Channel Coding via Robust Optimization Part 2: The Multi-User Channel

Chaithanya Bandi* Dimitris Bertsimas†

August 2015

Abstract

In this paper, we consider the optimal finite length (n) channel coding problem on multi-user Gaussian channels achieving an error probability bound of ϵ. We present novel optimization formulations of the channel coding problem on multi-user Gaussian interference and broadcast channels. Solving these problems to optimality leads to exact upper and lower bounds on the channel capacity for finite code length n, and as $n \to \infty$, the upper and lower bounds coincide. The nature and computational complexity of the optimization problem depends on the noise distribution in the following way: (a) for Gaussian channels the optimization problems involve a rank minimization problem subject to semidefinite constraints which we solve by iteratively solving semidefinite optimization problems; and (b) for exponential and uniform channels, the optimization problems are mixed integer linear optimization problems which we solve using commercial solvers. Because of the size and complexity of these formulations, we do not solve them to provable optimality. Still we provide a feasible code that leads to a valid lower bound on the capacity region, but we only provide approximations for the upper bound on the capacity region. We report these computations for $n = 60$ for two-user Gaussian interference channels.

1 Introduction

Network Information Theory is the study of capacity regions of noisy communication channels between multiple transmitters and receivers. While the capacity of a single-user channel was established by Shannon [1948], the problem of establishing the communication limits of many common channels such as the interference and the multicast channels still remain unknown. And indeed a general theory for communication limits on networks of channels is still largely open. Techniques such as random encoding that are effective for single-user channels no longer allow us to characterize the capacity regions of complex channels, and there is a need to develop widely extendable and structured ways of constructing optimal codes.

In this paper, we extend the robust optimization (RO) based approach introduced in Bandi and Bertsimas [2015] to compute the capacity region of multi-user interference channel and broadcast

*Assistant Professor, Kellogg School of Management, Northwestern University, IL 60208, USA. Email: c-bandi@kellogg.northwestern.edu.

†Boeing Professor of Operations Research, co-director, Operations Research Center, Massachusetts Institute of Technology, E40-147, Cambridge, MA 02139, USA. Email: dbertsim@mit.edu.

channel. In particular, (a) we use the Typical sets as Uncertainty sets; (b) we use binary variables and binary optimization to model the probabilistic constraints; and (c) then reformulate the underlying RO problem that computes the capacity region as either a mixed binary linear optimization problem (for non-Gaussian channels) or a non-convex quadratic optimization problem (for Gaussian channels). Solving these problems to optimality leads to exact upper and lower bounds on the channel capacity for finite code length n. These upper and lower bounds converge to the true capacity of these channels asymptotically as the code length $n \to \infty$ and the error probability $\epsilon \to 0$. The nature and computational complexity of the optimization problem depends on the noise distribution in the following way: (a) For Gaussian channels the optimization problems involve a rank minimization problem subject to semidefinite constraints which we solve by iteratively solving semidefinite optimization problems; and (b) For exponential and uniform channels, the optimization problems are mixed integer linear optimization problems which we solve using commercial solvers.

Notation

We denote scalar quantities by non-bold face symbols (e.g., $x \in \mathbb{R}$, $k \in \mathbb{N}$), vector quantities by boldface symbols (e.g., $\mathbf{x} \in \mathbb{R}^n, n > 1$), and matrices by uppercase boldface symbols (e.g., $\mathbf{A} \in \mathbb{R}^{n \times m}, n > 1, m > 1$). We denote scalar random variables as $\tilde{z}$ and vector random variables as $\tilde{\mathbf{z}}$. We use the notation $\tilde{\mathbf{z}} \sim N(\mathbf{0}, \sigma \cdot \boldsymbol{I})$ to denote that each component of $\tilde{\mathbf{z}}$ is normally distributed with mean 0 and standard deviation σ.

1.1 Relevant Literature

For a broad review of Information Theory we refer the reader to Verdú [1998], Verdú and McLaughlin [2000], Cover and Thomas [2006].

Ahlswede [1974] and Liao [1972] found various characterizations of the asymptotic capacity region of the two-user discrete memoryless multi-access channel. Urbanke and Rimoldi [1998] showed (using the suboptimal successive cancellation decoder) that the memoryless Gaussian multiple-access channel admits a very simple capacity region: the pentagon defined by the single-user capacities of the channels with powers equal to the individual powers and to the sum of the powers.

In contrast to the multi-access setting in which the receiver is interested in decoding the information sent by all the users, suppose now that we have as many receivers as transmitters and each receiver is interested in decoding only one of the sources. In spite of many efforts surveyed in Verdú and McLaughlin [2000], the capacity region of even the simplest two-user memoryless Gaussian interference channel remains an open problem. The only case in which the capacity is known is in the strong interference case, where each receiver has a better reception of the other user's signal than the intended receiver (Sason [2004]). The best known strategy for more general cases is due to Han and Kobayashi [1981]. Etkin et al. [2008] show that a simple Han–Kobayashi type scheme can in fact achieve rates within 1 bit/s/Hz of the capacity of the channel for all values of the channel parameters.

Although a general solution for the capacity region of the multicast channel is not yet known, considerable progress (surveyed in Verdú [1998]) has been made in exploring the fundamental limits of various classes of memoryless multicast channels. However, the main problem remains open.

More recently, many authors have considered the problem of capacity characterization for finite code lengths, (see Huang and Moulin [2012], MolavianJazi and Laneman [2012a,b]) for multi-access

channels. However, no such results have been reported for the case of interference channels.

1.2 Contributions and Structure

In this paper, we provide algorithms to compute the capacity regions and to find optimal codes for the following classical channels in information theory: the two-user Gaussian interference channel, the two-user multi-access and multicast Gaussian channels, and multi-user channels with exponentially distributed noise. In particular, the contributions of this paper are as follows:

1. *The two-user Gaussian interference channel*: The RO approach leads to new lower and upper bounds for the capacity region of multi-user channels with interference for finite code length n as well as a code that matches the lower bound. As $n \to \infty$, the bounds are tight. The bounds involve a rank minimization problem subject to semidefinite constraints that can be solved by iterative application of semidefinite optimization methods. Because of the size and complexity of these formulations, we do not solve them to provable optimality. Still we provide a feasible code that leads to a valid lower bound on the capacity region, but we only provide approximations for the upper bound on the capacity region.
2. *The two-user Gaussian multicast and multi-access channels*: We show that the RO approach extends to multicast and multi-access channels.
3. *Multi-user channels with Non-Gaussian noise*: We examine how the probability description of noise affects the nature of the corresponding optimization problem and show that for exponential, uniform and binary channels or when we model the noise sequences as satisfying certain asymptotic laws, like the central limit theorem, the lower and upper bounds involve mixed binary linear optimization problems that can be solved by commercial solvers.
4. *Computational Results*: We report computational results that show that the RO approach is computationally tractable for $n = 60$ for two-user Gaussian interference channels.

The structure of the paper is as follows. In Section 2, we present our approach in the context of two-user Gaussian Interference Channel. In Section 3, we consider the broadcast and multi-access Gaussian channels, respectively. In Section 4, we extend our approach to non-Gaussian channels. In Section 5, we present computational results for the two-user Gaussian interference channels with finite code length. In Section 6, we present some concluding remarks.

2 Gaussian Interference Channel

A two-user interference channel is a communication medium in which each user intends to transmit messages taken from their corresponding message books $\mathcal{M}^1 = \{1, 2, \ldots, M_1\}$ and $\mathcal{M}^2 = \{1, 2, \ldots, M_2\}$. User 1 selects message $m^1 = i \in \mathcal{M}^1$ and transmits $\mathbf{x}_i^1$ over the channel, while satisfying the power constraint

$$\left\|\mathbf{x}_i^1\right\|^2 \leq nP_1.$$

User 2 chooses message $m^2 = k \in \mathcal{M}^2$ and transmits $\mathbf{x}_k^2$ that satisfies

$$\left\|\mathbf{x}_k^2\right\|^2 \leq nP_2.$$

The channel introduces noise terms $\tilde{\mathbf{z}}^1$ and $\tilde{\mathbf{z}}^2$, and the transmitted messages $\mathbf{x}_i^1$ and $\mathbf{x}_k^2$ interfere to give rise to codewords $\mathbf{y}^1$ and $\mathbf{y}^2$ given by

$$\begin{aligned}\mathbf{y}^1 &= \mathbf{x}_i^1 + h_{12}\mathbf{x}_k^2 + \tilde{\mathbf{z}}^1,\\ \mathbf{y}^2 &= \mathbf{x}_k^2 + h_{21}\mathbf{x}_i^1 + \tilde{\mathbf{z}}^2,\end{aligned}$$

which are received by the users. The noise terms $\tilde{\mathbf{z}}^1, \tilde{\mathbf{z}}^2 \sim N(\mathbf{0}, \sigma\cdot\mathbf{I})$, and the interference parameters h_{12} and h_{21} are assumed to be real numbers. We let $m^1 = i$ and $m^2 = k$ to denote that Users 1 and 2 transmitted messages $i \in \mathcal{M}^1$ and $k \in \mathcal{M}^2$ on the channel, respectively.

The channel coding problem for a two-user Gaussian interference channel refers to the problem of constructing a code with inputs:

(a) The length n of the codewords;

(b) The rates R_1, R_2 of the code; Note that $M_i = 2^{nR_i},\ i = 1, 2$.

(c) The power constraints P_1, P_2 of the users;

(d) The common standard deviation σ of the normally distributed noises $\tilde{\mathbf{z}}^1$ and $\tilde{\mathbf{z}}^2$;

(e) The interference channel parameters h_{12}, h_{21};

(f) The average probability of error $\epsilon > 0$ (see Eqs. (1) and (2)) the users tolerate.

The outputs of $\mathcal{C}^{\mathrm{IC}}\left[n, R_1, R_2, P_1, P_2, h_{12}, h_{21}, \sigma, \epsilon\right]$ are:

(a) The codebooks $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$;

(b) The decoding functions $g^1 : \mathbb{R}^n \to \mathcal{B}^1$, $g^2 : \mathbb{R}^n \to \mathcal{B}^2$ that map each received codeword $\mathbf{y}^1, \mathbf{y}^2$ to one of the codewords in $\mathcal{B}^1$ and $\mathcal{B}^2$, respectively, so that the average probability of error satisfies

$$\frac{1}{M_1}\sum_{i\in\mathcal{M}^1}\mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] \leq \epsilon, \tag{1}$$

$$\frac{1}{M_2}\sum_{k\in\mathcal{M}^2}\mathbb{P}\left[g^2\left(\mathbf{y}^2\right) \neq k | m^2 = k\right] \leq \epsilon. \tag{2}$$

The capacity region $\mathcal{R}_n^{\mathrm{IC}}\left[P_1, P_2, h_{12}, h_{21}, \sigma, \epsilon\right]$ is defined as the set of all rate pairs (R_1, R_2) such that there exists a code $\mathcal{C}^{\mathrm{IC}}\left[n, R_1, R_2, P_1, P_2, h_{12}, h_{21}, \sigma, \epsilon\right]$. We let $\mathcal{R}^{\mathrm{IC}}\left[P_1, P_2, h_{12}, h_{21}, \sigma\right]$ denote the asymptotic capacity region.

2.1 Capacity Computation and Optimal Coding

In this section, we present an algorithm that produces lower and upper bounds on the capacity region and a code that matches the lower bound. The bounds become tight in the limit of $n \to \infty$ and $\epsilon \to 0$. The algorithm consists of two parts: **(a)** the *Encoding Algorithm* (Algorithm 1), and **(b)** the *Decoding Algorithm* (Algorithm 2). A key ingredient in our construction of this algorithm is the form of the decoder (3a,3b) that we propose. Let $r > 0$. In this proposal, User 1(2) after receiving $\mathbf{y}^1(\mathbf{y}^2)$, selects $i_1^*(i_2^*)$ by solving the problems:

$$i_1^* = \arg\max_{i\in\mathcal{M}^1}\left|\mathscr{B}_i^1\right|,\ \text{where } \mathscr{B}_i^1 = \left\{k \in \mathcal{M}^2\ :\ \left\|\mathbf{y}^1 - \left(\mathbf{x}_i^1 + h_{12}\mathbf{x}_k^2\right)\right\| \leq r\right\} \tag{3a}$$

$$i_2^* = \arg\max_{i\in\mathcal{M}^2}\left|\mathscr{B}_i^2\right|,\ \text{where } \mathscr{B}_i^2 = \left\{k \in \mathcal{M}^1\ :\ \left\|\mathbf{y}^2 - \left(\mathbf{x}_i^2 + h_{21}\mathbf{x}_k^1\right)\right\| \leq r\right\}, \tag{3b}$$

for some specific r. The intuition behind the optimality of this decoder can be obtained from Proposition 1, which states that (3a,3b) is the maximum likelihood decoder for an interference channel where the noise is distributed uniformly in $\mathcal{B}_n(r) = \{\mathbf{z} \in \mathbb{R}^n \,|\, \|\mathbf{z}\| \leq r\}$.

Proposition 1. *Consider an interference channel where the noise $\tilde{\mathbf{z}}$ is distributed uniformly in $\mathcal{B}_n(r)$. The maximum likelihood decoder for this channel is given by (3a,3b).*

Proof. Let $\mathbf{y}^1$ be the message received by User 1. The maximum likelihood decoder is given by

$$i^* = \arg\max_{i \in \mathcal{M}^1} \mathbb{P}\left[\mathbf{y}^1 \text{ is received} \middle| m^1 = i\right].$$

We have

$$\mathbb{P}\left[\mathbf{y}^1 \text{ is received} \middle| m^1 = i\right] = \frac{1}{M_2} \cdot \sum_{k=1}^{M_2} \mathbb{P}\left[\mathbf{y}^1 \text{ is received} \middle| m^1 = i, m^2 = k\right].$$

Since the noise $\tilde{\mathbf{z}}$ is distributed uniformly in $\mathcal{B}_n(r)$, we also have

$$\mathbf{1}\left\{\mathbf{y}^1 \text{ is received} \middle| m^1 = i, m^2 = k\right\} = \begin{cases} 1, & \text{if } \|\mathbf{y}^1 - (\mathbf{x}_i^1 + h_{12}\mathbf{x}_k^2)\| \leq r. \\ 0, & \text{otherwise,} \end{cases}$$

Therefore,

$$\mathbb{P}\left[\mathbf{y}^1 \text{ is received} \middle| m^1 = i\right] = \frac{1}{M_2} \cdot \left|\mathscr{B}_i^1\right|,$$

where $\mathscr{B}_i^1$ is defined in (3a). Finally, $i^* = \arg\max_{i \in \mathcal{M}^1} \mathbb{P}\left[\mathbf{y}^1 \text{ is received} \middle| m^1 = i\right] = \arg\max_{i \in \mathcal{M}^1} \left|\mathscr{B}_i^1\right|$. □

In Theorem 1, we show that it suffices to restrict to this decoder in order to construct capacity characterizing codewords. Based on this decoder, we next present the Encoding Algorithm which involves checking the feasibility of Problem (17-27). The inputs to the encoding algorithm are $(n, R_1, R_2, P_1, P_2, h_{12}, h_{21}, \sigma, \epsilon, \nu)$, where the parameter $\nu > 0$ regulates the tradeoff between the accuracy of the bound on the capacity of the Gaussian interference channel and the complexity of computing it; see the remark after Theorem 1. Given these inputs, we first calculate the following "derivative" quantities:

1. The parameter γ_ϵ, and M_0 which we choose so that

$$\mathbb{P}\left[\|\tilde{\mathbf{z}}_G\| \leq \gamma_\epsilon\right] \geq 1 - \epsilon, \tag{4}$$

$$M_0 = (1 + \nu) \cdot \gamma_\epsilon, \tag{5}$$

where $\tilde{\mathbf{z}}_G \sim N(\mathbf{0}, \sigma \cdot \mathbf{I})$;

2. The parameter T given by

$$T = \left(\frac{1+\nu}{\eta\nu} \cdot \frac{\gamma_\epsilon}{\sqrt{n}}\right)^n, \text{ with } \eta = \frac{\sigma}{\sqrt{n}} \cdot \Phi^{-1}\left(1 - \epsilon^{1/4}\right), \tag{6}$$

where $\Phi(\cdot)$ is the cdf of a standard normal and $\delta(\nu, n) = \exp\left(-n \cdot \frac{r - \log(1+r)}{2(1+3\nu)^2\sigma^2}\right)$, with $r = \sigma^2\left((1+3\nu)^2 - (1+2\nu)^2\right)$;

3. The set of vectors

$$\mathcal{Z} = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_T\} \tag{7}$$

with $\|\mathbf{z}_t\| = M_0,\ t = 1, \ldots, T$, are computed as in Bandi and Bertsimas [2015].

4. The quantities δ_1, α_1 defined as

$$\delta_1 = \delta_2 = \left(\frac{\eta\nu}{1+\nu}\right)^2 n + 4\Gamma_\epsilon^2 + 4M_0 \cdot \sqrt{\left(\frac{\eta\nu}{1+\nu}\right)^2 n + 4\Gamma_\epsilon^2}, \tag{8}$$

$$\alpha_1 = \frac{1}{8\eta^2 n}\left\{\beta_1 - \sqrt{\beta_1^2 - 16\eta^2 n\left(4h_{12}^2 P_2 n + 4M_0 h_{12}\sqrt{nP_2} - 3\delta_1\right)}\right\}, \tag{9}$$

$$\alpha_2 = \frac{1}{8\eta^2 n}\left\{\beta_2 - \sqrt{\beta_2^2 - 16\eta^2 n\left(4h_{21}^2 P_1 n + 4M_0 h_{21}\sqrt{nP_1} - 3\delta_2\right)}\right\},$$

where

$$\beta_1 = 4\eta^2 n + 4h_{12}^2 P_2 n + 4M_0 h_{12}\sqrt{nP_2} + \delta_1,$$
$$\beta_2 = 4\eta^2 n + 4h_{21}^2 P_1 n + 4M_0 h_{21}\sqrt{nP_1} + \delta_2.$$

The quantities δ_2, α_2 are defined in a similar manner. Note that as $\nu \to 0$ and $n \to \infty$, $\delta_1, \delta_2 \to 0$ and $\alpha_1, \alpha_2 \to 1$.

