Characterizing the Performance of Wireless Communication Architectures via Basic Diophantine Approximation Bounds

Bobak Nazer and Or Ordentlich

May 10, 2019

Abstract

Consider a wireless network where several users are transmitting simultaneously. Each receiver observes a linear combination of the transmitted signals, corrupted by random noise, and attempts to recover the codewords sent by one or more of the users. Within the context of network information theory, it is of interest to determine the maximum possible data rates as well as efficient strategies that operate at these rates. One promising recent direction has shown that if the users utilize a lattice-based strategy, then a receiver can recover an integer-linear combination of the codewords at a rate that depends on how well the real-valued channel gains can be approximated by integers. In other words, the performance of this lattice-based strategy is closely linked to a basic question in Diophantine approximation. This chapter provides an overview of the key findings in this emerging area, starting from first principles, and expanding towards state-of-the art results and open questions, so that it is accessible to researchers with either an information theory or Diophantine approximation background.

1 Introduction

Consider multiple transmitters and receivers that communicate with each other across a shared wireless channel. The two main challenges to establishing reliable communication between users are the noise introduced by

the channel and the interference between simultaneously transmitted signals. Over the past few decades, the field of network information theory has strived to determine the fundamental limits of reliable communication over multi-user channels as well as architectures that can approach these limits in practice [1–3].

In this chapter, we discuss recent developments in network information theory based on the use of lattice codebooks, i.e., codebooks that are a subset of a lattice over $\mathbb{R}^n$ [4]. The inherent linearity of these codebooks is appealing for two reasons. First, linearity lends itself to more efficient encoding and decoding algorithms. Second, since lattices are closed under integer-linear combinations, it is possible for a receiver to directly decode an integer-linear combination of transmitted codewords (without first recovering the individual codewords) [5]. This phenomenon can be used as a building block for communication strategies that operate beyond the performance available for classical coding schemes.

In general, the performance of these lattice-based strategies is determined by how closely the channel coefficients can be *approximated by* integer coefficients. For any particular choice of channel coefficients, we can identify the optimal integer coefficients, and the resulting performance. However, it is often of interest to have universal bounds that do not depend on the specific realization of the channel. As we will demonstrate, classical and modern results from Diophantine approximation can be used to establish such bounds.

Overall, this chapter attempts to provide a unified view of recent results that connect the performance of the "compute-and-forward" strategy of recovering an integer-linear combination to Diophantine approximation bounds. We also highlight scenarios where novel applications of Diophantine approximation techniques may lead to new results in network information theory.

1.1 Single-User Gaussian Channels

Consider the following channel model for time $t \in \{1, 2, \ldots, T\}$:

$$y[t] = x[t] + z[t] \tag{1}$$

where

- $y[t] \in \mathbb{R}$ represents the channel output at the receiver at time t,

- $x[t] \in \mathbb{R}$ is the channel input of the transmitter at time t,
- and $z[t] \in \mathbb{R}$ is the noise at time t, which is assumed to be Gaussian, $z[t] \sim \mathcal{N}(0,1)$, and generated independently for each time t.

Our goal is for the transmitter to reliably send information to the receiver at the highest possible data rates. To this end, the channel may be used during T time slots, which is often referred to as the *blocklength* of the communication scheme. The *communication rate* $R \geq 0$ is defined as the average number of bits that it transmits per time slot. One practical consideration is that the transmitter has a maximum power level that it can sustain during its transmission. This is modeled in the definition below via the *power constraint* $P \geq 0$. Let $\|\cdot\|$ denote the Euclidean norm.

Definition 1 (Code) *A $(2^{TR}, T, P)$ code for the channel (1) consists of*

- *a message set $\{1, 2, \ldots, 2^{TR}\}$,*
- *an encoder that assigns a T-dimensional vector $\mathbf{x}(m) \in \mathbb{R}^T$ to each message $m \in \{1, 2, \ldots, 2^{TR}\}$. The encoder is subject to a power constraint $P > 0$, which dictates that $\|\mathbf{x}(m)\|^2 \leq TP$ for all $m \in \{1, 2, \ldots, 2^{TR}\}$,*
- *and a decoder that assigns an estimate $\hat{m}$ of the transmitted message to each possible received sequence $[y[1]\ y[2]\ \cdots\ y[T]]$.*

The message M is assumed to be uniformly distributed over $\{1, 2, \ldots, 2^{TR}\}$. The average error probability of a code is defined as

$$p_{\text{error}} = \Pr\left(\hat{M} \neq M\right). \tag{2}$$

Definition 2 (Achievable rate) *A rate R is said to be achievable over the channel (1) with power constraint P if, for any $\epsilon > 0$ and T large enough, there exists a $(2^{TR}, T, P)$ code with $p_{error} < \epsilon$.*

Definition 3 (Capacity) *The capacity of the channel (1) with power constraint P is the supremum of the set of all achievable rates.*

The capacity of the Gaussian channel is due to Shannon [6].

Theorem 1 (Gaussian capacity) *The capacity of the channel* (1) *with power constraint* P *is*

$$C = \frac{1}{2}\log(1+P)\ . \tag{3}$$

The proof of Theorem 1 consists of two parts: a *converse* part where it is shown that if a $(2^{TR}, T, P)$ code with small error probability exists, then the rate R must satisfy $R \leq \frac{1}{2}\log(1+P)$, and a *direct* part, where it is shown that there exists a sequence of codes $(2^{TR}, T, P)$, with growing T and vanishing error probability so long as $R < \frac{1}{2}\log(1+P)$.

The main observation leading to the direct part is that, in high dimensions, the noise sequence lives inside a ball of radius $\sqrt{T(1+\delta)}$ for $\delta > 0$ with high probability. Thus, the coding task reduces to placing the centers of 2^{TR} balls of this radius inside a larger ball of radius $\sqrt{TP}$, with some small overlap between balls that corresponds to the small allowable error probability. Shannon's insight was that the existence of such a packing can be shown via the probabilistic method, i.e., by drawing the centers of the balls independently and uniformly within a ball of radius $\sqrt{TP}$. In this manner, the codewords are ensured to not violate the power constraint. Alternatively, we can draw the codewords i.i.d. according to a $\mathcal{N}(\mathbf{0}, P\mathbf{I})$ distribution.

A typical member of the i.i.d. code ensemble lacks structure, and thus the encoding and decoding operations require exponential complexity in T (i.e., they essentially correspond to lookup tables for all 2^{TR} codewords) and are not practically realizable. The field of coding theory has strived to develop families of codes with low encoding and decoding complexity and performance close to the capacity limit.

The art of coding for the AWGN channel is by now well-developed and low-complexity coding schemes operating near capacity, e.g., low-density parity-check (LDPC) codes [7–9], turbo codes [10], polar codes [11], etc., are known and implemented in various communication standards. A lot of these coding schemes are based on mapping a binary linear code, i.e., a subspace in $\mathbb{F}_2^T$, (or more generally, a p-ary linear code) to the Euclidean space. Consequently, the resulting code often has some linear structure, and can be thought of as a lattice code, as we define below.

A lattice Λ is a discrete subgroup of $\mathbb{R}^T$ that is closed under reflection and real addition. Formally, for any $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \Lambda$, we have that $-\boldsymbol{\lambda}_1, -\boldsymbol{\lambda}_2 \in \Lambda$ and $\boldsymbol{\lambda}_1 + \boldsymbol{\lambda}_2 \in \Lambda$. Note that, by definition, the zero vector $\mathbf{0}$ is always a

member of the lattice. Any lattice Λ in $\mathbb{R}^T$ is spanned by some $T \times T$ matrix $\mathbf{G}$ such that

$$\Lambda = \{\boldsymbol{\lambda} = \mathbf{G}\mathbf{q} : \mathbf{q} \in \mathbb{Z}^T\}.$$

We say that a lattice is full-rank if its spanning matrix $\mathbf{G}$ is full-rank.

Let $\mathcal{B}(\mathbf{0}, r) = \{\mathbf{x} \in \mathbb{R}^T : \|\mathbf{x}\| \leq r\}$ be the T-dimensional, zero-centered, closed ball of radius $r > 0$. A lattice code is constructed by intersecting a base lattice Λ, with some shaping region $\mathcal{V} \subset \mathcal{B}(\mathbf{0}, \sqrt{TP})$, whose role is to enforce the power constraint. The rate of the lattice code $\mathcal{L} = \Lambda \cap \mathcal{V}$ is therefore $R = \frac{1}{T} \log |\Lambda \cap \mathcal{V}|$.

The main motivation for using lattice codes for the AWGN channel is to exploit the linear structure of Λ for simplified encoding and decoding algorithms. In particular, for the AWGN channel, the optimal decoder corresponds to finding the codeword with the smallest Euclidean distance from the channel output. When a lattice code $\mathcal{L} = \Lambda \cap \mathcal{V}$ is used, this can be approximated by applying the nearest neighbor lattice quantizer defined as

$$Q_\Lambda(\mathbf{y}) = \arg\min_{\boldsymbol{\lambda} \in \Lambda} \|\mathbf{y} - \boldsymbol{\lambda}\|, \tag{4}$$

to the channel output, and returning the corresponding message if $Q_\Lambda(\mathbf{y}) \in \mathcal{V}$, or declaring an error otherwise.

The choice of the shaping region $\mathcal{V}$ should on the one hand result in a high rate, and on the other hand maintain much of the structure of the base lattice, such that there is a "convenient" mapping between the message set $\{1, 2, \ldots, 2^{RT}\}$ and the points in $\mathcal{L}$, and that a lattice decoder, which essentially ignores the shaping region, would still perform well. Erez and Zamir [12] showed that for any $P > 0$, there exists a base lattice Λ and a shaping region $\mathcal{V}$ (more precisely, a sequence in T of $\Lambda^{(T)}, \mathcal{V}^{(T)}$), such that the lattice code $\mathcal{L} = \Lambda \cap \mathcal{V}$ achieves the AWGN channel capacity under (a slight modification of) lattice decoding. In particular, they took $\mathcal{V}$ as the Voronoi region of a coarse lattice $\Lambda_c \subset \Lambda$.

For the point-to-point AWGN channel, the interest in lattice codes is motivated by the need to lower the complexity of encoding and decoding operations so as to render them practically feasible. For networks with multiple transmitters or receivers, lattice codes can also be used to approach the performance suggested by i.i.d. random codes. Interestingly, as we will explore below, lattice codes can also be used to derive lower bounds on multi-user capacity that cannot be established via i.i.d. ensembles.

2 Gaussian Multiple-Access Channel Model

We will focus on bounds for the Gaussian multiple-access channel (MAC), which is a canonical model for a wireless network where multiple transmitters simultaneously communicate with a single receiver. We assume that there are K users, each equipped with a single antennas, that wish to communicate with an N-antenna receiver for time $t \in \{1, 2, \ldots, T\}$, leading to the following model:

$$\mathbf{y}[t] = \sum_{k=1}^{K} \mathbf{h}_k x_k[t] + \mathbf{z}[t] \tag{5}$$

where

- $\mathbf{y}[t] \in \mathbb{R}^N$ represents the channel output at the receiver at time t,
- $x_k[t] \in \mathbb{R}$ is the channel input of the k^{th} user at time t,
- $\mathbf{h}_k \in \mathbb{R}^N$ is the vector of channel gains from the k^{th} user to the N antennas of the receiver,
- and $\mathbf{z}[t] \in \mathbb{R}^N$ is the noise vector at time t, which is assumed to be Gaussian, $\mathbf{z}[t] \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$, and generated independently for each time t.

