# Non-asymptotic Analysis of Single-Receiver Channels with Limited Feedback

Thesis by

Recep Can Yavas

In Partial Fulfillment of the Requirements for the
Degree of
Doctor of Philosophy

CALIFORNIA INSTITUTE OF TECHNOLOGY
Pasadena, California

2023
Defended on August 29, 2022

*To my beloved brother Efe*

# ACKNOWLEDGMENTS

First of all, I would like to thank my advisors Prof. Michelle Effros and Prof. Victoria Kostina for their constant support and patience in every aspect of my PhD, and also giving me the freedom to study the problems that I like. Their confidence in me has been an invaluable source of motivation during my PhD. I have learned a lot from them about how to be a good teacher and a good researcher.

I am grateful to the members of my defense and candidacy committees, Prof. Babak Hassibi and Prof. Jehoshua (Shuki) Bruck for their valuable feedback and comments on my research and their helpful advice on my future career.

One of the nicest things about having two advisors was to have two groups. I would like to thank my lab-mates Yuxin Liu, Siming Sun, Zihao (Jack) Li, Peida Tian, Shuqing Chen, Nian Guo, Eray Atay, and Dr. Oron Sabag for their friendship and stimulating discussions. I will always remember the wonderful time that I spent with you, and I will truly miss our group meetings.

I would like to thank my friends Şahin Lale, Dr. Hikmet Yıldız, Dr. Oğuzhan Teke, Kordağ Kılıç, Taylan Kargın, and Dr. Sinan Kefeli. Thanks to them, I have always felt like I am at home. I will definitely remember our NBA nights.

Lastly, my deepest gratitude goes to my parents Recayi and Fatma Nilüfer, and my little brother Efe. Being far from them was the hardest thing to deal with during my PhD. Their continuous love, support, and encouragement have been one of the biggest motivations in my PhD.

# ABSTRACT

Emerging Internet of Things, machine-type communication, and ultra-reliable low-latency communication in 5G demand codes that operate at short blocklengths, have low error probability and low energy consumption, and can handle the random activity of a large number of communicating devices. Since many of the applications have a single central device, e.g., a base station, that resolves the communication and a varying number of users, these requirements on the code design motivate interest in the non-asymptotic analysis of codes in a variety of single-receiver channels. This thesis investigates three channel coding problems with the goals of understanding the fundamental limits of channel coding under stringent requirements on reliability, delay, and power, and proposes novel coding architectures that employ constrained feedback to attain those limits. In the first part, we consider point-to-point channels without feedback, and analyze the non-asymptotic limits in the moderate deviations regime in probability theory. The moderate deviations regime is suitable for accurately approximating the maximum achievable coding rate in the operational regimes of practical interest because it simultaneously considers high rates and low error probabilities. We propose a new quantity, channel skewness, which governs the fundamental limit at short blocklengths and low error probabilities. Our approximation is the tightest among the state-of-the-art approximations for most error probability and latency constraints of interest. In the second part, we investigate rateless channel coding with limited feedback. Here, rateless means that decoding can occur at multiple decoding times. In our code design, feedback is limited both in frequency and content; it is sparse, meaning that it is available only at a few instants throughout the communication epoch; and it is stop-feedback, meaning that the receiver informs the transmitters only about whether decoding has occurred rather than what symbols it has received. Our results demonstrate that sporadically sending a few bits is almost as efficient as sending feedback at every time instant. In the third part, we focus on rateless random access channel codes, where the number of active transmitters is unknown to both the transmitters and the receiver. Our rateless code design that reserves a decoding time for each possible number of active transmitters achieves the same first two terms in the asymptotic expansion of the achievable rate as codes where the transmitter activity is known a priori. This means that, remarkably, the random transmitter activity has almost no effect on achievable rates.

To obtain tight channel coding bounds, we analyze some non-asymptotic and asymptotic state-of-the-art bounds on the probability of the sum of independent and identical random variables, whose applications extend to source coding, hypothesis testing, and many others. In the scenarios where these tools are not directly applicable such as for the Gaussian channel, we propose new techniques to overcome that difficulty.

# PUBLISHED CONTENT AND CONTRIBUTIONS

[1] R. C. Yavas, V. Kostina, and M. Effros, "Third-order analysis of channel coding in the moderate deviations regime," in *2022 IEEE International Symposium on Information Theory (ISIT)*,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript., Jun. 2022, pp. 2309–2314. DOI: 10.1109/ISIT50566.2022.9834841.

[2] ——, "Third-order analysis of channel coding in the small-to-moderate deviations regime," *Submitted to IT Transactions*, Aug. 2022,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript.

[3] ——, "Variable-length sparse feedback codes for point-to-point, multiple access and random access channels," *Submitted to IT Transactions*, Aug. 2022,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript.

[4] ——, "Gaussian multiple and random access channels: Finite-blocklength analysis," *IEEE Transactions on Information Theory*, vol. 67, no. 11, pp. 6983–7009, Nov. 2021,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript. DOI: 10.1109/TIT.2021.3111676.

[5] ——, "Nested sparse feedback codes for point-to-point, multiple access, and random access channels," in *2021 IEEE Information Theory Workshop (ITW)*,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript. This is an invited paper., Oct. 2021, pp. 1–6. DOI: 10.1109/ITW48936.2021.9611385.

[6] ——, "Random access channel coding in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2115–2140, Apr. 2021,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript. DOI: 10.1109/TIT.2020.3047630.

[7] ——, "Variable-length feedback codes with several decoding times for the gaussian channel," in *2021 IEEE International Symposium on Information Theory (ISIT)*,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript., Jun. 2021, pp. 1883–1888. DOI: 10.1109/ISIT45174.2021.9517993.

[8] ——, “Gaussian multiple and random access in the finite blocklength regime,” in *2020 IEEE International Symposium on Information Theory (ISIT)*,
R. C. Yavas participated in the conception of the project, solved the problem, and wrote the manuscript. This work was also presented in 2020 Information Theory and Applications Workshop (ITA) in a poster session., Jun. 2020, pp. 3013–3018. DOI: 10.1109/ISIT44484.2020.9174026.

[9] M. Effros, V. Kostina, and R. C. Yavas, “Random access channel coding in the finite blocklength regime,” in *2018 IEEE International Symposium on Information Theory (ISIT)*,
R. C. Yavas participated in the conception of the project, solution of the problem, and writing of the manuscript. The author order is alphabetical., Apr. 2018, pp. 1261–1265. DOI: 10.1109/ISIT.2018.8437831.

# TABLE OF CONTENTS

# LIST OF ILLUSTRATIONS

# LIST OF TABLES

# Chapter 1

# INTRODUCTION

## 1.1 Non-asymptotic Fundamental Limits in Channel Coding

In channel coding, a transmitter wants to communicate an equiprobable message $W$ on the set $\{1, \ldots, M\}$ to a receiver over $n$ channel uses. A channel, which is an abstraction of the noisy communication medium, is defined as a transition probability kernel $P_{Y^n|X^n}$ from the channel inputs $X^n$ to channel outputs $Y^n$. It expresses the probability of receiving an output sequence $y^n$ given that an input sequence $x^n$ is sent. A channel code, which determines the operations done by the transmitter and the receiver, consists of two mappings, an encoder $\mathsf{f}$ from $\{1, \ldots, M\}$ to the set of channel inputs $\mathcal{X}^n$, and a decoder $\mathsf{g}$ from the set of channel outputs $\mathcal{Y}^n$ to $\{1, \ldots, M\}$. The image of the encoder $\mathsf{f}$ is called the codebook.

An $(n, M, \epsilon)$-code is defined as the encoder-decoder pair $(\mathsf{f}, \mathsf{g})$ with blocklength $n$, codebook size $M$ (the number of messages), where the *average* error probability induced by the $(\mathsf{f}, \mathsf{g})$ pair is bounded by $\epsilon$, i.e.,

$$\mathbb{P}\left[\mathsf{g}(\mathsf{f}(W)) \neq W\right] \leq \epsilon \tag{1.1}$$

The fundamental limit of (block) channel coding is defined as

$$M^*(n, \epsilon) \triangleq \{\max M \colon \exists \text{ an } (n, M, \epsilon)\text{-code}\}, \tag{1.2}$$

which is the maximum achievable codebook size compatible with blocklength $n$ and error probability $\epsilon$. For a given application with an $(n, \epsilon)$ pair, the objective is to compute $M^*(n, \epsilon)$ and to determine which $(\mathsf{f}, \mathsf{g})$ pairs achieve it. The problem of finding $M^*(n, \epsilon)$ that gave birth to the field of information theory after Shannon's pioneering work [1] is still relevant today. This is because determining the optimal encoder $\mathsf{f}$ is intractable since the number of possible mappings grows doubly exponential with $n$ [2]. Therefore, a more tractable approach to the channel coding problem is to try to derive tight lower and upper bounds on $M^*(n, \epsilon)$ for any given $(n, \epsilon)$. This approach has become popular with [3] and later with [4] and [5]. However, the evaluation of the non-asymptotic bounds is difficult unless the channel has some certain symmetries such as in the binary symmetric channel (BSC) and in the Gaussian channel [5], [6]. Even if the exact computation of the bounds is possible for some channels, numerical evaluations lack insights about the fundamental limits. For example, we cannot easily say something about $M^*(n, \epsilon)$ as a function of $(n, \epsilon)$ by only looking at the bounds computed for several $(n, \epsilon)$ pairs.

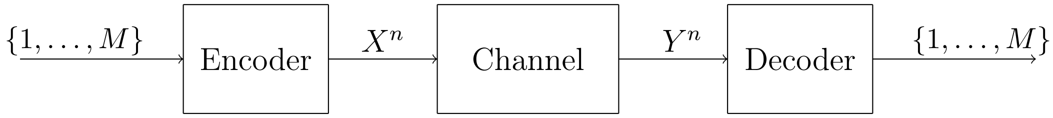


Figure 1.1: Channel coding setup

Towards the goal of analyzing $M^*(n, \epsilon)$ and understanding its behavior in a setting as general as possible, the literature investigates $M^*(n, \epsilon)$ in the asymptotic regime that $n \to \infty$. Of course, for such an analysis, one should also determine the asymptotic relationship between $\epsilon$ and $n$. The most common error probability regimes studied in the literature are the central limit theorem (CLT) and the large deviations (LD) regimes. The capacity of the channel, defined as

$$C \triangleq \lim_{\epsilon \to 0} \liminf_{n \to \infty} \frac{\log M^*(n, \epsilon)}{n}, \tag{1.3}$$

is the first-order term in the asymptotic expansion of the achievable rate, and is given by [1]

$$C = \max_{P_X} I(X; Y), \tag{1.4}$$

where $I(X; Y)$ is the mutual information between $X$ and $Y$, and the maximization is over the input distribution $P_X$.

Channel coding analyses in the CLT regime fix a target error probability $\epsilon \in (0, 1)$ and approximate $\log M^*(n, \epsilon)$ as the blocklength $n$ approaches infinity. Examples of such results include Strassen's expansion [7] for discrete memoryless point-to-point channels (DM-PPCs) under the maximal error probability constraint, showing

$$\log M^*(n, \epsilon) = nC - \sqrt{nV} Q^{-1}(\epsilon) + O(\log n). \tag{1.5}$$

Here, the function $Q^{-1}(\cdot)$ is the inverse of the complementary standard Gaussian cumulative distribution function, and $V$ is called the *channel dispersion*, and is defined as [5, Sec. IV]

$$V \triangleq \lim_{\epsilon \to \infty} \limsup_{n \to \infty} \left( \frac{nC - \log M^*(n, \epsilon)}{Q^{-1}(\epsilon)} \right)^2 , \tag{1.6}$$

Channel dispersion characterizes how fast the maximum achievable rate approaches the capacity as $n$ grows to infinity.

Strassen's result shows that

$$V = \min_{P_X : I(X;Y) = C} \mathrm{Var}\left[ \imath(X;Y) \right] , \tag{1.7}$$

where $\imath(x;y)$ is the *information density*

$$\imath(X;Y) = \log \frac{P_{Y|X}(Y|X)}{P_Y(Y)} . \tag{1.8}$$

The capacity $C$ and the dispersion $V$ are respectively the expected value and the variance of $\imath(X;Y)$ under the capacity-achieving input distribution. Analyzing the information density, e.g., computing its tail probability, is key in almost all asymptotic expansions derived in channel coding.

Hayashi [4] and Polyanskiy *et al.* [5] and revisit Strassen's result (1.5), showing that the same asymptotic expansion holds for the average error probability constraint[1], deriving lower and upper bounds on the coefficient of the $O(\log n)$ term, and extending the result to Gaussian channels with maximal and average power constraints.

For channel coding in the LD regime, one fixes a *rate* $R = \frac{\log M}{n}$ strictly below the channel capacity, and seeks to characterize the minimum achievable error probability $\epsilon^*(n, R)$ as the blocklength $n$ approaches infinity. In this regime, $\epsilon^*(n, R)$ decays exponentially with $n$. For $R$ above the critical rate, [8, Ch. 5] derives the error exponent $E(R)$, i.e.,

$$\epsilon^*(n, R) = e^{-n(E(R) + o(1))} . \tag{1.9}$$

The function $E(R)$ is called the error exponent (or the reliability function), and is the analog of dispersion $V$ in (1.5) since it tells us how fast the minimum achievable error probability decays to zero at a fixed rate $R$. The capacity $C$ is the zero of the error exponent function $E(\cdot)$. The error exponent and the

[1] The thesis mainly focuses on the average error probability.

dispersion are the second-order characteristics of the channel in the CLT and LD regimes, respectively.

Naturally, both the CLT- and LD-type asymptotic approximations become less accurate as the $(n, \epsilon)$ pair gets farther away from the regime that is considered. Namely, for a fixed $n$, CLT approximations fall short if $\epsilon$ is small, (or, equivalently, the rate gets much smaller than the capacity), and LD approximations fall short if $\epsilon$ is large, (or, equivalently, the rate gets closer to the capacity). Since the remainder terms $O\left(\frac{\log n}{n}\right)$ for the rate $\frac{\log M}{n}$ in (1.5) and $o(1)$ for the error exponent $E(R)$ in (1.9) decrease with $n$, the accuracy of both approximations deteriorates at shorter blocklengths. Motivated by the inability of CLT and LD regimes to provide accurate approximations for a wide range of $(n, \epsilon)$ pairs and the hope of deriving more accurate and computable approximations to the finite blocklength rate, we consider the moderate deviations (MD) regime. In the MD regime, the error probability $\epsilon_n$ decays sub-exponentially to zero, i.e., $\epsilon_n \to 0$ and $-\frac{1}{n} \log \epsilon_n \to 0$, and the rate approaches the capacity with a gap of order strictly greater than $\frac{1}{\sqrt{n}}$. This regime is practically relevant since it simultaneously considers low error probabilities and high achievable rates.

Before presenting the results of the thesis, in Chapter 2, we present the refined non-asymptotic and asymptotic bounds from the probability theory literature in the CLT, MD, and LD regimes. These are the main tools that are used to analyze the non-asymptotic bounds and to derive asymptotic lower and upper bounds on $\log M^*(n, \epsilon)$ in many channel coding problems. The scope of their applications in information theory is beyond channel coding problems. Other examples include source coding [9], [10], hypothesis testing [5], and group testing [11].

In Chapter 3, we refine the third-order term $O(\log n)$ in the asymptotic expansion in (1.5) in the MD regime. The form of this term depends on whether the channel is singular. Singular channels are channels for which the channel transition probability from $x$ to $y$ is the same for every compatible $(x, y)$ pair, while nonsingular channels are channels that do not satisfy this property (see Section 3.2.4 for formal definitions). We show that for nonsingular channels, given an MD sequence $\{\epsilon_n\}_{n\geq 0}$, it holds that

$$\log M^*(n, \epsilon_n) \gtrapprox nC - \sqrt{nV}Q^{-1}(\epsilon_n) + \frac{1}{2}\log n + \underline{S}Q^{-1}(\epsilon_n)^2 \tag{1.10}$$

$$\log M^*(n, \epsilon_n) \lessapprox nC - \sqrt{nV}Q^{-1}(\epsilon_n) + \frac{1}{2}\log n + \overline{S}Q^{-1}(\epsilon_n)^2, \tag{1.11}$$

where $\underline{S}$ and $\overline{S}$ are the lower and upper bounds on the fundamental quantity $S$ that governs the third-order behavior in channel coding. We term this quantity the *channel skewness*. For symmetric channels such as the BSC and the Gaussian channel with maximal power constraint, $S$ is determined exactly. For the BSC and most practically important $(n, \epsilon)$ pairs, including $n \in [100, 500]$ and $\epsilon \in [10^{-10}, 10^{-1}]$, an approximation up to the channel skewness is the most accurate among state-of-the-art CLT and LD approximations in the literature. We also derive the third-order term in the type-II error exponent of binary hypothesis testing in the MD regime; the resulting third-order term is similar to the channel skewness.

## 1.2 Channel Coding with Limited Feedback

In channel coding with feedback, the channel input at time $i$ for message $m$, $X_i(m)$, is a function of the message $m$ and the received signal until time $i-1$, $Y^{i-1}$. From this definition, obviously, feedback cannot decrease $M^*(n, \epsilon)$. Perhaps surprisingly, feedback does not increase the capacity of DM-PPCs [12]. However, feedback simplifies coding schemes and improves the speed of approach to capacity with coding delay. Examples that demonstrate this effect include Horstein's scheme for the BSC [13] and Schalkwijk and Kailath's scheme for the Gaussian channel [14].

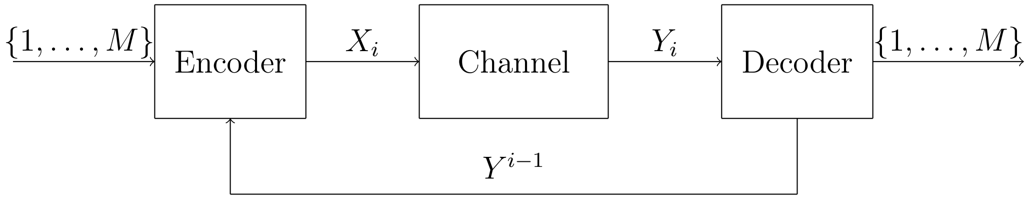


Figure 1.2: Feedback channel.

In practice, implementing a code with the feedback scheme as described above, i.e., after every symbol, the receiver feeds back all of the received output symbols until that time, can be infeasible due to limited capabilities of the transmitter and the receiver. For example, codes with feedback after every symbol can be infeasible for scenarios with half-duplex devices, where the transmitter cannot listen to the feedback signal and transmit its symbol at the same time. Similarly, in scenarios where the power consumption of the receiver is limited, the assumption that the receiver feeds back the output sequence $Y^{i-1}$ to the transmitter noiselessly, can be unreasonable.

An interesting question to ask is how much feedback is needed to still benefit from the improved achievable rate. We consider the frequency and content limitations on the feedback, addressing the scenarios described above in order.

- Sparse feedback (feedback frequency limitation): the receiver is allowed to send a feedback signal to the transmitter only at $L$ times, where $L$ is much smaller than the blocklength $n$.
- Coarse feedback (feedback content limitation): at every instance of feedback, only a small number of bits, $R_{\text{fb}} \ll n \log_2 |\mathcal{Y}|$, are fed back, where $\mathcal{Y}$ denotes the output alphabet.

If there is no frequency constraint, i.e., feedback can be sent at each time instant, we call it *dense* feedback. If there is no content constraint, i.e., the receiver can send all received symbols that it has received until that time, we call it *full* feedback.

It turns out that there are examples of both sparse and coarse feedback codes, where the performance of the code with limited feedback is similar to that of dense and/or full feedback. For an example of sparse feedback, in [15], Wagner *et al.* show that even a single instance of feedback at time $\frac{n}{2}$ improves the second-order rate for channels with multiple capacity-achieving input distributions giving distinct dispersions.

To find an example of coarse feedback codes with good performance, we turn our attention to *variable-length* (or, rateless) codes, where decoding can occur at multiple times rather than a single time $n$. In these codes, whenever feedback is available, the decoder has an opportunity to decode and stop the transmission. First, we need to re-define the rate since there are multiple decoding times. Let $n_1, \dots, n_L$ be $L$ pre-determined decoding times of the variable-length code. Similar to most prior work [16]–[18], we define the rate as

$$R \triangleq \frac{\log M}{\mathbb{E}\left[\tau\right]}, \tag{1.12}$$

where $\tau \in \{n_1, \ldots, n_L\}$ is the random decoding time, that is, we impose an average decoding time constraint on the code as

$$\mathbb{E}\left[\tau\right] \leq N. \tag{1.13}$$

One of the earliest works on variable-length feedback (VLF) codes is by Burnashev [16] who derives the error exponent of VLF codes, which is greater than the error exponent $E(R)$ in (1.9) achieved for fixed-length codes without feedback. Within VLF codes, we consider the most coarse feedback possible, that is, $R_{\text{fb}} = 1$ bit, and in addition, that one-bit feedback can only be used to tell the transmitter whether decoding is successful. If decoding occurs at a decoding time, then the receiver feeds back a “stop” symbol indicating that transmission should stop; if decoding does not occur, then the receiver feeds back a “continue” symbol indicating that transmission should continue. This type of feedback is called *stop-feedback*, and the VLF codes that employ stop-feedback are called variable-length stop-feedback (VLSF) codes. Polyanskiy *et al.* [18] show that in the CLT regime, $\log M^*(N, \epsilon)$, is sandwiched as

$$\frac{NC}{1-\epsilon} - \log N + O(1) \leq \log M^*(N, \epsilon) \leq \frac{NC}{1-\epsilon} + O(1) \tag{1.14}$$

for dense VLSF codes, i.e., $L = \infty$ and $n_\ell = \ell$ for all $\ell \in \mathbb{Z}_+$. First, compared to Strassen’s expansion (1.5), the first-order term improves by a factor of $\frac{1}{1-\epsilon}$. Second, the convergence to the first-order term is faster than of (1.5) ($O(\log N)$ rather than $O(\sqrt{N})$). Second, the upper bound in (1.14) holds for any dense VLF code, meaning that within dense VLF codes, the performance gap between the most coarse and the least coarse feedback codes is small, i.e., at most $\log N + O(1)$ in $\log M^*(n, \epsilon)$. This fact motivates the study of sparsity of the feedback for VLF codes rather than the coarseness.

In Chapter 4, we consider VLSF codes that are also sparse, and derive a second-order achievability bound as a function of the average error probability $\epsilon$, the average decoding time $N$, and the number of available decoding times $L$, while optimizing the values of $L$ available decoding times $n_1, \ldots, n_L$. The result shows that our sparse VLSF codes with only a small number of decoding times achieve rates close to that achieved by Polyanskiy *et al.*’s VLSF code

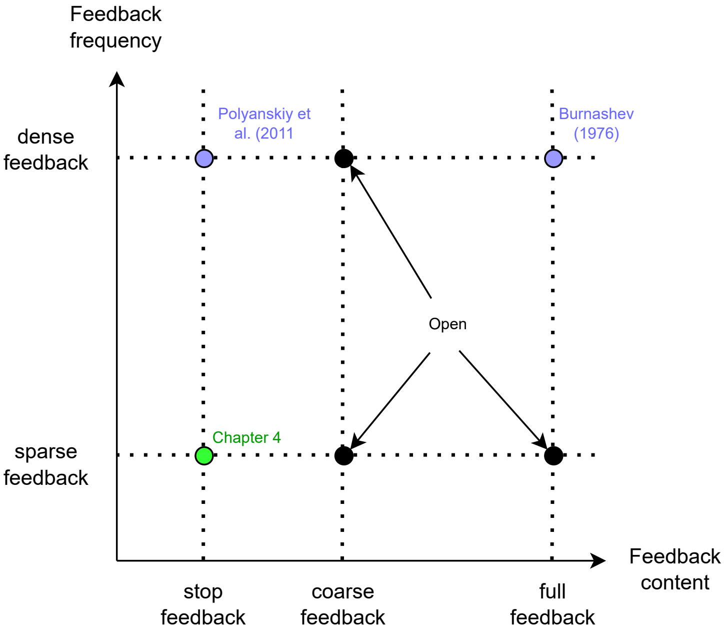


Figure 1.3: Feedback limitations in VLF codes.

with $L = \infty$, highlighting the efficiency of sparse VLSF coding schemes. For example, over the BSC with cross-over probability 0.11, our VLSF achievability bound with only $L = 4$ decoding times achieves 95.2% of the rate achieved by the VLSF code with $L = \infty$. Our analysis also shows the importance of the optimization of the values of $L$ decoding times for attaining the best second-order term. In Chapter 5, we extend our result on sparse VLSF codes to the discrete-memoryless multiple access channel (DM-MAC), where there are a fixed $K$ number of transmitters communicating to a single receiver, and the feedback signal is sent to all transmitters simultaneously whenever it is available. A summary of feedback limitations in VLF codes is given in Fig. 1.3.

## 1.3 Random Access Communication

Random access in general is defined as multi-transmitter, single-receiver communication, where the number and the identities of active transmitters are unknown to both the transmitters and the receiver.

Emerging communication systems such as Internet of Things and machine-type-communication systems impose four requirements on the code design: high reliability, low latency, low energy consumption, and random activity in a large number of communicating devices. These practical requirements on the

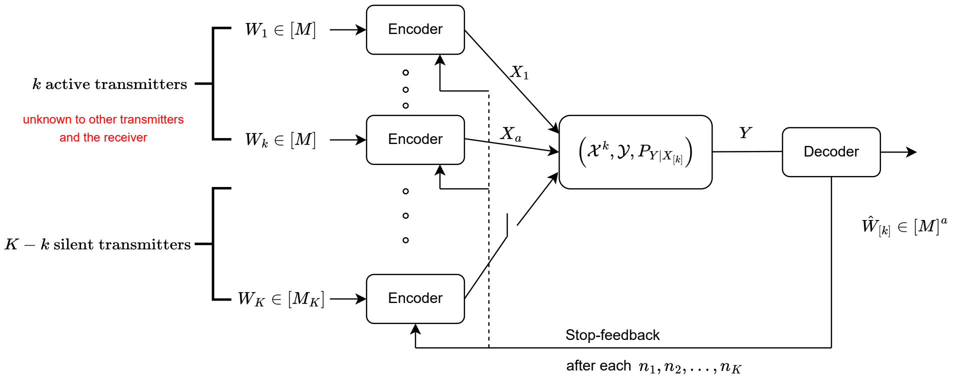

$k$ active transmitters
unknown to other transmitters and the receiver
$K - k$ silent transmitters
$W_1 \in [M]$
$W_k \in [M]$
$W_K \in [M_K]$
Encoder
Encoder
Encoder
$X_1$
$X_a$
$(\mathcal{X}^k, \mathcal{Y}, P_{Y|X_{[k]}})$
$Y$
Decoder
$\hat{W}_{[k]} \in [M]^a$
Stop-feedback
after each $n_1, n_2, \ldots, n_K$

Figure 1.4: Our RAC scheme.

code make the study of the random access problem in the CLT regime very appealing. Keeping the low energy constraint and the benefits of little feedback in mind, in Chapter 6, we extend the sparse rateless code that employs stop-feedback to random access channels (RACs), where the maximal number of transmitters is $K$, the decoding times are $n_0 < n_1 < \cdots < n_K$, and each $n_i$ is the decoding time used if the transmitter believes that $i$ transmitters are active. Stop-feedback synchronizes the transmitters and the receiver so that all parties are aware of the state of the communication epoch at all times. In our model, the transmitters must listen to the feedback signal only at a sparse collection of times. Fig. 1.4 illustrates our RAC scheme, where the decoder attempts to decode $k \leq K$ messages, and $K$ is the maximal number of transmitters.

Unlike VLSF codes for DM-PPCs, no average decoding time constraint is imposed since a single decoding time $n_i$ is dedicated to decoding of $i$ transmitters. In fact, our RAC code stops the transmission at time $n_k$ with high probability if $k$ is the number of active transmitters. Employing the same encoding function $\mathsf{f}$ for all transmitters, the rate for $k \in [K]$ active transmitters is

$$R_k = \frac{\log M}{n_k}, \tag{1.15}$$

where $M$ is the codebook size. Our central result in Chapter 6 demonstrates the achievability on a RAC of performance that is first-order optimal for the MAC in operation during each coding epoch. Our proposed code also performs as well in its dispersion term as the best-known code for a MAC with the transmitter activity known a priori [19]–[22]. This means that the random activity of transmitters does not cause a penalty in the dispersion term.[2]

Lastly, in Chapter 6, we extend VLSF codes introduced in Chapter 4 to RACs by combining the VLSF code strategy with the RAC code strategy described above. In VLSF codes for the RAC, the decoder can decode at one of the available times $n_{k,1}, n_{k,2}, \ldots, n_{k,L}$ if it believes that the number of active transmitters is $k$, and an average decoding time constraint is imposed for each number of active transmitters

$$\mathbb{E}\left[\tau_k\right] \leq N_k, \tag{1.16}$$

where $\tau_k$ is the random decoding time given that $k$ transmitters are active, taking values in $\{n_{k,\ell} \colon k \in \{0, \ldots, K\}, \ell \in \{1, \ldots, L\}\}$. We show a second-order achievability bound for this setting.

Although our achievability bound in Chapter 6 that employs independent and identically distributed (i.i.d.) codewords (across time) applies to the Gaussian RAC as well, using i.i.d. codewords for the Gaussian channel is sup-optimal in the dispersion term [24]. In Chapter 7, we present third-order asymptotic expansions in the CLT regime for the maximum achievable message set size for the Gaussian MAC under average error and maximal power constraints. Here, the maximal power constraint refers to

$$\|\mathsf{f}(m)^{n_k}\|_2^2 \leq n_k P \tag{1.17}$$

for all messages $m \in [M]$ and decoding times $n_k$, $k \in [K]$, and $P > 0$ is the available power.

Using random codewords uniformly distributed on a sphere and a maximum likelihood decoder, the derived MAC bound on each transmitter's rate matches the bound in [24] in its first- and second-order terms, and improves the third-order term achieved. The result then extends to the RAC model described in Chapter 6. In the Gaussian RAC code, random codewords are designed by concatenating $K$ partial codewords of blocklengths $n_1, n_2 - n_1, \ldots, n_K - n_{K-1}$, each drawn from a uniform distribution on a sphere of radius $\sqrt{(n_i - n_{i-1})P}$. When $k$ transmitters are active, the resulting codewords are uniformly distributed on a restricted subset of the sphere of radius $\sqrt{n_k P}$. For the RAC

[2] We are only comparing two achievability bounds, not the true value of maximum achievable message set size. Showing whether this dispersion term is tight for the MAC is an open problem [23].

model, the proposed code achieves the same first-, second- and third-order performance as the best known result for the Gaussian MAC in operation.

In the remainder of the chapter, we define notation used in this thesis.

## 1.4 Notation

### 1.4.1 Sets

For any $k, \ell \in \mathbb{N}$, we denote $[k] \triangleq \{1, \ldots, k\}$ and $[k : \ell] \triangleq \{k, \ldots, \ell\}$, where $[k : \ell] = \emptyset$ when $k > \ell$. The sets of integers, real numbers, and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. The non-negative integers and reals are denoted by $\mathbb{Z}_+$ and $\mathbb{R}_+$. We use calligraphic letters (e.g., $\mathcal{X}$) to denote alphabets and sets. For any set $\mathcal{A}$ and integer $k \leq |\mathcal{A}|$, $\binom{\mathcal{A}}{k} = \{\mathcal{B} \colon \mathcal{B} \subseteq \mathcal{A}, |\mathcal{B}| = k\}$. The collection of non-empty strict subsets of a set $\mathcal{A}$ is denoted by $\mathcal{P}(\mathcal{A}) \triangleq \{\mathcal{B} \colon \mathcal{B} \subseteq \mathcal{A}, 0 < |\mathcal{B}| < |\mathcal{A}|\}$, and the non-empty subsets are denoted by $\overline{\mathcal{P}}(\mathcal{A}) \triangleq \{\mathcal{B} \colon \mathcal{B} \subseteq \mathcal{A}, \mathcal{B} \neq \emptyset\}$.

### 1.4.2 Vectors

We use boldface letters (e.g., $\mathbf{x}$) to denote vectors if the dimension of the vector is clear from context; otherwise, we use $x^n \triangleq (x_1, \ldots, x_n)$ to indicate that it is an $n$-dimensional vector. For $a \leq b \leq n$, $x^{[a:b]} \triangleq (x_a, x_{a+1}, \ldots, x_b)$ denotes a sub-vector of $x^n$. The collection of length-$n$ vectors from the index set $\mathcal{A}$ is denoted by $x^n_{\mathcal{A}} \triangleq (x^n_a \colon a \in \mathcal{A})$, and $x^n_{\langle \mathcal{A} \rangle} \triangleq \sum_{a \in \mathcal{A}} x^n_a$.

For collection of vectors $x^n_{\mathcal{A}}$ and index $i \in [n]$, $x_{\mathcal{A},i}$ denotes the collection of scalars obtained by taking $i$-th coordinate from each vector in $x^n_{\mathcal{A}}$. We use sans serif font (e.g., $\mathsf{A}$) to denote matrices. The $i$-th entry of a vector $\mathbf{x}$ is denoted by $x_i$, and $(i, j)$-th entry of a matrix $\mathsf{A}$ is denoted by $\mathsf{A}_{i,j}$.

All-zero and all-one vectors are denoted by $\mathbf{0}$ and $\mathbf{1}$, respectively. A vector inequality $\mathbf{x} \leq \mathbf{y}$ for $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is understood element-wise, i.e., $x_i \leq y_i$ for all $i \in [n]$. We denote the inner product $\sum_{i=1}^n x_i y_i$ by $\langle \mathbf{x}, \mathbf{y} \rangle$. We use $\|\cdot\|_\infty$ and $\|\cdot\|_2$ to denote the $\ell_\infty$ and $\ell_2$ norms, i.e., $\|\mathbf{x}\|_\infty \triangleq \max\limits_{i \in [d]} |x_i|$ and $\|\mathbf{x}\|_2 \triangleq \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$. We write $\mathbf{x} \overset{\pi}{=} \mathbf{x}$ if there exists a permutation $\pi$ of $\mathbf{x}$ such that $\pi(\mathbf{x}) = \mathbf{y}$, and $\mathbf{x} \overset{\pi}{\neq} \mathbf{y}$ if such a permutation does not exist.

### 1.4.3 Random Variables

We denote random variables by capital letters (e.g., $X$) and individual realizations of random variables by lowercase letters (e.g., $x$). The set of all distributions on the channel input alphabet $\mathcal{X}$ (respectively the channel output alphabet $\mathcal{Y}$) is denoted by $\mathcal{P}$ (respectively $\mathcal{Q}$). We write $X \sim P_X$ to indicate that $X$ is distributed according to $P_X \in \mathcal{P}$. Given a distribution $P_X \in \mathcal{P}$ and a transition probability kernel $P_{Y|X}$ from $\mathcal{X}$ to $\mathcal{Y}$, we write $P_X \times P_{Y|X}$ to denote the joint distribution of $(X, Y)$, and $P_Y$ to denote the marginal distribution of $Y$, i.e., $P_Y(y) = \sum_{x \in \mathcal{X}} P_X(x) P_{Y|X}(y|x)$ for all $y \in \mathcal{Y}$. Given a conditional distribution $P_{Y|X}$, the distribution of $Y$ given $X = x$ is denoted by $P_{Y|X=x}$. The skewness of a random variable $X$ is denoted by

$$\mathrm{Sk}(X) \triangleq \frac{\mathbb{E}\left[(X - \mathbb{E}\left[X\right])^3\right]}{\mathrm{Var}\left[X\right]^{3/2}}. \tag{1.18}$$

For a sequence $\mathbf{x} = (x_1, \dots, x_n)$, the empirical distribution (or type) of $\mathbf{x}$ is denoted by

$$\hat{P}_{\mathbf{x}}(x) = \frac{1}{n} \sum_{i=1}^{n} 1\{x_i = x\}, \quad \forall\, x \in \mathcal{X}. \tag{1.19}$$

A lattice random variable is a random variable taking values in $\{a + kd \colon k \in \mathbb{Z}\}$, where $d \in \mathbb{R}_+$ is the *span* of the lattice. The special case that $a = 0$ is called arithmetic. We say that a random vector $\mathbf{X} = (X_1, \dots, X_n)$ is non-lattice if each of $X_i$, $i \in [n]$ is non-lattice, and is lattice if each of $X_i$, $i \in [n]$ is lattice.[3] We denote $X^+ \triangleq \max\{0, X\}$ and $X^- \triangleq -\min\{0, X\}$ for any random variable $X$.

The Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\mathsf{V}$ is denoted by $\mathcal{N}(\boldsymbol{\mu}, \mathsf{V})$. We use $Q(\cdot)$ to represent the complementary Gaussian cumulative distribution function (cdf)

$$Q(x) \triangleq \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left\{-\frac{t^2}{2}\right\} dt, \tag{1.20}$$

and $Q^{-1}(\cdot)$ to represent its functional inverse.

We denote the Radon-Nikodym derivative between distributions $P$ and $Q$ by $\frac{dP}{dQ}$. We denote the relative entropy and relative entropy variance between $P$ and $Q$ by $D(P\|Q) = \mathbb{E}\left[\log \frac{dP}{dQ}(X)\right]$ and by $V(P\|Q) = \mathrm{Var}\left[\log \frac{dP}{dQ}(X)\right]$, respectively, where $X \sim P$.

[3] The case where some of the coordinates of $\mathbf{X}$ are lattice and the rest of the coordinates are non-lattice is excluded.

### 1.4.4 Constants and Functions

Unless noted otherwise, we measure information in nats, and logarithms and exponents have base $e$. We define the nested logarithm function as

$$\log_{(L)}(x) \triangleq \begin{cases} \log(x) & \text{if } L = 1,\ x > 0 \\ \log(\log_{(L-1)}(x)) & \text{if } L \geq 2,\ \log_{(L-1)}(x) > 0, \end{cases} \tag{1.21}$$

where $\log_{(L)}(x)$ is undefined for all other $(L, x)$ pairs.

The $n \times n$ identity matrix is denoted by $\mathsf{I}_n$. The indicator function is denoted by $1\{\cdot\}$. For any scalar function $f(\cdot)$ and any vector $\mathbf{x} \in \mathbb{R}^n$, we form the vector of function values $f(\mathbf{x}) = (f(x_i) \colon i \in [n])$. For a set $\mathcal{D} \subseteq \mathbb{R}^n$, a vector $\mathbf{c} \in \mathbb{R}^n$, and a scalar $a$, $a\mathcal{D} + c \triangleq \{a\mathbf{x} + \mathbf{c} : \mathbf{x} \in \mathcal{D}\}$. The sphere with dimension $n$, radius $r$, and center at the origin is denoted by $\mathbb{S}^n(r) \triangleq \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| = r\}$.

### 1.4.5 Big-O and Small-o

The standard $O(\cdot)$, $o(\cdot)$, and $\Omega(\cdot)$ notations are defined as $f(n) = O(g(n))$ if $\limsup_{n\to\infty}|f(n)/g(n)| < \infty$, $f(n) = o(g(n))$ if $\lim_{n\to\infty}|f(n)/g(n)| = 0$, and $f(n) = \Omega(g(n))$ if $\lim_{n\to\infty}|f(n)/g(n)| > 0$.

Table 1.1: Vector Notation Summary

| Notation | Description |
|---|---|
| $x_s^n = \mathbf{x}_s = (x_{s,1}, \ldots, x_{s,n})$ | The length-$n$ vector that is a member of a collection indexed by $s \in \mathcal{S}$ |
| $x_{\mathcal{S}}^n = (x_s^n \colon s \in \mathcal{S})$ | The size-$\lvert\mathcal{S}\rvert$ ordered collection of length-$n$ vectors |
| $x_{\mathcal{S}}^{\mathcal{N}} = ((x_{s,t} \colon t \in \mathcal{N}) \colon s \in \mathcal{S})$ | The size-$\lvert\mathcal{S}\rvert$ ordered collection of length-$\lvert\mathcal{N}\rvert$ vectors with time indices in $\mathcal{N} \subseteq [n]$ |
| $x_{\langle\mathcal{S}\rangle}^n = \sum_{s\in\mathcal{S}} x_s^n$ | Summation of length-$n$ vectors from the collection $\mathcal{S}$ |

*Chapter 2*

# REFINED CLT, MD, AND LD THEOREMS IN PROBABILITY THEORY

## 2.1 Introduction

This chapter reviews the refined bounds and asymptotic equalities from the probability theory literature in the CLT, MD, and LD regimes.

Let $X_1, \ldots, X_n$ i.i.d. random variables with zero mean and variance $\mu_2$, and let $S_n$ denote their normalized sum

$$S_n \triangleq \frac{1}{\sqrt{n\mu_2}} \sum_{i=1}^{n} X_i. \tag{2.1}$$

We are interested in the tail probability of $S_n$, i.e., the cumulative distribution function

$$F_n(x) \triangleq \mathbb{P}\left[S_n \leq x\right]. \tag{2.2}$$

The asymptotic behavior of $F_n(x)$ is characterized by which of the following regimes $x$ falls in

- CLT regime: $x = O(1)$,
- MD regime: $x = o(\sqrt{n})$ and $\lim\limits_{n\to\infty} |x| = \infty$,
- LD regime: $x = \Omega(\sqrt{n})$.

The following section gives the preliminary definitions to present the theorems in each regime.

## 2.2 Moment and Cumulant Generating Functions

Below, we dedicate the letters $s$ and $t$ to real scalars and $z$ to complex scalars. The moment generating function (mgf) of $X$ is defined as

$$\phi(z) \triangleq \mathbb{E}\left[\exp\{zX\}\right], \quad z \in \mathbb{C}. \tag{2.3}$$

At $z = \mathsf{i}t$, where $\mathsf{i}$ is the imaginary unit, this function is called the characteristic function. The $j$-th central moment is denoted by

$$\mu_j \triangleq \mathbb{E}\left[(X - \mathbb{E}\left[X\right])^j\right]. \tag{2.4}$$

The cumulant generating function (cgf) of $X$ is defined as

$$\kappa(z) \triangleq \log \phi(z) = \sum_{j=1}^{\infty} \kappa_j \frac{z^j}{j!}, \tag{2.5}$$

where $\kappa_j$ is called the $j$-th cumulant of $X$, and there exists a one-to-one relationship between $\kappa_j$ and the central moments up to the order $j$. For example,

$$\kappa_1 = \mathbb{E}\left[X\right] \tag{2.6}$$

$$\kappa_2 = \mu_2 \tag{2.7}$$

$$\kappa_3 = \mu_3 \tag{2.8}$$

$$\kappa_4 = \mu_4 - 3\mu_2^2. \tag{2.9}$$

Skewness of a random variable $X$ is defined as

$$S(X) \triangleq \frac{\kappa_3}{\kappa_2^{3/2}}. \tag{2.10}$$

We use $\phi^{(X)}(\cdot)$ and $\kappa^{(X)}(\cdot)$ to denote the mgf and cgf of $X$ when the random variable is not clear from context. It is straightforward to see that the $j$-th cumulant of $cX$ is given by $\kappa_j^{(cX)} = c^j \kappa_j^{(X)}$, and the cgf of $X + Y$, where $X$ and $Y$ are independent, is

$$\kappa^{(X+Y)}(z) = \kappa^{(X)}(z) + \kappa^{(Y)}(z). \tag{2.11}$$

The mgf and cgf are naturally extended to $d$-dimensional random vectors. Let $\mathbf{S}$ be a $d$-dimensional random vector. The mgf and cgf of $\mathbf{S}$ are denoted by

$$\phi(\mathbf{z}) \triangleq \mathbb{E}\left[\exp\{\langle \mathbf{z}, \mathbf{S}\rangle\}\right], \quad \mathbf{z} \in \mathbb{C}^d, \tag{2.12}$$

$$\kappa(\mathbf{z}) \triangleq \log \phi(\mathbf{z}). \tag{2.13}$$

## 2.3 CLT Theorems

Central Limit Theorem states that if $\mu_2 < \infty$, then

$$S_n \to \mathcal{N}(0, 1) \quad \text{in distribution.} \tag{2.14}$$

Therefore, $F_n(x) = Q(-x)(1+o(1))$. The following theorem is a non-asymptotic refinement to this result.

**Theorem 2.3.1** (Berry-Esseen theorem [25, Ch. XVI.5, Th.2])**.** *Fix a positive integer $n$. Let $X_1, \ldots, X_n$ be $n$ independent zero-mean random variables. Let $\mu_2 \triangleq \frac{1}{n}\sum_{i=1}^{n} \mathrm{Var}\left[X_i\right] < \infty$. Define*

$$S_n = \frac{1}{\sqrt{n\mu_2}} \sum_{i=1}^{n} X_i \tag{2.15}$$

$$F_n = \mathbb{P}\left[S_n \leq x\right]. \tag{2.16}$$

*Then, for any $x \in \mathbb{R}$,*

$$|F_n(x) - Q(-x)| \leq \frac{B}{\sqrt{n}}, \tag{2.17}$$

*where*

$$T = \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[|X_i|^3\right] \tag{2.18}$$

$$B = \frac{c_0 T}{\mu_2^{3/2}}. \tag{2.19}$$

*and $0.4097 \leq c_0 \leq 0.5583$; in the i.i.d. case, the upper bound improves to $c_0 \leq 0.4690$ [26].*

The following theorem is an asymptotic equality that refines the constant $B$ in (2.17) in the i.i.d. case.

**Theorem 2.3.2** (Edgeworth Expansion [25, Ch. XVI.4, Th. 3])**.** *Let $X_1, \ldots, X_n$ be $n$ zero-mean i.i.d. random variables. Let $F_n(\cdot)$ be as defined in (2.16). Assume that $E|X_1|^{s+2} < \infty$, and*

$$\limsup_{|t|\to\infty} |\phi(\mathrm{i}t)| < 1. \tag{2.20}$$

*Then*

$$F_n(x) = Q(-x) - \phi(x)\left(\sum_{j=1}^{s} n^{-\frac{j}{2}} p_j(x)\right) + o(n^{-\frac{s}{2}}), \tag{2.21}$$

*where $p_j(x)$ is a real polynomial depending only on $\mu_1, \ldots, \mu_{j+2}$, and $\phi(x) \triangleq \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$ is the standard Gaussian density. The first two polynomials are given by*

$$p_1(x) = \frac{\kappa_3}{6\kappa_2^{3/2}}(x^2 - 1) \tag{2.22}$$

$$p_2(x) = \frac{\kappa_3^2}{72\kappa_2^3}(x^5 - 10x^3 + 15x) + \frac{\kappa^4}{24\kappa_2^2}(x^3 - 3x), \tag{2.23}$$

where $\kappa_j$'s are the cumulants defined in (2.5). The condition (2.20) is known as Cramér's characteristic function condition. It is satisfied for any random variable with absolutely continuous component and is not satisfied for any purely discrete random variable. For $s = 1$, that condition reduces to non-latticeness. Thus, Theorem 2.3.2 with $s = 1$ applies to discrete non-lattice random variables [27].

Since the cdf of lattice random variables is piece-wise constant, an approximation such as in (2.21) cannot be accurate for the entire real line. For the lattice case, the following theorem gives a corrected Edgeworth expansion that is accurate at the midpoints of the lattice.

**Theorem 2.3.3** (Continuity Corrected Edgeworth Expansion [27, Ch. 3.16])**.** *Let $X_1, \dots, X_n$ be zero-mean i.i.d. lattice random variables with span $h > 0$, and let $F_n$ be as defined in* (2.16)*. Define the adjusted cumulants*

$$\lambda_j^n \triangleq \kappa_j - \left(\frac{h}{\sqrt{\mu_2}}\right)^j \frac{B_j}{j}\frac{1}{n}, \tag{2.24}$$

*where $B_j$ is the $j$-th Bernoulli number.*[1] *Denote the infinite-length cumulant and adjusted cumulant vectors by $\boldsymbol{\kappa} = (\kappa_1, \kappa_2, \dots)$ and $\boldsymbol{\lambda} = (0, \lambda_2^n, \lambda_3^n, \dots)$. Let*

$$E_s(x, \boldsymbol{\kappa}) = Q(-x) - \phi(x)\sum_{j=1}^{s} n^{-\frac{j}{2}} p_j(x) \tag{2.25}$$

*be the Edgeworth expansion using the cumulants $\boldsymbol{\kappa}$. Then, it holds that*

$$F_n(x^+) = E_s(x^+, \boldsymbol{\lambda}) + o(n^{-\frac{s}{2}}), \tag{2.26}$$

*where $x^+$ is a midpoint on the lattice that $S_n$ is confined to, i.e., $x^+ = x + \frac{h}{2\sqrt{n\mu_2}}$ for some $x \in \mathbb{R}$ such that $\mathbb{P}\left[S_n = x\right] > 0$.*

We refer the reader to [25, Ch. XV-XVI] and [27, Ch. 2-3] for a more detailed review of the theorems in the CLT regime.

## 2.4 MD Theorems

Although Theorem 2.3.1 applies to any real $x$, if $x$ is in the MD regime (e.g., $x = \log n$), then, the remainder $\frac{B}{\sqrt{n}}$ in (2.17) becomes comparable to the Gaussian term, $Q(-x)$, making Theorem 2.3.1 loose in this regime.

[1] $B_j = 0$ for odd $j$; $B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}$.

The following theorem by Petrov gives a tight asymptotic expansion in the MD regime.

**Theorem 2.4.1** (Petrov Expansion [28, Ch. 8, Th. 4])**.** *Let $X_1, \dots, X_n$ be independent random variables. Let $\mathbb{E}\left[X_i\right] = 0$ for $i = 1, \dots, n$, $\kappa_j = \frac{1}{n}\sum_{i=1}^{n} \kappa_j^{(X_i)}$ for $j \geq 2$, and $\mathrm{Sk} = \frac{\kappa_3}{\kappa_2^{3/2}}$. Define*

$$S_n \triangleq \frac{1}{\sqrt{n\kappa_2}} \sum_{i=1}^{n} X_i \tag{2.27}$$

$$F_n(x) \triangleq \mathbb{P}\left[S_n \leq x\right]. \tag{2.28}$$

*Suppose that there exist some positive constants $t_0$ and $H$ such that the mgf satisfies*

$$\phi^{(X_i)}(t) < H \tag{2.29}$$

*for all $|t| \leq t_0$ and $i = 1, \dots, n$. This condition is called Cramér's condition. Let $x > 0$ and $x = o(\sqrt{n})$. Then, it holds that*

$$1 - F_n(x) = Q(x) \exp\left\{\frac{x^3}{\sqrt{n}}\lambda_n\left(\frac{x}{\sqrt{n}}\right)\right\}\left(1 + O\left(\frac{1+x}{\sqrt{n}}\right)\right) \tag{2.30}$$

$$F_n(-x) = Q(x) \exp\left\{\frac{-x^3}{\sqrt{n}}\lambda_n\left(\frac{-x}{\sqrt{n}}\right)\right\}\left(1 + O\left(\frac{1+x}{\sqrt{n}}\right)\right), \tag{2.31}$$

*where*

$$\lambda_n(x) \triangleq \sum_{i=0}^{\infty} a_i x^i \tag{2.32}$$

*is Cramér's series whose first two coefficients are*

$$a_0 = \frac{\mathrm{Sk}}{6} \tag{2.33}$$

$$a_1 = \frac{\kappa_4\kappa_2 - 3\kappa_3^2}{24\kappa_2^3}. \tag{2.34}$$

Inverting Theorem 2.4.1, namely, obtaining an expansion for $x$ in terms $y$ where $F_n(-x) = Q(y)$, is advantageous in many applications. For $Q(y) = \epsilon_n$, where $\{\epsilon_n\}_{n=1}^{\infty}$ is an MD sequence of probabilities (3.11), Lemma 2.4.1, below, gives the corresponding sequence of quantiles. In the CLT regime, in which $F_n(-x) \in (0, 1)$ is equal to a value independent of $n$, that expansion is known as the Corner-Fisher theorem [29], which inverts the Edgeworth expansion (Theorem 2.3.2).

**Lemma 2.4.1.** *Let $X_1, \ldots, X_n$ satisfy the conditions in Theorem 2.4.1. Let $y \triangleq Q^{-1}(\epsilon_n) = o(\sqrt{n})$. Suppose that $F_n(-x) = Q(y) = \epsilon_n$, then*

$$x = y - \frac{b_0 y^2}{\sqrt{n}} + \frac{b_1 y^3}{n} + O\left(\frac{y^4}{n^{3/2}}\right) + O\left(\frac{1}{\sqrt{n}}\right), \tag{2.35}$$

*where*

$$b_0 \triangleq \frac{\mathrm{Sk}}{6} \tag{2.36}$$

$$b_1 \triangleq \frac{3\kappa_4\kappa_2 - 4\kappa_3^2}{72\kappa_2^3}. \tag{2.37}$$

*Proof:* See Appendix A.1. ■

A weaker version of Lemma 2.4.1 with only the first two terms in (2.35), and with $\epsilon_n$ decaying polynomially with $n$ is proved in [10, Lemma 7]. Although the MD approximation to the cdf of the normalized sum in Theorem 2.4.1 is seemingly different than the CLT approximation to the same cdf (the Edgeworth expansion), their inverted theorems, i.e., Lemma 2.4.1 and the Cornish-Fisher theorem [29], respectively, have similar forms; for the continuous random variables, the Cornish-Fisher theorem admits the formula in (2.35), where $O\left(\frac{1}{\sqrt{n}}\right)$ is replaced by $\frac{b_0}{\sqrt{n}} + O\left(\frac{1}{n}\right)$. This is the main reason why the channel skewness bounds computed in the CLT regime extend to the MD regime without change. We refer the reader to [28] for further review of the MD regime.

## 2.5 LD Theorems

### 2.5.1 Chernoff Bound and Exponential Tilting

**Theorem 2.5.1** (Chernoff Bound)**.** *Let $X_1, \ldots, X_n$ be zero-mean i.i.d. random variables. Let $S_n \triangleq \sum_{i=1}^n X_i$. Then, for any $a \in \mathbb{R}$, it holds that*

$$\mathbb{P}\left[S_n \geq na\right] \leq \exp\left\{-n \sup_{t\geq 0}\{ta - \kappa(t)\}\right\}. \tag{2.38}$$

*Proof:* The proof follows by Markov's inequality after taking the exponent of $S_n$ and $na$. ■

Chernoff bound tells that probabilities in LD regime decay exponentially with $n$ unless $X$ has a heavy-tailed distribution, i.e., $\kappa(t) = \infty$ for all $t \neq 0$. For discrete $X$, (2.38) decays exponentially. In the following section, we will see that the exponent on the right-hand side of (2.38) is tight for many cases including all discrete random variables.

The operation that is applied in the proof of Chernoff's bound is called *exponential tilting* (or Esscher's transform [30]). The $t$-tilted $X$, denoted by $\tilde{X}_t$ is defined by the Radon-Nikodym derivative

$$\frac{dP_{\tilde{X}_t}}{dP_X}(x) = \exp\{tx - \kappa(t)\}, \quad \forall x \in \mathbb{R}. \tag{2.39}$$

Expressing a probability in terms of an expectation under a different measure is called *change of measure*, that is,

$$\mathbb{P}\left[X \in \mathcal{A}\right] = \int 1\{x \in \mathcal{A}\} dP = \int \left(\frac{dQ}{dP}(x)\right)^{-1} 1\{x \in \mathcal{A}\} dQ. \tag{2.40}$$

The general approach in the proofs of LD theorems is to change the measure to the tilted distribution with an appropriate $t$.

### 2.5.2 Strong Large Deviations Asymptotics

For the results in this section, we consider a sequence of $d$-dimensional random vectors $\mathbf{S}_n = (S_{n,1}, \ldots, S_{n,d})$, $n = 1, 2, \ldots$. Let $\phi_n(\cdot)$ denote the mgf of $\mathbf{S}_n$, and let $\kappa_n(\cdot)$ be the normalized cgf of $\mathbf{S}_n$ denoted by

$$\phi_n(\mathbf{z}) \triangleq \phi^{(\mathbf{S}_n)}(\mathbf{z}) \tag{2.41}$$

$$\kappa_n(\mathbf{z}) \triangleq \frac{1}{n} \log \phi_n(\mathbf{z}). \tag{2.42}$$

The Fenchel-Legendre transform of $\kappa_n(\cdot)$ is given by

$$\Lambda_n(\mathbf{x}) \triangleq \sup_{\mathbf{t} \in \mathbb{R}^d} \left\{ \langle \mathbf{t}, \mathbf{x} \rangle - \kappa_n(\mathbf{t}) \right\}, \tag{2.43}$$

where $\mathbf{x} \in \mathbb{R}^d$. The quantity (2.43) is commonly known as the *rate function* in the large deviations literature [31, Ch. 2.2].

Theorem 2.5.2, below, is a strong large deviations result for an arbitrary sequence of random vectors $\mathbf{S}_n$ in $\mathbb{R}^d$; here, *strong* refers to characterizing the exact prefactor in front of the LD exponent.

**Theorem 2.5.2** (Chaganty and Sethuraman [32, Th. 3.4])**.** *Let $\{\mathbf{a}_n\}_{n=1}^{\infty}$ be a bounded sequence of $d$-dimensional vectors. Assume that*

*(S) $\kappa_n(\mathbf{z})$ is bounded below and above, and is analytic in $\mathcal{D}^d$, where $\mathcal{D} \triangleq \{\mathbf{z} \in \mathbb{C} \colon |\mathbf{z}| < c\}$ and $c$ is a finite constant;*

*(ND) there exist a real sequence* $\{\mathbf{s}_n\}_{n=1}^{\infty}$ *and constants* $c_0$ *and* $c_1$ *that satisfy*

$$\nabla \kappa_n(\mathbf{s}_n) = \mathbf{a}_n \tag{2.44}$$

$$0 < c_0 < s_{n,j} < c_1 < c \text{ for all } j \in [d] \text{ and } n \geq 1, \tag{2.45}$$

*where* $c$ *is the constant given in condition (S), and the Hessian matrix* $\nabla^2 \kappa_n(\mathbf{s}_n)$*, which is a covariance matrix of a tilted distribution obtained from* $\mathbf{S}_n$*, is positive definite with a minimum eigenvalue bounded away from zero for all* $n$*;*

*(NL) there exists* $\delta_0 > 0$ *such that for any given* $\delta_1$ *and* $\delta_2$ *such that* $0 < \delta_1 < \delta_0 < \delta_2$

$$\sup_{\mathbf{t}:\delta_1 < \|\mathbf{t}\|_\infty \leq \delta_2} \left| \frac{\phi_n(\mathbf{s}_n + \mathrm{i}\mathbf{t})}{\phi_n(\mathbf{s}_n)} \right| = o\left(n^{-d/2}\right), \tag{2.46}$$

*where* $\mathrm{i} = \sqrt{-1}$ *is the imaginary unit.*

*Then,*

$$\mathbb{P}\left[\mathbf{S}_n \geq n\mathbf{a}_n\right] = \frac{E_{\mathrm{NL}}}{n^{d/2}} \exp\{-n\Lambda_n(\mathbf{a}_n)\}(1 + o(1)), \tag{2.47}$$

*where*

$$E_{\mathrm{NL}} \triangleq \frac{1}{(2\pi)^{d/2} \left( \prod_{j=1}^{d} s_{n,j} \right) \sqrt{\det(\nabla^2 \kappa_n(\mathbf{s}_n))}}. \tag{2.48}$$

Condition (S) of Theorem 2.5.2 is a *smoothness* assumption for the cgf $\kappa_n$, which is a generalization of Cramér's condition that appears in the large deviations theorem for the sum of i.i.d. random vectors [31, Th. 2.2.30]. Condition (S) implies that all moments of the tilted distribution obtained from $\mathbf{S}_n$ are finite. Condition (ND) is used to ensure that $\mathbf{S}_n$ is a *non-degenerate* random vector, meaning that it does not converge in distribution to a random vector with $\ell < d$ dimensions, and that the rate function $\Lambda_n(\mathbf{a}_n)$ is bounded and does not decay to zero. The latter follows from the boundedness condition in (2.45), and implies that the probability of interest is in the LD regime. The ratio $\frac{\phi_n(\mathbf{s}_n+\mathrm{i}\mathbf{t})}{\phi_n(\mathbf{s}_n)}$ in (2.46) is equal to the characteristic function of a random vector that is obtained by tilting $\mathbf{S}_n$ by $\mathbf{s}_n$ [32]. A random variable is non-lattice if and only if its characteristic function satisfies $|\phi(\mathrm{i}t)| < 1$ for all real $t \neq 0$

[25, Ch. XV, Sec. 1, Lemma 4]. Therefore, since tilting does not affect the support of a distribution, the condition (NL) requires $\mathbf{S}_n$ to be a non-lattice random vector. Condition (NL) is used to guarantee that the absolute value of that characteristic function decays to zero fast enough outside a neighborhood of the origin, which makes the random vector $\mathbf{S}_n$ behave like a sum of $n$ non-lattice random vectors.

When applied to the sum of $n$ i.i.d. random variables $\mathbf{S}_n = \sum_{i=1}^n \mathbf{A}_i$, $\kappa_n$ in (2.42) reduces to the cgf of $\mathbf{A}_1$ as

$$\kappa(\mathbf{z}) = \log \mathbb{E}\left[\exp\{\langle \mathbf{z}, \mathbf{A}_1 \rangle\}\right]. \tag{2.49}$$

In the case that $\mathcal{A}_1$ has a finite support, the expectation in (2.49) is bounded, and all moments of $\mathbf{A}_1$ are finite; therefore, condition (S) of Theorem 2.5.2 is satisfied. Further, the characteristic function of the sum of $n$ i.i.d. random vectors is equal to $n$-th power of the characteristic function of one of the summands. Therefore, the left-hand side of (2.46) decays to zero exponentially fast for the sum of i.i.d. non-lattice random vectors, satisfying condition (NL) of Theorem 2.5.2 with room to spare.

The following theorem is a strong large deviations theorem for lattice random vectors.

**Theorem 2.5.3.** *Suppose that $\mathbf{S}_n = (S_{n,1}, \ldots, S_{n,d})$, and $S_{n,j}$ is a lattice random variable with span $h_{n,j}$, i.e., $\mathbb{P}\left[S_{n,j} \in \{b_{n,j} + k h_{n,j} \colon k \in \mathbb{Z}\}\right] = 1$ for some $b_{n,j}$, such that there exist positive constants $\underline{h}_j$ and $\overline{h}_j$ satisfying $\underline{h}_j < h_{n,j} < \overline{h}_j$ for all $j \in [d]$, $n \geq 1$. Assume that conditions (S) and (ND) in Theorem 2.5.2 hold, and replace condition (NL) by*

*(L) there exists $\backslash\lambda > \backslash 0$ such that for any given $\backslash\delta$ satisfying $\backslash 0 < \backslash\delta < \backslash\lambda$,*

$$\sup_{\mathbf{t} : \delta_j < |t_j| \leq \frac{\pi}{h_{n,j}} \text{ for } j \in [d]} \left| \frac{\phi_n(\mathbf{s}_n + \mathrm{i}\mathbf{t})}{\phi_n(\mathbf{s}_n)} \right| = o\left(n^{-d/2}\right). \tag{2.50}$$

*Assume that $n\mathbf{a}_n$ is in the range of the random vector $\mathbf{S}_n$. Then,*

$$\mathbb{P}\left[\mathbf{S}_n \geq n\mathbf{a}_n\right] = \frac{E_{\mathrm{L}}}{n^{d/2}} \exp\{-n\Lambda_n(\mathbf{a}_n)\}(1 + o(1)), \tag{2.51}$$

*where*

$$E_{\mathrm{L}} \triangleq \frac{1}{(2\pi)^{d/2}\sqrt{\det(\nabla^2 \kappa_n(\mathbf{s}_n))}} \left( \prod_{j=1}^{d} \frac{h_{n,j}}{1 - \exp\{-s_{n,j} h_{n,j}\}} \right). \tag{2.52}$$

*Proof:* The one-dimensional lattice case, i.e., $d = 1$, is proved in [30, Th. 3.5]. The proof of the $d$-dimensional lattice case follows by inspecting the proofs for the $d$-dimensional non-lattice random vectors in [32, Th. 3.4] and the one-dimensional lattice random variables in [30, Th. 3.5]. Specifically, in the proof of [32, Th. 3.4], we replace [32, Th. 2.4] by [30, Th. 2.10]. The auxiliary result [30, Th. 2.10] gives the asymptotics of an expectation of a lattice random variable. The modification in the proof yields Theorem 2.5.3. ■

If $\mathbf{S}_n = (S_{n,1}, \dots, S_{n,d})$ is a sum of $n$ i.i.d. random vectors, where

$$S_{n,j} = \sum_{i=1}^{n} A_{i,j}, \quad j \in [d], \tag{2.53}$$

and $A_{1,j}$ is a lattice random variable with span $h_j$ for $j \in [d]$, then it holds that

$$\sup_{\delta_j < |t_j| \leq \frac{\pi}{h_j}} \left| \frac{\phi^{(X_{1,j})}(s_j + \mathrm{i}t_j)}{\phi^{(X_{1,j})}(s_j)} \right| < 1, \quad j \in [d]. \tag{2.54}$$

The bound (2.54) follows from [25, Ch. 15, Sec. 1, Lemma 4] since $\frac{\phi^{(A_{1,j})}(s_j+\mathrm{i}t_j)}{\phi^{(A_{1,j})}(s_j)}$ is a characteristic function of a lattice random variable with span $h_j$. The condition in (2.50) modifies the condition in (2.46) for lattice random vectors by considering a single period of that characteristic function. If $\mathbf{S}_n$ is an i.i.d. sum, the left-hand side of (2.50) decays exponentially with $n$, and condition (L), *lattice*, is satisfied. Note that if $h_{n,j} \to 0$ for all $(n, j)$ pairs, then $\mathbf{S}_n$ converges to a non-lattice random vector, and the prefactor $E_{\mathrm{L}}$ converges to the prefactor for the non-lattice random vectors, $E_{\mathrm{NL}}$.

Altuğ and Wagner derive a large deviations bound in [33, Lemma 3] that applies to the sum of $n$ i.i.d. 2-dimensional random vectors, where each summand can be either non-lattice or lattice. However, their prefactor is worse than both $E_{\mathrm{NL}}$ and $E_{\mathrm{L}}$. We refer the reader to [31], [34] for further review of the LD regime.

### 2.5.3 An LD Theorem as an Expectation

The following lemma by Polyanskiy *et al.* [5] is a non-asymptotic bound on an expectation involving $n$ independent random variables.

**Lemma 2.5.1** ([5, Lemma 47])**.** *Let $X_1, \dots, X_n$ be independent random variables, and $S_n = \sum_{i=1}^{n} X_i$. Let $\sigma^2 = \sum_{i=1}^{n} \mathrm{Var}\,[X_i] > 0$, and*

$T = \sum_{i=1}^{n} \mathbb{E}\left[|X_i - \mathbb{E}\left[X_i\right]|^3\right] < \infty$. *Then for every $\gamma$, it holds that*

$$\mathbb{E}\left[\exp\{-S_n\}1\{S_n > A\}\right] \leq 2\left(\frac{\log 2}{\sqrt{2\pi}} + \frac{2c_0 T}{\sigma^2}\right)\frac{1}{\sigma}\exp\{-A\}, \tag{2.55}$$

*where $c_0 \leq 0.56$ is given in* (2.19).

Lemma 2.5.1 becomes asymptotically tight when applied to the information density $\imath(\overline{X};Y)$, where $(\overline{X},Y) \sim P_X \times P_Y$. In this case, (2.55) becomes the expectation in change of measure given in (2.40) from $P_X \times P_Y$ to $P_X \times P_{Y|X}$, making Lemma 2.5.1 a very useful tool in channel coding analyses.

### 2.6 Usage of CLT, MD, and LD Theorems in Channel Coding

On high level analysis of channel coding, an error occurs if at least one of the following events happens

- the true message produces a small information density,
- at least one of the remaining $M-1$ (wrong) messages produces a large information density.

In Table 2.6, below, we summarize how the probabilities of these events that contribute to the error probability are bounded in various error probability regimes and coding problems.

Table 2.1: The probability theorems that are used in this thesis and in several works from the literature are summarized. No fb. and sf stand for no-feedback and stop-feedback. Error column specifies what error probability regime is considered in the asymptotic expansion.

| Work | Error | Coding problem | Probability theorem | |
|---|---|---|---|---|
| | | | True mes. | Wrong mes. |
| [5] | CLT | PPC, no fb. | Th. 2.3.1 | Lem. 2.5.1 |
| [35] | CLT | PPC, no fb. | Th. 2.3.2 | Th. 2.5.2–2.5.3 |
| [33] | LD | PPC, no fb. | Th. 2.5.2–2.5.3 | Th. 2.5.2–2.5.3 |
| Ch. 3 | MD | PPC, no fb. | Th. 2.4.1 | Th. 2.5.2–2.5.3 |
| Ch. 4–5 | CLT | PPC-MAC, sf | Th. 2.4.1 | Lem. 2.5.1 |
| [36] | Numerical | PPC, sf | Th. 2.3.2–2.3.3 | Lem. 2.5.1 |
| Ch. 6 | CLT | RAC, sf | Th. 2.3.1 | Lem. 2.5.1 |
| Ch. 7 | CLT | Gaussian MAC (no fb.)<br>Gaussian RAC (sf) | Th. 2.3.1 | Lem. 2.5.1 |

*Chapter 3*

# MODERATE DEVIATIONS ANALYSIS OF CHANNEL CODING

## 3.1 Introduction

The fundamental limit of channel coding is the maximum achievable message set size $M^*(n, \epsilon)$ given a channel $P_{Y|X}$, a blocklength $n$, and an average error probability $\epsilon$. Since determining $M^*(n, \epsilon)$ exactly is difficult for arbitrary triples $(P_{Y|X}, n, \epsilon)$, the literature investigating the behavior of $M^*(n, \epsilon)$ studies three asymptotic regimes: the CLT regime, also called the finite blocklength regime, where the error probability bound is kept constant and analyses bound the convergence of rate to capacity as $n$ grows, the large deviations (LD) regime, also called the error exponent regime, where the rate is kept constant and analyses bound the convergence of error probability to zero as $n$ grows, and the MD regime, where the error probability decays sub-exponentially to zero, and the rate approaches the capacity slower than $O(1/\sqrt{n})$. Provided more resources (in this case the blocklength), we would typically expect to see improvements in both the achievable rate and the error probability. Therefore, asymptotics that fix either rate or error probability are not practically relevant for many applications. Emerging applications in ultra-reliable low-latency communication such as tele-surgery and tactile internet have delay constraint as small as 1 ms and error probability constraint as small as $10^{-9}$ [37]. The fact that the accuracy of asymptotic expansions deteriorates at short blocklengths further motivates interest in refining the asymptotic expansions of the maximum achievable channel coding rate.

### 3.1.1 Literature Review

Channel coding analyses in the CLT regime fix a target error probability $\epsilon \in (0, 1)$ and approximate $\log M^*(n, \epsilon)$ as the blocklength $n$ approaches infinity. Examples of such results include Strassen's expansion [7] for discrete memoryless channels (DM-PPCs) with capacity $C$, positive $\epsilon$-dispersion $V_\epsilon$ [5, Sec. IV], and maximal error probability constraint $\epsilon$, showing

$$\log M^*(n, \epsilon) = nC - \sqrt{nV_\epsilon}Q^{-1}(\epsilon) + O(\log n). \tag{3.1}$$

Polyanskiy *et al.* [5] and Hayashi [4] revisit Strassen's result [7], showing that the same asymptotic expansion holds for the average error probability constraint, deriving lower and upper bounds on the coefficient of the $\log n$ term, and extending the result to Gaussian channels with maximal and average power constraints. In all asymptotic expansions other than Strassen's and throughout the paper, the *average* (over the codebook and channel statistics) error probability criterion is employed.

For channel coding in the LD regime, one fixes a rate $R = \frac{\log M}{n}$ strictly below the channel capacity and seeks to characterize the minimum achievable error probability $\epsilon^*(n, R)$ as the blocklength $n$ approaches infinity. In this regime, $\epsilon^*(n, R)$ decays exponentially with $n$. For $R$ above the critical rate, [8, Ch. 5] derives the error exponent $E(R)$, i.e.,

$$\epsilon^*(n, R) = e^{-nE(R)+o(n)}. \tag{3.2}$$

Bounds on the $o(n)$ term in (3.2) appear in [33], [38]–[40]. For the Gaussian channel with a maximal power constraint, in the LD regime, Shannon [6] derives achievability and converse bounds where the $o(n)$ term is tight up to an $O(1)$ gap. Erseghe [41] gives an alternative proof of these LD approximations using Laplace integration method.

The CLT and LD asymptotic approximations in (3.1) and (3.2), respectively, become less accurate as the $(n, \epsilon)$ pair gets farther away from the regime that is considered. Namely, the CLT approximation falls short if $\epsilon$ is small since there is a hidden $Q^{-1}(\epsilon)^2$ term inside the $O(\log n)$ term, which approaches $\infty$ as $\epsilon$ approaches 0. The LD approximation falls short if the rate $R$ is large since the second-order term $o(n)$ in the error exponent gets arbitrarily large as the rate approaches the capacity. The inability of CLT and LD regimes to provide accurate approximations for a wide range of $(n, \epsilon)$ pairs and the hope of deriving more accurate and computable approximations to the finite blocklength rate motivate a study of the non-Gaussianity in the moderate deviations (MD) regime. In the MD regime, the error probability $\epsilon_n$ decays sub-exponentially to zero, i.e., $\epsilon_n \to 0$ and $-\frac{1}{n}\log \epsilon_n \to 0$, and the rate approaches the capacity with a gap of order strictly greater than $\frac{1}{\sqrt{n}}$. This regime is practically relevant since it simultaneously considers low error probabilities and high achievable rates. For DM-PPCs with positive dispersion $V$ and a sequence of sub-exponentially decaying $\epsilon_n$, Altuğ and Wagner [42] show that

$$\log M^*(n, \epsilon_n) = nC - \sqrt{nV_{\epsilon_n}} Q^{-1}(\epsilon_n) + o(\sqrt{n} Q^{-1}(\epsilon_n)). \tag{3.3}$$

This result implies that the CLT approximation to the maximum achievable message set size $\log M^*(n, \epsilon_n) \approx nC - \sqrt{nV}Q^{-1}(\epsilon_n)$ as in (3.1), is still valid in the MD regime, leaving open the rate of convergence to that bound. Note that showing (3.9) with the knowledge of the CLT approximation (3.1) is not straightforward since, for instance, the Berry-Esseen theorem used in the CLT approximation becomes loose in the MD regime.

To discuss the accuracy of the CLT approximation (3.1), for any given channel, fix an average error probability $\epsilon$ and blocklength $n$. We define the channel's *non-Gaussianity* as

$$\zeta(n, \epsilon) \triangleq \log M^*(n, \epsilon) - (nC - \sqrt{nV_\epsilon}Q^{-1}(\epsilon)), \tag{3.4}$$

which captures the third-order term in the expansion of $\log M^*(n, \epsilon)$ around $nC$.

According to Strassen's expansion (3.1), $\zeta(n, \epsilon) = O(\log n)$, and several refinements to that result have since been obtained. For a DM-PPC with finite input alphabet $\mathcal{X}$ and output alphabet $\mathcal{Y}$, the results of [5] imply that the non-Gaussianity is bounded as

$$O(1) \leq \zeta(n, \epsilon) \leq \left(|\mathcal{X}| - \frac{1}{2}\right) \log n + O(1). \tag{3.5}$$

Further, improvements to (3.5) are enabled by considering additional characteristics of the channel. We next briefly define several channel characteristics and the corresponding refinements. Each definition relies on the channel transition probability kernel $[P_{Y|X}(y|x)]$ from $x$ to $y$, with rows corresponding to channel inputs and columns corresponding to channel outputs. See Section 3.2.4 for formal definitions. Singular channels are channels for which all entries in each column of the transition matrix are 0 or $p$ for some constant $p \in (0, 1]$, while nonsingular channels are channels that do not satisfy this property. Gallager-symmetric channels are channels for which the output alphabet can be partitioned into subsets so that for each subset of the transition probability kernel that uses inputs as rows and outputs of the subset as columns has the property that each row (respectively, column) is a permutation of each other row (respectively, column) [8, p. 94]. For Gallager-symmetric, singular channels, $\zeta(n, \epsilon) = O(1)$ [38]. For nonsingular channels, the random coding union (RCU) bound improves the lower bound in (3.5) to $\frac{1}{2} \log n + O(1)$ [2, Cor. 54]. For DM-PPCs with positive $\epsilon$-dispersion, Tomamichel and Tan [43] improve the upper bound to $\frac{1}{2}\log n + O(1)$. A random variable is called lattice if it takes values on a lattice with probability 1, and is called non-lattice otherwise. For nonsingular channels with positive $\epsilon$-dispersion and non-lattice information density, Moulin [35] shows[1]

$$\zeta(n,\epsilon) \geq \frac{1}{2}\log n + \underline{\mathrm{Sk}}\, Q^{-1}(\epsilon)^2 + \underline{B} + o(1) \tag{3.6}$$

$$\zeta(n,\epsilon) \leq \frac{1}{2}\log n + \overline{\mathrm{Sk}}\, Q^{-1}(\epsilon)^2 + \overline{B} + o(1), \tag{3.7}$$

where $\underline{\mathrm{Sk}}$, $\overline{\mathrm{Sk}}$. $\underline{B}$, and $\overline{B}$ are constants depending on the channel parameters. For the Gaussian channel with a maximal power constraint $P$, meaning that every codeword has power less than or equal to $nP$, in the CLT regime, Polyanskiy *et al.* [5] show that for the maximal power constraint $P$, the non-Gaussianity $\zeta(n,\epsilon,P)$ is bounded as

$$O(1) \leq \zeta(n,\epsilon,P) \leq \frac{1}{2}\log n + O(1). \tag{3.8}$$

Tan and Tomamichel [44] improve (3.8) to $\zeta(n,\epsilon,P) = \frac{1}{2}\log n + O(1)$, which means that in the CLT regime, the non-Gaussianity of the Gaussian channel is the same as that of nonsingular DM-PPCs with positive $\epsilon$-dispersion.

The MD result in (3.3) can be expressed as

$$\zeta(n,\epsilon_n) = o(\sqrt{n}Q^{-1}(\epsilon_n)). \tag{3.9}$$

Polyanskiy and Verdú [45] give an alternative proof of (3.9), and extend the result to the Gaussian channel with a maximal power constraint. In [46], Chubb *et al.* extend the second-order MD expansion in (3.9) to quantum channels. In [10, Lemma 3], Sakai *et al.* derive a third-order asymptotic expansion for the minimum achievable rate of lossless source coding, where $\epsilon_n$ decays polynomially with $n$, which can be extended to all MD sequences using the tools presented here. A second-order MD analysis of lossy source coding appears in [47].

Since binary hypothesis testing (BHT) is closely related to several information-theoretic problems, and admits a CLT approximation that is similar to that

[1] There is a sign error in [35, eq. (3.1)-(3.2)], which then propagates through the rest of the paper. The sign of the terms with $\mathrm{Sk}(P_X^*)$ should be positive rather than negative in both equations. The error in the achievability result originates in [35, eq. (7.15) and (7.19)], where it is missed that $\mathrm{Sk}(-X) = -\mathrm{Sk}(X)$ for any random variable $X$. The error in the converse result also stems from the sign error in [35, eq. (6.8)].

of channel coding [5], BHT is a topic of some interest in this work. Refined asymptotics of BHT receive significant attention from the information theory community. When the type-I error probability is a constant $1-\alpha \in (0,1)$ independent of the number of samples $n$ (i.e., in the Stein regime), the minimum achievable type-II error probability $\beta$ is a function of $\alpha$ and $n$, and a CLT approximation to the type-II error exponent, $-\log \beta_\alpha$, appears in [5, Lemma 58]. In [35, Th. 18], Moulin refines [5, Lemma 58] by deriving the $O(1)$ term in the type-II error exponent.[2] In the LD (or Chernoff) regime, where both error probabilities decay exponentially, the type-I and type-II error exponents appear in e.g.,[48, eq. (11.196)-(11.197)]. A second-order MD analysis of BHT appears in [49]. In [50, Th. 11], Chen *et al.* derive the third-order asymptotic expansion of the type-II error probability region in the CLT regime for composite hypothesis testing that considers a single null hypothesis and $k$ alternative hypotheses. The second-order term in their result includes an extension of the $Q^{-1}(\cdot)$ function to $k$-dimensional Gaussian random vectors.

Casting optimal coding problems in terms of hypothesis testing elucidates the fundamental limits of coding. Blahut [51] derives a lower bound on the error exponent in channel coding in terms of the asymptotics of BHT in the LD regime. Polyanskiy *et al.* derive a converse result [5, Th. 27] in channel coding using the minimax of the type-II error probability of BHT, the $\beta_\alpha$ function; they term this converse as the meta-converse bound. Kostina and Verdú prove a converse result [52, Th. 8] for fixed-length lossy compression of stationary memoryless sources using the $\beta_\alpha$ function. This result is extended to lossless joint source-channel coding in [53]. For lossless data compression, Kostina and Verdú give lower and upper bounds [52, eq. (64)] on the minimum achievable codebook size in terms of $\beta_\alpha$. For lossless multiple access source coding, also known as Slepian-Wolf coding, Chen *et al.* derive a converse result [50, Th. 19] in terms of the composite hypothesis testing version of the $\beta_\alpha$ function. The works in [5], [50], [52], [53] derive second- or third-order asymptotic expansions for their respective problems by using the asymptotics of the $\beta_\alpha$ function.

### 3.1.2 Contributions of This Chapter

The accuracy of Strassen's CLT approximation (3.1), giving $\zeta(n,\epsilon) = O(\log n)$, significantly decreases for a small blocklength $n$ and a small error probability

[2] There is a typo in [35, eq. (6.8)]. The sign of the third term in [35, eq. (6.8)] should be plus rather than minus.

$\epsilon$. This problem arises because there is a hidden $Q^{-1}(\epsilon)^2$ term inside the non-Gaussianity [35]. Note that $Q^{-1}(\epsilon)^2$ approaches $2\log\frac{1}{\epsilon}$, which in turn grows without bound as $\epsilon \to 0$. Therefore, $Q^{-1}(\epsilon)^2$ can dominate the $O(\log n)$ term if $\epsilon$ is small enough. To capture this phenomenon, we define the *channel skewness* operationally as

$$\mathrm{Sk} \triangleq \lim_{\epsilon\to 0}\liminf_{n\to\infty} \frac{\zeta(n,\epsilon)-\frac{1}{2}\log n}{Q^{-1}(\epsilon)^2}. \tag{3.10}$$

The channel skewness serves as the third-order fundamental channel characteristic after channel capacity and dispersion [5, Sec. IV]. The skewness of the information density (see (1.18), below) plays a critical role in characterizing the channel skewness. Throughout the paper, we use $\overline{S}$ and $\underline{S}$ to represent upper and lower bounds on the channel skewness $S$.

Our contributions in this chapter are summarized as follows.

- We show that for nonsingular DMCs with positive dispersion, in the MD regime, the lower and upper bounds on the non-Gaussianity in (3.6)–(3.7) hold up to the skewness term; this result justifies why the skewness approximations remain accurate even for error probabilities as small as $10^{-10}$ and blocklengths as short as $n \leq 500$.

- For Cover-Thomas symmetric channels [48, p. 190], in which all rows (and respectively columns) of the transition probability kernel are permutations of each other, the lower and upper bounds in (3.6)–(3.7) match, and we derive the term that is one order higher than the channel skewness.

- We compute the channel skewness of the Gaussian channel with a maximal power constraint by deriving refined bounds in the CLT regime; the resulting approximations have an accuracy similar to that of Shannon's LD approximations from [6].

- We derive tight bounds on the minimum achievable type-II error probability for BHT in the MD regime; our bounds yield a fourth-order asymptotic expansion that includes the third and fourth central moments of the log-likelihood ratio. The converse in our refined result for Cover-Thomas channels (second described above in the bullet) is a direct application of this expansion. Our expansion is also potentially useful in other applications, such as extending the results in [50]–[53], which rely on the BHT asymptotics, to the MD regime.

We proceed to detail each of these contributions.

A sequence of error probabilities $\{\epsilon_n\}_{n=1}^{\infty}$ is said to be a *small-to-moderate (SMD) sequence* if for all $c > 0$, there exists a positive integer $n_0(c)$ such that

$$\exp\{-cn\} \leq \epsilon_n \leq 1 - \exp\{-cn\} \tag{3.11}$$

for all $n \geq n_0(c)$, or, equivalently, $Q^{-1}(\epsilon_n) = o(\sqrt{n})$. This definition includes all error probability sequences except the LD sequences, i.e., the sequences that approach 0 or 1 exponentially fast. It therefore extends the family of MD error probability sequences to include, for example, the sequences that sub-exponentially approach 1, the sequences in the CLT regime, (where $\epsilon_n = \epsilon \in (0, 1)$, a constant independent of $n$) and sequences that do not converge. We show in Theorems 3.3.1–3.3.2 in Section 3.3.1 below that for nonsingular channels with positive dispersion and an SMD sequence $\epsilon_n$ (3.11), $\zeta(n, \epsilon_n)$ in (3.9) is bounded as

$$\begin{aligned}\zeta(n, \epsilon_n) \geq \frac{1}{2}\log n &+ \underline{\mathrm{Sk}}\, Q^{-1}(\epsilon_n)^2 \\ &+ O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1) \end{aligned} \tag{3.12}$$

$$\begin{aligned}\zeta(n, \epsilon_n) \leq \frac{1}{2}\log n &+ \overline{\mathrm{Sk}}\, Q^{-1}(\epsilon_n)^2 \\ &+ O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1), \end{aligned} \tag{3.13}$$

where the constants $\underline{\mathrm{Sk}}$ and $\overline{\mathrm{Sk}}$ are the same ones as in (3.6)–(3.7). The bounds (3.12)–(3.13) generalize (3.6)–(3.7) to non-constant error probabilities $\epsilon_n$ at the expense of not bounding the constant term; additionally (3.12)–(3.13) do not require the non-latticeness condition used in [35]. The non-Gaussianity $\zeta(n, \epsilon)$ gets arbitrarily close to $O(\sqrt{n})$ as $\epsilon_n$ approaches an exponential decay, rivaling the dispersion term in (3.1). Thus, refining the third-order term as we do in (3.12)–(3.13) is especially significant in the MD regime. The achievability bound (3.12) analyzes the RCU bound in [5, Th. 16]; the converse bound (3.13) uses the non-asymptotic converse bound in [43, Prop. 6] and the saddlepoint result in [35, Lemma 14]. For $\epsilon_n$ in the MD regime (i.e., (3.11) holds with either $\epsilon_n \to 0$ or $\epsilon_n \to 1$), neither the Berry-Esseen theorem used in [5] nor the refined Edgeworth expansion used in [35] to treat the constant $\epsilon$ case is sharp enough for the precision in (3.12)–(3.13). We replace these tools with the MD bounds found in [28, Ch. 8].

The constant terms $\underline{B}$ and $\overline{B}$ in (3.6)–(3.7) depend on whether the information density $\imath(X;Y)$ is a lattice or non-lattice random variable because both the Edgeworth expansion and the large deviation result used in [35] take distinct forms for lattice and non-lattice random variables. In [35], Moulin considers the channels with non-lattice information densities and the BSC as the only example with a lattice information density, which he analyzes separately in [35, Th. 7]. Our analysis shows that a single proof holds for lattice and non-lattice cases if we do not attempt to bound the $O(1)$ term as in this paper.

For Cover-Thomas symmetric channels, $\underline{S} = \overline{S} = S$, and we refine (3.12)–(3.13) in Theorem 3.3.3 in Section 3.3.3 below by deriving the coefficient of the $O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right)$ term. For the binary symmetric channel (BSC) and a wide range of $(n, \epsilon)$ pairs, our asymptotic approximation for the maximum achievable rate using terms up to the channel skewness, i.e., $\zeta(n, \epsilon) \approx \frac{1}{2} \log n + \mathrm{Sk}\, Q^{-1}(\epsilon)^2$ is more accurate than both of Moulin's bounds with $\underline{B}$ and $\overline{B}$ in (3.6) and (3.7); the accuracy of our approximation is similar to that of the saddlepoint approximations in [39], [40]. Moreover, for the BSC with an $(n, \epsilon)$ pair satisfying $\epsilon \in [10^{-10}, 10^{-1}]$ and $n \in [100, 500]$, including the $O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right)$ term from Theorem 3.3.3 in our approximation yields a less accurate approximation than is obtained by stopping at the channel skewness. This highlights the importance of channel skewness relative to the higher-order terms in characterizing the channel.

Theorem 3.3.4, in Section 3.3.4 below, derives lower and upper bounds on the non-Gaussianity of the Gaussian channel with a maximal power constraint in the CLT regime. Our bounds yield the channel skewness term exactly; the gap between the bounds is only $1 + \frac{1}{2}\log(1+P)$ nats for maximal power constraint $P$. Our bounds analyze Shannon's random coding and sphere-packing bounds [6] in the CLT regime, and use a tight approximation to the quantile of the noncentral $t$-distribution. It appears that Shannon's bounds are the tightest so far for the Gaussian channel, and the prior techniques from [5, Th. 54] and [44] are not sharp enough to derive the channel skewness.

Using the MD results in [28, Ch. 8] and the strong large deviations results in [32], in Theorem 3.3.5 in Section 3.3.5 below, we derive the asymptotics of BHT in the MD regime, characterizing the minimum achievable type-II error of a hypothesis test that chooses between two product distributions given that type-I error is an SMD sequence (3.11). Our result refines [49] to the third-order term.

### 3.1.3 Chapter Organization

The chapter is organized as follows. We define notation and give preliminaries to present our results in Section 3.2. Section 3.3 presents and discusses the main results. Proofs of the main results appear in Section 3.4 and in Appendix B.

## 3.2 Preliminaries

### 3.2.1 Definitions Related to Information Density

The relative entropy between distributions $P$ and $Q$ on a common alphabet, second and third central moments of the log-likelihood ratio, and the skewness of the log-likelihood ratio are denoted by

$$D(P\|Q) \triangleq \mathbb{E}\left[\log \frac{P(X)}{Q(X)}\right] \tag{3.14}$$

$$V(P\|Q) \triangleq \mathrm{Var}\left[\log \frac{P(X)}{Q(X)}\right] \tag{3.15}$$

$$T(P\|Q) \triangleq \mathbb{E}\left[\left(\log \frac{P(X)}{Q(X)} - D(P\|Q)\right)^3\right] \tag{3.16}$$

$$S(P\|Q) \triangleq \frac{T(P\|Q)}{V(P\|Q)^{3/2}}, \tag{3.17}$$

where $X \sim P$. Let $P_X \in \mathcal{P}$, $Q_Y \in \mathcal{Q}$, and $P_{Y|X}$ be a conditional distribution from $\mathcal{X}$ to $\mathcal{Y}$. The conditional versions of those quantities are denoted by

$$D(P_{Y|X}\|Q_Y|P_X) \triangleq \sum_{x\in\mathcal{X}} P_X(x) D(P_{Y|X=x}\|Q_Y) \tag{3.18}$$

$$V(P_{Y|X}\|Q_Y|P_X) \triangleq \sum_{x\in\mathcal{X}} P_X(x) V(P_{Y|X=x}\|Q_Y) \tag{3.19}$$

$$T(P_{Y|X}\|Q_Y|P_X) \triangleq \sum_{x\in\mathcal{X}} P_X(x) T(P_{Y|X=x}\|Q_Y) \tag{3.20}$$

$$\mathrm{Sk}(P_{Y|X}\|Q_Y|P_X) \triangleq \frac{T(P_{Y|X}\|Q_Y|P_X)}{V(P_{Y|X}\|Q_Y|P_X)^{3/2}}. \tag{3.21}$$

Let $(X, Y) \sim P_X \times P_{Y|X}$. The information density is defined as

$$\imath(x; y) \triangleq \log \frac{P_{Y|X}(y|x)}{P_Y(y)}, \quad \forall\, x \in \mathcal{X}, y \in \mathcal{Y}. \tag{3.22}$$

We define the following moments of the random variable $\imath(X; Y)$.

- The mutual information

$$I(P_X, P_{Y|X}) \triangleq \mathbb{E}\left[\imath(X; Y)\right] = D(P_{Y|X} \| P_Y | P_X), \tag{3.23}$$

- the unconditional information variance

$$\begin{aligned} V_{\mathrm{u}}(P_X, P_{Y|X}) &\triangleq V(P_X \times P_{Y|X} \| P_X \times P_Y) \\ &= \mathrm{Var}\left[\imath(X; Y)\right], \end{aligned} \tag{3.24}$$

- the unconditional information third central moment

$$\begin{aligned} T_{\mathrm{u}}(P_X, P_{Y|X}) &\triangleq T(P_X \times P_{Y|X} \| P_X \times P_Y) & (3.25) \\ &= \mathbb{E}\left[(\imath(X; Y) - I(P_X, P_{Y|X}))^3\right], & (3.26) \end{aligned}$$

- the unconditional information skewness

$$\mathrm{Sk}_{\mathrm{u}}(P_X, P_{Y|X}) \triangleq \mathrm{Sk}(\imath(X; Y)) = \frac{T_{\mathrm{u}}(P_X, P_{Y|X})}{V_{\mathrm{u}}(P_X, P_{Y|X})^{3/2}}, \tag{3.27}$$

- the conditional information variance

$$\begin{aligned} V(P_X, P_{Y|X}) &\triangleq V(P_{Y|X} \| P_Y | P_X) \\ &= \mathbb{E}\left[\mathrm{Var}\left[\imath(X; Y) | X\right]\right], \end{aligned} \tag{3.28}$$

- the conditional information third central moment

$$T(P_X, P_{Y|X}) \triangleq T(P_{Y|X} \| P_Y | P_X), \tag{3.29}$$

- the conditional information skewness

$$\mathrm{Sk}(P_X, P_{Y|X}) \triangleq \frac{T(P_{Y|X} \| P_Y | P_X)}{V(P_{Y|X} \| P_Y | P_X)^{3/2}}, \tag{3.30}$$

- the reverse dispersion [2, Sec. 3.4.5]

$$V_{\mathrm{r}}(P_X, P_{Y|X}) \triangleq \mathbb{E}\left[\mathrm{Var}\left[\imath(X; Y) | Y\right]\right]. \tag{3.31}$$

### 3.2.2 Discrete Memoryless Channel

A DMC is characterized by a finite input alphabet $\mathcal{X}$, a finite output alphabet $\mathcal{Y}$, and a transition probability kernel $P_{Y|X}$, where $P_{Y|X}(y|x)$ is the probability that the output of the channel is $y \in \mathcal{Y}$ given that the input to the channel is $x \in \mathcal{X}$. The $n$-letter input-output relation of a DMC is

$$P^n_{Y|X}(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i). \tag{3.32}$$

We proceed to define the channel code.

**Definition 3.2.1.** *An $(n, M, \epsilon)$-code for a DMC $P_{Y|X}$ comprises an encoding function*

$$\mathsf{f}\colon [M] \to \mathcal{X}^n, \tag{3.33}$$

*and a decoding function*

$$\mathsf{g}\colon \mathcal{Y}^n \to [M], \tag{3.34}$$

*that satisfy an average error probability constraint*

$$1 - \frac{1}{M}\sum_{m=1}^{M} P^n_{Y|X}(\mathsf{g}^{-1}(m)|\mathsf{f}(m)) \leq \epsilon. \tag{3.35}$$

The maximum achievable message set size $M^*(n, \epsilon)$ under the average error probability criterion is defined as

$$M^*(n, \epsilon) \triangleq \max\{M \colon \exists \, \text{an } (n, M, \epsilon)\text{-code}\}. \tag{3.36}$$

### 3.2.3 Definitions Related to the Optimal Input Distribution

The capacity of a DMC $P_{Y|X}$ is

$$C(P_{Y|X}) \triangleq \max_{P_X \in \mathcal{P}} I(P_X, P_{Y|X}). \tag{3.37}$$

We denote the set of capacity-achieving input distributions by

$$\mathcal{P}^\dagger \triangleq \{P_X \in \mathcal{P} \colon I(P_X, P_{Y|X}) = C(P_{Y|X})\}. \tag{3.38}$$

Even if the capacity-achieving input distributions are multiple ($|\mathcal{P}^\dagger| > 1$), the capacity-achieving output distribution is unique ($P_X, P'_X \in \mathcal{P}^\dagger$ implies

$\sum_{x\in\mathcal{X}} P_X(x)P_{Y|X}(y|x) = \sum_{x\in\mathcal{X}} P'_X(x)P_{Y|X}(y|x)$ for all $y \in \mathcal{Y}$) [8, Cor. 2 to Th. 4.5.2]. We denote this unique capacity-achieving output distribution by $Q_Y^* \in \mathcal{Q}$; $Q_Y^*$ satisfies $Q_Y^*(y) > 0$ for all $y \in \mathcal{Y}$ for which there exists an $x \in \mathcal{X}$ with $P_{Y|X}(y|x) > 0$ [8, Cor. 1 to Th. 4.5.2]. For any $P_X^\dagger \in \mathcal{P}^\dagger$, it holds that $V(P_X^\dagger, P_{Y|X}) = V_{\mathrm{u}}(P_X^\dagger, P_{Y|X})$ [5, Lemma 62].

