UNIVERSITY OF CALIFORNIA,
IRVINE

# Security, Robustness and Cooperation in Wireless Networks: Asymptotic and Extremal Analysis

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Electrical and Computer Engineering

by

Yao-Chia Chan

DISSERTATION Committee:
Chancellor's Professor Syed Ali Jafar, Chair
Chancellor's Professor Hamid Jafarkhani
Professor Ender Ayanoglu

2022

# TABLE OF CONTENTS

# LIST OF FIGURES

Page

# LIST OF TABLES

# ACKNOWLEDGMENTS

First and foremost, I am deeply indebted to my advisor, Professor Syed Jafar, for the enormous benefit I have gained from his brilliant insight, sharp vision, and immense knowledge. My doctoral study and research in the field of information theory have been a fruitful and life-changing adventure. This could not have happened without his patient guidance, valuable feedback, and unwavering support. In addition, the joy and enthusiasm he exhibits for his research have inspired and motivated me for the past years and will continue to do so in the future. It has been a great honor working with Profession Jafar and being his Ph.D. student.

I would also like to extend my gratitude to Professor Hamid Jafarkhani and Professor Ender Ayanoglu for serving on my dissertation committee, and to Professor Arnold Lee Swindlehurst and Professor Zhaoxia Yu for serving on my advancement committee. Their fresh viewpoints and practical suggestions make my research and dissertation more complete.

I could not have gone this far without such amazing company. I am thankful to Junge Wang, Chunhua Geng, and Pouya Pezeshkpour for collaborations in research works and coauthorships in publications. My appreciation also goes to my former and current colleagues, including Hua Sun, Arash Gholami Davoodi, Bofeng Yuan, Zhuqing Jia, Zhen Chen, Yuxiang Lu, Nilab İsmailoğlu, and Yuhang Yao. The inspirational moments that sparked in our active discussions are truly unforgettable and most enjoyable. I am proud of being a part of such a wonderful group.

This dissertation would not have been possible without funding from the Department of Electrical Engineering of the University of California, Irvine, and from the Ministry of Education, Republic of China (Taiwan).

Last but not least, I am grateful to my parents and siblings for their unconditional support and love throughout these years. They made me who I am, and I dedicate this dissertation to them.

# VITA

## Yao-Chia Chan

### EDUCATION

**Doctor of Philosophy in Electrical and Computer Engineering** **2022**
University of California, Irvine *Irvine, California*

**Master of Science in Communication Engineering** **2011**
National Taiwan University *Taipei, Taiwan*

**Bachelor of Science in Electrical Engineering**
**Bachelor of Art in Economics** **2009**
National Taiwan University *Taipei, Taiwan*

### RESEARCH EXPERIENCE

**Graduate Student Researcher** **2016–2022**
University of California, Irvine *Irvine, California*

**Research Assistant** **2015–2016**
National Taiwan University *Taipei, Taiwan*

**Research Assistant** **2012–2014**
National Taipei University of Technology *Taipei, Taiwan*

### TEACHING EXPERIENCE

**Teaching Assistant** **2022–2022**
University of California, Irvine *Irvine, California*

## Refereed Journal Publications

1. Y. -C. Chan, J. Wang and S. A. Jafar, “Toward an Extremal Network Theory—Robust GDoF Gain of Transmitter Cooperation Over TIN,” in *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3827-3845, June 2020.
2. Y. -C. Chan and S. A. Jafar, “Secure GDoF of the $Z$-Channel With Finite Precision CSIT: How Robust are Structured Codes?” in *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2410-2428, April 2022.
3. Y. -C. Chan, C. Geng and S. A. Jafar, “Robust Optimality of Secure TIN,” in *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3071-3082, May 2022.

## Refereed Conference Publications

1. Y. -C. Chan and S. A. Jafar, “Towards an Extremal Network Theory – Robust GDoF Gain of Transmitter Cooperation over TIN,” *2019 IEEE International Symposium on Information Theory (ISIT)*, 2019, pp. 3102-3106.
2. Y. -C. Chan and S. A. Jafar, “Secure GDoF of the $Z$-channel with Finite Precision CSIT: How Robust are Structured Codes?,” *2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 1558-1563.
3. Y. -C. Chan and S. A. Jafar, “Exploring Aligned-Images Bounds: Robust Secure GDoF of 3-to-1 Interference Channel,” *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1-6.

## Journal Articles Under Review

1. Y. -C. Chan, P. Pezeshkpour, C. Geng, and S. A. Jafar, “The Extremal GDoF Gain of Optimal versus Binary Power Control in $K$ User Interference Networks Is $\Theta(\sqrt{K})$,” submitted to *IEEE Transactions on Wireless Communications*.

# ABSTRACT OF THE DISSERTATION

Security, Robustness and Cooperation in Wireless Networks:
Asymptotic and Extremal Analysis

By

Yao-Chia Chan

Doctor of Philosophy in Electrical and Computer Engineering

University of California, Irvine, 2022

Chancellor's Professor Syed Ali Jafar, Chair

The emergence of 'Aligned Images Sum-set (AIS) Inequalities' has spurred much progress in Generalized Degrees of Freedom (GDoF) characterizations of wireless networks under robust assumptions that limit the channel state information at transmitters (CSIT). Much of this progress is limited to small networks, and to larger networks under highly symmetric parameter values. Extending these results to larger networks with asymmetric parameters is challenging because of the inherent curse of dimensionality, and also because the scope of AIS bounds is far from well understood. Making progress in this direction is the main goal of this dissertation.

We first explore the feasibility of an extremal network theory, i.e., a study of extremal networks within particular parameter regimes of interest. In particular, we quantify the extremal gain in sum GDoF brought about by transmitter cooperation in $K$ user interference channels in various parameter regimes that correspond to weak interference. Specifically, with the robust scheme of 'Treating Interference as Noise (TIN)' as the baseline, we find the extremal gain in a large parameter regime (known as the Simple Layered Superposition, or SLS, regime) to be $\Theta(\log_2 K)$, which scales logarithmically with the number of users.

As our next contribution we explore robust GDoF characterizations for large networks in the presence of security constraints. We identify surprisingly broad new regimes for both interference and broadcast networks, where robust secure GDoF are fully characterized for arbitrary number of users. The unifying feature of these regimes is the optimality of TIN along with wiretap coding, power control and jamming.

Continuing with the security constraint, in the final part of this dissertation we study the robustness of structured codes for secure GDoF characterizations under limited CSIT. In particular, structured jamming based on lattice codes is known to offer significant advantages by allowing receivers to decode and remove the sum of jamming and message signals in aggregate. However, we show that such advantages are completely lost in GDoF under the robust assumption of limited CSIT. The complete robust GDoF characterization of 2 user secure $Z$ channels comes as a byproduct of the analysis. Limitations of existing AIS bounds are identified that stand in the way of generalizations to larger networks in this case.

# Chapter 1

# Introduction

## 1.1 Background

Understanding the fundamental limits of wireless networks has been a long-standing holy grail for communications and information theory. It is one of the grand challenges in network information theory, given that only few types of networks are completely characterized in their capacity [1, 2], after Shannon's groundbreaking work on the capacity of point-to-point channels [3]. While the ultimate prize – the exact capacity characterizations – remains elusive, there is a rich history of recent progress, especially during the last two decades, through a number of breakthroughs that identify critical obstacles and find ways to circumvent them.

It starts around two decades ago [4–8] with the realization that in spite of the intractability of exact capacity characterizations, progress can be made by shifting the focus to capacity approximations. From this comes insightful deterministic models that are essential for such approximations [7, 8], as well as high Signal-to-Noise Ratio (SNR) asymptotic analysis of network Degrees of Freedom (DoF) [5, 6] that broadens the scope of approximations and leads to new ideas like interference alignment [9–12]. A limitation of the DoF metric is that it implicitly treats all channels as equally strong – every non-zero link carries exactly one DoF. This limitation is overcome by the *Generalized* Degrees of Freedom (GDoF) [7] metric, which is essential for capacity approximations of networks with different power in the links.

While GDoF characterizations provide important conceptual benchmarks, the optimal solutions are often too fragile to be implementable in practice [10, 11]. The main obstacle is the assumption of perfect channel state information at the transmitters (CSIT). Evidently, CSIT needs to be limited to finite precision. If the benefit of these optimal solutions is lost under finite precision, then this removes some of the obstacles that have made progress difficult in network information theory, and thus opens the door to a comprehensive and robust network information theory of wireless networks, based on optimality of random codes that are much better understood. Even if we set this theoretical concern aside, the emphasis on finite precision CSIT brings theory closer to practice, which is a worthy goal in itself.

Early attempts at high SNR analysis under finite precision CSIT run into formidable challenges, with a few notable exceptions [13–16]. The difficulty in studying finite precision CSIT is that bounds produced by various classical techniques (Csiszar-sum lemma [17], extremal inequalities [18], compound channel bounds [19]) fall short even in very simple settings, e.g., the two-user multiple-input single-output (MISO) broadcast channel (BC) as exemplified by the Lapidoth-Shamai-Wigger conjecture on the collapse of DoF [17]. This leads to the emergence of Aligned Images sum-set inequalities [20] which allow comparisons of entropies of received signals under finite precision CSIT.

Aligned Images sum-set inequalities make DoF characterizations possible for canonical interference and broadcast networks under finite precision CSIT, and help settle various conjectures along the way [17, 20–23]. Going beyond DoF to GDoF characterizations requires stronger generalizations of Aligned Images sum-set inequalities , that can compare entropies of *subsections* of signals. This leads to a new class of *sumset inequalities* in [24], which enable successful robust GDoF characterizations in many cases [18, 25–29]. Limitations of these sumset inequalities are also noted [30].

With the tools of Aligned Images sum-set inequalities, this dissertation explores different approaches to characterize the robust GDoF of large wireless networks with no symmetry in topologies assumed. The first approach is to apply an extremal network theory to analyze the benefit brought by transmitter cooperation to interference networks. The extremal network theory studies the extremal value of a metric of interest within some channel regimes, and offers analyses from a broad and approximate view. For exact analysis, in the next approach, we explore sharp characterizations for GDoF of large networks under secrecy. Broad new regimes are identified respectively for interference and broadcast networks, whose secure GDoF are characterized for an arbitrary number of users. Finding optimality beyond these regimes may require schemes such as structured codes, which appear as a key ingredient of optimal secure schemes under perfect CSIT. In the last part, we show that the benefit of the key features offered by structured jamming is completely lost with two user secure $Z$ channels, and structured jamming is thus not robust.

## 1.2 Overview of the Dissertation

We describe the problems associated each of the approaches and outline the accompanying contributions in each chapter as follows.

In Chapter 2, we apply an extremal network theory to characterize the robust GDoF of large-scale networks with asymmetric settings. As one way to avoid the curse of dimensionality, the extremal network theory characterizes large wireless networks with the extremal value of a metric of interest within a channel regime. To test its feasibility, we study the extremal gain in sum GDoF that transmitter cooperation can bring to $K$ user interference networks, with treating interference as noise as the baseline for comparison. The extremality is taken over all topologies within some weak-interference channel regimes. Treating Interference as Noise (TIN) is taken as the baseline, as we expect it would be powerful in weak interference regimes. We consider three weak interference regimes: the TIN, Convex TIN (CTIN), and Simple Layered Superposition (SLS) regimes. The extremal sum-GDoF gain found for the TIN and CTIN regimes are respectively 1.5 and $2 - \frac{1}{K}$. With the small extremal gains, one may conclude that it is not worthwhile for further study in the TIN and CTIN regimes. On the other hand, the extremal gain for the SLS regime is $\Theta(\log_2 K)$, which grows logarithmically with the number of users. Such a large extremal gain suggests important ideas in the SLS regime are yet to be discovered.

In Chapter 3, we fix a scheme of interest and discover larger parameter regimes where the scheme remains optimal by adding constraints to the networks. The scheme we consider is a secure version of TIN, which contains jamming to ensure message secrecy. For $K$ user interference networks, we identify the Secure TIN (STIN) regime, where the secure version of TIN remains GDoF optimal under finite precision CSIT. The STIN regime is the largest of all such parameter regimes previously identified for GDoF optimality in some network settings, including the SLS, CTIN, and the TIN regime. Next, we apply extremal analysis to the benefit of transmitter cooperation by comparing the secure robust GDoF of $K$ user interference network and the MISO broadcast counterpart. We show that the extremal gain of transmitter cooperation is unbounded in the STIN regime, while it is equal to one when restricted in the SLS regime. The SLS regime thus becomes the largest regime for the secure broadcast setting where the precise GDoF characterization is available. Finally, we extend the study of the optimality of secure TIN to explore the impact of helpers and eavesdroppers in various parameter regimes.

In Chapter 4, we study the robustness of structured codes under finite precision CSIT and secrecy. Structured codes are key ingredients of optimal schemes as they can align or cancel at unintended receivers when perfect CSIT is available. They also appear in secure communications as structured jamming, where lattices of jamming signal and messages can be aligned, decoded in aggregate, and removed at the unintended receivers, with no messages explicitly decoded. However, structured jamming may not be robust to channel uncertainty. In fact, we show such a benefit of aggregate decoding and cancellation is lost with a $Z$ interference channel with secrecy constraints. Such a setting is arguably a minimal one, because relaxing one of the settings (robustness, GDoF, secrecy) leads to questions which were studied in the literature. As byproducts, we characterize the secure GDoF regions for both $Z$ interference and broadcast channel. The challenge in proving optimality lies in the converse, which involves a non-trivial combination of the secrecy constraints and the use of Aligned Images sum-set inequalities.

## 1.3 Notations and Abbreviations

We use the following notations in this dissertation. For integers $x$ and $y$ satisfying $1 \leq x \leq y$, define $[x : y] = \{x, x+1, \cdots, y\}$, and $[x] = \{1, 2, \cdots, x\}$. The notation $(x)^+$ and $\{x\}^+$ represent $\max\{x, 0\}$. The notation $[\alpha]_{K\times K}$ represents a $K \times K$ matrix whose $(i,j)$–th element is $\alpha_{i,j}$ (or $\alpha_{ij}$ if no ambiguity arises). The cardinality of a set $\mathcal{S}$ is denoted as $|\mathcal{S}|$. For real functions $f(x)$ and $g(x)$, denote $f(x) = O(g(x))$ if $\limsup_{x\to\infty} \frac{f(x)}{g(x)} = c$ for some constant $c > 0$, $f(x) = o(g(x))$ if $\limsup_{x\to\infty} \frac{f(x)}{g(x)} = 0$, and $f(x) = \Theta(g(x))$ if $f(x) = O(g(x))$ and $g(x) = O(f(x))$. For random variables $X$, $Y$, $Z$ and a set of random variables $\mathcal{G}$, define $H_{\mathcal{G}}(X|Y) = H(X|Y, \mathcal{G})$ and $I_{\mathcal{G}}(X;Y|Z) = I(X;Y|Z,\mathcal{G})$. $\mathbb{R}$ is all real numbers. $\mathbb{R}_+$ is all non-negative real numbers. $\mathbb{F}_q$ is the finite field of order $q$. All logarithms are to the base 2 unless otherwise specified. Table 1.1 lists the abbreviations used in this dissertation.

Table 1.1: Abbreviations used in this dissertation.

| | |
|---|---|
| DoF | Degrees of Freedom |
| GDoF | Generalized Degrees of Freedom |
| SNR | Signal-to-Noise Ratio |
| SINR | Signal-to-Interference-and-Noise Ratio |
| CSIT | Channel State Information at Transmitters |
| MISO | Multiple-Input Single-Output |
| IC | Interference Channel |
| BC | Broadcast Channel |
| MAC | Multiple Access Channel |
| AI | Aligned Image |
| TIN | Treating Interference as Noise |
| CTIN | Convex Treating Interference as Noise |
| STIN | Secure Treating Interference as Noise |
| SLS | Simple Layered Superposition |

# Chapter 2

# Extremal Gain of Transmitter Cooperation Over TIN

## 2.1 Capacity Characterization with Practical Concerns

New tools are inspired along with the recent progress in characterizing network capacity under the Degrees of Freedom (DoF) or the Generalized Degress of Freedom (GDoF) framework. New schemes, such as those inspired by the idea of interference alignment, are brought forward to achieve optimality under the idealized assumption of perfect channel knowledge. New outer bounds, such as those based on the Aligned Image principles, are successfully applied under the robust assumption of channel knowledge. Given the new achievable schemes and the new outer bounds, a worthy goal is to bring the theory closer to practice by adapting the models and metric to increasingly incorporate practical consideration. As a step in this direction, in this chapter into the study of network capacity we include three practical concerns — robustness, simplicity, and scalability.

### 2.1.1 Robustness in Channel Knowledge

By robustness we refer specifically to the channel state information at the transmitters (CSIT). GDoF characterizations under perfect CSIT provide important theoretical benchmarks, but often lead to fragile schemes such as asymptotic [10] or real interference alignment [11] whose benefits are outweighed in practice by the potential for drastic failures due to imperfections in channel knowledge. Robustness to channel uncertainty is addressed by GDoF characterizations that limit the CSIT to finite[1] precision [17]. Optimal schemes for such GDoF characterizations tend to be naturally robust schemes that require only a coarse knowledge of channel strength[2] parameters $\alpha_{ij}$ at the transmitters. Aided by advances in Aligned Images (AI) bounds [20], GDoF characterizations under finite precision CSIT have been found for a variety of wireless networks in [23, 25, 31–33].

### 2.1.2 Simplicity in Achievable Schemes

The importance of simplicity is reflected in the goal of identifying parameter regimes where simple schemes are optimal in the GDoF sense [34–47]. The most relevant examples for our purpose are [34], [35] and [36]. Reference [34] identifies[3] a weak interference regime, called the TIN-regime (Definition 2.1), where the simple scheme of power control and treating interference as Gaussian noise (in short, TIN[4]) is GDoF optimal for the $K$ user interference channel (IC). A broader regime, called CTIN regime (Definition 2.2, the 'C' signifies 'convex') is identified by Yi and Caire in [35] where, quite remarkably, the GDoF region achievable by TIN is shown to be **c**onvex without the need for time-sharing. It is not known whether TIN is GDoF optimal in this regime. Reference [36] identifies an even broader regime,

[1] In this chapter by default the term GDoF will refer to GDoF under finite precision CSIT.

[2] $\alpha_{ij}$ represents the channel strength from the $j^{th}$ transmitter to the $i^{th}$ receiver, and is measured in the db scale.

[3] While originally established under the assumption of perfect CSIT, the robustness of the TIN scheme ensures that this result carries over to finite precision CSIT.

[4] Note that TIN also includes optimal power control.

called the SLS-regime (Definition 2.3), where a simple layered superposition (SLS) scheme is GDoF optimal for the corresponding $K$ user multiple-input single-output (MISO) broadcast channel (BC) under finite precision CSIT, but only for $K \leq 3$. Optimality of SLS for larger networks seems plausible, but a rapid growth in the number of parameters stands in the way of any such effort. Comparisons between the GDoF characterizations for interference and broadcast channels in these regimes are of interest because they shed light on the benefits of transmitter cooperation over TIN. However, based on existing results, our ability to make direct comparisons is limited to very small networks. This brings us to the third practical concern, scalability.

### 2.1.3 Scalablity in Analysis

Wireless networks often involve a large number of users. Studies of large networks have to deal with an explosion in the number of parameters. One way to limit the number of parameters is to study symmetric settings. For example, consider the symmetric setting obtained by setting $\alpha_{ij} = 1$ if $i = j$ and $\alpha_{ij} = \alpha$ if $i \neq j$, for all $i, j \in [K]$. Under finite precision CSIT, GDoF are characterized for the symmetric $K$ user interference channel in [25], and for the symmetric $K$ user MISO BC in [31]. Based on the symmetric settings, sum-GDoF gain of the symmetric $K$ user MISO BC over the symmetric $K$ user IC is at most a factor of $3/2$ for all values of $\alpha \in [0, 1]$. Furthermore, the TIN scheme can only achieve $\max(1, K(1-\alpha))$ GDoF [34] while the $K$ user MISO BC has $\alpha + K(1-\alpha)$ GDoF [31]. Therefore, transmitter cooperation can provide an improvement over TIN by a factor of at most $3/2$ in the TIN-regime and the CTIN regime (both correspond to $\alpha \leq 1/2$), and a factor of at most 2 in the SLS-regime ($\alpha \leq 1$). Evidently the benefits of optimal transmitter cooperation over a simple scheme like TIN, are bounded for large $K$ in both regimes.

But is this also true for *asymmetric* settings? To answer such questions, we need to venture beyond symmetric settings, and yet somehow avoid the curse of dimensionality. Other fields that face similar challenges, such as graph theory and set theory, find a path to progress through extremal analysis, i.e., the study of extremal graphs or extremal sets that satisfy various properties of interest. It stands to reason that a path to progress for wireless networks may be found in extremal network theory, i.e., the study of extremal networks. This is the main idea that we wish to explore in this chapter. Our interest in the benefits of transmitter cooperation provides us a context within which we can test the feasibility of the study of extremal networks.

## 2.2 Problem Statement and Contributions

We are interested specifically in the benefits of transmitter cooperation under *weak interference* over the simple baseline of TIN. The question is intriguing because on the one hand, we expect TIN to be a powerful scheme in weak interference regimes, but on the other hand full cooperation among all transmitters can also be quite powerful. Appealing to extremal network theory, we study the ratio,

$$\eta_K = \sup_{[\alpha]_{K\times K}\in\mathcal{A}} \frac{\mathcal{D}_{\Sigma,\mathrm{BC}}}{\mathcal{D}_{\Sigma,\mathrm{TINA}}}, \tag{2.1}$$

where $\mathcal{D}_{\Sigma,\mathrm{TINA}}$ is the supremum (maximum, if it exists) of the sum-GDoF values *achievable* by power control and TIN in a $K$ user IC. This is the baseline for comparison. $\mathcal{D}_{\Sigma,\mathrm{BC}}$ is the *optimal* sum-GDoF of the corresponding $K$ user MISO BC obtained by full transmitter cooperation. The study of $\eta_K$ is consistent with extremal network theory because of the maximization over $[\alpha]_{K\times K}$. Networks that maximize the ratio in (2.1) are extremal networks within the class of networks specified by the regime of interest, $\mathcal{A}$. The three regimes that we consider are, the TIN-regime, $\mathcal{A}_{\mathrm{TIN}}$, the CTIN-regime, $\mathcal{A}_{\mathrm{CTIN}}$, and the SLS-regime, $\mathcal{A}_{\mathrm{SLS}}$. No assumption of symmetry is made within these regimes.