The intuition of the *Encoding Algorithm* is as follows. We select codewords $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ that represent codewords for Users 1 and 2, respectively. In order to enforce the decoder (3a) for $r = M_0$, we would require that

$$\left|\left\{k' \in \mathcal{B}^2 \mid \left\|\mathbf{y}^1 - \mathbf{x}_{i_1^*}^1 - h_{12}\mathbf{x}_k^2\right\|^2 \le M_0^2\right\}\right| \ge \left|\left\{k' \in \mathcal{B}^2 \mid \left\|\mathbf{y}^1 - \mathbf{x}_i^1 - h_{12}\mathbf{x}_k^2\right\|^2 \le M_0^2\right\}\right|, \forall i \in \mathcal{M}^1.$$

Note that the optimization model we are developing only involves a discrete collection of noise vectors $\mathbf{z}_t$, $t \in \mathcal{T}$. However, the probabilistic guarantees we want to offer need to be valid for all Gaussian noise. For this reason, we create a "cushion" δ_1 as defined in (8), and instead require

$$\left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|\mathbf{y}^1 - \mathbf{x}_{i_1^*}^1 - h_{12}\mathbf{x}_k^2\right\|^2 \le M_0^2 + \delta_1\right\}\right| \ge$$
$$\left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|\mathbf{y}^1 - \mathbf{x}_i^1 - h_{12}\mathbf{x}_k^2\right\|^2 \le M_0^2 - \delta_1\right\}\right|, \forall i \in \mathcal{M}^1. \tag{10}$$

Using this decoder, we want to ensure that the average probability of error is at most $\epsilon^{1/4}$, that is,

$$\frac{1}{M_2}\sum_{k\in\mathcal{M}^2} \mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \ne i \,\middle|\, m^1 = i, m^2 = k\right] \le \epsilon^{1/4}. \tag{11}$$

In order to achieve this, we define the following "counting" variables $\{v_i^1, v_{ik}^1, v_{ikt}^1\}_{i\in\mathcal{M}^1, k\in\mathcal{M}^2, t\in\mathcal{T}}$:

$$v_{ikt}^1 = \begin{cases} 1, & \text{if } \left|\mathcal{B}_{ikt,i'}^1\right| \le \left|\mathcal{B}_{ikt,i}^1\right|, \forall i' \in \mathcal{M}^1, \\ 0, & \text{otherwise,} \end{cases} \tag{12}$$

$$v_{ik}^1 = \begin{cases} 1, & \text{if } \sum_{t\in\mathcal{T}} v_{ikt}^1 \ge \left(1 - \epsilon^{1/4}\right)\cdot T, \\ 0, & \text{otherwise,} \end{cases} \tag{13}$$

$$v_i^1 = \begin{cases} 1, & \text{if } \sum_{k\in\mathcal{M}^2} v_{ik}^1 \ge \left(1 - \epsilon^{1/4}\right)\cdot M_2, \\ 0, & \text{otherwise,} \end{cases} \tag{14}$$

where

$$\mathcal{B}^1_{ikt,i'} = \left\{ k' \in \mathcal{B}^2 \,:\, \left\| \mathbf{x}^1_i - \mathbf{x}^1_{i'} + h_{12}\left(\mathbf{x}^2_k - \mathbf{x}^2_{k'}\right) + \mathbf{z}_t \right\|^2 \leq M_0^2 - \delta_1 \right\},$$
$$\mathcal{B}^1_{ikt,i} = \left\{ k' \in \mathcal{B}^2 \,:\, \left\| h_{12}\left(\mathbf{x}^2_k - \mathbf{x}^2_{k'}\right) + \mathbf{z}_t \right\|^2 \leq M_0^2 + \delta_1 \right\}.$$

To model the cardinality constraints in (12), we define auxiliary variables $\{v^1_{ii'kk't}\}$ as follows

$$v^1_{ii'kk't} = \begin{cases} 1, & \text{if } \left\| \mathbf{x}^1_i - \mathbf{x}^1_{i'} + h_{12}\left(\mathbf{x}^2_k - \mathbf{x}^2_{k'}\right) + \mathbf{z}_t \right\|^2 \leq M_0^2 - \delta_1, \\ 0, & \text{otherwise}, \end{cases} \tag{15}$$

$$v^1_{iikk't} = \begin{cases} 1, & \text{if } \left\| h_{12}\left(\mathbf{x}^2_k - \mathbf{x}^2_{k'}\right) + \mathbf{z}_t \right\|^2 \leq M_0^2 + \delta_1, \\ 0, & \text{otherwise}. \end{cases} \tag{16}$$

The variables $\{v^2_k, v^2_{ki}, v^2_{kit}, v^2_{kk'ii't}\}$ corresponding to User 2 are defined in a similar manner. We next present the Encoding Algorithm 1 for the two-user interference channel.

Algorithm 1. ***Encoding algorithm for two-user interference channel.***
Input: *n, R_1, R_2, σ, P_1, P_2, ϵ, ν.*
Output: *Codewords $\mathbf{x}^1_i$, $\mathbf{x}^2_k$, and binary variables v^1_i, v^2_k, v^1_{ik}, v^2_{ik}, $\{v^1_{ikt}, v^2_{ikt}\}_{t\in\mathcal{T}}$.*
Algorithm:

1. *Calculate the quantities T, M_0, δ_1, δ_2 using (6) and (5).*

2. *Check the feasibility of the constraints*

$$\left\|\mathbf{x}_i^1\right\|^2 \leq nP_1, \qquad i \in \mathcal{M}^1, \tag{17}$$

$$\left\|\mathbf{x}_i^1 - \mathbf{x}_{i'}^1 + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \leq M_0^2 - \delta_1 + \left(1 - v_{ii'kk't}^1\right) M_0^2, \qquad i, i' \neq i \in \mathcal{M}^1, k, k' \in \mathcal{M}^2, t \in \mathcal{T}, \tag{18}$$

$$\left\|h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \leq M_0^2 + \delta_1 + \left(1 - v_{iikk't}^1\right) M_0^2, \qquad i \in \mathcal{M}^1, k, k' \in \mathcal{M}^2, t \in \mathcal{T}, \tag{19}$$

$$\sum_{k'=1}^{M_2} v_{iikk't}^1 \geq \sum_{k'=1}^{M_2} v_{ii'kk't}^1, \qquad i, i' \neq i \in \mathcal{M}^1, k \in \mathcal{M}^2, t \in \mathcal{T}, \tag{20}$$

$$v_{ii'kk't}^1 \leq v_{ikt}^1, \qquad i, i' \in \mathcal{M}^1, k, k' \in \mathcal{M}^2, t \in \mathcal{T}, \tag{21}$$

$$v_{ikt}^1 \leq v_{ik}^1, \qquad i \in \mathcal{M}^1, k \in \mathcal{M}^2, t \in \mathcal{T}, \tag{22}$$

$$\sum_{t=1}^{T} v_{ikt}^1 \geq (1 - \epsilon) \cdot T \cdot v_{ik}^1, \qquad i \in \mathcal{M}^1, k \in \mathcal{M}^2, \tag{23}$$

$$v_{ik}^1 \leq v_i^1, \qquad i \in \mathcal{M}^1, k \in \mathcal{M}^2, \tag{24}$$

$$\sum_{k=1}^{M_2} v_{ik}^1 \geq \left(1 - \epsilon^{1/4}\right) \cdot M_2 \cdot v_i^1, \qquad i \in \mathcal{M}^1, \tag{25}$$

$$\sum_{i=1}^{M_1} v_i^1 \geq \left(1 - \epsilon^{1/4}\right) \cdot M_1, \tag{26}$$

$$\left\|\mathbf{x}_i^1 - \mathbf{x}_{i'}^1 + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right)\right\| \geq 2(1 + 2\nu)\eta\sqrt{n} \cdot v_{ik}^1, \quad i, i' \in \mathcal{M}^1, k, k' \in \mathcal{M}^2, \tag{27}$$

$$\left\|\mathbf{x}_k^2\right\|^2 \leq nP_2, \qquad k \in \mathcal{M}^2, \tag{28}$$

$$\left\|\mathbf{x}_k^2 - \mathbf{x}_{k'}^2 + h_{21}\left(\mathbf{x}_i^1 - \mathbf{x}_{i'}^1\right) + \mathbf{z}_t\right\|^2 \leq M_0^2 - \delta_2 + \left(1 - v_{kk'ii't}^2\right) M_0^2, \qquad k, k' \neq k \in \mathcal{M}^2, i, i' \in \mathcal{M}^1, t \in \mathcal{T},$$

$$\left\|h_{21}\left(\mathbf{x}_i^1 - \mathbf{x}_{i'}^1\right) + \mathbf{z}_t\right\|^2 \leq M_0^2 + \delta_2 + \left(1 - v_{kkii't}^2\right) M_0^2, \qquad k \in \mathcal{M}^2, i, i' \in \mathcal{M}^1, t \in \mathcal{T},$$

$$\sum_{i'=1}^{M_1} v_{kkii't}^2 \geq \sum_{i'=1}^{M_1} v_{kk'ii't}^2, \qquad k, k' \neq k \in \mathcal{M}^2, i \in \mathcal{M}^1, t \in \mathcal{T},$$

$$v_{kk'ii't}^2 \leq v_{kit}^2, \qquad k, k' \in \mathcal{M}^2, i, i' \in \mathcal{M}^1, t \in \mathcal{T},$$

$$v_{kit}^2 \leq v_{ki}^2, \qquad k \in \mathcal{M}^2, i \in \mathcal{M}^1, t \in \mathcal{T},$$

$$\sum_{t=1}^{T} v_{kit}^2 \geq (1 - \epsilon) \cdot T \cdot v_{ki}^2, \qquad k \in \mathcal{M}^2, i \in \mathcal{M}^1,$$

$$v_{ki}^2 \leq v_k^2, \qquad k \in \mathcal{M}^2, i \in \mathcal{M}^1,$$

$$\sum_{i=1}^{M_1} v_{ki}^2 \geq \left(1 - \epsilon^{1/4}\right) \cdot M_1 \cdot v_k^2, \qquad k \in \mathcal{M}^2,$$

$$\sum_{k=1}^{M_2} v_k^2 \geq \left(1 - \epsilon^{1/4}\right) \cdot M_2, \tag{29}$$

$$\|\mathbf{x}_k^2 - \mathbf{x}_{k'}^2 + h_{21}\left(\mathbf{x}_i^1 - \mathbf{x}_{i'}^1\right)\| \geq 2(1+2\nu)\eta\sqrt{n}\cdot v_{ki}^2, \quad k,k' \in \mathcal{M}^2, i,i' \in \mathcal{M}^1, \tag{30}$$

$$v_i^1,\, v_k^2,\, v_{ik}^1,\, v_{iki'k't}^1,\, v_{ik}^2,\, v_{ikt}^1,\, v_{ikt}^2,\, v_{iki'k't}^2 \in \{0,1\}, \quad \forall i,k,t. \tag{31}$$

3. *If feasible, then declare* (R_1, R_2) *as achievable and use the resulting codewords to transmit messages.*

Constraints (17) impose power constraints on the codewords, and Constraints (18), (19) implement the cardinality constraints (15) and (16). Constraints (20) implement the decoding constraints (10), and Constraints (21-26) implement the counting constraints (12-14) that ensure that the probability of error is constrained.
The corresponding constraints for User 2 are defined in the same manner. We next present the *Decoding Algorithm* 2.

Algorithm 2. ***Decoding Algorithm for two-user Interference Channel***
Input: *Received codewords* $\mathbf{y^1}$, $\mathbf{y^2}$, ***Output:*** *Messages* i_1^*, i_2^*.
Algorithm: *Solve*

$$\begin{aligned} i_1^* &= \arg\max_{i\in\mathcal{M}^1} |\mathscr{B}_i^1|, \ \textit{where } \mathscr{B}_i^1 = \left\{k \in \mathcal{M}^2 \,\middle|\, \|\mathbf{y}^1 - (\mathbf{x}_i^1 + h_{12}\mathbf{x}_k^2)\|^2 \leq M_0^2 + 2\delta_1\right\}, \\ i_2^* &= \arg\max_{i\in\mathcal{M}^2} |\mathscr{B}_i^2|, \ \textit{where } \mathscr{B}_i^2 = \left\{k \in \mathcal{M}^1 \,\middle|\, \|\mathbf{y}^2 - (\mathbf{x}_i^2 + h_{21}\mathbf{x}_k^1)\|^2 \leq M_0^2 + 2\delta_2\right\}. \end{aligned} \tag{32}$$

We next reformulate the feasibility problem (17-27) that involves non-convex quadratic inequalities into a problem of minimizing the rank($\mathbf{Y}$) subject to linear constraints in $\mathbf{Y}$ and $\mathbf{Y} \succeq \mathbf{0}$. Let $\mathbf{y} = (1, \mathbf{x}_i^1, \mathbf{x}_k^2, v_i^1,\, v_k^2,\, v_{ik}^1,\, v_{ik}^2,\, v_{iki'k't}^1,\, v_{iki'k't}^2)$ be the concatenation in a single vector of all the decisions variables in the feasibility problem (17-27). Letting $\mathbf{Y} = \mathbf{y}\mathbf{y}'$, note that rank($\mathbf{Y}$) $= 1$ and $\mathbf{Y} \succeq \mathbf{0}$. We reformulate this feasibility problem (17-27) as the problem of minimizing the rank ($\mathbf{Y}$) subject to linear constraints in $\mathbf{Y}$ and $\mathbf{Y} \succeq 0$.

$$\begin{aligned} r^* = \min \quad & \operatorname{rank}(\mathbf{Y}) \\ \text{s.t.} \quad & \mathbf{A}_i^1 \bullet \mathbf{Y} \leq 0, && \forall i \in \mathcal{M}^1, \\ & \mathbf{B}_{iki'k't}^1 \bullet \mathbf{Y} \leq 0, && \forall t \in \mathcal{T},\, \forall i,i' \in \mathcal{M}^1, k,k' \in \mathcal{M}^2, \\ & \mathbf{C}_i^1 \bullet \mathbf{Y} \leq 0, && \forall i \in \mathcal{M}^1, \\ & \mathbf{D}_{it}^1 \bullet \mathbf{Y} = 0, && \forall i \in \mathcal{M}^1, t \in \mathcal{T}, \\ & \mathbf{E}_{ik}^1 \bullet \mathbf{Y} = 0, && \forall i, k \neq i \in \mathcal{M}^1, \\ & \mathbf{A}_k^2 \bullet \mathbf{Y} \leq 0, && \forall k \in \mathcal{M}^2, \\ & \mathbf{B}_{iki'k't}^2 \bullet \mathbf{Y} \leq 0, && \forall t \in \mathcal{T},\, \forall i,i' \in \mathcal{M}^1, k,k' \in \mathcal{M}^2, \\ & \mathbf{C}_k^2 \bullet \mathbf{Y} \leq 0, && \forall k \in \mathcal{M}^2, \\ & \mathbf{D}_{kt}^2 \bullet \mathbf{Y} = 0, && \forall k \in \mathcal{M}^2, t \in \mathcal{T}, \\ & \mathbf{E}_{ik}^2 \bullet \mathbf{Y} = 0, && \forall i, k \neq i \in \mathcal{M}^2, \\ & \mathbf{Y} \succeq \mathbf{0}, \end{aligned} \tag{33}$$

where $\mathbf{A}_i^1$, $\mathbf{B}_{iki'k't}^1$, $\mathbf{C}_i^1$, $\mathbf{D}_{it}^1$, $\mathbf{E}_{ik}^1$, $\mathbf{A}_k^2$, $\mathbf{B}_{iki'k't}^2$, $\mathbf{C}_k^2$, and $\mathbf{D}_{kt}^2$, $\mathbf{E}_{ik}^2$ are presented in Appendix A. We then use this resulting rank minimization problem with semidefinite constraints in Algorithm 3 to compute the optimal code.

Algorithm 3. ***Capacity Computation and Optimal Coding for the Two-User Interference Channel***

Input: R_1, R_2, P_1, P_2, σ, n, ϵ, ν.

Output: *Rank* r^*, *codewords* $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$,$\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$, *and auxiliary binary variables* v_i^1, v_k^2, v_{ik}^1, v_{ik}^2, $v_{iki'k't}^1$, $v_{iki'k't}^2$.

Algorithm:

1. *Solve the rank minimization semidefinite optimization problem (33) to compute* r^*, *codewords* $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$, *and auxiliary binary variables* v_i^1,v_k^2,v_{ik}^1,v_{ik}^2,$v_{iki'k't}^1$,$v_{iki'k't}^2$.

2. *If* $r^*=1$, *then declare* $(R_1,R_2)\in\mathcal{R}_n^{IC}\left[\alpha_1^2P_1,\alpha_2^2P_2,\frac{h_{12}}{\alpha_2},\frac{h_{21}}{\alpha_1},\sigma,3\epsilon^{\frac{1}{4}}\right]$, *that is, declare* (R_1,R_2) *as achievable using the codebooks* $\mathcal{B}^1=\{\alpha_1\mathbf{x}_i^1\}_{i=1}^{M_1}$, $\mathcal{B}^2=\{\alpha_2\mathbf{x}_k^2\}_{k=1}^{M_2}$ *and the decoding functions (32), achieving an average decoding error probability of* $3\epsilon^{\frac{1}{4}}$ *on a Gaussian interference channel with noise standard deviation* σ *and interference parameters* $\frac{h_{12}}{\alpha_2},\frac{h_{21}}{\alpha_1}$.