Define $V_{\min} \triangleq \min_{P_X^\dagger \in \mathcal{P}^\dagger} V(P_X^\dagger, P_{Y|X})$ and $V_{\max} \triangleq \max_{P_X^\dagger \in \mathcal{P}^\dagger} V(P_X^\dagger, P_{Y|X})$. The $\epsilon$-dispersion [5] of a channel is defined as

$$V_\epsilon \triangleq \begin{cases} V_{\min} & \text{if } \epsilon < \frac{1}{2} \\ V_{\max} & \text{if } \epsilon \geq \frac{1}{2}. \end{cases} \tag{3.39}$$

The set of dispersion-achieving input distributions is defined as

$$\mathcal{P}^* \triangleq \left\{ P_X^\dagger \in \mathcal{P}^\dagger \colon V(P_X^\dagger, P_{Y|X}) = V_\epsilon \right\}. \tag{3.40}$$

Any $P_X^\dagger \in \mathcal{P}^\dagger$ satisfies $D(P_{Y|X=x} \| Q_Y^*) = C$ for any $x \in \mathcal{X}$ with $P_X^\dagger(x) > 0$, and $D(P_{Y|X=x} \| Q_Y^*) \leq C$ for all $x \in \mathcal{X}$ [8, Th. 4.5.1]. Hence, the support of any capacity-achieving input distribution is a subset of

$$\mathcal{X}^\dagger = \{x \in \mathcal{X} \colon D(P_{Y|X=x} \| Q_Y^*) = C\}. \tag{3.41}$$

The support of any dispersion-achieving input distribution is a subset of

$$\mathcal{X}^* \triangleq \bigcup_{P_X^* \in \mathcal{P}^*} \mathrm{supp}(P_X^*) \subseteq \mathcal{X}^\dagger. \tag{3.42}$$

The quantities below are used to describe the input distribution that achieves our lower bound $\underline{S}$ on the channel skewness $S$ in (3.10). The gradient and the Hessian of the mutual information $I(P_X, P_{Y|X})$ with respect to $P_X$ are given by [35]

$$\nabla I(P_X, P_{Y|X})_x = D(P_{Y|X=x} \| P_Y) - 1 \tag{3.43}$$

$$\nabla^2 I(P_X, P_{Y|X})_{x,x'} = -\sum_{y\in\mathcal{Y}} \frac{P_{Y|X}(y|x) P_{Y|X}(y|x')}{P_Y(y)} \tag{3.44}$$

for $(x, x') \in \mathcal{X}^2$. The matrix $-\nabla^2 I(P_X^\dagger, P_{Y|X})$ is the same for all $P_X^\dagger \in \mathcal{P}^\dagger$, and is positive semidefinite. See [35, Sec. II-D and II-E] for other properties of $-\nabla^2 I(P_X^\dagger, P_{Y|X})$. Define the $|\mathcal{X}| \times |\mathcal{X}|$ matrix $\mathsf{J}$ via its entries as

$$\mathsf{J}_{x,x'} \triangleq \begin{cases} -\nabla^2 I(P_X^\dagger, P_{Y|X})_{x,x'} & \text{if } x, x' \in \mathcal{X}^\dagger, \\ 0 & \text{otherwise.} \end{cases} \tag{3.45}$$

Define the set of vectors

$$\begin{aligned}\mathcal{L} \triangleq \{\mathbf{h} \in \mathbb{R}^{|\mathcal{X}|} \colon \sum_{x \in \mathcal{X}} h_x = 0, h_{x'} = 0 \text{ for } x' \notin \mathcal{X}^\dagger, \\ h_{x''} \geq 0 \text{ for } x'' \in \mathcal{X}^\dagger \setminus \mathcal{X}^*\}. \end{aligned} \tag{3.46}$$

The following convex optimization problem arises in the optimization of the input distribution achieving the lower bound $\underline{S}$

$$\sup_{\mathbf{h} \in \mathcal{L} \cap \mathsf{row}(\mathsf{J})} \left( \mathbf{g}^\top \mathbf{h} - \frac{1}{2} \mathbf{h}^\top \mathsf{J} \mathbf{h} \right), \tag{3.47}$$

where row$(\cdot)$ denotes the row space of a matrix. For the channels with $\mathcal{X}^* = \mathcal{X}^\dagger$ that are the focus in this paper, $\mathbf{h}$ that achieves (3.47) is given by [35, Lemma 1]

$$\mathbf{h} = \tilde{\mathsf{J}} \mathbf{g}, \tag{3.48}$$

where

$$\tilde{\mathsf{J}} = \mathsf{J}^+ - \frac{1}{\mathbf{1}^\top \mathsf{J}^+ \mathbf{1}} (\mathsf{J}^+ \mathbf{1})(\mathsf{J}^+ \mathbf{1})^\top, \tag{3.49}$$

$\mathsf{J}^+$ denotes the Moore-Penrose pseudo-inverse[3] of $\mathsf{J}$, and the optimal value of the quadratic form in (3.47) is given by $\frac{1}{2}\mathbf{g}^\top \tilde{\mathsf{J}} \mathbf{g}$. The following notation is used in our results in Section 3.3.1.

$$\begin{aligned} \mathbf{v}(P_X)_x &\triangleq \nabla V(P_X, P_{Y|X})_x, &(3.50)\\ \tilde{\mathbf{v}}_x &\triangleq V(P_{Y|X=x} \| Q_Y^*), &(3.51)\\ \overline{\mathbf{v}}(P_X)_x &\triangleq \sum_{x' \in \mathcal{X}} P_X(x') \frac{\partial V(P_{Y|X=x'} \| P_Y)}{\partial P_X(x)} &(3.52)\end{aligned}$$

for $x \in \mathcal{X}$, and

$$\begin{aligned} A_0(P_X) &\triangleq \frac{1}{8V_\epsilon} \mathbf{v}(P_X)^\top \tilde{\mathsf{J}} \mathbf{v}(P_X), &(3.53)\\ A_1(P_X) &\triangleq \frac{1}{8V_\epsilon} \overline{\mathbf{v}}(P_X)^\top \tilde{\mathsf{J}} \overline{\mathbf{v}}(P_X). &(3.54)\end{aligned}$$

See [35, Lemma 2] for properties of these quantities.

[3] Given that $\mathsf{A} = \mathsf{U}\Sigma\mathsf{V}^\top$ is the singular value decomposition of $\mathsf{A}$, $\mathsf{A}^+ \triangleq \mathsf{V}\Sigma^{-1}\mathsf{U}^\top$.

### 3.2.4 Singularity of a DMC

The following definition divides DMCs into two groups, for which the non-Gaussianity behaves differently. An input distribution-channel pair $(P_X, P_{Y|X})$ is *singular* [33, Def. 1] if for all $(x, \overline{x}, y) \in \mathcal{X} \times \mathcal{X} \times \mathcal{Y}$ such that $P_X \times P_{Y|X}(x, y) > 0$ and $P_X \times P_{Y|X}(\overline{x}, y) > 0$, it holds that

$$P_{Y|X}(y|x) = P_{Y|X}(y|\overline{x}). \tag{3.55}$$

We define the singularity parameter [35, eq. (2.25)]

$$\eta(P_X, P_{Y|X}) \triangleq 1 - \frac{V_{\mathrm{r}}(P_X, P_{Y|X})}{V_{\mathrm{u}}(P_X, P_{Y|X})}, \tag{3.56}$$

which is a constant in $[0, 1]$. The pair $(P_X, P_{Y|X})$ is singular if and only if $\eta(P_X, P_{Y|X}) = 1$ [54, Remark 1]. A channel $P_{Y|X}$ is singular if and only if $\eta(P_X^*, P_{Y|X}) = 1$ for all $P_X^* \in \mathcal{P}^*$, and nonsingular otherwise. An example of a singular channel is the binary erasure channel. Our focus in this paper is on nonsingular channels.

For brevity, if the channel is clear from the context, we drop $P_{Y|X}$ in the notation for capacity, dispersion, skewness, and singularity parameter of the channel.

## 3.3 Main Results

Our first result is third-order asymptotic expansions for the lower and upper bounds on the non-Gaussianity of nonsingular channels in the SMD regime, refining the expansion in (3.9). For symmetric channels, we further refine these bounds up to the $O\left(\frac{Q^{-1}(\epsilon)^3}{\sqrt{n}}\right)$ term. We then derive tight lower and upper bounds for the non-Gaussianity of the Gaussian channel with a maximal power constraint in the CLT regime, giving the exact expression for the channel skewness for that channel. Our last result is a fourth-order asymptotic expansion (i.e., up to the $O\left(\frac{Q^{-1}(\epsilon)^3}{\sqrt{n}}\right)$ term) for the logarithm of the minimum achievable type-II error probability of binary hypothesis tests between two product distributions in the SMD regime.

### 3.3.1 Nonsingular Channels

Theorems 3.3.1 and 3.3.2 are our achievability and converse results, respectively.

**Theorem 3.3.1.** *Suppose that $\epsilon_n$ is an SMD sequence (3.11) and that $P_{Y|X}$ is a nonsingular DMC with $V_{\min} > 0$, and $\mathcal{X}^\dagger = \mathcal{X}^*$. It holds that*

$$\zeta(n, \epsilon_n) \geq \frac{1}{2}\log n + \underline{S}Q^{-1}(\epsilon_n)^2 + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1), \tag{3.57}$$

*where*

$$\underline{S} \triangleq \max_{P_X^* \in \mathcal{P}^*} \left(\frac{\mathrm{Sk_u}(P_X^*)\sqrt{V_{\epsilon_n}}}{6} + A_0(P_X^*) + \frac{1-\eta(P_X^*)}{2(1+\eta(P_X^*))}\right). \tag{3.58}$$

*Proof:* The proof consists of two parts and extends the argument in [35] to include $\epsilon_n$ that decreases to 0 or increases to 1 as permitted by (3.11). The first part analyzes a particular relaxation [2, Th. 53] of the RCU bound [5, Th. 16] for an arbitrary distribution $P_X \in \mathcal{P}$. This approach is used in the CLT regime for a third-order analysis in [2, Th. 53] and a fourth-order analysis in [35]; a slightly different relaxation of the RCU bound also comes up in the LD regime [33]. To bound the probability $\mathbb{P}\left[\imath(\mathbf{X};\mathbf{Y}) \leq \tau\right]$, we replace the Edgeworth expansion in [35, eq. (5.30)], which gives the refined asymptotics of the Berry-Esseen theorem, with its MD version from [28, Ch. 8, Th. 2]. Note that the Edgeworth expansion yields an additive remainder term $O\left(\frac{1}{\sqrt{n}}\right)$ to the Gaussian term. This remainder is too large for $\epsilon_n \leq \frac{1}{\sqrt{n}}$ in (3.11) since it would dominate the Gaussian term in the Edgeworth expansion. Therefore, a moderate deviation result that yields a multiplicative remainder term $(1+o(1))$ is desired. We apply the large deviations result in [32, Th. 3.4] to bound the probability $\mathbb{P}\left[\imath(\overline{\mathbf{X}};\mathbf{Y}) \geq \imath(\mathbf{X};\mathbf{Y}) \geq \tau\right]$ that appears in the relaxed RCU bound, where $\mathbf{X}$ and $\overline{\mathbf{X}}$ denote the transmitted random codeword and an independent codeword drawn from the same distribution, respectively. This bound replaces the bounds in [35, eq. (7.25)-(7.27)] and refines the large deviations bound [5, Lemma 47] used in [2, Th. 53]. We show an achievability result as a function of $I(P_X)$, $V_{\mathrm{u}}(P_X)$, and $\mathrm{Sk_u}(P_X)$. If $P_X = P_X^* \in \mathcal{P}^*$, the resulting bound is (3.57) with $A_0(P_X^*)$ replaced by zero. We then optimize the bound over $P_X$ using the second-, first- and zeroth-order Taylor series expansions around $P_X^* \in \mathcal{P}^*$ of $I(P_X), V_{\mathrm{u}}(P_X)$, and $\mathrm{Sk_u}(P_X)$, respectively. Interestingly, the right-hand side of (3.57) is achieved using

$$P_X = P_X^* - \frac{Q^{-1}(\epsilon_n)}{2\sqrt{nV_{\epsilon_n}}}\tilde{\mathbf{J}}\mathbf{v}(P_X^*) \in \mathcal{P} \tag{3.59}$$

instead of a dispersion-achieving input distribution $P_X^* \in \mathcal{P}^*$ to generate i.i.d. random codewords. Note that despite being in the neighborhood of a dispersion-achieving $P_X^*$, $P_X$ in (3.59), itself, might not belong to $\mathcal{P}^*$. See Section 3.4.1 for the details of the proof. ■

In the second-order MD result in [42], Altuğ and Wagner apply the non-asymptotic bound in [8, Cor. 2 on p. 140], which turns out to be insufficiently sharp for the derivation of the third-order term.

Recall from (3.39) that $V_{\epsilon_n}$ can be either $V_{\min}$ or $V_{\max}$. We require the condition $V_{\min} > 0$ in Theorem 3.3.1, which is equivalent to $V_{\epsilon_n} > 0$ for all sufficiently large $n$,[4] since the moderate (Theorem 2.4.1) and large (Theorems 2.5.2 and 2.5.3) deviations results apply only to the random variables with positive variance. In the CLT regime, [5, Th. 45 and 48] and [43, Prop. 9-10] derive bounds on the non-Gaussianity for DMCs with $V_{\epsilon_n} = 0$. If $V_{\epsilon_n} = 0$, the scaling of the non-Gaussianity changes according to whether the DMC is exotic [5, p. 2331], which most DMCs do not satisfy, and whether $\epsilon_n$ is less than, equal to, or greater than $\frac{1}{2}$. A summary of the non-Gaussianity terms under these cases appears in [43, Fig. 1].

The condition $\mathcal{X}^\dagger = \mathcal{X}^*$ is a technical one that yields a closed-form solution (3.59) for the input distribution achieving the lower bound $\underline{S}$. If that condition is not satisfied, then the second term in (3.59) is replaced by the solution to the convex optimization problem (3.47), and $A_0(P_X^*)$ in (3.58) is replaced by the optimal value of (3.47).

**Theorem 3.3.2.** *Under the conditions of Theorem 3.3.1,*

$$\zeta(n, \epsilon_n) \leq \frac{1}{2}\log n + \overline{S} Q^{-1}(\epsilon_n)^2 + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1), \tag{3.60}$$

*where*

$$\overline{S} \triangleq \max_{P_X^* \in \mathcal{P}^*} \left(\frac{\mathrm{Sk}_{\mathrm{u}}(P_X^*)\sqrt{V_{\epsilon_n}}}{6} + \frac{1}{2} + A_0(P_X^*) - A_1(P_X^*)\right). \tag{3.61}$$

*Proof:* The proof of Theorem 3.3.2 combines the converse bound from [43, Prop. 6], which relaxes the meta-converse bound [5, Th. 27], with a saddlepoint result in [35, Lemma 14]. Combining these results and not deriving the $O(1)$ term in (3.60) yield a much simpler proof than that in [35]. While [35, proof of Th. 4] relies on the asymptotic expansion of the $\beta_{1-\epsilon}$ function, the use

[4] Note that $V_{\max} > V_{\min} = 0$ is not possible due to the uniqueness of the capacity-achieving output distribution $Q_Y^*$.

of [43, Prop. 6] allows us to bypass this part. After carefully choosing the parameter $\delta$ in [43, Prop. 6], the problem reduces to a single-letter minimax problem involving the quantities $D(P_{Y|X}\|Q_Y|P_X)$ and $V(P_{Y|X}\|Q_Y|P_X)$, where the maximization is over $P_X \in \mathcal{P}$ and the minimization is over $Q_Y \in \mathcal{Q}$. Then, similar to the steps in [35, eq. (8.22)], for the maximization over $P_X$, we separate the cases where $\|P_X - P_X^*\|_\infty \leq c_0 \frac{Q^{-1}(\epsilon_n)}{\sqrt{n}}$ or not, where $P_X^* \in \mathcal{P}^*$, and $c_0 > 0$ is a constant, and then apply [35, Lemmas 14 and 9-iii]. See Section 3.4.2 for the details. ■

### 3.3.2 The Tightness of Theorems 3.3.1 and 3.3.2

If the channel satisfies $|\mathcal{P}^*| = 1$, implying that $V_{\epsilon_n} = V_{\min} = V_{\max}$, $A_0(P_X^*) = A_1(P_X^*) = 0$, and $\eta(P_X^*) = 0$, then achievability (3.57) and converse (3.60) bounds yield the channel skewness (3.10)

$$S = \frac{\mathrm{Sk}_{\mathrm{u}}(P_X^*)\sqrt{V_{\min}}}{6} + \frac{1}{2}. \tag{3.62}$$

Cover-Thomas symmetric channels [48, p. 190] satisfy all conditions;[5] the BSC is an example. Further, if $\epsilon_n$ satisfies $Q^{-1}(\epsilon_n) = O(n^{1/6})$, then the $O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right)$ in (3.57) and (3.60) is dominated by the $O(1)$ term, giving that for Cover-Thomas symmetric channels,

$$\zeta(n, \epsilon_n) = \frac{1}{2}\log n + \mathrm{Sk}\, Q^{-1}(\epsilon_n)^2 + O(1). \tag{3.63}$$

For the BSC with crossover probability 0.11, Fig. 3.1 compares asymptotic expansions for the maximum achievable rate, $\frac{\log_2 M^*(n,\epsilon_n)}{n}$, dropping $o(\cdot)$ and $O(\cdot)$ terms except where noted otherwise. The curves plotted in Fig. 3.1 include Theorems 3.3.1 and 3.3.2 both with and without the leading term of $O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right)$ computed, various other asymptotic expansions in the CLT and LD regimes, and the non-asymptotic bounds from [5, Th. 33 and 35]. The leading term of $O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right)$ in Theorems 3.3.1 and 3.3.2 is given in Theorem 3.3.3, below. Among these asymptotic expansions, Theorems 3.3.1 and 3.3.2 ignoring the $O(\cdot)$ are the closest to the non-asymptotic bounds for most $(n, \epsilon)$ pairs shown, which highlights the significance of the channel skewness in obtaining accurate approximations to the finite blocklength coding rate in the medium $n$, small $\epsilon$ regime.

[5] Channels that are (i) Cover-Thomas weakly symmetric, have (ii) $|\mathcal{X}| = |\mathcal{Y}|$ and (iii) a positive definite $\mathsf{J}$ satisfy the same conditions [35, Prop. 6].

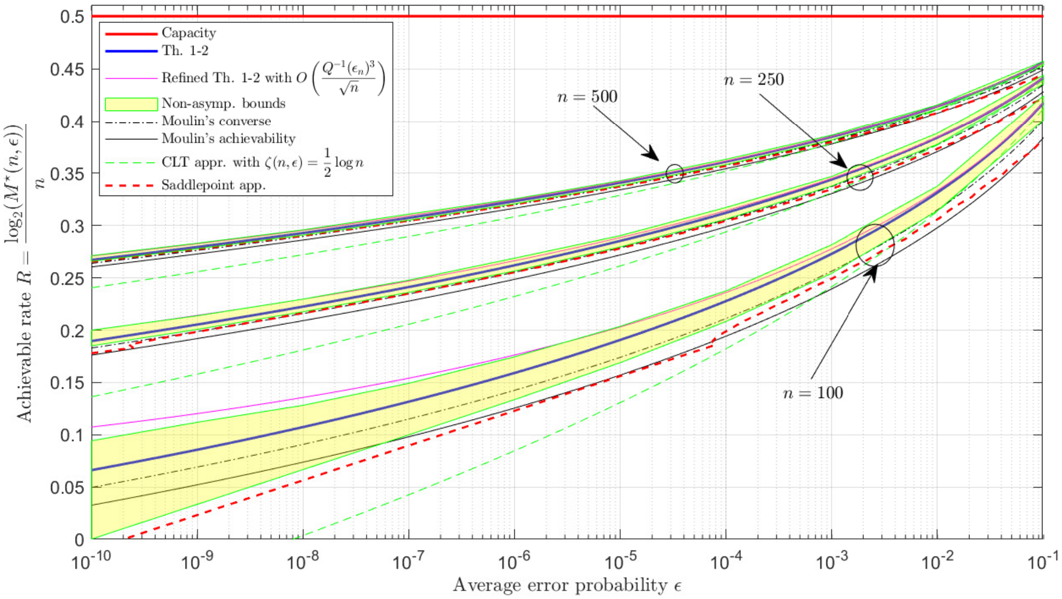


Figure 3.1: The expansion from Theorems 3.3.1 and 3.3.3, excluding the $O(\cdot)$ terms, are shown for the BSC(0.11) with $\epsilon \in [10^{-10}, 10^{-1}]$ and $n = \{100, 250, 500\}$. The upper and lower boundaries of the shaded region correspond to the non-asymptotic bounds in [5, Th. 33 and 35]; the CLT approximation that takes $\zeta(n, \epsilon) = \frac{1}{2}\log n$, is from [2, Th. 53]; Moulin's results are (3.6)–(3.7); the saddlepoint approximation is from [39, Th. 1] and [40, Sec. III-D].

In [38], Altuğ and Wagner show that in the LD regime, for Gallager-symmetric channels, the prefactors in the lower and upper bounds on the exponentially decaying error probability have the same order; that order depends on whether the channel is singular or nonsingular. Extending the analysis in [35, Sec. III-C-2)] to any Gallager-symmetric channel shows that Gallager-symmetric channels satisfy $A_0(P_X^*) = A_1(P_X^*) = 0$, but $\eta(P_X^*)$ is not necessarily zero (see [35, Sec. III-C-2)] for a counterexample), which means that (3.57) and (3.60) are not tight up to the $O(1)$ term for some Gallager-symmetric channels. The findings in [38] suggest that Theorem 3.3.1 or Theorem 3.3.2 or both could be improved for some channels. The main difference between the achievability bounds in [33], [38] and ours is that [33] bounds the error probability as

$$\epsilon \leq \mathbb{P}\left[\mathcal{D}\right] + (M-1)\mathbb{P}\left[\mathcal{D}^{\mathrm{c}} \cap \{\imath(\overline{\mathbf{X}}; \mathbf{Y}) \geq \imath(\mathbf{X}; \mathbf{Y})\}\right], \tag{3.64}$$

where

$$\mathcal{D} \triangleq \left\{ \log \frac{P^n_{Y|X}(\mathbf{Y}|\mathbf{X})}{Q^n_Y(\mathbf{Y})} < \tau \right\} \tag{3.65}$$

$$Q_Y(y) \triangleq c \left( \sum_{x \in \mathcal{X}} P_X(x) P_{Y|X}(y|x)^{1/1+\rho} \right)^{1+\rho}, \; y \in \mathcal{Y}. \tag{3.66}$$

Here $Q_Y$ is the tilted output distribution, and $\rho \in [0, 1]$, $\tau$, and $c$ are some constants. Our achievability bound uses a special case of (3.66) with $\rho = 0$, giving $Q_Y = P_Y$. Whether the more general bound in (3.66) yields an improved bound in the MD regime is a question for future work.

### 3.3.3 Refined Results for Symmetric Channels

Theorem 3.3.3 below, refines the achievability and converse results in Theorems 3.3.1–3.3.2 for Cover-Thomas symmetric channels.

**Theorem 3.3.3.** *Let $P_{Y|X}$ be a Cover-Thomas symmetric channel, $V > 0$, and $\{\epsilon_n\}_{n=1}^{\infty}$ be an SMD sequence (3.11). Then,*

$$\zeta(n, \epsilon_n) = \frac{1}{2} \log n + SQ^{-1}(\epsilon_n)^2 - \frac{3(\mu_4 - 3V^2)V - 4\mu_3^2}{72 V^{5/2}} \frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}$$
$$+ O\left( \frac{Q^{-1}(\epsilon_n)^4}{n} \right) + O(1), \tag{3.67}$$

*where $V$ and $S$ are the $\epsilon$-dispersion (3.39) and skewness (3.62) under the uniform input distribution $P_X^*$, and $\mu_k = \mathbb{E}\left[ (\imath(X;Y) - C)^k \right]$ is the $k$-th central moment of the information density under $X \sim P_X^*$.*

*Proof:* See Appendix B.5. ■

### 3.3.4 Gaussian Channel

The output of the memoryless Gaussian channel in response to the input $\mathbf{X} \in \mathbb{R}^n$ is

$$\mathbf{Y} = \mathbf{X} + \mathbf{Z}, \tag{3.68}$$

where the entries of $\mathbf{Z}$ are drawn i.i.d. from $\mathcal{N}(0, 1)$, independent of $\mathbf{X}$. The capacity and dispersion of the Gaussian channel are given by

$$C(P) \triangleq \frac{1}{2} \log(1 + P) \tag{3.69}$$

$$V(P) \triangleq \frac{P(P+2)}{2(1+P)^2}. \tag{3.70}$$

In addition to the average error probability constraint (3.35), an $(n, M, \epsilon, P)$ code for the Gaussian channel with a maximal power constraint requires that each codeword has power $nP$ exactly, i.e.,

$$\|\mathsf{f}(m)\|_2^2 \leq nP, \quad \forall\, m \in [M]. \tag{3.71}$$

The maximum achievable message set size $M^*(n, \epsilon, P)$ is defined similarly to (3.36); the corresponding non-Gaussianity is defined as

$$\zeta(n, \epsilon, P) \triangleq \log M^*(n, \epsilon, P) - (nC(P) - \sqrt{nV(P)}Q^{-1}(\epsilon)). \tag{3.72}$$

Theorem 3.3.4, below, gives lower and upper bounds on the non-Gaussianity $\zeta(n, \epsilon, P)$ in the CLT regime.

**Theorem 3.3.4.** *Fix $\epsilon \in (0, 1)$ and $P > 0$. Then,*

$$\zeta(n, \epsilon, P) \geq \frac{1}{2}\log n + S(P)Q^{-1}(\epsilon)^2 + \underline{B}(P) + O\left(\frac{1}{\sqrt{n}}\right) \tag{3.73}$$

$$\zeta(n, \epsilon, P) \leq \frac{1}{2}\log n + S(P)Q^{-1}(\epsilon)^2 + \overline{B}(P) + O\left(\frac{1}{\sqrt{n}}\right), \tag{3.74}$$

*where*

$$S(P) = \frac{6 + 6P + 4P^2 + P^3}{6(1+P)^2(2+P)} \tag{3.75}$$

$$\overline{B}(P) = \frac{9P + 14P^2 + 5P^3}{6(1+P)^2(2+P)} + \frac{1}{2}\log\left(\frac{2\pi P}{1+P}\right) \tag{3.76}$$

$$\underline{B}(P) = \overline{B}(P) - 1 - C(P) \tag{3.77}$$

*Proof:* See Appendix B.6. ■

In Fig. 3.2, the skewness approximations in Theorem 3.3.4 are compared with the non-asymptotic bounds and LD approximations from [6], and the CLT approximation from [44]. For the shown $(n, \epsilon, P)$ triples, our skewness approximation (3.74) is the closest to the non-asymptotic converse bound; our skewness approximation (3.73) is the closest to the non-asymptotic achievability bound for $\epsilon \gtrapprox 10^{-4}$ while for $\epsilon \lessapprox 10^{-4}$, Shannon's LD approximation becomes the closest.

Some remarks on Theorem 3.3.4 are given in order.

1. Although the bounds in Theorem 3.3.4 are only for the CLT regime but not the MD regime, they yield the channel skewness of the Gaussian

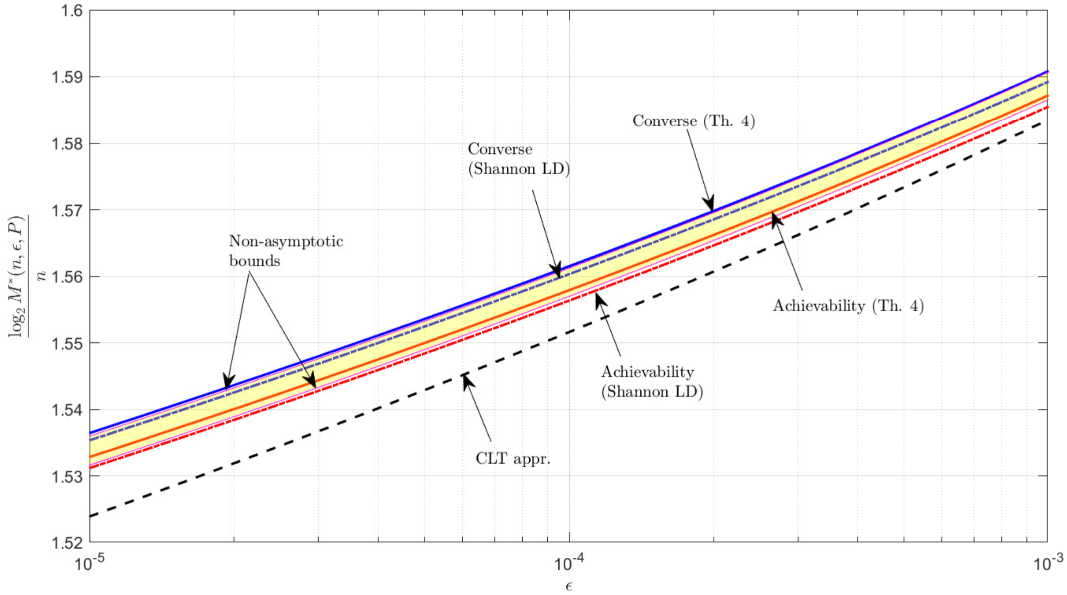


Figure 3.2: The expansions from Theorem 3.3.4, excluding the $O(\cdot)$ term, are shown for the Gaussian channel with $P = 10$, $n = 400$, and $\epsilon \in [10^{-5}, 10^{-3}]$. The upper and lower ends of the shaded region correspond to the non-asymptotic bounds from [6, eq. (20)]. Shannon's LD approximations are from [6, eq. (4)-(5)]; the CLT approximation that takes $\zeta(n, \epsilon, P) = \frac{1}{2}\log n$ is from [44].

channel as $S(P)$ since the channel skewness (3.10) is defined as the coefficient of the $Q^{-1}(\epsilon)^2$ term in the non-Gaussianity as $\epsilon \to 0$, and since the lower and upper bounds on the $Q^{-1}(\epsilon)^2$ term in (3.73)–(3.74) match.

2. The lower bound is derived by analyzing Shannon's random coding bound [6, eq. 5] in the CLT regime, which draws codewords uniformly over the sphere of radius $\sqrt{nP}$ and employs maximum likelihood decoder. The proof technique is slightly different than the bound (3.64) that we use for DMCs; we replace the auxiliary event $\mathcal{D}$ in (3.65) with $Q_Y = P_Y$ by the event

$$\mathcal{D} = \{\langle \mathbf{X}, \mathbf{Y} \rangle < \tau_n\}. \tag{3.78}$$

In the prior tightest CLT approximation for the Gaussian channel, Tan and Tomamichel [44] use (3.65) to show that $\zeta(n, \epsilon, P) \geq \frac{1}{2}\log n + O(1)$. It turns out that changing (3.65) to (3.78) is crucial in deriving the tight lower bound on the channel skewness for the Gaussian channel.

3. The converse bound (3.74) analyzes Shannon's sphere-packing bound [6, eq. 15], which is quite different than our method in Theorem 3.3.2 for DMCs. Shannon's sphere-packing converse turns out to be Polyanskiy's meta-converse [5, Th. 28] applied with the optimal auxiliary output distribution [55, Sec. VI-F], that is, after transforming the channel output $\mathbf{Y}$ to $\mathbf{Y}/\|\mathbf{Y}\|_2$, the uniform distribution over the $n$-dimensional unit sphere achieves the minimax in [5, Th. 28], and Shannon's converse bound is equal to that minimax bound. The prior tightest CLT approximation in the converse direction applies the meta-converse bound with the auxiliary output distribution $Q_Y^{(n)} = \mathcal{N}(\mathbf{0}, (1+P)\mathsf{I}_n)$, and derives $\zeta(n, \epsilon, P) \leq \frac{1}{2}\log n + O(1)$. This technique turns out to be insufficiently sharp to derive the sharp bound on the channel skewness.

4. In both of achievability and converse bounds, the quantile function of a noncentral $t$-distribution is needed. Since the noncentral $t$-distribution is not a sum of independent random variables, Theorem 2.4.1 below, which is for the MD regime, does not apply.[6] Instead, we use the Cornish-Fisher expansion of that distribution, which is available in the CLT regime. Based on the fact that the Cornish-Fisher expansions in general have the same skewness term for the CLT and MD regimes (see Lemma 2.4.1, below), we conjecture that the bounds in Theorem 3.3.4 hold in the MD regime up to the $S(P)Q^{-1}(\epsilon)^2$ term. The question that whether this is true is left to future work.

5. The converse proof first considers the codes such that all codewords have the same power, $nP$, and then uses the relationship [5, Lemma 39]

$$M(n, \epsilon, P)_{\text{eq}} \leq M(n, \epsilon, P) \leq M(n+1, \epsilon, P)_{\text{eq}}, \tag{3.79}$$

where $M(n, \epsilon, P)_{\text{eq}}$ is the maximum achievable message set size, where all codewords have equal powers. The bound in (3.79) is also shown by Shannon [6]. Let

$$\overline{B}(P)_{\text{eq}} \triangleq \overline{B}(P) - C(P) \tag{3.80}$$

$$\underline{B}(P)_{\text{eq}} \triangleq \underline{B}(P), \tag{3.81}$$

[6] The proof of Theorem 2.4.1 relies on the fact that all moments of the random variable are finite; however, the $n$-th and higher order moments of the noncentral $t$-distribution with $n$ degrees of freedom are undefined. Therefore, one needs to find another method to derive the asymptotic expansion of the cdf of the noncentral $t$-distribution in the MD regime.

giving $\overline{B}(P)_{\mathrm{eq}} - \underline{B}(P)_{\mathrm{eq}} = 1$. For codes with equal power codewords, Theorem 3.3.4 holds with $\overline{B}$ and $\underline{B}$ are replaced by the corresponding constants in (3.80)–(3.81). This extends the observation of Moulin [35] applicable to a class of symmetric DMCs with non-lattice information density, to the Gaussian channel with equal power constraint; the gap between the constant terms in the lower and upper bounds on the non-Gaussianity is also 1 nat.

### 3.3.5 Refined Asymptotics of BHT

We introduce binary hypothesis tests, which play a fundamental role in many coding theorems in the literature.

Let $P$ and $Q$ be two distributions on a common alphabet $\mathcal{X}$. Consider the binary hypothesis test

$$H_0 \colon X \sim P \tag{3.82}$$

$$H_1 \colon X \sim Q. \tag{3.83}$$

A randomized test between those two distributions is defined by a probability transition kernel $P_{W|X} \colon \mathcal{X} \to \{0, 1\}$, where 0 indicates that the test chooses $H_0$, i.e., $P$, and 1 indicates that the test chooses $H_1$, i.e., $Q$. We define the minimum achievable type-II error compatible with the type-I error bounded by $1 - \alpha$ as [5, eq. (100)]

$$\beta_\alpha(P, Q) \triangleq \min_{P_{W|X} \colon \mathbb{P}[W=0|H_0] \geq \alpha} \mathbb{P}\left[W = 0 | H_1\right]. \tag{3.84}$$

The minimum in (3.84) is achieved by test given in the Neyman-Pearson Lemma (e.g., [5, Lemma 57]), i.e.,

$$P_{W|X}(0|x) = \begin{cases} 1 & \text{if } z_x > \gamma \\ \tau & \text{if } z_x = \gamma \\ 0 & \text{if } z_x < \gamma \end{cases}, \tag{3.85}$$

where $z_x \triangleq \log \frac{dP}{dQ}(x)$ is the log-likelihood ratio, $\frac{dP}{dQ}$ denotes the Radon-Nikodym derivative, and $\tau$ and $\gamma$ are chosen so that $\alpha = \mathbb{P}\left[W = 0 | H_0\right]$.

Let $P^{(n)} = \prod_{i=1}^n P_i$ and $Q^{(n)} = \prod_{i=1}^n Q_i$, where $P_i$ and $Q_i$ are distributions on a common alphabet $\mathcal{X}$. Theorem 3.3.5, below, gives refined asymptotics of $\beta_\alpha(P^{(n)}, Q^{(n)})$ in the SMD regime.

Define $Z_i \triangleq \log \frac{dP_i}{dQ_i}(X_i)$, where $X_i \sim P_i$ for $i \in [n]$, and

$$D_i \triangleq \mathbb{E}\left[Z_i\right] = D(P_i \| Q_i) \tag{3.86}$$

$$V_i \triangleq \mathrm{Var}\left[Z_i\right] = V(P_i \| Q_i) \tag{3.87}$$

$$\mu_{k,i} \triangleq \mathbb{E}\left[(Z_i - D_i)^k\right], \quad k \geq 3 \tag{3.88}$$

$$\mathrm{Sk}_i \triangleq \mathrm{Sk}(P_i \| Q_i) = \frac{\mu_{3,i}}{V_i^{3/2}} \tag{3.89}$$

for $i \in [n]$. Define $\overline{Z}_i \triangleq \log \frac{dP_i}{dQ_i}(\overline{X}_i)$, where $\overline{X}_i \sim Q_i$ for $i \in [n]$, and the cumulant generating function of $\overline{Z}_i$

$$\kappa_i(s) \triangleq \log \mathbb{E}\left[\exp\{s\overline{Z}_i\}\right], \quad i \in [n]. \tag{3.90}$$

Let

$$D \triangleq \frac{1}{n}\sum_{i=1}^n D_i \qquad V \triangleq \frac{1}{n}\sum_{i=1}^n V_i \tag{3.91}$$

$$\mathrm{Sk} \triangleq \frac{1}{n}\sum_{i=1}^n \mathrm{Sk}_i \qquad \mu_k \triangleq \frac{1}{n}\sum_{i=1}^n \mu_{k,i},\ k \geq 3, \tag{3.92}$$

$$\kappa(s) \triangleq \frac{1}{n}\sum_{i=1}^n \kappa_i(s). \tag{3.93}$$

**Theorem 3.3.5.** *Let $P_i$, $Q_i$ be distributions on a common alphabet $\mathcal{X}$, and let $P_i$ be absolutely continuous with respect to $Q_i$ for $i \in [n]$. Let $\{\epsilon_n\}_{n=1}^\infty$ be an SMD sequence (3.11). Assume that*

*(A) $Z_i$ satisfies Cramér's condition for $i \in [n]$, i.e., $\mathbb{E}\left[\exp\{sZ_i\}\right] < \infty$ for $s \in \mathbb{R}$ in the neighborhood of 0;*

*(B) $V > 0$;*

*(C) there exist positive constants $\beta_0$, $\beta_1$, and $c > 1$ such that $\beta_0 < |\kappa(s)| < \beta_1$ for all $s \in \mathcal{D} \triangleq \{s' \in \mathbb{R} \colon |s'| < c\}$, and that $\kappa(s)$ is analytic in $\mathcal{D}$;*

*(D) if the sum $\sum_{i=1}^n \overline{Z}_i$ is non-lattice, then there exist a finite integer $\ell$, a sequence $\{w_n\}_{n=1}^\infty$ satisfying $\frac{w_n}{\log n} \to \infty$, and non-overlapping index sets $\mathcal{I}_1, \mathcal{I}_2, \ldots, \mathcal{I}_{w_n} \subset [n]$, each having size $\ell$, such that*

$$\sum_{i \in \mathcal{I}_j} \overline{Z}_i \text{ is non-lattice for } j \in [w_n]. \tag{3.94}$$

*Then, it holds that*

$$\begin{aligned}
&-\log \beta_{1-\epsilon_n}(P^{(n)}, Q^{(n)}) \\
&= nD - \sqrt{nV} Q^{-1}(\epsilon_n) + \frac{1}{2}\log n + \left( \frac{\mathrm{Sk}\sqrt{V}}{6} + \frac{1}{2} \right) Q^{-1}(\epsilon_n)^2 \\
&\quad - \frac{3(\mu_4 - 3V^2)V - 4\mu_3^2}{72 V^{5/2}} \frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}} \\
&\quad + O\left( \frac{Q^{-1}(\epsilon_n)^4}{n} \right) + O(1). \qquad (3.95)
\end{aligned}$$

*Proof:* See Appendix B.4. ■

In Fig. 3.3 below, we compare the asymptotic expansion in Theorem 3.3.5 with the true values from the Neyman-Pearson lemma, the CLT approximation from [5], and the LD approximation from [48] for BHT between two i.i.d. Bernoulli distributions. The first three terms on the right-hand side of (3.95) constitute the CLT approximation of BHT, and are shown in [5, Lemma 58] in the CLT regime. The coefficient of $Q^{-1}(\epsilon_n)^2$ in the fourth term of (3.95) is the skewness for BHT. The fifth term in (3.95) gives the fourth-order characteristic of BHT. A direct application of Theorem 3.3.5 to the meta-converse bound [5, Th. 27] shows the converse part of Theorem 3.3.3. Together with the achievability part of Theorem 3.3.3, this implies that the fourth-order characteristic of Cover-Thomas channels and BHT are the same in the sense that $C, V, S$, and $\mu_4$ in Theorem 3.3.3 are the same as $D, V, \frac{\mathrm{Sk}\sqrt{V}}{6} + \frac{1}{2}$, and $\mu_4$ in (3.95) evaluated at $P^{(n)} = P^n_{Y|X=x}$ and $Q^{(n)} = (Q^*_Y)^n$, where $x \in \mathcal{X}$ is arbitrary, and $Q^*_Y$ is the capacity-achieving output distribution.

In Theorem 3.3.5, conditions (A) and (B) are used to apply the MD result Lemma 2.4.1 to the sum $\sum_{i=1}^n Z_i$; conditions (C) and (D) are used to satisfy the conditions of the large deviations results (Theorems 2.5.2 and 2.5.3) for the random variable $\sum_{i=1}^n \overline{Z}_i$. Note that if $\sum_{i=1}^n \overline{Z}_i$ is lattice, then each of the random variables $\overline{Z}_i$, $i \in [n]$ is lattice. In the non-lattice case, the sum $\sum_{i=1}^n \overline{Z}_i$ can be non-lattice even if one of more of the $\overline{Z}_i$ is lattice. Condition (D) of Theorem 3.3.5 requires that there are $w_n \gg \log n$ non-overlapping, non-lattice partial sums of $\overline{Z}^n$, where each partial sum is a sum of $\ell$ random variables. A condition similar to condition (D) with $\ell \leq 2$ is introduced in [35, Def. 15] for the same purpose.

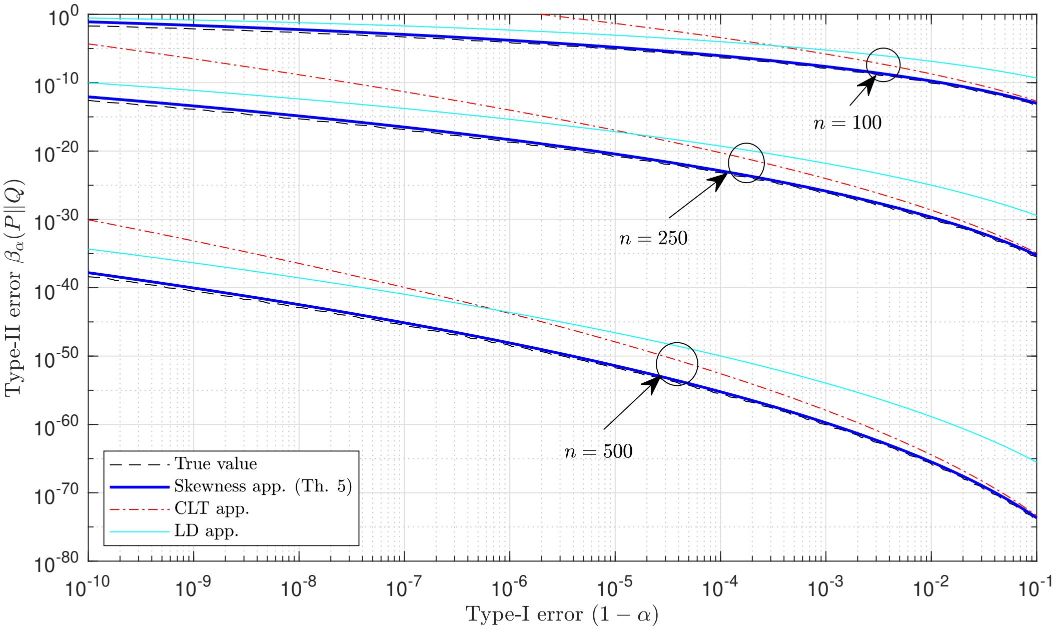


Figure 3.3: The expansion from Theorem 3.3.5, excluding the $O(\cdot)$ terms, is shown for $P_i = \text{Bern}(0.6)$, $Q_i = \text{Bern}(0.2)$, $i = 1, \ldots, n$, $n \in \{100, 250, 500\}$. Our skewness approximation is compared with the true values obtained by the Neyman-Pearson lemma, the CLT approximation from [5, Lemma 58], which consists of the terms up to $\frac{1}{2}\log n$, and the first-order LD approximation from [48, Th. 11.7.1].

## 3.4 Proofs of Theorems 3.3.1 and 3.3.2

### 3.4.1 Proof of Theorem 3.3.1

The proof consists of two parts, and follows steps similar to the achievability proof in [35]. First, we derive a refined asymptotic achievability bound for an arbitrary input distribution $P_X \in \mathcal{P}$. Then, we optimize that achievability bound over all $P_X \in \mathcal{P}$.

**Lemma 3.4.1.** *Suppose that $\epsilon_n$ is an SMD sequence (3.11). Fix some $P_X \in \mathcal{P}$ such that $(P_X, P_{Y|X})$ is a nonsingular pair and $V_{\text{u}}(P_X) > 0$ for all $n$. It holds that*

$$\begin{aligned}\log M^*(n,\epsilon_n) \geq nI(P_X) - \sqrt{nV_{\text{u}}(P_X)}Q^{-1}(\epsilon_n) + \frac{1}{2}\log n \\ +Q^{-1}(\epsilon_n)^2\left(\frac{\text{Sk}_{\text{u}}(P_X)\sqrt{V_{\text{u}}(P_X)}}{6} + \frac{1-\eta(P_X)}{2(1+\eta(P_X))}\right) \\ +O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1). \qquad (3.96)\end{aligned}$$

We require $V_{\text{u}}(P_X) > 0$ in order to apply Theorems 2.4.1–2.5.3.

*Proof of Lemma 3.4.1:* We generate $M$ i.i.d. codeword according to the input distribution $P_X^n$, and employ a maximum likelihood decoder. Let $W$ be the transmitted message that is equiprobably distributed on $[M]$, and let $\hat{W}$ be the decoder output. Define the random variables

$$Z \triangleq \imath(\mathbf{X};\mathbf{Y}) \tag{3.97}$$

$$\overline{Z} \triangleq \imath(\overline{\mathbf{X}};\mathbf{Y}), \tag{3.98}$$

where $(\mathbf{X}, \overline{\mathbf{X}}, \mathbf{Y})$ is distributed according to

$$P_{\mathbf{X},\overline{\mathbf{X}},\mathbf{Y}}(\mathbf{x},\overline{\mathbf{x}},\mathbf{y}) = P_X^n(\mathbf{x}^n)P_X^n(\overline{\mathbf{x}})P_{Y|X}^n(\mathbf{y}|\mathbf{x}). \tag{3.99}$$

The random variable $\overline{Z}$ corresponds to the information density obtained from a sample from the random codebook, independent from both $\mathbf{X}$ and the received vector $\mathbf{Y}$.

### Error analysis

Fix a threshold value $\tau_n$

$$\tau_n \triangleq nI(P_X) - \sqrt{nV_{\mathrm{u}}(P_X)}t_n, \tag{3.100}$$

where $t_n$ will be specified in (3.107), below. Define the event

$$\mathcal{D} \triangleq \{Z < \tau_n\}. \tag{3.101}$$

We weaken the RCU bound from [5, Th. 16] and bound the average error probability as

$$\begin{aligned}
&\mathbb{P}\left[\hat{W} \neq W\right] \\
&\leq \mathbb{E}\left[\min\left\{1, M-1\,\mathbb{P}\left[\overline{Z} \geq Z|\mathbf{X},\mathbf{Y}\right]\right\}\right] && (3.102)\\
&\leq \mathbb{P}\left[\mathcal{D}\right] + (M-1)\mathbb{P}\left[\overline{Z} \geq Z \geq \tau_n\right]. && (3.103)
\end{aligned}$$

Define the function

$$h(x) \triangleq \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{Q^{-1}(x)^2}{2}\right\} \tag{3.104}$$

and the sequences

$$h_n \triangleq \frac{1}{\sqrt{nV_{\mathrm{u}}(P_X)}} h(\epsilon_n) \tag{3.105}$$

$$\tilde{\epsilon}_n \triangleq \epsilon_n - h_n. \tag{3.106}$$

Below, we show that the first and second terms in (3.103) are bounded by $\tilde{\epsilon}_n$ and $h_n$, respectively. Here, $h_n$ is chosen so that $\log M$ is maximized up to the $O(Q^{-1}(\epsilon_n)^2)$ term given that the right-hand side of (3.103) is equal to $\epsilon_n$.

We set $t_n$ in (3.100) as

$$\mathbb{P}\left[\mathcal{D}\right] = \mathbb{P}\left[\frac{Z - nI(P_X)}{\sqrt{nV_u(P_X)}} \leq -t_n\right] = \tilde{\epsilon}_n. \tag{3.107}$$

Since the channel is a DMC, the random variable $\imath(X;Y)$ has a finite support and is bounded. Therefore, Cramér's condition in Theorem 2.4.1 is satisfied. Applying the MD result in Lemma 2.4.1 to (3.107), we get

$$\begin{aligned} t_n = Q^{-1}(\tilde{\epsilon}_n) &- \frac{\mathrm{Sk_u}(P_X) Q^{-1}(\tilde{\epsilon}_n)^2}{6\sqrt{n}} \\ &+ O\left(\frac{Q^{-1}(\tilde{\epsilon}_n)^3}{n}\right) + O\left(\frac{1}{\sqrt{n}}\right). \end{aligned} \tag{3.108}$$

We compute the first two derivatives of the $Q^{-1}(x)$ function as

$$(Q^{-1})'(x) = \frac{1}{Q'(Q^{-1}(x))} = \frac{-1}{h(x)} \tag{3.109}$$

$$(Q^{-1})''(x) = -\frac{Q^{-1}(x)}{h(x)^2}. \tag{3.110}$$

By taking the Taylor series expansion of $Q^{-1}(\cdot)$ around $\epsilon_n$ and using (3.108)–(3.110), we get

$$\begin{aligned} t_n = Q^{-1}(\epsilon_n) &- \frac{\mathrm{Sk_u}(P_X) Q^{-1}(\epsilon_n)^2}{6\sqrt{n}} \\ &+ O\left(\frac{Q^{-1}(\epsilon_n)^3}{n}\right) + O\left(\frac{1}{\sqrt{n}}\right). \end{aligned} \tag{3.111}$$

Next, we bound the probability $\mathbb{P}\left[\overline{Z} \geq Z \geq \tau_n\right]$. Define the random vector $\mathbf{U} \triangleq (U_1, U_2) = (Z, \overline{Z} - Z)$. and the sequence

$$\mathbf{a}_n = (a_{n,1}, a_{n,2}) = \left(\frac{\tau_n}{n}, 0\right). \tag{3.112}$$

Applying Theorems 2.5.2 or 2.5.3 depending on whether $\imath(X;Y)$ is non-lattice or lattice, we get

$$\begin{aligned} \mathbb{P}\left[\overline{Z} \geq Z \geq \tau_n\right] &= \mathbb{P}\left[\mathbf{U} \geq n\mathbf{a}_n\right] && (3.113) \\ &\leq \frac{E}{n} \exp\{-n\Lambda(\mathbf{a}_n)\}(1 + o(1)), && (3.114) \end{aligned}$$

where

$$E = \begin{cases} E_{\rm NL} & \text{if } \imath(X;Y) \text{ is non-lattice} \\ E_{\rm L} & \text{if } \imath(X;Y) \text{ is lattice.} \end{cases} \tag{3.115}$$

$$\Lambda(\mathbf{a}_n) = \sup_{\mathbf{s}_n \in \mathbb{R}^2} \{\langle \mathbf{a}_n, \mathbf{s}_n \rangle - \kappa(\mathbf{s}_n)\} \tag{3.116}$$

$$\kappa(\mathbf{s}_n) = \frac{1}{n} \log \mathbb{E}\left[\exp\{\langle \mathbf{s}_n, \mathbf{U} \rangle\}\right]. \tag{3.117}$$

Note that the functions $\kappa(\cdot)$ and $\Lambda(\cdot)$ do not depend on $n$ since $\mathbf{U}$ is an i.i.d. sum. The rate function $\Lambda(\mathbf{a}_n)$ has the Taylor series expansion

$$\begin{aligned} \Lambda(\mathbf{a}_n) = I(P_X) + (a_{n,1} - I(P_X)) + \frac{(a_{n,1} - I(P_X))^2}{(1+\eta(P_X))V_{\rm u}(P_X)} \\ + O(|a_{n,1} - I(P_X)|^3) \qquad (3.118) \\ = a_{n,1} + \frac{1}{n} \frac{Q^{-1}(\epsilon_n)^2}{1+\eta(P_X)} + O\left(\frac{Q^{-1}(\epsilon_n)^3}{n^{3/2}}\right) + O\left(\frac{1}{n}\right). \qquad (3.119) \end{aligned}$$

In the application of Theorems 2.5.2 and 2.5.3, conditions (S), (NL), and (L) are already satisfied since $U_1$ and $U_2$ have finite supports. The verification of condition (ND) and the derivation of (3.119) appear in Appendix B.1.

We set

$$\begin{aligned} \log M = nI(P_X) - \sqrt{nV_{\rm u}(P_X)}Q^{-1}(\epsilon_{\rm n}) + \frac{1}{2}\log n \\ + Q^{-1}(\epsilon_n)^2 \left( \frac{\mathrm{Sk}_{\rm u}(P_X)\sqrt{V_{\rm u}(P_X)}}{6} + \frac{1-\eta(P_X)}{2(1+\eta(P_X))} \right) \\ + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1). \end{aligned} \tag{3.120}$$

We put (3.100) into (3.111), and then (3.112) into (3.114) to bound the probability $\mathbb{P}\left[\overline{Z} \geq Z \geq \tau_n\right]$. Then, from the expansion (3.119), we get

$$M\mathbb{P}\left[\overline{Z} \geq Z \geq \tau_n\right] \leq h_n, \tag{3.121}$$

where $h_n$ is defined in (3.105). Combining (3.103), (3.107), and (3.121) completes the proof of Lemma 3.4.1. ■

To complete the proof of Theorem 3.3.1, it only remains to maximize the right-hand side of (3.96) over $P_X \in \mathcal{P}$. The following arguments extend the proof of [35, Lemma 9] to the MD regime. Define

$$G(P_X) \triangleq -\sqrt{V_{\rm u}(P_X)}Q^{-1}(\epsilon_n). \tag{3.122}$$

Let $\mathbf{g}$ be a vector whose components approach zero with a rate $O\left(\frac{Q^{-1}(\epsilon_n)}{\sqrt{n}}\right)$ satisfying $\mathbf{g}^\top\1 = 0$, and $f(\mathbf{g})$ be the right-hand side of (3.96) evaluated at $P_X = P_X^* + \mathbf{g} \in \mathcal{P}$ for some $P_X^* \in \mathcal{P}^*$. We apply the Taylor series expansion to $f(\mathbf{g})$ and get

$$\begin{aligned} f(\mathbf{g}) &\triangleq nI(P_X^*) + n\mathbf{g}^\top \nabla I(P_X^*) + \frac{n}{2}\mathbf{g}^\top \nabla^2 I(P_X^*)\mathbf{g} \\ &\quad + O(n\|\mathbf{g}\|_\infty^3) + \sqrt{n}G(P_X^*) + \sqrt{n}\mathbf{g}^\top \nabla G(P_X^*) \\ &\quad + \sqrt{n}O(\|\mathbf{g}\|_\infty^2) + \frac{1}{2}\log n \\ &\quad + Q^{-1}(\epsilon_n)^2\left(\frac{\mathrm{Sk_u}(P_X^*)\sqrt{V_\mathrm{u}(P_X^*)}}{6} + \frac{1-\eta(P_X^*)}{2(1+\eta(P_X^*))}\right) \\ &\quad + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1) & (3.123) \\ &= n\mathbf{g}^\top \nabla I(P_X^*) + \frac{n}{2}\mathbf{g}^\top \nabla^2 I(P_X^*)\mathbf{g} \\ &\quad + \sqrt{n}\mathbf{g}^\top \nabla G(P_X^*) + b, & (3.124) \end{aligned}$$

where $b$ is the right-hand side of (3.96), which is independent of $\mathbf{g}$. From (3.43) and [8, Th. 4.5.1], for every $\mathbf{g}$ such that $P_X^* + \mathbf{g}$ is a valid probability distribution and $n$ large enough, it holds

$$f(\mathbf{g}) \le \sup_{\mathbf{g}' \in \mathcal{L}} \left\{ -\frac{n}{2}\mathbf{g}'^\top \mathsf{J}\mathbf{g}' + \sqrt{n}\mathbf{g}'^\top \nabla G(P_X^*) + b \right\}, \qquad (3.125)$$

where $\mathsf{J}$ and $\mathcal{L}$ are defined in (3.45)–(3.46); and the right-hand side of (3.125) is achieved by some $\mathbf{g}$ with $g_x = 0$ for $x \notin \mathcal{X}^\dagger$. Since $P_X^*$ is dispersion-achieving, $\mathbf{g}^\top \nabla G(P_X^*) = 0$ for any $\mathbf{g}$ in the kernel of $\mathsf{J}$. Therefore, the problem (3.125) reduces to

$$\sup_{\mathbf{g} \in \mathcal{L}} \mathbf{g}^\top \mathbf{h} - \frac{1}{2}\mathbf{g}^\top \mathsf{J}\mathbf{g}, \qquad (3.126)$$

where $\mathbf{h}$ is the orthogonal projection of $\frac{\nabla G(P_X^*)}{\sqrt{n}}$ onto the row space of $\mathsf{J}$. Under the assumption $\mathcal{X}^\dagger = \mathcal{X}^*$, the supremum in (3.126) is achieved by

$$\mathbf{g}^* = \tilde{\mathsf{J}}\mathbf{h}, \qquad (3.127)$$

where $\tilde{\mathsf{J}}$ is given in (3.49), and the value of supremum in (3.126) is $A_0(P_X^*)Q^{-1}(\epsilon_n)^2$. See Appendix B.2 for the details. Combining the values of $b$ and the value of (3.126) gives the maximum of (3.96) over all input distributions $P_X \in \mathcal{P}$ and completes the proof of Theorem 3.3.1.

### 3.4.2 Proof of Theorem 3.3.2

The proof analyzes Tomamichel and Tan's non-asymptotic converse bound in [43, Prop. 6] using some techniques from [35, Lemmas 9 and 14].

The main difference between our proof and Moulin's proof in [35] is that while Moulin analyzes the meta-converse bound [5, Th. 27], we analyze a relaxation of the meta-converse, given in Lemma 3.4.3, below. In general, the analysis of the meta-converse is more involved since it requires to split the code into subcodes according to the types of the codewords, and then to carefully combine the bounds for each subcode. The advantage of Lemma 3.4.3 over the meta-converse bound is that the optimization problem in Lemma 3.4.3 can be converted into a simpler single-letter minimax problem as we show in Lemma 3.4.2, and the type-splitting step is avoided. A similar simplification to a single-letter problem using the meta-converse is possible (i) under the average error probability criterion for channels that satisfy certain symmetry conditions [5, Th. 28] (e.g., Cover-Thomas symmetric channels satisfy these symmetry conditions) and (ii) under the maximal error probability criterion for arbitrary DMCs [5, Th. 31]. While both approaches yield the same upper bound $\overline{S}$ on the skewness (in the CLT regime in Moulin's work and in the MD regime in our work), we note that Lemma 3.4.3 is not tight enough to obtain the tightest $O(1)$ term in the converse (3.60), which we do not focus on here.

We define the divergence spectrum [56, Ch. 4], [43], which gives a lower bound on the minimum type-II error probability of the binary hypothesis test, $\beta_{1-\epsilon}(P, Q)$,

$$D_s^{\epsilon}(P\|Q) \triangleq \sup\left\{\gamma \in \mathbb{R}\colon \mathbb{P}\left[\log\frac{P(X)}{Q(X)} \leq \gamma\right] \leq \epsilon\right\}, \tag{3.128}$$

where $\epsilon \in (0,1)$, $P, Q \in \mathcal{P}$, and $X \sim P$.

The main tools to prove Theorem 3.3.2, presented below, are an asymptotic expansion of the divergence spectrum in the MD regime, Lemma 3.4.2, and a channel coding converse based on the divergence spectrum, Lemma 3.4.3.

**Lemma 3.4.2.** *Fix some* $\mathbf{x} \in \mathcal{X}^n$ *and* $Q_Y \in \mathcal{Q}$. *Assume that* $\{\epsilon_n\}_{n=1}^{\infty}$ *is an*

$$\xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}) \triangleq nD(P_{Y|X}\|P_Y^{(\mathrm{o})}|P_X^{(\mathrm{i})}) - \sqrt{nV(P_{Y|X}\|P_Y^{(\mathrm{o})}|P_X^{(\mathrm{i})})}Q^{-1}(\epsilon_n) \\ + \frac{\mathrm{Sk}(P_{Y|X}\|P_Y^{(\mathrm{o})}|P_X^{(\mathrm{i})})\sqrt{V(P_{Y|X}\|P_Y^{(\mathrm{o})}|P_X^{(\mathrm{i})})}}{6}Q^{-1}(\epsilon_n)^2 \quad (3.134)$$

*SMD sequence* (3.11)*. It holds that*

$$D_s^{\epsilon_n}(P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}}\|Q_Y^n) \\ = nD_{\mathbf{x}} - \sqrt{nV_{\mathbf{x}}}Q^{-1}(\epsilon_n) + \frac{S_{\mathbf{x}}\sqrt{V_{\mathbf{x}}}}{6}Q^{-1}(\epsilon_n)^2 \\ + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1), \quad (3.129)$$

*where*

$$D_{\mathbf{x}} \triangleq D(P_{Y|X}\|Q_Y|\hat{P}_{\mathbf{x}}) \quad (3.130)$$

$$V_{\mathbf{x}} \triangleq V(P_{Y|X}\|Q_Y|\hat{P}_{\mathbf{x}}) \quad (3.131)$$

$$S_{\mathbf{x}} \triangleq S(P_{Y|X}\|Q_Y|\hat{P}_{\mathbf{x}}). \quad (3.132)$$

*Proof:* See Appendix B.3. ■

**Lemma 3.4.3** ([43, Prop. 6])**.** *Let $\epsilon_n$ be any sequence in $(0,1)$ and $P_{Y|X}$ be a DMC. Then, for any $\delta_n \in (0, 1-\epsilon_n)$, we have*

$$\log M^*(n,\epsilon_n) \leq \min_{Q_Y^{(n)} \in \mathcal{Q}^n} \max_{\mathbf{x}\in\mathcal{X}^n} D_s^{\epsilon_n+\delta_n}(P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}}\|Q_Y^{(n)}) - \log\delta_n, \quad (3.133)$$

*where $P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}} = \prod_{i=1}^n P_{Y|X=x_i}$.*

In the application of Lemma 3.4.3, we need to find the minimax of $D_s^{\epsilon_n}(P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}}\|Q_Y^n)$ in (3.129). Towards this goal, we define the asymptotic expansion $\xi\colon \mathcal{P}\times\mathcal{P} \to \mathbb{R}$ in (3.134) at the top of the next page, where $P_Y^{(\mathrm{o})}(y) = \sum_{x\in\mathcal{X}} P_X^{(\mathrm{o})}(x)P_{Y|X}(y|x)$ is the output distribution induced by $P_X^{(\mathrm{o})}$. From Lemma 3.4.2 and Lemma 3.4.3, we get

$$\log M^*(n,\epsilon) \leq \min_{P_X^{(\mathrm{o})}\in\mathcal{P}} \max_{P_X^{(\mathrm{i})}\in\mathcal{P}} \xi^{\epsilon_n+\delta_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}) - \log\delta_n \\ + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1). \quad (3.135)$$

The minimax of the first term $nD(P_{Y|X}\|P_Y^{(\mathrm{o})}|P_X^{(\mathrm{i})})$ in (3.134) satisfies the saddlepoint property (e.g., [57, Cor. 4.2])

$$D(P_{Y|X}\|Q_Y^*|P_X) \leq D(P_{Y|X}\|Q_Y^*|P_X^\dagger) \leq D(P_{Y|X}\|Q_Y|P_X^\dagger) \tag{3.136}$$

for all $P_X \in \mathcal{P}, Q_Y \in \mathcal{Q}$, where $P_X^\dagger \in \mathcal{P}^\dagger$ is a capacity-achieving input distribution, and $Q_Y^*$ is the capacity-achieving output distribution; the minimax solution for the first term only is $P_X^{(\mathrm{i})} = P_X^{(\mathrm{o})} = P_X^\dagger$; and the saddlepoint value is $D(P_{Y|X}\|Q_Y^*|P^\dagger) = C$. Since the higher-order terms in (3.134) are dominated by the first term $nD(P_{Y|X}\|P_Y^{(\mathrm{o})}|P_X^{(\mathrm{i})})$, and since the second term in (3.134) is maximized at a dispersion-achieving $P_X^*$ among the capacity-achieving $P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})} \in \mathcal{P}^\dagger$, asymptotically, the minimax

$$\min_{P_X^{(\mathrm{o})} \in \mathcal{P}} \max_{P_X^{(\mathrm{i})} \in \mathcal{P}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}) \tag{3.137}$$

is achieved when both $P_X^{(\mathrm{i})}$ and $P_X^{(\mathrm{o})}$ are in the neighborhood of some dispersion-achieving input distribution $P_X^* \in \mathcal{P}^*$. Therefore, we fix a $P_X^* \in \mathcal{P}^*$, and we consider the problem

$$\min_{P_X^{(\mathrm{o})} : \left\|P_X^{(\mathrm{o})} - P_X^*\right\|_\infty \leq \rho_n} \max_{P_X^{(\mathrm{i})} : \left\|P_X^{(\mathrm{i})} - P_X^*\right\|_\infty \leq \rho_n} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}), \tag{3.138}$$

where $\rho_n \to 0$.

After taking the Taylor series expansion of $\xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})})$ around $(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}) = (P_X^*, P_X^*)$, Moulin derives the asymptotic saddlepoint solution to the problem (3.138), which is given by [35, Lemma 14]

$$P_X^{(\mathrm{i})'} = P_X^* - \frac{Q^{-1}(\epsilon_n)}{2\sqrt{nV_{\epsilon_n}}}\tilde{\mathbf{J}}\mathbf{v}(P_X^*) \tag{3.139}$$

$$P_X^{(\mathrm{o})'} = P_X^* - \frac{Q^{-1}(\epsilon_n)}{2\sqrt{nV_{\epsilon_n}}}\tilde{\mathbf{J}}\tilde{\mathbf{v}}, \tag{3.140}$$

where $\mathbf{v}(P_X^*)$ and $\tilde{\mathbf{v}}$ are defined in (3.50)–(3.51), and the value of the saddlepoint is

$$\begin{aligned}\xi^{\epsilon_n *}(P_X^*) = nC &- \sqrt{nV_{\epsilon_n}}Q^{-1}(\epsilon_n) \\ &+ Q^{-1}(\epsilon_n)^2\left(\frac{\mathrm{Sk_u}(P_X^*)\sqrt{V_{\epsilon_n}}}{6} + A_0(P_X^*) - A_1(P_X^*)\right) \\ &+ O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1).\end{aligned} \tag{3.141}$$

We then turn our attention to (3.137). We upper bound the minimax separately for $P_X^{(\mathrm{i})}$ close to $P_X^*$ and far away from $P_X^*$. Define the set of input distributions

$$\mathcal{A} \triangleq \left\{P_X \in \mathcal{P} \colon \|P_X - P_X^*\|_\infty \leq \rho_n \text{ for some } P_X^* \in \mathcal{P}^*\right\}, \tag{3.142}$$

where

$$\rho_n \triangleq \frac{c_0 Q^{-1}(\epsilon_n)}{\sqrt{n}}, \tag{3.143}$$

and $c_0 > 0$ is a constant to be determined later. We further bound (3.137) by setting $P_X^{(\mathrm{o})} = P_X^{(\mathrm{o})\prime}$ and $P_X^{(\mathrm{o})} = P_X^*$ for some $P_X^* \in \mathcal{P}^*$ for the cases $P_X^{(\mathrm{i})} \in \mathcal{A}$ and $P_X^{(\mathrm{i})} \in \mathcal{A}^{\mathrm{c}}$, respectively, and get

$$\begin{aligned}&\min_{P_X^{(\mathrm{o})} \in \mathcal{P}} \max_{P_X^{(\mathrm{i})} \in \mathcal{P}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}) \\ &\leq \max\left\{\max_{P_X^{(\mathrm{i})} \in \mathcal{A}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})\prime}), \max_{P_X^{(\mathrm{i})} \in \mathcal{A}^{\mathrm{c}}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^*)\right\}. \end{aligned}\tag{3.144}$$

We bound the cases $P_X^{(\mathrm{i})} \in \mathcal{A}$ and $P_X^{(\mathrm{i})} \in \mathcal{A}^{\mathrm{c}}$, separately.

Considering each of the dispersion-achieving input distributions $P_X^* \in \mathcal{P}^*$ and taking the Taylor series expansion of $\xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})\prime})$ around $P_X^{(\mathrm{i})} = P_X^{(\mathrm{i})\prime}$ give

$$\max_{P_X^{(\mathrm{i})} \in \mathcal{A}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})\prime}) = \max_{P_X^* \in \mathcal{P}^*} \xi^{\epsilon_n *}(P_X^*) + O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right). \tag{3.145}$$

To bound $\max\limits_{P_X^{(\mathrm{i})} \in \mathcal{A}^{\mathrm{c}}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^*)$, we modify [35, Lemma 9 (iii)] for an SMD sequence. The result in [35] considers constant $Q^{-1}(\epsilon)$. In [35, eq. (4.7)], the third term is given as $-c_1\sqrt{n}\rho_n$, where $Q^{-1}(\epsilon)$ is absorbed in $c_1$. If we consider $Q^{-1}(\epsilon_n) \to \infty$ and carry out the same steps as [35, Lemma 9 (iii)], we see that the third term in our case becomes $-c_1\sqrt{n}\rho_n Q^{-1}(\epsilon_n)$, giving

$$\begin{aligned}&\max_{P_X^{(\mathrm{i})} \in \mathcal{A}^{\mathrm{c}}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^*) \\ &\leq nC - \sqrt{nV_{\epsilon_n}} Q^{-1}(\epsilon_n) - c_1\sqrt{n}\rho_n Q^{-1}(\epsilon_n)(1 + o(1)), \end{aligned}\tag{3.146}$$

where $c_1 > 0$ is a constant depending only on the channel parameters. We set the parameter $c_0$ so that

$$-c_0 c_1 < \max_{P_X^* \in \mathcal{P}^*} \frac{\mathrm{Sk}_{\mathrm{u}}(P_X^*)\sqrt{V_{\epsilon_n}}}{6} + A_0(P_X^*) - A_1(P_X^*). \tag{3.147}$$

Substituting (3.141) and (3.145)–(3.146) into (3.144), we get

$$\begin{aligned}&\min_{P_X^{(\mathrm{o})}\in\mathcal{P}}\ \max_{P_X^{(\mathrm{i})}\in\mathcal{P}} \xi^{\epsilon_n}(P_X^{(\mathrm{i})}, P_X^{(\mathrm{o})}) \leq nC - \sqrt{nV_{\epsilon_n}}Q^{-1}(\epsilon_n)\\ &+Q^{-1}(\epsilon_n)^2 \max_{P_X^*\in\mathcal{P}^*}\left(\frac{\mathrm{Sk_u}(P_X^*)\sqrt{V_{\epsilon_n}}}{6} + A_0(P_X^*) - A_1(P_X^*)\right)\\ &+O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right) + O(1). \end{aligned} \tag{3.148}$$

We set the parameter $\delta_n$ in (3.133) so that

$$\log\delta_n = -\frac{Q^{-1}(\epsilon_n)^2}{2} - \frac{1}{2}\log n. \tag{3.149}$$

Finally, we put (3.148) in (3.135) with $\epsilon_n$ replaced by $\epsilon_n + \delta_n$. Expanding the Taylor series of $Q^{-1}(\cdot)$ around $\epsilon_n$ completes the proof of Theorem 3.3.2.

### 3.5 Summary

This chapter investigates the third-order characteristic of nonsingular DM-PPCs, the Gaussian channel with maximal power constraint, and the binary hypothesis tests, defining a new term, the *channel skewness* for this purpose. Since the channel skewness is multiplied by $Q^{-1}(\epsilon)^2$ in the asymptotic expansion of logarithm of the maximum achievable message set size, including the channel skewness term in the approximation is particularly important to accurately approximate the non-asymptotic bounds in the small $\epsilon$ regime. In most of the chapter except the Gaussian channel extension, we derive tight bounds on the non-Gaussianity (3.4) in the MD regime. We show that Moulin's CLT approximations in (3.6)–(3.7) up to the skewness terms remain valid when the constant $\epsilon$ is replaced by an MD sequence $\epsilon_n$. For the BSC, for most pairs $(n, \epsilon)$ pairs satisfying $\epsilon \in [10^{-10}, 10^{-1}]$, $n \in [100, 500]$, we observe that our skewness approximation from Theorems 3.3.1-3.3.2 is the most accurate among the CLT approximation from [5] and the state-of-the-art LD approximations from [39], [40]. While the prefactor in those LD approximations requires to solve a different optimization problem for each $(n, \epsilon)$ pair, and arguably is less informative on the channel behavior, our skewness approximations are easily computable, and the skewness term informs us about the accuracy of the CLT approximation for a particular channel. By analyzing Shannon's bounds [6] in the CLT regime, we exactly compute the channel skewness for the Gaussian channel with maximal power constraint, and the gap between our lower and upper bounds on $\log M^*(n, \epsilon, P)$ is only $1 + C(P)$ nats. We leave the MD analysis for the Gaussian channel to future work due to lack of tools to bound the probabilities of non-i.i.d. random variables. Our techniques also apply to BHT in the MD regime, where the third-order term in the type-II error probability exponent has a similar characteristic as the channel skewness, i.e., the relative entropy skewness plays the role of information skewness in channel coding. Using our new MD approximations to BHT, many information-theoretic results that rely on BHT asymptotics such as [50], [52], [53] can be extended to the MD regime.

*Chapter 4*

# VARIABLE-LENGTH SPARSE FEEDBACK CODES FOR PPCS

## 4.1 Introduction

Although feedback does not increase the capacity of memoryless, point-to-point channels (PPCs) [12], feedback can simplify coding schemes and improve the speed of approach to capacity with coding delay. Examples that demonstrate this effect include Horstein's scheme for the binary symmetric channel (BSC) [13] and Schalkwijk and Kailath's scheme for the Gaussian channel [14], both of which leverage full channel feedback to simplify coding in the fixed-length regime. Wagner *et al.* [15] show that feedback improves the second-order term in the achievable rate as a function of blocklength for fixed-rate coding over discrete, memoryless, point-to-point channels (DM-PPCs) that have multiple capacity-achieving input distributions giving distinct dispersions.

The benefits of feedback increase for codes with multiple decoding times (called variable-length or rateless codes). In [16], Burnashev shows that feedback significantly improves the optimal error exponent of variable-length codes for DM-PPCs. In [18], Polyanskiy *et al.* extend the work of Burnashev to the finite-length regime with non-vanishing error probabilities, introducing variable-length feedback (VLF) codes, and deriving achievability and converse bounds on their performance. Tchamkerten and Telatar [58] show that Burnahsev's optimal error exponent is achieved for a family of BSCs and $Z$ channels, where the cross-over probability of the channel is unknown. For the BSC, Naghshvar *et al.* [59] propose a VLF coding scheme with a novel encoder called the small-enough-difference (SED) encoder and derive a non-asymptotic achievability bound by analyzing their scheme. Their scheme is an alternative to Burnashev's scheme to achieve the optimal error exponent. Yang *et al.* [60] extend the SED encoder to the binary asymmetric channel, of which the BSC is a special case, and derive refined non-asymptotic achievability bounds for the binary asymmetric channel. Guo and Kostina [61] propose an instantaneous SED code for a source whose symbols progressively arrive at the encoder in real time.

The feedback in VLF codes can be limited in two dimensions: amount and frequency. Here, the amount refers to how much feedback is sent from the receiver at each time feedback is available; the frequency refers to how many times feedback is available throughout the communication epoch. The extreme cases in the frequency are no feedback and feedback after every channel use. The extreme cases in the amount are full feedback and stop feedback. In full feedback, at time $n_i$, the receiver sends all symbols received until that time, $Y^{n_i}$, which can be used by the transmitter to encode the $n_{i+1}-$th symbol. In stop feedback, the receiver sends a single bit of feedback to inform the transmitter whether to stop transmitting. Unlike full-feedback codes, variable-length stop-feedback (VLSF) codes employ codewords that are fixed when the code is designed; that is, feedback affects how much of a codeword is sent but does not affect the codeword's value. VLSF codes with feedback after every channel use are defined by Polyanskiy *et al.* in [18]. The result in [18, Th. 2] shows that variable-length coding improves the first-order term in the asymptotic expansion of the maximum achievable message set size from $NC$ to $\frac{NC}{1-\epsilon}$, where $C$ is the capacity of the DM-PPC, $N$ is the average decoding time, and $\epsilon$ is the average error probability. The second-order term achievable for VLF codes is $O(\log N)$, which means that VLF codes have zero dispersion and that the convergence to the capacity is much faster than that achieved by the fixed-length codes [5], [62]. In [63], Altuğ *et al.* modify the VLSF coding paradigm by replacing the average decoding time constraint with a constraint on the probability that the decoding time exceeds a target value; the benefit in the first-order term does not appear under this probabilistic delay constraint, and the dispersion is no longer zero. A VLSF scenario where the feedback is noisy and the largest available decoding time is finite is studied in [64]. For VLSF codes, Forney [17] shows an achievable error exponent that is strictly better than that of fixed-length, no-feedback codes and is strictly worse than Burnashev's error exponent for variable-length full-feedback codes. Ginzach *et al.* [65] derive the exact error exponent of VLSF codes for the BSC.

Decoding of VLSF codes can be viewed through the lens of a number of sequential hypothesis tests (SHTs) equal to the number of possible messages. Each SHT, at increasingly larger stopping times, compares a hypothesis $H_0$ corresponding to a particular transmitted message to the hypothesis $H_1$ corresponding to the marginal distribution of the channel output. In [66], Berlin *et al.* derive a bound on the average stopping time of an SHT. They then use this bound to derive a non-asymptotic converse bound for VLF codes. This result is an alternative proof for the converse of Burnashev's error exponent [16]. Polyanskiy *et al.* [18] point out that the exact asymptotics of Wald's SHT framework in [67] can be used to improve the converse bound on the performance of VLF codes.

In the scenario where a decoding decision can be made at any time, Wald's sequential probability ratio test (SPRT) achieves the minimum average stopping time subject to type-I and type-II error probability constraints [67]. The SPRT takes new samples as long as the log-likelihood ratio stays between two thresholds. By analyzing SPRTs, Li and Tan [68] derive the second-order term in the achievable type-I and type-II error exponents, where both error probabilities decay exponentially with the average stopping time $N$. Pan *et al.* [69] study the second-order asymptotics of a composite SHT under a probabilistic constraint on the stopping time. Lalitha and Javidi [70] study the achievable error exponents in a scenario with only 2 available stopping times and a probabilistic stopping time constraint.

We use the number of potential decoding times, $L$, to classify the feedback frequency and assume that feedback is sent only at those potential decoding times. While high rates of feedback are impractical for many applications — especially wireless applications on half-duplex devices — most prior work on VLSF codes [18], [63], [71]–[75] considers the densest feedback possible, i.e., $L = \infty$ and any decoding time $n_i = i - 1$, $i \in \mathbb{Z}_+$ is available for decoding. Notable exceptions are [76] where Kim *et al.* choose the decoding time from the set $\{d, 2d, \ldots, Ld\}$ for some $d \in \mathbb{Z}_+$ and $L < \infty$ and [77] where Vakilinia *et al.* introduce a sequential differential optimization (SDO) algorithm to optimize the choices of the $L$ potential decoding times $n_1, \ldots, n_L$, approximating the distribution of the random decoding time $\tau$ by a Gaussian random variable. They apply the SDO algorithm to non-binary low-density parity-check codes over binary-input, additive white Gaussian channels; the mean and variance of $\tau$ are determined through simulation. Extensions of [77] include [78], which uses a new Viterbi algorithm at the decoder, and [79], which extends [77] to account for the feedback rate and applies the SDO algorithm to random linear codes over the binary erasure channel. Lalitha and Javidi [80] consider variable-length full-feedback codes with delay constraints, where they show that Burnashev's optimal error exponent can be achieved by only $L = 3$ decoding times by truncating the Yamamoto-Itoh scheme [81]. Building upon an earlier version of the present chapter [82], Yang *et al.* [36] construct an integer program to minimize the upper bound on the average blocklength subject to constraints on the average error probability and the minimum gap between consecutive decoding times. By employing a combination of the Edgeworth expansion [25, Sec. XVI.4] and the Petrov expansion (Theorem 2.4.1), that paper develops an approximation to the cumulative distribution function of the information density random variable $\imath(X^n; Y^n)$; the numerical comparison of their approximation and the empirical cumulant distribution function shows that the approximation is tight even for small values of $n$. Their analysis uses this tight approximation to numerically evaluate the non-asymptotic achievability bound (Theorem 4.3.2, below) for the BSC, binary erasure channel, and binary-input Gaussian PPC for all $L \leq 32$. The resulting numerical results show performance that closely approaches Polyanskiy's VLSF achievability bound [18] with a relatively small $L$. For the binary erasure channel, [36] also proposes a new zero-error code that employs systematic transmission followed by random linear fountain coding; the proposed code outperforms Polyanskiy's achievability bound.

Like [77]–[79], this chapter studies VLSF codes under a finite constraint $L$ on the number of decoding times. While [77]–[79] focus on practical coding and performance, our goal is new achievability bounds on the asymptotic rate achievable by VLSF codes between $L = 1$ (the fixed-length regime analyzed in [5], [44]) and $L = \infty$ (the classical variable-length regime defined in [18, Def. 1], where all decoding times 0, 1, 2, … are available). In this chapter, we study VLSF codes over DM-PPCs. In our analysis, we consider the asymptotic regime where the number of decoding times $L$ is fixed while the average decoding time $N$ grows to infinity, i.e., $L = O(1)$ with respect to $N$. We also extend our PPC result to the Gaussian PPC, where a maximal power constraint is employed for each of $L$ decoding times.

For the PPC, the feedback rate of our code is $\frac{\ell}{n_\ell}$ if the decoding time is $n_\ell$. In contrast, VLSF codes like in [17], [18] use feedback rate 1 bit per channel use. Throughout the chapter, we employ the average error and average decoding time criteria. Our main result shows that for VLSF codes with $L = O(1) \geq 2$

decoding times over a DM-PPC, message set size $M$ satisfying

$$\log M \approx \frac{NC}{1-\epsilon} - \sqrt{N \log_{(L-1)}(N) \frac{V}{1-\epsilon}} \tag{4.1}$$

is achievable. Here $\log_{(L)}(\cdot)$ denotes the $L$-fold nested logarithm, $N$ is the average decoding time, and $C$ and $V$ are the capacity and dispersion of the DM-PPC, respectively. The speed of convergence to $\frac{C}{1-\epsilon}$ depends on $L$. It is slower than the convergence to $C$ in the fixed-length scenario, which has second-order term $O(\sqrt{N})$ [5]. The $L = 2$ case in (4.1) recovers the rate of convergence for the variable-length scenario without feedback, which has second-order term $O(\sqrt{N \log N})$ [18, Proof of Th. 1]; that rate is achieved with $n_1 = 0$. We use the SDO algorithm introduced in [77] (see Appendix C.7) to optimize the decoding times $n_1, \ldots, n_L$ and achieve (4.1). Despite the order-wise dependence on $L$, (4.1) grows so slowly with $L$ that it suggests little benefit to choosing a large $L$. For example, when $L = 4$, $\sqrt{N \log_{(L-1)}(N)}$ behaves very similarly to $O(\sqrt{N})$ for practical values of $N$ (e.g., $N \in [10^3, 10^5]$). Notice, however, that the given achievability result provides a *lower* bound on the benefit of increasing $L$; bounding the benefit from above requires a converse result. The numerical results in [36] support our conclusion from the asymptotic achievability bound (4.1) that indicates diminishing performance increment as $L$ increases.

Linking the error probability of any given VLSF code to that of an SHT, in this chapter, we extend the meta-converse bound [5, Th. 27], which applies to fixed-length, no-feedback codes, to VLSF codes. Analyzing the new bound, we prove a converse for VLSF codes with infinitely many uniformly-spaced decoding times. The converse shows that in order to achieve (4.1) with evenly spaced decoding times, one needs at least $L = \Omega\left(\sqrt{\frac{N}{\log_{(L-1)}(N)}}\right)$ decoding times. In contrast, our optimized codes achieve (4.1) with a finite $L$ that does not grow with the average decoding time $N$.

Sections 4.2–4.4 introduce variable-length sparse stop-feedback codes for the DM-PPC and Gaussian PPC, respectively, and present our main theorems for those channel models; Section 3.5 concludes the chapter. The proofs appear in the Chapter C.

## 4.2 VLSF Codes with $L$ Decoding Times

Recall the capacity and dispersion from (1.4) and (1.7)

$$C = \max_{P_X \in \mathcal{P}} I(X;Y) \tag{4.2}$$

$$V = \min_{P_X \in \mathcal{P}: I(X;Y)=C} \mathrm{Var}\left[\imath(X;Y)\right]. \tag{4.3}$$

We consider VLSF codes with a finite number of potential decoding times $n_1 < n_2 < \cdots < n_L$ over a DM-PPC. The receiver chooses to end the transmission at the first time $n_\ell \in \{n_1, \ldots, n_L\}$ that it is ready to decode. The transmitter learns of the receiver's decision via a single bit of feedback at each of times $n_1, \ldots, n_\ell$. Feedback bit "0" at time $n_i$ means that the receiver is not yet ready to decode, and transmission should continue; feedback bit "1" means that the receiver can decode at time $n_i$, which signals the transmitter to stop. We employ average decoding time and average error probability constraints. Definition 4.2.1, below, formalizes our code description.

**Definition 4.2.1.** *Fix $\epsilon \in (0,1)$, positive integers $L$ and $M$, and a positive scalar $N$. An $(N, L, M, \epsilon)$ VLSF code for the DM-PPC comprises*

1. *integer-valued decoding times $0 \leq n_1 < \ldots < n_L$,*

2. *a finite alphabet $\mathcal{U}$ and a probability distribution $P_U$ on $\mathcal{U}$ defining a common randomness random variable $U$ that is revealed to both the transmitter and the receiver before the start of the transmission,*[1]

3. *an encoding function $\mathsf{f}_n: \mathcal{U} \times [M] \to \mathcal{X}$, for each $n = 1, \ldots, n_L$, that assigns a codeword*

$$\mathsf{f}(u,m)^{n_L} \triangleq (\mathsf{f}_1(u,m), \ldots, \mathsf{f}_{n_L}(u,m)) \tag{4.4}$$

   *to each message $m \in [M]$ and common randomness instance $u \in \mathcal{U}$,*

4. *a non-negative integer-valued random stopping time $\tau \in \{n_1, \ldots, n_L\}$ for the filtration generated by $\{U, Y^{n_i}\}_{i=1}^{L}$ that satisfies an average decoding time constraint*

$$\mathbb{E}\left[\tau\right] \leq N, \tag{4.5}$$

5. *and a decoding function $\mathsf{g}_{n_\ell}: \mathcal{U} \times \mathcal{Y}^{n_\ell} \to [M] \cup \{\mathsf{e}\}$ for each $\ell \in [L]$ (where $\mathsf{e}$ is the erasure symbol used to indicate that the receiver is not ready to decode), satisfying an average error probability constraint*

$$\mathbb{P}\left[\mathsf{g}_\tau(U, Y^\tau) \neq W\right] \leq \epsilon, \tag{4.6}$$

[1] The realization $u$ of $U$ specifies the codebook.

*where the message $W$ is equiprobably distributed on the set $[M]$, and $X^\tau = \mathsf{f}(U, W)^\tau$.*

As in [18], [73], we here need common randomness because the traditional random-coding argument does not prove the existence of a single (deterministic) code that simultaneously satisfies two conditions on the code (4.5) and (4.6). Therefore, randomized codes are necessary for our achievability argument; here, $|\mathcal{U}| \leq 2$ suffices (see Appendix E.4).

We define the maximum achievable message set size $M^*(N, L, \epsilon)$ with $L$ decoding times, average decoding time $N$, and average error probability $\epsilon$ as

$$M^*(N, L, \epsilon) \triangleq \max\{M\colon \text{ an } (N, L, M, \epsilon) \\ \text{VLSF code exists}\}. \tag{4.7}$$

The maximum achievable message set size for VLSF codes with $L$ decoding times $n_1, \dots, n_L$ that are restricted to belong to a subset $\mathcal{N} \subseteq \mathbb{Z}_+$ is denoted by $M^*(N, L, \epsilon, \mathcal{N})$.

### 4.2.1 Related Work

The following discussion summarizes prior asymptotic expansions of the maximum achievable message set size for the DM-PPC.

a) $M^*(N, 1, \epsilon)$: For $L = 1$ and $\epsilon \in (0, 1/2)$, Polyanskiy *et al.* [5, Th. 49] show that

$$\log M^*(N, 1, \epsilon) = NC - \sqrt{NV} Q^{-1}(\epsilon) + O(\log N). \tag{4.8}$$

For $\epsilon \in [1/2, 1)$, the dispersion $V$ in (4.3) is replaced by the maximum dispersion $V_{\max} \triangleq \max\limits_{P_X : \imath(X;Y) = C} V(X; Y)$. The $O(\log N)$ term is lower bounded by $O(1)$ and upper bounded by $\frac{1}{2} \log N + O(1)$. For nonsingular DM-PPCs, i.e., the channels that satisfy $\mathbb{E}\left[\mathrm{Var}\left[\imath(X; Y) | Y\right]\right] > 0$ for the distributions that achieve the capacity $C$ and the dispersion $V$, the $O(\log N)$ term is equal to $\frac{1}{2} \log N + O(1)$ [43]. Moulin [35] derives lower and upper bounds on the $O(1)$ term in the asymptotic expansion when the channel is nonsingular with non-lattice information density.

b) $M^*(N, \infty, \epsilon)$: For VLSF codes with $L = \infty$ and $n_i = i - 1, i \in \mathbb{Z}_+$, Polyanskiy *et al.* [18, Th. 2] show that for $\epsilon \in (0, 1)$,

$$\log M^*(N, \infty, \epsilon) \geq \frac{NC}{1 - \epsilon} - \log N + O(1) \tag{4.9}$$

$$\log M^*(N, \infty, \epsilon) \leq \frac{NC}{1-\epsilon} + \frac{h_b(\epsilon)}{1-\epsilon}, \tag{4.10}$$

where $h_b(\epsilon) \triangleq -\epsilon \log \epsilon - (1-\epsilon)\log(1-\epsilon)$ is the binary entropy function (in nats). The bounds in (4.9)–(4.10) indicate that the $\epsilon$-capacity (the first-order achievable term) is

$$\lim \inf_{N\to\infty} \frac{1}{N} \log M^*(N, \infty, \epsilon) = \frac{C}{1-\epsilon}. \tag{4.11}$$

The achievable dispersion term is zero, i.e., the second-order term in the fundamental limit in (4.9)–(4.10) is $o(\sqrt{N})$.

## 4.3 Achievability Bounds for DM-PPCs

Our main result is a second-order achievability bound for VLSF codes with $L = O(1)$ decoding times on the DM-PPC.

**Theorem 4.3.1.** *Fix an integer $L = O(1) \geq 2$ and real numbers $N > 0$ and $\epsilon \in (0, 1)$. For the DM-PPC with $V > 0$, the maximum message set size (4.7) achievable by $(N, L, M, \epsilon)$ VLSF codes satisfies*

$$\begin{aligned}\log M^*\left(N, L, \epsilon\right) \geq \frac{NC}{1-\epsilon} - \sqrt{N \log_{(L-1)}(N) \frac{V}{1-\epsilon}} \\ + O\left(\sqrt{\frac{N}{\log_{(L-1)}(N)}}\right).\end{aligned} \tag{4.12}$$

*The decoding times $\{n_1, \ldots, n_L\}$ that achieve (4.12) satisfy the equations*

$$\log M = n_\ell C - \sqrt{n_\ell \log_{(L-\ell+1)}(n_\ell) V} - \log n_\ell + O(1) \tag{4.13}$$

*for $\ell \in \{2, \ldots, L\}$, and $n_1 = 0$.*

*Proof sketch:* Polyanskiy *et al.* [5] interpret the information-density threshold test for a fixed-length code as a collection of hypothesis tests aimed at determining whether the channel output is ($H_0$) or is not ($H_1$) dependent on a given codeword. In our coding scheme, we use SHTs in a similar way. The coding scheme in the proof of Theorem 4.3.1 is inspired by that in [18] for DM-PPCs with $L = \infty$. A similar coding scheme is used in the achievability bounds in [71], [72]. The strategy is as follows.

The VLSF decoder at each time $n_1, \ldots, n_L$ runs $M$ SHTs between a hypothesis $H_0$ that the channel output results from transmission of the $m$-th codeword,

$m \in [M]$, and the hypothesis $H_1$ that the channel output was drawn from the unconditional channel output distribution. Transmission stops at the first time $n_i$ that $H_0$ is decided for some message $m$ or the first time $n_i$ that $H_1$ is decided for all $m$. The former marks a decoding event for message $m$. The latter is a failure to decode since deciding $H_1$ for some $m'$ indicates a decision that $m'$ cannot explain the observed channel output. When decoding fails, an error is declared. Transmission continues as long as one or more SHTs has not decided either $H_0$ or $H_1$. For simplicity of the analysis, we employ sub-optimal SHTs. Namely, we set the smallest decoding time to $n_1 = 0$. At time $n_1$, with probability $p$, all $M$ SHTs simultaneously decide $H_1$; with probability $1-p$, all $M$ SHTs pass $n_1$ without deciding. An information density threshold test is employed for the remaining $L-1$ decoding times $\{n_2, \dots, n_L\}$.

Let $\epsilon'_N$ and $N'$ be the average error probability and average decoding time conditioned on the event that the transmission has not stopped at time $n_1$. We set the parameters

$$\epsilon'_N = \frac{1}{\sqrt{N' \log N'}} \tag{4.14}$$

$$p = \frac{\epsilon - \epsilon'_N}{1 - \epsilon'_N} = \epsilon - O(\epsilon'_N). \tag{4.15}$$

The error probability of the resulting code is bounded by $\epsilon$, and the average decoding time is

$$N = N'(1-p) = N'(1-\epsilon) + O\left(\sqrt{\frac{N'}{\log N'}}\right). \tag{4.16}$$

The choice of decoding times $n_2, \dots, n_L$ chosen in (4.13) achieves the maximum codebook size $M$ among all possible choices while guaranteeing the error probability $\epsilon'_N$ in the non-asymptotic achievability bound (Theorem 4.3.2, below). Since the probabilities in (4.17)–(4.18), below, decay sub-exponentially to zero (e.g., the threshold $\gamma$ and $n_L$ are set so that $\mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right] = \epsilon'_N(1 - o(1)))$, we use a moderate deviations result from [28, Ch. 8] to bound those probabilities. We apply Karush-Kuhn-Tucker conditions to show that the decoding times in (4.13) yield a $\log M$ that is maximal achievable by the non-asymptotic bound up to terms of order $O\left(\sqrt{\frac{N}{\log_{(L-1)}(N)}}\right)$. The details of the proof appear in Appendix C.3. The achievability bounds for $L \in [4]$ and the converse bound (4.10) are illustrated for the BSC in Fig. 4.1. ■

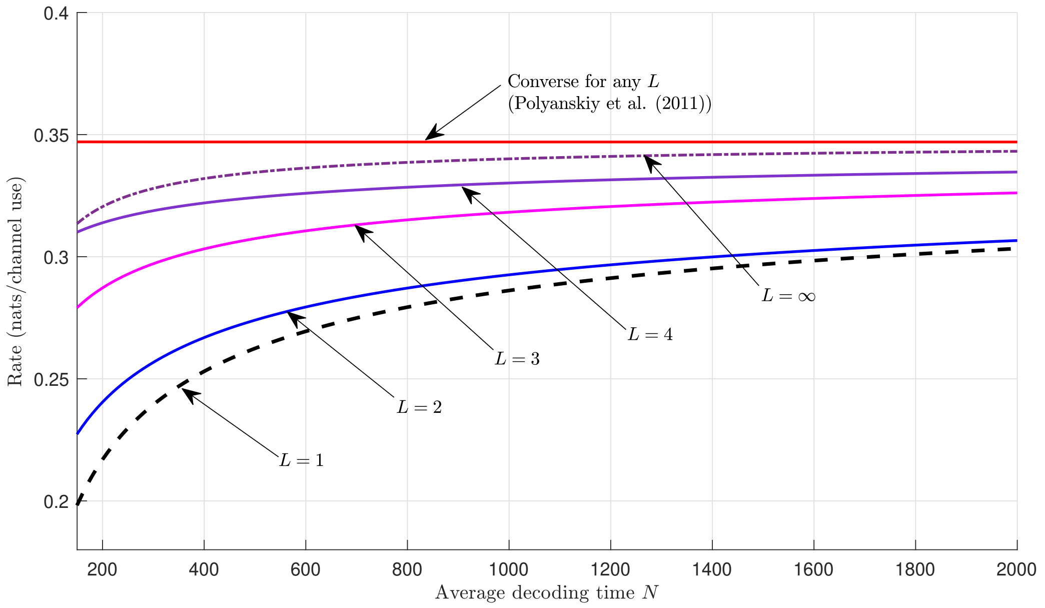


Figure 4.1: The achievability (Theorem 4.3.1) and converse (4.10) bounds for the maximum achievable rate $\frac{\log M^*(N,L,\epsilon)}{N}$ are shown for the BSC with crossover probability 0.11, $L \leq 4$, and $\epsilon = 10^{-3}$. The $O(\cdot)$ term in (4.12) is ignored. The curve that $L = \infty$ is Polyanskiy *et al.*'s achievability bound in (4.10).

Replacing that sub-optimal SHT in the proof sketch with the optimal SHT would improve the performance achieved on the right-hand side of (4.12) only by $O(1)$.

Since any $(N, L, M, \epsilon)$ VLSF code is also an $(N, \infty, M, \epsilon)$ VLSF code, (4.10) provides an upper bound on $\log M^*(N, L, \epsilon)$ for an arbitrary $L$. The order of the second-order term, $-\sqrt{N \log_{(L-1)}(N) \frac{V}{1-\epsilon}}$, depends on the number of decoding times $L$. The larger $L$, the faster the achievable rate converges to the capacity. However, the dependence on $L$ is weak since $\log_{(L-1)}(N)$ grows very slowly in $N$ even if $L$ is small. For example, for $L = 4$ and $N = 1000$, $\log_{(L-1)}(N) \approx 0.659$. For a finite $L$, this bound falls short of the $-\log N$ achievability bound in (4.10) achievable with $L = \infty$. Whether the second-order term achieved in Theorem 4.3.1 is tight remains an open problem.

Theorem 4.3.1 follows from an application of the non-asymptotic achievability bound in Theorem 4.3.2, below.

**Theorem 4.3.2.** *Fix a constant $\gamma$, decoding times $n_1 < \cdots < n_L$, and a positive integer $M$. For any positive number $N$ and $\epsilon \in (0, 1)$, there exists an*

*$(N, L, M, \epsilon)$ VLSF code for the DM-PPC $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ with*

$$\epsilon \leq \mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right] + (M-1)\exp\{-\gamma\}, \tag{4.17}$$

$$N \leq n_1 + \sum_{\ell=1}^{L-1} (n_{\ell+1} - n_\ell)\mathbb{P}\left[\imath(X^{n_\ell}; Y^{n_\ell}) < \gamma\right], \tag{4.18}$$

*where $P_{X^{n_L}}$ is a product of distributions of $L$ sub-vectors of lengths $n_j - n_{j-1}$, $j \in [L]$, i.e.,*

$$P_{X^{n_L}}(x^{n_L}) = \prod_{j=1}^{L} P_{X^{n_{j-1}+1:n_j}}(x^{n_{j-1}+1:n_j}), \tag{4.19}$$

*where $n_0 = 0$.*

*Proof sketch:* Theorem 4.3.2 analyzes the error probability and the average decoding time of the sub-optimal SHT-based decoder that is used at times $n_2, \dots, n_L$ in the proof sketch of Theorem 4.3.1. It employs a fixed information density threshold rule, and extends the achievability bound in [18, Th. 3] that considers $L = \infty$ to the scenario where only a finite number of decoding times is allowed. The bound on the average decoding time (4.18) is obtained by expressing the bound on the average decoding time in [18, eq. (27)] using the fact that the stopping time $\tau$ is in $\{n_1, \dots, n_L\}$. When we compare Theorem 4.3.2 with [18, Th. 3], we see that the error probability bound in (4.17) has an extra term $\mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right]$. This term appears since transmission always stops at or before time $n_L$. See Appendix C.2 for the proof details. ■

Theorem 4.3.2 is related to [76, Lemma 1], which similarly treats $L < \infty$ but requires $n_{\ell+1} - n_\ell = d$ for some constant $d \geq 1$, and [78, Cor. 2], where the transmitter retransmits the message if decoding attempts at times $n_1, \dots, n_L$ are unsuccessful.

