.1 reduces to the achievable rate region in Proposition 5.3.1 described in Section 5.3.1. To see this, fix input pmfs $p(x_1)$ and $p(x_2)$. The set of rate pairs satisfying (5.9) or (5.10) for $a = 1$ is equivalent to the rate region $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$.*

As a corollary of Proposition 5.4.1, we can come up with a smaller rate region achievable by random homologous codes that is easier to compute. As we will discuss in the next section, however, this smaller achievable rate region combined with channel transformation gives rise to the achievability of the capacity region. Let $\mathcal{B}$ denote the set of rank deficient $k \times k$ matrices over $\mathbb{F}_q$ that is not row equivalent[3] to a diagonal matrix. Note that $\mathcal{B} \subset \mathcal{A}$. Given a matrix $A \in \mathcal{B}$, a set $\mathcal{J} \in \mathscr{D}(A)$, and input pmfs $p(x_1), p(x_2), \ldots, p(x_k)$, we define the rate region $\tilde{\mathscr{R}}(A, \mathcal{J}, X^k)$ as the set of rate tuples $(R_1, R_2, \ldots, R_k)$ satisfying

$$\sum_{j \in \mathcal{J}} R_j < H(X(\mathcal{J})) - \min_{\mathcal{S} \in \mathscr{D}(A)} H(X(\mathcal{S})|Y).$$

[3] Two matrices are row equivalent if one can be obtained from the other by a sequence of elementary row operations.

Given input pmfs $p(x_1), p(x_2), \dots, p(x_k)$, we define the rate region

$$\mathscr{R}_{\mathrm{L}}(X^k) = \bigcap_{A \in \mathcal{B}} \bigcup_{\mathcal{J} \in \mathscr{D}(A)} \tilde{\mathscr{R}}(A, \mathcal{J}, X^k). \tag{5.11}$$

Corollary 5.4.1 (Shaping–Extension of Proposition 5.3.1 to k senders)**.** *A rate tuple $(R_1, R_2, \dots, R_k)$ is achievable by random homologous codes in $\mathbb{F}_q$ for the finite-field input DM-MAC $p(y|x_1, x_2, \dots, x_k)$, if*

$$(R_1, R_2, \dots, R_k) \in \mathscr{R}_{\mathrm{MAC}}(X^k) \cap \mathscr{R}_{\mathrm{L}}(X^k)$$

for some input pmfs $p(x_1), p(x_2), \dots, p(x_k)$.

We first revisit the 2-sender case with Corollary 5.4.1 and then provide a proof for Corollary 5.4.1.

Remark 5.4.3 (Revisit of the 2-sender DM-MAC with Corollary 5.4.1)**.** *For the case $k = 2$, the achievable rate region in Corollary 5.4.1 reduces to the achievable rate region in Proposition 5.3.1. To see this, fix input pmfs $p(x_1)$ and $p(x_2)$. A rank-deficient 2×2 matrix over $\mathbb{F}_q$ that is not row equivalent to a diagonal matrix must be row equivalent to a matrix of the form*

$$\begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix}$$

for some nonzero a_1 and a_2 over $\mathbb{F}_q$. Then, for every such matrix A, $\mathscr{D}(A) = \{\{1\}, \{2\}\}$. Therefore, the rate region $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$ defined in (5.11) is the set of rate pairs (R_1, R_2) such that

$$R_1 < H(X_1) - \min\{H(X_1|Y), H(X_2|Y)\}$$

or

$$R_2 < H(X_2) - \min\{H(X_1|Y), H(X_2|Y)\},$$

which is equivalent to the rate region $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$ defined in Section 5.3.1.

Proof of Corollary 5.4.1. We will show that given input pmfs $p(x_1), p(x_2), \ldots, p(x_k)$

$$(\mathscr{R}_{\mathrm{MAC}}(X^k) \cap \mathscr{R}_{\mathrm{L}}(X^k)) \subseteq \bigcap_{A \in \mathcal{A}} \bigcup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X^k),$$

by first showing that

$$\mathscr{R}_{\mathrm{MAC}}(X^k) = \bigcap_{A \in \mathcal{A} \setminus \mathcal{B}} \bigcup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X^k),$$

and then showing that

$$\mathscr{R}_{\mathrm{L}}(X^k) \subseteq \bigcap_{A \in \mathcal{B}} \bigcup_{\mathcal{J} \in \mathscr{D}(A)} \mathscr{R}(A, \mathcal{J}, X^k).$$

To prove the first claim, let A be a rank-deficient $k \times k$ matrix that is row equivalent to a diagonal matrix D (i.e., $A \in \mathcal{A} \setminus \mathcal{B}$), and let $\mathcal{J}$ be the set of indices such that $j \in \mathcal{J}$ if $D_{jj} = 0$. Then, by Lemma 5.G.1 in Appendix 5.G, $\mathscr{D}(A) = \mathcal{J}$ and $\mathscr{R}(A, \mathcal{J}, X^k)$ is reduced to the set of rate tuples $(R_1, R_2, \ldots, R_k)$ satisfying

$$\sum_{j \in \mathcal{J}} R_j < I(X(\mathcal{J}); Y, X(\mathcal{J}^c)).$$

Taking the intersection over all $A \in \mathcal{A} \setminus \mathcal{B}$ proves the first claim. For the second claim, it suffices to show that given a matrix $A \in \mathcal{B}$ and a set $\mathcal{J} \in \mathscr{D}(A)$

$$\tilde{\mathscr{R}}(A, \mathcal{J}, X^k) \subseteq \mathscr{R}(A, \mathcal{J}, X^k).$$

Now, a rate tuple $(R_1, R_2, \ldots, R_k) \in \tilde{\mathscr{R}}(A, \mathcal{J}, X^k)$ satisfies

$$\sum_{j \in \mathcal{J}} R_j < H(X(\mathcal{J})) - \min_{\mathcal{S} \in \mathscr{D}(A)} H(X(\mathcal{S})|Y)$$

$$\begin{aligned}
&\leq H(X(\mathcal{J})) - \min_{\mathcal{S} \in \mathscr{D}(A)} H(X(\mathcal{S})|Y, W_A) \\
&\overset{(a)}{=} H(X(\mathcal{J})) - H(X(\mathcal{J})|Y, W_A), \\
&= I(X(\mathcal{J}); Y, W_A),
\end{aligned}$$

where (a) follows since $H(X(\mathcal{J})|Y, W_A) = H(X^k|Y, W_A)$ is constant for every $\mathcal{J} \in \mathscr{D}(A)$. Therefore, we have $(R_1, R_2, \ldots, R_k) \in \mathscr{R}(A, \mathcal{J}, X^k)$, which completes the proof. □

5.4.2 Combination

We incorporate channel transformation into random homologous codes to prove the achievability of the capacity region of the k-sender DM-MAC. Similar to the idea discussed in Section 5.3.2, we can simply transform the channel $p(y|x_1, x_2, \ldots, x_k)$ into a *virtual channel* with finite-field inputs

$$p(y|v_1, v_2, \ldots, v_k) = p_{Y|X_1,X_2,\ldots,X_k}(y|\varphi_1(v_1), \varphi_2(v_2), \ldots, \varphi_k(v_k)) \tag{5.12}$$

for some symbol-by-symbol mappings $\varphi_j : \mathbb{F}_q \to \mathcal{X}_j$, $j \in [k]$.

Now, consider the virtual channel in (5.12) and random homologous codes for this channel. Then, Corollary 5.4.1 implies the following.

Proposition 5.4.2. *A rate tuple $(R_1, R_2, \ldots, R_k)$ is achievable by random homologous codes in $\mathbb{F}_q$ for the DM-MAC $p(y|x_1, x_2, \ldots, x_k)$, if*

$$(R_1, R_2, \ldots, R_k) \in \mathscr{R}_{\text{MAC}}(X^k) \cap \mathscr{R}_{\text{L}}(V^k)$$

for some $p(v_1), p(v_2), \ldots, p(v_k)$ on $\mathbb{F}_q$ and some mappings $x_1 = \varphi_1(v_1)$, $x_2 = \varphi_2(v_2)$, …, $x_k = \varphi_k(v_k)$, where $\mathscr{R}_{\text{L}}(V^k)$ is the set of rate tuples $(R_1, R_2, \ldots, R_k)$ satisfying (5.11) for the virtual channel $p(y|v_1, v_2, \ldots, v_k)$.

We are now ready to extend Theorem 5.3.1 to the k-sender case, which follows from Proposition 5.4.2 by optimizing over all channel transformations.

Theorem 5.4.1 (Combination)**.** *A rate tuple $(R_1, R_2, \ldots, R_k)$ is achievable by random homologous codes in some finite field for the DM-MAC $p(y|x_1, x_2, \ldots, x_k)$, if*

$$(R_1, R_2, \ldots, R_k) \in \mathscr{R}_{\text{MAC}}(X^k)$$

for some $p(x_1), p(x_2), \ldots, p(x_k)$.

Proof. We follow similar arguments to the proof of Theorem 5.3.1 and show that given input pmfs $p(x_1), p(x_2), \ldots, p(x_k)$, there exists a finite field $\mathbb{F}_q$, pmfs $p(v_1), p(v_2), \ldots, p(v_k)$ on $\mathbb{F}_q$, and mappings $x_1 = \varphi_1(v_1), x_2 = \varphi_2(v_2), \ldots, x_k = \varphi_k(v_k)$ such that

$$\mathscr{R}_{\text{MAC}}(X^k) \subseteq \mathscr{R}_{\text{L}}(V^k). \tag{5.13}$$

First, suppose that $p(x_j)$, $j \in [k]$, are of the form i/ρ^m for some $i, m \in \mathbb{Z}^+$ and prime ρ. We consider random homologous codes over $\mathbb{F}_q$ with $q = \rho^{k^k m}$. Let $q_j = \rho^{k^{(k-j+1)}m}$ for $j \in [k]$ and note that

$$\mathbb{F}_{q_k} \subset \mathbb{F}_{q_{k-1}} \subset \cdots \subset \mathbb{F}_{q_1} = \mathbb{F}_q.$$

Consider $V_j \sim \text{Unif}(\mathbb{F}_{q_j})$, and φ_j such that $\varphi_j(V_j) \overset{d}{=} X_j$ for $j \in [k]$ (this is possible due to the form of $p(x_j)$ and by the choice of q_j). To see (5.13), it suffices to show that for every matrix $A \in \mathcal{B}$, $\mathscr{R}_{\text{MAC}}(X^k) \subseteq \cup_{\mathcal{J} \in \mathscr{D}(A)} \tilde{\mathscr{R}}(A, \mathcal{J}, V^k)$. Consider a rate tuple $(R_1, R_2, \ldots, R_k) \in \mathscr{R}_{\text{MAC}}(X^k)$ and a matrix $A \in \mathcal{B}$. By Lemma 5.G.1 (see Appendix 5.G) and by the choice of $p(v_j)$, there exist at least two different sets $\mathcal{J}_1, \mathcal{J}_2 \in \mathscr{D}(A)$ such that

$$H(V(\mathcal{J}_1)) - H(V(\mathcal{J}_2)) \geq k \log \rho^m \geq H(X^k).$$

Then, $(R_1, R_2, \ldots, R_k)$ satisfies

$$\sum_{j \in \mathcal{J}_1} R_j < H(X^k)$$

$$
\begin{aligned}
&\le H(V(\mathcal{J}_1)) - H(V(\mathcal{J}_2))\\
&\le H(V(\mathcal{J}_1)) - \min_{\mathcal{S} \in \mathscr{D}(A)} H(V(\mathcal{S}))\\
&\le H(V(\mathcal{J}_1)) - \min_{\mathcal{S} \in \mathscr{D}(A)} H(V(\mathcal{S})|Y),
\end{aligned}
$$

which implies that $(R_1, R_2, \ldots, R_k) \in \tilde{\mathscr{R}}(A, \mathcal{J}_1, V^k)$. The claim follows since A is an arbitrary set in $\mathcal{B}$. The restrictions on the input pmfs can be removed again by the denseness argument. □

5.5 Multiple-Receiver Multiple Access Channels

We consider the two-receiver DM-MAC $p(y_1, y_2|x_1, x_2)$, where each sender wishes to convey its own message to both of the receivers. Given input pmfs $p(x_1)$ and $p(x_2)$, define $\mathscr{R}^{(1)}_{\text{MAC}}(X_1, X_2)$ as the set of rate pairs satisfying

$$
\begin{aligned}
R_1 &\le I(X_1; Y_1|X_2),\\
R_2 &\le I(X_2; Y_1|X_1),\\
R_1 + R_2 &\le I(X_1, X_2; Y_1),
\end{aligned}
$$

and $\mathscr{R}^{(2)}_{\text{MAC}}(X_1, X_2)$ as the set of rate pairs satisfying

$$
\begin{aligned}
R_1 &\le I(X_1; Y_2|X_2),\\
R_2 &\le I(X_2; Y_2|X_1),\\
R_1 + R_2 &\le I(X_1, X_2; Y_2).
\end{aligned}
$$

The following proposition then characterizes the achievable rate region by random homologous codes.

Proposition 5.5.1 (Extension of Theorem 5.3.1 to two-receiver)**.** *A rate pair (R_1, R_2) is achievable by random homologous codes in some finite field for the two-receiver DM-MAC*

$p(y_1, y_2|x_1, x_2)$, if

$$(R_1, R_2) \in \mathscr{R}_{\text{MAC}}^{(1)}(X_1, X_2) \cap \mathscr{R}_{\text{MAC}}^{(2)}(X_1, X_2)$$

for some pmfs $p(x_1)$ and $p(x_2)$.

Proof. The achievable rate region depends on the conditional pmf $p(y_1, y_2|x_1, x_2)$ only through the conditional marginal pmfs $p(y_1|x_1, x_2)$ and $p(y_2|x_1, x_1)$. First suppose that $p(x_1)$ and $p(x_2)$ are of the form (5.8). We consider random homologous codes over $\mathbb{F}_q$ with $q = \rho^{2m}$. Choose V_1 and φ_1 such that V_1 and $\varphi_1(V_1) \overset{d}{=} X_1$ are one-to-one on the support of V_1 (this is always possible since $q \geq \rho^m$). Also choose $V_2 \sim \text{Unif}(\mathbb{F}_q)$ and φ_2 such that $\varphi_2(V_2) \overset{d}{=} X_2$ (this is possible due to the form of $p(x_2)$). By Proposition 5.3.3, the achievable rate region is

$$\bigcap_{j=1}^{2} [\mathscr{R}_{\text{MAC}}^{(j)}(X_1, X_2) \cap \mathscr{R}_{\text{L}}^{(j)}(V_1, V_2)],$$

where $\mathscr{R}_{\text{L}}^{(j)}(V_1, V_2), j = 1, 2$, is the set of rate pairs (R_1, R_2) satisfying (5.2) or (5.3) for the virtual DM-MAC $p(y_j|v_1, v_2)$. The argument in the proof of Theorem 5.3.1 can be applied to both of the DM-MACs $p(y_1|x_1, x_2)$ and $p(y_2|x_1, x_2)$. As a result, the rate region $\mathscr{R}_{\text{MAC}}^{(j)}(X_1, X_2) \cap \mathscr{R}_{\text{L}}^{(j)}(V_1, V_2), j = 1, 2$, is equivalent to the rate region $\mathscr{R}_{\text{MAC}}^{(j)}(X_1, X_2)$, which implies the claim. The restriction on the input pmfs can be removed by the denseness argument. □

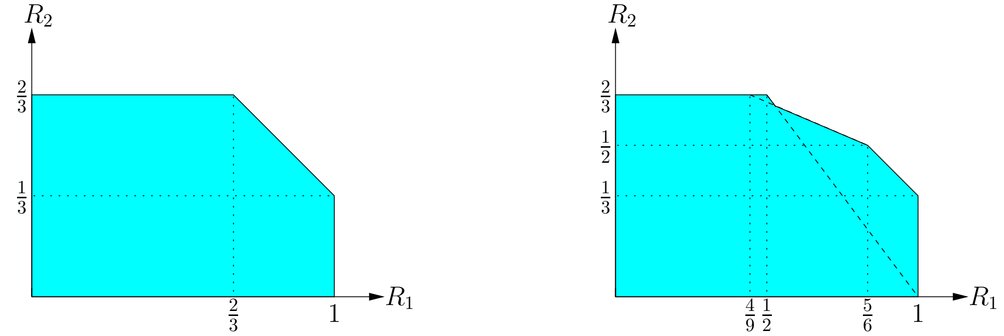
As shown in the examples of the binary adder MAC, the binary erasure MAC, and the on–off erasure MAC, the insufficiency of shaping or channel transformation for *single-receiver* MACs can be overcome by time sharing. Indeed, either shaping or channel transformation can achieve the corner points of $\mathscr{R}_{\text{MAC}}(X_1, X_2)$ of a general DM-MAC $p(y|x_1, x_2)$. This is no longer the case for multiple receivers, however. As illustrated by the following example, a proper combination of shaping and channel transformation can strictly outperform shaping or channel transformation alone even when time sharing is allowed only for the individual techniques.

Example 5.5.1 (A two-receiver MAC). *Let $Y_1 = X_1 + X_2$ (binary erasure MAC), and $Y_2 = (2X_1 - 1) + Z(2X_2 - 1)$ (on–off erasure MAC), where $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$ and $Z \sim \mathrm{Bern}(2/3)$ is independent of X_1 and X_2. The capacity region of this two-receiver MAC is achieved by random coding with i.i.d.* Bern(1/2) *inputs X_1 and X_2, and is sketched in Fig. 5.11a. Given input pmfs $p(x_1)$ and $p(x_2)$, the achievable rate region via shaping in Proposition 5.3.1 (and Proposition 5.4.1) is*

$$\bigcap_{j=1}^{2} [\mathscr{R}_{\mathrm{MAC}}^{(j)}(X_1, X_2) \cap \mathscr{R}_{\mathrm{L}}^{(j)}(X_1, X_2)],$$

where $\mathscr{R}_{\mathrm{L}}^{(j)}(X_1, X_2), j = 1, 2$, is the set of rate pairs (R_1, R_2) satisfying (5.2) or (5.3) for the DM-MAC $p(y_j|x_1, x_2)$. The union of this rate region over input pmfs $p(x_1)$ and $p(x_2)$ is shown in Fig. 5.11b. Even after convexification via time sharing, it is strictly smaller than the capacity region with the largest symmetric rate of 11/18, *whereas the symmetric capacity is* 2/3. *In comparison, we can combine shaping with channel transformation to achieve the entire capacity region as follows. Consider random homologous codes over $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$. Let $V_1 \sim \mathrm{Unif}(\mathbb{F}_4)$ and $V_2 \sim \mathrm{Bern}(1/2)$ be independent. For channel transformation, let $x_j = \varphi(v_j)$ where $\varphi(0) = \varphi(\alpha) = 0$, and $\varphi(1) = \varphi(\alpha + 1) = 1$. By this construction, X_1 and X_2 are i.i.d.* Bern(1/2). *Following similar steps to the proof of Proposition 5.5.1, it is easy to see that the achievable rate region under this construction is equivalent to $\mathscr{R}_{\mathrm{MAC}}^{(1)}(X_1, X_2) \cap \mathscr{R}_{\mathrm{MAC}}^{(2)}(X_1, X_2)$, which is the capacity region of this channel since $p(x_1)$ and $p(x_2)$ are chosen as the capacity-achieving distributions. Thus, combination of shaping with channel transformation not only achieves higher rates than the shaping technique alone, but also achieves the capacity region* without *the need for time sharing.*

Remark 5.5.1. *Proposition 5.5.1 can be extended to k-sender and r-receiver DM-MACs and compound MACs via the proof of Theorem 5.4.1.*



(a) The capacity region.

(b) The achievable rate region implied by Proposition 5.3.1.

Figure 5.11. The two-receiver MAC in Example 5.5.1.

5.6 Gaussian Multiple Access Channels

Consider the 2-sender Gaussian MAC model

$$Y = g_1X_1 + g_2X_2 + Z,$$

with channel gains g_1 and g_2, additive noise $Z \sim \mathrm{N}(0,1)$, and average power constraints $\sum_{i=1}^{n} x_{ji}^2(m_j) \leq nP$ for $j = 1,2$. Let $S_j = g_j^2 P$, $j = 1,2$. The following theorem establishes the achievability of the capacity region of the Gaussian MAC by random homologous codes.

Theorem 5.6.1 (Gaussian MACs)**.** *A rate pair* (R_1, R_2) *is achievable by random homologous codes in some finite field for the* 2*-sender Gaussian MAC, if*

$$\begin{aligned} R_1 &\leq \mathsf{C}(S_1), \\ R_2 &\leq \mathsf{C}(S_2), \\ R_1 + R_2 &\leq \mathsf{C}(S_1 + S_2), \end{aligned}$$

where $\mathsf{C}(x) = (1/2)\log(1+x), x \geq 0,$ *is the Gaussian capacity function.*

Proof. Theorem 5.6.1 can be proved using the discretization argument in [6, Section 3.4.1] together with the achievability proof for the 2-sender DM-MAC by random homologous codes. The proof along this line, however, needs two limit arguments—one for approximating a Gaussian random variable by a discrete random variable, and one for approximating the resulting pmf on a finite alphabet to the desired form in (5.8). We instead provide a simpler proof via a discretization mapping that results in a pmf of desired form in (5.8) and thus eliminates one of the limit arguments.

Let X_1 and X_2 be i.i.d. $\mathrm{N}(0, P)$. For every $j = 1, 2, \ldots$, let $[X_1]_j \in \{F_{X_1}^{-1}(i/2^j) : i \in [2^j - 1]\}$ be a quantized version of X_1 obtained by mapping X_1 to the closest point $[X_1]_j$ such that $|[X_1]_j| \leq |X_1|$, where $F_{X_1}(x)$ denotes the cdf of random variable X_1. Clearly, $\mathsf{E}([X_1]_j^2) \leq \mathsf{E}(X_1^2) = P$ and the pmf of $[X_1]_j$ is of the form $r/2^j$ for some positive integer r. Define $[X_2]_j$ in a similar manner. Let $Y_j = g_1[X_1]_j + g_2[X_2]_j + Z$ be the output corresponding to the input pair $[X_1]_j$ and $[X_2]_j$, and let $[Y_j]_k$ be a quantized version of Y_j defined in the same manner. Now, by the achievability proof of Theorem 5.3.1, for every j, k, random homologous codes over $\mathbb{F}_q$ with $q = 2^{2j}$ can achieve the rate pair satisfying

$$\begin{aligned} R_1 &\leq I([X_1]_j; [Y_j]_k | [X_2]_j), \\ R_2 &\leq I([X_2]_j; [Y_j]_k | [X_1]_j), \\ R_1 + R_2 &\leq I([X_1]_j, [X_2]_j; [Y_j]_k). \end{aligned}$$

By this type of discretization, weak convergence of $[X_1]_j$ to X_1 and $[X_2]_j$ to X_2 is preserved, and $([Y_j]_k - Y_j)$ tends to 0 as $k \to \infty$. Therefore, one can follow the same steps in the proof of [6, Lemma 3.2] to show that

$$\begin{aligned} \liminf_{j\to\infty} \lim_{k\to\infty} I([X_1]_j; [Y_j]_k | [X_2]_j) &\geq I(X_1; Y | X_2), \\ \liminf_{j\to\infty} \lim_{k\to\infty} I([X_2]_j; [Y_j]_k | [X_1]_j) &\geq I(X_2; Y | X_1), \\ \liminf_{j\to\infty} \lim_{k\to\infty} I([X_1]_j, [X_2]_j; [Y_j]_k) &\geq I(X_1, X_2; Y), \end{aligned}$$

which establishes the claim. □

Remark 5.6.1. *It is straightforward to extend the discretization argument described for the* 2*-sender Gaussian MAC to the* k*-sender case. Therefore, the capacity region of a Gaussian MAC in general is achievable by random homologous codes.*

5.7 Simultaneous Computation and Communication Over Multiple Access Channels

In the previous sections, we have investigated the performance of homologous codes—which were originally proposed for computing linear combinations of the transmitted codewords—for message communication over MACs. One immediate question arising from our investigations is whether one can use homologous codes for computation and communication at the same time. To be more specific, consider a multiple-receiver MAC in which some receiver wishes to recover a desired linear combination of codewords (computation) while another receiver wishes to recover the messages themselves (communication). In this section, we demonstrate how random homologous codes discussed thus far can be adapted to simultaneously achieve such competing goals, highlighting the potential of homologous codes for a broader class of applications beyond multiple access communication.

Consider the two-sender two-receiver DM-MAC $p(y_1, y_2|x_1, x_2)$ with finite-field inputs $\mathcal{X}_1 = \mathcal{X}_2 = \mathbb{F}_q$, in which the first receiver wishes to recover a desired linear combination of codewords in $\mathbb{F}_q$

$$W_{\mathbf{a}}^n = a_1 X_1^n \oplus a_2 X_2^n$$

for a given $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$, as formally defined in Chapter 3, and the second receiver wishes to recover the messages themselves. We refer to this channel as the *compute-communicate* DM-MAC.

We start with the performance of random i.i.d. codes. Given an input pmf

$p = p(x_1)p(x_2)$, let $\mathscr{R}^{(j)}_{\text{MAC}}(X_1, X_2)$, $j = 1, 2$, denote the pentagonal region in (5.1) evaluated for the DM-MAC $p(y_j|x_1, x_2)$ and let $\mathscr{R}^{(1)}_{\text{TIN}}(X_1, X_2, \mathbf{a})$ denote the rate region in (3.31) evaluated for the DM-MAC $p(y_1|x_1, x_2)$. We can define the achievability by p-distributed random i.i.d. codes for the compute-communicate DM-MAC $p(y_1, y_2|x_1, x_2)$ in a similar manner to Section 3.5. The following achievability result follows from Proposition 3.5.1 and the fact that the rate region $\mathscr{R}^{(j)}_{\text{MAC}}(X_1, X_2)$ is achievable for the DM-MAC $p(y_j|x_1, x_2)$ by random i.i.d. codes, which was proved in [].

Corollary 5.7.1 (i.i.d. codes for compute-communicate)**.** *Given a pmf* $p = p(x_1)p(x_2)$ *and* $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$*, a rate pair* (R_1, R_2) *is achievable by p-distributed random i.i.d. codes for the compute-communicate DM-MAC* $p(y_1, y_2|x_1, x_2)$ *if*

$$(R_1, R_2) \in [\mathscr{R}^{(1)}_{TIN}(X_1, X_2, \mathbf{a}) \cup \mathscr{R}^{(1)}_{\text{MAC}}(X_1, X_2)] \cap \mathscr{R}^{(2)}_{\text{MAC}}(X_1, X_2).$$

We then return back to our discussion on random homologous codes. Propositions 5.3.1 and 3.2.1 imply the following.