3. *If* $r^*\geq 2$, *then declare that* (R_1,R_2) *cannot be achieved on a Gaussian interference channel with noise standard deviation* $(1+3\nu)\sigma$ *with probability of error less than or equal to* $\bar{\epsilon}$, *where*

$$\bar{\epsilon}=\epsilon\cdot\left(1-\delta\left(\nu,n\right)\right)^4, \tag{34}$$

where

$$\delta\left(\nu,n\right)=\exp\left(-n\cdot\frac{r-\log\left(1+r\right)}{2\left(1+3\nu\right)^2\sigma^2}\right),\ \textit{with}\ r=\sigma^2\left(\left(1+3\nu\right)^2-\left(1+2\nu\right)^2\right).$$

That is,

$$\textit{If}\ r^*\geq 2,\ \textit{then declare that}\ (R_1,R_2)\notin\mathcal{R}_n^{IC}\left[P_1,P_2,h_{12},h_{21},\left(1+3\nu\right)\sigma,\bar{\epsilon}\right],$$

where $\bar{\epsilon}$ *is defined as in Eq. (34).*

We next present the main result of this paper.

Theorem 1. ***(Capacity Region in a Two User Gaussian Interference Channel)*** *Let* $\mathcal{R}_n^{IC}\left[P_1,P_2,h_{12},h_{21},\sigma,\epsilon\right]$ *be the set of all rate pairs* (R_1,R_2) *that can be transmitted by two users with powers* (P_1,P_2), *on a two-user Gaussian interference channel with noise with standard deviation* σ *and interference parameters* (h_{12},h_{21}) *with a maximum decoding error probability of* ϵ. *Consider the optimization problem (33) constructed for parameters* $n,P_1,P_2,h_{12},h_{21},\sigma,\epsilon$ *and let* r^* *and* $\{\mathbf{x}_i\}_{i\in\mathcal{M}}$ *be an optimal solution, then*

(a) *If* $r^*=1$, *then* $(R_1,R_2)\in\mathcal{R}_n^{IC}\left[\alpha_1^2P_1,\alpha_2^2P_2,\frac{h_{12}}{\alpha_2},\frac{h_{21}}{\alpha_1},\sigma,3\epsilon^{\frac{1}{4}}\right]$, *with* α_1,α_2 *defined in (9). That is,* (R_1,R_2) *is achievable using the codebooks* $\mathcal{B}^1=\{\alpha_1\mathbf{x}_i^1\}_{i=1}^{M_1}$, $\mathcal{B}^2=\{\alpha_2\mathbf{x}_k^2\}_{k=1}^{M_2}$ *and the decoding functions (32), achieving an average decoding error probability of* $3\epsilon^{\frac{1}{4}}$ *on a Gaussian interference channel with noise standard deviation* σ *and interference parameters* $\frac{h_{12}}{\alpha_2},\frac{h_{21}}{\alpha_1}$.

(b) *If* $r^*\geq 2$, *then* $(R_1,R_2)\notin\mathcal{R}_n^{IC}\left[P_1,P_2,h_{12},h_{21},\left(1+3\nu\right)\sigma,\bar{\epsilon}\right]$, *where* $\bar{\epsilon}$ *is defined as in Eq. (34).*

Discussion

Theorem 1 allows us to compute lower and upper bounds in the following way. Let ϵ_1,ϵ_2 be given by

$$\begin{aligned}\epsilon_1 &= (\epsilon/3)^4,\\ \epsilon_2 &= \epsilon/\left(1-\delta(\nu,n)\right)^4.\end{aligned}$$

Then, Part (a) of Theorem 1 indicates that for an interference channel with parameters

$$\left(n, \epsilon_1, P_1/\alpha_1^2, P_2/\alpha_2^2, \sigma, \alpha_2 h_{12}, \alpha_1 h_{21}, \nu, R_1, R_2\right),$$

if $r^* = 1$, then the rate pair (R_1, R_2) is achievable, and thus such a rate pair (R_1, R_2) provides an lower bound of the capacity $\mathcal{R}_n^{IC}[P_1, P_2, h_{12}, h_{21}, \sigma, \epsilon]$.
Part (b) of Theorem 1 indicates that for an interference channel with parameters

$$(n, \epsilon_2, P_1, P_2, \sigma/(1+3\nu), h_{12}, h_{21}, \nu, R_1, R_2),$$

if $r^* \geq 2$, then the rate pair (R_1, R_2) is not achievable, and thus such a rate pair (R_1, R_2) provides an upper bound on the capacity $\mathcal{R}_n^{IC}[P_1, P_2, h_{12}, h_{21}, \sigma, \epsilon]$.
In this way, Algorithm 3 provides upper and lower bounds for the capacity of a two user Gaussian Interference channel for finite n. In the limit of $\nu, \epsilon \to 0$ and $n \to \infty$ the lower and upper bounds are tight. So, in principle our approach provides valid upper and lower bounds. In numerical implementations, however, we do not solve problem (33) to provable optimality due to its size and complexity. When we find $r^* = 1$, we still provide a valid lower bound on channel capacity, but when we report $r^* \geq 2$, we do not have a guarantee as we have not solved problem (33) to provable optimality. In this way, the upper bound we report can only be seen as an approximation.

2.2 Proof of Theorem 1

We present the proof of Theorem 1 in this section. Before we proceed, we establish the following notation for this section. We let $\mathscr{E}_{ik}^1[\tilde{\mathbf{z}}]$ denote the indicator variable corresponding to the event that a decoding error occurs when User 1 sends message i and User 2 sends message k on the channel and noise vector $\tilde{\mathbf{z}}$ is realized, that is,

$$\mathscr{E}_{ik}^1[\tilde{\mathbf{z}}] = \mathbf{1}\left\{\exists i' \neq i \,:\, \left|\mathscr{B}_{ik,i'}^1[\tilde{\mathbf{z}}]\right| \geq \left|\mathscr{B}_{ik,i}^1[\tilde{\mathbf{z}}]\right|\right\},$$

where $\mathscr{B}_{ik,i'}^1[\tilde{\mathbf{z}}] = \left\{k' \in \mathcal{B}^2 \,:\, \|(\mathbf{x}_i^1 + h_{12}\mathbf{x}_k^2) - (\mathbf{x}_{i'}^1 + h_{12}\mathbf{x}_{k'}^2) + \tilde{\mathbf{z}}\|^2 \leq M_0^2 + 2\delta_1\right\}$. For ease of exposition, we also let $\mathbf{a}_{ii'} = \mathbf{x}_i^1 - \mathbf{x}_{i'}^1$, $\forall i, i' \in \mathcal{M}^1$, *and* $\mathbf{b}_{kk'} = h_{12}(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2)$, $\forall k, k' \in \mathcal{M}^2$. Let $\mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon) = \left\{\mathbf{z} \,\middle|\, n\sigma^2 - \Gamma_\epsilon \leq \|\mathbf{z}\|^2 \leq n\sigma^2 + \Gamma_\epsilon\right\}$, where Γ_ϵ is chosen such that

$$\mathbb{P}\left[\tilde{\mathbf{z}}_U \notin \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] = \epsilon^{1/4} - \epsilon. \tag{35}$$

Let $\tau(\mathbf{s}) = \arg\min_{t=1,\ldots,T} \|\mathbf{s} - \mathbf{z}_t\|$. We begin by presenting the following propositions which we will use in the proof of Theorem 1.
Proposition 2 will be useful in choosing codewords that have good decoding properties.
Proposition 2. *Consider any sequence of numbers* $\{a_1, a_2, \ldots, a_N\}$ *with* $\sum_{i=1}^N a_i \leq N\alpha$. *Then, for each fraction* $f \in (0,1)$, *there exists a subset* $\mathcal{A} \subseteq \{a_1, a_2, \ldots, a_N\}$ *of size at least* $f \cdot N$ *such that*

$$a_i \leq \alpha \cdot \frac{1}{1-f}, \, \forall i \in \mathcal{A}.$$

In the following result, we consider a rate pair (R_1, R_2) that is declared as achievable by Algorithm 3, providing us optimal codewords $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ and optimal binary solutions v_i^1, v_k^2, v_{ik}^1, v_{ik}^2, $\{v_{ikt}^1, v_{ikt}^2\}_{t\in\mathcal{T}}$ by solving Problem (33). We then obtain the following key result.

Proposition 3. *Consider an interference channel with noise* $\tilde{\boldsymbol{z}}_G^1, \tilde{\boldsymbol{z}}_G^2 \sim N(\mathbf{0}, \sigma \cdot \mathbf{I})$*, power constraints* $\{\alpha_1^2 P_1, \alpha_2^2 P_2\}$*, and interference parameters* $\left\{\frac{h_{12}}{\alpha_2}, \frac{h_{21}}{\alpha_1}\right\}$*. Consider a rate pair* (R_1, R_2) *that is declared as achievable by Algorithm 3, and let* $\{\mathbf{x}_i^1\}_{i \in \mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k \in \mathcal{M}^2}$ *and* v_i^1, v_k^2, v_{ik}^1, v_{ik}^2, $\{v_{ikt}^1, v_{ikt}^2\}_{t \in \mathcal{T}}$ *be the optimal solutions of Problem (33). Let* $i \in \mathcal{M}^1$*, and* $j \in \mathcal{M}^2$ *satisfy* $v_{ik}^1 = 1$*. Suppose user 1 transmits message* i *and user 2 trasnmits message* k *by transmitting the codewords* $\alpha_1 \mathbf{x}_i^1$, $\alpha_2 \mathbf{x}_k^2$*, respectively. And suppose the receiver uses the decoder (32). Then the probability of error is given by*

$$\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\boldsymbol{z}}_G^1\right]\right] \leq \epsilon^{1/4}.$$

The following proposition shows that codes that have good decoding properties with Gaussian noise, also have good decoding properties with uniform noise.

Proposition 4. *Consider two noises* $\tilde{\mathbf{z}}_G \sim N(\mathbf{0}, \sigma \cdot \mathbf{I})$ *and* $\tilde{\mathbf{z}}_U$ *uniformly distributed in the ball* $\mathcal{B}_n(\overline{\sigma}\sqrt{n})$ *with* $\overline{\sigma} < \sigma$*. If* $\mathcal{C}$ *be a code such that* $\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\mathbf{z}}_G\right]\right] \leq \epsilon$, $\forall i \in \mathcal{B}$*, then*

$$\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\mathbf{z}}_U\right]\right] \leq \frac{\epsilon}{1 - \exp(-n\beta)}, \text{ with } \beta = \frac{\sigma^2 - \overline{\sigma}^2 - \log(1 + \sigma^2 - \overline{\sigma}^2)}{2\sigma^2}.$$

We next reproduce the following result from Wyner [1967].

Proposition 5 (Wyner [1967])**.** *Let* $\mathcal{A} = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N\}$ *be a Voronoi tessellation on* $\mathcal{S}_n(\gamma)$*. Then,* $\forall \mathbf{s} \in \mathcal{S}_n(\gamma)$, $\exists \mathbf{a}_i \in \mathcal{A}$ *such that* $\|\mathbf{s} - \mathbf{a}_i\| \leq \gamma / N^{1/n}$.

We also reproduce the following result from Bandi and Bertsimas [2015].

Proposition 6 (Cover and Thomas [2006])**.** *Let* $\tilde{\mathbf{z}}_G \sim N(\mathbf{0}, \sigma \cdot \mathbf{I})$.

(a) (Bernstein's inequality) *The vectors* $\tilde{\mathbf{z}}_G$ *are concentrated in a thin shell of radius* $\sigma\sqrt{n}$*, that is,*

$$\mathbb{P}\left[\frac{1}{n}\|\tilde{\mathbf{z}}_G\|^2 > \sigma^2 - r\right] \geq 1 - \exp\left(-n \cdot \frac{r - \log(1 + r)}{2\sigma^2}\right).$$

(b) (Spherical symmetry) *The random vector* $\tilde{\boldsymbol{u}} = \tilde{\mathbf{z}}_G / \|\tilde{\mathbf{z}}_G\|$ *is distributed uniformly in* $\mathcal{S}_n(1)$.

(c) *Let* $\tilde{d}$ *be a random variable distributed identically to the norm of* $\tilde{\mathbf{z}}_G$*, that is,* $\tilde{d} \sim \|\tilde{\mathbf{z}}_G\|$*. Then,* $\tilde{\mathbf{z}}_G \sim \tilde{d} \cdot \tilde{\mathbf{s}}_n(1)$.

All the proofs are presented in Appendix B. We next present the proof of Theorem 1.

Proof of Theorem 1.
In Part (a), we have $r^* = 1$ and therefore, we compute the codewords $\{\mathbf{x}_i^1, \mathbf{x}_k^2\}$ and binary variables v_i^1, v_k^2, v_{ik}^1, v_{ik}^2, $\{v_{ikt}^1, v_{ikt}^2\}_{t \in \mathcal{T}}$. We then transmit the codewords $\{\alpha_1 \mathbf{x}_i^1\}_{i \in \mathcal{M}^1}$, $\{\alpha_2 \mathbf{x}_k^2\}_{k \in \mathcal{M}^2}$ on the channel with noise $\tilde{\boldsymbol{z}}_G^1, \tilde{\boldsymbol{z}}_G^2 \sim N(\mathbf{0}, \sigma \cdot \mathbf{I})$, power constraints $\{\alpha_1^2 P_1, \alpha_2^2 P_2\}$, and interference parameters $\left\{\frac{h_{12}}{\alpha_2}, \frac{h_{21}}{\alpha_1}\right\}$, and use the decoder defined by Eq. (32). We then show that the probability of error is bounded by $3\epsilon^{1/4}$.
In Part (b), when $r^* = 2$, we cannot compute feasible codewords $\{\mathbf{x}_i^1, \mathbf{x}_k^2\}$, and we then show that rate pair (R_1, R_2) cannot be achieved on a channel with noise standard deviation $(1 + 3\nu)\sigma$ achieving an error probability $\bar{\epsilon}$ given by Eq. (34). We prove this by proving its contra-positive. That is we show that if the rate pair (R_1, R_2) could be achieved on a channel with noise standard deviation $(1+3\nu)\sigma$ achieving an error probability $\bar{\epsilon}$, then it would have been accepted by Algorithm

3. In order to show this, we show any code achieving the rate pair (R_1, R_2) satisfies the constraints (17)–(31) of the optimization problem (33).

Proof of Part(a)
In Part(a), we have $r^* = 1$, and we can compute the codewords $\{\mathbf{x}_i^1,\ \mathbf{x}_k^2\}$ and binary variables v_i^1, v_k^2, v_{ik}^1, v_{ik}^2, $\{v_{ikt}^1,\, v_{ikt}^2\}_{t\in\mathcal{T}}$. Next, consider all messages $i \in \mathcal{M}^1$, and $j \in \mathcal{M}^2$ such that the value of the binary variable v_{ik}^1 in the optimal solution has the property that $v_{ik}^1 = 1$. For these messages we show in Proposition 3 that when user 1 transmits $\alpha_1\mathbf{x}_i^1$ and user 2 transmits $\alpha_2\mathbf{x}_k^2$, the error probability is bounded by

$$\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\boldsymbol{z}}_G^1\right]\right] \leq \epsilon^{1/4}. \tag{36}$$

By averaging this error probability over all messages $k \in \mathcal{M}^2$, we obtain the average probability of the incorrectly decoding message i trasnmitted by user 1 is given by

$$\begin{aligned}
\mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] &= \frac{1}{M_2}\sum_{k=1}^{M_2}\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\boldsymbol{z}}_G^1\right]\right] \\
&= \frac{1}{M_2}\left(\sum_{k:v_{ik}^1=1}\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\boldsymbol{z}}_G^1\right]\right] + \sum_{k:v_{ik}^1=0}\mathbb{P}\left[\mathscr{E}_{ik}^1\left[\tilde{\boldsymbol{z}}_G^1\right]\right]\right) \\
\text{(from (36))} \quad &\leq \frac{1}{M_2}\left(\left|\left\{k : v_{ik}^1 = 1\right\}\right| \cdot \left(\epsilon^{1/4}\right) + \left|\left\{k : v_{ik}^1 = 0\right\}\right| \cdot 1\right) \\
\text{(from (25))} \quad &\leq \frac{1}{M_2}\left(M_2 \cdot \left(\epsilon^{1/4}\right) + \left(1 - \left(1 - \epsilon^{\frac{1}{4}}\right)\right) \cdot M_2 \cdot 1\right) \\
&= 2\epsilon^{\frac{1}{4}},
\end{aligned}$$

where $|\mathcal{S}|$ refers to the cardinality of any set $\mathcal{S}$. Next, the average decoding error probability of the code is given by

$$\begin{aligned}
\mathbb{P}_{\text{avg}} &= \frac{1}{M_1}\sum_{i=1}^{M_1}\mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] \\
&= \frac{1}{M_1}\left(\sum_{i:v_i^1=1}\mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] + \sum_{i:v_i^1=0}\mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \neq i | m^1 = i\right]\right) \\
&\leq \frac{1}{M_1}\left(\left|\left\{i : v_i^1 = 1\right\}\right| \cdot \left(2\epsilon^{\frac{1}{4}}\right) + \left|\left\{i : v_i^1 = 0\right\}\right| \cdot 1\right) \\
\text{(from (26))} \quad &\leq \frac{1}{M_1}\left(M_1 \cdot \left(2\epsilon^{\frac{1}{4}}\right) + \left(1 - \left(1 - \epsilon^{\frac{1}{4}}\right)\right) \cdot M_1 \cdot 1\right) \\
&= 3\epsilon^{\frac{1}{4}}.
\end{aligned}$$

Therefore, we have shown that, using the codewords $\{\alpha_1\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$ and $\{\alpha_2\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$, we can transmit messages at rates (R_1, R_2) with error probability less than $3\epsilon^{\frac{1}{4}}$ on a channel with noise standard deviation σ, interference parameters $(h_{12}/\alpha_2, h_{21}/\alpha_1)$ and power constraints $(\alpha_1^2 P_1, \alpha_2^2 P_2)$. That is, $(R_1, R_2) \in \mathcal{R}_n^{\text{IC}}\left[\alpha_1^2 P_1, \alpha_2^2 P_2, \frac{h_{12}}{\alpha_2}, \frac{h_{21}}{\alpha_1}, \sigma, 3\epsilon^{\frac{1}{4}}\right]$. This concludes the proof of Part (a).