The following theorem gives achievability and converse bounds for VLSF codes with decoding times uniformly spaced as $\{0, d_N, 2d_N, \dots\}$.

**Theorem 4.3.3.** *Fix $\epsilon \in (0,1)$. Let $d_N = o(N)$, and let $P_{Y|X}$ be any DM-PPC. Then, it holds that*

$$\log M^*(N, \infty, \epsilon, d_N\mathbb{Z}_+) \geq \frac{NC}{1-\epsilon} - \frac{d_N C}{2} - \log N + o(d_N). \tag{4.20}$$

*If the DM-PPC $P_{Y|X}$ is a Cover-Thomas symmetric DM-PPC [48, p. 190] i.e., the rows (and resp. the columns) of the transition probability matrix are* *permutations of each other, then*

$$\log M^*(N, \infty, \epsilon, d_N \mathbb{Z}_+) \leq \frac{NC}{1-\epsilon} - \frac{d_N C}{2} + o(d_N). \tag{4.21}$$

*Proof:* The achievability bound (4.20) employs the sub-optimal SHT in the proof sketch of Theorem 4.3.1. To prove the converse in (4.21), we first derive in Theorem C.4.1, in Appendix C.4 below, the meta-converse bound for VLSF codes. The meta-converse bound in Theorem C.4.1 bounds the error probability of any given VLSF code from below by the minimum achievable type-II error probability of the corresponding SHT; it is an extension and a tightening of Polyanskiy *et al.*'s converse in (4.10) since for $d_N = 1$, weakening it by applying a loose bound on the performance of SHTs from [83, Th. 3.2.2] recovers (4.10). The Cover-Thomas symmetry assumption allows us to circumvent the maximization of that minimum type-II error probability over codes since the log-likelihood ratio $\log \frac{P_{Y|X}(Y|x)}{P_Y(Y)}$ is the same regardless of the channel input $x$ for that channel class. In both bounds in (4.20)–(4.21), we use the expansions for the average stopping time and the type-II error probability from [83, Ch. 2-3]. See Appendix C.4 for details. ■

Theorem 4.3.3 establishes that when $\frac{d_N}{\log N} \to \infty$, the second-order term of the logarithm of maximum achievable message set size among VLSF codes with uniformly spaced decoding times is $-\frac{d_N C}{2}$. Theorem 4.3.3 implies that in order to achieve the same performance as achieved in Theorem 4.3.1 (4.12) with $L$ decoding times, one needs on average $\Omega\left(\sqrt{\frac{N}{\log_{(L-1)}(N)}}\right)$ uniformly spaced stop-feedback instances, suggesting that the optimization of available decoding times considered in Theorem 4.3.1 is crucial for attaining the second-order term in (4.12).

The case where $d_N = \Omega(N)$ is not as interesting as $d_N = o(N)$ since analyzing Theorem C.4.1 using Chernoff bound would yield that the probability that the optimal SHT makes a decision at times other than $n_1 = 0$ and $\frac{N}{1-\epsilon}(1 + o(1))$ decays exponentially with $N$, making the scenario with $L = \infty$ and $d_N = \Omega(N)$ asymptotically equivalent to $L = 2$. For example, for $d_N = \frac{1}{\ell}\frac{N}{1-\epsilon}\left(1 + O\left(\frac{1}{\sqrt{N \log N}}\right)\right)$ for some $\ell \in \mathbb{Z}_+$, the right-hand side of (4.12) is tight up to the second-order term.

## 4.4 VLSF Codes for the Gaussian PPC with Maximal Power Constraints

Recall the Gaussian channel, its capacity $C(P)$, and dispersion $V(P)$ from (3.68)–(3.70).

We first introduce the maximal and average power constraints on VLSF codes for the PPC. Given a VLSF code with $L$ decoding times $n_1, \dots, n_L$, the maximal power constraint requires that the length-$n$ prefixes, $n \in \{n_1, \dots, n_L\}$, of each codeword all satisfy a power constraint $P$, i.e.,

$$\|\mathsf{f}(u, m)^{n_\ell}\|_2^2 \leq n_\ell P \text{ for all } m \in [M], u \in \mathcal{U}, \quad \ell \in [L]. \quad . \tag{4.22}$$

The average power constraint on the length-$n_L$ codewords, as defined by [72, Def. 1], is

$$\mathbb{E}\left[\|\mathsf{f}(U, W)^{n_L}\|_2^2\right] \leq NP. \tag{4.23}$$

The definitions of $(N, L, M, \epsilon, P)_{\text{max}}$ and $(N, L, M, \epsilon, P)_{\text{ave}}$ VLSF codes for the Gaussian PPC are similar to 4.2.1 with the addition of maximal (4.22) and average (4.23) power constraints, respectively. Similar to (4.7), $M^*(N, L, \epsilon, P)_{\text{max}}$ (resp. $M^*(N, L, \epsilon, P)_{\text{ave}}$) denotes the maximum achievable message set size with $L$ decoding times, average decoding time $N$, average error probability $\epsilon$, and maximal (resp. average) power constraint $P$.

In the following, we discuss prior asymptotic expansions of $M^*(N, L, \epsilon, P)_{\text{max}}$ and $M^*(N, L, \epsilon, P)_{\text{ave}}$ for the Gaussian PPC, where $L \in \{1, \infty\}$.

a) $M^*(N, 1, \epsilon, P)_{\text{max}}$: For $L = 1$, $P > 0$, and $\epsilon \in (0, 1)$, Tan and Tomamichel [44, Th. 1] and Polyanskiy *et al.* [5, Th. 54] show that

$$\begin{aligned} &\log M^*(N, 1, \epsilon, P)_{\text{max}} \\ &\quad = NC(P) - \sqrt{NV(P)}Q^{-1}(\epsilon) + \frac{1}{2}\log N + O(1). \end{aligned} \tag{4.24}$$

The converse for (4.24) is derived in [5, Th. 54] and the achievability for (4.24) in [44, Th. 1]. The achievability scheme in [44, Th. 1] generates i.i.d. codewords uniformly distributed on the $n$-dimensional sphere with radius $\sqrt{nP}$, and applies maximum likelihood (ML) decoding. These results imply that random codewords uniformly distributed on a sphere and ML decoding are, together, third-order optimal, meaning that the gap between the achievability and converse bounds in (4.24) is $O(1)$.

b) $M^*(N, 1, \epsilon, P)_{\text{ave}}$: For $L = 1$ with an average-power-constraint, Yang *et al.* show in [84] that

$$\log M^*(N, 1, \epsilon, P)_{\text{ave}} = N\, C\left(\frac{P}{1-\epsilon}\right) - \\ - \sqrt{N \log N\, V\left(\frac{P}{1-\epsilon}\right)} + O(\sqrt{N}). \tag{4.25}$$

Yang *et al.* use a power control argument to show the achievability of (4.25). They divide the messages into disjoint sets $\mathcal{A}$ and $[M] \setminus \mathcal{A}$, where $|\mathcal{A}|= M(1-\epsilon)(1-o(1))$. For the messages in $\mathcal{A}$, they use an $\left(N, 1, |\mathcal{A}|, \frac{2}{\sqrt{N \log N}}, \frac{P}{1-\epsilon}(1-o(1))\right)$ VLSF code with a single decoding time $N$. The codewords are generated i.i.d. uniformly on the sphere with center at 0 and radius $\sqrt{N\frac{P}{1-\epsilon}(1-o(1))}$. The messages in $[M] \setminus \mathcal{A}$ are assigned the all-zero codeword. The converse for (4.25) follows from an application of the meta-converse [5, Th. 26].

c) $M^*(N, \infty, \epsilon, P)_{\text{ave}}$: For VLSF codes with $L = \infty$, $n_i = i - 1$ for $i \in \mathbb{Z}_+$, and average power constraint (4.23), Truong and Tan show in [71, Th. 1] that for $\epsilon \in (0, 1)$ and $P > 0$,

$$\log M^*(N, \infty, \epsilon, P)_{\text{ave}} \geq \frac{NC(P)}{1-\epsilon} - \log N + O(1) \tag{4.26}$$

$$\log M^*(N, \infty, \epsilon, P)_{\text{ave}} \leq \frac{NC(P)}{1-\epsilon} + \frac{h_b(\epsilon)}{1-\epsilon}, \tag{4.27}$$

where $h_b$ is the binary entropy function. The results in (4.26)–(4.27) are analogous to the fundamental limits for DM-PPCs (4.9)–(4.10) and follow from arguments similar to those in [18]. Since the information density $\imath(X; Y)$ for the Gaussian channel is unbounded, bounding the expected value of the decoding time in the proof of [71, Th. 1] requires different techniques from those applicable to DM-PPCs [18].

### 4.4.1 Main Result

The theorem below is our main result for the Gaussian PPC under the maximal power constraint (4.22).

**Theorem 4.4.1.** *Fix an integer $L = O(1) \geq 2$ and real numbers $P > 0$ and $\epsilon \in (0, 1)$. For the Gaussian channel with maximal power constraint (4.22), the maximum message set size achievable by $(N, L, M, \epsilon, P)$ VLSF codes satisfies*

$$\log M^*\left(N, L, \epsilon, P\right)_{\max} \geq \frac{NC(P)}{1-\epsilon} - \sqrt{N \log_{(L-1)}(N) \frac{V(P)}{1-\epsilon}}$$

$$+ O\left(\sqrt{\frac{N}{\log_{(L-1)}(N)}}\right). \tag{4.28}$$

*The decoding times that achieve* (4.28) *satisfy the equations*

$$\log M^*(N, L, \epsilon, P)_{\max} = n_\ell C(P) - \sqrt{n_\ell \log_{(L-\ell+1)}(n_\ell) V(P)} - \log n_\ell + O(1) \tag{4.29}$$

*for* $\ell \in \{2, \dots, L\}$*, and* $n_1 = 0$.

*Proof:* See Appendix C.6. ■

## 4.5 Summary

This chapter investigates the maximum achievable message set size for sparse VLSF codes over the DM-PPC (Theorem 4.3.1), DM-MAC (Theorem 5.3.1), DM-RAC (Theorem 6.6.1), and Gaussian PPC (Theorem 3.3.4) in the asymptotic regime where the number of decoding times $L$ is constant as the average decoding time $N$ grows without bound. Under our second-order achievability bounds, the performance improvement due to adding more decoding time opportunities to our code quickly diminishes as $L$ increases. For example, for the BSC with crossover probability 0.11, at average decoding time $N = 1000$, our VLSF coding bound with only $L = 4$ decoding times achieves 95.2% of the rate of Polyanskiy *et al.*'s VLSF coding bound for $L = \infty$. Incremental redundancy automatic repeat request codes, which are some of the most common feedback codes, employ only a small number of decoding times and stop feedback. Our analysis shows that such a code design is not only practical but also has performance competitive with the best known dense feedback codes.

In all channel types considered, the first-order term in our achievability bounds is $\frac{NC}{1-\epsilon}$, where $N$ is the average decoding time, $\epsilon$ is the error probability, and $C$ is the capacity (or the sum-rate capacity in the multi-transmitter case), and the second-order term is $O\left(-\sqrt{N \log_{(L-1)}(N)}\right)$. For DM-PPCs, there is a mismatch between the second-order term of our achievability bound for VLSF codes with $L = O(1)$ decoding times (Theorem 4.3.1) and the second-order term of the best known converse bound (4.10); the latter applies to $L = \infty$, and therefore to any $L$. Towards closing the gap between the achievability and converse bounds, in Theorem C.4.1 in Appendix C.4, below, we derive a non-asymptotic converse bound that links the error probability of a VLSF code with the minimum achievable type-II error probability of an SHT. However, since the threshold values of the optimal SHT with $L$ decoding times do not have a closed-form expression [83, pp. 153-154], analyzing the non-asymptotic converse bound in Theorem C.4.1 is a difficult task. We leave whether the second-order term in Theorem 4.3.1 is optimal to future work.

In sparse VLSF codes, optimizing the values of $L$ available decoding times is important since to achieve the same performance as $L = O(1)$ optimized decoding times (Theorem 4.3.1), one needs $\Omega\left(\sqrt{\frac{N}{\log_{(L-1)}(N)}}\right)$ uniformly spaced decoding times (Theorem 4.3.3).

Chapter 5

# VARIABLE-LENGTH SPARSE FEEDBACK CODES FOR MACS

## 5.1 Introduction

This chapter extends VLSF codes introduced in Chapter 4 to DM-MACs. Some prior work on VLF codes over MACs are as follows. Truong and Tan [72] extend the results in [18] to the Gaussian MAC under an average power constraint. Trillingsgaard *et al.* [73] study the VLSF scenario where a common message is transmitted across a $K$-user discrete memoryless broadcast channel. Heidari *et al.* [74] extend Burnashev's work to the DM-MAC and derive lower and upper bounds on the error exponents of VLF codes for the DM-MAC. Bounds on the performance of VLSF codes for the DM-MAC with an unbounded number of decoding times appear in [75]. The $K$-transmitter MAC achievability bounds from [72] and [75] employ $2^K - 1$ simultaneous information density threshold rules.

## 5.2 Definitions for MACs

We begin by introducing the definitions used for the multi-transmitter setting. A $K$-transmitter DM-MAC is defined by a triple $\left(\prod_{k=1}^{K} \mathcal{X}_k, P_{Y_K|X_{[K]}}, \mathcal{Y}_K\right)$, where $\mathcal{X}_k$ is the finite input alphabet for transmitter $k \in [K]$, $\mathcal{Y}_K$ is the finite output alphabet of the channel, and $P_{Y_K|X_{[K]}}$ is the channel transition probability.

Let $P_{Y_K}$ denote the marginal output distribution induced by the input distribution $P_{X_{[K]}}$. The unconditional and conditional information densities are defined for each non-empty $\mathcal{A} \subseteq [K]$ as

$$\imath_K(x_{\mathcal{A}}; y) \triangleq \ln \frac{P_{Y_K|X_{\mathcal{A}}}(y|x_{\mathcal{A}})}{P_{Y_K}(y)} \tag{5.1}$$

$$\imath_K(x_{\mathcal{A}}; y|x_{\mathcal{A}^c}) \triangleq \ln \frac{P_{Y_K|X_{[K]}}(y|x_{[K]})}{P_{Y_K|X_{\mathcal{A}^c}}(y|x_{\mathcal{A}^c})}, \tag{5.2}$$

where $\mathcal{A}^c = [K] \setminus \mathcal{A}$. Note that in (5.1)–(5.2), the information density functions depend on the transmitter set $\mathcal{A}$ unless further symmetry conditions are assumed (e.g., in some cases we assume that the components of $P_{X_{[K]}}$ are i.i.d., and $P_{Y_K|X_{[K]}}$ is invariant to permutations of the inputs $X_{[K]}$).

The corresponding mutual informations under the input distribution $P_{X_{[K]}}$ and the channel transition probability $P_{Y_K|X_{[K]}}$ are defined as

$$I_K(X_{\mathcal{A}}; Y_K) \triangleq \mathbb{E}\left[\imath_K(X_{\mathcal{A}}; Y_K)\right] \tag{5.3}$$

$$I_K(X_{\mathcal{A}}; Y_K|X_{\mathcal{A}^c}) \triangleq \mathbb{E}\left[\imath_K(X_{\mathcal{A}}; Y_K|X_{\mathcal{A}^c})\right]. \tag{5.4}$$

The dispersions are defined as

$$V_K(X_{\mathcal{A}}; Y_K) \triangleq \mathrm{Var}\left[\imath_K(X_{\mathcal{A}}; Y_K)\right] \tag{5.5}$$

$$V_K(X_{\mathcal{A}}; Y_K|X_{\mathcal{A}^c}) \triangleq \mathrm{Var}\left[\imath_K(X_{\mathcal{A}}; Y_K|X_{\mathcal{A}^c})\right]. \tag{5.6}$$

For brevity, we define

$$I_K \triangleq I_k(X_{[K]}; Y_K) \tag{5.7}$$

$$V_K \triangleq \mathrm{Var}\left[\imath_K(X_{[K]}; Y_K)\right]. \tag{5.8}$$

A VLSF code for the MAC with $K$ transmitters is defined similarly to the VLSF code for the PPC.

**Definition 5.2.1.** *Fix $\epsilon \in (0, 1)$, $N \in (0, \infty)$, and positive integers $M_k, k \in [K]$. An $(N, L, M_{[K]}, \epsilon)$ VLSF code for the MAC comprises*

1. *integer-valued decoding $0 \leq n_1 < \cdots < n_L$,*
2. *$K$ finite alphabets $\mathcal{U}_k$, $k \in [K]$, defining common randomness random variables $U_1, \ldots, U_K$,*
3. *$K$ sequences of encoding functions $\mathsf{f}_n^{(k)}: \mathcal{U}_k \times [M_k] \to \mathcal{X}_k$, $k \in [K]$,*
4. *a stopping time $\tau \in \{n_1, \ldots, n_L\}$ for the filtration generated by $\{U_1, \ldots, U_K, Y_K^{n_\ell}\}_{\ell=1}^L$, satisfying an average decoding time constraint (4.5), and*
5. *$L$ decoding functions $\mathsf{g}_{n_\ell}: \mathcal{U}_{[K]} \times \mathcal{Y}_K^{n_\ell} \to \prod_{k=1}^{K} [M_k] \cup \{\mathsf{e}\}$ for $\ell \in [L]$, satisfying an average error probability constraint*

$$\mathbb{P}\left[\mathsf{g}_\tau(U_{[K]}, Y_K^\tau) \neq W_{[K]}\right] \leq \epsilon, \tag{5.9}$$

*where the independent messages $W_1, \ldots, W_K$ are uniformly distributed on the sets $[M_1], \ldots, [M_K]$, respectively.*

## 5.3 Achievability Bounds

Our main results are second-order achievability bounds for the rates approaching a point on the sum-rate boundary of the MAC achievable region increased by a factor of $\frac{1}{1-\epsilon}$. Theorem 5.3.1, below, is an achievability bound for the asymptotic regime $L = O(1)$.

**Theorem 5.3.1.** *Fix $\epsilon \in (0,1)$, an integer $L = O(1) \geq 2$, and distributions $P_{X_k}$, $k \in [K]$, and arbitrary constants $a^{(\mathcal{A})} \in (0, I_K(X_{\mathcal{A}}; Y_K | X_{\mathcal{A}^c}))$ for $\mathcal{A} \in \mathcal{P}([K])$. For any $K$-transmitter DM-MAC $(\prod_{k=1}^K \mathcal{X}_k, P_{Y_K|X_{[K]}}, \mathcal{Y}_K)$, there exists an $(N, L, M_{[K]}, \epsilon)$ VLSF code with*

$$\sum_{k\in[K]} \ln M_k \leq \frac{NI_K}{1-\epsilon} - \sqrt{N \ln_{(L-1)}(N) \frac{V_K}{1-\epsilon}} + O\left(\sqrt{\frac{N}{\ln_{(L-1)}(N)}}\right), \tag{5.10}$$

$$\sum_{k\in\mathcal{A}} \ln M_k \leq \frac{N(I_K(X_{\mathcal{A}}; Y_K | X_{\mathcal{A}^c}) - a^{(\mathcal{A})})}{1-\epsilon} + o(N) \tag{5.11}$$

*for all $\mathcal{A} \in \mathcal{P}([K])$.*

Theorem 5.3.1 follows from an application of the non-asymptotic achievability bound, Theorem 5.3.2, below.

**Theorem 5.3.2.** *Fix constants $\epsilon \in (0,1)$, $\gamma$, $\lambda^{(\mathcal{A})} > 0$ for $\mathcal{A} \in \mathcal{P}([K])$, integers $0 \leq n_1 < \cdots < n_L$, and distributions $P_{X_k}$, $k \in [K]$. For any DM-MAC with $K$ transmitters $(\prod_{k=1}^K \mathcal{X}_k, P_{Y_K|X_{[K]}}, \mathcal{Y}_K)$, there exists an $(N, L, M_{[K]}, \epsilon)$ VLSF code with*

$$\epsilon \leq \mathbb{P}\left[\imath_K(X_{[K]}^{n_L}; Y_K^{n_L}) < \gamma\right] \tag{5.12}$$

$$+ \prod_{k=1}^K (M_k - 1) \exp\{-\gamma\} \tag{5.13}$$

$$+ \sum_{\ell=1}^L \sum_{\mathcal{A}\in\mathcal{P}([K])} \mathbb{P}\left[\imath_K(X_{\mathcal{A}}^{n_\ell}; Y_K^{n_\ell}) > N(I_K(X_{\mathcal{A}}; Y) + \lambda^{(\mathcal{A})})\right] \tag{5.14}$$

$$+ \sum_{\mathcal{A}\in\mathcal{P}([K])} \left(\prod_{k\in\mathcal{A}^c} (M_k - 1)\right) \exp\{-\gamma + NI_K(X_{\mathcal{A}}; Y_K) + N\lambda^{(\mathcal{A})}\} \tag{5.15}$$

$$N \leq n_1 + \sum_{\ell=1}^{L-1} (n_{\ell+1} - n_\ell) \mathbb{P}\left[\imath_K(X_{[K]}^{n_\ell}; Y_K^{n_\ell}) < \gamma\right]. \tag{5.16}$$

*Proof sketch:* The proof of Theorem 5.3.2 uses a random coding argument that employs $K$ i.i.d. codebook ensembles with distributions $P_{X_k}$, $k \in [K]$. The receiver employs $L$ decoders that operate by comparing an information density $\imath_K(x_{[K]^n}; y^n)$ for each possible transmitted codeword set to a threshold. At time $n_\ell$, decoder $g_{n_\ell}$ computes the information densities $\imath_K(X_{[K]}^{n_\ell}(m_{[K]}); Y_K^{n_\ell})$; if there exists a message vector $\hat{m}_{[K}$ satisfying $\imath_K(X_{[K]}^{n_\ell}(\hat{m}_{[K]}); Y_K^{n_\ell}) > \gamma$, then the receiver decodes to the message vector $\hat{m}_{[K]}$. Otherwise, the decoder emits output $\mathsf{e}$, and the receiver passes the decoding time $n_\ell$ without decoding. If $n_\ell < n_L$, the transmission continues until the next decoding time. The term (5.12) bounds the probability that the information density corresponding to the true messages is below the threshold for all decoding times; (5.13) bounds the probability that all messages are decoded incorrectly; and (5.14)-(5.15) bound the probability that the messages from the transmitter index set $\mathcal{A} \subseteq [K]$ are decoded incorrectly, and the messages from the index set $\mathcal{A}^c$ are decoded correctly. ■

In the application of Theorem 5.3.2 to prove Theorem 5.3.1, we choose the parameters $\lambda^{(\mathcal{A})}$ and $\gamma$ so that the terms in (5.14)-(5.15) decay exponentially with $N$, which become negligible compared to (5.12) and (5.13). Between (5.12) and (5.13), the term (5.12) is dominant when $L$ does not grow with $N$, and (5.13) is dominant when $L$ grows linearly with $N$.

Like the single-threshold rule from [85] for the RAC, the single-threshold rule employed in the proof of Theorem 5.3.2 differs from the decoding rules employed in [72] for VLSF codes over the Gaussian MAC with expected power constraints and in [75] for the DM-MAC. In both [72] and [75], $L = \infty$, and the decoder employs $2^K - 1$ simultaneous threshold rules for each of the boundaries that define the achievable region of the MAC with $K$ transmitters. Those rules fix thresholds $\gamma^{(\mathcal{A})}$, $\mathcal{A} \in \mathcal{P}([K])$, and decode messages $m_{[K]}$ if for all $\mathcal{A} \in \mathcal{P}([K])$, the codeword for $m_{[K]}$ satisfies

$$\imath_K(X_{\mathcal{A}}^{n_\ell}(m_{\mathcal{A}}); Y_K^{n_\ell} | X_{\mathcal{A}^c}^{n_\ell}(m_{\mathcal{A}^c})) > \gamma^{(\mathcal{A})}, \tag{5.17}$$

for some $\gamma^{(\mathcal{A})}$, $\mathcal{A} \in \mathcal{P}([K])$. Our decoder can be viewed as a special case of (5.17) obtained by setting $\gamma^{(\mathcal{A})} = -\infty$ for $\mathcal{A} \neq [K]$.

Analyzing Theorem 5.3.2 in the asymptotic regime $L = \Omega(N)$, we determine that there exists an $(N, \infty, M_{[K]}, \epsilon)$ VLSF code if (5.11) holds and

$$\sum_{k\in[K]} \ln M_k \leq \frac{NI_K}{1-\epsilon} - \ln N + O(1). \tag{5.18}$$

Here, the asymptotic regime between $L$ and $N$ (e.g., $L = \Omega(N)$ or $L = O(1)$) is important rather than whether $L < \infty$ or $L = \infty$. This is because if we truncate an infinite-length code at time $n = 2N$, by Chernoff bound, the resulting penalty term added to the error probability decays exponentially with $N$, whose effect in (5.18) is $o(1)$. Therefore, for any VLSF code, $L = \infty$ case can be treated as $L = \Omega(N)$ regardless of the number of transmitters. See Appendix D.2.1 for the proof of (5.18).

For $L = \infty$, Trillingsgaard *et al.* [75] numerically evaluate their non-asymptotic achievability bound for a DM-MAC while Truong and Tan [72] provide an achievability bound with second-order term $-O(\sqrt{N})$ for the Gaussian MAC with average power constraints. Applying our single-threshold rule and analysis to the Gaussian MAC with average power constraints improves the second-order term in [72] from $-O(\sqrt{N})$ to $-\ln N + O(1)$ for all non-corner points in the achievable region. The main challenge in [72] is to derive a tight bound on the expected value of the maximum over $\mathcal{A} \subseteq [K]$ of stopping times $\tau^{(\mathcal{A})}$ for the corresponding threshold rules in (5.17). In our analysis, we avoid that challenge by employing a single-threshold decoder whose average decoding time is bounded by $\mathbb{E}\left[\tau^{([K])}\right]$.

Under the same model and assumptions on $L$, to achieve non-corner rate points that do not lie on the sum-rate boundary, which corresponds to $a^{(\mathcal{A})} = 0$ in (5.11) for one or more $\mathcal{A} \in \mathcal{P}([K])$, we modify our single-threshold rule to (5.17), where $\mathcal{A}$ is the transmitter index set corresponding to the capacity region's active sum-rate bound at the (non-corner) point of interest. Following steps similar to the proof of (5.18) gives second-order term $-\ln N + O(1)$ for those points as well. For corner points, more than one boundary is active[1]; therefore, more than one threshold rule in (5.17) is needed at the decoder. In this case, again for $L = \infty$, [72] proves an achievability bound with a second-order term $-O(\sqrt{N})$. Whether this bound can be improved to $-\ln N + O(1)$ as in (5.18) remains an open problem.

[1] The capacity region of a $K$-transmitter MAC is characterized by the region bounded by $2^K - 1$ planes. By definition of a corner point, at least two inequalities corresponding to these planes are active at a corner point.

*Chapter 6*

# RAC CODES THAT EMPLOY STOP-FEEDBACK

## 6.1 Introduction

Access points like WiFi hot spots and cellular base stations are, for wireless devices, the gateway to the network. Unfortunately, access points are also the network's most critical bottleneck. As more kinds of devices become network-reliant, both the number of communicating devices and the diversity of their communication needs grow. Little is known about how to code under high variation in the number and variety of communicators.

As more kinds of devices become network-reliant, both the number of communicating devices and the diversity of their communication needs grow. Little is known about how to code under high variation in the number and variety of communicators.

Multiple-transmitter single-receiver channels are well understood in information theory when the number and identities of transmitters are fixed and known. Unfortunately, even in this known-transmitter regime, information-theoretic solutions are too complex to implement. As a result, orthogonalization methods, such as TDMA, FDMA, and orthogonal CDMA, are used instead. Orthogonalization strategies simplify coding by allocating resources (e.g., time slots, frequency) among the transmitters, but applying such methods to discrete memoryless MACs can at best attain a sum-rate equal to the single-transmitter capacity of the channel, which is often significantly smaller than the maximal multi-transmitter sum-rate.

Most random access protocols currently in use rely on collision avoidance, which cannot surpass the single-transmitter capacity of the channel and may be significantly worse since the unknown transmitter set makes it difficult to schedule or coordinate among transmitters. Collision avoidance is achieved through variations of the legacy (slotted) ALOHA and carrier sense multiple access (CSMA) algorithms. ALOHA, which uses random transmission times and back-off schedules, achieves only about 37% of the single-transmitter capacity of the channel [86]. In CSMA, each transmitter tries to avoid collisions by verifying the absence of other traffic before starting a transmission over the shared channel; when collisions do occur, all transmissions are aborted, and a jamming signal is sent to ensure that all transmitters are aware of the collision. The procedure starts again at a random time, which again introduces inefficiencies. The state of the art in random access coding is "treating interference as noise," which is part of newer CDMA-based standards. While this strategy can deal with random access better than ALOHA, it is still far inferior to the theoretical limits. Even from a purely theoretical perspective, a satisfactory solution to random access remains to be found.

Even from a purely theoretical perspective, a satisfactory solution to random access remains to be found. The MAC model in which a fixed number, $k$, out of the total available $K$ transmitters are active was studied by D'yachkov and Rykov [87] and Mathys [88] for zero-error coding on a noiseless adder MAC, and by Bassalygo and Pinsker [89] for an asynchronous model in which the information is considered erased if more than one transmitter is active at a time. See [90] for a more detailed history. Two-layer MAC decoders, with outer layer codes that work to remove channel noise and inner layer codes that work to resolve conflicts, are proposed in [91], [92]. Like the codes in [87]–[89], the codes in [90], [91] are designed for a predetermined number of transmitters, $k$; it is not clear how robust they are to randomness in the transmitters' arrivals and departures. In [93], Minero *et al.* study a random access model in which the receiver knows the transmitter activity pattern, and the transmitters opportunistically send data at the highest possible rate. The receiver recovers only a portion of the messages sent, depending on the current level of activity in the channel.

This chapter poses the question of whether it is possible, in a scenario where no one knows how many transmitters are active, for the receiver to almost always recover the messages sent by all active transmitters. Surprisingly, we find that not only is reliable decoding possible in this regime, but, for the class of permutation-invariant channels considered in [90], our proposed RAC code performs as well in its capacity and dispersion terms as the best-known code for a MAC with the transmitter activity known a priori [19]–[22]. Since the capacity region of a MAC varies with the number of transmitters, it is tempting to believe that the transmitters of a random access system must somehow vary their codebook size in order to match their transmission rate to the capacity region of the MAC in operation. Instead, we here allow the decoder to vary its decoding time depending on the observed channel output—thereby adjusting the rate at which each transmitter communicates by changing not the size but the blocklength of each transmitter's codebook.

We view the RAC as a collection of all possible MACs that might arise as a result of the transmitter activity pattern. Barring the intricacies of multiuser decoding, the model that views an unknown channel as a collection of possible channels without assigning an a priori probability to each is known as the *compound channel* model [94]. In the context of single-transmitter compound channels, it is known that if the decoding time is fixed, the transmission rate cannot exceed the capacity of the weakest channel from the collection [94], though the dispersion may be better (smaller) [95]. With feedback and a variable decoding time, one can do much better [96]–[99].

In [90], Polyanskiy argues for removing the transmitter identification task from the physical layer encoding and decoding procedures of a MAC. As he points out, such a scenario was previously discussed by Berger [100] in the context of conflict resolution. Polyanskiy further suggests studying MACs whose conditional channel output distributions are insensitive to input permutations. For such channels, if all transmitters use the same codebook, then the receiver can at best hope to recover the messages sent without recovering who transmitted which message (the transmitter identity). In some networks the transmitter identification task can be insignificant. For example, in some sensor networks, we might be interested in the collected measurements but indifferent to the identities of the collecting sensors. In scenarios where transmitter identity is required, it can be included in the payload.

In Section 6.4, we propose a code for a random access communication channel model built from a family of permutation-invariant MACs. Our code employs identical encoders at all transmitters and identity-blind decoding at the receiver. Although not critical for the feasibility of our approach, these assumptions lead to a number of pleasing simplifications of both our scheme and its analysis. For example, using identical encoders at all transmitters simplifies design and implementation. Further, the collection of MACs comprising our compound RAC model can be parameterized by the number of active transmitters rather than by the full transmitter activity pattern.

We provide a second-order analysis of the rate universally achieved by our multiuser scheme over all transmitter activity patterns, taking into account the possibility that the decoder may misdetect the current activity pattern and decode for the wrong channel. Leveraging our observation that for a symmetric MAC, the fair rate point is not a corner point of the capacity region, we are able to show that a single-threshold decoding rule attains the fair rate point. This differs significantly from traditional MAC analyses, which use $2^k - 1$ simultaneous threshold rules. In the context of a MAC with a known number of transmitters, second-order analyses of multiple-threshold decoding rules are given in [19]–[22] (finite alphabet MAC) and in [24] (Gaussian MAC). A non-asymptotic analysis of variable-length coding with “single-bit" feedback over a (known) Gaussian MAC appears in [101].

The sparse recovery problem is identical to a special case of the RAC problem in which each transmitter sends only its “signature" to the receiver. Here, the decoder's only task is to determine who is active. Active transmitters in this variant of the RAC problem may correspond to defective items or positive test outcomes in the sparse recovery problem, and successful decoding is identified with successfully detecting the set of defective or confirmed-positive elements. A group testing problem in which an unknown subset of $k$ defective items out of $K$ items total is observed through an OR MAC, is studied in [11], [102]–[105]; this problem is a special case of the sparse recovery problem. In these works, the decoder reaches a conclusion about tested items at a fixed blocklength $n$. Atia and Saligrama [104] consider a noiseless group testing scenario in which the number of transmitted elements, $k$, does not grow with the total number of elements, $K$, showing that the smallest possible number of measurements needed to detect the defective items is $O(k \log \frac{K}{k})$. In in [11], Scarlett and Cevher extend this result to the scenario where $k$ scales as $O(K^{\theta})$ for $\theta \in (0, 1)$. In [105], Scarlett and Cevher derive the information-theoretic limits of the exact and partial support recovery problems for general probabilistic models, where exact recovery refers to detecting all $k$ defective items, and partial recovery refers to detecting at least $s$ out of $k$ defective items. While we consider a nonvanishing average error probability and operate in the central limit theorem regime, [11], [102]–[105] assume vanishing average error probability and operate in the large deviations regime. The main difference between the decoder designs in [11], [102]–[105] and our decoder design is that [11], [102]–[105] use $2^k - 1$ simultaneous information density threshold tests at a single blocklength $n$, while our decoder uses a single information density threshold test at multiple decoding times, allowing successful detection with a computationally less complex decoder even when the number of active transmitters to be detected is unknown.

### Chapter Organization

Our system model and proposed communication strategy are laid out in Section 6.2. The main result, showing that for a nontrivial class of channels our proposed RAC code performs as well in terms of capacity and dispersion as the best-known code for a MAC with the transmitter activity known a priori, is presented in Section 6.3. The proofs are presented in Section 6.4. Section 6.4.4 includes discussions of the effect of using maximum likelihood decoding, the choice of an input distribution in the random code design, the difficulties in proving a converse, an extension of our strategy that enables transmitter identity decoding, and performance bounds under the per-user error probability criterion. Interestingly, the problem of decoding for $k \geq 1$ unknown transmitters is substantially different from the problem of detecting whether there are any active transmitters at all. In Section 6.5, we employ universal hypothesis testing to solve the latter problem. Section 6.7 concludes the chapter with a discussion of our results and their implications.

## 6.2 Problem Setup

**Definition 6.2.1.** *A stationary, memoryless, symmetric, random access channel (henceforth called simply a RAC) is a memoryless channel with one receiver and an unknown number of transmitters. It is described by a family of stationary, memoryless MACs*

$$\left\{\left(\mathcal{X}^k, P_{Y_k|X_{[k]}}(y_k|x_{[k]}), \mathcal{Y}_k\right)\right\}_{k=0}^{K}, \tag{6.1}$$

*each indexed by a number of transmitters, $k$; the maximal number of transmitters is $K \leq \infty$. When $k = 0$, no transmitters are active; we discuss this case separately below. For $k \geq 1$, the $k$-transmitter MAC has input alphabet $\mathcal{X}^k$, output alphabet $\mathcal{Y}_k$, and conditional distribution $P_{Y_k|X_{[k]}}$. When $k$ transmitters are active, the RAC output is $Y = Y_k$. The input and output alphabets $\mathcal{X}$ and $\mathcal{Y}_k$ can be abstract.*

### 6.2.1 Assumptions on the Channel

We assume that the impact of a channel input on the channel output is independent of the transmitter from which it comes; therefore, each channel in

(6.1) is assumed to be *permutation-invariant* [90], giving

$$P_{Y_k|X_{[k]}}(y_k|x_{[k]}) = P_{Y_k|X_{[k]}}(y_k|\hat{x}_{[k]}) \tag{6.2}$$

for all $\hat{x}_{[k]} \overset{\pi}{=} x_{[k]}$ and $y_k \in \mathcal{Y}_k$, $k \in [K]$. We further assume that for any $s < k$, an $s$-transmitter MAC is physically identical to a $k$-transmitter MAC operated with $s$ active and $k-s$ silent transmitters. At each time step of the communication period, each silent transmitter transmits a silence symbol, here denoted by $0 \in \mathcal{X}$. This *reducibility* constraint gives

$$P_{Y_s|X_{[s]}}(y|x_{[s]}) = P_{Y_k|X_{[k]}}(y|x_{[s]}, 0^{k-s}) \tag{6.3}$$

for all $s < k$, $x_{[s]} \in \mathcal{X}_{[s]}$, and $y \in \mathcal{Y}_s$. An immediate consequence of reducibility is that $\mathcal{Y}_s \subseteq \mathcal{Y}_k$ for any $s < k$. Another consequence is that when there are no active transmitters, the MAC $\left(\mathcal{X}^0, P_{Y_0|X_{[0]}}(y|x_{[0]}), \mathcal{Y}_0\right)$ satisfies $\mathcal{X}^0 = \{0\}$ and $P_{Y_0|X_{[0]}}(y|x_{[0]}) = P_{Y_k|X_{[k]}}(y|0^k)$ for all $k$.

### 6.2.2 RAC Communication Strategy

We here propose a new RAC communication strategy. In the proposed strategy, communication occurs in epochs, with each epoch beginning in the time step following the previous epoch's end. Each epoch ends when the receiver's scheduled broadcast to all transmitters indicates a decoding event, signaling that the prior transmission can stop and a new transmission can begin. At this point, each transmitter decides whether to be active or silent in the new epoch; the decision is binding for the length of the epoch, meaning that a transmitter must either actively transmit for all time steps in the epoch or remain silent for the same period. Thus, while the total number of transmitters, $K$, is potentially unlimited and can change arbitrarily from one epoch to the next, the number of active transmitters, $k$, remains constant throughout each epoch.

Each active transmitter uses the epoch to describe a message $W$ from the alphabet $[M]$. When the active transmitters are $[k]$, the messages are $W_{[k]} \in [M]^k$, where the messages $W_1, \ldots, W_k$ of different transmitters are independent and uniformly distributed. The proposed strategy fixes the potential decoding times $n_0 < n_1 < \cdots < n_K$.[1] The receiver chooses to end the epoch (without

[1] We focus the exposition on the scenario where the decoding blocklengths are ordered both for simplicity and because a particular choice of ordered blocklengths emerges as optimal within our architecture (see (6.67) in Section 6.4.3, below).

decoding) at time $n_0$ if it believes at time $n_0$ that no transmitters are active and chooses to end the epoch and decode at time $n_t$ if it believes at time $n_t$ that the number of active transmitters is $t$. The transmitters are informed of the decoder's decision through a single-bit feedback $Z_s$ at each time $n_s$ with $s \in \{0, 1, \ldots, t\}$; here $Z_s = 0$ for all $s < t$ and $Z_t = 1$, with "1" signaling the end of one epoch and the beginning of the next. Since the blocklength for a given epoch is the decoding time chosen by the receiver, the result is a *rateless code*. As we show in Section 6.4 below, with an appropriately designed decoding rule, correct decoding is performed at time $n_k$ with high probability.

It is important to stress that in this domain each transmitter knows nothing about the set of active transmitters $\mathcal{A} \subset \mathbb{N}$ beyond its own membership and what it learns from the receiver's feedback, and the receiver knows nothing about $\mathcal{A}$ beyond what it learns from the channel output $Y$; we call this *agnostic* random access. In addition, since designing a different encoder for each transmitter is expensive from the perspective of both code design and code operation, as in [90], we assume through most of this chapter that every transmitter employs the same encoder; we call this *identical encoding*. Under the assumptions of permutation-invariance and identical encoding, what the transmitters and receiver can learn about $\mathcal{A}$ is quite limited. Together, these properties imply that the decoder can at best distinguish *which messages were transmitted* rather than *by whom they were sent*. In practice, transmitter identity could be included in the header of each $\log M$-bit message or at some other layer of the stack; transmitter identity is not, however, handled by the RAC code. Instead, since the channel output statistics depend on the dimension of the channel input but not the identity of the active transmitters, the receiver's task is to decode the messages transmitted but not the identities of their senders. We therefore assume without loss of generality that $|\mathcal{A}|= k$ implies $\mathcal{A} = [k]$. Thus the family of $k$-transmitter MACs in (6.2) fully describes the behavior of a RAC.[2]

### 6.2.3 Code Definition

The following definition formalizes our code.

**Definition 6.2.2.** *For any number of messages $M$, ordered blocklengths $n_0 < n_1 < \cdots < n_K$, and error probabilities $\epsilon_0, \ldots, \epsilon_K$, an $(M, \{(n_k, \epsilon_k)\}_{k=0}^{K})$ RAC*

[2] Section 6.4.4 treats a variant of our RAC communication strategy that enables decoding of transmitter identity. Mathematically, the variants are quite similar.

*code comprises a (rateless) encoding function*

$$\mathsf{f}\colon \mathcal{U} \times [M] \to \mathcal{X}^{n_K} \tag{6.4}$$

*and a collection of decoding functions*

$$\mathsf{g}_k\colon \mathcal{U} \times \mathcal{Y}_k^{n_k} \to [M]^k \cup \{\mathsf{e}\}, \quad k = 0, 1, \ldots, K, \tag{6.5}$$

*where* $\mathsf{e}$ *denotes the erasure symbol, which is the decoder's output when it is not ready to decode. At the start of each epoch, a common randomness random variable* $U \in \mathcal{U}$*, with* $U \sim P_U$*, is generated independently of the transmitter activity and revealed to the transmitters and the receiver, thereby initializing the encoders and the decoder. If* $k$ *transmitters are active, then with probability at least* $1 - \epsilon_k$*, the* $k$ *messages are correctly decoded at time* $n_k$*. That is,*[3]

$$\frac{1}{M^k} \sum_{w_{[k]} \in [M]^k} \mathbb{P}\Bigg[ \left\{ \mathsf{g}_k(U, Y_k^{n_k}) \overset{\pi}{\neq} w_{[k]} \right\} \bigcup \\ \left\{ \bigcup_{t=0}^{k-1} \{\mathsf{g}_t(U, Y_k^{n_t}) \neq \mathsf{e}\} \right\} \Bigg| W_{[k]} = w_{[k]} \Bigg] \leq \epsilon_k, \tag{6.6}$$

*where* $W_{[k]}$ *are the independent and equiprobable messages of transmitters* $[k]$*, and the given probability is calculated using the conditional distribution* $P_{Y_k^{n_k}|X_{[k]}^{n_k}} = P_{Y_k|X_{[k]}}^{n_k}$*; here* $X_i^{n_k} = \mathsf{f}(U, W_i)^{n_k}$*,* $i = 1, \ldots, k$*. At time* $n_s$*, the decoder outputs the erasure symbol "*$\mathsf{e}$*" if it decides that the number of active transmitters is not* $s$*. If* $k = 0$ *transmitters are active, the unique message "0", denoted* $[M]^0 \triangleq \{0\}$ *to simplify the notation, is decoded at time* $n_0$ *with probability at least* $1 - \epsilon_0$*. That is,*

$$\mathbb{P}\left[\mathsf{g}_0(U, Y_0^{n_0}) \neq 0 | W_{[0]} = 0\right] \leq \epsilon_0. \tag{6.7}$$

In Definition 6.2.2, we index the family of possible codes by the elements of some set $\mathcal{U}$ and include $u \in \mathcal{U}$ as an argument for both the RAC encoder and the RAC decoder. We then represent encoding as the application of a code indexed by some random variable $U \in \mathcal{U}$ chosen independently for each new epoch. Deterministic codes are represented under this code definition by setting the distribution on $U$ as $\mathbb{P}[U = u_0] = 1$ for some $u_0 \in \mathcal{U}$. In practice, we can implement a RAC code with random code choice $U$ using

[3] Recall that $\overset{\pi}{=}$ and $\overset{\pi}{\neq}$ denote equality and inequality up to a permutation.

common randomness. Common randomness available to the transmitters and the receiver allows all nodes to choose the same random variable $U$ to specify a new codebook in each epoch. Operationally, this common randomness can be implemented by allowing the receiver to choose random instance $U$ at the start of each epoch and to broadcast that value to the transmitters just after the feedback bit that ends the previous epoch. Alternatively, all communicators can use synchronized pseudo-random number generators. Broadcasting the value of $U$ increases the epoch-ending feedback from 1 bit to $\lceil \log|\mathcal{U}| \rceil + 1$ bits; Theorem E.4.1 shows that $|\mathcal{U}| \leq K + 1$ suffices to achieve the optimal performance.

In Section 6.4, we employ a general random coding argument to show that a given error vector $(\epsilon_0, \ldots, \epsilon_K)$ is achievable when averaged over the ensemble of codes. Unfortunately, this traditional approach does not show the existence of a deterministic RAC code (i.e., a code with $|\mathcal{U}| = 1$) that achieves the given error vector $(\epsilon_0, \ldots, \epsilon_K)$. The challenge here is that our proof showing that the random code's expected error probability meets each of the $K + 1$ error constraints does not suffice to show that any of the codes in the ensemble meets all of our error constraints simultaneously. A similar issue arises in [18], [58]. For example, in [18], a variable-length feedback code is designed with the aim of achieving average error probability no greater than $\epsilon$ and expected decoding time no greater than $\ell$. To design a single code satisfying both constraints, [18] relies on common randomness. Similarly, [58] describes a variable-length feedback code designed to satisfy an error exponent criterion for every channel in a continuum of binary symmetric or Z channels. Their proof that a single, deterministic code can simultaneously satisfy this continuum of constraints exploits the ordering among the channels in the given family. While channel symmetry can sometimes be leveraged to show the existence of a deterministic code [18, eq. (29)], the symmetries in a RAC are quite different from those in point-to-point channels. We leave the question of whether a single-code solution exists for the RAC to future work.

The code model introduced in Definition 6.2.2 employs identical encoding in addition to common randomness. Under identical encoding, each transmitter uses the same encoder, $\mathsf{f}$, to form a codeword of length $n_K$. That codeword is fed into the channel symbol by symbol. According to Definition 6.2.2, if $k$ transmitters are active, then with probability at least $1 - \epsilon_k$, the decoder recovers the transmitted messages correctly after observing the first $n_k$ channel outputs. As noted previously, the decoder $\mathsf{g}_k$ does not attempt to recover transmitter identity; successful decoding means that the list of messages in the decoder output coincides with the list of messages sent. The error event defined in Definition 6.2.2 differs from the one in [90]. Our definition (6.6) requires that all transmitted messages are decoded correctly. In contrast, [90] bounds a per-user probability of error (PUPE), which measures the fraction of transmitted messages that are missing from the list of decoded messages. In Section 6.4.4, we discuss the error probability for our code under the PUPE criterion.

### 6.2.4 Assumptions on the Input Distribution

To ensure the existence of codes satisfying the error constraints in Definition 6.2.2, we assume that there exists a $P_X$ such that when $X_1, X_2, \ldots, X_K$ are distributed i.i.d. $P_X$, then the conditions in (6.8)–(6.13) below are satisfied.

The *friendliness* assumption states that for all $s \le k \le K$,

$$I_k(X_{[s]}; Y_k | X_{[s+1:k]} = 0^{k-s}) \ge I_k(X_{[s]}; Y_k | X_{[s+1:k]}). \tag{6.8}$$

Friendliness implies that by remaining silent, inactive transmitters enable communication by the active transmitters at rates at least as large as those achievable if the inactive transmitters had actively participated and their codewords were known to the receiver.

The *interference* assumption states that for any $s$ and $t$, $X_{[s]}$ and $X_{[s+1:t]}$ are conditionally dependent given $Y_k$, giving

$$P_{X_{[t]}|Y_k} \ne P_{X_{[s]}|Y_k} P_{X_{[s+1:t]}|Y_k} \quad \forall 1 \le s < t \le k, \forall k. \tag{6.9}$$

Assumption (6.9) eliminates trivial RACs in which transmitters do not interfere.

In order for the decoder to be able to distinguish the time-$n_0$ output $Y_0^{n_0}$ that results when no transmitters are active from the time-$n_0$ output $Y_k^{n_0}$ that results when $k \ge 1$ transmitters are active, we assume that there exists a $\delta_0 > 0$ such that the output distributions satisfy

$$\sup_{y \in \mathcal{Y}_K} |F_k(y) - F_0(y)| \ge \delta_0 \text{ for all } k \in [K], \tag{6.10}$$

where $F_k(y)$ denotes the cdf of $P_{Y_k}$ for $k \in \{0, \ldots, K\}$.[4] The measure of discrepancy between distributions on the left-hand side of (6.10) is known as the Kolmogorov-Smirnov distance. The assumption in (6.10) is only needed to detect the scenario when no transmitters are active; the remainder of the code functions proceed unhampered when (6.10) fails. When $K$ is finite, (6.10) is equivalent to $P_{Y_0} \neq P_{Y_k}$ for all $k \in [K]$.

Finally, the *moment* assumptions

$$\mathrm{Var}\left[\imath_k(X_{[k]}; Y_k)\right] > 0 \tag{6.11}$$

$$\mathbb{E}[|\imath_k(X_{[k]}; Y_k) - I_k(X_{[k]}; Y_k)|^3] < \infty \tag{6.12}$$

enable the second-order analysis presented in Theorem 6.3.1, below. In the case when $\imath_t(X_{[s]}; Y_k) > -\infty$ almost surely, we also require

$$\mathrm{Var}\left[\imath_t(X_{[s]}; Y_k)\right] < \infty \quad \forall s \leq t \leq k. \tag{6.13}$$

Moment assumptions like (6.11)–(6.13) are common in the finite-blocklength literature, e.g., [5], [21].

In the discussion that follows, we say that a channel satisfies our channel assumptions ((6.2), (6.3), (6.8)–(6.13)) if there exists an input distribution $P_X$ under which those conditions are satisfied. All discrete memoryless channels (DMCs) satisfy finite second- and third-moment assumptions (6.12)–(6.13) [5, Lemma 46], as do Gaussian noise channels. Common channel models from the literature typically satisfy a non-zero second-moment assumption (6.11) as well. Example channels that meet our channel assumptions ((6.2), (6.3), and (6.8)–(6.13)) include the Gaussian RAC,

$$Y_k = \sum_{i=1}^{k} X_i + Z, \tag{6.14}$$

where each $X_i \in \mathbb{R}$ operates under power constraint $P$ and $Z \sim \mathcal{N}(0, N)$ for some $N > 0$, and the adder-erasure RAC [92],

$$Y_k = \begin{cases} \sum_{i=1}^{k} X_i, & \text{w.p. } 1 - \delta \\ \mathsf{e} & \text{w.p. } \delta, \end{cases} \tag{6.15}$$

[4] Although the cdf is defined for real-valued random variables, i.e., $\mathcal{Y}_k \subseteq \mathcal{Y}_K \subseteq \mathbb{R}$ is required, it can be generalized to abstract alphabets by introducing a partial order $\leq$ on the set $\mathcal{Y}_K$. Then $F_k(y) \triangleq \mathbb{P}\left[Y_k \leq y\right]$.

where $X_i \in \{0,1\}$ and $Y_k \in \{0,\ldots,k\} \cup \{\mathsf{e}\}$. In [92], the adder-erasure RAC (6.15) is used to model a scenario where a digital encoder and decoder communicate over an analog channel using a modulator and demodulator. The modulator converts the bits into analog signals; the channel output equals the sum of the transmitted signals plus random noise; the demodulator quantizes that output, declaring an erasure, $\mathsf{e}$, if reliable quantization is not possible due to high noise. Thus, one can view the adder-erasure RAC as a discretization of the Gaussian RAC.

For the Gaussian RAC, $\imath_t(X_{[s]};Y_k) > -\infty$ almost surely, and (6.13) is satisfied. For the adder-erasure RAC, $\imath_t(X_{[s]};Y_k) = -\infty$ for some channel realizations and user activity patterns, and (6.13) is not required.

We conclude this section with a series of lemmas that describe the natural orderings possessed by RACs that satisfy our permutation-invariance, reducibility, friendliness, and interference constraints ((6.2), (6.3), (6.8), and (6.9)). These properties are key to the feasibility of the approach proposed in our achievability argument in Section 6.3. Proofs are relegated to Appendix E.1.

The first lemma shows that the quality of the channel for each active transmitter deteriorates as the number of active transmitters grows (even though the sum capacity may increase).

**Lemma 6.2.1.** *Let $X_1, X_2, \ldots, X_k \sim$ i.i.d. $P_X$. Under permutation-invariance (6.2), reducibility (6.3), friendliness (6.8), and interference (6.9),*

$$\frac{I_k}{k} < \frac{I_s}{s} \quad \text{for } k > s \geq 1. \tag{6.16}$$

The second lemma shows that a similar relationship holds even when the number of transmitters is fixed.

**Lemma 6.2.2.** *Let $X_1, X_2, \ldots, X_k \sim$ i.i.d. $P_X$. Under permutation-invariance (6.2), reducibility (6.3) and interference (6.9),*

$$\frac{1}{k} I_k(X_{[k]};Y_k) < \frac{1}{s} I_k(X_{[s]};Y_k|X_{[s+1:k]}) \quad \text{for } k > s \geq 1. \tag{6.17}$$

Lemma 6.2.2 ensures that the equal-rate point of the $k$-MAC lies on the sum-rate boundary and away from all the corner points of the rate region achieved with $P_X$. In their work on the group testing problem [103, Th. 3], Malyutov and Mateev prove a non-strict version of (6.17) for permutation-invariant channels (6.2). They use this non-strict version of (6.17) to conclude that their achievability and converse results in [103, Th. 1 and 2] coincide for permutation-invariant channels. Adding the reducibility (6.3) and interference (6.9) assumptions to the permutation-invariance assumption (6.2) enables us to prove the strict inequality in Lemma 6.2.2, which in turn enables the use of a single threshold rule at the decoder, as discussed in Section 6.4.

Lemma 6.2.3 compares the expected values of the information densities for different channels.

**Lemma 6.2.3.** *Let $X_1, X_2, \ldots, X_k \sim$ i.i.d. $P_X$. If a RAC is permutation-invariant (6.2), reducible (6.3), friendly (6.8), and exhibits interference (6.9), then for any $1 \leq s \leq t < k$,*

$$\mathbb{E}[\imath_t(X_{[s]}; Y_k)] \leq I_k(X_{[s]}; Y_k) < I_t(X_{[s]}; Y_t). \tag{6.18}$$

The orderings in Lemma 6.2.1–6.2.3 are used in bounding the performance of our agnostic random access code.

## 6.3 An Asymptotic Achievability Result

Our main result is the following bound on achievable rates for the RAC.

**Theorem 6.3.1.** *(Achievability) For any RAC*

$$\left\{\left(\mathcal{X}^k, P_{Y_k|X_{[k]}}(y_k|x_{[k]}), \mathcal{Y}_k\right)\right\}_{k=0}^{K}$$

*satisfying (6.2) and (6.3), any $K < \infty$, and any fixed $P_X$ satisfying (6.8)–(6.13), there exists an $(M, \{(n_k, \epsilon_k)\}_{k=0}^{K})$ code provided that*

$$k \log M \leq n_k I_k - \sqrt{n_k V_k} Q^{-1}(\epsilon_k) - \frac{1}{2}\log n_k + O(1) \tag{6.19}$$

*for all $k \in [K]$, and*

$$n_0 \geq c_0 \log n_1 + o(\log n_1), \tag{6.20}$$

*where $c_0$ is a known positive constant. The $O(1)$ term in (6.19) is constant with respect to $n_1$; it depends on the number of active transmitters, $k$, but not on the total number of transmitters, $K$.*

The code in Theorem 6.3.1 assigns equal rates $R_{[k]} = (R, \ldots, R)$, $R = \frac{\log M}{n_k}$, to all active transmitters. The sum-rate $kR$ converges as $O\left(\frac{1}{\sqrt{n_k}}\right)$ to $I_k(X_{[k]}; Y_k)$

for some input distribution $P_{X_{[k]}}(x_{[k]}) = \prod_{i=1}^{k} P_X(x_i)$ for all $k$. Note that $P_X$ is independent of the number of active transmitters, $k$. If the RAC is discrete and memoryless and a single $P_X$ maximizes $I_k(X_{[k]}; Y_k)$ for every $k$, then the achievable rate in (6.19) not only converges to the symmetrical rate point on the capacity region of the MAC in operation but also achieves the best-known second-order term [19]–[22][5] (see Section 6.3.1 for details.)

To better understand Theorem 6.3.1, consider a channel satisfying (6.8)–(6.13) for which the same distribution $P_X$ maximizes $I_k$ for all $k$. For example, for the adder-erasure RAC in (6.15), setting $P_X$ to be Bernoulli$(1/2)$ maximizes $I_k$ for all $k$. By Lemma 6.2.1, for $M$ large enough and any $\epsilon_1, \epsilon_2, \ldots, \epsilon_K$, one can pick $n_1 < n_2 < \cdots < n_K$ so that equality holds in (6.19) for all $k$. Therefore, Theorem 6.3.1 certifies that for some channels, rateless codes with encoders that are, until feedback, agnostic to the transmitter activity pattern perform as well in both first- and second-order terms as the best-known scheme [19]–[22] designed with complete knowledge of transmitter activity. Moreover for any fixed $0 < \epsilon_0 < 1$, the probability that at time $n_0 \geq c_0 \log n_1 + o(\log n_1)$ the decoder correctly detects the scenario where no transmitters are active is no smaller than $1 - \epsilon_0$. Thus, a new epoch can begin very quickly when no transmitters are active in the current epoch.

The constant $c_0$ in (6.20) depends on the output distributions $P_{Y_k}$, $k = 0, \ldots, K$, and on the hypothesis test chosen in Section 6.5 but not on the target probability of error $\epsilon_0$. In contrast, the $o(\log n_1)$ term in (6.20) depends on $\epsilon_0$. See Section 6.5 (eq. (6.146)) for an example where we bound the dependence of the $o(\log n_1)$ term on $\epsilon_0$ under the log-likelihood ratio test.

Our achievability result in Theorem 6.3.1 assumes that the total number of transmitters, $K$, is constant. The asymptotic regime in which $K$ grows with the decoding times, $n_1, n_2, \ldots, n_K$, seeks to characterize scenarios with massive numbers of communicators [11], [90], [108]. Understanding the fundamental limits of random access communications in that regime presents an interesting challenge for future work.

[5] Note that we are comparing the RAC achievable rate with rate-0 feedback to the MAC capacity without feedback. Wagner *et al.* [106] show that if a discrete, memoryless, point-to-point channel has at least two capacity-achieving input distributions and their dispersions $V_1$ (5.5) are distinct, then using one-bit feedback improves the achievable second-order term. Although rate-0 feedback does not change the capacity region of a discrete memoryless MAC [107], in light of [106] it is plausible that even one-bit feedback can improve the achievable second-order term for some MACs.

### 6.3.1 Comparison With the Existing Achievability Results

#### Discrete Memoryless RACs

Our achievable region (Theorem 6.3.1) is consistent with the achievability results for the 2-transmitter MACs given in [19]–[22]. The proofs in [19]–[21] use i.i.d. random code design, an approach that we follow in Theorem 6.3.1. In [22], Scarlett *et al.* use constant-composition codes. In [19]–[21], the achievable rate region of a discrete memoryless MAC is expressed as a three-dimensional vector inequality that relies on a $3 \times 3$ dispersion matrix $\mathsf{V}_2$ defined in [21, eq. (48)]; the entry of $\mathsf{V}_2$ at location $(3, 3)$ is $V_2$ (5.5) for some input distribution $(P_{X_1}, P_{X_2})$. For rate pairs approaching interior (i.e., non-corner) points on the sum-rate boundary for $(P_{X_1^*}, P_{X_2^*})$, i.e., rate pairs satisfying

$$\begin{aligned}(R_1, R_2) \in \{&(r_1 + o(1), r_2 + o(1))\colon \\ &r_1 < I_2(X_1^*; Y_2^*|X_2^*), r_2 < I_2(X_2^*; Y_2^*|X_1^*), r_1 + r_2 = I_2(X_1^*, X_2^*; Y_2^*)\},\end{aligned} \tag{6.21}$$

the achievable region in [19]–[21] reduces to the scalar inequality

$$R_1 + R_2 \leq I_2^* - \sqrt{\frac{V_2^*}{n}} Q^{-1}(\epsilon) + O\left(\frac{\log n}{n}\right), \tag{6.22}$$

where

$$I_2^* \triangleq I_2(X_1^*, X_2^*; Y_2^*) \tag{6.23}$$

is the sum-rate capacity and $V_2^*$ is the dispersion $V_2$ (5.5) evaluated using $(P_{X_1^*}, P_{X_2^*})$. The bound in (6.22) implies that the only component of $\mathsf{V}_2$ employed in the second-order characterization of the region (6.21) is $V_2^*$. The result in (6.22) is proved in [109, Prop. 4 case ii)].

In [22, Th. 1], Scarlett *et al.* use constant-composition codes to show that the dispersion matrix $\mathsf{V}_2$ in the second-order achievable region can be improved to $\tilde{\mathsf{V}}_2$, defined in [22, eq. (13)]. Further, they show that $\tilde{\mathsf{V}}_2 \preceq \mathsf{V}_2$, where $\preceq$ designates positive semidefinite order. Therefore, the second-order rate region that is obtained using constant-composition codes includes that achieved with i.i.d. random coding when the target error probability satisfies $\epsilon < \frac{1}{2}$. Scarlett *et al.* [22] present two examples for which $\tilde{\mathsf{V}}_2 \prec \mathsf{V}_2$, demonstrating that the inclusion can be strict. The $(3, 3)$ component of $\tilde{\mathsf{V}}_2$ is

$$\tilde{V}_2^* = V_2^* - \mathrm{Var}\left[\mathbb{E}\left[\imath_2(X_1^*, X_2^*; Y_2^*)|X_1^*\right]\right] - \mathrm{Var}\left[\mathbb{E}\left[\imath_2(X_1^*, X_2^*; Y_2^*)|X_2^*\right]\right], \tag{6.24}$$

where $P_{X_1^*}P_{X_2^*}P_{Y_2^*|X_1^*,X_2^*} = P_{X_1^*}P_{X_2^*}P_{Y_2|X_1,X_2}$. The right side of (6.22) is achievable with $V_2^*$ replaced by $\tilde{V}_2^*$. In Lemma 6.3.1, below, we derive a saddle point condition for general MACs without cost constraints. Lemma 6.3.1 implies that

$$\tilde{V}_2^* = V_2^*. \tag{6.25}$$

This means that while constant-composition code design can yield achievability results with second-order terms superior to those derived through i.i.d. code design, on the sum-rate boundary that superior performance is observed only at corner points. For any rate point approaching an interior point on the sum-rate boundary, the i.i.d. random code design employed in this chapter achieves first- and second-order performance identical to that achieved by constant-composition code design.

**Lemma 6.3.1.** *Let $P_{Y_2|X_1,X_2}$ be a 2-transmitter MAC with finite sum-rate capacity. Assume that the $\sigma$-algebra on the abstract input alphabets $\mathcal{X}_i$ includes all singletons on $\mathcal{X}_i$, $i = 1,2$. Let $(X_1^*, X_2^*, Y_2^*) \sim P_{X_1^*}P_{X_2^*}P_{Y_2|X_1,X_2}$, where $(P_{X_1^*}, P_{X_2^*})$ is a sum-rate capacity achieving input distribution, i.e.,*

$$I_2^* \triangleq I_2(X_1^*, X_2^*; Y_2^*) = \sup_{P_{X_1}P_{X_2}} I_2(X_1, X_2; Y_2) < \infty. \tag{6.26}$$

*Then, for $i = 1, 2$,*

$$\mathbb{E}\left[\imath_2(X_1^*, X_2^*; Y_2^*)|X_i^*\right] = I_2^*, \tag{6.27}$$

*where (6.27) holds $P_{X_i^*}$-almost surely.*

*Proof:* See Appendix E.2. ■

A version of Lemma 6.3.1 for discrete memoryless MACs appears in [110, Prop. 1]. The result is proved by verifying that (6.27) satisfies the Karush-Kuhn-Tucker (KKT) conditions for the maximization problem in (6.26) (Although the maximization problem in (6.26) is not convex, it satisfies a regularity condition ensuring the necessity of the KKT conditions for optimality [110].) We extend [110, Prop. 1] to general MACs by demonstrating a saddle point condition for MACs. The saddle point condition is more general in the sense that it applies to abstract alphabets.

From (6.27), we deduce that

$$\mathrm{Var}\left[\mathbb{E}\left[\imath_2(X_1^*, X_2^*; Y_2^*)|X_i^*\right]\right] = 0, \quad i = 1, 2. \tag{6.28}$$

Substituting (6.28) into (6.24), we obtain (6.25).

The result in (6.26)–(6.27) extends the following well-known properties of point-to-point DMCs to MACs. In [8, Th. 4.5.1], the KKT conditions in (6.26)–(6.27) for point-to-point DMCs are

$$I_1^* \triangleq \max_{P_{X_1}} I_1(X_1;Y_1) \tag{6.29}$$

$$\mathbb{E}\left[\imath_1(X_1^*;Y_1^*)|X_1^*\right] = I_1^* \quad \text{if } P_{X_1^*}(x_1) > 0 \tag{6.30}$$

$$\mathbb{E}\left[\imath_1(X_1^*;Y_1^*)|X_1^* = x_1\right] \leq I_1^* \quad \text{if } P_{X_1^*}(x_1) = 0; \tag{6.31}$$

these conditions are necessary and sufficient for optimality. As noted in [5, Lemma 62], (6.30)–(6.31) indicate that for a capacity-achieving input distribution $P_{X_1^*}$,

$$\mathrm{Var}\left[\mathbb{E}\left[\imath_1(X_1^*;Y_1^*)|X_1^*\right]\right] = 0. \tag{6.32}$$

From (6.32) and the law of total variance, it follows that the unconditional and conditional variances of $\imath_1(X_1^*;Y_1^*)$ given $X_1^*$ are equal, i.e.,

$$V_1 = \mathbb{E}\left[\mathrm{Var}\left[\imath_1(X_1^*;Y_1^*)|X_1^*\right]\right]. \tag{6.33}$$

For point-to-point DMCs, Moulin [111] shows that the second-order term $\tilde{V}_1$ achievable using constant-composition coding equals the right-hand side of (6.33), meaning that i.i.d. random code design and constant-composition random code design achieve the same fundamental limits for point-to-point DMCs.

### The Gaussian RAC

While the RAC code definition (Definition 6.2.2) does not impose cost constraints on the codewords, cost constraints can be added where needed. In the case of the Gaussian RAC defined in (6.14), the maximal power constraint $P$ on the codewords requires that

$$\|\mathsf{f}(u,w)^{n_k}\|_2^2 \leq n_k P \tag{6.34}$$

for all $u \in \mathcal{U}$, $w \in [M]$, and $k \in [K]$, where $\|\cdot\|_2$ denotes the Euclidean norm. If any encoder attempts to transmit a codeword that does not satisfy (6.34), we count that event as an error. Hence, the maximal power constraints add the term

$$\mathbb{P}\left[\bigcup_{j=1}^{k}\bigcup_{i=1}^{k}\left\{\|X_i^{n_j}\|_2^2 > n_j P\right\}\right] \tag{6.35}$$

to the error terms in (6.6).

For the Gaussian $k$-MAC under maximal power constraints, drawing codewords i.i.d. according to distribution $P_X \sim \mathcal{N}(0, P - \delta_{n_k})$ for any $\delta_{n_k} \to 0$ as $n_k \to \infty$ yields a worse second-order performance bound than the one achieved by drawing codewords uniformly at random from the $n_k$-dimensional power sphere [24], [112]. MolavianJazi and Laneman [24] and Scarlett *et al.* [22] derive the improved second-order term for the Gaussian MAC by drawing codewords uniformly at random over an $n_k$-dimensional power sphere and by combining constant-composition code design with a quantization argument, respectively. The improved achievability bounds on the Gaussian MAC and RAC by employing non-i.i.d. inputs are presented in Chapter 7, below.

### 6.3.2 An Example RAC

The following example investigates rates achievable for the adder-erasure RAC in (6.15).

**Example 6.3.1.** For the adder-erasure RAC, the capacity achieving distribution is the equiprobable (Bernoulli(1/2)) distribution for all $k$. (See the proof of Theorem E.3.1 in Appendix E.3.) For this channel, one can exactly calculate $I_k$ and $V_k$ for this channel for every $k$ (labelled “True” in Fig. 6.1). The approximating characterizations

$$I_k = (1-\delta)\left(\frac{1}{2}\log\frac{\pi e k}{2} - \frac{\log e}{12k^2}\right) + O(k^{-3}) \tag{6.36}$$

$$\begin{aligned} V_k = (1-\delta)\Bigg[&\frac{\delta}{4}\log^2\frac{\pi e k}{2} + \frac{\log^2 e}{2} - \frac{\log^2 e}{2k} \\ &- \left(\frac{\log e}{2} + \frac{\delta\log\frac{\pi e k}{2}}{12}\right)\frac{\log e}{k^2}\Bigg] + O\left(\frac{\log k}{k^3}\right), \end{aligned} \tag{6.37}$$

which capture the first- and second-order behavior of $I_k$ and $V_k$ for each $k$, are, nonetheless, useful since they highlight how each depends on $k$ and $\delta$. These values, without the $O(\cdot)$ terms in (6.36)–(6.37), are labelled “Approximation" in Fig. 6.1. The approximations are quite tight even for small $k$. Both $I_k$ and $\sqrt{V_k}$ are of order $O(\log k)$, indicating that as $k$ grows, the sum-rate capacity grows, albeit slowly, while the per-user rate vanishes as $O\left(\frac{\log k}{k}\right)$. The dispersion $V_k$ also grows, and the speed of approach to the sum-rate capacity is slower. Interestingly, the dispersion behavior is different for the pure adder RAC ($\delta = 0$), in which case $V_k = \frac{\log^2 e}{2} + O\left(\frac{1}{k}\right)$ is almost constant as a function of $k$. The derivation of (6.36) and (6.37) relies on an approximation for the probability mass function of the $(k, 1/2)$ Binomial distribution using a higher order Stirling's approximation (Appendix E.3).

Fig. 6.2 shows the approximate rate per transmitter, $R_k = \frac{\log M}{n_k}$ (neglecting the $O(1)$ term in (6.19)), achieved by the proposed scheme as a function of the number of active transmitters, $k$, and the choice of blocklength $n_1$ for a fixed error probability $\epsilon_k = 10^{-6}$ for all $k$. Fixing $n_1$ and $\epsilon_k$ fixes the maximum achievable message size, $M$, according to (6.19). The remaining $n_k$ for $k \geq 2$ are found by choosing the smallest $n_k$ that satisfies (6.19) using the given $M$ and $\epsilon_k$. Each curve illustrates how the rate per transmitter ($R_k$) decreases as the number of active users $k$ increases. The curves differ in their choice of blocklength $n_1$ and the resulting changes in $M$ and $n_0, n_2, \ldots, n_K$. Here $n_1$ is fixed to $20, 100, 500$ and $2500$. For a fixed $k$, the points on the same vertical line demonstrate how the gap between the per-user capacity and the finite-blocklength achievable rate decreases as blocklength increases.

### 6.3.3 A Non-asymptotic Achievability Result

Theorem 6.3.1 follows from Theorem 6.3.2, stated next, which bounds the error probability of the RAC code defined in Section 6.4. When $k$ transmitters are active, the error probability $\epsilon_k$ captures both errors in the estimate $t$ of $k$ and errors in the reproduction $\hat{W}_{[t]}$ of $W_{[k]}$ when $t = k$. Theorem 6.3.2 is formulated for an arbitrary choice of a statistic $h\colon \mathcal{Y}^{n_0} \mapsto \mathbb{R}$ used to decide whether any transmitters are active. Possible choices for $h(\cdot)$ appear in (6.121) and (6.128) in Section 6.5, below.

**Theorem 6.3.2.** *Fix constants $\gamma_0$, $\lambda^k_{s,t} \geq 0$, and $\gamma_t > 0$ for all $1 \leq s \leq t \leq k$. For any RAC*

$$\left\{\left(\mathcal{X}^k, P_{Y_k|X_{[k]}}(y_k|x_{[k]}), \mathcal{Y}_k\right)\right\}_{k=0}^{K}$$

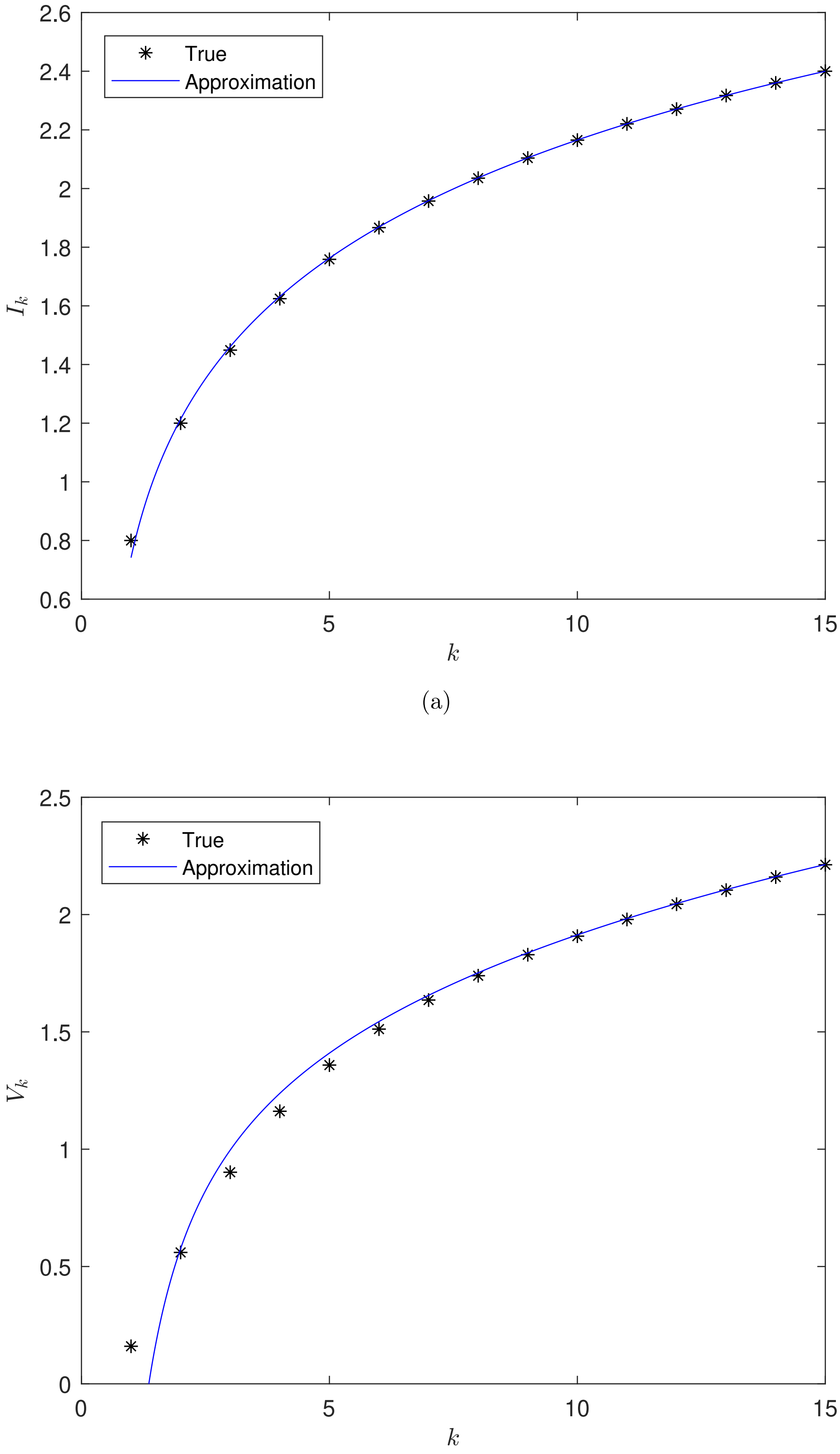
*satisfying (6.2) and (6.3), any $K \leq \infty$[6], and any fixed input distribution $P_X$, there exists an $(M, \{(n_k, \epsilon_k)\}_{k=0}^K)$ code such that*

$$\epsilon_0 \leq \mathbb{P}\left[h(Y_0^{n_0}) > \gamma_0\right], \tag{6.38}$$

*and for all $k \geq 1$,*

$$\epsilon_k \leq \mathbb{P}[\imath_k(X_{[k]}^{n_k}; Y_k^{n_k}) \leq \log \gamma_k] \tag{6.39a}$$

[6] Note that while Theorem 6.3.1 requires $K < \infty$, Theorem 6.3.2 allows $K = \infty$. For $K = \infty$, (6.39) holds for every finite $k$ since the bound on $\epsilon_k$ depends only on the RAC with at most $k$ active transmitters.



(a)

(b)

Figure 6.1: (a) Sum-rate capacity $I_k$ (in bits) and (b) dispersion $V_k$ (in bits$^2$) for the adder-erasure RAC with $\delta = 0.2$.

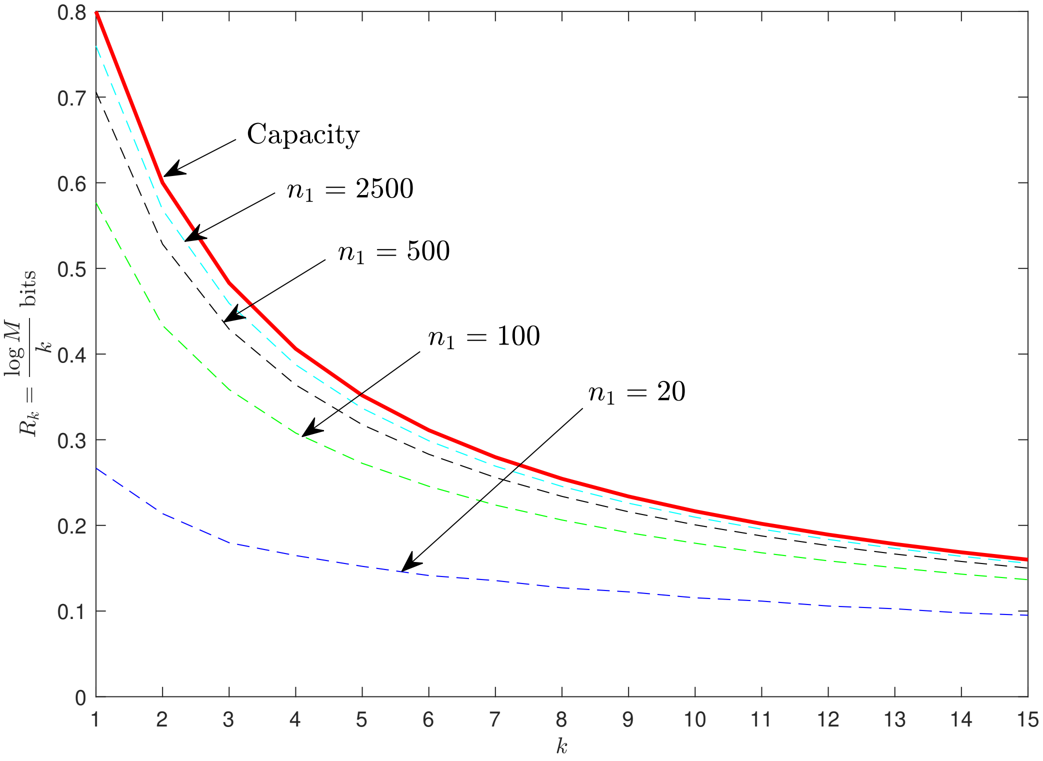


Figure 6.2: Capacity and approximate achievable rates (in bits per user) for the adder-erasure RAC with erasure probability $\delta = 0.2$ are given for the target error probability $\epsilon_k = 10^{-6}$ for all $k$. For each curve, the message size $M$ is fixed so that the rates $\{R_k\}$ are achievable with $n_1$ set to $20, 100, 500$, and $2500$, respectively.

$$
\begin{aligned}
&+\mathbb{P}\left[h(Y_k^{n_0}) \leq \gamma_0\right] && \textit{(6.39b)}\\
&+\frac{k(k-1)}{2M} && \textit{(6.39c)}\\
&+\sum_{t=1}^{k-1}\binom{k}{t}\mathbb{P}[\imath_t(X_{[t]}^{n_t};Y_k^{n_t}) > \log\gamma_t] && \textit{(6.39d)}\\
&+\sum_{t=1}^{k}\sum_{s=1}^{t-1}\binom{k}{t-s}\mathbb{P}\Big[\imath_t(X_{[s+1:t]}^{n_t};Y_k^{n_t})\\
&\quad > n_t\mathbb{E}[\imath_t(X_{[s+1:t]};Y_k)] + \lambda_{s,t}^k\Big] && \textit{(6.39e)}\\
&+\sum_{t=1}^{k}\sum_{s=1}^{t}\binom{k}{t-s}\binom{M-k}{s}\mathbb{P}\Big[\imath_t(\overline{X}_{[s]}^{n_t};Y_k^{n_t}|X_{[s+1:t]}^{n_t})\\
&\quad > \log\gamma_t - n_t\mathbb{E}[\imath_t(X_{[s+1:t]};Y_k)] - \lambda_{s,t}^k\Big], && \textit{(6.39f)}
\end{aligned}
$$

*where for any* $n$, $(X_{[k]}^n, \overline{X}_{[k]}^n, Y_k^n)$ *is a random sequence drawn i.i.d. from*

$$P_{X_{[k]}\overline{X}_{[k]}Y_k}(x_{[k]}, \overline{x}_{[k]}, y_k) = \left(\prod_{i=1}^{k} P_X(x_i)P_X(\overline{x}_i)\right) P_{Y_k|X_{[k]}}(y_k|x_{[k]}). \tag{6.40}$$

The operational regime of interest is when $\epsilon_0, \ldots, \epsilon_k$ are constant; that is, $\epsilon_k$ does not vanish as $n_k$ grows. For $k = 0$, the error term in (6.38) is the probability that the decoder does not correctly determine that the number of active transmitters is 0 at time $n_0$. For $k > 0$, (6.39a) is the probability that the true codeword set produces a low information density. This is the dominating term in the regime of interest. All remaining terms are negligible, as shown in the refined asymptotic analysis of the bound in Theorem 6.3.2 (see Section 6.4.3, below.) The remaining terms bound the probability that the decoder incorrectly estimates the number of active transmitters as 0 (6.39b), the probability that two or more transmitters send the same message (6.39c),[7] the probability that the decoder estimates the number of active transmitters as $t$ for some $1 \leq t < k$ and decodes those $t$ messages correctly (6.39d), and the probability that the decoder estimates the number of active transmitters as $t$ for some $1 \leq t \leq k$ and decodes to $s$ messages that were not transmitted and $t - s$ messages that were transmitted (6.39e)–(6.39f).

For $k = 1, 2$, the expression in (6.39) particularizes to

$$\begin{aligned}
\epsilon_1 \leq\ & \mathbb{P}[\imath_1(X_1^{n_1}; Y_1^{n_1}) \leq \log \gamma_1] + \mathbb{P}\left[h(Y_1^{n_0}) \leq \gamma_0\right] \\
&+ (M-1)\mathbb{P}[\imath_1(\overline{X}_1^{n_1}; Y_1^{n_1}) > \log \gamma_1 - \lambda_{1,1}^1]
\end{aligned} \tag{6.41}$$

$$\begin{aligned}
\epsilon_2 \leq\ & \mathbb{P}[\imath_2(X_{[2]}^{n_2}; Y_2^{n_2}) \leq \log \gamma_2] + \mathbb{P}\left[h(Y_2^{n_0}) \leq \gamma_0\right] \\
&+ \frac{1}{M} + 2\mathbb{P}[\imath_1(X_1^{n_1}; Y_2^{n_1}) > \log \gamma_1] \\
&+ 2\mathbb{P}[\imath_2(X_2^{n_2}; Y_2^{n_2}) \geq n_2 I_2(X_2; Y_2) + \lambda_{1,2}^2] \\
&+ (M-1)\mathbb{P}[\imath_1(\overline{X}_1^{n_1}; Y_2^{n_1}) > \log \gamma_1 - \lambda_{1,1}^2] \\
&+ 2(M-2)\mathbb{P}[\imath_2(\overline{X}_1^{n_2}; Y_2^{n_2} | X_2^{n_2}) > \log \gamma_2 - n_2 I_2(X_2; Y_2) - \lambda_{1,2}^2] \\
&+ \frac{(M-2)(M-3)}{2}\mathbb{P}[\imath_2(\overline{X}_{[2]}^{n_2}; Y_2^{n_2}) > \log \gamma_2 - \lambda_{2,2}^2].
\end{aligned} \tag{6.42}$$

For the MAC with $K$ transmitters, i.e., the scenario where $K$ transmitters are always active, the only decoding time is $n_K$. The error terms associated

[7] Given the use of identical encoders, multiple encoders sending the same message can be beneficial or harmful, depending on the channel. To simplify the analysis, we treat this (exponentially rare) event as an error.

with incorrect decoding times are no longer needed in this case, and the error probability bound in (6.39) becomes

$$\epsilon_K \leq \mathbb{P}[\imath_K(X_{[K]}^{n_K}; Y_K^{n_K}) \leq \log \gamma_K] + \frac{K(K-1)}{2M} \tag{6.43}$$

$$+ \sum_{s=1}^{K-1} \binom{K}{K-s} \mathbb{P}\left[\imath_K(X_{[s+1:K]}^{n_K}; Y_K^{n_K}) > n_K \mathbb{E}[\imath_K(X_{[s+1:K]}; Y_K)] + \lambda_{s,K}^K\right] \tag{6.44}$$

$$+ \sum_{s=1}^{K} \binom{K}{K-s} \binom{M-K}{s} \mathbb{P}\Big[\imath_K(\overline{X}_{[s]}^{n_K}; Y_K^{n_K} | X_{[s+1:K]}^{n_K})$$
$$> \log \gamma_K - n_K \mathbb{E}[\imath_K(X_{[s+1:K]}; Y_K)] - \lambda_{s,K}^K\Big]. \tag{6.45}$$

A description of the proposed RAC code and the proofs of Theorems 6.3.1 and 6.3.2 appear in Section 6.4.

## 6.4 RAC Code and Its Performance

### 6.4.1 Code Design

We construct the RAC code used in the proofs of Theorems 6.3.1 and 6.3.2 as follows.

**Encoder Design**: The common randomness random variable
$U = (U(1), \ldots, U(M))$ has distribution

$$P_U \triangleq P_{U(1)} \times \cdots \times P_{U(M)}, \tag{6.46}$$

where $P_{U(w)} = P_X^{n_K}$, $w = 1, \ldots, M$, and $P_X$ is a fixed distribution on alphabet $\mathcal{X}$. Each realization of $U$ defines a codebook with $M$ i.i.d. vectors $U(1), \ldots, U(M)$ of dimension $n_K$ (the codewords). Note that the cardinality of the alphabet $U$ is $|\mathcal{X}|^{Mn_K}$. In [18, Th. 19], Polyanskiy *et al.* use Carathéodory's Theorem to show that the common randomness $U$ can be replaced with common randomness $U'$ with cardinality at most $K+2$. We reduce this alphabet size to $K+1$ in Appendix E.4. As described in Definition 6.2.2, an $(M, \{(n_k, \epsilon_k)\}_{k=0}^K)$ RAC code with identical encoders employs the same encoder $\mathsf{f}(\cdot)$ at every transmitter. The encoder $\mathsf{f}(U, \cdot)$ depends on $U$ as

$$\mathsf{f}(U, w) = U(w) \quad \text{for } w = 1, \ldots, M. \tag{6.47}$$

For brevity, we omit $U$ in the encoding and decoding functions and write $\mathsf{f}(U, w) = \mathsf{f}(w)$ for $w = 1, \ldots, M$, and $\mathsf{g}_k(U, y^{n_k}) = \mathsf{g}_k(y^{n_k})$ for $y^{n_k} \in \mathcal{Y}_K^{n_k}, k \in$

$\{0, \ldots, K\}$. Recall that $\mathsf{f}(w)$ is a $n_K$-dimensional vector. We use $\mathsf{f}(w)^{n_k}$ to denote the first $n_k$ coordinates of vector $\mathsf{f}(w)$. For any collection of messages $w_{[k]} \in [M]^k$, we use $\mathsf{f}\left(w_{[k]}\right) \triangleq (\mathsf{f}(w_1), \ldots, \mathsf{f}(w_k))$ to denote the collection of encoded descriptions produced by the encoders.

**Decoder Design**: Upon receiving the first $n_0$ samples of the channel output $Y$, the decoder runs the following composite hypothesis test

$$\mathsf{g}_0(y^{n_0}) = \begin{cases} 0 & \text{if} \quad h(y^{n_0}) \leq \gamma_0 \\ \mathsf{e} & \text{otherwise} \end{cases} \tag{6.48}$$

to decide whether there are any active transmitters. Decoder output 0 signifies that the decoder decides that all transmitters are silent, sending a feedback bit '1' to all transmitters to start a new coding epoch. Decoder output $\mathsf{e}$ indicates that the receiver believes that there are active transmitters; the decoder transmits feedback bit '0' to the transmitters, telling them that it is not ready to decode, and therefore that transmissions must continue. Statistic $h$: $\mathcal{Y}^{n_0} \mapsto \mathbb{R}$ is used to decide whether any transmitters are active.

For each $k \geq 1$, decoder $\mathsf{g}_k$ observes output $y^{n_k}$ and employs a single threshold rule

$$\mathsf{g}_k(y^{n_k}) = \begin{cases} w_{[k]} & \text{if} \quad \imath_k(\mathsf{f}\left(w_{[k]}\right)^{n_k}; y^{n_k}) > \log \gamma_k \quad \text{and } w_i < w_j \ \forall\, i < j \\ \mathsf{e} & \text{otherwise} \end{cases} \tag{6.49}$$

for some constant $\gamma_k$ chosen before the transmission starts. Under permutation-invariance (6.2) and identical encoding (6.4), all permutations of the message vector $w_{[k]}$ give the same information density. We use the ordered permutation specified in (6.49) as a representative of the equivalence class with respect to the binary relation $\overset{\pi}{=}$. The choice of a representative is immaterial since decoding is identity-blind. When there is more than one ordered $w_{[k]}$ that satisfies the threshold condition, decoder $\mathsf{g}_k$ chooses among these options arbitrarily. All such events are counted as errors in the analysis in Section 6.4.2, below. If the decoder output is a message vector $w_{[k]}$, then the decoder sends feedback bit '1', telling them to stop transmission. Otherwise, the decoder sends feedback bit '0', and the epoch continues. For $k \geq 1$, the decoder $\mathsf{g}_k(y^{n_k})$ depends on $U$ through its dependence on the encoding function $\mathsf{f}\left(w_{[k]}\right)$; for $k = 0$, $\mathsf{g}_0(y^{n_0})$ does not depend on $U$.

The proof of Theorem 6.3.2, below, bounds the error probability for the proposed code.

### 6.4.2 Proof of Theorem 6.3.2

In the discussion that follows, we bound the error probability of the code $(\mathsf{f}, \{\mathsf{g}_k\}_{k=0}^K)$ defined above. For $k = 0$, the only error event is that the received vector at time $n_0$, $Y_0^{n_0}$, fails to pass the test

$$\epsilon_0 \leq \mathbb{P}\left[\mathsf{g}_0(Y_0^{n_0}) \neq 0 | W_0 = 0\right] \tag{6.50}$$

given in (6.48). For $k > 0$, the analysis relies on the independence of codewords $\mathsf{f}(W_i)$ and $\mathsf{f}(W_j)$ from distinct transmitters $i$ and $j$. Given identical encoders and i.i.d. codeword design, this assumption is valid provided that $W_i \neq W_j$; we therefore count events of the form $W_i = W_j$ as errors. Let $\mathbb{P}_{\text{rep}}$ denote the probability of such a repetition; the union bound gives

$$\mathbb{P}_{\text{rep}} \leq \frac{k(k-1)}{2M}. \tag{6.51}$$

The discussion that follows uses $w_{[k]}^* = (1, 2, \ldots, k)$ as an example instance of a message vector $w_{[k]}$ in which $w_i \neq w_j$ for all $i \neq j$. The set $\tilde{\mathcal{W}}_{[s]}$ describes all ordered message vectors that do not share any messages in common with $w_{[k]}^*$, i.e.,

$$\tilde{\mathcal{W}}_{[s]} \triangleq \{\tilde{w}_{[s]} \in [M]^s \colon \tilde{w}_1 > k, \tilde{w}_i < \tilde{w}_j \ \ \forall i < j\}. \tag{6.52}$$

Let the components of the vectors $(X_{[k]}^{n_k}, \overline{X}_{[k]}^{n_k}, Y_k^{n_k})$ be i.i.d. with joint distribution

$$P_{X_{[k]}\overline{X}_{[k]}Y_k}(x_{[k]}, \overline{x}_{[k]}, y_k) = P_{X_{[k]}}(x_{[k]}) P_{X_{[k]}}(\overline{x}_{[k]}) P_{Y_k|X_{[k]}}(y_k|x_{[k]}). \tag{6.53}$$

Recall that the information density $\imath_t(x_{[t]}^{n_t}; y_t^{n_t})$ in (5.1) is defined with respect to $(X_{[t]}^{n_t}, Y_t^{n_t})$, not with respect to $(\overline{X}_{[t]}^{n_t}, Y_t^{n_t})$. The resulting error bound proceeds as shown in (6.54)–(6.59), below,

$$\begin{aligned}\epsilon_k = \frac{1}{M^k} \sum_{w_{[k]} \in [M]^k} & \mathbb{P}[\{\mathsf{g}_0(Y_k^{n_0}) \neq \mathsf{e}\} \cup \{\cup_{t=1}^{k-1} \mathsf{g}_t(Y_k^{n_t}) \neq \mathsf{e}\} \\ & \cup \{\mathsf{g}_k(Y_k^{n_k}) \overset{\pi}{\neq} w_{[k]}\} | W_{[k]} = w_{[k]}]\end{aligned} \tag{6.54}$$

$$
\begin{aligned}
&\le \mathbb{P}_{\text{rep}} + (1-\mathbb{P}_{\text{rep}})\mathbb{P}[\{\mathsf{g}_0(Y_k^{n_0}) \neq \mathsf{e}\} \\
&\quad \cup \{\cup_{t=1}^{k-1}\mathsf{g}_t(Y_k^{n_t}) \neq \mathsf{e}\} \cup \{\mathsf{g}_k(Y_k^{n_k}) \overset{\pi}{\neq} w^*_{[k]}\}|W_{[k]} = w^*_{[k]}] && (6.55)\\
&\le \mathbb{P}_{\text{rep}} + \mathbb{P}[\mathsf{g}_0(Y_k^{n_0}) \neq \mathsf{e}|W_{[k]} = w^*_{[k]}] + \sum_{t=1}^{k-1}\binom{k}{t}\mathbb{P}[\mathsf{g}_t(Y_k^{n_t}) \overset{\pi}{=} w^*_{[t]}|W_{[k]} = w^*_{[k]}] \\
& && (6.56)\\
&\quad + \sum_{t=1}^{k}\sum_{s=1}^{t}\binom{k}{t-s}\mathbb{P}[\cup_{\tilde{w}_{[s]}\in\tilde{\mathcal{W}}_{[s]}}\{\mathsf{g}_t(Y_k^{n_t}) \overset{\pi}{=} (\tilde{w}_{[s]}, w^*_{[s+1:t]})\}|W_{[k]} = w^*_{[k]}] \\
&\quad + \mathbb{P}[\mathsf{g}_k(Y_k^{n_k}) = \mathsf{e}|W_{[k]} = w^*_{[k]}] && (6.57)\\
&\le \frac{k(k-1)}{2M} + \mathbb{P}\left[h(Y_k^{n_0}) \le \gamma_0\right] + \sum_{t=1}^{k-1}\binom{k}{t}\mathbb{P}[\imath_t(X_{[t]}^{n_t}; Y_k^{n_t}) > \log\gamma_t] && (6.58)\\
&\quad + \sum_{t=1}^{k}\sum_{s=1}^{t}\binom{k}{t-s}\mathbb{P}[\cup_{\tilde{w}_{[s]}\in\tilde{\mathcal{W}}_{[s]}}\{\imath_t(\overline{X}_{[s]}^{n_t}(\tilde{w}_{[s]}), X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > \log\gamma_t\}] \\
&\quad + \mathbb{P}[\imath_k(X_{[k]}^{n_k}; Y_k^{n_k}) \le \log\gamma_k]. && (6.59)
\end{aligned}
$$

Here $X_{[k]}$ is the vector of transmitted codewords, and $\overline{X}_{[s]}(\tilde{w}_{[s]})$ is an i.i.d. copy of $\overline{X}_{[s]}$, which represents the codeword for a collection of messages $\tilde{w}_{[s]} \in \tilde{\mathcal{W}}_{[s]}$ that was not transmitted. Line (6.55) separates the case where at least one message is repeated from the case where there are no repetitions. Lines (6.56)–(6.57) enumerate the error events in the no-repetition case; these include all cases where the transmitted codeword passes the binary hypothesis test (6.48) for “no active transmitters" (6.56), all cases where a subset of the transmitted codewords meets the threshold for some $t < k$ (6.56), all cases where a codeword that is incorrect in $s$ dimensions and correct in $t-s$ dimensions meets the threshold for $t \le k$ (6.57), and all cases where the transmitted codeword fails to meet the threshold (6.57). We apply the union bound and the symmetry of the code design to represent the probability of each case by the probability of an example instance times the number of instances. Equations (6.58)-(6.59) apply the bound in (6.51) and replace decoders by the threshold rules in their definitions.