Corollary 5.7.2 (Homologous codes for compute-communicate)**.** *Given a pmf* $p = p(x_1)p(x_2)$ *and* $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$*, a rate pair* (R_1, R_2) *is achievable by random homologous codes for the compute-communicate DM-MAC* $p(y_1, y_2|x_1, x_2)$ *if it is included in*

$$\mathscr{R}^{(1)}_{\text{CF}}(X_1, X_2, \mathbf{a}) \cap \mathscr{R}^{(2)}_{\text{MAC}}(X_1, X_2) \cap \mathscr{R}^{(2)}_{\text{L}}(X_1, X_2), \tag{5.14}$$

where $\mathscr{R}^{(1)}_{\text{CF}}(X_1, X_2, \mathbf{a})$ *denotes the* compute–forward *rate region defined in (3.8) evaluated for the DM-MAC* $p(y_1|x_1, x_2)$ *with the input pmfs* $p(x_1)$ *and* $p(x_2)$*.*

Indeed, it is possible to construct homologous codes over the extension field $\mathbb{F}_{q^r}$ for some positive integer r to enlarge the achievable rate region in Corollary 5.7.2. By allowing extension fields $\mathbb{F}_{q^r}$ for some positive integer r in the channel transformation step, we get the following.

Corollary 5.7.3 (Homologous codes over extension fields)**.** *Given a pmf $p = p(x_1)p(x_2)$ and $\mathbf{a} \neq \mathbf{0} \in \mathbb{F}_q^2$, a rate pair (R_1, R_2) is achievable by random homologous codes for the compute-communicate DM-MAC $p(y_1, y_2|x_1, x_2)$ if it is included in*

$$\mathscr{R}_{\mathrm{CF}}^{(1)}(U_1, U_2, \mathbf{a}) \cap \mathscr{R}_{\mathrm{MAC}}^{(2)}(X_1, X_2) \cap \mathscr{R}_{\mathrm{L}}^{(2)}(U_1, U_2), \tag{5.15}$$

for some input pmfs $p(u_1)$ and $p(u_2)$ over $\mathbb{F}_{q^r}$ for $r \in \mathbb{Z}^+$ and for some mapping $\varphi : \mathbb{F}_{q^r} \to \mathbb{F}_q$ such that

$$x_1 = \varphi(u_1), \quad x_2 = \varphi(u_2),$$

and

$$\varphi(a_1 u_1 \oplus a_2 u_2) = a_1 \varphi(u_1) \oplus a_2 \varphi(u_2).$$

The results presented thus far in this section can be extended to arbitrary number of senders and receivers. As an example, we consider simultaneous computation and communication over a two-sender three-receiver DM-MAC and illustrate that random homologous codes, combined with carefully chosen channel transformation, outperform random i.i.d. codes as well as random homologous codes without channel transformation.

Example 5.7.1. *Consider the* compute-communicate *DM-MAC $p(y_1, y_2, y_3|x_1, x_2)$, in which $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$ and*

$$\begin{aligned} &Y_1 = X_1 \oplus X_2, && \textit{(binary adder MAC)} \\ &Y_2 = X_1 + X_2, && \textit{(binary erasure MAC)} \\ &Y_3 = (2X_1 - 1) + Z(2X_2 - 1), && \textit{(on–off erasure MAC)} \end{aligned}$$

where $Z \sim \mathrm{Bern}(2/3)$ is independent of X_1 and X_2. Receiver 1 wishes to recover $M_1 \oplus M_2$ over a binary field $\mathbb{F}_2$, whereas both receivers 2 and 3 wish to recover the message pair (M_1, M_2).

We now compare achievable rates by different class of codes.

1. ***Random i.i.d. codes:*** *Corollary 5.7.1 implies that a rate pair* (R_1, R_2) *is achievable if it is included in the intersection of the capacity regions of the DM-MACs* $p(y_1|x_1, x_2)$*,* $p(y_2|x_1, x_2)$*, and* $p(y_3|x_1, x_2)$*, any one of which is achieved by i.i.d.* Bern(1/2) *inputs* X_1 *and* X_2*, and so is the intersection. Fig. 5.12a sketches the rate region. In particular, the largest possible symmetric rate achievable by random i.i.d. codes is* 1/2*.*

2. ***Binary random homologous codes:*** *Corollary 5.7.2 implies that for any given input pmfs* $p(x_1)$ *and* $p(x_2)$ *over* $\mathbb{F}_2$*, a rate pair* (R_1, R_2) *is achievable if it is included in*

$$\mathscr{R}_{\mathrm{CF}}^{(1)}(X_1, X_2, [1\ 1]) \cap \bigcap_{j=2}^{3} [\mathscr{R}_{\mathrm{MAC}}^{(j)}(X_1, X_2) \cap \mathscr{R}_{\mathrm{L}}^{(j)}(X_1, X_2)]. \tag{5.16}$$

Note that the rate region $\mathscr{R}_{\mathrm{CF}}^{(1)}(X_1, X_2, [1\ 1])$ *is larger than the rest of the terms in (5.16) for any given input pmfs* $p(x_1)$ *and* $p(x_2)$*. Taking the union of the rate region in (5.16) over the input pmfs results in the same rate region sketched earlier in Fig. 5.11b for the two-receiver DM-MAC* $p(y_2, y_3|x_1, x_2)$ *and is given in Fig. 5.12b for comparison. Therefore, the largest achievable symmetric rate in this region is* 3/5*.*

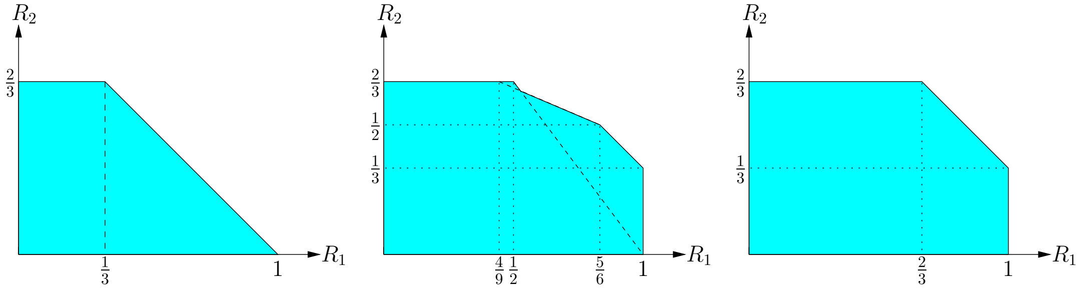
3. ***Quaternary random homologous codes:*** *We are now allowed to use a larger finite field via channel transformation, but we need to be more careful for the choice of channel transformation because we have an additional receiver decoding for the sum of virtual codewords rather than the messages themselves. Let* $U_1 \sim \mathrm{Unif}(\mathbb{F}_4)$ *and*

$$U_2 = \begin{cases} 0 & \textit{with probability } \frac{1-\gamma}{2} \\ 1 & \textit{with probability } \frac{1-\gamma}{2} \\ \alpha & \textit{with probability } \frac{\gamma}{2} \\ \alpha+1 & \textit{with probability } \frac{\gamma}{2} \end{cases},$$

be independent for some γ chosen such that $H(\gamma) \in [1/3, 2/3]$. Let $x_j = \varphi(u_j)$ where $\varphi(0) = \varphi(\alpha) = 0$, and $\varphi(1) = \varphi(\alpha + 1) = 1$. By this construction, X_1 and X_2 are i.i.d. Bern(1/2)*. By Corollary 5.7.3, for a given γ and the corresponding pmf $p(u_1, u_2, x_1, x_2)$, it is easy to see that a rate pair (R_1, R_2) is achievable if it satisfies*

$$
\begin{aligned}
R_1 &< 4/3 - H(\gamma), \\
R_2 &< H(\gamma).
\end{aligned}
$$

Taking the union over γ such that $H(\gamma) \in [1/3, 2/3]$ results in the rate region sketched in Fig. 5.12c. Therefore, the largest achievable symmetric rate is 2/3, which can be shown to be the symmetric capacity for this example.



(a) Corollary 5.7.1. **(b)** Corollary 5.7.2. **(c)** Corollary 5.7.3.

Figure 5.12. Achievable rate regions for the compute-communicate MAC in Example 5.7.1.

5.8 Discussion

In this chapter, we examined the possibility of reestablishing the well-known achievable rate regions by random code ensembles for the MACs by using structured, homologous codes. We identified two key techniques to employ nonuniform codewords while preserving a similar structure across the codes of users. The analysis tools developed for these techniques, shaping and channel transformation, imply that their individual performance is insufficient. It is unclear, however, whether there is a fundamental limitation behind each technique. As a constructive alternative to these two techniques and their limits, we showed that an appropriately designed combination of the two can establish the performance of random code ensembles. This development and its generalization to multiple senders and receivers motivate further research into the potential of homologous coding in network information theory.

5.A A Proposition on Coset Codes for the Binary Erasure MAC

Proposition 5.A.1. *For the binary erasure MAC, no pair of binary coset codes with the same generator matrix can achieve the rate pair* $(1/2+\epsilon, 1/2+\epsilon)$ *for* $\epsilon > 0$.

Proof. Let $\epsilon > 0$ and $R_1 = R_2 = R = 1/2 + \epsilon$. Suppose without loss of generality that $nR \in \mathbb{Z}^+$, and that the generator matrix G is a fixed full rank $nR \times n$ matrix and does not have an all zero column. Let d_1^n and d_2^n be two arbitrary fixed binary coset sequences of length n. The messages M_1 and M_2 are assumed to be i.i.d. Unif$(\mathbb{F}_2^{nR})$. The received sequence is then written as

$$Y^n = (M_1\mathsf{G} \oplus d_1^n) + (M_2\mathsf{G} \oplus d_2^n).$$

Define $\tilde{Y}_i = (Y_i) \mod 2$ for every $i \in [n]$, which implies

$$\tilde{Y}^n = (M_1 \oplus M_2)\mathsf{G} \oplus (d_1^n \oplus d_2^n).$$

Define the random set $\mathcal{S}(\tilde{Y}^n) = \{i : \tilde{Y}_i = 0\}$, and let the random variable $N_0 = |\mathcal{S}(\tilde{Y}^n)|$ denote the number of positions where sequence $\tilde{Y}^n$ has 0. We construct a new (random) matrix $G_{\mathcal{S}}$ of size $nR \times N_0$ by including the columns g_i of G for $i \in \mathcal{S}$. Note that the randomness in $G_{\mathcal{S}}$ is only due to the randomness of the messages M_1 and M_2 because the coset code parameters $(\mathsf{G}, d_1^n, d_2^n)$ are arbitrarily fixed. Then, the decoder makes an error if the following event occurs

$$\mathcal{E} = \{N_0 < nR\}.$$

This observation follows from the fact that on $\mathcal{E}$, the dimension of the null space of $G_{\mathcal{S}}^T$ is strictly larger than 0, so $\exists\, (m_1, m_2) \neq (M_1, M_2)$ such that $(m_1 \oplus M_1)G_{\mathcal{S}} = \mathbf{0}$ and $m_1 \oplus m_2 = M_1 \oplus M_2$, which leads to the same received sequence Y^n.

By the union of events bound, we have $P_e^{(n)} \geq \mathsf{P}(\mathcal{E}) = 1 - \mathsf{P}(\mathcal{E}^c)$. To bound the probability $\mathsf{P}(\mathcal{E}^c)$, we define the coset code $\mathcal{C} = \{x^n \in \mathbb{F}_2^n : x^n = m\mathsf{G} \oplus d_1^n \oplus d_2^n,\ m \in \mathbb{F}_2^{nR}\}$. Then, $\tilde{Y}^n$ is uniformly distributed among $\mathcal{C}$, and we have

$$\begin{aligned}
P(\mathcal{E}^c) &\overset{(a)}{\leq} \frac{\mathsf{E}[N_0]}{nR} \\
&= \frac{\sum\limits_{x^n \in \mathcal{C}} \mathsf{P}(\tilde{Y}^n = x^n) wt((x^n)^c)}{nR} \\
&= \frac{\sum\limits_{x^n \in \mathcal{C}} 2^{-nR} wt((x^n)^c)}{nR}, \\
&\overset{(b)}{=} \frac{2^{-nR}(n 2^{nR-1})}{nR}, \\
&= \frac{1}{1+2\epsilon},
\end{aligned}$$

where function $wt : \mathbb{F}_2^n \to \mathbb{Z}^+$ returns the Hamming weight of the input, (a) follows from Markov's inequality and (b) follows from the fact that for a binary coset code $\mathcal{C}$, at a given index, exactly half of the codewords have 0 and exactly half of the codewords have 1 (remember that its generator matrix G has no all-zero column). It follows that $P_e^{(n)} \geq \frac{2\epsilon}{1+2\epsilon}$, which proves the claim. $\square$

5.B Equivalence of Two Rate Regions

Lemma 5.B.1. *Given input pmfs $p(x_1)$ and $p(x_2)$, let the rate region $\mathscr{R}(X_1, X_2)$ consist of the set of rate pairs (R_1, R_2) such that*

$$\min\{R_1 + H(X_2), R_2 + H(X_1)\} < H(X_1) + H(X_2) - \min\{H(X_1|Y), H(X_2|Y)\}.$$

The rate region $\mathscr{R}(X_1, X_2)$ is equivalent to the rate region $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$ described in (5.2) and (5.3).

Proof. It is easy to see that $\mathscr{R}(X_1, X_2) \subseteq \mathscr{R}_{\mathrm{L}}(X_1, X_2)$. To see the other direction, let the rate pair $(R_1, R_2) \in \mathscr{R}_{\mathrm{L}}(X_1, X_2)$ such that $R_1 + H(X_2) \le R_2 + H(X_1)$. By the definition of the rate region $\mathscr{R}_{\mathrm{L}}(X_1, X_2)$, we have

$$R_1 + H(X_2) \le \max\{H(X_2) + I(X_1; Y), H(X_1) + I(X_2; Y)\},$$

which implies that $(R_1, R_2) \in \mathscr{R}(X_1, X_2)$. Similarly, a rate pair $(R_1, R_2) \in \mathscr{R}_{\mathrm{L}}(X_1, X_2)$ such that $R_2 + H(X_1) \le R_1 + H(X_2)$ is in $\mathscr{R}(X_1, X_2)$. Therefore, $\mathscr{R}_{\mathrm{L}}(X_1, X_2) \subseteq \mathscr{R}(X_1, X_2)$, from which the claim follows. □

5.C The Binary Adder MAC

The Achievable Rate Region by Proposition 5.3.1

When specialized to the binary adder MAC, the achievable rate region in Proposition 5.3.1 is reduced to the rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y), \\ R_2 &< I(X_2; Y|X_1) = H(X_2), \end{aligned}$$

or

$$\begin{aligned} R_1 &< I(X_1; Y|X_2) = H(X_1), \\ R_2 &< I(X_2; Y), \end{aligned}$$

for some input pmfs $p(x_1)$ and $p(x_2)$, which is equivalent to the capacity region depicted in Fig. 5.2a. To see this, let $\alpha \in [0, 1/2]$, and consider $X_1 \sim \text{Bern}(\alpha)$ and $X_2 \sim \text{Bern}\left(\frac{1}{2}\right)$. Then, the rate pairs (R_1, R_2) that satisfy

$$\begin{aligned} R_1 &< H(\alpha), \\ R_2 &< 1 - H(\alpha) \end{aligned}$$

are achievable, where $H(\alpha)$ denotes the binary entropy function defined in Section 2.1. Since $H(\alpha)$ is continuous on α, taking the union over $\alpha \in [0, 1/2]$ implies that every point within the capacity region is achievable by the shaping technique. It follows from the converse proof for the capacity region of the binary adder MAC that the achievable rate region in Proposition 5.3.1 (over all input pmfs) is indeed equivalent to the capacity region.

5.D The Binary Erasure MAC

The Achievable Rate Region by Proposition 5.3.1

For the binary erasure MAC, we will evaluate the rate region in Proposition 5.3.1. Let $\alpha, \beta \in [0, 1/2]$, and consider $X_1 \sim \text{Bern}(\alpha)$ and $X_2 \sim \text{Bern}(\beta)$. By Proposition 5.3.1, the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(X_1; Y) = f(\alpha, \beta), \\ R_2 &< I(X_2; Y|X_1) = H(\beta), \end{aligned}$$

or

$$R_1 < I(X_1; Y|X_2) = H(\alpha),$$
$$R_2 < I(X_2; Y) = f(\beta, \alpha),$$

is achievable, where the function $f : [0, 1/2] \times [0, 1/2] \to \mathbb{R}$ is defined as

$$f(x, y) = H(x) - y(1-x)\log\left(1 + \frac{x}{1-x}\frac{1-y}{y}\right) - x(1-y)\log\left(1 + \frac{1-x}{x}\frac{y}{1-y}\right). \tag{5.17}$$

Since $f(x, y)$ is increasing on x for any $y \in [0, 1/2]$, the union of such regions over $\alpha, \beta \in [0, 1/2]$ is the set of rate pairs (R_1, R_2) satisfying

$$R_1 < 1 - \frac{H(\alpha)}{2},$$
$$R_2 < H(\alpha),$$

or

$$R_1 < H(\alpha),$$
$$R_2 < 1 - \frac{H(\alpha)}{2},$$

for some $\alpha \in [0, 1/2]$. By the fact that $H(\alpha) \in [0, 1]$ is continuous on α, this union is equivalent to the union of two trapezoids defined by

$$R_2 < 1,$$
$$2R_1 + R_2 < 2,$$

and

$$R_1 < 1,$$

$$R_1 + 2R_2 < 2,$$

which proves the claim.

The Achievable Rate Region by Corollary 5.3.1

For the binary erasure MAC, we will evaluate the rate region in Corollary 5.3.1. Let $\alpha, \beta \in [0, 1/2]$, and consider $X_1 \sim \text{Bern}(\alpha)$ and $X_2 \sim \text{Bern}(\beta)$. By Corollary 5.3.1, the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \min\{I(X_1;Y|X_2), \max[I(X_1;Y), I(X_2;Y)]\} \\ &= \min\{H(\alpha), \max[f(\alpha,\beta), f(\beta,\alpha)]\}, \\ R_2 &< I(X_2;Y|X_1) = H(\beta), \\ R_1 + R_2 &< I(X_1, X_2; Y) \\ &= H(\alpha) + f(\beta,\alpha) = H(\beta) + f(\alpha,\beta), \end{aligned} \tag{5.18}$$

or

$$\begin{aligned} R_1 &< I(X_1;Y|X_2) = H(\alpha), \\ R_2 &< \min\{I(X_2;Y|X_1), \max[I(X_1;Y), I(X_2;Y)]\} \\ &= \min\{H(\beta), \max[f(\alpha,\beta), f(\beta,\alpha)]\}, \\ R_1 + R_2 &< I(X_1, X_2; Y) \\ &= H(\alpha) + f(\beta,\alpha) = H(\beta) + f(\alpha,\beta), \end{aligned} \tag{5.19}$$

is achievable, where the function f is as defined in (5.17). First, consider the union of such regions over $\alpha, \beta \in [0, 1/2]$ such that $\alpha \geq \beta$ (or equivalently $f(\alpha,\beta) \geq f(\beta,\alpha)$), which results in the rate region defined by

$$\begin{aligned} R_1 &< f(\alpha,\beta), \\ R_2 &< H(\beta), \end{aligned}$$

or

$$\begin{aligned} R_1 &< H(\alpha), \\ R_2 &< \min\{H(\beta), f(\alpha,\beta)\}, \\ R_1 + R_2 &< H(\beta) + f(\alpha,\beta), \end{aligned}$$

for some $\alpha, \beta \in [0, 1/2]$ such that $\alpha \geq \beta$. Since $f(x, y)$ is increasing over x for any $y \in [0, 1/2]$, the resulting region consists of the rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_1 &< f(1/2, \beta) = 1 - \frac{H(\beta)}{2}, \\ R_2 &< H(\beta), \end{aligned} \tag{5.20}$$

or

$$\begin{aligned} R_1 &< 1, \\ R_2 &< \min\{H(\beta), 1 - \frac{H(\beta)}{2}\}, \\ R_1 + R_2 &< 1 + \frac{H(\beta)}{2}, \end{aligned} \tag{5.21}$$

for some $\beta \in [0, 1/2]$. The union of the rate region defined in (5.20) over $\beta \in [0, 1/2]$ is equivalent to the trapezoid defined by $R_2 < 1$, and $2R_1 + R_2 < 2$. The union of the rate region defined in (5.21) over $\beta \in [0, 1/2]$ is clearly included in the trapezoid defined by $R_1 < 1$, $R_1 + 2R_2 < 2$.

By similar arguments, the union of the rate region defined in (5.18) and (5.19) over $\alpha, \beta \in [0, 1/2]$ such that $\beta \geq \alpha$, is reduced to the rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< \min\{H(\alpha), 1 - \frac{H(\alpha)}{2}\}, \\ R_2 &< 1, \\ R_1 + R_2 &< 1 + \frac{H(\alpha)}{2}, \end{aligned}$$

or

$$
\begin{aligned}
R_1 &< H(\alpha), \\
R_2 &< 1 - \frac{H(\alpha)}{2},
\end{aligned}
$$

for some $\alpha \in [0, 1/2]$. By symmetry, the overall achievable rate region in Corollary 5.3.1 is equivalent to the union of two trapezoids defined by $R_2 < 1$, $2R_1 + R_2 < 2$ and $R_1 < 1$, $R_1 + 2R_2 < 2$.

5.E The On–off Erasure MAC

The Achievable Rate Region by Proposition 5.3.1

For the on–off erasure MAC, we will evaluate the achievable rate region in Proposition 5.3.1. If the channel parameter $p \le 2/3$, it is easy to see that i.i.d. Bern(1/2) inputs X_1 and X_2 can achieve the capacity region in Fig. 5.6a. Suppose that $p > 2/3$. Let $\alpha, \beta \in [0, 1/2]$, and consider $X_1 \sim \text{Bern}(\alpha)$ and $X_2 \sim \text{Bern}(\beta)$. Then, by Proposition 5.3.1, the set of rate pairs (R_1, R_2) such that

$$
\begin{aligned}
R_1 &< I(X_1; Y) = (1-p)H(\alpha) + pf(\alpha, \beta), \\
R_2 &< I(X_2; Y|X_1) = pH(\beta),
\end{aligned}
\tag{5.22}
$$

or

$$
\begin{aligned}
R_1 &< I(X_1; Y|X_2) = H(\alpha), \\
R_2 &< \min\{I(X_2; Y|X_1), H(X_2) - H(X_1) + I(X_1; Y)\} \\
&= \min\{pH(\beta), (1-p)H(\beta) + pf(\beta, \alpha)\}, \\
R_1 + R_2 &< H(\alpha) + pf(\beta, \alpha),
\end{aligned}
\tag{5.23}
$$

is achievable, where function f is as defined in (5.17). First, consider the union of the rate region defined in (5.22) over $\alpha, \beta \in [0, 1/2]$. Since $f(x, y)$ is increasing on x for every

$y \in [0, 1/2]$, the union is equivalent to the set of rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_1 &< 1 - p + p\left(1 - \frac{H(\beta)}{2}\right) = 1 - \frac{pH(\beta)}{2}, \\ R_2 &< pH(\beta), \end{aligned}$$

for some $b \in [0, 1/2]$, that reduces to the trapezoid defined by $R_2 < p$ and $2R_1 + R_2 < 2$.

Second, we consider the union of the rate region defined in (5.23) over $\alpha, \beta \in [0, 1/2]$. By similar arguments, the union is equivalent to the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< H(\alpha), \\ R_2 &< \min\{p, 1 - \frac{pH(\alpha)}{2}\}, \\ R_1 + R_2 &< p + H(\alpha)\left(1 - \frac{p}{2}\right), \end{aligned}$$

for some $\alpha \in [0, 1/2]$, that is equivalent to the hexagon defined by $R_1 < 1$, $R_2 < p$, $R_1 + R_2 < 1 + p/2$, and $(p/2)R_1 + R_2 < 1 - (p/2) + (p^2)/2$.

The Achievable Rate Region by Corollary 5.3.1

For the on–off erasure MAC, we will evaluate the achievable rate region in Corollary 5.3.1. Again, if the channel parameter $p \leq 2/3$, it is easy to see that i.i.d. Bern(1/2) inputs X_1 and X_2 can achieve the capacity region in Fig. 5.6a. Suppose that $p > 2/3$. Let $\alpha, \beta \in [0, 1/2]$, and consider $X_1 \sim \text{Bern}(\alpha)$ and $X_2 \sim \text{Bern}(\beta)$. Then, by Corollary 5.3.1, the set of rate pairs (R_1, R_2) such that

$$R_1 < I(X_1; Y|X_2) = H(\alpha), \tag{5.24a}$$

$$\begin{aligned} R_1 &< \max\{I(X_1; Y), I(X_2; Y)\} \\ &= \max\{pf(\alpha, \beta) + (1-p)H(\alpha), pf(\beta, \alpha)\}, \end{aligned} \tag{5.24b}$$

$$R_2 < I(X_2; Y|X_1) = pH(\beta), \tag{5.24c}$$

$$R_1 + R_2 < I(X_1, X_2; Y) = H(\alpha) + pf(\beta, \alpha), \tag{5.24d}$$

or

$$\begin{aligned} R_1 &< I(X_1; Y|X_2) = H(\alpha), \\ R_2 &< I(X_2; Y|X_1) = pH(\beta), \\ R_2 &< \max\{I(X_1; Y), I(X_2; Y)\} \\ &= \max\{pf(\alpha, \beta) + (1-p)H(\alpha), pf(\beta, \alpha)\}, \\ R_1 + R_2 &< I(X_1, X_2; Y) = H(\alpha) + pf(\beta, \alpha), \end{aligned} \tag{5.25}$$

is achievable, where the function f is as defined in (5.17). First, consider the union of the rate region defined in (5.24) over $\alpha, \beta \in [0, 1/2]$ such that $H(\alpha) > pH(\beta)$ (or equivalently $pf(\alpha, \beta) + (1-p)H(\alpha) > pf(\beta, \alpha)$). Then, the inequalities in (5.24a) and (5.24d) are inactive. Since $f(x, y)$ is increasing on x for every $y \in [0, 1/2]$, the union is equivalent to the set of rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_1 &< p\left(1 - \frac{H(\beta)}{2}\right) + (1-p) = 1 - \frac{pH(\beta)}{2}, \\ R_2 &< pH(\beta), \end{aligned}$$

for some $\beta \in [0, 1/2]$, that reduces to the trapezoid defined by $R_2 < p$ and $2R_1 + R_2 < 2$. It is easy to see that the union of the rate region defined in (5.24) over $\alpha, \beta \in [0, 1/2]$ such that $H(\alpha) \le pH(\beta)$ is included in this trapezoid.

Second, we consider the union of the rate region defined in (5.25) over $\alpha, \beta \in [0, 1/2]$ such that $H(\alpha) > pH(\beta)$. By similar arguments, the union is equivalent to the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< 1, \\ R_2 &< \min\{pH(\beta), 1 - \frac{pH(\beta)}{2}\}, \end{aligned}$$

$$R_1 + R_2 < 1 + \frac{p}{2} H(\beta),$$

for some $\beta \in [0, 1/2]$, that is equivalent to the hexagon defined by $R_1 < 1$, $R_2 < 2/3$, $R_1 + R_2 < 1 + p/2$, and $R_1 + 2R_2 < 2$. Finally, it is easy to see that the union of the rate region defined in (5.25) over $\alpha, \beta \in [0, 1/2]$ such that $H(\alpha) \le pH(\beta)$ is equivalent to the trapezoid defined by $R_1 < p$ and $(p/2)R_1 + R_2 < p$.