It will be useful to express all of the channel gains together in matrix notation,

$$\mathbf{y}[t] = \mathbf{H}\mathbf{x}[t] + \mathbf{z}[t] \tag{6}$$

$$\mathbf{H} = [\mathbf{h}_1 \ \mathbf{h}_2 \ \cdots \ \mathbf{h}_K] \tag{7}$$

$$\mathbf{x}[t] = [x_1[t] \ x_2[t] \ \cdots \ x_K[t]]^{\mathsf{T}} \tag{8}$$

where the $(n, k)^{\text{th}}$ entry $h_{n,k}$ of $\mathbf{H}$ represents the channel gain from the k^{th} user to the n^{th} antenna.

Definition 4 *A $(2^{TR_1}, \ldots, 2^{TR_K}, T, P)$ code for the channel (6) consists of*

- *K message sets $\{1, 2, \ldots, 2^{TR_k}\}$, $k = 1, \ldots, K$,*
- *K encoders, where encoder k assigns a T-dimensional vector $\mathbf{x}_k(m_k) \in \mathbb{R}^T$ to each message $m_k \in \{1, 2, \ldots, 2^{TR_k}\}$. All encoders are subject to a power constraint $P > 0$, which dictates that $\|\mathbf{x}_k(m_k)\|^2 \leq TP$ for all $k = 1, \ldots, K$ and $m_k \in \{1, 2, \ldots, 2^{TR_k}\}$,*

- *and a decoder that assigns an estimate* $(\hat{m}_1, \ldots, \hat{m}_K)$ *of the transmitted messages to each possible received sequence* $\mathbf{Y} = [\mathbf{y}[1]\ \mathbf{y}[2]\ \cdots\ \mathbf{y}[T]] \in \mathbb{R}^{N\times T}$.

In the sequel, it will be useful to compactly represent all time slots t together:

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{Z}, \tag{9}$$

where

$$\mathbf{Y} = [\mathbf{y}[1]\ \cdots\ \mathbf{y}[T]] \in \mathbb{R}^{N\times T} \tag{10}$$

$$\mathbf{X} = [\mathbf{x}[1]\ \cdots\ \mathbf{x}[T]] = [\mathbf{x}_1(m_1)\ \cdots\ \mathbf{x}_K(m_K)]^{\mathsf{T}} \in \mathbb{R}^{K\times T} \tag{11}$$

$$\mathbf{Z} = [\mathbf{z}[1]\ \cdots\ \mathbf{z}[T]] \in \mathbb{R}^{N\times T}. \tag{12}$$

The message M_k of the k^{th} user is assumed to be uniformly distributed over $\{1, 2, \ldots, 2^{TR_k}\}$, and $M_1, \ldots, M_K$ are assumed to be mutually independent. The average error probability of a code is defined as

$$p_{\text{error}} = \Pr\left((\hat{M}_1, \ldots, \hat{M}_K) \neq (M_1, \ldots, M_K)\right). \tag{13}$$

Definition 5 (Achievable rates) *A rate tuple* $(R_1, \ldots, R_K)$ *is said to be achievable over the channel* (6) *with power constraint* P *if, for any* $\epsilon > 0$ *and* T *large enough, there exists a* $(2^{TR_1}, \ldots, 2^{TR_k}, T, P)$ *code with* $p_{error} < \epsilon$.

Definition 6 (Capacity region) *The capacity region of the channel* (6) *with power constraint* P *is the closure of the set of all achievable rate tuples.*

The Gaussian MAC (6) with power constraint P, is a special case of the family of discrete memoryless MACs, for which the capacity region is known, and can be expressed in closed form [1, 13, 14].

Theorem 2 (MAC capacity region) *The capacity region of the Gaussian MAC* (6) *with power constraint* P *is the set of all rates satisfying*

$$\sum_{k\in\mathcal{S}} R_k \leq \frac{1}{2}\log\det\left(\mathbf{I} + P\mathbf{H}_{\mathcal{S}}^{\mathsf{T}}\mathbf{H}_{\mathcal{S}}\right), \tag{14}$$

for all $\mathcal{S} = \{i_1, \ldots, i_{|\mathcal{S}|}\} \subset [K]$, *where* $\mathbf{H}_{\mathcal{S}} = [\mathbf{h}_{i_1}\ \cdots\ \mathbf{h}_{i_{|\mathcal{S}|}}]$.

As in the point-to-point AWGN case, the direct (achievability) part of Theorem 2 is established by drawing each user's codebook independently at random from an i.i.d. ensemble [2, §9.2.1]. Consequently, the proof does not lead to practical communication schemes for this channel.

Note also that unlike the point-to-point AWGN model, here the channel is characterized by a channel matrix $\mathbf{H}$. Thus, in general, different codes are needed for different channel matrices, even if $R_1, \ldots, R_K, T$ and P are fixed. In practical scenarios, $\mathbf{H}$ is seldom known in advance, and typically it is changing with time. Thus, a more natural approach is to design the encoders independently of $\mathbf{H}$, and to only adapt the decoder w.r.t. the actual channel matrix $\mathbf{H}$. Moreover, since capacity-approaching codes with low-complexity for the point-to-point AWGN channel exist, a very appealing approach is to manipulate the MAC output $\mathbf{Y}$ using signal processing, in order to induce parallel point-to-point channels from it.

The most natural, and widely used, example of such an approach is based on linear estimation. In particular, in order to decode $\mathbf{x}_k = \mathbf{x}_k(M_k)$, we can first set $\tilde{\mathbf{y}}_k^{\mathsf{T}} = \mathbf{b}_k^{\mathsf{T}}\mathbf{Y}$, where the vector $\mathbf{b}_k \in \mathbb{R}^N$ is selected to minimize $\sigma_k^2 = \mathbb{E}\|\mathbf{x}_k - \tilde{\mathbf{y}}_k\|^2$. Now, the channel from $\mathbf{x}_k$ to $\tilde{\mathbf{y}}_k$ can be thought of as a point-to-point AWGN channel with noise variance σ_k^2. Thus, if $\mathbf{x}_k$ is encoded via a "good" code for the AWGN channel, we can apply the corresponding decoder, and decode $\mathbf{x}_k$ from $\tilde{\mathbf{y}}_k$ with small error probability, if $R_k < \frac{1}{2}\log\left(\frac{P}{\sigma_k^2}\right)$.[1] We refer to the above communication scheme as a *linear equalization* scheme, since roughly speaking, the vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_K\}$ attempt to equalize the channel matrix $\mathbf{H} \in \mathbb{R}^{N\times K}$ to $\mathbf{I}_K$, the identity matrix of size K. The achievable rates for linear equalization are characterized in the following theorem (see, e.g., [16]).

Theorem 3 (Performance of linear equalization) *Let* $\mathbf{\Sigma} = \left(P^{-1}\mathbf{I}_K + \mathbf{H}^{\mathsf{T}}\mathbf{H}\right)^{-1}$ *and let* $\sigma_k^2 = \mathbf{\Sigma}_{kk}$. *Then, any rate tuple* $(R_1, \ldots, R_K)$ *that satisfies*

$$R_k < \frac{1}{2}\log\left(\frac{P}{\sigma_k^2}\right) \tag{15}$$

is achievable over the Gaussian MAC (6) *with power constraint* P, *under linear equalization.*

[1] The 1+ term from the capacity expression $C = \frac{1}{2}\log(1+P)$ is lost to compensate for the dependence between $\mathbf{x}_k$ and $\mathbf{e}_k = \mathbf{x}_k - \tilde{\mathbf{y}}_k$. However, if we set $\mathbf{H} = 1$ to model a point-to-point AWGN channel, we find that (15) is equal to the AWGN capacity $1/2\log(1+P)$ as desired. See [4], [15, Lemma 2] for more details.

3 Exploiting Linear Structure

As discussed above, many of the coding strategies employed in practice can be viewed as lattice codes. It turns out that the linear structure of these lattice code ensembles opens up a new equalization possibility: rather than decoding each codeword individually, we can directly decode any integer-linear combination of codewords. Specifically, since the lattice is closed under addition, any integer-linear combination of lattice points is itself a lattice point, and thus afforded the same protection against noise as the original codewords.

To illustrate the potential gains of this approach, consider the following example from [17].

Example 1 *There are $K = 2$ users and $N = 2$ receive antennas. The channel matrix is integer-valued*

$$\mathbf{H} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \tag{16}$$

From (6)*, the receiver observes*

$$\mathbf{Y} = \begin{bmatrix} 2\mathbf{x}_1^{\mathsf{T}} + \mathbf{x}_2^{\mathsf{T}} \\ \mathbf{x}_1^{\mathsf{T}} + \mathbf{x}_2^{\mathsf{T}} \end{bmatrix} + \mathbf{Z} \ . \tag{17}$$

For large P, the linear equalizer roughly reduces to inverting the matrix $\mathbf{H}$, i.e., $\mathbf{b}_1^{\mathsf{T}} = [1 \quad -1]$ and $\mathbf{b}_2^{\mathsf{T}} = [-1 \quad 2]$, which yields the effective channel outputs

$$\tilde{\mathbf{y}}_1 = \mathbf{x}_1 + \mathbf{b}_1^{\mathsf{T}}\mathbf{Z} \tag{18}$$

$$\tilde{\mathbf{y}}_2 = \mathbf{x}_2 + \mathbf{b}_2^{\mathsf{T}}\mathbf{Z} \ , \tag{19}$$

and rates

$$R_1 = \frac{1}{2}\log\left(1 + \frac{P}{2}\right) \approx \frac{1}{2}\log\left(\frac{P}{2}\right) \tag{20}$$

$$R_2 = \frac{1}{2}\log\left(1 + \frac{P}{5}\right) \approx \frac{1}{2}\log\left(\frac{P}{5}\right) \tag{21}$$

where the approximations become tight as P increases. On the other hand, if both encoders employ the same lattice code, then the integer-linear combinations $2\mathbf{x}_1 + \mathbf{x}_2$ and $\mathbf{x}_1 + \mathbf{x}_2$ are themselves codewords and can be decoded at

rates

$$R_1 = \frac{1}{2}\log\left(\frac{1}{5} + P\right) \approx \frac{1}{2}\log(P) \tag{22}$$

$$R_2 = \frac{1}{2}\log\left(\frac{1}{2} + P\right) \approx \frac{1}{2}\log(P)\ . \tag{23}$$

as will be shown by Theorem 4. After removing the noise, we can solve for the desired codewords $\mathbf{x}_1$ *and* $\mathbf{x}_2$*. The high-level intuition is that this strategy offers an advantage since it does not enhance the noise during the linear equalization step.*

The example above demonstrates that there can be performance advantages to recovering integer-linear combinations as an intermediate step towards decoding the transmitted messages. We now turn to the general case where the channel coefficients are not necessarily integer-valued. As we will see, it is still possible to decode integer-linear combinations of codewords, and the performance is determined by how closely the integer coefficients approximate the real-valued channel gains. First, we need to be a bit more precise about what we mean by recovering linear combinations.