The delay in applying the union bound to the first probability in (6.59) is deliberate. It allows us to exploit the symmetry assumptions on the channel and to use a single threshold rule instead of $2^k - 1$ threshold rules as in [19]–

[22]. Applying the bound

$$\mathbb{P}\left[\bigcup_{\tilde{w}_{[s]}\in\tilde{\mathcal{W}}_{[s]}}\{\imath_t(\overline{X}_{[s]}^{n_t}(\tilde{w}_{[s]}), X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > \log\gamma_t\}\right] \tag{6.60}$$

$$\begin{aligned}
&= \mathbb{P}\left[\bigcup_{\tilde{w}_{[s]}\in\tilde{\mathcal{W}}_{[s]}}\{\imath_t(\overline{X}_{[s]}^{n_t}(\tilde{w}_{[s]}), X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > \log\gamma_t\}\right.\\
&\qquad\qquad \left.\bigcap\left\{\imath_t(X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > n_t\mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] + \lambda_{s,t}^k\right\}\right]\\
&+ \mathbb{P}\left[\bigcup_{\tilde{w}_{[s]}\in\tilde{\mathcal{W}}_{[s]}}\{\imath_t(\overline{X}_{[s]}^{n_t}(\tilde{w}_{[s]}), X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > \log\gamma_t\}\right.\\
&\qquad\qquad \left.\bigcap\left\{\imath_t(X_{[s+1:t]}^{n_t}; Y_k^{n_t}) \le n_t\mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] + \lambda_{s,t}^k\right\}\right]\\
&\le \mathbb{P}\left[\imath_t(X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > n_t\mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] + \lambda_{s,t}^k\right]\\
&+ \mathbb{P}\left[\bigcup_{\tilde{w}_{[s]}\in\tilde{\mathcal{W}}_{[s]}}\{\imath_t(\overline{X}_{[s]}^{n_t}(\tilde{w}_{[s]}); Y_k^{n_t}|X_{[s+1:t]}^{n_t}) > \log\gamma_t - n_t\mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] - \lambda_{s,t}^k\}\right]
\end{aligned} \tag{6.61}$$

before applying the union bound to the first probability in (6.59) yields a tighter bound. Combining (6.59) and (6.61) and applying the union bound to the second probability in (6.61) completes the proof.

### 6.4.3 Proof of Theorem 6.3.1

We fix $P_X$, $M$, $\{\epsilon_k\}_{k=0}^K$, and we set the blocklengths $\{n_k\}_{k=1}^K$ as

$$n_k = \gamma_k^2\left(\frac{e}{k}(M-k)\right)^{-2k}, \tag{6.62}$$

where

$$\log\gamma_k \triangleq n_k I_k - \tau_k\sqrt{n_k V_k} \tag{6.63}$$

$$\tau_k \triangleq Q^{-1}\left(\epsilon_k - \frac{B_k + C_k}{\sqrt{n_k}}\right), \tag{6.64}$$

$C_k$ is a constant to be chosen in (6.93),

$$B_k \triangleq \frac{0.56\ T_k}{V_k^{3/2}} \tag{6.65}$$

is the Berry-Esseen constant Theorem 2.3.1 (which is finite by the moment assumptions (6.11) and (6.12)), and

$$T_k \triangleq \mathbb{E}\left[|\imath_k(X_{[k]}; Y_k) - I_k|^3\right]. \tag{6.66}$$

The choice of the threshold $\gamma_k$ (6.63) follows the approach established for the point-to-point channel in [5]. Solving (6.62) for $M$ and applying the Taylor series expansion to $Q^{-1}(\cdot)$, we see that the size of the codebook admits the following expansion

$$k \log M = n_k I_k - \sqrt{n_k V_k} Q^{-1}(\epsilon_k) - \frac{1}{2}\log n_k + O(1) \tag{6.67}$$

simultaneously for all $k \in [K]$. Note that the expansion in (6.67) is the best-known performance up to the second-order term for MACs without random access [19]–[22], and we have chosen our parameters with the goal of matching that best prior performance. By Lemma 6.2.1, the resulting blocklengths satisfy $n_1 < n_2 < \cdots < n_K$ for $M$ large enough.

We proceed to apply Theorem 6.3.2 to show that under the given parameter choices, the probability of decoding error at time $n_k$ is bounded above by $\epsilon_k$. The constants $\left\{\lambda^k_{s,t}\right\}$ used in the error probability bound (6.39e)–(6.39f) are set as

$$\lambda^k_{s,t} = \frac{n_t}{2}\left(I_t(X_{[s]}; Y_t | X_{[s+1:t]}) - \frac{s}{t} I_t\right) \tag{6.68}$$

to ensure that $\lambda^k_{s,t} > 0$ when $s < t$ (see Lemma 6.2.2) and that $\lambda^k_{s,t} = 0$ when $s = t$. Next, we sequentially bound the terms in Theorem 6.3.2 using the parameters chosen in (6.62), (6.63), and (6.68).

- (6.39a): As noted previously, this is the dominant term. Since $\imath_k(X^{n_k}_{[k]}; Y^{n_k}_k)$ is a sum of $n_k$ independent random variables, by the Berry-Esseen theorem [25, Chapter XVI.5 Th. 2] and (6.63)–(6.65),

$$\mathbb{P}\left[\imath_k(X^{n_k}_{[k]}; Y^{n_k}_k) \le \log \gamma_k\right] \le \epsilon_k - \frac{C_k}{\sqrt{n_k}}. \tag{6.69}$$

- (6.39b): The test statistic $h(\cdot)$ and the threshold $\gamma_0$ given in (6.48) are chosen in Section 6.5 to satisfy

$$\mathbb{P}\left[h(Y^{n_0}_k) \le \gamma_0\right] \le \frac{E_k}{\sqrt{n_k}} \tag{6.70}$$

$$\mathbb{P}\left[h(Y_0^{n_0}) > \gamma_0\right] \leq \epsilon_0 \tag{6.71}$$

for some constant $E_k > 0$. Lemma 6.4.1, below, bounds the type-II error in (6.70) in terms of $n_0$ when the type-I error in (6.71) is bounded by $\epsilon_0$.

**Lemma 6.4.1.** *Fix $\epsilon_0 \in (0,1)$. Assume that (6.10) holds. Then there exists a test function $h(\cdot)$ such that (6.71) is satisfied and*

$$\mathbb{P}\left[h(Y_k^{n_0}) \leq \gamma_0\right] \leq \exp\{-n_0 C' + o(n_0)\} \tag{6.72}$$

*for some $C' > 0$ depending on the output distributions $P_{Y_i}$ for $i = 0, \ldots, K$.*

*Proof:* See Section 6.5. ■

From (6.67), $n_k = O\left(n_1\right)$ for $k \geq 1$. To make (6.72) behave as $O\left(\frac{1}{\sqrt{n_k}}\right)$ in Lemma 6.4.1, we pick $n_0$ as in (6.20) with $c_0 = \frac{1}{2C'}$.

- (6.39c): According to (6.62), the upper bound $\frac{k(k-1)}{2M}$ on $\mathbb{P}_{\text{rep}}$ in (6.51) decays exponentially with $n_k$.
- (6.39d): Define $p$ as

$$p \triangleq \mathbb{P}[\imath_t(X_{[t]}; Y_k) > -\infty]. \tag{6.73}$$

We next analyze (6.39d) for the cases $p = 1$ and $p < 1$.

Case 1: $p = 1$. By Lemma 6.2.3 and moment assumption (6.13),

$$I_t - \mathbb{E}\left[\imath_t(X_{[t]}; Y_k)\right] - \tau_t \sqrt{\frac{V_t}{n_t}} > 0 \tag{6.74}$$

for sufficiently large $n_t$. Chebyshev's inequality gives

$$\begin{aligned} &\mathbb{P}[\imath_t(X_{[t]}^{n_t}; Y_k^{n_t}) > \log \gamma_t] \\ &\quad \leq \frac{\operatorname{Var}[\imath_t(X_{[t]}; Y_k)]}{n_t\left(I_t - \mathbb{E}\left[\imath_t(X_{[t]}; Y_k)\right] - \tau_t\sqrt{\frac{V_t}{n_t}}\right)^2}. \end{aligned} \tag{6.75}$$

The right side of (6.75) behaves as $O\left(\frac{1}{n_t}\right)$.

Case 2: $p < 1$. Here

$$\begin{aligned} \mathbb{P}[\imath_t(X_{[t]}^{n_t}; Y_k^{n_t}) > \log \gamma_t] &\leq \mathbb{P}[\imath_t(X_{[t]}^{n_t}; Y_k^{n_t}) > -\infty] && (6.76) \\ &= p^{n_t}, && (6.77) \end{aligned}$$

where (6.77) holds because $\imath_t(X_{[t]}^{n_t}; Y_k^{n_t})$ is the sum of $n_t$ i.i.d. random variables, and that sum is greater than $-\infty$ if and only if all the summands satisfy the same inequality. From (6.75) and (6.77), (6.39d) contributes $O\left(\frac{1}{n_k}\right)$ to our error bound.

- (6.39e): As in the analysis of (6.39d), we define

$$q \triangleq \mathbb{P}[\imath_t(X_{[s+1:t]}; Y_k) > -\infty], \tag{6.78}$$

and treat the cases $q = 1$ and $q < 1$ separately. Observe that for $q = 1$, Chebyshev's inequality implies

$$\begin{aligned} &\mathbb{P}\left[\imath_t(X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > n_t \mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] + \lambda_{t,s}^k\right] \\ &\quad\leq \frac{\mathrm{Var}\left[\imath_t(X_{[s+1:t]}; Y_k)\right]}{n_t\left(\frac{1}{2}(I_t(X_{[s]}; Y_t | X_{[s+1:t]}) - \frac{s}{t} I_t)\right)^2}, \end{aligned} \tag{6.79}$$

which is of order $O\left(\frac{1}{n_t}\right)$ by the moment assumption (6.13) and Lemma 6.2.2. For $q < 1$,

$$\mathbb{P}\left[\imath_t(X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > n_t \mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] + \lambda_{t,s}^k\right] \leq q^{n_t}. \tag{6.80}$$

Therefore (6.39e) contributes $O\left(\frac{1}{n_k}\right)$ to our error bound.

- (6.39f): First, consider the case where $s < t \leq k$. By Lemma 6.2.3 and Chernoff's bound,

$$\mathbb{P}[\imath_t(\overline{X}_{[s]}^{n_t}; Y_k^{n_t} | X_{[s+1:t]}^{n_t}) > \log \gamma_t - n_t \mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] - \lambda_{s,t}^k] \tag{6.81}$$

$$\leq \mathbb{P}[\imath_t(\overline{X}_{[s]}^{n_t}; Y_k^{n_t} | X_{[s+1:t]}^{n_t}) > \log \gamma_t - n_t I_t(X_{[s+1:t]}; Y_t) - \lambda_{s,t}^k] \tag{6.82}$$

$$\begin{aligned} &\leq \mathbb{E}\left[\exp\left\{\imath_t\left(\overline{X}_{[s]}^{n_t}; Y_k^{n_t} | X_{[s+1:t]}^{n_t}\right)\right\}\right] \\ &\quad \exp\{-(\log \gamma_t - n_t I_t(X_{[s+1:t]}; Y_t) - \lambda_{s,t}^k)\} \end{aligned} \tag{6.83}$$

$$= \exp\{-(\log \gamma_t - n_t I_t(X_{[s+1:t]}; Y_t) - \lambda_{s,t}^k)\}. \tag{6.84}$$

Using Stirling's bound

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k, \tag{6.85}$$

we find that for all $s \leq t \leq k$

$$\log \binom{M-k}{s} \leq s \log\left(\frac{e(M-k)}{s}\right) \tag{6.86}$$

$$\leq s \log\left(\frac{e(M-t)}{t}\right) + s\log\left(\frac{t}{s}\right) \tag{6.87}$$

$$= \frac{s}{t}\left(\log\gamma_t - \frac{1}{2}\log n_t\right) + s\log\left(\frac{t}{s}\right), \tag{6.88}$$

where (6.88) follows from (6.62). From (6.63), (6.68), (6.84), and (6.88), we have

$$\begin{aligned}
&\binom{M-k}{s}\mathbb{P}[\imath_t(\overline{X}_{[s]}^{n_t}; Y_k^{n_t}|X_{[s+1:t]}^{n_t}) > \log\gamma_t - n_t I_t(X_{[s+1:t]}; Y_t) - \lambda_{s,t}^k] \\
&\leq \exp\Bigg\{ - n_t \frac{1}{2}\left(I_t(X_{[s]}; Y_t|X_{[s+1:t]}) - \frac{s}{t}I_t\right) \\
&\qquad + \left(1 - \frac{s}{t}\right)\tau_t\sqrt{n_t V_t} - \frac{s}{2t}\log n_t + s\log\left(\frac{t}{s}\right)\Bigg\}.
\end{aligned} \tag{6.89}$$

Lemma 6.2.2 ensures that the exponent in (6.89) is negative for $n_t$ large enough.

For $s = t < k$, from (6.84) and (6.88) with $s = t$, we get

$$\binom{M-k}{t}\mathbb{P}[\imath_t(\overline{X}_{[t]}^{n_t}; Y_k^{n_t}) > \log\gamma_t] \leq \frac{\binom{M-k}{t}}{\gamma_t} \leq \frac{1}{\sqrt{n_t}}. \tag{6.90}$$

For $s = t = k$, changing to the measure $P_{X_{[k]}}P_{Y_k|X_{[k]}}$, by (6.85) and the parameter choice (6.62), we write

$$\begin{aligned}
&\binom{M-k}{k}\mathbb{P}[\imath_k(\overline{X}_{[k]}^{n_k}; Y_k^{n_k}) > \log\gamma_k] \\
&\leq \left(\frac{e}{k}(M-k)\right)^k \mathbb{E}\left[\exp\{-\imath_k(X_{[k]}^{n_k}; Y_k^{n_k})\}\ 1\{\imath_k(X_{[k]}^{n_k}; Y_k^{n_k}) > \log\gamma_k\}\right] \\
&\leq \frac{D_k}{n_k},
\end{aligned} \tag{6.91}$$

where

$$D_k \triangleq 2\left(\frac{\log 2}{\sqrt{2\pi V_k}} + 2B_k\right) \tag{6.92}$$

and $B_k$ is defined in (6.65). Inequality (6.92) follows from Lemma 2.5.1. Combining the bounds for the three cases in (6.89), (6.90), and (6.91), we conclude that (6.39f) contributes $O\left(\frac{1}{\sqrt{n_k}}\right)$ to the total error.

Finally, we set the constant $C_k$ in (6.64) to ensure

$$(6.39\text{b}) + (6.39\text{c}) + (6.39\text{d}) + (6.39\text{e}) + (6.39\text{f}) \leq \frac{C_k}{\sqrt{n_k}}. \tag{6.93}$$

The existence of such a constant is guaranteed by our analysis above demonstrating that the terms (6.39b)–(6.39f) do not contribute more than $O\left(\frac{1}{\sqrt{n_k}}\right)$ to the total.[8]

Due to (6.69) and (6.93), the total probability of making an error at time $n_k$ is bounded by $\epsilon_k$, and the proof of Theorem 6.3.1 is complete.

### 6.4.4 Discussion of the Main Result

#### Refining the Third-Order Term Using a Maximum Likelihood Decoder

For a RAC that satisfies the conditions in Theorem 6.3.1 and the conditional variance condition

$$\mathbb{E}\left[\mathrm{Var}\left[\imath_k(X_{[k]};Y_k)|Y_k\right]\right] > 0 \quad \forall s \in [k], \tag{6.94}$$

we can improve the achievable third-order performance in (6.19) from $-\frac{1}{2}\log n_k$ to $+\frac{1}{2}\log n_k$. Prior work showing the achievability of the $+\frac{1}{2}\log n$ third-order term includes [2, Th. 53] for point-to-point channels satisfying (6.94) with $k = 1$, [44, Th. 1] for the Gaussian point-to-point channel, [113, Th. 7], [114, Th. 14] for discrete memoryless MACs satisfying (6.94). We will see in Chapter 7 that it can also be achieved for the Gaussian MAC and RAC. We can achieve the result here by replacing the threshold rule in (6.49) with a combination of a hypothesis test and a maximum likelihood decoder, giving

$$\mathsf{g}_k(U, y^{n_k}) = \begin{cases} \arg\max\limits_{w_{[k]}} \imath_k(\mathsf{f}(w_{[k]})^{n_k}; y^{n_k}) & \text{if } h_k(y^{n_k}) \le \gamma_k \\ \mathsf{e} & \text{otherwise,} \end{cases} \tag{6.95}$$

where the maximum is over the ordered message vectors $w_{[k]}$, and $h_k(\cdot)$ is a suitable test function that allows us to distinguish $P_{Y_k}$ from any $P_{Y_t}$ with $t \neq k$. As in prior work, the analysis applies the random coding union bound from [5, Th. 16]. As discussed in Section 6.5, suitable test functions $h_k(\cdot)$ can be found provided that $P_{Y_k} \neq P_{Y_t}$ for all $t \neq k$. For instance, in Chapter 7, below, we use $h_k(y^{n_k}) = \left|\frac{1}{n_k}\left\|y^{n_k}\right\|_2^2 - (1 + kP)\right|$ for the Gaussian RAC, where $P$ is the maximal power constraint. The result does not apply to channels such as the adder-erasure RAC (6.15), which does not satisfy the condition in (6.94).

[8] Our bounds on (6.39b)–(6.39f) technically depend on $\gamma_k$ and therefore on $C_k$. However, it is easy to see that their dependence on $C_k$ is weak, and for large enough $n_k$, it can be eliminated entirely. Thus the choice of $C_k$ satisfying (6.93) is possible.

### Choosing the Input Distribution $P_X$

Although there are RACs for which a single input distribution $P_X$ achieves the capacity for all $k$-MACs, $k \in [K]$, (e.g., the adder-erasure channel), the permutation-invariance (6.2) and reducibility (6.3) assumptions do not imply that such a distribution exists for all RACs. In the following, we discuss how to choose the input distribution when the optimal input distribution varies with $k$.

Given a permutation-invariant (6.2) and reducible (6.3) RAC, $M$, $\boldsymbol{\epsilon} = (\epsilon_0, \ldots, \epsilon_K)$, and any $P_X$ such that (6.8)–(6.13) are satisfied for the given RAC under input distribution $P_X$, let

$$\mathcal{R}(M, \boldsymbol{\epsilon}, P_X) = \{(R_0, \ldots, R_K) \colon \text{(6.19) and (6.20) hold}\} \tag{6.96}$$

denote the achievable rate region under input distribution $P_X$. Here

$$R_k = \frac{\log M}{n_k} \text{ for all } k \in \{0, \ldots, K\}. \tag{6.97}$$

Let

$$\mathcal{R}(M, \boldsymbol{\epsilon}) = \bigcup_{P_X \colon \text{(6.8)–(6.13) hold}} \mathcal{R}(M, \boldsymbol{\epsilon}, P_X) \tag{6.98}$$

denote the achievable rate region over all i.i.d. input distributions. A point in this set is called *dominant* if no other points in the set are element-wise greater than or equal to that point. To optimize the achievable rate vector over the allowed input distributions, we must choose a distribution $P_{X^*}$ that achieves a dominant point for the set $\mathcal{R}(M, \boldsymbol{\epsilon})$.

Note that for the dominant points of $\mathcal{R}(M, \boldsymbol{\epsilon})$ corresponding to different values of $P_{X^*}$, there is an $O(1)$ difference between the left and right sides of the inequalities in (6.19). If the achievable rate region $\mathcal{R}(M, \boldsymbol{\epsilon})$ is not convex, it can be improved to its convex hull using time sharing. For the modifications to the coding strategy that enable us to incorporate time sharing, see [19], [21], [22].

To illustrate what happens when different $P_{X^*}$ values achieve different dominant points of $\mathcal{R}(M, \boldsymbol{\epsilon})$, we consider the following example.

**Example 6.4.1.** Consider a RAC with $K = 2$, $\mathcal{X} = \mathcal{Y}_2 = \{0, 1\}$, and transition probability matrix $P_{Y_2|X_1,X_2}$

| $Y_2 \setminus X_1X_2$ | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| 0 | $1-b$ | $b$ | $b$ | $1-a$ |
| 1 | $b$ | $1-b$ | $1-b$ | $a$ |

(6.99)

where $a, b \in [0, 1]$. This RAC is permutation-invariant since the “01" and the “10" columns are identical. When $k = 1$, the channel reduces to the binary symmetric channel with crossover probability $b$. Fig. 6.3 illustrates the set of achievable rate vectors $\mathcal{R}(M, \boldsymbol{\epsilon})$ (neglecting the $O(1)$ term in (6.19)) with $\log M = 1000$ and $\boldsymbol{\epsilon} = 10^{-3}\mathbf{1}$ for two choices of parameters in the channel in (6.99). In Fig. 6.3a, $a = 0.7, b = 0.11$, and in Fig. 6.3b, $a = b = 0.11$; for each, the finite blocklength and capacity boundaries are demonstrated. In Fig. 6.3a, the dominant points are highlighted. The input distribution $P_{X^*} = (0.65, 0.35)$ (i.e., the Bernoulli(0.35) distribution) achieves the dominant point $(R_1, R_2) = (0.400, 0.204)$; the corresponding region $\mathcal{R}(M, \boldsymbol{\epsilon}, P_{X^*})$ is shown as the region bounded by the dashed lines. In Fig. 6.3b, the only dominant point $(0.437, 0.227)$ is achieved by the input distribution $P_{X^*} = (0.5, 0.5)$ (i.e., the Bernoulli(0.5) distribution.) Therefore, for the channel in Fig. 6.3b, the achievable rate region $\mathcal{R}(M, \boldsymbol{\epsilon})$ coincides with $\mathcal{R}(M, \boldsymbol{\epsilon}, P_{X^*})$, and we must choose $P_{X^*}$ as our input distribution. For this channel, $P_{X^*} = (0.5, 0.5)$ simultaneously maximizes the mutual informations $I_1$ and $I_2$, and the maxima are $I_1 = I_2 = 0.5$.

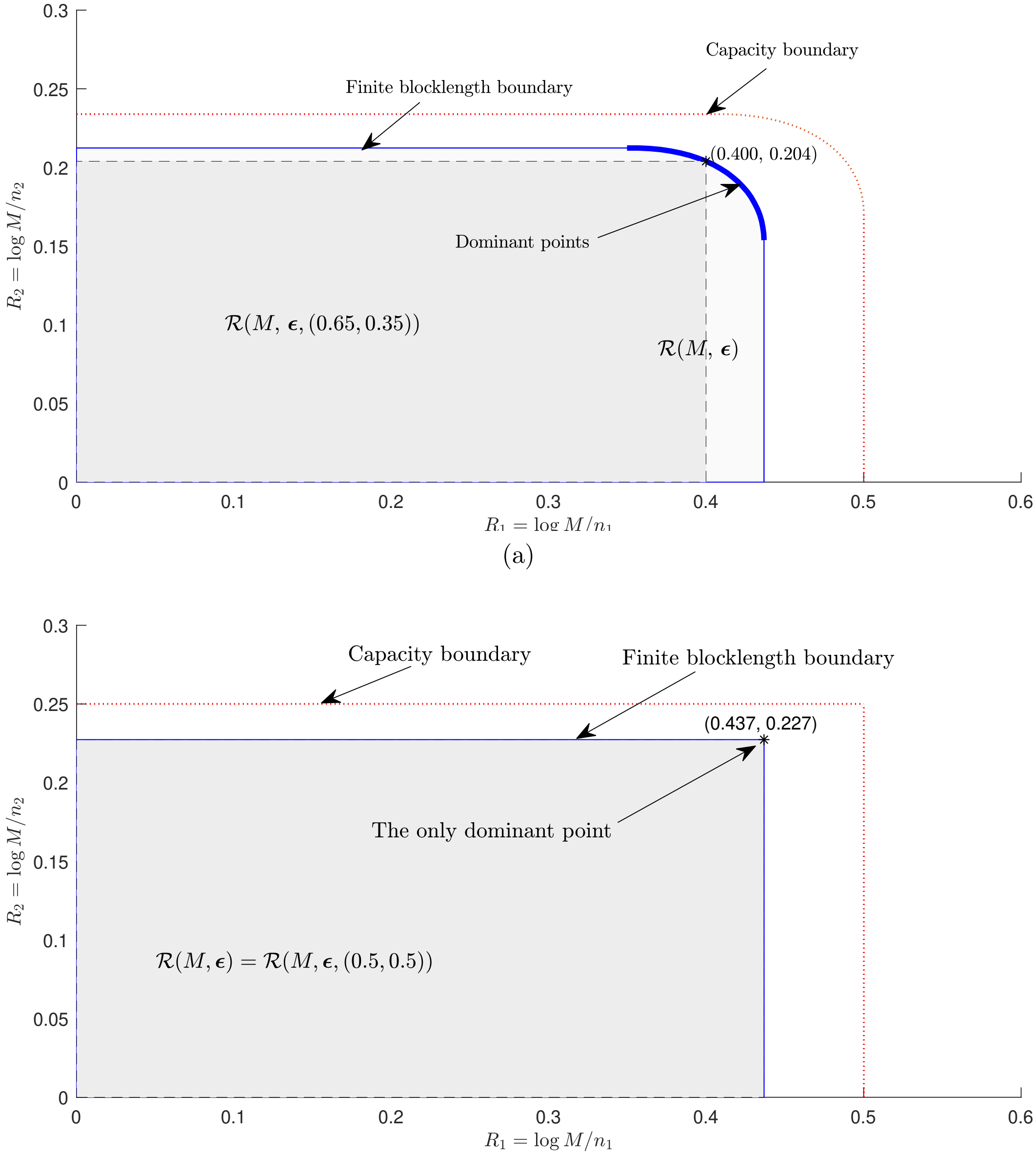
### Discussion of the Converse

Even for MACs with only 2 transmitters, the capacity region for the MAC remains incompletely understood. A brief summary of related results follows. For any blocklength $n$ and average error probability $\epsilon \in (0, 1)$, let

$$\mathcal{R}(n, \epsilon) = \left\{ \left( \frac{\log M_1}{n}, \frac{\log M_2}{n} \right) : \exists \text{ an } (n, M_1, M_2, \epsilon) \text{ code} \right\} \tag{6.100}$$

denote the set of achievable rate pairs, where $M_i$ is the message size for transmitter $i \in \{1, 2\}$. The capacity region of the MAC [115], [116] is

$$\mathcal{C} = \bigcup_{P_Q P_{X_1|Q} P_{X_2|Q}} \{(R_1, R_2):$$



(a)

(b)

Figure 6.3: The achievable rate region from Theorem 6.3.1 (excluding the $O(1)$ term) applied to the channel in (6.99) with $\log M = 1000$ and $\epsilon_k = 10^{-3}$ for $k \in [2]$. The results are shown for (a) $a = 0.7$ and $b = 0.11$ and blocklengths $(n_1, n_2) = (2501, 4904)$, and (b) for $a = b = 0.11$ and blocklengths $(n_1, n_2) = (2290, 4399)$.

$$\begin{aligned} R_1 &\leq I_2(X_1; Y_2|X_2, Q) \\ R_2 &\leq I_2(X_2; Y_2|X_1, Q) \\ R_1 + R_2 &\leq I_2(X_1, X_2; Y_2|Q)\}, \end{aligned} \tag{6.101}$$

where $Q$ is the time sharing random variable. In [117], Dueck uses the blowing-up lemma to derive the first strong converse for discrete memoryless MACs. In [118], for discrete memoryless MACs, Ahlswede uses a wringing technique to show

$$\mathcal{R}(n, \epsilon) \subseteq \mathcal{C} + O\left(\frac{\log n}{\sqrt{n}}\right)\mathbf{1}, \tag{6.102}$$

which improves Dueck's result. The coefficients of the term $O\left(\frac{\log n}{\sqrt{n}}\right)\mathbf{1}$ in (6.102) are bounded by a multiple of the product of input and output alphabet sizes $|\mathcal{X}_1||\mathcal{X}_2||\mathcal{Y}_2|$. In [119, Th. 1], Fong and Tan improve Ahlswede's second-order term $O\left(\frac{\log n}{\sqrt{n}}\right)\mathbf{1}$ to $O\left(\sqrt{\frac{\log n}{n}}\right)\mathbf{1}$ for the Gaussian MAC. They derive this result by applying Ahlswede's wringing technique [118] to quantized channel inputs. In [23], Kosut further improves the second-order term to $O\left(\frac{1}{\sqrt{n}}\right)\mathbf{1}$. The second-order term in [23, Th. 7] has the same order and, for some channels, the same sign as the best-known second-order achievable term in [22]. Kosut's result applies to all discrete memoryless MACs and to the Gaussian MAC. To prove this converse, Kosut introduces a new measure of dependence between two random variables called “wringing dependence." A key aspect of the approach is to restrict the channel inputs so that the wringing dependence between them is small. Note that Kosut's converse result in [23] applies to our RAC model since the code does not allow the encoding function to depend on the feedback. Therefore, [23] establishes that the scaling of the second-order term, $O(\sqrt{n})$, is tight.[9]

In [120], Moulin proposes a new converse technique for maximum-error capacity. His approach relies on strong large deviations for binary hypothesis tests and leads to a second-order term as in (6.19) when no time sharing is needed. Since the capacity regions for the maximum and average error probability can differ [121], Moulin's result does not give a converse for the average-error capacity. Whether it is possible to derive a converse for the average-error capacity with a second-order term matching the ones in [19]–[22], [24] remains an open problem.

[9] One should still extend the result from $K = 2$ to any $K$ transmitters.

In the sparse recovery literature, where achievability proofs typically consider the expected error probability evaluated under i.i.d. codebook design (see, e.g., [11], [102]–[105]), converses derive lower bounds on the expected error probability *assuming i.i.d. code design.* Although a lower bound on the expected error probability for our problem could be derived using tools from [11], such a bound would yield a bound for the best i.i.d. random code rather than a bound for all possible codes.

### A RAC Code That Decodes Transmitter Identity

While the use of identical encoding at all transmitters has a number of practical advantages, the techniques employed in this work are not limited to that case.

We next briefly explore the use of distinct encoders at each transmitter of a RAC. Under permutation-invariance (6.2) and identical encoding, the decoder cannot distinguish which transmitter sent each of the decoded messages. Maintaining permutation-invariance but replacing identical encoders with a different instance of the same random codebook for each encoder, we get a code that achieves the same first- and second-order terms as in Theorem 6.3.1, with a decoder that can also associate the corresponding transmitter identity to each decoded message. The following definition formalizes the resulting RAC codes.

**Definition 6.4.1.** *An* $(M, \{(n_k, \epsilon_k)\}_{k=0}^{K})$ *identity-preserving code comprises a collection of encoding functions*

$$\mathsf{f}_k \colon \mathcal{U} \times [M] \to \mathcal{X}^{n_K}, \quad k = 1, \dots, K, \tag{6.103}$$

*and a collection of decoding functions*

$$\mathsf{g}_k \colon \mathcal{U} \times \mathcal{Y}_k^{n_k} \to \left\{ [M]^k \times \binom{[K]}{k} \right\} \cup \{\mathsf{e}\}, \ k = 0, 1, \dots, K, \tag{6.104}$$

*where erasure symbol* $\mathsf{e}$ *is the decoder's output when the decoder is not ready to decode. At the start of each epoch, a random variable* $U \in \mathcal{U}$*, with* $U \sim P_U$*, is generated independently of the transmitter activity, and revealed to the transmitters and the receiver for use in initializing the encoders and the decoder. If the set of active transmitters* $\mathcal{A} \subseteq [K]$ *satisfies* $|\mathcal{A}| = k > 0$*, i.e.,* $k$ *transmitters are active, then the messages of* $\mathcal{A}$ *and their corresponding transmitter* *identities are decoded correctly at time* $n_k$*, with probability at least* $1-\epsilon_k$*, i.e.,*

$$\frac{1}{M^k}\sum_{w_{\mathcal{A}}\in[M]^k}\mathbb{P}\Bigg[\{\mathsf{g}_k(U,Y_k^{n_k})\neq(w_{\mathcal{A}},\mathcal{A})\}\bigcup \left\{\bigcup_{t=0}^{k-1}\{\mathsf{g}_t(U,Y_k^{n_t})\neq\mathsf{e}\}\right\}\Bigg| W_{\mathcal{A}}=w_{\mathcal{A}}\Bigg]\leq\epsilon_k, \tag{6.105}$$

*where* $W_{\mathcal{A}}$ *are the independent and equiprobable messages of the transmitters in* $\mathcal{A}$*, and the given probability is calculated using the conditional distribution* $P_{Y_k^{n_k}|X_{\mathcal{A}}^{n_k}} = P_{Y_k|X_{\mathcal{A}}}^{n_k}$ *where* $X_i^{n_k} = \mathsf{f}_i(U,W_i)^{n_k}$*,* $i\in\mathcal{A}$*. If* $\mathcal{A}=\emptyset$*, then the probability that at time* $n_0$ *the receiver decodes to the unique message in set* $[M]^0=\{0\}$ *is no smaller than* $1-\epsilon_0$*. That is,*

$$\mathbb{P}\left[\mathsf{g}_0(U,Y_0^{n_0})\neq 0|W_{[0]}=0\right]\leq\epsilon_0. \tag{6.106}$$

If we continue to assume permutation-invariance (6.2) and to employ the same input distribution $P_X$ at all encoders, then the channel output statistics again depend on the dimension of the channel input but not on the identity of the active transmitters. In this case, we can apply the proof from the identical-encoding single-threshold-decoding argument in Section 6.4.1 to derive an achievability result for the general case.[10] In particular, consider a code with $KM$ (rather than $M$) messages. Replacing $M$ by $KM$ in Theorem 6.3.1 implies that our RAC code with identical encoders gives a penalty of $-k\log K$ on the right-hand side of the rate bound (6.19). Suppose that we use this identical-encoding code to design a general code in which codewords indexed from $(t-1)M+1$ to $tM$ are used exclusively by transmitter $t$ for $t=1,\dots,K$. Since each message belongs to a single transmitter, the list of decoded messages reveals the identities of the active transmitters. Under this allocation of codewords, the repetition error $\mathbb{P}_{\text{rep}}$ in (6.51) disappears since transmitters send messages from distinct sets. The error probability from decoding the wrong codeword values decreases since there are fewer legitimate codeword combinations to consider. Therefore, in the case where $K$ is a finite constant and the receiver decodes both messages and transmitter identities, the first three terms in (6.19) are preserved, and the penalty $-k\log K$ only affects the constant term $O(1)$ in (6.19).

When applied to a scenario with $M=1$ and identity decoding, the bound in Theorem 6.3.2, modified as described in the preceding paragraph, extends the

[10] This simple argument was suggested by Dr. Jonathan Scarlett.

non-asymptotic achievability bound in the group testing problem [11, Th. 4] to the scenario where an unknown number $k$ out of a total of $K$ items are defective. In the scenario considered in [11], the number of defective items $k$ is known, and our MAC bound (6.43) with $K$ replaced by $k$, $M$ replaced by $KM = K$, and the term $\frac{K(K-1)}{2M}$ removed applies. The resulting bound is similar to [11, Th. 4]. The difference is that the bound in (6.43) uses a single information density threshold rule, while [11, Th. 4] uses $2^k - 1$ simultaneous information density threshold rules.

### Per-user Probability of Error

We extend the definition of the PUPE from [90, Def. 1] to the RAC with $k \in [K]$ active transmitters as

$$e_k \triangleq \frac{1}{M^k} \sum_{w_{[k]} \in [M]^k} \sum_{i=1}^{k} \frac{1}{k} \mathbb{P}\left[w_i \notin \mathsf{g}_T(U, Y_k^{n_T}) | W_{[k]} = w_{[k]}\right], \tag{6.107}$$

where $Y_k^{n_T}$ is the received output at time $n_T$, and

$$T \triangleq \min\{t \in \{0\} \cup [K] \colon \mathsf{g}_t(U, Y_k^{n_t}) \neq \mathsf{e}\} \tag{6.108}$$

is the random variable describing the decoder's estimate of the number of active transmitters.[11] We set $T = K$ if $\mathsf{g}_t(U, Y_k^{n_t}) = \mathsf{e}$ for all $t \in \{0\} \cup [K]$. For $k = 0$, we define $e_0 \triangleq \mathbb{P}\left[\mathsf{g}_0(U, Y_0^{n_0}) \neq 0 | W_{[0]} = 0\right]$ as in (6.7).

For a RAC with a total of $K$ transmitters and a MAC with $K$ transmitters, the following corollary to Theorem 6.3.2 gives non-asymptotic achievability bounds under the PUPE criterion (6.107).

**Corollary 6.4.1.** *Fix constants $\gamma_0$, $\lambda_{s,t}^k \geq 0$, and $\gamma_t > 0$ for all $1 \leq s \leq t \leq k$. For any $k$ and $n$, let $(X_{[k]}^n, \overline{X}_{[k]}^n, Y_k^n)$ be a random sequence drawn i.i.d. $\sim P_{X_{[k]}\overline{X}_{[k]}Y_k}(x_{[k]}, \overline{x}_{[k]}, y_k) = \left(\prod_{i=1}^k P_X(x_i) P_X(\overline{x}_i)\right) P_{Y_k|X_{[k]}}(y_k|x_{[k]})$.*

1. *For any RAC $\left\{\left(\mathcal{X}^k, P_{Y_k|X_{[k]}}(y_k|x_{[k]}), \mathcal{Y}_k\right)\right\}_{k=0}^{K}$ satisfying (6.2) and (6.3), any $K \leq \infty$, and any fixed input distribution $P_X$, there exists an*

[11] Note that the joint error probability in (6.6) can likewise be written as

$$\frac{1}{M^k} \sum_{w_{[k]} \in [M]^k} \mathbb{P}\left[\mathsf{g}_T(U, Y_k^{n_T}) \overset{\pi}{\neq} w_{[k]} \middle| W_{[k]} = w_{[k]}\right].$$

*$(M, \{(n_k, e_k)\}_{k=0}^{K})$ RAC code under the PUPE criterion (6.107) such that*

$$e_0 \leq \mathbb{P}\left[h(Y_0^{n_0}) > \gamma_0\right], \tag{6.109}$$

*and for all $k \geq 1$,*

$$\begin{aligned}
e_k \leq\ & \mathbb{P}[\imath_k(X_{[k]}^{n_k}; Y_k^{n_k}) \leq \log \gamma_k] && (6.110)\\
& + \mathbb{P}\left[h(Y_k^{n_0}) \leq \gamma_0\right] + \frac{k(k-1)}{2M} && (6.111)\\
& + \sum_{t=1}^{k-1} \binom{k-1}{t} \mathbb{P}[\imath_t(X_{[t]}^{n_t}; Y_k^{n_t}) > \log \gamma_t] && (6.112)\\
& + \sum_{t=1}^{k} \sum_{s=1}^{t-1} \binom{k-1}{t-s} \mathbb{P}\left[\imath_t(X_{[s+1:t]}^{n_t}; Y_k^{n_t}) > n_t \mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] + \lambda_{s,t}^{k}\right] && \\
& && (6.113)\\
& + \sum_{t=1}^{k} \sum_{s=1}^{t} \binom{k-1}{t-s} \binom{M-k}{s} && \\
& \quad \mathbb{P}\left[\imath_t(\overline{X}_{[s]}^{n_t}; Y_k^{n_t} | X_{[s+1:t]}^{n_t}) > \log \gamma_t - n_t \mathbb{E}[\imath_t(X_{[s+1:t]}; Y_k)] - \lambda_{s,t}^{k}\right]. && \\
& && (6.114)
\end{aligned}$$

2. *For a MAC with $K$ transmitters satisfying (6.2), there exists a MAC code for $M$ messages and decoding blocklength $n_K$ such that*

$$\begin{aligned}
e_K \leq\ & \mathbb{P}[\imath_K(X_{[K]}^{n_K}; Y_K^{n_K}) \leq \log \gamma_K] + \frac{K(K-1)}{2M}\\
& + \sum_{s=1}^{K-1} \binom{K-1}{K-s}\\
& \quad \mathbb{P}\left[\imath_K(X_{[s+1:K]}^{n_K}; Y_K^{n_K}) > n_K \mathbb{E}[\imath_K(X_{[s+1:K]}; Y_K)] + \lambda_{s,K}^{K}\right]\\
& + \sum_{s=1}^{K} \binom{K-1}{K-s} \binom{M-K}{s}\\
& \quad \mathbb{P}\left[\imath_K(\overline{X}_{[s]}^{n_K}; Y_K^{n_K} | X_{[s+1:K]}^{n_K}) > \log \gamma_K - n_K \mathbb{E}[\imath_K(X_{[s+1:K]}; Y_K)] - \lambda_{s,K}^{K}\right].
\end{aligned} \tag{6.115}$$

*Proof:* Notice that in (6.110), the only modification from Theorem 6.3.2 is the replacement of the coefficients $\binom{k}{t}$ in (6.39d) and $\binom{k}{t-s}$ in (6.39e)–(6.39f) by the coefficients $\binom{k-1}{t}$ and $\binom{k-1}{t-s}$, respectively. To see how Corollary 6.4.1 is derived from Theorem 6.3.2, observe that the PUPE (6.107) measures the fraction of transmitted messages missing from the list of decoded messages. Therefore, to bound the PUPE for the RAC, we can multiply the error probability bounds in (6.39) that correspond to the case where $t$ out of $k$ messages are decoded by $\frac{k-(t-s)}{k}$, where $s$ is the number of messages decoded incorrectly.

Similarly, under the PUPE, the coefficient $\binom{K}{K-s}$ in the $K$-transmitter MAC bound (6.43) is replaced by $\binom{K-1}{K-s}$ in (6.115) since we can multiply the error probability bounds in (6.44)–(6.45), corresponding to the case where $s$ out of $K$ messages are decoded incorrectly, by $\frac{s}{K}$. ■

From the proof of Theorem 6.3.1, the error probability bounds in (6.112)–(6.114) behave as $O\left(\frac{1}{\sqrt{n_k}}\right)$. This implies that under the PUPE criterion (6.107), our encoding and decoding scheme described in Section 6.4.1 achieves the same first three order terms as Theorem 6.3.1. Only the constant $O(1)$ term in (6.19) is affected by the change from the joint error probability to the PUPE.

The PUPE criterion becomes critical in applications of the Gaussian RAC with $K \to \infty$, where the energy per bit $(\frac{nP}{2\log_2 M})$ and the number of bits sent by each transmitter $(\log_2 M)$ are fixed as the blocklength $n$ grows, and all $K$ transmitters are active. In [90], Polyanskiy shows that in this regime, the joint error probability goes to 1 as $K \to \infty$. As we saw in (6.115), the PUPE introduces scaling factors $\frac{s}{K}$ in front of the error terms corresponding to $s$ out of $K$ messages decoded incorrectly, for $s = 1, \ldots, K$. In the regime $K \to \infty$, the number of these terms is infinite, and the PUPE can be strictly less than 1 even as the joint error probability approaches 1. In [90], Polyanskiy shows that the PUPE behaves nontrivially in this regime.

## 6.5 Tests for No Active Transmitters

In this section, we give an analysis of the error probabilities of the composite binary hypothesis test that we use to decide between $H_0$: “no active transmitters," and $H_1$: “$k \in [K]$ active transmitters;" that is

$$\begin{aligned} H_0 &: Y^{n_0} \sim P_{Y_0}^{n_0} \\ H_1 &: Y^{n_0} \sim P_{Y_k}^{n_0} \text{ for some } 1 \leq k \leq K. \end{aligned} \tag{6.116}$$

In the context of Theorem 6.3.2, the maximal number of transmitters, $K$, can be infinite. In that case, enumerating all alternative possibilities as in (6.116) becomes infeasible, and a universal (goodness-of-fit) test

$$H_0 \colon Y^n \sim P_{Y_0}^n$$

$$H_1 \colon Y^n \not\sim P_{Y_0}^n \tag{6.117}$$

is appropriate.

Following [122], a *test statistic* $h_n \colon \mathcal{Y}^n \mapsto \mathbb{R}$ is a function that maps the observed sequence $y^n$ to a real number used to measure the correspondence between that sequence and the null hypothesis. A (randomized) test corresponding to the test statistic $h_n$ is a binary random variable that depends only on $h_n(Y^n)$. The test is deterministic if it outputs $H_0$ if $h_n(y^n) \leq \gamma_0$ for some constant $\gamma_0$, and $H_1$ otherwise.

Type-I and type-II errors corresponding to a deterministic test with the statistic $h_n$ are defined as

$$\alpha(h_n) \triangleq P_{Y_0}[h_n(Y^n) > \gamma_0] \tag{6.118}$$

$$\beta(h_n) \triangleq Q[h_n(Y^n) \leq \gamma_0], \tag{6.119}$$

where $Q$ is the unknown alternative distribution of $Y$, and $\gamma_0$ is a constant determined by the desired error criterion. Throughout the following discussion and in our application of these results in Lemma 6.4.1, we employ deterministic tests. For these deterministic tests, we choose $\gamma_0$ to ensure that we meet the zero-transmitter error bound $\alpha(h_n) \leq \epsilon_0$, and then we show that $\beta(h_n)$ decays exponentially with $n$ for each $Q$ in $\{P_{Y_1}, \dots, P_{Y_K}\}$ to ensure (6.20) in Theorem 6.3.1.

In Sections A and B, below, we consider Hoeffding's test and the Kolmogorov-Smirnov test as possible hypothesis tests for recognizing the zero-transmitter scenario. Both tests are universal in the sense that the test statistic does not vary with the alternative output distributions $P_{Y_1}, \dots, P_{Y_K}$. They both give an exponentially decaying type-II error for a fixed type-I error $\epsilon_0 \in (0, 1)$. The disadvantage of Hoeffding's test is that its traditional form requires the channel output alphabet to be finite for every $k$ (as in the adder-erasure RAC in (6.15)); the advantage of Hoeffding's test is that it achieves the same exponent as the Neyman-Pearson Lemma, which is optimal for a given collection of output distributions $P_{Y_1}, \dots, P_{Y_K}$, but is not universal, meaning that a different test statistic is necessary for each collection $\{P_{Y_k} \colon k \in [K]\}$. In contrast to Hoeffding's test, the Kolmogorov-Smirnov test does not require $\mathcal{Y}$ to be finite; however, when applied to a setting with finite $\mathcal{Y}$, it achieves a type-II error exponent that is inferior to that achieved by Hoeffding's test. In Section 6.5.3, we compare the performances of these universal test statistics to that of the log-likelihood ratio (LLR) threshold test, which is third-order optimal in terms of the type-II error exponent for composite hypothesis testing [123] and relies explicitly on alternative output distributions $P_{Y_1}, \dots, P_{Y_K}$.

### 6.5.1 Hoeffding's Test

Denote the empirical distribution of an observed sequence $y_1, \dots, y_n$ by

$$\hat{P}_{y^n}(a) \triangleq \frac{1}{n} \sum_{i=1}^{n} 1\{y_i = a\} \quad \forall\, a \in \mathcal{Y}. \tag{6.120}$$

Hoeffding's test is based on the relative entropy, denoted by $D(\cdot\|\cdot)$, between $\hat{P}_{y^n}$ and $P_{Y_0}$, giving the test statistic

$$h_n^H(y^n) = D(\hat{P}_{y^n} \| P_{Y_0}). \tag{6.121}$$

Note that if $P_{Y_0}$ is a continuous distribution, $h_n^H(y^n) = +\infty$.

**Theorem 6.5.1** (Hoeffding's test[124])**.** *Let $\mathcal{Y}$ be a finite set, and let $Q$ be an unknown alternative distribution for $Y_0$. If $P_{Y_0}$ is absolutely continuous with respect to $Q$, and $P_{Y_0} \neq Q$, then the type-I and type-II errors of Hoeffding's test satisfy*

$$\alpha(h_n^H) \leq \exp\{-n\gamma_0 + O(\log n)\} \tag{6.122}$$

$$\beta(h_n^H) \leq \exp\left\{-n \inf_{P: D(P\|P_{Y_0}) < \gamma_0} D(P\|Q) + O(\log n)\right\}. \tag{6.123}$$

In [124], a more restrictive assumption ($P_{Y_0}(y) > 0$ and $Q(y) > 0$ for all $y \in \mathcal{Y}$) is used. Absolute continuity is sufficient according to the proofs given in [122] and [125, Th. 2.3], which both rely on Sanov's theorem. The error exponents of Hoeffding's test coincide with the exponents of the optimal (Neyman-Pearson Lemma) binary hypothesis test. Therefore, Hoeffding's test is asymptotically universally most powerful.

Setting $\gamma_0 = \frac{|\mathcal{Y}| \log n}{n}$ achieves type-I error $\epsilon_0 \to 0$ as $n \to \infty$; therefore, the type-I error condition is satisfied for any $\epsilon_0 > 0$ and sufficiently large $n$. Under this choice, type-II error $\exp\{-nD(P_{Y_0}\|Q) + o(n)\}$ is achieved (see [125, Th. 2.3]). Therefore, in (6.72), the maximum type-II error decays with exponent

$$C' = \inf_{k \in [K]} D(P_{Y_0} \| P_{Y_k}) \tag{6.124}$$

$$\geq 2 \inf_{k\in[K]} \left\{ \left( \sup_{x\in\mathbb{R}} |F_k(x) - F_0(x)| \right)^2 + \frac{4}{9} \left( \sup_{x\in\mathbb{R}} |F_k(x) - F_0(x)| \right)^4 \right\} \tag{6.125}$$

$$\geq 2\delta_0^2 + \frac{4}{9}\delta_0^4. \tag{6.126}$$

The inequality in (6.125) is due to [126, eq. (5)-(6)] and Pinsker's inequality [127]. The inequality in (6.126) follows from (6.10).

In [122], Zeitouni and Gutman extend Hoeffding's test to continuous distributions. Their test, which also uses the empirical distribution, employs "δ-smoothing" of the decision regions obtained by a relative entropy comparison. The Zeitouni-Gutman test is optimal under a slightly weaker optimality criterion than the standard first-order type-II error exponent criterion. Using [122, Th. 2], it can be shown that the Zeitouni-Gutman test also yields the desired exponentially decaying maximum type-II error.

### 6.5.2 Kolmogorov-Smirnov Test

The Kolmogorov-Smirnov test **smirnov1944**, [128] relies on the empirical cdf

$$\hat{F}^{(n)}(x|y^n) \triangleq \frac{1}{n}\sum_{i=1}^{n} 1\{y_i \leq x\} \quad \forall x \in \mathbb{R} \tag{6.127}$$

of the observed sequence $y_1, \ldots, y_n \in \mathbb{R}$. The Kolmogorov-Smirnov test uses a deterministic test

$$h_n^{KS}(y^n) = \sup_{x\in\mathbb{R}} |\hat{F}^{(n)}(x|y^n) - F_0(x)| \tag{6.128}$$

to test whether the observed sequence $y^n$ is well-explained by $P_{Y_0}$ with the cdf $F_0$.

The following theorem bounds the probability that the Kolmogorov-Smirnov statistic exceeds a threshold $\gamma_0$.

**Theorem 6.5.2** (Dvoretzky-Kiefer-Wolfowitz [129], [130])**.** *Let $Y_1, \ldots, Y_n$ be drawn i.i.d. according to an arbitrary distribution $P_{Y_0}$ with the cdf $F_0$ on $\mathbb{R}$. For any $n \in \mathbb{N}$ and $\gamma_0 > 0$, it holds that*

$$\alpha(h_n^{KS}) \leq 2\exp\{-2n\gamma_0^2\}. \tag{6.129}$$

In [129], Dvoretzky *et al.* prove Theorem 6.5.2 with an unspecified multiplicative constant $C$ in front of the exponential on the right side of (6.129). In [130], Massart establishes that $C = 2$.

In our operational regime of interest, we set the type-I error to a given constant $\epsilon_0$, which by Theorem 6.5.2 corresponds to setting the threshold $\gamma_0$ to

$$\gamma_0 = \sqrt{\frac{\log \frac{2}{\epsilon_0}}{2n}} = O\left(\frac{1}{\sqrt{n}}\right). \tag{6.130}$$

We next bound the type-II errors for every $k \in [K]$. For each $k \in \{0, \ldots, K\}$, let $F_k$ denote the cdf of $P_{Y_k}$. The type-II error when $k \geq 1$ transmitters are active is bounded as

$$\begin{aligned}
\beta_k(h_n^{KS}) &= \mathbb{P}\left[\sup_{x\in\mathbb{R}} |\hat{F}^{(n)}(x|Y_k^n) - F_0(x)| \leq \gamma_0\right] && (6.131)\\
&\leq \mathbb{P}\left[\sup_{x\in\mathbb{R}} \left(|F_k(x) - F_0(x)| - |\hat{F}^{(n)}(x|Y_k^n) - F_k(x)|\right) \leq \gamma_0\right] && (6.132)\\
&\leq \mathbb{P}\left[\sup_{x\in\mathbb{R}} |\hat{F}^{(n)}(x|Y_k^n) - F_k(x)| \geq \sup_{x\in\mathbb{R}} |F_k(x) - F_0(x)| - \gamma_0\right] && (6.133)\\
&\leq 2\exp\left\{-2n\left(\sup_{x\in\mathbb{R}} |F_k(x) - F_0(x)|\right)^2 + O(\sqrt{n})\right\}, && (6.134)
\end{aligned}$$

where (6.132) follows from triangle inequality $|x+y| \geq |x| - |y|$, and (6.134) follows from Theorem 6.5.2 and (6.130). Applying (6.10) to (6.134), we conclude that the maximum type-II error in (6.72) decays exponentially with $n$, with exponent

$$\begin{aligned}
C' &= 2 \inf_{k\in[K]} \left(\sup_{x\in\mathbb{R}} |F_k(x) - F_0(x)|\right)^2 && (6.135)\\
&\geq 2\delta_0^2. && (6.136)
\end{aligned}$$

Comparing (6.135) and (6.125), from (6.10), we see that the type-II error exponent achieved by the Kolmogorov-Smirnov test is always inferior to that achieved by Hoeffding's test.

### 6.5.3 The Optimal Composite Hypothesis Test

From (6.126) and (6.136), we know that there exists a positive constant $c_0$ such that

$$n_0 \geq c_0 \log n_1 + o(\log n_1) \tag{6.137}$$

suffices to meet the error requirements of the composite hypothesis test given in (6.70) and (6.71). Since the proposed tests are universal, Theorem 6.3.2 allows us to decode any message set of $k \leq K$ active transmitters without knowing the total number of transmitters, $K$. In this section, we find the smallest first three terms on the right side of (6.137) that we can achieve when $K$ is finite and we allow the composite hypothesis test to depend on the distributions $P_{Y_1}, \dots, P_{Y_K}$.

Let $\beta_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K)$ denote the minimax type-II error among the alternative distributions $P_{Y_1}, \dots, P_{Y_K}$ such that type-I error (under $P_{Y_0}$) does not exceed $\epsilon_0$; that is,

$$\beta_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K) \triangleq \min_{h_n : \alpha(h_n) \leq \epsilon_0} \max_{k \in [K]} \beta_k(h_n), \tag{6.138}$$

where the minimum is over all tests including deterministic and randomized tests.

The LLR test statistic $h_n^{\mathrm{LLR}} \colon \mathcal{Y}^n \mapsto \mathbb{R}^K$ is given by

$$h_n^{\mathrm{LLR}}(y^n) = \sum_{i=1}^n h_1^{\mathrm{LLR}}(y_i), \tag{6.139}$$

where

$$h_1^{\mathrm{LLR}}(y) \triangleq \begin{bmatrix} \log \frac{P_{Y_0}(y)}{P_{Y_1}(y)} \\ \log \frac{P_{Y_0}(y)}{P_{Y_2}(y)} \\ \vdots \\ \log \frac{P_{Y_0}(y)}{P_{Y_K}(y)} \end{bmatrix}. \tag{6.140}$$

Given a threshold vector $\boldsymbol{\tau} \in \mathbb{R}^K$, the corresponding LLR test outputs $H_0$ if $h_n^{\mathrm{LLR}}(y^n) \geq \boldsymbol{\tau}$, and $H_1$ otherwise.

The gap in the type-II error exponent ($C'$ in (6.72)) between the general optimal tests and the LLR tests with the optimal threshold vector $\boldsymbol{\tau}$ is $O\left(\frac{1}{n}\right)$ [123]; therefore, we only consider minimizing over the LLR tests in (6.138) for asymptotic optimality.

Denote by $\mathbf{D}$ and $\mathsf{V}$ the mean and covariance matrix of the random vector $h_1^{\mathrm{LLR}}(Y_0)$, respectively. Define

$$D_{\min} \triangleq \min_{k \in [K]} D(P_{Y_0} \| P_{Y_k}) \tag{6.141}$$

$$\mathcal{I}_{\min} \triangleq \{k \in [K] \colon D(P_{Y_0} \| P_{Y_k}) = D_{\min}\} \tag{6.142}$$

$$\mathsf{V}_{\min} \triangleq \mathrm{Cov}\left[\left(h_1^{\mathrm{LLR}}(Y_0)\right)_{\mathcal{I}_{\min}}\right] \in \mathbb{R}^{|\mathcal{I}_{\min}| \times |\mathcal{I}_{\min}|}. \tag{6.143}$$

The following theorem gives the asymptotics of the minimax type-II error defined in (6.138).

**Theorem 6.5.3.** *Assume that $P_{Y_0}$ is absolutely continuous with respect to $P_{Y_k}$, $0 < D(P_{Y_0} \| P_{Y_k}) < \infty$ for $k = 1, \ldots, K$, $\mathsf{V}$ is positive definite, and $T = \mathbb{E}[\|h_1^{\mathrm{LLR}}(Y_0) - \mathbf{D}\|_2^3] < \infty$. Then for any $\epsilon_0 \in (0, 1)$, the asymptotic minimax type-II error satisfies*

$$\beta_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K) = \exp\Big\{ - nD_{\min} + \sqrt{n}b \\ - \frac{1}{2}\log n + O(1)\Big\}, \tag{6.144}$$

*where $b$ is the solution to*

$$\mathbb{P}\left[\mathbf{Z} \le b\mathbf{1}\right] = 1 - \epsilon_0, \tag{6.145}$$

*for $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V}_{\min}) \in \mathbb{R}^{|\mathcal{I}_{\min}|}$. Moreover, the minimax error in (6.144) is achieved by a LLR test with some threshold vector $\boldsymbol{\tau}$.*

*Proof:* See Appendix E.5. ■

Rewriting (6.144), defining $b$ as given in (6.145), and using the condition in (6.70) with any fixed $E_k$, we see that a decision about whether any of the transmitters are active can be made at time

$$n_0 = \frac{1}{2D_{\min}}\log n_1 + \frac{b}{\sqrt{2D_{\min}^3}}\sqrt{\log n_1} - \frac{1}{2D_{\min}}\log\log n_1 + O(1) \tag{6.146}$$

while guaranteeing both that the probability that we do not decode at time $n_0$ when no transmitters are active does not exceed $\epsilon_0$ and that the probability that we decode at time $n_0$ when $k > 0$ transmitters are active does not exceed $\frac{E_k}{\sqrt{n_k}}$. Note that $E_k$ only affects the constant term $O(1)$ in (6.146). Theorem 6.5.3 implies that the coefficients in front of $\log n_1$, $\sqrt{\log n_1}$, and $\log\log n_1$ in (6.146) are optimal. Juxtaposing (6.124) and (6.146), we see that Hoeffding's test achieves the optimal first-order error exponent (that is, the optimal coefficient in front of $\log n_1$).

## 6.6 VLSF Codes for the DM-RAC with at Most $K$ Transmitters

The VLSF RAC code defined here combines the rateless communication strategy that we introduce in Section 6.4 with the sparse feedback VLSF PPC and MAC codes with optimized average decoding times in Chapters 4–5. Namely, if the decoder concludes that $k \neq 0$ transmitters are active, it can decode at any of the $L$ decoding times $n_{k,1} < n_{k,2} < \cdots < n_{k,L}$ rather than just the single time $n_k$ used in Section 6.4. For every $k \in [K]$, the locations of the $L$ decoding times are optimized to attain the minimum average decoding delay.

We formally define VLSF codes for the RAC as follows.

**Definition 6.6.1.** *Fix $\epsilon \in (0,1)$ and $N_0, \dots, N_K \in (0, \infty)$. An $(\{N_k\}_{k=0}^K, L, M, \{\epsilon_k\}_{k=0}^K)$ VLSF code with identical encoders comprises*

1. *a set of integers $\mathcal{N} \triangleq \{n_0\} \cup \{n_{k,\ell} \colon k \in [K], \ell \in [L]\}$ (without loss of generality, assume that $n_{K,L}$ is the largest available decoding time),*
2. *a common randomness random variable $U$ on an alphabet $\mathcal{U}$,*
3. *a sequence of encoding functions $\mathsf{f}_n \colon \mathcal{U} \times [M] \to \mathcal{X}$, $n = 1, 2, \dots, n_{K,L}$, defining $M$ length-$n_{K,L}$ codewords,*
4. *$KL+1$ decoding functions $\mathsf{g}_{n_0} \colon \mathcal{U} \times \mathcal{Y}_0^{n_0} \to \{\emptyset\} \cup \{\mathsf{e}\}$ and $\mathsf{g}_{n_{k,\ell}} \colon \mathcal{U} \times \mathcal{Y}_k^{n_{k,\ell}} \to [M]^k \cup \{\mathsf{e}\}$ for $k \in [K]$ and $\ell \in [L]$, satisfying an average error probability constraint*
$$\mathbb{P}\left[\mathsf{g}_{\tau_k}(U, Y_k^{\tau_k}) \overset{\pi}{\neq} W_{[k]}\right] \leq \epsilon_k \tag{6.147}$$
*if $k \in [K]$ messages $W_{[k]} = (W_1, \dots, W_k)$ are transmitted, where $W_i$'s are independent and equiprobable on the set $[M]$. If no transmitters are active, the error probability constraint*
$$\mathbb{P}\left[\mathsf{g}_{\tau_0}(U, Y_0^{\tau_0}) \neq \emptyset\right] \leq \epsilon_0 \tag{6.148}$$
*is satisfied, and*
5. *$K$ non-negative integer-valued random stopping times $\tau_k \in \mathcal{N}$ for the filtration generated by $\{U, Y_k^n\}_{n \in \mathcal{N}}$, satisfying*
$$\mathbb{E}\left[\tau_k\right] \leq N_k \tag{6.149}$$
*if $k \in \{0\} \cup [K]$ transmitters are active.*

In order to be able to detect the number of active transmitters using the received symbols $Y^{n_{k,\ell}}$ but not the codewords themselves, we require that the input distribution $P_X$ satisfies the *distinguishability* assumption

$$P_{Y_{k_1}} \neq P_{Y_{k_2}} \quad \forall\, k_1 \neq k_2 \in \{0\} \cup [K], \tag{6.150}$$

where $P_{Y_k}$ is the marginal output distribution under the DM-MAC with $k$ transmitters and the input distribution $P_{X_{[k]}} = (P_X)^k$.

The following theorem is a second-order achievability result for VLSF codes for DM-RACs.

**Theorem 6.6.1.** *Fix $\epsilon \in (0,1)$, finite integers $K \geq 1$ and $L \geq 2$, and a distribution $P_X$ satisfying (6.9) and (6.150). For any permutation-invariant (6.2) and reducible (6.3) DM-RAC $\left\{(\mathcal{X}^k, P_{Y_k|X_{[k]}}, \mathcal{Y}_k)\right\}_{k=0}^{K}$, there exists an $(\{N_k\}_{k=0}^K, L, M, \{\epsilon_k\}_{k=0}^K)$ VLSF code provided that*

$$k \ln M \leq \frac{N_k I_k}{1-\epsilon_k} - \sqrt{N_k \ln_{(L-1)}(N_k) \frac{V_k}{1-\epsilon_k}} + O\left(\sqrt{\frac{N_k}{\ln_{(L)}(N_k)}}\right) \tag{6.151}$$

*for $k \in [K]$, and*

$$N_0 \geq c \ln N_1 + o(\ln N_1) \tag{6.152}$$

*for some $c > 0$.*

*Proof sketch:* The coding strategy to prove Theorem 6.6.1 is as follows. The decoder applies a $(K+1)$-ary hypothesis test using the output sequence $Y^{n_0}$ and decides an estimate $\hat{k}$ of the number of active transmitters $k \in \{0, 1, \ldots, K\}$. If the hypothesis test declares that $\hat{k} = 0$, then the receiver stops the transmission at time $n_0$, decoding no messages. If $\hat{k} \neq 0$, then the receiver decodes $k$ messages at one of the times $n_{k,1}, \ldots, n_{k,L}$ using the VLSF code in Theorem 5.3.1 for the DM-MAC with $k$ transmitters and $L$ decoding times. If the receiver decodes at time $n_{k,\ell}$, then it sends feedback bit '0' at all previous decoding times $\{n \in \mathcal{N} \colon n < n_{k,\ell}\}$ and feedback bit '1' at time $n_{k,\ell}$. Note that alternatively, the receiver can send its estimate $\hat{k}$ using $\lceil \log_2(K+1) \rceil + L$ bits at time $n_0$, informing the transmitters that the decoding must lie in set $\{n_{\hat{k},1}, \ldots, n_{\hat{k},L}\}$; in this case, the number of feedback bits is less than the worst-case $KL + 1$ that results from the strategy described above. The details of the proof appear in Appendix E.5.1. ■

## 6.7 Summary

We study the agnostic random access model, in which each transmitter knows nothing about the set of active transmitters beyond what it learns from limited scheduled feedback from the receiver, and the receiver knows nothing about the set of active transmitters beyond what it learns from the channel output. In our proposed rateless coding strategy, the decoder attempts to decode only at a fixed, finite collection of decoding times. At each decoding time $n_t$, it sends a single bit of feedback to all transmitters indicating whether or not its estimate for the number of active transmitters is $t$. We prove non-asymptotic and second-order achievability results for the equal rate point $(R, \ldots, R)$ under our assumptions on the channel (permutation-invariance (6.2), reducibility (6.3), friendliness (6.8), and interference (6.9)). For a nontrivial class of discrete, memoryless RACs, our proposed RAC code performs as well in its capacity and dispersion terms as the best-known code for the discrete memoryless MAC in operation; that is, it performs as well as if the transmitter set were known *a priori*. The assumptions of permutation-invariance (6.2), reducibility (6.3), and interference (6.9) together with our use of identical encoding guarantee (by Lemma 6.2.2) that the equal rate point always lies on the sum-rate boundary rather than on one of the corner points. For example, for two users, the capacity region is a symmetric pentagon. This ensures that our simplified, single-threshold decoding rule results in no loss in the first- or second-order achievable rate terms, making the codes far more practical than prior schemes [19]–[22] in which decoders employ $2^k - 1$ simultaneous threshold-rules. In Section 6.4.4, we show that as long as $K < \infty$, there is no loss in the first two terms even if the decoder is tasked with decoding transmitter identity.

We also provide a tight approximation for the capacity and dispersion of the adder-erasure RAC (6.15), which is an example channel satisfying our symmetry conditions.

In order to decide whether there are any active transmitters without enumerating all $K$ alternative hypotheses, we analyze universal hypothesis tests. Results are given both for the case where the channel output alphabet is finite and the case where the channel output alphabet is countably or uncountably infinite. Using existing literature, it is possible in both cases to obtain exponentially decaying maximum type-II error under the condition that $\sup_{x\in\mathbb{R}}|F_k(x) - F_0(x)|\geq \delta_0 > 0$ for all $k \in [K]$. We also derive the best third-order asymptotics of the minimax type-II error (Theorem 6.5.3).

We conclude the chapter by giving some directions for generalizations and future work.

- *Achievability of unequal rate points*: While identical encoding is appealing from a practical perspective, it is also possible to design codes with different transmitters operating at different rates. Such codes would employ non-identical encoding at the transmitters, and they could also employ a decoding rule with multiple, simultaneous threshold rules. In [131, Section VI], Chen *et al.* use a similar strategy to derive third-order achievability and converse results for the random access source coding problem where operation at both identical and distinct rates is allowed.

- *Unordered decoding times:* Example scenarios where unordered decoding times can arise include channels that do not satisfy the assumptions (6.8) or (6.9), applications characterized by small message sizes (e.g., in the internet of things), and scenarios where the system designer chooses unordered decoding times (e.g., when a quick error is preferable to a long period of low individual data rates caused by unusually high traffic in the network). It is easy to modify our nonasymptotic bound (Theorem 6.3.2) to capture the case where $n_0, \ldots, n_K$ are unordered.

- *Non-i.i.d. input distributions at the random encoders:* Our random coding design generalizes to scenarios where an arbitrary input distribution $P_{X^{n_K}}$ is employed instead of $P_X \times \cdots \times P_X$. More broadly, non-stationary input distributions can arise in communication over RACs where no single $P_X$ simultaneously maximizes all mutual informations $I_k$. While we explore in Section 6.4.4 how to choose the "best" single-letter input distribution $P_X$ for this scenario, it is possible to employ different input distributions for each of the sub-codewords $n_1, n_2 - n_1, \ldots, n_K - n_{K-1}$ to achieve higher rates. The special case of Gaussian RAC, where the codewords are drawn from a restricted subset of the power sphere is the topic of the next chapter.

- *Fading channels*: A rateless code design for quasi-static fading RACs where the channel fading coefficients are unavailable either at the transmitters or at the receiver would constitute one of the most practically relevant extensions of this work. In the quasi-static fading channel model with a fixed blocklength, the achievable rate is dictated by a quantity called the *outage probability* [132]. If the fading coefficient is small in a communication epoch, then the channel is declared to be in *outage* and reliable communication is not achieved. However, using rateless codes, it is possible to maintain reliable communication at the expense of reduced rates (i.e., larger decoding times) when the fading coefficient is small while achieving larger rates when the fading coefficient is large. While Kowshik *et al.* [133] derive achievability results for the quasi-static fading RAC in the fixed blocklength regime under the PUPE (6.107) criterion, *rateless coding* over fading RACs is yet to be fully explored.

*Chapter 7*

# GAUSSIAN MULTIPLE AND RANDOM ACCESS CHANNELS

## 7.1 Introduction

We consider a communication scenario where $K$ transmitters are communicating with a single receiver through a Gaussian channel. We study two problems in this network: multiple access and random access communication. In the multiple access problem, the identity of active transmitters is known to all transmitters and to the receiver. In the random access problem, the set of active transmitters is unknown to the transmitters and to the receiver.

For $K = 1$, Shannon's 1948 paper [1] derives the capacity

$$C(P) = \frac{1}{2}\log(1+P) \tag{7.1}$$

using codewords with symbols drawn independently and identically distributed (i.i.d.) according to the Gaussian distribution with variance $P - \delta$ for a very small value $\delta$; here $P$ is the maximal (per-codeword) power constraint, and the noise variance is 1. In [6], Shannon shows the performance improvement in the achievable reliability function using codewords drawn uniformly at random on an $n$-dimensional sphere of radius $\sqrt{nP}$ and a maximum likelihood decoder. Tan and Tomamichel [44] use the same distribution and decoder to prove the achievability of a maximal rate of

$$C(P) - \sqrt{\frac{V(P)}{n}}Q^{-1}(\epsilon) + \frac{1}{2}\frac{\log n}{n} + O\left(\frac{1}{n}\right) \tag{7.2}$$

at blocklength $n$, average error probability $\epsilon$, and maximal power $P$, where

$$V(P) = \frac{P(P+2)}{2(1+P)^2} \tag{7.3}$$

is the *dispersion* of the point-to-point Gaussian channel; Polyanskiy *et al.* prove a matching converse in [5]. Under a maximal-error constraint, the first- and second-order terms in (7.2) remain the same under both maximal- and average-power constraints across codewords; under an average-error constraint, average- and maximal-power constraints yield different first- and second-order performance limits [2, Ch. 4]. In this chapter, we only consider average-error and maximal-power constraints.

MolavianJazi and Laneman [24] and Scarlett *et al.* [22] generalize the asymptotic expansion in (7.2) to the two-transmitter Gaussian MAC, bounding the achievable rate as a function of the $3 \times 3$ dispersion matrix $\mathsf{V}(P_1, P_2)$, an analogue of $V(P)$ assuming transmitters with per-codeword power constraints $P_1$ and $P_2$. The bound in [24] uses codewords uniformly distributed on the power sphere and threshold decoding based on the *information density*; the bound in [22] uses constant composition codes and a quantization argument for the Gaussian channel. This chapter improves those bounds using codewords uniformly distributed on the power sphere and a maximum likelihood decoding rule.

Motivated by the desire to build superior RAC codes for Gaussian channels, we here propose a new code design for the Gaussian RAC. In the proposed code design, random codewords are designed by concatenating $K$ partial codewords of blocklengths $n_1, n_2 - n_1, \ldots, n_K - n_{K-1}$, each drawn from a uniform distribution on a sphere of radius $\sqrt{(n_i - n_{i-1})P}$. When $k$ transmitters are active, the resulting codewords are uniformly distributed on a restricted subset of the sphere of radius $\sqrt{n_k P}$. The receiver uses output typicality to determine the number of transmitters and then applies a maximum likelihood decoding rule. Despite the restricted subset of codewords that result from our design, we achieve the same first-, second-, and third-order performance as the MAC code. While this chapter focuses on Gaussian channels with maximal-power and average-error constraints, we note that the ideas developed here may be useful beyond this example channel and communication scenario.

### 7.1.1 Chapter Organization

The organization of the chapter is as follows. The system model, main result, and discussions for the Gaussian MAC and Gaussian RAC appear in Sections 7.2 and 7.3. The proofs of the achievability bounds for the two-transmitter Gaussian MAC, the $K$-transmitter Gaussian MAC, and the Gaussian RAC appear in Sections 7.4–7.7.

## 7.2 An RCU Bound and its Analysis for the Gaussian MAC

### 7.2.1 An RCU Bound for General MACs

We begin by defining a two-transmitter MAC code.

**Definition 7.2.1.** *An* $(M_1, M_2, \epsilon)$*-MAC code for the channel with transition law* $P_{Y_2|X_1X_2}$ *consists of two encoding functions* $\mathsf{f}_1 \colon [M_1] \to \mathcal{X}_1$ *and* $\mathsf{f}_2 \colon [M_2] \to$

*$\mathcal{X}_2$ and a decoding function $\mathsf{g}\colon \mathcal{Y}_2 \to [M_1] \times [M_2]$ such that*

$$\frac{1}{M_1 M_2} \sum_{m_1=1}^{M_1} \sum_{m_2=1}^{M_2} \mathbb{P}[\mathsf{g}(Y_2) \neq (m_1, m_2) \mid (X_1, X_2) = (\mathsf{f}_1(m_1), \mathsf{f}_2(m_2))] \leq \epsilon, \quad (7.4)$$

*where $Y_2$ is the channel output under inputs $X_1$ and $X_2$, and $\epsilon$ is the average-error constraint.*

We define the information densities for a MAC with channel transition law $P_{Y_2|X_1X_2}$ as

$$\imath_1(x_1; y|x_2) \triangleq \log \frac{P_{Y_2|X_1X_2}(y|x_1, x_2)}{P_{Y_2|X_2}(y|x_2)} \quad (7.5a)$$

$$\imath_2(x_2; y|x_1) \triangleq \log \frac{P_{Y_2|X_1X_2}(y|x_1, x_2)}{P_{Y_2|X_1}(y|x_1)} \quad (7.5b)$$

$$\imath_{1,2}(x_1, x_2; y) \triangleq \log \frac{P_{Y_2|X_1X_2}(y|x_1, x_2)}{P_{Y_2}(y)}, \quad (7.5c)$$

where $P_{X_1}$ and $P_{X_2}$ are the channel input distributions, and $P_{X_1}P_{X_2} \to P_{Y_2|X_1X_2} \to P_{Y_2}$. The information density random vector is defined as

$$\boldsymbol{\imath}_2 \triangleq \begin{bmatrix} \imath_1(X_1; Y_2|X_2) \\ \imath_2(X_2; Y_2|X_1) \\ \imath_{1,2}(X_1, X_2; Y_2) \end{bmatrix}, \quad (7.6)$$

where $(X_1, X_2, Y_2)$ is distributed according to $P_{X_1}P_{X_2}P_{Y_2|X_1X_2}$.

Theorem 7.2.1, below, generalizes Polyanskiy *et al.*'s random-coding union (RCU) achievability bound [5, Th. 16] to the MAC. Theorem 7.2.1 is derived by Liu and Effros [113] in their work on LDPC codes and is inspired by a new RCU bound for the Slepian-Wolf setting [134, Th. 2]. Its proof combines random code design and a maximum likelihood decoder, which decodes to the message pair with the maximum information density $\imath_{1,2}(X_1, X_2; Y_2)$. Our main result on the Gaussian MAC, Theorem 7.2.2, below, analyzes the RCU bound with $P_{X_1}$ and $P_{X_2}$ uniform on the power spheres.

**Theorem 7.2.1** (RCU bound for the MAC [113, Th. 6])**.** *Fix input distributions $P_{X_1}$ and $P_{X_2}$. Let*

$$\begin{aligned} &P_{X_1,\overline{X}_1,X_2,\overline{X}_2,Y_2}(x_1, \overline{x}_1, x_2, \overline{x}_2, y) \\ &= P_{X_1}(x_1)P_{X_1}(\overline{x}_1)P_{X_2}(x_2)P_{X_2}(\overline{x}_2)P_{Y_2|X_1X_2}(y|x_1, x_2). \end{aligned} \quad (7.7)$$

*There exists an $(M_1, M_2, \epsilon)$-MAC code for $P_{Y_2|X_1X_2}$ such that*

$$\epsilon \leq \mathbb{E}\Big[\min\Big\{1, (M_1-1)\mathbb{P}[\imath_1(\overline{X}_1; Y_2|X_2) \geq \imath_1(X_1;Y_2|X_2) \mid X_1, X_2, Y_2]$$
$$+(M_2-1)\mathbb{P}[\imath_2(\overline{X}_2; Y_2|X_1) \geq \imath_2(X_2;Y_2|X_1) \mid X_1, X_2, Y_2]$$
$$+(M_1-1)(M_2-1)\mathbb{P}[\imath_{1,2}(\overline{X}_1, \overline{X}_2; Y_2) \geq \imath_{1,2}(X_1, X_2; Y_2) \mid X_1, X_2, Y_2]\Big\}\Big]. \quad (7.8)$$

**Remark 7.2.1.** *As noted in [113], Theorem 7.2.1 generalizes to the $K$-transmitter MAC. Define the conditional information densities for the $K$-transmitter MAC as*

$$\imath_{\mathcal{S}}(x_{\mathcal{S}}; y|x_{\mathcal{S}^c}) \triangleq \log \frac{P_{Y_K|X_{[K]}}(y|x_{[K]})}{P_{Y_K|X_{\mathcal{S}^c}}(y|x_{\mathcal{S}^c})}, \quad (7.9)$$

*where $\mathcal{S} \subset [K]$, $\mathcal{S} \neq \emptyset$, and $\mathcal{S}^c = [K] \setminus \mathcal{S}$, and the unconditional information density as*

$$\imath_{[K]}(x_{[K]}; y) \triangleq \log \frac{P_{Y_K|X_{[K]}}(y|x_{[K]})}{P_{Y_K}(y)}. \quad (7.10)$$

*Following arguments identical to those in the proof of Theorem 7.2.1, inequality (7.8) extends to the $K$-transmitter MAC as*

$$\epsilon \leq \mathbb{E}\Bigg[\min\Bigg\{1, \sum_{\mathcal{S} \in \overline{\mathcal{P}}([K])} \Bigg(\prod_{s \in \mathcal{S}} (M_s - 1)\Bigg) \mathbb{P}[\imath_{\mathcal{S}}(\overline{X}_{\mathcal{S}}; Y_K|X_{\mathcal{S}^c})$$
$$\geq \imath_{\mathcal{S}}(X_{\mathcal{S}}; Y_K|X_{\mathcal{S}^c}) \mid X_{[K]}, Y_K]\Bigg\}\Bigg]. \quad (7.11)$$

### 7.2.2 A Third-order Achievability Bound for the Gaussian MAC

We begin by modifying our code definition to incorporate maximal-power constraints $(P_1, P_2)$ on the channel inputs. Let $(\mathbf{X}_1, \mathbf{X}_2)$ and $\mathbf{Y}_2$ be the MAC inputs and output, respectively.

**Definition 7.2.2.** *An $(n, M_1, M_2, \epsilon, P_1, P_2)$-MAC code for a two-transmitter MAC comprises encoding functions $\mathsf{f}_1 \colon [M_1] \to \mathbb{R}^n$ and $\mathsf{f}_2 \colon [M_2] \to \mathbb{R}^n$, and a decoding function $\mathsf{g} \colon \mathbb{R}^n \to [M_1] \times [M_2]$ such that*

$$\|\mathsf{f}_i(m_i)\|_2^2 \leq nP_i \ \ \forall i \in \{1,2\}, \ \ m_i \in [M_i]$$
$$\frac{1}{M_1M_2} \sum_{m_1=1}^{M_1} \sum_{m_2=1}^{M_2} \mathbb{P}\left[\mathsf{g}(\mathbf{Y}_2) \neq (m_1, m_2) | (\mathbf{X}_1, \mathbf{X}_2) = (\mathsf{f}_1(m_1), \mathsf{f}_2(m_2))\right] \leq \epsilon.$$

The following notation is used in presenting our achievability result for the Gaussian MAC with $k \geq 1$ transmitters. Over $n$ channel uses, the channel has inputs $\mathbf{X}_1, \ldots, \mathbf{X}_k \in \mathbb{R}^n$, additive noise $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{I}_n)$, and output

$$\mathbf{Y}_k = \mathbf{X}_{\langle [k] \rangle} + \mathbf{Z}. \tag{7.12}$$

The channel transition law induced by (7.12) can be written as

$$P_{\mathbf{Y}_k | \mathbf{X}_{[k]}}(\mathbf{y} | \mathbf{x}_{[k]}) = \prod_{i=1}^{n} P_{Y_k | X_{[k]}}(y_i | x_{1i}, \ldots, x_{ki}), \tag{7.13}$$

where

$$P_{Y_k | X_{[k]}}(y | x_{[k]}) = \frac{1}{\sqrt{2\pi}} \exp\left\{ -\frac{\left(y - x_{\langle [k] \rangle}\right)^2}{2} \right\}. \tag{7.14}$$

When $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V})$, and $\mathsf{V}$ is a $d \times d$ positive semi-definite matrix, the multidimensional analogue of the inverse $Q^{-1}(\cdot)$ of the complementary Gaussian cumulative distribution is

$$\mathscr{Q}_{\text{inv}}(\mathsf{V}, \epsilon) \triangleq \left\{ \mathbf{z} \in \mathbb{R}^d : \mathbb{P}\left[\mathbf{Z} \leq \mathbf{z}\right] \geq 1 - \epsilon \right\}. \tag{7.15}$$

For $d = 1$, we have $Q^{-1}(\epsilon) = \min\{z \colon z \in Q_{\text{inv}}(1, \epsilon)\}$.

Recall that $C(P)$ is the capacity function (7.1). The capacity vector for the two-transmitter Gaussian MAC is defined as

$$\mathbf{C}(P_1, P_2) \triangleq \begin{bmatrix} C(P_1) \\ C(P_2) \\ C(P_1 + P_2) \end{bmatrix}. \tag{7.16}$$

The dispersion matrix [24, eq. (25)] for the two-transmitter Gaussian MAC is defined as

$$\mathsf{V}(P_1, P_2) \triangleq \begin{bmatrix} V(P_1) & V_{1,2}(P_1, P_2) & V_{1,12}(P_1, P_2) \\ V_{1,2}(P_1, P_2) & V(P_2) & V_{2,12}(P_1, P_2) \\ V_{1,12}(P_1, P_2) & V_{2,12}(P_1, P_2) & V_{12}(P_1, P_2) \end{bmatrix}, \tag{7.17}$$

where $V(P)$ is the dispersion function (7.3), and

$$V_{1,2}(P_1, P_2) = \frac{1}{2} \frac{P_1 P_2}{(1 + P_1)(1 + P_2)} \tag{7.18}$$

$$V_{i,12}(P_1, P_2) = \frac{1}{2} \frac{P_i(2 + P_1 + P_2)}{(1 + P_i)(1 + P_1 + P_2)}, \quad i \in \{1, 2\} \tag{7.19}$$

$$V_{12}(P_1, P_2) = V(P_1 + P_2) + \frac{P_1 P_2}{(1 + P_1 + P_2)^2}. \tag{7.20}$$

The following theorem is the main result of this section.

**Theorem 7.2.2.** *For any $\epsilon \in (0,1)$ and any $P_1, P_2 > 0$, an $(n, M_1, M_2, \epsilon, P_1, P_2)$-MAC code for the two-transmitter Gaussian MAC exists provided that*

$$\begin{bmatrix} \log M_1 \\ \log M_2 \\ \log M_1 M_2 \end{bmatrix} \in n\mathbf{C}(P_1, P_2) - \sqrt{n} Q_{\text{inv}}(\mathsf{V}(P_1, P_2), \epsilon) + \frac{1}{2}\log n \mathbf{1} + O(1)\mathbf{1}. \tag{7.21}$$

*Proof:* See Section 7.4. ■

Theorem 7.2.2 extends to the general $K$-transmitter Gaussian MAC. The definition of an $(n, M_{[K]}, \epsilon, P_{[K]})$-MAC code for the $K$-transmitter Gaussian MAC with message set sizes $M_1, \ldots, M_K$ and power constraints $P_1, \ldots, P_K$ is a natural extension of Definition 7.2.2, which defines the two-transmitter MAC code. The following theorem bounds the achievable region for the $K$-transmitter Gaussian MAC.

**Theorem 7.2.3.** *For any $\epsilon \in (0,1)$, and $P_i > 0$, $i \in [K]$, an $(n, M_{[K]}, \epsilon, P_{[K]})$-MAC code for the $K$-transmitter Gaussian MAC exists provided that*

$$\begin{aligned} \left( \sum_{s \in \mathcal{S}} \log M_s \colon \mathcal{S} \in \overline{\mathcal{P}}([K]) \right) &\in n\mathbf{C}(P_{[K]}) \\ &-\sqrt{n} Q_{\text{inv}}(\mathsf{V}(P_{[K]}), \epsilon) + \frac{1}{2}\log n \mathbf{1} + O\left(1\right)\mathbf{1}, \end{aligned} \tag{7.22}$$

*where $\mathbf{C}(P_{[K]})$ is the capacity vector*

$$\mathbf{C}(P_{[K]}) \triangleq \left( C(P_{\langle \mathcal{S} \rangle}) : \mathcal{S} \in \overline{\mathcal{P}}([K]) \right) \in \mathbb{R}^{2^K - 1}, \tag{7.23}$$

*and $\mathsf{V}(P_{[K]})$ is the $\left(2^K - 1\right) \times \left(2^K - 1\right)$ dispersion matrix with the elements $\mathsf{V}_{\mathcal{S}_1, \mathcal{S}_2}(P_{[K]})$, $\mathcal{S}_1, \mathcal{S}_2 \in \overline{\mathcal{P}}([K])$, given by*

$$\mathsf{V}_{\mathcal{S}_1, \mathcal{S}_2 (P_{[K]})} \triangleq \frac{P_{\langle \mathcal{S}_1 \rangle} P_{\langle \mathcal{S}_2 \rangle} + 2P_{\langle \mathcal{S}_1 \cap \mathcal{S}_2 \rangle} + \left(P_{\langle \mathcal{S}_1 \cap \mathcal{S}_2 \rangle}\right)^2 - P^2_{\langle \mathcal{S}_1 \cap \mathcal{S}_2 \rangle}}{2(1 + P_{\langle \mathcal{S}_1 \rangle})(1 + P_{\langle \mathcal{S}_2 \rangle})}. \tag{7.24}$$

*Proof:* See Section 7.5. ■

Before concluding this section, we make several remarks about Theorems 7.2.2 and 7.2.3 above.

1. Theorems 7.2.2 and 7.2.3 apply the RCU bound (Theorem 7.2.1) with independent inputs uniformly distributed on the $n$-dimensional origin-centered spheres with radii $\sqrt{nP_i}$, $i \in [K]$. Theorem 7.2.2 matches the

first- and second-order terms of MolavianJazi and Laneman [24] and Scarlett *et al.* [22], and improves the third-order term from $O\left(n^{1/4}\right)\mathbf{1}$ in [24] and $O\left(n^{1/4}\log n\right)\mathbf{1}$ in [22] to $\frac{1}{2}\log n\mathbf{1}+O(1)\mathbf{1}$.

2. Our proof technique in Theorem 7.2.2 differs from the technique in [24] in two key ways. First, we use a maximum likelihood decoder in place of the set of simultaneous threshold rules based on unconditional and conditional information densities from [24]; the change of the decoding rule is essential for obtaining the third-order term $\frac{1}{2}\log n\mathbf{1}+O(1)\mathbf{1}$ in Theorem 7.2.2. Second, we refine the analysis bounding the probability that the information density random vector $\boldsymbol{\imath}_2$ belongs to a set $\mathcal{D}\subseteq\mathbb{R}^3$. Our non-i.i.d. input distribution prevents direct application of the Berry-Esseen theorem. However, given that the inner product of the inputs $\langle\mathbf{X}_1,\mathbf{X}_2\rangle$ equals a constant, the information density random vector $\boldsymbol{\imath}_2$ can be written as a sum of independent random vectors. Therefore, we apply the Berry-Esseen theorem after conditioning on the inner product $\langle\mathbf{X}_1,\mathbf{X}_2\rangle$ and then integrate the resulting probabilities over the range of the inner product. In order to approximate the resulting probability by the probability that a Gaussian vector belongs to the same set, we use a result (Lemma 7.4.5 in Section 7.4.1, below) that approximates the normalized inner product $\frac{1}{\sqrt{nP_1P_2}}\langle\mathbf{X}_1,\mathbf{X}_2\rangle$ by a standard Gaussian random variable. We then derive a bound (Lemma 7.4.4 in Section 7.4.1, below) on the total variation distance between two Gaussian vectors. This analysis appears in Section 7.4.6.

   This approach contrasts with [24], which bounds the probability that the information density random vector $\boldsymbol{\imath}_2$ belongs to a set $\mathcal{D}$. Writing $\boldsymbol{\imath}_2$ as a vector-valued function of an average of i.i.d. Gaussian vectors, [24, Prop. 1] applies a central limit theorem for functions of sums to prove $O\left(\frac{1}{n^{1/4}}\right)$ convergence to normality. Our technique, described above, improves the rate of convergence to normality to $O\left(\frac{1}{\sqrt{n}}\right)$, which is the rate of convergence for i.i.d. sums. This improvement implies that the threshold-based decoding rule in [24] achieves a third-order term $O(1)\mathbf{1}$.

3. Our technique for proving Theorems 7.2.2 and 7.2.3 parallels those used for non-singular discrete memoryless channels [2, Th. 53] and for the point-to-point Gaussian channel [44]. In [2, Th. 53], Polyanskiy applies the RCU bound using a refined large deviations result Lemma 2.5.1;

the use of a non-i.i.d. input distribution for the Gaussian channel prevents the direct application of Lemma 2.5.1. In [44, eq. (52)], Tan and Tomamichel derive an alternative to Lemma 2.5.1 for the point-to-point Gaussian channel in order to accommodate codewords drawn uniformly on an $n$-dimensional sphere. While evaluating the RCU bound in this chapter, we extend the bound in [44, eq. (52)] to the Gaussian MAC.

4. For the symmetric setting, where $P_i = P$ and $M_i = M$ for all $i \in [K]$, Theorem 7.2.3 reduces to the scalar inequality, below. This result refines the result in [24, Th. 2] to the third-order term and generalizes it to the $K$-transmitter MAC.

**Corollary 7.2.1.** *For any $\epsilon \in (0, 1)$ and $P > 0$, an $(n, M\mathbf{1}, \epsilon, P\mathbf{1})$-MAC code for the $K$-transmitter Gaussian MAC exists provided that*

$$\begin{aligned} K \log M \leq{}& nC(KP) \\ &- \sqrt{n(V(KP) + V_{\mathrm{cr}}(K, P))}Q^{-1}(\epsilon) + \frac{1}{2}\log n + O(1). \end{aligned} \tag{7.25}$$

*Again, $C(\cdot)$ and $V(\cdot)$ are the capacity (7.1) and dispersion (7.3) functions, respectively, and $V_{\mathrm{cr}}(K, P)$ is the cross dispersion term*

$$V_{\mathrm{cr}}(K, P) \triangleq \frac{K(K-1)P^2}{2(1+KP)^2}. \tag{7.26}$$

*Proof:* See Appendix F.1. ■

5. In [119], Fong and Tan derive a converse for the Gaussian MAC with a second-order term $O(\sqrt{n \log n})\mathbf{1}$. Kosut [23] improves the second-order term in the converse to $O\left(\sqrt{n}\right)\mathbf{1}$. The coefficients of the second-order term in [23] do not match the second-order term in the achievability bounds proven in Theorem 7.2.2. As discussed in Chapter 6, closing the gap between the second-order terms of the MAC achievability and converse results is a challenging open problem.

## 7.3 A Nonasymptotic Bound and its Analysis for the Gaussian Random Access Channel

### 7.3.1 System Model

*Channel model*: Given an unknown set of active transmitters $\mathcal{A}$, the Gaussian channel (7.14) depends on $\mathcal{A}$ only through the number of active transmitters,

$|\mathcal{A}|= k$, that is, $P_{Y_k|X_{\mathcal{A}}} = P_{Y_k|X_{[k]}}$. Therefore, in order to capture the scenario of a memoryless Gaussian channel with $K$ possible transmitters, a single receiver, and an unknown activity pattern $\mathcal{A} \subseteq [K]$, we describe the Gaussian RAC by a family of Gaussian MACs $\{P_{Y_k|X_{[k]}}\}_{k=0}^{K}$ (7.14), each indexed by the number of active transmitters $k \in \{0, \dots, K\}$. Recall that this Gaussian RAC model satisfies the assumptions in Section 6.2.4. As in Chapter 6, we choose a *compound channel* model in order to avoid the need to assign probabilities to each activity pattern $\mathcal{A}$.

*Communication strategy*: We apply the epoch-based *rateless* communication strategy that we proposed in Chapter 6. Each transmitter is either active or silent during a whole epoch. At each of times $n_0, n_1, \dots,$ the decoder broadcasts to all transmitters a single bit — sending value 1 if it can decode and 0 otherwise. The transmission of 1 at time $n_t$ ends the current epoch and starts the next, indicating that the decoder's estimate of the number of transmitters is $t$. As in Chapter 6, we employ identical encoding, with each active transmitter $i$ using the same encoding function to describe its message $W_i \in [M]$. Identical encoding here requires $P_i = P$ and $M_i = M$ for all $i$. The task of the decoder is to decode a list of messages sent by the active transmitters $\mathcal{A}$ but not the identities of those transmitters. The messages in $W_{\mathcal{A}}$ are independent and uniformly distributed on alphabet $[M]$.

Since encoding is identical and the channel is invariant to permutation of its inputs, we assume without loss of generality that $|\mathcal{A}|= k$ implies $\mathcal{A} = [k]$. Intuitively, given identical encoding and our Gaussian channel, one would expect that interference increases with the number of active transmitters $k$, and therefore that the decoding time $n_k$ increases with $k$. Since the capacity per transmitter for the $k$-transmitter Gaussian MAC, $\frac{1}{k}C(kP)$, decreases with $k$, we can choose $n_0 < \cdots < n_K$ for $M$ large enough (see Lemma 6.2.1). As a notational convenience, we use $n_K$ to represent the largest decoding time. Unless it stops the encoders' transmissions earlier, at time $n_K$, the decoder sees

$$\mathbf{Y}_k = \mathbf{X}_{\langle [k] \rangle} + \mathbf{Z} \in \mathbb{R}^{n_K} \qquad \text{for } k \in [K], \tag{7.27}$$

where $\mathbf{X}_1, \dots, \mathbf{X}_k$ are $n_K$-dimensional channel inputs, $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{I}_{n_K})$ is the Gaussian noise, and $\mathbf{Y}_k$ is the $n_K$-dimensional output when $k$ transmitters are active. When no transmitters are active, $\mathbf{X}_{\langle [0] \rangle} = \mathbf{0}$ and $\mathbf{Y}_0 = \mathbf{Z}$. At each time $n_t < n_K$, the decoder has access to the first $n_t$ components of vector $\mathbf{Y}_k$, which is denoted by $\mathbf{Y}_k^{[n_t]}$.[1]

As in Chapter 6, we assume an *agnostic* random access model, where the transmitters know nothing about the set $\mathcal{A}$ of active transmitters except their own membership and the feedback from the receiver. The receiver knows nothing about $\mathcal{A}$ except what it can learn from the channel output $\mathbf{Y}_k$. Beside these, we require that every code must satisfy a power constraint for every available decoding time.

*Code definition*: The following definition formalizes the rateless Gaussian RAC code described above.

**Definition 7.3.1.** *An $\left(\{n_j, \epsilon_j\}_{j=0}^K, M, P\right)$-RAC code for the Gaussian RAC with $K$ transmitters consists of a single encoding function $\mathsf{f}\colon \mathcal{U} \times [M] \to \mathbb{R}^{n_K}$ and decoding functions $\mathsf{g}_k\colon \mathcal{U} \times \mathbb{R}^{n_k} \to [M]^k \cup \{\mathsf{e}\}$ for $k = 0, \ldots, K$, where the input $u \in \mathcal{U}$ to the encoder and decoders is common randomness shared by all transmitters and the receiver.*[2] *If it cannot decode at time $n_k$, the decoder outputs the erasure symbol "$\mathsf{e}$" and broadcasts value 0 to the transmitters, informing them that they should keep transmitting. If it can decode at time $n_k$, the decoder broadcasts value 1 to the transmitters, informing them that they should stop transmitting. The codewords satisfy the maximal-power constraints*

$$\left\|\mathsf{f}(u, m)^{[n_j]}\right\|_2^2 \leq n_j P \text{ for } m \in [M], u \in \mathcal{U}, j \in [K]. \tag{7.28}$$

*If $k$ transmitters are active, then the average error probability in decoding $k$ messages at time $n_k$ is bounded as*

$$\begin{aligned}\frac{1}{M^k} \sum_{m_{[k]} \in [M]^k} \mathbb{P}\Bigg[\Bigg\{ \bigcup_{t : n_t \leq n_k, t \neq k} \left\{\mathsf{g}_t(U, \mathbf{Y}_k^{[n_t]}) \neq \mathsf{e}\right\} \Bigg\} \bigcup \\ \left\{\mathsf{g}_k(U, \mathbf{Y}_k^{[n_k]}) \overset{\pi}{\neq} m_{[k]}\right\} \Bigg| \mathbf{X}_{[k]}^{[n_k]} = \mathsf{f}(U, m_{[k]})^{[n_k]}\Bigg] \leq \epsilon_k,\end{aligned} \tag{7.29}$$

*where $\mathsf{f}(U, m_i)$ is the codeword for the message $m_i \in [M]$, $U$ is the common randomness random variable, and the output $\mathbf{Y}_k$ is generated according to*

[1] $\mathbf{Y}_k^{[n_t]}$ is denoted by $Y_k^{n_t}$ in Chapter 6; we here switch to $\mathbf{Y}_k^{[n_t]}$ for notational consistency with the remainder of the chapter.

[2] The realization $u$ of the common randomness random variable $U$ initializes the encoders and the decoder. At the start of each communication epoch, $u$ is shared by all transmitters and the receiver. We show in Appendix E.4 that the alphabet size of $U$ need never exceed $K + 1$.

(7.27). *If no transmitters are active, then the decoder decodes to the unique message* $[M]^0 \triangleq \{0\}$ *with probability of error bounded as*

$$\mathbb{P}\left[\mathsf{g}_0(U, \mathbf{Y}_0^{[n_0]}) \neq 0\right] \leq \epsilon_0. \tag{7.30}$$

### 7.3.2 A Third-order Achievability Result for the Gaussian RAC

The following theorem is the main result of this section.