We characterize the extremal GDoF gain, $\eta_K$, from transmitter cooperation over TIN for the TIN-, CTIN- and SLS-regime. For the CTIN and TIN regimes, we show that $\eta_K = \Theta(1)$, i.e., it is bounded by a constant regardless of the number of users, $K$. In fact $\eta_K = 3/2$ in the TIN regime (Theorem 2.1), and $\eta_K = 2 - 1/K$ in the CTIN regime (Theorem 2.2), for arbitrary number of users $K > 1$. The bounded gain is consistent with and generalizes the insight obtained from the GDoF characterizations of symmetric IC and BC in [25, 31]. For the SLS regime, we show that, $\eta_K = \Theta(\log_2(K))$, i.e., the extremal GDoF gain of transmitter cooperation over TIN grows logarithmically with the number of users (Theorem 2.3) for large networks. This is in contrast with the insights from the symmetric case where the improvement is at most by a factor of 2. The constructive proof of this result reveals a hierarchical topology (Section 2.7.2) that benefits greatly from transmitter cooperation. It is also remarkable that the SLS scheme suffices to achieve the logarithmic extremal GDoF gain from transmitter cooperation over TIN. As a byproduct of our analysis we discover (Theorem A.1) an important cyclic partition property of a TIN achievable region known as polyhedral TIN [34] (Definition 2.8) that holds everywhere in the SLS-regime.

### 2.2.1 Significance of Extremal Analysis

To understand the significance of these results, and of extremal network theory in general, it is important to be clear about what extremal results represent. As a visual aid, consider Figure 2.1 where an arbitrary function is shown in black, whose rich variations make it difficult to characterize it exactly for all parameter values, and contrast it with the simpler description shown in red which bounds the *range* of the function in different regimes of interest by its corresponding extremal values. The simplicity of the extremal characterization makes it a compelling alternative to the complexity of the complete characterization. This is also the case with GDoF characterizations for large networks, where a central challenge is the overwhelming richness of the parameter space. We similarly propose extremal network

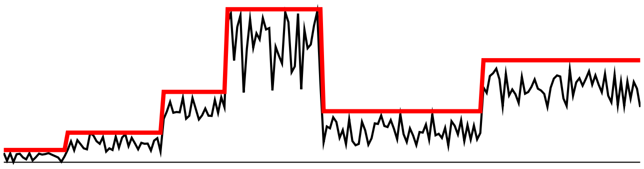


Figure 2.1: A conceptual depiction of a function over a rich parameter space and its simplified representation through extremal values over various regimes of interest.

analysis as a solution to this challenge.

However, in using extremal results, it is important to remember that extremal values represent the *potential* within each regime, and not necessarily the *typical* or *average* behavior. Here, let us consider two possibilities. Suppose extremal analysis shows that the potential is small, e.g., in the TIN and CTIN regimes we find that cooperation can provide at most a constant factor gain in GDoF for arbitrarily large networks, i.e., the multiplicative gain from cooperation does not scale with $K$. In fact, the constant is quite small, 1.5 for TIN and at most 2 for CTIN. At this point, one might reasonably conclude that the gain is too small to be be worthwhile for further studying this class of channels. Thus, small extremal values bring a measure of closure to the corresponding parameter regimes. On the other hand, surprisingly large extremal values identify regimes that merit further study. By the elephant-matchbox doctrine (elephants cannot hide in matchboxes) these are the regimes where important ideas may be discovered. It is also important to identify the extremal networks that may be studied carefully to isolate these ideas.

Last but not the least, extremal features are interesting by definition, in the same way that the speed of light, the blue whale, and Mount Everest are interesting. So whether it is intellectual curiosity, or the potential for the discovery of big ideas, or the need for a coarse understanding of overwhelmingly rich parameter spaces, the take home message of this chapter is that the study of extremal networks presents a promising way forward.

## 2.3 System Model

For GDoF studies, the $K$ user interference channel is modeled as [20, 25]

$$Y_k(t) = \sum_{i=1}^{K} \bar{P}^{\alpha_{ki}} G_{ki}(t) X_i(t) + Z_k(t), \qquad \forall k \in [K]. \tag{2.2}$$

During the $t^{th}$ channel use, $X_i(t), Y_k(t), Z_k(t) \in \mathbb{C}$ are, respectively, the symbol transmitted by Transmitter $i$ subject to a normalized unit transmit power constraint, the symbol received by User $k$, and the zero mean unit variance additive white Gaussian noise (AWGN) at User $k$. $\bar{P} \triangleq \sqrt{P}$, is a nominal parameter that approaches infinity to define the GDoF limit (see Section 2.3.2). The exponent $\alpha_{ki} \geq 0$ is referred to as the channel strength of the link between Transmitter $i$ and Receiver $k$, and is known to all transmitters and receivers. The channel coefficients $G_{ki}(t)$ are known perfectly to the receivers but only available to finite precision at the transmitters. The finite precision CSIT assumption implies that from the transmitter's perspective, the joint and conditional probability density functions of the channel coefficients exist and the peak values of these distributions are bounded, i.e., they do not grow with $P$ (see [20] for further description of the bounded density assumption). Note that the transmitters know the distributions but not the actual realizations of $G_{ki}(t)$, therefore the transmitted symbols $X_i(t)$ are independent of the realizations of $G_{ki}(t)$. In the $K$ user IC, there are $K$ independent messages, one for each user, and each message is independently encoded by its corresponding transmitter. The definitions of achievable rate tuples and capacity region, $\mathcal{C}_{\text{IC}}(P)$ are standard, see e.g., [20]. The GDoF region of the $K$ user interference channel is defined as

$$\mathcal{D}_{\text{IC}} = \left\{ (d_k)_{k\in[K]} \middle| d_k = \lim_{P\to\infty} \frac{R_k(P)}{\log(P)}, (R_k(P))_{k\in[K]} \in \mathcal{C}_{\text{IC}}(P) \right\}. \tag{2.3}$$

The maximum sum-GDoF value is denoted $\mathcal{D}_{\Sigma,\text{IC}}$.

Allowing full cooperation among the transmitters changes the problem into a $K$ user MISO BC, where the $K$ messages are jointly encoded by all $K$ transmitters. The GDoF region for the MISO BC is denoted $\mathcal{D}_{\text{BC}}$ and the maximum sum-GDoF value is denoted $\mathcal{D}_{\Sigma,\text{BC}}$.

### 2.3.1 Deterministic Model

As shown in [20] the GDoF of the channel model in (2.2) are bounded above by the GDoF of the corresponding deterministic model with inputs $\bar{X}_k(t)$ and outputs $\bar{Y}_k(t)$, defined as

$$\bar{Y}_k(t) = \sum_{i=1}^{K} \left\lfloor \bar{P}^{\alpha_{ki}-\alpha_{\max,i}} G_{ki}(t)\bar{X}_i(t) \right\rfloor, \tag{2.4}$$

where $\bar{X}_i(t) = \bar{X}_i^R(t) + j\bar{X}_i^I(t)$ with $\bar{X}_i^R(t), \bar{X}_i^I(t) \in \{0,1,2,\cdots,\lceil \bar{P}^{\alpha_{\max,i}} \rceil\}$, and $\alpha_{\max,i} = \max_{j\in[K]} \alpha_{ji}$. For all the parameter regimes considered in this chapter, $\alpha_{\max,i} = \alpha_{ii}$. The assumptions regarding channel coefficients $G_{ki}(t)$, channel knowledge at transmitters and receivers, and definitions of messages, codebooks, achievable rates, and GDoF are the same as before. Let us also recall a very useful bound for our current purpose, a special case of Lemma 1 in [25].

**Lemma 2.1** (Lemma 1 in [25])**.**

$$\begin{aligned} H&\left(\left(\sum_{i=1}^{K} \lfloor \bar{P}^{\lambda_i-\alpha_{\max,i}} G_{ki}(t)\bar{X}_i(t) \rfloor\right)^{[1:T]} \middle| \mathcal{G}, W_S\right) \\ &- H\left(\left(\sum_{i=1}^{K} \lfloor \bar{P}^{\nu_i-\alpha_{\max,i}} G_{k'i}(t)\bar{X}_i(t) \rfloor\right)^{[1:T]} \middle| \mathcal{G}, W_S\right) \\ &\qquad \le \max_{i\in[K]} (\lambda_i - \nu_i)^+ T \log(P) + T\ o(\log(P)), \end{aligned} \tag{2.5}$$

*where $H(Z)$ is the entropy of $Z$, the notation $(A(t))^{[1:T]}$ stands for $(A(1), A(2), \cdots, A(T))$, $\mathcal{G}$ is a random vector containing the values of all channel coefficients $G_{ki}(t), G_{k'i}(t)$ for $k, k', i \in$*

*$[K], t \in [1:T]$, the constants $\lambda_i, \nu_i$ are arbitrary values between $0$ and $\alpha_{\max,i}$, the set $S \subset [K]$ is an arbitrary (possibly empty) subset of users, say $S = \{i_1, i_2, \cdots, i_M\}$, and $W_S = (W_{i_1}, W_{i_2}, \cdots, W_{i_M})$ is comprised of the corresponding users' desired messages.*

The significance of Lemma 2.1 may be intuitively understood as follows. Suppose there are $K$ transmitters, transmitting symbols $\bar{X}_i(t)$, $i \in [K]$, independent of the realizations of the bounded density channel coefficients $G_{ki}(t), G_{k'i}(t)$, for all $i, k, k' \in [K], t \in [1:T]$, and the transmitted symbols $\bar{X}_i(t)$ can be heard at two receivers, $k$ and $k'$ with power levels up to $\lambda_i$ and $\nu_i$ respectively. Then the maximum difference of entropies in the GDoF sense, that can exist between the signals received at the two receivers is no more than the maximum of the difference of the corresponding values of $\lambda_i$ and $\nu_i$ (or zero if the maximum difference is negative). In other words, the greatest difference in the GDoF sense that can be created between the entropies of received signals at two receivers can be achieved by simply transmitting from only one antenna, which is the antenna that experiences the largest difference of channel strengths between the two receivers. Remarkably, Lemma 2.1 holds for both interference and broadcast settings, i.e., the symbols $\bar{X}_i$ may be independent across $i \in [K]$ as in the IC, or dependent as in the BC.

It will be convenient to introduce a more compact notation for Lemma 2.1. Let us define,

$$\mathbb{H}_g([\lambda_1, \lambda_2, \cdots, \lambda_K] \mid W_S) \triangleq H\left(\left(\sum_{i=1}^{K} \lfloor \bar{P}^{\lambda_i - \alpha_{\max,i}} G_{ki}(t) \bar{X}_i(t) \rfloor\right)^{[1:T]} \middle| \mathcal{G}, W_S\right). \tag{2.6}$$

Using this compact notation and ignoring $o(\log(P))$ terms that are inconsequential for GDoF, the statement of Lemma 2.1 becomes

$$\begin{aligned} &\mathbb{H}_g([\lambda_1, \lambda_2, \cdots, \lambda_K] \mid W_S) - \mathbb{H}_g([\nu_1, \nu_2, \cdots, \nu_K] \mid W_S) \\ &\leq \max(\lambda_1 - \nu_1, \lambda_2 - \nu_2, \cdots, \lambda_K - \nu_K)^+ T \log(P). \end{aligned} \tag{2.7}$$

Note that the bounded density channel coefficients that appear in the two entropy terms in Lemma 2.1, $G_{ki}$ and $G_{k'i}$ may be different, however the $W_S$ that appears in the conditioning in both entropy terms must be the same. When Lemma 2.1 is applied in the context of interference channels, the conditioning on a subset of messages allows the corresponding codeword symbols $\bar{X}_i, i \in S$ to be eliminated from the received signal, essentially by setting the corresponding $\lambda_i, \nu_i$ values to 0, after which the conditioning on $W_S$ can be dropped because the remaining $\bar{X}_i$ are independent of $W_S$. Once the conditioning on $W_S$ is dropped, any two entropy terms may be compared and their difference bounded by Lemma 2.1. For example, in the interference channel context,

$$\begin{aligned}\mathbb{H}_g([\lambda_1, \lambda_2, \lambda_3] \mid W_2) - \mathbb{H}_g([\nu_1, \nu_2, \nu_3] \mid W_3) &= \mathbb{H}_g([\lambda_1, 0, \lambda_3]) - \mathbb{H}_g([\nu_1, \nu_2, 0]) &\quad (2.8)\\ &\leq \max(\lambda_1 - \nu_1, -\nu_2, \lambda_3)^+ T \log(P). &\quad (2.9)\end{aligned}$$

However, when Lemma 2.1 is applied in the context of broadcast channels, the conditioning on $W_S$ cannot be dropped because all $\bar{X}_i$ may depend on all messages. In that case, only entropy terms conditioned on the same set of messages may be compared through Lemma 2.1. This is the main difference in how Lemma 2.1 may be applied to interference and broadcast channels.

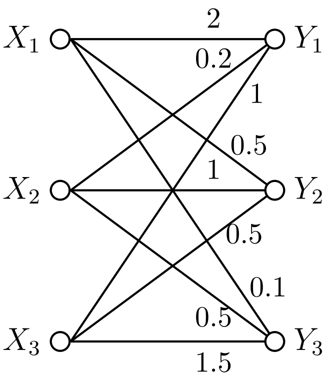
### 2.3.2 Significance of GDoF

The GDoF model is essentially a generalization of the deterministic model of [8]. The significance of the GDoF model may be intuitively understood as follows. The channel strength parameters represent the arbitrary and finite values of corresponding link SNRs and INRs in dB scale for a given network setting, i.e., $\alpha_{ii} = \log(\mathrm{SNR}_{ii})$ and $\alpha_{ij} = \log(\mathrm{INR}_{ij})$ (see, for example [34] for a more detailed explanation). Note that $\alpha_{ii}$ and $\alpha_{ij}$ may also be understood to be the approximate capacities of the corresponding links in isolation. Unlike the DoF metric which proportionately scales all the transmit *powers*, the GDoF model proportionately scales all the link *capacities*. The exponential scaling of powers in the GDoF model corresponds to a linear scaling of all of the corresponding link capacities by the same factor, and this factor is $\log(P)$ (note that the isolated link with signal strength $P^{\alpha_{ij}}$ has capacity $\approx \alpha_{ij}\log(P)$, thus the scaling factor is $\log(P)$). The linear scaling of powers in the DoF model causes the ratios of capacities of any two non-zero links to approach 1 as $P \to \infty$. Thus, a very weak channel and a very strong channel become essentially *equally* strong in the DoF limit, thereby fundamentally changing the character of the original network of interest. The GDoF model on the other hand keeps the ratios of all capacities unchanged as $P \to \infty$, so that strong channels remain strong, and weak channels remain weak. The intuition behind GDoF is that if the capacities of all the individual links in a network are scaled by the *same* factor, then the overall network capacity region should scale by approximately the same factor as well — essentially a principle of scale invariance.[5] If so, then normalizing by the scaling factor $\log(P)$ should produce an approximation to the capacity region of the original finite SNR network setting. This is precisely how GDoF are measured, note the normalization by $\log(P)$ in (2.3). Indeed, the validity of this intuition is borne out by numerous bounded-gap capacity approximations that have been enabled by GDoF characterizations (e.g., [48–52]), starting with the original result – the capacity characterization of the two user interference channel within a 1 bit gap in [7].

[5] While the scaling of $P$ may be interpreted as a physical scaling of transmit powers in the DoF metric (which unfortunately changes the character of the given network), $P$ does not have the same interpretation of physical transmit power in GDoF. Instead, in the GDoF setting, $P$ is just a nominal parameter, such that each value of $P$ identifies a new network according to (2.2). These distinct networks are lumped together by the GDoF metric based on the intuition that comes from the principle of scale invariance, i.e., when normalized by $\log(P)$ all of these networks should have *approximately* the same capacity region (see also the discussion in [47]).

### 2.3.3 Significance of Finite-Precision CSIT

Asymptotic analysis under perfect CSIT often leads to fragile schemes that are difficult to translate into practice, for example the DoF of the $K$ user interference channel have been shown in [11,53] to depend on whether the channels take rational or irrational values – a distinction of no practical significance. Zero forcing schemes that rely on precise channel phase knowledge to cancel signals can fail catastrophically due to relatively small phase perturbations. Robust schemes are much more valuable in practice. Restricting the CSIT to finite precision naturally shifts the focus to robust schemes that rely primarily on a coarse knowledge of channel strengths at the transmitters. While the finite precision CSIT model [17,20] allows arbitrary fading distributions subject to bounded densities, it is instructive to consider in particular the model $G_{ki}(t) = g_{ki}^R(t) + jg_{ki}^I(t)$ where $g_{ki}^R(t), g_{ki}^I(t)$ are independent and uniformly distributed over $(1-\epsilon, 1+\epsilon)$ for some arbitrarily small but positive $\epsilon$. Interpreted this way, $G_{ki}(t)$ are seen as arbitrarily small *perturbations* in the channel state that serve primarily to limit CSIT in the channel model to $\epsilon$-precision, while the coarse knowledge of channel strengths remains available to the transmitters in the form of the parameters $\alpha_{ij}$. From a GDoF perspective, these perturbations filter out fragile schemes that rely on highly precise CSIT. Indeed, the GDoF benefits of most sophisticated interference alignment and zero forcing schemes disappear under finite precision CSIT [20]. However, the benefits of robust schemes that rely only on the knowledge of channel strengths, such as rate-splitting [54], elevated multiplexing [55], layered superposition coding [8, 56], and treating interference as noise [34, 57–59] remain accessible. Thus, GDoF characterizations under finite precision CSIT provide approximately optimal solutions for power control, rate-splitting, layered superposition based schemes that are quite robust in practice. The approximately optimal solutions serve as good initialization points for finer numerical optimizations needed at finite SNR, and inspire approximately optimal resource allocation schemes such as ITLinQ [60] and ITLinQ+ [61]. As such GDoF characterizations under finite precision CSIT are tremen-



$$\mathcal{D}_{\text{IC}} = \left\{ \begin{array}{rcl} (d_1, d_2, d_3) \in \mathbb{R}_+^3 : & & \\ d_1 & \leq & 2 \\ d_2 & \leq & 1 \\ d_3 & \leq & 1.5 \\ d_1 + d_2 & \leq & 2.3 \\ d_1 + d_3 & \leq & 2.4 \\ d_2 + d_3 & \leq & 1.5 \\ d_1 + d_2 + d_3 & \leq & 2.5 \end{array} \right\}, \ \mathcal{D}_{\text{BC}} = \left\{ \begin{array}{rcl} (d_1, d_2, d_3) \in \mathbb{R}_+^3 : & & \\ d_1 & \leq & 2 \\ d_2 & \leq & 1 \\ d_3 & \leq & 1.5 \\ d_1 + d_2 & \leq & 2.5 \\ d_1 + d_3 & \leq & 2.5 \\ d_2 + d_3 & \leq & 2.0 \\ d_1 + d_2 + d_3 & \leq & 3.0 \end{array} \right\}$$

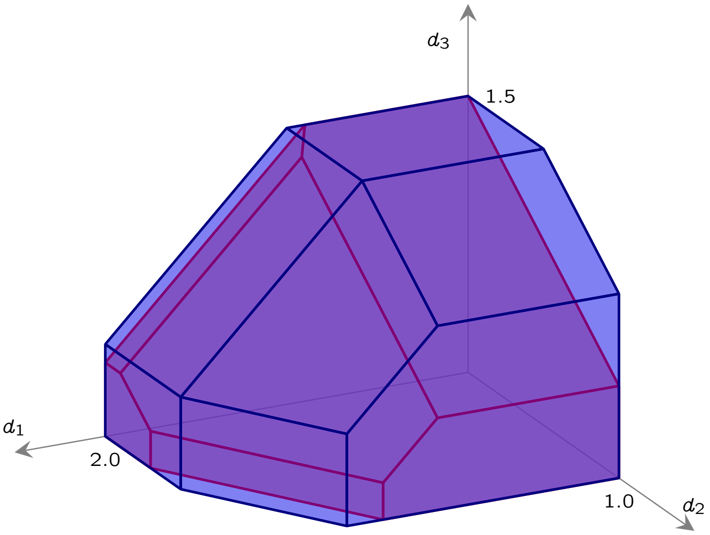


Figure 2.2: The GDoF region of the 3 user interference channel in red is superimposed upon the GDoF region of the same channel with transmitter cooperation in blue. A 20% GDoF gain is seen due to transmitter cooperation for this example.

dously useful in bringing theory closer to practice.

### 2.3.4 GDoF Comparisons

Comparing the GDoF of interference and broadcast channels under finite precision CSIT reveals the benefits of transmitter cooperation. As an example, consider the 3 user interference channel with the values of $\alpha_{ij}$ parameters as shown in Fig. 2.2. The channel parameters place this setting in the TIN regime [34], so its GDoF region is achieved by a TIN scheme. The GDoF region is shown in red in Fig. 2.2. Allowing transmitter cooperation under finite precision CSIT gives us a MISO BC. Since the TIN regime is included in the SLS regime, the GDoF of this MISO BC are characterized in [36]. The GDoF region is shown in blue in Fig. 2.2. Superposing the two GDoF regions we notice a significant improvement in sum-GDoF due to transmitter cooperation – 20% for this example. We would like to perform such comparisons for larger networks, i.e., networks with more than 3 users. However, since the results of [36] are limited to 3 users, direct comparisons are not currently feasible. Instead we will explore extremal GDoF gains for large number of users. Furthermore we will limit our focus to sum-GDoF achievable by TIN and the optimal GDoF with transmitter cooperation.