Definition 7 *A* $(2^{TR_1}, \ldots, 2^{TR_K}, T, P)$ *computation code for the channel* (6) *consists of*

- K *message sets* $\{1, 2, \ldots, 2^{TR_k}\}$, $k = 1, \ldots, K$,
- K *encoders, where encoder* k *assigns a unique* T*-dimensional vector* $\mathbf{x}_k(m_k) \in \mathbb{R}^T$ *to each message* $m_k \in \{1, 2, \ldots, 2^{TR_k}\}$*. All encoders are subject to a power constraint* $P > 0$*, which dictates that* $\|\mathbf{x}_k(m_k)\|^2 \leq TP$ *for all* $k = 1, \ldots, K$ *and* $m_k \in \{1, 2, \ldots, 2^{TR_k}\}$,
- *and, for a chosen integer vector* $\mathbf{a} = [a_1 \ \cdots \ a_K]^\mathsf{T} \in \mathbb{Z}^K$*, a decoder that assigns an estimate* $\hat{\mathbf{v}}$ *of the integer-linear combination of the codewords* $\mathbf{v} = \sum_{k=1}^K a_k \mathbf{x}_k(m_k)$ *to each possible received sequence* $\mathbf{Y} \in \mathbb{R}^{N \times T}$*.*

For a given channel matrix $\mathbf{H} \in \mathbb{R}^{N \times K}$ and integer vector $\mathbf{a} \in \mathbb{Z}^K$, the average error probability of a computation code is defined as

$$p_{\text{error}} = \Pr(\hat{\mathbf{v}} \neq \mathbf{v})\ . \tag{24}$$

The rates at which it is possible to recover an integer-combination depends on both the vector of integer coefficients $\mathbf{a} \in \mathbb{Z}^K$ and the channel matrix $\mathbf{H} \in \mathbb{R}^{N \times K}$ as well as the power P. The definition below is useful for concisely describing the computation rate.

Definition 8 *The computation rate function $R(\mathbf{H}, \mathbf{a}, P)$ is achievable over the channel (6) if, for any $\epsilon > 0$ and T large enough, there exists a $(2^{TR_1}, \ldots, 2^{TR_K}, T, P)$ computation code such that, for any $\mathbf{H} \in \mathbb{R}^{N \times K}$ and $\mathbf{a} \in \mathbb{Z}^K$, we have that $p_{error} < \epsilon$ if*

$$R_k < R(\mathbf{H}, \mathbf{a}, P) \quad \forall k \ . \tag{25}$$

According to the definition above, the receiver is free to recover *any* integer-linear combination of codewords for which (25) is satisfied. That is, the transmitters are completely agnostic as to the choice of the integer coefficients as well as the channel matrix $\mathbf{H}$, i.e., a codeword depends only on the selected message.

Remark 1 *For the sake of conciseness, we have focused on the symmetric case $R_1 = \cdots = R_K$. Specifically, for a given $\mathbf{H}$ and $\mathbf{a}$, all rates $R_1, \ldots, R_K$ must be below the scalar rate threshold given by $R(\mathbf{H}, \mathbf{a}, P)$, which can be thought of as setting all rates equal to one another. More generally, we might expect to describe the attainable performance by a region. See [18] for relevant definitions and theorems.*

Example 2 *We can interpret a capacity-achieving multiple-access code as a computation code in the following sense. A multiple-access code allows the receiver to decode all of the transmitted messages, from which it can reconstruct the transmitted codewords, and then any integer-linear combination of interest. It follows from Theorem 2 that the computation rate described by the function*

$$R(\mathbf{H}, \mathbf{a}, P) = \min_{\mathcal{S} \subset [K]} \frac{1}{2|\mathcal{S}|} \log \det \left(\mathbf{I} + P \mathbf{H}_{\mathcal{S}}^{\mathsf{T}} \mathbf{H}_{\mathcal{S}} \right), \tag{26}$$

which has no dependence on the integer vector $\mathbf{a}$, is achievable.

Intuitively, we expect that, for a more interesting computation code, $R(\mathbf{H}, \mathbf{a}, P)$ should depend on $\mathbf{a}$ and should be larger than (26) whenever $\mathbf{H}$ and $\mathbf{a}$ are "close." Our approach is for each encoder to employ the same

lattice codebook $\mathcal{L} = \Lambda \cap \mathcal{V}$. Since all codewords can be viewed as elements of the lattice, $\mathbf{x}_k(m_k) \in \Lambda$, then we have that integer-linear combinations are elements of the lattice as well $\sum_{k=1}^{K} a_k \mathbf{x}_k(m_k) \in \Lambda$. The key idea is that, if the lattice codebook is designed to tolerate noise up to a certain variance, then we can recover any integer-linear combinations for which the effective noise variance is below this level. Overall, the job of the each encoder is simple: it maps its message m_k into the corresponding lattice codeword $\mathbf{x}_k(m_k)$, and transmits it, paying no attention to nature's choice of the channel matrix $\mathbf{H}$ or the receiver's choice of the integer vector $\mathbf{a}$.

At the receiver, our goal is to recover $\mathbf{v} = \sum_{k=1}^{K} a_k \mathbf{x}_k(m_k) = \mathbf{a}^{\mathsf{T}}\mathbf{X}$ from $\mathbf{Y}$. We are free to select the integer vector $\mathbf{a}$ based on our knowledge of $\mathbf{H}$. As a first step, we use an equalization vector $\mathbf{b} \in \mathbb{R}^N$ to create the effective channel

$$\begin{aligned} \tilde{\mathbf{y}}^{\mathsf{T}} &= \mathbf{b}^{\mathsf{T}}\mathbf{Y} && (27)\\ &= \mathbf{b}^{\mathsf{T}}\mathbf{H}\mathbf{X} + \mathbf{b}^{\mathsf{T}}\mathbf{Z} && (28)\\ &= \mathbf{a}^{\mathsf{T}}\mathbf{X} + \mathbf{z}_{\text{eff}}^{\mathsf{T}} && (29) \end{aligned}$$

where

$$\mathbf{z}_{\text{eff}}^{\mathsf{T}} = (\mathbf{b}^{\mathsf{T}}\mathbf{H} - \mathbf{a}^{\mathsf{T}})\mathbf{X} + \mathbf{b}^{\mathsf{T}}\mathbf{Z} \ . \tag{30}$$

It can be shown that the effective noise variance is

$$\frac{1}{n}\mathbb{E}\|\mathbf{z}_{\text{eff}}\|^2 = \|\mathbf{b}\|^2 + P\|\mathbf{H}^{\mathsf{T}}\mathbf{b} - \mathbf{a}\|^2 \ . \tag{31}$$

This variance is minimized by taking $\tilde{\mathbf{y}}^{\mathsf{T}}$ to be the linear least-squares error (LLSE) estimator of the integer-linear combination $\mathbf{a}^{\mathsf{T}}\mathbf{X}$ from the channel output $\mathbf{Y}$, which corresponds to setting the equalization vector to

$$\mathbf{b} = P\mathbf{a}^{\mathsf{T}}\mathbf{H}^{\mathsf{T}}\big(\mathbf{I} + P\mathbf{H}\mathbf{H}^{\mathsf{T}}\big)^{-1} \ . \tag{32}$$

We define the resulting effective noise variance to be

$$\sigma^2_{\text{eff}}(\mathbf{H}, \mathbf{a}, P) = \mathbf{a}^{\mathsf{T}}\big(P^{-1}\mathbf{I} + \mathbf{H}^{\mathsf{T}}\mathbf{H}\big)^{-1}\mathbf{a} \ . \tag{33}$$

After this equalization step, the receiver uses a lattice quantizer to obtain an estimate of the integer-linear combination $\hat{\mathbf{v}} = Q_\Lambda(\tilde{\mathbf{y}})$. For a good lattice code, the receiver can successfully decode if $R < \log(P/\sigma^2_{\text{eff}}(\mathbf{H}, \mathbf{a}, P))$. Overall, this strategy leads to the following theorem [5, 17, 18].

Theorem 4 (Computation rate region) *The computation rate region described by the function*

$$R(\mathbf{H}, \mathbf{a}, P) = \frac{1}{2} \log \left(\frac{P}{\sigma^2_{\text{eff}}(\mathbf{H}, \mathbf{a}, P)} \right) \tag{34}$$

$$= -\frac{1}{2} \log \left(\mathbf{a}^{\mathsf{T}} \left(\mathbf{I} + P \mathbf{H}^{\mathsf{T}} \mathbf{H} \right)^{-1} \mathbf{a} \right) \tag{35}$$

is achievable over the channel (6) *with power constraint* P.

Note that the matrix $\left(\mathbf{I} + P \mathbf{H}^{\mathsf{T}} \mathbf{H} \right)^{-1}$ is symmetric and positive definite, and therefore admits a Cholesky decomposition

$$\left(\mathbf{I} + P \mathbf{H}^{\mathsf{T}} \mathbf{H} \right)^{-1} = \mathbf{L} \mathbf{L}^{\mathsf{T}}, \tag{36}$$

where $\mathbf{L}$ is a lower triangular matrix with strictly positive diagonal entries. With this notation, we can express the computation rate function as

$$R(\mathbf{H}, \mathbf{a}, P) = -\frac{1}{2} \log \| \mathbf{L}^{\mathsf{T}} \mathbf{a} \|^2. \tag{37}$$

In many cases, the receiver is interested in decoding L linearly independent linear combinations, but does not care about the particular coefficients. Therefore, we can use the L linearly independent integer vectors $\mathbf{a}_1, \ldots, \mathbf{a}_L$ that yield the highest computation rates $R(\mathbf{H}, \mathbf{a}_1, P) \geq \cdots \geq R(\mathbf{H}, \mathbf{a}_L, P)$. Accordingly, we define the k^{th} computation rate $R_{\text{comp},k}(\mathbf{H}, P) \triangleq R(\mathbf{H}, \mathbf{a}_k, P)$ to be the rate associated with decoding the k^{th} best integer coefficient vector $\mathbf{a}_k$ that is linearly independent of $\{\mathbf{a}_1, \ldots, \mathbf{a}_{k-1}\}$.

In some applications, it suffices to recover $L < K$ linear combinations at a single receiver. For instance, K receivers could each decode one (linearly independent) integer-linear combination and forward it to a single node that solves for the transmitted codewords. In other cases, it will be of interest to recover K (linearly independent) integer-linear combinations at a single receiver. Overall, if we wish to recover L linear combinations, then the rate of the lattice codebook must be smaller than $R_{\text{comp},L}(\mathbf{H}, P)$.

As a concrete example, consider the *integer-forcing* architecture for a Gaussian MAC as illustrated in Figure 1. Each of the K users employs the same lattice codebook. Similarly to the strategy used to establish Theorem 3, the receiver applies a linear equalizer $\mathbf{B}$ to its observation $\mathbf{Y}$ to obtain the effective channel output $\tilde{\mathbf{Y}} = \mathbf{B}\mathbf{Y}$. In Theorem 3, this equalization step

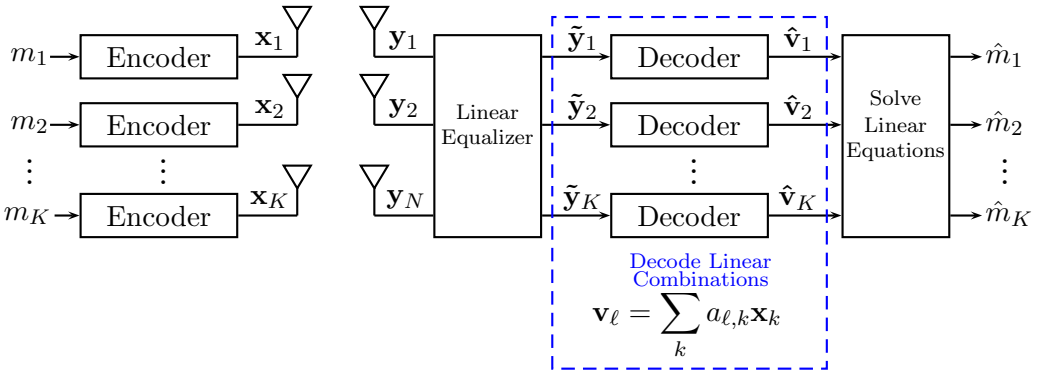

Figure 1: The integer-forcing receiver architecture. The receiver employs linear equalization followed by parallel decoding to recover K linear combinations of the transmitted codewords. It can then solve for the individual codewords (and thus the original messages).

is used to induce an effective channel that is close to the identity matrix, which facilitates the parallel decoding of the K transmitter codewords. For the integer-forcing receiver, the equalization is instead used to create any effective integer-valued, full-rank channel matrix $\mathbf{A}$. Parallel decoding can then be used to reliably decode the integer-linear combinations $\mathbf{AX}$, which can then be solved for the desired individual messages.