5.F Proof of Proposition 5.3.2

We use a pair of $(n, nR_1, \mathbb{F}_q)$ and $(n, nR_2, \mathbb{F}_q)$ random coset code ensembles constructed for the virtual channel $p(y|v_1, v_2)$ as follows. A generator matrix $G \in \mathbb{F}_q^{n\max\{R_1,R_2\}\times n}$ and coset sequences D_1^n and D_2^n are randomly generated by drawing each entry i.i.d. $\mathrm{Unif}(\mathbb{F}_q)$. Given the realizations of G, d_1^n and d_2^n, for every message $m_j \in \mathbb{F}_q^{nR_j}$, encoder $j = 1, 2$ then assigns

$$v_j^n(m_j) = [m_j \; \mathbf{0}_{n(\max\{R_1,R_2\}-R_j)}]\mathsf{G} + d_j^n.$$

Upon receiving y^n, the decoder first fixes an $\epsilon > 0$ and then searches a unique pair of $(\hat{m}_1, \hat{m}_2)$ such that $(v_1^n(\hat{m}_1), v_2^n(\hat{m}_2), y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y)$, where V_1 and V_2 are i.i.d. $\mathrm{Unif}(\mathbb{F}_q)$. If the decoder finds the unique pair, then it declares that $(\hat{m}_1, \hat{m}_2)$ was transmitted. Otherwise, it declares error. Assume that (M_1, M_2) is the transmitted message pair. We bound the probability of error $\mathsf{E}[P_e^{(n)}]$ averaged over (M_1, M_2) and (G, D_1^n, D_2^n). The code construction is symmetric with respect to the transmitted message pair. Therefore, $\mathsf{E}[P_e^{(n)}] = \mathsf{E}[P_e^{(n)} | (M_1, M_2) = (\mathbf{0}, \mathbf{0})]$ and without loss of generality, we can assume that $(M_1, M_2) = (\mathbf{0}, \mathbf{0})$. The decoder makes an error only if one or more of the following events occur:

$$\mathcal{E}_1 = \{(V_1^n(\mathbf{0}), V_2^n(\mathbf{0}), Y^n) \notin \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y)\},$$

$$\mathcal{E}_2 = \{(V_1^n(\mathbf{0}), V_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y) \text{ for some } m_2 \neq \mathbf{0}\},$$

$$\begin{aligned}
\mathcal{E}_3 &= \{(V_1^n(m_1), V_2^n(\mathbf{0}), Y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y) \text{ for some } m_1 \neq \mathbf{0}\},\\
\mathcal{E}_4 &= \{(V_1^n(m_1), V_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y) \text{ for some } m_1 \neq \mathbf{0}, m_2 \neq \mathbf{0} \text{ such that}\\
&\qquad [m_1\ \mathbf{0}] \text{ and } [m_2\ \mathbf{0}] \text{ are linearly independent}\},\\
\mathcal{E}_5 &= \{(V_1^n(m_1), V_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y) \text{ for some } m_1 \neq \mathbf{0}, m_2 \neq \mathbf{0} \text{ such that}\\
&\qquad [m_1\ \mathbf{0}] \text{ and } [m_2\ \mathbf{0}] \text{ are linearly dependent}\}.
\end{aligned}$$

Thus, by the union of events bound, $\mathsf{E}[P_e^{(n)}] \leq \sum_{k=1}^5 \mathsf{P}(\mathcal{E}_k)$. Since $V_1^n(\mathbf{0}) = D_1^n$ and $V_2^n(\mathbf{0}) = D_2^n$ are i.i.d. Unif$(\mathbb{F}_q^n)$ and independent from each other, by the law of large numbers, $\mathsf{P}(\mathcal{E}_1 \big| (M_1, M_2) = (\mathbf{0}, \mathbf{0}))$ tends to zero as $n \to \infty$. For the second term, note that for $m_2 \neq \mathbf{0}$, $V_2^n(m_2) \sim \prod_{i=1}^n p_{V_2}(v_{2i})$ is independent of $(V_1^n(\mathbf{0}), Y^n) \sim \prod_{i=1}^n p_{V_1,Y}(v_{1i}, y_i)$. Hence, by the packing lemma in [6, Section 3.2], $\mathsf{P}(\mathcal{E}_2)$ tends to zero as $n \to \infty$ if $R_2 \leq I(V_2; V_1, Y) - \delta(\epsilon)$. Changing the role of sender 1 and 2, $\mathsf{P}(\mathcal{E}_3)$ tends to zero as $n \to \infty$ if $R_1 \leq I(V_1; V_2, Y) - \delta(\epsilon)$. For the forth term, note that if $m_1 \neq \mathbf{0}$ and $m_2 \neq \mathbf{0}$ are linearly independent, then by [5, Lemma 14], $(V_1^n(m_1), V_2^n(m_2)) \sim \prod_{i=1}^n p_{V_1}(v_{1i}) p_{V_2}(v_{2i})$; i.e., linear independence implies statistical independence. Moreover, in this case, the pair $(V_1^n(m_1), V_2^n(m_2))$ is independent from the tuple $(V_1^n(\mathbf{0}), V_2^n(\mathbf{0}), Y^n)$. Hence, again by the packing lemma $\mathsf{P}(\mathcal{E}_4)$ tends to zero as $n \to \infty$ if $R_1 + R_2 \leq I(V_1, V_2; Y) - \delta(\epsilon)$.

Due to linear dependency among $V_1^n(m_1)$ and $V_2^n(m_2)$, to bound the last term, we will use a similar technique in Lemma 5.3.1. Define the rate $R = \min\{R_1, R_2\}$ and the set

$$\mathcal{D} = \{(m_1, m_2) \in \mathbb{F}_q^{nR_1} \times \mathbb{F}_q^{nR_2} : [m_1\ \mathbf{0}] \neq \mathbf{0} \text{ and } [m_2\ \mathbf{0}] \neq \mathbf{0} \text{ are linearly dependent}\}.$$

Then,

$$\begin{aligned}
\mathsf{P}(\mathcal{E}_5) &= \mathsf{P}((V_1^n(m_1), V_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y) \text{ for some } (m_1, m_2) \in \mathcal{D})\\
&\overset{(a)}{\leq} \sum_{(m_1, m_2) \in \mathcal{D}} \mathsf{P}((V_1^n(m_1), V_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)}(V_1, V_2, Y))
\end{aligned}$$

$$
\begin{aligned}
&\leq \sum_{(m_1,m_2)\in\mathcal{D}} \mathsf{P}((V_2^n(m_2),Y^n)\in\mathcal{T}_\epsilon^{(n)}(V_2,Y)) \\
&= \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{(v_2^n,y^n)\in\mathcal{T}_\epsilon^{(n)}(V_2,Y)} \mathsf{P}(V_2^n(m_2)=v_2^n, Y^n=y^n) \\
&= \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{\substack{(v_2^n,y^n)\in \\ \mathcal{T}_\epsilon^{(n)}(V_2,Y)}} \sum_{\substack{\tilde{v}_1^n\in\mathbb{F}_q^n, \\ \tilde{v}_2^n\in\mathbb{F}_q^n}} \mathsf{P}(V_2^n(m_2)=v_2^n, Y^n=y^n, V_1^n(\mathbf{0})=\tilde{v}_1^n, V_2^n(\mathbf{0})=\tilde{v}_2^n) \\
&= \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{\substack{(v_2^n,y^n)\in \\ \mathcal{T}_\epsilon^{(n)}(V_2,Y)}} \sum_{\substack{\tilde{v}_1^n\in\mathbb{F}_q^n, \\ \tilde{v}_2^n\in\mathbb{F}_q^n}} \mathsf{P}([m_2\ \mathbf{0}]G+D_2^n=v_2^n, D_1^n=\tilde{v}_1^n, D_2^n=\tilde{v}_2^n, Y^n=y^n) \\
&\overset{(b)}{=} \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{\substack{(v_2^n,y^n)\in \\ \mathcal{T}_\epsilon^{(n)}(V_2,Y)}} \sum_{\substack{\tilde{v}_1^n\in\mathbb{F}_q^n, \\ \tilde{v}_2^n\in\mathbb{F}_q^n}} \mathsf{P}\begin{pmatrix} [m_2\ \mathbf{0}]G+D_2^n=v_2^n, \\ D_1^n=\tilde{u}_1^n, D_2^n=\tilde{v}_2^n \end{pmatrix} p(y^n|\tilde{v}_1^n,\tilde{v}_2^n) \\
&\overset{(c)}{=} \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{(v_2^n,y^n)\in\mathcal{T}_\epsilon^{(n)}(V_2,Y)} \sum_{\substack{\tilde{v}_1^n\in\mathbb{F}_q^n, \\ \tilde{v}_2^n\in\mathbb{F}_q^n}} q^{-3n} p(y^n|\tilde{v}_1^n,\tilde{v}_2^n) \\
&= \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{(v_2^n,y^n)\in\mathcal{T}_\epsilon^{(n)}(V_2,Y)} q^{-n} p(y^n|\tilde{v}_1^n,\tilde{v}_2^n) \\
&= \sum_{(m_1,m_2)\in\mathcal{D}} \sum_{y^n\in\mathcal{T}_\epsilon^{(n)}(Y)} p(y^n|\tilde{v}_1^n,\tilde{v}_2^n) \sum_{v_2^n\in\mathcal{T}_\epsilon^{(n)}(V_2|y^n)} q^{-n} \\
&\leq |\mathcal{D}|\, q^{n(H(V_2|Y)+\delta(\epsilon))} q^{-n} \\
&\overset{(d)}{\leq} q^{n(R-I(V_2;Y)+\delta(\epsilon))},
\end{aligned}
$$

where (a) follows by the union of events bound, (b) follows since under the assumption that $(M_1,M_2)=(\mathbf{0},\mathbf{0})$, the the triple $G\to(D_1^n,D_2^n)\to Y^n$ form a Markov chain, (c) follows since $m_2\neq\mathbf{0}$ and the entries of G, D_1^n and D_2^n are chosen i.i.d., and (d) follows since $H(V_2)=1$ and $|\mathcal{D}|\leq qq^{nR}$. By changing the order of V_1^n and V_2^n, we can conclude that

$$\mathsf{P}(\mathcal{E}_5)\leq q^{n(R-\max\{I(V_1;Y),I(V_2;Y)\}+\delta(\epsilon))},$$

which tends to zero as $n\to\infty$ if $R=\min\{R_1,R_2\}<\max\{I(V_1;Y),I(V_2;Y)\}-\delta(\epsilon)$.

Letting $\epsilon \to 0$ yield that the rate pairs (R_1, R_2) is achievable if

$$\begin{aligned} R_1 &< I(V_1; Y | X_2), \\ R_2 &< I(V_2; Y | X_1), \\ R_1 + R_2 &< I(V_1, V_2; Y), \\ \min\{R_1, R_2\} &< \max\{I(V_1; Y), I(V_2; Y)\}, \end{aligned}$$

as claimed.

5.G A Variation of Steinitz Lemma

Lemma 5.G.1. *Suppose that $Z = \{z_1, z_2, \ldots, z_r\}$ is a set of linearly independent vectors in a vector space V of dimension $k > r$, and $W = \{w_1, w_2, \ldots, w_k\}$ span V. Let $T \subseteq W$ be a set such that*

i) $|T| = k - r$, and

ii) $Z \cup T$ span V.

(The existence of such T is guaranteed by the Steinitz Lemma in [10]). Then, for a given set $J \subseteq W$ with $|J| = r$, $T = W \setminus J$ is the unique subset of W satisfying i) and ii) if and only if $\mathrm{span}(Z) = \mathrm{span}(J)$.

Proof. Let $J \subseteq W$ with $|J| = r$. First suppose that $\mathrm{span}(Z) = \mathrm{span}(J)$. Then, it is easy to see that $T = W \setminus J$ is the only subset of W that satisfies i) and ii). Now, suppose that $T = W \setminus J$ is the unique subset of W that satisfies i) and ii). We will show that

$$\mathrm{span}(Z) = \mathrm{span}(J).$$

Both Z and J consist of r linearly independent vectors, so it suffices to show that for every $w \in J$, $w \in \text{span}(Z)$. Let $w \in J$. Since $Z \cup T$ span V, we have

$$w = \sum_{l=1}^{r} a_l z_l + \sum_{w_i \in T} b_i w_i. \tag{5.26}$$

We want to show that $b_i = 0$ for all $w_i \in T$ in (5.26). Assume to the contrary that $b_m \neq 0$ for some $w_m \in T$. Then we can write w_m as a linear combination of the vectors in $Z \cup T \setminus \{w_m\} \cup \{w\}$. Note that $w \neq w_m$ since J and T are disjoint. Thus, $T' := T \setminus \{w_m\} \cup \{w\}$ also satisfies i) and ii), which contradicts with the uniqueness of T. The claim follows since $w \in J$ is arbitrary. □

Acknowledgment

This chapter is, in part, a reprint of the material in the papers: Pinar Sen and Young-Han Kim, "Homologous Codes for Multiple Access Channels," in *IEEE Transactions on Information Theory,* vol. 66, no. 3, pp. 1549-1571, March 2020; and Pinar Sen and Young-Han Kim, "Homologous Codes for Multiple Access Channels," *Proceedings of the IEEE International Symposium on Information Theory*, Aachen, Germany, June 2017. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] Rudolf Ahlswede. Multiway communication channels. In *Proc. 2nd Int. Symp. Inf. Theory*, pages 23–52, Tsahkadsor, Armenian SSR, 1971.

[2] Henry H. J. Liao. *Multiple access channels.* Ph.D. thesis, University of Hawaii, Honolulu, HI, September 1972.

[3] A. Padakandla and S. S. Pradhan. An achievable rate region based on coset codes for multiple access channel with states. *IEEE Trans. Inf. Theory*, 63(10):6393–6415, Oct 2017.

[4] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. A joint typicality approach to compute–forward. *IEEE Trans. Inf. Theory*, 64(12):7657–7685, Dec 2018.

[5] S. H. Lim, C. Feng, A. Pastore, B. Nazer, and M. Gastpar. Towards an algebraic network information theory: Simultaneous joint typicality decoding. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 1818–1822, June 2017.

[6] Abbas El Gamal and Young-Han Kim. *Network Information Theory.* Cambridge University Press, Cambridge, 2011.

[7] R. G. Gallager. *Information Theory and Reliable Communication.* Wiley, New York, 1968.

[8] P. Sen, S. H. Lim, and Y.-H. Kim. Optimal achievable rates for computation with random homologous codes. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 2351–2355, June 2018.

[9] P. Sen, S. H. Lim, and Y.-H. Kim. Optimal achievable rates for computation with random homologous codes. submitted to *IEEE Trans. Inf. Theory*, 2018.

[10] Y. Katznelson and Y.R. Katznelson. *A (terse) Introduction to Linear Algebra.* Student mathematical library. American Mathematical Soc., 2008.

Chapter 6

Successive Gray–Wyner Network

A distributed source coding problem is introduced in which two encoders having access to nested sets of discrete memoryless sources describe them to four decoders via common and private channels. A single-letter characterization for the optimal rate region of this problem is established. Lower boundaries on the optimal rate region are investigated and a sufficient condition on the source distribution is provided to attain these lower bounds. A relation to conditional Wyner's common information is presented: it arises as an answer to the minimum rate of common link such that more informed encoder efficiently describes the sources when the strategy of less informed encoder is fixed.

6.1 Introduction

Gray–Wyner network in Fig. 6.1 was first proposed as a distributed source coding problem in [1], in which a pair of sequences (X_1^n, X_2^n) drawn i.i.d. from $p(x_1, x_2)$ is described by an encoder to two decoders via a common channel of rate R_0 and two private channels of rates R_1 and R_2, respectively, so that decoder d, $d = 1, 2$, having the descriptions $M_0 \in [2^{nR_0}]$ and $M_d \in [2^{nR_d}]$, can losslessly recover X_d^n. A single letter characterization for the achievable rate tuples was provided in [1] as the set of rate tuples

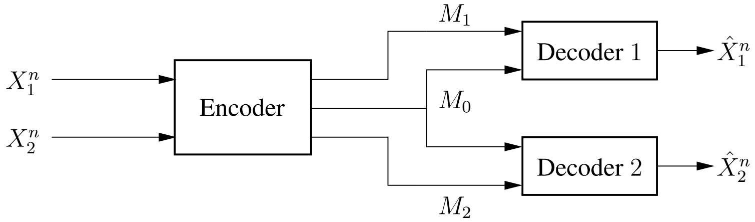


Figure 6.1. Gray–Wyner network.

(R_0, R_1, R_2) such that

$$R_0 \geq I(X_1, X_2; W), \tag{6.1a}$$

$$R_1 \geq H(X_1|W), \tag{6.1b}$$

$$R_2 \geq H(X_2|W) \tag{6.1c}$$

for some conditional pmf $p(w|x_1, x_2)$ with $|\mathcal{W}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 2$.

This problem later inspired the formulation of a common information measure between two random variables X_1 and X_2, referred to as Wyner's common information in [2], that appears as an answer to the minimum rate of the common channel for efficient encoding of source pair (X_1^n, X_2^n) in the Gray–Wyner network and is characterized as

$$C(X_1; X_2) := \min_{\substack{p(w|x_1,x_2) \\ I(X_1;X_2|W)=0}} I(X_1, X_2; W). \tag{6.2}$$

More recently, Gray–Wyner network was found to be related to a single-user caching problem [3], in which a server storing some file contents aims to reduce peak network traffic by sending partial data to users during the off-peak hours before the actual requests are known. After user requests a file, server delivers more data to user so that it can decode its requested file by combining this new information with the previously stored data in its cache. In this setting, cache placement corresponds to the private channel of Gray–Wyner network and delivery after the requests are revealed corresponds to private channels.

Similar to [3], with the goal of creating a close connection to dynamic caching problems formulated in the subsequent chapters, in this chapter, we describe a successive version of Gray–Wyner network (or the *successive Gray–Wyner network* in short, cf. Fig. 6.2) and establish a single-letter characterization for the optimal rate region of this network.

6.2 Successive Gray–Wyner Network

Consider the *successive* Gray–Wyner network in Fig. 6.2, in which a tuple of sequences $(X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n)$ drawn i.i.d. from $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ is described by two encoders so that decoder $(d, 1)$, $d = 1, 2$, having the descriptions L_1 and M_{d1}, can losslessly recover X_{d1}^n and decoder $(d', 2)$, $d' = 1, 2$, having the descriptions L_1, L_2, and $M_{d'2}$, can losslessly recover $X_{d'2}^n$.

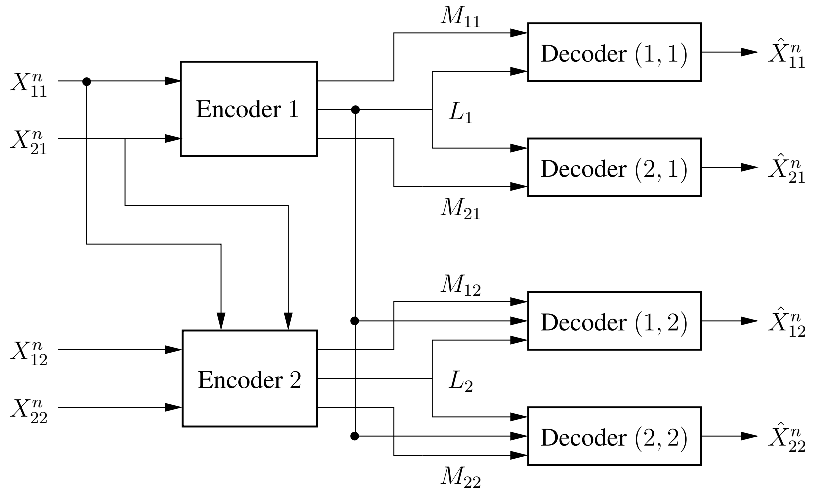


Figure 6.2. Successive Gray–Wyner network.

An $(nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}, n)$ code for the successive Gray–Wyner network consists of

- two encoders, where encoder 1 assigns an index tuple $(l_1, m_{11}, m_{21})(x_{11}^n, x_{21}^n) \in [2^{nC_1}] \times [2^{nR_{11}}] \times [2^{nR_{21}}]$ to each pair of sequences $(x_{11}^n, x_{21}^n) \in \mathcal{X}_{11}^n \times \mathcal{X}_{21}^n$ while encoder 2 assigns an index tuple $(l_2, m_{12}, m_{22})(x_{11}^n, x_{21}^n, x_{12}^n, x_{22}^n) \in [2^{nC_2}] \times [2^{nR_{12}}] \times [2^{nR_{22}}]$ to each tuple of sequences $(x_{11}^n, x_{21}^n, x_{12}^n, x_{22}^n) \in \mathcal{X}_{11}^n \times \mathcal{X}_{21}^n \times \mathcal{X}_{12}^n \times \mathcal{X}_{22}^n$,

- four decoders, where decoder $(d,1)$, $d=1,2$, assigns an estimate $\hat{x}_{d1}^n(l_1,m_{d1})$ to each index pair $(l_1,m_{d1})\in[2^{nC_1}]\times[2^{nR_{d1}}]$ and decoder $(d',2)$, $d'=1,2$, assigns an estimate $\hat{x}_{d'2}^n(l_1,l_2,m_{d'2})$ to each index tuple $(l_1,l_2,m_{d'2})\in[2^{nC_1}]\times[2^{nC_2}]\times[2^{nR_{d'2}}]$.

The probability of error is defined as

$$P_e^{(n)}=\mathsf{P}\{(\hat{X}_{11}^n,\hat{X}_{21}^n,\hat{X}_{12}^n,\hat{X}_{22}^n)\neq(X_{11}^n,X_{21}^n,X_{12}^n,X_{22}^n)\}.$$

A rate tuple $(C_1,R_{11},R_{21},C_2,R_{12},R_{22})$ is said to be achievable if there exists a sequence of $(nC_1,nR_{11},nR_{21},nC_2,nR_{12},nR_{22},n)$ codes such that $\lim_{n\to\infty}P_e^{(n)}=0$.

6.3 Optimal Rate Region for Successive Gray–Wyner Network

Define the optimal rate region $\mathscr{R}$ as the set of achievable rate tuples $(C_1,R_{11},R_{21},C_2,R_{12},R_{22})$ for the successive Gray–Wyner network. The following theorem presents a single-letter characterization of the optimal rate region $\mathscr{R}$, the proof of which is given in Appendix 6.A.

Theorem 6.3.1. *The optimal rate region $\mathscr{R}$ consists of the rate tuples such that*

$$C_1\geq I(X_1^{(1)},X_2^{(1)};W_1), \tag{6.3a}$$

$$R_{d1}\geq H(X_d^{(1)}|W_1),\quad d=1,2, \tag{6.3b}$$

$$C_2\geq I(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)};W_2|W_1), \tag{6.3c}$$

$$R_{d'2}\geq H(X_{d'}^{(2)}|W_1,W_2),\quad d'=1,2, \tag{6.3d}$$

for some conditional pmfs $p(w_1|x_1^{(1)},x_2^{(1)})$ and $p(w_2|w_1,x_1^{(1)},x_2^{(1)},x_1^{(2)},x_2^{(2)})$ with $|\mathcal{W}_1|\leq|\mathcal{X}_{11}||\mathcal{X}_{21}|+2$ and $|\mathcal{W}_2|\leq|\mathcal{X}_{11}||\mathcal{X}_{21}||\mathcal{X}_{12}||\mathcal{X}_{22}|+2$.

Remark 6.3.1. *The optimal rate region $\mathscr{R}$ in Theorem 6.3.1 is convex.*

Remark 6.3.2. *The projection of the optimal rate region $\mathscr{R}$ onto the first three coordinates (C_1, R_{11}, R_{21}) is equivalent to the optimal rate region for the classical Gray–Wyner network [1] in (6.1).*

Remark 6.3.3. *Instead of a pair of two files in Fig. 6.2, consider a pair of N files $(X_{j1}^n : j \in [N])$ and $(X_{j2}^n : j \in [N])$, which are described by two encoders to $2N$ decoders. Encoder 1 maps the tuple $(X_{j1}^n : j \in [N])$ to the descriptions L_1 and $(M_{d1} : d \in [N])$, whereas encoder 2 maps all the files to the descriptions L_2 and $(M_{d2} : d \in [N])$. Decoder (d, i), $d \in [N]$ and $i \in \{1, 2\}$, having access to $(L_k)_{k=1}^i$ and M_{di}, then wishes to recover X_{di}^n. Defining a code, achievability, and the optimal rate region in a similar way, we can characterize the optimal rate region $\mathscr{R}$ as the set of rate tuples such that*

$$\begin{aligned}
C_1 &\geq I(X_1^{(1)}, X_2^{(1)}, \ldots, X_N^{(1)}; W_1), \\
R_{d,1} &\geq H(X_d^{(1)} | W_1), \quad d \in [N], \\
C_2 &\geq I(X_1^{(1)}, X_2^{(1)}, \ldots, X_N^{(1)}, X_1^{(2)}, X_2^{(2)}, \ldots, X_N^{(2)}; W_2 | W_1), \\
R_{d',2} &\geq H(X_{d'}^{(2)} | W_1, W_2), \quad d' \in [N],
\end{aligned}$$

for some pmfs $p(w_1 | x_1^{(1)}, x_2^{(1)}, \ldots, x_N^{(1)})$ and $p(w_2 | w_1, x_1^{(1)}, x_2^{(1)}, \ldots, x_N^{(1)}, x_1^{(2)}, x_2^{(2)}, \ldots, x_N^{(2)})$ with $|\mathcal{W}_1| \leq \prod_{j=1}^N |\mathcal{X}_{j1}| + 2$ and $|\mathcal{W}_2| \leq \prod_{j=1}^N |\mathcal{X}_{j1}||\mathcal{X}_{j2}| + 2$.

6.4 Lower Boundaries of the Optimal Rate Region

To better understand the boundaries of the optimal rate region $\mathscr{R}$, we now provide some lower bounds.