## 2.4 Definitions

**Definition 2.1** (TIN Regime)**.** *Define*

$$\mathcal{A}_{\text{TIN}} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \middle| \alpha_{ii} \geq \alpha_{il} + \alpha_{mi} \ \forall i, l, m \in [K], i \notin \{l, m\} \right\}. \tag{2.10}$$

The significance of the TIN regime is that in this regime, it was shown by Geng et al. in [34] that TIN is GDoF-optimal.

**Definition 2.2** (CTIN Regime)**.** *Define*

$$\mathcal{A}_{\text{CTIN}} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \middle| \begin{array}{l} \alpha_{ii} \geq \max(\alpha_{ij} + \alpha_{ji}, \alpha_{ik} + \alpha_{ji} - \alpha_{jk}), \\ \forall i, j, k \in [K], i \notin \{j, k\} \end{array} \right\}. \tag{2.11}$$

The significance of the CTIN regime is that in this regime, it was shown by Yi and Caire in [35] that the GDoF region achievable with TIN (also known as $\mathcal{D}_{\text{TINA}}$, see Definition 2.10), is convex, without the need for time-sharing, and equal to the polyhedral TIN region over the set of all $K$ users (see Definition 2.8). It is also shown in [62, Theorem 1] that TIN

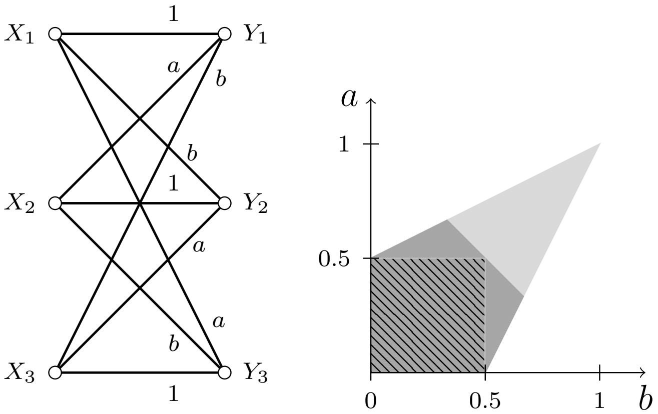


Figure 2.3: For the 3 user symmetric setting shown here, the TIN regime is marked by the slanted line pattern, the CTIN regime includes the TIN regime and the region shaded in dark gray, and the SLS regime includes the CTIN regime and the region shaded in light gray.

achieves the optimal GDoF region in the CTIN regime for the $K$ user interference channel under finite precision CSIT.

**Definition 2.3** (SLS Regime)**.** *Define the SLS regime,*

$$\mathcal{A}_{SLS} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \middle| \alpha_{ii} \geq \max(\alpha_{ij}, \alpha_{ki}, \alpha_{ik} + \alpha_{ji} - \alpha_{jk}),\ \forall i,j,k \in [K], i \notin \{j,k\} \right\}. \tag{2.12}$$

The significance of the SLS regime is that in this regime, it was shown by Davoodi and Jafar in [36] that a simple layered superposition scheme is GDoF-optimal for the MISO BC obtained by allowing transmitter cooperation in a $K$ user interference channel. Note that the result of [36] is limited to $K \leq 3$, however the regime is defined for all $K$. Also note that the SLS regime includes the CTIN regime, which includes the TIN regime. Fig 2.3 illustrates the progressively larger regimes for TIN, CTIN and SLS in a 3 user cyclically symmetric setting parameterized by channel strengths $a, b$.

**Definition 2.4** (Cycle $\pi$)**.** *A cycle $\pi$ of length $M > 1$ denoted as*

$$\pi = (i_1 \to i_2 \to \cdots \to i_M \circlearrowleft) \tag{2.13}$$

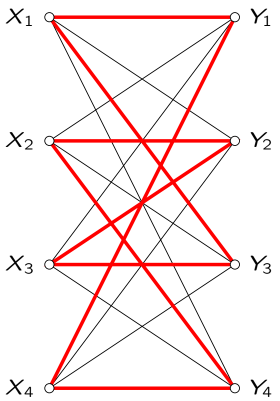


Figure 2.4: The links included in the cycle $\pi = (2 \to 4 \to 1 \to 3 \circlearrowleft)$ are highlighted in red.

*is an ordered collection of links in the* $K \times K$ *interference network, that includes the desired link between Transmitter* $i_m$ *and Receiver* $i_m$*, and the interfering link between Transmitter* $i_m$ *and Receiver* $i_{m+1}$*, for all* $m \in [1 : M]$*, where we set* $i_{M+1} = i_1$*, and the indices* $i_1, i_2, \cdots, i_M \in [K]$ *are all distinct. See Fig. 2.4 for an example. A cycle of length* $M = 1$ *is called a trivial cycle, represented simply as* $\pi = (i_1 \circlearrowleft)$ *for some* $i_1 \in [K]$*, and it includes only the desired link between Transmitter* $i_1$ *and Receiver* $i_1$*.*

*Also define the following terms related to the cycle* $\pi$*.*

1. *Define* $\pi(1) = i_1$ *as the head of the cycle. Other elements of the cycle may be similarly referenced, e.g.,* $\pi(2) = i_2, \pi(3) = i_3$*, and so on. Thus, the cycle may be equivalently represented as* $\pi = (\pi(1) \to \pi(2) \to \cdots \to \pi(M) \circlearrowleft)$*. Also note that if the cycle has length* $M$*, then the indices are interpreted modulo* $M$*, i.e.,* $\pi(M + i) = \pi(i)$ *for all integers* $i$*. For example, if* $\pi$ *is a cycle of length* $M = 5$*, then* $\pi(6) = \pi(1), \pi(7) = \pi(2)$*, etc.*

2. *Define* $\{\pi\} = \{i_1, i_2, \cdots, i_M\}$*, i.e.,* $\{\pi\}$ *represents the set of users involved in the cycle* $\pi$*.*

3. *Define* $w(\pi)$*, called the weight of the cycle* $\pi$*, as the sum of strengths of all interfering links included in the cycle, i.e.,* $w(\pi) = \sum_{m=1}^{M} \alpha_{i_{m+1} i_m}$*. The weight of a trivial cycle is*

*zero because it includes no interfering links.*

4. *Define* $\Pi$ *as the set of all cycles in the* $K$ *user network.*

5. *Cycles* $\pi_1, \pi_2, \cdots, \pi_n$ *are said to be disjoint if the sets* $\{\pi_1\}, \{\pi_2\}, \cdots, \{\pi_n\}$ *are disjoint.*

6. *Cycles* $\pi_1, \pi_2, \cdots, \pi_n$ *are said to comprise a cyclic partition of the set* $S \subset [K]$*, if they are disjoint and* $\bigcup_{i=1}^{n} \{\pi_i\} = S$*.*

The significance of cycles is that they lead to bounds on the sum-GDoF of the users involved in the cycle. For the interference channel, each cycle $\pi$ leads to a cycle bound $\sum_{k \in \pi} d_k \leq \Delta_\pi$ (see Definition 2.7) which is a bound on the GDoF region achievable by a restricted form of TIN, called polyhedral TIN (Definition 2.8). For the broadcast channel, each cycle $\pi$ leads to a bound $\sum_{k \in \pi} d_k \leq \Delta_\pi + \alpha_{\pi(i+1)\pi(i)}$ (see Lemma A.6 in Section A.2.4). Unlike the interference channel, the bounds for the BC are information theoretic bounds on the optimal GDoF region. These bounds are the key to all the results in this chapter.

**Definition 2.5** (Combined Cycles)**.** *For disjoint cycles*

$$\pi_1 = (i_1 \to \cdots \to i_{M_1} \underline{\Lsh}\,), \tag{2.14}$$

$$\pi_2 = (j_1 \to \cdots \to j_{M_2} \underline{\Lsh}\,), \tag{2.15}$$

*the combined cycle, denoted* $\pi_{1,2} = (\pi_1 \to \pi_2 \underline{\Lsh}\,)$*, is defined as*

$$\pi_{1,2} = (\pi_1 \to \pi_2 \underline{\Lsh}\,) = (i_1 \to \cdots \to i_{M_1} \to j_1 \to \cdots \to j_{M_2} \underline{\Lsh}\,). \tag{2.16}$$

*Note that* $\pi_{1,2}$ *is in general different from* $\pi_{2,1}$*. Combinations of more than 2 cycles are similarly defined. For example,* $\pi_{1,2,3} = (\pi_1 \to \pi_2 \to \pi_3 \underline{\Lsh}\,)$*.*

**Definition 2.6** ($\delta_{ij}$)**.** *For $i, j \in [K]$, define*

$$\delta_{ij} = \begin{cases} \alpha_{ii} - \alpha_{ji}, & i \neq j, \\ 0, & i = j. \end{cases} \tag{2.17}$$

**Definition 2.7** ($\Delta_\pi$)**.** *For any cycle $\pi$ of length $M$, $\pi = (i_1 \to i_2 \to \cdots \to i_M \circlearrowleft)$, define*

$$\Delta_\pi = \begin{cases} \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-1} i_M} + \delta_{i_M i_1}, & \textit{if } M > 1, \\ \alpha_{i_1 i_1}, & \textit{if } M = 1. \end{cases} \tag{2.18}$$

**Definition 2.8** ($\mathcal{D}_{\text{P-TIN}}(S)$)**.** *For any subset of users, $S \subset [K]$, the polyhedral-TIN region [34] is defined as*

$$\mathcal{D}_{\text{P-TIN}}(S) = \left\{ (d_k : k \in [K]) \;\middle|\; \begin{array}{ll} 0 = d_k, & \forall k \in [K] \backslash S, \\ 0 \leq d_k, & \forall k \in S, \\ \sum_{k \in \{\pi\}} d_k \leq \Delta_\pi, & \forall \pi \in \Pi, \{\pi\} \subset S \end{array} \right\}. \tag{2.19}$$

*The bounds, $\sum_{k \in \{\pi\}} d_k \leq \Delta_\pi$, are called cycle-bounds. Note that these are not bounds on the general GDoF region, rather these are only bounds on the polyhedral TIN region for a given subset $S$. The sum-GDoF value of polyhedral-TIN over the set $S$ is defined as*

$$\mathcal{D}_{\Sigma,\text{P-TIN}}(S) = \max_{\mathcal{D}_{\text{P-TIN}}(S)} \sum_{k \in S} d_k. \tag{2.20}$$

*If $S = [K]$, then we will simply write $\mathcal{D}_{\Sigma,\text{P-TIN}}([K]) = \mathcal{D}_{\Sigma,\text{P-TIN}}$.*

A remarkable fact about the polyhedral TIN region is that even if $S_1 \subset S_2$, it is possible that the polyhedral region for $S_1$ is strictly larger than the polyhedral region for $S_2$. See the simple example at the end of this section.

**Definition 2.9** (P-optimal Cyclic Partition of $S$)**.** *A cyclic partition of a subset of users $S$,*

*$S \subset [K]$, say into the $n$ disjoint cycles $\pi_1, \pi_2, \cdots, \pi_n$, is said to be p-optimal if*

$$\mathcal{D}_{\Sigma,\text{P-TIN}}(S) = \Delta_{\pi_1} + \Delta_{\pi_2} + \cdots + \Delta_{\pi_n}. \tag{2.21}$$

In general a p-optimal cyclic partition does not exist. Reference [37] showed that such partitions exist in the TIN regime. As one of the key elements of this chapter, it is shown in Theorem A.1 in Appendix A.1, that such partitions must exist in the SLS regime. Since CTIN and TIN regimes are all included in the SLS regime, these cyclic partitions exist in all three regimes.

**Definition 2.10** ($\mathcal{D}_{\text{TINA}}$)**.** *The TINA region [34, 35] is defined as*

$$\mathcal{D}_{\text{TINA}} = \bigcup_{S:S\subset[K]} \mathcal{D}_{\text{P-TIN}}(S). \tag{2.22}$$

*The sum-GDoF over the TINA region are defined as*

$$\mathcal{D}_{\Sigma,\text{TINA}} = \max_{\mathcal{D}_{\text{TINA}}} \sum_{k\in[K]} d_k. \tag{2.23}$$

Thus the TINA region is a union of polyhedral TIN regions. In general this union does not produce a convex region. For example, consider the two user interference channel shown in Fig. 2.5 where all $\alpha_{ij}$ values are equal to 1. Incidentally this channel is in the SLS regime. For this channel, $\mathcal{D}_{\text{P-TIN}}(\{1\}) = \{(d_1, d_2) : 0 \leq d_1 \leq 1, d_2 = 0\}, \mathcal{D}_{\text{P-TIN}}(\{2\}) = \{(d_1, d_2) : d_1 = 0, 0 \leq d_2 \leq 1\}, \mathcal{D}_{\text{P-TIN}}(\{1, 2\}) = \{(d_1, d_2) : 0 \leq d_1 + d_2 \leq 0\} = \{(d_1, d_2) : d_1 = 0, d_2 = 0\}$. The union of these three regions, $\mathcal{D}_{\Sigma,\text{TINA}} = \mathcal{D}_{\text{P-TIN}}(\{1\}) \bigcup \mathcal{D}_{\text{P-TIN}}(\{2\}) \bigcup \mathcal{D}_{\text{P-TIN}}(\{1, 2\})$, is not convex. However, remarkably, the region $\mathcal{D}_{\text{TINA}}$ is convex for channels in the TIN regime as shown by Geng et al. in [34], and for channels in the CTIN regime as shown by Yi and Caire in [35].

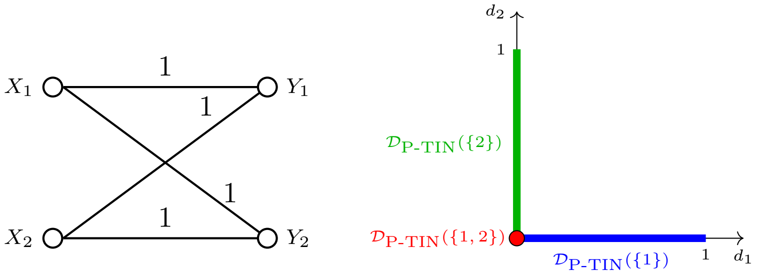

$X_1$
$Y_1$
$X_2$
$Y_2$
1
1
1
1
$d_2$
1
$\mathcal{D}_{\text{P-TIN}}(\{2\})$
$\mathcal{D}_{\text{P-TIN}}(\{1,2\})$
$\mathcal{D}_{\text{P-TIN}}(\{1\})$
1
$d_1$

Figure 2.5: A two user interference channel in the SLS regime and its non-convex TINA region corresponding to the union of three polyhedral TIN regions shown in green, blue and red.

## 2.5 Extremal Gain from Transmitter Cooperation in TIN Regime

First, let us compare the sum GDoFs when the topology falls in the TIN regime. Note that $K = 1$ is a degenerate case because there can be no cooperation among transmitters when there is only one transmitter.

**Theorem 2.1.** *For $K \geq 2$ users,*

$$\max_{[\alpha]_{K\times K}\in\mathcal{A}_{\text{TIN}}} \frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{IC}}} = \max_{[\alpha]_{K\times K}\in\mathcal{A}_{\text{TIN}}} \frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{TINA}}} = \frac{3}{2}. \tag{2.24}$$

### 2.5.1 Proof of Theorem 2.1: Upper Bound

In the TIN regime, the GDoF of the $K$ user interference channel are achieved by TIN as shown in [34], so $\mathcal{D}_{\Sigma,\text{IC}} = \mathcal{D}_{\Sigma,\text{TINA}}$. First, let us prove the upper bound, i.e., in the TIN-regime, $\mathcal{D}_{\Sigma,\text{BC}} \leq 1.5\mathcal{D}_{\Sigma,\text{IC}}$. Let $\pi = (i_1 \to i_2 \cdots \to i_M \circlearrowleft)$ be any cycle of length $M > 1$, and consider the corresponding IC cycle bound, which is an information theoretic bound on $\mathcal{D}_{\Sigma,\text{IC}}(\{\pi\})$, i.e., the sum-GDoF of the IC restricted to just the users that are involved in the cycle,

$$\mathcal{D}_{\Sigma,\text{IC}}(\{\pi\}) \leq \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-1} i_M} + \delta_{i_M i_1} = \Delta_\pi. \tag{2.25}$$

Note that $\Delta_\pi \geq \alpha_{i_1 i_1}$ because $\alpha_{i_1 i_1}$ GDoF are trivially achievable by simply allowing only user $i_1$ to transmit. For the same $M$ users, by Lemma A.6 in Appendix A.2 the sum-GDoF in the BC are bounded in two ways as,

$$\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-1} i_M} + \delta_{i_M i_1} + \alpha_{i_1 i_M} = \Delta_\pi + \alpha_{i_1 i_M}, \tag{2.26}$$

$$\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-1} i_M} + \delta_{i_M i_1} + \alpha_{i_2 i_1} = \Delta_\pi + \alpha_{i_2 i_1}, \tag{2.27}$$

$$\implies 2\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq 2\Delta_\pi + \alpha_{i_2 i_1} + \alpha_{i_1 i_M} \leq 2\Delta_\pi + \alpha_{i_1 i_1} \leq 3\Delta_\pi. \tag{2.28}$$

In (2.28) we made use of the fact that in the TIN-regime, $\alpha_{i_2 i_1} + \alpha_{i_1 i_M} \leq \alpha_{i_1 i_1} \leq \Delta_\pi$. Also for a trivial cycle, $\pi$, of length $M = 1$, say comprised of only user $m$, we have $\mathcal{D}_{\Sigma,\text{IC}}(\{\pi\}) = \mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) = \alpha_{mm} = \Delta_\pi$, so here also $\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq 1.5\Delta_\pi$. Therefore for every cycle $\pi$ we have $\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq 1.5\Delta_\pi$. Now, let us consider the total GDoF of all $K$ users. Since $[\alpha]_{K\times K} \in \mathcal{A}_{\text{TIN}}$, from [37] we know that $\mathcal{D}_{\Sigma,\text{IC}}$ is given by a cycle partition, comprised of, say the $N$ cycles $\pi_1, \pi_2, \cdots, \pi_N$. Note that the cycles are disjoint and $\bigcup_{i=1}^{n}\{\pi_i\} = [K]$.

$$\mathcal{D}_{\Sigma,\text{IC}} = \sum_{n=1}^{N} \Delta_{\pi_n}, \tag{2.29}$$

$$\mathcal{D}_{\Sigma,\text{BC}} \leq \sum_{n=1}^{N} \mathcal{D}_{\Sigma,\text{BC}}(\{\pi_n\}) \leq \sum_{n=1}^{N} 1.5\Delta_{\pi_n} = 1.5\mathcal{D}_{\Sigma,\text{IC}}. \tag{2.30}$$

This completes the proof of the upper bound for Theorem 2.1. □

### 2.5.2 Proof of Theorem 2.1: Lower Bound

Next, let us prove the lower bound for Theorem 2.1, i.e., for any $K \geq 2$, there exist $[\alpha]_{K\times K} \in \mathcal{A}_{\text{TIN}}$, such that $\mathcal{D}_{\Sigma,\text{BC}} \geq 1.5\mathcal{D}_{\Sigma,\text{IC}}$. For $K = 2$ users consider the channel with $\alpha_{11} = \alpha_{22} = 1, \alpha_{12} = \alpha_{21} = 0.5$, for which $\mathcal{D}_{\Sigma,\text{IC}} = 1$ according to [34] but $\mathcal{D}_{\Sigma,\text{BC}} = 1.5$ according to [63]. For $K \geq 3$ it is trivial to generate such $[\alpha]_{K\times K} \in \mathcal{A}_{\text{TIN}}$ simply by adding trivial users $k \in [3 : K]$ such that all $\alpha_{ij}$ (including the desired links $\alpha_{ii}$) associated with these additional users are zero, i.e., $\alpha_{ij} = 0$ for $i$ or $j$ is in $[3 : K]$. The resulting network is still in $\mathcal{A}_{\text{TIN}}$. This completes the proof of Theorem 2.1. □

## 2.6 Extremal Gain from Transmitter Cooperation in CTIN Regime

**Theorem 2.2.** *For arbitrary number of users, $K$,*

$$\max_{[\alpha]_{K\times K}\in\mathcal{A}_{\text{CTIN}}} \frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{TINA}}} = \max_{[\alpha]_{K\times K}\in\mathcal{A}_{\text{CTIN}}} \frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{IC}}} = 2 - \frac{1}{K}. \tag{2.31}$$

Thus, the extremal GDoF gain is always less than 2 in the CTIN regime, regardless of the number of users.

### 2.6.1 Proof of Theorem 2.2: Upper Bound

From Theorem 1 in [62] we already know that $\mathcal{D}_{\Sigma,\text{TINA}} = \mathcal{D}_{\Sigma,\text{IC}}$. Now let us prove the upper bound for Theorem 2.2, i.e., $\mathcal{D}_{\Sigma,\text{BC}}/\mathcal{D}_{\Sigma,\text{IC}} \leq 2 - 1/K$ in the CTIN regime. For any cycle $\pi$ of length $M$, define

$$\alpha_{\max}(\pi) = \max_{m\in[M]} \alpha_{\pi(m)\pi(m)}, \tag{2.32}$$

$$\alpha_{\min}(\pi) = \begin{cases} \min_{m\in[M]} \alpha_{\pi(m+1)\pi(m)}, & M > 1, \\ 0, & M = 1. \end{cases} \tag{2.33}$$

In the CTIN regime, $\mathcal{D}_{\Sigma,\text{P-TIN}}(\{\pi\}) \leq \Delta_\pi$, and as shown by [35], $\mathcal{D}_{\Sigma,\text{P-TIN}}(\{\pi\}) \geq \mathcal{D}_{\Sigma,\text{P-TIN}}(\{\pi(m)\}) = \alpha_{\pi(m)\pi(m)}$ for all $m \in [M]$. Therefore,

$$\Delta_\pi \geq \alpha_{\max}(\pi). \tag{2.34}$$

From Definition 2.7,

$$\begin{aligned} \Delta_\pi &= \sum_{m\in[M]} \alpha_{\pi(m)\pi(m)} - \alpha_{\pi(m+1)\pi(m)} && (2.35) \\ &\leq M\alpha_{\max}(\pi) - M\alpha_{\min}(\pi). && (2.36) \end{aligned}$$

From Lemma A.6,

$$\begin{aligned} \mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) &\leq \Delta_\pi + \alpha_{\min}(\pi) && (2.37) \\ &= \Delta_\pi \left(1 + \frac{\alpha_{\min}(\pi)}{\Delta_\pi}\right) && (2.38) \\ &\leq \Delta_\pi \left(1 + \frac{\alpha_{\max}(\pi)}{\Delta_\pi} - \frac{1}{M}\right) && (2.39) \\ &\leq \Delta_\pi \left(2 - \frac{1}{M}\right). && (2.40) \end{aligned}$$

To obtain (2.39) we used (2.36), and to obtain (2.40) we used (2.34).