4 Universal Bounds via Successive Minima

In this section, we derive bounds on the computation rates $\{R_{\text{comp},k}(\mathbf{H}, P)\}_{k=1}^{K}$ using known results about the successive minima of a lattice. These bounds can be used to approximate computation rates without first finding the optimal integer coefficients.

Definition 9 (Successive minima) *Let $\Lambda(\mathbf{G})$ be the lattice spanned by the full-rank matrix $\mathbf{G} \in \mathbb{R}^{K\times K}$. For $k = 1, \ldots, K$, we define the k^{th} successive minimum as*

$$\lambda_k(\mathbf{G}) \triangleq \inf\left\{r \;:\; \dim\left(\text{span}\left(\Lambda(\mathbf{G})\bigcap \mathcal{B}(\mathbf{0}, r)\right)\right) \geq k\right\}.$$

In words, the k^{th} successive minimum of a lattice is the minimal radius of a ball centered around $\mathbf{0}$ that contains k linearly independent lattice points.

Let $\mathbf{L}$ be the matrix defined in (36), $\Lambda(\mathbf{L}^\mathsf{T})$ be the lattice generated by $\mathbf{L}^\mathsf{T}$, and $\lambda_k(\mathbf{L}^\mathsf{T})$ its k^{th} successive minimum. By (37) and the definition of $R_{\text{comp},k}(\mathbf{H}, P)$, we have that

$$R_{\text{comp},k}(\mathbf{H}, P) = -\log \lambda_k(\mathbf{L}^\mathsf{T}). \tag{38}$$

It follows that any upper bound on $\lambda_k(\mathbf{L}^\mathsf{T})$ immediately translates to a lower bound on $R_{\text{comp},k}(\mathbf{H}, P)$. For $k = 1$, such bounds are given by Minkowski's first theorem. Let $V_K = \text{Vol}(\mathcal{B}(\mathbf{0}, 1))$ be the volume of the K-dimensional unit ball. While an explicit expression

$$V_K = \frac{\pi^{K/2}}{\Gamma(K/2+1)},$$

exists, we will be content with the estimate $V_K \geq 2^K K^{-K/2}$, which is obtained by noting that $\mathcal{B}(\mathbf{0}, 1)$ contains a cube with side $2/\sqrt{K}$ [19].

Theorem 5 (Minkowski's First Theorem) *For any full-rank* $\mathbf{G}$*,*

$$\lambda_1(\mathbf{G}) \leq 2\left(\frac{\left|\det(\mathbf{G})\right|}{V_K}\right)^{\frac{1}{K}} \leq \sqrt{K}\left|\det(\mathbf{G})\right|^{\frac{1}{K}}. \tag{39}$$

From Minkowki's first theorem we immediately obtain a lower bound on $R_{\text{comp},1}(\mathbf{H}, P)$, given as a simple function of $\mathbf{H}$, K, and P.

Theorem 6

$$R_{\text{comp},1}(\mathbf{H}, P) \geq \frac{1}{2K}\log\det(\mathbf{I} + P\mathbf{H}^\mathsf{T}\mathbf{H}) - \frac{1}{2}\log K. \tag{40}$$

Proof. From (38) and Theorem 5 we have that

$$\begin{aligned} R_{\text{comp},1}(\mathbf{H}, P) &\geq -\frac{1}{K}\log\left|\det(\mathbf{L}^T)\right| - \frac{1}{2}\log K \\ &= -\frac{1}{2K}\log\left|\det(\mathbf{L}\mathbf{L}^T)\right| - \frac{1}{2}\log K \\ &= \frac{1}{2K}\log\det(\mathbf{I} + P\mathbf{H}^\mathsf{T}\mathbf{H}) - \frac{1}{2}\log K, \end{aligned}$$

where the last equality follows from (36). ■

Theorem 2 implies that for any rate-tuple $(R_1, \ldots, R_K)$ that is achievable over the channel (6) with power constraint P, we must have

$$\sum_{k=1}^{K} R_k \leq \frac{1}{2} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}). \tag{41}$$

The expression on the right hand side of (41) is referred to as the *sum-capacity* of the channel.[2] Consequently, if the symmetric rate-tuple $(R, ..., R)$ is achievable, then we must have that

$$R \leq \frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}), \tag{42}$$

where the expression in the right hand side of (42) is an upper bound on the *symmetric capacity* of the channel. In light of this, the interpretation of Theorem 6 is that $R_{\text{comp},1}(\mathbf{H}, P)$ cannot be much smaller than the symmetric capacity, for all $\mathbf{H}$ and P.

Next, we turn to estimating $\sum_{k=1}^{K} R_{\text{comp},k}(\mathbf{H}, P)$. By (38), we have

$$\begin{aligned} \sum_{k=1}^{K} R_{\text{comp},k}(\mathbf{H}, P) &= -\sum_{k=1}^{K} \log \lambda_k(\mathbf{L}^{\mathsf{T}}) \\ &= -\log\left(\prod_{k=1}^{K} \lambda_k(\mathbf{L}^{\mathsf{T}})\right). \end{aligned} \tag{43}$$

Our goal is therefore to estimate the product of successive minima. Let $\mathbf{a}_1, \ldots, \mathbf{a}_K \in \mathbb{Z}^K$ be linearly independent vectors such that $\lambda_k(\mathbf{L}^{\mathsf{T}}) = \|\mathbf{L}^{\mathsf{T}}\mathbf{a}_k\|$, and let $\mathbf{A} = [\mathbf{a}_1|\cdots|\mathbf{a}_K] \in \mathbb{Z}^{K\times K}$. Since $|\det(\mathbf{A})| \geq 1$, we have

$$\left|\det(\mathbf{L}^T)\right| \leq \left|\det(\mathbf{L}^T)\right| \cdot \left|\det(\mathbf{A})\right| = \left|\det(\mathbf{L}^T\mathbf{A})\right| \leq \prod_{k=1}^{K} \|\mathbf{L}^{\mathsf{T}}\mathbf{a}_k\| = \prod_{k=1}^{K} \lambda_k(\mathbf{L}^{\mathsf{T}}). \tag{44}$$

An upper bound on the product of the successive minima is given by Minkowski's second theorem.

[2]Specifically, it can be shown that there is a choice of rates $R_1, \ldots, R_K$ satisfying $\sum_k R_k = \frac{1}{2}\log\det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H})$ that satisfies the capacity region constraints from Theorem 2 and any choice of rates with a higher sum rate $\sum_k R_k > \frac{1}{2}\log\det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H})$ will violate these capacity constraints.

Theorem 7 (Minkowski's Second Theorem) *For any full-rank* $\mathbf{G}$*,*

$$\prod_{k=1}^{K} \lambda_k(\mathbf{G}) \le 2^K \left(\frac{\left|\det(\mathbf{G})\right|}{V_K} \right) \le K^{K/2} \left|\det(\mathbf{G})\right|. \tag{45}$$

With (43), (44) and Theorem 7, we can establish the following.

Theorem 8 *[20, Theorem 3]*

$$\begin{aligned} \frac{1}{2}\log\det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}) - \frac{K}{2}\log K \le & \sum_{k=1}^{K} R_{\mathrm{comp},k}(\mathbf{H}, P) \\ & \le \frac{1}{2}\log\det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}). \end{aligned} \tag{46}$$

Proof. By the definition of $\mathbf{L}$ in (36), we have

$$\log\left|\det(\mathbf{L}^{\mathsf{T}})\right| = \frac{1}{2}\log\left|\det(\mathbf{L}\mathbf{L}^{\mathsf{T}})\right| = \frac{1}{2}\log\det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}). \tag{47}$$

The lower bound now follows from (43), (45) and (47), whereas the upper bound follows from (43), (44) and (47). ■

Theorem 8 asserts that the sum of the computation rates is never too far from the sum capacity of the channel (6) with power constraint P. An operational meaning for $\sum_{k=1}^{K} R_{\mathrm{comp},k}(\mathbf{H}, P)$ is given in [20], where a low-complexity coding scheme based on compute-and-forward for the Gaussian MAC (6) that achieves this sum-rate is proposed. The remarkable conclusion from Theorem 8, is that while the individual computation rates $\{R_{\mathrm{comp},k}(\mathbf{H}, P)\}$ may be very sensitive to the entries of $\mathbf{H}$, their sum is, to the first order, only influenced by the corresponding sum-capacity. This phenomenon is illustrated in Figure 2.

We are often particularly interested in estimating the value of $R_{\mathrm{comp},K}(\mathbf{H}, P)$, as this is the quantity that dictates the symmetric communication rate over the MAC channel (6) with power constraint P, when decoding is done via first recovering K integer linear combinations. However, directly estimating this quantity may be challenging, as it requires to first find $K-1$ linearly independent shortest lattice vectors. Estimating $R_{\mathrm{comp},1}(\mathbf{H}, P)$, on the

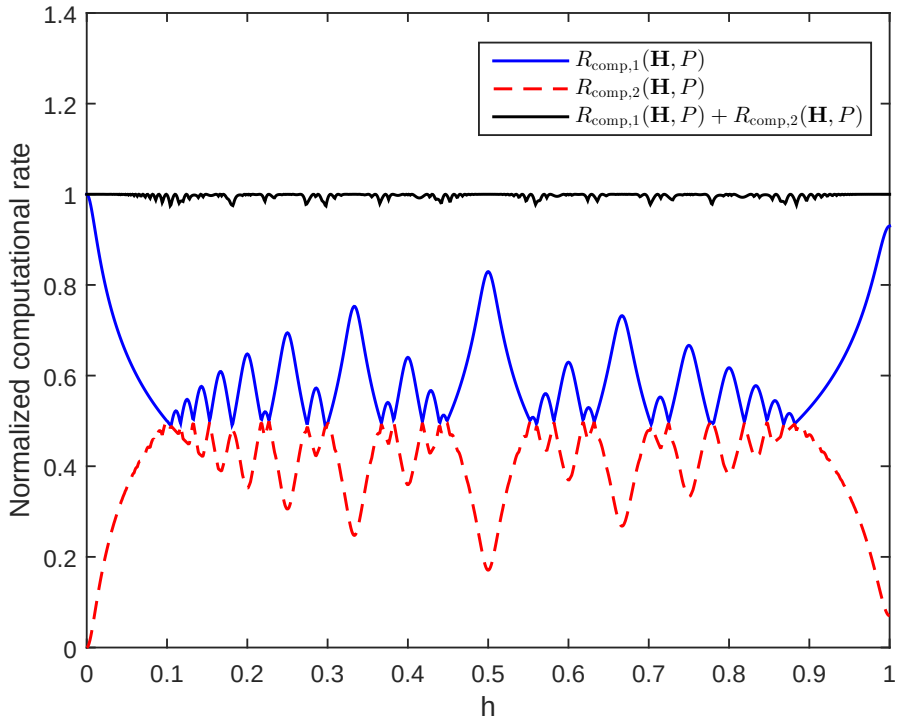

Figure 2: $R_{\text{comp},1}(\mathbf{H}, P)$ and $R_{\text{comp},2}(\mathbf{H}, P)$ as a function of h for the channel $\mathbf{y} = \mathbf{x}_1 + h\mathbf{x}_2 + \mathbf{z}$ at $P = 40$dB. The sum of these computation rates is nearly equal to the multiple-access sum capacity. All rates are normalized by this sum capacity $1/2 \log(1 + (1 + h^2)P)$.

other hand, is a much simpler task, as it only involves one shortest lattice vector. It is thus desirable to estimate $R_{\text{comp},K}(\mathbf{H}, P)$ as a function of $R_{\text{comp},1}(\mathbf{H}, P)$. Using the monotonicity of $R_{\text{comp},k}(\mathbf{H}, P)$ in k and Theorem 8, yields the following simple estimate, which shows that if $R_{\text{comp},1}(\mathbf{H}, P)$ is close to $\frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H})$, then so is $R_{\text{comp},K}(\mathbf{H}, P)$.