**Theorem 7.3.1.** *Fix* $K < \infty$, $\epsilon_k \in (0,1)$ *for* $k \in \{0\} \cup [K]$, *and* $M$. *An* $\left(\{n_j, \epsilon_j\}_{j=0}^K, M, P\right)$*-RAC code exists for the Gaussian RAC with* $K$ *possible transmitters provided that*

$$k \log M \leq n_k C(kP) - \sqrt{n_k(V(kP) + V_{\mathrm{cr}}(k,P))}Q^{-1}(\epsilon_k) + \frac{1}{2}\log n_k + O(1) \tag{7.31}$$

*for* $k \in [K]$, *and*

$$n_0 \geq \frac{4(1+P^2)}{P^2}\log n_1 + o(\log n_1), \tag{7.32}$$

*where* $C(\cdot)$, $V(\cdot)$, *and* $V_{\mathrm{cr}}(\cdot,\cdot)$ *are the capacity* (7.1), *dispersion* (7.3), *and cross dispersion functions* (7.26), *respectively. All uses of* $O(\cdot)$ *and* $o(\cdot)$ *are taken with respect to* $n_1$.

**Remark 7.3.1.** *From* (7.31), $n_1 \to \infty$ *implies that* $n_2, \ldots, n_K$ *also grow without bound. Since all target error values* $\epsilon_k$ *are assumed to be constants with respect to* $n_1$, *choosing decoding times* $n_0, \ldots, n_K$ *so that* (7.31) *and* (7.32) *hold with equality results in* $n_k = O(n_1)$ *for* $k \geq 2$, *and* $n_0 = O(\log n_1)$ *(see* (7.35)*, below).*

*Proof:* Theorem 7.3.1 follows from the non-asymptotic achievability bound in Theorem 7.3.2, below, which bounds the average error probability of the proposed Gaussian RAC code. See Section 7.7 for details. ■

**Theorem 7.3.2.** *Fix constants* $\lambda_k > 0$ *for* $k \in \{0\} \cup [K]$ *and distribution* $P_{\mathbf{X}}$ *on* $\mathbb{R}^{n_K}$. *Then, there exists an* $\left(\{n_j, \epsilon_j\}_{j=0}^K, M, P\right)$*-RAC code with*

$$\epsilon_0 \leq \mathbb{P}\left[\left|\left\|\mathbf{Y}_0^{[n_0]}\right\|^2 - n_0\right| > n_0\lambda_0\right] \tag{7.33}$$

$$\epsilon_k \leq \frac{k(k-1)}{2M} + \mathbb{P}\left[\bigcup_{i=1}^{k}\bigcup_{\substack{j: n_j \leq n_k \\ j \geq 1}}\left\{\left\|\mathbf{X}_i^{[n_j]}\right\|_2^2 > n_j P\right\}\right] \tag{7.34a}$$

$$+\,\mathbb{P}\Bigg[\bigcup_{\substack{t:n_t\le n_k\\ t\neq k}}\left\{\left|\left\|\mathbf{Y}_k^{[n_t]}\right\|_2^2-n_t(1+tP)\right|\le n_t\lambda_t\right\}$$

$$\bigcup\left\{\left|\left\|\mathbf{Y}_k^{[n_k]}\right\|_2^2-n_k(1+kP)\right|>n_k\lambda_k\right\}\Bigg] \tag{7.34b}$$

$$+\,\mathbb{E}\Bigg[\min\Bigg\{1,\sum_{s=1}^{k}\binom{k}{s}\binom{M-k}{s}$$

$$\mathbb{P}[\imath_{[s]}(\overline{\mathbf{X}}_{[s]}^{[n_k]};\mathbf{Y}_k^{[n_k]}|\mathbf{X}_{[s+1:k]}^{[n_k]})\imath_{[s]}(\mathbf{X}_{[s]}^{[n_k]};\mathbf{Y}_k^{[n_k]}|\mathbf{X}_{[s+1:k]}^{[n_k]})\mid\mathbf{X}_{[k]}^{[n_k]},\mathbf{Y}_k^{[n_k]}]\Bigg\}\Bigg] \tag{7.34c}$$

*for all $k\in[K]$, where $\mathbf{X}_{[K]},\overline{\mathbf{X}}_{[K]},\mathbf{Y}_k\in\mathbb{R}^{n_K}$ are distributed according to $P_{\mathbf{X}_{[K]},\overline{\mathbf{X}}_{[K]},\mathbf{Y}_k}(\mathbf{x}_{[K]},\overline{\mathbf{x}}_{[K]},\mathbf{y}_k)=\Big(\prod_{j\in[K]}P_{\mathbf{X}}(\mathbf{x}_j)P_{\mathbf{X}}(\overline{\mathbf{x}}_j)\Big)P_{\mathbf{Y}_k|\mathbf{X}_{[k]}}(\mathbf{y}_k|\mathbf{x}_{[k]})$, and $P_{\mathbf{Y}_k|\mathbf{X}_{[k]}}$ is given in (7.27).*

*Proof:* The terms in (7.34a) capture the probability that at least two transmitters send the same message and the probability of a power constraint violation, respectively. We treat the event that at least two transmitters send the same message as an error because the analysis relies on the codeword independence across transmitters. The probability in (7.34b) captures the probability that the decoder decodes at a wrong decoding time, and the expectation in (7.34c) captures the probability that the decoder decodes an incorrect message list at the correct decoding time $n_k$ for $k$ active transmitters. See Section 7.6 for details. ■

We conclude this section with some remarks concerning Theorems 7.3.1 and 7.3.2.

1. Theorem 7.3.1 shows that for the Gaussian RAC, our proposed rateless code performs as well in the first-, second-, and third-order terms as the best known MAC communication scheme without feedback (Corollary 7.2.1). In other words, the first three terms on the right-hand side of (7.31) for $k$ active transmitters match the first three terms of the largest achievable sum-rate in our achievability bound in (7.25) for the $k$-transmitter MAC.

2. To prove Theorem 7.3.1, we particularize the distribution of the random codewords, $P_{\mathbf{X}}$, in Theorem 7.3.2 as follows. The first $n_1$ symbols are drawn uniformly from $\mathbb{S}^{n_1}(\sqrt{n_1P})$. The sub-vector of symbols indexed from $n_{j-1}+1$ to $n_j$ is drawn uniformly from $\mathbb{S}^{n_j-n_{j-1}}(\sqrt{(n_j-n_{j-1})P})$ for

$j = 2, \ldots, K$. These $K$ sub-codewords, each uniformly distributed on an incremental power sphere, are independent. Under this $P_{\mathbf{X}}$, the maximal-power constraint in (7.28) is satisfied with equality for each number of active transmitters. Rather than using an encoding function that depends on the feedback from the receiver to the transmitters, we use an encoding function that is suitable for all possible transmitter activity patterns and does not depend on the receiver's feedback. Given that a decision is made at time $n_k$, the active transmitters have transmitted only the first $n_k$ symbols of the codewords representing their messages during that epoch, and the remaining $n_K - n_k$ symbols of the codewords are not transmitted.

3. As noted in [91], our achievability proofs leverage the fact that the number of active transmitters can be reliably estimated from the total received power. This is possible because when $k$ active transmitters send $k$ distinct messages, the average received power $\frac{1}{n_k}\mathbb{E}\left[\left\|\mathbf{Y}_k^{[n_k]}\right\|_2^2\right]$ at time $n_k$, concentrates around its mean value, $1 + kP$, and this mean is distinct for each $k \in \{0\} \cup [K]$. The decoding function used at time $n_k$ combines the maximum likelihood decoding rule for the $k$-transmitter MAC with a typicality rule based on the power of the output. The typicality rule decides to decode at time $n_k$ if the average received power at time $n_k$ lies in the interval $\left[1 + kP - \frac{P}{2}, 1 + kP + \frac{P}{2}\right]$ for $k \geq 1$ and $\left[1 - O({n_0}^{-\frac{1}{2}}), 1 + O({n_0}^{-\frac{1}{2}})\right]$ for $k = 0$. In this case, the decoder decodes $k$ messages at time $n_k$ by using the maximum likelihood decoding rule. When at least two transmitters send the same message (e.g., $\mathbf{X}_1^{[n_k]} = \mathbf{X}_2^{[n_k]}$), $\frac{1}{n_k}\mathbb{E}\left[\left\|\mathbf{Y}_k^{[n_k]}\right\|_2^2\right] \geq 1+(k+2)P$. In our decoder design, we choose not to handle this scenario because the probability that at least two transmitters send the same message is negligible as shown in (7.177) in Section 7.6.2, below.

4. Theorem 7.3.2 applies without change to non-Gaussian RACs with power constraints satisfying the conditions in Theorem 6.3.1; the tightness of the bound depends on how well $k$ can be estimated from the received power.

5. The proof of Theorem 7.3.1 indicates that the constant term $O(1)$ in (7.31) depends on the number of active transmitters $k$, but not on the

total number of transmitters $K$. Not requiring the decoder to determine transmitter identity is crucial for this $O(1)$ bound to hold.

6. By choosing $n_1, \ldots, n_K$ such that the inequalities in (7.31) are satisfied with equality for each $k$, we can express each $n_k$ as a function of $n_1, \epsilon_1$, $\epsilon_k$, $k$, and $P$, given by

$$\begin{aligned} n_k = n_1 \frac{kC_1}{C_k} &+ \sqrt{n_1}\left(\frac{1}{C_k}\sqrt{\frac{kC_1V_k}{C_k}}Q^{-1}(\epsilon_k) - \frac{k}{C_k}\sqrt{V_1}Q^{-1}(\epsilon_1)\right) \\ &+ \frac{k-1}{2C_k}\log n_1 + O(1), \end{aligned} \tag{7.35}$$

where $C_k = C(kP)$ and $V_k = V(kP) + V_{\rm cr}(k, P)$. We derive (7.35) by computing the Taylor series expansion of the equation for $n_k$ (7.31) in terms of $k, P, \epsilon_k$, and $\log M$; we then replace $\log M$ by (7.31) for $k = 1$. Fig. 7.1 shows the approximate decoding times $\{n_k\}_{k=1}^{6}$ (neglecting the $O(1)$ term in (7.35)), where $P = 1$, $\epsilon_k = 10^{-3}$ for all $k$, and the smallest decoding time $n_1 \in [100, 1000]$.

7. Theorem 7.3.1 implies that the input distribution used for the Gaussian RAC also achieves the performance in Theorem 7.2.3 for the $K$-transmitter Gaussian MAC. As long as $n_j - n_{j-1} \geq cn_K$ holds for some constant $c > 0$ for all $j \in [K]$, requiring separate power constraints on each sub-block of the codewords as

$$\left\|\mathsf{f}_i(m_i)^{[n_j]}\right\|_2^2 \leq n_j P_i \text{ for } m_i \in [M_i], i \in [K], j \in [K] \tag{7.36}$$

does not degrade our performance bound, which matches the first three terms in the expansion in Theorem 7.2.3. The support of the distribution from which the codewords are drawn for the Gaussian MAC and RAC is illustrated in Fig. 7.2.

8. As described above, the number of active transmitters in an epoch is estimated via a sequence of decodability tests. An alternative strategy is to estimate the number of active transmitters in one shot from the received power at time $n_0$, and to inform the transmitters about the estimate, $t$, of the number of active transmitters via a $\lceil \log(K+1) \rceil$-bit feedback at time $n_0$. Given this knowledge, active transmitters can employ an encoding function matched to $t$. We show in Appendix F.2 that this modified coding strategy affects our bound in (7.31) only in the $O(1)$ term.

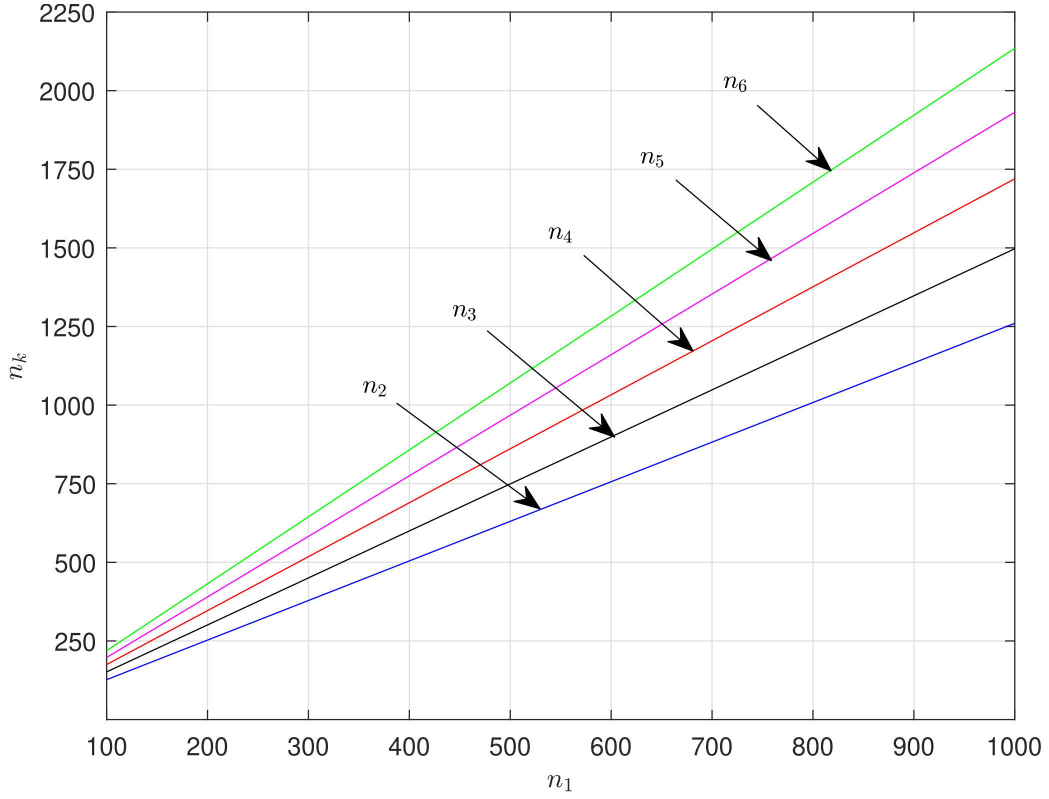


Figure 7.1: Let $P = 1$, $\epsilon_k = 10^{-3}$ for all $k$. The decoding times $\{n_k\}_{k=1}^{6}$ are given according to (7.35), where the $O(1)$ term in (7.35) is ignored,

and $n_1 \in [100, 1000]$.

9. By using distinct codebooks for each transmitter, the decoder can associate transmitter identities with the decoded messages. We show that the first three terms of the expansion in (7.31) are still achievable in this setting.

## 7.4 Proof of Theorem 7.2.2

### 7.4.1 Supporting Lemmas

We begin by presenting the lemmas that play a key role in the proof of Theorem 7.2.2. The first two lemmas are used to bound the probability that the squared norm of the output of the channel, $\mathbf{Y}_2 = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}$, does not belong to its typical interval around $1 + P_1 + P_2$.

Lemma 7.4.1 from [24, Prop. 2] uniformly bounds the Radon-Nikodym derivative of the conditional and unconditional output distributions of the Gaussian MAC (7.13) in response to the spherical inputs with respect to the output distributions that result under i.i.d. Gaussian inputs. The squared norm of the

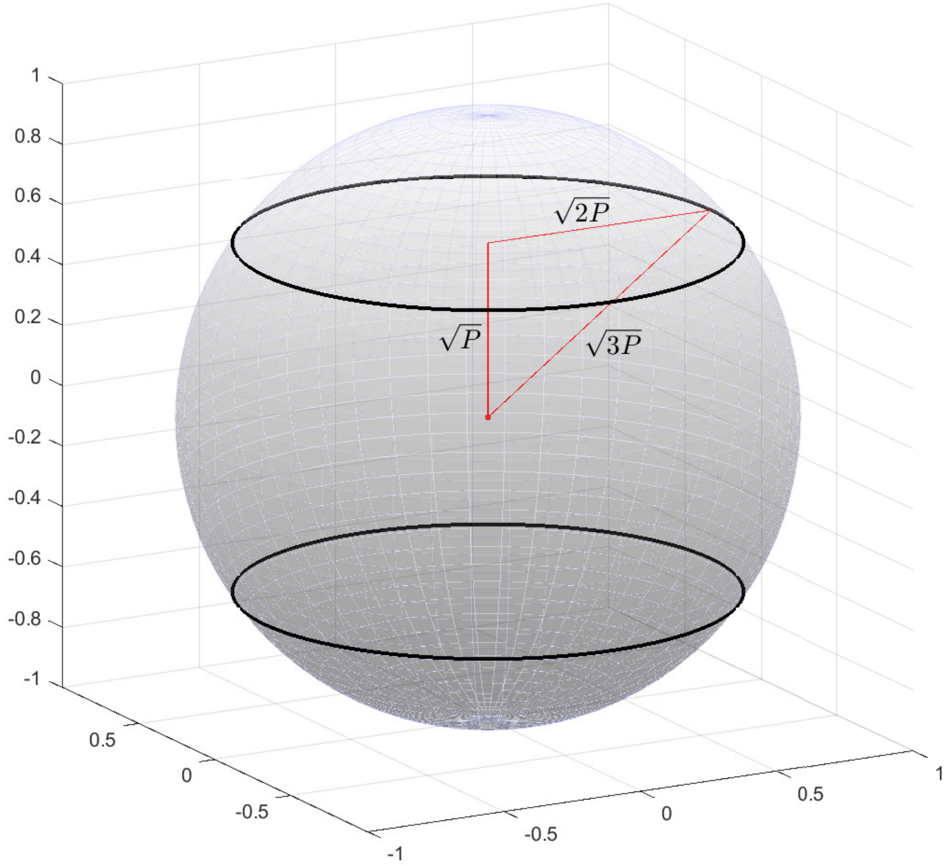


Figure 7.2: Let $K = 2$, $n_1 = 2, n_2 = 3$, and $P_1 = P_2 = P = \frac{1}{3}$. The support of the input distribution for the Gaussian RAC is the Cartesian product of $\mathbb{S}^{n_1}(\sqrt{n_1 P})$ (here a circle with radius $\sqrt{2P}$) and $\mathbb{S}^{n_2-n_1}(\sqrt{(n_2-n_1)P})$ (here the set $\{-\sqrt{P}, \sqrt{P}\}$.) This set, shown above as a pair of circles, is a subset of $\mathbb{S}^{n_2}(\sqrt{n_2 P})$; the set $\mathbb{S}^{n_2}(\sqrt{n_2 P})$ is the support of the input distribution used in Theorem 7.2.3 for the Gaussian MAC.

output in response to the i.i.d. Gaussian inputs has a chi-squared distribution.

**Lemma 7.4.1** (MolavianJazi and Laneman [24, Prop. 2])**.** *1. 2-Transmitter MAC: Let $\mathbf{X}_1$ and $\mathbf{X}_2$ be independent, distributed uniformly on $\mathbb{S}^n(\sqrt{nP_1})$ and $\mathbb{S}^n(\sqrt{nP_2})$, respectively. Let $\tilde{\mathbf{X}}_i \sim \mathcal{N}(\mathbf{0}, P_i \mathsf{I}_n)$, $i \in [2]$, be independent of each other. Let $P_{\mathbf{X}_1\mathbf{X}_2} \to P_{\mathbf{Y}_2|\mathbf{X}_1\mathbf{X}_2} \to P_{\mathbf{Y}_2}$, and $P_{\tilde{\mathbf{X}}_1\tilde{\mathbf{X}}_2} \to P_{\mathbf{Y}_2|\mathbf{X}_1\mathbf{X}_2} \to P_{\tilde{\mathbf{Y}}_2}$, where $P_{\mathbf{Y}_2|\mathbf{X}_1\mathbf{X}_2}$ is the Gaussian MAC (7.13) with $k = 2$ transmitters. Then there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $\forall\, (\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}) \in \mathbb{R}^{n\otimes 3}$, it holds that*

$$\frac{P_{\mathbf{Y}_2|\mathbf{X}_2}(\mathbf{y}|\mathbf{x}_2)}{P_{\tilde{\mathbf{Y}}_2|\tilde{\mathbf{X}}_2}(\mathbf{y}|\mathbf{x}_2)} \leq \kappa_1(P_1) = 27\sqrt{\frac{\pi}{8}}\frac{1+P_1}{\sqrt{1+2P_1}} \tag{7.37}$$

$$\frac{P_{\mathbf{Y}_2}(\mathbf{y})}{P_{\tilde{\mathbf{Y}}_2}(\mathbf{y})} \le \kappa_2(P_1, P_2) = \frac{9}{2\pi\sqrt{2}} \frac{P_1 + P_2}{\sqrt{P_1 P_2}}. \tag{7.38}$$

*If there is no additive noise* $\mathbf{Z}$ *in* (7.12), (7.38) *continues to hold. Inequalities* (7.37)–(7.38) *are generalized to the* $K$*-transmitter Gaussian MAC as follows.*

2. $K$*-Transmitter MAC: Let* $\mathbf{X}_1, \dots, \mathbf{X}_K$ *be independent, and for each* $i \in [K]$*, let* $\mathbf{X}_i$ *be distributed uniformly on* $\mathbb{S}^n(\sqrt{nP_i})$*. Let* $\tilde{\mathbf{X}}_i \sim \mathcal{N}(\mathbf{0}, P_i \mathsf{I}_n)$ *for* $i \in [K]$*, where* $\mathbf{X}_i$ *are independent of each other. Let* $P_{\mathbf{X}_{[K]}} \to P_{\mathbf{Y}_K|\mathbf{X}_{[K]}} \to P_{\mathbf{Y}_K}$*, and* $P_{\tilde{\mathbf{X}}_{[K]}} \to P_{\mathbf{Y}_K|\mathbf{X}_{[K]}} \to P_{\tilde{\mathbf{Y}}_K}$*, where* $P_{\mathbf{Y}_K|\mathbf{X}_{[K]}}$ *is the Gaussian MAC in* (7.13) *with* $K$ *transmitters. Then there exists* $n_K \in \mathbb{N}$ *such that for all* $n \ge n_K$*, for any* $\mathbf{x}_{[K]} \in \mathbb{R}^{n \otimes K}$*,* $\mathbf{y} \in \mathbb{R}^n$*, and non-empty* $\mathcal{S} \in \overline{\mathcal{P}}([K])$*, it holds that*

$$\frac{P_{\mathbf{Y}_K|\mathbf{X}_{\mathcal{S}^c}}(\mathbf{y}|\mathbf{x}_{\mathcal{S}^c})}{P_{\tilde{\mathbf{Y}}_K|\tilde{\mathbf{X}}_{\mathcal{S}^c}}(\mathbf{y}|\mathbf{x}_{\mathcal{S}^c})} \le \kappa_{|\mathcal{S}|}(P_s : s \in \mathcal{S}), \tag{7.39}$$

*where* $\kappa_{|\mathcal{S}|}(P_s : s \in \mathcal{S})$ *is a constant depending only on the power values* $(P_s : s \in \mathcal{S})$*.*

The proof of (7.39), which is given in [135, eq. (5.138)], relies on a recursive formula for the distribution of $\mathbf{Y}_K$.

Lemma 7.4.2, stated next, bounds the tail probabilities of the chi-squared distribution from above.

**Lemma 7.4.2** (Laurent and Massart **laurent2000Chi**)**.** *Let* $\chi_n^2$ *be a random variable with a chi-squared distribution and* $n$ *degrees of freedom. Then for* $t > 0$*,*

$$\mathbb{P}\left[\chi_n^2 - n \ge 2\sqrt{nt} + 2t\right] \le \exp\{-t\} \tag{7.40}$$

$$\mathbb{P}\left[\chi_n^2 - n \le -2\sqrt{nt}\right] \le \exp\{-t\}. \tag{7.41}$$

Lemma 7.4.3, stated next, is used as the main tool to obtain large deviation bounds on the information density random variables that arise when we apply the RCU bound.

**Lemma 7.4.3** (Tan and Tomamichel [44, eq. (52)])**.** *Let* $\mathbf{Z} = (Z_1, \dots, Z_n) \sim \mathcal{N}(\mathbf{0}, \mathsf{I}_n)$*,* $\mathbf{x} = (\sqrt{nP}, 0, \dots, 0)$*, and let* $s > 0$ *and* $P > 0$ *be constants. Then* *for any $a \in \mathbb{R}$, $\mu > 0$, and $n$ large enough,*

$$\mathbb{P}\left[Z_1 \in \left[\frac{a}{\sqrt{nP}}, \frac{a+\mu}{\sqrt{nP}}\right] \middle| \|\mathbf{x}+\mathbf{Z}\|_2^2 = ns\right] \leq \frac{L(P,s)\mu}{\sqrt{n}}, \tag{7.42}$$

*where*

$$L(P,s) \triangleq \frac{8(Ps)^{3/2}}{\sqrt{2\pi}} \sqrt{\frac{1+4Ps-\sqrt{1+4Ps}}{(\sqrt{1+4Ps}-1)^5}}. \tag{7.43}$$

We state the multidimensional Berry-Esseen theorem for sums of independent but not necessarily identical random vectors. The theorem is used as the main tool to bound the probability that the information density random vector belongs to a given set.

**Theorem 7.4.1** (Bentkus [136])**.** *Let $\mathbf{U}_1, \ldots, \mathbf{U}_n$ be zero mean, independent random vectors in $\mathbb{R}^d$, and let $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{I}_d)$. Denote $\mathbf{S} = \sum_{i=1}^n \mathbf{U}_i$, and $T = \sum_{i=1}^n \mathbb{E}\left[\|\mathbf{U}_i\|^3\right]$. Assume that* $\mathrm{Cov}\left[\mathbf{S}\right] = \mathsf{I}_d$*. Then, there exists a constant $c > 0$ such that*

$$\sup_{\mathcal{A} \in \mathfrak{C}_d} \left|\mathbb{P}\left[\mathbf{S} \in \mathcal{A}\right] - \mathbb{P}[\mathbf{Z} \in \mathcal{A}]\right| \leq c d^{1/4} T, \tag{7.44}$$

*where $\mathfrak{C}_d$ is the set of all convex, Borel measurable subsets of $\mathbb{R}^d$.*

Raič [137, Th. 1.1] establishes that the constant $cd^{1/4}$ in (7.44) can be replaced by $42d^{1/4} + 16$. Tan and Kosut [21] provide the following corollary to Theorem 7.4.1 for the case of a general nonsingular $\mathrm{Cov}\left[\mathbf{S}\right]$.

**Corollary 7.4.1** (Tan and Kosut [21, Corollary 8])**.** *For the setup in Theorem 7.4.1, assume that* $\mathrm{Cov}\left[\mathbf{S}\right] = n\mathsf{V}$*, where $\lambda_{\min}(\mathsf{V}) > 0$ denotes the minimum eigenvalue of $\mathsf{V}$, and $T = \frac{1}{n}\sum_{i=1}^n \mathbb{E}\left[\|\mathbf{U}_i\|^3\right]$. Let $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V})$. Then, there exists a constant $c > 0$ such that*

$$\sup_{\mathcal{A} \in \mathfrak{C}_d} \left|\mathbb{P}\left[\frac{1}{\sqrt{n}}\mathbf{S} \in \mathcal{A}\right] - \mathbb{P}[\mathbf{Z} \in \mathcal{A}]\right| \leq \frac{c d^{1/4} T}{\sqrt{n}\lambda_{\min}(\mathsf{V})^{3/2}}. \tag{7.45}$$

Lemmas 7.4.4 and 7.4.5, below, are used to bound the probability that the information density random vector belongs to a set. The total variation distance between the measures $P_X$ and $P_Y$ on $\mathbb{R}^d$ is defined as

$$\mathrm{TV}(P_X, P_Y) \triangleq \sup_{\mathcal{D} \in \mathbb{R}^d} \left|\mathbb{P}\left[X \in \mathcal{D}\right] - \mathbb{P}\left[Y \in \mathcal{D}\right]\right|$$

$$= \frac{1}{2} \int_{x \in \mathbb{R}^d} |dP_X(x) - dP_Y(x)| \,. \tag{7.46}$$

Lemma 7.4.4, stated next, bounds the total variation distance between two Gaussian vectors.

**Lemma 7.4.4.** *Let $\Sigma_1$ and $\Sigma_2$ be two positive definite $d \times d$ matrices, and let $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in \mathbb{R}^d$ be two constant vectors. Then,*

$$\begin{aligned} &\mathrm{TV}(\mathcal{N}(\boldsymbol{\mu}_1, \Sigma_1), \mathcal{N}(\boldsymbol{\mu}_2, \Sigma_2)) \\ &\leq \frac{2+\sqrt{6}}{4} \left\| \Sigma_1^{-1/2} \Sigma_2 \Sigma_1^{-1/2} - \mathsf{I}_d \right\|_F + \frac{1}{2} \sqrt{(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)^T \Sigma_1^{-1} (\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)}, \end{aligned} \tag{7.47}$$

*where $\|\cdot\|_F$ denotes the Frobenius norm.*

*Proof:* See Appendix F.3. ■

A weaker version of the bound in Lemma 7.4.4 by Devroye *et al.* appears in [138, Th. 1.1]. Like our proof, the proof of [138, Th. 1.1] relies on Pinsker's inequality. We improve the factor in front of the Frobenius norm from 1.5 in [138, Th 1.1] to $\frac{2+\sqrt{6}}{4} \approx 1.113$ by using the result in [139, Th. 1.1] to lower bound the logdeterminant of the matrix $\Sigma_1^{-1/2} \Sigma_2 \Sigma_1^{-1/2} - \mathsf{I}_d$ in (7.47).

Lemma 7.4.5, stated next, gives an upper bound on the total variation distance between the marginal distribution of the first $k$ dimensions of a random variable distributed uniformly on $\mathbb{S}^n(\sqrt{n})$ and the $k$-dimensional standard Gaussian random vector.

**Lemma 7.4.5** (Stam [140, Th. 2])**.** *Let $\mathbf{X} = (X_1, \dots, X_n)$ be distributed uniformly on $\mathbb{S}^n(\sqrt{n})$. Let $\mathbf{X}^{[k]} = (X_1, \dots, X_k)$ contain the first $k$ coordinates of $\mathbf{X}$. Then,*

$$\mathrm{TV}(P_{\mathbf{X}^{[k]}}, \mathcal{N}(\mathbf{0}, \mathsf{I}_k)) \leq n^{\frac{1}{2}k} (n-k-2)^{-\frac{1}{2}k} - 1 \tag{7.48}$$

*for $n > k+2$.*

We use Lemma 7.4.5 with $k = 1$ to approximate the inner product $\langle \mathbf{X}_1, \mathbf{X}_2 \rangle$ by a Gaussian random variable, which facilitates an application of the Berry-Esseen theorem in Section 7.4.6.

The proof of Theorem 7.2.2 relies on a random coding argument and Theorem 7.2.1. The asymptotic analysis of the RCU bound (Theorem 7.2.1) borrows some techniques from the point-to-point case [44].

### 7.4.2 Encoding and Decoding for the MAC

We select the distributions of the independent inputs $\mathbf{X}_1$ and $\mathbf{X}_2$ as the uniform distributions on $\mathbb{S}^n(\sqrt{nP_1})$ and $\mathbb{S}^n(\sqrt{nP_2})$, which are the $n$-dimensional spheres centered at the origin with radii $\sqrt{nP_1}$ and $\sqrt{nP_2}$, respectively. The resulting distribution is

$$P_{\mathbf{X}_1}(\mathbf{x}_1)P_{\mathbf{X}_2}(\mathbf{x}_2) = \frac{\delta(\|\mathbf{x}_1\|_2^2 - nP_1)}{S_n(\sqrt{nP_1})}\frac{\delta(\|\mathbf{x}_2\|_2^2 - nP_2)}{S_n(\sqrt{nP_2})}, \tag{7.49}$$

where $\delta(\cdot)$ is the Dirac delta function, and

$$S_n(r) \triangleq \frac{2\pi^{n/2}}{\Gamma(n/2)} r^{n-1} \tag{7.50}$$

is the surface area of an $n$-dimensional sphere $\mathbb{S}^n(r)$ with radius $r$. We draw $M_1$ codewords i.i.d. from $P_{\mathbf{X}_1}$ and $M_2$ codewords i.i.d. from $P_{\mathbf{X}_2}$, respectively. We denote these by $\mathsf{f}_i(m_i)$ for $m_i \in [M_i]$, $i \in \{1, 2\}$.

In order to use Theorem 7.2.1, the channel $P_{Y_2|X_1X_2}$ is particularized to the two-transmitter Gaussian MAC in (7.13). Upon receiving the output sequence $\mathbf{y}$, the decoder employs a maximum likelihood decoding rule, given by

$$\mathsf{g}(\mathbf{y}) = \begin{cases} (m_1, m_2) & \text{if } \imath_{1,2}(\mathsf{f}_1(m_1), \mathsf{f}_2(m_2); \mathbf{y}) > \imath_{1,2}(\mathsf{f}_1(m_1'), \mathsf{f}_2(m_2'); \mathbf{y}) \\ & \text{for all } (m_1', m_2') \neq (m_1, m_2), (m_1', m_2') \in [M_1] \times [M_2] \\ \text{error} & \text{otherwise.} \end{cases} \tag{7.51}$$

We treat all ties in (7.51) as errors because the probability that two codewords result in exactly the same information density is negligible due to the continuity of the noise. Substituting the transition law of the Gaussian MAC (7.13) and the uniform input distributions on the power spheres (7.49) into (7.5a)–(7.5c), we compute for any $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}) \in \mathbb{R}^{n\otimes 3}$

$$\begin{aligned} \imath_1(\mathbf{x}_1; \mathbf{y}|\mathbf{x}_2) &= \frac{n}{2}\log\frac{1}{2\pi} + \langle \mathbf{y} - \mathbf{x}_2, \mathbf{x}_1\rangle - \frac{\|\mathbf{y} - \mathbf{x}_2\|_2^2}{2} \\ &\quad - \frac{nP_1}{2} - \log P_{\mathbf{Y}_2|\mathbf{X}_2}(\mathbf{y}|\mathbf{x}_2) \qquad (7.52) \\ \imath_2(\mathbf{x}_2; \mathbf{y}|\mathbf{x}_1) &= \frac{n}{2}\log\frac{1}{2\pi} + \langle \mathbf{y} - \mathbf{x}_1, \mathbf{x}_2\rangle - \frac{\|\mathbf{y} - \mathbf{x}_1\|_2^2}{2} \\ &\quad - \frac{nP_2}{2} - \log P_{\mathbf{Y}_2|\mathbf{X}_1}(\mathbf{y}|\mathbf{x}_1) \qquad (7.53) \\ \imath_{1,2}(\mathbf{x}_1, \mathbf{x}_2; \mathbf{y}) &= \frac{n}{2}\log\frac{1}{2\pi} + \langle \mathbf{y}, \mathbf{x}_1 + \mathbf{x}_2\rangle - \frac{\|\mathbf{y}\|_2^2}{2} \end{aligned}$$

$$-\frac{\|\mathbf{x}_1+\mathbf{x}_2\|_2^2}{2}-\log P_{\mathbf{Y}_2}(\mathbf{y}). \tag{7.54}$$

Observe that for each $\mathbf{x}_2$ and $\mathbf{y}$, $\imath_1(\mathbf{x}_1;\mathbf{y}|\mathbf{x}_2)$ depends on $\mathbf{x}_1$ only through the inner product $\langle \mathbf{y}-\mathbf{x}_2,\mathbf{x}_1\rangle$, and for each $\mathbf{y}$, $\imath_{1,2}(\mathbf{x}_1,\mathbf{x}_2;\mathbf{y})$ depends on $(\mathbf{x}_1,\mathbf{x}_2)$ only through $\langle \mathbf{y},\mathbf{x}_1+\mathbf{x}_2\rangle-\langle \mathbf{x}_1,\mathbf{x}_2\rangle$. By the input-output relation in (7.12), the conditional information density for two transmitters, $\imath_1(\mathbf{x}_1;\mathbf{y}|\mathbf{x}_2)$, can be reduced to the unconditional information density for a single transmitter as

$$\imath_1(\mathbf{x}_1;\mathbf{y}|\mathbf{x}_2)=\imath_1(\mathbf{x}_1;\mathbf{y}-\mathbf{x}_2)\triangleq\log\frac{P_{\mathbf{Y}_1|\mathbf{X}_1}(\mathbf{y}-\mathbf{x}_2|\mathbf{x}_1)}{P_{\mathbf{Y}_1}(\mathbf{y}-\mathbf{x}_2)}, \tag{7.55}$$

where $\mathbf{Y}_1=\mathbf{X}_1+\mathbf{Z}$ is the output of the channel with a single transmitter.

### 7.4.3 Typical Set for the MAC

For the rest of the proof, $\mathbf{Z}\sim\mathcal{N}(\mathbf{0},\mathsf{I}_n)$ denotes the Gaussian noise, which is independent of the channel inputs $\mathbf{X}_1$ and $\mathbf{X}_2$. Note that the expectations of the squared norms of $\mathbf{X}_1+\mathbf{Z},\mathbf{X}_2+\mathbf{Z}$ and $\mathbf{Y}_2$ are $n(1+P_1),n(1+P_2)$, and $n(1+P_1+P_2)$, respectively. We define a typical set for vector $(\mathbf{X}_1+\mathbf{Z},\mathbf{X}_2+\mathbf{Z},\mathbf{Y}_2)$ by

$$\mathcal{F}\triangleq\bigtimes_{\mathcal{S}\in\overline{\mathcal{P}}([2])}\mathcal{F}(\mathcal{S})\subseteq\mathbb{R}^{n\otimes 3}, \tag{7.56}$$

where

$$\mathcal{F}(\mathcal{S})\triangleq\left\{\mathbf{x}_{\langle\mathcal{S}\rangle}+\mathbf{z}\in\mathbb{R}^n\colon\frac{1}{n}\left\|\mathbf{x}_{\langle\mathcal{S}\rangle}+\mathbf{z}\right\|_2^2\in\mathcal{I}(\mathcal{S})\right\} \tag{7.57}$$

$$\mathcal{I}(\mathcal{S})\triangleq[1+P_{\langle\mathcal{S}\rangle}-n^{-1/3},1+P_{\langle\mathcal{S}\rangle}+n^{-1/3}]. \tag{7.58}$$

We next show that for $n$ large enough,

$$\mathbb{P}\left[(\mathbf{X}_1+\mathbf{Z},\mathbf{X}_2+\mathbf{Z},\mathbf{Y}_2)\notin\mathcal{F}\right]\leq\exp\{-c_2n^{1/3}\}, \tag{7.59}$$

where $c_2>0$ is a constant.

To bound the probability that the triplet $(\mathbf{X}_1+\mathbf{Z},\mathbf{X}_2+\mathbf{Z},\mathbf{Y}_2)$ does not belong to the typical set $\mathcal{F}$, we use Lemma 7.4.1 to approximate the squared norms $\|\mathbf{X}_1+\mathbf{Z}\|_2^2$, $\|\mathbf{X}_2+\mathbf{Z}\|_2^2$, and $\|\mathbf{Y}_2\|_2^2$ by multiples of chi-squared distributed random variables with $n$ degrees of freedom. We then use Lemma 7.4.2 to bound the two-sided tail probability of these chi-squared distributed random variables. Weakening the upper bound (7.40) in Lemma 7.4.2 using

$2\sqrt{2nt} \geq 2\sqrt{nt} + 2t$ for $0 < t \leq \frac{n}{8} \leq (3 - 2\sqrt{2})n$, we get the following concentration inequalities for the squared norms of the random vectors $\mathbf{X}_1 + \mathbf{Z}$ and $\mathbf{Y}_2$

$$\mathbb{P}\left[\left|\|\mathbf{X}_1 + \mathbf{Z}\|_2^2 - n(1 + P_1)\right| > nt_1\right] \leq 2\kappa_1(P_1) \exp\left\{-\frac{nt_1^2}{8(1 + P_1)^2}\right\} \tag{7.60}$$

$$\mathbb{P}\left[\left|\|\mathbf{Y}_2\|_2^2 - n(1 + P_1 + P_2)\right| > nt_2\right] \leq 2\kappa_2(P_1, P_2) \exp\left\{-\frac{nt_2^2}{8(1 + P_1 + P_2)^2}\right\} \tag{7.61}$$

for $t_1 \in (0, 1 + P_1)$, and $t_2 \in (0, 1 + P_1 + P_2)$, where $\kappa_1(P_1)$ and $\kappa_2(P_1, P_2)$ are constants defined in Lemma 7.4.1. We deduce (7.59) by the union bound and setting $t_1 = t_2 = n^{-1/3}$ in (7.60)–(7.61).

### 7.4.4 A Large Deviation Bound on the Mutual Information Random Variables

We introduce the following functions that are analogous to the one used in the point-to-point channel in [44, eq. (27)]

$$g_1(t; \mathbf{y}, \mathbf{x}_2) \triangleq \mathbb{P}\left[\imath_1(\overline{\mathbf{X}}_1; \mathbf{Y}_2|\mathbf{X}_2) \geq t \mid \mathbf{X}_2 = \mathbf{x}_2, \mathbf{Y}_2 = \mathbf{y}\right] \tag{7.62}$$

$$g_2(t; \mathbf{y}, \mathbf{x}_1) \triangleq \mathbb{P}\left[\imath_2(\overline{\mathbf{X}}_2; \mathbf{Y}_2|\mathbf{X}_1) \geq t \mid \mathbf{X}_1 = \mathbf{x}_1, \mathbf{Y}_2 = \mathbf{y}\right] \tag{7.63}$$

$$g_{1,2}(t; \mathbf{y}) \triangleq \mathbb{P}\left[\imath_{1,2}(\overline{\mathbf{X}}_1, \overline{\mathbf{X}}_2; \mathbf{Y}_2) \geq t \mid \mathbf{Y}_2 = \mathbf{y}\right], \tag{7.64}$$

where

$$\begin{aligned} &P_{\mathbf{X}_1\mathbf{X}_2\overline{\mathbf{X}}_1\overline{\mathbf{X}}_2\mathbf{Y}_2}(\mathbf{x}_1, \mathbf{x}_2, \overline{\mathbf{x}}_1, \overline{\mathbf{x}}_2, \mathbf{y}) \\ &= P_{\mathbf{X}_1}(\mathbf{x}_1) P_{\mathbf{X}_2}(\mathbf{x}_2) P_{\mathbf{X}_1}(\overline{\mathbf{x}}_1) P_{\mathbf{X}_2}(\overline{\mathbf{x}}_2) P_{\mathbf{Y}_2|\mathbf{X}_1\mathbf{X}_2}(\mathbf{y}|\mathbf{x}_1, \mathbf{x}_2). \end{aligned}$$

The following lemma, which generalizes [44, eq. (53)] to the Gaussian MAC, gives upper bounds on these functions. We use Lemma 7.4.6 in the evaluation of the RCU bound.

**Lemma 7.4.6.** *Let* $(\mathbf{y} - \mathbf{x}_2, \mathbf{y} - \mathbf{x}_1, \mathbf{y}) \in \mathcal{F}$*, where the set* $\mathcal{F}$ *is defined in* (7.56)*. Then, for* $n$ *large enough,*

$$g_1(t; \mathbf{y}, \mathbf{x}_2) \leq \frac{G_1 \exp\{-t\}}{\sqrt{n}} \tag{7.65a}$$

$$g_2(t; \mathbf{y}, \mathbf{x}_1) \leq \frac{G_2 \exp\{-t\}}{\sqrt{n}} \tag{7.65b}$$

$$g_{1,2}(t; \mathbf{y}) \leq \frac{G_{1,2} \exp\{-t\}}{\sqrt{n}}, \tag{7.65c}$$

*where $G_1, G_2$, and $G_{1,2}$ are positive constants depending only on $P_1, P_2$, and $(P_1, P_2)$, respectively.*

*Proof:* The bounds in (7.65a) and (7.65b) follow from the equivalence (stated in (7.55)) between the conditional information density for two transmitters and the unconditional information density for a single transmitter combined with the analysis in [44, Sec. IV-E]. The constants in (7.65a) and (7.65b) are

$$G_i = (3\log 2)L(P_i, 1+P_i), \quad i \in \{1,2\}, \tag{7.66}$$

where $L(\cdot,\cdot)$ is the function defined in (7.43).

Bounding the function $g_{1,2}(t;\mathbf{y})$ is more challenging. While $\|\mathbf{X}_1\|_2^2$ is a constant under the uniform distribution on a power sphere, $\|\mathbf{X}_1+\mathbf{X}_2\|_2^2$ is not. The proof of (7.65c) follows steps similar to [44, Sec. IV-E]. First, we change the measure from $P_{\mathbf{X}_1}P_{\mathbf{X}_2}P_{\mathbf{Y}_2}$ to $P_{\mathbf{X}_1}P_{\mathbf{X}_2}P_{\mathbf{Y}_2|\mathbf{X}_1\mathbf{X}_2}$ to get

$$g_{1,2}(t;\mathbf{y}) = \mathbb{E}[\exp\{-\imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2)\}1\{\imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2)\geq t\} \mid \mathbf{Y}_2 = \mathbf{y}]. \tag{7.67}$$

To bound (7.67), we define function $h_{1,2}(\mathbf{y};a,\mu)$ for constants $a\in\mathbb{R}$ and $\mu>0$ as

$$\begin{aligned}
&h_{1,2}(\mathbf{y};a,\mu)\\
&\triangleq \mathbb{P}\left[\imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2)\in[a,a+\mu]\middle|\mathbf{Y}_2=\mathbf{y}\right] && (7.68)\\
&= \mathbb{P}\left[\langle\mathbf{X}_1+\mathbf{X}_2,\mathbf{Y}_2\rangle - \frac{\|\mathbf{X}_1+\mathbf{X}_2\|_2^2}{2}\in[a',a'+\mu]\middle|\mathbf{Y}_2=\mathbf{y}\right], && (7.69)
\end{aligned}$$

where $a'$ is shifted from $a$ by some amount depending on $\mathbf{y}$, and (7.69) follows from (7.54). By spherical symmetry of the distribution of $\mathbf{Y}_2$, (7.69) depends on $\mathbf{y}$ only through its norm $\|\mathbf{y}\|_2$. We have

$$\begin{aligned}
h_{1,2}(s;a,\mu) &\triangleq h_{1,2}(\mathbf{y};a,\mu)\\
&= \mathbb{P}\left[\langle\mathbf{X}_1+\mathbf{X}_2,\mathbf{Y}_2\rangle - \frac{\|\mathbf{X}_1+\mathbf{X}_2\|_2^2}{2}\in[a',a'+\mu]\;\middle|\;\|\mathbf{Y}_2\|_2^2=ns\right],
\end{aligned} \tag{7.70}$$

where $\|\mathbf{y}\|_2^2 = ns$, and $s\in\mathcal{I}([2])$, and $\mathcal{I}(\mathcal{S})$ is defined in (7.58). Recall that the support of the norm $\|\mathbf{X}_1+\mathbf{X}_2\|_2^2$ is $[n(\sqrt{P_1}-\sqrt{P_2})^2, n(\sqrt{P_1}+\sqrt{P_2})^2]$. To avoid the cases where $\|\mathbf{X}_1+\mathbf{X}_2\|_2^2$ is too small, we separate the probability term (7.70) according to whether or not the event

$$\mathcal{B} = \left\{\|\mathbf{X}_1+\mathbf{X}_2\|_2^2 < n(P_1+P_2-\sqrt{P_1P_2})\right\} \tag{7.71}$$

occurs under the condition that $\|\mathbf{Y}_2\|_2^2 = ns$. Here, the choice $\sqrt{P_1 P_2}$ is arbitrary and can be replaced by any constant in $(0, 2\sqrt{P_1 P_2})$.

In (7.70), conditioning on the event $\mathcal{B}$ and then bounding the corresponding probability terms by 1 gives

$$\begin{aligned} h_{1,2}(s; a, \mu) \leq \mathbb{P}&\left[\mathcal{B} \,\middle|\, \|\mathbf{Y}_2\|_2^2 = ns\right] \\ &+ \mathbb{P}\left[\langle \mathbf{X}_1 + \mathbf{X}_2, \mathbf{Y}_2 \rangle - \frac{\|\mathbf{X}_1 + \mathbf{X}_2\|_2^2}{2} \in [a', a' + \mu] \,\middle|\, \|\mathbf{Y}_2\|_2^2 = ns, \mathcal{B}^c\right]. \end{aligned} \tag{7.72}$$

For $n$ large enough, we bound the first term on the right-hand side of (7.72) by

$$\mathbb{P}\left[\mathcal{B} \,\middle|\, \|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|_2^2 = ns\right] \leq \exp\{-nC\}, \tag{7.73}$$

where $C > 0$ is a constant. The proof of (7.73) appears in Appendix F.4.

By spherical symmetry, the distribution of $\langle \mathbf{X}_1 + \mathbf{X}_2, \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z} \rangle$ depends on $\mathbf{X}_1 + \mathbf{X}_2$ only through the norm $\|\mathbf{X}_1 + \mathbf{X}_2\|_2$. Therefore, fixing $\mathbf{X}_1 + \mathbf{X}_2$ to $\mathbf{x} = (\sqrt{nu}, 0, \ldots, 0)$, we find that for any $u \in [P_1 + P_2 - \sqrt{P_1 P_2}, (\sqrt{P_1} + \sqrt{P_2})^2]$, $s \in \mathcal{I}([2])$, and $n$ large enough,

$$\begin{aligned} \mathbb{P}&\Bigg[\langle \mathbf{X}_1 + \mathbf{X}_2, \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z} \rangle - \frac{nu}{2} \in [a', a' + \mu] \\ &\quad \Bigg| \; \|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|_2^2 = ns, \|\mathbf{X}_1 + \mathbf{X}_2\|_2^2 = nu\Bigg] \\ &= \mathbb{P}\left[Z_1 + \frac{\sqrt{nu}}{2} \in \left[\frac{a'}{\sqrt{nu}}, \frac{a' + \mu}{\sqrt{nu}}\right] \,\middle|\, \|\mathbf{x} + \mathbf{Z}\|_2^2 = ns\right] && (7.74) \\ &\leq \frac{L(u, s)\mu}{\sqrt{n}} && (7.75) \\ &\leq \frac{3}{2}\frac{L(u, 1 + P_1 + P_2)\mu}{\sqrt{n}}, && (7.76) \end{aligned}$$

where (7.75) follows by Lemma 7.4.3, and (7.76) holds for $n$ large enough by the continuity of the map $s \mapsto L(u, s)$ since $s \in \mathcal{I}([2])$. Using (7.76), we bound the second term in (7.72) as

$$\begin{aligned} \mathbb{P}&\Bigg[\langle \mathbf{X}_1 + \mathbf{X}_2, \mathbf{Y}_2 \rangle - \frac{\|\mathbf{X}_1 + \mathbf{X}_2\|_2^2}{2} \in [a', a' + \mu] \\ &\quad \Bigg| \; \|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|_2^2 = ns, \mathcal{B}^c\Bigg] \\ &\leq \max_{u \in [P_1 + P_2 - \sqrt{P_1 P_2}, (\sqrt{P_1} + \sqrt{P_2})^2]} \frac{3\mu L(u, 1 + P_1 + P_2)}{2\sqrt{n}}. \end{aligned} \tag{7.77}$$

By (7.72), (7.73), (7.77), and because $L(u, 1+P_1+P_2)$ is bounded above for $u \in [P_1+P_2-\sqrt{P_1P_2}, (\sqrt{P_1}+\sqrt{P_2})^2]$, there exists a constant $K_2(P_1, P_2) > 0$ such that

$$h_{1,2}(s; a, \mu) \leq K_2(P_1, P_2)\frac{\mu}{\sqrt{n}} \tag{7.78}$$

for $n$ large enough. By following the same steps as [44, eq. (55)-(57)], we conclude that

$$g_{1,2}(t; \mathbf{y}) \leq \frac{G_{1,2}\exp\{-t\}}{\sqrt{n}}, \tag{7.79}$$

where $G_{1,2} = (2\log 2)K_2(P_1, P_2)$.

■

### 7.4.5 Evaluating the RCU Bound for the MAC

We here bound the right-hand side of (7.8) in Theorem 7.2.1. The information density random vector is defined as

$$\boldsymbol{\imath}_2 \triangleq \begin{bmatrix} \imath_1(\mathbf{X}_1; \mathbf{Y}_2|\mathbf{X}_2) \\ \imath_2(\mathbf{X}_2; \mathbf{Y}_2|\mathbf{X}_1) \\ \imath_{1,2}(\mathbf{X}_1, X_2; \mathbf{Y}_2) \end{bmatrix}, \tag{7.80}$$

where $\mathbf{X}_1$ and $\mathbf{X}_2$ are distributed according to (7.49), and $P_{\mathbf{X}_1}P_{\mathbf{X}_2} \to P_{\mathbf{Y}_2|\mathbf{X}_1+\mathbf{X}_2} \to P_{\mathbf{Y}_2}$.

Define the typical events

$$\mathcal{E}(\mathcal{S}) \triangleq \left\{\mathbf{X}_{\langle\mathcal{S}\rangle} + \mathbf{Z} \in \mathcal{F}(\mathcal{S})\right\} \tag{7.81}$$

$$\mathcal{E} \triangleq \bigcap_{\mathcal{S}\in\overline{\mathcal{P}}([2])} \mathcal{E}(\mathcal{S}) \tag{7.82}$$

$$\mathcal{A} \triangleq \left\{ \boldsymbol{\imath}_2 \geq \log \begin{bmatrix} M_1(G_1)^2\alpha_1 \\ M_2(G_2)^2\alpha_1 \\ M_1M_2(G_{1,2})^2\alpha_2 \end{bmatrix} - \frac{1}{2}\log n\mathbf{1} \right\}, \tag{7.83}$$

where $G_1$, $G_2$ and $G_{1,2}$ are the constants given in (7.65), $\mathcal{F}(\mathcal{S})$ is defined in (7.57), and

$$\alpha_s \triangleq 2\binom{2}{s}, \quad s = 1, 2. \tag{7.84}$$

Denote for brevity

$$g_1 \triangleq g_1(\imath_1(\mathbf{X}_1; \mathbf{Y}_2|\mathbf{X}_2); \mathbf{Y}_2, \mathbf{X}_2) \tag{7.85a}$$

$$g_2 \triangleq g_2(\imath_2(\mathbf{X}_2; \mathbf{Y}_2|\mathbf{X}_1); \mathbf{Y}_2, \mathbf{X}_1) \tag{7.85b}$$

$$g_{1,2} \triangleq g_{1,2}(\imath_{1,2}(\mathbf{X}_1, \mathbf{X}_2; \mathbf{Y}_2); \mathbf{Y}_2), \tag{7.85c}$$

where $g_1(\cdot), g_2(\cdot)$, and $g_{1,2}(\cdot)$, are defined in (7.62)–(7.64).

The right-hand side of (7.8) is bounded in (7.86)–(7.90) at the top of the next page. Here, $c_2$ is the positive constant defined in (7.59). Equality (7.86) follows from the definitions of the functions $g_1(t; \mathbf{y}, \mathbf{x}_2)$ and $g_{1,2}(t; \mathbf{y})$ and splitting the expectation into two cases according to whether the event $\{\mathcal{A}^c \cup \mathcal{E}^c\}$ occurs or not. Inequality (7.87) follows by bounding the minimum inside the first expectation in (7.86) by 1; bounding the minimum inside the second expectation in (7.86) by its second argument; writing the indicator function $1\{\mathcal{A} \cap \mathcal{E}\}$ as a multiplication of 3 indicator functions using the definitions in (7.82) and (7.83) and distributing that multiplication over the summation. Inequality (7.88) follows from Lemma 7.4.6 and by bounding the probability terms by 1. Inequality (7.89) is obtained by applying the union bound to $\mathbb{P}[\mathcal{A}^c \cup \mathcal{E}^c]$ and by using Lemma 7.4.6 with $t = \log \frac{M_1 (G_1)^2 \alpha_1}{\sqrt{n}}$, $t = \log \frac{M_2 (G_2)^2 \alpha_1}{\sqrt{n}}$, and $t = \log \frac{M_1 M_2 (G_{1,2})^2 \alpha_2}{\sqrt{n}}$ to bound the three remaining terms, respectively. Inequality (7.90) follows from (7.59).

### 7.4.6 A Multidimensional Berry-Esseen Type Inequality

To complete the proof of Theorem 7.2.2, it remains only to evaluate the probability $\mathbb{P}[\mathcal{A}^c]$ in (7.90). If the operational rate pair $\left(\frac{\log M_1}{n}, \frac{\log M_2}{n}\right)$ does not lie at a corner point of the achievable capacity region, applying the union bound to $\mathbb{P}[\mathcal{A}^c]$ gives a tight achievability bound since two of the three probability terms that appear after applying the union bound to $\mathbb{P}[\mathcal{A}^c]$ are $O\left(\frac{1}{\sqrt{n}}\right)$. However, for the corner points, $\mathbb{P}[\mathcal{A}^c]$ needs to be bounded without using the union bound in order to obtain a tighter achievability bound (see [135, Sec. 5.1.1]). In this section, we bound $\mathbb{P}[\mathcal{A}^c]$ jointly by deriving a multidimensional Berry-Esseen type inequality.

Due to the non-i.i.d. input distribution, the random vector $\boldsymbol{\imath}_2$ cannot be separated into a sum of $n$ random vectors. Therefore, to approximate $\boldsymbol{\imath}_2$, we define the modified conditional and unconditional information densities whose denominators have Gaussian distributions corresponding to

$$\tilde{\imath}_1(\mathbf{x}_1; \mathbf{y}|\mathbf{x}_2) \triangleq \sum_{i=1}^{n} \log \frac{P_{Y_2|X_1X_2}(y_i|x_{1i}, x_{2i})}{P_{\tilde{Y}_2|\tilde{X}_2}(y_i|x_{2i})} \tag{7.91a}$$

$$
\begin{aligned}
&\mathbb{E}\Big[\min\Big\{1, (M_1-1)\mathbb{P}\left[\imath_1(\overline{\mathbf{X}}_1;\mathbf{Y}_2|\mathbf{X}_2) \geq \imath_1(\mathbf{X}_1;\mathbf{Y}_2|\mathbf{X}_2) \mid \mathbf{X}_1,\mathbf{X}_2,\mathbf{Y}_2\right]\\
&+(M_2-1)\mathbb{P}\left[\imath_2(\overline{\mathbf{X}}_2;\mathbf{Y}_2|\mathbf{X}_1) \geq \imath_2(\mathbf{X}_2;\mathbf{Y}_2|\mathbf{X}_1) \mid \mathbf{X}_1,\mathbf{X}_2,\mathbf{Y}_2\right]\\
&+(M_1-1)(M_2-1)\mathbb{P}\left[\imath_{1,2}(\overline{\mathbf{X}}_1,\overline{\mathbf{X}}_2;\mathbf{Y}_2) \geq \imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2) \mid \mathbf{X}_1,\mathbf{X}_2,\mathbf{Y}_2\right]\Big\}\Big]\\
&=\mathbb{E}\Big[\min\Big\{1,(M_1-1)g_1+(M_2-1)g_2+(M_1-1)(M_2-1)g_{1,2}\Big\}1\left\{\mathcal{A}^c\cup\mathcal{E}^c\right\}\Big]\\
&+\mathbb{E}\Big[\min\Big\{1,(M_1-1)g_1+(M_2-1)g_2+(M_1-1)(M_2-1)g_{1,2}\Big\}1\left\{\mathcal{A}\cap\mathcal{E}\right\}\Big]
\end{aligned}
\tag{7.86}
$$

$$
\begin{aligned}
&\leq \mathbb{P}\left[\mathcal{A}^c\cup\mathcal{E}^c\right]\\
&+\mathbb{P}\left[\mathcal{E}(\{1\})\right]\ M_1\,\mathbb{E}\left[g_1 1\left\{\imath_1(\mathbf{X}_1;\mathbf{Y}_2|\mathbf{X}_2)\geq\log\frac{M_1(G_1)^2\alpha_1}{\sqrt{n}}\right\}\,\middle|\,\mathcal{E}(\{1\})\right]\\
&+\mathbb{P}\left[\mathcal{E}(\{2\})\right]\ M_2\,\mathbb{E}\left[g_2 1\left\{\imath_2(\mathbf{X}_2;\mathbf{Y}_2|\mathbf{X}_1)\geq\log\frac{M_2(G_2)^2\alpha_1}{\sqrt{n}}\right\}\,\middle|\,\mathcal{E}(\{2\})\right]\\
&+\mathbb{P}\left[\mathcal{E}(\{1,2\})\right]\ M_1M_2\\
&\cdot\ \mathbb{E}\left[g_{1,2}1\left\{\imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2)\geq\log\frac{M_1M_2(G_{1,2})^2\alpha_2}{\sqrt{n}}\right\}\,\middle|\,\mathcal{E}(\{1,2\})\right]
\end{aligned}
\tag{7.87}
$$

$$
\begin{aligned}
&\leq \mathbb{P}\left[\mathcal{A}^c\cup\mathcal{E}^c\right]+\frac{M_1G_1}{\sqrt{n}}\mathbb{E}\Big[\exp\{-\imath_1(\mathbf{X}_1;\mathbf{Y}_2|\mathbf{X}_2)\}\\
&\quad 1\left\{\imath_1(\mathbf{X}_1;\mathbf{Y}_2|\mathbf{X}_2)\geq\log\frac{M_1(G_1)^2\alpha_1}{\sqrt{n}}\right\}\,\Big|\,\mathcal{E}(\{1\})\Big]\\
&+\frac{M_2G_2}{\sqrt{n}}\mathbb{E}\Big[\exp\{-\imath_2(\mathbf{X}_2;\mathbf{Y}_2|\mathbf{X}_1)\}\\
&\quad 1\left\{\imath_2(\mathbf{X}_2;\mathbf{Y}_2|\mathbf{X}_1)\geq\log\frac{M_2(G_2)^2\alpha_1}{\sqrt{n}}\right\}\,\Big|\,\mathcal{E}(\{2\})\Big]\\
&+\frac{M_1M_2G_{1,2}}{\sqrt{n}}\mathbb{E}\Big[\exp\{-\imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2)\}\\
&\quad 1\Big\{\imath_{1,2}(\mathbf{X}_1,\mathbf{X}_2;\mathbf{Y}_2)\geq\log\frac{M_1M_2(G_{1,2})^2\alpha_2}{\sqrt{n}}\Big]\Big\}\,|\mathcal{E}(\{1,2\})\Big]
\end{aligned}
\tag{7.88}
$$

$$
\leq \mathbb{P}\left[\mathcal{A}^c\right]+\mathbb{P}\left[\mathcal{E}^c\right]+\frac{\frac{2}{\alpha_1}+\frac{1}{\alpha_2}}{\sqrt{n}} \tag{7.89}
$$

$$
\leq \mathbb{P}\left[\mathcal{A}^c\right]+\exp\left\{-c_2n^{1/3}\right\}+\frac{1}{\sqrt{n}} \tag{7.90}
$$

$$
\tilde{\imath}_2(\mathbf{x}_2;\mathbf{y}|\mathbf{x}_1)\triangleq\sum_{i=1}^{n}\log\frac{P_{Y_2|X_1X_2}(y_i|x_{1i},x_{2i})}{P_{\tilde{Y}_2|\tilde{X}_1}(y_i|x_{1i})} \tag{7.91b}
$$

$$
\tilde{\imath}_{1,2}(\mathbf{x}_1,\mathbf{x}_2;\mathbf{y})\triangleq\sum_{i=1}^{n}\log\frac{P_{Y_2|X_1X_2}(y_i|x_{1i},x_{2i})}{P_{\tilde{Y}_2}(y_i)}, \tag{7.91c}
$$

where $\tilde{X}_i \sim \mathcal{N}(0, P_i)$, $i \in [2]$, and $P_{\tilde{X}_1} P_{\tilde{X}_2} \to P_{Y_2|X_1X_2} \to P_{\tilde{Y}_2} = \mathcal{N}(0, 1 + P_1 + P_2)$. Denote the modified and centered information density random vector by

$$\tilde{\boldsymbol{\imath}}_2 \triangleq \frac{1}{\sqrt{n}} \left( \begin{bmatrix} \tilde{\imath}_1(\mathbf{X}_1; \mathbf{Y}_2 | \mathbf{X}_2) \\ \tilde{\imath}_2(\mathbf{X}_2; \mathbf{Y}_2 | \mathbf{X}_1) \\ \tilde{\imath}_{1,2}(\mathbf{X}_1, \mathbf{X}_2; \mathbf{Y}_2) \end{bmatrix} - n\mathbf{C}(P_1, P_2) \right), \tag{7.92}$$

where $\mathbf{C}(P_1, P_2) = \frac{1}{n}\mathbb{E}\left[\boldsymbol{\imath}_2\right]$ is the capacity vector defined in (7.16). Define the threshold vector

$$\boldsymbol{\tau} \triangleq \log \begin{bmatrix} M_1 (G_1)^2 \kappa_1(P_1) \alpha_1 \\ M_2 (G_2)^2 \kappa_1(P_2) \alpha_1 \\ M_1 M_2 (G_{1,2})^2 \kappa_2(P_1, P_2) \alpha_2 \end{bmatrix} - \frac{1}{2} \log n \mathbf{1} - n\mathbf{C}(P_1, P_2). \tag{7.93}$$

Our method to bound the probability $\mathbb{P}\left[\mathcal{A}^c\right]$ involves 5 steps.

**Step 1:** We first replace $\boldsymbol{\imath}_2$ by $\tilde{\boldsymbol{\imath}}_2$. Unlike $\boldsymbol{\imath}_2$, $\tilde{\boldsymbol{\imath}}_2$ can be written as a sum of $n$ dependent random vectors. Prior uses of this approach include [44, eq. (65)] for the point-to-point channel and [24, eq. (2)] for the MAC. We then bound $\mathbb{P}\left[\mathcal{A}^c\right]$ in terms of the modified information density random vector $\tilde{\boldsymbol{\imath}}_2$. By (7.83) and Lemma 7.4.1,

$$\begin{aligned} \mathbb{P}\left[\mathcal{A}^c\right] &= 1 - \mathbb{P}\left[ \boldsymbol{\imath}_2 - \mathbb{E}\left[\boldsymbol{\imath}_2\right] \geq \left( \boldsymbol{\tau} - \log \begin{bmatrix} \kappa_1(P_1) \\ \kappa_1(P_2) \\ \kappa_2(P_1, P_2) \end{bmatrix} \right) \right] && (7.94) \\ &\leq 1 - \mathbb{P}\left[ \tilde{\boldsymbol{\imath}}_2 \geq \frac{1}{\sqrt{n}} \boldsymbol{\tau} \right]. && (7.95) \end{aligned}$$

From (7.91a)–(7.91c), we see that

$$\tilde{\boldsymbol{\imath}}_2 \sim \frac{1}{\sqrt{n}} \begin{bmatrix} \frac{(n - \|\mathbf{Z}\|_2^2) P_1 + 2\langle \mathbf{X}_1, \mathbf{Z} \rangle}{2(1 + P_1)} \\ \frac{(n - \|\mathbf{Z}\|_2^2) P_2 + 2\langle \mathbf{X}_2, \mathbf{Z} \rangle}{2(1 + P_2)} \\ \frac{(n - \|\mathbf{Z}\|_2^2)(P_1 + P_2) + 2\langle \mathbf{X}_1, \mathbf{X}_2 \rangle + 2\langle \mathbf{Z}, \mathbf{X}_1 + \mathbf{X}_2 \rangle}{2(1 + P_1 + P_2)} \end{bmatrix}. \tag{7.96}$$

Although the right-hand side of (7.96) is not a sum of $n$ independent random vectors, the conditional distribution of $\tilde{\boldsymbol{\imath}}_2$ given $(\mathbf{X}_1, \mathbf{X}_2)$ is such a sum. Therefore, the multidimensional Berry-Esseen theorem is applicable to the corresponding conditional probability. In the remainder of Step 1, we detail the distribution of $\tilde{\boldsymbol{\imath}}_2$.

By spherical symmetry, the conditional distribution of $\tilde{\boldsymbol{\imath}}_2$ given $(\mathbf{X}_1, \mathbf{X}_2) = (\mathbf{x}_1, \mathbf{x}_2)$ depends on $(\mathbf{x}_1, \mathbf{x}_2)$ only through the inner product $\langle \mathbf{x}_1, \mathbf{x}_2 \rangle$ given that each squared norm satisfies $\|\mathbf{x}_i\|_2^2 = nP_i$, $i \in [2]$. Define the normalized inner product random variable

$$H \triangleq \frac{\langle \mathbf{X}_1, \mathbf{X}_2 \rangle}{\sqrt{nP_1P_2}}, \tag{7.97}$$

and set

$$\mathbf{x}_1 = (\sqrt{nP_1}, 0, \ldots, 0) \tag{7.98}$$

$$\mathbf{x}_2 = (h\sqrt{P_2}, \sqrt{(n-h^2)P_2}, 0, \ldots, 0) \tag{7.99}$$

for some $h \in [-\sqrt{n}, \sqrt{n}]$, which satisfy

$$\frac{\langle \mathbf{x}_1, \mathbf{x}_2 \rangle}{\sqrt{nP_1P_2}} = h. \tag{7.100}$$

Putting (7.98)–(7.99) into (7.96) gives that the conditional distribution of $\tilde{\boldsymbol{\imath}}_2$ given $H = h$ equals the conditional distribution of $\tilde{\boldsymbol{\imath}}_2$ given $(\mathbf{X}_1, \mathbf{X}_2) = (\mathbf{x}_1, \mathbf{x}_2)$, which equals the conditional distribution of the random variable

$$\boldsymbol{\mu}(h) + \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \mathbf{J}_i(h), \tag{7.101}$$

where

$$\boldsymbol{\mu}(h) \triangleq \mathbb{E}\left[\tilde{\boldsymbol{\imath}}_2 | H = h\right] = h \begin{bmatrix} 0 \\ 0 \\ \frac{\sqrt{P_1P_2}}{1+P_1+P_2} \end{bmatrix} \tag{7.102}$$

$$\mathbf{J}_i(h) \triangleq \begin{bmatrix} \frac{(1-Z_i^2)P_1 + 2x_{1i}Z_i}{2(1+P_1)} \\ \frac{(1-Z_i^2)P_2 + 2x_{2i}Z_i}{2(1+P_2)} \\ \frac{(1-Z_i^2)(P_1+P_2) + 2(x_{1i}+x_{2i})Z_i}{2(1+P_1+P_2)} \end{bmatrix}, \quad i \in [n]. \tag{7.103}$$

Here, $\mathbf{J}_i(h)$ depends on $h$ through the vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ given in (7.98)–(7.99). Conditioned on the event that $H = h$, the modified information density random vector $\tilde{\boldsymbol{\imath}}_2$ behaves as a sum of conditionally independent but not identical random vectors $\frac{1}{n}\boldsymbol{\mu}(h) + \frac{1}{\sqrt{n}}\mathbf{J}_i(h)$ in (7.101).

We next find the distribution of $H$. By spherical symmetry, the distribution of $H$ does not depend on $\mathbf{X}_1$. Therefore, we can set $\mathbf{X}_1 = \mathbf{x}_1$ and get

$$H \sim \frac{X_{21}}{\sqrt{P_2}}, \tag{7.104}$$

where $X_{21}$ denotes the first coordinate of $\mathbf{X}_2$. Therefore, $H$ is distributed according to the marginal distribution of the first coordinate of a random vector distributed uniformly on $\mathbb{S}^n(\sqrt{n})$. The distribution of $H$ is computed as (e.g., [140, Th. 1])

$$P_H(h) = \frac{\Gamma(\frac{n}{2})}{\sqrt{\pi n}\Gamma(\frac{n-1}{2})} \left(1 - \frac{h^2}{n}\right)_+^{\frac{n-3}{2}}, \tag{7.105}$$

where $\Gamma(\cdot)$ denotes the Gamma function, and $x_+ \triangleq \max\{0, x\}$ for all $x \in \mathbb{R}$. The support of $H$ is $[-\sqrt{n}, \sqrt{n}]$. From (7.105), we compute

$$\mathbb{E}[H] = 0, \quad \mathrm{Var}[H] = 1. \tag{7.106}$$

By Stirling's approximation, $H \to \mathcal{N}(0,1)$ in distribution as $n \to \infty$ (e.g., [140, Th. 1]). Recall that an upper bound on the total variation distance between $P_H$ and $\mathcal{N}(0,1)$ is given in Lemma 7.4.5.

From (7.101), we find the conditional covariance matrix of the modified information density random vector as

$$\begin{aligned} \mathsf{\Sigma}(h) &\triangleq \mathrm{Cov}[\tilde{\boldsymbol{\imath}}_2 | H = h] & (7.107)\\ &= \mathrm{Cov}\left[\frac{1}{\sqrt{n}} \sum_{i=1}^{n} \mathbf{J}_i(h)\right] & (7.108)\\ &= \mathsf{\Sigma} + \frac{h}{\sqrt{n}}\mathsf{B}, & (7.109) \end{aligned}$$

where

$$\mathsf{\Sigma} \triangleq \begin{bmatrix} V(P_1) & V_{1,2}(P_1,P_2) & V_{1,12}(P_1,P_2) \\ V_{1,2}(P_1,P_2) & V(P_2) & V_{2,12}(P_1,P_2), \\ V_{1,12}(P_1,P_2) & V_{2,12}(P_1,P_2) & V(P_1+P_2) \end{bmatrix} \tag{7.110}$$

$$\begin{aligned} \mathsf{B} \triangleq & \frac{\sqrt{P_1P_2}}{(1+P_1)(1+P_2)(1+P_1+P_2)} \\ & \cdot \begin{bmatrix} 0 & 1+P_1+P_2 & 1+P_2 \\ 1+P_1+P_2 & 0 & 1+P_1 \\ 1+P_2 & 1+P_1 & \frac{(1+P_1)(1+P_2)}{(1+P_1+P_2)} \end{bmatrix}, \end{aligned} \tag{7.111}$$

and $V(P), V_{1,2}(P_1,P_2)$, and $V_{i,12}(P_1,P_2)$, $i \in [2]$, are given in (7.3), (7.18), and (7.19), respectively. Note that $\mathsf{\Sigma}$ and $\mathsf{B}$ depend only on $P_1$ and $P_2$. Using (7.102), (7.106), (7.109), by the law of total expectation and variance, we compute

$$\mathbb{E}[\tilde{\boldsymbol{\imath}}_2] = 0 \tag{7.112}$$

$$\mathrm{Cov}\left[\tilde{\boldsymbol{\imath}}_2\right] = \mathsf{V}(P_1, P_2), \tag{7.113}$$

where $\mathsf{V}(P_1, P_2)$ is the dispersion matrix defined in (7.17).

**Step 2:** We next approximate the distribution of $\tilde{\boldsymbol{\imath}}_2$ by a Gaussian. Toward that end, we consider some auxiliary random variables. Based on our observation in (7.101), we express the probability on the right-hand side of (7.95) by conditioning on $H$ and taking the expectation with respect to $P_H$. Define the probability measure $P_{\tilde{H}}$, and the transition probability kernels $P_{\mathbf{V}|H}$ and $P_{\mathbf{W}|H}$ as

$$P_{\tilde{H}} \triangleq \mathcal{N}(0,1) \tag{7.114}$$

$$P_{\mathbf{V}|H=h} \triangleq \begin{cases} \mathcal{N}\left(\boldsymbol{\mu}(h), \Sigma(h)\right) & \text{if } |h|\leq \sqrt{n} \\ \mathcal{N}\left(\boldsymbol{\mu}(h), \Sigma\right) & \text{if } |h|> \sqrt{n} \end{cases} \tag{7.115}$$

$$P_{\mathbf{W}|H=h} \triangleq \mathcal{N}\left(\boldsymbol{\mu}(h), \Sigma\right) \qquad \text{for } h \in (-\infty, \infty). \tag{7.116}$$

As with $P_{\mathbf{V}|H}$, we extend the definition of the kernel $P_{\tilde{\boldsymbol{\imath}}_2|H}$ given in (7.101) for $|H|> \sqrt{n}$ by choosing $P_{\tilde{\boldsymbol{\imath}}_2|H=h} = \mathcal{N}(\boldsymbol{\mu}(h), \Sigma)$ for $|h|> \sqrt{n}$ in order for the joint distribution $P_{\tilde{H}}P_{\tilde{\boldsymbol{\imath}}_2|H}$ to be valid. Recall that $\tilde{H}$ is a Gaussian random variable with the same mean and variance as $H$, and the mean and covariance matrix according to $P_{\mathbf{V}|H=h}$ are the same as those for $P_{\tilde{\boldsymbol{\imath}}_2|H=h}$. The Gaussian kernel $P_{\mathbf{W}|H}$ is obtained from $P_{\mathbf{V}|H}$ by replacing its covariance matrix $\Sigma(H)$ by the mean value of $\Sigma(H)$, $\Sigma$.

We define the joint distributions $P_{H\,\tilde{\boldsymbol{\imath}}_2}$, $P_{\tilde{H}\,\boldsymbol{\imath}_2^*}$, $P_{\tilde{H}\,\mathbf{V}}$ and $P_{\tilde{H}\,\mathbf{W}}$ as

$$P_{H\,\tilde{\boldsymbol{\imath}}_2} = P_H P_{\tilde{\boldsymbol{\imath}}_2|H} \tag{7.117a}$$

$$P_{\tilde{H}\,\boldsymbol{\imath}_2^*} = P_{\tilde{H}} P_{\tilde{\boldsymbol{\imath}}_2|H} \tag{7.117b}$$

$$P_{\tilde{H}\,\mathbf{V}} = P_{\tilde{H}} P_{\mathbf{V}|H} \tag{7.117c}$$

$$P_{\tilde{H}\,\mathbf{W}} = P_{\tilde{H}} P_{\mathbf{W}|H}, \tag{7.117d}$$

where

$$\mathbf{W} \sim \mathcal{N}(\mathbf{0}, \mathsf{V}(P_1, P_2)), \tag{7.118}$$

which has the desired Gaussian distribution in our Berry-Esseen type bound.

Let $\mathcal{D}$ be any convex, Borel-measurable subset of $\mathbb{R}^3$. Then,

$$\left|\mathbb{P}\left[\tilde{\boldsymbol{\imath}}_2 \in \mathcal{D}\right] - \mathbb{P}\left[\mathbf{W} \in \mathcal{D}\right]\right| \tag{7.119a}$$

$$
\begin{aligned}
&\leq \left|\mathbb{P}\left[\tilde{\boldsymbol{\imath}}_2 \in \mathcal{D}\right] - \mathbb{P}\left[\boldsymbol{\imath}_2^* \in \mathcal{D}\right]\right| && \text{(7.119b)}\\
&\quad + \left|\mathbb{P}\left[\boldsymbol{\imath}_2^* \in \mathcal{D}\right] - \mathbb{P}\left[\mathbf{V} \in \mathcal{D}\right]\right| && \text{(7.119c)}\\
&\quad + \left|\mathbb{P}\left[\mathbf{V} \in \mathcal{D}\right] - \mathbb{P}\left[\mathbf{W} \in \mathcal{D}\right]\right|, && \text{(7.119d)}
\end{aligned}
$$

where the inequality in (7.119b) follows from the triangle inequality. The absolute differences in (7.119b), (7.119c), and (7.119d) reflect the change of the input measure from $P_H$ to $P_{\tilde{H}}$, the change of the transition probability kernel from $P_{\tilde{\boldsymbol{\imath}}_2|H}$ to $P_{\mathbf{V}|H}$, and the change of the transition probability kernel from $P_{\mathbf{V}|H}$ to $P_{\mathbf{W}|H}$, respectively. We next bound (7.119a) by showing that the absolute difference in each of (7.119b)–(7.119d) is $O\left(\frac{1}{\sqrt{n}}\right)$. In the next three steps, we bound each of these absolute differences in turn.

**Step 3:** We bound the absolute difference in the right-hand side of (7.119b) as

$$
\begin{aligned}
&\left|\mathbb{P}\left[\tilde{\boldsymbol{\imath}}_2 \in \mathcal{D}\right] - \mathbb{P}\left[\boldsymbol{\imath}_2^* \in \mathcal{D}\right]\right|\\
&= \left|\int_{-\infty}^{\infty} \mathbb{P}\left[\tilde{\boldsymbol{\imath}}_2 \in \mathcal{D} | H = h\right] \left(P_H(h) - P_{\tilde{H}}(h)\right) dh\right| && \text{(7.120)}\\
&\leq \int_{-\infty}^{\infty} \left|P_H(h) - P_{\tilde{H}}(h)\right| dh && \text{(7.121)}\\
&= 2\,\mathrm{TV}(P_H, P_{\tilde{H}}) && \text{(7.122)}\\
&\leq 2\frac{\sqrt{n}}{\sqrt{n-3}} - 2 && \text{(7.123)}\\
&\leq \frac{C_{\mathrm{H}}}{n}, && \text{(7.124)}
\end{aligned}
$$

where $C_{\mathrm{H}} = 8$. Inequality (7.121) follows by moving the absolute value to the inside of the integral and bounding the conditional probability by 1 for all $h$, and (7.123) holds for any $n \geq 4$ by Lemma 7.4.5. Inequality (7.124) holds for $n \geq 4$. We conclude that (7.124) holds for any $n$ since (7.120) is trivially bounded by 1.

**Step 4:** We bound the absolute difference due to changing the transition probability kernel from $P_{\boldsymbol{\imath}_2|H}$ to the Gaussian kernel $P_{\mathbf{V}|H}$ as

$$
\begin{aligned}
\left|\mathbb{P}\left[\boldsymbol{\imath}_2^* \in \mathcal{D}\right] - \mathbb{P}\left[\mathbf{V} \in \mathcal{D}\right]\right| &= \left|\mathbb{E}\left[\mathbb{P}\left[\boldsymbol{\imath}_2^* \in \mathcal{D}\middle|\tilde{H}\right] - \mathbb{P}\left[\mathbf{V} \in \mathcal{D}\middle|\tilde{H}\right]\right]\right| && \text{(7.125)}\\
&\leq \mathbb{E}\left[\left|\mathbb{P}\left[\boldsymbol{\imath}_2^* \in \mathcal{D}\middle|\tilde{H}\right] - \mathbb{P}\left[\mathbf{V} \in \mathcal{D}\middle|\tilde{H}\right]\right| 1\left\{\left|\tilde{H}\right| \leq \frac{\sqrt{n}}{2}\right\}\right]\\
&\quad + \mathbb{P}\left[\left|\tilde{H}\right| > \frac{\sqrt{n}}{2}\right] && \text{(7.126)}
\end{aligned}
$$

$$\leq \max_{h\in\left[-\frac{\sqrt{n}}{2},\frac{\sqrt{n}}{2}\right]} \frac{C(h)}{\sqrt{n}} + \mathbb{P}\left[\left|\tilde{H}\right| > \frac{\sqrt{n}}{2}\right] \tag{7.127}$$

$$\leq \frac{C_{\text{BE}}}{\sqrt{n}} + 2\exp\left\{-\frac{n}{8}\right\} \tag{7.128}$$

$$\leq \frac{C_{\text{BE}} + C_{\text{Ch}}}{\sqrt{n}}, \tag{7.129}$$

where

$$T(h) \triangleq \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[\|\mathbf{J}_i(h)\|_2^3\right] \tag{7.130}$$

$$C(h) \triangleq \frac{c\,3^{1/4}T(h)}{\lambda_{\min}(\Sigma(h))^{3/2}} \tag{7.131}$$

$$C_{\text{BE}} \triangleq \max_{h\in\left[-\frac{\sqrt{n}}{2},\frac{\sqrt{n}}{2}\right]} C(h) \tag{7.132}$$

$$C_{\text{Ch}} \triangleq 4\exp\left\{-\frac{1}{2}\right\}, \tag{7.133}$$

each $\mathbf{J}_i(h)$ is defined in (7.103), and $c$ is the Berry-Esseen constant given in Theorem 7.4.1. Here, (7.126) moves the absolute value in (7.125) to the inside of the expectation. We then separate the expectation into two cases in order to guarantee that we apply the Berry-Esseen theorem for values of $h$ such that $\Sigma(h)$ is positive-definite. Inequality (7.127) follows from Corollary 7.4.1, and (7.128) follows from the Chernoff bound applied to a Gaussian random variable. Inequality (7.129) holds for any $n$. For every $h \in \left[-\frac{\sqrt{n}}{2}, \frac{\sqrt{n}}{2}\right]$, $\Sigma(h)$ is a non-degenerate covariance matrix, and $T(h) < \infty$. Therefore, we conclude that $C_{\text{BE}} < \infty$.

**Step 5:** We next bound the probability in (7.119d), which is the absolute difference due to changing the covariance matrix of the Gaussian kernel from $\Sigma(h)$ to $\Sigma$, using Lemma 7.4.4, which bounds the total variation distance between two Gaussian vectors. Denote the spectral radius of a $d \times d$ symmetric matrix $\mathsf{M}$ by

$$\rho(\mathsf{M}) \triangleq \max_{i\in[d]} |\lambda_i(\mathsf{M})|, \tag{7.134}$$

where $\lambda_i(\cdot)$ is the $i$-th largest eigenvalue of its matrix argument. Let

$$\mathsf{A} \triangleq \Sigma^{-1/2}\mathsf{B}\Sigma^{-1/2}, \tag{7.135}$$

where matrices $\Sigma$ and $\mathsf{B}$ are defined in (7.110)–(7.111). Then

$$|\mathbb{P}\left[\mathbf{V} \in \mathcal{D}\right] - \mathbb{P}\left[\mathbf{W} \in \mathcal{D}\right]|$$

$$= \left| \mathbb{E}\left[ \mathbb{P}\left[ \mathbf{V} \in \mathcal{D} \middle| \tilde{H} \right] - \mathbb{P}\left[ \mathbf{W} \in \mathcal{D} \middle| \tilde{H} \right] \right] \right| \tag{7.136}$$

$$\leq \mathbb{E}\left[ \left| \mathbb{P}\left[ \mathbf{V} \in \mathcal{D} \middle| \tilde{H} \right] - \mathbb{P}\left[ \mathbf{W} \in \mathcal{D} \middle| \tilde{H} \right] \right| \right] \tag{7.137}$$

$$\leq \mathbb{E}\left[ \mathrm{TV}(\mathcal{N}(\boldsymbol{\mu}(\tilde{H}), \Sigma), \mathcal{N}(\boldsymbol{\mu}(\tilde{H}), \Sigma(\tilde{H}))) \right] \tag{7.138}$$

$$\leq \frac{2+\sqrt{6}}{4} \left\| \mathsf{A} \right\|_F \frac{\mathbb{E}\left[ \left| \tilde{H} \right| \right]}{\sqrt{n}}, \tag{7.139}$$

where (7.137) follows by moving the absolute value inside the expectation in (7.136), $\mu(\cdot)$ and $\Sigma(\cdot)$ are defined in (7.102) and (7.107), respectively, and (7.139) follows from Lemma 7.4.4.

The matrices $\Sigma$, $\Sigma + \mathsf{B}$, and $\Sigma - \mathsf{B}$ are all positive semidefinite as they are special cases of $\mathrm{Cov}\left[\tilde{\boldsymbol{\imath}}_2 | H = h\right]$ in (7.107) with $h$ equal to $0, \sqrt{n}$, and $-\sqrt{n}$, respectively. Hence $\Sigma^{-1/2}(\Sigma + \mathsf{B})\Sigma^{-1/2}$ and $\Sigma^{-1/2}(\Sigma - \mathsf{B})\Sigma^{-1/2}$ are also positive semidefinite. Since their eigenvalues are respectively given by $1 + \lambda_i(\mathsf{A})$ and $1 - \lambda_i(\mathsf{A})$, it follows then that $-1 \leq \lambda_i(\mathsf{A}) \leq 1$ for $i \in [d]$, giving $\rho(\mathsf{A}) \leq 1$.[3] Using the fact that $\left\| \mathsf{M} \right\|_F \leq \sqrt{d}\rho(\mathsf{M})$ for any $d \times d$ symmetric matrix $\mathsf{M}$, and employing the value of the expectation in (7.139), we conclude that

$$\left| \mathbb{P}\left[ \mathbf{V} \in \mathcal{D} \right] - \mathbb{P}\left[ \mathbf{W} \in \mathcal{D} \right] \right| \leq \frac{C_{\mathrm{G}}}{\sqrt{n}}, \tag{7.140}$$

where $C_{\mathrm{G}} = \frac{2\sqrt{6}+6}{4\sqrt{\pi}}$.

Combining the bounds in (7.124), (7.129), and (7.140), we have the following Berry-Esseen-type inequality

$$\left| \mathbb{P}\left[ \tilde{\boldsymbol{\imath}}_2 \in \mathcal{D} \right] - \mathbb{P}\left[ \mathbf{W} \in \mathcal{D} \right] \right| \leq \frac{C_{\mathrm{H}} + C_{\mathrm{BE}} + C_{\mathrm{Ch}} + C_{\mathrm{G}}}{\sqrt{n}} \tag{7.141}$$

for the modified information density random vector.

### 7.4.7 Completion of the Proof of Theorem 7.2.2

We employ the set $\mathcal{D} = \left\{ \mathbf{x} \in \mathbb{R}^3 : \mathbf{x} \geq \frac{1}{\sqrt{n}} \boldsymbol{\tau} \right\}$ in (7.141), where $\boldsymbol{\tau}$ is given in (7.93). Combining (7.95) and (7.141), we conclude that the probability $\mathbb{P}\left[\mathcal{A}^c\right]$ in (7.90) satisfies

$$\mathbb{P}\left[\mathcal{A}^c\right] \leq 1 - \mathbb{P}\left[ \mathbf{W} \geq \frac{1}{\sqrt{n}} \boldsymbol{\tau} \right] + \frac{C_{\mathrm{H}} + C_{\mathrm{BE}} + C_{\mathrm{Ch}} + C_{\mathrm{G}}}{\sqrt{n}} \tag{7.142}$$

[3] Actually, $\rho(\mathsf{A}) = 1$. Indeed, for $h = \sqrt{n}$, the random variables in the first and the second index of the vectors in (7.103) are identical. Therefore, both $\Sigma(\sqrt{n}) = \Sigma + \mathsf{B}$ and $\Sigma^{-1/2}(\Sigma + \mathsf{B})\Sigma^{-1/2}$ have an eigenvalue 0, and $\mathsf{A}$ has an eigenvalue $-1$.

$$= 1 - \mathbb{P}\left[\mathbf{W} \le -\frac{1}{\sqrt{n}}\boldsymbol{\tau}\right] + \frac{C_{\text{Out}}}{\sqrt{n}}, \tag{7.143}$$

where $\mathbf{W} \sim \mathcal{N}(\mathbf{0}, \mathsf{V}(P_1, P_2))$ and

$$C_{\text{Out}} \triangleq C_{\text{H}} + C_{\text{BE}} + C_{\text{Ch}} + C_{\text{G}}. \tag{7.144}$$

Equality (7.143) follows since $\mathbf{W} \sim -\mathbf{W}$. Suppose that $\boldsymbol{\tau}$ satisfies

$$-\frac{1}{\sqrt{n}}\boldsymbol{\tau} \in Q_{\text{inv}}\left(\mathsf{V}(P_1, P_2), \epsilon - \gamma_n\right) \tag{7.145}$$

$$\gamma_n \triangleq \exp\left\{-c_2 n^{1/3}\right\} + \frac{1 + C_{\text{Out}}}{\sqrt{n}}, \tag{7.146}$$

where the constant $c_2$ is as in (7.90). Then, the right-hand side of (7.90) is bounded by $\epsilon$. From the Taylor series expansion of $Q_{\text{inv}}(\mathsf{V}, \cdot)$ (e.g., [134, Lemma 13]), we conclude that (7.145) is equivalent to the inequality in (7.21), which completes the proof.

## 7.5 Proof of Theorem 7.2.3

In this section, we sketch the proof of Theorem 7.2.3 by detailing the modifications to generalize the proof of Theorem 7.2.2 from 2 to $K \ge 2$ transmitters. Assume that $\mathcal{S} \in \overline{\mathcal{P}}([K])$. Define the information densities as

$$\imath_{\mathcal{S}}(\mathbf{x}_{\mathcal{S}}; \mathbf{y} | \mathbf{x}_{\mathcal{S}^c}) \triangleq \log \frac{P_{\mathbf{Y}_K | \mathbf{X}_{[K]}}(\mathbf{y} | \mathbf{x}_{[K]})}{P_{\mathbf{Y}_K | \mathbf{X}_{\mathcal{S}^c}}(\mathbf{y} | \mathbf{x}_{\mathcal{S}^c})}, \tag{7.147}$$

where $\mathcal{S}^c = [K] \backslash \mathcal{S}$. The information density random vector for $K$ transmitters is

$$\boldsymbol{\imath}_K \triangleq (\imath_{\mathcal{S}}(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}_K | \mathbf{X}_{\mathcal{S}^c}) \colon \mathcal{S} \in \overline{\mathcal{P}}([K])) \in \mathbb{R}^{2^K - 1}, \tag{7.148}$$

where $\mathbf{X}_k$ is distributed uniformly on $\mathbb{S}^n(\sqrt{nP_k})$ for $k \in [K]$, $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{I}_n)$, $\mathbf{X}_1, \ldots, \mathbf{X}_K$ and $\mathbf{Z}$ are independent, and $\mathbf{Y}_K = \mathbf{X}_{\langle [K] \rangle} + \mathbf{Z}$.

Below, we use Lemma 7.4.1 and the generalization of Lemma 7.4.6 given in (7.152). The following lemma, which generalizes Lemma 7.4.5 to $K$ transmitters, is the critical part of the proof of Theorem 7.2.3.

**Lemma 7.5.1.** *Let $\mathbf{X}_i = (X_{i1}, \ldots, X_{in})$, $i = 1, \ldots, K$, be $K$ independent random vectors, distributed uniformly on $\mathbb{S}^n(1)$. Let $H_{ij} = \sqrt{n}\langle \mathbf{X}_i, \mathbf{X}_j \rangle$ for $1 \le i < j \le K$, and $\mathbf{H} = (H_{ij} \colon 1 \le i < j \le K)$. Then*

$$\text{TV}\left(P_{\mathbf{H}}, \mathcal{N}\left(\mathbf{0}, \mathsf{I}_{\frac{K(K-1)}{2}}\right)\right) \le \frac{C_K}{\sqrt{n}} \tag{7.149}$$

*for some constant $C_K$ depending only on $K$.*

*Proof:* See Appendix F.5. ■

The modifications in Section 7.4 are as follows.

1. The two-transmitter maximum likelihood decoder given in (7.51) is replaced by a $K$-transmitter maximum likelihood decoder, which chooses the message vector $m_{[K]} = (m_1, \dots, m_K)$ corresponding to the maximal information density $\imath_{[K]}(\mathsf{f}_{[K]}(m_{[K]}); \mathbf{y})$.

2. The typical set $\mathcal{F}$ defined in (7.56) is replaced by

$$\mathcal{F}_K \triangleq \bigtimes_{\mathcal{S} \in \overline{\mathcal{P}}([K])} \mathcal{F}(\mathcal{S}) \subseteq \mathbb{R}^{n \otimes (2^K - 1)}, \tag{7.150}$$

   where $\mathcal{F}(\mathcal{S})$ is defined in (7.57). Inequality (7.59) extends to $\mathcal{F}_K$ by Lemma 7.4.1.

3. The functions given in (7.62)–(7.64) are extended as

$$g_{\mathcal{S}}(t; \mathbf{y}, \mathbf{x}_{\mathcal{S}^c}) \triangleq \mathbb{P}[\imath_{\mathcal{S}}(\overline{\mathbf{X}}_{\mathcal{S}}; \mathbf{Y}_K | \mathbf{X}_{\mathcal{S}^c}) \geq t \mid \mathbf{X}_{\mathcal{S}^c} = \mathbf{x}_{\mathcal{S}^c}, \mathbf{Y}_K = \mathbf{y}]. \tag{7.151}$$

   In the proof of Lemma 7.4.6, we replace $P_1 + P_2$ by $P_{\langle \mathcal{S} \rangle}$, and $P_1 P_2$ by $\sum_{\substack{i,j \in [K] \\ i<j}} P_i P_j$. Inequality (7.73) generalizes to the $K$-transmitter MAC by applying its proof from Appendix F.4 with Lemma 7.4.1 from Section 7.4.1. Hence, Lemma 7.4.6 generalizes as

$$g_{\mathcal{S}}(t; \mathbf{y}, \mathbf{x}_{\mathcal{S}^c}) \leq \frac{G(\mathcal{S}) \exp\{-t\}}{\sqrt{n}}, \tag{7.152}$$

   where $G(\mathcal{S})$ is a constant depending only on the powers $(P_s : s \in \mathcal{S})$.

4. The high probability events given in (7.82) and (7.83) are replaced by

$$\mathcal{E}_K \triangleq \bigcap_{\mathcal{S} \in \overline{\mathcal{P}}([K])} \mathcal{E}(\mathcal{S}), \tag{7.153}$$

$$\begin{aligned} \mathcal{A}_K \triangleq \Bigg\{ \boldsymbol{\imath}_K \geq \Bigg( \log\Bigg( \Bigg( \prod_{s \in \mathcal{S}} M_s \Bigg) (G(\mathcal{S})^2) \alpha_{|\mathcal{S}|,K} \Bigg) : \mathcal{S} \in \overline{\mathcal{P}}([K]) \Bigg) \\ - \frac{1}{2} \log n \mathbf{1} \Bigg\}, \end{aligned} \tag{7.154}$$

   where

$$\alpha_{s,K} \triangleq K \binom{K}{s}, \quad s = 1, \dots, K. \tag{7.155}$$

Using the extension of the RCU bound for $K$ transmitters given in Remark 7.2.1 and following the same steps as Section 7.4.5, we replace the right-hand side of the inequality in (7.90) by

$$\mathbb{P}\left[\mathcal{A}_K^c\right] + \exp\left\{-c_K n^{1/3}\right\} + \frac{1}{\sqrt{n}}, \tag{7.156}$$

where $c_K$ is a constant.

5. To understand the differences between bounding $\mathbb{P}\left[\mathcal{A}_K^c\right]$ and $\mathbb{P}\left[\mathcal{A}^c\right]$, we first extend the definition of the modified and centered information density random vector to $K$ transmitters by defining

$$\tilde{\imath}_{\mathcal{S}}(\mathbf{x}_{\mathcal{S}}; \mathbf{y}_K | \mathbf{x}_{\mathcal{S}^c}) \triangleq \sum_{i=1}^{n} \log \frac{P_{Y_K|X_{[K]}}(y_i | x_{[K]i})}{P_{\tilde{Y}_K|\tilde{X}_{\mathcal{S}^c}}(y_i | x_{\mathcal{S}^c i})} \tag{7.157}$$

$$\tilde{\boldsymbol{\imath}}_K \triangleq \frac{1}{\sqrt{n}}\left[\left(\tilde{\imath}_{\mathcal{S}}(\mathbf{X}_{\mathcal{S}}; \mathbf{Y}_K | \mathbf{X}_{\mathcal{S}^c}) \colon \mathcal{S} \in \overline{\mathcal{P}}([K])\right) - n\mathbf{C}(P_{[K]})\right], \tag{7.158}$$

where $\mathbf{C}(P_{[K]})$ is the capacity vector defined in (7.23), $\tilde{X}_k \sim \mathcal{N}(0, P_k)$ for $k \in [K]$, and $\prod_{k=1}^{K} P_{\tilde{X}_k} \to P_{Y_K|X_{[K]}} \to P_{\tilde{Y}_K} = \mathcal{N}(0, 1 + P_{[K]})$.