Now let $\pi_1, \pi_2, \cdots, \pi_N$ be a p-optimal cyclic partition of $[K]$ into $N$ cycles of lengths

$M_1, M_2, \cdots, M_N$, respectively. Then we have

$$\begin{aligned}
\mathcal{D}_{\Sigma,\text{BC}} &\leq \sum_{n=1}^{N} \mathcal{D}_{\Sigma,\text{BC}}(\{\pi_n\}) && (2.41)\\
&\leq \sum_{n=1}^{N} \Delta_{\pi_n} \left(2 - \frac{1}{M_n}\right) && (2.42)\\
&\leq \sum_{n=1}^{N} \Delta_{\pi_n} \left(2 - \frac{1}{K}\right) && (2.43)\\
&= \mathcal{D}_{\Sigma,\text{IC}} \left(2 - \frac{1}{K}\right). && (2.44)
\end{aligned}$$

(2.42) was obtained by using (2.40), and (2.43) follows because any cycle involves at most $K$ users, $M_n \leq K$. Finally, (2.44) follows because $\pi_1, \cdots, \pi_N$ represent the p-optimal cyclic partition, so $\mathcal{D}_{\Sigma,\text{P-TIN}}([K]) = \sum_{n=1}^{N} \Delta_{\pi_n}$, and because we are in the CTIN regime, according to [35], $\mathcal{D}_{\Sigma,\text{P-TIN}}([K]) = \mathcal{D}_{\Sigma,\text{TINA}}$ which is equal to $\mathcal{D}_{\Sigma,\text{IC}}$ according to [62, Theorem 1]. This proves the upper bound, i.e., $\mathcal{D}_{\Sigma,\text{BC}}/\mathcal{D}_{\Sigma,\text{TINA}} = \mathcal{D}_{\Sigma,\text{BC}}/\mathcal{D}_{\Sigma,\text{IC}} \leq 2 - 1/K$ for all $[\alpha]_{K\times K} \in \mathcal{A}_{\text{CTIN}}$. □

### 2.6.2 Proof of Theorem 2.2: Lower Bound

Next let us prove the lower bound for Theorem 2.2, i.e., there exists $[\alpha]_{K\times K} \in \mathcal{A}_{\text{CTIN}}$ such that $\mathcal{D}_{\Sigma,\text{BC}}/\mathcal{D}_{\Sigma,\text{IC}} \geq 2 - 1/K$. Let us define channel strength parameters as follows. $\alpha_{ij}$ takes the value $K$ if $i = j$, and $\alpha_{ij}$ takes the value in $[1 : K-1]$ that is equivalent to $(j - i)$

mod $K$ when $i \neq j$. The channel strength parameter matrix can be written explicitly as,

$$[\alpha]_{K\times K} = \begin{bmatrix} K & 1 & 2 & 3 & \cdots & K-2 & K-1 \\ K-1 & K & 1 & 2 & \cdots & K-3 & K-2 \\ K-2 & K-1 & K & 1 & \cdots & K-4 & K-3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 2 & 3 & 4 & 5 & \cdots & K & 1 \\ 1 & 2 & 3 & 4 & \cdots & K-1 & K \end{bmatrix}. \tag{2.45}$$

Let us verify that $[\alpha]_{K\times K} \in \mathcal{A}_{\text{CTIN}}$. Due to the symmetry in this topology, it suffices to verify $\alpha_{11} \geq \alpha_{1j} + \alpha_{j1}$ for all $j \in [2:K]$, and $\alpha_{11} + \alpha_{jk} \geq \alpha_{1k} + \alpha_{j1}$ for all $j,k \in [2:K], j \neq k$. For $j \in [2:K]$, $\alpha_{1j} = j-1$, and $\alpha_{j1} = K-(j-1)$, so we have $\alpha_{1j} + \alpha_{j1} = K \leq \alpha_{11}$. Furthermore, since $\alpha_{jk} = (k-j) \bmod K$, we have

$$\alpha_{11} + \alpha_{jk} - \alpha_{j1} - \alpha_{1k} \tag{2.46}$$

$$= K + ((k-j) \bmod K) - (K-(j-1)) - (k-1) \tag{2.47}$$

$$= ((k-j) \bmod K) - (k-j) \geq 0. \tag{2.48}$$

Thus, the parameters are in the CTIN regime. Next we show that $\mathcal{D}_{\Sigma,\text{TINA}} = K$. According to [35], in the CTIN regime we have $\mathcal{D}_{\Sigma,\text{TINA}}([K]) = \mathcal{D}_{\Sigma,\text{P-TIN}}([K])$. So consider the cycle $\pi = (1 \to 2 \to 3 \to \cdots \to K \circlearrowleft)$,

$$\mathcal{D}_{\Sigma,\text{TINA}}([K]) = \mathcal{D}_{\Sigma,\text{P-TIN}}([K]) \leq \Delta_\pi = \sum_{i=1}^{K} (K-(K-1)) = K. \tag{2.49}$$

But we also know that $\mathcal{D}_{\Sigma,\text{TINA}} \geq \alpha_{11} = K$ because it is possible to activate only user 1 and achieve $K$ GDoF. Therefore, $\mathcal{D}_{\Sigma,\text{TINA}} = K$. Moreover, since TIN is GDoF-optimal in the CTIN regime according to Theorem 1 in [62], we have $\mathcal{D}_{\Sigma,\text{IC}} = K$. Finally, let us show that for the given channel strength parameters, $\mathcal{D}_{\Sigma,\text{BC}} = 2K-1$. We already know from

Lemma A.6, that $\mathcal{D}_{\Sigma,\text{BC}} \leq \Delta_\pi + \alpha_{21} = 2K-1$. Let us show that $2K-1$ sum-GDoF are also achievable in the MISO BC as follows. Let $U$ be a Gaussian codeword carrying $K-1$ GDoF, as a common message for all users. Let $V_i, i \in [K]$ be a codeword carrying 1 GDoF, as a private message for User $i$. Let the $i^{th}$ transmit antenna send $X_i = c(\bar{P}^0 U + \bar{P}^{-(K-1)} V_i)$ where $c = \frac{1}{\sqrt{1+P^{-(K-1)}}} = \Theta(1)$ is a constant chosen to satisfy the input power constraint. Receiver $k$ ($k \in [K]$) can decode codeword $U$ first while treating all $V_i$ as noise, because $U$ is heard with power $P^K$, and the noise floor due to all $V_i$ is no more than $P^1$. Thus, the SINR for decoding $U$ is $P^{K-1}$, which suffices because $U$ carries only $K-1$ GDoF. After decoding and removing $U$ from the received signal, Receiver $k$ can decode $V_k$. This decoding is successful because $V_k$ is heard by Receiver $k$ with power $P$, while the interference from every other $V_i, i \neq k$ is received with no more than power $P^0$. Thus, the SINR for decoding $V_k$ at Receiver $k$ is $P^1$, which suffices because $V_k$ carries only 1 GDoF. Thus, the BC achieves a total of $(K-1)+K = 2K-1$ sum-GDoF. This completes the proof of the lower bound for Theorem 2.2. □

## 2.7 Extremal Gain from Transmitter Cooperation in SLS Regime

**Theorem 2.3.**

$$\sup_{[\alpha]_{K\times K} \in \mathcal{A}_{\text{SLS}}} \frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{TINA}}} = \Theta(\log(K)). \tag{2.50}$$

### 2.7.1 Proof of Theorem 2.3: Upper Bound

Let us describe an iterative procedure. Stage $\lambda$ of the procedure, $\lambda \in [0:\Lambda]$, is characterized by a subset of users, $S_\lambda \subset [K]$, a cyclic partition of $S_\lambda$ into $N_\lambda$ disjoint cycles

$\pi_1^{S_\lambda}, \pi_2^{S_\lambda}, \cdots, \pi_{N_\lambda}^{S_\lambda}$, and a cyclic partition of $[K]$ into $N_\lambda$ disjoint cycles $\pi_1^\lambda, \pi_2^\lambda, \cdots, \pi_{N_\lambda}^\lambda$. The procedure stops in stage $\lambda = \Lambda$ as soon as we find $N_\lambda = 1$.

Stage 0 is the initialization stage. The procedure is initialized with the set $S_o = [K]$, the set of all users. Let $\pi_1^{S_o}, \pi_2^{S_o}, \cdots, \pi_{N_o}^{S_o}$ be a p-optimal cyclic partition of $S_o$ with at most one trivial cycle. Such a partition exists and produces the tight sum-GDoF bound for polyhedral TIN over $S_o$ so that

$$\mathcal{D}_{\Sigma,\text{P-TIN}}(S_o) = \Delta_{\pi_1^{S_o}} + \Delta_{\pi_2^{S_o}} + \cdots + \Delta_{\pi_{N_o}^{S_o}}. \tag{2.51}$$

Choose $(\pi_1^o, \pi_2^o, \cdots, \pi_{N_o}^o) = (\pi_1^{S_o}, \pi_2^{S_o}, \cdots, \pi_{N_o}^{S_o})$. This completes the initialization stage. Note that because the p-optimal cyclic partition cannot have more than one trivial cycle, we must have $N_o \leq (K+1)/2$. If $N_o = 1$, then $\Lambda = 0$ and the procedure stops here. If not, then we move to the next stage.

Stage 1 begins by defining the set of users,

$$S_1 = \{\pi_1^o(1), \pi_2^o(1), \cdots, \pi_{N_o}^o(1)\}. \tag{2.52}$$

Let $\pi_1^{S_1}, \pi_2^{S_1}, \cdots, \pi_{N_1}^{S_1}$ be a p-optimal cyclic partition of $S_1$ with at most one trivial cycle, so that

$$\mathcal{D}_{\Sigma,\text{P-TIN}}(S_1) = \Delta_{\pi_1^{S_1}} + \Delta_{\pi_2^{S_1}} + \cdots + \Delta_{\pi_{N_1}^{S_1}}. \tag{2.53}$$

Note that these cycles only span $S_1$. For each of these cycles, $\pi_n^{S_1}$, $n \in [1 : N_1]$, we will create a combined cycle, $\pi_n^1$ such that the $N_1$ combined cycles will be a cyclic partition of $[K]$. This is done as follows. Let us write the $n^{th}$ cycle, $\pi_n^{S_1}$, explicitly as,

$$\pi_n^{S_1} = (\pi_{n_1}^o(1) \rightarrow \pi_{n_2}^o(1) \rightarrow \cdots \rightarrow \pi_{n_{m_n}}^o(1) \underline{\Lsh}). \tag{2.54}$$

Then the corresponding combined cycle is defined as

$$\pi_n^1 = (\pi_{n_1}^o \to \pi_{n_2}^o \to \cdots \to \pi_{n_{m_n}}^o \underline{\Lsh}\,) \tag{2.55}$$

for $n \in [1 : N_1]$. Now note that $\pi_1^1, \pi_2^1, \cdots, \pi_{N_1}^1$ span $[K]$, in fact they constitute a cyclic partition of $[K]$. This completes Stage 1.

Note that $S_1$ has $N_o$ users, and the p-optimal cyclic partition does not have more than one trivial cycle, so we must have $N_1 \leq (N_o + 1)/2$. Furthermore, it follows from Lemma A.5 that

$$\Delta_{\pi_n^1} \leq \Delta_{\pi_{n_1}^o} + \Delta_{\pi_{n_2}^o} + \cdots + \Delta_{\pi_{n_{m_n}}^o} + \Delta_{\pi_n^{S_1}}. \tag{2.56}$$

Summing over all $n \in [1 : N_1]$ we have

$$\begin{aligned}
\Delta_{\pi_1^1} + \Delta_{\pi_2^1} + \cdots + \Delta_{\pi_{N_1}^1} &\leq \Delta_{\pi_1^o} + \Delta_{\pi_2^o} + \cdots + \Delta_{\pi_{N_o}^o} + \Delta_{\pi_1^{S_1}} + \Delta_{\pi_2^{S_1}} + \cdots + \Delta_{\pi_{N_1}^{S_1}} && (2.57)\\
&= \Delta_{\pi_1^o} + \Delta_{\pi_2^o} + \cdots + \Delta_{\pi_{N_o}^o} + \mathcal{D}_{\Sigma,\text{P-TIN}}(S_1) && (2.58)\\
&\leq \Delta_{\pi_1^o} + \Delta_{\pi_2^o} + \cdots + \Delta_{\pi_{N_o}^o} + \mathcal{D}_{\Sigma,\text{TINA}}. && (2.59)
\end{aligned}$$

If $N_1 = 1$, then we set $\Lambda = 1$ and the procedure stops here. If not, then we proceed to the next stage.

The procedure now simply repeats, so that at the $(\lambda + 1)^{th}$ stage we have the set of users

$$S_{\lambda+1} = \{\pi_1^\lambda(1), \pi_2^\lambda(1), \cdots, \pi_{N_\lambda}^\lambda(1)\}. \tag{2.60}$$

A p-optimal cyclic partition of $S_{\lambda+1}$ with at most one trivial cycle produces $N_{\lambda+1}$ disjoint cycles, $\pi_1^{S_{\lambda+1}}, \pi_2^{S_{\lambda+1}}, \cdots, \pi_{N_{\lambda+1}}^{S_{\lambda+1}}$, such that the $l^{th}$ cycle in this partition,

$$\pi_l^{S_{\lambda+1}} = (\pi_{l_1}^{\lambda}(1) \to \pi_{l_2}^{\lambda}(1) \to \cdots \to \pi_{l_{m_l}}^{\lambda}(1) \Lsh) \tag{2.61}$$

produces the $l^{th}$ combined cycle

$$\pi_l^{\lambda+1} = (\pi_{l_1}^{\lambda} \to \pi_{l_2}^{\lambda} \to \cdots \to \pi_{l_{m_l}}^{\lambda} \Lsh) \tag{2.62}$$

for $l \in [1 : N_{\lambda+1}]$. This completes Stage $\lambda + 1$. Since $S_{\lambda+1}$ has $N_\lambda$ users, and the p-optimal cycle cannot have more than one trivial cycle, we must have $N_{\lambda+1} \leq (N_\lambda + 1)/2$. Furthermore, it follows from Lemma A.5 that

$$\Delta_{\pi_1^{\lambda+1}} + \Delta_{\pi_2^{\lambda+1}} + \cdots + \Delta_{\pi_{N_{\lambda+1}}^{\lambda+1}} \leq \Delta_{\pi_1^{\lambda}} + \Delta_{\pi_2^{\lambda}} + \cdots + \Delta_{\pi_{N_\lambda}^{\lambda}} + \mathcal{D}_{\Sigma,\text{TINA}}. \tag{2.63}$$

If $N_{\lambda+1} = 1$, then the procedure stops and $\Lambda = \lambda + 1$, otherwise the procedure continues. This completes the description of the procedure.

$\Lambda$ can be bounded by using $N_{\lambda+1} \leq (N_\lambda + 1)/2$, $N_o \leq (K + 1)/2$ and $N_{\Lambda-1} \geq 2$, as follows. $N_{\Lambda-1} \geq 2 \Rightarrow N_{\Lambda-2} \geq 3 \Rightarrow N_{\Lambda-3} \geq 5 \Rightarrow \cdots \Rightarrow N_o \geq 2^{\Lambda-1} + 1 \Rightarrow K \geq 2^{\Lambda} + 1 \Rightarrow \Lambda \leq \log_2(K - 1)$.

Finally, we complete the proof of the upper bound as follows.

$$\begin{aligned}
\mathcal{D}_{\Sigma,\text{TINA}} &\geq \mathcal{D}_{\Sigma,\text{P-TIN}}(S_o) && (2.64)\\
&= \Delta_{\pi_1^o} + \Delta_{\pi_2^o} + \cdots + \Delta_{\pi_{N_o}^o} && (2.65)\\
&\geq \Delta_{\pi_1^1} + \Delta_{\pi_2^1} + \cdots + \Delta_{\pi_{N_1}^1} - \mathcal{D}_{\Sigma,\text{TINA}} && (2.66)\\
&\geq \Delta_{\pi_1^2} + \Delta_{\pi_2^2} + \cdots + \Delta_{\pi_{N_2}^2} - 2\mathcal{D}_{\Sigma,\text{TINA}} && (2.67)\\
&\vdots\\
&\geq \Delta_{\pi_1^\Lambda} - \Lambda\mathcal{D}_{\Sigma,\text{TINA}} && (2.68)
\end{aligned}$$

$$\geq \mathcal{D}_{\Sigma,\text{BC}} - \mathcal{D}_{\Sigma,\text{TINA}} - \Lambda\mathcal{D}_{\Sigma,\text{TINA}}, \tag{2.69}$$

where in the last step we used Lemma A.6. Substituting the bound for $\Lambda$ we obtain

$$\frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{TINA}}} \leq 2 + \log_2(K-1) \tag{2.70}$$

$$= \Theta(\log_2(K)), \tag{2.71}$$

and the proof of the upper bound is complete. □

### 2.7.2 Proof of Theorem 2.3: Lower Bound

For the lower bound, let us define a class of interference networks, $\mathcal{N}^{[n,\nu]}$, that is parameterized by the two numbers, $n \in \mathbb{N}, \nu \in \mathbb{R}$, $0 \leq \nu \leq 1$. The number of users $K(n) = 2^n$, all desired channel strengths $\alpha_{kk} = 1$, and cross-channel strengths satisfy $\alpha_{ij}^{[n,\nu]} = \alpha_{ji}^{[n,\nu]}$ for all $i, j, k \in [K(n)]$. Since $\alpha_{ij}^{[n,\nu]} = \alpha_{ii} - \delta_{ji}^{[n,\nu]} = 1 - \delta_{ji}^{[n,\nu]} = 1 - \delta_{ij}^{[n,\nu]}$, it suffices to specify the $\delta_{ij}^{[n,\nu]}$ values instead of the $\alpha_{ij}^{[n,\nu]}$ values. To specify the $\delta_{ij}^{[n,\nu]}$ values it will be useful to represent $\mathcal{N}^{[n,\nu]}$ as a full binary tree of depth $n$. The $2^n$ leaf nodes of this tree represent the $2^n$ users. The value of $\delta_{ij}^{[n,\nu]} = \delta_{ji}^{[n,\nu]} = \left(\frac{2^{p-1}}{2^n}\right)\nu$ if the closest common ancestor of user $i$ and user $j$ is $p$ levels above them. For example, $\delta_{ij}^{[n,\nu]} = \frac{\nu}{2^n}$ if user $i$ and $j$ are siblings (share a common parent), $\frac{2\nu}{2^n}$ if they share the same grandparent (but not the same parent), and the largest possible value of $\delta_{ij}^{[n,\nu]}$ in $\mathcal{N}^{[r,\nu]}$ is $\nu/2$, between users whose closest common ancestor is the root node. An interference network with these parameter values is said to be an $\mathcal{N}^{[n,\nu]}$ network. Fig. 2.6 shows the binary tree for the network $\mathcal{N}^{[3,1]}$. We are primarily interested in the network for $\nu = 1$. [6]

[6] Even though we are interested primarily in $\nu = 1$, the network $\mathcal{N}^{[n,\nu]}$ is defined for arbitrary $\nu$ because the network has a hierarchical structure and the two parameters, $n$ and $\nu$, can be used to specify the subnetworks in the hierarchy. For example, the $\mathcal{N}^{[3,1]}$ network in Fig. 2.6 consists of two $\mathcal{N}^{[2,1/2]}$ subnetworks, and each of them in turn contains two $\mathcal{N}^{[1,1/4]}$ subnetworks. These subnetworks are important for the proof of achievability (see e.g., (2.78)).

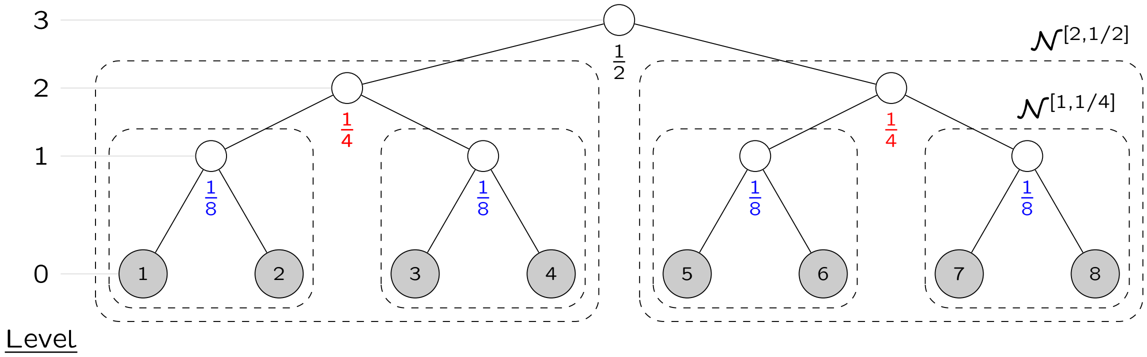


Figure 2.6: The binary tree representation of the network $\mathcal{N}^{[3,1]}$, and its subnetworks. The value of $\delta_{ij}^{[n,1]} = 1 - \alpha_{ij}^{[n,1]}$ between users $i$ and $j$ is given by the number indicated under their closest common ancestor. For example, $\delta_{78} = \delta_{87} = 1/8, \delta_{14} = \delta_{41} = 1/4, \delta_{37} = \delta_{73} = 1/2$.