Corollary 6.4.1. *If $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22}) \in \mathscr{R}$, then*

$$C_1 + R_{11} + R_{21} \geq H(X_1^{(1)}, X_2^{(1)}), \tag{6.4}$$

$$C_1 + C_2 + R_{12} + R_{22} \geq H(X_1^{(2)}, X_2^{(2)}). \tag{6.5}$$

To see this, fix two pmfs $p(w_1|x_1^{(1)}, x_2^{(1)})$ *and* $p(w_2|w_1, x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ *(or equivalently, fix a pmf* $p(w_1, w_2|x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ *such that* $(X_1^{(2)}, X_2^{(2)}) \to (X_1^{(1)}, X_2^{(1)}) \to W_1$ *form a Markov chain). Then,*

$$\begin{aligned} C_1 + R_{11} + R_{21} &\geq I(X_1^{(1)}, X_2^{(1)}; W_1) + H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) \\ &= H(X_1^{(1)}, X_2^{(1)}) + I(X_1^{(1)}; X_2^{(1)}|W_1) \overset{(a)}{\geq} H(X_1^{(1)}, X_2^{(1)}), \end{aligned}$$

where (a) *holds with equality if and only if* $X_1^{(1)} \to W_1 \to X_2^{(1)}$ *form a Markov chain. For example, if we let* $p(w_1|x_1^{(1)}, x_2^{(1)})$ *attain Wyner's common information* $C(X_1^{(1)}; X_2^{(1)})$ *defined in (6.2), then (6.4) holds with equality. Similarly for (6.5), we have*

$$\begin{aligned} C_1 + C_2 + R_{12} + R_{22} &\geq I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}; W_2|W_1) \\ &\qquad + H(X_1^{(2)}|W_1, W_2) + H(X_2^{(2)}|W_1, W_2) \\ &= H(X_1^{(2)}, X_2^{(2)}) + I(X_1^{(2)}; X_2^{(2)}|W_1, W_2) \\ &\qquad + I(X_1^{(1)}, X_2^{(1)}; W_1, W_2|X_1^{(2)}, X_2^{(2)}) \\ &\overset{(b)}{\geq} H(X_1^{(2)}, X_2^{(2)}), \end{aligned}$$

where (b) *holds with equality if and only if* $X_1^{(2)} \to (W_1, W_2) \to X_2^{(2)}$ *and*

$$(X_1^{(1)}, X_2^{(1)}) \to (X_1^{(2)}, X_2^{(2)}) \to (W_1, W_2)$$

form Markov chains. For example, if we let $W_1 = \emptyset$ *and let* $p(w_2|x_1^{(2)}, x_2^{(2)})$ *attain Wyner's common information* $C(X_1^{(2)}; X_2^{(2)})$*, then (6.5) holds with equality.*

Intuitively, Corollary 6.4.1 expresses the fact that the communication system in Fig.6.2 cannot perform better than the optimistic case where decoders $(1, 1)$ and $(2, 1)$ cooperates as well as decoders $(1, 2)$ and $(2, 2)$. A natural question then arises: is there any achievable rate tuple $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22})$ that attains the lower bounds in (6.4) and (6.5) simultaneously? The answer is affirmative if and only if there exists a pmf $p(w_1, w_2|x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ such that

$$(X_1^{(2)}, X_2^{(2)}) \to (X_1^{(1)}, X_2^{(1)}) \to W_1, \tag{6.6a}$$

$$(X_1^{(1)}, X_2^{(1)}) \to (X_1^{(2)}, X_2^{(2)}) \to W_1, \tag{6.6b}$$

$$X_1^{(1)} \to W_1 \to X_2^{(1)}, \tag{6.6c}$$

$$(X_1^{(1)}, X_2^{(1)}) \to (X_1^{(2)}, X_2^{(2)}, W_1) \to W_2, \tag{6.6d}$$

$$X_1^{(2)} \to (W_1, W_2) \to X_2^{(2)} \tag{6.6e}$$

form Markov chains. We can simplify these constraints using the following lemma.

Lemma 6.4.1. *For every conditional pmf $p(w_1|x_1^{(1)}, x_2^{(1)})$, there exists a conditional pmf $p(w_2|w_1, x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ such that*

$$I(X_1^{(1)}, X_2^{(1)}; W_2|X_1^{(2)}, X_2^{(2)}, W_1) = I(X_1^{(2)}; X_2^{(2)}|W_1, W_2) = 0.$$

It is easy to justify Lemma 6.4.1 by letting $W_2 = (X_2^{(2)}, X_2^{(2)})$ as one example among many. As a result, there exists an achievable rate tuple $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22})$ attaining (6.4) and (6.5) if and only if there exists a pmf $p(w_1|x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ such that (6.6a)-(6.6c) form Markov chains. A simple example can be constructed as follows.

Example 6.4.1. *Suppose that $X_1^{(1)}$ and $X_2^{(1)}$ are independent, i.e.,*

$$p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) = p(x_1^{(1)})p(x_2^{(1)})p(x_1^{(2)}, x_2^{(2)}|x_1^{(1)}, x_2^{(1)}).$$

Let $W_1 = \emptyset$ and let $p(w_2|x_1^{(2)}, x_2^{(2)})$ attain Wyner's common information $C(X_1^{(2)}; X_2^{(2)})$. Then, (6.6a)-(6.6e) form Markov chains and thus there exists an achievable rate tuple $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22})$ that attains the lower bounds in (6.4) and (6.5).

If $X_1^{(1)}$ and $X_2^{(1)}$ are correlated unlike Example 6.4.1, is it still possible to find such a W_1? The answer does in fact depend on the distribution of the whole content,

$p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$. In the following, we present a necessary condition on the content distribution to attain the lower bounds in Corollary 6.4.1.

Proposition 6.4.1. *Suppose that $(X_1^{(1)}, X_2^{(1)})$ are not independent. Let G be a bipartite graph with vertex set $\mathcal{A} \cup \mathcal{B}$ where $\mathcal{A} = \mathcal{X}_{1,1} \times \mathcal{X}_{2,1}$ and $\mathcal{B} = \mathcal{X}_{1,2} \times \mathcal{X}_{2,1}$ such that there is an edge between two vertices (t_1, t_2) if and only if $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) > 0$ where $t_1 = (x_1^{(1)}, x_2^{(1)})$ and $t_2 = (x_1^{(2)}, x_2^{(2)})$. If G is connected, then the lower bounds in (6.4) and (6.5) cannot be attained simultaneously.*

Proof. We prove by contradiction. Suppose that there is a pmf $p(w_1|x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ such that (6.6a)-(6.6c) form Markov chains and that the described bipartite graph G is connected. The Markov chains in (6.6a) and (6.6b) implies that for any $w_1 \in \mathcal{W}_1$, $p(w_1|x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ is a constant over each connected component of G. Since G is connected, then

$$p(w_1|x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) = p(w_1), \quad \forall (x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) \in \mathcal{X}_{1,1} \times \mathcal{X}_{2,1} \times \mathcal{X}_{1,2} \times \mathcal{X}_{2,2}.$$

Thus, W_1 is independent of $(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)})$, which contradicts with the Markov chain in (6.6c) since $X_1^{(2)}$ and $X_2^{(2)}$ are correlated. □

The necessary condition in Proposition 6.4.1 is in fact closely related to Gács-Korner common information [4], which is another well-known quantity proposed to measure the common information between two random variables and is defined as

$$K(X;Y) := \max_{\substack{p(w|x,y): \\ W \to X \to Y, \\ W \to Y \to X}} I(X,Y;W).$$

[5, Corollary 1] provides a way to compute $K(X;Y)$. Let G be a bipartite graph with vertex set $\mathcal{X} \cup \mathcal{Y}$ such that there is an edge between two vertices (x, y) if and only if $p(x, y) > 0$ and let W be the labels of the connected components of G. Then, $K(X;Y) = H(W)$. Therefore, $K(X;Y) = 0$ if and only if G is connected. Letting $X \leftarrow (X_1^{(1)}, X_2^{(1)})$ and $Y \leftarrow (X_1^{(2)}, X_2^{(2)})$ implies the following in our setting.

Corollary 6.4.2. *For a correlated pair of $(X_1^{(1)}, X_2^{(1)})$, it is not possible to attain the lower bounds in (6.4) and (6.5) if*

$$K(X_1^{(1)}, X_2^{(1)}; X_1^{(2)}, X_2^{(2)}) = 0.$$

We next construct an example where the information carried over the common link (L_1) is useful for all decoders, which allows to attain (6.4) and (6.5).

Example 6.4.2. *Suppose the pmf $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ is given as*

$(x_1^{(1)}, x_2^{(1)})/(x_1^{(2)}, x_2^{(2)})$	00	11	01	10
00	$\overline{\alpha}/2$	0	0	0
11	0	$\overline{\alpha}/2$	0	0
01	0	0	$\alpha/2-\beta$	β
10	0	0	β	$\alpha/2-\beta$

.

Note that both $(x_1^{(1)}, x_2^{(1)})$ and $(x_1^{(2)}, x_2^{(2)})$ are doubly symmetric binary source with parameter α. Let

$$W_1 | x_1^{(1)}, x_2^{(1)} = \begin{cases} \text{Bern}(q), & \textit{if } (x_1^{(1)}, x_2^{(1)}) = (0,0) \\ \text{Bern}(\bar{q}), & \textit{if } (x_1^{(1)}, x_2^{(1)}) = (1,1) \\ \text{Bern}(0.5), & \textit{otherwise} \end{cases}, \tag{6.7}$$

where $q = 0.5 - 0.5\sqrt{1-2\alpha}/(1-\alpha)$, which attains both of the Wyner common information $C(X_1^{(1)}; X_2^{(1)})$ and $C(X_1^{(2)}; X_2^{(2)})$ (refer to [2, 6] for the proof). Therefore, letting $W_2 = \emptyset$ attains the lower bounds in (6.4) and (6.5).

6.5 Relation to Conditional Wyner's Common Information

Given a fixed strategy for Encoder 1, what would be the optimal strategy for Encoder 2 to minimize the total rate of the descriptions transmitted from Encoder 2 to

Decoders $(1,2)$ and $(2,2)$? First, Theorem 6.3.1 implies that given a pmf $p(w|x_1^{(1)}, x_2^{(1)})$, a rate tuple $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22}) \in \mathscr{R}$ must satisfy

$$C_2 + R_{12} + R_{22} \geq H(X_1^{(2)}, X_2^{(2)}|W).$$

Therefore, given a pmf $p(w|x_1^{(1)}, x_2^{(1)})$, we define

$$C_2^*(W) = \min_{\substack{(C_1,R_{11},R_{21},C_2,R_{12},R_{22}) \in \mathscr{R} \\ C_2+R_{12}+R_{22}=H(X_1^{(2)},X_2^{(2)}|W)}} C_2.$$

In words, $C_2^*(W)$ is the smallest rate of the common link to Decoders $(1,2)$ and $(2,2)$ required to losslessly describe $(X_1^{(2)}, X_2^{(2)})$ by the help of W. Note that $H(X_1^{(2)}, X_2^{(2)}|W)$ is the minimum compression rate required for a single receiver to recover both X_{12}^n and X_{22}^n when both encoder and decoders are furnished with a side information sequence W^n drawn i.i.d. from $p(w|x_1^{(2)}, x_2^{(2)})$. In our successive setting, on the other hand, W^n is not such a standard side information but related to (X_{12}^n, X_{22}^n) through (X_{11}^n, X_{21}^n). We, however, can still establish a closed form solution for $C_2^*(W)$ as a corollary of Theorem 6.3.1.

As a corollary of Theorem 6.3.1, one can prove the following.

Corollary 6.5.1. *Given a pmf $p(w|x_1^{(1)}, x_2^{(1)})$, the minimum rate*

$$C_2^*(W) = C(X_1^{(2)}; X_2^{(2)}|W),$$

where $C(X_1^{(2)}; X_2^{(2)}|W)$ denotes the conditional Wyner's common information [7] and is defined by

$$C(X_1^{(2)}; X_2^{(2)}|W) := \min_{\substack{p(v|x_1^{(2)},x_2^{(2)},w) \\ X_1^{(2)}-(W,V)-X_2^{(2)}}} I(X_1^{(2)}, X_2^{(2)}; V|W). \tag{6.8}$$

It is worth to note that Lapidoth and Wigger [7] studied the Gray–Wyner network with i.i.d. side information W^n available at encoder and decoders and obtained the same answer in (6.8) for the minimum common rate to achieve the sum rate of $H(X_1^{(2)}, X_2^{(2)}|W)$.

6.6 Discussion

In this chapter, we have introduced the successive Gray–Wyner network and presented its optimal rate region. In the subsequent chapters, we will describe two new dynamic caching problems and establish a close connection of each problem to the successive Gray–Wyner network. We will utilize the optimal rate region presented in Theorem 6.3.1 when analyzing the optimal performance for those dynamic caching problems.

6.A Proof of Theorem 6.3.1

We first provide an outer bound (achievability) and then an inner bound (converse) for the optimal rate region $\mathscr{R}$.

For the achievability, given the source distribution $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$, fix two conditional pmfs $p(w_1|x_1^{(1)}, x_2^{(1)})$ and $p(w_2|w_1, x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$, and let $\epsilon > 0$. Generate 2^{nC_1} sequences $w_1^n(j), j \in [1 : 2^{nC_1}]$ i.i.d. with respect to $p(w_1)$. Encoder 1 chooses an index l_1 such that

$$(w_1^n(l_1), x_{11}^n, x_{21}^n) \in \mathcal{T}_\epsilon^{(n)}(W_1, X_1^{(1)}, X_2^{(1)}),$$

and transmits to all four decoders. Given $w_1^n(l_1)$, encoder 1 assigns indices $m_{11} \in [2^{nR_{11}}]$ and $m_{21} \in [2^{nR_{21}}]$ to the sequences in $\mathcal{T}_\epsilon^{(n)}(X_1^{(1)}|w_1^n(l_1))$ and $\mathcal{T}_\epsilon^{(n)}(X_2^{(1)}|w_1^n(l_1))$, respectively, and send them to decoders $(1, 1)$ and $(2, 1)$, respectively. Decoder $(d, 1)$, $d = 1, 2$, first decodes w_1^n from l_1 and then decode for x_{d1}^n.

Similarly, at encoder 2, given $w_1^n(l_1)$, generate 2^{nC_2} sequences $w_2^n(k), k \in [1 : 2^{nC_2}]$ i.i.d. with respect to the conditional pmf $p(w_2|w_1)$. Encoder 2 chooses an index l_2

such that

$$(w_2^n(l_2), w_1^n(j), x_{11}^n, x_{21}^n, x_{12}^n, x_{22}^n) \in \mathcal{T}_\epsilon^{(n)}(W_1, W_2, X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}),$$

and transmits l_2 to decoders $(1,2)$ and $(2,2)$. Given $(w_1^n(l_1), w_2^n(l_2))$, encoder 2 assigns indices $m_{12} \in [2^{nR_{12}}]$ and $m_{22} \in [2^{nR_{22}}]$ to the sequences in $\mathcal{T}_\epsilon^{(n)}(X_1^{(2)}|w_1^n(l_1), w_2^n(l_2))$ and $\mathcal{T}_\epsilon^{(n)}(X_2^{(2)}|w_1^n(l_1), w_2^n(l_2))$, respectively, and send them to decoders $(1,2)$ and $(2,2)$, respectively. Decoder $(d,2)$, $d = 1, 2$, first recovers w_1^n, w_2^n from l_1 and l_2, and then decode for x_{d2}^n. By standard arguments similar to the proof of Slepian-Wolf coding, it is easy to see that $P_e^{(n)} \to 0$ as $n \to \infty$ if the rate tuple $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22})$ satisfies

$$\begin{aligned}
C_1 &\geq I(X_1^{(1)}, X_2^{(1)}; W_1) + \delta(\epsilon), \\
R_{d1} &\geq H(X_d^{(1)}|W_1) + \delta(\epsilon), \quad d = 1, 2, \\
C_2 &\geq I(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}; W_2|W_1) + \delta(\epsilon), \\
R_{d2} &\geq H(X_d^{(2)}|W_1, W_2) + \delta(\epsilon), \quad d = 1, 2,
\end{aligned}$$

where $\delta(\epsilon)$ is a function of ϵ such that $\delta(\epsilon)$ tends to zero as $\epsilon \to 0$. Letting $\epsilon \to 0$ completes the proof of the achievability.

For the converse, suppose that the rate tuple $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22}) \in \mathscr{R}$. By Gray and Wyner [1], $(C_1, R_{11}, R_{21}, C_2, R_{12}, R_{22})$ must satisfy (6.3a) and (6.3b). We now prove (6.3c). Suppose that the i'th entry of X_{dt}^n is denoted by $(X_{dt})_i$ and the sequence consisting of the first i entries of X_{dt}^n is denoted by X_{dt}^i for $d, t \in \{1, 2\}$. Define the auxiliary random variables $W_{1i} := (L_1, X_{11}^{i-1}, X_{21}^{i-1})$ and $W_{2i} := (L_2, X_{12}^{i-1}, X_{22}^{i-1})$, $i \in [n]$. We start with

$$\begin{aligned}
nC_2 &\geq H(L_2|L_1) \\
&\geq I(L_2; X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n|L_1)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} I(L_2; (X_{11})_i, (X_{21})_i, (X_{12})_i, (X_{22})_i | L_1, X_{11}^{i-1}, X_{21}^{i-1}, X_{12}^{i-1}, X_{22}^{i-1}) \\
&= \sum_{i=1}^{n} I(L_2, X_{12}^{i-1}, X_{22}^{i-1}; (X_{11})_i, (X_{21})_i, (X_{12})_i, (X_{22})_i | L_1, X_{11}^{i-1}, X_{21}^{i-1}) \\
&\qquad\qquad - I(X_{12}^{i-1}, X_{22}^{i-1}; (X_{11})_i, (X_{21})_i, (X_{12})_i, (X_{22})_i | L_1, X_{11}^{i-1}, X_{21}^{i-1}) \\
&\overset{(a)}{=} \sum_{i=1}^{n} I(L_2, X_{12}^{i-1}, X_{22}^{i-1}; (X_{11})_i, (X_{21})_i, (X_{12})_i, (X_{22})_i | L_1, X_{11}^{i-1}, X_{21}^{i-1}) \\
&= \sum_{i=1}^{n} I(W_{2i}; (X_{11})_i, (X_{21})_i, (X_{12})_i, (X_{22})_i | W_{1i}),
\end{aligned}
$$

where (a) follows since

$$
\big(X_{12}^{i-1}, X_{22}^{i-1}\big) \to \big(X_{11}^{i-1}, X_{21}^{i-1}\big) \to \big(L_1, (X_{11})_i, (X_{21})_i, (X_{12})_i, (X_{22})_i\big)
$$

form a Markov chain.

Lastly, to prove (6.3d), for $d = 1, 2$, we start with

$$
\begin{aligned}
nR_{d2} &\geq H(M_{d2} | L_1, L_2) \\
&\geq I(M_{d2}; X_{d2}^n | L_1, L_2) \\
&\overset{(a)}{\geq} H(X_{d2}^n | L_1, L_2) - n\epsilon_n \\
&= \sum_{i=1}^{n} H\big((X_{d2})_i | L_1, L_2, X_{d2}^{i-1}\big) - n\epsilon_n \\
&\geq \sum_{i=1}^{n} H\big((X_{d2})_i | L_1, L_2, X_{11}^{i-1}, X_{21}^{i-1}, X_{12}^{i-1}, X_{22}^{i-1}\big) - n\epsilon_n \\
&= \sum_{i=1}^{n} H\big((X_{d2})_i | W_{1i}, W_{2i}\big) - n\epsilon_n,
\end{aligned}
$$

where (a) follows by Fano's inequality.

Finally, the cardinality bound on $\mathcal{W}_1$ and $\mathcal{W}_2$ can be shown using the convex cover method in [8].

Acknowledgment

This chapter is, in part, a reprint of the material in the paper: Pinar Sen and Michael Gastpar, “Successive Refinement to Caching for Dynamic Content,” *Proceedings of IEEE International Symposium on Information Theory*, Paris, France, June 2019. This chapter is, in part, currently being prepared for submission for publication of the material in *IEEE Transactions of Information Theory*, 2020 with authors Pinar Sen, Michael Gastpar, and Young-Han Kim. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] R. M. Gray and A. D. Wyner. Source coding for a simple network. *Bell Syst. Tech. J.*, 53(9):1681–1721, 1974.

[2] Aaron D. Wyner. The common information of two dependent random variables. *IEEE Trans. Inf. Theory*, 21(2):163–179, March 1975.

[3] C. Wang, S. H. Lim, and M. Gastpar. Information-theoretic caching. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 1776–1780, June 2015.

[4] P. Gács and J. Körner. Common information is far less than mutual information. *Probl. Control Inf. Theory*, 2(2):149–162, 1973.

[5] R. Ahlswede and J. Körner. *Appendix: On Common Information and Related Characteristics of Correlated Information Sources*, pages 664–677. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[6] Chien-Yi Wang. *Function Computation over Networks Efficient Information Processing for Cache and Sensor Applications.* EPFL, Lausanne, 2015.

[7] A. Lapidoth and M. Wigger. Conditional and relevant common information. In *2016 IEEE International Conference on the Science of Electrical Engineering (ICSEE)*, pages 1–5, Nov 2016.

[8] Abbas El Gamal and Young-Han Kim. *Network Information Theory.* Cambridge University Press, Cambridge, 2011.

Chapter 7

Successive Refinement to Caching for Dynamic Contents

To reduce the load of the heavy network traffic, servers deliver partial data to users during the off-peak hours of the network before the actual requests are known, which is known as *caching*. This chapter introduces a new single-user caching problem in which the file contents are subject to random modifications during the cache placement phase (*dynamic contents*). To cope with the dynamic nature of the contents, a two-step successive refinement approach is proposed: some partial information of the original data is cached in the first step and second step refines the cache content stored in the first step when the file contents are modified. Given a fixed cache rate, there is a tension between the rates of two cache descriptions to minimize the delivery rate. Founding a close connection to the successive Gray–Wyner network in Chapter 6, a single-letter characterization of the minimum average-case delivery rate is established as an optimization problem, which is solved explicitly for certain classes of contents.

7.1 Introduction

Due to exponentially growing number of devices, networks usually encounter heavy traffic during the popular time of the day. A recent solution to reduce the network traffic during these busy hours is to deliver partial data for future use before database knows which file is to be requested by the users [1, 2]. In the classical (static) single-user caching problem [3], communication is divided into three phases. In *caching phase*, database delivers partial information about the file contents to user. Database is informed which of the files is requested by the user in *request phase*. Finally, in *delivery phase*, the remaining part of the requested file is delivered. Taking an information theoretical approach, [3, 4] formulated this problem through its similarity to Gray-Wyner network [5] and discussed the optimal caching strategy. This information-theoretic approach was extended to multi-user networks in [4, 6]. In parallel, building on rate–distortion theory, counterparts of these caching problems for lossy reconstruction were investigated in [7–11].

On the other hand, the database has a *dynamic* nature in the sense that the content files could be modified or completely changed into different files. For example, news websites are continuously updated throughout the day with the most current information. This dynamic nature is taken into account in a more recent work [12], which studied random modifications to the file contents that occur after cache placement is completed. In this formulation, cache content is designed by using only the original files and is placed in a single step, whereas delivery content is designed to benefit from the correlation between the original and modified contents.

In all the existing caching problems, cache placement is completed in a single step, which falls short of capturing the unpredictable nature of contents in real networks. In this chapter, we introduce a new caching problem to address contents being subject to random modifications during the cache placement phase and we propose a successive refinement approach to cache placement as an answer to this dynamic caching problem.

Taking an information-theoretic approach similar to [3, 4], we relate this problem to the successive Gray–Wyner network in Chapter 6, in which the common message to all decoders corresponds to the first step of cache placement whereas the common message to a subset of decoders corresponds to the second step. Utilizing the results derived in Chapter 6, we establish a single-letter characterization of the optimal tradeoff between the total cache rate and the minimum average-case delivery rate as an optimization problem. We then derive an explicit characterization of the optimal tradeoff for certain classes of content distributions.

7.2 Problem Formulation

In this section, we introduce a new caching model in which the file contents stored in the server are subject to random changes within the cache placement phase. For ease of exposition, suppose that the server originally stores a pair of files (X_{11}^n, X_{21}^n) drawn i.i.d. from the pmf $p(x_1^{(1)}, x_2^{(1)})$ over a finite alphabet, which is modified to (X_{12}^n, X_{22}^n) with probability $\rho \in [0, 1]$, where the tuple $(X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n)$ is distributed i.i.d. with respect to a given pmf $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ over a finite alphabet. The indices i and j in $X_{ij}^n \overset{\text{i.i.d.}}{\sim} p(x_i^{(j)})$ denotes the file content and the version, respectively. As illustrated in Fig. 7.1, server first sends out partial information about the original files (X_{11}^n, X_{21}^n) to be cached at the user. If any modification occurs, having access to both versions of the files, server conveys additional bits as an *update* for the cache. Once user request arises, it then delivers the information required by the user to losslessly recover its desired file. Combining this delivery with its cache, the user, which is aware of any possible change, decodes for its desired file. Given a fixed cache rate, our goal is to minimize the expected delivery rate with respect to uniform file popularity and randomness in the modification. There is, however, a tension between caching for only (X_{11}^n, X_{21}^n) as if there will be no modification on the content and sparing all the cache rate for (X_{12}^n, X_{22}^n), resulting in an optimization problem of how to split the cache rate into two descriptions.

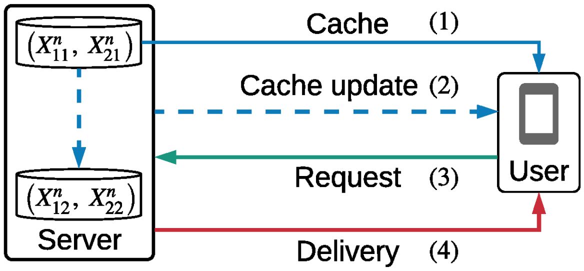


Figure 7.1. Caching for dynamic contents: server first places some cache (1) based on the original files (X_{11}^n, X_{21}^n) and then if there is any modification, it further places an update on the cache (2). When the request arises (3), server delivers the required content for user to decode its desired file (4).

We start with formalizing the problem. An $\left(n, nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}\right)$ successive caching scheme for dynamic contents consists of

- two caching functions where

$$\phi_1 : \mathcal{X}_{11}^n \times \mathcal{X}_{21}^n \rightarrow \{0,1\}^{nC_1}$$

maps the original files (X_{11}^n, X_{21}^n) into a cache content

$$L_1 := \phi_1(X_{11}^n, X_{21}^n)$$

to be placed at the user during the first step of the successive cache placement phase and

$$\phi_2 : \mathcal{X}_{11}^n \times \mathcal{X}_{21}^n \times \mathcal{X}_{12}^n \times \mathcal{X}_{22}^n \rightarrow \{0,1\}^{nC_2}$$

maps the original files and modified files $(X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n)$ into a cache content

$$L_2 := \phi_2(X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n)$$

to be placed at the user during the second step of the successive cache placement phase,

- four encoding functions, where

  $$\psi_{d1} : \mathcal{X}_{11}^n \times \mathcal{X}_{21}^n \to \{0,1\}^{nR_{d1}}, \quad d \in \{1,2\},$$

  maps the files (X_{11}^n, X_{21}^n) to the delivery content

  $$M_{d1} := \psi_{d1}(X_{11}^n, X_{21}^n)$$

  corresponding to the request for file $d \in \{1,2\}$ when modification does not occur, and

  $$\psi_{d2} : \mathcal{X}_{11}^n \times \mathcal{X}_{21}^n \times \mathcal{X}_{12}^n \times \mathcal{X}_{22}^n \to \{0,1\}^{nR_{d2}}, \quad d \in \{1,2\},$$

  maps the files $(X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n)$ to the delivery content

  $$M_{d2} := \psi_{d2}(X_{11}^n, X_{21}^n, X_{12}^n, X_{22}^n)$$

  corresponding to the request for file $d \in \{1,2\}$ when there is modification,

- four decoding functions, where

  $$\mu_{d1} : \{0,1\}^{nC_1} \times \{0,1\}^{nR_{d1}} \to \mathcal{X}_{d1}^n$$

  maps the first piece of the cache content and the delivery content into an estimate

  $$\hat{X}_{d1}^n := \mu_{d1}\big(L_1, M_{d1}\big)$$

  of the requested file X_{d1}^n when the request vector $d \in \{1,2\}$ is received by the server without any modification to the file contents and

  $$\mu_{d2} : \{0,1\}^{n(C_1+C_2)} \times \{0,1\}^{nR_{d2}} \to \mathcal{X}_{d2}^n$$

maps both of the cache contents and the delivery content into an estimate

$$\hat{X}_{d2}^n := \mu_{d2}\big(L_1, L_2, M_{d2}\big)$$

of the requested file X_{d2}^n when the request vector $d \in \{1,2\}$ is received by the server after the file contents are modified.