Proposition 1

$$\left[\frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}) - \frac{K}{2} \log K \right.$$
$$\left. - (K-1) \left(R_{\text{comp},1}(\mathbf{H}, P) - \frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}) \right) \right]^+$$

$$\leq R_{\text{comp},K}(\mathbf{H}, P) \leq \frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}), \tag{48}$$

where $[x]^+ = \max\{0, x\}$.

Proof. By definition, we have that $R_{\text{comp},1}(\mathbf{H}, P) \geq \cdots \geq R_{\text{comp},K}(\mathbf{H}, P)$, which implies that

$$\sum_{k=1}^{L} R_{\text{comp},k}(\mathbf{H}, P) \leq L \cdot R_{\text{comp},1}(\mathbf{H}, P) \tag{49}$$

$$\sum_{k=1}^{L} R_{\text{comp},k}(\mathbf{H}, P) \geq L \cdot R_{\text{comp},L}(\mathbf{H}, P). \tag{50}$$

The upper bound in (48) follows from (50) with $L = K$, combined with the upper bound from (43). To establish the lower bound in (48) we can write

$$\begin{aligned} R_{\text{comp},K}(\mathbf{H}, P) &= \sum_{k=1}^{K} R_{\text{comp},k}(\mathbf{H}, P) - \sum_{k=1}^{K-1} R_{\text{comp},k}(\mathbf{H}, P) \\ &\geq \frac{1}{2} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}) - \frac{K}{2} \log K - (K-1) R_{\text{comp},1}(\mathbf{H}, P), \end{aligned}$$

where we have used the lower bound from (43), and (49) applied with $L = K - 1$ in the last inequality. To arrive at the left hand side of (48), we write

$$\begin{aligned} R_{\text{comp},1}(\mathbf{H}, P) = &\frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}) \\ &+ \left(R_{\text{comp},1}(\mathbf{H}, P) - \frac{1}{2K} \log \det(\mathbf{I} + P\mathbf{H}^{\mathsf{T}}\mathbf{H}) \right). \end{aligned} \tag{51}$$

■

An alternative route for estimating $R_{\text{comp},K}(\mathbf{H}, P)$ involves studying the *dual lattice* of $\Lambda(\mathbf{L}^T)$.

Definition 10 (Dual lattice) *For a lattice* $\Lambda(\mathbf{G})$ *with a full-rank generator matrix* $\mathbf{G} \in \mathbb{R}^{K \times K}$*, the dual lattice is defined by*

$$\Lambda^*(\mathbf{G}) \triangleq \Lambda\left((\mathbf{G}^{\mathsf{T}})^{-1}\right). \tag{52}$$

By definition, we have that if $\mathbf{x} \in \Lambda(\mathbf{G})$ and $\mathbf{x}^* \in \Lambda^*(\mathbf{G})$, then $\mathbf{x}^\mathsf{T}\mathbf{x}^* \in \mathbb{Z}$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_K \in \Lambda(\mathbf{G})$ be linearly independent vectors such that $\|\mathbf{x}_k\| = \lambda_k(\mathbf{G})$ for $k = 1, \ldots, K$ and let $\mathbf{x}^* \in \Lambda^*(\mathbf{G})$ be such that $\|\mathbf{x}^*\| = \lambda_1\left((\mathbf{G}^\mathsf{T})^{-1}\right)$. Since $\{\mathbf{x}_1, \ldots, \mathbf{x}_K\}$ form a basis for $\mathbb{R}^K$, we must have that $\mathbf{x}_k^T\mathbf{x}^* \neq 0$ for some $k \in \{1, \ldots, K\}$. Thus, for this k, we must have that

$$\lambda_k(\mathbf{G})\,\lambda_1\left((\mathbf{G}^\mathsf{T})^{-1}\right) = \|\mathbf{x}_k\| \cdot \|\mathbf{x}^*\| \geq |\mathbf{x}_k^T\mathbf{x}^*| \geq 1, \tag{53}$$

where we have used the Cauchy-Schwartz inequality and the fact that $\mathbf{x}_k^T\mathbf{x}^* \in \mathbb{Z}$. Since $\lambda_k(\mathbf{G})$ is monotone in k and $k \leq K$, we conclude that

$$\lambda_K(\mathbf{G})\,\lambda_1\left((\mathbf{G}^\mathsf{T})^{-1}\right) \geq 1. \tag{54}$$

It turns out that the product of successive minima of a lattice and its dual can also be upper bounded.

Theorem 9 (Banaszczyk [21, Theorem 2.1]) *Let $\Lambda(\mathbf{G})$ be a lattice with a full-rank generating matrix $\mathbf{G} \in \mathbb{R}^{K\times K}$ and let $\Lambda^*(\mathbf{G}) = \Lambda\left((\mathbf{G}^\mathsf{T})^{-1}\right)$ be its dual lattice. The successive minima of $\Lambda(\mathbf{G})$ and $\Lambda^*(\mathbf{G})$ satisfy the following inequality*

$$\lambda_k(\mathbf{G})\,\lambda_{K-k+1}\left((\mathbf{G}^\mathsf{T})^{-1}\right) \leq K, \quad \forall k = 1, 2, \ldots, K.$$

Banaszczyk's theorem and (54) yield the following estimate on $R_{\mathrm{comp},K}(\mathbf{H}, P)$.

Theorem 10 *[22]*

$$\frac{1}{2}\log\left(\min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\|\mathbf{H}\mathbf{a}\|^2\right) - \log K \leq R_{\mathrm{comp},K}(\mathbf{H}, P) \leq \frac{1}{2}\log\left(\min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\|\mathbf{H}\mathbf{a}\|^2\right) \tag{55}$$

Proof. By (38), Theorem 9, applied with $k = K$, and (54) we have that

$$\log\lambda_1(\mathbf{L}^{-1}) - \log K \leq R_{\mathrm{comp},K}(\mathbf{H}, P) \leq \log\lambda_1(\mathbf{L}^{-1}). \tag{56}$$

By definition of successive minima,

$$\begin{aligned}\lambda_1^2(\mathbf{L}^{-1}) &= \min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{L}^{-1}\mathbf{a}\|^2 \\ &= \min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \mathbf{a}^{\mathsf{T}}(\mathbf{L}\mathbf{L}^{\mathsf{T}})^{-1}\mathbf{a} \\ &= \min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \mathbf{a}^{\mathsf{T}}(\mathbf{I}+P\mathbf{H}^{\mathsf{T}}\mathbf{H})\mathbf{a}, \end{aligned} \tag{57}$$

where we have used the definition of $\mathbf{L}$ from (36) in the last equality. The theorem now follows by substituting (57) in (56). ■

5 Asymptotic Bounds

For the single-user AWGN channel (1) with power constraint P, the capacity is $C(P) = \frac{1}{2}\log(1+P)$ bits/channel use, by Theorem 1. The MAC channel model (6) with power constraint P is richer than the AWGN model (unless $N = K = 1$), but we would nevertheless like to compare it to a simple AWGN channel. In our context, the notion of degrees-of-freedom (DoF) is a first-order approximation that measures how many AWGN channels (or fractions thereof) are needed to attain the same rate as the MAC sum capacity. To be precise, let $C(\mathbf{H}, P)$ be the sum-capacity of the channel (6), i.e.,

$$C(\mathbf{H}, P) \triangleq \frac{1}{2}\log\det\left(\mathbf{I}+P\mathbf{H}^{\mathsf{T}}\mathbf{H}\right). \tag{58}$$

Then, the DoF offered by the MAC channel (6) with channel matrix $\mathbf{H}$ is defined as

$$\mathsf{DoF}(\mathbf{H}) \triangleq \lim_{P\to\infty}\frac{C(\mathbf{H},P)}{C(P)} = \lim_{P\to\infty}\frac{\log\det\left(\mathbf{I}+P\mathbf{H}^{\mathsf{T}}\mathbf{H}\right)}{\log(1+P)}. \tag{59}$$

It is well known that $\mathsf{DoF}(\mathbf{H}) = \mathrm{rank}(\mathbf{H})$. In particular, for almost all $\mathbf{H} \in \mathbb{R}^{N\times K}$ (w.r.t. Lebesgue measure) we have that $\mathsf{DoF}(\mathbf{H}) = \min(K, N)$.

In order to characterize the asymptotic behavior of communication schemes based on decoding integer-linear combinations, we define the DoF associated with decoding the best ℓ equations as

$$d_{\mathrm{comp},\ell}(\mathbf{H}) = \lim_{P\to\infty}\frac{R_{\mathrm{comp},\ell}(\mathbf{H},P)}{\frac{1}{2}\log(1+P)}. \tag{60}$$

By Theorem 8, we have that

$$\frac{C(\mathbf{H},P)-\frac{K}{2}\log(K)}{C(P)} \leq \sum_{k=1}^{K} \frac{R_{\mathrm{comp},k}(\mathbf{H},P)}{\frac{1}{2}\log(1+P)} \leq \frac{C(\mathbf{H},P)}{C(P)}. \tag{61}$$

Since the upper and lower bounds coincide in the limit of $P \to \infty$, we see that

$$\sum_{k=1}^{K} d_{\mathrm{comp},k}(\mathbf{H}) = \mathsf{DoF}(\mathbf{H}) = \mathrm{rank}(\mathbf{H}) \leq \min\{K,N\}. \tag{62}$$

The main purpose of this section is to show that for almost all $\mathbf{H} \in \mathbb{R}^{N\times K}$ (w.r.t. the Lebesgue measure) we have that $d_{\mathrm{comp},1}(\mathbf{H}) = \cdots = d_{\mathrm{comp},K}(\mathbf{H}) = \frac{\min\{K,N\}}{K}$. By (62) and the monotonicity of $d_{\mathrm{comp},k}(\mathbf{H})$, it suffices to show that for almost every $\mathbf{H}$ we have $d_{\mathrm{comp},K}(\mathbf{H}) \geq \frac{\min\{K,N\}}{K}$. Our focus will therefore be on establishing lower bounds for $d_{\mathrm{comp},K}(\mathbf{H})$.