Let us first prove that an $\mathcal{N}^{[n,\nu]}$ network is indeed in the SLS regime. From the definition of $\delta_{ij}^{[n,\nu]} = 1 - \alpha_{ij}^{[n,\nu]}$, we have

$$\alpha_{ij}^{[n,\nu]} = 1 - \left(\frac{2^{p_{ij}-1}}{2^n}\right)\nu, \tag{2.72}$$

$$\alpha_{ki}^{[n,\nu]} = 1 - \left(\frac{2^{p_{ki}-1}}{2^n}\right)\nu. \tag{2.73}$$

Since $\alpha_{ii} = 1$ and $\nu \geq 0$, it is trivially verified that $\alpha_{ii} \geq \max(\alpha_{ij}(\nu), \alpha_{ki}(\nu))$ for all $i, j, k \in [K(n)]$. Now, if users $i, j$ have their closest common ancestor $p_{ij}$ levels above them, and if users $i, k$ have their closest common ancestor $p_{ki}$ levels above them, then the users $j, k$ must have a common ancestor no more than $\max(p_{ij}, p_{ki})$ levels above them. Therefore,

$$\alpha_{jk}^{[n,\nu]} \geq 1 - \left(\frac{2^{\max(p_{ij},p_{ki})-1}}{2^n}\right)\nu \tag{2.74}$$

$$\implies \alpha_{ii} + \alpha_{jk}^{[n,\nu]} \geq 1 + 1 - \left(\frac{2^{\max(p_{ij},p_{ki})-1}}{2^n}\right)\nu \tag{2.75}$$

$$\geq 1 + 1 - \left(\frac{2^{p_{ij}-1}}{2^n} + \frac{2^{p_{ki}-1}}{2^n}\right)\nu \tag{2.76}$$

$$= \alpha_{ij}^{[n,\nu]} + \alpha_{ki}^{[n,\nu]}. \tag{2.77}$$

Thus the SLS condition is satisfied.

Next we will prove that the TINA region for this network does not allow more than 2 sum-GDoF. For this let us go through the following three steps.

1. The main argument for this proof is recursive, where we repeatedly reduce a network into its subnetworks. In particular, we are interested in the *left* and *right* subnetworks of $\mathcal{N}^{[n,\nu]}$, as described next. Consider the root node of the binary tree representation of $\mathcal{N}^{[n,\nu]}$. It has two child nodes, say labeled as 'left' and 'right'. If the root node is eliminated, then the tree splits into two binary trees, and each of those original child nodes becomes the root node of one of those trees. Let us denote these two networks as Left($\mathcal{N}^{[n,\nu]}$) and Right($\mathcal{N}^{[n,\nu]}$). Let us show that each of the networks Left($\mathcal{N}^{[n,\nu]}$) and Right($\mathcal{N}^{[n,\nu]}$) is an $\mathcal{N}^{[n-1,\nu/2]}$ network, as follows. Since the original root node is eliminated, it is obvious that the binary tree representation of each of these subnetworks has depth $n-1$, and correspondingly each subnetwork has $2^{n-1}$ users. The channel strengths are the same as before, but since the value of $n$ has changed to $n-1$, the value of $\nu$ needs to change to $\nu/2$ to preserve the channel strengths, so in the new subnetworks we have

$$\delta_{ij}^{[n-1,\nu/2]} = \left(\frac{2^{p-1}}{2^{n-1}}\right)\left(\frac{\nu}{2}\right) = \left(\frac{2^{p-1}}{2^{n}}\right)\nu = \delta_{ij}^{[n,\nu]}. \tag{2.78}$$

   where either both $i, j$ belong to the left subnetwork or both belong to the right subnetwork.

2. Next we show that $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]} \leq \max\left(1, \frac{1}{2}\mathcal{D}_{\Sigma,\text{TINA}}^{[n,2\nu]}\right)$, where $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]}$ represents the optimal sum-GDoF value over the $\mathcal{D}_{\text{TINA}}^{[n,\nu]}$ region for $\mathcal{N}^{[n,\nu]}$. This is proved as follows. From Definition 2.10, we know that $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]}$ is equal to $\mathcal{D}_{\Sigma,\text{P-TIN}}^{[n,\nu]}(S)$ for some subset of users, $S \subset [K(n)]$. From Theorem A.1 we know that $\mathcal{D}_{\Sigma,\text{P-TIN}}^{[n,\nu]}(S)$ is determined by the cycle bounds corresponding to a p-optimal cyclic partition of $S$. There are two possibilities — either the cyclic partition includes a trivial cycle, or it does not, and we will consider

them one by one.

First, suppose the p-optimal cyclic partition of $S$ does not include any trivial cycles. In that case, let $\pi = (i_1 \to \cdots \to i_M \circlearrowleft)$ be any cycle from the p-optimal cyclic partition of $S$. By assumption, the length of $\pi$ is $M > 1$. The cycle bound corresponding to $\pi$ for $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]}$ is

$$\sum_{k \in \{i_1, \cdots, i_M\}} d_k \leq \delta_{i_1 i_2}^{[n,\nu]} + \cdots + \delta_{i_{M-1} i_M}^{[n,\nu]} + \delta_{i_M i_1}^{[n,\nu]} \tag{2.79}$$

$$= \frac{1}{2}\left(\delta_{i_1 i_2}^{[n,2\nu]} + \cdots + \delta_{i_{M-1} i_M}^{[n,2\nu]} + \delta_{i_M i_1}^{[n,2\nu]}\right). \tag{2.80}$$

Therefore, all the non-trivial cycle bounds $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]}$ are exactly half as large as the corresponding cycle bounds in $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,2\nu]}$, proving that in this case $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]} = \frac{1}{2}\mathcal{D}_{\Sigma,\text{TINA}}^{[n,2\nu]}$.

Now consider the remaining alternative, that the p-optimal cyclic partition of $S$ includes a trivial cycle. We claim that in this case $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]} = 1$. This is shown as follows. Suppose $\pi = \{i\}$ is a trivial cycle included in the p-optimal cyclic partition of $S$. Since the trivial cycle bound is active we must have $d_i = \alpha_{ii} = 1$. Now, let User $j$ be any other user in $S$. We immediately have the bound $d_i + d_j \leq \delta_{ij} + \delta_{ji} \leq 1$ (because in $\mathcal{N}^{[n,\nu]}$, all $\delta_{ij} \leq \nu/2$ and $\nu \leq 1$). Since $d_i = 1$, we must have $d_i + d_j = 1$ and therefore, $d_j = 0$. This is true for every user in $S$ besides user $i$. Therefore, $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]} = 1$ in this case.

3. The final step is to prove that $\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]} \leq 2$. Based on previous steps, this is proved as follows. Isolating the left and right subnetworks of $\mathcal{N}^{[n,\nu]}$ from each other's interference does not hurt either of them, therefore,

$$\mathcal{D}_{\Sigma,\text{TINA}}^{[n,\nu]} \leq \mathcal{D}_{\Sigma,\text{TINA}}^{[n-1,\nu/2]} + \mathcal{D}_{\Sigma,\text{TINA}}^{[n-1,\nu/2]} \tag{2.81}$$

$$= 2\mathcal{D}_{\Sigma,\text{TINA}}^{[n-1,\nu/2]} \tag{2.82}$$

$$\leq 2\max\left(1, \frac{1}{2}\mathcal{D}_{\Sigma,\text{TINA}}^{[n-1,\nu]}\right) \tag{2.83}$$

$$
\begin{aligned}
&= \max(2, \mathcal{D}_{\Sigma,\text{TINA}}^{[n-1,\nu]}) && (2.84)\\
&\leq \max(2, \max(2, \mathcal{D}_{\Sigma,\text{TINA}}^{[n-2,\nu]})) && (2.85)\\
&= \max(2, \mathcal{D}_{\Sigma,\text{TINA}}^{[n-2,\nu]}) && (2.86)\\
&\quad \vdots \\
&\leq \max(2, \mathcal{D}_{\Sigma,\text{TINA}}^{[1,\nu]}) && (2.87)\\
&= 2. && (2.88)
\end{aligned}
$$

Thus, TIN cannot achieve more than 2 sum-GDoF for our network.

Henceforth we will set $\nu = 1$ and prove that by allowing transmitter cooperation in this network, a sum-GDoF value of $1 + \frac{1}{2}\log_2(K)$ is achievable (and optimal). Recall that in a GDoF model, if Transmitter $j$ sends a message $W$ with power level $-\gamma_j$ to Receiver $i$ over a channel with strength $\alpha_{ij}$, then the received signal strength level is $\alpha_{ij} - \gamma_j$. The power levels are additive because these are exponents of $P$, or equivalently because they are being measured in dB scale. If the effective noise floor, i.e., the maximum power level of noise and interference from other messages heard by Receiver $i$ is $\mu_i$, and $W$ carries $d_W$ GDoF, then $W$ can be decoded successfully while treating all other signals as noise if $d_W \leq \alpha_{ij} - \gamma_j - \mu_i$. Once a message is decoded it can be subtracted from the received signal before decoding other messages. This is the basic principle of successive decoding, and we will use it for the achievability proof.

Before a detailed presentation of the achievable scheme for $\mathcal{N}^{[n,1]}$ networks, let us start with a sketch of the achievable scheme for the example network $\mathcal{N}^{[3,1]}$, as shown in Fig. 2.7. We saw the binary tree representation of this network earlier in Fig. 2.6. Recall that for this example, all direct links are of strength $\alpha_{ii} = 1$. For the cross links, in Fig. 2.7 the dotted blue lines are links of strength $\alpha_{ij} = 7/8$, the dashed red lines are of strength $\alpha_{ij} = 3/4$, and the gray lines are links of strength $\alpha_{ij} = 1/2$. The same gray common message at the

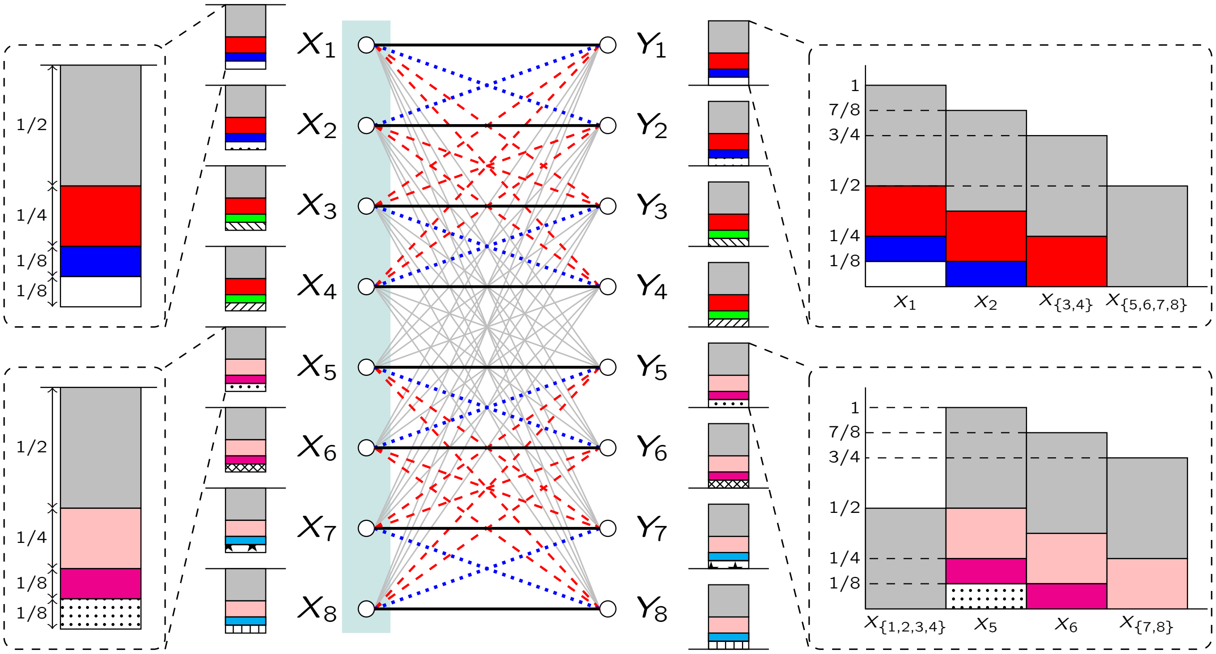


Figure 2.7: The SLS scheme for $\mathcal{N}^{[3,1]}$ that achieves $1 + \frac{1}{2}\log_2(K) = \frac{5}{2}$ sum-GDoF by transmitter cooperation.

top level is sent from all antennas to all users and carries 1/2 sum GDoF. The dashed red links are in two separate clusters of 4 users each, representing 2 subnetworks, each of the type $\mathcal{N}^{[2,1/2]}$ containing 4 users. A red common message is sent for the first cluster and a pink common message is used for the second cluster, each carrying 1/4 GDoF. Similarly, the dotted blue links are in 4 separate clusters of 2 users each, representing 4 subnetworks, each of the type $\mathcal{N}^{[1,1/4]}$ containing 2 users. The corresponding blue, green, magenta and cyan power levels represent separate common messages for each of the 4 subnetworks, carrying 1/8 GDoF each. Finally, at the bottom level there is an independent message carrying 1/8 GDoF for each user. The total sum-GDoF value thus achieved is $\left(\frac{1}{2}\right) + 2\left(\frac{1}{4}\right) + 4\left(\frac{1}{8}\right) + 8\left(\frac{1}{8}\right) = 5/2$. For the decoding, consider User 5 as an example. The gray message which carries 1/2 GDoF, is seen with power level 1 and noise floor due to interference from other messages is at power level 1/2 so it is successfully decoded and subtracted. Then the pink message, which carries 1/4 GDoF, is seen with power level 1/2 and effective noise floor 1/4, so it is also decoded and subtracted. Next, the magenta message which carries 1/8 GDoF is seen with power level 1/4 and noise floor 1/8, so it is also decoded and subtracted successfully. Finally, only the dotted white message, which carries 1/8 GDoF is seen with power levels 1/8 and noise floor 0, so it is decoded as well.

Now, let us explain the scheme for arbitrary $\mathcal{N}^{[n,1]}$. As in the example, the achievable scheme is also hierarchical where we will start with a common message for all users in $\mathcal{N}^{[n,\nu]}$ and then progressively include additional messages for its subnetworks while maintaining the successive decodability of all messages. For ease of reference, let us call the common message for the users in a $\mathcal{N}^{[n,\nu]}$ network a level $n$ message.

The same level-$n$ message, is sent from every transmitter with strength $\gamma = 0$, so that it is received at every receiver with strength $\gamma + \alpha_{ii} = 1$. It carries 0.5 GDoF. The power levels of all other messages are set to $-1/2$ or less so that all other messages are received with strength no more than $-1/2 + 1 = 1/2$. Since the noise floor from other messages is at 1/2, the common message is received at strength level 1, and it carries only 1/2 GDoF, it is decodable at every receiver, After decoding it, every receiver subtracts out the codeword due to the level $n$ message.

There are two different level $n-1$ sub-networks. Within each of these two networks a different level $n-1$ message is sent with power level $-1/2$, so it is received at power level 1/2 at each receiver within the sub-network. Signals from one sub-network are not heard by the other subnetwork because the channel strength between the users in different sub-networks is 1/2 and the transmit power of the level $n-1$ message is $-1/2$. All lower level messages are sent with power levels less than $-3/4$, so the noise floor due to lower level messages at each receiver is at power level 1/4. Thus, the level $n-1$ message is able to achieve $1/2-1/4 = 1/4$ GDoF. Since there are 2 such messages corresponding to the 2 subnetworks, the total sum GDoF value contributed by level $n-1$ messages is $1/4 + 1/4 = 1/2$. After decoding each receiver subtracts out the codeword due to level $n-1$ message from its own subnetwork.

Next, there are 4 level $n-2$ sub-networks. A different common message is sent within each subnetwork with power level $-1 + (1/2)^2 = -3/4$, so it is received at power level $1/4$, while all lower level messages are sent with power no more than $-1 + (1/2)^3 = -7/8$, so the noise floor due to lower level messages is $1 - 7/8 = 1/8$. The sub-networks do not interfere with each other because the cross-subnetwork channel strengths are $1 - 1/2^2 = 3/4$ so the received signals from other subnetworks are below the noise floor. Thus, each of the 4 of the $(n-2)$-level messages is able to achieve $1/4 - 1/8 = 1/8$ GDoF for a total of $4 \times 1/8 = 1/2$. The decoded messages are subtracted.

This pattern continues, so that for each $i \in [0 : n]$, there are $2^i$ different level-$(n - i)$ subnetworks. Within each of these subnetworks, a different common message is sent with power level $-1 + (1/2)^i$ so it is received at power level $(1/2)^i$ while all lower level messages are sent with power level no more than $-1+(1/2)^{i+1}$ so that the noise floor due to lower level messages is $(1/2)^{i+1}$ at each receiver. Thus each of the $2^i$ subnetworks achieves $1/2^i - 1/2^{i+1} = 1/2^{i+1}$ GDoF for a total of $2^i/2^{i+1} = 1/2$ sum GDoF.

Adding these values across all $n$ levels we achieve a total of $n/2$ sum-GDoF. In fact, it is possible to do a little bit better. At level 0, there are $2^n$ subnetworks comprised of individual users, and since there are no more lower level messages, the noise floor is 0, so it is possible to achieve $1/2^n - 0 = 1/2^n$ GDoF per user for a total of 1 GDoF instead of just 1/2 GDoF for level 0 messages. Thus, the total sum-GDoF value achieved is $1 + n/2 = 1 + \frac{1}{2}\log_2(K)$ sum-GDoF. Now note that for the $\mathcal{N}^{[n,1]}$ network, the sum-GDoF value in the BC setting is $\mathcal{D}_{\Sigma,\text{BC}} \geq 1+\frac{1}{2}\log_2(K)$, while the sum-GDoF value achieved by TIN is $\mathcal{D}_{\Sigma,\text{TINA}} \leq 2$. Therefore, we have

$$\frac{\mathcal{D}_{\Sigma,\text{BC}}}{\mathcal{D}_{\Sigma,\text{TINA}}} \geq \frac{1 + \frac{1}{2}\log_2(K)}{2} = \Theta(\log_2(K)), \tag{2.89}$$

which concludes the proof of the lower bound.

As a final remark, the sum-GDoF $1 + \frac{n}{2} = 1 + \frac{1}{2}\log_2(K)$ is optimal for the BC obtained by allowing transmitter cooperation in $\mathcal{N}^{[n,1]}$. Applying Lemma A.6 with cycle $\pi = (1 \to 2 \to \cdots \to K \Lsh)$, we have the sum-GDoF in the BC bounded above by

$$\begin{aligned}
\mathcal{D}^{[n,1]}_{\Sigma,\mathrm{BC}}([K]) &\leq \Delta_\pi + \alpha^{[n,1]}_{1K} && (2.90)\\
&= \sum_{k=1}^{K-1} \delta^{[n,1]}_{k,k+1} + \delta^{[n,1]}_{K1} + \alpha^{[n,1]}_{1K} && (2.91)\\
&= \sum_{\ell=1}^{n} \frac{1}{2^{n-\ell+1}} 2^{n-\ell} + \frac{1}{2} + \frac{1}{2} && (2.92)\\
&= \frac{1}{2}\log_2 K + 1, && (2.93)
\end{aligned}$$

which matches the achieved sum-GDoF.

## 2.8 Summary

The main message of this chapter is to underscore the importance of extremal analysis in order to advance our understanding of fundamental limits of large wireless networks beyond symmetric settings, where the curse of dimensionality stands in the way. It is exemplified by the results of this chapter, which identify the extremal gain of transmitter cooperation in weak interference regimes. Extremal analysis used in conjunction with the GDoF metric under finite precision CSIT thus appears to be a promising research avenue to bridge the gap between theory and practice.

# Chapter 3

# Robust Optimality of Secure TIN

## 3.1 Paths to Characterize GDoF of Large Networks

Most networks for which robust Generalized Degrees of Freedom (GDoF) have been found are either small, e.g., limited to two or three users [26, 31, 33, 36, 63], or limited to symmetric parameter values which cover a negligible fraction of the overall parameter space [25]. With the availability of new bounds based on the Aligned Image principle, the natural next goal is to apply them to larger networks under larger parameter regimes. The obstacle is the inherent curse of dimensionality. To avoid this obstacle, two paths have emerged. One path focuses on parameter regimes of interest and leads to extremal network theory, where instead of exact GDoF characterizations, the extremal GDoF values are studied over the chosen parameter regimes. See Chapter 2 and [64–66] for the applications of the extremal network theory.

The other path puts its focus on certain schemes of interest, such as those that treat interference as noise (TIN) [34, 35, 62, 67, 68], and seeks to identify large parameter regimes where the chosen schemes are GDoF optimal. As the current frontiers of research, these paths exemplify the progress thus far. For example, GDoF studies of TIN combine the appeal of information theoretic optimality with the advantage of practical robustness, and the sharpness of exact GDoF characterizations with the surprising breadth of parameter regimes where TIN schemes are GDoF-optimal. They target the regimes that are the most relevant in practice, considering that well-designed networks tend to operate under weak interference, and indeed they have inspired new interference management algorithms [60, 61, 69, 70] based on information theoretic principles.

### 3.1.1 Parameter Regimes Identified for GDoF Optimality

The parameter regimes where TIN and similar robust schemes are known to be GDoF-optimal are the largest regimes where exact GDoF characterizations have been found. Progress along this path has corresponded to the discoveries of larger and larger regimes where such schemes are GDoF-optimal. Interest in the optimality of TIN for interference networks started with the discovery of a relatively small parameter regime where the exact capacity of the two user interference channel is achieved by TIN [57–59]. A larger regime is found in [7] where TIN is GDoF optimal for the two user interference channel. For the $K$ user interference channel under perfect channel state information at transmitters (CSIT), a parameter regime, denoted simply as the TIN regime, was identified by Geng et al. in [34] where TIN with power control is GDoF-optimal. A still larger regime, called the CTIN regime, was discovered by Yi and Caire in [35] which had the curious property that the TIN region is convex without the need for time-sharing. By restricting CSIT to finite precision, TIN was shown to be GDoF-optimal throughout the CTIN regime by Chan et al. in [62].