The probability of error is defined as

$$P_e^{(n)} := \mathsf{P}(\hat{X}_{dt}^n \neq X_{dt}^n \text{ for some } t \in \{1,2\}, d \in \{1,2\}).$$

Given a pair of cache rates (C_1, C_2), a delivery rate tuple $(R_{dt})_{d,t\in\{1,2\}}$ is said to be *achievable for dynamic contents* if there exists an $\big(n, nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}\big)$ successive caching scheme for dynamic contents with $\lim_{n\to\infty} P_e^{(n)} = 0$. Given a cache rate $C \geq 0$ and modification probability $\rho \in [0,1]$, a delivery rate R is said to be *average-case achievable for dynamic contents* if there exists an $\big(n, nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}\big)$ successive caching scheme for dynamic contents such that

$$C_1 + C_2 \leq C$$

and

$$(1-\rho)\frac{R_{11}+R_{21}}{2} + \rho\frac{R_{12}+R_{22}}{2} \leq R.$$

We define the optimal average-case delivery rate function for dynamic contents as

$$R^*_{\text{cont,avg}}(\rho, C) := \min\{R : R \text{ is average-case achievable for dynamic contents}\}. \quad (7.1)$$

Similarly, a delivery rate R is said to be *worst-case achievable for dynamic contents* if there exists an $\big(n, nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}\big)$ successive caching scheme for dynamic contents such that

$$C_1 + C_2 \leq C$$

and

$$\max_{i,j\in\{1,2\}} R_{ij} \le R.$$

We define the optimal worst-case delivery rate function for dynamic contents as

$$R^*_{\text{cont,worst}}(C) := \min\{R : R \text{ is worst-case achievable for dynamic contents}\}. \tag{7.2}$$

We are now ready to present the main result of this chapter.

7.3 Main Results

We next present a single-letter characterization of the optimal average-case delivery rate function as well as the optimal worst-case delivery rate function.

Theorem 7.3.1. *Given modification probability $\rho \in [0,1]$, the optimal average-case delivery rate function is equal to*

$$\begin{aligned} R^*_{\text{cont,avg}}(\rho, C) = \min_{\substack{p(w_1|x_1^{(1)},x_2^{(1)}),\\ p(w_2|w_1,x_1^{(1)},x_2^{(1)},x_1^{(2)},x_2^{(2)}):\\ I(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)};W_1,W_2)\le C}} & \Big[(1-\rho)\frac{H(X_1^{(1)}|W_1)+H(X_2^{(1)}|W_1)}{2} \\ & + \rho\frac{H(X_1^{(2)}|W_1,W_2)+H(X_2^{(2)}|W_1,W_2)}{2}\Big]. \end{aligned} \tag{7.3}$$

Similarly, the optimal worst-case delivery rate function is equal to

$$\begin{aligned} & R^*_{\text{cont,worst}}(C) \\ & = \min_{\substack{p(w_1|x_1^{(1)},x_2^{(1)}),\\ p(w_2|w_1,x_1^{(1)},x_2^{(1)},x_1^{(2)},x_2^{(2)}):\\ I(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)};W_1,W_2)\le C}} \max\left\{\begin{array}{c} H(X_1^{(1)}|W_1), H(X_2^{(1)}|W_1), \\ H(X_1^{(2)}|W_1,W_2)+H(X_2^{(2)}|W_1,W_2) \end{array}\right\}. \end{aligned} \tag{7.4}$$

Proof. The key observation is that the described caching problem for dynamic contents is equivalent to the source coding problem defined over the successive Gray–Wyner network, in which encoders correspond to the server before and after modification and decoders correspond to the realizations of different requests. It is then easy to see that there exists an $\big(n, nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}\big)$ successive caching scheme for dynamic contents if and only if there exists an $\big(n, nC_1, nR_{11}, nR_{21}, nC_2, nR_{12}, nR_{22}\big)$ code for the successive Gray–Wyner network. Following a similar notation to Chapter 6, let $\mathscr{R}$ denote the optimal rate region for the successive Gray–Wyner network described in Section 6.3. Then, the optimal average-case delivery rate function for dynamic contents can be written as

$$\begin{aligned} R^*_{\text{cont,avg}}(\rho, C) &= \min_{\substack{(C_1,R_{11},R_{21},C_2,R_{12},R_{22})\in\mathscr{R} \\ C_1+C_2\le C}} \left[(1-\rho)\frac{R_{11}+R_{21}}{2} + \rho\frac{R_{12}+R_{22}}{2}\right] \\ &\overset{(a)}{=} \min_{\substack{p(w_1|x_1^{(1)},x_2^{(1)}), \\ p(w_2|w_1,x_1^{(1)},x_2^{(1)},x_1^{(2)},x_2^{(2)}): \\ I(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)};W_1,W_2)\le C}} \left[(1-\rho)\frac{H(X_1^{(1)}|W_1)+H(X_2^{(1)}|W_1)}{2}\right. \\ &\qquad\qquad\left. + \rho\frac{H(X_1^{(2)}|W_1,W_2)+H(X_2^{(2)}|W_1,W_2)}{2}\right], \end{aligned}$$

where (a) follows by Theorem 6.3.1. Similarly, the optimal worst-case delivery rate function for dynamic contents can be written as

$$\begin{aligned} &R^*_{\text{cont,worst}}(C) \\ &= \min_{\substack{(C_1,R_{11},R_{21},C_2,R_{12},R_{22})\in\mathscr{R} \\ C_1+C_2\le C}} \max[R_{11}, R_{21}, R_{12}, R_{22}] \\ &\overset{(b)}{=} \min_{\substack{p(w_1|x_1^{(1)},x_2^{(1)}), \\ p(w_2|w_1,x_1^{(1)},x_2^{(1)},x_1^{(2)},x_2^{(2)}): \\ I(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)};W_1,W_2)\le C}} \max\left\{\begin{array}{c} H(X_1^{(1)}|W_1), H(X_2^{(1)}|W_1), \\ H(X_1^{(2)}|W_1,W_2)+H(X_2^{(2)}|W_1,W_2) \end{array}\right\}, \end{aligned}$$

where (b) follows by Theorem 6.3.1. □

The explicit solutions of the optimization problems in (7.3) and (7.4) are nontrivial in general. In the rest of this section, we particularly focus on the optimal average-case delivery rate function $R^*_{\text{cont,avg}}(\rho, C)$ for uniformly at random modifications ($\rho = 0.5$) and continue with the notation $R^*_{\text{cont,avg}}(C) := R^*_{\text{cont,avg}}(\rho = 0.5, C)$, which reduces to

$$R^*_{\text{cont,avg}}(C) = \min_{\substack{p(w_1|x_1^{(1)},x_2^{(1)}),\\ p(w_2|w_1,x_1^{(1)},x_2^{(1)},x_1^{(2)},x_2^{(2)}):\\ I(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)};W_1,W_2)\le C}} \Bigg[\frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1)}{4} + \frac{H(X_1^{(2)}|W_1,W_2) + H(X_2^{(2)}|W_1,W_2)}{4}\Bigg].$$

The solution of this minimization occurs at the boundary of

$$I(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}; W_1, W_2) = C.$$

It is, however, still a nontrivial optimization problem for an arbitrary content distribution $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$. Nonetheless, for some classes of distributions, we can characterize the explicit solution.

Example 7.3.1 (Nested Contents)**.** *Suppose that* $H(X_1^{(1)}|X_2^{(1)}) = H(X_2^{(1)}|X_1^{(2)}) = H(X_1^{(2)}|X_2^{(2)}) = 0$*. Define*

$$\bar{H}(C) := \frac{1}{4}\sum_{i=1}^{2}\sum_{t=1}^{2}\Big[H\big(X_i^{(t)}\big) - C\Big]^+, \tag{7.5}$$

where $[a]^+ := \max\{0, a\}$*. We then have*

$$R^*_{\text{cont,avg}}(C) = \bar{H}(C).$$

To see this, note that $\bar{H}(C) \le R^*_{\text{cont,avg}}(C)$*, in general. For the achievability, first cache* $(X_1^{(1)}, X_2^{(1)})$ *up to the cache rate (via* W_1*). If* $C > H(X_1^{(1)}, X_2^{(1)}) = H(X_2^{(1)})$*, cache* $(X_1^{(2)}, X_2^{(2)})$ *given* $(X_1^{(1)}, X_2^{(1)})$ *(via* W_2*) until the total cache rate* C *is exhausted.*

Example 7.3.2 (Partially Nested Contents)**.** *Suppose that pmf* $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$

satisfies

$$p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) = p(x_1^{(1)}, x_2^{(1)})p(x_1^{(2)}|x_1^{(1)})p(x_2^{(2)}|x_2^{(1)}) \tag{7.6}$$

and

$$H(X_1^{(1)}, X_2^{(1)}|X_1^{(2)}, X_2^{(2)}) = 0. \tag{7.7}$$

If $C \geq C(X_1^{(1)}; X_2^{(1)})$*, then*

$$R^*_{\text{cont,avg}}(C) = \frac{\left[H(X_1^{(1)}, X_2^{(1)}) - C\right]^+ + [H(X_1^{(2)}, X_2^{(2)}) - C]^+}{4}.$$

The converse follows from the general lower bound in Proposition 7.3.2. We show the achievability of the corner points, from which the claim follows by time sharing. For $C = C(X_1^{(1)}; X_2^{(1)})$*, let* W_1 *attain Wyner's common information* $C(X_1^{(1)}; X_2^{(1)})$ *defined in (6.2) and let* $W_2 = \emptyset$*. By Theorem 7.3.1, we have*

$$\begin{aligned}
&R^*_{\text{cont,avg}}(C)\\
&\leq \frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) + H(X_1^{(2)}|W_1) + H(X_2^{(2)}|W_1)}{4}\\
&= \frac{H(X_1^{(1)}, X_2^{(1)}) - I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}; X_2^{(1)}|W_1)}{4}\\
&\qquad + \frac{H(X_1^{(2)}, X_2^{(2)}) - I(X_1^{(2)}, X_2^{(2)}; W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1)}{4}\\
&\overset{(a)}{=} \frac{H(X_1^{(1)}, X_2^{(1)}) - C + H(X_1^{(2)}, X_2^{(2)}) - I(X_1^{(2)}, X_2^{(2)}; W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1)}{4}\\
&\overset{(b)}{=} \frac{H(X_1^{(1)}, X_2^{(1)}) - C + H(X_1^{(2)}, X_2^{(2)}) - I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1)}{4}\\
&\overset{(c)}{=} \frac{H(X_1^{(1)}, X_2^{(1)}) - C + H(X_1^{(2)}, X_2^{(2)}) - C}{4},
\end{aligned}$$

where (a) *follows since* W_1 *attains Wyner's common information* $C(X_1^{(1)}; X_2^{(1)})$*,* (b) *follows by (7.7) since* $(X_1^{(2)}, X_2^{(2)}) \to (X_1^{(1)}, X_2^{(1)}) \to W_1$ *forms a Markov chain, and* (c) *follows by the fact that* $X_1^{(2)} \to W_1 \to X_2^{(2)}$ *form a Markov chain, which can be seen from (7.6) since* $(X_1^{(2)}, X_2^{(2)}) \to (X_1^{(1)}, X_2^{(1)}) \to W_1$ *and* $X_1^{(1)} \to W_1 \to X_2^{(1)}$ *each form a*

Markov chain.

For $C = H(X_1^{(1)}, X_2^{(1)})$*, let* $W_1 = (X_1^{(1)}, X_2^{(1)})$ *and let* $W_2 = \emptyset$*. By Theorem 7.3.1, we have*

$$\begin{aligned}
R^*_{\text{cont,avg}}(C) &\leq \frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) + H(X_1^{(2)}|W_1) + H(X_2^{(2)}|W_1)}{4} \\
&= \frac{H(X_1^{(2)}|X_1^{(1)}, X_2^{(1)}) + H(X_2^{(2)}|X_1^{(1)}, X_2^{(1)})}{4} \\
&\overset{(d)}{=} \frac{H(X_1^{(2)}, X_2^{(2)}|X_1^{(1)}, X_2^{(1)})}{4} \\
&\overset{(e)}{=} \frac{H(X_1^{(2)}, X_2^{(2)}) - C}{4},
\end{aligned}$$

where (*d*) *follows by (7.6) and* (*e*) *follows by (7.7).*

Finally, for $C = H(X_1^{(2)}, X_2^{(2)})$*, let* $W_1 = (X_1^{(1)}, X_2^{(1)})$ *and let* $W_2 = (X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)})$*. By Theorem 7.3.1, it is easy to see that* $R^*_{\text{cont,avg}}(C) = 0$*, which proves the claim.*

Fig. 7.2 illustrates the optimal average-case delivery rate function for dynamic contents, $R^*_{\text{cont,avg}}(C)$*, for* $C \geq C(X_1^{(1)}; X_2^{(1)})$*. For* $C < C(X_1^{(1)}; X_2^{(1)})$*, we provide a lower bound that follows from Proposition 7.3.2 and an upper bound that follows from time sharing between* $(W_1, W_2) = (\emptyset, \emptyset)$ *and* (W_1, W_2) *attaining* $R^*_{\text{cont,avg}}(C = C(X_1^{(1)}; X_2^{(1)}))$*. In this example, to benefit from the correlation between the original and the modified files, the cache rate is initially exhausted on the original file pair* $(X_1^{(1)}, X_2^{(1)})$*. If the cache rate is larger than* $H(X_1^{(1)}, X_2^{(1)})$*, then additional information about the modified file pair* $(X_1^{(2)}, X_2^{(2)})$ *is cached when modification occurs (if any).*

Example 7.3.3 (Pairwise Independent Content)**.** *Suppose that*

$$p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) = p(x_1^{(1)}, x_2^{(1)})p(x_1^{(2)}, x_2^{(2)}).$$

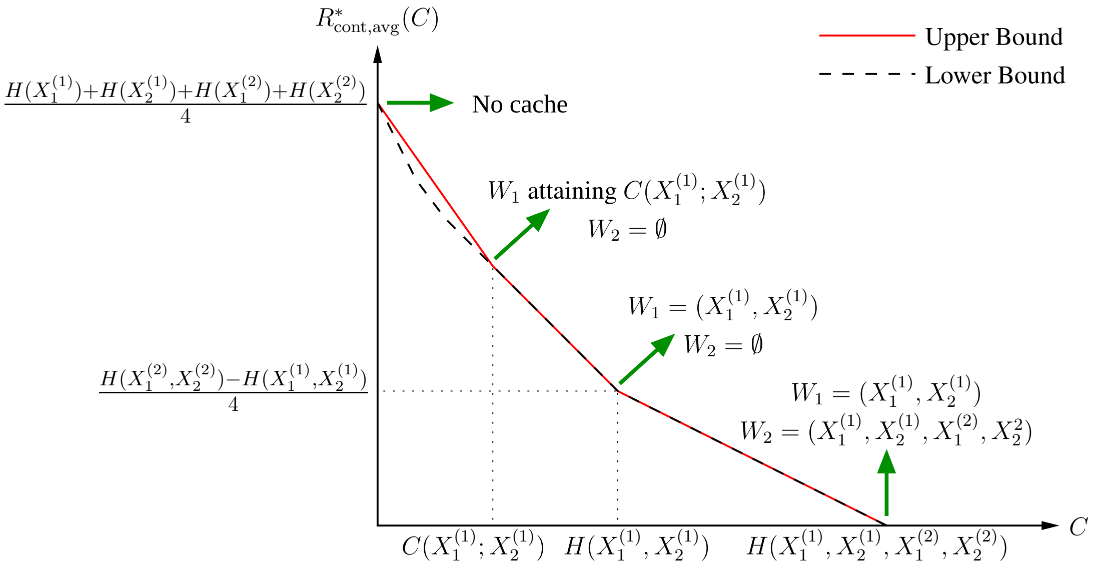


Figure 7.2. Bounds on the optimal average-case delivery rate function for dynamic contents in Example 7.3.2.

If $C \geq C(X_1^{(1)};X_2^{(1)}) + C(X_1^{(2)};X_2^{(2)})$*, then*

$$R^*_{\text{cont,avg}}(C) = \frac{[H(X_1^{(1)},X_2^{(1)}) + H(X_1^{(2)},X_2^{(2)}) - C]^+}{4}.$$

The converse follows from the general lower bound in Proposition 7.3.2. The achievability follows by time sharing between $(W_1,W_2) = ((X_1^{(1)},X_2^{(1)}),(X_1^{(2)},X_2^{(2)}))$ *and* $(W_1,W_2) = (W_1^*,W_2^*)$ *in Theorem 7.3.1, for* W_j^**,* $j=1,2$*, attaining Wyner's common information* $C(X_1^{(j)};X_2^{(j)})$*. This result implies that some of the cache rate should be spared for the modified files while dealing with two independent libraries if the total cache rate is large enough.*

In these examples, we have used the structure of the content distribution to propose upper bounds on the optimal average-case delivery rate function for dynamic contents $R^*_{\text{cont,avg}}(C)$. To provide an upper bound for arbitrarily correlated contents, let W^* attain Wyner's common information $C(X_1^{(1)};X_2^{(1)})$ and define function $R(C)$ as the lower complex envelope of the points

$$\begin{cases} \frac{H(X_1^{(1)})+H(X_2^{(1)})+H(X_1^{(2)})+H(X_2^{(2)})}{4}, & C = 0 \\ \frac{H(X_1^{(1)},X_2^{(1)})+H(X_1^{(2)},X_2^{(2)})-C-I(X_1^{(2)},X_2^{(2)};W^*)}{4}, & C = \begin{array}{c} C(X_1^{(1)};X_2^{(1)}) \\ +C(X_1^{(2)};X_2^{(2)}|W^*) \end{array} \\ \frac{H(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)})-C}{4}, & C = \begin{array}{c} H(X_1^{(1)},X_2^{(1)}) \\ +C(X_1^{(2)};X_2^{(2)}|X_1^{(1)},X_2^{(1)}) \end{array} \\ 0, & C = H(X_1^{(1)},X_2^{(1)},X_1^{(2)},X_2^{(2)}) \end{cases},$$

which is illustrated in Fig. 7.3 by the red solid line. The following is an upper bound on the optimal average-case delivery rate function.

Proposition 7.3.1 (Upper bound)**.** *For every pmf* $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$,

$$R^*_{\text{cont,avg}}(C) \leq R(C). \tag{7.8}$$

Proof. It suffices to prove the achievability of the corner points of $R(C)$ since the lower convex envelope of these points can be achieved by time sharing. First, by Theorem 7.3.1, it is trivial to see that $C = 0$ results in

$$R^*_{\text{cont,avg}}(C=0) = \frac{H(X_1^{(1)}) + H(X_2^{(1)}) + H(X_1^{(2)}) + H(X_2^{(2)})}{4}.$$

For $C = C(X_1^{(1)}; X_2^{(1)}) + C(X_1^{(2)}; X_2^{(2)}|W^*)$, we let $W_1 = W^*$ and let W_2 attain conditional Wyner's common information $C(X_1^{(2)}; X_2^{(2)}|W^*)$. By Theorem 7.3.1, we have

$$\begin{aligned} R^*_{\text{cont,avg}}(C) &\leq \frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) + H(X_1^{(2)}|W_1, W_2) + H(X_2^{(2)}|W_1, W_2)}{4} \\ &= \frac{H(X_1^{(1)}; X_2^{(1)}) - I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}; X_2^{(1)}|W_1)}{4} \\ &\quad + \frac{H(X_1^{(2)}, X_2^{(2)}|W_1) - I(X_1^{(2)}, X_2^{(2)}; W_2|W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1, W_2)}{4} \\ &\overset{(a)}{=} \frac{H(X_1^{(1)}; X_2^{(1)}) + H(X_1^{(2)}, X_2^{(2)}|W_1) - C}{4} \end{aligned}$$

$$= \frac{H(X_1^{(1)}; X_2^{(1)}) + H(X_1^{(2)}, X_2^{(2)}) - C - I(X_1^{(2)}, X_2^{(2)}; W^*)}{4},$$

where (a) follows by the choice of W_1 and W_2. Similarly, for $C = H(X_1^{(1)}, X_2^{(1)}) + C(X_1^{(2)}; X_2^{(2)} | X_1^{(1)}, X_2^{(1)})$, we let $W_1 = (X_1^{(1)}, X_2^{(1)})$ and let W_2 attain conditional Wyner's common information $C(X_1^{(2)}; X_2^{(2)} | X_1^{(1)}, X_2^{(1)})$ to get

$$R^*_{\text{cont,avg}}(C) \leq [H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}) - C]/4.$$

Finally, for $C = H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)})$, we let $W_1 = (X_1^{(1)}, X_2^{(1)})$ and we let $W_2 = (X_1^{(2)}, X_2^{(2)})$ to get $R^*_{\text{cont,avg}}(C) \leq 0$. □

We next present a lower bound on the optimal average-case delivery rate function.

Proposition 7.3.2 (Lower bound). *For every pmf* $p(x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$*,*

$$R^*_{\text{cont,avg}}(C) \geq \max\left\{ \begin{array}{c} \frac{\bar{H}(C)}{4}, \frac{[H(X_1^{(1)}, X_2^{(1)}) - C]^+ + [H(X_1^{(2)}, X_2^{(2)}) - C]^+}{4}, \\ \frac{[H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}) - C]^+}{4} \end{array} \right\}, \tag{7.9}$$

where $\bar{H}(C)$ is as defined in (7.5). Equality at

$$R^*_{\text{cont,avg}}(C) = \frac{[H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}) - C]^+}{4}$$

holds if and only if

$$C \geq C^* := \min_{p(w_1, w_2 | x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)}) \in \mathcal{P}} [I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(2)}, X_2^{(2)}; W_2 | W_1)], \tag{7.10}$$

where $\mathcal{P}$ is a class of conditional pmfs $p(w_1, w_2 | x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ such that

$$(X_1^{(2)}, X_2^{(2)}) \to (X_1^{(1)}, X_2^{(1)}) \to W_1,$$
$$(X_1^{(1)}, X_2^{(1)}) \to W_1 \to (X_1^{(2)}, X_2^{(2)}),$$
$$X_1^{(1)} \to W_1 \to X_2^{(1)},$$

$$X_1^{(2)} \to (W_1, W_2) \to X_2^{(2)},$$
$$(X_1^{(1)}, X_2^{(1)}) \to (X_1^{(2)}, X_2^{(2)}, W_1) \to W_2$$

form Markov chains.

Proof. For every pmf $p(w_1|x_1^{(1)}, x_2^{(1)})p(w_2|w_1, x_1^{(1)}, x_2^{(1)}, x_1^{(2)}, x_2^{(2)})$ such that

$$I(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}; W_1, W_2) \le C, \tag{7.11}$$

the objective function of the optimization problem in Theorem 7.3.1 satisfies

$$\begin{aligned}
&\frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) + H(X_1^{(2)}|W_1, W_2) + H(X_2^{(2)}|W_1, W_2)}{4} \\
&= \frac{\sum_{i=1}^{2}[H(X_i^{(1)}) - I(X_i^{(1)}; W_1)] + \sum_{j=1}^{2}[H(X_j^{(2)}) - I(X_j^{(2)}; W_1, W_2)]}{4} \\
&\overset{(a)}{\ge} \frac{\sum_{i=1}^{2}[H(X_i^{(1)}) - C]^+ + \sum_{j=1}^{2}[H(X_j^{(2)}) - C]^+}{4} \\
&= \bar{H}(C),
\end{aligned} \tag{7.12}$$

where (a) follows by the condition in (7.11). Similarly, we have

$$\begin{aligned}
&\frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) + H(X_1^{(2)}|W_1, W_2) + H(X_2^{(2)}|W_1, W_2)}{4} \\
&= \frac{H(X_1^{(1)}, X_2^{(1)}) - I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}; X_2^{(1)}|W_1)}{4} \\
&\quad + \frac{H(X_1^{(2)}, X_2^{(2)}) - I(X_1^{(2)}, X_2^{(2)}; W_1, W_2) + I(X_1^{(2)}; X_2^{(2)}|W_1, W_2)}{4} \\
&\ge \frac{[H(X_1^{(1)}, X_2^{(1)}) - C]^+ + [H(X_1^{(2)}, X_2^{(2)}) - C]^+}{4}
\end{aligned} \tag{7.13}$$

and

$$\begin{aligned}
&\frac{H(X_1^{(1)}|W_1) + H(X_2^{(1)}|W_1) + H(X_1^{(2)}|W_1, W_2) + H(X_2^{(2)}|W_1, W_2)}{4} \\
&= \frac{H(X_1^{(1)}, X_2^{(1)}) - I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}; X_2^{(1)}|W_1)}{4}
\end{aligned}$$

$$
\begin{aligned}
&\quad + \frac{H(X_1^{(2)}, X_2^{(2)}|W_1) - I(X_1^{(2)}, X_2^{(2)}; W_2|W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1, W_2)}{4} \\
&\overset{(b)}{=} \frac{H(X_1^{(1)}, X_2^{(1)}) - I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}; X_2^{(1)}|W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1, W_2)}{4} \\
&\quad + \frac{H(X_1^{(2)}, X_2^{(2)}|X_1^{(1)}, X_2^{(1)}) + I(X_1^{(2)}, X_2^{(2)}; X_1^{(1)}, X_2^{(1)}|W_1) - I(X_1^{(2)}, X_2^{(2)}; W_2|W_1)}{4} \\
&= \frac{H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}) + I(X_1^{(1)}; X_2^{(1)}|W_1) + I(X_1^{(2)}; X_2^{(2)}|W_1, W_2)}{4} \\
&\quad + \frac{I(X_1^{(2)}, X_2^{(2)}; X_1^{(1)}, X_2^{(1)}|W_1) + I(X_1^{(1)}, X_2^{(1)}; W_2|W_1, X_1^{(2)}, X_2^{(2)})}{4} \\
&\quad - \frac{I(X_1^{(1)}, X_2^{(1)}; W_1) + I(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}; W_2|W_1)}{4} \\
&\overset{(c)}{\geq} \frac{[H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}) - C]^+}{4}, \qquad (7.14)
\end{aligned}
$$

where (b) follows since $(X_1^{(2)}, X_2^{(2)}) \to (X_1^{(1)}, X_2^{(1)}) \to W_1$ form a Markov chain and (c) follows by the condition in (7.11). Combining (7.12)-(7.14) implies the claim.