(b) To prove Part(b), we prove its contra-positive, that is, we will show that if the rate pair (R_1, R_2) can be transmitted on a two user interference channel with parameters $(P_1, P_2, h_{12}, h_{21}, (1+3\nu)\,\sigma)$

with error probability less than $\overline{\epsilon}$, then any such code will satisfy the constraints (17)–(31) of the optimization problem (33).

That is, we show that if the rate pair $(R_1, R_2) \in \mathcal{R}_n^{\mathrm{IC}}\left[P_1, P_2, h_{12}, h_{21}, (1+3\nu)\,\sigma, \overline{\epsilon}\right]$, then there exists codebooks $\mathcal{B}^1, \mathcal{B}^2$ that satisfy the constraints (17)–(31) of the optimization problem (33), which implies that $r^* = 1$. Consider a rate pair $(R_1, R_2) \in \mathcal{R}_n^{\mathrm{IC}}\left[P_1, P_2, h_{12}, h_{21}, (1+3\nu)\,\sigma, \overline{\epsilon}\right]$, and let

$$\mathcal{B}^1 = \left\{\mathbf{x}_i^1\right\}_{i\in\mathcal{M}^1} \text{ and } \mathcal{B}^2 = \left\{\mathbf{x}_k^2\right\}_{k\in\mathcal{M}^2}$$

be the codebooks and let $g(\cdot)$ be the decoding function that achieves this average error-probability of $\overline{\epsilon}$, that is,

$$\frac{1}{M_1}\sum_{i=1}^{M_1}\mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] \leq \overline{\epsilon}, \qquad \frac{1}{M_2}\sum_{k=1}^{M_2}\mathbb{P}\left[g\left(\mathbf{y}^2\right) \neq k | m^2 = k\right] \leq \overline{\epsilon}.$$

In what follows, we restrict ourselves to the analysis of User 1 and show that the codewords satisfy the constraints (17)–(31) of the optimization problem (33). And we let m^1 and m^2 denote the messages sent by users 1 and 2, respectively.

We achieve this in the following steps:

Step 1. We show that the codewords satisfy Eqs. (24–26). To do this, we show that there exists a subset $\mathcal{F}_1 \in \mathcal{B}^1$ of user 1's codewords with size at least $\left(1-\epsilon^{\frac{1}{4}}\right)M_1$ and a subset of user 2's codewords $\mathcal{B}_i^{1,2} \subseteq \mathcal{B}^2$ with size at least $\left(1-\epsilon^{\frac{1}{4}}\right)M_2$ such that

$$\mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i,\, m^2 = k\right] \leq \overline{\epsilon}^{\frac{1}{2}},\ \forall k \in \mathcal{B}_i^{1,2},\ \forall i \in \mathcal{F}_1.$$

This step allows us to set the values of binary variables $v_i^1, v_{ik}^1, v_k^2, v_{ki}^2$, for all $i \in \mathcal{M}^1,\ k \in \mathcal{M}^2$.

Step 2. We show that the codewords satisfy the set of constraints (27).

Step 3. We show that the codewords satisfy the remaining set of constraints (18–23).

Proof of Step 1. Applying Proposition 2 with

$$f = 1-\epsilon^{\frac{1}{4}},\ N = M_1,\ \alpha = \overline{\epsilon}, \text{ and } a_i = \mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i\right],\ \forall i \in \mathcal{M}^1,$$

we obtain that there exists a subset of codewords $\mathcal{F}^1 \subseteq \mathcal{B}^1$ such that

$$\mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] \leq \frac{\overline{\epsilon}}{1-\left(1-\epsilon^{\frac{1}{4}}\right)} \leq \overline{\epsilon}^{\frac{3}{4}},\ \forall i \in \mathcal{F}^1, \text{ and } \left|\mathcal{F}^1\right| \geq \left(1-\epsilon^{\frac{1}{4}}\right)M_1. \tag{37}$$

Assign $v_i^1 = 1,\ \forall i \in \mathcal{F}_1$, and assign zero otherwise. Fixing some $i \in \mathcal{F}^1$, we have

$$\mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] = \frac{1}{M_2}\sum_{k=1}^{M_2}\mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i,\, m^2 = k\right] \leq \overline{\epsilon}^{\frac{3}{4}}.$$

Applying Proposition 2 with

$$f = 1-\epsilon^{\frac{1}{4}},\ N = M_2,\ \alpha = \overline{\epsilon}^{\frac{3}{4}}, \text{ and } a_k = \mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i,\, m^2 = k\right],\ \forall k \in \mathcal{M}^2,$$

we obtain that there exists a subset of codewords $\mathcal{B}_i^{1,2} \subseteq \mathcal{B}^2$ such that

$$\begin{gathered}\mathbb{P}\left[g\left(\mathbf{y}^1\right) \neq i | m^1 = i,\, m^2 = k\right] \leq \frac{\overline{\epsilon}^{\frac{3}{4}}}{1-\left(1-\epsilon^{\frac{1}{4}}\right)} \leq \overline{\epsilon}^{\frac{1}{2}},\quad \forall k \in \mathcal{B}_i^{1,2},\\ \left|\mathcal{B}_i^{1,2}\right| \geq \left(1-\epsilon^{\frac{1}{4}}\right)M_2.\end{gathered} \tag{38}$$

Using this assign $v_{ik}^1 = 1,\ \forall k \in \mathcal{B}_i^{1,2},\ \forall i \in \mathcal{F}_1$, else assign $v_{ik}^1 = 0$.

Proof of Step 2. From Step 1, we have that User 1 is able to use $g(\cdot)$ to decode $\mathbf{y}^1 = \mathbf{x}_i^1 + h_{12}\mathbf{x}_k^2 + \tilde{\mathbf{z}}_G^1$ correctly as message i with probability at least $1 - \overline{\epsilon}^{\frac{1}{2}}$. Now consider a single-user Gaussian channel, call it A, with noise $\tilde{\mathbf{z}}_G^1 \sim N(\mathbf{0}, (1+2\nu)\sigma\mathbf{I})$. Consider a code for channel A with codebook $\mathbb{V}$ given by

$$\mathbb{V} = \left\{ \mathbf{v}_{ik_i} = \mathbf{x}_i^1 + h_{12}\mathbf{x}_{k_i}^2,\ \forall k_i \in \mathcal{B}_i^{1,2},\ \forall i \in \mathcal{F}^1 \right\},$$

with size $\sum_{i \in \mathcal{F}^1} \left| \mathcal{B}_i^{1,2} \right|$. We will next construct a decoding function $\tilde{g}(\cdot) : \mathbb{R}^n \to \mathbb{V}$ for channel A by using the interference channel decoding function $g(\cdot)$ as follows:

$$\tilde{g}\left(\mathbf{y}^1\right) = \mathbf{x}_{g(\mathbf{y}^1)}^1 + h_{12}\mathbf{x}_{h(\mathbf{y}^1)}^2,$$

where

$$h\left(\mathbf{y}^1\right) = \arg \min_{k \in \mathcal{B}_{g(\mathbf{y}^1)}^{1,2}} \left\| \mathbf{y}^1 - \left(\mathbf{x}_{g(\mathbf{y}^1)}^1 + h_{12}\mathbf{x}_k^2 \right) \right\|.$$

In words, $\tilde{g}(\cdot)$ computes the message index m^1 by using $g(\cdot)$ and chooses the message index m^2 by using a minimum distance criterion. Observe that we have the following property that $\tilde{g}(\cdot)$ satisfies:

$$g\left(\mathbf{y}^1\right) = i \iff \tilde{g}\left(\mathbf{y}^1\right) \in \mathbb{V}_i, \text{ where } \mathbb{V}_i = \bigcup_{k' \in \mathcal{B}_i^{1,2}} \{\mathbf{v}_{ik'}\}.$$

Therefore, using the codebook $\mathbb{V}$ and the decoding function $\tilde{g}(\cdot)$ on channel A, we have

$$\begin{aligned} \mathbb{P}\left[\tilde{g}\left(\mathbf{v}_{ik} + \tilde{\mathbf{z}}_G^1\right) \in \mathbb{V} \setminus \mathbb{V}_i | \mathbf{v}_{ik} \text{ was sent on A}\right] &= \mathbb{P}\left[g(\mathbf{y}) \neq i | m^1 = i,\, m^2 = k\right], \\ &\leq \overline{\epsilon}^{\frac{1}{2}}, \quad \text{(from (38))} \end{aligned}$$

Furthermore, by taking averages, we have

$$\frac{1}{|\mathbb{V}|} \sum_{\mathbf{v}_{ik} \in \mathbb{V}} \mathbb{P}\left[\tilde{g}\left(\mathbf{v}_{ik} + \tilde{\mathbf{z}}_G^1\right) \in \mathbb{V} \setminus \mathbb{V}_i | \mathbf{v}_{ik} \text{ was sent on A}\right] \leq \overline{\epsilon}^{\frac{1}{2}}, \tag{39}$$

which implies that the decoder $\tilde{g}(\cdot)$ achieves an error probability of less than $\overline{\epsilon}^{1/2}$ on a single-user channel. Therefore, the minimum distance decoder $g_0(\cdot)$, which is the maximum likelihood decoder and hence the optimal decoder for channel A, also satisfies

$$\frac{1}{|\mathbb{V}|} \sum_{\mathbf{v}_{ik} \in \mathbb{V}} \mathbb{P}\left[g_0\left(\mathbf{v}_{ik} + \tilde{\mathbf{z}}_G^1\right) \in \mathbb{V} \setminus \mathbb{V}_i | \mathbf{v}_{ik} \text{ was sent on A}\right] \leq \overline{\epsilon}^{\frac{1}{2}}. \tag{40}$$

Applying Proposition 2 with

$$f = 1 - \epsilon^{\frac{1}{4}},\ N = |\mathbb{V}|,\ \alpha = \overline{\epsilon}^{\frac{1}{2}},\ a_{ik} = \mathbb{P}\left[g_0\left(\mathbf{v}_{ik} + \tilde{\mathbf{z}}_G^1\right) \in \mathbb{V} \setminus \mathbb{V}_i | \mathbf{v}_{ik} \text{ was sent on A}\right],\ \forall \mathbf{v}_{ik} \in \mathbb{V},$$

we obtain that there exists a subset of vectors $\tilde{\mathbb{V}} \subseteq \mathbb{V}$ such that

$$\begin{aligned} \mathbb{P}\left[g_0\left(\mathbf{v}_{ik} + \tilde{\mathbf{z}}_G^1\right) \in \mathbb{V} \setminus \mathbb{V}_i | \mathbf{v}_{ik} \text{ was sent on A}\right] &\leq \frac{\overline{\epsilon}^{\frac{1}{2}}}{1 - \left(1 - \epsilon^{\frac{1}{4}}\right)} \leq \overline{\epsilon}^{\frac{1}{4}}, \quad \forall \mathbf{v}_{ik} \in \tilde{\mathbb{V}}, \\ \left|\tilde{\mathbb{V}}\right| &\geq \left(1 - \epsilon^{\frac{1}{4}}\right) |\mathbb{V}|. \end{aligned} \tag{41}$$

We now show that (41) implies that the quantity $\|\mathbf{v}_{i'k'} - \mathbf{v}_{ik}\|$ is lower bounded. Consider the probability of incorrectly decoding $\mathbf{v}_{ik}$ as $\mathbf{v}_{i'k'}$ on channel A, we have

$$\begin{aligned}
\mathbb{P}\left[\mathbf{v}_{ik} \text{ decoded as } \mathbf{v}_{i'k'}\right] &\geq \mathbb{P}\left[\left\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'} + \tilde{\mathbf{z}}_G^1\right\| \leq \left\|\tilde{\mathbf{z}}_G^1\right\|\right] \\
&= \mathbb{P}\left[\frac{\langle \mathbf{v}_{ik} - \mathbf{v}_{i'k'}, \tilde{\mathbf{z}}_G^1 \rangle}{(1+2\nu)\,\sigma\,\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'}\|} \geq \frac{\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'}\|}{2\,(1+2\nu)\,\sigma}\right] \\
&= 1 - \Phi\left(\frac{\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'}\|}{2\,(1+2\nu)\,\sigma}\right).
\end{aligned}$$

Since we know that $\mathbb{P}\left[\mathbf{v}_{ik} \text{ decoded as } \mathbf{v}_{i'k'}\right] \leq \overline{\epsilon}^{\frac{1}{4}}$, we have

$$\begin{aligned}
&\mathbb{P}\left[\mathbf{v}_{ik} \text{ decoded as } \mathbf{v}_{i'k'}\right] \leq \epsilon^{\frac{1}{4}} \\
\implies &\epsilon^{\frac{1}{4}} \geq 1 - \Phi\left(\frac{\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'}\|}{2\,(1+2\nu)\,\sigma}\right) \\
\implies &\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'}\| \geq 2\,(1+2\nu)\,\sigma\Phi^{-1}\left(1 - \epsilon^{\frac{1}{4}}\right) \\
\implies &\|\mathbf{v}_{ik} - \mathbf{v}_{i'k'}\| \geq 2\sqrt{n}\,(1+2\nu)\,\eta, \qquad (42)
\end{aligned}$$

which implies that the codewords satisfy the constraints (27).

Proof of Step 3. We next show that remaining constraints (18–23) are also satisfied. We begin by comparing the performance of the codes $\mathcal{B}^1, \mathcal{B}^2$ when the noise is uniform. We choose uniform distribution because the optimal decoder for uniform noise takes a simpler form as shown in Proposition 1. In particular, we consider the uniform noise $\tilde{\mathbf{z}}_U^1$ to be uniformly distributed in the ball $\mathcal{B}^n\left(\sigma_1\sqrt{n}\right)$, where

$$\sigma_1\sqrt{n} = \sqrt{n\sigma^2 + \Gamma_\epsilon} < (1+3\nu)\,\sigma\sqrt{n}.$$

In order to evaluate the probability of error under this uniform noise, we apply Proposition 4 and obtain

$$\mathbb{P}\left[\mathscr{O}_{ik}^1\left[\tilde{\boldsymbol{z}}_U\right]\right] \leq \frac{\mathbb{P}\left[\mathscr{O}_{ik}^1\left[\tilde{\boldsymbol{z}}_G\right]\right]}{1 - \delta\left(\nu, n\right)} \leq \frac{\overline{\epsilon}^{1/4}}{1 - \delta\left(\nu, n\right)} = \epsilon^{1/4}. \qquad (43)$$

Now let $\tilde{\mathbf{z}}_D$ be a discrete uniform distribution given by $\mathbb{P}\left[\tilde{\mathbf{z}}_D = \mathbf{z}_t\right] = \frac{1}{T},\ \forall t = 1, \ldots, T$, where the set of vectors

$$\mathcal{Z} = \{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_T\}$$

are computed as in Bandi and Bertsimas [2015], and satisfy $\|\mathbf{z}_t\| = M_0,\ t = 1, \ldots, T$ (See Eqs. (5–7)). From Consider $\tilde{\mathbf{z}} \in \mathcal{U}_\epsilon\left(\sigma, \Gamma_\epsilon\right)$ and let $\tau\left(\tilde{\mathbf{z}}\right) = t$. We have

$$\|\tilde{\mathbf{z}} - \mathbf{z}_t\| \leq \theta\sqrt{n} + 2\Gamma_\epsilon, \text{ with } \theta = \frac{\eta\nu}{1+\nu}.$$

Suppose that $v_{ikt}^1 = 0$, then

$$\begin{aligned}
\exists i' \in \mathcal{M}^1, i' \neq i \text{ such that } &\left|\left\{k' \in \mathcal{B}^2 \,:\, \|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 - \delta_1}\right\}\right| \\
&\geq \left|\left\{k' \in \mathcal{B}^2 \,:\, \|\mathbf{b}_{kk'} + \mathbf{z}_t\|^2 \leq \sqrt{M_0^2 + \delta_1}\right\}\right|. \qquad (44)
\end{aligned}$$

Then, we obtain the following:
(a) For $k' \in \mathcal{B}^2$ such that $\|\mathbf{b}_{kk'} + \mathbf{z}_t\| \geq \sqrt{M_0^2 + \delta_1}$,

$$\begin{aligned}\left\|\mathbf{x}_i^1 - \mathbf{x}_i^1 + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| &= \|\mathbf{b}_{kk'} + \tilde{\mathbf{z}}\| \\ &\geq \|\mathbf{b}_{kk'} + \mathbf{z}_t\| - \|\tilde{\mathbf{z}} - \mathbf{z}_t\| \\ &\geq \sqrt{M_0^2 + \delta_1} - \left(\theta\sqrt{n} + 2\Gamma_\epsilon\right) \\ &\geq M_0 \ \text{ (by the choice of } \delta_1). \end{aligned} \tag{45}$$

(b) For $k' \in \mathcal{B}^2$ such that $\|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 - \delta_1}$,

$$\begin{aligned}&\left\|\mathbf{x}_i^1 - \mathbf{x}_{i'}^1 + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \\ &\quad\leq \left\|\mathbf{x}_i^1 - \mathbf{x}_{i'}^1 + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \mathbf{z}_t\right\| + \|\tilde{\mathbf{z}} - \mathbf{z}_t\| \\ &\quad\leq \sqrt{M_0^2 - \delta_1} + \theta\sqrt{n} + 2\Gamma_\epsilon \\ &\quad\leq M_0 \ \text{ (by the choice of } \delta_1). \end{aligned} \tag{46}$$

Next we show that from (45) and (46), we obtain that $\forall \tilde{\mathbf{z}}$ with $\tau(\tilde{\mathbf{z}}) = t$, and $v_{ikt}^1 = 0$

$$\begin{aligned}\exists i' \in \mathcal{M}^1, i' \neq i \text{ such that } &\left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|\mathbf{x}_i^1 - \mathbf{x}_{i'}^1 + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \leq M_0\right\}\right| \\ &\geq \left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \leq M_0\right\}\right|. \end{aligned} \tag{47}$$