An even larger parameter regime was discovered in [36] where a simple layered superposition (SLS) strategy is GDoF optimal for the multiple-input single-output (MISO) broadcast channel (BC) obtained by allowing full cooperation among the transmitters of a $K$ user interference channel, under finite precision CSIT. It is notable that the SLS regime is defined for arbitrary $K$, but the optimality was established in [36] only for $K \leq 3$. Comparisons between broadcast and interference settings for arbitrary $K$ were conducted via extremal analysis in Chapter 2, where we showed that the extremal sum-GDoF gain of broadcast over interference, i.e., the extremal gain of transmitter cooperation under finite precision CSIT, is equal to 1.5 in the TIN regime, $2 - 1/K$ in the CTIN regime, and of the order of $\log(K)$ in the SLS regime. For cellular networks, modeled as interfering multiple-access channels in the uplink and interfering broadcast channels in the downlink, non-trivial parameter regimes where TIN-like schemes are GDoF-optimal, were discovered by Joudeh et al. in [64, 67, 68].

## 3.2 Problem Statement and Contributions

### 3.2.1 Discovering Larger Regimes by Adding Constraints

In this chapter, we aim at discovering even larger parameter regimes where TIN-like schemes are GDoF optimal. The motivating intuition is that just as including robustness constraints (finite precision CSIT) into the problem formulation led to the discovery of a larger parameter regime (CTIN) where TIN is GDoF optimal, perhaps further including secrecy constraints into the problem formulation may lead to the discovery of even larger parameter regimes where the corresponding secure versions of TIN would be GDoF optimal. Finding these larger parameter regimes is the main goal of this this chapter.

It is worth mentioning that the combination of robustness and secrecy constraints is quite natural, because robustness is very important for communication under *secrecy* constraints. While there is an abundance of literature on information theoretic secrecy [42, 71–94], robustness issues, especially for larger networks, remain relatively unexplored. Fragile schemes are susceptible to catastrophic failures due to small deviations from their idealized assumptions.

In the absence of secrecy constraints, a failed communication attempt may prompt a more conservative re-transmission. Failure in a secure communication setting on the other hand, may also lead to a loss of secrecy which is irreversible. Therefore, it is especially important to avoid the idealized assumption of perfect CSIT when studying secure communication [95–98].

### 3.2.2 Regimes Where Secure TIN is Optimal

The contributions of this chapter are threefold. First, our main result, confirming the intuition that motivated the work in this chapter, is the discovery of a new parameter regime, labeled the Secure-TIN regime (STIN in short), for a $K$ user interference channel where a secure version of TIN (including jamming) is GDoF optimal under finite precision CSIT. The STIN regime is the largest of all such parameter regimes previously identified — it includes the SLS regime, which includes the CTIN regime, which includes the TIN regime, and all these inclusions are strict.

For our second set of results we employ extremal analysis to compare the secure robust GDoF of the $K$ user interference channel with the corresponding $K$ user MISO broadcast channel. We show that the extremal GDoF gain from transmitter cooperation in the STIN regime is unbounded, but when restricted to the SLS parameter regime, the extremal gain is equal to one. Remarkably, this settles the GDoF of the $K$ user MISO BC in the SLS regime under both robustness and secrecy constraints, for *arbitrary* $K$. Recall that without secrecy constraints, the GDoF of the MISO BC have been characterized in the SLS regime only for $K \leq 3$ [36]. As such the SLS regime under secrecy constraints now represents the largest regime for the BC setting where a precise characterization of robust GDoF is now available for arbitrary $K$. We also find the secure robust GDoF of the MISO BC for *all* parameter regimes when $K = 2$. Table 3.1 summarizes the available results, from both prior works and this chapter, regarding the GDoF region and extremal gain of BC and IC in different

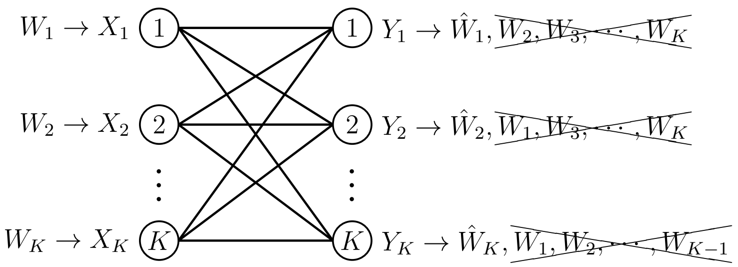

$W_1 \to X_1$
1
$W_2 \to X_2$
2
$W_K \to X_K$
K
1
$Y_1 \to \hat{W}_1,$ ~~$W_2, W_3, \cdots, W_K$~~
2
$Y_2 \to \hat{W}_2,$ ~~$W_1, W_3, \cdots, W_K$~~
K
$Y_K \to \hat{W}_K,$ ~~$W_1, W_2, \cdots, W_{K-1}$~~

Figure 3.1: Secure $K$ user interference network.

channel regimes under finite precision CSIT, with and without secrecy constraints.

The third set of results extends the study of TIN optimality to settings where either helpers (transmitters) or eavesdroppers (receivers) are added to the interference network. This may enlarge or reduce the secure GDoF (SGDoF) region of the original interference channel [91, 92, 99, 100]. Using insights from the first set of results, we identify various parameter regimes where adding helpers or eavesdroppers does or does not have an impact on the GDoF.

## 3.3 System Model

### 3.3.1 Secure $K$ User Interference Network

We consider a $K$ user Gaussian interference channel (IC) depicted in Figure 3.1. For $i \in [K]$, Transmitter $i$ encodes message $W_i \in \{1, 2, \cdots, \lceil 2^{nR_i} \rceil\}$, independently of the other transmitters, into an $n$-length codeword $X_i^n = \{X_i(t) : t \in [n]\}$ with a stochastic encoder subject to a unit average power constraint $\frac{1}{n}\sum_{t\in[n]} |X_i(t)|^2 \leq 1$. Then $X_i^n$ is sent by Transmitter $i$ with its single antenna as the channel input. For $k \in [K]$, Receiver (User) $k$ desires message $W_k$, and within the robust GDoF framework, its received signal at the $t$-th channel use is

Table 3.1: The GDoF region and extremal gain of BC/IC in different channel regimes under finite precision CSIT (with and without secrecy).

| Settings | | Without Secrecy | | With Secrecy | |
|---|---|---|---|---|---|
| Regime | User | IC | BC | IC | BC |
| TIN | $K \leq 3$ | TIN [34] | SLS [36] | Polyhedral TIN [42] | Polyhedral TIN<br>(Thm. 3.1, 3.2 & 3.3) |
| | $K \geq 4$ | | GDoF region unknown<br>Extremal Gain $= 1.5^{\dagger}$ [62] | | |
| CTIN | $K \leq 3$ | TIN [62] | SLS [36] | | |
| | $K \geq 4$ | | GDoF region unknown<br>Extremal Gain $= 2 - \frac{1}{K}^{\dagger}$ [62] | | |
| SLS | $K = 2$ | Han-Kobayashi*[7] | SLS [36] | | |
| | $K = 3$ | GDoF region unknown | | | |
| | $K \geq 4$ | | GDoF region unknown<br>Extremal Gain $= \Theta(\log K)^{\dagger}$ [62] | | |
| STIN | $K = 2$ | Han-Kobayashi*[7] | SLS [36] | | |
| | $K \geq 3$ | GDoF region unknown | | Polyhedral TIN (Thm. 3.1) | GDoF region unknown<br>Extremal Gain $= \infty^{\ddagger}$ (Thm. 3.2) |

[*] This is referred to as the GDoF region achieved by the Han-Kobayashi scheme.

[†] Extremal gain is defined as the supremum of the ratio between the sum GDoFs with transmitter cooperation (BC) and the one achievable by TIN, over all channels in the regime of interest.

[‡] Extremal gain is defined by the ratio between the weighted sum GDoFs with the BC and the IC setting, and then taking its supremum over all possible weights and all channels in the regime of interest. See Definition 3.6 in Section 3.4.2 for more details.

described as

$$Y_k(t) = \sum\nolimits_{i=1}^{K} \bar{P}^{\alpha_{ki}} G_{ki}(t) X_i(t) + Z_k(t) \qquad\qquad \forall k \in [K]. \tag{3.1}$$

All $X_i(t), Y_k(t), Z_k(t), G_{ki}(t) \in \mathbb{C}$. Subscript $i$ refers to Transmitter $i$, and subscript $k$ to Receiver $k$. $Z_k(t) \sim \mathcal{CN}(0,1)$ is the additive white Gaussian noise. $\bar{P} = \sqrt{P}$, and $P > 1$ is a nominal variable (referred to as *power*) whose asymptotic limit (i.e., $P \to \infty$) is used to define the GDoF metric. The channel strength parameters $\alpha_{ki} \geq 0$ represent the strength of the link from Transmitter $i$ to Receiver $k$. $G_{ki}(t) \in \mathcal{G}$ are the channel coefficient values, whose statistical assumptions are described in Section 3.3.3.

**Remark 3.1.** *The channel strength parameters $\alpha_{ki}$ correspond to the approximate capacity values of the point-to-point channels in a given setting to which the GDoF framework is applied. The capacity of the link from Transmitter i to Receiver k in the GDoF model is* $\log(1 + P^{\alpha_{ki}}) \approx \alpha_{ki} \log(P)$ *for large $P$. The GDoF framework scales the original capacity of each link, $\alpha_{ki}$, by the same nominal factor* $\log(P)$*. This intuitively scales the network capacity approximately by the same factor* $\log(P)$ *as well. Normalizing all rates by* $\log(P)$*, as in the definition of GDoF (See (3.3)), yields an approximation to the capacity of the original network setting.*

A secure rate tuple $(R_1, R_2, ..., R_K)$ is achievable if, for any $\epsilon > 0$, there exist $n$-length codes such that (i) $|W_j| \geq 2^{nR_j}$; (ii) the decoding error probabilities at all users are less than $\epsilon$; and (iii) the following[1] secrecy constraints are satisfied,

$$I_{\mathcal{G}}(W_{-i}^{K}; Y_i^n) \leq n\epsilon \qquad\qquad \forall i \in [K], \tag{3.2}$$

where $W_{-i}^{K} \triangleq \{W_k : \ \forall k \in [K] \backslash \{i\}\}$, $Y_i^n = \{Y_i(t) : \ t \in [n]\}$, and $\mathcal{G}$ is the set of channel coefficients defined in Section 3.3.3. The secure channel capacity region $\mathcal{C}$ is the closure of the

[1] Notably, all the GDoF results in this chapter hold even if the secrecy constraints are weakened as noted in Remark 3.4.

set of all achievable secure rate tuples. With channel strength parameter values collectively labeled as $[\boldsymbol{\alpha}] \triangleq \{\alpha_{ij} : i, j \in [K]\}$, the secure GDoF region and the sum-GDoF of the IC under finite precision CSIT, are defined as

$$SGDoF_{IC}^{f.p.}([\boldsymbol{\alpha}]) \triangleq \left\{(d_1, d_2, ..., d_K) \middle| \, d_i = \lim_{P\to\infty} \frac{R_i}{\log P}, \forall i \in [K], (R_1, R_2, ..., R_K) \in \mathcal{C} \right\} \tag{3.3}$$

$$SGDoF_{IC,\,\Sigma}^{f.p.}([\boldsymbol{\alpha}]) \triangleq \max_{(d_1, d_2, \cdots, d_K) \in SGDoF_{IC}^{f.p.}([\boldsymbol{\alpha}])} \sum_{i=1}^{K} d_i \tag{3.4}$$

The superscript '*f.p.*' refers to finite precision CSIT, and may be replaced with '*p*' to refer to prefect CSIT. The subscript '*IC*' may be replaced with '*BC*' for the broadcast channel as defined next.

### 3.3.2 Secure $K$ User Broadcast Network

The secure $K$ user broadcast channel (BC) with $K$ transmit antennas is obtained from the secure $K$ user IC by allowing all the $K$ transmitters to *jointly* encode all the messages $W_1, W_2, \cdots, W_K$ with a stochastic encoder. The achievable secure rate tuple, secure capacity region, and the secure GDoF region of BC are the identical to those defined in Section 3.3.1.

### 3.3.3 Finite precision CSIT

In the setting of finite precision CSIT, we assume that the channel coefficients $G_{ki}(t) = G_{R,ki}(t) + jG_{I,ki}(t)$ are known to the transmitter only up to finite precision. Specifically, the transmitter knows only the joint probability density function of the channel coefficients $\mathcal{G} \triangleq \{G_{R,ki}(t), G_{I,ki}(t) : \ t \in [n], i, k \in [K]\}$. The joint density of $\mathcal{G}$ is assumed to follow the "bounded density assumption" [20], i.e., there exists a positive finite constant $f_{max}$, such that, for any finite disjoint subsets of $\mathcal{G}$, say $\mathcal{G}_1$ and $\mathcal{G}_2$, the density of $\mathcal{G}_1$ conditioned on $\mathcal{G}_2$ satisfies $f_{\mathcal{G}_1|\mathcal{G}_2}(\boldsymbol{g}_1|\boldsymbol{g}_2) \leq f_{max}^{|\mathcal{G}_1|}$, where $\boldsymbol{g}_i$ is a realization of $\mathcal{G}_i$, $i = 1, 2$. This assumption introduces the elements in $\mathcal{G}$ into the model as random perturbation factors, with their realizations known perfectly to the receivers but not to the transmitters. It thus limits the CSIT to finite precision. To avoid degenerate scenarios, the magnitudes of channel coefficient values are also bounded away from zero and infinity, i.e., there exists a finite constant $\Delta > 1$ such that $1/\Delta \leq |G_{ki}(t)| \leq \Delta$ for all channel coefficients.

### 3.3.4 Definitions

**Definition 3.1** (Polyhedral TIN Region [34])**.** *The polyhedral TIN region, denoted as $\texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$, is a set of tuples $(d_1, d_2, \cdots, d_K)$ satisfying*

$$0 \leq d_i \leq \alpha_{ii} \qquad \forall i \in [K], \tag{3.5}$$

$$\sum\nolimits_{j\in\{\pi_m\}} d_j \leq \Delta_{\pi_m} \qquad \forall \pi_m \in \Pi_m, m \in [2:K], \tag{3.6}$$

*where $\pi_m$ is a permutation of some $m$ distinct elements taken from $[K]$, $\Pi_m$ collects all such permutations, and $\{\pi_m\}$ denotes the set of all elements in $\pi_m$. The term $\Delta_{\pi_m} \triangleq \sum_{j\in\{\pi_m\}} \alpha_{jj} - \alpha_{j\pi_m(j)}$, where $\pi_m(j)$ is the successor of $j$ in $\pi_m$. We abbreviate $\texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ as $\texttt{TIN}_{\mathcal{P}}$ if no ambiguity in the choice of channel strengths arises.*

Recall that in the absence of secrecy constraints, for a $K$ user IC with channel strengths $[\boldsymbol{\alpha}]$, the GDoF region achievable by TIN and power control (without time-sharing) is $\overline{\texttt{TIN}} \triangleq \bigcup_{S\subseteq[K]} \texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}_S])$, where $[\boldsymbol{\alpha}_S] = \left\{\alpha'_{ij} = \alpha_{ij}\mathbb{1}(i \text{ and } j \in S) : \ i, j \in [K]\right\}$, and $\mathbb{1}(x)$ is the indicator function which takes the value 1 if $x$ is true, and 0 otherwise [34]. In general $\overline{\texttt{TIN}}$ is not convex. On the other hand, when secrecy constraints are present, $\texttt{TIN}_{\mathcal{P}}$ is achievable and turns out to be the SGDoF region in the STIN regime, as explained in Section 3.4.1.

**Definition 3.2** (TIN Regime. Definition 3.1 of [62])**.** *Define the TIN regime as*

$$\mathcal{A}_{\text{TIN}} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \middle| \alpha_{ii} \geq \alpha_{il} + \alpha_{mi}, \forall i, l, m \in [K], i \notin \{l, m\} \right\}. \tag{3.7}$$

$\mathcal{A}_{\text{TIN}}$ was identified in [34] as a regime where TIN is GDoF optimal without secrecy constraints under perfect CSIT. The optimal GDoF region in this parameter regime is $\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$. As a starting point that subsequent results build upon in order to identify larger regimes where robust schemes are optimal under various assumptions, $\mathcal{A}_{\text{TIN}}$ serves as an important benchmark.

**Definition 3.3** (CTIN Regime. Definition 3.2 of [62])**.** *Define the CTIN regime as*

$$\mathcal{A}_{\text{CTIN}} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \middle| \begin{array}{r} \alpha_{ii} \geq \max\left(\alpha_{ij} + \alpha_{ji}, \alpha_{ik} + \alpha_{ji} - \alpha_{jk}\right), \\ \forall i, j, k \in [K], i \notin \{j, k\} \end{array} \right\}. \tag{3.8}$$

The CTIN regime is so-named due to the discovery by Yi and Caire in [35] that $\overline{\mathtt{TIN}}$ becomes convex when the channel is in this regime. $\mathcal{A}_{\text{CTIN}}$ was established in [62] as a regime where TIN is GDoF optimal without secrecy constraints under finite precision CSIT. The optimal GDoF region in this parameter regime is $\overline{\mathtt{TIN}}$. When secrecy constraints are imposed, $\overline{\mathtt{TIN}}$, which is equal to $\mathtt{TIN}_{\mathcal{P}}$ in $\mathcal{A}_{\text{CTIN}}$, remains the SGDoF region (Lemma 3.1 in Section 3.3.5). It is of interest to go beyond $\mathcal{A}_{\text{CTIN}}$ and explore the secure optimality of $\mathtt{TIN}_{\mathcal{P}}$.

**Definition 3.4** (SLS Regime. Definition 3.3 of [62])**.** *Define the SLS regime,*

$$\mathcal{A}_{\text{SLS}} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \middle| \begin{array}{r} \alpha_{ii} \geq \max\left(\alpha_{ik}, \alpha_{ki}, \alpha_{ik} + \alpha_{ji} - \alpha_{jk}\right), \\ \forall i, j, k \in [K], i \notin \{j, k\} \end{array} \right\}. \tag{3.9}$$

It was shown in [36] that when the channel is in the SLS regime, then a *simple layered superposition (SLS)* scheme is GDoF optimal for BC without secrecy constraints, provided

$K \leq 3$. Defined for arbitrary $K$, the regime will be shown in Section 3.4.2 to be sufficient for $\mathtt{TIN}_{\mathcal{P}}$ to be the optimal SGDoF region for BC.

### 3.3.5 Polyhedral TIN Region Under Secrecy Constraints

The polyhedral TIN region $\mathtt{TIN}_{\mathcal{P}}$ is known (Theorem 4.1 of [62]) to be GDoF optimal under finite precision CSIT in the CTIN regime, in the absence of secrecy constraints. Based on the known results it can be further deduced that $\mathtt{TIN}_{\mathcal{P}}$ remains GDoF optimal under finite precision CSIT in the CTIN regime if we also impose secrecy constraints. This is formally noted in the following lemma.

**Lemma 3.1.** *If a $K$ user IC is in the CTIN regime, then the secure GDoF region under finite precision CSIT is equal to the polyhedral TIN region $\boldsymbol{\mathit{TIN}}_{\mathcal{P}}$ , i.e.,*

$$[\boldsymbol{\alpha}] \in \mathcal{A}_{\text{CTIN}} \qquad \Longrightarrow \qquad \mathit{SGDoF}_{IC}^{f.p.}([\boldsymbol{\alpha}]) = \boldsymbol{\mathit{TIN}}_{\mathcal{P}}([\boldsymbol{\alpha}]). \tag{3.10}$$

*Proof.* Achievability of $\mathtt{TIN}_{\mathcal{P}}$ follows from Corollary 3.1 that appears below. The converse follows from Theorem 4.1 of [62], because imposing secrecy constraints cannot make the GDoF region any larger than the GDoF region without secrecy constraints. □

**Corollary 3.1.** *In a $K$ user Gaussian interference channel with secrecy constraints and finite precision CSIT, the polyhedral TIN region is achievable, i.e., $\boldsymbol{\mathit{TIN}}_{\mathcal{P}}([\boldsymbol{\alpha}]) \subset \mathit{SGDoF}_{IC}^{f.p.}([\boldsymbol{\alpha}])$.*

*Proof.* The corollary follows from Lemma 1 of [42] which shows that $\mathtt{TIN}_{\mathcal{P}}$ is robust to secrecy constraints, i.e., it remains achievable with secrecy constraints. While [42] assumes perfect CSIT, the conclusion extends to finite precision CSIT because the achievability of $\mathtt{TIN}_{\mathcal{P}}$ in [42] only needs the knowledge of the channel strength parameters $\alpha_{ki}$ at the transmitters, which is also available under the finite precision CSIT assumption. □

## 3.4 Results

Our results for the $K$ user IC are presented in Section 3.4.1, corresponding results for $K$ user MISO BC are presented in Section 3.4.2, and extensions to helpers and eavesdroppers are presented in Section 3.4.3.

### 3.4.1 Secure GDoF of the $K$ User Interference Channel Under Finite Precision CSIT

We start by defining a new parameter regime.

**Definition 3.5** (STIN Regime). *Define the STIN regime,*

$$\mathcal{A}_{\text{STIN}} = \left\{ [\alpha]_{K\times K} \in \mathbb{R}_+^{K\times K} \;\middle|\; \begin{array}{r} \alpha_{ii} \geq \max\left(\alpha_{ki}, \alpha_{ik} + \alpha_{ji} - \alpha_{jk}\right), \\ \forall i,j,k \in [K], i \notin \{j,k\} \end{array} \right\}. \tag{3.11}$$

What makes the new regime particularly interesting is that it is the largest of all "weak interference" regimes discussed previously for which GDoF have been characterized thus far.