We replace the threshold value in (7.93) by

$$\begin{aligned}\boldsymbol{\tau} \triangleq \log \Bigg( & \frac{\left(\prod_{s \in \mathcal{S}} M_s\right) (G(\mathcal{S}))^2 \kappa_{|\mathcal{S}|}(P_{\mathcal{S}}) \alpha_{|\mathcal{S}|,K}}{\sqrt{n}} \colon \\ & \mathcal{S} \in \overline{\mathcal{P}}([K]) \Bigg) - n\mathbf{C}(P_{[K]}),\end{aligned} \tag{7.159}$$

where $\kappa_{|\mathcal{S}|}(P_{\mathcal{S}})$ is the constant (which depends only on $P_{\mathcal{S}}$) in (7.39). Using the joint distribution of $(\mathbf{X}_{[K]}, \mathbf{Y}_K)$, we get

$$\begin{aligned}\tilde{\boldsymbol{\imath}}_K \sim \frac{1}{\sqrt{n}} \Bigg( & \frac{(n - \|\mathbf{Z}\|_2^2) P_{\langle \mathcal{S} \rangle}}{2(1 + P_{\langle \mathcal{S} \rangle})} \\ & + \frac{\sum_{\substack{i,j \in \mathcal{S} \\ i < j}} \langle \mathbf{X}_i, \mathbf{X}_j \rangle + \langle \mathbf{Z}, \mathbf{X}_{\langle \mathcal{S} \rangle} \rangle}{1 + P_{\langle \mathcal{S} \rangle}} \colon \mathcal{S} \in \overline{\mathcal{P}}([K]) \Bigg).\end{aligned} \tag{7.160}$$

Define the random vector

$$\mathbf{H} \triangleq (H_{ij} \colon 1 \leq i < j \leq K) \in \mathbb{R}^{\binom{K}{2}}, \tag{7.161}$$

where $H_{ij} = \frac{\langle \mathbf{X}_i, \mathbf{X}_j \rangle}{\sqrt{n P_i P_j}}$ denotes the normalized inner product of $\mathbf{X}_i$ and $\mathbf{X}_j$. The inner product random vector $\mathbf{H}$ replaces $H$ in (7.104). Observe that for all different $(i_1, j_1)$ and $(i_2, j_2)$ pairs, $H_{i_1 j_1}$ and $H_{i_2 j_2}$ are independent of each other, which follows by independence of $\mathbf{X}_1, \ldots, \mathbf{X}_K$. However, $\mathbf{H}$ does not have a product distribution due to the fact that any triplets in $\mathbf{H}$ are not jointly independent.[4] While $P_{\mathbf{H}}$ is not a product distribution, Lemma 7.5.1 implies that $P_{\mathbf{H}}$ converges to the distribution of $\binom{K}{2}$ i.i.d. standard Gaussian random variables in total variation, allowing us to use the Berry-Esseen theorem just as we did for the two-transmitter MAC.

As for the two-transmitter MAC, the distribution in (7.160) depends on $\mathbf{X}_{[K]}$ only through the inner product random vector $\mathbf{H}$. The conditional distribution of $\tilde{\boldsymbol{\imath}}_K$ given $\mathbf{H} = \mathbf{h}$ is the same as the conditional distribution of

$$\boldsymbol{\mu}(\mathbf{h}) + \frac{1}{\sqrt{n}} \sum_{i=1}^{n} \mathbf{J}_i(\mathbf{h}), \tag{7.162}$$

where

$$\begin{aligned} \boldsymbol{\mu}(\mathbf{h}) &\triangleq \mathbb{E}\left[\boldsymbol{\imath}_K | \mathbf{H} = \mathbf{h}\right] \\ &= \sum_{\substack{i,j \in [K] \\ i<j}} h_{ij} \left( \frac{\sqrt{P_i P_j}}{1 + P_{\langle \mathcal{S} \rangle}} 1\left\{i, j \in \mathcal{S}\right\} : \mathcal{S} \in \overline{\mathcal{P}}([K]) \right) \qquad (7.163) \\ \mathbf{J}_i(\mathbf{h}) &\triangleq \left( \frac{(1 - Z_i^2) P_{\langle \mathcal{S} \rangle} + 2 \sum_{s \in \mathcal{S}} x_{si} Z_i}{2(1 + P_{\langle \mathcal{S} \rangle})} : \mathcal{S} \in \overline{\mathcal{P}}([K]) \right) \qquad (7.164) \end{aligned}$$

for $i \in [n]$, and $\mathbf{x}_{[K]}$ are vectors on the $n$-dimensional power spheres, satisfying $\frac{\langle \mathbf{x}_i, \mathbf{x}_j \rangle}{\sqrt{n P_i P_j}} = h_{ij}$ for all $i < j \in [K]$. The conditional covariance matrix given in (7.109) is extended to $K$ transmitters as

$$\mathsf{\Sigma}(\mathbf{h}) = \mathrm{Cov}\left[\tilde{\boldsymbol{\imath}}_K | \mathbf{H} = \mathbf{h}\right] = \mathsf{\Sigma}_K + \sum_{i,j \in [K], i<j} \frac{h_{ij}}{\sqrt{n}} \mathsf{B}_{ij}, \tag{7.165}$$

where the $\left(\mathbb{R}^{2^K - 1}\right) \times \left(\mathbb{R}^{2^K - 1}\right)$ matrices $\mathsf{\Sigma}_K$ and $\mathsf{B}_{ij}$ have elements

$$\begin{aligned} \Sigma_{\mathcal{S}_1 \mathcal{S}_2} &= \frac{P_{\mathcal{S}_1} P_{\mathcal{S}_2} + 2 P_{\mathcal{S}_1 \cap \mathcal{S}_2}}{2(1 + P_{\mathcal{S}_1})(1 + P_{\mathcal{S}_2})} \qquad (7.166) \\ b_{\mathcal{S}_1 \mathcal{S}_2} &= \frac{\sqrt{P_i P_j}}{(1 + P_{\mathcal{S}_1})(1 + P_{\mathcal{S}_2})} \\ &\quad \cdot 1\left\{\{i \in \mathcal{S}_1, j \in \mathcal{S}_2\} \cup \{i \in \mathcal{S}_2, j \in \mathcal{S}_1\}\right\} \qquad (7.167) \end{aligned}$$

for $\mathcal{S}_1, \mathcal{S}_2 \in \overline{\mathcal{P}}([K])$. These formulas generalize the formulas for the two-transmitter MAC given in (7.110) and (7.111). By (7.163), (7.165),

[4] Given that $H_{12} = H_{13} = \sqrt{n}$, we have that $\mathbf{X}_1 = \mathbf{X}_2 = \mathbf{X}_3$. Therefore, $H_{23}$ is necessarily equal to $\sqrt{n}$ under this condition, and $H_{12}, H_{13}, H_{23}$ are not jointly independent.

and the pairwise independence of $H_{i_1 j_1}$, $H_{i_2 j_2}$ for all different $(i_1, j_1)$ and $(i_2, j_2)$ pairs, using the law of total expectation and variance, we find that

$$\mathbb{E}\left[\tilde{\boldsymbol{\imath}}_K\right] = \mathbf{0} \tag{7.168}$$

$$\mathrm{Cov}\left[\tilde{\boldsymbol{\imath}}_K\right] = \mathsf{V}(P_{[K]}), \tag{7.169}$$

where the covariance matrix $\mathsf{V}(P_{[K]})$ is defined in (7.24).

The rest of the proof follows the proof in Section 7.4.6, where we replace $H$ by $\mathbf{H}$, $\tilde{H}$ by the $\binom{K}{2}$-dimensional standard Gaussian random vector $\tilde{\mathbf{H}}$, $P_{\tilde{\boldsymbol{\imath}}_2|H}$ by $P_{\tilde{\boldsymbol{\imath}}_K|\mathbf{H}}$, $P_{\mathbf{V}|H}$ by $P_{\mathbf{V}|\mathbf{H}}$, and $P_{\mathbf{W}|H}$ by $P_{\mathbf{W}|\mathbf{H}}$. For the probability transition kernels $P_{\mathbf{V}|\mathbf{H}}$ and $P_{\mathbf{W}|\mathbf{H}}$, we replace $\boldsymbol{\mu}(h)$ by $\boldsymbol{\mu}(\mathbf{h})$, $\Sigma$ by $\Sigma_K$, and $\Sigma(h)$ by $\Sigma(\mathbf{h})$. We replace all conditions in the form $|h|\leq t$ by $|\mathbf{h}|\leq t\mathbf{1}$.

The only critical modification is that the bound on the total variation distance $\mathrm{TV}(P_H, P_{\tilde{H}})$ in (7.123) is replaced by the bound on the total variation distance $\mathrm{TV}(P_{\mathbf{H}}, P_{\tilde{\mathbf{H}}})$, which is $O\left(\frac{1}{\sqrt{n}}\right)$ by Lemma 7.5.1. We conclude that

$$\left|\mathbb{P}\left[\tilde{\boldsymbol{\imath}}_K \in \mathcal{D}\right] - \mathbb{P}\left[\mathbf{W} \in \mathcal{D}\right]\right| \leq \frac{C_K}{\sqrt{n}} \tag{7.170}$$

for some constant $C_K > 0$, where $\mathbf{W} \sim \mathcal{N}(\mathbf{0}, \mathsf{V}(P_{[K]}))$.

By combining (7.156) and (7.170) as in Section 7.4.7, we complete the proof of Theorem 7.2.3.

## 7.6 Proof of Theorem 7.3.2

The main difference between the coding strategies for the Gaussian MAC and RAC is that for the Gaussian RAC, an output typicality condition is added to the decoding function in order to reliably detect the number of active transmitters.

### 7.6.1 Encoding and Decoding

**Encoding**: Recall that $n_K$ is the largest decoding time. In our encoding strategy, rather than adapting the codebook to the estimate of the number of active transmitters at the receiver, we generate codewords with length $n_K$. Each active transmitter transmits one symbol of its message codeword at each time step until the decoder signals at time $n_k \in \{n_0, \ldots, n_K\}$ that it is able to decode. If decoding happens at time $n_k$, only the initial sub-codeword of length $n_k$ is used.

The common randomness random variable $U \in \mathbb{R}^{Mn_K}$ has the distribution

$$P_U = \underbrace{P_{U(1)} \times P_{U(2)} \times \cdots \times P_{U(M)}}_{M\text{times}}, \tag{7.171}$$

where $P_{U(m)} = P_{\mathbf{X}}$ for $m \in [M]$. The realization of $U$ defines $M$ length-$n_K$ i.i.d. codewords. In other words, the encoding function is given by

$$\mathsf{f}(U, m) = U(m), \quad m \in [M]. \tag{7.172}$$

As discussed in Chapter 6, the need for using common randomness in encoding is due to the requirement that a single code must satisfy multiple constraints, i.e., the error probability constraints in (7.29).

**Decoding**: Unlike the MAC, for the Gaussian RAC, we require the decoder to determine the time $n_k \in \{n_0, \ldots, n_K\}$ at which to decode. Therefore, we couple the maximum likelihood decoder given in (7.51) with a threshold rule, used to estimate the number of transmitters and a single bit of feedback at each time $n_i$ up to and including the time $n_k$ at which the decoder decides to decode. The maximum likelihood decoder is applied only if the threshold test is satisfied. Here, the role of the threshold rule is to reliably determine the true channel in the communication epoch. We use a threshold rule to determine the number of active transmitters because for any $P > 0$, under an input distribution $P_{\mathbf{X}}$ such that the expected input power meets the power constraint in (7.28) with equality (i.e., $\frac{1}{n_k}\mathbb{E}\left[\left\|\mathbf{X}^{[n_k]}\right\|_2^2\right] = P$), for each $k$, the normalized squared norm of the output $\mathbf{Y}_k^{[n_k]}$ concentrates around its mean. That mean is different for each $k \in \{0, 1, \ldots, K\}$; specifically

$$\frac{1}{n_k}\mathbb{E}\left[\left\|\mathbf{Y}_k^{[n_k]}\right\|_2^2\right] = 1 + kP, \quad \forall k \in \{0\} \cup [K]. \tag{7.173}$$

Upon receiving the first $n_0$ symbols of the output, $\mathbf{y}^{[n_0]}$, the decoder computes the following function

$$\mathsf{g}_0(U, \mathbf{y}^{[n_0]}) = \begin{cases} 0 & \text{if } \left|\frac{1}{n_0}\left\|\mathbf{y}^{[n_0]}\right\|_2^2 - 1\right| \le \lambda_0 \\ \mathsf{e} & \text{otherwise} \end{cases} \tag{7.174}$$

to decide whether there are any active transmitters; here $\lambda_0$ is a parameter that is determined by the error criterion $\epsilon_0$. At time $n_0$, if $\mathsf{g}_0(U, \mathbf{y}^{[n_0]}) = 0$, the receiver broadcasts a bit value 1 to all transmitters, signaling that the receiver estimates “no active transmitters" and the epoch ends. Otherwise the receiver broadcasts a bit value 0 and the epoch continues.

For $k \geq 1$, the decoder applies the following function to make a decision at each subsequent time $n_k \leq n_K$

$$\mathsf{g}_k(U, \mathbf{y}^{[n_k]}) = \begin{cases} m_{[k]} & \text{if } \imath_{[k]}(\mathsf{f}(U, m_{[k]})^{[n_k]}; \mathbf{y}^{[n_k]}) \\ & \quad > \imath_{[k]}(\mathsf{f}(U, m'_{[k]})^{[n_k]}; \mathbf{y}^{[n_k]}) \\ & \quad \text{for all } m'_{[k]} \overset{\pi}{\neq} m_{[k]}, \\ & m_1 \leq \ldots \leq m_k, \\ & \left| \frac{1}{n_k} \left\| \mathbf{y}^{[n_k]} \right\|_2^2 - (1 + kP) \right| \leq \lambda_k \\ \mathsf{e} & \text{otherwise,} \end{cases} \tag{7.175}$$

where $\lambda_k$ is a parameter chosen to satisfy the error criterion $\epsilon_k$. At time $n_k$, if $\mathsf{g}_k(U, \mathbf{y}^{[n_k]}) \neq \mathsf{e}$ or $k = K$, then the receiver broadcasts the bit value 1 to all transmitters, signaling the end of epoch and the start of next one. Otherwise, the receiver sends feedback 0 and the epoch continues.

By the permutation-invariance of the channel in terms of the inputs $\mathbf{X}_{[k]}$ and the identical encoding in (7.172), all permutations of the messages $m_{[k]}$ give the same information density. Therefore, without loss of generality, the output of our decoder is always the ordered message vector in (7.175). The condition $\left| \frac{1}{n_k} \left\| \mathbf{y}^{[n_k]} \right\|_2^2 - (1 + kP) \right| \leq \lambda_k$, which does not depend on the randomly generated codebook, allows us with high probability to decode at time $n_k$ when the number of active transmitters is $k$, rather than decoding earlier or failing to decode at the time $n_k$ intended for the $k$-transmitter scenario.

### 7.6.2 Error Analysis

In this section, we bound the probability of error for the random access code in Definition 7.3.1.

*No active transmitters*: For $k = 0$, the only error event is that the squared norm of the output $\mathbf{Y}_0^{[n_0]}$ is away from its mean:

$$\epsilon_0 \leq \mathbb{P}\left[ \left| \frac{1}{n_0} \left\| \mathbf{Y}_0^{[n_0]} \right\|_2^2 - 1 \right| > \lambda_0 \right]. \tag{7.176}$$

$k \geq 1$ *active transmitters*: When there is at least one active transmitter, the encoding function (7.172) and decoding rule (7.175) yield an error if and only if at least one of the following events occurs:

- $\mathcal{E}_{\text{codeword}}$: At least one of the $k$ codewords associated with the sent messages $m_{[k]}$ violates the power constraint in (7.28) in the first $n_k$ symbols. In this case, an error occurs since it is forbidden to transmit those codewords. We do not need to include the power constraint violation beyond the $n_k$-th symbol since that event is captured by the event of decoding time error, stated next.
- $\mathcal{E}_{\text{time}}$: A list of messages is decoded at a wrong decoding time $n_t \neq n_k$, or no messages is decoded during the entire epoch.
- $\mathcal{E}_{\text{message}}$: A list of messages $m'_{[k]} \neq m_{[k]}$ is decoded at time $n_k$.

In the following discussion, we bound the probability of these events separately, and apply the union bound to combine them.

Since we are employing identical encoders at all encoders, we simplify the analysis by treating the event $\mathcal{E}_{\text{rep}} = \{W_i = W_j \text{ for some } i \neq j\}$ that at least one message among transmitted messages is repeated as an error. While this case is actually advantageous to decoding, it requires special treatment since it violates the assumption of codeword independence employed in our analysis.

By the union bound,

$$\mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] \leq \frac{k(k-1)}{2M}. \tag{7.177}$$

Applying the union bound, we bound the error probability as

$$\begin{aligned} \epsilon_k = \frac{1}{M^k} \sum_{m_{[k]} \in [M]^k} \mathbb{P}\Bigg[ & \bigcup_{t: n_t \leq n_k, t \neq k} \left\{ \mathsf{g}_t(U, \mathbf{Y}_k^{[n_t]}) \neq \mathsf{e} \right\} \\ & \bigcup \left\{ \mathsf{g}_k(U, \mathbf{Y}_k^{[n_k]}) \overset{\pi}{\neq} m_{[k]} \right\} \Bigg| W_{[k]} = m_{[k]} \Bigg] & (7.178) \\ \leq \mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{rep}}^c\right] & \Big( \mathbb{P}\left[\mathcal{E}_{\text{codeword}} \middle| \mathcal{E}_{\text{rep}}^c\right] & (7.179) \\ & + \mathbb{P}\left[\mathcal{E}_{\text{time}} \middle| \mathcal{E}_{\text{rep}}^c\right] + \mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^c\right] \Big) & (7.180) \\ \leq \mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{codeword}} \middle| \mathcal{E}_{\text{rep}}^c\right] & \\ & + \mathbb{P}\left[\mathcal{E}_{\text{time}} \middle| \mathcal{E}_{\text{rep}}^c\right] + \mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^c\right]. & (7.181) \end{aligned}$$

*Power constraint violation*: The probability that a power constraint violation occurs in the first $n_k$ symbols for at least one of the $k$ distinct messages is

$$\mathbb{P}\left[\mathcal{E}_{\text{codeword}} \middle| \mathcal{E}_{\text{rep}}^c\right] = \mathbb{P}\left[\bigcup_{i=1}^{k} \bigcup_{\substack{j: n_j \leq n_k \\ j \geq 1}} \left\{ \frac{1}{n_j} \left\| \mathbf{X}_i^{[n_j]} \right\|_2^2 > P \right\}\right]. \tag{7.182}$$

*Wrong decoding time:* According to the decoding rule in (7.175), decoding occurs at time $n_k$ if and only if the output typicality criterion is not satisfied for any $t$ with $n_t \leq n_k$ and $t \neq k$ (that is $\left| \frac{1}{n_t} \left\| \mathbf{y}^{[n_t]} \right\|_2^2 - (1 + tP) \right| > \lambda_t$), and is satisfied for $k$ (that is $\left| \frac{1}{n_k} \left\| \mathbf{y}^{[n_k]} \right\|_2^2 - (1 + kP) \right| \leq \lambda_k$). Note that it is possible that no message set is decoded during an entire epoch. This would happen if $\left| \frac{1}{n_t} \left\| \mathbf{y}^{[n_t]} \right\|_2^2 - (1 + tP) \right| > \lambda_t$ for $t \in \{0, \dots, K\}$. The probability $\mathbb{P}\left[\mathcal{E}_{\text{time}} \middle| \mathcal{E}_{\text{rep}}^c\right]$ is computed as

$$\mathbb{P}\left[\mathcal{E}_{\text{time}} \middle| \mathcal{E}_{\text{rep}}^c\right] = \mathbb{P}\Bigg[\bigcup_{\substack{t: n_t \leq n_k \\ t \neq k}} \left\{ \left| \frac{1}{n_t} \left\| \mathbf{Y}_k^{[n_t]} \right\|_2^2 - (1 + tP) \right| \leq \lambda_t \right\}$$
$$\bigcup \left\{ \left| \frac{1}{n_k} \left\| \mathbf{Y}_k^{[n_k]} \right\|_2^2 - (1 + kP) \right| > \lambda_k \right\}\Bigg]. \tag{7.183}$$

*Wrong message:* By using the RCU bound in Remark 7.2.1 and the permutation-invariance of the information density, we bound $\mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^c\right]$ as

$$\mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^c\right] \leq \mathbb{E}\Bigg[\min\Bigg\{1, \sum_{s=1}^{k} \binom{k}{s} \binom{M-k}{s}$$
$$\mathbb{P}\left[\imath_{[s]}(\overline{\mathbf{X}}_{[s]}^{[n_k]}; \mathbf{Y}_k^{[n_k]} | \mathbf{X}_{[s+1:k]}^{[n_k]}) \geq \imath_{[s]}(\mathbf{X}_{[s]}^{[n_k]}; \mathbf{Y}_k^{[n_k]} | \mathbf{X}_{[s+1:k]}^{[n_k]}) \;\middle|\; \mathbf{X}_{[k]}^{[n_k]}, \mathbf{Y}_k^{[n_k]}\right]\Bigg\}\Bigg]. \tag{7.184}$$

Combining (7.176), (7.177) and (7.181)–(7.184) completes the proof. Note that compared to the achievability proof of the Gaussian MAC in (7.11), the multiplicative constant in (7.184) is $\binom{M-k}{s}$ instead of $(M-1)^s$ since we are given that the transmitted messages are distinct.

## 7.7 Proof of Theorem 7.3.1

In this section, we analyze the achievability bound in Theorem 7.3.2 by particularizing the input distribution, $P_{\mathbf{X}}$ in Theorem 7.3.2, choosing the free parameters $\lambda_k$, decoding times $n_0, n_1, \dots, n_K$, and bounding the probability and expectation terms in (7.34). In the rest of the proof, we assume that the decoding times satisfy $n_0 < n_1 < \cdots < n_K$, which we make explicit in (7.211).

### 7.7.1 Particularizing $P_{\mathbf{X}}$

We modify the input distribution used in Theorem 7.2.2 for the Gaussian MAC so that the randomly generated codewords meet the power constraints with probability 1.

A random codeword distributed according to $P_{\mathbf{X}}$ has length $n_K$ and consists of $K$ independent sub-codewords. The $j$-th sub-codeword has length $|\mathcal{N}(j)|$, where

$$\mathcal{N}(j) \triangleq \begin{cases} [n_1] & \text{if } j = 1 \\ \{n_{j-1}+1, n_{j-1}+2, \ldots, n_j\} & \text{if } 2 \leq j \leq K \end{cases} \tag{7.185}$$

for $j \in [K]$ is the index set for the $j$-th block in our code design. Thus, the input distribution $P_{\mathbf{X}}$ in Theorem 7.3.2 is

$$P_{\mathbf{X}}(\mathbf{x}) = \prod_{j=1}^{K} P_{\mathbf{X}^{\mathcal{N}(j)}}\left(\mathbf{x}^{\mathcal{N}(j)}\right), \tag{7.186}$$

where

$$P_{\mathbf{X}^{\mathcal{N}(j)}}\left(\mathbf{x}^{\mathcal{N}(j)}\right) = \frac{\delta\left(\left\|\mathbf{x}^{\mathcal{N}(j)}\right\|_2^2 - |\mathcal{N}(j)|P\right)}{S_{|\mathcal{N}(j)|}(\sqrt{|\mathcal{N}(j)|P})}, \tag{7.187}$$

that is, $\mathbf{X}^{\mathcal{N}(j)} \sim \text{Uniform}\left(\mathbb{S}^{|\mathcal{N}(j)|}(\sqrt{|\mathcal{N}(j)|P})\right)$, and $\mathbf{X}^{\mathcal{N}(1)}, \ldots, \mathbf{X}^{\mathcal{N}(K)}$ are independent.

Codewords chosen according to (7.186) satisfy the power constraints in (7.28) with equality, giving

$$\mathbb{P}\left[\bigcup_{i=1}^{k}\bigcup_{j=1}^{k}\left\{\frac{1}{n_j}\left\|\mathbf{X}_i^{[n_j]}\right\|_2^2 > P\right\}\right] = 0. \tag{7.188}$$

### 7.7.2 Error Analysis

We separate the analysis into 3 steps: deriving an output typicality bound, evaluation of the RCU bound, and evaluation of a Berry-Esseen type inequality.

**Step 1**: In this step, we bound the probability that the output $\mathbf{Y}_k^{[n_k]}$ does not satisfy the condition $\left|\frac{1}{n_k}\left\|\mathbf{Y}_k^{[n_k]}\right\|_2^2 - (1+kP)\right| \leq \lambda_k$ given in the decoding rule (7.175). Since for

$k \geq 1$, $\mathbf{Y}_k^{\mathcal{N}(1)}, \mathbf{Y}_k^{\mathcal{N}(2)}, \ldots, \mathbf{Y}_k^{\mathcal{N}(K)}$ are independent due to the input distribution in (7.186), Lemma 7.4.1 and Lemma 7.4.2 imply

$$\begin{aligned}&\mathbb{P}\left[\left|\left\|\mathbf{Y}_k^{[n_k]}\right\|_2^2 - n_k(1+kP)\right| > n_k\lambda_k\right] \\ &\quad \leq 2\left(\kappa_k(P\mathbf{1})\right)^k \exp\left\{-\frac{n_k\lambda_k^2}{8(1+kP)^2}\right\}\end{aligned} \tag{7.189}$$

for $\lambda_k \in (0, 1+kP)$, where $\kappa_j(P\mathbf{1})$ is the constant defined in Lemma 7.4.1. For $k = 0$, we have

$$\mathbb{P}\left[\left|\left\|\mathbf{Y}_0^{[n_0]}\right\|_2^2 - n_0\right| > n_0\lambda_0\right] \leq 2\exp\left\{-\frac{n_0\lambda_0^2}{8}\right\} \tag{7.190}$$

for $\lambda_0 \in (0, 1)$. We pick

$$\lambda_0 = \sqrt{\frac{-8\log\frac{\epsilon_0}{2}}{n_0}} \tag{7.191}$$

to ensure that the right-hand side of (7.190) is bounded above by $\epsilon_0$. By setting $\lambda_t = \frac{P}{2}$ for $t \geq 1$, using (7.189) and (7.190), and applying the union bound, we bound the probability of decoding time error in (7.34b) by

$$\begin{aligned}B \triangleq\ & 2\kappa_1(P)\exp\left\{-\frac{n_0((k-\frac{\lambda_0}{P})P)^2}{8(1+kP)^2}\right\} \\ & + 2\sum_{t=1}^{k}\left(\kappa_k(P\mathbf{1})\right)^t \exp\left\{-\frac{n_t((k-t-\frac{1}{2})P)^2}{8(1+kP)^2}\right\}.\end{aligned} \tag{7.192}$$

**Step 2**: To bound the expectation in (7.34c), we first modify the definition of the typical output set $\mathcal{F}(\mathcal{S})$ in (7.57) as

$$\mathcal{F}(\mathcal{S})_{\mathrm{RAC}} \triangleq \left\{\mathbf{y}^{[n_k]} \in \mathbb{R}^{n_k}\colon \frac{1}{|\mathcal{N}(j)|}\left\|\mathbf{y}^{\mathcal{N}(j)}\right\|_2^2 \in \mathcal{I}(j,\mathcal{S}) \text{ for } j \in [k]\right\}. \tag{7.193}$$

$$\mathcal{I}(j,\mathcal{S}) \triangleq [1+|\mathcal{S}|P - |\mathcal{N}(j)|^{-1/3}, 1+|\mathcal{S}|P + |\mathcal{N}(j)|^{-1/3}]. \tag{7.194}$$

We then show that Lemma 7.4.6 holds under input distribution (7.186) with typical output set (7.193). That is, for every $0 < s \leq k$, and $\mathbf{y}^{[n_k]}$ and $\mathbf{x}_{[k]\setminus[s]}^{[n_k]}$ such that $\mathbf{y}^{[n_k]} - \mathbf{x}_{\langle[k]\setminus[s]\rangle}^{[n_k]} \in \mathcal{F}([s])_{\mathrm{RAC}}$, we prove that

$$\begin{aligned}& g_{[s]}(t; \mathbf{y}^{[n_k]}, \mathbf{x}_{[k]\setminus[s]}^{[n_k]}) \\ &\triangleq \mathbb{P}\left[\imath_{[s]}(\overline{\mathbf{X}}_{[s]}^{[n_k]}; \mathbf{Y}_k^{[n_k]}|\mathbf{X}_{[k]\setminus[s]}^{[n_k]}) \geq t \,\middle|\, \mathbf{X}_{[k]\setminus[s]}^{[n_k]} = \mathbf{x}_{[k]\setminus[s]}^{[n_k]}, \mathbf{Y}_k^{[n_k]} = \mathbf{y}^{[n_k]}\right]\end{aligned} \tag{7.195}$$

$$\leq \frac{G'_{s,k} \exp\{-t\}}{\sqrt{n_k}}, \tag{7.196}$$

where $G'_{s,k}$ is a positive constant depending on $s, k$ and $P$.

The derivation of the bound in (7.196) follows the analysis in Section 7.4.4. The critical goal is to verify steps (7.74)–(7.76) for the modified input distribution in (7.186). This requires showing that

$$\mathbb{P}\left[\langle \mathbf{X}_{\langle [s] \rangle}^{[n_k]}, \mathbf{X}_{\langle [s] \rangle}^{[n_k]} + \mathbf{Z}^{[n_k]} \rangle - \sum_{j=1}^{k} \frac{|\mathcal{N}(j)| u_j}{2} \in [a, a+\mu] \middle| \mathcal{E} \right] \leq O\left(\frac{1}{\sqrt{n_k}}\right), \tag{7.197}$$

where

$$\mathcal{E} = \left\{ \left\| \mathbf{X}_{\langle [s] \rangle}^{\mathcal{N}(j)} + \mathbf{Z}^{\mathcal{N}(j)} \right\|_2^2 = |\mathcal{N}(j)| s_j, \left\| \mathbf{X}_{\langle [s] \rangle}^{\mathcal{N}(j)} \right\|_2^2 = |\mathcal{N}(j)| u_j \text{ for } j \in [k] \right\}, \tag{7.198}$$

$s_j \in \mathcal{I}(j, [s])$, and $u_j > 0$. The proof of (7.197) is similar to the one in [44, Appendix A] for parallel Gaussian channels since we can consider $K$ independent sub-codewords with lengths $|\mathcal{N}(j)|$, $j \in [K]$, as $K$ parallel channels, each having blocklength $|\mathcal{N}(j)|$, $j \in [K]$.

Taking an arbitrary $t \in [k]$, we get

$$\begin{aligned}
&\mathbb{P}\left[\langle \mathbf{X}_{\langle [s] \rangle}^{[n_k]}, \mathbf{X}_{\langle [s] \rangle}^{[n_k]} + \mathbf{Z}^{[n_k]} \rangle - \sum_{j=1}^{k} \frac{|\mathcal{N}(j)| u_j}{2} \in [a, a+\mu] \middle| \mathcal{E} \right] \\
&= \int_{\mathbb{R}^{k-1}} \mathbb{P}\Bigg[ Z_{n_{t-1}+1} + \frac{\sqrt{|\mathcal{N}(j)|}}{2} \in \left[ \frac{a'}{\sqrt{|\mathcal{N}(j)|}}, \frac{a'+\mu}{\sqrt{|\mathcal{N}(j)|}} \right] \\
&\qquad \Bigg| \, \mathcal{E}, \{ Z_{n_{j-1}+1} = z_j, j \in [k] \setminus \{t\} \} \Bigg] \Bigg( \prod_{\substack{j \in [k] \\ j \neq t}} f_{Z_{n_{j-1}+1} | \mathcal{E}}(z_j) dz_j \Bigg) && (7.199) \\
&\leq \frac{L(u_t, s_t)\mu}{\sqrt{|\mathcal{N}(t)|}} && (7.200) \\
&\leq \frac{3}{2} \frac{L(u_t, 1+sP)\mu}{\sqrt{|\mathcal{N}(t)|}} && (7.201) \\
&\leq \frac{3}{2} \frac{\max_{j \in [k]} L(u_j, 1+sP)\mu}{\sqrt{|\mathcal{N}(t)|}}, && (7.202)
\end{aligned}$$

where $a'$ is related to $a$ by a constant shift, and (7.199) follows by setting $\mathbf{X}_{\langle [s] \rangle}^{\mathcal{N}(j)} = (\sqrt{|\mathcal{N}(j)| u_j}, 0, \ldots, 0)$, and conditioning on the event that $\{Z_{n_{j-1}+1} =$

$z_j$ for $j \neq t\}$. Since $t$ is arbitrary in (7.199), we have

$$\begin{aligned}
&\mathbb{P}\left[\langle \mathbf{X}_{\langle[s]\rangle}^{[n_k]}, \mathbf{X}_{\langle[s]\rangle}^{[n_k]} + \mathbf{Z}^{[n_k]}\rangle - \sum_{j=1}^{k} \frac{|\mathcal{N}(j)|u_j}{2} \in [a, a+\mu] \middle| \mathcal{E}\right] \\
&\leq \frac{3}{2}\frac{\max_{j\in[k]} L(u_j, 1+sP)\mu}{\sqrt{\max_{t\in[k]}|\mathcal{N}(t)|}} && (7.203)\\
&\leq \frac{3}{2}\frac{\sqrt{k}\max_{j\in[k]} L(u_j, 1+sP)\mu}{\sqrt{n_k}}, && (7.204)
\end{aligned}$$

which implies (7.197), and (7.196) follows.

In the following discussion, we modify the analysis in Section 7.4.5 according to the input distribution in (7.186). Define the information density random vector $\boldsymbol{\imath}_k$ and the typical events analogous to (7.81)–(7.83) as

$$\begin{aligned}
\boldsymbol{\imath}_k &\triangleq (\imath_{\mathcal{S}}(\mathbf{X}_{\mathcal{S}}^{[n_k]}; \mathbf{Y}_k^{[n_k]} | \mathbf{X}_{\mathcal{S}^c}^{[n_k]}) \colon \mathcal{S} \in \overline{\mathcal{P}}([k])) && (7.205)\\
\mathcal{E}(\mathcal{S})_{\text{RAC}} &\triangleq \left\{\mathbf{X}_{\langle\mathcal{S}\rangle}^{[n_k]} + \mathbf{Z}^{[n_k]} \in \mathcal{F}(\mathcal{S})_{\text{RAC}}\right\} && (7.206)\\
\mathcal{E}_{\text{RAC}} &\triangleq \bigcap_{\mathcal{S}\in\overline{\mathcal{P}}([k])} \mathcal{E}(\mathcal{S})_{\text{RAC}} && (7.207)\\
\mathcal{A}_k &\triangleq \left\{\boldsymbol{\imath}_k \geq \left(\log\left(\binom{M-k}{|\mathcal{S}|}(G'_{|\mathcal{S}|,k})^2\alpha_{|\mathcal{S}|,k}\right) \colon \mathcal{S} \in \overline{\mathcal{P}}([k])\right) - \frac{1}{2}\log n_k \mathbf{1}\right\}, && (7.208)
\end{aligned}$$

where $\alpha_{s,k}$ is given in (7.155). By Lemma 7.4.2 and the union bound, we have

$$\mathbb{P}\left[\mathcal{E}_{\text{RAC}}^c\right] \leq \sum_{j=1}^{k} \exp\left\{-c_k|\mathcal{N}(j)|^{1/3}\right\}, \tag{7.209}$$

where $c_k$ is a positive constant. Combining (7.196) and (7.209) and following the analysis in Section 7.4.5, we bound the expectation in (7.34c) by

$$\mathbb{P}\left[\mathcal{A}_k^c\right] + \sum_{j=1}^{k} \exp\left\{-c_k|\mathcal{N}(j)|^{1/3}\right\} + \frac{1}{\sqrt{n_k}}. \tag{7.210}$$

**Step 3**: Given $M$ and $\{\epsilon_k\}_{k=0}^K$, we set the decoding times $n_1, \ldots, n_K$ according to the equalities

$$\begin{aligned}
k\log M = n_k C(kP) &- \sqrt{n_k(V(kP) + V_{\text{cr}}(k,P))}Q^{-1}\left(\epsilon_k - \frac{D_k}{\sqrt{n_k}}\right)\\
&+ \frac{1}{2}\log n_k + \eta_k - k\log\kappa_k(P\mathbf{1}) && (7.211)
\end{aligned}$$

for all $k \in [K]$, where $D_k$ is a positive constant to be chosen later in (7.225), and $\eta_k \triangleq -2\log G'_{k,k} + (k-1)\log k - k$. Since $\frac{1}{s}C(sP) > \frac{1}{k}C(kP)$ for $s < k$ and (7.211), we reach a sequence of conclusions.

1. There exists a constant $c_0 > 0$ such that $\min_{j\in[k]}|\mathcal{N}(j)| \geq c_0 n_k$ for large enough $M$. In other words, $|\mathcal{N}(j)|$ is of the same order as $n_k$ for all $j \in [k]$.

2. The bound on the probability of message repetition, $\frac{k(k-1)}{2M}$, decays exponentially with $n_k$.

3. In order to bound the expression in (7.192) as $B \leq O\left(\frac{1}{\sqrt{n_k}}\right)$, we choose $n_0 \geq \frac{4(1+P^2)}{P^2}\log n_1 + o(\log n_1)$.

4. By the union bound, Chebyshev's inequality, $\alpha_{k,k} = k$ in (7.155), and the fact that

$$\binom{M}{k} \leq \left(\frac{eM}{k}\right)^k, \tag{7.212}$$

we get

$$\mathbb{P}\left[\mathcal{A}_k^c\right] \leq \frac{E_k}{n_k} + \mathbb{P}\left[\imath_{[k]}(\mathbf{X}_{[k]}^{[n_k]}; \mathbf{Y}_k^{[n_k]}) < k\log M - \frac{1}{2}\log n_k - \eta_k\right] \tag{7.213}$$

for some positive constant $E_k$.

Therefore, it remains only to evaluate the probability term in (7.213). Define the modified and centered information density random variable

$$\tilde{\imath}_k \triangleq \frac{1}{\sqrt{n_k}}\left(\sum_{i=1}^{n_k}\log\frac{P_{Y_k|X_{[k]}}(Y_i|X_{[k],i})}{P_{\tilde{Y}_k}(Y_i)} - n_k C(kP)\right), \tag{7.214}$$

where $\tilde{Y}_k \sim \mathcal{N}(0, 1+kP)$. By Lemma 7.4.1 and (7.211), we get

$$\begin{aligned}\mathbb{P}&\left[\imath_{[k]}(\mathbf{X}_{[k]}^{[n_k]}; \mathbf{Y}_k^{[n_k]}) < k\log M - \frac{1}{2}\log n_k - \eta_k\right]\\ &\leq \mathbb{P}\left[\tilde{\imath}_k < -\sqrt{V(kP) + V_{\mathrm{cr}}(k,P)}\,Q^{-1}\left(\epsilon_k - \frac{D_k}{\sqrt{n_k}}\right)\right].\end{aligned} \tag{7.215}$$

The conditional distribution of $\tilde{\imath}_k$ given $\mathbf{X}_{[k]}^{[n_k]} = \mathbf{x}_{[k]}^{[n_k]}$ is the same as the conditional distribution of $\tilde{\imath}_k$ given $\mathbf{H} = \mathbf{h}$, where

$$\mathbf{H} = (H_{ij} \colon i,j \in [k], i < j) \in \mathbb{R}^{\binom{k}{2}}, \tag{7.216}$$

and $H_{ij} = \frac{\langle \mathbf{X}_i^{[n_k]}, \mathbf{X}_j^{[n_k]} \rangle}{\sqrt{n_k P^2}}$. To bound the right-hand side of (7.215), in a manner similar to the arguments in Section 7.5, we only need to verify that

$$\mathrm{TV}(P_{\mathbf{H}}, P_{\tilde{\mathbf{H}}}) \leq \frac{\psi_k}{\sqrt{n_k}} \tag{7.217}$$

for some constant $\psi_k$, where $\tilde{\mathbf{H}} \sim \mathcal{N}\left(\mathbf{0}, \mathsf{I}_{\binom{k}{2}}\right)$. To show (7.217), we define

$$\mathbf{H}^{(t)} \triangleq (H_{ij}^{(t)} \colon i, j \in [k], i < j) \in \mathbb{R}^{\binom{k}{2}}, \tag{7.218}$$

where $H_{ij}^{(t)} = \frac{\langle \mathbf{X}_i^{\mathcal{N}(t)}, \mathbf{X}_j^{\mathcal{N}(t)} \rangle}{\sqrt{|\mathcal{N}(t)| P^2}}$, then write

$$\mathbf{H} = \sum_{t=1}^{k} \frac{\sqrt{|\mathcal{N}(t)|}}{\sqrt{n_k}} \mathbf{H}^{(t)}. \tag{7.219}$$

By the data processing inequality of the total variation distance and the independence of $\mathbf{H}^{(t)}$, $t \in [k]$, we get

$$\begin{aligned}
\mathrm{TV}(P_{\mathbf{H}}, P_{\tilde{\mathbf{H}}}) &\leq \mathrm{TV}\left(\prod_{t=1}^{k} P_{\mathbf{H}^{(t)}}, P_{\tilde{\mathbf{H}}}^{k}\right) && (7.220)\\
&\leq \sum_{t=1}^{k} \mathrm{TV}(P_{\mathbf{H}^{(t)}}, P_{\tilde{\mathbf{H}}}) && (7.221)\\
&\leq \sum_{t=1}^{k} \frac{F_k}{\sqrt{|\mathcal{N}(t)|}} && (7.222)\\
&\leq \frac{kF_k}{\sqrt{c_0 n_k}}, && (7.223)
\end{aligned}$$

where (7.221) applies [141, eq. (4.5)], which bounds the total variation distance between two product measures $P^k$ and $Q^k$ by $k$ times the total variation distances between $P$ and $Q$. The bound in [141, eq. (4.5)] is extended to arbitrary product measures $\prod_{i=1}^{k} P_i$ and $\prod_{i=1}^{k} Q_i$ in [142, Lemma 2.1]. Inequality (7.222) follows from Lemma 7.5.1, $F_k$ is the constant from Lemma 7.5.1, and (7.223) follows from (7.211), which proves (7.217).

By (7.223), and following arguments similar to those in Section 7.5, we conclude that

$$\begin{aligned}
&\mathbb{P}\left[\tilde{\imath}_k < -\sqrt{V(kP) + V_{\mathrm{cr}}(k, P)}Q^{-1}\left(\epsilon_k - \frac{D_k}{\sqrt{n_k}}\right)\right]\\
&\leq \epsilon_k - \frac{D_k}{\sqrt{n_k}} + \frac{C_k}{\sqrt{n_k}}, && (7.224)
\end{aligned}$$

where $C_k$ is a Berry-Esseen constant. We choose the constant $D_k$ such that

$$\begin{aligned}\frac{D_k}{\sqrt{n_k}} \leq \frac{k(k-1)}{2M} + B + \frac{C_k}{\sqrt{n_k}} + \frac{E_k}{n_k} \\ +k\exp\left\{-c_k(c_0 n_k)^{1/3}\right\} + \frac{1}{\sqrt{n_k}},\end{aligned} \tag{7.225}$$

where $B$ is in (7.192). For large enough $n_k$, such a constant exists by the enumerated consequences of (7.211), above. From Theorem 7.3.2 and the inequalities (7.188), (7.210)–(7.213), (7.215), (7.224) and (7.225), we conclude that the probability of error is bounded by $\epsilon_k$. By the Taylor series expansion of the function $Q^{-1}(\cdot)$ in (7.211), we complete the proof.

## 7.8 Summary

This chapter studies the Gaussian multi-access channels in the finite-blocklength regime for two communication scenarios. In the first scenario, called the Gaussian MAC, $K$ active transmitters are fixed and known to the transmitters and the receiver; in the second scenario, called the Gaussian RAC, an unknown subset of $K$ transmitters is active, and neither the transmitters nor the receiver knows the set of active transmitter.

For the Gaussian MAC problem, we build on the RCU bound (Theorem 7.2.1) for general MACs to prove a third-order achievability result (Theorem 7.2.2). Our random encoder design chooses codewords distributed independently and uniformly on the $n$-dimensional sphere. At the receiver, we employ a maximum likelihood decoder. Compared to the result of MolavianJazi and Laneman [24], our coding scheme improves the achievable third-order term to $\frac{1}{2}\log n\mathbf{1} + O(1)\mathbf{1}$. Theorem 7.2.3 extends our result for the Gaussian MAC with two transmitters to the $K$-transmitter Gaussian MAC.

We generalize the rateless coding strategy in Chapter 6 for the permutation-invariant random access channels by allowing non-i.i.d. input distributions at the random encoding function. For the Gaussian RAC, our strategy uses concatenated codewords such that each sub-codeword is uniformly distributed on a power sphere and independent of the other sub-codewords. In our proposed coding strategy, the decoding occurs at finitely many time instants $n_0, \ldots, n_K$, with the choice of $n_k$ indicating that the decoder's estimate of the number of active transmitters is $k$. The receiver broadcasts a single bit to all transmitters at each decoding time, indicating whether or not it is ready to decode. The decoding rule combines a threshold rule based on the total received power and a maximum likelihood decoder. Building upon our result on the Gaussian MAC, we show in Theorem 7.3.1 that our rateless Gaussian RAC code achieves the same performance up to the third-order term as the best known code for the Gaussian MAC in operation (Corollary 7.2.1). Furthermore, by forcing decoding at time $n_K$ our feedback RAC code in Theorem 7.3.1 can be used with a $K$-transmitter MAC without feedback. While this can only reduce the error probability determined in Theorem 7.3.2 by eliminating the error events that result from deciding upon an incorrect number of active transmitters, that reduction is negligible in our asymptotic regime (see the proof of Theorem 7.3.1). Thus, Theorem 7.3.1 also describes the performance of the length-$n_K$ codebook of the RAC code when used with a $K$-transmitter MAC without feedback. That means that although the length-$n_K$ codebook of the RAC code is supported on only a subset of the power sphere (see Fig. 7.2), it achieves the same first three order terms on a $K$-transmitter MAC as the more traditional code in Corollary 7.2.1 that uses the entire power sphere.

*Chapter 8*

# CONCLUSION, FUTURE WORK, AND OPEN PROBLEMS

## 8.1 Conclusion

With stringent latency and reliability constraints of ultra-reliable, low-latency communication, non-asymptotic analyses of channel coding problems have become more and more important for code design and understanding the fundamental limits. This thesis analyzes PPC codes without feedback, variable-length sparse stop-feedback codes over PPCs and MACs, and rateless RAC codes with non-asymptotic tightness in mind.

Ultra-reliable low-latency communication applications demand codes with error probability around $10^{-8}$–$10^{-6}$ and latency around 1 millisecond, which corresponds to a few hundreds in blocklength; Polyanskiy *et al.*'s CLT approximation from [5] becomes inaccurate for such applications (see Fig. 3.1). In Chapter 3, we investigate the third-order asymptotics of the logarithm of the maximum achievable message set size for nonsingular DM-PPCs and the Gaussian PPC in the MD regime. Our asymptotic approximations in Theorem 3.3.1 and Theorem 3.3.2 that involve the channel skewness are the most accurate among the state-of-the-art expansions from the literature in the ultra-reliable low-latency communication regime. Using similar techniques, in Theorem 3.3.5, we also derive a refined approximation for the minimum achievable type-II error of BHTs. Our results show that in the low-error and high-reliability regime, the channel skewness is very crucial to obtain tight approximations.

Chapters 4–5 investigate the maximum achievable message set size for VLSF codes that have only a small number of feedback instances over PPCs and MACs. The central results in Theorem 4.3.1 and Theorem 5.3.1 show the achievability of VLSF codes, where the values of $L$ decoding times $n_1, \dots, n_L$ are optimized. In sparse VLSF codes, the optimization of $n_1, \dots, n_L$ is particularly important for this class of codes since to achieve the same performance as $L = O(1)$ optimized decoding times (Theorem 4.3.1), one needs $\Omega\left(\sqrt{\frac{N}{\ln_{(L-1)}(N)}}\right)$ uniformly-spaced decoding times (Theorem 4.3.3).

Chapters 6–7 investigate the RAC codes over general permutation-invariant

RACs and the Gaussian RAC, respectively. In RAC codes, we utilize the stop-feedback to synchronize the transmitters and the receiver in a channel model where neither the transmitters nor the receiver knows the number of active transmitters. Our code uses a single information density threshold rules, while codes such as in [19], [112] use $2^k - 1$ simultaneous threshold-rules for $k$-MAC. Our central result in Theorem 6.3.1 shows that as long as the total number of transmitters satisfies $K < \infty$, there is no loss in the first two terms in the maximum achievable message set size even if the decoder is tasked with decoding transmitter identity. Chapter 7 extends this result to the Gaussian RAC by designing codewords that concatenate $K$ sub-codewords of block-lengths $n_1, n_2 - n_1, \dots, n_K - n_{K-1}$, each drawn from a uniform distribution on a sphere of radius $\sqrt{(n_i - n_{i-1})P}$. While the codes in Chapter 6 employ i.i.d. random codewords, Chapter 7 contributes to develop tools and techniques to analyze codes that do not employ i.i.d. random codewords.

Below, we discuss the future research directions, some of which are already discussed throughout the thesis.

## 8.2 On the Third-Order Analysis of DM-PPCs

For DM-PPCs, the state-of-the-art error analyses in the CLT and LD regimes ([35] and [33], respectively) both start from the RCU bound in [5, Th. 16], then weaken it in different ways, and then bound the probabilities in the weakened bound using appropriate probability theorems from Chapter 2. Namely, in [33], which considers the LD regime, the information density $\imath(x; y)$ used in the proof is replaced by

$$\log \frac{P_{Y|X}(y|x)}{Q_Y(y)} \tag{8.1}$$

where

$$Q_Y(y) \triangleq c \left( \sum_{x \in \mathcal{X}} P_X(x) P_{Y|X}(y|x)^{1/1+\rho} \right)^{1+\rho}, \ y \in \mathcal{Y}. \tag{8.2}$$

where $c$ is a normalizing constant, and $\rho \in [0, 1]$ is a parameter to be optimized. Note that since the $\rho = 0$ case reduces to the information density, the LD approach can only improve the resulting bound from the CLT (information density) approach. In Chapter 3, we choose to use the same approach in the CLT regime, i.e., $\rho = 0$ since allowing an arbitrary $\rho$ makes the analysis more cumbersome in the MD regime.

This difference in the proof techniques brings the question whether one can unify the weakening methods used in the CLT, MD, and LD regimes so that the resulting asymptotic expansion for the maximum achievable message set size is the tightest in all three regimes. The implications of such a possible unification are beyond "the proof technique" because it would also imply that the information density is not the right metric in threshold decoders when the error probability is small enough.

When we turn to the Gaussian PPC, we observe that such a unification is indeed possible. In Chapter 3, following Shannon's weakening [6] of the RCU bound rather than the standard information-density based weakening results in a better lower bound on the channel skewness, which matches the upper bound.

## 8.3 Different Directions in Limiting the Feedback in VLSF Codes

In Chapters 4–5, we focus on the sparse, stop-feedback codes. The other direction of the limited feedback spectrum that we discuss in Section 1.2 (e.g., sparse with full feedback) is also practically and theoretically interesting since there might be scenarios where bursty feedback is sparsely available. Moreover, we can also consider the scenario where the feedback is limited by $R_{\mathrm{fb}}$ bits. In this case, one strategy is to design a variable-length code so that the receiver requests a shorter or a longer codeword from the transmitter depending on how reliable its current estimated message is, and informs the transmitter about this codeword length using $R_{\mathrm{fb}}$ bits available. We leave this research direction as future work.

## 8.4 Converse for VLSF Codes with $L$ Decoding Times

One of the most desirable results that would enhance our findings is a converse with a second-order term matching that in Theorem 4.3.1. Towards this goal, we can use the meta-converse that we derive in Theorem C.4.1, which converts the problem into finding the fundamental limits of sequential hypothesis testing. However, this new problem is still difficult. In the case where all times up to a fixed $n_L$ are available for decision-making, [83, Th. 3.2.3] characterizes the optimal two-sided test, where the lower and upper thresholds are defined implicitly. Despite being challenging, the investigation of what these thresholds would be if $L$ out of $n_L$ times are available can give us a solution to our converse problem.

## 8.5 Converse for the RAC

Whether the second-order term achieved in Theorem 6.3.1 is tight is one of the most important questions that this thesis unfortunately does not answer. We first note that any converse result on a fixed-length, no-feedback MAC code gives a converse for our RAC model because the encoding function in our RAC code definition does not use depend on the feedback, and because introducing uncertainty in the number of active transmitter cannot increase the maximum achievable rate. Even after this observation, the task of deriving a tight converse in the second-order term remarkably remains a very difficult one. Between Ahlswede's result [118] in 1982 and Kosut's result [23] in 2022, there had been no improvement on the converse bounds for MACs. Yet, Kosut's result in [23] only shows that the second-order term in Theorem 6.3.1 is order-optimal, i.e., it is $O(\sqrt{n})$, but it does not answer whether the dispersion $V_k$ is optimal. We leave this question as an open problem.

# BIBLIOGRAPHY

[1] C. E. Shannon, “A mathematical theory of communication,” *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948, ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[2] Y. Polyanskiy, “Channel coding: Non-asymptotic fundamental limits,” Ph.D. dissertation, Princeton University, Nov. 2010.

[3] S. Verdu and T. S. Han, “A general formula for channel capacity,” *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1147–1157, Jul. 1994. DOI: 10.1109/18.335960.

[4] M. Hayashi, “Information spectrum approach to second-order coding rate in channel coding,” *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 4947–4966, Nov. 2009. DOI: 10.1109/TIT.2009.2030478.

[5] Y. Polyanskiy, H. V. Poor, and S. Verdu, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010, ISSN: 0018-9448. DOI: 10.1109/TIT.2010.2043769.

[6] C. E. Shannon, “Probability of error for optimal codes in a Gaussian channel,” *The Bell System Technical Journal*, vol. 38, no. 3, pp. 611–656, May 1959, ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1959.tb03905.x.

[7] V. Strassen, “Asymptotische abschätzugen in Shannon’s informationstheorie,” in *Trans. Third Prague Conf. Inf. Theory*, Prague, 1962, pp. 689–723.

[8] R. G. Gallager, *Information Theory and Reliable Communication*. New York, NY, USA: Wiley, 1968, ISBN: 0471290483.

[9] V. Kostina, “Lossy data compression: Nonasymptotic fundamental limits,” Ph.D. dissertation, Princeton University, Sep. 2013.

[10] Y. Sakai, R. C. Yavas, and V. Y. F. Tan, “Third-order asymptotics of variable-length compression allowing errors,” *IEEE Tran. Inf. Theory*, vol. 67, no. 12, pp. 7708–7722, Dec. 2021. DOI: 10.1109/TIT.2021.3117591.

[11] J. Scarlett and V. Cevher, “Phase transitions in group testing,” in *Proc. 27th Annual ACM-SIAM Symposium on Discrete Algorithms*, ser. SODA ’16, Arlington, Virginia: Society for Industrial and Applied Mathematics, Jan. 2016, pp. 40–53, ISBN: 9781611974331. DOI: 10.1137/1.9781611974331.ch4.

[12] C. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. on Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956. DOI: 10.1109/TIT.1956.1056798.

[13] M. Horstein, "Sequential transmission using noiseless feedback," *IEEE Trans. Inf. Theory*, vol. 9, no. 3, pp. 136–143, Jul. 1963. DOI: 10.1109/TIT.1963.1057832.

[14] J. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback–I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, no. 2, pp. 172–182, Apr. 1966. DOI: 10.1109/TIT.1966.1053879.

[15] A. B. Wagner, N. V. Shende, and Y. Altuğ, "A new method for employing feedback to improve coding performance," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6660–6681, Nov. 2020. DOI: 10.1109/TIT.2020.2997385.

[16] M. V. Burnashev, "Data transmission over a discrete channel with feedback: Random transmission time," *Problems of Information Transmission*, vol. 12, no. 4, pp. 10–30, 1976.

[17] G. Forney, "Exponential error bounds for erasure, list, and decision feedback schemes," *IEEE Trans. Inf. Theory*, vol. 14, no. 2, pp. 206–220, 1968. DOI: 10.1109/TIT.1968.1054129.

[18] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Feedback in the non-asymptotic regime," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4903–4925, Aug. 2011. DOI: 10.1109/TIT.2011.2158476.

[19] Y.-W. Huang and P. Moulin, "Finite blocklength coding for multiple access channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012, pp. 831–835. DOI: 10.1109/ISIT.2012.6284677.

[20] E. M. Jazi and J. N. Laneman, "Simpler achievable rate regions for multiaccess with finite blocklength," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, USA, Jul. 2012, pp. 36–40.

[21] V. Y. Tan and O. Kosut, "On the dispersions of three network information theory problems," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 881–903, Feb. 2014. DOI: 10.1109/TIT.2013.2291231.

[22] J. Scarlett, A. Martinez, and A. G. i Fàbregas, "Second-order rate region of constant-composition codes for the multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 157–172, Jan. 2015, ISSN: 0018-9448. DOI: 10.1109/TIT.2014.2371026.

[23] O. Kosut, "A second-order converse bound for the multiple-access channel via wringing dependence," *IEEE Tran, Inf. Theory*, vol. 68, no. 6, pp. 3552–3584, Jun. 2022. DOI: 10.1109/TIT.2022.3151711.

[24] E. MolavianJazi and J. N. Laneman, "A second-order achievable rate region for Gaussian multi-access channels via a central limit theorem for functions," *IEEE Trans. Inf. Theory*, vol. 61, no. 12, pp. 6719–6733, Dec. 2015.

[25] W. Feller, *An Introduction to Probability Theory and its Applications*, Second. John Wiley & Sons, 1971, vol. II.

[26] I. G. Shevtsova, "On the absolute constants in the berry–esseen inequality and its structural and nonuniform improvements," *Informatika i Ee Primeneniya [Informatics and its Applications]*, vol. 7, no. 1, pp. 124–125, 2013.

[27] J. E. Kolassa, *Series approximation methods in statistics*. NY, USA: Springer, 2006, vol. 88.

[28] V. V. Petrov, *Sums of independent random variables*. New York, USA: Springer, Berlin, Heidelberg, 1975.

[29] E. A. Cornish and R. A. Fisher, "Moments and cumulants in the specification of distributions," vol. 5, no. 4, pp. 307–320, 1938, ISSN: 03731138.

[30] N. R. Chaganty and J. Sethuraman, "Strong large deviation and local limit theorems," *The Annals of Probability*, vol. 21, no. 3, pp. 1671–1690, Jul. 1993. DOI: 10.1214/aop/1176989136.

[31] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*. Berlin, Germany: Springer-Verlag, 2009, ISBN: 9783642033117.

[32] N. R. Chaganty and J. Sethuraman, "Multidimensional strong large deviation theorems," *Journal of Statistical Planning and Inference*, vol. 55, no. 3, pp. 265–280, Nov. 1996, ISSN: 0378-3758. DOI: https://doi.org/10.1016/S0378-3758(96)00083-3.

[33] Y. Altuğ and A. B. Wagner, "Refinement of the random coding bound," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6005–6023, Oct. 2014. DOI: 10.1109/TIT.2014.2345374.

[34] R. W. Butler, *Saddlepoint Approximations with Applications*, ser. Cambridge Series in Statistical and Probabilistic Mathematics. Cambridge University Press, 2007. DOI: 10.1017/CBO9780511619083.

[35] P. Moulin, "The log-volume of optimal codes for memoryless channels, asymptotically within a few nats," *IEEE Trans. Inf. Theory*, vol. 63, no. 4, pp. 2278–2313, Apr. 2017. DOI: 10.1109/TIT.2016.2643681.

[36] H. Yang, R. C. Yavas, V. Kostina, and R. D. Wesel, "Variable-length coding for binary-input channels with limited stop feedback," *arXiv:2205.15399*, May 2022.

[37] M. Shirvanimoghaddam, M. S. Mohammadi, R. Abbas, *et al.*, "Short block-length codes for ultra-reliable low latency communications," *IEEE Communications Magazine*, vol. 57, no. 2, pp. 130–137, 2019. DOI: 10.1109/MCOM.2018.1800181.

[38] Y. Altuğ and A. B. Wagner, "On exact asymptotics of the error probability in channel coding: Symmetric channels," *IEEE Trans. Inf. Theory*, vol. 67, no. 2, pp. 844–868, Feb. 2021. DOI: 10.1109/TIT.2020.3042592.

[39] J. Honda, "Exact asymptotics of random coding error probability for general memoryless channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 1844–1848. DOI: 10.1109/ISIT.2018.8437822.

[40] J. Font-Segura, A. Martinez, and A. G. i Fàbregas, "Asymptotics of the random coding union bound," in *Int. Symp. Inf. Theory and Its Applications (ISITA)*, Singapore, Oct. 2018, pp. 125–129. DOI: 10.23919/ISITA.2018.8664295.

[41] T. Erseghe, "Coding in the finite-blocklength regime: Bounds based on laplace integrals and their asymptotic approximations," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 6854–6883, Dec. 2016. DOI: 10.1109/TIT.2016.2616900.

[42] Y. Altuğ and A. B. Wagner, "Moderate deviations in channel coding," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4417–4426, Aug. 2014. DOI: 10.1109/TIT.2014.2323418.

[43] M. Tomamichel and V. Y. F. Tan, "A tight upper bound for the third-order asymptotics of discrete memoryless channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, Jul. 2013, pp. 1536–1540. DOI: 10.1109/ISIT.2013.6620484.

[44] V. Y. F. Tan and M. Tomamichel, "The third-order term in the normal approximation for the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2430–2438, May 2015, ISSN: 0018-9448. DOI: 10.1109/TIT.2015.2411256.

[45] Y. Polyanskiy and S. Verdú, "Channel dispersion and moderate deviations limits for memoryless channels," in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2010, pp. 1334–1339.

[46] C. Chubb, V. Y. F. Tan, and M. Tomamichel, "Moderate deviation analysis for classical communication over quantum channels," *Commun. Math. Phys.*, vol. 355, pp. 1283–1315, Aug. 2017.

[47] V. Y. F. Tan, "Moderate-deviations of lossy source coding for discrete and gaussian sources," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Jul. 2012, pp. 920–924. DOI: 10.1109/ISIT.2012.6284697.

[48] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. NJ, USA: Wiley, 2006.

[49] I. Sason, "Moderate deviations analysis of binary hypothesis testing," in *IEEE Int. Symp. on Inf. Theory (ISIT)*, Jul. 2012, pp. 821–825. DOI: 10.1109/ISIT.2012.6284675.

[50] S. Chen, M. Effros, and V. Kostina, "Lossless source coding in the point-to-point, multiple access, and random access scenarios," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6688–6722, Nov. 2020. DOI: 10.1109/TIT.2020.3005155.

[51] R. Blahut, "Hypothesis testing and information theory," *IEEE Trans. Inf. Theory*, vol. 20, no. 4, pp. 405–417, Jul. 1974. DOI: 10.1109/TIT.1974.1055254.

[52] V. Kostina and S. Verdú, "Fixed-length lossy compression in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3309–3338, Jun. 2012. DOI: 10.1109/TIT.2012.2186786.

[53] ——, "Lossy joint source-channel coding in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2545–2575, May 2013. DOI: 10.1109/TIT.2013.2238657.

[54] Y. Altuğ and A. B. Wagner, "The third-order term in the normal approximation for singular channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, Jul. 2014, pp. 1897–1901. DOI: 10.1109/ISIT.2014.6875163.

[55] Y. Polyanskiy, "Saddle point in the minimax converse for channel coding," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2576–2595, 2013. DOI: 10.1109/TIT.2012.2236382.

[56] T. S. Han, *Information-Spectrum Methods in Information Theory*. Berlin, Germany: Springer-Verlag, 2003, ISBN: 3662120674.

[57] Y. Polyanskiy and Y. Wu, *Lecture notes on information theory*, [Online]. Available: http://people.lids.mit.edu/yp/homepage/data/itlectures_v5.pdf, Aug. 2017.

[58] A. Tchamkerten and I. E. Telatar, "Variable length coding over an unknown channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2126–2145, May 2006, ISSN: 0018-9448. DOI: 10.1109/TIT.2006.872974.

[59] M. Naghshvar, T. Javidi, and M. Wigger, "Extrinsic jensen–shannon divergence: Applications to variable-length coding," *IEEE Trans. Inf, Theory*, vol. 61, no. 4, pp. 2148–2164, Apr. 2015. DOI: 10.1109/TIT.2015.2401004.

[60] H. Yang, M. Pan, A. Antonini, and R. D. Wesel, "Sequential transmission over binary asymmetric channels with feedback," *arXiv:2111.15042*, Nov. 2021. DOI: 10.48550/ARXIV.2111.15042.

[61] N. Guo and V. Kostina, "Instantaneous sed coding over a dmc," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 148–153. DOI: 10.1109/ISIT45174.2021.9518087.

[62] S. L. Fong and V. Y. F. Tan, "Asymptotic expansions for the AWGN channel with feedback under a peak power constraint," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, China, Jun. 2015, pp. 311–315. DOI: 10.1109/ISIT.2015.7282467.

[63] Y. Altuğ, H. V. Poor, and S. Verdú, "Variable-length channel codes with probabilistic delay guarantees," in *53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, USA, Sep. 2015, pp. 642–649. DOI: 10.1109/ALLERTON.2015.7447065.

[64] J. Östman, R. Devassy, G. Durisi, and E. G. Ström, "Short-packet transmission via variable-length codes in the presence of noisy stop feedback," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 214–227, 2021. DOI: 10.1109/TWC.2020.3024152.

[65] S. Ginzach, N. Merhav, and I. Sason, "Random-coding error exponent of variable-length codes with a single-bit noiseless feedback," in *IEEE Inf. Theory Workshop (ITW)*, Nov. 2017, pp. 584–588. DOI: 10.1109/ITW.2017.8278012.

[66] P. Berlin, B. Nakiboğlu, B. Rimoldi, and E. Telatar, "A simple converse of burnashev's reliability function," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3074–3080, 2009. DOI: 10.1109/TIT.2009.2021322.

[67] A. Wald and J. Wolfowitz, "Optimum Character of the Sequential Probability Ratio Test," *The Annals of Mathematical Statistics*, vol. 19, no. 3, pp. 326–339, 1948. DOI: 10.1214/aoms/1177730197.

[68] Y. Li and V. Y. F. Tan, "Second-order asymptotics of sequential hypothesis testing," *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 7222–7230, 2020. DOI: 10.1109/TIT.2020.3006014.

[69] J. Pan, Y. Li, and V. Y. F. Tan, "Asymptotics of sequential composite hypothesis testing under probabilistic constraints," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 172–177. DOI: 10.1109/ISIT45174.2021.9517987.

[70] A. Lalitha and T. Javidi, "Reliability of sequential hypothesis testing can be achieved by an almost-fixed-length test," in *2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 1710–1714. DOI: 10.1109/ISIT.2016.7541591.

[71] L. V. Truong and V. Y. F. Tan, "On Gaussian MACs with variable-length feedback and non-vanishing error probabilities," *arXiv:1609.00594v2*, Sep. 2016.

[72] ——, "On Gaussian MACs with variable-length feedback and non-vanishing error probabilities," *IEEE Trans. Inf. Theor.*, vol. 64, no. 4, pp. 2333–2346, Apr. 2018, ISSN: 0018-9448. DOI: 10.1109/TIT.2018.2793283.

[73] K. F. Trillingsgaard, W. Yang, G. Durisi, and P. Popovski, "Common-message broadcast channels with feedback in the nonasymptotic regime: Stop feedback," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7686–7718, Dec. 2018. DOI: 10.1109/TIT.2018.2868953.

[74] M. Heidari, A. Anastasopoulos, and S. S. Pradhan, "On the reliability function of discrete memoryless multiple-access channel with feedback," in *2018 IEEE Information Theory Workshop (ITW)*, 2018, pp. 1–5. DOI: 10.1109/ITW.2018.8613494.

[75] K. F. Trillingsgaard and P. Popovski, "Variable-length coding for short packets over a multiple access channel with feedback," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, 2014, pp. 796–800. DOI: 10.1109/ISWCS.2014.6933462.

[76] S. H. Kim, D. K. Sung, and T. Le-Ngoc, "Variable-length feedback codes under a strict delay constraint," *IEEE Communications Letters*, vol. 19, no. 4, pp. 513–516, Apr. 2015. DOI: 10.1109/LCOMM.2015.2398866.

[77] K. Vakilinia, S. V. S. Ranganathan, D. Divsalar, and R. D. Wesel, "Optimizing transmission lengths for limited feedback with nonbinary ldpc examples," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2245–2257, 2016. DOI: 10.1109/TCOMM.2016.2538770.

[78] A. R. Williamson, T. Chen, and R. D. Wesel, "Variable-length convolutional coding for short blocklengths with decision feedback," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2389–2403, Jul. 2015. DOI: 10.1109/TCOMM.2015.2429583.

[79] A. Heidarzadeh, J. Chamberland, R. D. Wesel, and P. Parag, "A systematic approach to incremental redundancy with application to erasure channels," *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 2620–2631, Apr. 2019. DOI: 10.1109/TCOMM.2018.2889254.

[80] A. Lalitha and T. Javidi, "On error exponents of almost-fixed-length channel codes and hypothesis tests," *arXiv:2012.00077*, Nov. 2020. DOI: 10.48550/ARXIV.2012.00077.

[81] H. Yamamoto and K. Itoh, "Asymptotic performance of a modified schalkwijk-barron scheme for channels with noiseless feedback (corresp.)," *IEEE Trans. Inf. Theory*, vol. 25, no. 6, pp. 729–733, Nov. 1979. DOI: 10.1109/TIT.1979.1056119.

[82] R. C. Yavas, V. Kostina, and M. Effros, "Variable-length feedback codes with several decoding times for the Gaussian channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 1883–1888. DOI: 10.1109/ISIT45174.2021.9517993.

[83] A. Tartakovsky, I. Nikiforov, and M. Basseville, *Sequential Analysis: Hypothesis Testing and Changepoint Detection*, 1st. Chapman and Hall CRC, 2014, ISBN: 1439838208.

[84] W. Yang, G. Caire, G. Durisi, and Y. Polyanskiy, "Optimum power control at finite blocklength," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4598–4615, Sep. 2015. DOI: 10.1109/TIT.2015.2456175.

[85] R. C. Yavas, V. Kostina, and M. Effros, "Random access channel coding in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2115–2140, 2021. DOI: 10.1109/TIT.2020.3047630.

[86] L. G. Roberts, "ALOHA packet system with and without slots and capture," *SIGCOMM Comput. Commun. Rev.*, vol. 5, no. 2, pp. 28–42, Apr. 1975, ISSN: 0146-4833. DOI: 10.1145/1024916.1024920.

[87] A. G. D'yachkov and V. V. Rykov, "On a coding model for a multiple-access adder channel," *Problemy Peredachi Informatsii*, vol. 17, no. 2, pp. 26–38, 1981.

[88] P. Mathys, "A class of codes for a $t$ active users out of $n$ multiple-access communication system," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1206–1219, 1990.

[89] L. A. Bassalygo and M. S. Pinsker, "Restricted asynchronous multiple access," *Problemy Peredachi Informatsii*, vol. 19, no. 4, pp. 92–96, 1983.

[90] Y. Polyanskiy, "A perspective on massive random-access," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2523–2527.

[91] O. Ordentlich and Y. Polyanskiy, "Low complexity schemes for the random access Gaussian channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2528–2532.

[92] M. Ebrahimi, F. Lahouti, and V. Kostina, "Coded random access design for constrained outage," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2732–2736.

[93] P. Minero, M. Franceschetti, and D. N. C. Tse, "Random access: An information-theoretic perspective," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 909–930, Feb. 2012, ISSN: 0018-9448. DOI: 10.1109/TIT.2011.2173711.

[94] D. Blackwell, L. Breiman, and A. Thomasian, "The capacity of a class of channels," *The Annals of Mathematical Statistics*, pp. 1229–1241, 1959.

[95] Y. Polyanskiy, "On dispersion of compound DMCs," in *Proceedings 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, USA, Oct. 2013, pp. 26–32. DOI: 10.1109/Allerton.2013.6736501.

[96] A. Tchamkerten and E. Telatar, "A feedback strategy for binary symmetric channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Lausanne, Switzerland, 2002, p. 362.

[97] S. C. Draper, B. J. Frey, and F. R. Kschischang, "Efficient variable length channel coding for unknown DMCs," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Chicago, IL, USA, Jun. 2004, pp. 379–379.

[98] N. Shulman, "Communication over an unknown channel via common broadcasting," Ph.D. dissertation, Tel Aviv University, 2003.

[99] N. Blits and M. Feder, "Universal rateless coding with finite message set," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, USA, Jul. 2012, pp. 1772–1776.

[100] T. Berger, "The Poisson multiple-access conflict resolution problem," *Multi-user communication systems*, pp. 1–27, 1981.

[101] L. V. Truong and V. Y. Tan, "On the Gaussian MAC with stop-feedback," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2303–2307.

[102] M. B. Malyutov, "The separating property of random matrices," *Mathematical notes of the Academy of Sciences of the USSR*, vol. 23, no. 1, pp. 84–91, 1978.

[103] M. B. Malyutov and P. S. Mateev, "Planning of screening experiments for a nonsymmetric response function," *Mathematical notes of the Academy of Sciences of the USSR*, vol. 27, no. 1, pp. 57–68, 1980.

[104] G. K. Atia and V. Saligrama, "Boolean compressed sensing and noisy group testing," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1880–1901, Mar. 2012.

[105] J. Scarlett and V. Cevher, "Limits on support recovery with probabilistic models: An information-theoretic framework," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 593–620, Jan. 2017.

[106] A. B. Wagner, N. V. Shende, and Y. Altuğ, "A new method for employing feedback to improve coding performance," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6660–6681, Nov. 2020. DOI: 10.1109/TIT.2020.2997385.

[107] A. D. Sarwate and M. Gastpar, "Some observations on limited feedback for multiaccess channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seoul, Korea, Jun. 2009, pp. 394–397. DOI: 10.1109/ISIT.2009.5205742.

[108] X. Chen, T. Y. Chen, and D. Guo, "Capacity of Gaussian many-access channels," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3516–3539, Jun. 2017, ISSN: 0018-9448. DOI: 10.1109/TIT.2017.2668391.

[109] E. Haim, Y. Kochman, and U. Erez, "A note on the dispersion of network problems," in *2012 IEEE 27th Convention of Electrical and Electronics Engineers in Israel*, Nov. 2012, pp. 1–9.

[110] Y. Watanabe, "The total capacity of two-user multiple-access channel with binary output," *IEEE Trans. Inf. Theory*, vol. 42, no. 5, pp. 1453–1465, Sep. 1996.

[111] P. Moulin, "The log-volume of optimal constant-composition codes for memoryless channels, within o(1) bits," in *Proc. 2012 IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, USA, Jul. 2012, pp. 826–830.

[112] E. MolavianJazi and J. N. Laneman, "On the second-order cost of TDMA for Gaussian multiple access," in *Proc. 2014 IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, Jun. 2014, pp. 266–270.

[113] Y. Liu and M. Effros, "Finite-blocklength and error-exponent analyses for LDPC codes in point-to-point and multiple access communication," in *Proc. 2020 IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 361–366. DOI: 10.1109/ISIT44484.2020.9173963.

[114] Y. Liu and M. Effros, "Finite-blocklength and error-exponent analyses for LDPC codes in point-to-point and multiple access communication," *arXiv Preprints, arxiv/2005.06428*, May 2020.

[115] H. H. J. Liao, "Multiple access channels," Ph.D. dissertation, University of Hawaii, Honolulu, HI, USA, Sep. 1972.

[116] R. Ahlswede, "Multi-way communication channels," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Tsahkadsor, Armenia, USSR, Sep. 1971.

[117] G. Dueck, "The strong converse to the coding theorem for the multiple–access channel," *J. Comb. Inform. Syst. Sci*, vol. 6, no. 3, pp. 187–196, 1981.

[118] R. Ahlswede, "An elementary proof of the strong converse theorem for the multiple-access channel," *J. Combinatorics, Information and System Sciences*, vol. 7, no. 3, 1982.

[119] S. L. Fong and V. Y. F. Tan, "A proof of the strong converse theorem for Gaussian multiple access channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4376–4394, Aug. 2016, ISSN: 0018-9448. DOI: 10.1109/TIT.2016.2570243.

[120] P. Moulin, "A new metaconverse and outer region for finite-blocklength MACs," in *Proceedings 2013 Information Theory and Applications Workshop (ITA)*, San Diego, CA, USA, Feb. 2013, pp. 1–8. DOI: 10.1109/ITA.2013.6503004.

[121] G. Dueck, "Maximal error capacity regions are smaller than average error capacity regions for multi-user channels," *Problems of Control and Information Theory*, vol. 7, pp. 409–413, 1978.

[122] O. Zeitouni and M. Gutman, "On universal hypotheses testing via large deviations," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 285–290, Mar. 1991, ISSN: 0018-9448. DOI: 10.1109/18.75244.

[123] Y. Huang and P. Moulin, "Strong large deviations for composite hypothesis testing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2014, pp. 556–560. DOI: 10.1109/ISIT.2014.6874894.

[124] W. Hoeffding, "Asymptotically optimal tests for multinomial distributions," *Ann. Math. Statist.*, vol. 36, no. 2, pp. 369–401, Apr. 1965. DOI: 10.1214/aoms/1177700150.

[125] I. Csiszár and P. C. Shields, "Information theory and statistics: A tutorial," *Commun. Inf. Theory*, vol. 1, no. 4, pp. 417–528, Dec. 2004, ISSN: 1567-2190. DOI: 10.1561/0100000004.

[126] A. L. Gibbs and F. E. Su, "On choosing and bounding probability metrics," *INTERNAT. STATIST. REV.*, pp. 419–435, 2002.

[127] S. Kullback, "Correction to a lower bound for discrimination information in terms of variation," *IEEE Trans. Inf. Theory*, vol. 16, no. 5, pp. 652–652, Sep. 1970, ISSN: 0018-9448. DOI: 10.1109/TIT.1970.1054514.

[128] A. N. Kolmogorov, "Sulla Determinazione Empirica di una Legge di Distribuzione," *Giornale dell'Istituto Italiano degli Attuari*, vol. 4, pp. 83–91, 1933.

[129] A. Dvoretzky, J. Kiefer, and J. Wolfowitz, "Asymptotic minimax character of the sample distribution function and of the classical multinomial estimator," *Ann. Math. Statist.*, vol. 27, no. 3, pp. 642–669, Sep. 1956. DOI: 10.1214/aoms/1177728174.

[130] P. Massart, "The tight constant in the Dvoretzky-Kiefer-Wolfowitz inequality," *Ann. Probab.*, vol. 18, no. 3, pp. 1269–1283, Jul. 1990. DOI: 10.1214/aop/1176990746.

[131] S. Chen, M. Effros, and V. Kostina, "Lossless source coding in the point-to-point, multiple access, and random access scenarios," *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6688–6722, Jul. 2020. DOI: 10.1109/TIT.2020.3005155.

[132] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Quasi-static multiple-antenna fading channels at finite blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4232–4265, 2014. DOI: 10.1109/TIT.2014.2318726.

[133] S. S. Kowshik, K. Andreev, A. Frolov, and Y. Polyanskiy, "Energy efficient coded random access for the wireless uplink," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4694–4708, 2020. DOI: 10.1109/TCOMM.2020.3000635.

[134] S. Chen, M. Effros, and V. Kostina, "Lossless source coding in the point-to-point, multiple access, and random access scenarios," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1692–1696. DOI: 10.1109/ISIT.2019.8849742.

[135] E. MolavianJazi, "A unified approach to Gaussian channels with finite blocklength," Ph.D. dissertation, University of Notre Dame, Jul. 2014.

[136] V. Bentkus, "A Lyapunov-type bound in $\mathbb{R}^d$," *Theory of Probability & Its Applications*, vol. 49, no. 2, pp. 311–323, 2005. DOI: 10.1137/S0040585X97981123.

[137] M. Raič, "A multivariate Berry–Esseen theorem with explicit constants," *Bernoulli*, vol. 25, no. 4A, pp. 2824–2853, 2019.

[138] L. Devroye, A. Mehrabian, and T. Reddad, "The total variation distance between high-dimensional Gaussians," *arXiv preprint arXiv:1810.08693*, 2018.

[139] S. M. Rump, "Estimates of the determinant of a perturbed identity matrix," *Linear Algebra and its Applications*, vol. 558, pp. 101–107, 2018, ISSN: 0024-3795. DOI: https://doi.org/10.1016/j.laa.2018.08.009.

[140] A. J. Stam, "Limit theorems for uniform distributions on spheres in high-dimensional Euclidean spaces," *Journal of Applied Probability*, vol. 19, no. 1, pp. 221–228, 1982, ISSN: 00219002.

[141] W. Hoeffding and J. Wolfowitz, "Distinguishability of sets of distributions," *Ann. Math. Statist.*, vol. 29, no. 3, pp. 700–718, Sep. 1958. DOI: 10.1214/aoms/1177706531.

[142] W. Sendler, "A note on the proof of the zero-one law of Blum and Pathak," *The Annals of Probability*, vol. 3, no. 6, pp. 1055–1058, 1975. DOI: 10.1214/aop/1176996234.

[143] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*. Dover, 1972.

[144] R. A. Fisher and E. A. Cornish, "The percentile points of distributions having known cumulants," *Technometrics*, vol. 2, no. 2, pp. 209–225, 1960.

[145] C. van Eeden, "Some approximations to the percentage points of the non-central t-distribution," *Revue de l'Institut International de Statistique / Review of the International Statistical Institute*, vol. 29, no. 1, pp. 4–31, 1961.

[146] D. Hogben, R. S. Pinkham, and M. B. Wilk, "The moments of the non-central t-distribution," *Biometrika*, vol. 48, no. 3/4, pp. 465–468, Dec. 1961.

[147] A. Wald, "Sequential Tests of Statistical Hypotheses," *The Annals of Mathematical Statistics*, vol. 16, no. 2, pp. 117–186, 1945. DOI: 10.1214/aoms/1177731118.

[148] L. V. Truong, S. L. Fong, and V. Y. F. Tan, "On Gaussian channels with feedback under expected power constraints and with non-vanishing error probabilities," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1746–1765, Mar. 2017. DOI: 10.1109/TIT.2017.2648822.

[149] L. Shepp and I. Olkin, "Entropy of the sum of independent bernoulli random variables and of the multinomial distribution," in *Contributions to Probability*, Academic Press, 1981, pp. 201–206, ISBN: 978-0-12-274460-0. DOI: doi.org/10.1016/B978-0-12-274460-0.50022-9.

[150] H. G. Eggleston, *Convexity*, ser. Cambridge Tracts in Mathematics. Cambridge University Press, 1958. DOI: 10.1017/CBO9780511566172.

[151] C. Leang and D. Johnson, "On the asymptotics of m-hypothesis bayesian detection," *IEEE Trans. Inf. Theory*, vol. 43, no. 1, pp. 280–282, 1997. DOI: 10.1109/18.567705.

[152] R. Paris, "An inequality for the Bessel function $J_\nu(\nu x)$," *SIAM journal on mathematical analysis*, vol. 15, no. 1, pp. 203–205, 1984.

*Appendix A*

# APPENDIX FOR CHAPTER 2

## A.1 Proof of Lemma 2.4.1

Lemma 2.4.1 reduces to the Cornish-Fisher theorem if $y = O(1)$; therefore, we focus on the case $y \to \infty$ or $y \to -\infty$ with $y \in o(\sqrt{n})$. We here prove the case where $y \to \infty$. The case $y \to -\infty$ follows similarly using (2.30). From (2.31), we have

$$F_n(-x) = Q(x) \exp\left\{ -a_0 \frac{x^3}{\sqrt{n}} + a_1 \frac{x^4}{n} - O\left(\frac{x^5}{n^{3/2}}\right) + O\left(\frac{x}{\sqrt{n}}\right) \right\}. \qquad \text{(A.1)}$$

Let $x = y + \delta$ where $\delta/y \to 0$. Substituting $F_n(-x) = Q(y)$ into (A.1), we get

$$\frac{Q(y+\delta)}{Q(y)} = \exp\left\{ a_0 \frac{x^3}{\sqrt{n}} - a_1 \frac{x^4}{n} + O\left(\frac{y^5}{n^{3/2}}\right) + O\left(\frac{y}{\sqrt{n}}\right) \right\}. \qquad \text{(A.2)}$$

As $y \to \infty$, we have the asymptotic expansion [143, eq. 26.2.12]

$$Q(y) = \frac{1}{\sqrt{2\pi}} \exp\left\{ -\frac{y^2}{2} \right\} \frac{1}{y} \left( 1 - \frac{1}{y^2} + \frac{3}{y^4} - O\left(\frac{1}{y^6}\right) \right). \qquad \text{(A.3)}$$

Substituting (A.3) into the left-hand side of (A.2) and taking the logarithm of both sides of (A.2), we get

$$\begin{aligned} &-\delta y - \frac{\delta^2}{2} - \frac{\delta}{y} + O\left(\frac{\delta^2}{y^2}\right) \\ &= a_0 \frac{y^3}{\sqrt{n}} + a_0 \frac{3y^2\delta}{\sqrt{n}} + a_0 \frac{3y\delta^2}{\sqrt{n}} + a_0 \frac{\delta^3}{\sqrt{n}} - a_1 \frac{y^4}{n} \\ &\quad + O\left(\frac{y^5}{n^{3/2}}\right) + O\left(\frac{y^3\delta}{n}\right) + O\left(\frac{y}{\sqrt{n}}\right). \end{aligned} \qquad \text{(A.4)}$$

Equating the coefficients of $\frac{y^3}{\sqrt{n}}$ and $\frac{y^4}{n}$ of both sides of (A.4), we get

$$b_0 = a_0 \qquad \text{(A.5)}$$

$$b_1 = \frac{5}{2} a_0^2 + a_1, \qquad \text{(A.6)}$$

which completes the proof.

*Appendix B*

# APPENDIX FOR CHAPTER 3

## B.1 Proof of (3.119)

From (3.100) and (3.112), we get $\mathbf{a}_n \to (I(P_X), 0)$ as $n \to \infty$. To evaluate the gradient and the Hessian of $\Lambda(\mathbf{a}_n)$, we start from the equation in condition (ND)

$$\nabla\kappa(\mathbf{s}_n) = \mathbf{a}_n. \tag{B.1}$$

Viewing $\mathbf{a}_n$ as a vector-valued function of $\mathbf{s}_n$ and differentiating both sides of (B.1) with respect to $\mathbf{s}_n$, we get

$$J_{\mathbf{s}_n}(\mathbf{a}_n) = \nabla^2\kappa(\mathbf{s}_n), \tag{B.2}$$

where $J_{\mathbf{s}_n}(\mathbf{a}_n) \triangleq \begin{bmatrix} \frac{\partial a_{n,1}}{\partial s_{n,1}} & \frac{\partial a_{n,1}}{\partial s_{n,2}} \\ \frac{\partial a_{n,2}}{\partial s_{n,1}} & \frac{\partial a_{n,2}}{\partial s_{n,2}} \end{bmatrix}$ is the Jacobian of $\mathbf{a}_n$ with respect to $\mathbf{s}_n$.

Differentiating the equation $\Lambda(\mathbf{a}_n) = \langle \mathbf{s}_n, \nabla\kappa(\mathbf{s}_n)\rangle - \kappa(\mathbf{s}_n)$ with respect to $\mathbf{s}_n$, we get a 2-dimensional row vector

$$J_{\mathbf{s}_n}(\Lambda(\mathbf{a}_n)) = \mathbf{s}_n^\top \nabla^2\kappa(\mathbf{s}_n). \tag{B.3}$$

Applying the function inversion theorem and using (B.2), we reach

$$\begin{aligned} J_{\mathbf{a}_n}(\Lambda(\mathbf{a}_n)) &= J_{\mathbf{s}_n}(\Lambda(\mathbf{a}_n)) J_{\mathbf{a}_n}(\mathbf{s}_n) &\text{(B.4)}\\ &= \mathbf{s}_n^\top \nabla^2\kappa(\mathbf{s}_n)(\nabla^2\kappa)^{-1}(\mathbf{s}_n) &\text{(B.5)}\\ &= \mathbf{s}_n^\top, &\text{(B.6)} \end{aligned}$$

equivalently

$$\nabla\Lambda(\mathbf{a}_n) = \mathbf{s}_n. \tag{B.7}$$

Differentiating (B.7) with respect to $\mathbf{a}_n$, we get

$$\begin{aligned} \nabla^2\Lambda(\mathbf{a}_n) &= \nabla(\nabla\Lambda(\mathbf{a}_n)) &\text{(B.8)}\\ &= J_{\mathbf{a}_n}(\mathbf{s}_n) &\text{(B.9)}\\ &= (\nabla^2\kappa)^{-1}(\mathbf{s}_n). &\text{(B.10)} \end{aligned}$$

We would like to obtain the Taylor series expansion of $\Lambda(\cdot)$ around $\mathbf{a} = (I(P_X), 0)$. By direct computation, we get

$$\Lambda(\mathbf{a}) = I(P_X) \tag{B.11}$$

$$\nabla\Lambda(\mathbf{a}) = (1, 1) \tag{B.12}$$

$$\nabla\kappa((1, 1)) = \mathbf{a}, \tag{B.13}$$

giving $\mathbf{s}_n \to \mathbf{s} \triangleq (1, 1)$, which verifies condition (ND). Define

$$\mathbf{T} \triangleq (T_1, T_2) \tag{B.14}$$

$$T_1 \triangleq \log \frac{P_{Y|X}(Y|X)}{P_Y(Y)} \tag{B.15}$$

$$T_2 \triangleq \log \frac{P_{Y|X}(Y|\overline{X})}{P_{Y|X}(Y|X)}, \tag{B.16}$$

where $P_{X,\overline{X},Y}(x, \overline{x}, y) = P_X(x)P_X(\overline{x})P_{Y|X}(y|x)$. We have

$$\nabla^2\kappa(\mathbf{s}) = \mathrm{Cov}(\tilde{\mathbf{T}})^{-1}, \tag{B.17}$$

where $\tilde{\mathbf{T}}$ is distributed according to the tilted distribution

$$P_{\tilde{\mathbf{T}}} = \exp\{\langle \mathbf{s}, \mathbf{T} \rangle\} P_{\mathbf{T}} = \frac{P_{Y|X}(Y|\overline{X})}{P_Y(Y)} P_{\mathbf{T}}, \tag{B.18}$$

and $P_{\mathbf{T}}$ denotes the distribution of $\mathbf{T}$. We compute the inverse of the covariance matrix of $\tilde{\mathbf{T}}$ as

$$\mathrm{Cov}(\tilde{\mathbf{T}})^{-1} = \begin{bmatrix} \frac{2}{1+\eta(P_X)} & \frac{1}{1+\eta(P_X)} \\ \frac{1}{1+\eta(P_X)} & \frac{1}{1-\eta(P_X)^2} \end{bmatrix} \frac{1}{V_{\mathrm{u}}(P_X)}. \tag{B.19}$$

From (B.11), (B.12), and (B.19), we get

$$\begin{aligned} \Lambda(\mathbf{a}_n) &= I(P_X) + (a_{n,1} - I(P_X)) \\ &\quad + \frac{1}{2}(a_{n,1} - I(P_X))^2 \mathrm{Cov}(\tilde{\mathbf{T}})^{-1}_{1,1} + O(|a_{n,1} - I(P_X)|^3) \qquad \text{(B.20)} \\ &= a_{n,1} + \frac{1}{n}\frac{Q^{-1}(\epsilon_n)^2}{1+\eta(P_X)} + O\left(\frac{Q^{-1}(\epsilon_n)^3}{n^{3/2}}\right) + O\left(\frac{1}{n}\right). \qquad \text{(B.21)} \end{aligned}$$

### B.2 Proof of (3.127)

We solve the convex optimization problem in (3.126) by writing the Lagrangian

$$L(\mathbf{g}, \lambda) = \mathbf{g}^\top \mathbf{h} - \frac{1}{2}\mathbf{g}^\top \mathsf{J}\mathbf{g} - \lambda \mathbf{g}^\top \mathbf{1}. \tag{B.22}$$

The Karush-Kuhn-Tucker condition $\nabla L(\mathbf{g}, \lambda) = 0$ gives

$$\mathsf{J}\mathbf{g} = \mathbf{h} - \lambda \mathbf{1} \tag{B.23}$$

$$\mathbf{g}^\top \mathbf{1} = 0, \tag{B.24}$$

where $\mathsf{J}$ is given in (3.45). The equation (B.23) has a solution since both $\mathbf{h}$ and $\mathbf{1}$ are in the row space of $\mathsf{J}$, which is equal to the column space since $\mathsf{J}$ is symmetric. Solving the system of equations in (B.23) and (B.24), we get the dual variable

$$\lambda^* = \frac{\mathbf{1}^\top \mathsf{J}^+ \mathbf{h}}{\mathbf{1}^\top \mathsf{J}^+ \mathbf{1}}. \tag{B.25}$$

Plugging (B.25) in (B.24), we get

$$\begin{aligned} \mathbf{g}^* &= \tilde{\mathsf{J}}\mathbf{h} && \text{(B.26)} \\ &= -\frac{Q^{-1}(\epsilon_n)}{2\sqrt{n\underline{V}}} \tilde{\mathsf{J}} \mathbf{v}(P_X^*), && \text{(B.27)} \end{aligned}$$

where $\tilde{\mathsf{J}}$ and $\mathbf{v}$ are given in (3.49) and (3.50). An equivalent characterization of (B.27) in terms of the eigenvalue decomposition of $\mathsf{J}$ is given in [35, Lemma 1 (v)]. The value of the supremum in (3.126) is $\frac{1}{2}\mathbf{g}^{*\top}\tilde{\mathsf{J}}\mathbf{g}^* = A_0(P_X^*)Q^{-1}(\epsilon_n)^2$, where $A_0(\cdot)$ is given in (3.53).

## B.3 Proof of Lemma 3.4.2

We compute the first 3 central moments of the random variable $\sum_{i=1}^n \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}$, where $\mathbf{Y} \sim P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}}$, which is the sum of $n$ independent, but not necessarily identically distributed random variables. We have

$$\begin{aligned} &\frac{1}{n}\mathbb{E}\left[\sum_{i=1}^n \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}\right] \\ &= \sum_{y\in\mathcal{Y}} \sum_{\tilde{x}\in\mathcal{X}} \hat{P}_{\mathbf{x}}(\tilde{x}) P_{Y|X}(y|\tilde{x}) \log \frac{P_{Y|X}(y|\tilde{x})}{Q_Y(y)} && \text{(B.28)} \\ &= D_{\mathbf{x}}. && \text{(B.29)} \end{aligned}$$

Similarly, it follows that

$$\frac{1}{n}\mathrm{Var}\left[\sum_{i=1}^n \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}\right] = V_{\mathbf{x}} \tag{B.30}$$

$$\mathbb{E}\left[\left(\frac{1}{n}\sum_{i=1}^n \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)} - D_{\mathbf{x}}\right)^3\right] = T_{\mathbf{x}}. \tag{B.31}$$

Note that Cramér's condition in Theorem 2.4.1 is satisfied since $\log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}$ is a discrete random variable for all $i \in [n]$. Applying Lemma 2.4.1 by setting $X_i$ to $\log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}$ gives (3.129).

$$\begin{aligned}
&\frac{1}{n}\mathbb{E}\left[\sum_{i=1}^{n} \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}\right] \\
&= \sum_{y\in\mathcal{Y}} \sum_{\tilde{x}\in\mathcal{X}} \hat{P}_{\mathbf{x}}(\tilde{x}) P_{Y|X}(y|\tilde{x}) \log \frac{P_{Y|X}(y|\tilde{x})}{Q_Y(y)} \qquad \text{(B.32)} \\
&= D_{\mathbf{x}}. \qquad \text{(B.33)}
\end{aligned}$$

Similarly, it follows that

$$\frac{1}{n}\mathrm{Var}\left[\sum_{i=1}^{n} \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}\right] = V_{\mathbf{x}} \qquad \text{(B.34)}$$

$$\mathbb{E}\left[\left(\frac{1}{n}\sum_{i=1}^{n} \log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)} - D_{\mathbf{x}}\right)^3\right] = T_{\mathbf{x}}. \qquad \text{(B.35)}$$

Note that Cramér's condition in Theorem 2.4.1 is satisfied since $\log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}$ is a discrete random variable for all $i \in [n]$. Applying Lemma 2.4.1 by setting $X_i$ to $\log \frac{P_{Y|X}(Y_i|x_i)}{Q_Y(Y_i)}$ gives (3.129).

## B.4 Proof of Theorem 3.3.5

Assume that $\sum_{i=1}^{n} Z_i$ is lattice with span $h > 0$. Let $\underline{\gamma}$ and $\overline{\gamma}$ satisfy

$$\mathbb{P}\left[\sum_{i=1}^{n} Z_i \geq \underline{\gamma}\right] = 1 - \underline{\epsilon}_n \geq 1 - \epsilon_n \qquad \text{(B.36)}$$

$$\mathbb{P}\left[\sum_{i=1}^{n} Z_i \geq \overline{\gamma}\right] = 1 - \overline{\epsilon}_n \leq 1 - \epsilon_n, \qquad \text{(B.37)}$$

where $\underline{\gamma}$ and $\overline{\gamma}$ are in the range of $\sum_{i=1}^{n} Z_i$, $\overline{\gamma} - \underline{\gamma} = h$, and $\underline{\epsilon}_n \leq \epsilon_n \leq \overline{\epsilon}_n$. Let $\lambda \in [0, 1]$ satisfy

$$\mathbb{P}\left[\sum_{i=1}^{n} Z_i \geq \underline{\gamma}\right]\lambda + \mathbb{P}\left[\sum_{i=1}^{n} Z_i \geq \overline{\gamma}\right](1-\lambda) = 1 - \epsilon_n. \qquad \text{(B.38)}$$

By the Neyman-Pearson Lemma (see [5, eq. (101)]),

$$\begin{aligned}
&\beta_{1-\epsilon_n}(P^{(n)}, Q^{(n)}) \\
&= \mathbb{P}\left[\sum_{i=1}^{n} \overline{Z}_i \geq \underline{\gamma}\right]\lambda + \mathbb{P}\left[\sum_{i=1}^{n} \overline{Z}_i \geq \overline{\gamma}\right](1-\lambda). \qquad \text{(B.39)}
\end{aligned}$$

Define the asymptotic expansion

$$\begin{aligned}\chi(\epsilon) \triangleq D - \sqrt{\frac{V}{n}} Q^{-1}(\epsilon) + \frac{\mathrm{Sk}\sqrt{V}}{6n} Q^{-1}(\epsilon)^2 \\ - \frac{3(\mu_4 - 3V^2)V - 4\mu_3^2}{72V^{5/2}} \frac{Q^{-1}(\epsilon)^3}{n^{3/2}} \\ + O\left(\frac{Q^{-1}(\epsilon)^4}{n^2}\right) + O\left(\frac{1}{n}\right).\end{aligned} \tag{B.40}$$

By conditions (A) and (B) of Theorem 3.3.5, the conditions of Theorem 2.4.1 are satisfied for the sum $\sum_{i=1}^n Z_i$. We apply Lemma 2.4.1 to (B.36)–(B.37), and get the asymptotic expansions

$$\underline{\gamma} = n\chi(\underline{\epsilon}_n) \tag{B.41}$$

$$\overline{\gamma} = n\chi(\overline{\epsilon}_n). \tag{B.42}$$

From the Taylor series expansion of $\chi(\cdot)$ around $\epsilon_n$, (B.41)–(B.42), and $\overline{\gamma} - \underline{\gamma} = O(1)$, it holds that

$$\underline{\gamma} = n\chi(\epsilon_n) + O(1) \tag{B.43}$$

$$\overline{\gamma} = n\chi(\epsilon_n) + O(1). \tag{B.44}$$

The arguments above hold in the non-lattice case with $\underline{\gamma} = \overline{\gamma}$.