To show this, fix i, i', k, t with $v_{ikt}^1 = 1$, and let

$$\begin{aligned}\mathscr{A} &= \left\{k' \in \mathcal{B}^2 \,\middle|\, \|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 - \delta_1}\right\}, \\ \mathscr{B} &= \left\{k' \in \mathcal{B}^2 \,\middle|\, \|\mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 + \delta_1}\right\}, \\ \hat{\mathscr{A}} &= \left\{k' \in \mathcal{B}^2 \,|\, \|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \tilde{\mathbf{z}}\| \leq M_0\right\}, \\ \hat{\mathscr{B}} &= \left\{k' \in \mathcal{B}^2 \,|\, \|\mathbf{b}_{kk'} + \tilde{\mathbf{z}}\| \leq M_0\right\}. \end{aligned}$$

In this notation, from (44) implies that $|\mathscr{A}| \geq |\mathscr{B}|$. In (45), we have shown that $\mathscr{B}^C \subseteq \hat{\mathscr{B}}^C$, implying that $|\mathscr{B}| \geq \left|\hat{\mathscr{B}}\right|$. In (46), we have shown that $\mathscr{A} \subseteq \hat{\mathscr{A}}$, implying that $|\mathscr{A}| \leq \left|\hat{\mathscr{A}}\right|$. Therefore,

$$\left|\hat{\mathscr{A}}\right| \geq |\mathscr{A}| \geq |\mathscr{B}| \geq \left|\hat{\mathscr{B}}\right|.$$

Next from (47), we obtain that by using the optimal decoder, we decode incorrectly for all $\tilde{\mathbf{z}} \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)$ with $\tau(\tilde{\mathbf{z}}) = t$. Therefore, we have

$$\left\{v_{ik\tau(\tilde{\boldsymbol{z}}_U)}^1 = 0\right\} \implies \mathscr{E}_{ik}^1[\tilde{\boldsymbol{z}}_U] = 1$$

which implies $\mathbb{P}\left[\mathscr{E}_{ik}^1[\tilde{\boldsymbol{z}}_U] \,\middle|\, \tilde{\mathbf{z}}_U \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] \geq \mathbb{P}\left[v_{ik\tau(\tilde{\boldsymbol{z}}_U)}^1 = 0\right]$ .Next, for each $i \in \mathcal{M}^1$, $k \in \mathcal{M}^2$

$$\mathbb{P}\left[v_{ik\tau(\tilde{\boldsymbol{z}}_U)}^1 = 0\right] = \sum_{t=1}^{T} \mathbb{P}\left[v_{ik\tau(\tilde{\boldsymbol{z}}_U)}^1 = 0 \middle| \tau(\tilde{\boldsymbol{z}}_U) = t\right] \cdot \mathbb{P}\left[\tau(\tilde{\boldsymbol{z}}_U) = t\right]. \tag{48}$$

We have

$$\mathbb{P}\left[v^1_{ik\tau(\tilde{\boldsymbol{z}}_U)}=0\middle|\tau\left(\tilde{\boldsymbol{z}}_U\right)=t\right]=\begin{cases}1, & \text{if } v^1_{ikt}=0,\\ 0, & \text{otherwise,}\end{cases}=1-v^1_{ikt}. \tag{49}$$

Since the set of vectors $\mathcal{Z}$ forms a Voronoi tessellation of $\mathcal{S}_n((1+\nu)\gamma_\epsilon)$, the Voronoi regions of the points $\mathbf{z}_t \in \mathcal{Z}$ are identical with the same area. Moreover, since $\tilde{\mathbf{z}}_U$ is uniform, we know that $\tilde{\mathbf{z}}_U$ induces a uniform distribution for $\tau\left(\tilde{\mathbf{z}}_U\right)$ on the elements of the set $\{1,\ldots,T\}$, that is,

$$\mathbb{P}\left[\tau\left(\tilde{\mathbf{z}}_U\right)=t\right]=\frac{1}{T},\ \forall t=1,\ldots,T. \tag{50}$$

Therefore, we have

$$\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}_U\right]\middle|\tilde{\mathbf{z}}_U\in\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]\geq\mathbb{P}\left[v^1_{ik\tau(\tilde{\boldsymbol{z}}_U)}=0\right]=\frac{1}{T}\sum_{t=1}^{T}\left(1-v^1_{ikt}\right).$$

We next have

$$\begin{aligned}\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}_U\right]\right]&=\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}_U\right]\middle|\tilde{\mathbf{z}}_U\in\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]\cdot\mathbb{P}\left[\tilde{\mathbf{z}}_U\in\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]\\&\qquad+\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}_U\right]\middle|\tilde{\mathbf{z}}_U\notin\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]\cdot\mathbb{P}\left[\tilde{\mathbf{z}}_U\notin\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]\\&\geq\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}_U\right]\middle|\tilde{\mathbf{z}}_U\in\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]+\mathbb{P}\left[\tilde{\mathbf{z}}_U\notin\mathcal{U}_\epsilon\left(\sigma,\Gamma_\epsilon\right)\right]\\\text{From Eq. (35)}\qquad&\geq\frac{1}{T}\sum_{t=1}^{T}\left(1-v^1_{ikt}\right)+(\epsilon^{1/4}-\epsilon).\end{aligned}$$

From Eq. (43), we have

$$\frac{1}{T}\sum_{t=1}^{T}\left(1-v^1_{ikt}\right)\leq\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}_U\right]\right]-(\epsilon^{1/4}-\epsilon)\leq\epsilon.$$

This implies that the codewords satisfy the constraints (18-19). This observation along with the repetition of a similar argument from the point of view of User 2 concludes the proof. □

3 The Multi-access and the Multicast Channels

Multi-access and multicast channels are special cases of the interference channel, where either the receivers cooperate or the senders cooperate, respectively.

3.1 Capacity Region of a Gaussian Multi-access channel (MAC)

This is a channel in which two (or more) senders send information to a common receiver. A common example of this channel is a satellite receiver with many independent ground stations, or a set of cell phones communicating with a base station. As in interference channels, we see that the senders must contend not only with the receiver noise but with interference from each other as

well. Sender k chooses a message $m^k = i_k \in \mathcal{B}^k$ and transmits $\mathbf{x}_{i_k}^k$ over the channel while satisfying $\left\|\mathbf{x}_{i_k}^k\right\|^2 \leq nP_k$. The receiver receives the combined signal

$$\mathbf{y} = \sum_{k=1}^{K} \mathbf{x}_{i_k}^k + \tilde{\mathbf{z}},$$

where $\tilde{\mathbf{z}} \sim N(\mathbf{0}, \sigma \cdot \mathbf{I})$ is Gaussian noise. The receiver is required to decode *all* the K messages from the senders. We let $m^k = i$ denote that sender k transmits message $i \in \mathcal{B}^k$.

We present the special case of a two-user multi-access channel. The channel coding problem for such a channel refers to the problem of constructing a code $\mathcal{C}^{\text{MAC}}[\cdot]$ with inputs $n, R_1, R_2, \sigma, P_1, P_2, \epsilon$. The outputs of $\mathcal{C}^{\text{MAC}}[n, R_1, R_2, P_1, P_2, \sigma, \epsilon]$ are:

1. The codebooks $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i \in \mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k \in \mathcal{M}^2}$;

2. The decoding function $g : \mathbb{R}^n \to \mathcal{B}^1 \times \mathcal{B}^2$ that map each received codeword $\mathbf{y}$ to a pair of codewords in $\mathcal{B}^1$ and $\mathcal{B}^2$, so that the average probability of error satisfies

$$\mathbb{P}\left[g(\mathbf{y}) \neq (i,k) \mid m^1 = i,\, m^2 = k\right] \quad \leq \quad \epsilon, \tag{51}$$

In addition, we define the capacity region of a two-user multicast channel $\mathcal{R}_n^{\text{MAC}}[P_1, P_2, \sigma, \epsilon]$ as the set of all rate pairs (R_1, R_2) such that there exists a code $\mathcal{C}^{\text{MAC}}[n, R_1, R_2, P_1, P_2, \sigma, \epsilon]$.

Capacity Computation and Optimal Coding

Algorithm 4, which we use to characterize the capacity region, while simultaneously constructing the optimal code is based on (a) the *Encoding Algorithm* 4, and (b) the *Decoding Algorithm* 5. A key ingredient in our construction is that the maximum likelihood decoder is the minimum distance decoder for this problem. In particular, we use the following decoder

$$(i^*, k^*) = \arg \min_{i \in \mathcal{B}^1} \min_{k \in \mathcal{B}^2} \left\|\mathbf{y} - (\mathbf{x}_i^1 + \mathbf{x}_k^2)\right\|, \tag{52}$$

The intuition of the *Encoding Algorithm* is as follows. We select codewords $\{\mathbf{x}_i^1\}_{i \in \mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k \in \mathcal{M}^2}$ that represent codewords for Users 1 and 2, respectively. In order to enforce the decoder (52), we would require that

$$\left\|\mathbf{y} - \left(\mathbf{x}_{i^*}^1 + \mathbf{x}_{k^*}^2\right)\right\| \leq \left\|\mathbf{y} - \left(\mathbf{x}_i^1 + \mathbf{x}_k^2\right)\right\|, \forall i \in \mathcal{M}^1, k \in \mathcal{M}^2.$$

Using this decoder, we want to ensure that the average probability of error is at most $\epsilon^{1/2}$, that is,

$$\frac{1}{M_1 M_2} \sum_{i \in \mathcal{M}^1, k \in \mathcal{M}^2} \mathbb{P}\left[g(\mathbf{y}) \neq (i,k) \,\middle|\, m^1 = i, m^2 = k\right] \leq \epsilon^{1/2}. \tag{53}$$

In order to achieve this, we define the following "counting" variables $\{v_{ikt}\}_{t \in \mathcal{T}}$ defined as

$$v_{ikt} = \begin{cases} 1, & \text{if } \left\|(\mathbf{x}_i^1 + \mathbf{x}_k^2) - (\mathbf{x}_{i'}^1 + \mathbf{x}_{k'}^2) + \mathbf{z}_t\right\| \geq \left\|\mathbf{z}_t\right\|, \ \forall i' \in \mathcal{M}^1, k' \in \mathcal{M}^2, \\ 0, & \text{otherwise.} \end{cases}$$

We first present the *Encoding Algorithm* 4.

Algorithm 4. ***Encoding Algorithm for two-user Multi-access Channel***
Input: *n, R_1, R_2, σ, P_1, P_2, ϵ, ν.*
Output: *Codewords $\mathbf{x}_i^1$, $\mathbf{x}_k^2$, and binary variables v_{ik}, $\{v_{ikt}\}_{t=1}^T$.*
Algorithm:

1. *Calculate the quantities T, M_0, and the set of equidistant vectors $\mathcal{Z} = \{\mathbf{z}_t\}_{t=1}^T$ using (6), (5) and (7), respectively.*
2. *Check the feasibility of the constraints*

$$\begin{aligned}
\|\mathbf{x}_i^1\|^2 &\le nP_1 && i \in \mathcal{M}^1, \\
\|\mathbf{x}_k^2\|^2 &\le nP_2 && k \in \mathcal{M}^2, \\
\|(\mathbf{x}_i^1 + \mathbf{x}_k^2) - (\mathbf{x}_{i'}^1 + \mathbf{x}_{k'}^2) + \mathbf{z}_t\| + (1 - v_{ikt})\, M_0 &\ge \|\mathbf{z}_t\|, && t \in \mathcal{T},\ \forall i, i' \in \mathcal{M}^1,\ k, k' \in \mathcal{M}^2, \\
\|(\mathbf{x}_i^1 + \mathbf{x}_k^2) - (\mathbf{x}_{i'}^1 + \mathbf{x}_{k'}^2)\| &\ge 2\sigma\Phi^{-1}\left(1 - \epsilon^{\frac{1}{2}}\right), && i, i' \in \mathcal{M}^1,\ k, k' \in \mathcal{M}^2, \\
\sum_{t=1}^{T} v_{ikt} &\ge \left(1 - \epsilon^{\frac{1}{2}}\right) T, && i \in \mathcal{M}^1,\ k \in \mathcal{M}^2, \\
v_{ikt} &\in \{0, 1\}, && i \in \mathcal{M}^1,\ k \in \mathcal{M}^2, t \in \mathcal{T}.
\end{aligned} \tag{54}$$

3. *If feasible, then (R_1, R_2) is achievable and the resulting codewords can be used to transmit messages.*

We next present the *Decoding Algorithm* 5

Algorithm 5. ***Decoding Algorithm for two-user Multi-access Channel***
Input: *Received codeword $\mathbf{y}$.*
Output: *Messages i_1^*, i_2^*.*
Algorithm: *: Solve*

$$(i^*, k^*) = g^{MAC}(\mathbf{y}) = \arg\min_{i \in \mathcal{B}^1} \min_{k \in \mathcal{B}^2} \|\mathbf{y} - (\mathbf{x}_i^1 + \mathbf{x}_k^2)\|, \tag{55}$$

As before, we reformulate this feasibility problem into an equivalent rank-constrained semidefinite optimization problem. Let r^* be the optimal solution value. The overall algorithm is as follows.

Algorithm 6. ***Capacity Computation and Optimal Coding for the Two-User Multi-access Channel***
Input: *R_1, R_2, P_1, P_2, σ, n, ϵ, ν.*
Output: *Rank r^*, codewords$\{\mathbf{x}_i^1\}_{i \in \mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k \in \mathcal{M}^2}$, and auxiliary binary variables $\{v_{ikt}\}_{t=1}^T$.*
Algorithm :

1. *Solve the rank minimization semidefinite optimization problem to compute its optimal solution value r^*.*
2. *If $r^* = 1$, then (R_1, R_2) is achievable using the codebooks $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i \in \mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k \in \mathcal{M}^2}$ and the decoding functions (52), achieving a decoding error probability of ϵ. That is,*

$$\textit{If } r^* = 1, \textit{ then } (R_1, R_2) \in \mathcal{R}_n^{MAC}[P_1, P_2, \sigma, 2\epsilon].$$

3. *If $r^* \ge 2$, then we can conclude using Theorem 2 that, (R_1, R_2) cannot be achieved on a Gaussian multi-access channel with noise standard deviation $(1 + 2\nu)\sigma$ with probability of error less than or equal to $\overline{\epsilon} = \epsilon(1 - \delta(\nu, n))$. That is,*

$$\textit{If } r^* \ge 2, \textit{ then } (R_1, R_2) \notin \mathcal{R}_n^{MAC}[P_1, P_2, (1 + 2\nu)\sigma, \overline{\epsilon}],$$

where

$$\delta(\nu, n) = \exp\left(-n \cdot \frac{r - \log(1+r)}{2(1+2\nu)^2 \sigma^2}\right), \text{ with } r = \sigma^2\left((1+2\nu)^2 - (1+\nu)^2\right).$$

Note that $\delta(\nu, n) \to 0$, *as* $n \to \infty$.

We next show the correctness of Algorithm 6.

Theorem 2. *Let* r^*, $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ *be an optimal solution of the rank-constrained SDP formulation of (54).*

(a) *If* $r^* = 1$, *then* (R_1, R_2) *is achievable using the codebooks* $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ *and the decoding functions (52), achieving a decoding error probability of* ϵ. *That is,*

$$\text{If } r^* = 1, \text{ then } (R_1, R_2) \in \mathcal{R}_n^{MAC}[P_1, P_2, \sigma, \epsilon].$$

(b) *If* $r^* \geq 2$, *then* (R_1, R_2) *cannot be achieved on a Gaussian multi-access channel with noise standard deviation* $(1+2\nu)\sigma$ *with probability of error less than or equal to* $\bar{\epsilon} = \epsilon(1 - \delta(\nu, n))$. *That is,*

$$\text{If } r^* \geq 2, \text{ then } (R_1, R_2) \notin \mathcal{R}_n^{MAC}[P_1, P_2, (1+2\nu)\sigma, \epsilon(1 - \delta(\nu, n))].$$

Proof. The proof is similar to Theorem 1 and it is omitted. □

3.2 Multicast Channel

The multicast channel is a communication channel in which there is one sender and two or more receivers. The basic problem is to find the set of simultaneously achievable rates for communication in a multicast channel. Here we consider the case of two receivers. Assume that we have a sender of power P and two distant receivers. To encode the messages, the transmitter first picks a parameter $\alpha \in [0, 1]$ to generate two codebooks, one with power αP at rate R_1, and another with power $(1-\alpha)P$ at rate R_2, where $\{R_1, R_2\}$ lie in the capacity region of the channel. The transmitter, then chooses a message $i \in \mathcal{M}^1$ and $k \in \mathcal{M}^2$ and transmits codewords $\mathbf{x}_i^1$ and $\mathbf{x}_k^2$ on the channel. Each receiver receives $\mathbf{y}^1$ and $\mathbf{y}^2$ given by

$$\mathbf{y}^1 = \mathbf{x}_i^1 + \mathbf{x}_k^2 + \tilde{\mathbf{z}}^1, \qquad \mathbf{y}^2 = \mathbf{x}_i^1 + \mathbf{x}_k^2 + \tilde{\mathbf{z}}^2,$$

where $\tilde{\mathbf{z}}^1$ and $\tilde{\mathbf{z}}^2$ are Gaussian noise vectors with common standard deviation σ.