Our starting point is Theorem 10. Denoting the K^{th} singular value of $\mathbf{H}$ by $\sigma_K(\mathbf{H})$, this theorem gives

$$\begin{aligned} R_{\mathrm{comp},K}(\mathbf{H},P) &\geq \frac{1}{2}\log\left(\min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\|\mathbf{H}\mathbf{a}\|^2\right) - \log K \\ &\geq \frac{1}{2}\log\left(\min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\sigma_K^2(\mathbf{H})\|\mathbf{a}\|^2\right) - \log K \\ &\geq \frac{1}{2}\log\left(1+P\sigma_K^2(\mathbf{H})\right) - \log K. \end{aligned} \tag{63}$$

Since $\sigma_K^2(\mathbf{H})$ is strictly above 0 whenever $\mathrm{rank}(\mathbf{H}) = K$, we conclude that if $\mathrm{rank}(\mathbf{H}) = K$ then $d_{\mathrm{comp},K}(\mathbf{H}) = 1$. For $K \leq N$, this is indeed the case for almost every $\mathbf{H} \in \mathbb{R}^{N\times K}$. Thus, we have established that if $K \leq N$ then $d_{\mathrm{comp},K}(\mathbf{H}) \geq \frac{\min\{K,N\}}{K}$ for almost every $\mathbf{H} \in \mathbb{R}^{N\times K}$. The interesting case is therefore $N < K$, which we assume in the proceeding derivation.

Instead of bounding (63) in terms of $\sigma_K(\mathbf{H})$, we can resort to the tradeoff between the allowed length of $\mathbf{a}$ and the smallest attainable $\|\mathbf{H}\mathbf{a}\|$ [22]

$$\begin{aligned} R_{\mathrm{comp},K}(\mathbf{H},P) &\geq \frac{1}{2}\log\left(\min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\|\mathbf{H}\mathbf{a}\|^2\right) - \log K \\ &\geq \frac{1}{2}\log\left(\min_{\mathbf{a}\in\mathbb{Z}^K\setminus\{\mathbf{0}\}} \|\mathbf{a}\|_\infty^2 + P\|\mathbf{H}\mathbf{a}\|_\infty^2\right) - \log K, \end{aligned} \tag{64}$$

where for $\mathbf{x} \in \mathbb{R}^m$ we define $\|\mathbf{x}\|_\infty = \max\{|x_1|, \ldots, |x_m|\}$. For $0 < \epsilon < 1$, define $\kappa_\epsilon(\mathbf{H}) \geq 0$ as

$$\kappa_\epsilon(\mathbf{H}) \triangleq \inf_{\mathbf{a} \in \mathbb{Z}^K \setminus \{\mathbf{0}\}} \frac{\|\mathbf{H}\mathbf{a}\|_\infty}{\|\mathbf{a}\|_\infty^{1 - \frac{K}{N}\frac{1}{1-\epsilon}}}. \tag{65}$$

We have that

$$\begin{aligned}
\min_{\mathbf{a} \in \mathbb{Z}^K \setminus \{\mathbf{0}\}} \|\mathbf{a}\|_\infty^2 + P\|\mathbf{H}\mathbf{a}\|_\infty^2 &\geq \min_{\ell = 1,2,\ldots} \ell^2 + P\kappa_\epsilon^2(\mathbf{H})\ell^{2\left(1 - \frac{K}{N}\frac{1}{1-\epsilon}\right)} \\
&\geq \min_{t > 0} t + P\kappa_\epsilon^2(\mathbf{H}) t^{1 - \frac{K}{N}\frac{1}{1-\epsilon}} \\
&= \frac{1}{1 - \frac{N}{K}(1-\epsilon)} \cdot \left(\frac{K}{N} \frac{1}{1-\epsilon} - 1 \right)^{\frac{N}{K}(1-\epsilon)} \cdot \left(\kappa_\epsilon^2(\mathbf{H}) P \right)^{\frac{N}{K}(1-\epsilon)},
\end{aligned} \tag{66}$$

where the last equality is obtained by straightforward differentiation. Substituting (66) in (64) and recalling the definition of $d_{\mathrm{comp},K}(\mathbf{H})$, we have established that for any $0 < \epsilon < 1$, the following holds

$$d_{\mathrm{comp},K}(\mathbf{H}) \geq \frac{N}{K}(1-\epsilon) \left(1 + 2 \lim_{P \to \infty} \frac{\log \kappa_\epsilon(\mathbf{H})}{\log P} \right). \tag{67}$$

It now remains to show that $\kappa_\epsilon(\mathbf{H}) > 0$ for every $0 < \epsilon < 1$, and almost every $\mathbf{H}$. To this end, we resort to the literature on *systems of small linear forms*. Several results in this field can be used, depending on whether the entries of $\mathbf{H}$ are independent or dependent (i.e., they can be characterized by fewer than NK parameters). Below, we state the most general available result, which was recently obtained by Beresnevich, Bernik and Budarina [23].

5.1 Small Linear Forms

We will need several definitions before we can state (an adaptation of) the main result from [23].

For $j = 1, \ldots, N$, let $U_j \subset \mathbb{R}^{d_j}$ be an open ball, and $\mathbf{f}_j = (f_{j1}, \ldots, f_{jK}) : U_j \mapsto \mathbb{R}^K$ be functions. For $(\mathbf{x}_1, \ldots, \mathbf{x}_N) \in U_1 \times \cdots \times U_N$, we define

$$\mathbf{F} = \mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_N) \triangleq \begin{bmatrix} \mathbf{f}_1(\mathbf{x}_1) \\ \vdots \\ \mathbf{f}_N(\mathbf{x}_N) \end{bmatrix} = \begin{bmatrix} f_{11}(\mathbf{x}_1) & \ldots & f_{1K}(\mathbf{x}_1) \\ \vdots & \vdots & \vdots \\ f_{N1}(\mathbf{x}_N) & \ldots & f_{NK}(\mathbf{x}_N) \end{bmatrix} \in \mathbb{R}^{N \times K}. \tag{68}$$

For $\rho > 0$, define the set

$$\mathcal{W}(\mathbf{F}, \rho) \triangleq \Big\{ (\mathbf{x}_1, \ldots, \mathbf{x}_N) \in U_1 \times \cdots \times U_N \ : \ \|\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_N)\mathbf{a}\|_\infty < (\|\mathbf{a}\|_\infty)^{-\rho}) \text{ for infinitely many } \mathbf{a} \in \mathbb{Z}^K \setminus \{\mathbf{0}\} \Big\}. \tag{69}$$

Theorem 11 ([23, Theorem 2]) *Let $K > N \geq 1$ be integers, and let $U_1, \ldots, U_N$, $\mathbf{f}_1, \ldots, \mathbf{f}_N$, $\mathbf{F}$ and $\mathcal{W}(\mathbf{F}, \rho)$ be as above. Suppose that for each $j = 1, \ldots, N$ the coordinate functions $f_{j1}, \ldots, f_{jK}$ of the map $\mathbf{f}_j$ are analytic and linearly independent over $\mathbb{R}$. Then,*

$$\mu\left(\mathcal{W}(\mathbf{F}, \rho)\right) = \begin{cases} 0 & \text{if } \rho > \frac{K}{N} - 1, \\ \prod_{j=1}^{N} \mu(U_j) & \text{if } \rho \leq \frac{K}{N} - 1 \end{cases} \tag{70}$$

where $\mu(B)$ denotes the Lebesgue measure of a set $B \subset \mathbb{R}^d$.

An immediate corollary of Theorem 11 is the following.

Corollary 1 *Let $K > N \geq 1$ be integers, and let $U_1, \ldots, U_N$, $\mathbf{f}_1, \ldots, \mathbf{f}_N$, $\mathbf{F}$ and $\mathcal{W}(\mathbf{F}, \rho)$ be as above. Suppose that, for each $j = 1, \ldots, N$, the coordinate functions $f_{j1}, \ldots, f_{jK}$ of the map $\mathbf{f}_j$ are analytic and linearly independent over $\mathbb{R}$. Then, for any $0 < \epsilon < 1$ and almost every $(\mathbf{x}_1, \ldots, \mathbf{x}_N) \in U_1 \times \cdots \times U_N$, we have that $\kappa_\epsilon(\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_N)) > 0$.*

We can now combine Corollary 1 and (67) for several cases of particular interest.

5.2 Independent Channel Gains

A common assumption in wireless communication is that the entries h_{ij} of the channel matrix $\mathbf{H} \in \mathbb{R}^{N \times K}$ are independent. In the context of Theorem 11, this corresponds to taking $U_j = [-\tau, \tau]^K$ for all $j = 1, \ldots, N$, where $\tau \in \mathbb{R}^+$ is some large number, and $\mathbf{f}_j(\mathbf{x}_j) = (x_{j1}, \ldots, x_{jK})$. These functions certainly satisfy the conditions of Corollary 1, and we can therefore deduce the following.

Corollary 2 *Let $K > N \geq 1$. For almost every $\mathbf{H} \in \mathbb{R}^{N \times K}$ we have that $\kappa_\epsilon(\mathbf{H}) > 0$.*

Now, combining the corollary above and (67) we see that for $K > N \geq 1$ we have that $d_{\mathrm{comp},K}(\mathbf{H}) \geq \frac{N}{K}$ for almost every $\mathbf{H} \in \mathbb{R}^{N\times K}$. Recalling that for $1 \leq K \leq N$ we have that $d_{\mathrm{comp},K}(\mathbf{H}) \geq 1$ for almost every $\mathbf{H} \in \mathbb{R}^{N\times K}$, we recover the following lemma from [22].[3]

Lemma 1 ([22, Lemma 3]) *For almost every* $\mathbf{H} \in \mathbb{R}^{N\times K}$,

$$K \cdot d_{comp,K}(\mathbf{H}) = \min\{K, N\}. \tag{71}$$

Roughly speaking, this allows us to conclude that, in the limit of large P, the integer-forcing strategy does as well as the optimal sum-capacity-achieving scheme.

5.3 Dependent Channel Gains

In many applications of interest, the channel model $\mathbf{Y} = \mathbf{HX} + \mathbf{Z}$ represents an effective channel induced by certain signal processing operations performed at the transmitters and the receivers. Often, these operations create dependencies between the entries of $\mathbf{H}$, which requires replacing the Lebesgue measure in the DoF analysis with a measure on a suitable manifold.