Next, we evaluate the probability $\mathbb{P}\left[\sum_{i=1}^n \overline{Z}_i \geq \underline{\gamma}\right]$ in (B.39) separately in the lattice and non-lattice cases.

### B.4.1 Lattice Case

We will apply Theorem 2.5.3 to evaluate the probability of interest. By [35, Appendix D],

$$\kappa(1) = 0 \tag{B.45}$$

$$\kappa'(1) = D \tag{B.46}$$

$$\kappa''(1) = V \tag{B.47}$$

$$\kappa'''(1) = \mu_3. \tag{B.48}$$

From (B.43), we have $\frac{1}{n}\underline{\gamma} = D + o(1)$. Therefore, by (B.46), condition (ND) of Theorem 2.5.2 is satisfied with $s = 1 + o(1)$. Condition (S) of Theorem 2.5.2 is satisfied by condition (C) of Theorem 3.3.5. Therefore, it only remains to verify condition (L) of Theorem 2.5.3 in the one-dimensional case. Since $\sum_{i=1}^n \overline{Z}_i$ is lattice with span $h$, each of $\overline{Z}_i$ is also lattice whose span is a multiple of $h$. By [30, p. 1687], we have

$$\sup_{\delta<|t|\leq\frac{\pi}{h}} \left|\frac{\phi_i(s+\mathrm{i}t)}{\phi_i(s)}\right| \leq c_1 < 1, \quad i \in [n] \tag{B.49}$$

for every $0 < \delta \leq \frac{\pi}{h}$, where $\phi_i(\cdot)$ is the mgf of $\overline{Z}_i$. Since $\overline{Z}_1, \dots, \overline{Z}_n$ are i.i.d., the mgf $\phi(\cdot)$ of $\sum_{i=1}^n \overline{Z}_i$ satisfies

$$\begin{aligned} \sup_{\delta<|t|\leq\frac{\pi}{h}} \left|\frac{\phi(s+\mathrm{i}t)}{\phi(s)}\right| &= \sup_{\delta<|t|\leq\frac{\pi}{h}} \left|\prod_{i=1}^n \frac{\phi_i(s+\mathrm{i}t)}{\phi_i(s)}\right| \qquad \text{(B.50)} \\ &\leq c_1^n = o(n^{-1/2}). \qquad \text{(B.51)} \end{aligned}$$

Therefore, condition (L) of Theorem 2.5.3 is satisfied. Applying Theorem 2.5.3 to $\mathbb{P}\left[\sum_{i=1}^n \overline{Z}_i \geq \underline{\gamma}\right]$, we have

$$\mathbb{P}\left[\sum_{i=1}^n \overline{Z}_i \geq \underline{\gamma}\right] = \exp\left\{-n\Lambda(a_n) - \frac{1}{2}\log n + O(1)\right\}, \tag{B.52}$$

where

$$\Lambda(a_n) = \sup_{t\in\mathbb{R}}\{ta_n - \kappa(t)\} \tag{B.53}$$

$$a_n = \chi(\epsilon_n) + O\left(\frac{1}{n}\right). \tag{B.54}$$

We expand the Taylor series of $\Lambda(\cdot)$ around $D$ as

$$\begin{aligned} \Lambda(a_n) = \Lambda(D) + (a_n - D)\Lambda'(D) + \frac{(a_n-D)^2}{2}\Lambda''(D) \\ + \frac{(a_n-D)^3}{6}\Lambda'''(D) + O(|a_n - D|^4). \qquad \text{(B.55)} \end{aligned}$$

By [35, Appendix D],

$$\Lambda(D) = D \tag{B.56}$$

$$\Lambda'(D) = 1 \tag{B.57}$$

$$\Lambda''(D) = \frac{1}{V} \tag{B.58}$$

$$\Lambda'''(D) = -\frac{\mu_3}{V^3}. \tag{B.59}$$

Combining (B.52) and (B.56)–(B.59), we get

$$\Lambda(a_n) = a_n + \frac{Q^{-1}(\epsilon_n)^2}{2n} + O\left(\frac{Q^{-1}(\epsilon_n)^4}{n^2}\right) + O\left(\frac{1}{n}\right). \tag{B.60}$$

By (B.43)–(B.44), the asymptotic expansion on the right-hand side of (B.52) holds for the probability $\mathbb{P}\left[\sum_{i=1}^n \overline{Z}_i \geq \overline{\gamma}\right]$ too. Combining (B.39), (B.52), and (B.60) completes the proof for the lattice case.

### B.4.2 Non-lattice Case

The proof for the non-lattice case is identical to the proof for the lattice case except the verification of condition (NL) in Theorem 2.5.2. Denote

$$\tilde{S}_j \triangleq \sum_{i \in \mathcal{I}_j} Z_i, \quad j \in [w_n], \tag{B.61}$$

which are non-lattice by condition (D) of Theorem 3.3.5. By [30, p. 1687],

$$\sup_{j \in [w_n]} \sup_{\delta < |t| \leq \lambda} \left| \frac{\tilde{\phi}_j(s + \mathrm{i}t)}{\tilde{\phi}_j(s)} \right| \leq c_2 < 1 \tag{B.62}$$

for every $0 < \delta < \lambda$, where $\tilde{\phi}_j$ denotes the mgf of $\tilde{S}_j$. Since $\overline{Z}_1, \dots, \overline{Z}_n$ are i.i.d., we have

$$\begin{aligned} \sup_{\delta < |t| \leq \lambda} \left| \frac{\phi(s + \mathrm{i}t)}{\phi(s)} \right| &= \sup_{\delta < |t| \leq \lambda} \left| \prod_{j=1}^{w_n} \frac{\tilde{\phi}_j(s + \mathrm{i}t)}{\tilde{\phi}_j(s)} \right| \cdot 1 \qquad &\text{(B.63)} \\ &\leq c_2^{w_n} &\text{(B.64)} \\ &= o(n^{-1/2}), &\text{(B.65)} \end{aligned}$$

where (B.63) follows since $\frac{\tilde{\phi}_j(s+\mathrm{i}t)}{\tilde{\phi}_j(s)}$ is a characteristic function of a non-lattice random variable [30], (B.64) follows from (B.62), and (B.65) follows from condition (D) and $c_2 < 1$. This verifies condition (NL) of Theorem 2.5.2. Applying Theorem 2.5.2 similarly to (B.52) completes the proof.

## B.5 Proof of Theorem 3.3.3

*Proof of the achievability:* To prove the achievability, we derive the coefficient of $O\left(\frac{Q^{-1}(\epsilon_n)^3}{\sqrt{n}}\right)$ in Lemma 3.4.1, and invoke the refined Lemma 3.4.1 with $P_X = P_X^*$. For this purpose, we need to modify the proof of Lemma 3.4.1 at two steps. First, using Lemma 2.4.1, the expansion for $t_n$ in (3.111) is refined as

$$\begin{aligned} t_n = Q^{-1}(\epsilon_n) &- \frac{\mathrm{Sk_u} Q^{-1}(\epsilon_n)^2}{6\sqrt{n}} \\ &+ \frac{3(\mu_4 - 3V^2)V - 4\mu_3^2}{72V^3} \frac{Q^{-1}(\epsilon_n)^3}{n} \\ &+ O\left(\frac{Q^{-1}(\epsilon_n)^4}{n^{3/2}}\right) + O\left(\frac{1}{\sqrt{n}}\right). \end{aligned} \tag{B.66}$$

Second, we refine the expansion in (3.119) by computing the third-order gradient $\nabla^3 \Lambda(\mathbf{a}_n)$. Taking the gradient of (B.10), we get

$$\nabla^3 \Lambda(\mathbf{a}_n)_{i,j,k} = - \sum_{(a,b,c) \in [2]^3} \nabla^3 \kappa(\mathbf{s}_n)_{a,b,c} (\nabla^2 \kappa)^{-1}(\mathbf{s}_n)_{a,i}$$

$$\cdot(\nabla^2\kappa)^{-1}(\mathbf{s}_n)_{b,j}(\nabla^2\kappa)^{-1}(\mathbf{s}_n)_{c,k}, \quad (i,j,k) \in [2]^3. \tag{B.67}$$

In the case $\eta(P_X^*) = 0$, the inverse of the Hessian $(\nabla^2\kappa)^{-1}(\mathbf{s})$ in (B.17) becomes

$$(\nabla^2\kappa)^{-1}(\mathbf{s}) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \frac{1}{V}, \tag{B.68}$$

and we compute

$$\nabla^3\kappa(\mathbf{s})_{1,1,1} = \mu_3 \tag{B.69}$$

$$\nabla^3\kappa(\mathbf{s})_{1,1,2} = -\mu_3 \tag{B.70}$$

$$\nabla^3\kappa(\mathbf{s})_{1,2,2} = \mu_3 \tag{B.71}$$

$$\nabla^3\kappa(\mathbf{s})_{2,2,2} = 0. \tag{B.72}$$

Note that (B.69)–(B.72) is sufficient to determine $\nabla^3\kappa(\mathbf{s})$ since it is a symmetric order-3 tensor. From (B.67)–(B.72), we compute

$$\nabla^3\Lambda(\mathbf{a})_{1,1,1} = -\frac{2\mu_3}{V^3}. \tag{B.73}$$

Using (B.68) and (B.73), we refine (3.119) as

$$\begin{aligned}\Lambda(\mathbf{a}_n) &= a_{n,1} + \frac{(a_{n,1} - I(P_X^*))^2}{V} - \frac{1}{6}(a_{n,1} - I(P_X^*))^3 \frac{2\mu_3}{V^3} \\ &\quad + O(|a_{n,1} - I(P_X^*)|^4) \qquad \text{(B.74)} \\ &= a_n + \frac{Q^{-1}(\epsilon_n)^2}{n} + O\left(\frac{Q^{-1}(\epsilon_n)^4}{n^2}\right) + O\left(\frac{1}{n}\right). \qquad \text{(B.75)}\end{aligned}$$

Following the steps in the proof Lemma 3.4.1 and using (B.66) and (B.75) completes the proof. ■

*Proof of the converse:* Set $Q_Y^{(n)} = (Q_Y^*)^n$, where $Q_Y^*$ is the equiprobable capacity-achieving output distribution. Since Cover-Thomas symmetric channels have rows that are permutation of each other, we have that $\beta_{1-\epsilon_n}(P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}}, Q_Y^{(n)})$ is independent of $\mathbf{x} \in \mathcal{X}^n$. By [5, Th. 28], we have

$$\log M^*(n, \epsilon_n) \leq -\log \beta_{1-\epsilon_n}(P_{\mathbf{Y}|\mathbf{X}=\mathbf{x}}, Q_Y^{(n)}), \tag{B.76}$$

where $\mathbf{x} = (x_0, \ldots, x_0)$ for some $x_0 \in \mathcal{X}$. Applying Theorem 3.3.5 to the right-hand side of (B.76) completes the proof. ■

## B.6 Proof of Theorem 3.3.4

We begin by presenting the preliminary definitions about the subsets of a $n$-dimensional sphere. A centered, unit sphere embedded on $\mathbb{R}^n$ (the manifold dimension is $n-1$) is defined as

$$\mathbb{S}^{n-1} \triangleq \{\mathbf{x} \in \mathbb{R}^n \colon \|\mathbf{x}\| = 1\}. \tag{B.77}$$

A centered, unit-radius spherical cap embedded in $\mathbb{R}^n$ is defined as

$$\mathrm{cap}(\mathbf{x}, a) \triangleq \{\mathbf{y} \in \mathbb{R}^n \colon \langle \mathbf{x}, \mathbf{y} \rangle \geq a, \|\mathbf{y}\|_2 = 1\}, \tag{B.78}$$

where $\mathbf{x} \in \mathbb{S}^{n-1}$ is the center point of the cap, and $a \in [-1, 1]$ defines the size of the cap, which is equal to the cosine of the half-angle of the cap. For example, $\mathrm{cap}(\mathbf{x}, -1) = \mathbb{S}^{n-1}$ and $\mathrm{cap}(\mathbf{x}, 0)$ is a half-sphere. We use $\mathrm{Area}(\cdot)$ to denote the surface area of an $(n-1)$-dimensional manifold embedded in $\mathbb{R}^n$. For example, the surface area of a unit sphere is

$$\mathrm{Area}(\mathbb{S}^{n-1}) = \frac{2\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}, \tag{B.79}$$

where $\Gamma(\cdot)$ denotes the Gamma function. Below, we use $\hat{\mathbf{X}} \triangleq \frac{\mathbf{X}}{\|\mathbf{X}\|_2}$ to denote the projection of $\mathbf{X}$ onto $\mathbb{S}^{n-1}$.

### B.6.1 Shannon's Random Coding Bound

Shannon's random coding bound from [6] is also a relaxation of the RCU bound (3.102), but differently than the one in (3.103). We generate $M$ independent codewords uniformly distributed on the power sphere $\sqrt{nP}\mathbb{S}^{n-1}$. Since all codewords lie on the power sphere and since the maximum likelihood decoding rule is equal to the minimum distance decoder for the Gaussian channel, (3.102) is equivalent to

$$\epsilon \leq \mathbb{P}\left[\cup_{m=2}^{M}\{\langle \hat{\mathbf{X}}(m), \hat{\mathbf{Y}} \rangle \geq \langle \hat{\mathbf{X}}(1), \hat{\mathbf{Y}} \rangle\} | W = 1\right]. \tag{B.80}$$

We bound the right-hand side of (B.80) by

$$\mathbb{P}\left[\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle < a\right] + M\mathbb{P}\left[\langle \hat{\overline{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle \geq \langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle \geq a\right] \tag{B.81}$$

for some $a \in [-1, 1]$ to be determined later. Here, $\mathbf{X}$ is uniformly distributed on $\sqrt{nP}\mathbb{S}^{n-1}$, $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$, where $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{I}_n)$, independent of $\mathbf{X}$, and $\overline{\mathbf{X}}$ is distributed identically to $\mathbf{X}$, and is independent of $\mathbf{X}$ and $\mathbf{Y}$. The bound in

(B.81) is exactly equal to [6, eq. (19)] and [41, eq. (61)]. Both of [6] and [41] set the threshold $a$ to satisfy

$$\mathbb{P}\left[\langle \hat{\bar{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle \geq a\right] = \frac{1}{M} \tag{B.82}$$

to analyze the bound in the LD regime. We here set $a$ slightly differently for the CLT regime, namely, as

$$\mathbb{P}\left[\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle < a\right] = \tilde{\epsilon} = \epsilon - \frac{1}{\sqrt{2\pi n V(P)}} \exp\left\{-\frac{Q^{-1}(\epsilon)^2}{2}\right\}, \tag{B.83}$$

which is the same choice that we make in (3.106).

Using the same steps as [6, eq. (16)-(17)] and [41, Appendix G], we express the probability (B.83) in terms of a cdf of a noncentral $t$-distribution with noncentrality parameter $\sqrt{nP}$ and $n-1$ degrees of freedom as[1]

$$\mathbb{P}\left[\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle < a\right] = \mathbb{P}\left[\rho < \sqrt{n-1}\frac{a}{\sqrt{1-a^2}}\right], \tag{B.84}$$

where $\rho \sim$ noncentral$-t(n-1, \sqrt{nP})$, which is defined as

$$\frac{A_1 + \sqrt{nP}}{\sqrt{\frac{1}{n-1}\sum_{i=2}^{n} A_i^2}}, \tag{B.85}$$

where $A_1, \ldots, A_n$ are i.i.d. $\mathcal{N}(0,1)$.

Due to spherical symmetry, $\langle \hat{\bar{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle$ is independent of $\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle$, and from [6, Sec. IV],

$$\mathbb{P}\left[\langle \hat{\bar{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle \geq b\right] = \frac{\text{Area}(\text{cap}(\mathbf{x}_0, b))}{\text{Area}(\mathbb{S}^{n-1})} \quad \text{for } b \in (-1, 1), \tag{B.86}$$

where $\mathbf{x}_0$ is any point on the unit-sphere. Shannon proves the following asymptotic expansion of (B.86)

$$\begin{aligned} v_n(b) &\triangleq \frac{1}{n} \log \frac{\text{Area}(\text{cap}(\mathbf{x}_0, b))}{\text{Area}(\mathbb{S}^{n-1})} && \text{(B.87)} \\ &= \frac{1}{2}\log(1-b^2) \\ &\quad - \frac{1}{2n}\log n - \frac{1}{2n}\log(2\pi b^2(1-b^2)) + O\left(\frac{1}{n^2}\right). && \text{(B.88)} \end{aligned}$$

[1] To see this, set $\mathbf{X}$ to $(\sqrt{nP}, 0, \ldots, 0)$ and use spherical symmetry.

To find the value of $a$ in (B.83) as a function of $\epsilon$, we first derive a Cornish-Fisher expansion of the random variable $\rho$. Fisher and Cornish [144] extend the Cornish-Fisher expansion of the random variables with known cumulants that do not need to be sum of independent random variables; they give the expansions for $t$ and chi-squared distributions as examples. Van Eeden [145] uses the same technique for the noncentral $t$-distribution, where the noncentrality parameter is fixed and the number of degrees of freedom approaches infinity. In our application, $\rho$ has a noncentrality parameter $\sqrt{nP}$ growing to infinity. Below, we will use [144] to extend [145] to the case where the noncentrality parameter also grows.

For the expansion in [144] that uses cumulants up to order $s$ to hold, the random variable needs to be continuous and its first $s+1$ cumulants need to satisfy $\kappa_j = O\left(\frac{1}{n^{\frac{j}{2}-1}}\right)$, $j \leq s+1$. From [29], [144], the quantile $t$ of $\rho$ at the value $\tilde{\epsilon}$ admits the expansion

$$\tilde{\epsilon} = \mathbb{P}\left[\rho < t\right] \tag{B.89}$$

$$t = \kappa_1 - \sqrt{\kappa_2}(Q^{-1}(\tilde{\epsilon}) - \frac{\mathrm{Sk}}{6}(Q^{-1}(\tilde{\epsilon})^2 - 1)) + O\left(\frac{1}{n}\right), \tag{B.90}$$

where $\kappa_1 = \mathbb{E}\left[\rho\right]$, $\kappa_2 = \mathrm{Var}\left[\rho\right]$, and $\mathrm{Sk} = \frac{\mathbb{E}\left[(\rho-\kappa_1)^3\right]}{\kappa_2^{3/2}}$ is the skewness.

From the moments of noncentral $t$-distribution [146] and Taylor series expansions, we calculate the asymptotic expansions for $\kappa_1, \kappa_2$, and Sk as

$$\kappa_1 = \sqrt{nP} + \frac{3}{4}\sqrt{\frac{P}{n}} + O\left(n^{-3/2}\right) \tag{B.91}$$

$$\kappa_2 = \left(1 + \frac{P}{2}\right) + \frac{2 + \frac{19P}{8}}{n} + O\left(n^{-3/2}\right) \tag{B.92}$$

$$\mathrm{Sk} = \frac{12\sqrt{P} + 5P^{3/2}}{\sqrt{2n}\,(2+P)^{3/2}} + O\left(n^{-3/2}\right), \tag{B.93}$$

and check that the fourth cumulant satisfies $\kappa_4 = O(n^{-1})$. Applying the Taylor series expansion to $Q^{-1}(\tilde{\epsilon})$, we get

$$Q^{-1}(\tilde{\epsilon}) = Q^{-1}(\epsilon) + \frac{1}{\sqrt{nV(P)}} + O\left(\frac{1}{n}\right). \tag{B.94}$$

Juxtaposing (B.84) and (B.89), we note

$$a = \frac{\frac{t}{\sqrt{n-1}}}{\sqrt{1 + \frac{t^2}{n-1}}}. \tag{B.95}$$

Substituting (B.91)–(B.94) into (B.90), and the latter into (B.95), we get

$$\begin{aligned} a =& \frac{\sqrt{P}}{\sqrt{1+P}} - \frac{1}{\sqrt{n}} \frac{\sqrt{2+P}Q^{-1}(\epsilon)}{\sqrt{2}(1+P)^{3/2}} \\ &+ \frac{1}{n} \frac{18\sqrt{P} + 28P^{3/2} + 10P^{5/2}}{12(1+P)^{5/2}(2+P)} \\ &- \frac{Q^{-1}(\epsilon)^2}{n} \frac{24\sqrt{P} + 19P^{3/2} + 4P^{5/2}}{12(1+P)^{5/2}(2+P)} \\ &- \frac{1}{n} \frac{\sqrt{2+P}}{\sqrt{2}(1+P)^{3/2}\sqrt{V(P)}}. \end{aligned} \tag{B.96}$$

It only remains to find the asymptotic expansion of the probability $\mathbb{P}\left[\langle \hat{\bar{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle \geq \langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle \geq a\right]$. Note that this probability is in the LD regime. Using the analysis in [41, Sec. V-B], we find the density of $\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle$ as

$$f_{\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle}(a) = \exp\{n u_n(a)\} \tag{B.97}$$

$$u_n(a) = u_0(a) + \frac{\log n}{2n} - \frac{u_1(a)}{2n} + O(n^{-2}) \tag{B.98}$$

$$\begin{aligned} u_0(a) =& \frac{1}{2}\log(1-a^2) - 2\alpha^2 + (\alpha a)^2 + \alpha a\sqrt{1+(\alpha a)^2} \\ &+ \log(\alpha a + \sqrt{1+(\alpha a)^2}) \end{aligned} \tag{B.99}$$

$$\begin{aligned} u_1(a) =& \log(1 + (\alpha a)^2 + \alpha a\sqrt{1+(\alpha a)^2}) \\ &+ 3\log(1-a^2) + \log(2\pi), \end{aligned} \tag{B.100}$$

where $\alpha \triangleq \sqrt{\frac{P}{4}}$.

In [41], the asymptotic expansion to the probability $\mathbb{P}\left[\langle \hat{\bar{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle \geq \langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle \geq a\right]$ is derived using the Laplace integration method as

$$\begin{aligned} &\mathbb{P}\left[\langle \hat{\bar{\mathbf{X}}}, \hat{\mathbf{Y}} \rangle \geq \langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle \geq a\right] \\ &= \int_a^1 f_{\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle}(b) \frac{\mathrm{Area}(\mathrm{cap}(\mathbf{x}_0, b))}{\mathrm{Area}(\mathbb{S}^{n-1})} db \qquad \text{(B.101)} \\ &= \int_a^1 \exp\{n g_n(b)\} db \qquad \text{(B.102)} \\ &= \exp\{n g_n(a)\} \left( \frac{1}{-n g_n'(a)} + O(n^{-2}) \right), \qquad \text{(B.103)} \end{aligned}$$

where $g_n(b) = u_n(b) + v_n(b)$ and $g_n'(a)$ is the derivative of $g_n(\cdot)$ evaluated at $a$.

Finally, equating the second term in (B.81) to $\frac{1}{\sqrt{2\pi n V(P)}} \exp\left\{-\frac{Q^{-1}(\epsilon)^2}{2}\right\}$, i.e.,

$$M \exp\{n g_n(a)\} \frac{1}{-n g_n'(a)} = \frac{1}{\sqrt{2\pi n V(P)}} \exp\left\{-\frac{Q^{-1}(\epsilon)^2}{2}\right\}, \tag{B.104}$$

and using (B.96)–(B.100) along with necessary Taylor series expansions, we complete the proof for the lower bound (3.73).

### B.6.2 Shannon's Sphere-Packing Converse

In [6, eq. (15)], Shannon derives a converse bound for the Gaussian channel with an equal power constraint using a sphere-packing idea. Being equal to Polyanskiy's minimax bound in [5, Th. 28], Shannon's converse bound is still the tightest for any error probability to this date. We here analyze [6, eq. (15)] in the CLT regime.

Shannon's sphere-packing converse for the equal-power case is given by

$$\epsilon \geq \mathbb{P}\left[\langle \hat{\mathbf{X}}, \hat{\mathbf{Y}} \rangle < a^*\right], \tag{B.105}$$

where $a^*$ satisfies

$$\frac{1}{M} = \frac{\text{Area}(\text{cap}(\mathbf{x}_0, a^*))}{\text{Area}(\mathbb{S}^{n-1})}. \tag{B.106}$$

To evaluate (B.105), we express $a^*$ in terms of $\epsilon$ using the Cornish-Fisher expansion in (B.90). Then, we plug the value of $a^*$ in (B.106). Using the asymptotic expansion in (B.88), necessary Taylor series expansions, and the bound on the right-hand side of (3.79), we obtain the upper bound in (3.74).

*Appendix C*

# APPENDIX FOR CHAPTER 4

## C.1 A General SHT-based Achievability Bound

In this section, we derive an achievability bound based on a general SHT, which we use to prove Theorems 4.3.1–4.3.2.

### C.1.1 SHT: Definitions

We begin by formally defining a SHT. Let $\{Z_i\}_{i=1}^{\infty}$ be the observed sequence. Consider two hypotheses for the distribution of $Z^{\infty}$

$$H_0\colon Z^{\infty} \sim P_0^{(\infty)} \tag{C.1}$$

$$H_1\colon Z^{\infty} \sim P_1^{(\infty)}, \tag{C.2}$$

where $P_0^{(\infty)}$ and $P_1^{(\infty)}$ are distributions on a common alphabet $\mathcal{Z}^{\infty}$. Let $\mathcal{N} \subseteq \{0, 1, 2, \dots\}$ be a set of non-negative integers. Let $\mathcal{F}(X)$ denote the $\sigma$-algebra generated by the random variable $X$, and let $\tau$ be a stopping time adapted to the filtration $\{\mathcal{F}(X^n)\}_{n\in\mathcal{N}}$. Let $\delta$ be a $\{0, 1\}$-valued, $\mathcal{F}(\tau)$-measurable function. An SHT is a triple $(\delta, \tau, \mathcal{N})$, where $\delta$ is called the decision rule, $\tau$ is called the stopping time, and $\mathcal{N}$ is the set of available decision times. Type-I and type-II error probabilities are defined as

$$\alpha \triangleq \mathbb{P}\left[\delta = 1 | H_0\right] \tag{C.3}$$

$$\beta \triangleq \mathbb{P}\left[\delta = 0 | H_1\right]. \tag{C.4}$$

Below, we derive an achievability using a general SHT.

### C.1.2 Achievability Bound

Given some input distribution $P_{X^{n_L}}$, define the common randomness random variable $U$ on $\mathbb{R}^{Mn_L}$ with the distribution

$$P_U = \underbrace{P_{X^{n_L}} \times P_{X^{n_L}} \times \cdots \times P_{X^{n_L}}}_{M \text{times}}. \tag{C.5}$$

The realization of $U$ defines $M$ length-$n_L$ codewords $X^{n_L}(1), X^{n_L}(2), \dots, X^{n_L}(M)$. Denote the set of available decodeing times by

$$\mathcal{N} \triangleq \{n_1, \dots, n_L\}. \tag{C.6}$$

Let $\{(\delta_m, \tilde{\tau}_m, \mathcal{N})\}_{m=1}^M$ be $M$ copies of an SHT that distinguishes between the hypotheses

$$H_0\colon (X^{n_L}, Y^{n_L}) \sim P_{X^{n_L}} \times P_{Y|X}^{n_L} \tag{C.7}$$

$$H_1\colon (X^{n_L}, Y^{n_L}) \sim P_{X^{n_L}} \times P_{Y^{n_L}} \tag{C.8}$$

for each message $m \in [M]$, where the type-I and type-II error probabilities are $\alpha$ and $\beta$, respectively. Define for $m \in [M]$ and $j \in \{0, 1\}$,

$$\tau_m^j \triangleq \begin{cases} \tilde{\tau}_m & \text{if } \delta_m = j \\ \infty & \text{otherwise.} \end{cases} \tag{C.9}$$

To simplify the notation later in the analysis, we denote

$$\tau_m \triangleq \tau_m^0, \tag{C.10}$$

i.e., $\tau_m = \infty$ if and only if $H_1$ is decided for $m$, or, equivalently, $\delta_m = 1$.

**Theorem C.1.1.** *Fix $L \leq \infty$, integers $M > 0$ and $0 \leq n_1 < n_2 < \cdots < n_L \leq \infty$, a distribution $P_{X^{n_L}}$ as in (C.5), and $M$ copies of an SHT $\{(\delta_m, \tilde{\tau}_m, \{n_1, \ldots n_L\})\}_{m=1}^M$ as in (C.7)–(C.9). There exists an $(N, L, M, \epsilon)$ VLSF code for the DM-PPC $(\mathcal{X}, P_{Y|X}, \mathcal{Y})$ with*

$$\epsilon \leq \alpha + (M-1)\beta \tag{C.11}$$

$$N \leq \mathbb{E}\left[\min\left\{\min_{m\in[M]}\left\{\tau_m^0\right\}, \max_{m\in[M]}\left\{\tau_m^1\right\}\right\}\right]. \tag{C.12}$$

*Proof:* We generate $M$ i.i.d. codewords according to (C.5). For each of $M$ messages, we run the hypothesis test given in (C.7)–(C.8). We decode at the earliest time that one of the following events happens

- $H_0$ is declared for some message $m \in [M]$,
- $H_1$ is declared for all $m \in [M]$.

The decoding output is $m$ if $H_0$ is declared for $m$; if there exist more than one such $m$ or if there exists no such $m$, the decoder declares an error.

Mathematically, the average decoding time of this code is expressed as

$$\tau^* = \min\left\{\min_{m\in[M]}\left\{\tau_m^0\right\}, \max_{m\in[M]}\left\{\tau_m^1\right\}\right\}. \tag{C.13}$$

The average decoding time bound in (C.12) immediately follows from (C.13). The decoder output is

$$\hat{W} \triangleq \begin{cases} m & \text{if } \exists!\ m \in [M] \text{ s. t. } \tau^* = \tau_m^0 \\ \text{error} & \text{otherwise.} \end{cases} \tag{C.14}$$

Since the messages are equiprobable, without loss of generality, assume that message $m = 1$ is transmitted. An error occurs if and only if $H_1$ is decided for $m = 1$ or if $H_0$ is decided for some $m \neq 1$, giving

$$\epsilon = \mathbb{P}\left[\{\delta_1 = 1\} \cup \left\{\bigcup_{m=2}^{M} \{\delta_m = 0\}\right\}\right]. \tag{C.15}$$

Applying the union bound to (C.15) shows (C.11). ■

## C.2 Proof of Theorem 4.3.2

Theorem 4.3.2 particularizes the SHTs in Theorem C.1.1 as an information density threshold rule, which constitutes the decision rule used at times $\{n_2, \dots, n_L\}$ in the proof sketch of Theorem 4.3.1.

In addition to the random code design in (C.5), let $P_{X^{n_L}}$ satisfy (4.19). We here specify the stopping rule $\tau_m$ and the decision rule $\delta_m$ for the SHT in (C.7)–(C.8).

Define the information density for message $m$ and decoding time $n_\ell$ as

$$S_{m,n_\ell} \triangleq \imath(X^{n_\ell}(m); Y^{n_\ell}) \text{ for } m \in [M], \ell \in [L]. \tag{C.16}$$

Note that $S_{m,n_\ell}$ is the log-likelihood ratio between the distributions in hypotheses $H_0$ and $H_1$. We fix a threshold $\gamma \in \mathbb{R}$ and construct the SHTs

$$\tau_m = \inf\{n_\ell \in \mathcal{N} \colon S_{m,n_\ell} \geq \gamma\} \tag{C.17}$$

$$\tilde{\tau}_m = \min\{\tau_m, n_L\} \tag{C.18}$$

$$\delta_m = \begin{cases} 0 & \text{if } S_{m,\tilde{\tau}_m} \geq \gamma \\ 1 & \text{if } S_{m,\tilde{\tau}_m} < \gamma \end{cases} \tag{C.19}$$

for all $m \in [M]$, that is, we decide $H_0$ for message $m$ at the first time $n_\ell$ that $S_{m,n_\ell}$ passes $\gamma$; if this never happens for $n_\ell \in \{n_1, \dots, n_L\}$, then we decide $H_1$ for $m$.

The optimal SHT for the problem in (C.7)–(C.8) with $L$ decision times is a two-sided information density threshold rule with some finite lower and upper thresholds $-a_1(n_\ell)$ and $a_0(n_\ell)$, $\ell \in [L]$, that are determined according to the constraints on the test [83]. The SHT given in (C.18)–(C.19) sets the upper threshold as $a_0(n_\ell) = \gamma$ for all $\ell \in [L]$ and the lower threshold as $-a_1(n_\ell) = -\infty$ for $\ell \in [L-1]$, and $-a_1(n_L) = \gamma$.

Bounding (C.12) from above, we get

$$\begin{aligned} N &\leq \mathbb{E}\left[\min\{\tau_1, n_L\}\right] && \text{(C.20)} \\ &= \sum_{n=0}^{\infty} \mathbb{P}\left[\min\{\tau_1, n_L\} > n\right] && \text{(C.21)} \\ &= n_1 + \sum_{\ell=1}^{L-1} (n_{\ell+1} - n_\ell) \mathbb{P}\left[\tau_1 > n_\ell\right]. && \text{(C.22)} \end{aligned}$$

The probability $\mathbb{P}\left[\tau_1 > n_\ell\right]$ is further bounded as

$$\begin{aligned} \mathbb{P}\left[\tau_1 > n_\ell\right] &= \mathbb{P}\left[\bigcap_{j=1}^{\ell} \{\imath(X^{n_j}(1); Y^{n_j}) < \gamma\}\right] && \text{(C.23)} \\ &\leq \mathbb{P}\left[\imath(X^{n_\ell}(1); Y^{n_\ell}) < \gamma\right]. && \text{(C.24)} \end{aligned}$$

Combining (C.22) and (C.24) proves (4.18).

We bound the type-I error probability of the given SHT as

$$\begin{aligned} \alpha &\triangleq \mathbb{P}\left[\delta_1 = 1\right] && \text{(C.25)} \\ &= \mathbb{P}\left[\tau_1 = \infty\right] && \text{(C.26)} \\ &= \mathbb{P}\left[\bigcap_{j=1}^{L} \{\imath(X^{n_j}(1); Y^{n_j}) < \gamma\}\right] && \text{(C.27)} \\ &\leq \mathbb{P}\left[\imath(X^{n_L}(1); Y^{n_L}) < \gamma\right], && \text{(C.28)} \end{aligned}$$

where (C.27) uses the definition of the decision rule (C.19). The type-II error probability is bounded as

$$\begin{aligned} \beta &\triangleq \mathbb{P}\left[\delta_2 = 0\right] && \text{(C.29)} \\ &\leq \mathbb{P}\left[\tau_2 < \infty\right] && \text{(C.30)} \\ &= \mathbb{E}\left[\exp\{-\imath(X^{n_L}(1); Y^{n_L})\} 1\{\tau_1 < \infty\}\right] && \text{(C.31)} \\ &= \mathbb{E}\left[\exp\{-\imath(X^{\tau}(1); Y^{\tau})\} 1\{\tau_1 < \infty\}\right] && \text{(C.32)} \\ &\leq \exp\{-\gamma\}, && \text{(C.33)} \end{aligned}$$

where (C.31) follows from changing measure from $P_{X^{n_L}(2) Y^{n_L}} = P_{X^{n_L}} P_{Y^{n_L}}$ to $P_{X^{n_L}(1), Y^{n_L}} = P_{X^{n_L}} P_{Y|X}^{n_L}$. Equality (C.32) uses the same arguments as in

[18, eq. (111)-(118)] and the fact that $\{\exp\{-\imath(X^{n_\ell}(1);Y^{n_\ell})\}\colon n_\ell \in \mathcal{N}\}$ is a martingale due to the product distribution in (4.19). Inequality (C.33) follows from the definition of $\tau_1$ in (C.17). Applying (C.11) together with (C.28) and (C.33) proves (4.17). ■

In his analysis of the error exponent regime, Forney [17] uses a slightly different threshold rule than the one in (C.17). Specifically, he uses a maximum a posteriori threshold rule, which can also be written as

$$\log \frac{P_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell}(m))}{\frac{1}{M}\sum_{j=1}^{M} P_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell}(j))} \geq \gamma, \tag{C.34}$$

whose denominator is the output distribution induced by the code rather than by the random codeword distribution $P_X^{n_\ell}$.

### C.3 Proof of Theorem 4.3.1

We here particularize Theorem C.1.1 to the sub-optimal SHTs that are described in the proof sketch of Theorem 4.3.1.

For message $m \in [M]$, let $\delta'_m$ and $\tau'_m$ denote $\delta_m$ and $\tau_m$ in (C.10) conditioned on the event $\{\tau^* \neq 0\}$, i.e., transmission has not stopped at time 0. Following the proof sketch, with this notation, (C.12) is rewritten as

$$N \leq p \cdot 0 + (1-p)\mathbb{E}\left[\min\left\{\min_{m\in[M]}\{\tau'_m\}, n_L\right\}\right], \tag{C.35}$$

where we use the fact that $\tau^* = 0$ occurs with probability $p$. The error probability (C.15) is rewritten as

$$\epsilon \leq p \cdot 1 + (1-p)\left(\mathbb{P}\left[\{\delta'_1 = 1\} \cup \bigcup_{m=2}^{M}\{\delta'_m = 0\}\right]\right). \tag{C.36}$$

By (C.12) and (C.15),

$$N' \triangleq \mathbb{E}\left[\min\left\{\min_{m\in[M]}\{\tau'_m\}, n_L\right\}\right] \tag{C.37}$$

$$\epsilon'_N \triangleq \mathbb{P}\left[\{\delta'_1 = 1\} \cup \bigcup_{m=2}^{M}\{\delta'_m = 0\}\right] \tag{C.38}$$

are the average decoding time and average error probability of an SHT-based VLSF code that is restricted to decoding times $\{n_2, \ldots, n_L\}$.

Recall the choice of parameters $\epsilon'_N$ and $p$ from (4.14)–(4.15) and the resulting average decoding time in (4.16). This choice achieves the best second-order term within our code construction (see Appendix C.7, below), Inverting (4.16), we get

$$N' = \frac{N}{1-\epsilon}\left(1 + O\left(\frac{1}{\sqrt{N\log N}}\right)\right). \tag{C.39}$$

We particularize the decision rules in the SHT at times $n_2, \ldots, n_L$ to the information density threshold rule. Lemma C.3.1, below, is an achievability bound for an $\left(N, L, M, \frac{1}{\sqrt{N\log N}}\right)$ VLSF code that employs this decoder with the optimized decoding times.

**Lemma C.3.1.** *Fix an integer $L = O(1) \geq 1$. For the DM-PPC with $V > 0$, the maximum message set size (4.7) achievable by $\left(N, L, M, \frac{1}{\sqrt{N\log N}}\right)$ VLSF codes satisfies*

$$\begin{aligned}\log M^*\left(N, L, \frac{1}{\sqrt{N\log N}}\right) \geq NC - \sqrt{N\log_{(L)}(N)\, V} \\ + O\left(\sqrt{\frac{N}{\log_{(L)}(N)}}\right).\end{aligned} \tag{C.40}$$

*The decoding times $n_1, \ldots, n_L$ that achieve (C.40) satisfy the equations*

$$\log M = n_\ell C - \sqrt{n_\ell \log_{(L-\ell+1)}(n_\ell) V} - \log n_\ell + O(1) \tag{C.41}$$

*for $\ell \in [L]$.*

*Proof:* Lemma C.3.1 analyzes Theorem 4.3.2. See Appendix C.5, below. ■

We use the average decoding time $N$ and average error probability $\epsilon$ of a VLSF code in Lemma C.3.1 in the places of $N'$ and $\epsilon'_N$ in (C.37)–(C.38). By Lemma C.3.1, there exists an $(N', L-1, M, \epsilon'_N)$ VLSF code with

$$\log M = N'C - \sqrt{N'\log_{(L-1)}(N')\, V} + O\left(\sqrt{\frac{N'}{\log_{(L-1)}(N')}}\right). \tag{C.42}$$

Plugging (C.39) into (C.42) and applying the necessary Taylor series expansions complete the proof. ■

Lemma C.3.1 is an achievability bound in the moderate deviations regime since the error probability $\frac{1}{\sqrt{N\log N}}$ decays sub-exponentially to zero. The fixed-length scenario in Lemma C.3.1, i.e., $L = 1$, is recovered by [45], which investigates the moderate deviations regime in channel coding. A comparison between the right-hand side of (C.40) and [45, Th. 2] highlights the benefit of using VLSF codes in the moderate deviations regime. The second-order rate achieved by a VLSF code with $L \geq 2$ decoding times, average decoding time $N$, and error probability $\frac{1}{\sqrt{N \log N}}$ is achieved by a fixed-length code with blocklength $N$ and error probability $\frac{1}{\sqrt{\log_{(L-1)}(N) \log_{(L)}(N)}}$.

## C.4 Proof of Theorem 4.3.3

Let $P_0$ and $P_1$ be two distributions. Let $Z \triangleq \log \frac{dP_0}{dP_1}$ be the log-likelihood ratio, and let

$$S_n = \sum_{i=1}^{n} Z_i, \tag{C.43}$$

where $Z_i$'s are i.i.d. and have the same distribution as $Z$. For $i \in \{0, 1\}$, we denote the probability measures and expectations under distribution $P_i$ by $\mathbb{P}_i$ and $\mathbb{E}_i$, respectively. Given a threshold $a_0 \in \mathbb{R}$, define the stopping time

$$T \triangleq \inf\{n \geq 1 \colon S_n \geq a_0\} \tag{C.44}$$

and the overshoot

$$\xi_0 = S_T - a_0. \tag{C.45}$$

The following lemma from [83], which gives the refined asymptotics for the stopping time $T$, is the main tool to prove our bounds.

**Lemma C.4.1** ([83, Cor. 2.3.1, Th. 2.3.3, Th. 2.5.3, Lemma 3.1.1])**.** *Suppose that $\mathbb{E}_0[(Z_1^+)^2] < \infty$, and $Z_1$ is non-arithmetic. Then, it holds that*

$$\begin{aligned}\mathbb{E}_0[T] &= \frac{1}{D(P_0\|P_1)}(a_0 + \mathbb{E}_0[\xi]) && \text{(C.46)}\\ &= \frac{1}{D(P_0\|P_1)}\Bigg(a_0 + \frac{\mathbb{E}_0[Z_1^2]}{2D(P_0\|P_1)} \\ &\qquad - \sum_{n=1}^{\infty} \frac{1}{n}\mathbb{E}_0[S_n^-] + o(1)\Bigg), && \text{(C.47)}\end{aligned}$$

*and*

$$\mathbb{P}_0[T < \infty] = 1 \tag{C.48}$$

$$\mathbb{P}_1[T < \infty] = e^{-a_0}\mathbb{E}_0[e^{-\xi_0}] \tag{C.49}$$

$$\mathbb{E}_0[e^{-\lambda\xi_0}] = \frac{1}{\lambda D(P_0\|P_1)} \exp\left\{-\sum_{n=1}^{\infty}\frac{1}{n}\mathbb{E}_0[e^{-\lambda S_n^+}]\right\}. \tag{C.50}$$

### C.4.1 Achievability Proof

Let $P_X$ be a capacity-achieving distribution of the DM-PPC. Define the hypotheses

$$H_0\colon (X^{d_N}, Y^{d_N})^\infty \sim P_0^\infty = ((P_X \times P_{Y|X})^{d_N})^\infty \tag{C.51}$$
$$H_1\colon (X^{d_N}, Y^{d_N})^\infty \sim P_1^\infty = ((P_X \times P_Y)^{d_N})^\infty, \tag{C.52}$$

and the random variables

$$W_i \triangleq \frac{1}{d_N} \log \frac{dP_0}{dP_1} \left(X^{(i-1)d_N+1:id_N}, Y^{(i-1)d_N+1:id_N}\right) \tag{C.53}$$

for $i = 1, 2, \ldots$. Note that under $P_0$,

$$W_i = \frac{1}{d_N} \imath(X^{(i-1)d_N+1:id_N}; Y^{(i-1)d_N+1:id_N}), \tag{C.54}$$

and $\mathbb{E}\left[W_i\right] = C$. Define

$$S_n \triangleq \sum_{i=1}^{n} W_i, \tag{C.55}$$

and

$$\tau \triangleq \inf\{k \geq 1\colon S_k \geq a_0/d_N\} \tag{C.56}$$
$$T \triangleq d_N\, \tau. \tag{C.57}$$

We employ the sub-optimal SHT strategy described in the proof sketch of Theorem 4.3.1 with $\epsilon'_N = \frac{1}{\mathbb{E}_0[T]}$ and the information density threshold rule (C.16)–(C.19) from the proof of Theorem 4.3.2, where the threshold $\gamma$ is set to $a_0$. Here, $T$ is as in (C.44). We set $M$ and $a_0$ so that

$$M\mathbb{P}_1[T < \infty] \leq Me^{-a_0} = \epsilon'_N = \frac{1}{\mathbb{E}_0[T]}, \tag{C.58}$$

where the inequality follows from (C.49). Following steps identical to (C.35)–(C.36) and (C.39), and noting that $\mathbb{P}_0[T = \infty] = 0$, we get

$$N = (1 - \epsilon)\mathbb{E}_0[T] + O(1), \tag{C.59}$$

and the average error probability of the code is bounded by $\epsilon$.

To evaluate $\mathbb{E}_0[T]$, we use Lemma C.4.1 with $W_i$ in place of $Z_i$. A straightforward calculation yields

$$\mathbb{E}_0[W_1^2] = C^2 + O\left(\frac{1}{d_N}\right). \tag{C.60}$$

Next, we have that

$$\mathbb{E}_0[S_n^-] = -nd_N \mathbb{E}\left[\frac{1}{nd_N} S_n 1\left\{\frac{1}{nd_N} S_n \leq 0\right\}\right], \tag{C.61}$$

where $S_n = \sum_{j=1}^{nd_N} \imath(X_j; Y_j)$. Applying the saddlepoint approximation (e.g., [34, eq. (1.2)]) to $\frac{1}{nd_N} S_n$, we get

$$\mathbb{E}_0[S_n^-] = -nd_N \int_{-\infty}^{0} c(x)\sqrt{nd_N} e^{-nd_N g(x) + \log x} dx, \tag{C.62}$$

where $c(x)$ and $g(x)$ are bounded below a positive constant for all $x \in (-\infty, 0]$. Applying the Laplace's integral [34, eq. (2.5)] to (C.62), we get

$$\mathbb{E}_0[S_n^-] = -e^{-nd_N c_n + o(nd_N)} \tag{C.63}$$

for all $n \in \mathbb{Z}_+$, where each $c_n$ is a positive constant depending on $n$. Putting (C.60) and (C.63) into (C.47) and (C.57), we get

$$\mathbb{E}_0[T] = \frac{a_0}{C} + \frac{d_N}{2} + o(d_N). \tag{C.64}$$

From (C.58)–(C.59), we get

$$\mathbb{E}_0[T] = \frac{N}{1-\epsilon} + O(1) \tag{C.65}$$

$$\log M = a_0 - \log N. \tag{C.66}$$

Putting (C.64)–(C.66) together completes the proof of (4.20).

### C.4.2 Converse Proof

Recall the definition of an SHT $(\delta, \tau, \mathcal{N})$ from Appendix C.1.1 that tests the hypotheses

$$H_0 \colon Z^\infty \sim P_0^{(\infty)} \tag{C.67}$$

$$H_1 \colon Z^\infty \sim P_1^{(\infty)}, \tag{C.68}$$

where $P_0^{(\infty)}$ and $P_1^{(\infty)}$ are distributions on a common alphabet $\mathcal{Z}^\infty$. We define the minimum achievable type-II error probability, subject to a type-I error probability bound and a maximal expected decoding time constraint, with decision times restricted to the set $\mathcal{N}$ as

$$\beta_{(\epsilon,N,\mathcal{N})}(P_0^{(\infty)}, P_1^{(\infty)}) \triangleq \min_{\substack{(\delta,\tau,\mathcal{N}) : \mathbb{P}_0[\delta=1]\leq\epsilon, \\ \max\{\mathbb{E}_0[\tau], \mathbb{E}_1[\tau]\}\leq N}} \mathbb{P}_1[\delta = 0], \tag{C.69}$$

which is the SHT version of the $\beta_\alpha$-function defined for the fixed-length binary hypothesis test [5].

The following theorem extends the meta-converse bound [5, Th. 27], which is a fundamental theorem used to show converse results in fixed-length channel coding without feedback and many other applications (e.g., [50], [52], [53]).

**Theorem C.4.1.** *Fix any set $\mathcal{N} \subseteq \mathbb{Z}_+$, a real number $N > 0$, and a DM-PPC $P_{Y|X}$. Then, it holds that*

$$\begin{aligned} &\log M^*(N, |\mathcal{N}|, \epsilon, \mathcal{N}) \\ &\quad \leq \sup_{P_{X^\infty}} \inf_{Q_{Y^\infty}} -\log \beta_{(\epsilon, N, \mathcal{N})}(P_{X^\infty} \times P_{Y|X}^\infty, P_{X^\infty} \times Q_{Y^\infty}). \end{aligned} \tag{C.70}$$

*Proof:* The proof is similar to that in [5]. Let $W$ denote a message equiprobably distributed on $[M]$, and let $\hat{W}$ be its reconstruction. Given any VLSF code with the set of available decoding times $\mathcal{N}$, average decoding time $N$, error probability $\epsilon$, and codebook size $M$, let $\hat{P}_{X^\infty}$ denote the input distribution induced by the code's codebook. The code operation creates a Markov chain $W \to X^\infty \to Y^\infty \to \hat{W}$. As full-feedback breaks this Markov chain, stop-feedback does not since the channel inputs are conditionally independent of the channel outputs given the message $W$. Fix an arbitrary output distribution $Q_{Y^\infty}$, and consider the SHT

$$H_0\colon (X^\infty, Y^\infty) \sim \hat{P}_{X^\infty} \times P_{Y|X}^\infty \tag{C.71}$$

$$H_1\colon (X^\infty, Y^\infty) \sim \hat{P}_{X^\infty} \times Q_{Y^\infty} \tag{C.72}$$

with a test $\delta = 1\{\hat{W} \neq W\}$, where $(W, \hat{W})$ are generated by the (potentially random) encoder-decoder pair of the VLSF code. The type-I and type-II error probabilities of this code-induced SHT are

$$\alpha = \mathbb{P}_0[\delta = 1] = \mathbb{P}\left[\hat{W} \neq W\right] \leq \epsilon \tag{C.73}$$

$$\beta = \mathbb{P}_1[\delta = 0] = \frac{1}{M}, \tag{C.74}$$

where (C.74) follows since the sequence $Y^\infty$ is independent of $X^\infty$ under $H_1$. The stopping time of this SHT under $H_0$ or $H_1$ is bounded by $N$ by the definition of a VLSF code. Since the error probabilities in (C.73)–(C.74) cannot be better than that of the optimal SHT, it holds that

$$\log M$$

$$\leq -\log \beta_{(\epsilon, N, \mathcal{N})}(\hat{P}_{X^\infty} \times P_{Y|X}^\infty, \hat{P}_{X^\infty} \times Q_{Y^\infty}) \tag{C.75}$$

$$\leq \inf_{Q_{Y^\infty}} -\log \beta_{(\epsilon, N, \mathcal{N})}(\hat{P}_{X^\infty} \times P_{Y|X}^\infty, \hat{P}_{X^\infty} \times Q_{Y^\infty}) \tag{C.76}$$

$$\leq \sup_{P_{X^\infty}} \inf_{Q_{Y^\infty}} -\log \beta_{(\epsilon, N, \mathcal{N})}(P_{X^\infty} \times P_{Y|X}^\infty, P_{X^\infty} \times Q_{Y^\infty}), \tag{C.77}$$

where (C.76) follows since the choice $Q_{Y^\infty}$ is arbitrary. ■

To prove (4.21), we apply Theorem C.4.1 and get

$$\log M \leq -\log \beta_{(\epsilon, N, \mathcal{N})}(P_{Y|X}^\infty, P_Y^\infty), \tag{C.78}$$

where $P_Y$ is the capacity-achieving output distribution, and $\mathcal{N} = \{0, d_N, 2d_N, \dots\}$. The reduction from Theorem C.4.1 to (C.78) follows since $\log \frac{P_{Y|X}(Y|x)}{P_Y(Y)}$ has the same distribution for all $x \in \mathcal{X}$ for Cover-Thomas symmetric channels [48, p. 190]. In the remainder of the proof, we derive an upper bound for the right-hand side of (C.78).

Consider any SHT $(\delta, \tau, \mathcal{N})$ with $\mathbb{E}_0[\tau] \leq N$ and $\mathbb{E}_1[\tau] \leq N$. Our definition in (C.69) is slightly different than the classical SHT definition from [147] since our definition allows one to make a decision at time 0. Notice that at time 0, any test has three choices: decide $H_0$, decide $H_1$, or decide to start taking samples. When the test decides to start taking samples, the remainder of the procedure becomes a classical SHT. From this observation, any test satisfies

$$\epsilon \geq \alpha = \epsilon_0 + (1 - \epsilon_0 - \epsilon_1)\alpha' \geq \epsilon_0 \tag{C.79}$$

$$\beta = \epsilon_1 + (1 - \epsilon_0 - \epsilon_1)\beta' \geq (1 - \epsilon_0)\beta', \tag{C.80}$$

where at time 0, the test decides $H_i$ with probability $\epsilon_{1-i}$, and $\alpha'$ and $\beta'$ are the type-I and type-II error probabilities conditioned on the event that the test decides to take samples at time 0, which occurs with probability $1 - \epsilon_0 - \epsilon_1$.

Let $\tau'$ denote the average stopping time of the test with error probabilities $(\alpha', \beta')$. We have

$$\mathbb{E}_0[\tau] = (1 - \epsilon_0 - \epsilon_1)\mathbb{E}_0[\tau'] \tag{C.81}$$

$$= (1 - \epsilon_0)(\mathbb{E}_0[\tau'] + e^{-O(N)}) \leq N \tag{C.82}$$

$$\mathbb{E}_1[\tau] = (1 - \epsilon_0 - \epsilon_1)\mathbb{E}_1[\tau'] \tag{C.83}$$

$$= (1 - \epsilon_0)(\mathbb{E}_1[\tau'] + e^{-O(N)}) \leq N \tag{C.84}$$

since $\beta$ decays exponentially with $\mathbb{E}_0[\tau]$.

The following argument is similar to that in [68, Sec. V-C]. Set an arbitrary $\nu > 0$ and the thresholds

$$\tilde{a}_0 = C\left(\frac{N}{1-\epsilon_0} - \frac{d_N}{2} - o(d_N) + \nu\right) \tag{C.85}$$

$$\tilde{a}_1 = D(P_Y \| P_{Y|X=x})\left(\frac{N}{1-\epsilon_0} - \frac{d_N}{2} - o(d_N) + \nu\right), \tag{C.86}$$

where $x \in \mathcal{X}$ is arbitrary, and let $(\tilde{\delta}, \tilde{\tau}, \mathcal{N})$ be the SPRT associated with the thresholds $(-\tilde{a}_1, \tilde{a}_0)$, and type-I and type-II error probabilities $\tilde{\alpha}$ and $\tilde{\beta}$.

Applying [83, eq. (3.56)] to (C.64), we get

$$\mathbb{E}_0[\tilde{\tau}] = \frac{\tilde{a}_0}{C} + \frac{d_N}{2} + o(d_N) \tag{C.87}$$

$$\mathbb{E}_1[\tilde{\tau}] = \frac{\tilde{a}_1}{D(P_Y \| P_{Y|X=x})} + \frac{d_N}{2} + o(d_N). \tag{C.88}$$

Combining (C.85)–(C.88) gives

$$\mathbb{E}_0[\tilde{\tau}] \geq \frac{N}{1-\epsilon_0} + \nu \tag{C.89}$$

$$\mathbb{E}_1[\tilde{\tau}] \geq \frac{N}{1-\epsilon_0} + \nu. \tag{C.90}$$

Letting $\nu = O\left(\frac{1}{N}\right)$, it follows from (C.81)–(C.84) and (C.89)–(C.90) that

$$\mathbb{E}_0[\tilde{\tau}] \geq \mathbb{E}_0[\tau'] \tag{C.91}$$

$$\mathbb{E}_1[\tilde{\tau}] \geq \mathbb{E}_1[\tau'] \tag{C.92}$$

for a large enough $N$. Using Wald and Wolfowitz's SPRT optimality result [67], we get

$$\alpha' \geq \tilde{\alpha} \tag{C.93}$$

$$\beta' \geq \tilde{\beta}. \tag{C.94}$$

Now it only remains to lower bound $\tilde{\beta}$. Applying [83, Th. 3.1.2, 3.1.3] and (C.50) gives

$$\tilde{\beta} = \tilde{\zeta} e^{-\tilde{a}_0}(1 + o(1)), \tag{C.95}$$

where

$$\tilde{\zeta} = \frac{1}{d_N C}\left(\exp\left\{-\sum_{n=1}^{\infty} \frac{1}{n}\mathbb{P}_0[S_n < 0] + \mathbb{P}_1[S_n > 0]\right\}\right), \tag{C.96}$$

and $S_n$ is as in (C.55). Since $S_n$ is a sum of $nd_N \to \infty$ i.i.d. random variables, where the summands have a non-zero mean, the Chernoff bound implies that each of the probabilities in (C.96) decays exponentially with $d_N$. Thus,

$$\tilde{\zeta} = \frac{1}{d_N C}(1 + o(1)). \tag{C.97}$$

From (C.85) and (C.97), we get

$$-\log \tilde{\beta} = C\left(\frac{N}{1-\epsilon_0} - \frac{d_N}{2} - o(d_N) + o(\log d_N)\right) \tag{C.98}$$

$$\leq C\left(\frac{N}{1-\epsilon} - \frac{d_N}{2} - o(d_N) + o(\log d_N)\right), \tag{C.99}$$

where (C.99) follows from (C.79). Inequalities (C.80), (C.94), and (C.99) imply (4.21).

## C.5 Proof of Lemma C.3.1

We first present a lemma that is used in the proof of Lemma C.3.1 (step 1), we then choose the distribution $P_X^{n_L}$ of the random codewords (step 2) and the parameters $n_1, \dots, n_L, \gamma$ in Theorem 4.3.2 (step 3), and finally, we analyze the bounds in Theorem 4.3.2 using the supporting lemmas (step 4).

Lemma C.5.1, below, gives the asymptotic expansion of the root of an equation. We use Lemma C.5.1 to find the asymptotic expansion for the gap between two consecutive decoding times $n_\ell$ and $n_{\ell+1}$.

**Lemma C.5.1.** *Let $f(x)$ be a differentiable increasing function that satisfies $f'(x) \to 0$ as $x \to \infty$. Suppose that*

$$x + f(x) = y. \tag{C.100}$$

*Then, as $x \to \infty$ it holds that*

$$x = y - f(y)\left(1 - o(1)\right). \tag{C.101}$$

*Proof of Lemma C.5.1:* Define the function $F(x) \triangleq x + f(x) - y$. Applying Newton's method with the starting point $x_0 = y$ yields

$$x_1 = x_0 - \frac{F(x_0)}{F'(x_0)} \tag{C.102}$$

$$= y - \frac{f(y)}{1 + f'(y)} \tag{C.103}$$

$$= y - f(y)(1 - f'(y) + O(f'(y)^2). \tag{C.104}$$

Recall that $f'(y) = o(1)$ by assumption. Equality (C.104) follows from the Taylor series expansion of the function $\frac{1}{1+x}$ around $x = 0$. Let

$$x^\star = y - f(y)(1 - o(1)). \tag{C.105}$$

From Taylor's theorem, it follows that

$$f(x^\star) = f(y) - f'(y_0)f(y)(1 - o(1)), \tag{C.106}$$

for some $y_0 \in [y - f(y)(1 - o(1)), y]$. Therefore, $f'(y_0) = o(1)$, and $f(x^\star) = f(y)(1-o(1))$. Putting (C.105)–(C.106) in (C.100), we see that $x^\star$ is a solution to the equality in (C.100).

■

### Random encoder design

We set the distribution of the random codewords $P_{X^{n_L}}$ as the product of $P_X^*$'s, where $P_X^*$ is the capacity-achieving distribution with minimum dispersion, i.e.,

$$P_{X^{n_L}} = (P_X^*)^{n_L} \tag{C.107}$$

$$P_X^* = \arg\min_{P_X}\{\mathrm{Var}\left[\imath(X;Y)\right] : I(X;Y) = C\}. \tag{C.108}$$

### Choosing the decoding times $n_1, \dots, n_L$

We choose $\gamma, n_1, \dots, n_L$ so that the equalities

$$\gamma = n_\ell C - \sqrt{n_\ell \log_{(L-\ell+1)}(n_\ell) V} \tag{C.109}$$

hold for all $\ell \in [L]$. This choice minimizes the upper bound (4.18) on the average decoding time up to the second-order term in the asymptotic expansion. See Appendix C.7 for the proof. Applying Lemma C.5.1 with

$$x = n_{\ell+1} \tag{C.110}$$

$$y = n_\ell - \frac{1}{C}\sqrt{n_i \log_{(L-\ell+1)}(n_\ell) V} \tag{C.111}$$

$$f(x) = -\frac{1}{C}\sqrt{n_{\ell+1} \log_{(L-\ell)}(n_{\ell+1}) V} \tag{C.112}$$

for $\ell \in \{1, \dots, L-1\}$, gives the following gaps between consecutive decoding times

$$n_{\ell+1} - n_\ell = \frac{1}{C}\Big(\sqrt{n_\ell \log_{(L-\ell)}(n_\ell) V} - \sqrt{n_i \log_{(L-\ell+1)}(n_\ell) V}\Big)(1 + o(1)). \tag{C.113}$$

### Analyzing the bounds in Theorem 4.3.2

Cramér's condition in Theorem 2.4.1 is satisfied for the information density of a DM-PPC since $\imath(X;Y)$ is a bounded random variable. For each $\ell \in [L]$, applying Theorem 2.4.1 with $\gamma, n_1, \dots, n_L$ satisfying (C.109) gives

$$\begin{aligned}
&\mathbb{P}\left[\imath(X^{n_\ell};Y^{n_\ell}) < \gamma\right] \\
&\quad \le Q\left(\sqrt{\log_{(L-\ell+1)}(n_\ell)}\right) \exp\left\{\frac{-(\log_{(L-\ell+1)}(n_\ell))^{3/2}\mu_3}{6\sqrt{n}V^{3/2}}\right\} \\
&\qquad + O\left(\frac{1}{\sqrt{n}}\exp\left\{-\frac{\log_{(L-\ell+1)}(n_\ell)}{2}\right\}\right) \qquad \text{(C.114)} \\
&\quad \le \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{\log_{(L-\ell)}(n_\ell)}}\frac{1}{\sqrt{\log_{(L-\ell+1)}(n_\ell)}}\left(1 + O\left(\frac{(\log_{(L-\ell+1)}(n_\ell))^{(3/2)}}{\sqrt{n_\ell}}\right)\right) \qquad \text{(C.115)}
\end{aligned}$$

for $\ell < L$, where

$$\mu_3 \triangleq \mathbb{E}\left[(\imath(X;Y) - C)^3\right] < \infty, \qquad \text{(C.116)}$$

and (C.115) follows from the Taylor series expansion $\exp\{x\} = 1 + x + O(x^2)$ as $x \to 0$, and the well-known bound (e.g., [28, Ch. 8, eq. (2.46)])

$$Q(x) \le \frac{1}{\sqrt{2\pi}}\frac{1}{x}\exp\left\{-\frac{x^2}{2}\right\} \quad \text{for } x > 0. \qquad \text{(C.117)}$$

For $\ell = L$, Theorem 2.4.1 gives

$$\mathbb{P}\left[\imath(X^{n_L};Y^{n_L}) < \gamma\right] \le \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{n_L}}\frac{1}{\sqrt{\log n_L}}\left(1 + O\left(\frac{(\log n_L)^{(3/2)}}{\sqrt{n_L}}\right)\right). \qquad \text{(C.118)}$$

By Theorem 4.3.2, there exists a VLSF code with $L$ decoding times $n_1 < n_2 < \dots < n_L$ such that the expected decoding time is bounded as

$$N \le n_1 + \sum_{\ell=1}^{L-1}(n_{\ell+1} - n_\ell)\mathbb{P}\left[\imath(X^{n_\ell};Y^{n_\ell}) < \gamma\right]. \qquad \text{(C.119)}$$

By (C.113), we have

$$n_\ell = n_1(1 + o(1)) \qquad \text{(C.120)}$$

for $\ell \in [L]$. Plugging (C.113), (C.115), and (C.120) into (C.119), we get

$$N \le n_1 + \frac{\sqrt{V}}{\sqrt{2\pi}\,C}\frac{\sqrt{n_1}}{\sqrt{\log_{(L)}(n_1)}}(1 + o(1)). \qquad \text{(C.121)}$$

Applying Lemma C.5.1 to (C.121), we get

$$n_1 \geq N - \frac{\sqrt{V}}{2\,C} \frac{\sqrt{N}}{\sqrt{\log_{(L)}(N)}} \tag{C.122}$$

for $n_1$ large enough. Comparing (C.122) and (C.113), we observe that for $n_1$ large enough,

$$n_1 < N < n_2 < \cdots < n_L. \tag{C.123}$$

Further, from (C.109) and (C.121), we have

$$n_L = N\left(1 + O\left(\sqrt{\frac{\log N}{N}}\right)\right). \tag{C.124}$$

Finally, we set message set size $M$ such that

$$\log M = \gamma - \log N. \tag{C.125}$$

Plugging (C.118) and (C.125) into (4.17), we bound the error probability as

$$\begin{aligned}
&\mathbb{P}\left[\mathsf{g}_{\tau^*}(U, Y^{\tau^*}) \neq W\right] \\
&\leq \mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right] + (M-1)\exp\{-\gamma\} && \text{(C.126)}\\
&\leq \frac{1}{2}\frac{1}{\sqrt{n_L}}\frac{1}{\sqrt{\log n_L}} + \frac{1}{N} && \text{(C.127)}\\
&\leq \frac{1}{2}\frac{1}{\sqrt{N}}\frac{1}{\sqrt{\log N}} + \frac{1}{N}, && \text{(C.128)}
\end{aligned}$$

where (C.127) holds for $n_L$ large enough and (C.128) follows from (C.123). Inequality (C.128) implies that the error probability is bounded by $\frac{1}{\sqrt{N \log N}}$ for $N$ large enough. Plugging (C.122) and (C.125) into (C.109) with $\ell = 1$, we conclude that there exists an $(N, L, M, \frac{1}{\sqrt{N \log N}})$ VLSF code with

$$\log M \geq NC - \sqrt{N \log_{(L)}(N) V} - \frac{1}{2}\sqrt{\frac{NV}{\log_{(L)}(N)}} - \log N \tag{C.129}$$

for $N$ large enough, which completes the proof. ■

## C.6 Proof of Theorem 4.4.1

The non-asymptotic achievability bound in Theorem 4.3.2 applies to the Gaussian PPC with maximal power constraint $P$ (4.22) with the modification that the error probability (4.17) has an additional term for the power violation probability

$$\mathbb{P}\left[\bigcup_{\ell=1}^{L}\left\{\|X^{n_\ell}\|_2^2 > n_\ell P\right\}\right]. \tag{C.130}$$

The proof follows similarly to the proof of Theorem 4.3.1 as we employ the sup-optimal SHT strategy in the proof sketch of Theorem 4.3.1. We Lemma C.3.1 to the Gaussian PPC, stating

$$\begin{aligned}&\log M^*\left(N, L, \frac{1}{\sqrt{N\log N}}, P\right)\\ &\geq NC(P) - \sqrt{N\log_{(L)}(N)\, V(P)} + O\left(\sqrt{\frac{N}{\log_{(L)}(N)}}\right).\end{aligned} \tag{C.131}$$

The proof of (C.131) differs from the proof of Lemma C.3.1 in the input distribution $P_{X^{n_L}}$, the analysis on the probability $\mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right]$, and the threshold $\gamma$ in (C.109). Below, we detail these differences.

### The input distribution $P_{X^{n_L}}$

We choose the distribution of the random codewords, $P_{X^{n_L}}$, in Theorem 4.3.2 as follows. Set $n_0 = 0$. For each codeword, we independently draw sub-codewords $X_{n_{j-1}+1}^{n_j}$, $j \in [L]$ from the uniform distribution on the $(n_j - n_{j-1})$-dimensional sphere of radius $\sqrt{(n_j - n_{j-1})P}$. Let $P_{X^{n_L}}$ denote the distribution of the length-$n_L$ random codewords described above. Codewords chosen under $P_{X^{n_L}}$ never violate the power constraint (4.22), thus the power violation probability in (C.130) is 0.

### Bounding the probability of the information density random variable

For each $\ell \in [L]$, we here bound the probability

$$\mathbb{P}\left[\imath(X^{n_\ell}; Y^{n_\ell}) < \gamma\right] \tag{C.132}$$

that appears in Theorem 4.3.2 under the input distribution described above. Note that the random variable $\imath(X^{n_\ell}; Y^{n_\ell})$ is not a sum of $n_\ell$ i.i.d. random variables. We wish to apply the moderate deviations result in Theorem 2.4.1. To do this, we first introduce the following lemma that uniformly bounds the

Radon-Nikodym derivative of the channel output distribution in response to the uniform distribution on a sphere compared to the channel output distribution in response to i.i.d. Gaussian distribution.

**Lemma C.6.1** (MolavianJazi and Laneman [24, Prop. 2])**.** *Let $X^n$ be distributed uniformly over the $n$-dimensional sphere of radius $\sqrt{nP}$. Let $\tilde{X}^n \sim \mathcal{N}(\mathbf{0}, P\mathsf{I}_n)$. Let $P_{Y^n}$ and $P_{\tilde{Y}^n}$ denote the channel output distributions in response to $P_{X^n}$ and $P_{\tilde{X}^n}$, respectively, where $P_{Y^n|X^n}$ is the point-to-point Gaussian channel* (3.68)*. Then there exists an $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ and $y^n \in \mathbb{R}^n$, it holds that*

$$\frac{dP_{Y^n}(y^n)}{dP_{\tilde{Y}^n}(y^n)} \leq J(P) \triangleq 27\sqrt{\frac{\pi}{8}}\frac{1+P}{\sqrt{1+2P}}. \tag{C.133}$$

Let $P_{\tilde{Y}}^{n_\ell}$ be $\mathcal{N}(\mathbf{0}, (1+P)\mathsf{I}_{n_\ell})$. By Lemma C.6.1, we bound (C.132) as

$$\begin{aligned} &\mathbb{P}\left[\imath(X^{n_\ell}; Y^{n_\ell}) < \gamma\right] \\ &= \mathbb{P}\left[\log\frac{dP_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell})}{dP_{\tilde{Y}^{n_\ell}}(Y^{n_\ell})} < \gamma + \log\frac{dP_{Y^{n_\ell}}(Y^{n_\ell})}{dP_{\tilde{Y}^{n_\ell}}(Y^{n_\ell})}\right] &\text{(C.134)} \\ &\leq \mathbb{P}\left[\log\frac{dP_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell})}{dP_{\tilde{Y}^{n_\ell}}(Y^{n_\ell})} < \gamma + \ell\log J(P)\right], &\text{(C.135)} \end{aligned}$$

where $J(P)$ is the constant given in (C.133), and (C.135) follows from the fact that $P_{Y^{n_\ell}}$ is product of $\ell$ output distributions with dimensions $n_j - n_{j-1}, j \in [\ell]$, each induced by a uniform distribution over a sphere with the corresponding radius. As argued in [5], [24], [44], by spherical symmetry, the distribution of the random variable

$$\log\frac{dP_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell})}{dP_{\tilde{Y}^{n_\ell}}(Y^{n_\ell})} \tag{C.136}$$

depends on $X^{n_\ell}$ only through its norm $\|X^{n_\ell}\|_2$. Since $\|X^{n_\ell}\|_2^2 = n_\ell P$ with probability 1, any choice of $x^{n_\ell}$ such that $\|x^{n_i}\|_2^2 = n_i P$ for $i \in [\ell]$ gives

$$\begin{aligned} &\mathbb{P}\left[\log\frac{dP_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell})}{dP_{\tilde{Y}^{n_\ell}}(Y^{n_\ell})} < \gamma + \ell\log J(P)\right] \\ &= \mathbb{P}\left[\log\frac{dP_{Y^{n_\ell}|X^{n_\ell}}(Y^{n_\ell}|X^{n_\ell})}{dP_{\tilde{Y}^{n_\ell}}(Y^{n_\ell})} < \gamma + \ell\log J(P)\middle| X^{n_\ell} = x^{n_\ell}\right] &\text{(C.137)} \end{aligned}$$

We set $x^{n_\ell} = (\sqrt{P}, \sqrt{P}, \ldots, \sqrt{P}) = \sqrt{P}\mathbf{1}$ to obtain an i.i.d. sum in (C.137). Given $X^{n_\ell} = \sqrt{P}\mathbf{1}$, the distribution of (C.136) is the same as the distribution of the sum

$$\sum_{i=1}^{n_\ell} A_i \tag{C.138}$$

of $n_\ell$ i.i.d. random variables

$$A_i = C(P) + \frac{P}{2(1+P)}\left(1 - Z_i^2 + \frac{2}{\sqrt{P}} Z_i\right), \quad i \in [n_\ell], \tag{C.139}$$

where $Z_1, \dots, Z_{n_\ell}$ are drawn independently from $\mathcal{N}(0,1)$ (see e.g., [5, eq. (205)]). The mean and variance of $A_1$ are

$$\mathbb{E}\left[A_1\right] = C(P) \tag{C.140}$$

$$\mathrm{Var}\left[A_1\right] = V(P). \tag{C.141}$$

From (C.135)–(C.138), we get

$$\mathbb{P}\left[\imath(X^{n_\ell}; Y^{n_\ell}) < \gamma\right] \leq \mathbb{P}\left[\sum_{i=1}^{n_\ell} A_i < \gamma + \ell \log J(P)\right]. \tag{C.142}$$

To verify that Theorem 2.4.1 is applicable to the right-hand side of (C.142), it only remains to show that $\mathbb{E}\left[(A_1 - C(P))^3\right]$ is finite, and $A_1 - C(P)$ satisfies Cramér's condition, that is, there exists some $t_0 > 0$ such that $\mathbb{E}\left[\exp\{t(A_1 - C(P))\}\right] < \infty$ for all $|t|< t_0$. From (C.139), $(A_1 - C(P))^3$ is distributed the same as a 6-degree polynomial of the Gaussian random variable $Z \sim \mathcal{N}(0,1)$. This polynomial has a finite mean since all moments of $Z$ are finite. Let $c \triangleq \frac{P}{2(1+P)}$, $f \triangleq \frac{2}{\sqrt{P}}$, and $t' \triangleq tc$. To show that Cramér's condition holds, we compute

$$\begin{aligned}
&\mathbb{E}\left[\exp\{t(A_1 - C(P))\}\right] \\
&= \mathbb{E}\left[\exp\{t'(1 - Z^2 + fZ)\}\right] && \text{(C.143)}\\
&= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{x^2}{2} + t'(1 - x^2 + fx)\right\} dx && \text{(C.144)}\\
&= \frac{1}{\sqrt{1+2t'}} \exp\left\{t' + \frac{t'f}{2(1+2t')}\right\}. && \text{(C.145)}
\end{aligned}$$

Thus, $\mathbb{E}\left[\exp\{t(A_1 - C(P))\}\right] < \infty$ for $t' > -\frac{1}{2}$, and $t_0 = \frac{1}{2c} > 0$ satisfies Cramér's condition.

### The threshold $\gamma$

We set $\gamma, n_1, \dots, n_L$ so that the equalities

$$\gamma = n_\ell C(P) - \sqrt{n_\ell \log_{(L-\ell+1)}(n_\ell) V(P)} - \ell \log J(P) \tag{C.146}$$

hold for all $\ell \in [L]$.

The rest of the proof follows identically to (C.114)–(C.129) with $C$ and $V$ replaced by $C(P)$ and $V(P)$, respectively, giving

$$\log M \geq NC(P) - \sqrt{N \log_{(L)}(N) V(P)} - \frac{1}{2}\sqrt{\frac{NV(P)}{\log_{(L)}(N)}} \\ - \log N - L \log J(P). \tag{C.147}$$

■

From Shannon's work in [6], it is well-known that for the Gaussian channel with a maximal power constraint, drawing i.i.d. Gaussian codewords yields a performance inferior to that achieved by the uniform distribution on the power sphere. As a result, almost all tight achievability bounds for the Gaussian channel in the fixed-length regime under a variety of settings (e.g., all four combinations of the maximal/average power constraint and feedback/no feedback [44], [62], [84], [148] in Table I) employ random codewords drawn uniformly on the power sphere. A notable exception is Truong and Tan's result in (4.26) [71, Th. 1] for VLSF codes with an average power constraint; that result employs i.i.d. Gaussian inputs. The Gaussian distribution works in this scenario because when $L = \infty$, the usually dominant term $\mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right]$ in (4.17) disappears. The second term $(M-1)\exp\{-\gamma\}$ in (4.17) is not affected by the input distribution. Unfortunately, the approach from [71, Th. 1] does not work here since drawing codewords i.i.d. $\mathcal{N}(0, P)$ satisfies the average power constraint (4.23) but not the maximal power constraint (4.22). When $L = O(1)$ and the probability $\mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right]$ dominates, using i.i.d. $\mathcal{N}(0, P)$ inputs achieves a worse second-order term in the asymptotic expansion (4.28) of the maximum achievable message set size. This implies that when $L = O(1)$, using our uniform distribution on a subset of the power sphere is superior to choosing codewords i.i.d. $\mathcal{N}(0, P)$ even under the average power constraint. In particular, i.i.d. $\mathcal{N}(0, P)$ inputs achieve (4.12), where the dispersion $V(P)$ is replaced by the variance $\tilde{V}(P) = \frac{P}{1+P}$ of $\imath(X; Y)$ when $X \sim \mathcal{N}(0, P)$; here $\tilde{V}(P)$ is greater than the dispersion $V(P)$ for all $P > 0$ (see [135, eq. (2.56)]). Whether our input distribution is optimal in the second-order term remains an open question.

## C.7 Second-order optimality of the decoding times in Theorem 4.3.1

From the code construction in Appendix C.3 and Theorem 4.3.2, the average decoding time is

$$N(n_2, \dots, n_L, \gamma) = N'(1-\epsilon)\frac{1}{1-\epsilon'_N}, \tag{C.148}$$

where

$$N' = n_2 + \sum_{i=2}^{L-1}(n_{i+1}-n_i)\mathbb{P}\left[\imath(X^{n_i}; Y^{n_i}) < \gamma\right] \tag{C.149}$$

$$\epsilon'_N = \mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right] + M\exp\{-\gamma\}. \tag{C.150}$$

We here show that given a fixed $M$, the parameters $n_2, n_3, \dots, n_L, \gamma$ chosen according to (C.109) and (C.125) (and also the error value $\epsilon'_N$ chosen in (4.14) since $\epsilon'_N$ is a function of $(n_L, \gamma)$) minimize the average decoding time in (C.148) in the sense that the second-order expansion of $\log M$ in terms of $N$ is maximum. That is, our parameter choice optimizes our bound on our code construction.

### C.7.1 Optimality of $n_2, \dots, n_{L-1}$

We first set $n_L$ and $\gamma$ to satisfy the equations

$$\frac{1}{\sqrt{n_L \log n_L}} = \mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right] + (M-1)\exp\{-\gamma\} \tag{C.151}$$

$$\log M = \gamma - \log n_L, \tag{C.152}$$

and optimize the values of $n_2, \dots, n_{L-1}$ under (C.151)–(C.152). Section C.7.2 proves the optimality of the choices in (C.151)–(C.152).

Under (C.151)–(C.152), the optimization problem in (C.148)–(C.150) reduces to

$$\begin{aligned} \min \quad & N'(n_2, \dots, n_{L-1}) \\ & = n_2 + \sum_{i=2}^{L-1}(n_{i+1}-n_i)\mathbb{P}\left[\imath(X^{n_i}; Y^{n_i}) < \gamma\right] \\ \text{s.t.} \quad & \frac{1}{\sqrt{n_L \log n_L}} = \mathbb{P}\left[\imath(X^{n_L}; Y^{n_L}) < \gamma\right] \\ & \qquad + (M-1)\exp\{-\gamma\}. \end{aligned} \tag{C.153}$$

Next, we define the functions

$$g(n) \triangleq \frac{nC-\gamma}{\sqrt{nV}} \tag{C.154}$$

$$F(n) \triangleq Q(-g(n)) = 1 - Q(g(n)) \tag{C.155}$$

$$f(n) \triangleq F'(n) = \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{g(n)^2}{2}\right\} g'(n). \tag{C.156}$$

Assume that $\gamma = \gamma_n$ is such that $g(n) = O(n^{1/6})$, and $\lim_{n\to\infty} g(n) = \infty$. Then by Theorem 2.4.1, $\mathbb{P}[\imath(X^n; Y^n) < \gamma]$, which is a step-wise constant function of $n$, is approximated by differentiable function $1 - F(n)$ as

$$\mathbb{P}[\imath(X^n; Y^n) < \gamma] = (1 - F(n))(1 + o(1)). \tag{C.157}$$

Taylor series expansions give

$$1 - F(n) = \frac{1}{g(n)} \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{g(n)^2}{2}\right\} (1 + o(1)) \tag{C.158}$$

$$f(n) = (1 - F(n)) g(n) g'(n) (1 + o(1)) \tag{C.159}$$

$$g'(n) = \frac{C}{\sqrt{nV}} (1 + o(1)). \tag{C.160}$$

Let $\mathbf{n}^* = (n_2^*, \ldots, n_{L-1}^*)$ denote the solution to the optimization problem in (C.153) with $\mathbb{P}[\imath(X^n; Y^n) < \gamma]$ replaced by $(1 - F(n))$. Then $\mathbf{n}^*$ must satisfy the Karush-Kuhn-Tucker conditions $\nabla N'(\mathbf{n}^*) = \mathbf{0}$, giving

$$\left.\frac{\partial N'}{\partial n_2}\right|_{\mathbf{n}=\mathbf{n}^*} = F(n_2^*) - (n_3^* - n_2^*) f(n_2^*) = 0 \tag{C.161}$$

$$\left.\frac{\partial N'}{\partial n_\ell}\right|_{\mathbf{n}=\mathbf{n}^*} = F(n_\ell^*) - F(n_{L-1}^*) - (n_{\ell+1}^* - n_\ell^*) f(n_\ell^*) = 0 \tag{C.162}$$

for $\ell = 3, \ldots, L - 1$.

Let $\tilde{\mathbf{n}} = (\tilde{n}_2, \ldots, \tilde{n}_{L-1})$ be the decoding times chosen in (C.109). We evaluate

$$g(\tilde{n}_i) = \sqrt{\log_{(L-i+1)}(\tilde{n}_i)} (1 + o(1)) \tag{C.163}$$

$$1 - F(g(\tilde{n}_i)) = \frac{1}{\sqrt{2\pi}} \frac{1}{g(\tilde{n}_{i+1}) g(\tilde{n}_i)} (1 + o(1)) \tag{C.164}$$

$$f(g(\tilde{n}_i)) = \frac{1}{\sqrt{2\pi}} \frac{g'(\tilde{n}_i)}{g(\tilde{n}_{i+1})} \tag{C.165}$$

$$\tilde{n}_{i+1} - \tilde{n}_i = \frac{g(\tilde{n}_{i+1})}{g'(\tilde{n}_i)} (1 + o(1)) \tag{C.166}$$

for $i = 2, \ldots, L - 1$, and

$$\nabla N'(\tilde{\mathbf{n}}) = \left(1 - \frac{1}{\sqrt{2\pi}}, -\frac{1}{\sqrt{2\pi}}, -\frac{1}{\sqrt{2\pi}}, \ldots, -\frac{1}{\sqrt{2\pi}}\right)$$

$$(1+o(1)). \tag{C.167}$$

Our goal is to find a vector $\mathbf{\Delta n} = (\Delta n_2, \ldots, \Delta n_{L-1})$ such that

$$\nabla N'(\tilde{\mathbf{n}} + \mathbf{\Delta n}) = \mathbf{0}, \tag{C.168}$$

Assume that $\Delta n = O(\sqrt{n})$. By plugging $n + \Delta n$ into (C.158)–(C.160) and using the Taylor series expansion of $g(n+\Delta n)$, we get

$$\begin{aligned} 1 - F(n+\Delta n) &= (1-F(n)) \\ &\quad \cdot \exp\{-\Delta n g(n) g'(n)\}(1+o(1)) && \text{(C.169)} \\ f(n+\Delta n) &= f(n)\exp\{-\Delta n g(n) g'(n)\}(1+o(1)). && \text{(C.170)} \end{aligned}$$

Using (C.169)–(C.170), and putting $\tilde{\mathbf{n}} + \mathbf{\Delta n}$ in (C.161)–(C.162), we solve (C.168) as

$$\begin{aligned} \Delta n_2 &= -\frac{\log\sqrt{2\pi}}{g(\tilde{n}_2)g'(\tilde{n}_2)}(1+o(1)) && \text{(C.171)} \\ &= -\frac{\sqrt{V}\,\log\sqrt{2\pi}}{C}\frac{\sqrt{\tilde{n}_2}}{\sqrt{\log_{(L-1)}(\tilde{n}_2)}}(1+o(1)) && \text{(C.172)} \\ \Delta n_i &= \frac{1}{2}\frac{g(\tilde{n}_{i-1})^2}{g(\tilde{n}_i)g'(\tilde{n}_i)} = o(\Delta n_2)(1+o(1)) && \text{(C.173)} \end{aligned}$$

for $i = 3, \ldots, L-1$. Hence, $\tilde{\mathbf{n}} + \mathbf{\Delta n}$ satisfies the optimality criterion, and $\mathbf{n}^* = \tilde{\mathbf{n}} + \mathbf{\Delta n}$.

It remains only to evaluate the gap $N'(\mathbf{n}^*) - N'(\tilde{\mathbf{n}})$. We have

$$\begin{aligned} &N'(\mathbf{n}^*) - N'(\tilde{\mathbf{n}}) \\ &= \Bigg(\Delta n_2 + \sum_{i=2}^{L-1}(\tilde{n}_{i+1} - \tilde{n}_i)Q(g(\tilde{n}_i)) \\ &\quad \cdot (\exp\{-\Delta n_i g(\tilde{n}_i)g'(\tilde{n}_i)\} - 1)\Bigg)(1+o(1)) && \text{(C.174)} \\ &= \left(\Delta n_2 + \left(1 - \frac{1}{\sqrt{2\pi}}\right)\frac{1}{g(\tilde{n}_1)g'(\tilde{n}_i)} - \sum_{i=3}^{L-1}\Delta n_i\right) \\ &\quad \cdot (1+o(1)) && \text{(C.175)} \\ &= -B\frac{\sqrt{\tilde{n}_2}}{\sqrt{\log_{(L-1)}(\tilde{n}_2)}}(1+o(1)), && \text{(C.176)} \end{aligned}$$

where $B = \left(\log\sqrt{2\pi} + \frac{1}{\sqrt{2\pi}} - 1\right)\frac{\sqrt{V}}{C}$ is a positive constant. From the relationship between $n_\ell$ and $n_2$ in (C.120) and the equality (C.176), we get

$$N'(\tilde{\mathbf{n}}) = N'(\mathbf{n}^*) + B\frac{\sqrt{N'(\mathbf{n}^*)}}{\sqrt{\log_{(L-1)}(N'(\mathbf{n}^*))}}(1+o(1)). \tag{C.177}$$

Plugging (C.177) into our VLSF achievability bound (C.129) gives

$$\begin{aligned}\log M \geq{} & N'(\mathbf{n}^*)C - \sqrt{N'(\mathbf{n}^*)\log_{(L-1)}(N'(\mathbf{n}^*))V} \\ & - O\left(\sqrt{\frac{N'(\mathbf{n}^*)}{\log_{(L-1)}(N'(\mathbf{n}^*))}}\right). \end{aligned} \tag{C.178}$$

Comparing (C.178) and (C.129), note that the decoding times chosen in (C.109) have the optimal second-order term in the asymptotic expansion of the maximum achievable message set size within our code construction. Moreover, the order of the third-order term in (C.178) is the same as the order of the third-order term in (C.129). ■

**Remark C.7.1.** *The method of approximating the probability* $\mathbb{P}\left[\imath(X^n; Y^n) \geq \gamma\right]$*, which is an upper bound for* $\mathbb{P}\left[\tau \leq n\right]$ *(see (C.22)), by a differentiable function* $F(n)$ *is introduced in [77, Sec. III] for the optimization problem in (C.153). In [77], Vakilinia* et al. *approximate the distribution of the random stopping time* $\tau$ *by the Gaussian distribution, where* $\mathbb{E}\left[\tau\right]$ *and* $\mathrm{Var}\left[\tau\right]$ *are found empirically. They derive the Karush-Kuhn-Tucker conditions in (C.161)–(C.162), which is known as the SDO algorithm. A similar analysis appears in [79] for the binary erasure channel. The analyses in [77], [79] use the SDO algorithm to numerically solve the equations (C.161)–(C.162) for a fixed* $L$*,* $M$*, and* $\epsilon$*. Unlike [77], [79], we find the analytic solution to (C.161)–(C.162) as decoding times* $n_2, \ldots, n_L$ *approach infinity, and we derive the achievable rate in Theorem 4.3.1 as a function of* $L$*.*

### C.7.2 Optimality of $n_L$ and $\gamma$

Let $(\mathbf{n}^*, \gamma^*) = (n_2^*, \ldots, n_L^*, \gamma^*)$ be the solution to $\nabla N(\mathbf{n}^*, \gamma^*) = \mathbf{0}$ in (C.148). Section A finds the values of $n_2^*, n_3^*, \ldots, n_{L-1}^*$ that minimize $N'$. Minimizing $N'$ also minimizes $N$ in (C.148) since $\epsilon'_N$ depends only on $n_L$ and $\gamma$, and $\epsilon$ is a constant. Therefore, to minimize $N$, it only remains to find $(n_L^*, \gamma^*)$ such that

$$\left.\frac{\partial N}{\partial n_L}\right|_{(\mathbf{n},\gamma)=(\mathbf{n}^*,\gamma^*)} = 0 \tag{C.179}$$

$$\left.\frac{\partial N}{\partial \gamma}\right|_{(\mathbf{n},\gamma)=(\mathbf{n}^*,\gamma^*)} = 0. \tag{C.180}$$

Consider the case where $L > 2$. Solving (C.179) and (C.180) using (C.161)–(C.166) gives

$$g(n_L^*) = \sqrt{\log n_L^* + \log_{(2)}(n_L^*) + \log_{(3)}(n_L^*) + O(1)} \tag{C.181}$$

$$0 = c_0 + N'\left(\frac{1}{\sqrt{2\pi n_L^*}} \exp\left\{-\frac{g(n_L^*)^2}{2}\right\}(1+o(1)) \right.$$
$$\left. - M\exp\{-\gamma^*\}\right), \tag{C.182}$$

where $c_0$ is a positive constant. Solving (C.181)–(C.182) simultaneously, we obtain

$$\log M = \gamma^* - \log n_L^* + O(1). \tag{C.183}$$

Plugging (C.181) and (C.183) into (C.150), we get

$$\epsilon_{N'}{}^* = \frac{c_1}{\sqrt{n_L^* \log_{(2)}(n_L^*) \log n_L^*}}(1+o(1)), \tag{C.184}$$

where $c_1$ is a constant. Let $(\tilde{\mathbf{n}}, \tilde{\gamma}) = (\tilde{n}_2, \dots, \tilde{n}_K, \tilde{\gamma})$ be the parameters chosen in (C.109) and (C.125). Note that $\epsilon_N'^*$ is order-wise different than $\epsilon_N'$ in (4.14). Following steps similar to (C.174)–(C.176), we compute

$$N(\mathbf{n}^*, \gamma^*) - N(\tilde{\mathbf{n}}, \tilde{\gamma}) = -O\left(\sqrt{\frac{n_L^*}{\log n_L^*}}\right). \tag{C.185}$$

Plugging (C.185) into (4.12) gives

$$\log M = \frac{N(\mathbf{n}^*, \gamma^*)C}{1-\epsilon}$$
$$- \sqrt{N(\mathbf{n}^*, \gamma^*) \log_{(L-1)}(N(\mathbf{n}^*, \gamma^*))\frac{V}{1-\epsilon}}$$
$$+ O\left(\sqrt{\frac{N(\mathbf{n}^*, \gamma^*)}{\log_{(L-1)}(N(\mathbf{n}^*, \gamma^*))}}\right). \tag{C.186}$$

Comparing (4.12) and (C.186), we see that although (4.14) and (C.184) are different, the parameters $(\tilde{\mathbf{n}}, \tilde{\gamma})$ chosen in (C.109) and (C.125) have the same second-order term in the asymptotic expansion of the maximum achievable message set size as the parameters $(\mathbf{n}^*, \gamma^*)$ that minimize the average decoding time in the achievability bound in Theorem 4.3.2.

For $L = 2$, the summation term in (C.149) disappears; in this case, the solution to (C.179) gives

$$\epsilon_{N'}{}^{*} = \frac{c_2}{\sqrt{n_L^* \log n_L^*}}(1 + o(1)) \tag{C.187}$$

for some constant $c_2$. Following the steps in (C.185)–(C.186), we conclude that the parameter choices in (C.109) and (C.125) are second-order optimal for $L = 2$ as well.

# Appendix D

# APPENDIX FOR CHAPTER 5

In this section, we prove our main results for the DM-MAC, beginning with Theorem 5.3.2, which is used to prove Theorem 5.3.1.

## D.1 Proof of Theorem 5.3.2

For each transmitter $k$, $k \in [K]$, we generate $M_k$ $n_L$-dimensional codewords i.i.d. from $P_{X_k}^{n_L}$. Codewords for distinct transmitters are drawn independently of each other. Denote the codeword for transmitter $k$ and message $m_k$ by $X_k^{n_L}(m_k)$ for $k \in [K]$ and $m_k \in [M_k]$. The proof extends the DM-PPC achievability bound in Theorem 4.3.2 that is based on a sub-optimal SHT to the DM-MAC. Below, we explain the differences.

Without loss of generality, assume that $m_{[K]} =$ \1 is transmitted. The hypothesis test in (C.7)–(C.8) is replaced by

$$H_0\colon (X_{[K]}^{n_L}, Y_K^{n_L}) \sim \left(\prod_{k=1}^{K} P_{X_k}^{n_L}\right) \times P_{Y_K|X_{[K]}}^{n_L} \tag{D.1}$$

$$H_1\colon (X_{[K]}^{n_L}, Y_K^{n_L}) \sim \left(\prod_{k=1}^{K} P_{X_k}^{n_L}\right) \times P_{Y_K}^{n_L}, \tag{D.2}$$

which is run for every message tuple $m_{[K]} \in \prod_{k=1}^{K} [M_k]$. The information density (C.16), the stopping times (C.17)–(C.18), and the decision rule (C.19) are extended to the DM-MAC as

$$S_{m_{[K]}}^n \triangleq \imath_K(X_{[K]}^n(m_{[K]}); Y_K^n) \tag{D.3}$$

$$\tau_{m_{[K]}} \triangleq \inf\{n_\ell \in \mathcal{N}\colon S_{m_{[K]}, n_\ell} \geq \gamma\} \tag{D.4}$$

$$\tilde{\tau}_{m_{[K]}} \triangleq \min\{\tau_{m_{[K]}}, n_L\} \tag{D.5}$$

$$\delta_{m_{[K]}} \triangleq \begin{cases} 0 & \text{if } S_{m_{[K]}, n_\ell} \geq \gamma \\ 1 & \text{if } S_{m_{[K]}, n_\ell} < \gamma \end{cases} \tag{D.6}$$

for every message tuple $m_{[K]}$. For brevity, define the random variables

$$\tau \triangleq \inf\{n_\ell \in \mathcal{N}\colon \imath_K(X_{[K]}^{n_\ell}; Y_K^{n_\ell}) \geq \gamma\} \tag{D.7}$$

$$\bar{\tau} \triangleq \inf\{n_\ell \in \mathcal{N} \colon \imath_K(\bar{X}_{[K]}; Y_K^{n_\ell}) \geq \gamma\}, \tag{D.8}$$

where the components of $(X_{[K]}^{n_\ell}, Y_K^{n_\ell}, \bar{X}_{[K]}^{n_\ell})$ are drawn i.i.d. according to the joint distribution

$$\begin{aligned} &P_{X_{[K]},Y_K,\bar{X}_{[K]}}(x_{[K]}, y, \bar{x}_{[K]}) \\ &= P_{Y_K|X_{[K]}}(y|x_{[K]}) \prod_{k=1}^{K} P_{X_k}(x_k) P_{X_k}(\bar{x}_k). \end{aligned} \tag{D.9}$$

*Expected decoding time analysis:* Following steps identical to (C.20)–(C.22), we get (5.16).

*Error probability analysis:* The following error analysis extends the PPC bounds in (C.15) and (C.25)–(C.33) to the DM-MAC.

In the analysis below, for brevity, we write $m_{\mathcal{A}} \neq 1$ to denote that $m_i \neq 1$ for $i \in \mathcal{A}$. The error probability is bounded as

$$\epsilon \leq \mathbb{P}\Bigg[ \bigcup_{m_{[K]} \neq \mathbf{1}} \{\tau_{m_{[K]}} \leq \tau_{\mathbf{1}} < \infty\} \bigcup \{\tau_{\mathbf{1}} = \infty\} \Bigg] \tag{D.10}$$

$$\leq \mathbb{P}\left[\tau_{\mathbf{1}} = \infty\right] + \mathbb{P}\left[ \bigcup_{m_{[K]} \neq 1} \{\tau_{m_{[K]}} < \infty\} \right] \tag{D.11}$$

$$+ \mathbb{P}\left[ \bigcup_{\substack{m_{[K]} \neq \mathbf{1} : \exists\, i \in [K] \\ m_i = 1}} \{\tau_{m_{[K]}} < \infty\} \right], \tag{D.12}$$

where (D.11)–(D.12) apply the union bound to separate the probabilities of the following error events:

1. the information density of the true message tuple does not satisfy the threshold test for any available decoding time;
2. the information density of a message tuple in which all messages are incorrect satisfies the threshold test for some decoding time;
3. the information density of a message tuple in which the messages from some transmitters are correct and the messages from the other transmitters are incorrect satisfies the threshold test for some decoding time.