**Lemma 3.2.** *The TIN, CTIN, SLS, and STIN regimes satisfy the following inclusion relationship,*

$$\mathcal{A}_{\text{TIN}} \subseteq \mathcal{A}_{\text{CTIN}} \subseteq \mathcal{A}_{\text{SLS}} \subseteq \mathcal{A}_{\text{STIN}} \tag{3.12}$$

*and in all cases the inclusion is strict in general.*

*Proof.* This is easily verified from the definitions. In particular, the relationship $\mathcal{A}_{\text{TIN}} \subseteq \mathcal{A}_{\text{CTIN}} \subseteq \mathcal{A}_{\text{SLS}}$ is already noted in [62]. The remaining condition $\mathcal{A}_{\text{SLS}} \subseteq \mathcal{A}_{\text{STIN}}$ follows because

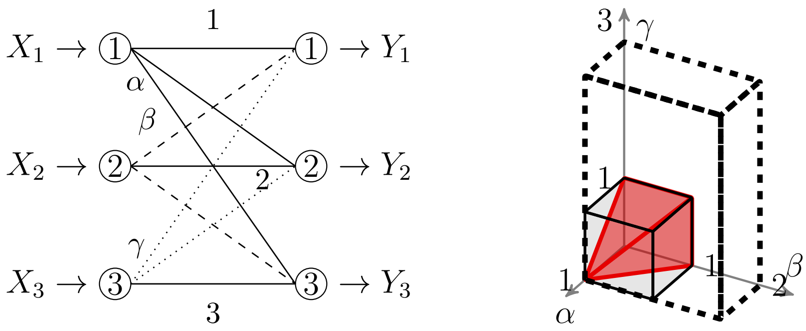


Figure 3.2: A $K = 3$ user IC, and the parameter regimes corresponding to CTIN (red polyhedron), SLS (gray-shaded cube), and STIN (dashed box).

the SLS regime includes an additional constraint, $\alpha_{ii} \geq \max_k \alpha_{ik}$, that is relaxed for the STIN regime. □

Figure 3.2 illustrates the progressive inclusion relationship between $\mathcal{A}_{\text{CTIN}}$, $\mathcal{A}_{\text{SLS}}$ and $\mathcal{A}_{\text{STIN}}$ for a $K = 3$ user interference network where the desired channel strengths are equal to 1, and the interfering links originating at transmitters $1, 2, 3$ have strengths $\alpha, \beta, \gamma$, respectively. Note that the STIN regime is significantly larger than the CTIN and SLS regimes. The significance of the STIN regime is established in the following theorem.

**Theorem 3.1.** *If an IC is in the STIN regime then the GDoF region under finite precision CSIT and secrecy constraints is equal to the polyhedral TIN region, which is achievable by TIN with cooperative jamming.*

$$[\boldsymbol{\alpha}] \in \mathcal{A}_{\text{STIN}} \qquad \implies \qquad SGDoF^{f.p.}_{IC}([\boldsymbol{\alpha}]) = \boldsymbol{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}]) \tag{3.13}$$

Achievability proof for Theorem 3.1 follows directly from Corollary 3.1. The converse is proved in Section 3.5.1, and relies on a combination of Aligned Images bounds and secrecy constraints. Theorem 3.1 formalizes our original intuition that because imposing secrecy constraints does not hurt the GDoF region achievable by TIN schemes, these constraints should work in conjunction with Aligned Images bounds to produce a stronger converse that allows a precise GDoF characterization for a broader regime of parameters. This new and broader regime of parameters is explicitly identified in Theorem 3.1 as the STIN regime.

**Remark 3.2.** *The STIN regime is not strictly necessary for robust TIN optimality. For example, consider a two-user GIC with* $\alpha_{11} = \alpha_{22} = 1, \alpha_{21} = 0$ *and* $\alpha_{12} = 2$*, which is not in the STIN regime, but TIN with cooperative jamming still achieves the entire GDoF region [29]. However, we expect that such* $[\boldsymbol{\alpha}]$ *constitute a set of measure zero, similar to the situation in [34]. On the other hand, there exist other schemes capable of achieving more than TIN when the channel is out of the STIN regime. To see this, consider a two-user symmetric GIC with* $\alpha_{ii} = 1$ *and* $\alpha_{ij} = \frac{4}{3}$*, where* $i, j \in [2]$ *and* $i \neq j$*. The polyhedral TIN region is* $\{(0,0)\}$ *by Definition 3.1, but the tuple* $(2/3, 0)$ *is actually achievable with the following scheme: let* $X_1 = \bar{P}^{-\frac{1}{3}} V_1$*, where* $V_1$ *is encoded from message* $W_1$ *of GDoF* $\frac{2}{3}$*, and* $X_2 = J_2$ *is a jamming signal of GDoF* $\frac{2}{3}$*. It can be found that* $W_1$ *is decodable at Receiver 1 by decoding and then removing* $J_2$ *first, while it remains secret from Receiver 2 as it is aligned with the jamming signal in power.*

### 3.4.2 Secure GDoF of the $K$ User MISO BC Under Finite Precision CSIT

Consider the secure, robust GDoF of the MISO BC in the STIN regime. $\mathtt{TIN}_{\mathcal{P}}$ is still *achievable* in the MISO BC setting, because transmitter cooperation cannot hurt, but as we will see in this section, it is no longer optimal. Remarkably, of the two bounds (3.5)-(3.6) that define the polyhedral TIN region $\mathtt{TIN}_{\mathcal{P}}$, the more complex bound, (3.6), still holds in the MISO BC setting, but the simpler bound, (3.5), i.e., $d_i \leq \alpha_{ii}$, is the one that fails. Replacing this bound with the optimal single-user bound for the MISO BC is also non-trivial, because of the presence of the $K-1$ eavesdroppers, makes this a non-degraded compound wiretap channel setting [101] for which little is known beyond Degrees of Freedom (DoF) for degraded special cases. The nature of achievable schemes also changes from TIN and jamming to include secret-sharing schemes (see Figure 3.5 as an example). Therefore, we will take an extremal network theory approach instead [62]. Let us define the extremal gain $\eta([\boldsymbol{\alpha}])$ of the BC over the IC.

**Definition 3.6.** *(Extremal Gain) Define extremal gain as*

$$\eta(\boldsymbol{\alpha}) = \sup_{\boldsymbol{\lambda}\in\mathbb{R}_+^K} \frac{\max_{(d_1,d_2,\cdots,d_K)\in SGDoF_{BC}^{f.p.}([\boldsymbol{\alpha}])} d(\boldsymbol{\lambda})}{\max_{(d_1,d_2,\cdots,d_K)\in SGDoF_{IC}^{f.p.}([\boldsymbol{\alpha}])} d(\boldsymbol{\lambda})} \tag{3.14}$$

*where* $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_K)$*, and* $d(\boldsymbol{\lambda}) = \sum_{i=1}^{K} \lambda_i d_i$.

**Theorem 3.2.** *The extremal gain in the STIN regime is*

$$\eta_{\text{STIN}} \triangleq \sup_{[\boldsymbol{\alpha}]\in\mathcal{A}_{\text{STIN}}} \eta([\boldsymbol{\alpha}]) = \begin{cases} 1 & \text{if } K = 2, \\ \infty & \text{if } K \geq 3 \end{cases} \tag{3.15}$$

The proof of Theorem 3.2 is presented in Section 3.5.2. The unbounded extremal gain in the STIN regime is mainly a reflection of the fact that the STIN regime is so much larger than the previously studied TIN, CTIN and SLS regimes where the extremal gain is bounded. Specifically we find a sequence of channels in the STIN regime, and the associated weights, such that the weighted sum GDoF of the IC setting goes to zero while that of the corresponding BC setting remains constant.

Focusing on the smaller SLS regime reveals a strong result.

**Theorem 3.3.** *The extremal gain in the SLS regime,* $\eta_{\text{SLS}} \triangleq \sup_{[\boldsymbol{\alpha}]\in\mathcal{A}_{\text{SLS}}} \eta([\boldsymbol{\alpha}]) = 1$.

An extremal gain of unity immediately yields the following corollary.

**Corollary 3.2.** *If a $K$ user MISO BC is in the SLS regime then the GDoF region under finite precision CSIT and secrecy constraints is equal to the polyhedral TIN region, which is*

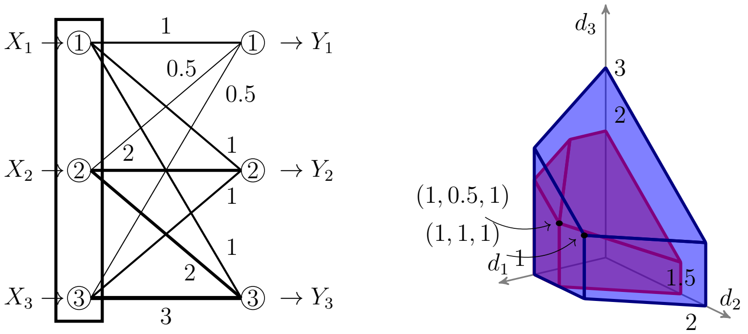


Figure 3.3: A 3-user MISO BC in the SLS regime, and its GDoF region under finite precision CSIT with (red) and without (blue) the secrecy constraints.

*achievable by TIN with cooperative jamming.*

$$[\boldsymbol{\alpha}] \in \mathcal{A}_{\text{SLS}} \qquad \Longrightarrow \qquad \mathit{SGDoF}^{f.p.}_{BC}([\boldsymbol{\alpha}]) = \boldsymbol{\mathit{TIN}}_{\mathcal{P}}([\boldsymbol{\alpha}]). \tag{3.16}$$

The proof of Theorem 3.3 is a straightforward extension of the proof of Theorem 3.1 and is presented in Section 3.5.3. According to Corollary 3.2 a sharp SGDoF characterization is obtained for the BC in the SLS regime with finite precision CSIT *for arbitrary $K$*. Recall that in the absence of secrecy constraints, the GDoF of the $K$ user BC are still open in the SLS regime for $K \geq 3$ [36]. Thus, Corollary 3.2 presents the largest known parameter regime where a robust (finite precision CSIT) GDoF characterization is available for the MISO BC with *arbitrarily large $K$*. Figure 3.3 shows a 3-user MISO BC and its GDoF regions with (red) and without (blue) secrecy constraints. Also note that in the SLS regime, *without secrecy constraints*, the extremal gain under finite precision CSIT, was shown to be of the order of $\log(K)$ in [62]. Theorem 3.3 shows that the GDoF benefits of transmitter cooperation disappear under secrecy constraints.

**Remark 3.3.** *Because any transmitter (transmit antenna) can be used to communicate to any receiver (receive antenna) in a BC, even if a given $K$ user IC is not in the SLS regime, its corresponding BC may be in the SLS regime after a permutation of its transmit antenna indices. The result of Corollary 3.2 would still determine the exact SGDoF region of such a*

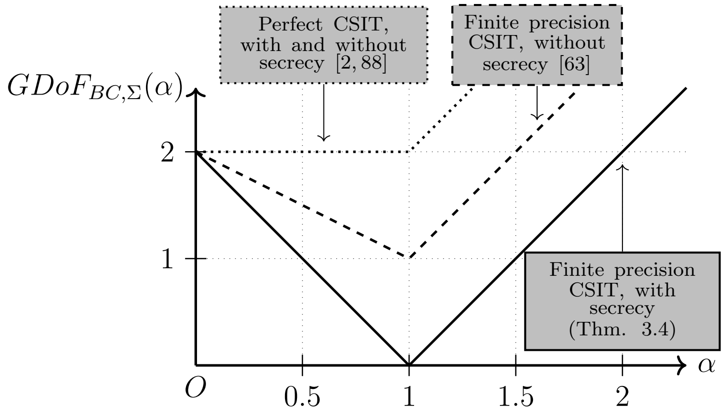


Figure 3.4: Sum GDoF $GDoF_{BC,\Sigma}(\alpha)$ for a two user symmetric MISO BC.

*BC, even though the SGDoF of the original IC may be unknown.*

Building on previous results, we fully (for all parameter regimes) settle the 2 user case.

**Theorem 3.4.** *For a BC setting with 2 users and $K$ transmit antennas ($K \geq 2$),*

$$SGDoF^{f.p.}_{BC,\Sigma}([\boldsymbol{\alpha}]) = \max_{k\in[K]}(\alpha_{1k} - \alpha_{2k})^+ + \max_{k\in[K]}(\alpha_{2k} - \alpha_{1k})^+. \tag{3.17}$$

The proof of Theorem 3.4 appears in Section 3.5.4.

Figure 3.4 considers a symmetric MISO BC with two users and two transmit antennas, where $\alpha_{11} = \alpha_{22} = 1$ and $\alpha_{12} = \alpha_{21} = \alpha$. Under perfect CSIT, the sum GDoF with or without secrecy constraints (the dotted line) is achievable via zero-forcing [2, 88]. Under finite precision CSIT, the sum GDoF without secrecy constraints (the dashed line) is achieved by rate-splitting, which allows public messages that are decodable by both users [63]. Under finite precision CSIT and secrecy constraints the sum GDoF, given by Theorem 3.4, is shown with a solid line. Evidently, both finite precision CSIT and the secrecy constraints incur a penalty on the sum-GDoF: the former by eliminating the gains of zero-forcing, and the latter by preventing the use of public messages.

### 3.4.3 The Impact of Helpers and Eavesdroppers

In this section we return to our original setting of the interference channel and explore the impact of helpers and eavesdroppers on the GDoF. Little is known about the impact of helpers and eavesdroppers in interference networks under finite precision CSIT and secrecy constraints. The problem is challenging in general, indeed as noted before, even the DoF of the single user setting with multiple eavesdroppers, also known as the compound wiretap channel [101], remains an open problem. Our goal here is rather modest, to extract insights about helpers and eavesdroppers from the new GDoF region characterization in Theorem 3.1. To see this connection, consider adding a user to an interference network, such that the newly added user achieves zero GDoF. In the absence of secrecy constraints, this new user is of no consequence and does not impact the GDoF region. However, under secrecy constraints, the transmitter of the new user can act as a helper, by sending jamming signals that secure other transmissions, potentially making the GDoF region larger, while the receiver of the new user acts as an eavesdropper, imposing additional secrecy constraints, and potentially making the GDoF region smaller. This is what we wish to explore in this section.

We start from a $K$ user IC, with the transmitters and their paired receivers labeled from 1 to $K$, and the channel parameters $[\boldsymbol{\alpha}] = \{\alpha_{ij} : \ i, j \in [K]\}$. Suppose $H$ independent transmitters (with no knowledge of the messages of the $K$ users, nor any common randomness) are added to the network, and labeled as $K+1, K+2, \cdots, K+H$. Newly-added Transmitter $h$ is connected to the $K$ receivers with links of channel strengths collected in $[\boldsymbol{\alpha}_H] \triangleq \{\alpha_{ih} : \ i \in [K], h \in [K+1 : K+H]\}$. Each newly added transmitter produces input $X_h^n$, which is subject to the unit power constraint, and is independent of all the other codewords. In the following we refer to such a network setting as a $K$ user IC with $H$ helpers, whose channel strengths are $[\boldsymbol{\alpha}] \cup [\boldsymbol{\alpha}_H]$.

On the other hand, instead of transmitters, suppose we add $E$ receivers to the network, which are respectively labeled $K+1, K+1, \cdots, K+E$. The channel strengths of the links connecting the newly added receivers and the transmitters are collected in $[\boldsymbol{\alpha}_E] = \{\alpha_{ej} : j \in [K], e \in [K+1 : K+E]\}$. The outputs of the newly added receivers, $Y_e^n$, are subject to secrecy constraints $I(Y_e^n; W^K) < n\epsilon$, where $W^K = \{W_1, \cdots, W_K\}$. We refer such a network setting as a $K$ user IC with $E$ eavesdroppers, whose channel strengths are $[\boldsymbol{\alpha}] \cup [\boldsymbol{\alpha}_E]$.

Our first result identifies a regime where adding helpers does not improve the GDoF.

**Corollary 3.3.** *For a $K$ user IC with $H$ helpers, if $[\boldsymbol{\alpha}]$ is in the STIN regime, and $[\boldsymbol{\alpha}] \cup [\boldsymbol{\alpha}_H]$ satisfies*

$$\alpha_{ii} + \alpha_{jh} \geq \alpha_{ji} + \alpha_{ih}, \qquad \forall i, j \in [K], h \in [K+1 : K+H], \tag{3.18}$$

*then the SGDoF region with helpers is equal to $\boldsymbol{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$, same as without helpers.*

The proof is presented in Section 3.5.5.

In contrast to these additional helpers that do not impact GDoF if the original network is in the STIN regime, it turns out that additional eavesdroppers are always harmful for certain regimes that are included in the STIN regime.

**Theorem 3.5.** *For a $K$ user IC with channel strength parameters $[\boldsymbol{\alpha}]$ that lie in the* interior *of the CTIN regime, adding a non-trivial eavesdropper (not all channel strengths to the eavesdropper are zero) makes the GDoF region strictly smaller.*

The proof of Theorem 3.5 is relegated to Section 3.5.6.

However, it is not true in general that additional eavesdroppers must always be detrimental to the GDoF region. The following theorem formalizes this observation.

**Theorem 3.6.** *For a $K$ user IC with $E$ eavesdroppers, if $[\boldsymbol{\alpha}]$ is in the* interior *of the STIN* *regime, and for all $i \in [K]$, there exists $j \in [K]$ with $j \neq i$, such that*

$$\alpha_{jj} < \alpha_{ij} + \alpha_{ji}, \tag{3.19}$$

*then there exists $\mathcal{A}_E \subset \mathbb{R}^{KE}$ with non-zero Lebesgue measure, such that, when $[\boldsymbol{\alpha}_E] \in \mathcal{A}_E$, the SGDoF region is equal to $\boldsymbol{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$, same as without eavesdroppers.*

The proof of Theorem 3.6 is relegated to Section 3.5.7.

**Remark 3.4.** *As a final observation, let us note that all our results in Section 3.4 hold even if the (strong) secrecy constraints in* (3.2) *are weakened to*

$$I_{\mathcal{G}}(W_j; Y_i^n) \leq n\epsilon \qquad \forall i, j \in [K], i \neq j. \tag{3.20}$$

*This is because weakening the secrecy constraints does not hurt achievability, and it is easily verified that all our converse proofs need only the weak secrecy constraints. Thus, somewhat surprisingly, for all cases considered in this chapter, weakening the secrecy constraints does not produce a larger SGDoF region.*

## 3.5 Proof

### 3.5.1 Proof of Converse of Theorem 3.1

The bounds in (3.5) are trivial single user capacity bounds. For the bounds in (3.6), the proof is mainly based on Aligned Images bounds [32]. Proceeding as usual for the application of Aligned Images bounds, we define a deterministic model for (3.1) as follows:

$$\bar{Y}_k(t) = \sum\nolimits_{i=1}^{K} \left\lceil \bar{P}^{\alpha'_{ki}} G_{ki} \bar{X}_i(t) \right\rceil \qquad \forall k \in [K], \tag{3.21}$$

where $\alpha'_{ki} \triangleq \alpha_{ki} - \max_{m\in[K]} \alpha_{mi} = \alpha_{ki} - \alpha_{ii}$, because according to Definition 3.5, in the STIN regime we have $\alpha_{ii} = \max_{m\in[K]} \alpha_{mi}$. The notation $\lceil z \rceil = \lceil x \rceil + j\lceil y \rceil$ for a complex number $z = x + jy$. The channel input $\bar{X}_i(t) = \lceil X_i(t) \rceil \mod \lceil \bar{P}^{\alpha_{ii}} \rceil = \bar{X}_{R,i}(t) + j\bar{X}_{I,i}(t)$, and

$$\bar{X}_{R,i}(t), \bar{X}_{I,i}(t) \in \left\{0, 1, \cdots, \lceil \bar{P}^{\alpha_{ii}} \rceil \right\}. \tag{3.22}$$

Next, we will prove that, with finite precision CSIT and the secrecy constraints, the GDoF region of the deterministic model (3.21) constitutes an outer bound of the original BC (3.1). To this end, we need the following lemma.

**Lemma 3.3.** *For all $k \in [K]$,*

$$I_{\mathcal{G}}(W_k; Y_k^n) \leq I_{\mathcal{G}}(W_k; \bar{Y}_k^n) + no(\log P), \tag{3.23}$$

$$I_{\mathcal{G}}(W_{-k}^K; \bar{Y}_k^n) \leq I_{\mathcal{G}}(W_{-k}^K; Y_k^n) + no(\log P), \tag{3.24}$$

*where $W_{-k}^K \triangleq \{W_i : \forall i \in [K]\backslash\{k\}\}$.*

The proof of Lemma 3.3 is relegated to Appendix B.1. Let $(i_1, i_2, \cdots, i_m) \in \Pi_m$ with $2 \leq m \leq K$. (See Definition 3.1 for the definition of $\Pi_m$.) For all $\epsilon > 0$ and all $j \in [m]$ with the modulo-$m$ arithmetic implicitly used (i.e., $i_0 = i_m$), we have

$$nR_{i_j} \leq I_{\mathcal{G}}(W_{i_j}; \bar{Y}_{i_j}^n) + no(\log P) \tag{3.25}$$

$$\leq I_{\mathcal{G}}(W_{i_j}; \bar{Y}_{i_j}^n) - I_{\mathcal{G}}(W_{i_{j+1}}; \bar{Y}_{i_j}^n) + no(\log P) \tag{3.26}$$

$$\leq H_{\mathcal{G}}(\bar{Y}_{i_j}^n \mid W_{i_{j+1}}) - H_{\mathcal{G}}(\bar{Y}_{i_j}^n \mid W_{i_j}) + no(\log P). \tag{3.27}$$

We apply Fano's inequality and (3.23) to get (3.25). Then to obtain (3.26), we apply $I_{\mathcal{G}}(W_{i_{j+1}}; \bar{Y}_{i_j}^n) \leq no(\log P)$, which is deduced from (3.24) and the secrecy constraints. Summing the rate $R_{i_j}$ over all $j \in [m]$, one gets (with $no(\log P)$ suppressed)

$$n\sum_{j=1}^{m} R_{i_j} \leq \sum\nolimits_{j=1}^{m} H_{\mathcal{G}}(\bar{Y}_{i_j}^n \mid W_{i_{j+1}}) - H_{\mathcal{G}}(\bar{Y}_{i_{j+1}}^n \mid W_{i_{j+1}}) \tag{3.28}$$

$$\leq \sum\nolimits_{j=1}^{m} \max_{k\in[K]} \left(\alpha_{i_j k} - \alpha_{i_{j+1}k}\right)^+ n\log P \tag{3.29}$$

$$= \sum\nolimits_{j=1}^{m} \left(\alpha_{i_j i_j} - \alpha_{i_{j+1} i_j}\right) n\log P. \tag{3.30}$$

In (3.29), we invoke the Aligned Images bound stated in the following lemma.