Note that the solution to the optimization problem in Theorem 7.3.1 occurs at the boundary of (7.11). Therefore, the lower bound in (7.14) is attained if and only if $C \geq C^*$. □

Remark 7.3.1. *Let $W_1 = (X_1^{(1)}, X_2^{(1)})$. The threshold C^* in (7.10) then satisfies*

$$C^* \leq H(X_1^{(1)}, X_2^{(1)}) + C(X_1^{(2)}; X_2^{(2)}|X_1^{(1)}, X_2^{(1)}).$$

Therefore, if $C \geq H(X_1^{(1)}, X_2^{(1)}) + C(X_1^{(2)}; X_2^{(2)}|X_1^{(1)}, X_2^{(1)})$, by Proposition 7.3.2,

$$R^*_{\text{cont,avg}}(C) = \frac{[H(X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}) - C]^+}{4}.$$

Remark 7.3.2. *The upper and lower bounds in Propositions 7.3.1 and 7.3.2 respectively are demonstrated in Fig. 7.3, where the gap Δ between these two bounds satisfies*

$$\Delta \leq \min\{C, I(X_1^{(1)}, X_2^{(1)}; X_1^{(2)}, X_2^{(2)})\}/4,$$

if $C(X_1^{(1)};X_2^{(1)}) + C(X_1^{(2)};X_2^{(2)}|W^*) \leq C \leq C^*$. *Note that the gap* Δ *is tight for independent pair of files in Example 6.4.1.*

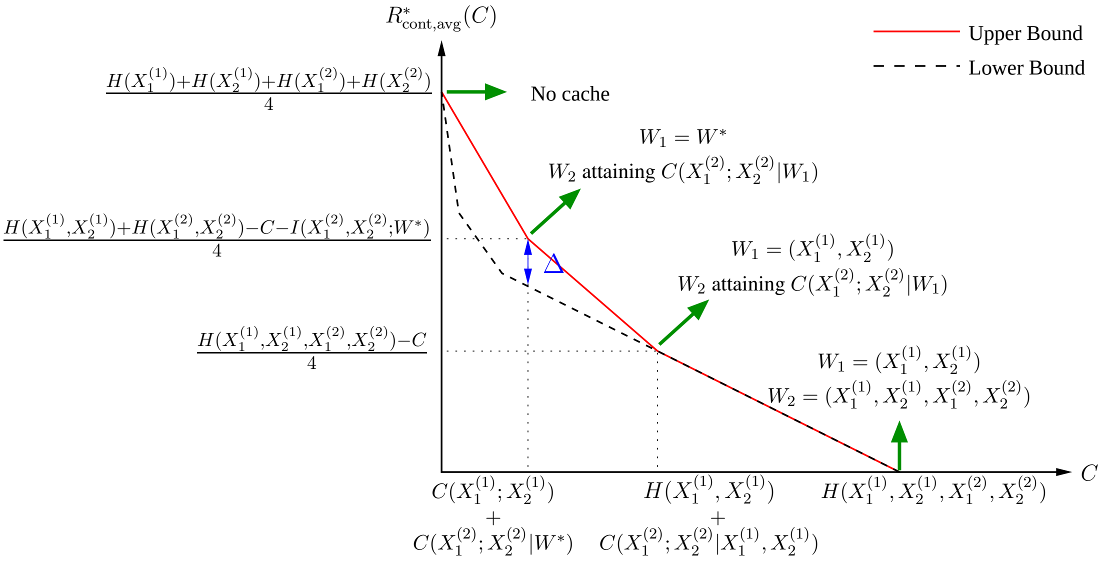


Figure 7.3. Bounds on the optimal average-case delivery rate function for arbitrarily correlated dynamic contents.

7.4 Discussion

In this chapter, we have introduced a new caching problem to capture the unpredictable nature of contents. As an answer to this dynamic caching problem, we have proposed to place cache in small increments through successive steps to address the modifications within the contents (if any). In particular, we have followed an information-theoretic approach considering a single user and we have established a single-letter characterization of the optimal tradeoff between the total cache rate and the average-case delivery rate in terms of an optimization problem. We have also presented a counterpart of this result for the worst-case delivery rate. For both cases, the explicit solution to the corresponding optimization problem is left as an open problem. Another open problem is to extend our results to an arbitrary number of users. This direction was investigated for the classical (static) caching setup in [6], in which the minimum average-case delivery rate was established only up to upper and lower bounds when there are multiple users in the network. A coding-theoretic approach building an algorithm for dynamic contents is also left as an open problem.

Acknowledgment

This chapter is, in part, a reprint of the material in the paper: Pinar Sen and Michael Gastpar, "Successive Refinement to Caching for Dynamic Content," *Proceedings of IEEE International Symposium on Information Theory*, Paris, France, June 2019. This chapter is, in part, currently being prepared for submission for publication of the material in *IEEE Transactions of Information Theory*, 2020 with authors Pinar Sen, Michael Gastpar, and Young-Han Kim. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] Y. Birk and T. Kol. Coding on demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients. *IEEE Trans. Inf. Theory*, 52(6):2825–2830, June 2006.

[2] M. A. Maddah-Ali and U. Niesen. Fundamental limits of caching. *IEEE Trans. Inf. Theory*, 60(5):2856–2867, May 2014.

[3] C. Wang, S. H. Lim, and M. Gastpar. Information-theoretic caching: Sequential coding for computing. *IEEE Transactions on Information Theory*, 62(11):6393–6406, Nov 2016.

[4] Chien-Yi Wang. *Function Computation over Networks Efficient Information Processing for Cache and Sensor Applications.* EPFL, Lausanne, 2015.

[5] R. M. Gray and A. D. Wyner. Source coding for a simple network. *Bell Syst. Tech. J.*, 53(9):1681–1721, 1974.

[6] S. H. Lim, C. Wang, and M. Gastpar. Information-theoretic caching: The multi-user case. *IEEE Trans. Inf. Theory*, 63(11):7018–7037, Nov 2017.

[7] P. Hassanzadeh, E. Erkip, J. Llorca, and A. Tulino. Distortion-memory tradeoffs in cache-aided wireless video delivery. In *Proc. 53th Ann. Allerton Conf. Comm. Control Comput.*, pages 1150–1157, Sep. 2015.

[8] Giel Op 't Veld and Michael C. Gastpar. Caching gaussians: Minimizing total correlation on the gray–wyner network. *Proceedings of the 50th Annual Conference on Information Systems and Sciences (CISS)*, page 6, 2016.

[9] Q. Yang and D. Gündüz. Centralized coded caching for heterogeneous lossy requests. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 405–409, July 2016.

[10] Q. Yang and D. Gündüz. Coded caching and content delivery with heterogeneous distortion requirements. *IEEE Trans. Inf. Theory*, 64(6):4347–4364, June 2018.

[11] R. Timo, S. Saeedi Bidokhti, M. Wigger, and B. C. Geiger. A rate-distortion approach to caching. *IEEE Trans. Inf. Theory*, 64(3):1957–1976, March 2018.

[12] P. Hassanzadeh, A. M. Tulino, J. Llorca, and E. Erkip. On coding for cache-aided delivery of dynamic correlated content. *IEEE J. Sel. Areas Commun.*, 36(8):1666–1681, Aug 2018.

Chapter 8

Successive Refinement to Caching for Dynamic Requests

This chapter introduces another new caching problem in which the user requests arise at any point of time possibly interrupting the cache placement phase (*dynamic requests*). To cope with the dynamic nature of the demands, a successive refinement approach is proposed: some partial information about file contents are cached in small increments through successive steps to satisfy delayed requests while guaranteeing to serve for earlier requests as well. Taking an information-theoretic approach, the optimal tradeoff among average-case delivery rates at different request times is characterized when the cache rate is above a well-defined threshold. For the class of i.i.d. Bern(1/2) contents and an arbitrary number of users, taking a coding-theoretic approach, a successive caching algorithm that achieves near-optimal average-case delivery rates simultaneously at every request time is developed. This algorithm is also shown to be uniformly near-optimal when the performance criterion is the worst-case delivery rates.

8.1 Introduction

Recently, coding-theoretic approaches were proposed to develop practical close-to-optimal codes for cache placement and content delivery. Breaking off from earlier studies [1, 2] that concentrated on optimizing either cache placement or content delivery while the other is fixed, Maddah-Ali and Niesen [3] proposed a coding scheme that optimizes both phases, achieving the optimal tradeoff among communication rates for cache placement and content delivery up to a constant multiplicative factor. In this pioneering work, each file is split into subfiles, where a set of properly chosen subfiles is cached at user devices and a set of linearly encoded subfiles is broadcast in the delivery phase. Following [3], extensive research effort was put into improving the multiplicative gap [4–8] and extending the results to heterogeneous cache sizes [9–12], to nonuniform file popularity [13–15], to correlated contents [16], and to dynamic contents that is modified after cache placement is completed [17].

As argued in Chapter 7 for information-theoretic approaches, all these existing caching problems studied from a coding-theoretic perspective also limits the cache placement to a single step, which falls short of capturing the unpredictable nature of demands in real networks. In this chapter, we introduce another new caching problem that addresses requests arising at any point of time possibly interrupting the cache placement phase (*dynamic requests*). To answer this dynamic caching problem, we propose a successive refinement approach to cache placement.

In particular, we formulate a caching problem for dynamic requests, in which the cache placement phase consists of an arbitrary number of successive steps and each step refines the cache content stored in prior steps for possible requests arising at that moment in time. First, taking an information-theoretic approach, we consider a single user and two time points at which the request can arise, and relate this problem to the successive Gray–Wyner network discussed in Chapter 6. We characterize the optimal tradeoff between the average-case delivery rates at different request times when the cache rate is above a well-defined threshold. Second, we consider a coding-theoretic version of the problem with an arbitrary number of users and a finite set of time points at which requests can arise, assuming the class of i.i.d. Bern(1/2) contents. For this setting, we develop a successive caching algorithm that can achieve average-case delivery rates that are uniformly within a constant multiplicative factor of their respective minima at every request time. Our algorithm is also uniformly near-optimal when the performance criterion is the *worst-case* delivery rates.

8.2 Problem Formulation

Formally, consider a server with a fixed number of N files $(X_1^n, X_2^n, \ldots, X_N^n)$ drawn i.i.d. from $p(x_1, x_2, \ldots, x_N)$ and K users, each with a cache rate of nC bits. As illustrated in Fig. 8.1, each user successively caches some information about the contents in T steps of increments. At step $t \in [T]$, additional information $L_t^{(k)}$ of rate C_t is stored in the local cache of user $k \in [K]$, where $C_1 + C_2 + \cdots + C_T = C$. A request can arise at any time point $t \in [T]$, the knowledge of which server does not have a priori. For a request arising at time point $t \in [T]$, denoted by the request vector $\mathbf{d} = [d_1 \ d_2 \ \ldots \ d_K] \in [N]^K$ where $d_k \in [N]$ corresponds to the request of user $k \in [K]$, server broadcasts some other information about the contents $M_{\mathbf{d},t}$ of rate $R_{\mathbf{d},t}$ to all users so that each user is able to recover the rest of its desired file.

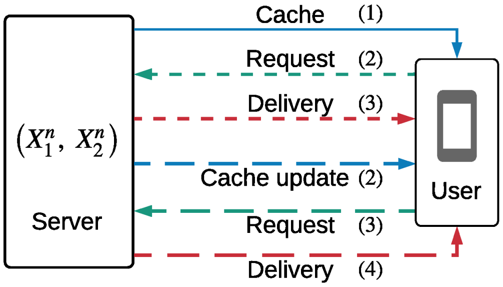


Figure 8.1. Caching for dynamic requests with $N = 2$ files, $K = 1$ user, and $T = 2$ successive steps: server first places some cache (1) based on the files (X_1^n, X_2^n). If a request arises at $T = 1$ (2), it delivers the required content for user to decode its desired file (3); otherwise, it continues with placing an update on the cache (2). If a request arises at $T = 2$ (3), server delivers the required content for user to decode its desired file (4).

An $\left(n, (nC_t, nR_{\mathbf{d},t})_{\mathbf{d}\in[N]^K, t\in[T]}\right)$ T-step successive caching scheme for dynamic requests consists of

- KT caching functions where

  $$\phi_t^{(k)} : \{0,1\}^{nN} \to \{0,1\}^{nC_t}$$

  maps the files $(X_1^n, X_2^n, \ldots, X_N^n)$ into a cache content

  $$L_t^{(k)} := \phi_t^{(k)}(X_1^n, X_2^n, \ldots, X_N^n)$$

  to be placed at user $k \in [K]$ during step t of the successive cache placement phase for $t \in [T]$,

- $N^K T$ encoding functions, where

  $$\psi_{\mathbf{d},t} : \{0,1\}^{nN} \to \{0,1\}^{nR_{\mathbf{d},t}}$$

  maps the files $(X_1^n, X_2^n, \ldots, X_N^n)$ to the delivery content

  $$M_{\mathbf{d},t} := \psi_{\mathbf{d},t}(X_1^n, X_2^n, \ldots, X_N^n)$$

  corresponding to the request vector $\mathbf{d} = [d_1 \ d_2 \ \ldots \ d_K] \in [N]^K$ received by the server at time point $t \in [T]$,

- KT decoding functions, where

  $$\mu_t^{(k)} : \{0,1\}^{n(\sum_{r=1}^{t} C_r)} \times \{0,1\}^{nR_{\mathbf{d},t}} \to \{0,1\}^n$$

  maps the cache contents placed until time point $t \in [T]$ and the delivery contents into an estimate

$$\hat{X}^n_{d_k,t} := \mu^{(k)}_t\big((L^{(k)}_i : i \in [t]), M_{\mathbf{d},t}\big)$$

of the requested file $X^n_{d_k}$ by user $k \in [K]$ when the request vector $\mathbf{d} \in [N]^K$ is received by the server at time point t.

The probability of error is defined as

$$P^{(n)}_e := \mathsf{P}(\hat{X}^n_{d_k,t} \neq X^n_{d_k} \text{ for some } t \in [T], k \in [K], d_k \in [N]).$$

Given a cache rate tuple $(C_1, C_2, \ldots, C_T)$, a delivery rate tuple $(R_{\mathbf{d},t})_{\mathbf{d}\in[N]^K, t\in[T]}$ is said to be *achievable for dynamic requests* if there exists an $\big(n, (nC_t, nR_{\mathbf{d},t})_{\mathbf{d}\in[N]^K, t\in[T]}\big)$ T-step successive caching scheme for dynamic requests with $\lim_{n\to\infty} P^{(n)}_e = 0$.

Remark 8.2.1. *One can distinguish the caching problem formulated above for dynamic requests with the extension of the classical caching problem to heterogeneous cache rates, which allows users utilize different amount of cache rates. In the heterogeneous caching problem [9, 11, 12], the goal is to minimize the delivery rate for the given heterogeneous cache rates. In our setting, on the other hand, every user stores the* same *amount of information until the request arises, which could happen at any point of time, and the goal is to simultaneously minimize the delivery rates corresponding to different request times.*

We are interested in the average delivery rates when the requested file tuple is uniformly at random among $[N]^K$. Formally, given a tuple of cache rates $(C_1, C_2, \ldots, C_T)$, a rate tuple $(R_t)_{t\in[T]}$ is said to be *average-case achievable for dynamic requests* if there exists a delivery rate tuple $(R_{\mathbf{d},t})_{\mathbf{d}\in[N]^K, t\in[T]}$ achievable for dynamic requests such that its average satisfies

$$\frac{1}{N^K} \sum_{\mathbf{d}\in[N]^K} R_{\mathbf{d},t} \leq R_t$$

for every $t \in [T]$.

Similarly, we look at worst-case delivery rates when the requested file tuple is arbitrary among $[N]^K$. Formally, given a tuple of cache rates $(C_1, C_2, \ldots, C_T)$, a rate tuple $(R_1, R_2, \ldots, R_T)$ is said to be *worst-case achievable for dynamic requests* if there exists a delivery rate tuple $(R_{\mathbf{d},t})_{\mathbf{d}\in[N]^K, t\in[T]}$ achievable for dynamic requests such that its maximum satisfies

$$\max_{\mathbf{d}\in[N]^K} R_{\mathbf{d},t} \leq R_t$$

for every $t \in [T]$.

In Section 8.3, we consider a simplified version of this dynamic request problem for a single user and two files to analyze the optimal tradeoff among the average-case achievable delivery rates. In Section 8.4, we continue with an arbitrary number of users and the class of i.i.d. Bern(1/2) files to propose a successive caching algorithm to simultaneously reduce the delivery rates and we characterize the performance of this algorithm in terms of both average-case and worst-case delivery rates.

8.3 Information-Theoretic Approach

We analyze the optimal tradeoff among the average-case achievable delivery rates for a single user ($K = 1$) and a pair of files ($N = 2$) X_1^n and X_2^n that are drawn i.i.d. from the pmf $p(x_1, x_2)$ over a finite alphabet. We first consider a request that is known to arise after utilizing all of the cache rate C, which is referred to as *static request* and corresponds to $T = 1$ in our dynamic setup. Define the optimal average-case delivery rate function for static requests as

$$\begin{aligned} R^*_{\text{req,avg}}(C) := \min\{R : R & \text{ is average-case achievable for static requests} \\ & \text{for a given cache rate } C\}, \end{aligned} \tag{8.1}$$

where the achievability for static requests is defined similarly by letting $T = 1$. This function captures the tradeoff between the utilized cache rate and the average delivery rate under the traditional caching problem and characterized by Wang, Lim, and Gastpar [18, 19] as follows.

Proposition 8.3.1 ([18, Proposition 3]). *The optimal average-case delivery rate function for static requests is*

$$\begin{aligned} R^*_{\text{req,avg}}(C) &= \min_{\substack{p(w|x_1,x_2):\\ I(X_1,X_2;W)\le C}} \frac{H(X_1|W)+H(X_2|W)}{2} \\ &= \frac{H(X_1,X_2)-C}{2} + \frac{1}{2} \min_{\substack{p(w|x_1,x_2):\\ I(X_1,X_2;W)=C}} I(X_1;X_2|W). \end{aligned} \tag{8.2}$$

In particular, for $C \ge C(X_1;X_2)$

$$R^*_{\text{req,avg}}(C) = \frac{H(X_1,X_2)-C}{2}.$$

Returning back to our dynamic model, assume now that user requests a file at one of the two possible time points ($T = 2$). As illustrated in Fig. 8.2, the request is dynamic in time in the sense that it is received either at $t = 1$ or at $t = 2$, which correspond to the time right after placing nC_1 and $n(C_1 + C_2)$ bits of cache, respectively. Depending on the realization d of *uniformly random* request $D \in [2]$ received at time point t, the server transmits $nR_{d,t}$ bits to deliver the remaining part of the requested file X^n_d. The question is whether the rate pair of $(R_1, R_2) = (R^*_{\text{req,avg}}(C_1), R^*_{\text{req,avg}}(C_1 + C_2))$ is average-case achievable for dynamic requests. Note that the problem is not trivial since a successive caching scheme that is optimal at the first and the second intermediate step may not achieve $R^*_{\text{req,avg}}(C_1 + C_2)$, which is obtained by optimizing over two steps combined. We next present a sufficient condition on the cache rates to simultaneously achieve these lower bounds.

Theorem 8.3.1. *Given $C_1 > 0$, let W^* denote the random variable defined by the*

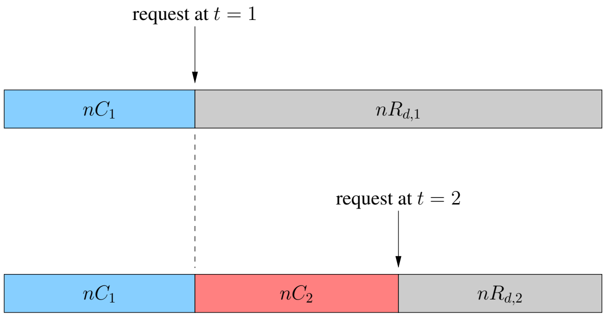


Figure 8.2. Caching for dynamic requests from user perspective: server first places nC_1 bits into the cache of user and checks if request arises. If it does, server delivers $nR_{d,1}$ bits so that user can decode its requested file. Otherwise, server places nC_2 more bits into the cache of user and waits for the request, after which it delivers $nR_{d,2}$ so that user can decode its requested file.

conditional pmf $p(w^*|x_1, x_2)$ that attains $R^*_{\text{req,avg}}(C_1)$ in (8.2) and let $C(X_1; X_2|W^*)$ be the conditional Wyner common information defined in (6.8). For every $C_1 > 0$ and $C_2 \geq C(X_1; X_2|W^*)$, a rate pair (R_1, R_2) is average-case achievable for dynamic requests if

$$R_1 \geq R^*_{\text{req,avg}}(C_1), \tag{8.3a}$$

$$R_2 \geq R^*_{\text{req,avg}}(C_1 + C_2). \tag{8.3b}$$

Conversely, for every $C_1, C_2 > 0$, if a rate pair (R_1, R_2) is average-case achievable for dynamic requests, then it must satisfy (8.3).

Proof. The converse follows from the operational definition. Intuitively, the performance of a successive caching strategy for dynamic requests is bounded below by the static caching strategies each of which is individually optimized for the corresponding cache rate and request time. We next show that under the given sufficient condition on the cache rates, these lower bounds can be attained simultaneously. To prove this, once again, we benefit from the successive Gray–Wyner network in Fig. 6.2, which also captures the dynamic request problem when we set $(X^n_{1,1}, X^n_{2,1}) = (X^n_{1,2}, X^n_{2,2}) = (X^n_1, X^n_2)$ with i.i.d. elements drawn from the pmf $p(x_1, x_2)$. Consequently, a rate tuple $(C_1, R_{1,1}, R_{2,1}, C_2, R_{1,2}, R_{2,2})$ is achievable for dynamic requests if and only if it is in the optimal rate region of the successive Gray–Wyner network evaluated for $p := p(x_1,x_2)\mathbf{1}_{\{(x_1^{(2)},x_2^{(2)})=(x_1,x_2)\}}$, which will be referred to as $\mathscr{R}(p)$. Therefore, given a pair of cache rates (C_1,C_2), a rate pair (R_1,R_2) is average-case achievable for dynamic requests if and only if there exists $(C_1,R_{1,1},R_{2,1},C_2,R_{1,2},R_{2,2}) \in \mathscr{R}(p)$ such that

$$\frac{R_{1,1}+R_{2,1}}{2} \leq R_1$$

and

$$\frac{R_{1,2}+R_{2,2}}{2} \leq R_2.$$

Now, given $C_1 > 0$, let $p_{W^*|X_1,X_2}(w|x_1,x_2)$ denote the pmf attaining $R^*_{\text{req,avg}}(C_1)$, which directly implies

$$I(X_1,X_2;W^*) = C_1. \tag{8.4}$$

Suppose that $C_2 \geq C(X_1;X_2|W^*)$. We let $W_1 = W^*$. It then suffices to show that there exist a conditional pmf $p_{W_2|W_1,X_1,X_2}(w_2|w_1,x_1,x_2)$ such that

$$I(X_1,X_2;W_2|W_1) = C_2$$

and

$$\frac{H(X_1|W_1,W_2)+H(X_2|W_1,W_2)}{2} \leq R^*_{\text{req,avg}}(C_1+C_2), \tag{8.5}$$

from which the claim follows by Theorem 6.3.1 and letting $R_{j,1} = H(X_j|W_1)$ and $R_{j,2} = H(X_j|W_1,W_2)$ for $j = 1,2$.

Consider now the conditional pmf

$$p_{W_2|W_1,X_1,X_2}(w_2|w_1,x_1,x_2) = \begin{cases} p_{W_2^*|W_1,X_1,X_2}(w_2|w,x_1,x_2) & \text{with probability } \gamma \\ \mathbf{1}_{\{w_2=(x_1,x_2)\}} & \text{with probability } 1-\gamma \end{cases}, \tag{8.6}$$

where $p_{W_2^*|W_1,X_1,X_2}(w_2|w_1,x_1,x_2)$ attains the conditional Wyner common information

$C(X_1;X_2|W_1)$ defined in (6.8) and $\gamma \in [0,1]$ is chosen such that

$$I(X_1,X_2;W_2|W_1) = \gamma C(X_1;X_2|W_1) + (1-\gamma)H(X_1,X_2|W_1) = C_2, \tag{8.7}$$

which is always possible since $C_2 \geq C(X_1;X_2|W_1)$ by our assumption and

$$C_2 \leq H(X_1,X_2) - C_1 = H(X_1,X_2|W_1)$$

by (8.4). Now, we verify (8.5) by using the conditional pmf in (8.6).

$$\begin{aligned}
&\frac{H(X_1|W_1,W_2) + H(X_2|W_1,W_2)}{2} \\
&= \frac{H(X_1,X_2|W_1) - I(X_1,X_2;W_2|W_1) + I(X_1;X_2|W_1,W_2)}{2} \\
&\overset{(a)}{=} \frac{H(X_1,X_2) - C_1 - C_2}{2} \\
&\overset{(b)}{\leq} R^*_{\text{req,avg}}(C_1 + C_2),
\end{aligned}$$

where (a) follows by (8.4) and (8.7), and by the fact that

$$I(X_1;X_2|W_1,W_2) = 0,$$

and (b) follows by Proposition 8.3.1. □

Theorem 8.3.1 implies that if the user is equipped with sufficiently large memory left for the cache refinement, then the problem of dynamic requests can be handled as well as two separate problems of static requests. We next relax the sufficient condition on the cache rate for the refinement, C_2, and put the burden on the amount of cache placed at the first step.

Corollary 8.3.1. *For every $C_1 \geq C(X_1;X_2)$ and $C_2 \geq 0$, a rate pair (R_1,R_2) is average-case achievable for dynamic requests if and only if it satisfies (8.3).*

Proof. It suffices to prove the achievability. Note that for a given conditional pmf $p(w|x_1, x_2)$ such that $X_1 \to W \to X_2$ form a Markov chain, the conditional Wyner common information $C(X_1; X_2|W)$ is zero by definition since

$$C(X_1; X_2|W) = \min_{\substack{p_{V|W,X_1,X_2}(v|w,x_1,x_2) \\ I(X_1;X_2|W,V)=0}} I(X_1, X_2; V|W) = 0$$

is attained by letting $V = \emptyset$. If $C_1 \geq C(X_1; X_2)$ in Theorem 8.3.1, the conditional pmf $p(w^*|x_1, x_2)$ that attains $R^*_{\text{req,avg}}(C_1)$ satisfies $I(X_1; X_2|W^*) = 0$ by Proposition 8.3.1. Therefore, the conditional Wyner common information $C(X_1; X_2|W^*) = 0$, from which the result follows. □

Inspired from Corollary 8.3.1, we consider independent files in the proceeding example, where we have the full characterization of the average-case achievable rate pairs for dynamic requests.

Example 8.3.1 (Independent files). *If $p(x_1, x_2) = p(x_1)p(x_2)$, then the Wyner common information between X_1 and X_2 is $C(X_1; X_2) = 0$. Therefore, by Corollary 8.3.1, for* every *given $C_1, C_2 \geq 0$, a rate pair (R_1, R_2) is average-case achievable for dynamic requests if and only if it satisfies*

$$\begin{aligned} R_1 &\geq R^*_{\text{req,avg}}(C_1) = \frac{H(X_1) + H(X_2) - C_1}{2}, \\ R_2 &\geq R^*_{\text{req,avg}}(C_1 + C_2) = \frac{H(X_1) + H(X_2) - C_1 - C_2}{2}. \end{aligned}$$

For a given memory pair (C_1, C_2), the set of average-case achievable rate pairs for dynamic requests is demonstrated in Fig. 8.3.