The channel coding problem for a two-user Gaussian multi-access channel refers to the problem of constructing a code $\mathcal{C}^{\text{MCC}}[n, R_1, R_2, P, \alpha, \sigma, \epsilon]$, where $\alpha \in [0, 1]$ is a fraction which determines the fraction of power allocated to receiver 1. The outputs of $\mathcal{C}^{\text{MCC}}[n, R_1, R_2, P, \alpha, \sigma, \epsilon]$ are:

1. The codebooks $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$, satisfying

$$\left\|\mathbf{x}_i^1\right\|^2 \leq \alpha P, \qquad \left\|\mathbf{x}_k^2\right\|^2 \leq (1-\alpha)P.$$

2. The decoding functions $g^1 : \mathbb{R}^n \to \mathcal{B}^1$, $g^2 : \mathbb{R}^n \to \mathcal{B}^2$ that map each received codeword $\mathbf{y}^1, \mathbf{y}^2$ to one of the codewords in $\mathcal{B}^1$ and $\mathcal{B}^2$, respectively, so that the average probability of error satisfies

$$\frac{1}{M_1}\sum_{i\in\mathcal{M}^1} \mathbb{P}\left[g^1\left(\mathbf{y}^1\right) \neq i | m^1 = i\right] \leq \epsilon, \qquad \frac{1}{M_2}\sum_{k\in\mathcal{M}^2} \mathbb{P}\left[g^2\left(\mathbf{y}^2\right) \neq k | m^2 = k\right] \leq \epsilon.$$

As before, the capacity region $\mathcal{R}_n^{\text{MCC}}[P, \sigma, \epsilon]$ is defined as the set of all rate pairs (R_1, R_2) such that there exists a code $\mathcal{C}_n^{\text{IC}}[R_1, R_2, P, \alpha, \sigma, \epsilon]$ for some $\alpha \in [0, 1]$.

Capacity Computation and Optimal Coding

In this section, we begin by obtaining a relationship between the capacity regions of a multicast channel and an interference channel, respectively. In particular, we show that the capacity computation of a multicast channel is a special case of an interference channel.

Proposition 7. *Let* $\mathcal{R}_n^{MCC}[P,\sigma,\epsilon]$ *be the finite capacity region of a multicast channel, and*

$$\mathcal{R}_n^{IC}[P_1,P_2,h_{12},h_{21},\sigma,\epsilon]$$

be the finite capacity region of a two-user interference channel. Then

$$\mathcal{R}_n^{MCC}[P,\sigma,\epsilon]=\left\{(R_1,R_2)\,\middle|\,\exists\alpha\in[0,1]\ \textit{such that}\ (R_1,R_2)\in\mathcal{R}_n^{IC}[\alpha P,(1-\alpha)P,\sigma,\epsilon]\right\}.$$

Proof. Let (R_1,R_2) be a rate pair such that for some $\alpha\in[0,1]$

$$(R_1,R_2)\in\mathcal{R}_n^{\mathrm{IC}}[\alpha P,(1-\alpha)P,\sigma,\epsilon].$$

Then there exists codebooks $\mathcal{B}^1$, $\mathcal{B}^2$ and decoding functions $g^1(\cdot),g^2(\cdot)$ such that

$$\begin{aligned}\left\|\mathbf{x}_i^1\right\|^2&\leq\alpha P,\ \forall\mathbf{x}_i^1\in\mathcal{B}^1,\\ \left\|\mathbf{x}_k^2\right\|^2&\leq(1-\alpha)P,\ \forall\mathbf{x}_k^2\in\mathcal{B}^2,\\ \frac{1}{M_1}\sum_{i\in\mathcal{M}^1}\mathbb{P}\left[g^1\left(\mathbf{y}^1\right)\neq i|m^1=i\right]&\leq\epsilon,\\ \frac{1}{M_2}\sum_{k\in\mathcal{M}^2}\mathbb{P}\left[g^2\left(\mathbf{y}^2\right)\neq k|m^2=i\right]&\leq\epsilon.\end{aligned}$$

Therefore, the codebooks $\mathcal{B}^1$, $\mathcal{B}^2$ and decoding functions $g^1(\cdot),g^2(\cdot)$ satisfy the properties for a two user multi-access channel when the transmitter chooses α as the fraction to distribute power among the receivers.

Now suppose that $(R_1,R_2)\in\mathcal{R}_n^{\mathrm{MCC}}[P,\sigma,\epsilon]$, then $\exists\alpha\in[0,1]$, $\mathcal{B}^1$, $\mathcal{B}^2$ and decoding functions $g^1(\cdot),g^2(\cdot)$ such that

$$\begin{aligned}\left\|\mathbf{x}_i^1\right\|^2&\leq\alpha P,\ \forall\mathbf{x}_i^1\in\mathcal{B}^1,\\ \left\|\mathbf{x}_k^2\right\|^2&\leq(1-\alpha)P,\ \forall\mathbf{x}_k^2\in\mathcal{B}^1,\\ \frac{1}{M_1}\sum_{i\in\mathcal{M}^1}\mathbb{P}\left[g^1\left(\mathbf{y}^1\right)\neq i|m^1=i\right]&\leq\epsilon,\\ \frac{1}{M_2}\sum_{k\in\mathcal{M}^2}\mathbb{P}\left[g^2\left(\mathbf{y}^2\right)\neq k|m^2=i\right]&\leq\epsilon.\end{aligned}$$

Therefore, $(R_1,R_2)\in\mathcal{R}_n^{\mathrm{IC}}[\alpha P,(1-\alpha)P,\sigma,\epsilon]$. This concludes the proof. □

Observe that Proposition 7 is a key result that allows us to characterize the capacity region of the multicast channel. Proposition 7 tells us that the problem of characterizing the capacity region of a multicast channel can be transformed into the problem of characterizing the capacity region of an interference channel. Based on this observation, we present Algorithm 7.

Algorithm 7. ***Capacity Computation and Optimal Coding for the Two-User Multicast Channel***

Input: R_1, R_2, P, σ, n, ϵ, ν.

Output: *Rank* r^*, *fraction* $\alpha \in [0,1]$, *codewords* $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$, *and auxiliary binary variables* v_i^1, v_k^2, v_{ik}^1, v_{ik}^2, $\{v_{iki'k't}^1, v_{iki'k't}^2\}_{t=1}^T$.

Algorithm :

1. *Use Algorithm 3 to check if there exists* $\alpha \in [0,1]$ *such that* (R_1, R_2) *is feasible to 33 with* $P_1 = \alpha P$, $P_2 = (1-\alpha)P$.
2. *If* $r^* = 1$, *then* (R_1, R_2) *is achievable using the fraction* α, *codebooks* $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ *and the decoding functions (32), achieving an average decoding error probability of* $3\epsilon^{\frac{1}{4}} + \epsilon$. *That is,*

$$\text{If } r^* = 1, \text{ then } (R_1, R_2) \in \mathcal{R}_n^{MCC}\left[P_1, P_2, \sigma, 3\epsilon^{\frac{1}{4}} + \epsilon\right].$$

3. *If* $r^* \geq 2$, *then we can conclude using Theorem 3 that,* (R_1, R_2) *cannot be achieved on a multicast channel with noise standard deviation* $(1+3\nu)\sigma$ *with probability of error less than or equal to* $\bar{\epsilon} = (\epsilon + \epsilon^{1/4})^4 \cdot (1 - \delta(\nu, n))$, *where*

$$\delta(\nu, n) = \exp\left(-n \cdot \frac{r - \log(1+r)}{2(1+3\nu)^2\sigma^2}\right), \text{ with } r = \sigma^2\left((1+3\nu)^2 - (1+2\nu)^2\right).$$

That is,

$$\text{If } r^* \geq 2, \text{ then } (R_1, R_2) \notin \mathcal{R}_n^{IC}\left[P_1, P_2, (1+3\nu)\sigma, \bar{\epsilon}\right].$$

We next present Theorem 3 that shows the correctness of Algorithm 7.

Theorem 3. *Let* r^*, α^*, $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ *be as computed by Algorithm 8.*

(a) *If* $r^* = 1$, *then* (R_1, R_2) *is achievable using the fraction* α^* *and the codebooks* $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$, *achieving a decoding error probability of* $3\epsilon^{\frac{1}{4}} + \epsilon$. *That is,*

$$\text{If } r^* = 1, \text{ then } (R_1, R_2) \in \mathcal{R}_n^{MCC}\left[P_1, P_2, \sigma, 3\epsilon^{\frac{1}{4}} + \epsilon\right].$$

(b) *If* $r^* \geq 2$, *then* (R_1, R_2) *cannot be achieved on a Gaussian multicast channel with noise standard deviation* $(1+3\nu)\sigma$ *with probability of error less than or equal to* $\bar{\epsilon} = (\epsilon + \epsilon^{1/4})^4 \cdot (1 - \delta(\nu, n))$, *where*

$$\delta(\nu, n) = \exp\left(-n \cdot \frac{r - \log(1+r)}{2(1+3\nu)^2\sigma^2}\right), \text{ with } r = \sigma^2\left((1+3\nu)^2 - (1+2\nu)^2\right).$$

That is,

$$\text{If } r^* \geq 2, \text{ then } (R_1, R_2) \notin \mathcal{R}_n^{MCC}\left[P_1, P_2, (1+3\nu)\sigma, \bar{\epsilon}\right].$$

Proof. The proof follows from the reduction of a multicast channel to an interference channel based on Proposition 7. □

4 Channels with Exponential Noise

In this section, we extend our approach to the cases when the noise is exponentially distributed. We consider the multi-user channel when the noise is exponentially distributed. Just as in the case of a Gaussian channel, we first identify a decoding function that will suffice to construct optimal codes. In this case, the optimal decoder is given by

$$i_1^*(\mathbf{y}) = \arg\max_{i \in \mathcal{B}^1} \left[\max_{k \in \mathcal{B}_i^2(\mathbf{y})} \sum_{j=1}^{n} \left(x_{ij}^1 + h_{12} x_{kj}^2 \right) \right], \tag{56}$$

where $\mathcal{B}_i^2(\mathbf{y}) = \left\{ k \in \mathcal{B}^2 \middle| y_j \geq x_{ij}^1 + h_{12} x_{kj}^2, \ \forall j = 1, \ldots, n \right\}$. Motivated by this, we next present the optimization problem that characterizes the capacity region of an exponential interference channel in Algorithm 8.

Algorithm 8. ***Encoding algorithm for two-user exponential interference channel.***
Input: n, R_1, R_2, λ, P_1, P_2, ϵ, ν.
Output: *Codewords* $\mathbf{x}_i^1$, $\mathbf{x}_k^2$, *and binary variables* $v_{ikt}^1, v_{iki'k't}^1, v_{ikt}^2, v_{iki'k't}^2$.
Algorithm:

1. *Solve the mixed binary linear optimization problem:*

$$\max \quad \sum_{i,k,t} v_{iki'k't}^1 + \sum_{i,k,t} v_{iki'k't}^2 \tag{57}$$

$$\sum_{j=1}^{n} x_{ij}^1 \leq nP_1, \qquad \forall i = 1, \ldots, M_1,$$

$$\sum_{j=1}^{n} x_{ij}^1 + h_{12} \sum_{j=1}^{n} x_{kj}^2 + \left(2 - v_{ikt}^1 - v_{iki'k't}^1\right) M_0^E \geq \sum_{j=1}^{n} x_{i'j}^1 + h_{12} \sum_{j=1}^{n} x_{k'j}^2, \quad \forall t, \forall i' \neq i, \forall i, k, k',$$

$$x_{ij}^1 + h_{12} x_{kj}^2 + z_{tj}^E \geq x_{i'j}^1 + h_{12} x_{k'j}^2 - M_0^E \left(1 - v_{iki'k't}^1\right), \qquad \forall i, k, j, t,$$

$$\sum_{t=1}^{T} v_{ikt}^1 \geq (1 - \epsilon) T, \qquad \forall i,$$

$$\sum_{j=1}^{n} x_{ij}^2 \leq nP_2, \qquad \forall i = 1, \ldots, M_2,$$

$$\sum_{j=1}^{n} x_{ij}^2 + h_{21} \sum_{j=1}^{n} x_{kj}^1 + \left(2 - v_{ikt}^2 - v_{iki'k't}^2\right) M_0^E \geq \sum_{j=1}^{n} x_{i'j}^2 + h_{21} \sum_{j=1}^{n} x_{k'j}^1, \quad \forall t \, \forall i' \neq i, \forall i, k, k',$$

$$x_{ij}^2 + h_{21} x_{kj}^1 + z_{tj}^E \geq x_{i'j}^2 + h_{21} x_{k'j}^1 - M_0^E \left(1 - v_{iki'k't}^2\right), \qquad \forall i, k, j, t,$$

$$\sum_{t=1}^{T} v_{ikt}^2 \geq (1 - \epsilon) T, \qquad \forall i,$$

$$v_{ikt}^1, v_{iki'k't}^1, v_{ikt}^2, v_{iki'k't}^2 \in \{0, 1\}, \qquad \forall i, k, t.$$

2. *If the problem defined by constraints (57) is feasible, then* (R_1, R_2) *is achievable and the resulting codewords can be used to transmit messages.*

Just as in the case of the Gaussian channel, we show in Theorem *4* that Algorithm *8* correctly characterizes the capacity region $\mathcal{R}_n^{\text{EIC}}[P_1, P_2, \lambda, \epsilon]$ of the exponential interference channel.

Theorem 4. ***(Capacity Region in a Two User Exponential Interference Channel)***

(a) *If problem (57) is feasible, then* $(R_1, R_2) \in \mathcal{R}_n^{EIC}\left[P_1, P_2, \lambda, 2\epsilon^{1/2} + \epsilon\right]$, *that is,* (R_1, R_2) *is achievable using the codebooks* $\mathcal{B}^1 = \{\mathbf{x}_i^1\}_{i=1}^{M_1}$, $\mathcal{B}^2 = \{\mathbf{x}_k^2\}_{k=1}^{M_2}$ *and the decoding functions (56), achieving an average decoding error probability of* $2\epsilon^{1/2} + \epsilon$.

(b) *If problem (57) is infeasible, then* $(R_1, R_2) \notin \mathcal{R}_n^{EIC}\left[P_1, P_2, (1+2\nu)^{-1}\lambda, 2\epsilon\right]$.

5 Computational Results

In this section, we present computational results to illustrate the effectiveness of the RO approach for the two-user interference channels. Algorithm 1 for coding in two-user interference Gaussian channels involves the solution of a rank minimization problem subject to semidefinite constraints:

$$\begin{array}{ll} \min & \operatorname{rank}(\mathbf{X}) \\ \text{s.t.} & \tilde{\mathbf{A}} \bullet \mathbf{X} \leq \mathbf{0}, \\ & \mathbf{X} \succeq \mathbf{0}, \end{array} \tag{58}$$

As before, we use the iterative algorithm developed by Fazell et al. [2003], to solve this problem. We chose this algorithm based on Yu and Lau [2011], Wang and Sha [2011] who have reported that this algorithm finds the minimum rank successfully in signal processing applications.

In what follows, we consider the two user Gaussian Interference channel and compare our bounds for finite n with the state of the art asymptotic ($n \to \infty$) bounds from the literature. We choose values of $n = 60, \epsilon = 0.001, \nu = 0.05$, and construct the capacity region as follows:

1. Choose a rate pair $\{R_1, R_2\}$.

2. Using $M_1 = 2^{nR_1}$, $M_2 = 2^{nR_2}$, we solve Problem (33) and apply Algorithm 1.

The resulting semidefinite optimization problems for $n = 60$ involved around 1 billion variables. We use the open source implementation of the SDPARA algorithm (Yamashita et al. [2003]) which allows parallelization and divides the problem in 5000 instances each with around 200 thousand variables. This algorithm took 40 hours on a multi-core linux machine with 48GB RAM and 8 processors.

We next present comparisons with three rate regions proposed in the literature.

Comparison with the rate regions of Carleial [1975]

Carleial [1975] showed that the rate pairs

$$\{(D_1, D_2), (C_1, \min(D_2, T_2)), (\min(D_1, T_1), C_2), (\min(C_1, T_1), \min(C_2, T_2))\},$$

where

$$C_1 = \frac{1}{2}\log(1+P_1), \qquad C_2 = \frac{1}{2}\log(1+P_2), \qquad D_1 = \frac{1}{2}\log\left(\frac{1+P_1}{1+h_{12}P_2}\right),$$
$$D_2 = \frac{1}{2}\log\left(\frac{1+P_2}{1+h_{21}P_1}\right), \quad T_1 = \frac{1}{2}\log\left(\frac{1+h_{21}P_1}{1+P_2}\right), \quad T_2 = \frac{1}{2}\log\left(\frac{1+h_{12}P_2}{1+P_1}\right).$$

are asymptotically achievable. We used $P_1 = 1.5$, $P_2 = 2$, $h_{12} = 0.3$, $h_{21} = 0.3$ and obtained $C_1 = 0.66096$, $C_2 = 0.7924$, $D_1 = 0.3219$, and $D_2 = 0.5244$. In Figure 1, we record the lower and upper bounds from the RO approach for $n = 60, \epsilon = 0.001, \nu = 0.05$. We observe that the lower bounds from the RO approach for $n = 60, \epsilon = 0.001, \nu = 0.05$ dominate the asymptotic lower bounds from Carleial [1975].