As a canonical example, we will consider the symmetric two-user X-channel [25–29]. This channel consists of two transmitters emitting the signals $\mathbf{x}_1$ and $\mathbf{x}_2$, respectively, each in $\mathbb{R}^{1\times T}$ and satisfying the power constraint $\|\mathbf{x}_k\|^2 \leq TP$, and two receivers observing the signals

$$\begin{aligned}\mathbf{y}_1 &= \mathbf{x}_1 + g\mathbf{x}_2 + \mathbf{z}_1\\ \mathbf{y}_2 &= g\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{z}_2,\end{aligned}$$

respectively, where $\mathbf{z}_1, \mathbf{z}_2 \in \mathbb{R}^{1\times T}$ are two statistically independent i.i.d. $\mathcal{N}(0,1)$ noises. Each transmitter has two messages, one for the first receiver and one for the second receiver, and we assume all four messages are of the same rate R. We now describe one particular transmission scheme for this channel. We use one lattice codebook of rate R and power P, such that the message from user k to receiver j is encoded to a lattice codeword $\tilde{\mathbf{x}}_{jk}$. The users then transmit

$$\mathbf{x}_1 = \frac{1}{\sqrt{1+g^2}}\left(\tilde{\mathbf{x}}_{11} + g\tilde{\mathbf{x}}_{21}\right)$$

[3]The proof of Lemma 3 from [22] relied on [24, Corollary 2], which can be obtained as a special case of [23, Theorem 2].

$$\mathbf{x}_2 = \frac{1}{\sqrt{1+g^2}} \left(\tilde{\mathbf{x}}_{22} + g\tilde{\mathbf{x}}_{12} \right).$$

Consequently, the receivers observe

$$\mathbf{y}_1 = \frac{1}{\sqrt{1+g^2}} \left(\tilde{\mathbf{x}}_{11} + g(\tilde{\mathbf{x}}_{21} + \tilde{\mathbf{x}}_{22}) + g^2\tilde{\mathbf{x}}_{12} \right) + \mathbf{z}_1$$
$$\mathbf{y}_2 = \frac{1}{\sqrt{1+g^2}} \left(\tilde{\mathbf{x}}_{22} + g(\tilde{\mathbf{x}}_{12} + \tilde{\mathbf{x}}_{11}) + g^2\tilde{\mathbf{x}}_{21} \right) + \mathbf{z}_1.$$

Since the channel output is symmetric across receivers, it suffices to analyze the rates that allow the first receiver to decode its two desired codewords $\tilde{\mathbf{x}}_{11}$ and $\tilde{\mathbf{x}}_{12}$. Noting that $\tilde{\mathbf{x}}_2 \triangleq \tilde{\mathbf{x}}_{12} + \tilde{\mathbf{x}}_{11}$ is a lattice codeword itself, we can write

$$\mathbf{y}_1 = \mathbf{h}^{\mathsf{T}}\mathbf{X}_1 + \mathbf{z}_1, \tag{72}$$

where

$$\mathbf{h} = \mathbf{h}(g) = \frac{1}{\sqrt{1+g^2}}[1 \; g^2 \; g], \; \mathbf{X}_1 = \left[\tilde{\mathbf{x}}_{11}^{\mathsf{T}} \; \tilde{\mathbf{x}}_{12}^{\mathsf{T}} \; \tilde{\mathbf{x}}_2^{\mathsf{T}}\right]^{\mathsf{T}}. \tag{73}$$

Thus, the effective channel (72) induced by our transmission scheme falls within our generic model introduced in the first section. We can decode the two desired codeword $\tilde{\mathbf{x}}_{11}$ and $\tilde{\mathbf{x}}_{12}$, as well as the nuisance codeword $\tilde{\mathbf{x}}_2$, by decoding three integer-linear combinations and then inverting them. Thus, the asymptotic performance of our scheme depends on $d_{\mathrm{comp},3}(\mathbf{h})$.

We would like to apply Corollary 1 in order to show that $\kappa_\epsilon(\mathbf{h}(g)) > 0$ for almost every $g \in \mathbb{R}$. To this end, we take $U_1 = [-\tau, \tau]$ for some large $\tau \in \mathbb{R}^+$ and set

$$\mathbf{f}_1(x) = \left(\frac{1}{\sqrt{1+x^2}}, \frac{x^2}{\sqrt{1+x^2}}, \frac{x}{\sqrt{1+x^2}} \right), \tag{74}$$

such that $\mathbf{h}(g) = \mathbf{f}_1(g) \in \mathbb{R}^{1\times 3}$. Certainly, $\mathbf{f}_1$ satisfies the conditions of Corollary 1, and we therefore obtain the following.

Corollary 3 *For almost every $g \in \mathbb{R}$ we have that $\kappa_\epsilon(\mathbf{h}(g)) > 0$.*

Combining the corollary above with (67), we have established that for almost every $g \in \mathbb{R}$, the proposed communication scheme attains $d_{\mathrm{comp},3}(\mathbf{h}(g)) = 1/3$.

The operational implication of this result, is that using the lattice-based communication scheme proposed above, each user can send both of its messages reliably, each with a rate that scales like $\frac{1}{3} \cdot \frac{1}{2} \log(P)$ with P. To appreciate this, note that the naïve scheme, which avoids interference by transmitting each of the 4 messages over different $T/4$ channel uses, can only achieve reliable communication with rates below $\frac{1}{4} \cdot \frac{1}{2} \log(1 + 4P)$.

6 Non-Asymptotic Bounds

For communication applications, it is often of interest to understand performance for finite P, as in practice the allowed transmission power is limited, and usually quite moderate.

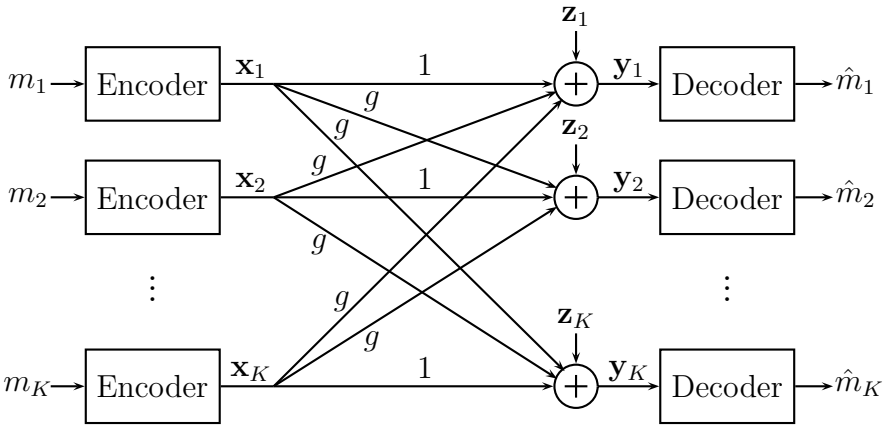

Figure 3: Block diagram of a symmetric Gaussian K-user interference channel.

As a canonical example, consider the symmetric K-user Gaussian interference channel, depicted in Figure 3. In this channel model, there are K users, each transmitting a signal $\mathbf{x}_k \in \mathbb{R}^T$, $k = 1, \ldots, K$, subject to the power constraint $\|\mathbf{x}_k\|^2 \leq TP$. There are also K receivers with observations

$$\mathbf{y}_k = \mathbf{x}_k + g \sum_{j \neq k} \mathbf{x}_j + \mathbf{z}_k, \ k = 1, \ldots, K \tag{75}$$

where $g \in \mathbb{R}$ is the (symmetric) interference gain, and $\mathbf{z}_k$ is i.i.d. Gaussian noise with zero mean and unit variance. The goal of the k^{th} receiver is to

decode only the codeword $\mathbf{x}_k$, whereas all other codewords are interference. In the proceeding discussion, we will assume that $1 < g < \sqrt{P}$.

The naïve approach for dealing with interference is to avoid it entirely. This corresponds to splitting the channel uses into T/K different slots, and letting only one user transmit within each slot. In this scheme, when the k^{th} user transmits, the k^{th} receiver observes its signal without any interference, and the resulting achievable rate is $\frac{1}{K} \cdot \frac{1}{2} \log(1 + KP)$.

A different, and sometimes more efficient, approach, is *interference alignment*. For the symmetric interference channel, this approach boils down to having all users encode their messages using the same lattice codebook. Consider the sum of interfering codewords at receiver k, $\mathbf{x}_{\text{interference},k} = \sum_{j \neq k} \mathbf{x}_j$. Owing to the fact that the lattice is closed under integer-linear combinations, $\mathbf{x}_{\text{interference},k}$ is itself a lattice codeword. Consequently, the effective two-user channel seen by receiver k is

$$\mathbf{y}_k = \mathbf{x}_k + g\, \mathbf{x}_{\text{interference},k} + \mathbf{z}_k. \tag{76}$$

Now, it is possible to recover $\mathbf{x}_k$ by decoding two linearly independent integer-linear combinations of $\mathbf{x}_k$ and $\mathbf{x}_{\text{interference},k}$.

The achievable rate of this interference alignment scheme is therefore the second computation rate[4] for the channel $\mathbf{H} = [1\ g]$. By Theorem 10, we can lower bound the second computation rate by

$$R_{\text{comp},2}(\mathbf{H}, P) \geq \frac{1}{2} \log \left(\min_{\mathbf{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}} \|\mathbf{a}\|^2 + P \|\mathbf{H}\mathbf{a}\|^2 \right) - 1. \tag{77}$$

Setting $\mathbf{H} = [1\ g]$, $\mathbf{a} = [-p\ q]$, and assuming without loss of generality that $q \geq 0$, we can write

$$\min_{\mathbf{a} \in \mathbb{Z}^2 \setminus \{\mathbf{0}\}} \|\mathbf{a}\|^2 + P \|\mathbf{H}\mathbf{a}\|^2 = \min_{p \in \mathbb{Z}, q \in \mathbb{N}, (p,q) \neq (0,0)} p^2 + q^2 + P|qg - p|^2. \tag{78}$$

Defining $\tilde{p} = p - q\lfloor g \rfloor$ and $\tilde{g} = g - \lfloor g \rfloor$, we can rewrite this as

$$\min_{\tilde{p} \in \mathbb{Z}, q \in \mathbb{N}, (\tilde{p},q) \neq (0,0)} (q\lfloor g \rfloor + \tilde{p})^2 + q^2 + P\left|q\lfloor g \rfloor + q\tilde{g} - q\lfloor g \rfloor - \tilde{p}\right|^2 \tag{79}$$

$$= \min_{\tilde{p} \in \mathbb{Z}, q \in \mathbb{N}, (\tilde{p},q) \neq (0,0)} (q\lfloor g \rfloor + \tilde{p})^2 + q^2 + P\left|q\tilde{g} - \tilde{p}\right|^2. \tag{80}$$

[4]Up to a small correction term, due to the fact that the effective user $\mathbf{x}_{\text{interference},k}$ has power $(K-1)P$ instead of P. See [20] for more details.

Since $\tilde{g} \geq 0$ by definition, we see that for $\tilde{p} < 0$ the expression above is lower bounded by P. We can therefore write

$$\begin{aligned}\min_{\mathbf{a}\in\mathbb{Z}^2\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\|\mathbf{H}\mathbf{a}\|^2 &\geq \min_{\tilde{p}\in\mathbb{Z},q\in\mathbb{N},(\tilde{p},q)\neq(0,0)} (q\lfloor g\rfloor + \tilde{p})^2 + q^2 + P\left|q\tilde{g} - \tilde{p}\right|^2 \\ &\geq \min\{P, \min_{(\tilde{p},q)\in\mathbb{N}^2\setminus\{\mathbf{0}\}} (q\lfloor g\rfloor + \tilde{p})^2 + q^2 + P\left|q\tilde{g} - \tilde{p}\right|^2\} \\ &\geq \min\{P, \min_{(\tilde{p},q)\in\mathbb{N}^2\setminus\{\mathbf{0}\}} \max(q^2\lfloor g\rfloor^2,\ P|q\tilde{g} - \tilde{p}|^2)\}. \end{aligned} \tag{81}$$

Next, we will study the behavior of the last term in (81). In particular, for an integer $1 \leq b \leq \sqrt{P}$ and $0 < \delta < 1$, we will study the Lebesgue measure of the "outage set"

$$\begin{aligned}\mathcal{W}_{b,\delta} &= \left\{ g \in [b, b+1) \ : \min_{(\tilde{p},q)\in\mathbb{N}^2\setminus\{\mathbf{0}\}} \max(q^2\lfloor g\rfloor^2,\ P|q\tilde{g} - \tilde{p}|^2) < \frac{\sqrt{g}}{2} P^{\frac{1}{2}(1-\delta)} \right\} \\ &\subset b + \left\{ x \in [0,1) : |qx - \tilde{p}| < \sqrt{b} P^{-\frac{1}{4}(1+\delta)} \text{ for some } q \leq \frac{P^{\frac{1}{4}(1-\delta)}}{\sqrt{b}},\ \tilde{p} \in \mathbb{N} \right\}. \end{aligned} \tag{82}$$

Note that for all $g \in [b, b+1) \setminus \mathcal{W}_{b,\delta}$, we have that

$$\min_{\mathbf{a}\in\mathbb{Z}^2\setminus\{\mathbf{0}\}} \|\mathbf{a}\|^2 + P\|\mathbf{H}\mathbf{a}\|^2 \geq \frac{\sqrt{g}}{2} P^{\frac{1}{2}(1-\delta)}, \tag{83}$$

which implies, by (77), that

$$R \geq \frac{1}{4}\log(g^2 P) - \frac{\delta}{4}\log P - \frac{3}{2} \tag{84}$$

for all $g \in [b, b+1) \setminus \mathcal{W}_{b,\delta}$, $1 \leq b \leq \sqrt{P}$.