Remark 8.3.1. *For independent files, it is easy to extend the single-letter characterization of the average-case achievable rate pairs for dynamic requests that arise at one of the two time points ($T = 2$) to an arbitrary number of time points. One can follow similar arguments starting from the successive Gray–Wyner network and utilizing its optimal*

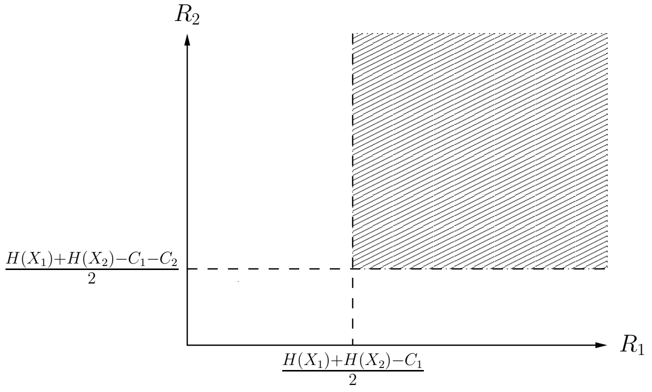


Figure 8.3. The set of average-case achievable rate pairs for dynamic requests of independent files.

rate region for the dynamic caching problem to obtain that for every $C_1, C_2, \dots C_T \geq 0$, a rate tuple $(R_1, R_2, \dots, R_T)$ is average-case achievable for dynamic requests if and only if it satisfies

$$R_t \geq R^*_{\text{req,avg}}(C_1 + C_2 + \cdots + C_t) = \frac{H(X_1) + H(X_2) - \sum_{r=1}^{t} C_r}{2}$$

for every $t \in [T]$. Such an extension for arbitrarily correlated files is left as an open problem.

8.4 Coding-Theoretic Approach

We propose a successive caching algorithm to simultaneously reduce the delivery rates for an arbitrary number N of files and K of users. We concentrate on independent files, each of which is i.i.d. Bern(1/2). For the simplicity of the notation, we denote the file X^n as $\mathbf{X}$ for the rest of this section. Similar to Section 8.3, we start with revisiting the problem of static requests ($T = 1$) from a coding-theoretic perspective studied by [3, 6]. Let the optimal average-case delivery rate function for static requests $R^*_{\text{req,avg}}(C)$ be defined as in (8.1) for K users and N files i.i.d. with respect to Bern(1/2). Similarly, define the optimal worst-case delivery rate function for static requests as

$$R^*_{\text{req,worst}}(C) := \min\{R : R \text{ is worst-case achievable for static requests for a given cache rate } C\}. \tag{8.8}$$

To present an upper bound on $R^*_{\text{req,avg}}(C)$ and $R^*_{\text{req,worst}}(C)$, we define $R(\mathbf{d}, C)$ as the lower convex envelope of

$$\frac{\binom{K}{KC/N+1} - \binom{K-|\text{supp}(\mathbf{d})|}{KC/N+1}}{\binom{K}{KC/N}}, \tag{8.9}$$

for $C \in \{0, N/K, 2N/K, \dots, N\}$, where $|\text{supp}(\mathbf{d})|$ denotes the number of distinct elements in the request vector $\mathbf{d}$. We also define function $R_{\text{avg}}(C)$ as

$$R_{\text{avg}}(C) := \mathsf{E}_{\mathbf{D}}[R(\mathbf{D}, C)], \tag{8.10}$$

where the expectation is taken with respect to the request vector $\mathbf{D}$ that is uniformly random among $[N]^K$. Note that $R_{\text{avg}}(C)$ can be expressed as the lower convex envelope of

$$\mathsf{E}_{\mathbf{D}}\left[\frac{\binom{K}{KC/N+1} - \binom{K-|\text{supp}(\mathbf{D})|}{KC/N+1}}{\binom{K}{KC/N}}\right]$$

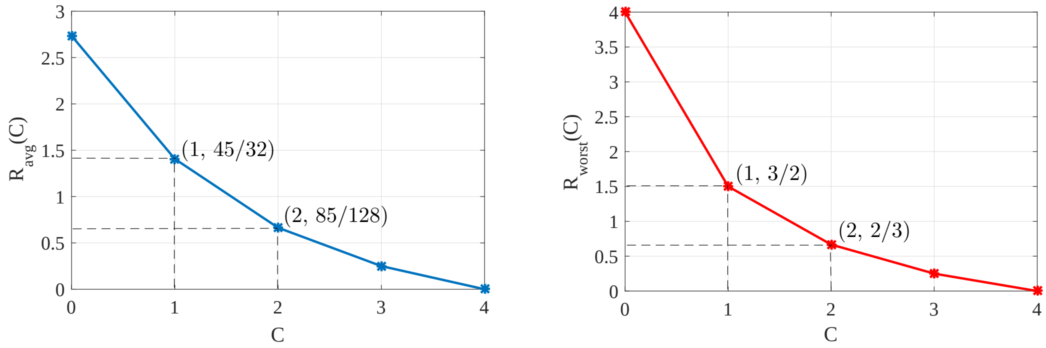
for $C \in \{0, N/K, 2N/K, \dots, N\}$. Similarly, we define function $R_{\text{worst}}(C)$ as

$$R_{\text{worst}}(C) := \max_{\mathbf{d} \in [N]^K} R(\mathbf{d}, C), \tag{8.11}$$

which can be expressed as the lower convex envelope of

$$\frac{\binom{K}{KC/N+1} - \binom{K-\min\{K,N\}}{KC/N+1}}{\binom{K}{KC/N}}$$

for $C \in \{0, N/K, 2N/K, \dots, N\}$. Fig. 8.4 demonstrates the functions $R_{\text{avg}}(C)$ and $R_{\text{worst}}(C)$ for $(K, N) = (4, 4)$.



(a) Average-case. **(b)** Worst-case.

Figure 8.4. Demonstration of the functions $R_{\text{avg}}(C)$ and $R_{\text{worst}}(C)$ for $K = 4$ users and $N = 4$ files.

The following results by [6, 7] present upper bounds on the optimal values of $R^*_{\text{req,avg}}(C)$ and $R^*_{\text{req,worst}}(C)$, and characterizes their gap to the respective optimal.

Proposition 8.4.1 ([6,7])**.** *For N files and K users each equipped with a cache rate of $C \leq N$,*

$$1 \leq \frac{R_{\text{avg}}(C)}{R^*_{\text{req,avg}}(C)} \leq 2.00884.$$

and

$$1 \leq \frac{R_{\text{worst}}(C)}{R^*_{\text{req,worst}}(C)} \leq 2.00884.$$

We are now ready to present the main result of this section, which generalizes the previous works for $T \geq 2$.

Theorem 8.4.1. *For N files, K users, and given a tuple of cache rates $(C_1, C_2, \ldots, C_T)$, a rate tuple $(R_1, R_2, \ldots, R_T)$ is average-case achievable for dynamic requests if*

$$R_t \geq R_{\text{avg}}(C_1 + C_2 + \cdots + C_t) \tag{8.12}$$

for every $t \in [T]$. Conversely, if a rate tuple $(R_1, R_2, \ldots, R_T)$ is average-case achievable for dynamic requests, then it must satisfy

$$R_t \geq \frac{R_{\text{avg}}(C_1 + C_2 + \cdots + C_t)}{2.00884} \tag{8.13}$$

for every $t \in [T]$. Similarly, a rate tuple $(R_1, R_2, \ldots, R_T)$ is worst-case achievable for dynamic requests if

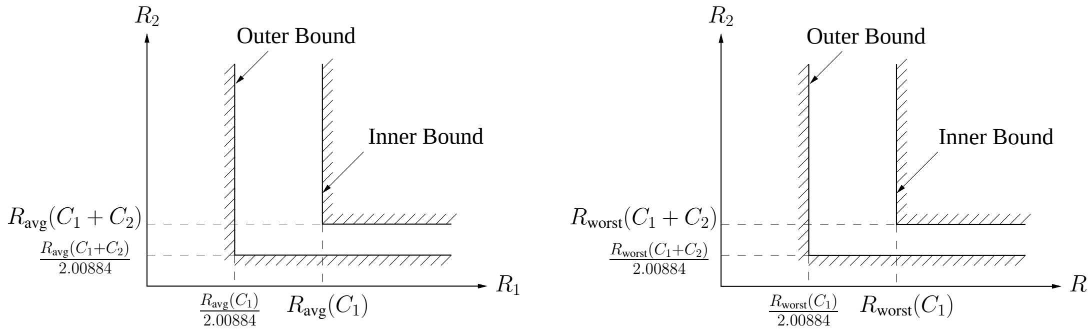
$$R_t \geq R_{\text{worst}}(C_1 + C_2 + \cdots + C_t) \tag{8.14}$$

for every $t \in [T]$. Conversely, if a rate tuple $(R_1, R_2, \ldots, R_T)$ is worst-case achievable for dynamic requests, then it must satisfy

$$R_t \geq \frac{R_{\text{worst}}(C_1 + C_2 + \cdots + C_t)}{2.00884} \tag{8.15}$$

for every $t \in [T]$.

The inner and outer bounds on the achievable rate pairs for dynamic requests established in Theorem 8.4.1 are illustrated in Fig. 8.5 for $T = 2$.


R_2
Outer Bound
Inner Bound
$R_{\text{avg}}(C_1 + C_2)$
$\frac{R_{\text{avg}}(C_1+C_2)}{2.00884}$
R_1
$\frac{R_{\text{avg}}(C_1)}{2.00884}$
$R_{\text{avg}}(C_1)$
R_2
Outer Bound
Inner Bound
$R_{\text{worst}}(C_1 + C_2)$
$\frac{R_{\text{worst}}(C_1+C_2)}{2.00884}$
R_1
$\frac{R_{\text{worst}}(C_1)}{2.00884}$
$R_{\text{worst}}(C_1)$

(a) Average-case.

(b) Worst-case.

Figure 8.5. The inner and outer bounds on the achievable rate pairs for dynamic requests in Theorem 8.4.1.

Proof of Theorem 8.4.1. We start with the converse. For every given cache rate tuple $(C_t)_{t=1}^T$, if a rate tuple $(R_1, R_2, \ldots, R_T)$ is average-case achievable for dynamic requests, then it must satisfy

$$\begin{aligned} R_t &\overset{(a)}{\geq} R^*_{\text{req,avg}}(C_1 + C_2 + \ldots + C_t) \\ &\overset{(b)}{\geq} \frac{R_{\text{avg}}(C_1 + C_2 + \ldots + C_t)}{2.00884} \end{aligned}$$

for every $t \in [T]$, where (a) follows by operational definition and (b) follows by Proposition 8.4.1. In words, the delivery rate R_t at step t of the successive caching scheme cannot be lower than the delivery rate minimized knowing a priori that a total amount of $(C_1 + C_2 + \ldots + C_t)$ information is cached before the delivery. By similar arguments, it is easy to see the converse for the worst-case delivery rates.

For the achievability, we provide a successive caching algorithm that can attain a delivery rate of $R(\mathbf{d}, \sum_{r=1}^{t} C_r)$ when the request $\mathbf{d} \in [N]^K$ arises at the successive step $t \in [T]$. We first prove this claim assuming that $T = K$ and $C_t = \frac{N}{K}$ for every $t \in [K]$. We then extend our proof to an arbitrary tuple of $(C_t)_{t=1}^{T}$ by using a *memory sharing* argument accommodating the successive nature of the cache placement.

Suppose now that $T = K$ and $C_t = \frac{N}{K}$ for every $t \in [K]$. The cache placement is performed successively on T steps. In the first step, file $\mathbf{X}_j$, $j \in [N]$, is split into K disjoint subfiles of equal size to be cached at different users. The subfiles of file $\mathbf{X}_j$ after splitting are labeled as $(\mathbf{X}_j)_{(i_1)}, i_1 \in [K]$, and the subfile $(\mathbf{X}_j)_{(i_1)}$ is cached at user i_1. In the second step, subfile $(\mathbf{X}_j)_{(i_1)}, j \in [N], i_1 \in [K]$, is further split into $(K-1)$ disjoint subfiles of equal size to be cached at the users except user i_1. Using a similar notation, subfiles of $(\mathbf{X}_j)_{(i_1)}$ formed in the second step are labeled as $(\mathbf{X}_j)_{(i_1,i_2)}, i_2 \in [K]\backslash\{i_1\}$, and the subfile $(\mathbf{X}_j)_{(i_1,i_2)}$ is cached at user i_2 in the second step. Repeating this procedure successively, at step $t \in [T]$, subfile $(\mathbf{X}_j)_{(i_1,i_2,\ldots,i_{t-1})}$ for every $j \in [N]$ and every ordered subset $(i_1, i_2, \ldots, i_{t-1})$ of $[K]$, is further split into $(K - t + 1)$ disjoint subfiles of equal size to be cached at the users that do not have access to $(\mathbf{X}_j)_{(i_1,i_2,\ldots,i_{t-1})}$. Subfiles after this splitting are labeled as

$$(\mathbf{X}_j)_{(i_1,i_2,\ldots,i_{t-1},i_t)}, \quad i_t \in [K] \setminus \{i_1, i_2, \ldots, i_{t-1}\},$$

each of which has the rate of $\prod_{r=1}^{t} \frac{1}{K-r+1}$, and the subfile $(\mathbf{X}_j)_{(i_1,i_2,\ldots,i_t)}$ is cached at user i_t at step t. The content cached at user $k \in [K]$ during step t of the successive cache placement is then written as

$$L_t^{(k)} = \big((\mathbf{X}_j)_{(\sigma(\mathcal{S}),k)} : \mathcal{S} \subset [K] \setminus k \text{ such that } |\mathcal{S}| = t-1, \sigma \in \Sigma_{t-1}, j \in [N]\big)$$

and has the rate of

$$N\binom{K-1}{t-1}(t-1)!\frac{1}{K(K-1)\cdots(K-t+1)} = \frac{N}{K} = C_t,$$

which satisfies the given cache rate. To see the total cache rate utilized at the end of step t, note that the subfile $(\mathbf{X}_j)_{(i_1,i_2,\ldots,i_{t-1},i_t)}$ is cached at user k if and only if $k \in \{i_1, i_2, \ldots, i_t\}$. Therefore, at the end of step t, each user utilizes a total cache rate of

$$N\binom{K-1}{t-1}t!\frac{1}{K(K-1)\cdots(K-t+1)} = \frac{tN}{K} = \sum_{r=1}^{t} C_r,$$

as claimed.

Suppose now that the request vector $\mathbf{d} = [d_1\ d_2\ \ldots\ d_K] \in [N]^K$ is received by the server at step $t \in [T]$. For the content delivery corresponding to this request, we utilize the delivery scheme in [6] by relabeling the subfiles in accordance with our new cache placement scheme. Server first chooses a set of $|\text{supp}(\mathbf{d})|$ users, denoted by $\mathcal{U}(\mathbf{d})$, such that every user within this set requests different files. These users will be referred to as *leaders*. For a positive integer t, let Σ_t denote the set of all permutations over $[t]$. For a permutation $\sigma \in \Sigma_t$ and a set $\mathcal{S}$ of size t over integers, let $\sigma(\mathcal{S})$ denote the sequence obtained by applying the permutation σ to the ascending order of set $\mathcal{S}$. For every subset $\mathcal{S} \subset [K]$ such that $|\mathcal{S}| = t+1$ and $\mathcal{S} \cap \mathcal{U}(\mathbf{d}) \neq \emptyset$, and for every permutation $\sigma \in \Sigma_t$, server then broadcasts the linear combination

$$\mathbf{Y}_{\sigma,\mathcal{S}} := \bigoplus_{s\in\mathcal{S}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{S}\setminus\{s\})}, \tag{8.16}$$

which has the rate of $\prod_{r=1}^{t} \frac{1}{K-r+1}$. The delivery content is then written as

$$M_{\mathbf{d},t} = \Big\{ \mathbf{Y}_{\sigma,\mathcal{S}} : \mathcal{S} \subset [K] \text{ such that } \mathcal{S} \cap \mathcal{U}(\mathbf{d}) \neq \emptyset \text{ and } |\mathcal{S}| = t+1, \sigma \in \Sigma_t \Big\} \tag{8.17}$$

and has the rate of

$$\begin{aligned} R_{\mathbf{d},t} &= \left[\binom{K}{t+1} - \binom{K - |\mathrm{supp}(\mathbf{d})|}{t+1} \right] t! \prod_{r=1}^{t} \frac{1}{K-r+1} \\ &= \frac{\binom{K}{t+1} - \binom{K-|\mathrm{supp}(\mathbf{d})|}{t+1}}{\binom{K}{t}} = R(\mathbf{d}, tN/K). \end{aligned}$$

These cache placement and delivery steps are summarized in Algorithm 1. It remains to show that every user can recover its desired file from the delivery content in (8.17). Let $u \in \mathcal{U}(\mathbf{d})$ be a leader user. We start with proving that user u can recover file $\mathbf{X}_{d_u}$ by similar arguments to [3, 6]. For every $\mathcal{T} \subset [K] \setminus \{u\}$ such that $|\mathcal{T}| = t$ and for every permutation $\sigma \in \Sigma_t$,

$$\mathbf{Y}_{\sigma,\mathcal{T}\cup\{u\}} = (\mathbf{X}_{d_u})_{\sigma(\mathcal{T})} \oplus \bigoplus_{s \neq u \in \mathcal{T}\cup\{u\}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{T}\cup\{u\}\setminus\{s\})} \tag{8.18}$$

is among the broadcasted linear combination. Since every subfile $(\mathbf{X}_{d_s})_{\sigma(\mathcal{T}\cup\{u\}\setminus\{s\})}$ for $s \neq u$ is already cached at user u, it is easy to see from (8.18) that user u can recover $(\mathbf{X}_{d_u})_{\sigma(\mathcal{T})}$. It then follows that user u is able to recover all subfiles of the form

$$\{(\mathbf{X}_{d_u})_{\sigma(\mathcal{T})} : \mathcal{T} \subset [K] \setminus \{u\} \text{ such that } |\mathcal{T}| = t, \sigma \in \Sigma_t\}$$

of its requested file $\mathbf{X}_{d_u}$. With the remaining subfiles already available in its cache, user u can completely recover its requested file $\mathbf{X}_{d_u}$. We now consider *non-leader* users and provide computationally more efficient decoding approach than [6], answering the open problem stated in [6, Remark 10]. Let $a \in [K] \setminus \mathcal{U}(\mathbf{d})$ be a non-leader user with the request $d_a = d_u$ for a leader user $u \in \mathcal{U}(\mathbf{d})$. Note that for every $\mathcal{T} \subset [K] \setminus \{a\}$ such that

$|\mathcal{T}| = t$ and $\mathcal{T} \cap \mathcal{U}(\mathbf{d}) \neq \emptyset$, and for every permutation $\sigma \in \Sigma_t$,

$$\mathbf{Y}_{\sigma, \mathcal{T} \cup \{a\}} = (\mathbf{X}_{d_u})_{\sigma(\mathcal{T})} \oplus \bigoplus_{s \neq a \in \mathcal{T} \cup \{a\}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{T} \cup \{a\} \setminus \{s\})} \tag{8.19}$$

is among the broadcasted linear combination. Since every subfile $(\mathbf{X}_{d_u})_{\sigma(\mathcal{T} \cup \{a\} \setminus \{s\})}$ for $s \neq a$ is already cached at user a, it is easy to see from (8.19) that user a can recover $(\mathbf{X}_{d_u})_{\sigma(\mathcal{T})}$. It then follows that user a is able to recover all subfiles of the form

$$\{(\mathbf{X}_{d_u})_{\sigma(\mathcal{T})} : \mathcal{T} \subset [K] \setminus \{a\} \text{ such that } |\mathcal{T}| = t \text{ and } \mathcal{T} \cap \mathcal{U}(\mathbf{d}) \neq \emptyset, \sigma \in \Sigma_t\}. \tag{8.20}$$

The rest of the subfiles of file $\mathbf{X}_{d_u}$ is either cached at user a or is of the form of $(\mathbf{X}_{d_u})_{\sigma(\mathcal{A})}$ for some set $\mathcal{A} \subset [K] \setminus \{a\}$ such that $|\mathcal{A}| = t$ and $\mathcal{A} \cap \mathcal{U}(\mathbf{d}) = \emptyset$, and for some permutation $\sigma \in \Sigma_t$. For the second type of subfiles, we need the following lemma, the proof of which is deferred to Appendix 8.A.

Lemma 8.4.1. *Given a leader user $u \in \mathcal{U}(\mathbf{d})$ and a set $\mathcal{A} \subset [K] \setminus \{a\}$ such that $|\mathcal{A}| = t$ and $\mathcal{A} \cap \mathcal{U}(\mathbf{d}) = \emptyset$, define the set of users within $\mathcal{A}$ that does not request file d_u as*

$$\mathcal{A}_{u^c} := \{z \in \mathcal{A} : d_z \neq d_u\},$$

define the family of subsets of $\mathcal{A}_{u^c}$ that requests different files as

$$\mathcal{F}(\mathcal{A}_{u^c}) = \{\mathcal{V} \subset \mathcal{A}_{u^c} : d_y \neq d_z \ \forall y, z \in \mathcal{V}, y \neq z\},$$

and define the set of leader users covering the request span of $\mathcal{V} \in \mathcal{F}(\mathcal{A}_{u^c})$ as

$$\mathcal{U}(\mathcal{V}) = \{u \in \mathcal{U}(\mathbf{d}) : d_u = d_v \text{ for some } v \in \mathcal{V}\}.$$

Then, for every permutation $\sigma \in \Sigma_t$,

$$\bigoplus_{\mathcal{V} \in \mathcal{F}(\mathcal{A}_{u^c})} \mathbf{Y}_{\sigma,(\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus \mathcal{V}} = \bigoplus_{\mathcal{V} \subset \mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{\substack{v \in \mathcal{A} \cup \{u\}: \\ d_v = d_u}} (\mathbf{X}_{d_u})_{\sigma((\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus (\mathcal{V} \cup \{v\}))}. \tag{8.21}$$

We now show that for every $\mathcal{A} \subset [K] \setminus \{a\}$ such that $|\mathcal{A}| = t$ and $\mathcal{A} \cap \mathcal{U}(\mathbf{d}) = \emptyset$, and for every $\sigma \in \Sigma_t$, user a can recover $(\mathbf{X}_{d_u})_{\sigma(\mathcal{A})}$ from

$$\bigoplus_{\mathcal{V} \in \mathcal{F}(\mathcal{A}_{u^c})} \mathbf{Y}_{\sigma,(\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus \mathcal{V}}, \tag{8.22}$$

which can be computed from the delivery content since $\mathbf{Y}_{\sigma,(\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus \mathcal{V}}$ is among the broadcasted linear combinations. By Lemma 8.4.1, (8.22) can be rewritten as

$$\begin{aligned}
&\bigoplus_{\mathcal{V} \in \mathcal{F}(\mathcal{A}_{u^c})} \mathbf{Y}_{\sigma,(\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus \mathcal{V}} \\
&= \bigoplus_{\mathcal{V} \subset \mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{\substack{v \in \mathcal{A} \cup \{u\}: \\ d_v = d_u}} (\mathbf{X}_{d_u})_{\sigma((\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus (\mathcal{V} \cup \{v\}))} \\
&= \bigoplus_{\substack{v \in \mathcal{A} \cup \{u\}: \\ d_v = d_u}} (\mathbf{X}_{d_u})_{\sigma((\mathcal{A} \cup \{u\}) \setminus \{v\})} \oplus \bigoplus_{\substack{\mathcal{V} \subset \mathcal{F}(\mathcal{A}_{u^c}) \\ \mathcal{V} \neq \emptyset}} \bigoplus_{\substack{v \in \mathcal{A} \cup \{u\}: \\ d_v = d_u}} (\mathbf{X}_{d_u})_{\sigma((\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus (\mathcal{V} \cup \{v\}))} \\
&= (\mathbf{X}_{d_u})_{\sigma(\mathcal{A})} \oplus \bigoplus_{\substack{v \in \mathcal{A}: \\ d_v = d_u}} (\mathbf{X}_{d_u})_{\sigma((\mathcal{A} \cup \{u\}) \setminus \{v\})} \oplus \bigoplus_{\substack{\mathcal{V} \subset \mathcal{F}(\mathcal{A}_{u^c}) \\ \mathcal{V} \neq \emptyset}} \bigoplus_{\substack{v \in \mathcal{A} \cup \{u\}: \\ d_v = d_u}} (\mathbf{X}_{d_u})_{\sigma((\mathcal{A} \cup \{u\} \cup \mathcal{U}(\mathcal{V})) \setminus (\mathcal{V} \cup \{v\}))}.
\end{aligned} \tag{8.23}$$

Since every term in (8.23) except the first one is of the form of (8.20), user a has already recovered them. Therefore, it can recover the desired subfile $(\mathbf{X}_{d_u})_{\sigma(\mathcal{A})}$ by canceling out those previously recovered terms. Since the set $\mathcal{A}$ and user a are arbitrary, it follows that nonleader users can also recover their requested files from the delivery content in (8.17).

We can remove the assumptions on the cache rates as follows. Suppose we are given an arbitrary, positive tuple of cache rates $(C_1, C_2, \ldots, C_T)$. For every $t \in [T]$, we decompose the total utilized cache rate until the end of step t as

$$\sum_{r=1}^{t} C_r = z_t \frac{N}{K} + \alpha_t \frac{N}{K}, \tag{8.24}$$

for $z_t \in \mathbb{Z}^+$ and $\alpha_t \in [0,1]$, where z_t denotes the integer multiple of N/K that is closest to $\sum_{r=1}^{t} C_r$ from below, and α_t denotes the remaining fraction. At the end of step $t \in [T]$ of the successive cache placement, following similar steps to Algorithm 1, the cache of user $u \in [K]$ includes the subfiles

$$(\mathbf{X}_j)_{\sigma(\mathcal{S})}, \quad \mathcal{S} \subset [K] \text{ such that } u \in \mathcal{S} \text{ and } |\mathcal{S}| = z_t, \sigma \in \Sigma_{z_t}, j \in [N],$$

as well as the first α_t fraction of the subfiles

$$(\mathbf{X}_j)_{(\sigma(\mathcal{S}'),u)}, \quad \mathcal{S}' \subset [K] \text{ such that } u \notin \mathcal{S}' \text{ and } |\mathcal{S}'| = z_t, \sigma \in \Sigma_{z_t}, j \in [N].$$

Upon receiving the request vector $\mathbf{d} \in [N]^K$ at step $t \in [T]$ for a total utilized cache rate in the form of (8.24), server utilizes time sharing between the two delivery contents corresponding to the cache rates $(z_t+1)N/K$ and $z_t N/K$, respectively, resulting in a delivery rate of

$$R_{\mathbf{d},t} = \alpha_t \frac{\binom{K}{z_t+2} - \binom{K-|\mathrm{supp}(\mathbf{d})|}{z_t+2}}{\binom{K}{z_t+1}} + (1-\alpha_t)\frac{\binom{K}{z_t+1} - \binom{K-|\mathrm{supp}(\mathbf{d})|}{z_t+1}}{\binom{K}{z_t}} = R(\mathbf{d}, \sum_{r=1}^{t} C_r). \tag{8.25}$$

Finally, the achievability of $R_{\mathrm{avg}}(\sum_{r=1}^{t} C_r)$ for the average-case delivery rates follows by taking the expectation of (8.25) with respect to uniformly random request vector. Similarly, the achievability of $R_{\mathrm{worst}}(\sum_{r=1}^{t} C_r)$ for the worst-case delivery rates follows by taking the maximum of (8.25) over arbitrary request vector.

□

We next present an example to illustrate the algorithm.