Comparison with the rate regions of Han and Kobayashi [1981] and the bounds of Etkin et al. [2008]

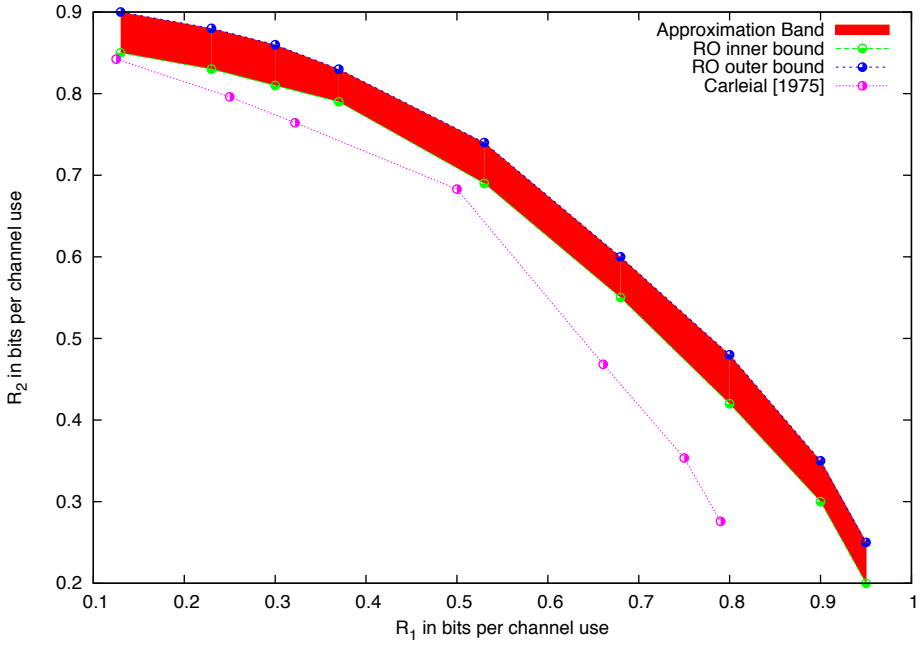

Figure 1: Comparison of the lower and upper bounds provided by the RO approach for $n = 60, \epsilon = 0.001, \nu = 0.05$ and the asymptotic lower bound of Carleial [1975] for the two-user Gaussian interference channel.

We next consider the asymptotic rate regions of Han and Kobayashi [1981] given by

$$\mathcal{R} = \left\{ \begin{array}{c} R_1 \leq \frac{1}{2}\log\left(1+P_1\right) \\ R_2 \leq \frac{1}{2}\log\left(1+P_2\right) \\ R_1 + R_2 \leq \min\left[\frac{1}{2}\log\left(1+P_1+h_{12}P_2\right), \frac{1}{2}\log\left(1+P_2+h_{21}P_1\right)\right] \end{array} \right\}.$$

Etkin et al. [2008] proposed asymptotic upper bounds for the interference channel. In Figure 2, we compare the asymptotic lower bounds from Han and Kobayashi [1981], the asymptotic upper bounds from Etkin et al. [2008] with the lower and upper bounds from the RO approach for $n = 60, \epsilon = 0.001, \nu = 0.05$. We observe that the lower bounds from the RO approach dominate the asymptotic lower bounds from Han and Kobayashi [1981] and the upper bounds from the RO approach dominate the asymptotic upper bounds from Etkin et al. [2008].

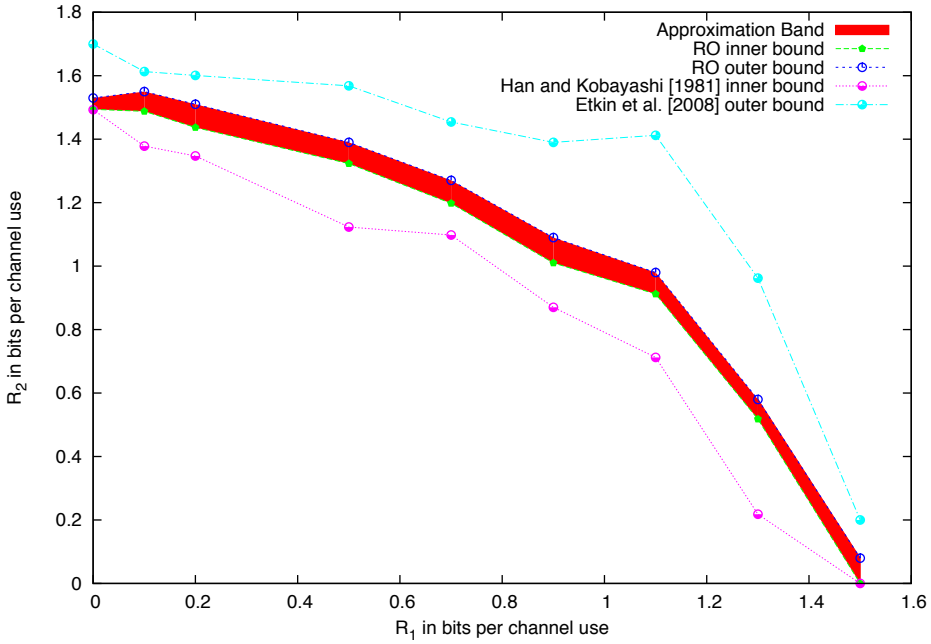

Figure 2: Comparison of the lower and upper bounds provided by the RO approach for $n = 60, \epsilon = 0.001, \nu = 0.05$, with the asymptotic lower bound of Han and Kobayashi [1981] and the asymptotic upper bound of Etkin et al. [2008] for the two-user Gaussian interference channel with $P_1 = 10, P_2 = 20, h_{12} = 0.2, h_{21} = 0.25$.

6 Conclusions

In this paper, we considered the optimal finite length (n) channel coding problem on multi-user Gaussian channels achieving an error probability bound of ϵ. We present novel optimization formulations of the channel coding problem on a multi-user Gaussian interference channel and a broadcast channel. Our main result shows that the optimization problem formulations imply lower and upper bounds on the capacity of the corresponding channels in the finite code length regime for a given error probability of ϵ. Moreover, we show that these upper and lower bounds converge to the true capacity of these channels asymptotically as the code length $n \to \infty$ and the error probability $\epsilon \to 0$. Finally, we report computational results that show that the proposed approach is computationally tractable for $n = 60$ for two-user Gaussian interference channels.

Acknowledgements

We thank the Associate editor Professor Guo and the referees for insightful comments that improved the paper significantly.

References

R. Ahlswede. The capacity region of a channel with two senders and two receivers. *The Annals of Probability*, pages 805–814, 1974.

C. Bandi and D. Bertsimas. Channel coding via robust optimization, part 1: The case of a single channel. *Submitted for publication*, 2015.

A. B. Carleial. A case where interference does not reduce capacity. *IEEE Transactions on Information Theory*, 21(5):569–570, 1975.

T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, New York, 2006.

R. Etkin, D. N. C. Tse, and H. Wang. Gaussian interference channel capacity to within one bit. *IEEE Transactions on Information Theory*, 54(12):5534–5562, 2008.

M. Fazell, H. Hindi, and S. P. Boyd. Log-det heuristic for matrix rank minimization with applications to hankel and euclidean distance matrices. *Proceedings American Control Conference*, 3: 2156–2162, 2003.

T. S. Han and K. Kobayashi. A new achievable rate region for the interference channel. *IEEE Transactions on Information Theory*, 27(1):49–60, 1981.

Y.-W. Huang and P. Moulin. Finite blocklength coding for multiple access channels. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 831–835. IEEE, 2012.

H. Liao. A coding theorem for multiple access communications. In *Proceedings of IEEE International Symposium on Information Theory*, 1972.

E. MolavianJazi and J. N. Laneman. Simpler achievable rate regions for multiaccess with finite blocklength. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 36–40. IEEE, 2012a.

E. MolavianJazi and J. N. Laneman. A random coding approach to gaussian multiple access channels with finite blocklength. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, pages 286–293. IEEE, 2012b.

I. Sason. On achievable rate regions for the Gaussian interference channel. *IEEE Transactions on Information Theory*, 50(6):1345–1356, 2004.

C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27: 379–423, 1948.

R. Urbanke and B. Rimoldi. Lattice codes can achieve capacity on the awgn channel. *IEEE Transactions on Information Theory*, 44:273–278, 1998.

S. Verdú. Fifty years of shannon theory. *IEEE Transactions on information theory*, 44(6):2057–2078, 1998.

S. Verdú and S. W. McLaughlin, editors. *Information Theory: 50 Years of Discovery*. IEEE Press, Piscataway, NJ, USA, 2000. ISBN 0-7803-5363-3.

M. Wang and F. Sha. Information theoretical clustering via semidefinite programming. *AISTATS*, pages 761–769, 2011.

A. Wyner. Random packing and coverings of the unit n-sphere. *Bell System Technical Journal*, 46(9):2111–2118, 1967.

M. Yamashita, K. Fujisawa, and M. Kojima. Sdpara: Semidefinite programming algorithm parallel version. *Parallel Computing*, 29(8):1053–1067, 2003.

H. Yu and V. K. Lau. Rank-constrained schur-convex optimization with multiple trace/log-det constraints. *IEEE Transactions on Signal Processing*, 59(1):304–314, 2011.

Appendix A - Reformulation of (17–30) into a rank minimization problem with semidefinite constraints

We present the complete rank minimization problem reformulation of the feasibility problem (17–30). Recall that $\mathbf{y} = (1, \mathbf{x}_i^1, \mathbf{x}_k^2, v_i^1,\, v_k^2,\, v_{ik}^1,\, v_{ik}^2,\, v_{iki'k't}^1,\, v_{iki'k't}^2)$ is the concatenation in a single vector of all the decisions variables in the feasibility problem (17-27). Letting $\mathbf{Y} = \mathbf{y}\mathbf{y}'$, note that $\text{rank}(\mathbf{Y}) = 1$ and $\mathbf{Y} \succeq \mathbf{0}$. Using an approach similar to Bandi and Bertsimas [2015], we reformulate the feasibility problem (17–30) as the problem of minimizing the rank $(\mathbf{Y})$ subject to linear constraints in $\mathbf{Y}$ and $\mathbf{Y} \succeq 0$.

$$
\begin{aligned}
r^* = \min \quad & \text{rank}\,(\mathbf{Y}) \\
\text{s.t.} \quad & \mathbf{A}_i^1 \bullet \mathbf{Y} \leq 0, && \forall i \in \mathcal{M}^1, \\
& \mathbf{B}_{iki'k't}^1 \bullet \mathbf{Y} \leq 0, && \forall t \in \mathcal{T},\, \forall i, i' \in \mathcal{M}^1, k, k' \in \mathcal{M}^2, \\
& \mathbf{C}_i^1 \bullet \mathbf{Y} \leq 0, && \forall i \in \mathcal{M}^1, \\
& \mathbf{D}_{it}^1 \bullet \mathbf{Y} = 0, && \forall i \in \mathcal{M}^1, t \in \mathcal{T}, \\
& \mathbf{E}_{ik}^1 \bullet \mathbf{Y} = 0, && \forall i, k \neq i \in \mathcal{M}^1, \\
& \mathbf{A}_k^2 \bullet \mathbf{Y} \leq 0, && \forall k \in \mathcal{M}^2, \\
& \mathbf{B}_{iki'k't}^2 \bullet \mathbf{Y} \leq 0, && \forall t \in \mathcal{T},\, \forall i, i' \in \mathcal{M}^1, k, k' \in \mathcal{M}^2, \\
& \mathbf{C}_k^2 \bullet \mathbf{Y} \leq 0, && \forall k \in \mathcal{M}^2, \\
& \mathbf{D}_{kt}^2 \bullet \mathbf{Y} = 0, && \forall k \in \mathcal{M}^2, t \in \mathcal{T}, \\
& \mathbf{E}_{ik}^2 \bullet \mathbf{Y} = 0, && \forall i, k \neq i \in \mathcal{M}^2, \\
& \mathbf{Y} \succeq \mathbf{0}, &&
\end{aligned}
$$

where

$$
\mathbf{A}_i^1\,(p,q) = \begin{cases} -nP_1, & \text{if } p = 1,\, q = 1, \\ 0, & \text{if } p = 1,\, q > 1, \\ 0, & \text{if } p > 1,\, q = 1, \\ 1, & \text{if } \forall p = q = (i-1)n + 1, \ldots, in + 1, \\ 0, & \text{otherwise.} \end{cases}
$$

$$
\mathbf{A}_k^2\,(p,q) = \begin{cases} -nP_2, & \text{if } p = 1,\, q = 1, \\ 0, & \text{if } p = 1,\, q > 1, \\ 0, & \text{if } p > 1,\, q = 1, \\ 1, & \text{if } \forall p = q = (k-1)n + 1, \ldots, kn + 1, \\ 0, & \text{otherwise.} \end{cases}
$$

$$\mathbf{B}^1_{iki'k't}(p,q)=\begin{cases}-M_0^2, & \text{if } p=1,\ q=1,\\ z_{tr}, & \text{if } p=1,\ q=(k-1)n+1+r,\ \forall r=1,\ldots,n,\\ z_{tr}, & \text{if } q=1,\ p=(k-1)n+1+r,\ \forall r=1,\ldots,n,\\ -z_{tr}, & \text{if } p=1,\ q=(i-1)n+1+r,\ \forall r=1,\ldots,n,\\ -z_{tr}, & \text{if } q=1,\ p=(i-1)n+1+r,\ \forall r=1,\ldots,n,\\ -1, & \text{if } \forall p=q=(i-1)n+1,\ldots,in+1,\\ -1, & \text{if } \forall p=q=(k-1)n+1,\ldots,kn+1,\\ 1, & \text{if } q=(k-1)n+1+r,\ p=(i-1)n+1+r,\ \forall r=1,\ldots,n,\\ 1, & \text{if } q=(i-1)n+1+r,\ p=(k-1)n+1+r,\ \forall r=1,\ldots,n,\\ \frac{M_0^2}{2} & \text{if } p=1,\ q=n^2+1+(i-1)T+t,\\ \frac{M_0^2}{2} & \text{if } q=1,\ p=n^2+1+(i-1)T+t,\\ 0, & \text{otherwise.}\end{cases}$$

$$\mathbf{B}^2_{iki'k't}(p,q)=\begin{cases}-M_0^2, & \text{if } p=1,\ q=1,\\ z_{tr}, & \text{if } p=1,\ q=(k-1)n+1+r,\ \forall r=1,\ldots,n,\\ z_{tr}, & \text{if } q=1,\ p=(k-1)n+1+r,\ \forall r=1,\ldots,n,\\ -z_{tr}, & \text{if } p=1,\ q=(i-1)n+1+r,\ \forall r=1,\ldots,n,\\ -z_{tr}, & \text{if } q=1,\ p=(i-1)n+1+r,\ \forall r=1,\ldots,n,\\ -1, & \text{if } \forall p=q=(i-1)n+1,\ldots,in+1,\\ -1, & \text{if } \forall p=q=(k-1)n+1,\ldots,kn+1,\\ 1, & \text{if } q=(k-1)n+1+r,\ p=(i-1)n+1+r,\ \forall r=1,\ldots,n,\\ 1, & \text{if } q=(i-1)n+1+r,\ p=(k-1)n+1+r,\ \forall r=1,\ldots,n,\\ \frac{M_0^2}{2} & \text{if } p=1,\ q=n^2+1+(i-1)T+t,\\ \frac{M_0^2}{2} & \text{if } q=1,\ p=n^2+1+(i-1)T+t,\\ 0, & \text{otherwise.}\end{cases}$$

$$\mathbf{C}^1_i(p,q)=\begin{cases}(1-\epsilon)\,T, & \text{if } p=1,\ q=1,\\ -1, & \text{if } \forall p=q=n^2+1+(i-1)T+t,\ \forall t=1,\ldots,T,\\ 0, & \text{otherwise.}\end{cases}$$

$$\mathbf{C}^2_k(p,q)=\begin{cases}(1-\epsilon)\,T, & \text{if } p=1,\ q=1,\\ -1, & \text{if } \forall p=q=n^2+1+(k-1)T+t,\ \forall t=1,\ldots,T,\\ 0, & \text{otherwise.}\end{cases}$$

$$\mathbf{D}^1_{it}(p,q) = \begin{cases} 0, & \text{if } p=1,\ q=1, \\ -\frac{1}{2}, & \text{if } p=1,\ q=n^2+1+(i-1)T+t, \\ -\frac{1}{2}, & \text{if } q=1,\ p=n^2+1+(i-1)T+t, \\ 1, & \text{if } \forall p=q=n^2+1+(i-1)T+t, \\ 0, & \text{otherwise.} \end{cases}$$

$$\mathbf{D}^2_{kt}(p,q) = \begin{cases} 0, & \text{if } p=1,\ q=1, \\ -\frac{1}{2}, & \text{if } p=1,\ q=n^2+1+(k-1)T+t, \\ -\frac{1}{2}, & \text{if } q=1,\ p=n^2+1+(k-1)T+t, \\ 1, & \text{if } \forall p=q=n^2+1+(k-1)T+t, \\ 0, & \text{otherwise.} \end{cases}$$

$$\mathbf{E}^1_{ik}(p,q) = \begin{cases} 4n\zeta^2, & \text{if } p=1,\ q=1, \\ 0, & \text{if } p=1,\ q>1, \\ 0, & \text{if } p>1,\ q=1, \\ 1, & \text{if } \forall q>1, p=(i-1)n+1,\ldots,in+1, \\ -1, & \text{if } \forall p>1, q=(k-1)n+1,\ldots,kn+1, \\ 0, & \text{otherwise.} \end{cases}$$

$$\mathbf{E}^2_{ik}(p,q) = \begin{cases} 4n\zeta^2, & \text{if } p=1,\ q=1, \\ 0, & \text{if } p=1,\ q>1, \\ 0, & \text{if } p>1,\ q=1, \\ 1, & \text{if } \forall q>1, p=(i-1)n+1,\ldots,in+1, \\ -1, & \text{if } \forall p>1, q=(k-1)n+1,\ldots,kn+1, \\ 0, & \text{otherwise.} \end{cases}$$

Appendix B. Proofs of Auxilliary Results

Proof of Proposition 2.
Without loss of generality, we assume that $f \cdot N$ is an integer and that the numbers $\{a_1, a_2, \ldots, a_N\}$ are sorted such that

$$a_1 \leq a_2 \leq \ldots \leq a_N.$$

It suffices to show that $a_{fN} \leq \alpha \cdot \dfrac{1}{1-f}\cdot$ We consider the following linear optimization problem

$$\begin{aligned} \max \quad & x_{fN} \\ \text{s.t.} \quad & \sum_{i=1}^{N} x_i \leq \alpha N, \\ & x_{fN} \geq x_i, \qquad \forall i < fN, \\ & x_{fN} \leq x_i, \qquad \forall i > fN, \\ & x_i \geq 0, \qquad \forall i, \end{aligned} \tag{59}$$

whose dual problem is given by

$$\begin{aligned} \min \quad & \alpha N q \\ \text{s.t.} \quad & q + p_i \geq 0, && \forall i < fN, \\ & q - p_i \geq 0, && \forall i > fN, \\ & q + \sum_{i>fN} p_i - \sum_{i<fN} p_i \geq 1, \\ & p_i \geq 0. \end{aligned} \tag{60}$$