In order to upper bound $\mu(\mathcal{W}_{b,\delta})$, for any $q \in \mathbb{Z}^+$, we define the set

$$\mathcal{T}_{b,\delta}(q) \triangleq \left[\left\{ 0, \frac{1}{q}, \ldots, \frac{q-1}{q} \right\} + \frac{\Phi_{b,\delta}}{q} \mathcal{I} \right] \bmod [0,1), \tag{85}$$

where $\mathcal{I} \triangleq [-1, 1]$ and $\Phi_{b,\delta} \triangleq \sqrt{b} P^{-\frac{1}{4}(1+\delta)}$. It is easy to see that

$$\mathcal{W}_{b,\delta} \subset b + \bigcup_{q=1}^{q_{\max}(b,\delta)} \mathcal{T}_{b,\delta}(q), \tag{86}$$

where $q_{\max}(b,\delta) \triangleq \left\lfloor \frac{P^{\frac{1}{4}(1-\delta)}}{\sqrt{b}} \right\rfloor$. Therefore,

$$\begin{aligned}
\mu(\mathcal{W}_{b,\delta}) &\leq \mu\left(\bigcup_{q=1}^{q_{\max}(b,\delta)} \mathcal{T}_{b,\delta}(q)\right) \\
&\leq \sum_{q=1}^{q_{\max}(b,\delta)} \mu\left(\mathcal{T}_{b,\delta}(q)\right) \\
&\leq \sum_{q=1}^{q_{\max}(b,\delta)} 2\Phi_{b,\delta} \\
&= 2q_{\max}(b,\delta)\Phi_{b,\delta} \\
&\leq 2P^{-\frac{\delta}{2}}. \qquad (87)
\end{aligned}$$

Now, setting $\delta = 2(\gamma+1)/\log(P)$, (84) and (87) imply that we can achieve a rate satisfying

$$\begin{aligned}
R &\geq \frac{1}{4}\log(g^2P) - \frac{\gamma+1}{2} - \frac{3}{2} \\
&= \frac{1}{4}\log(g^2P) - \frac{\gamma}{2} - 2 \qquad (88)
\end{aligned}$$

for all $g \in [b, b+1) \setminus \mathcal{W}$, where $\mathcal{W} = \mathcal{W}_{b,2(\gamma+1)/\log(P)}$ has Lebesgue measure at most $2^{-\gamma}$.

To appreciate this result, it should be contrasted with the rate attained by interference avoidance. The interference alignment rate scales with P as $\frac{1}{4}\log(g^2P)$ whereas that of interference avoidance only scales as $\frac{1}{2K}\log(P)$. For $K \geq 3$ and large P, the improvement is very significant. It can also be shown that the symmetric capacity of the symmetric K-user Gaussian interference channel is upper bounded by $\frac{1}{4}\log(g^2P) + 1$. Thus, we have the following theorem.

Theorem 12 ([20]) *The lattice interference alignment scheme described above attains the symmetric capacity of the symmetric K-user Gaussian interference channel to within $3 + \gamma/2$ bits for all $g \in [1, \sqrt{P}) \setminus \{\mathcal{W}\}$, where the set $\mathcal{W} \subset [1, \sqrt{P})$ has Lebesgue measure at most $(\sqrt{P} - 1)2^{-\gamma}$.*

7 Conclusions and Open Problems

In this chapter, we demonstrated that classical and modern results from the theory of Diophantine approximation are extremely useful for obtaining upper and lower bounds for the performance of lattice-based communication strategies. In particular, the compute-and-forward strategy makes it possible for a receiver to obtain integer-linear combinations of codewords, with the rate determined by how well the real-valued channel coefficients are approximated by the chosen integer coefficients. Though not discussed in this survey, similar ideas have been found useful for distributed data compression, where the compression rates are determined by how well the source covariance matrix can be approximated by a matrix with integer coefficients [30–32]. While explicitly identifying these integer coefficients is a challenging optimization problem, we can obtain universal bounds on the achievable communication rates via Diophantine approximation.

A major focus of this chapter was on degrees-of-freedom characterizations, i.e., the first-order term in the rate expression as the power P tends to infinity. For this regime, Diophantine approximation results allow us to obtain tight bounds up to a set of channel matrices with Lebesgue measure zero, even when dependencies exist between the channel gains, as in interference alignment. Going further, one can follow a similar approach to determine the degrees-of-freedom of essentially any interference network (see, for instance, [28, 33–35] for more details).

We also considered non-asymptotic bounds that hold for any choice of P. Specifically, we examined the symmetric K-user Gaussian interference, and derived a lower bound on the capacity whose gap to the upper bound depends on the measure of the excluded channel gains. Similar results are available for the two-user X channel [27]. For larger networks, we need to rely on more sophisticated interference alignment schemes, and more research is needed to develop non-asymptotic bounds that can handle the resulting dependencies. Specifically, alignment schemes for K-user interference channels (with arbitrary channel gains) utilize many signaling directions based on monomials constructed from the channel gains [28, 33]. This corresponds to a codeword emitted per signaling direction with a rate penalty for each additional codeword layer. In the limit as P tends to infinity, these rate penalties can be safely ignored to approach the optimal degrees-of-freedom of $1/2$ per user. However, for finite P, we must carefully tradeoff the number of codeword layers with the measure of excluded channel gains to attain the best per-

formance. This in turn requires non-asymptotic Diophantine approximation bounds over manifolds. See [36, 37] for recent progress in this direction.

References

[1] T. Cover and J. Thomas, *Elements of Information Theory*. Hoboken, NJ: Wiley-Interscience, 2nd ed., 2006.

[2] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[3] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge: Cambridge University Press, 2005.

[4] R. Zamir, *Lattice Coding for Signals and Networks*. Cambridge University Press, 2014.

[5] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, pp. 6463–6486, October 2011.

[6] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[7] R. Gallager, "Low-density parity-check codes," *IRE Transactions on information theory*, vol. 8, no. 1, pp. 21 – 28, 1962.

[8] T. Richardson and R. Urbanke, *Modern coding theory*. Cambridge university press, 2008.

[9] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 db of the Shannon limit," *IEEE Communications Letters*, vol. 5, pp. 58–60, Feb 2001.

[10] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on communications*, vol. 44, pp. 1261 – 1271, October 1996.

[11] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, pp. 3051 – 3073, July 2009.

[12] U. Erez and R. Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Transactions on Information Theory*, vol. 50, pp. 2293–2314, October 2004.

[13] R. Ahlswede, "Multi-way communication channels," in *Proceedings of the 2nd International Symposium on Information Theory, Prague*, pp. 23–52, Publishing House of the Hungarian Academy of Sciences, 1971.

[14] H. Liao, *Multiple access channels*. PhD thesis, University of Hawaii, Honolulu, 1972.

[15] J. M. Cioffi, G. P. Dudevoir, M. V. Eyuboglu, and G. D. Forney, "MMSE decision-feedback equalizers and coding. I. Equalization results," *IEEE Transactions on Communications*, vol. 43, pp. 2582–2594, Oct 1995.

[16] T. Guess and M. K. Varanasi, "An information-theoretic framework for deriving canonical decision-feedback receivers in Gaussian channels," *IEEE Transactions on Information Theory*, vol. 51, pp. 173–187, Jan 2005.

[17] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," *IEEE Transactions on Information Theory*, vol. 60, pp. 7661–7685, December 2014.

[18] B. Nazer, V. R. Cadambe, V. Ntranos, and G. Caire, "Expanding the compute-and-forward framework: Unequal powers, signal levels, and multiple linear combinations," *IEEE Transactions on Information Theory*, vol. 62, pp. 4879–4909, Sept 2016.

[19] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, vol. 671 of The Kluwer International International Series in Engineering and Computer Science. Cambridge, UK: Kluwer Academic Publishers, 2002.

[20] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric K-user Gaussian interference channel," *IEEE Transactions on Information Theory*, vol. 60, pp. 3450–3482, June 2014.

[21] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Mathematische Annalen*, vol. 296, no. 1, pp. 625–635, 1993.

[22] O. Ordentlich and U. Erez, "Precoded integer-forcing universally achieves the MIMO capacity to within a constant gap," *IEEE Transactions on Information Theory*, vol. 61, pp. 323–340, January 2015.

[23] V. Beresnevich, V. Bernik, and N. Budarina, "Systems of small linear forms and Diophantine approximation on manifolds," *ArXiv e-prints*, July 2017. Avaiable online http://arxiv.org/abs/1707.00371.

[24] M. Hussain and J. Levesley, "The metrical theory of simultaneously small linear forms," *Functiones et Approximatio Commentarii Mathematici*, vol. 48, no. 2, pp. 167–181, 2013.

[25] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Transactions on Information Theory*, vol. 54, pp. 3457–3470, August 2008.

[26] S. A. Jafar and S. Shamai (Shitz), "Degrees of freedom region for the MIMO X channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 151–170, January 2008.

[27] U. Niesen and M. A. Maddah-Ali, "Interference alignment: From degrees-of-freedom to constant-gap capacity approximations," *IEEE Transactions on Information Theory*, vol. 59, pp. 4855–4888, August 2013.

[28] A. S. Motahari, S. Oveis-Gharan, M.-A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Transactions on Information Theory*, vol. 60, pp. 4799–4810, August 2014.

[29] S. A. Jafar, "Interference alignment - a new look at signal dimensions in a communication network," in *Foundations and Trends in Communications and Information Theory*, vol. 7, NOW Publishers, 2011.

[30] O. Ordentlich and U. Erez, "Integer-forcing source coding," *IEEE Transactions on Information Theory*, vol. 63, pp. 1253–1269, Feb 2017.

[31] W. He and B. Nazer, "Integer-forcing source coding: Successive cancellation and source-channel duality," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 155–159, July 2016.

[32] E. Domanovitz and U. Erez, "Outage probability bounds for integer-forcing source coding," in *Proceedings of the IEEE Information Theory Workshop (ITW 2017)*, (Kaohsiung, Taiwan), Nov. 2017.

[33] V. R. Cadambe and S. A. Jafar, "Interference alignment and the degrees of freedom for the K-user interference channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 3425–3441, August 2008.

[34] V. R. Cadambe and S. A. Jafar, "Interference alignment and the degrees of freedom of wireless X networks," *IEEE Transactions on Information Theory*, vol. 55, pp. 2334–2344, May 2009.

[35] Y. Wu, S. Shamai (Shitz), and S. Verdú, "Information dimension and the degrees of freedom of the interference channel," *IEEE Transactions on Information Theory*, vol. 61, pp. 256–279, January 2015.

[36] F. Adiceam, V. Beresnevich, J. Levesley, S. Velani, and E. Zorin, "Diophantine approximation and applications in interference alignment," *Advances in Mathematics*, vol. 302, pp. 231 – 279, 2016.

[37] E. Domanovitz and U. Erez, "Outage behavior of integer forcing with random unitary pre-processing," *IEEE Transactions on Information Theory*, vol. 64, pp. 2774–2790, April 2018.