The terms in (D.11) are bounded using steps identical to (C.25)–(C.33) as

$$\mathbb{P}\left[\tau_{\mathbf{1}} = \infty\right] \leq \mathbb{P}\left[\imath_K(X_{[K]}^{n_L}; Y_K^{n_L}) < \gamma\right] \tag{D.13}$$

$$\mathbb{P}\left[\bigcup_{m_{[K]} \neq 1} \{\tau_{m_{[K]}} < \infty\}\right] \leq \prod_{k=1}^{K} (M_k - 1) \exp\{-\gamma\}. \tag{D.14}$$

For the cases where at least one message is decoded correctly, we delay the application of the union bound. Let $\mathcal{A} \in \mathcal{P}([K])$ be the set of transmitters whose messages are decoded correctly. Define

$$\begin{aligned} \mathcal{M}^{(\mathcal{A})} \triangleq \{m_{[K]} \in [M]^K \colon & m_k = 1 \text{ for } k \in \mathcal{A}, \\ & m_k \neq 1 \text{ for } k \in \mathcal{A}^{\mathrm{c}}\} \end{aligned} \tag{D.15}$$

$$\tilde{\mathcal{M}}^{(\mathcal{A})} \triangleq \{m_{\mathcal{A}} \in [M]^{|\mathcal{A}|} \colon m_k \neq 1 \text{ for } k \in \mathcal{A}\}. \tag{D.16}$$

We first bound the probability term in (D.12) by applying the union bound according to which subset $\mathcal{A}$ of the transmitter set $[K]$ is decoded correctly, and get

$$\begin{aligned} &\mathbb{P}\left[\bigcup_{\substack{m_{[K]} \neq \mathbf{1} : \exists\, i \in [K] \\ m_i = 1}} \{\tau_{m_{[K]}} < \infty\}\right] \\ &\leq \sum_{\mathcal{A} \in \mathcal{P}([K])} \mathbb{P}\left[\bigcup_{m_{[K]} \in \mathcal{M}^{(\mathcal{A})}} \{\tau_{m_{[K]}} < \infty\}\right] && \text{(D.17)} \\ &= \sum_{\mathcal{A} \in \mathcal{P}([K])} \mathbb{P}\left[\bigcup_{\substack{m_{\mathcal{A}^c} \in \tilde{\mathcal{M}}^{(\mathcal{A}^c)} \\ n_\ell \in \mathcal{N}}} \{\imath_K(\bar{X}_{\mathcal{A}^c}^{n_\ell}(m_{\mathcal{A}^c}), X_{\mathcal{A}}^{n_\ell}; Y_K^{n_\ell}) \geq \gamma\}\right], && \text{(D.18)} \end{aligned}$$

where $\bar{X}_{\mathcal{A}^c}^{n_\ell}(m_{\mathcal{A}^c})$ refers to the random sample from the codebooks of transmitter set $\mathcal{A}^c$, independent from the codewords $X_{\mathcal{A}^c}^{n_\ell}$ transmitted by the transmitters $\mathcal{A}^c$ and the received output $Y^{n_\ell}$.

We bound the right-hand side of (D.18) using the same method as in [85, eq. (65)–(66)]. This step is crucial in enabling the single-threshold rule for the rate vectors approaching a point on the sum-rate boundary. Set an arbitrary $\lambda^{(\mathcal{A})} > 0$. Define two events

$$\mathcal{E}(\mathcal{A}) \triangleq \bigcup_{n_\ell \in \mathcal{N}} \{\imath_K(X_{\mathcal{A}}^{n_\ell}; Y_K^{n_\ell}) > N I_K(X_{\mathcal{A}}; Y_K) + N\lambda^{(\mathcal{A})}\} \tag{D.19}$$

$$\mathcal{F}(\mathcal{A}) \triangleq \bigcup_{\substack{m_{\mathcal{A}^c} \in \tilde{\mathcal{M}}^{(\mathcal{A}^c)} \\ n_\ell \in \mathcal{N}}} \left\{ \imath_K(\bar{X}_{\mathcal{A}^c}^{n_\ell}(m_{\mathcal{A}^c}), X_{\mathcal{A}}^{n_\ell}; Y_K^{n_\ell}) \geq \gamma \right\}. \tag{D.20}$$

Define the threshold

$$\bar{\gamma}^{(\mathcal{A})} \triangleq \gamma - N I_K(X_{\mathcal{A}}; Y_K) - N\lambda^{(\mathcal{A})}. \tag{D.21}$$

We have

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{F}(\mathcal{A})\right] \\
&= \mathbb{P}\left[\mathcal{F}(\mathcal{A}) \cap \mathcal{E}(\mathcal{A})\right] + \mathbb{P}\left[\mathcal{F}(\mathcal{A}) \cap \mathcal{E}(\mathcal{A})^c\right] && \text{(D.22)} \\
&\leq \mathbb{P}\left[\mathcal{E}(\mathcal{A})\right] \\
&+ \mathbb{P}\left[ \bigcup_{\substack{m_{\mathcal{A}^c} \in \tilde{\mathcal{M}}^{(\mathcal{A}^c)} \\ n_\ell \in \mathcal{N}}} \left\{ \imath_K(\bar{X}_{\mathcal{A}^c}^{n_\ell}(m_{\mathcal{A}^c}); Y_K^{n_\ell} | X_{\mathcal{A}}^{n_\ell}) \geq \bar{\gamma}^{(\mathcal{A})} \right\} \right] && \text{(D.23)} \\
&\leq \sum_{n_\ell \in \mathcal{N}} \mathbb{P}\left[ \imath_K(X_{\mathcal{A}}^{n_\ell}; Y_K^{n_\ell}) > N I_K(X_{\mathcal{A}}; Y_K) + N\lambda^{(\mathcal{A})} \right] \\
&+ \prod_{k \in \mathcal{A}^c} (M_k - 1) \mathbb{P}\left[ \bigcup_{n_\ell \in \mathcal{N}} \left\{ \imath_K(\bar{X}_{\mathcal{A}^c}^{n_\ell}; Y_K^{n_\ell} | X_{\mathcal{A}}^{n_\ell}) \geq \bar{\gamma}^{(\mathcal{A})} \right\} \right] && \text{(D.24)} \\
&\leq \sum_{n_\ell \in \mathcal{N}} \mathbb{P}\left[ \imath_K(X_{\mathcal{A}}^{n_\ell}; Y_K^{n_\ell}) > N I_K(X_{\mathcal{A}}; Y_K) + N\lambda^{(\mathcal{A})} \right] \\
&\quad + \prod_{k \in \mathcal{A}^c} (M_k - 1) \exp\{-\bar{\gamma}^{(\mathcal{A})}\}, && \text{(D.25)}
\end{aligned}$$

where inequality (D.23) uses the chain rule for mutual information, (D.24) applies the union bound, and (D.25) follows from [72, eq. (88)].

Applying the bound in (D.25) to each of the probabilities in (D.18) and plugging (D.13), (D.14), and (D.18) into (D.11)–(D.12), we complete the proof of Theorem 5.3.2.

## D.2 Proof of Theorem 5.3.1

We employ the sub-optimal SHT strategy in the proof sketch of Theorem 4.3.1 with $\epsilon'_N = \frac{1}{\sqrt{N' \log N'}}$. Therefore, we first show that there exists an $(N, L, M_{[K]}, 1/\sqrt{N \log N})$ VLSF code satisfying

$$\begin{aligned}
\sum_{k=1}^{K} \log M_k = N I_K - \sqrt{N \log_{(L)}(N) V_K} \\
+ O\left( \sqrt{\frac{N V_K}{\log_{(L)}(N)}} \right).
\end{aligned} \tag{D.26}$$

We set the parameters

$$\gamma = n_\ell I_K - \sqrt{n_\ell \log_{(L-\ell+1)}(n_\ell) V_K} \quad \forall\, \ell \in [L] \tag{D.27}$$

$$= \sum_{k=1}^{K} \log M_k + \log N \tag{D.28}$$

$$\lambda^{(\mathcal{A})} = \frac{N I_K(X_{\mathcal{A}^c}; Y_K | X_{\mathcal{A}}) - \sum_{k \in \mathcal{A}^c} \log M_k}{2N}, \quad \mathcal{A} \in \mathcal{P}([K]). \tag{D.29}$$

Recall that $\lambda^{(\mathcal{A})}$'s are bounded below by a positive constant since the rate point lies on the sum-rate boundary (5.11).

By Theorem 5.3.2, there exists a VLSF code with $L$ decoding times $n_1 < n_2 < \cdots < n_L$ such that the average decoding time is bounded as

$$N \leq n_1 + \sum_{\ell=1}^{L-1} (n_{\ell+1} - n_\ell) \mathbb{P}\left[\imath_K(X_{[K]}^{n_\ell}; Y_K^{n_\ell}) < \gamma\right]. \tag{D.30}$$

Following the analysis in (C.121)–(C.124), we conclude that

$$n_\ell = N(1 + o(1)) \tag{D.31}$$

for all $\ell \in [L]$. Applying the Chernoff bound to the probability terms in (5.14)–(5.15) using (D.27) and (D.31), we get that the sum of the terms in (5.14)–(5.15) is bounded by $\exp\{-NE\}$ for some $E > 0$.

Applying Theorem 2.4.1 to the probability in (5.12) with (D.27) gives

$$\mathbb{P}\left[\imath_K(X_{[K]}^{n_L}; Y_K^{n_L}) < \gamma\right] \leq \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{n_L}} \frac{1}{\sqrt{\log n_L}} \cdot \left(1 + O\left(\frac{(\log n_L)^{(3/2)}}{\sqrt{n_L}}\right)\right). \tag{D.32}$$

Applying Theorem 5.3.2 with (D.28), (D.32), and the exponential bound on the sum of the terms in (5.14)–(5.15), we bound the error probability as

$$\mathbb{P}\left[\mathsf{g}_{\tau^*}(U, Y^{\tau^*}) \neq W_{[K]}\right] \leq \frac{1}{\sqrt{2\pi}} \frac{1}{\sqrt{N}} \frac{1}{\sqrt{\log N}} \cdot \left(1 + O\left(\frac{(\log N)^{(3/2)}}{\sqrt{N}}\right)\right) + \frac{1}{N} + \exp\{-NE\}, \tag{D.33}$$

which is further bounded by $\frac{1}{\sqrt{N \log N}}$ for $N$ large enough. Following steps identical to (C.121)–(C.129), we prove the existence of a VLSF code that satisfies (D.26) for the DM-MAC with $L$ decoding times and error probability $\frac{1}{\sqrt{N \log N}}$.

Finally, invoking (D.26) with $L$ replaced by $L-1$ and the sub-optimal SHT strategy in the proof sketch of Theorem 4.3.1 with $\epsilon'_N = \frac{1}{\sqrt{N' \log N'}}$, we complete the proof of Theorem 5.3.1.

### D.2.1 Proof of (5.18)

The proof of (5.18) and the proof of Theorem 5.3.1 differ in several ways. (5.18),

1. In (5.18), we choose $cN+1$ decoding times as $n_i = i-1$ for $i = 1, \dots, cN+1$ for a sufficiently large constant $c > 1$, while in the proof of Theorem 5.3.1, $L = O(1)$ decoding times where the gaps between consecutive decoding times are not the same.

2. We set the parameter $\gamma$ differently than (D.27) and (D.28). Specifically, we set

$$\gamma = NI_K - a \tag{D.34}$$

$$= \sum_{k=1}^{K} \log M_k + \log N + b, \tag{D.35}$$

   where $a$ is an upper bound on the information density $\imath_K(X_{[K]}; Y_K)$, and $b$ is a positive constant to be determined later. Since the number of decoding times $L$ grows linearly with $N$ and $c > 1$, applying the Chernoff bound gives

$$(5.12) + (5.14) + (5.15) \leq \exp\{-NE\} \tag{D.36}$$

   for some $E > 0$ and $N$ large enough. Hence, the error probability $\epsilon$ in Theorem 5.3.2 is bounded by $\frac{\exp\{-b\}}{N} + \exp\{-NE\}$, which can be further bounded by $\frac{1}{N}$ by appropriately choosing the constant $b$.

3. We bound the average decoding time $\mathbb{E}\left[\tau^*\right]$ as

$$\mathbb{E}\left[\tau^*\right] \leq \frac{\gamma + a}{I_K} = N \tag{D.37}$$

   using Doob's optional stopping theorem as used in[18, eq. (106)-(107)] while $\mathbb{E}\left[\tau^*\right]$ in the proof of Theorem 5.3.1 is bounded by bounding the tail probability of information density.

The steps above show the achievability of an $(N, cN, M_{[K]}, 1/N)$ code with

$$\sum_{k=1}^{K} \log M_k = NI_K - \log N + O(1). \tag{D.38}$$

4. Lastly, we invoke the sub-optimal SHT strategy from the proof sketch of Theorem 4.3.1 with $\epsilon'_N = \frac{1}{N'}$, which is used with $\epsilon'_N = \frac{1}{\sqrt{N' \log N'}}$,

*Appendix E*

# APPENDIX FOR CHAPTER 6

## E.1 Proofs of Lemmas 6.2.1–6.2.3

We first state and prove Lemma E.1.1, which we then use to prove Lemmas 6.2.2, 6.2.1, and 6.2.3 (in that order).

**Lemma E.1.1.** *Let $X_1, X_2, \ldots, X_k$ be i.i.d., and let the interference (6.9), permutation-invariance (6.2), and reducibility (6.3) assumptions hold. Then $I_k(X_i; Y_k|X_{[i-1]})$ is strictly increasing in $i$, i.e., for all $i < j \leq k$,*

$$I_k(X_i; Y_k|X_{[i-1]}) < I_k(X_j; Y_k|X_{[j-1]}). \tag{E.1.1}$$

*Proof of Lemma E.1.1:* By permutation-invariance (6.9) and the i.i.d. distribution of $X_1, \ldots, X_k$, we have

$$I_k(X_i; Y_k|X_{[i-1]}) = I_k(X_j; Y_k|X_{[i-1]}). \tag{E.1.2}$$

Let $(U, V, T)$ be mutually independent random variables. Then $I(U; V) = I(U; T, V) = 0$. Since $I(U; T, Y) \leq I(U; T, V, Y)$, the chain rule implies that

$$I(U; Y|T) \leq I(U; Y|T, V). \tag{E.1.3}$$

Setting $U$ to $X_j$, $Y$ to $Y_k$, $T$ to $X_{[i-1]}$, and $V$ to $X_{[i:j-1]}$ in (E.1.3) and then applying (E.1.2) gives (E.1.1) with $<$ replaced by $\leq$. Equality in (E.1.3) is attained if and only if $U$ and $V$ are conditionally independent given $(Y, T)$. As a result, equality in our modified form of (E.1.1) occurs if and only if $X_j$ and $X_{[i:j-1]}$ are conditionally independent given $(Y_k, X_{[i-1]})$. We proceed to show that this is not possible using a proof by contradiction.

Assume that $X_j$ and $X_{[i:j-1]}$ are conditionally independent given $(Y_k, X_{[i-1]})$, i.e.,

$$P_{X_{[i:j]}|Y_k,X_{[i-1]}} = P_{X_{[i:j-1]}|Y_k,X_{[i-1]}} P_{X_j|Y_k,X_{[i-1]}}. \tag{E.1.4}$$

Set $X_{[i-1]} = 0^{i-1}$ and use Bayes' rule to show

$$P_{X_{[i:j]}|Y_k,X_{[i-1]}=0^{i-1}} = P_{X_{[j-(i-1)]}|Y_{k-(i-1)}} \tag{E.1.5}$$

$$P_{X_{[i:j-1]}|Y_k, X_{[i-1]}=0^{i-1}} = P_{X_{[2:j-(i-1)]}|Y_{k-(i-1)}} \tag{E.1.6}$$

$$P_{X_j|Y_k, X_{[i-1]}=0^{i-1}} = P_{X_1|Y_{k-(i-1)}} \tag{E.1.7}$$

due to reducibility (6.2), permutation-invariance (6.3), and the i.i.d. distribution of $X_1, \ldots, X_k$. Therefore, (E.1.4) implies that $X_1$ and $X_{[2:j-(i-1)]}$ are conditionally independent given $Y_{k-(i-1)}$, which is not possible by interference assumption (6.9). ■

*Proof of Lemma 6.2.2:* We wish to show that

$$\frac{1}{k} I_k(X_{[k]}; Y_k) < \frac{1}{s} I_k(X_{[s]}; Y_k | X_{[s+1:k]}). \tag{E.1.8}$$

By the chain rule for mutual information, the left-hand side of (E.1.8) equals the average of $k$ terms

$$\frac{1}{k} I_k(X_{[k]}; Y_k) = \frac{1}{k} \sum_{i=1}^{k} I_k(X_i; Y_k | X_{[i-1]}). \tag{E.1.9}$$

By permutation-invariance (6.2) and the chain rule, the right-hand side of (E.1.8) equals the average of the last $s$ of those $k$ terms

$$\frac{1}{s} I_k(X_{[s]}; Y_k | X_{[s+1:k]}) = \frac{1}{s} I_k(X_{[k-s+1:k]}; Y_k | X_{[k-s]}) \tag{E.1.10}$$

$$= \frac{1}{s} \sum_{i=k-s+1}^{k} I_k(X_i; Y_k | X_{[i-1]}). \tag{E.1.11}$$

Since the terms in these averages are strictly increasing in $i$ by Lemma E.1.1, we have the desired result. ■

*Proof of Lemma 6.2.1:* We wish to show that $\frac{1}{s} I_s > \frac{1}{k} I_k$. We proceed by representing $I_s$ in terms of $I_k$ as

$$\frac{1}{s} I_s = \frac{1}{s} I_k(X_{[s]}; Y_k | X_{[s+1:k]} = 0^{k-s}) \tag{E.1.12}$$

$$\geq \frac{1}{s} I_k(X_{[s]}; Y_k | X_{[s+1:k]}) \tag{E.1.13}$$

$$> \frac{1}{k} I_k, \tag{E.1.14}$$

where (E.1.12) follows from reducibility (6.3), (E.1.13) follows from friendliness (6.8), and (E.1.14) follows from Lemma 6.2.2. ■

*Proof of Lemma 6.2.3:* To derive the bound $\mathbb{E}[\imath_t(X_{[s]}; Y_k)] \leq I_k(X_{[s]}; Y_k) < I_t(X_{[s]}; Y_t)$, we write

$$\mathbb{E}[\imath_t(X_{[s]}; Y_k)] = \mathbb{E}\left[\log \frac{P_{Y_t|X_{[s]}}(Y_k|X_{[s]})}{P_{Y_t}(Y_k)}\right] \tag{E.1.15}$$

$$
\begin{aligned}
&= -D(P_{X_{[s]}}P_{Y_k|X_{[s]}}\|P_{X_{[s]}}P_{Y_t|X_{[s]}}) + D(P_{Y_k}\|P_{Y_t}) \\
&\quad +D(P_{X_{[s]}}P_{Y_k|X_{[s]}}\|P_{X_{[s]}}P_{Y_k}) && \text{(E.1.16)}\\
&= -D(P_{X_{[s]}}P_{Y_k|X_{[s]}}\|P_{X_{[s]}}P_{Y_t|X_{[s]}}) + D(P_{Y_k}\|P_{Y_t}) \\
&\quad +I_k(X_{[s]};Y_k) && \text{(E.1.17)}\\
&\leq I_k(X_{[s]};Y_k) && \text{(E.1.18)}\\
&= \sum_{i=1}^{s} I_k(X_i;Y_k|X_{[i-1]}) && \text{(E.1.19)}\\
&< \sum_{i=1}^{s} I_k(X_i;Y_k|X_{[i-1]}, X_{[s+1:s+k-t]}) && \text{(E.1.20)}\\
&= I_k(X_{[s]};Y_k|X_{[t+1:k]}) && \text{(E.1.21)}\\
&\leq I_k(X_{[s]};Y_k|X_{[t+1:k]}=0^{k-t}) && \text{(E.1.22)}\\
&= I_t(X_{[s]};Y_t), && \text{(E.1.23)}
\end{aligned}
$$

where (E.1.18) follows from data processing inequality of relative entropy (e.g., [57, Th. 2.2.5]), (E.1.19) follows from the chain rule, (E.1.20) follows from permutation-invariance (6.2) and Lemma E.1.1, (E.1.21) follows from permutation-invariance (6.2) and the chain rule, and (E.1.22) and (E.1.23) follow from friendliness (6.8) and reducibility (6.3), respectively.

■

## E.2 Proof of Lemma 6.3.1

To prove Lemma 6.3.1, we first derive the saddle point condition for the MAC.

**Theorem E.2.1** (Saddle point condition for the MAC)**.** *Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be convex set of distributions on alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, respectively. Suppose that there exists a product distribution $P_{X_1^*}P_{X_2^*}$ such that*

$$
\sup_{\substack{P_{X_1}P_{X_2} \\ P_{X_1}\in\mathcal{P}_1, P_{X_2}\in\mathcal{P}_2}} I_2(X_1,X_2;Y_2) = I_2(X_1^*,X_2^*;Y_2^*) = I_2^*, \tag{E.2.1}
$$

*where $P_{Y_2^*|X_1^*,X_2^*} = P_{Y_2|X_1,X_2}$. Then, for all $P_{X_1}\in\mathcal{P}_1$ and for all $Q_{Y_2}$, it holds that*

$$
\begin{aligned}
D(P_{X_1}P_{X_2^*}P_{Y_2|X_1,X_2}\|P_{X_1}P_{X_2^*}P_{Y_2^*}) &\leq I_2^* && \text{(E.2.2)}\\
&\leq D(P_{X_1^*}P_{X_2^*}P_{Y_2|X_1,X_2}\|P_{X_1^*}P_{X_2^*}Q_{Y_2}). && \text{(E.2.3)}
\end{aligned}
$$

*Proof of Lemma 6.3.1:* Lemma 6.3.1 follows by an application of Theorem E.2.1 to the setting where $\mathcal{P}_1$ includes the set of all distributions with a singleton on $\mathcal{X}_1$ having probability 1, i.e., $\{\delta_{x_1} : x_1 \in \mathcal{X}_1\} \subseteq \mathcal{P}_1$, and $I_2^* < \infty$. Particularizing $P_{X_1}$ in (E.2.2) to any $P_{X_1} = \delta_{x_1}$ with $x_1 \in \mathcal{X}_1$ yields

$$D(P_{X_2^*} P_{Y_2|X_1=x_1,X_2} \| P_{X_2^*} P_{Y_2^*}) \leq I_2^* \tag{E.2.4}$$

for all $x_1 \in \mathcal{X}_1$. Since the left-hand side of (E.2.4) is equal to the conditional expectation of $\imath_2(X_1^*, X_2^*; Y_2^*)$ given $X_1^* = x_1$, (6.27) follows with less than or equal to. The equality in (6.27) follows since otherwise (E.2.4) would give the contradiction $I_2(X_1^*, X_2^*; Y_2^*) < I_2^*$. ■

*Proof of Theorem E.2.1:* The proof of Theorem E.2.1 is similar to the proof of the saddle point condition for point-to-point channels in [57, Th. 4.4] and extends [57, Th. 4.4] to the MAC. Although the optimization in (E.2.1) is not convex in general [110], the optimization

$$\sup_{P_{X_1} \in \mathcal{P}_1} I_2(X_1, X_2^*; Y_2), \tag{E.2.5}$$

where $P_{X_1 X_2^* Y_2} = P_{X_1} P_{X_2^*} P_{Y_2|X_1,X_2}$ is convex.

Inequality (E.2.3) follows from the golden formula (e.g., [57, Th. 3.3])

$$\begin{aligned} I_2^* &= D(P_{X_1^*} P_{X_2^*} P_{Y_2|X_1,X_2} \| P_{X_1^*} P_{X_2^*} P_{Y_2^*}) \qquad &\text{(E.2.6)}\\ &= D(P_{X_1^*} P_{X_2^*} P_{Y_2|X_1,X_2} \| P_{X_1^*} P_{X_2^*} Q_{Y_2}) - D(P_{Y_2^*} \| Q_{Y_2}) \qquad &\text{(E.2.7)} \end{aligned}$$

and the nonnegativity of the relative entropy. Notice that for $I_2^* = \infty$, (E.2.2) is trivial. Assume that $I_2^* < \infty$. Fix any $P_{X_1} \in \mathcal{P}_1$. Let $\lambda \in (0, 1)$. Set

$$P_{X_{1\lambda}} = \lambda P_{X_1} + (1 - \lambda) P_{X_1^*} \in \mathcal{P}_1. \tag{E.2.8}$$

Let $\theta \sim \text{Bernoulli}(\lambda)$, so that $P_{X_{1\lambda}|\theta=0} = P_{X_1^*}$ and $P_{X_{1\lambda}|\theta=1} = P_{X_1}$, and let

$$P_{X_{1\lambda} X_2^* Y_{2\lambda}} = P_{X_{1\lambda}} P_{X_2^*} P_{Y_2|X_1,X_2}. \tag{E.2.9}$$

Then

$$\begin{aligned} I_2^* &\geq I_2(X_{1\lambda}, X_2^*; Y_{2\lambda}) \qquad &\text{(E.2.10)}\\ &= D(P_{X_{1\lambda}} P_{X_2^*} P_{Y_2|X_1,X_2} \| P_{X_{1\lambda}} P_{X_2^*} P_{Y_{2\lambda}}) \qquad &\text{(E.2.11)}\\ &= \lambda D(P_{X_1} P_{X_2^*} P_{Y_2|X_1,X_2} \| P_{X_1} P_{X_2^*} P_{Y_{2\lambda}}) \\ &\quad + (1 - \lambda) D(P_{X_1^*} P_{X_2^*} P_{Y_2|X_1,X_2} \| P_{X_1^*} P_{X_2^*} P_{Y_{2\lambda}}) \qquad &\text{(E.2.12)} \end{aligned}$$

$$\geq \lambda D(P_{X_1}P_{X_2^*}P_{Y_2|X_1,X_2}\|P_{X_1}P_{X_2^*}P_{Y_{2\lambda}}) \\ +(1-\lambda)I_2^*, \tag{E.2.13}$$

where (E.2.13) follows from (E.2.3). By subtracting $(1-\lambda)I_2^*$ from both sides of (E.2.13) and dividing by $\lambda$, we get

$$I_2^* \geq D(P_{X_1}P_{X_2^*}P_{Y_2|X_1,X_2}\|P_{X_1}P_{X_2^*}P_{Y_{2\lambda}}). \tag{E.2.14}$$

By taking $\liminf_{\lambda\to 0}$ in (E.2.14) and applying the lower semicontinuity of the relative entropy (e.g., [57, Th. 3.6]), (E.2.2) is proved. ■

Note that $(P_{X_1^*}, P_{X_2^*})$ does not have to be unique for Theorem E.2.1 and Lemma 6.3.1 to hold.

## E.3 Adder-erasure RAC

Here, we approximate the sum-capacity and dispersion of the adder-erasure RAC for a large number of transmitters ($k$).

**Theorem E.3.1.** *The optimal input distribution for the adder-erasure RAC defined in* (6.15) *is the Bernoulli(1/2) distribution at all encoders. That input distribution achieves the sum-rate capacity, and*

$$I_k = (1-\delta)\left(\frac{1}{2}\log\frac{\pi e k}{2} - \frac{\log e}{12k^2}\right) + O(k^{-3}) \tag{E.3.1}$$

$$V_k = (1-\delta)\Bigg[\frac{\delta}{4}\log^2\frac{\pi e k}{2} + \frac{\log^2 e}{2} - \frac{\log^2 e}{2k} \\ - \left(\frac{\log e}{2} + \frac{\delta\log\frac{\pi e k}{2}}{12}\right)\frac{\log e}{k^2}\Bigg] + O\left(\frac{\log k}{k^3}\right). \tag{E.3.2}$$

The calculation leading to Theorem E.3.1 is presented in Lemmas E.3.1–E.3.2, which rely on Stirling's approximation and the Taylor series expansion.

Consider a binomial random variable $X \sim \text{Binom}(n, 1/2)$. Lemma E.3.1, below, shows that the probability mass that this Binomial distribution puts at $k$ is well approximated by

$$\tilde{P}_X(k) \triangleq \frac{1}{\sqrt{\frac{\pi n}{2}}} e^{-\frac{(k-\frac{n}{2})^2}{\frac{n}{2}}}\left(1 + \frac{f(k)}{n} + \frac{g(k)}{n^2}\right), \tag{E.3.3}$$

where

$$f(x) \triangleq -\frac{1}{12}\frac{(2x-n)^4}{n^2} + \frac{1}{2}\frac{(2x-n)^2}{n} - \frac{1}{4} \tag{E.3.4}$$

$$\begin{aligned} g(x) \triangleq \frac{1}{288}\frac{(2x-n)^8}{n^4} - \frac{3}{40}\frac{(2x-n)^6}{n^3} + \frac{19}{48}\frac{(2x-n)^4}{n^2} \\ - \frac{11}{24}\frac{(2x-n)^2}{n} + \frac{1}{32}. \end{aligned} \tag{E.3.5}$$

Define the interval

$$\mathcal{K} \triangleq \left[\frac{n}{2} - \frac{A}{2}\sqrt{n\log n},\ \frac{n}{2} + \frac{A}{2}\sqrt{n\log n}\right] \tag{E.3.6}$$

for some constant $A > 0$.

**Lemma E.3.1.** *Let* $X \sim \mathrm{Binom}(n, 1/2)$*. Then for any* $k \in \mathcal{K}$*,*

$$P_X(k) = \binom{n}{k}2^{-n} = \tilde{P}_X(k)\left(1 + O\left(\frac{\log^6 n}{n^3}\right)\right). \tag{E.3.7}$$

*Proof of Lemma E.3.1:* We apply Stirling's approximation [143, eq. (6.1.37)]

$$n! = \sqrt{2\pi}n^{n+\frac{1}{2}}e^{-n}\left(1 + \frac{1}{12n} + \frac{1}{288n^2} + O(n^{-3})\right), \tag{E.3.8}$$

and a Taylor series expansion of $\binom{n}{k}$ around $x = 0$, where

$$k = \frac{n}{2} + \frac{x}{2}\sqrt{n\log n}, \tag{E.3.9}$$

to $P_X(k) = \binom{n}{k}2^{-n}$, to derive (E.3.7). ■

Let $V(X)$

$$V(X) = \mathrm{Var}\left[\log\frac{1}{P_X(X)}\right]. \tag{E.3.10}$$

denote the varentropy of $X$.

**Lemma E.3.2** (Entropy and varentropy of Binom $(n, 1/2)$)**.** *For* $X \sim$ Binom $(n, 1/2)$*,*

$$H(X) = \frac{1}{2}\log\frac{\pi e n}{2} - \frac{\log e}{12n^2} + O(n^{-3}) \tag{E.3.11}$$

$$V(X) = \frac{\log^2 e}{2} - \frac{\log^2 e}{2n} - \frac{\log^2 e}{2n^2} + O(n^{-3}). \tag{E.3.12}$$

*Proof of Lemma E.3.2:* Let $\tilde{T}(k)$ denote the first 3 terms of the Taylor series expansion of $\log\frac{1}{\tilde{P}_X(k)}$ around $\frac{n}{2}$ evaluated at $k$, giving

$$\tilde{T}(k) \triangleq \frac{1}{2}\log\frac{\pi n}{2} + \log e\Bigg(\frac{(k-\frac{n}{2})^2}{\frac{n}{2}}$$

$$- \frac{f(k)}{n} + \frac{-g(k) + \frac{f^2(k)}{2}}{n^2}\Bigg). \tag{E.3.13}$$

Recall the definition of interval $\mathcal{K}$ from (E.3.6). Then we can write the entropy $H(X)$ as

$$\begin{aligned} H(X) &= \sum_{k=0}^{n} \frac{\binom{n}{k}}{2^n} \log \left( \frac{2^n}{\binom{n}{k}} \right) & \text{(E.3.14)} \\ &= \mathbb{E}\left[\tilde{T}(X)\right] \\ &\quad + \mathbb{E}\left[\left(\log \frac{1}{P_X(X)} - \tilde{T}(X)\right) 1\{X \in \mathcal{K}\}\right] \\ &\quad + \mathbb{E}\left[\left(\log \frac{1}{P_X(X)} - \tilde{T}(X)\right) 1\{X \notin \mathcal{K}\}\right]. & \text{(E.3.15)} \end{aligned}$$

Using the moments of Binom $(n, 1/2)$ (e.g., [143, eq. (26.1.20)]), the first term in (E.3.15) is

$$\mathbb{E}\left[\tilde{T}(X)\right] = \frac{1}{2} \log \frac{\pi e n}{2} - \frac{\log e}{12n^2}. \tag{E.3.16}$$

By Lemma E.3.1, the second term in (E.3.15) is

$$\mathbb{E}\left[\left(\log \frac{1}{P_X(X)} - \tilde{T}(X)\right) 1\{X \in \mathcal{K}\}\right] = O\left(\frac{\log^6 n}{n^3}\right). \tag{E.3.17}$$

By Hoeffding's inequality,

$$\mathbb{P}\left[X \notin \mathcal{K}\right] \leq 2n^{-\frac{A^2 \log e}{2}}, \tag{E.3.18}$$

where $A$ is the constant in (E.3.6). Since the minimum of $P_X(k)$ over $k$ is achieved at $k = n$, using (E.3.18), we get

$$\mathbb{E}\left[\log \frac{1}{P_X(X)} 1\{X \notin \mathcal{K}\}\right] = O\left(\frac{\log^6 n}{n^3}\right) \tag{E.3.19}$$

for $A \geq \frac{3}{\sqrt{\log e}}$. Similarly, by taking the derivative of $\tilde{T}(k)$, one can show that $\tilde{T}(k) \leq \tilde{T}(n) \leq n$ for all $k \in [0, n]$, which gives

$$\mathbb{E}\left[\tilde{T}(X) 1\{X \notin \mathcal{K}\}\right] = O\left(\frac{\log^6 n}{n^3}\right). \tag{E.3.20}$$

Combining (E.3.15)–(E.3.17), (E.3.19)–(E.3.20) gives

$$H(X) = \frac{1}{2} \log \frac{\pi e n}{2} - \frac{\log e}{12n^2} + O\left(\frac{\log^6 n}{n^3}\right). \tag{E.3.21}$$

Via an argument similar to (E.3.19) and (E.3.20), we can show that for $A \geq \frac{4}{\sqrt{\log e}}$, the contribution of $k \notin \mathcal{K}$ to the varentropy is $O\left(\frac{\log^6 n}{n^3}\right)$. Therefore, using the moments of $\text{Binom}(n, 1/2)$ and Lemma E.3.1, we can approximate the varentropy $V(X)$ as

$$\begin{aligned} V(X) &= \mathbb{E}\left[\log^2 \frac{1}{P_X(X)}\right] - (H(X))^2 && \text{(E.3.22)} \\ &= \mathbb{E}\left[(\tilde{T}(X))^2\right] - (H(X))^2 + O\left(\frac{\log^6 n}{n^3}\right) && \text{(E.3.23)} \\ &= \log^2 e \left(\frac{1}{2} - \frac{1}{2n} - \frac{1}{2n^2}\right) + O\left(\frac{\log^6 n}{n^3}\right). && \text{(E.3.24)} \end{aligned}$$

The above analyses use the first 3 terms of the Stirling series (E.3.8) to obtain the remainder $O\left(\frac{\log^6 n}{n^3}\right)$. Applying the same analyses with 4 terms of the Stirling series improves the remainder to $O(n^{-3})$, as claimed in (E.3.11) and (E.3.12) in the statement of Lemma E.3.2. ■

We are now equipped to prove Theorem E.3.1.

*Proof of Theorem E.3.1:* Define

$$E \triangleq 1\{Y = \mathsf{e}\}. \qquad \text{(E.3.25)}$$

By the chain rule for entropy, we have for the adder-erasure RAC

$$\begin{aligned} I_k(X_{[k]}; Y_k) &= H(Y_k) - H(Y_k|X_{[k]}) && \text{(E.3.26)} \\ &= H(Y_k, E) - H(E) && \text{(E.3.27)} \\ &= H(Y_k|E) && \text{(E.3.28)} \\ &= (1-\delta)H(Y_k|E=0). && \text{(E.3.29)} \end{aligned}$$

Given the independent inputs $X_i \sim \text{Bernoulli}(p_i)$ for $i \in [k]$, $H(Y_k|E=0)$ is equal to the entropy of the sum of $k$ independent Bernoulli random variables with parameters $(p_1, \ldots, p_k)$, which is maximized when $p_i = 1/2$ for all $i$ [149]. Therefore, for any $\delta \in [0,1]$, the equiprobable input distribution at all encoders, $X_i^* \sim \text{Bernoulli}(1/2)$, maximizes the mutual information $I_k(X_{[k]}; Y_k)$ for all $k$. Let $(X_{[k]}^* Y_k^*) \sim P_{X_{[k]}^*} P_{Y_k|X_{[k]}}$. Then

$$I_k(X_{[k]}^*; Y_k^*) = (1-\delta)H(Z), \qquad \text{(E.3.30)}$$

where $Z \sim \text{Binom}(k, 1/2)$, and (E.3.1) follows from Lemma E.3.2. Furthermore,

$$\imath_k(X^*_{[k]}; Y^*_k) = \begin{cases} 0 & \text{w.p. } \delta \\ \log \frac{2^k}{\binom{k}{i}} & \text{w.p. } (1-\delta)\frac{\binom{k}{i}}{2^k}, \quad 0 \leq i \leq k, \end{cases} \tag{E.3.31}$$

which gives

$$V_k = \text{Var}\left[\imath_k(X^*_{[k]}; Y^*_k)\right] = (1-\delta)\left[V(Z) + \delta(H(Z))^2\right], \tag{E.3.32}$$

and (E.3.2) follows from Lemma E.3.2. ■

## E.4 Bound on the Cardinality $|\mathcal{U}|$

While the analysis in Section 6.4.2 employs common randomness $U$ with $|\mathcal{U}| = |\mathcal{X}|^{Mn_K}$, [18, Th. 19] shows that $|\mathcal{U}| \leq K+2$ suffices to achieve the optimal performance. Theorem E.4.1, stated next, improves the cardinality bound on $|\mathcal{U}|$ from $K+2$ [18, Th. 19] to $K+1$ by using the connectedness of the set of achievable error vectors defined in (E.4.1).

**Theorem E.4.1.** *If an $(M, \{(n_k, \epsilon_k)\}_{k=0}^K)$ RAC code exists, then there exists an $(M, \{(n_k, \epsilon_k)\}_{k=0}^K)$ RAC code with $|\mathcal{U}| \leq K+1$.*

*Proof of Theorem E.4.1:* For fixed $M, n_0, \ldots, n_K$, let $G_u$ denote the set of achievable error vectors compatible with message size $M$, blocklengths $n_0, \ldots, n_K$, and cardinality $|\mathcal{U}| \leq u$; that is,

$$\begin{aligned} G_u = \{(\epsilon'_0, \ldots, \epsilon'_K) : \exists (M, \{(n_k, \epsilon'_k)\}_{k=0}^K) \text{ code with} \\ |\mathcal{U}| \leq u\}. \end{aligned} \tag{E.4.1}$$

Let $G$ denote the set of achievable error vectors compatible with message size $M$ and blocklengths $n_0, \ldots, n_K$; that is,

$$G = \{(\epsilon'_0, \ldots, \epsilon'_K) : \exists (M, \{(n_k, \epsilon'_k)\}_{k=0}^K) \text{ code}\}. \tag{E.4.2}$$

As observed in [18, Proof of Th. 19], $G = G_{|\mathcal{X}|^{Mn_K}}$ is the convex hull of $G_1$. Indeed, every vector $(\epsilon'_0, \ldots, \epsilon'_K)$ in $G$ is a convex combination of vectors in $G_1$, and the coefficients of the convex combination are determined by the distribution of the common randomness random variable $U$.

Furthermore, $G_1$ is a connected set. To see this, take any $\boldsymbol{\epsilon}_1, \boldsymbol{\epsilon}_2 \in G_1$. For any $\boldsymbol{\epsilon}' \geq \boldsymbol{\epsilon}$ with $\boldsymbol{\epsilon} \in G_1$, the line segments $L_i = \{\lambda \boldsymbol{\epsilon}_i + (1-\lambda)\mathbf{1} \colon \lambda \in [0,1]\}$, $i = 1, 2$, also belong to $G_1$, and the path $L_1 \cup L_2$ connects $\boldsymbol{\epsilon}_1$ and $\boldsymbol{\epsilon}_2$. Therefore, $G_1$ is a connected set.

Since $G = \mathrm{conv}(G_1) \subset \mathbb{R}^{K+1}$, and $G_1$ is a connected set, by Fenchel-Eggleston-Carathéodory's theorem [150, Th. 18 (ii)], $G = G_{K+1}$ holds. Therefore, $(\epsilon_0, \dots, \epsilon_K) \in G$ implies that $(\epsilon_0, \dots, \epsilon_K) \in G_{K+1}$. ■

## E.5 Composite Hypothesis Testing

We begin with a lemma that is used in the proof of Theorem 6.5.3. See Fig. E.1 for an illustration of Lemma E.5.1.

**Lemma E.5.1.** *Let $f\colon \mathbb{R}^d \to \mathbb{R}$ be a continuous function that satisfies coordinate-wise partial ordering, i.e., $f(\mathbf{x}) \leq f(\mathbf{y})$ for any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ with $\mathbf{x} \leq \mathbf{y}$. Then for any $a$ in the image of $f$ (denoted $a \in \mathrm{Im} f$), it holds that*

$$b^\star = \min_{\mathbf{b} \in \mathbb{R}^d : f(\mathbf{b}) \geq a} \max_{1 \leq j \leq d} b_j = \min_{x \in \mathbb{R} : f(x\mathbf{1}) \geq a} x. \tag{E.5.1}$$

*Proof:* Since $a \in \mathrm{Im} f$, there exists some $\mathbf{b} \in \mathbb{R}^d$ such that $f(\mathbf{b}) = a$. Denote by $b_{\min}$ and $b_{\max}$ the minimum and maximum components of $\mathbf{b}$, respectively. Since $f$ is nondecreasing,

$$f(b_{\min}\mathbf{1}) \leq a = f(\mathbf{b}) \leq f(b_{\max}\mathbf{1}). \tag{E.5.2}$$

Therefore, since the function mapping $b$ to $f(b\mathbf{1})$ is continuous and nondecreasing, by the intermediate value theorem there exists some $b \leq b_{\max}$ such that $f(b\mathbf{1}) = a$. Equation (E.5.1) follows. ■

Let $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V})$. Define the multidimensional counterpart of the function $Q^{-1}(\cdot)$ as

$$\mathcal{Q}_{\mathrm{inv}}(\mathsf{V}, \epsilon) \triangleq \left\{ \mathbf{z} \in \mathbb{R}^K : \mathbb{P}\left[\mathbf{Z} \leq \mathbf{z}\right] \geq 1 - \epsilon \right\}. \tag{E.5.3}$$

*Proof of Theorem 6.5.3:* For any $\epsilon_0 \in (0, 1)$, consider all composite hypothesis tests in the form given in (6.116) that achieve type-I error no greater than $\epsilon_0$. Let

$$\mathcal{E}_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K) \triangleq \Big\{ (e_1, \dots, e_K) : \exists \text{ a (randomized) test}$$

such that

$$\mathbb{P}\left[\text{Decide } H_1 | H_0\right] \leq \epsilon_0,$$

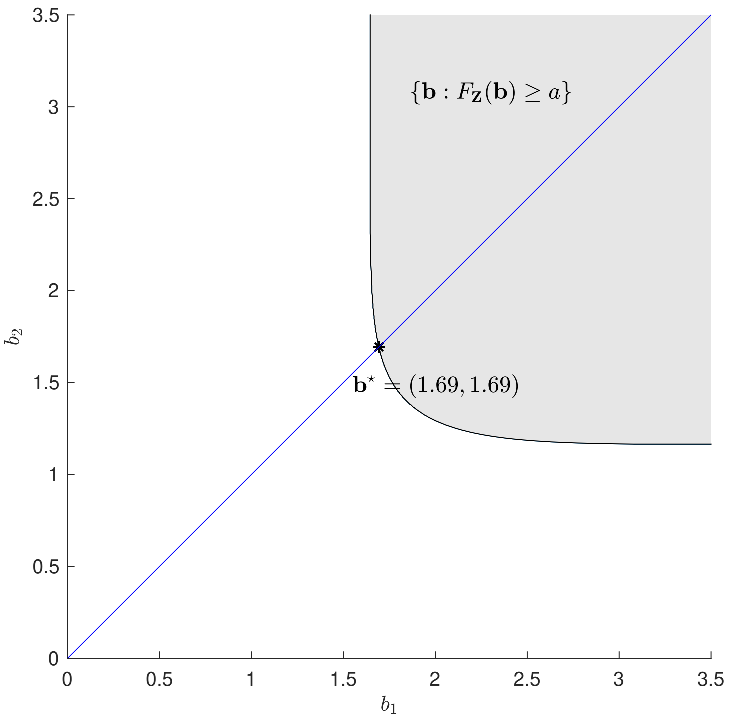


Figure E.1: An example to illustrate Lemma E.5.1. Here $f(\mathbf{b}) = F_{\mathbf{Z}}(\mathbf{b})$ is the CDF of $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V})$, where $\mathsf{V} = \left[\begin{smallmatrix} 1 & 0.4 \\ 0.4 & 0.5 \end{smallmatrix}\right]$. The shaded region illustrates the set $\{\mathbf{b} \in \mathbb{R}^2 : f(\mathbf{b}) \geq a = 0.95\}$. Lemma E.5.1 shows that the minimax on this set is achieved at a point described by a scalar multiple of $\mathbf{1}$. For this example, the optimizer is $\mathbf{b}^\star = (1.69, 1.69)$.

$$\mathbb{P}\left[\text{Decide } H_0 | H_1\right] = e_k, 1 \leq k \leq K \Big\} \tag{E.5.4}$$

denote the set of type-II errors achievable by these tests. Huang and Moulin [123, Th. 1][1] show that the asymptotic form of the error region defined in (E.5.4) is given by

$$\begin{aligned} &\mathcal{E}_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K) \\ &= \exp\left\{ -n\mathbf{D} + \sqrt{n}\mathcal{Q}_{\text{inv}}(\mathsf{V}, \epsilon_0) - \frac{1}{2}\log n\mathbf{1} + O(1)\mathbf{1} \right\}. \end{aligned} \tag{E.5.5}$$

[1] In the converse part of the proof of [123, Th. 1], Huang and Moulin show that for any LLR test (6.139) with threshold vector $\boldsymbol{\tau}$ such that the type-I error is bounded by $\epsilon_0$, it holds that $\boldsymbol{\tau} = n\mathbf{D} - \sqrt{n}\mathbf{b} + O(1)\mathbf{1}$ for some $\mathbf{b} \in \mathcal{Q}_{\text{inv}}(\mathsf{V}, \epsilon_0)$. Then, it is assumed that $\mathbf{b} = O(1)\mathbf{1}$, and [123, Lemma 2] is applied. However, according to the definition of $\mathcal{Q}_{\text{inv}}(\mathsf{V}, \epsilon_0)$ in (E.5.3), $\mathbf{b}$ can have coordinates growing with $n$, which violates this assumption. In [131, Th. 11], Chen *et al.* confirm that the asymptotic expansion in (E.5.5) holds. They prove the converse part of the expansion (E.5.5) by evaluating a converse bound that they derive in [131, Lemma 9] for the composite hypothesis testing.

By the definition of the minimax error (6.138) and the characterization of the achievable error region asymptotics in (E.5.5), we have

$$\beta_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K)$$
$$= \min_{\mathbf{z} \in \exp\{-n\mathbf{D} + \sqrt{n}\mathcal{Q}_{\text{inv}}(\mathsf{V}, \epsilon_0) - \frac{1}{2}\log n \mathbf{1} + O(1)\mathbf{1}\}} \max_{1 \leq k \leq K} z_k. \tag{E.5.6}$$

Applying Lemma E.5.1 with $f(\mathbf{z}) = \mathbb{P}[-n\mathbf{D} + \sqrt{n}\mathbf{Z} \leq \mathbf{z}]$ and $a = 1-\epsilon_0$, where $\mathbf{Z} \sim \mathcal{N}(\mathbf{0}, \mathsf{V})$, we obtain

$$\beta_{\epsilon_0}(P_{Y_0}, \{P_{Y_k}\}_{k=1}^K)$$
$$= \min_{z \in \mathbb{R}: f(z\mathbf{1}) \geq 1-\epsilon_0} \exp\left\{z - \frac{1}{2}\log n + O(1)\right\}. \tag{E.5.7}$$

Since $f(z\mathbf{1})$ is nondecreasing and continuous in $z$,

$$f(z^\star \mathbf{1}) = 1 - \epsilon_0 \tag{E.5.8}$$

holds, where $z^\star$ is the argument that achieves the minimum on the right-hand side of (E.5.7). Recall the definitions of $D_{\text{min}}$ and $\mathcal{I}_{\text{min}}$ from (6.141)–(6.142). By Chernoff's bound on $f(\mathbf{z})$, for any $z = nE + o(n)$ with $E > -D_{\text{min}}$, we have $f(z\mathbf{1}) = 1 - o(1)$. Similarly, for $E < -D_{\text{min}}$, we have $f(z\mathbf{1}) = o(1)$, giving

$$z^\star = -nD_{\text{min}} + o(n). \tag{E.5.9}$$

We proceed to show that the minimum on the right-hand side of (E.5.7) is achieved at

$$z^\star = -nD_{\text{min}} + \sqrt{n}b + O\left(1\right), \tag{E.5.10}$$

where $b$ is defined in (6.145). Here

$$\mathbb{P}\left[-nD_{\text{min}}\mathbf{1} + \sqrt{n}\mathbf{Z}_{\mathcal{I}_{\text{min}}} \leq z^\star\mathbf{1}\right]$$
$$= \mathbb{P}\left[-n\mathbf{D} + \sqrt{n}\mathbf{Z} \leq z^\star\mathbf{1}\right]$$
$$+ \mathbb{P}\Big[\{-nD_{\text{min}}\mathbf{1} + \sqrt{n}\mathbf{Z}_{\mathcal{I}_{\text{min}}} \leq z^\star\mathbf{1}\} \bigcap \{-n\mathbf{D}_{\mathcal{I}^c_{\text{min}}} + \sqrt{n}\mathbf{Z}_{\mathcal{I}^c_{\text{min}}} \not\leq z^\star\mathbf{1}\}\Big] \tag{E.5.11}$$
$$= 1 - \epsilon_0 + O\left(\frac{1}{n}\right), \tag{E.5.12}$$

where (E.5.12) follows from (E.5.8), (E.5.9), and the union bound and Chebyshev's inequality on $\mathbb{P}\left[-n\mathbf{D}_{\mathcal{I}^c_{\text{min}}} + \mathbf{Z}_{\mathcal{I}^c_{\text{min}}} \not\leq z^\star\mathbf{1}\right]$. By the Taylor series expansion of $Q_{\text{inv}}(\mathsf{V}, \cdot)$, we conclude that

$$\mathbb{P}\left[\mathbf{Z}_{\mathcal{I}_{\text{min}}} \leq \frac{1}{\sqrt{n}}(z^\star + nD_{\text{min}})\mathbf{1} + O\left(\frac{1}{n}\right)\right] = 1 - \epsilon_0, \tag{E.5.13}$$

which implies (E.5.10). Combining (E.5.7) and (E.5.10) completes the proof.

■

### E.5.1 Proof of Theorem 6.6.1

The main difference between the proofs of Theorem 6.6.1 and Theorem 5.3.1 is that for the DM-RAC, we employ multiple hypothesis testing to estimate the number of active transmitters at time $n_0$ that is smaller than or equal to any of the decoding times. If the test decides that the number of active transmitters is $\hat{k} = 0$, then the decoder declares no active transmitters at time $n_0$ and stops the transmission at that time. If the estimated number of active transmitters is $\hat{k} \neq 0$, then the decoder decides to decode at one of the available times $n_{k,1}$, $\dots$, $n_{k,L}$ using the MAC decoder with $k$ transmitters.

#### Encoding and decoding

**Encoding**: As in the DM-PPC and DM-MAC cases, the codewords are generated i.i.d. from the distribution $P_X^{n_{K,L}}$.

**Decoding**: The decoder combines a $(K+1)$-ary hypothesis test and the threshold test that is used for the DM-MAC.

*Multiple hypothesis test*: Given distributions $P_{Y_k}$, $k \in \{0, \dots, K\}$ where $\mathcal{Y}_K$ is the common alphabet, we test the hypotheses

$$H_k\colon Y^{n_0} \sim P_{Y_k}^{n_0}, \quad k \in \{0, \dots, K\}. \tag{E.5.14}$$

The error probability constraints of our test are

$$\mathbb{P}\left[\text{Decide } H_s \text{ where } s \neq 0 | H_0\right] \leq \epsilon_0 \tag{E.5.15}$$

$$\mathbb{P}\left[\text{Decide } H_s \text{ where } s \neq k | H_k\right] \leq \exp\{-n_0 E + o(n_0)\} \tag{E.5.16}$$

for $k \in [K]$, where $E > 0$ is a constant.

Due to the asymmetry in (E.5.15)–(E.5.16), we employ a composite hypothesis testing to decide whether $H_0$ is true; that is, the test declares $H_0$ if

$$\ln \frac{P_{Y_0}^{n_0}(y^{n_0})}{P_{Y_s}^{n_0}(y^{n_0})} \geq \tau_s \tag{E.5.17}$$

for all $s \in [K]$, where the threshold values $\tau_s$, $s \in [K]$, are determined according to (E.5.15). If the condition in (E.5.17) is not satisfied, then the test applies the maximum likelihood decoding rule, i.e., it outputs $H_s$, where

$$s = \arg\max_{s \in [K]} P_{Y_s}^{n_0}(y^{n_0}). \tag{E.5.18}$$

From the asymptotics of the composite hypothesis testing in Theorem 6.5.3, the maximum type-II error of the composite hypothesis test is bounded as

$$\begin{aligned} &\max_{k \in [K]} \mathbb{P}\left[\text{Decide } H_0 | H_k\right] \\ &\qquad \leq \exp\left\{-n_0 \min_{k \in [K]} D(P_{Y_0} \| P_{Y_k}) + O(\sqrt{n_0})\right\}. \end{aligned} \tag{E.5.19}$$

If $P_{Y_0}$ is not absolutely continuous with respect to $P_{Y_k}$, (E.5.19) still remains valid with $D(P_{Y_0} \| P_{Y_k}) = \infty$ since we can achieve arbitrarily large type-II error probability exponent in that case (see [5, Lemmas 57-58].

From [151], the maximum likelihood test yields

$$\max_{(k,s) \in [K]^2} \mathbb{P}\left[\text{Decide } H_s | H_k\right] \leq \exp\{-nE_C + o(n)\}, \tag{E.5.20}$$

where

$$E_C = \min_{k,s} \min_{\lambda \in (0,1)} \ln \sum_{y \in \mathcal{Y}_K} P_{Y_k}(y)^{1-\lambda} P_{Y_s}(y)^{\lambda} \tag{E.5.21}$$

is the minimum Chernoff distance between the pairs $(P_{Y_k}, P_{Y_s})$, $k \neq s \in [K]$. Combining (E.5.19) and (E.5.21), the conditions in (E.5.15)–(E.5.16) are satisfied with

$$E = \min\left\{\min_{k \in [K]} D(P_{Y_0} \| P_{Y_k}), E_C\right\} > 0. \tag{E.5.22}$$

If the hypothesis test declares the hypothesis $H_{\hat{k}}$, $\hat{k} \neq 0$, then the receiver decides to decode $\hat{k}$ messages at one of the decoding times in $\{n_{\hat{k},1}, \ldots, n_{\hat{k},L}\}$ using the VLSF code in Section D for the $\hat{k}$-MAC, where $n_{\hat{k},1}$ is set to $n_0$.

### E.5.2 Error analysis

In this section, we bound the probability of error for the random access code in Definition 6.6.1.

*No active transmitters*: For $k = 0$, the only error event is that the composite hypothesis test at time $n_0$ does not declare $H_0$ given that $H_0$ is true. By (E.5.15), the probability of this event is bounded by $\epsilon_0$.

$k \geq 1$ *active transmitters*: When there is at least one active transmitter, the encoding function and decoding rule yield an error if and only if at least one of the following events occurs:

- $\mathcal{E}_{\text{number}}$: The number of active transmitters is estimated incorrectly at time $n_0$, i.e., $\hat{k} \neq k$, which results in decoding of $\hat{k}$ messages instead of $k$ messages.
- $\mathcal{E}_{\text{message}}$: A list of messages $m'_{[k]} \neq m_{[k]}$ is decoded at one of the times in $\{n_{k,1}, \ldots, n_{k,L}\}$.

In the following discussion, we bound the probability of these events separately, and apply the union bound to combine them.

Since the encoders are identical, treating the event $\mathcal{E}_{\text{rep}} = \{W_i = W_j \text{ for some } i \neq j\}$ that at least one message among transmitted messages is repeated as an error simplifies the analysis.

By the union bound, we have

$$\mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] \leq \frac{k(k-1)}{2M}. \tag{E.5.23}$$

Applying the union bound, we bound the error probability as

$$\begin{aligned}\epsilon_k &\leq \mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{rep}}^{\text{c}}\right] \mathbb{P}\left[\mathcal{E}_{\text{number}} \cup \mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}}\right] \\ &\leq \mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{number}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}} \cap \mathcal{E}_{\text{number}}^{\text{c}}\right]. \end{aligned} \tag{E.5.24}$$

By (E.5.16), the probability $\mathbb{P}\left[\mathcal{E}_{\text{number}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}}\right]$ is bounded as

$$\mathbb{P}\left[\mathcal{E}_{\text{number}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}}\right] \leq \exp\{-n_0 E + o(n_0)\}. \tag{E.5.25}$$

Since the number of active transmitters $k$ is not available at the decoder at time 0, we here slightly modify the sub-optimal SHT strategy from the proof sketch of Theorem 4.3.1. We set the smallest decoding time $n_{j,1}$ to $n_0 \neq 0$ for all $j \in [K]$. Given that $\hat{k}$ is the estimate of the true number of active transmitters $k$, we employ the sub-optimal SHT strategy with the triple $(N', \epsilon, \epsilon'_N)$ replaced by $(N'_{\hat{k}}, \epsilon_{\hat{k}}, \epsilon_{N'_{\hat{k}}})$.

Let $\mathcal{E}_{\text{stop}}$ denote the event that the decoder chooses to stop at time $n_{k,1} = n_0$ to decode an arbitrary message vector. We further bound $\mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}} \cap \mathcal{E}_{\text{number}}^{\text{c}}\right]$ as

$$\mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}} \cap \mathcal{E}_{\text{number}}^{\text{c}}\right] \leq \mathbb{P}\left[\mathcal{E}_{\text{stop}} \middle| \mathcal{E}_{\text{rep}}^{\text{c}} \cap \mathcal{E}_{\text{number}}^{\text{c}}\right]$$

$$+\,\mathbb{P}\left[\mathcal{E}_{\text{stop}}^{\text{c}}\middle|\mathcal{E}_{\text{rep}}^{\text{c}}\cap\mathcal{E}_{\text{number}}^{\text{c}}\right]\mathbb{P}\left[\mathcal{E}_{\text{message}}\middle|\mathcal{E}_{\text{rep}}^{\text{c}}\cap\mathcal{E}_{\text{number}}^{\text{c}}\cap\mathcal{E}_{\text{stop}}^{\text{c}}\right]. \tag{E.5.26}$$

Extending Theorem 5.3.2 by letting the RAC decoder at time $n_{k,\ell}$ decode a list of $k$ messages from $[M]$, we get

$$\mathbb{P}\left[\mathcal{E}_{\text{message}}\middle|\mathcal{E}_{\text{rep}}^{\text{c}}\cap\mathcal{E}_{\text{number}}^{\text{c}}\cap\mathcal{E}_{\text{stop}}^{\text{c}}\right] \tag{E.5.27}$$

$$\leq \mathbb{P}\left[\imath_k(X_{[k]}^{n_{k,L}};Y_k^{n_{k,L}})<\gamma_k\right] \tag{E.5.28}$$

$$+\binom{M-k}{k}\exp\{-\gamma_k\} \tag{E.5.29}$$

$$+\sum_{\ell=2}^{L}\sum_{\mathcal{A}\in\mathcal{P}([k])}$$

$$\mathbb{P}\left[\imath_k(X_{\mathcal{A}}^{n_{k,\ell}};Y_k^{n_{k,\ell}})>N_k'I_k(X_{\mathcal{A}};Y_k)+N_k'\lambda^{(k,\mathcal{A})}\right] \tag{E.5.30}$$

$$+\sum_{\mathcal{A}\in\mathcal{P}([k])}\binom{M-k}{|\mathcal{A}|}$$

$$\exp\{-\gamma+N_k'I_k(X_{\mathcal{A}};Y_k)+N_k\lambda^{(k,\mathcal{A})}\}, \tag{E.5.31}$$

where $N_k'$ is the average decoding time given $\mathcal{E}_{\text{stop}}^{c}$, and $\gamma_k$ and $\lambda^{(k,\mathcal{A})}$ are constants that satisfy the equations

$$\gamma_k = n_{k,\ell}I_k-\sqrt{n_{k,\ell}\ln_{(L-\ell+1)}(n_{k,\ell})V_k} \tag{E.5.32}$$

$$= k\ln M+\ln N_k'+O(1) \tag{E.5.33}$$

for all $\ell\in\{2,\dots,L\}$, and

$$\lambda^{(k,\mathcal{A})}=\frac{N_k'I_k(X_{\mathcal{A}^c};Y_k|X_{\mathcal{A}})-|\mathcal{A}^c|\ln M}{2N_k'},\quad \mathcal{A}\in\mathcal{P}([k]). \tag{E.5.34}$$

The fact that $\lambda^{(k,\mathcal{A})}$'s are bounded below by a positive constant follows from (E.5.33), Lemma 6.2.1, and the symmetry assumptions on the RAC.

Following the analysis in Appendix D.2, we conclude that

$$k\ln M = N_k'I_k-\sqrt{N_k'\ln_{(L-1)}(N_k')V_k}$$

$$+\,O\left(\sqrt{\frac{N_k'V_k}{\ln_{(L-1)}(N_k')}}\right) \tag{E.5.35}$$

$$\mathbb{P}\left[\mathcal{E}_{\text{message}}\middle|\mathcal{E}_{\text{rep}}^{\text{c}}\cap\mathcal{E}_{\text{number}}^{\text{c}}\cap\mathcal{E}_{\text{stop}}^{\text{c}}\right]\leq\frac{1}{\sqrt{N_k'\ln N_k'}}. \tag{E.5.36}$$

Note that by (E.5.23) and (E.5.35), $\mathbb{P}\left[\mathcal{E}_{\text{rep}}\right]$ is bounded exponentially with $N_k$. A consequence of (E.5.32) and (E.5.35) is that

$$N'_k = n_{k,\ell}(1 + o(1)) \tag{E.5.37}$$

for all $\ell \geq 2$ and $k \in [K]$.

Note that from (E.5.35), the right-hand side of (E.5.23) is bounded by $\frac{1}{N'_k}$ for $N'_k$ large enough. We set the time $n_0$ so that the right-hand side of (E.5.25) is bounded by $\frac{1}{4\sqrt{N'_k \ln N'_k}}$ for all $k \in [K]$. This condition is satisfied if

$$n_0 \geq \frac{1}{2E} \ln N'_k + o(\ln N'_k). \tag{E.5.38}$$

The above arguments imply that

$$\mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{number}} \middle| \mathcal{E}^{\text{c}}_{\text{rep}}\right] \leq \frac{1}{2\sqrt{N'_k \ln N'_k}} \tag{E.5.39}$$

for $N'_k$ large enough. As in the DM-MAC case, we set

$$p \triangleq \mathbb{P}\left[\mathcal{E}_{\text{stop}} | \mathcal{E}^{\text{c}}_{\text{rep}} \cap \mathcal{E}^{\text{c}}_{\text{number}}\right] = \frac{\epsilon'_k - \frac{1}{\sqrt{N'_k \ln N'_k}}}{1 - \frac{1}{\sqrt{N'_k \ln N'_k}}} \tag{E.5.40}$$

where

$$\epsilon'_k = \epsilon_k - \frac{1}{2\sqrt{N'_k \ln N'_k}}. \tag{E.5.41}$$

Combining (E.5.24), (E.5.26), (E.5.36), and (E.5.39)–(E.5.40), the error probability of the RAC code is bounded by

$$\begin{aligned}
&\mathbb{P}\left[\mathcal{E}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{number}} \middle| \mathcal{E}^{\text{c}}_{\text{rep}}\right] + \mathbb{P}\left[\mathcal{E}_{\text{stop}} | \mathcal{E}^{\text{c}}_{\text{rep}} \cap \mathcal{E}^{\text{c}}_{\text{number}}\right] \\
&\quad + \mathbb{P}\left[\mathcal{E}^{\text{c}}_{\text{stop}} | \mathcal{E}^{\text{c}}_{\text{rep}} \cap \mathcal{E}^{\text{c}}_{\text{number}}\right] \mathbb{P}\left[\mathcal{E}_{\text{message}} \middle| \mathcal{E}^{\text{c}}_{\text{rep}} \cap \mathcal{E}^{\text{c}}_{\text{number}} \cap \mathcal{E}^{\text{c}}_{\text{stop}}\right] && \text{(E.5.42)} \\
&\quad \leq \frac{1}{2\sqrt{N'_k \ln N'_k}} + p + (1-p)\frac{1}{\sqrt{N'_k \ln N'_k}} && \text{(E.5.43)} \\
&\quad = \epsilon_k. && \text{(E.5.44)}
\end{aligned}$$

The average decoding time of the code is bounded as

$$\begin{aligned}
N_k \leq{}& \mathbb{E}\left[\tau^*_k | \mathcal{E}_{\text{number}} \cup \mathcal{E}_{\text{rep}}\right] \mathbb{P}\left[\mathcal{E}_{\text{number}} \cup \mathcal{E}_{\text{rep}}\right] \\
&+ \mathbb{E}\left[\tau^*_k | \mathcal{E}^{\text{c}}_{\text{number}} \cap \mathcal{E}^{\text{c}}_{\text{rep}}\right] \mathbb{P}\left[\mathcal{E}^{\text{c}}_{\text{number}} \cap \mathcal{E}^{\text{c}}_{\text{number}}\right] && \text{(E.5.45)}
\end{aligned}$$

$$\leq \frac{N_{K,L}}{2\sqrt{N'_k \ln N'_k}} + n_0 p + N'_k(1-p). \tag{E.5.46}$$

From (E.5.37), (E.5.40)–(E.5.41), we get

$$N'_k = \frac{N_k}{1-\epsilon'_k}\left(1 + O\left(\frac{1}{\sqrt{N_k \ln N_k}}\right)\right). \tag{E.5.47}$$

Plugging (E.5.47) in (E.5.35) completes the proof.

*Appendix F*

# APPENDIX FOR CHAPTER 7

## F.1 Proof of Corollary 7.2.1

In order to prove Corollary 7.2.1, we show that for any $M$ that satisfies the inequality (7.25), it holds that

$$(|\mathcal{S}|\log M \colon \mathcal{S}) \in \overline{\mathcal{P}}([K]) \in n\mathbf{C}(P\mathbf{1}) - \sqrt{n}Q_{\text{inv}}(\mathsf{V}(P\mathbf{1}), \epsilon) \\ + \frac{1}{2}\log n\mathbf{1} + O\left(1\right)\mathbf{1}. \tag{F.1.1}$$

Let $\mathbf{Z} = (Z(\mathcal{S}) : \mathcal{S} \in \overline{\mathcal{P}}([K])) \sim \mathcal{N}(\mathbf{0}, \mathsf{V}(P\mathbf{1}), \epsilon))$. Take $M$ such that the asymptotic expansion in (7.25) holds, implying that

$$\mathbb{P}\Big[Z([K]) > \sqrt{n}\left(C(KP) - \frac{K\log M}{n}\right) + \frac{1}{2}\frac{\log n}{\sqrt{n}} + O\left(\frac{1}{\sqrt{n}}\right)\Big] \leq \epsilon. \tag{F.1.2}$$

Consider any $\mathcal{S} \in \overline{\mathcal{P}}([K])$ with $|\mathcal{S}| < K$. Then

$$\mathbb{P}\Big[Z(\mathcal{S}) > \sqrt{n}\left(C(|\mathcal{S}|P) - \frac{|\mathcal{S}|\log M}{n}\right) + \frac{1}{2}\frac{\log n}{\sqrt{n}} + O\left(\frac{1}{\sqrt{n}}\right)\Big] \leq O\left(\frac{1}{n}\right), \tag{F.1.3}$$

which follows from Chebyshev's inequality since $C(sP) - \frac{s}{K}C(KP) > 0$ for $s < K$.

By the union bound, (F.1.2) and (F.1.3), we get

$$\mathbb{P}\Bigg[\bigcup_{\mathcal{S}\in\overline{\mathcal{P}}([K])}\left\{Z(\mathcal{S}) > \sqrt{n}\left(C(|\mathcal{S}|P) - \frac{|\mathcal{S}|\log M}{n}\right) + \frac{1}{2}\frac{\log n}{\sqrt{n}} + O\left(\frac{1}{\sqrt{n}}\right)\right\}\Bigg] \\ \leq \epsilon + O\left(\frac{1}{n}\right), \tag{F.1.4}$$

which, by the definition (7.15), is equivalent to

$$\left(|\mathcal{S}|\log M \colon \mathcal{S} \in \overline{\mathcal{P}}([K])\right) \in n\mathbf{C}(P\mathbf{1}) \\ - \sqrt{n}Q_{\text{inv}}\left(\mathsf{V}(P\mathbf{1}), \epsilon + O\left(\frac{1}{n}\right)\right) + \frac{1}{2}\log n\mathbf{1} + O\left(1\right)\mathbf{1}. \tag{F.1.5}$$

Applying the Taylor series expansion to $Q_{\text{inv}}(\mathsf{V}(P\mathbf{1}), \cdot)$ completes the proof.

## F.2 Adopting the Codebooks Based on the Channel Estimate at Time $n_0$

In our encoder and decoder design, we use the fact that the received output power concentrates around its mean value. In the proof of Theorem 7.2.2, we show that $n_0 = O(\log n_1)$ symbols are sufficient to ensure that the probability that the decision is made at the correct decoding time, i.e., $n_k$ when $k$ transmitters are active, decays with $O\left(\frac{1}{\sqrt{n_k}}\right)$. In our strategy, we make a binary decision at each decoding time $n_0, \ldots, n_K$ of whether or not to decode. An alternative to this strategy would be to decide the number of active transmitters at time $n_0$, which is much smaller than the rest of the decoding times, and to inform the transmitters about the decoding time in the epoch at time $n_0$. This alternative allows for a code design that depends on the feedback from the receiver to the transmitters at time $n_0$. Using its knowledge of the typical interval, in which the squared norm of the output, $\frac{1}{n_0}\left\|\mathbf{Y}_k^{[n_0]}\right\|^2$, lies for each $k \leq K$, the decoder estimates the number of active transmitters. We denote this value by $t$. The decoder could then transmit $t$ to all transmitters, so that all parties understand that the communication epoch is going to end at time $n_t$. This strategy requires $\lceil \log(K+1) \rceil$ bits of feedback from the receiver to transmitters at time $n_0$; in contrast, the strategy in the proof of Theorem 7.3.1 requires a number of bits of feedback that varies with the decoder's estimate of the number of active transmitters with a maximum of $K+1$ bits. Let the decoder choose $t$ as the nearest integer to $\frac{1}{P}\left(\frac{1}{n_0}\left\|\mathbf{y}^{[n_0]}\right\|^2 - 1\right)$. Then, the bound in (7.192) on the probability that the decoder errs in determining the number of active transmitters can be bounded as

$$\mathbb{P}\left[\mathcal{E}_{\text{time}} \middle| \mathcal{E}_{\text{rep}}^c\right] \leq 2\left(\prod_{j=1}^{k} \kappa_j(P\mathbf{1})\right) \exp\left\{-\frac{n_0(\frac{P}{2})^2}{8(1+kP)^2}\right\} \tag{F.2.6}$$

in the case when the decision is made at time $n_0$. Like (7.192), this bound decays exponentially with $n_0$. Here, however, the exponential rate is smaller than (7.192). Hence, this modification in the strategy increases the constant $c$ in (7.32), and affects the achievable $O(1)$ term in (7.31).

As the encoders learn the estimate of the number of active transmitters at an earlier time, an encoding function that depends on the feedback from the receiver could be employed as follows. Recall from (7.28) that the maximal-power constraints apply to the decoding times $n_1, \ldots, n_K$, but not to $n_0$. Given the estimate $t$ of the number of active transmitters $k$, length-$n_t$ codewords are drawn such that the first $n_1$ symbols are uniformly distributed on $n_1$-dimensional sphere with radius $\sqrt{n_1 P}$, and the symbols indexed from $n_1+1$ to $n_t$ are distributed on $(n_t - n_1)$-dimensional sphere with radius $\sqrt{(n_t - n_1)P}$, i.e., instead of $K$ independent spherical sub-codewords, we use two independent sub-codewords. The length of the second sub-codeword depends on the estimate $t$. The effect of this modification on the error analysis is that under this input distribution, the total variation bound in (7.223) can be improved to

$$\mathrm{TV}(P_{\mathbf{H}}, P_{\tilde{\mathbf{H}}}) \leq \frac{F_k}{\sqrt{n_1}} + \frac{F_k}{\sqrt{n_k - n_1}}, \tag{F.2.7}$$

which decays with the same asymptotic rate as (7.223). Therefore, this modification affects only the $O(1)$ term in (7.31), meaning that the same expansion as Theorem 7.3.1 is achieved.

## F.3 Proof of Lemma 7.4.4

Pinsker's inequality (e.g., [57, Th. 6.5]) states that for any distributions $P$ and $Q$,

$$\mathrm{TV}(P, Q) \leq \sqrt{\frac{1}{2} D(P \| Q)}. \tag{F.3.8}$$

Let $\mathrm{tr}(\cdot)$ denote trace of its matrix argument. The relative entropy between two $d$-dimensional Gaussian distributions with positive covariance matrices is given (e.g., [57, eq. (1.18)]) by

$$\begin{aligned} &D(\mathcal{N}(\boldsymbol{\mu}_1, \Sigma_1) \| \mathcal{N}(\boldsymbol{\mu}_2, \Sigma_2)) \\ &= \frac{1}{2}\Big(\mathrm{tr}(\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2} - \mathsf{I}_d) + (\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)^T \Sigma_1^{-1} (\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2) \\ &\quad - \log\det(\Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2})\Big). \end{aligned} \tag{F.3.9}$$

Define

$$\mathsf{G} \triangleq \Sigma_1^{-1/2}\Sigma_2\Sigma_1^{-1/2} - \mathsf{I}_d \tag{F.3.10}$$

$$a \triangleq \frac{1}{2}\sqrt{(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)^T \Sigma_1^{-1} (\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)}. \tag{F.3.11}$$

Combining (F.3.8) and (F.3.9) and using the inequality $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$, we get

$$\mathrm{TV}(\mathcal{N}(\boldsymbol{\mu}_1, \Sigma_1), \mathcal{N}(\boldsymbol{\mu}_2, \Sigma_2))$$

$$\leq a + \frac{1}{2}\sqrt{\mathrm{tr}(\mathsf{G}) - \log\det(\mathsf{I}_d + \mathsf{G})}. \tag{F.3.12}$$

To bound the logdeterminant term in (F.3.12) from below, we use the following result from [139, Th. 1.1]. Let $\rho(\cdot)$ denote the spectral radius, i.e., the maximum absolute eigenvalue, and let $\|\cdot\|_F$ denote the Frobenius norm. If $\rho(\mathsf{G}) < 1$, then

$$\exp\left\{\mathrm{tr}(\mathsf{G}) - \frac{\|\mathsf{G}\|_F^2}{2(1-\rho(\mathsf{G}))}\right\} \leq \det(\mathsf{I}_d + \mathsf{G}). \tag{F.3.13}$$

For $\rho(\mathsf{G}) < 1$, we apply (F.3.13) to (F.3.12) and get

$$\mathrm{TV}(\mathcal{N}(\boldsymbol{\mu}_1, \Sigma_1), \mathcal{N}(\boldsymbol{\mu}_2, \Sigma_2)) \leq \frac{1}{2\sqrt{2}}\frac{\|\mathsf{G}\|_F}{\sqrt{1-\rho(\mathsf{G})}} + a. \tag{F.3.14}$$

In addition, trivially, we have that

$$\begin{aligned} \mathrm{TV}(\mathcal{N}(\boldsymbol{\mu}_1, \Sigma_1), \mathcal{N}(\boldsymbol{\mu}_2, \Sigma_2)) &\leq 1 && \text{(F.3.15)} \\ &\leq \frac{\|\mathsf{G}\|_F}{\rho(\mathsf{G})} + a, && \text{(F.3.16)} \end{aligned}$$

where in (F.3.16), we use the fact that Frobenius norm is an upper bound to the spectral radius. Taking the tighter bound among (F.3.14) and (F.3.16), we conclude that for $\rho(\mathsf{G}) < 1$,

$$\begin{aligned} &\mathrm{TV}(\mathcal{N}(\boldsymbol{\mu}_1, \Sigma_1), \mathcal{N}(\boldsymbol{\mu}_2, \Sigma_2)) \\ &\leq \min\left\{\frac{1}{2\sqrt{2}}\frac{1}{\sqrt{1-\rho(\mathsf{G})}}, \frac{1}{\rho(\mathsf{G})}\right\}\|\mathsf{G}\|_F + a && \text{(F.3.17)} \\ &\leq \frac{2+\sqrt{6}}{4}\|\mathsf{G}\|_F + a. && \text{(F.3.18)} \end{aligned}$$

Inequality (F.3.18) follows since the maximum of the minimum term in (F.3.17) is achieved by $\rho(\mathsf{G}) = 2\sqrt{6} - 4 \approx 0.899$ and that maximum value is $\frac{2+\sqrt{6}}{4}$. Since the coefficient $\frac{2+\sqrt{6}}{4} > 1 \geq \frac{1}{\rho(\mathsf{G})}$ for $\rho(\mathsf{G}) \geq 1$, we conclude that (F.3.18) holds for any $\rho(\mathsf{G})$.

## F.4 Proof of (7.73)

We show a more general result. Fix any constant $u < P_1 + P_2$. We prove below that for $n$ large enough,

$$\begin{aligned} g(y) &\triangleq \mathbb{P}\left[\|\mathbf{X}_1 + \mathbf{X}_2\|^2 \leq nu \,\middle|\, \|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|^2 = y\right] && \text{(F.4.19)} \\ &\leq \exp\{-nC\} && \text{(F.4.20)} \end{aligned}$$

for all $y \in \mathcal{I}$, where

$$\mathcal{I} \triangleq [n(1+P_1+P_2-\epsilon), n(1+P_1+P_2+\epsilon)] \tag{F.4.21}$$
$$\epsilon \triangleq n^{-1/3}, \tag{F.4.22}$$

and $C$ is a positive constant depending on $u$. Taking $u = P_1 + P_2 - \sqrt{P_1 P_2}$ in (F.4.19) then proves the desired inequality (7.73).

We proceed to prove (F.4.20). Since the support of $\|\mathbf{X}_1 + \mathbf{X}_2\|^2$ is

$$\mathcal{S} = [n(\sqrt{P_1} - \sqrt{P_2})^2, n(\sqrt{P_1} + \sqrt{P_2})^2], \tag{F.4.23}$$

inequality (F.4.20) is trivially satisfied for $u < (\sqrt{P_1} - \sqrt{P_2})^2$. To show (F.4.20) for $(\sqrt{P_1} - \sqrt{P_2})^2 \le u < P_1 + P_2$, we show two concentration results. First, we show that

$$g(y) = g(n(1+P_1+P_2)) \exp\{O(n\epsilon)\} \tag{F.4.24}$$

for all $y \in \mathcal{I}$; second, we show that for $n$ large enough,

$$p \triangleq \mathbb{P}\left[\|\mathbf{X}_1 + \mathbf{X}_2\|^2 \le nu \,\middle|\, \mathcal{A}\right] \tag{F.4.25}$$
$$\le \exp\{-nC'\} \tag{F.4.26}$$

for some $C' > 0$, where the event $\mathcal{A}$ is defined as

$$\mathcal{A} \triangleq \left\{\|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|^2 \in \mathcal{I}\right\}. \tag{F.4.27}$$

Using (F.4.24) and (F.4.26), we show (F.4.20) as follows. By conditioning the probability in (F.4.25) on each value of $\|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|^2$, we express $p$ as

$$p = \int_{\mathcal{I}} g(y) f_{\|\mathbf{X}_1+\mathbf{X}_2+\mathbf{Z}\|^2|\mathcal{A}}(y)dy \tag{F.4.28}$$
$$= g(n(1+P_1+P_2)) \exp\{O(n\epsilon)\} \tag{F.4.29}$$
$$\le \exp\{-nC'\}, \tag{F.4.30}$$

where (F.4.29) follows from (F.4.24) and

$$\min_{y\in\mathcal{I}} g(y) \le \int_{\mathcal{I}} g(y) f_{\|\mathbf{X}_1+\mathbf{X}_2+\mathbf{Z}\|^2|\mathcal{A}}(y)dy \le \max_{y\in\mathcal{I}} g(y). \tag{F.4.31}$$

Inequality (F.4.30) follows from (F.4.26). Inequalities (F.4.24) and (F.4.30) imply that since $O(n\epsilon) = o(n)$, there exists a constant $C > 0$ such that for $n$ large enough, (F.4.20) holds for all $y \in \mathcal{I}$.

We proceed to show (F.4.26). By Bayes' rule, we have

$$p = \frac{\mathbb{P}\left[\|\mathbf{X}_1 + \mathbf{X}_2\|^2 \le nu\right] \mathbb{P}\left[\mathcal{A} \,\middle|\, \|\mathbf{X}_1 + \mathbf{X}_2\|^2 \le nu\right]}{\mathbb{P}\left[\mathcal{A}\right]}. \tag{F.4.32}$$

Changing measure from $P_{\mathbf{X}_1+\mathbf{X}_2} P_{\mathbf{Z}}$ to $P_{\tilde{\mathbf{U}}} P_{\mathbf{Z}}$, where $\tilde{\mathbf{U}} \sim \mathcal{N}(0, (P_1 + P_2)\mathsf{I}_n)$, and then applying Lemma 7.4.1, we get

$$\begin{aligned}
p &\le \frac{\kappa_2(P_1, P_2)\mathbb{P}\left[\left\|\tilde{\mathbf{U}}\right\|^2 \le nu\right] \cdot 1}{1 - \kappa_2(P_1, P_2)\mathbb{P}\left[\left|\left\|\tilde{\mathbf{U}} + \mathbf{Z}\right\|^2 - n(1 + P_1 + P_2)\right| > n\epsilon\right]} && \text{(F.4.33)}\\
&\le \kappa_2(P_1, P_2)\frac{\exp\left\{\frac{-n(P_1+P_2-u)^2}{4(P_1+P_2)^2}\right\}}{1 - 2\kappa_2(P_1, P_2)\exp\{\frac{-n\epsilon^2}{8(1+P_1+P_2)^2}\}} && \text{(F.4.34)}\\
&\le 2\kappa_2(P_1, P_2)\exp\left\{\frac{-n(P_1 + P_2 - u)^2}{4(P_1 + P_2)^2}\right\} && \text{(F.4.35)}\\
&\le \exp\{-nC'\} && \text{(F.4.36)}
\end{aligned}$$

for all $n$ large enough, where $\kappa_2(P_1, P_2)$ is the constant defined in (7.38), and $C'$ is a positive constant. Inequality (F.4.34) follows from the tail bounds on the chi-squared distribution in Lemma 7.4.2, and (F.4.35) follows since the denominator on the right-hand side of (F.4.34) is greater than $\frac{1}{2}$ for $n$ large enough. Inequality (F.4.36) holds since $u < P_1 + P_2$.

We proceed to prove (F.4.24). Define the events $\mathcal{B} \triangleq \{\|\mathbf{X}_1 + \mathbf{X}_2\|^2 \le nu\}$ and $\mathcal{B}(\lambda) \triangleq \{\|\mathbf{X}_1 + \mathbf{X}_2\|^2 = \lambda\}$ for any $\lambda \in \mathcal{S}$. By Bayes' rule, we can express $g(y)$ as

$$g(y) = \frac{\mathbb{P}\left[\mathcal{B}\right] f_{\|\mathbf{X}_1+\mathbf{X}_2+\mathbf{Z}\|^2|\mathcal{B}}(y)}{f_{\|\mathbf{X}_1+\mathbf{X}_2+\mathbf{Z}\|^2}(y)}. \tag{F.4.37}$$

By the spherical symmetry of the distribution of $\mathbf{X}_1 + \mathbf{X}_2$, the conditional distribution of $\|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|^2$ given $\mathcal{B}(\lambda)$ does not depend on $\mathbf{u}$ when we fix $\mathbf{X}_1 + \mathbf{X}_2$ to any $\mathbf{u}$ such that $\|\mathbf{u}\|^2 = \lambda \in \mathcal{S}$. Therefore, the conditional distribution of $\|\mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z}\|^2$ given $\mathcal{B}(\lambda)$ equals the distribution of

$$\sum_{i=1}^{n} \left\|Z_i + \frac{\sqrt{\lambda}}{\sqrt{n}}\right\|^2, \tag{F.4.38}$$

which has non-central chi-squared distribution with $n$ degrees of freedom and non-centrality parameter $\lambda$. That is, the probability density function is

$$f(x; n, \lambda) = \frac{1}{2}\exp\left\{-\frac{(x + \lambda)}{2}\right\}\left(\frac{x}{\lambda}\right)^{\frac{n}{4}-\frac{1}{2}} I_{\frac{n}{2}-1}(\sqrt{\lambda x}), \tag{F.4.39}$$

where $I_\nu(x)$ denotes the modified Bessel function of the first kind with order $\nu$. Fix some $\lambda > 0$, $x_1 = nb$, and $x_2 = n(b+\delta)$, where $0 < \delta \le \epsilon$ and $b > 0$. Consider the ratio

$$\frac{f(x_1; n, \lambda)}{f(x_2; n, \lambda)} = \exp\{x_2 - x_1\} \left(\frac{x_1}{x_2}\right)^{\frac{n}{4}-\frac{1}{2}} \frac{I_{\frac{n}{2}-1}(\sqrt{\lambda x_1})}{I_{\frac{n}{2}-1}(\sqrt{\lambda x_2})}. \tag{F.4.40}$$

Paris [152] bounds $I_\nu(x)/I_\nu(y)$ as

$$\exp\{x-y\}\left(\frac{x}{y}\right)^\nu < \frac{I_\nu(x)}{I_\nu(y)} < \left(\frac{x}{y}\right)^\nu \tag{F.4.41}$$

for any $0 < x < y$ and $\nu > -1/2$. Using (F.4.41), we bound (F.4.40) as

$$\begin{aligned}
&\exp\{n\delta\}\left(1-\frac{\delta}{b+\delta}\right)^{\frac{n}{2}-1} \exp\left\{-\sqrt{n\lambda}\left(\sqrt{b+\delta}-\sqrt{b}\right)\right\} \\
&\le \frac{f(x_1; n, \lambda)}{f(x_2; n, \lambda)} && \text{(F.4.42)} \\
&\le \exp\{n\delta\}\left(1-\frac{\delta}{b+\delta}\right)^{\frac{n}{2}-1}. && \text{(F.4.43)}
\end{aligned}$$

Applying the Taylor series expansion at $\delta = 0$ gives

$$\log\left(1-\frac{\delta}{b+\delta}\right) = -\frac{\delta}{b} + O(\delta^2) \tag{F.4.44}$$

$$-\sqrt{n\lambda}\left(\sqrt{b+\delta}-\sqrt{b}\right) = -\sqrt{n\lambda}\left(\frac{\delta}{2\sqrt{b}} + O(\delta^2)\right). \tag{F.4.45}$$

Substituting (F.4.44) and (F.4.45) in (F.4.42) and (F.4.43), we get

$$\frac{f(x_1; n, \lambda)}{f(x_2; n, \lambda)} = \exp\{O(n\delta)\}. \tag{F.4.46}$$

We can also verify the validity of (F.4.46) for $\lambda = 0$ by using the probability density function of chi-squared distribution with $n$ degrees of freedom instead of (F.4.39). Particularizing (F.4.46) to $b = 1 + P_1 + P_2$, we get for all $\lambda \in \mathcal{S}$ that

$$\begin{aligned}
&f_{\|\mathbf{X}_1+\mathbf{X}_2+\mathbf{Z}\|^2|\mathcal{B}(\lambda)}(y) \\
&= f_{\|\mathbf{X}_1+\mathbf{X}_2+\mathbf{Z}\|^2|\mathcal{B}(\lambda)}(n(1+P_1+P_2))\exp\{O(n\epsilon)\}, && \text{(F.4.47)}
\end{aligned}$$

which together with (F.4.37) implies (F.4.24).

## F.5 Proof of Lemma 7.5.1

We use the induction technique from [140, Th. 4] to prove this lemma, showing that the total variation distance in (7.149) diminishes as $n$ goes to infinity. We here prove that the convergence rate is $O\left(\frac{1}{\sqrt{n}}\right)$. Since the distribution of $\mathbf{H}$ is invariant to rotation, we fix

$$\mathbf{X}_1 = (1, 0, 0, \ldots, 0). \tag{F.5.48}$$

Then $H_{1j} = \sqrt{n}X_{j1}$ for $2 \leq j \leq K$. Define the vectors

$$\mathbf{H}_1 \triangleq (H_{1j} : 2 \leq j \leq K) \tag{F.5.49}$$

$$\mathbf{H}_2 \triangleq (H_{ij} : 2 \leq i < j \leq K), \tag{F.5.50}$$

which consist of all the inner product random variables including $\mathbf{X}_1$, and not including $\mathbf{X}_1$, respectively. Hence $\mathbf{H} = (\mathbf{H}_1, \mathbf{H}_2)$. Notice that $\mathbf{H}_1$ is a product distribution since $X_{j1}$'s are independent.

Note that we have for $2 \leq i < j \leq K$

$$H_{ij} = \sqrt{n}X_{i1}X_{j1} + \frac{\sqrt{n}}{\sqrt{n-1}}(1 - X_{i1}^2)^{\frac{1}{2}}(1 - X_{j1}^2)^{\frac{1}{2}}V_{ij} \tag{F.5.51}$$

$$V_{ij} = \sqrt{n-1}\langle \mathbf{Y}_i, \mathbf{Y}_j \rangle, \tag{F.5.52}$$

where $\mathbf{Y}_i = (1 - X_{i1}^2)^{-\frac{1}{2}}(X_{i2}, \ldots, X_{in}) \in \mathbb{R}^{n-1}$ for $i = 2, \ldots, K$. Denote by $p_K^{(n)}$ the distribution of the $\binom{K}{2}$-dimensional random vector $(\sqrt{n}\langle \mathbf{Z}_i, \mathbf{Z}_j \rangle : 1 \leq i < j \leq K)$, where the $\mathbf{Z}_i$, $i \in [K]$, are distributed independently and uniformly on $\mathbb{S}^n(1)$.

Since $\mathbf{Y}_i$, $i \in \{2, \ldots, K\}$, are distributed independently and uniformly on $\mathbb{S}^{n-1}(1)$, the joint distribution of $\mathbf{V} = (V_{ij} : 2 \leq i < j \leq K)$ is $p_{K-1}^{(n-1)}$. By (F.5.51), the conditional distribution of $H_{ij}$ given $\mathbf{H}_1 = \mathbf{h}_1$ is the same as the distribution of

$$\frac{h_{1i}h_{1j}}{\sqrt{n}} + \frac{\sqrt{n}}{\sqrt{n-1}}\left(1 - \frac{h_{1i}^2}{n}\right)^{\frac{1}{2}}\left(1 - \frac{h_{1j}^2}{n}\right)^{\frac{1}{2}}V_{ij} \tag{F.5.53}$$

for $2 \leq i < j \leq K$. We define the random vector $\mathbf{H}_2^* = (H_{ij}^* : 2 \leq i < j \leq K)$ through $\mathbf{H}_1$ as follows. The conditional distribution of $H_{ij}^*$ given $\mathbf{H}_1 = \mathbf{q}_1$ is the same as the distribution of

$$\frac{h_{1i}h_{1j}}{\sqrt{n}} + \frac{\sqrt{n}}{\sqrt{n-1}}\left(1 - \frac{h_{1i}^2}{n}\right)^{\frac{1}{2}}\left(1 - \frac{h_{1j}^2}{n}\right)^{\frac{1}{2}}Z_{ij} \tag{F.5.54}$$

for $2 \leq i < j \leq K$, where $Z_{ij} \sim \mathcal{N}(0,1)$, and $H^*_{ij}$, $2 \leq i < j \leq K$, are conditionally independent given $\mathbf{H}_1$. Now, we are ready to apply the mathematical induction.

**Base case:** For $K = 2$, we have

$$\mathrm{TV}(p_2^{(n)}, \mathcal{N}(0,1)) \leq \frac{4}{n} \tag{F.5.55}$$

by Lemma 7.4.5 with $k = 1$.

**Inductive step:** For $K > 2$, assume that for any $n$,

$$\mathrm{TV}\left(p_{K-1}^{(n)}, \mathcal{N}\left(\mathbf{0}, \mathsf{I}_{\frac{1}{2}(K-1)(K-2)}\right)\right) \leq \frac{C_{K-1}}{\sqrt{n}} \tag{F.5.56}$$

for some constant $C_{K-1}$. Let $P_{\tilde{\mathbf{H}}_1} = \mathcal{N}(\mathbf{0}, \mathsf{I}_{K-1})$ and $P_{\tilde{\mathbf{H}}_2} = \mathcal{N}\left(\mathbf{0}, \mathsf{I}_{\binom{K-1}{2}}\right)$. Since the total variation distance is $\ell_1$ norm, applying the triangle inequality gives

$$\begin{aligned}
&\mathrm{TV}\left(p_K^{(n)}, \mathcal{N}\left(\mathbf{0}, \mathsf{I}_{\binom{K}{2}}\right)\right) \\
&= \mathrm{TV}\left(P_{\mathbf{H}_1} P_{\mathbf{H}_2|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\tilde{\mathbf{H}}_2}\right) && \text{(F.5.57)} \\
&\leq \mathrm{TV}\left(P_{\mathbf{H}_1} P_{\mathbf{H}_2|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2|\mathbf{H}_1}\right) && \text{(F.5.58)} \\
&\quad + \mathrm{TV}\left(P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2^*|\mathbf{H}_1}\right) && \text{(F.5.59)} \\
&\quad + \mathrm{TV}\left(P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2^*|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\tilde{\mathbf{H}}_2}\right). && \text{(F.5.60)}
\end{aligned}$$

Here, (F.5.58) approximates the input measure $P_{\mathbf{H}_1}$ with the corresponding i.i.d. Gaussian measure $P_{\tilde{\mathbf{H}}_1}$, (F.5.59) approximates the inner product random variables $V_{ij}$ in the definition of the probability transition kernel given in (F.5.53) with i.i.d. standard Gaussian random variables, and (F.5.60) approximates the mean in (F.5.54) by 0 and the variance by 1. We next bound the right-hand sides of (F.5.58)–(F.5.60) in that order. We have

$$\begin{aligned}
&\mathrm{TV}\left(P_{\mathbf{H}_1} P_{\mathbf{H}_2|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2|\mathbf{H}_1}\right) \\
&= \mathrm{TV}\left(P_{\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1}\right) && \text{(F.5.61)} \\
&\leq (K-1)\mathrm{TV}\left(P_{H_{12}}, \mathcal{N}(0,1)\right) && \text{(F.5.62)} \\
&\leq \frac{4(K-1)}{n}, && \text{(F.5.63)}
\end{aligned}$$

where (F.5.62) follows from [142, Lemma 2.1] since $P_{\mathbf{H}_1} = (P_{H_{12}})^{K-1}$ and $P_{\tilde{\mathbf{H}}_1} = (\mathcal{N}(0,1))^{K-1}$ are both product distributions, and (F.5.63) follows from Lemma 7.4.5. The total variation distance in (F.5.59) is bounded as

$$\mathrm{TV}\left(P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2^*|\mathbf{H}_1}\right)$$

$$= \mathbb{E}\left[\mathrm{TV}\left(P_{\mathbf{H}_2|\mathbf{H}_1=\tilde{\mathbf{H}}_1}, P_{\mathbf{H}_2^*|\mathbf{H}_1=\tilde{\mathbf{H}}_1}\right)\middle|\tilde{\mathbf{H}}_1\right] \tag{F.5.64}$$

$$= \mathrm{TV}\left(p_{K-1}^{(n-1)}, \mathcal{N}\left(\mathbf{0}, \mathsf{I}_{\binom{K-1}{2}}\right)\right) \tag{F.5.65}$$

$$\le \frac{C_{K-1}}{\sqrt{n-1}}, \tag{F.5.66}$$

where (F.5.65) follows from the definitions (F.5.53) and (F.5.54) since the total variation distance is shift and scale invariant and (F.5.66) follows from the inductive assumption (F.5.56). The total variation distance in (F.5.60) is bounded as

$$\mathrm{TV}\left(P_{\tilde{\mathbf{H}}_1} P_{\mathbf{H}_2^*|\mathbf{H}_1}, P_{\tilde{\mathbf{H}}_1} P_{\tilde{\mathbf{H}}_2}\right)$$

$$= \mathbb{E}\left[\mathrm{TV}\left(P_{\mathbf{H}_2^*|\mathbf{H}_1=\tilde{\mathbf{H}}_1}, P_{\tilde{\mathbf{H}}_2}\right)\middle|\tilde{\mathbf{H}}_1\right] \tag{F.5.67}$$

$$\le \mathbb{E}\left[\sum_{2\le i<j\le K} \mathrm{TV}\left(P_{H_{ij}^*|\mathbf{H}_1=\tilde{\mathbf{H}}_1}, \mathcal{N}(0,1)\right)\middle|\tilde{\mathbf{H}}_1\right] \tag{F.5.68}$$

$$= \binom{K-1}{2}\mathbb{E}\Bigg[\mathrm{TV}\Bigg(\mathcal{N}\Bigg(\frac{\tilde{H}_{12}\tilde{H}_{13}}{\sqrt{n}}, \frac{n}{n-1}\left(1-\frac{\tilde{H}_{12}^2}{n}\right)\left(1-\frac{\tilde{H}_{13}^2}{n}\right)\Bigg), \mathcal{N}(0,1)\Bigg)\Bigg] \tag{F.5.69}$$

$$\le \binom{K-1}{2}\left\{\frac{1}{2}\frac{\mathbb{E}\left[\left|\tilde{H}_{12}\right|\right]^2}{\sqrt{n}} + \frac{2+\sqrt{6}}{4}\left|\frac{n}{n-1}\left(\mathbb{E}\left[1-\frac{\tilde{H}_{12}^2}{n}\right]\right)^2 - 1\right|\right\} \tag{F.5.70}$$

$$= \binom{K-1}{2}\left(\frac{1}{\pi\sqrt{n}} + \frac{2+\sqrt{6}}{4n}\right), \tag{F.5.71}$$

where (F.5.68) follows from [142, Lemma 2.1] since the conditional distribution of $\mathbf{H}_2^*$ given $\mathbf{H}_1 = \mathbf{h}_1$ is a product distribution and $P_{\tilde{\mathbf{H}}_2}$ is an i.i.d. standard Gaussian. Equality (F.5.69) follows since the conditional distribution of $H_{ij}^*$ given $\mathbf{H}_1 = \mathbf{h}_1$ is identically distributed for $2 \le i < j \le K$. Inequality (F.5.70) follows from Lemma 7.4.4 with $d = 1$ using the i.i.d. distribution of $\tilde{H}_{12}$ and $\tilde{H}_{13}$. Combining (F.5.63), (F.5.66), (F.5.71), and the inequality in (F.5.58) completes the proof by induction.

We note that the convergence rate of the total variation distance of interest is $O\left(\frac{1}{\sqrt{n}}\right)$ for $K > 2$, while it is faster $\left(O\left(\frac{1}{n}\right)\right)$ for $K = 2$.