Consider the following solution to (59) and (60)

$$\begin{aligned} x_i^* &= 0, \quad \forall i < fN, \\ x_i^* &= \frac{\alpha}{1-f}, \quad \forall i \geq fN, \\ q^* &= \frac{1}{N(1-f)}, \\ p_i^* &= q^*, \quad \forall i > fN, \\ p_i^* &= 0, \quad \forall i < fN. \end{aligned}$$

It is easy to verify that $\{x_i^*\}_{i=1}^N$ is feasible to (59), and q^*, $\{p_i^*\}_{i=1}^N$ is feasible to (60) with the same objective value. Therefore, an optimal solution to (59) will satisfy $x_i^* = 0, \forall i < fN$ and $x_i^* = x_{fN}^*, \forall i > fN$ and thus $x_{fN}^* = \alpha \cdot \frac{1}{1-f}$. □

Proof of Proposition 3.
Constraints (18–20) imply that the optimal codewords $\{\mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ satisfy that, for the noise vector $\mathbf{z}_t \in \mathcal{Z}$ with $v_{ikt}^1 = 1$,

$$\left|\left\{k' \in \mathcal{B}^2 \,:\, \|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\|^2 \leq M_0^2 - \delta_1\right\}\right| \leq \left|\left\{k' \in \mathcal{B}^2 \,:\, \|\mathbf{b}_{kk'} + \mathbf{z}_t\|^2 \leq M_0^2 + \delta_1\right\}\right|, \forall i' \in \mathcal{M}^1. \tag{61}$$

Consider the codewords $\{\boldsymbol{\chi}_i^1 = \alpha_1 \mathbf{x}_i^1\}_{i\in\mathcal{M}^1}$, $\{\boldsymbol{\chi}_k^2 = \alpha_2 \mathbf{x}_k^2\}_{k\in\mathcal{M}^2}$ transmitted on a channel with interference parameters $\left\{h_{12}' = \frac{h_{12}}{\alpha_2},\, h_{21}' = \frac{h_{21}}{\alpha_1}\right\}$. For $k' \in \mathcal{B}^2$ such that $\|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\|^2 \geq M_0^2 - \delta_1$, we have

$$\begin{aligned} &\left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h_{12}'\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \\ &\quad = \left\|\alpha_1\left(\mathbf{x}_i^1 - \mathbf{x}_{i'}^1\right) + h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \\ &\quad = \left\|\alpha_1 \mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\right\|^2 \\ &\quad = \alpha_1^2 \left\|\mathbf{a}_{ii'}\right\|^2 + 2\alpha_1 \left(\mathbf{b}_{kk'} + \mathbf{z}_t\right)' \mathbf{a}_{ii'} + \left\|\mathbf{b}_{kk'} + \mathbf{z}_t\right\|^2 \\ &\quad = \left(\alpha_1^2 - \alpha_1\right)\left\|\mathbf{a}_{ii'}\right\|^2 + \alpha_1 \cdot \left\|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\right\|^2 + (1-\alpha_1)\left\|\mathbf{b}_{kk'} + \mathbf{z}_t\right\|^2 \\ &\quad \geq \left(\alpha_1^2 - \alpha_1\right)\left\|\mathbf{a}_{ii'}\right\|^2 + \alpha_1 M_0^2 - \alpha_1\delta_1 + (1-\alpha_1)\left\|\mathbf{z}_t\right\|^2 + (1-\alpha_1)\cdot\left(\left\|\mathbf{b}_{kk'}\right\|^2 + 2\mathbf{z}_t'\mathbf{b}_{kk'}\right) \\ &\quad = M_0^2 - \alpha_1\delta_1 + \left(\alpha_1^2 - \alpha_1\right)\left\|\mathbf{a}_{ii'}\right\|^2 + (1-\alpha_1)\cdot\left(\left\|\mathbf{b}_{kk'}\right\|^2 + 2\mathbf{z}_t'\mathbf{b}_{kk'}\right) \qquad (\text{since } \|\mathbf{z}_t\| = M_0) \end{aligned} \tag{62}$$

From (27) for $k = k'$, we have

$$\left\|\mathbf{a}_{ii'}\right\|^2 = \left\|\mathbf{x}_i^1 - \mathbf{x}_{i'}^1\right\|^2 \geq 4\eta^2 n. \tag{63}$$

We also have

$$\|\mathbf{b}_{kk'}\| = h_{12}\left\|\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right\| \le h_{12}\left(\left\|\mathbf{x}_k^2\right\| + \left\|\mathbf{x}_{k'}^2\right\|\right) \le 2h_{12}\sqrt{nP_2}$$

which implies that

$$\|\mathbf{b}_{kk'}\|^2 + 2\mathbf{z}_t'\mathbf{b}_{kk'} \le \|\mathbf{b}_{kk'}\|^2 + 2\|\mathbf{z}_t\|\|\mathbf{b}_{kk'}\| \le 4h_{12}^2P_2n + 4M_0h_{12}\sqrt{nP_2}. \tag{64}$$

From (63), (64), and (62) we have

$$\begin{aligned}&\left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h_{12}'\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \\ &\quad\ge M_0^2 - \alpha_1\delta_1 + \left(\alpha_1^2 - \alpha_1\right)\cdot 4\eta^2 n + (1-\alpha_1)\cdot\left(4h_{12}^2P_2n + 4M_0h_{12}\sqrt{nP_2}\right).\end{aligned}$$

Using α_1 from (9), which is the lower root of the quadratic equation

$$\left(y^2 - y\right)\cdot 4\eta^2 n + (1-y)\cdot\left(4h_{12}^2P_2n + 4M_0h_{12}\sqrt{nP_2}\right) - y\delta_1 - 3\delta_1 = 0,$$

we obtain

$$\begin{aligned}&\left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h_{12}'\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \\ &\quad\ge M_0^2 - \alpha_1\delta_1 + \left(\alpha_1^2 - \alpha_1\right)\cdot 4\eta^2 n + (1-\alpha_1)\cdot\left(4h_{12}^2P_2n + 4M_0h_{12}\sqrt{nP_2}\right) \\ &\quad\ge M_0^2 + 3\delta_1.\end{aligned} \tag{65}$$

For $k' \in \mathcal{B}^2$ such that $\|\mathbf{b}_{kk'} + \mathbf{z}_t\|^2 \le M_0^2 + \delta_1$, we have

$$\begin{aligned}&\left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_i^1 + h_{12}'\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \mathbf{z}_t\right\|^2 \\ &\quad= \|\mathbf{b}_{kk'} + \mathbf{z}_t\|^2 \\ &\quad\le M_0^2 + \delta_1.\end{aligned} \tag{66}$$

Consider $\tilde{\mathbf{z}} \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)$, and let $\tilde{\mathbf{z}}_0 = M_0\cdot\tilde{\mathbf{z}}/\|\tilde{\mathbf{z}}\|$. Suppose $\tau(\tilde{\mathbf{z}}') = t$. Since $\{\mathbf{z}_1, \mathbf{z}_2, \ldots, \mathbf{z}_T\}$ forms a Voronoi tessellation of $\mathcal{S}_n((1+\nu)\gamma_\epsilon)$, from Proposition 5 applied to $\mathcal{A} = \mathcal{Z}$, $N = T$, $\Lambda = \gamma_\epsilon/\sqrt{n}$, we obtain that

$$\|\tilde{\mathbf{z}}_0 - \mathbf{z}_t\| \le \theta\sqrt{n}, \text{ where } \theta = \frac{\gamma_\epsilon}{\sqrt{n}T^{1/n}} = \frac{\zeta'\nu}{1+\nu}.$$

Therefore, we have

$$\begin{aligned}\|\tilde{\mathbf{z}} - \mathbf{z}_t\| &\le \|\tilde{\mathbf{z}}_0 - \mathbf{z}_t\| + \|\tilde{\mathbf{z}} - \tilde{\mathbf{z}}_0\| \\ &\le \theta\sqrt{n} + \left\|\tilde{\mathbf{z}} - \frac{M_0}{\|\tilde{\mathbf{z}}\|}\cdot\tilde{\mathbf{z}}\right\| \\ &= \theta\sqrt{n} + M_0 - \|\tilde{\mathbf{z}}\| \le \theta\sqrt{n} + M_0 - (M_0 - 2\Gamma_\epsilon) = \theta\sqrt{n} + 2\Gamma_\epsilon.\end{aligned} \tag{67}$$

Next, we obtain the following:
Using the definition of δ_1 from (8), we obtain

$$\sqrt{M_0^2 + \delta_1} + \theta\sqrt{n} + 2\Gamma_\epsilon \le \sqrt{M_0^2 + 2\delta_1} \le \sqrt{M_0^2 + 3\delta_1} - \left(\theta\sqrt{n} + 2\Gamma_\epsilon\right). \tag{68}$$

(a) For $k' \in \mathcal{B}^2$ such that $\|\mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 + \delta_1}$,

$$\begin{aligned}
&\left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_i^1 + h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \\
&\quad = \left\|h_{12}\left(\mathbf{x}_k^2 - \mathbf{x}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| = \|\mathbf{b}_{kk'} + \tilde{\mathbf{z}}\| \\
&\quad \leq \|\mathbf{b}_{kk'} + \mathbf{z}_t\| + \|\tilde{\mathbf{z}} - \mathbf{z}_t\| \\
&\quad \leq \sqrt{M_0^2 + \delta_1} + \theta\sqrt{n} + 2\Gamma_\epsilon \\
&\quad \leq \sqrt{M_0^2 + 2\delta_1} \ \text{ (from (68)).}
\end{aligned} \tag{69}$$

(b) For $k' \in \mathcal{B}^2$ such that $\|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\| \geq \sqrt{M_0^2 - \delta_1}$,

$$\begin{aligned}
&\left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \\
&\quad \geq \left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \mathbf{z}_t\right\| - \|\tilde{\mathbf{z}} - \mathbf{z}_t\| \\
&\quad \geq \sqrt{M_0^2 + 3\delta_1} - \left(\theta\sqrt{n} + 2\Gamma_\epsilon\right) \\
&\quad \geq \sqrt{M_0^2 + 2\delta_1} \ \text{ (from (68)).}
\end{aligned} \tag{70}$$

Next we show that from (69) and (70), we obtain that $\forall \tilde{\mathbf{z}}$ with $\tau(\tilde{\mathbf{z}}) = t$, and $v_{ikt}^1 = 1$

$$\begin{aligned}
&\left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\|^2 \leq M_0^2 + 2\delta_1\right\}\right| \\
&\qquad \leq \left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\|^2 \leq M_0^2 + 2\delta_1\right\}\right|, \ \forall i' \in \mathcal{M}^1.
\end{aligned}$$

To show this, fix i, i', k, t with $v_{ikt}^1 = 1$, and let

$$\begin{aligned}
\mathscr{A} &= \left\{k' \in \mathcal{B}^2 \,\middle|\, \|\mathbf{a}_{ii'} + \mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 - \delta_1}\right\}, \\
\mathscr{B} &= \left\{k' \in \mathcal{B}^2 \,\middle|\, \|\mathbf{b}_{kk'} + \mathbf{z}_t\| \leq \sqrt{M_0^2 + \delta_1}\right\}, \\
\hat{\mathscr{A}} &= \left\{k' \in \mathcal{B}^2 \,\middle|\, \left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \leq \sqrt{M_0^2 + 2\delta_1}\right\}, \\
\hat{\mathscr{B}} &= \left\{k' \in \mathcal{B}^2 \,\middle|\, \left\|h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\| \leq \sqrt{M_0^2 + 2\delta_1}\right\}.
\end{aligned}$$

In this notation, from (18) with $v_{ikt}^1 = 1$ implies that $|\mathscr{A}| \leq |\mathscr{B}|$. In (69), we have shown that $\mathscr{B} \subseteq \hat{\mathscr{B}}$, implying that $|\mathscr{B}| \leq \left|\hat{\mathscr{B}}\right|$. In (70), we have shown that $\mathscr{A}^C \subseteq \hat{\mathscr{A}}^C$, implying that $|\mathscr{A}| \geq \left|\hat{\mathscr{A}}\right|$. Therefore,

$$\left|\hat{\mathscr{A}}\right| \leq |\mathscr{A}| \leq |\mathscr{B}| \leq \left|\hat{\mathscr{B}}\right|.$$

Therefore, we have shown that $\forall \tilde{\mathbf{z}}$ with $\tau(\tilde{\mathbf{z}}) = t$, and $v_{ikt}^1 = 1$

$$\begin{aligned}
&\left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|\boldsymbol{\chi}_i^1 - \boldsymbol{\chi}_{i'}^1 + h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\|^2 \leq M_0^2 + 2\delta_1\right\}\right| \\
&\qquad \leq \left|\left\{k' \in \mathcal{B}^2 \,:\, \left\|h'_{12}\left(\boldsymbol{\chi}_k^2 - \boldsymbol{\chi}_{k'}^2\right) + \tilde{\mathbf{z}}\right\|^2 \leq M_0^2 + 2\delta_1\right\}\right|, \ \forall i' \in \mathcal{M}^1.
\end{aligned} \tag{71}$$

That is, by using the decoder (32), we decode correctly for $\tilde{\mathbf{z}} \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)$ with $\tau(\tilde{\mathbf{z}}) = t$. Therefore, we have

$$\left\{v_{ik\tau(\tilde{\mathbf{z}})} = 1\right\} \implies \left\{\mathscr{E}^1_{ik}[\tilde{\boldsymbol{z}}] = 0\right\},$$

which implies $\mathbb{P}\left[\mathscr{E}^1_{ik}[\tilde{\boldsymbol{z}}] \,\middle|\, \tilde{\mathbf{z}} \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] \leq \mathbb{P}\left[v^1_{ik\tau(\tilde{\mathbf{z}})} = 0\right]$.

Next, for each $i \in \mathcal{M}^1$, $k \in \mathcal{M}^2$

$$\mathbb{P}\left[v^1_{ik\tau(\tilde{\mathbf{z}})} = 0\right] = \sum_{t=1}^{T} \mathbb{P}\left[v^1_{ik\tau(\tilde{\mathbf{z}})} = 0 \,\middle|\, \tau(\tilde{\mathbf{z}}) = t\right] \cdot \mathbb{P}\left[\tau(\tilde{\mathbf{z}}) = t\right]. \tag{72}$$

We have

$$\begin{aligned}\mathbb{P}\left[v^1_{ik\tau(\tilde{\mathbf{z}})} = 0 \,\middle|\, \tau(\tilde{\mathbf{z}}) = t\right] &= \begin{cases} 1, & \text{if } v^1_{ikt} = 0, \\ 0, & \text{otherwise,} \end{cases} \\ &= 1 - v^1_{ikt}. \end{aligned} \tag{73}$$

Since the set of vectors $\mathcal{Z}$ forms a Voronoi tessellation of $\mathcal{S}_n((1+\nu)\gamma_\epsilon)$, the Voronoi regions of the points $\mathbf{z}_t \in \mathcal{Z}$ are identical with the same area. Moreover, since $\tilde{\mathbf{z}}$ is Gaussian, from Proposition 6(b), we know that $\tilde{\mathbf{z}}$ induces a uniform distribution for $\tau(\tilde{\mathbf{z}})$ on the elements of the set $\{1, \ldots, T\}$, that is,

$$\mathbb{P}\left[\tau(\tilde{\mathbf{s}}) = t\right] = \frac{1}{T}, \ \forall t = 1, \ldots, T. \tag{74}$$

Substituting (73) and (74) in (72), we have

$$\begin{aligned}\mathbb{P}\left[\mathscr{E}^1_{ik}[\tilde{\boldsymbol{z}}] \,\middle|\, \tilde{\mathbf{z}} \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] &\leq \mathbb{P}\left[v^1_{ik\tau(\tilde{\mathbf{z}})} = 0\right] \\ &= \sum_{t=1}^{T} \mathbb{P}\left[v^1_{ik\tau(\tilde{\mathbf{z}})} = 0 \,\middle|\, \tau(\tilde{\mathbf{z}}) = t\right] \cdot \mathbb{P}\left[\tau(\tilde{\mathbf{z}}) = t\right] \\ &= \frac{1}{T} \sum_{t=1}^{T} \left(1 - v^1_{ikt}\right) \leq \frac{1}{T} \cdot \epsilon T \qquad \text{(from (23))} \\ &= \epsilon.\end{aligned}$$

Next, we will calculate $\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}^1_G\right]\right]$

$$\begin{aligned}\mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}^1_G\right]\right] &= \mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}^1_G\right] \,\middle|\, \tilde{\boldsymbol{z}}^1_G \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] \cdot \mathbb{P}\left[\tilde{\boldsymbol{z}}^1_G \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] + \\ &\qquad \mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}^1_G\right] \,\middle|\, \tilde{\boldsymbol{z}}^1_G \notin \mathcal{U}(\sigma, \Gamma_\epsilon)\right] \cdot \mathbb{P}\left[\tilde{\boldsymbol{z}}^1_G \notin \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] \\ &\leq \mathbb{P}\left[\mathscr{E}^1_{ik}\left[\tilde{\boldsymbol{z}}^1_G\right] \,\middle|\, \tilde{\boldsymbol{z}}^1_G \in \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] + \mathbb{P}\left[\tilde{\boldsymbol{z}}^1_G \notin \mathcal{U}_\epsilon(\sigma, \Gamma_\epsilon)\right] \\ &\leq \epsilon + (\epsilon^{1/4} - \epsilon) \qquad \text{(from (35))} \\ &= \epsilon^{1/4}.\end{aligned}$$

This concludes the proof. □