Example 8.4.1. *Consider a network of $K = 4$ users and a server of $N = 4$ files.*

Algorithm 1 Successive caching for dynamic requests assuming $C_t = N/K$, $\forall t \in [K]$.

```
for $j = 1 : N$ do
    $(\mathbf{X}_j)_{()} \leftarrow \mathbf{X}_j$                                        ▷ initialization
end for
RequestBit $\leftarrow 0$
$t \leftarrow 1$
while RequestBit $= 0$ and $t \leq K$ do
    for $j = 1 : N$, $\sigma \in \Sigma_{t-1}$ do
        for $\mathcal{S} \subset [K], |\mathcal{S}| = t-1$ do
            Split the subfile $(\mathbf{X}_j)_{(\sigma(\mathcal{S}))}$ into $(K-t+1)$ subfiles $(\mathbf{X}_j)_{(\sigma(\mathcal{S}),i_t)}$ for $i_t \in [K] \setminus \mathcal{S}$
        end for
    end for
    for $u = 1 : K$ do
        At user $u$, cache subfiles
            $\big((\mathbf{X}_j)_{(\sigma(\mathcal{S}),u)} : \mathcal{S} \subset [K] \setminus \{u\}$ such that $|\mathcal{S}| = t-1, \sigma \in \Sigma_{t-1}, j \in [N]\big)$
                                                            ▷ successive cache placement
    end for
```

For $T = 2$, suppose that the cache rates successively utilized at the users are given as $(C_1, C_2) = (1, 1)$. In the first step of the cache placement, user $u \in [4]$ stores the collection of subfiles

$$L_1^{(u)} = \big((\mathbf{X}_1)_{(u)}, (\mathbf{X}_2)_{(u)}, (\mathbf{X}_3)_{(u)}, (\mathbf{X}_4)_{(u)}\big)$$

in its cache, in which each subfile $(\mathbf{X}_j)_{(u)}$ has the rate of $1/4$ resulting in a cache rate of 1. In the second step, user $u \in [4]$ adds the collection of subfiles

$$L_2^{(u)} = \big((\mathbf{X}_j)_{(v,u)} : v \in [4] \setminus \{u\}, j \in [4]\big)$$

to its cache, in which each subfile $(\mathbf{X}_j)_{(v,u)}$ has the rate of $1/12$ resulting in a cache rate of 1. For example, user 2 additionally stores $(\mathbf{X}_j)_{(1,2)}$, $(\mathbf{X}_j)_{(3,2)}$, and $(\mathbf{X}_j)_{(4,2)}$ for $j \in [4]$ at step $t = 2$. Partition of file $\mathbf{X}_j$ for this two-step successive caching strategy is demonstrated in Fig. 8.6.

We now closely look at the delivery content. Suppose that the request vector $\mathbf{d} = [1\ 2\ 1\ 2]$ is received at step $t = 1$. In this case, server chooses $\mathcal{U}(\mathbf{d}) = \{1, 2\}$ as the

Algorithm 1 (continued)

```
    if request $\mathbf{d} = [d_1\ d_2\ \ldots\ d_K]$ received then
        $\mathcal{U}(\mathbf{d}) \leftarrow \emptyset$                          ▷ Initialize the set of leader users
        for $d \in \mathrm{supp}(\mathbf{d})$ do
            $u \leftarrow \mathrm{find}(d_u = d)$                    ▷ Find a user that requests file $d$
            $\mathcal{U}(\mathbf{d}) \leftarrow \mathcal{U}(\mathbf{d}) \cup \{u\}$         ▷ Add user $u$ to the set of leader users
        end for
        $\Theta \leftarrow \{\mathcal{S} \subset [K] : |\mathcal{S}| = t+1, \mathcal{S} \cap \mathcal{U}(\mathbf{d}) \neq \emptyset\}$
        for $\mathcal{S} \in \Theta, \sigma \in \Sigma_t$ do
            for $s \in \mathcal{S}$ do
                Broadcast $\bigoplus_{s \in \mathcal{S}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{S}\setminus\{s\})}$                ▷ coded delivery
            end for
        end for
        RequestBit $= 1$
    end if
    $t = t + 1$
end while
```

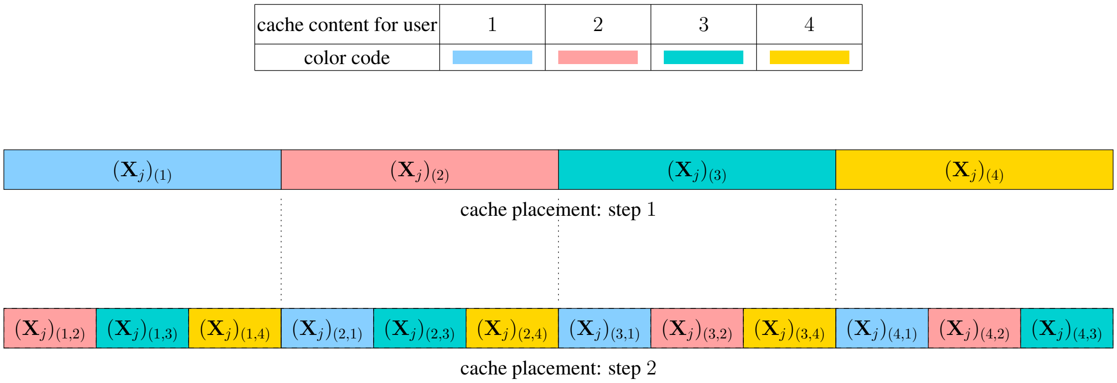


Figure 8.6. Two-step successive cache placement for $(C_1, C_2) = (1, 1)$ when $K = 4$ users and $N = 4$ files.

leader users and broadcasts the collection of linear combinations

$$\begin{aligned} M_{\mathbf{d},1} &= \{\mathbf{Y}_{\sigma,\{1,2\}}, \mathbf{Y}_{\sigma,\{1,3\}}, \mathbf{Y}_{\sigma,\{1,4\}}, \mathbf{Y}_{\sigma,\{2,3\}}, \mathbf{Y}_{\sigma,\{2,4\}}\} \\ &= \big\{(\mathbf{X}_1)_{(2)} \oplus (\mathbf{X}_2)_{(1)}, (\mathbf{X}_1)_{(3)} \oplus (\mathbf{X}_1)_{(1)}, (\mathbf{X}_1)_{(4)} \oplus (\mathbf{X}_2)_{(1)}, \\ &\qquad (\mathbf{X}_2)_{(3)} \oplus (\mathbf{X}_1)_{(2)}, (\mathbf{X}_2)_{(4)} \oplus (\mathbf{X}_2)_{(2)}\big\}, \end{aligned}$$

where $\sigma \in \Sigma_1$ is just the identity permutation. Here, each broadcasted linear combination *is of rate* $1/4$*, resulting in the delivery rate of* $5/4$*, which is equal to the delivery rate of* $R(\mathbf{d}, C_1)$*, as claimed. Note that user* 1*, as a leader user, can recover* $(\mathbf{X}_1)_{(2)}$*,* $(\mathbf{X}_1)_{(3)}$*, and* $(\mathbf{X}_1)_{(4)}$ *by simply canceling its cache from* $\mathbf{Y}_{\sigma,\{1,2\}}$*,* $\mathbf{Y}_{\sigma,\{1,3\}}$*, and* $\mathbf{Y}_{\sigma,\{1,4\}}$*. Similarly, user* 2 *can recover the subfiles of* $\mathbf{X}_2$ *that is not stored in its cache. Of the nonleader users, user* 3 *can recover* $(\mathbf{X}_1)_{(1)}$ *and* $(\mathbf{X}_1)_{(2)}$ *by simply canceling its cache from* $\mathbf{Y}_{\sigma,\{1,3\}}$ *and* $\mathbf{Y}_{\sigma,\{2,3\}}$*. To recover the missing subfile* $(\mathbf{X}_1)_{(4)}$*, it computes*

$$\mathbf{Y}_{\sigma,\{1,4\}} \oplus \mathbf{Y}_{\sigma,\{1,2\}} = (\mathbf{X}_1)_{(2)} \oplus (\mathbf{X}_1)_{(4)}.$$

By canceling the previously decoded subfile $(\mathbf{X}_1)_{(2)}$ *from this linear combination, user* 3 *gains access to* $(\mathbf{X}_1)_{(4)}$ *and successfully recover the file* $\mathbf{X}_1$*. Similar arguments can be applied for user* 4 *as well, concluding that every user can successfully recover their desired file for the given request vector. Repeating same arguments, it can be seen that a delivery rate of* $R(\mathbf{d}, C_1)$ *can be achieved when request* $\mathbf{d} \in [N]^K$ *arises at step 1.*

On one hand, by taking the expectation over uniformly random request vector, we get the average-case delivery rate of

$$\begin{aligned}\sum_{\mathbf{d}\in[N]^K} \left[\frac{\binom{4}{2} - \binom{4-|\mathrm{supp}(\mathbf{d})|}{2}}{4}\right] P(\mathbf{D}=\mathbf{d}) &= \sum_{\theta=1}^{4} \sum_{\substack{\mathbf{d}\in[N]^K:\\ |\mathrm{supp}(\mathbf{d})|=\theta}} \frac{6 - \binom{4-\theta}{2}}{4} P(\mathbf{D}=\mathbf{d}) \\ &= \frac{3}{4} \times \frac{1}{64} + \frac{5}{4} \times \frac{21}{64} + \frac{6}{4} \times \frac{42}{64} = \frac{45}{32},\end{aligned}$$

corresponding to the first point $(1, 45/32)$ *in Fig. 8.4a.*

On the other hand, by taking the maximum over all request vectors, we get the worst-case delivery rate of $\binom{4}{2}/\binom{4}{1} = 3/2$*, corresponding to the first point* $(1, 3/2)$ *in Fig. 8.4b.*

Suppose now that the request $\mathbf{d} = [1\ 2\ 1\ 2]$ *is received at step* $t = 2$*. In this case, server again chooses* $\mathcal{U}(\mathbf{d}) = \{1, 2\}$ *as the leaser users and broadcasts the collection of* *linear combinations*

$$\begin{aligned}M_{\mathbf{d},2} &= \cup_{\sigma\in\Sigma_2}\big\{\mathbf{Y}_{\sigma,\{1,2,3\}}, \mathbf{Y}_{\sigma,\{1,2,4\}}, \mathbf{Y}_{\sigma,\{1,3,4\}}, \mathbf{Y}_{\sigma,\{2,3,4\}}\big\}\\ &= \big\{(\mathbf{X}_1)_{(2,3)} \oplus (\mathbf{X}_2)_{(1,3)} \oplus (\mathbf{X}_1)_{(1,2)}, (\mathbf{X}_1)_{(3,2)} \oplus (\mathbf{X}_2)_{(3,1)} \oplus (\mathbf{X}_1)_{(2,1)},\\ &\quad (\mathbf{X}_1)_{(2,4)} \oplus (\mathbf{X}_2)_{(1,4)} \oplus (\mathbf{X}_2)_{(1,2)}, (\mathbf{X}_1)_{(4,2)} \oplus (\mathbf{X}_2)_{(4,1)} \oplus (\mathbf{X}_2)_{(2,1)},\\ &\quad (\mathbf{X}_1)_{(3,4)} \oplus (\mathbf{X}_1)_{(1,4)} \oplus (\mathbf{X}_2)_{(1,3)}, (\mathbf{X}_1)_{(4,3)} \oplus (\mathbf{X}_1)_{(4,1)} \oplus (\mathbf{X}_2)_{(3,1)},\\ &\quad (\mathbf{X}_2)_{(3,4)} \oplus (\mathbf{X}_1)_{(2,4)} \oplus (\mathbf{X}_2)_{(2,3)}, (\mathbf{X}_2)_{(4,3)} \oplus (\mathbf{X}_1)_{(4,2)} \oplus (\mathbf{X}_2)_{(3,2)}\big\}.\end{aligned}$$

Here, each broadcasted linear combination is of rate $1/12$*, resulting in the delivery rate of* $2/3$*, which is equal to the delivery rate of* $R(\mathbf{d}, C_1+C_2)$*, as claimed. This time, note that every user* $u \in [K]$ *can recover the subfile* $(\mathbf{X}_{d_u})_{(v,v')}$ *for every* $v, v' \in [4]\backslash\{u\}$*,* $v \neq v'$ *from the linear combination* $\mathbf{Y}_{\sigma,\{u,v,v'\}}$ *for some permutation* σ*. With the remaining subfiles already available in its cache, user* u *is able to completely recover* $\mathbf{X}_{d_u}$*. Repeating same arguments, it can be seen that a delivery rate of* $R(\mathbf{d}, C_1 + C_2)$ *can be achieved when request* $\mathbf{d} \in [N]^K$ *arises at step 2.*

On one hand, by taking the expectation over uniformly random request vector, we get the average-case delivery rate of

$$\begin{aligned}\sum_{\mathbf{d}\in[N]^K}\left[\frac{\binom{4}{3}-\binom{4-|\mathrm{supp}(\mathbf{d})|}{3}}{\binom{4}{2}}\right]P(\mathbf{D}=\mathbf{d}) &= \sum_{\theta=1}^{4}\sum_{\substack{\mathbf{d}\in[N]^K:\\ |\mathrm{supp}(\mathbf{d})|=\theta}}\frac{4-\binom{4-\theta}{3}}{6}P(\mathbf{D}=\mathbf{d})\\ &= \frac{1}{2}\times\frac{1}{64}+\frac{2}{3}\times\frac{63}{64}=\frac{85}{128},\end{aligned}$$

corresponding to the second point $(2, 85/128)$ *in Fig. 8.4a.*

On the other hand, by taking the maximum over all request vectors, we get the worst-case delivery rate of $\binom{4}{3}/\binom{4}{2} = 2/3$*, corresponding to the second point* $(2, 2/3)$ *in Fig. 8.4b.*

As demonstrated, the successive caching algorithm, the average-case delivery rates of $R_{\mathrm{avg}}(C_1)$ *and* $R_{\mathrm{avg}}(C_1+C_2)$ *are achieved respectively at step 1 and 2, simultaneously.*

Similarly, the worst-case delivery rates of $R_{\text{worst}}(C_1)$ and $R_{\text{worst}}(C_1 + C_2)$ are achieved respectively at step 1 and 2, simultaneously.

Remark 8.4.1. *Yu, Maddah-Ali, and Avestimehr proved in [7] that the average-case and worst-case achievable delivery rates for static requests given in Proposition 8.4.1 are optimal provided that the cache placement is uncoded. This result implies that our successive caching algorithm achieving the average-case and worst-case delivery rates for dynamic requests in Theorem 8.4.1 are optimal provided that the cache placement is restricted to be uncoded at every successive step.*

8.5 Discussion

In this chapter, we have introduced a new caching problem to capture the unpredictable nature of demands. As an answer to this dynamic caching problem, we have proposed to place cache in small increments through successive steps to satisfy delayed requests while guaranteeing to serve for earlier requests as well. In particular, first, we have followed an information-theoretic approach considering a single user and two time points at which requests can arise and we have established the optimal tradeoff between the average-case delivery rates at different request times when the cache rate is above a well-defined threshold. Extension of this result to an arbitrary number of users is left as an open problem. We then have followed a coding-theoretic approach for an arbitrary number of users while focusing only on the class of i.i.d. Bern(1/2) contents and we have proposed a successive caching algorithm. We have shown that the delivery rate of our algorithm is within a constant multiplicative gap to the optimal at every request time for both the performance criteria of the average-case delivery rates and the worst-case delivery rates. We have left the study of arbitrarily correlated contents from a coding theoretic-approach as another open problem.

8.A Proof of Lemma 8.4.1

We start with expanding $\mathbf{Y}_{\sigma,\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}}$ as follows.

$$\begin{aligned}\bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \mathbf{Y}_{\sigma,\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}} &= \bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{v\in\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}} (\mathbf{X}_{d_v})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{v\}))}\\
&= \bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{\substack{v\in\mathcal{A}\cup\{u\}:\\ d_v=d_u}} (\mathbf{X}_{d_u})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{v\}))}\\
&\qquad\oplus \bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{s\}))}.\end{aligned}$$

It suffices to show that

$$\bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{s\}))} = 0.$$

For every given set of users $\mathcal{K}\subset[K]$, define the set $\mathcal{D}(\mathcal{K}) := \{d\in[N] : d_j = d \text{ for some } j\in\mathcal{K}\}$ as the set of requested files by the users in $\mathcal{K}$. We start with

$$\begin{aligned}&\bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}} (\mathbf{X}_{d_s})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{s\}))}\\
&\qquad= \bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{d\in\mathcal{D}(\mathcal{A}_{u^c})} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}:\\ d_s=d}} (\mathbf{X}_{d})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{s\}))}\\
&\qquad= \bigoplus_{d\in\mathcal{D}(\mathcal{A}_{u^c})} \bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\backslash\mathcal{V}:\\ d_s=d}} (\mathbf{X}_{d})_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\backslash(\mathcal{V}\cup\{s\}))}.\end{aligned}$$

Note that for every $d\in\mathcal{D}(\mathcal{A}_{u^c})$,

$$\begin{aligned}\mathcal{F}(\mathcal{A}_{u^c}) &= \{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}) : d\notin\mathcal{D}(\mathcal{V})\}\sqcup\{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}) : d\in\mathcal{D}(\mathcal{V})\}\\
&= \{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}) : d\notin\mathcal{D}(\mathcal{V})\}\\
&\quad\ \sqcup\{\mathcal{V}\cup\{y\} : \mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}) \text{ such that } d\notin\mathcal{D}(\mathcal{V}), y\in\mathcal{A}_{u^c} \text{ such that } d_y = d\},\end{aligned}$$

where $\sqcup$ denotes the disjoint union. Utilizing this expansion, for every $d \in \mathcal{D}(\mathcal{A}_{u^c})$, we have

$$
\begin{aligned}
&\bigoplus_{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c})} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\setminus\mathcal{V}:\\ d_s=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\setminus(\mathcal{V}\cup\{s\}))}\\
&= \bigoplus_{\substack{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V})}} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\setminus\mathcal{V}:\\ d_s=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\setminus(\mathcal{V}\cup\{s\}))}\\
&\qquad\quad \oplus \bigoplus_{\substack{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\in\mathcal{D}(\mathcal{V})}} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\setminus\mathcal{V}:\\ d_s=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\setminus(\mathcal{V}\cup\{s\}))}\\
&= \bigoplus_{\substack{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V})}} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V})\setminus\mathcal{V}:\\ d_s=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\setminus(\mathcal{V}\cup\{s\}))}\\
&\qquad\quad \oplus \bigoplus_{\substack{\mathcal{V}'\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V}')}} \bigoplus_{\substack{y\in\mathcal{A}_{u^c}:\\ d_y=d}} \bigoplus_{\substack{z\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y\}):\\ d_z=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y,z\}))}\\
&\overset{(a)}{=} \bigoplus_{\substack{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V})}} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}:\\ d_s=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\setminus(\mathcal{V}\cup\{s\}))}\\
&\qquad\quad \oplus \bigoplus_{\substack{\mathcal{V}'\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V}')}} \bigoplus_{\substack{y\in\mathcal{A}_{u^c}:\\ d_y=d}} \bigoplus_{\substack{z\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y\}):\\ d_z=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y,z\}))}\\
&\overset{(b)}{=} \bigoplus_{\substack{\mathcal{V}\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V})}} \bigoplus_{\substack{s\in\mathcal{A}_{u^c}:\\ d_s=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V})\setminus(\mathcal{V}\cup\{s\}))}\\
&\qquad\quad \oplus \bigoplus_{\substack{\mathcal{V}'\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V}')}} \bigoplus_{\substack{y\in\mathcal{A}_{u^c}:\\ d_y=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}')\setminus(\mathcal{V}'\cup\{y\}))}\\
&\qquad\quad \oplus \bigoplus_{\substack{\mathcal{V}'\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V}')}} \bigoplus_{\substack{y\in\mathcal{A}_{u^c}:\\ d_y=d}} \bigoplus_{\substack{z\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V}')\setminus(\mathcal{V}'\cup\{y\}):\\ d_z=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y,z\}))}\\
&= \bigoplus_{\substack{\mathcal{V}'\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V}')}} \bigoplus_{\substack{y\in\mathcal{A}_{u^c}:\\ d_y=d}} \bigoplus_{\substack{z\in\mathcal{A}_{u^c}\cup\mathcal{U}(\mathcal{V}')\setminus(\mathcal{V}'\cup\{y\}):\\ d_z=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y,z\}))}\\
&= \bigoplus_{\substack{\mathcal{V}'\in\mathcal{F}(\mathcal{A}_{u^c}):\\ d\notin\mathcal{D}(\mathcal{V}')}} \bigoplus_{\substack{y\in\mathcal{A}_{u^c}:\\ d_y=d}} \bigoplus_{\substack{z\in\mathcal{A}_{u^c}\setminus\{y\}:\\ d_z=d}} (\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y,z\}))}\\
&\overset{(c)}{=} 0,
\end{aligned}
$$

where (a) follows since $d \notin \mathcal{D}(\mathcal{V})$ in the first binary summation, (b) follows by taking the term $z = \mathcal{U}(\{y\})$, the leader user requesting $\mathbf{X}_d$, out of the binary summation, and (c) follows since every pair $\{y, z\} \subset \mathcal{A}_{u^c}$ is counted twice and results in the same subfile $(\mathbf{X}_d)_{\sigma(\mathcal{A}\cup\{u\}\cup\mathcal{U}(\mathcal{V}'\cup\{y\})\setminus(\mathcal{V}'\cup\{y,z\}))}$.

Acknowledgment

This chapter is, in part, a reprint of the material in the paper: Pinar Sen, Michael Gastpar, and Young-Han Kim, "Successive Refinement to Caching for Dynamic Requests," *Proceedings of IEEE International Symposium on Information Theory*, Los Angeles, California, June 2020. Chapter 8 is, in part, currently being prepared for submission for publication of the material in *IEEE Transactions of Information Theory*, 2020 with authors Pinar Sen, Michael Gastpar, and Young-Han Kim. The dissertation author was the primary investigator and author of this paper.

Bibliography

[1] Y. Birk and T. Kol. Coding on demand by an informed source (ISCOD) for efficient broadcast of different supplemental data to caching clients. *IEEE Trans. Inf. Theory*, 52(6):2825–2830, June 2006.

[2] S. Borst, V. Gupta, and A. Walid. Distributed caching algorithms for content distribution networks. In *Proc. 29th Ann. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, pages 1–9, March 2010.

[3] M. A. Maddah-Ali and U. Niesen. Fundamental limits of caching. *IEEE Trans. Inf. Theory*, 60(5):2856–2867, May 2014.

[4] Kai Wan, D. Tuninetti, and P. Piantanida. On the optimality of uncoded cache placement. In *Proc. IEEE Inf. Theory Workshop*, pages 161–165, Sep. 2016.

[5] H. Ghasemi and A. Ramamoorthy. Improved lower bounds for coded caching. *IEEE Trans. Inf. Theory*, 63(7):4388–4413, July 2017.

[6] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr. Characterizing the rate-memory tradeoff in cache networks within a factor of 2. In *Proc. IEEE Int. Symp. Inf. Theory*, pages 386–390, June 2017.

[7] Q. Yu, M. A. Maddah-Ali, and A. S. Avestimehr. The exact rate-memory tradeoff for caching with uncoded prefetching. *IEEE Trans. Inf. Theory*, 64(2):1281–1296, Feb 2018.

[8] C. Wang, S. Saeedi Bidokhti, and M. Wigger. Improved converses and gap results for coded caching. *IEEE Trans. Inf. Theory*, 64(11):7051–7062, Nov 2018.

[9] A. Sengupta, R. Tandon, and T. C. Clanc. Layered caching for heterogeneous storage. In *Proc. 50th Asilomar Conf. Signals, Syst. Comp.*, pages 719–723, Nov 2016.

[10] M. Mohammadi Amiri, Q. Yang, and D. Gündüz. Decentralized caching and coded delivery with distinct cache capacities. *IEEE Trans. Commun.*, 65(11):4657–4669, Nov 2017.

[11] Q. Yang and D. Gündüz. Coded caching and content delivery with heterogeneous distortion requirements. *IEEE Trans. Inf. Theory*, 64(6):4347–4364, June 2018.

[12] A. M. Ibrahim, A. A. Zewail, and A. Yener. Coded caching for heterogeneous systems: An optimization perspective. *IEEE Trans. Commun.*, 67(8):5321–5335, Aug 2019.

[13] U. Niesen and M. A. Maddah-Ali. Coded caching with nonuniform demands. *IEEE Trans. Inf. Theory*, 63(2):1146–1158, Feb 2017.

[14] M. Ji, A. M. Tulino, J. Llorca, and G. Caire. Order-optimal rate of caching and coded multicasting with random demands. *IEEE Trans. Inf. Theory*, 63(6):3923–3949, June 2017.

[15] J. Zhang, X. Lin, and X. Wang. Coded caching under arbitrary popularity distributions. *IEEE Trans. Inf. Theory*, 64(1):349–366, Jan 2018.

[16] P. Hassanzadeh, A. Tulino, J. Llorca, and E. Erkip. Correlation-aware distributed caching and coded delivery. In *Proc. IEEE Inf. Theory Workshop*, pages 166–170, Sep. 2016.

[17] P. Hassanzadeh, A. M. Tulino, J. Llorca, and E. Erkip. On coding for cache-aided delivery of dynamic correlated content. *IEEE J. Sel. Areas Commun.*, 36(8):1666–1681, Aug 2018.

[18] C. Wang, S. H. Lim, and M. Gastpar. Information-theoretic caching: Sequential coding for computing. *IEEE Transactions on Information Theory*, 62(11):6393–6406, Nov 2016.

[19] Chien-Yi Wang. *Function Computation over Networks Efficient Information Processing for Cache and Sensor Applications.* EPFL, Lausanne, 2015.

Chapter 9

Concluding Remarks

We conclude this dissertation with comments for future research directions.

In Chapters 2, 3, and 5, we have studied the performance of homologous codes for various communication problems defined over multiple access channels, such as linear computation of codewords, message communication, and simultaneous computation and communication. The results implies that such structured codes can outperform conventional random codes when the structure is matched with the problem of interest (such as linear structure benefits linear computation) or at least can completely replace them. In order to develop a fundamental framework towards a general family of structured codes built on shared linearity over different encoders, one should investigate the connection between homologous codes and lattice-based structured codes. Another open problem is the *capacity region* of the linear computation problem, for which we have established general inner and outer bounds in Chapter 3. In Chapter 4, we adapted the proof techniques we developed for homologous codes to analyze the performance of random Marton codes with the optimal the maximum likelihood decoder. These proof techniques seem to be a recurring path to establishing the optimal performance of random code ensembles.

In Chapters 6,7, and 8, we have formulated two new caching problems to capture the unpredictable nature of contents and requests. As an answer to these problems, we have proposed to place cache in small increments through successive steps to address the modifications within the contents (if any) or to satisfy delayed requests while guaranteeing to serve for earlier requests as well. For each problem, we have followed an information-theoretic approach considering a single user and we have established a single-letter characterization of the optimal tradeoff between the total cache rate and the delivery rate in terms of an optimization problem. The extension of our results to an arbitrary number of users is left as an open problem. For dynamic requests, we have also followed a coding-theoretic approach for an arbitrary number of users while focusing only on the class of i.i.d. Bern(1/2) contents and proposed a near-optimal successive caching algorithm. In order to formulate and solve a unified caching problem that captures both dynamic contents and requests, one should better understand the connection between information-theoretic and coding-theoretic approaches. In particular, there are two research directions to investigate: information-theoretic approaches when there are multiple users in the network and coding-theoretic approaches when the file contents are arbitrarily correlated.