**Lemma 3.4** (Lemma 1 in [32]). *For $j \in [m]$, we have*

$$H_{\mathcal{G}}(\bar{Y}_{i_j}^n \mid W_{i_{j+1}}) - H_{\mathcal{G}}(\bar{Y}_{i_{j+1}}^n \mid W_{i_{j+1}}) \ \ \leq \max_{k\in[K]}(\alpha_{i_j k} - \alpha_{i_{j+1}k})^+ n\log P + no(\log P). \tag{3.31}$$

Since the channel $[\boldsymbol{\alpha}]$ is assumed in the STIN regime, we have $\alpha_{i_j i_j} - \alpha_{i_{j+1} i_j} \geq \alpha_{i_j k} - \alpha_{i_{j+1}k}$ and $\alpha_{i_j i_j} \geq \alpha_{i_{j+1} i_j}$ for all $k \in [K]$ and $j \in [m]$, and equality (3.30) holds. Finally, by reordering the negative terms in the summands of (3.30) and applying the definition of GDoF, we establish (3.6).

### 3.5.2 Proof of Theorem 3.2

The case $K = 2$ is not usually the focus of extremal analysis (which is motivated by large networks), but is included nevertheless for completeness. Its proof is relegated to Appendix B.2. For $K \geq 3$, it suffices to consider the 3 user network shown in Figure 3.5, whose channel strength parameters ($[\boldsymbol{\alpha}_0]$ for ease of reference) place it in the STIN regime. Note that this network is included in all networks with $K \geq 4$ in the STIN regime as a special case, by setting the strength of all the links not appearing therein as 0. Let $(\lambda_1, \lambda_2, \lambda_3) = (1, \varepsilon, \varepsilon)$. From Theorem 3.1, it follows that $\max_{(d_1,d_2,d_3)\in SGDoF_{IC}^{f.p.}([\boldsymbol{\alpha}_0])} d_1 + \varepsilon d_2 + \varepsilon d_3 = 3\varepsilon$. Although the SGDoF region of the BC setting remains open, it is possible to achieve $(d_1, d_2, d_3) = (0.5, 0, 0)$

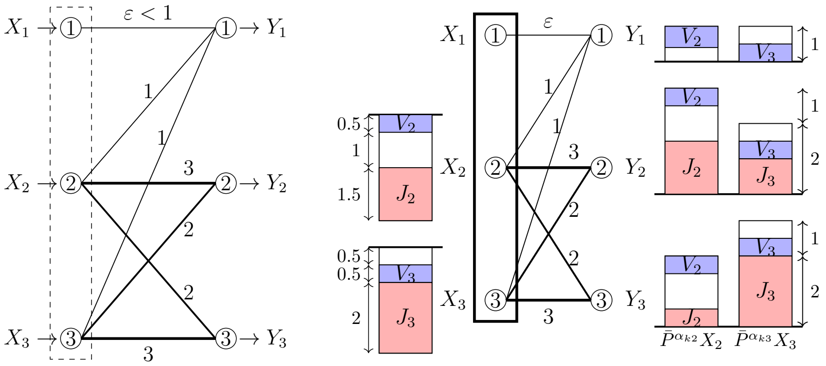


Figure 3.5: A network in the STIN regime and a scheme achieving secure GDoF tuple $(d_1, d_2, d_3) = (0.5, 0, 0)$. Codeword $V_2$ and $V_3$ are encoded from 'messages' $Z$ and $W_1 \oplus Z$, where $Z$ is i.i.d. uniform secret-sharing noise independent of $W_1$, and $\oplus$ indicates addition modulo the support size of $W_1$. Decoding either $Z$ (at User 2) or $W_1 \oplus Z$ (at User 3) individually reveals nothing about $W_1$, but decoding both (at User 1) reveals $W_1$ fully.

by the scheme depicted in Figure 3.5, making $\max_{(d_1,d_2,d_3)\in SGDoF_{BC}^{f.p.}([\boldsymbol{\alpha}_0])} d_1 + \varepsilon d_2 + \varepsilon d_3 \geq 0.5$. The scheme in Figure 3.5 uses secret-sharing ideas similar to [101] can be alternatively obtained by starting from the secure Polyhedral TIN scheme that achieves $(d_2, d_3) = (1.5, 0.5)$ for Users 2 and 3 in the absence of User 1, reducing $d_2$ to 0.5 (by reducing the size of the codebook), and then adding User 1 while replacing $W_2$ with $Z$, $W_3$ with $W_1 \oplus Z$ for uniform noise $Z$ that is independent of $W_1$ and has the same number of bits as $W_1$ (the addition is bit-wise in $\mathbb{F}_2$). Thus, Users 2 or 3 learn nothing about $W_1$, while User 1 is able to decode both $Z$ and $W_1 \oplus Z$, to recover $W_1$. Hence we have a lower bound for $\eta_{\text{STIN}}$,

$$\eta_{\text{STIN}} \geq \frac{\max_{SGDoF_{BC}^{f.p.}([\boldsymbol{\alpha}_0])} d_1 + \varepsilon d_2 + \varepsilon d_3}{\max_{SGDoF_{IC}^{f.p.}([\boldsymbol{\alpha}_0])} d_1 + \varepsilon d_2 + \varepsilon d_3} \geq \frac{1}{6\varepsilon}. \tag{3.32}$$

Since $\varepsilon$ can be made arbitrarily small, the lower bound approaches $\infty$ when $\varepsilon \to 0^+$.

### 3.5.3 Proof of Theorem 3.3

Since the SLS regime is contained in the STIN regime according to Lemma 3.2, and transmitter cooperation cannot hurt, Theorem 3.1 implies the achievability of $\mathtt{TIN}_{\mathcal{P}}$ in the BC setting. For the converse of Theorem 3.3 (equivalently, Corollary 3.2) we need to prove (3.5) and (3.6). Out of these, the proof of (3.6) for Theorem 3.1 provided in Section 3.5.1 also applies to the BC setting, because none of the Aligned Images bounds used in the proof assumes independence of inputs. The only remaining bound, (3.5), is trivial in the SLS regime, because the single user GDoF even without secrecy constraints and with perfect CSIT, are still bounded above as $d_i \leq \max_{k\in[K]} \alpha_{ik}$. This can be further bounded above by $\alpha_{ii}$ in the SLS regime because of the SLS condition (see Definition 3.4) that $\alpha_{ii} \geq \alpha_{ik}$ for all $i, k \in [K]$.

### 3.5.4 Proof of Theorem 3.4

The converse part of (3.17) can be obtained by applying Lemma 3.4 to (3.28) with $m = 2$. In the following, we provide the scheme to achieve (3.17). Let $i = \arg\max_{k\in[K]}(\alpha_{1k} - \alpha_{2k})^+$ and $j = \arg\max_{k\in[K]}(\alpha_{2k} - \alpha_{1k})^+$. If there are multiple indices reaching the maximum, then we choose an arbitrary one of them. We consider the following non-trivial cases:

1. $\alpha_{1i} - \alpha_{2i} > 0$ **and** $\alpha_{2j} - \alpha_{1j} > 0$

   In this case, $i \neq j$. By re-labeling Transmitter $i$ and $j$ respectively as 1 and 2, we find the achievability follows from Corollary 3.1.

2. **Either** $\alpha_{1i} - \alpha_{2i} \leq 0$ **or** $\alpha_{2j} - \alpha_{1j} \leq 0$**, but not both**

   Without loss of generality, we assume $\alpha_{2j} - \alpha_{1j} \leq 0$, which yields $SGDoF^{f.p.}_{BC,\Sigma}([\boldsymbol{\alpha}]) = \alpha_{1i} - \alpha_{2i}$. This can be achieved with the following scheme, which achieves the secure GDoF tuple $(\alpha_{1i} - \alpha_{2i}, 0)$. We prepare a Gaussian wiretap codebook of size $2^{n(R_s+R_c)}$, where

$$R_s = \log\left(1 + P^{\alpha_{1i}-\alpha_{2i}}\Delta^{-2}\right) - \log(1 + \Delta^2), \tag{3.33}$$

$$R_c = \log(1 + \Delta^2). \tag{3.34}$$

The wiretap codebook contains codewords $V(t)$, where $V(t) \sim \mathcal{CN}(0, P^{-\alpha_{2i}})$ for all $t \in [n]$. We encode $W_1$ at rate $R_s$ into $V(t)$, set $X_i(t) = V(t)$, and shut the rest transmitters off ($X_k(t) = 0, \forall k \neq i$). Such a scheme turns the channel into a wiretap one, where $W_1$ is desired by Receiver 1 and kept secret from Receiver 2. An achievable secure rate for $W_1$, denoted by $R_1$, can be inferred from [74] to be

$$R_1 = \inf_{\boldsymbol{g} \in \operatorname{supp}\{\mathcal{G}\}} \left\{ I(V; Y_1 | \mathcal{G} = \boldsymbol{g}) - I(V; Y_2 | V_2, \mathcal{G} = \boldsymbol{g}) \right\}, \tag{3.35}$$

where $\boldsymbol{g} = \{G_{lk} : \; l \in [2], k \in [K]\}$ is a realization of $\mathcal{G}$, and $\operatorname{supp}\{\mathcal{G}\}$ is the support of the random variables in $\mathcal{G}$. It can be further shown that $R_1 \geq R_s$, because

$$\begin{aligned} R_1 &= \inf_{\boldsymbol{g} \in \operatorname{supp}\{\mathcal{G}\}} \left\{ \log(1 + P^{\alpha_{1i} - \alpha_{2i}} |G_{1i}|^2) - \log(1 + |G_{2i}|^2) \right\} && (3.36) \\ &\geq \log\left(1 + P^{\alpha_{1i} - \alpha_{2i}} \Delta^{-2}\right) - \log(1 + \Delta^2) = R_s, && (3.37) \end{aligned}$$

where in (3.37) the inequality holds because it is assumed $1/\Delta \leq |G_{lk}(t)| \leq \Delta$. Since $R_s = (\alpha_{1i} - \alpha_{2i}) \log P + o(\log P)$, we have $d_1 = \alpha_{1i} - \alpha_{2i}$.

### 3.5.5 Proof of Corollary 3.3

The achievability part follows from Corollary 3.1 with $X_h(t) = 0$ for $h \in [K+1 : K+H]$. The converse part largely follows the proof for Theorem 3.1 provided in Section 3.5.1. The only difference lies in the number of the input codewords constituting the channel outputs, which is $K + H$ instead of $K$. This makes the index set over which the maximum in (3.29) is taken expand from $[K]$ to $[K+H]$. However, equality (3.30) still holds, since $[\boldsymbol{\alpha}]$ is in the SLS regime, and $[\boldsymbol{\alpha}_H]$ satisfies (3.18).

### 3.5.6 Proof of Theorem 3.5

We prove Theorem 3.5 by showing that not all single-user GDoF tuples $d_i = \alpha_{ii}$ and $d_j = 0$ for $j \neq i$, which are achievable without eavesdroppers, remain achievable after a non-trivial eavesdropper is added. This implies that the SGDoF region of the IC with eavesdroppers is strictly smaller than $\mathtt{TIN}_{\mathcal{P}}\left([\boldsymbol{\alpha}]\right)$.

We add a non-trivial eavesdropper of label $K+1$ to the IC, and assume $\alpha_{K+1,1} = \max_{j\in[K]} \alpha_{K+1,j} > 0$, without loss of generality. Note that the tuple $\boldsymbol{d}^* \triangleq (\alpha_{11}, 0, 0 \cdots, 0)$ is in $\mathtt{TIN}_{\mathcal{P}}\left([\boldsymbol{\alpha}]\right)$ and thus securely achievable before we add the eavesdropper, as is implied by Lemma 3.1. To facilitate the proof we define the following terms. First we define $\mathcal{E} \triangleq \{j \in [K] : \ \alpha_{K+1,j} = \alpha_{K+1,1}\}$, $\tilde{\delta} \triangleq \alpha_{K+1,1} - \max_{j\in[K]\setminus\mathcal{E}} \alpha_{K+1,j}$, and $\delta \triangleq \min\{\tilde{\delta}, \min_{j\in\mathcal{E}} \alpha_{1j}\}$. Note that $\delta > 0$, because $\tilde{\delta} > 0$, and $\alpha_{1j} > 0$ due to the assumption that $[\boldsymbol{\alpha}]$ lies in the *interior* of the CTIN regime. Next we cast $Y_1^n$ and $Y_{K+1}^n$ into the deterministic model $\bar{Y}_1^n$ and $\bar{Y}_{K+1}^n$ in a same way as is done in (3.21). Also, we define $\bar{Y}_\delta^n \triangleq \left\{\bar{Y}_\delta(t) : \ t \in [n]\right\}$, where

$$\bar{Y}_\delta(t) = \sum\nolimits_{j\in\mathcal{E}} \left\lceil G_{K+1,j}(t)(\bar{X}_j(t))^\delta \right\rceil, \tag{3.38}$$

and for a real value $X = O(\bar{P}^\alpha)$, and $0 \le \mu \le \alpha$, we define $(X)^\mu \triangleq \left\lceil X/\bar{P}^{\alpha-\mu} \right\rceil$.

Now we show that $d_1 < \alpha_{11}$ when Receiver $K+1$ is present. Starting from Fano's inequality,

$$\begin{aligned}
nR_1 &\le I_{\mathcal{G}}(Y_1^n; W_1) && (3.39)\\
&\le I_{\mathcal{G}}(\bar{Y}_1^n; W_1) = H_{\mathcal{G}}(\bar{Y}_1^n) - H_{\mathcal{G}}(\bar{Y}_1^n|W_1) && (3.40)\\
&\le H_{\mathcal{G}}(\bar{Y}_1^n) - H_{\mathcal{G}}(\bar{Y}_\delta^n|W_1) && (3.41)\\
&= H_{\mathcal{G}}(\bar{Y}_1^n) - H_{\mathcal{G}}(\bar{Y}_\delta^n) && (3.42)\\
&\le \max\left\{\max_{j\in\mathcal{E}} \left(\alpha_{1j} - \delta\right)^+, \max_{j\in[K]\setminus\mathcal{E}} \alpha_{1j}\right\} n \log P && (3.43)\\
&< \alpha_{11} n \log P. && (3.44)
\end{aligned}$$

We apply (3.23) of Lemma 3.3 to get (3.40). Inequality (3.41) holds due to Lemma 3.4 and the fact that $\delta \leq \alpha_{1j}$ for $j \in [K]\backslash\mathcal{E}$. Next we apply (3.24) of Lemma 3.3 (with detailed steps given later) to obtain $I_{\mathcal{G}}(\bar{Y}_\delta^n; W_1) \leq no(\log P)$, and therefore (3.42). Then we apply Lemma 3.4 to obtain (3.43). Finally, we apply the assumption of the CTIN regime to obtain the strict inequality (3.44). The strict inequality (3.44) implies $d_1 < \alpha_{11}$, which concludes the proof.

The remaining part is to show $I_{\mathcal{G}}(\bar{Y}_\delta^n; W_1) \leq no(\log P)$, which is done as below.

$$I_{\mathcal{G}}(\bar{Y}_\delta^n; W_1) \overset{(a)}{=} I_{\mathcal{G}}((\bar{Y}_{K+1}^n)^\delta; W_1) \overset{(b)}{\leq} I_{\mathcal{G}}(\bar{Y}_{K+1}^n; W^K) \overset{(c)}{\leq} no(\log P), \tag{3.45}$$

where $(\bar{Y}_{K+1}^n)^\delta = \left\{(\bar{Y}_{K+1}(t))^\delta : \ t \in [n]\right\}$. Equality (a) holds because for all $t \in [n]$, $\bar{Y}_\delta(t)$ and $(\bar{Y}_{K+1}(t))^\delta$ are within bounded distortion (See Lemma 4.6 and its following discussion for details). Inequality (b) follows because $(\bar{Y}_{K+1}^n)^\delta$ is a function of $\bar{Y}_{K+1}^n$, and $W^K$ includes $W_1$. Finally, we apply (3.24) of Lemma 3.3 to obtain (c).

### 3.5.7 Proof of Theorem 3.6

To show the existence of a set for $[\boldsymbol{\alpha}_E]$ which is not of measure zero, we identify an interval for each parameter in $[\boldsymbol{\alpha}_E]$ satisfying the following requirement: When the parameters are taken from the interval, we can find a TIN with cooperative jamming scheme for each $\boldsymbol{d} \in \texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$, such that none of the messages appear above the noise floors of the newly added eavesdroppers. Then the cube generated by the interval forms a set for $[\boldsymbol{\alpha}_E]$ of a non-zero Lebesgue measure.

To identify the interval, it suffices to show that all GDoF tuples in $\texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ can be achieved with the TIN scheme and some power control parameters bounded above by some negative value. By Theorem 3 of [39], a set of power control parameters $r_i$ achieving $\boldsymbol{d} =$

$(d_1, d_2, \cdots, d_K) \in \texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ can be found as

$$r_k(\boldsymbol{d}) = \min\left\{0, \min_{m\in[2:K]} \min_{\pi_m\in\Pi_m(k)} \left\{\Delta_{\pi_m} - \left(\alpha_{kk} - \alpha_{k\pi_m(k)}\right) - \sum\nolimits_{j\in\{\pi_m\}} d_j + d_k\right\}\right\} \tag{3.46}$$

for all $k \in [K]$, where $\Pi_m(k)$ is the collection of all permutations $\pi_m$ with $k$ included. (Refer to Definition 3.1 for the definition of $\pi_m, \{\pi_m\}, \pi_m(k)$ and $\Delta_{\pi_m}$.) Although $r_k(\boldsymbol{d})$ are not necessarily negative, yet one still can achieve the same GDoF tuple while reducing all $r_k(\boldsymbol{d})$ uniformly by $\xi(\boldsymbol{d})$ defined as

$$\begin{aligned}\xi(\boldsymbol{d}) &\triangleq \min_{k\in[K]} \alpha_{kk} + r_i(\boldsymbol{d}) - d_k \\ &= \min_{k\in[K]} \left\{\alpha_{kk} - d_k, \min_{m\in[2:K]} \min_{\pi_m\in\Pi_m(k)} \left\{\Delta_{\pi_m} + \alpha_{k\pi_m(k)} - \sum\nolimits_{j\in\{\pi_m\}} d_j\right\}\right\}. \end{aligned} \tag{3.47}$$

Note that $\xi(\boldsymbol{d})$ sets a upper bound in the power level: it takes at most $O(P^{-\xi(\boldsymbol{d})})$ for each transmitter to achieve $\boldsymbol{d}$.

It can be verified that $\xi(\boldsymbol{d}) > 0$ for all $\boldsymbol{d} \in \texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ as follows. First, the definition of $\texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ with $[\boldsymbol{\alpha}]$ being in the *interior* of the STIN regime implies $\Delta_{\pi_m} + \alpha_{k\pi_m(k)} - \sum_{j\in\{\pi_m\}} d_j \geq \alpha_{k\pi_m(k)} > 0$. Next we show that $d_k < \alpha_{kk}$. This is because

$$d_k^* \triangleq \max\nolimits_{\boldsymbol{d}\in\texttt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])} d_k \tag{3.48}$$

$$= \min\left\{\alpha_{kk}, \min_{m\in[2:K]} \min_{\pi_m\in\Pi_m(k)} \Delta_{\pi_m}\right\} \tag{3.49}$$

$$= \min\left\{\alpha_{kk}, \min_{\pi_2\in\Pi_2(k)} \Delta_{\pi_2}\right\} \tag{3.50}$$

$$= \min\left\{\alpha_{kk}, \min_{j\in[K], j\neq k} \alpha_{kk} + \alpha_{jj} - \alpha_{kj} - \alpha_{jk}\right\}, \tag{3.51}$$

where (3.50) holds because for every $\pi_m \in \Pi_m(k)$, from the assumption of the STIN regime, we can find a $\pi_2 \in \Pi_2(k)$ such that $\Delta_{\pi_m} \geq \Delta_{\pi_2}$. By (3.19), we have

$$d_k^* - \alpha_{kk} = \min\left\{0, \min_{j\in[K],j\neq k} \alpha_{kk} - \alpha_{kj} - \alpha_{jk}\right\} < 0. \tag{3.52}$$

Seeing that $\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ is compact, we have $\Xi \triangleq \min_{\boldsymbol{d}\in\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])} \xi(\boldsymbol{d}) > 0$. Note that to achieve all GDoF tuples in $\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$, it suffices for all the codewords $X_k^n$ to have power at most $O(P^{-\Xi})$. If all links to the eavesdroppers take their strengths $\alpha_{ek}$ from $[0, \Xi)$, the messages never appear above the noise floor of the eavesdroppers, and are thus kept secret. As a result, we identify for $[\boldsymbol{\alpha}_E]$ a cube $[0,\Xi)^{KE}$, which is a subset of $\mathbb{R}^{KE}$ with a positive Lebesgue measure, such that the SGDoF region of the IC with eavesdroppers remains to be $\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$.

## 3.6 Summary

By adding secrecy constraints we obtain the largest parameter regimes known thus far (the STIN regime for interference networks, and the SLS regime for broadcast networks) where sharp characterizations of robust (finite precision CSIT) GDoF regions are obtained for arbitrary number of users, and robust TIN-like schemes are optimal. The robustness aspect is especially strong for interference networks, because the solution is robust not only against the transmitters' finite precision knowledge of channel coefficients, but also against errors in the transmitters' knowledge of channel strengths (the $\alpha_{ij}$ parameters), provided that the transmitters' estimates of channel strengths are conservative. In other words, as long as the channel strengths for desired links are not overestimated and those for interfering links are not underestimated by the transmitter(s), the messages remain decodable and secure, and therefore the GDoF characterizations continue to hold. This is because each receiver finds its desired codeword and the accompanying jammer shifted upward in power, compared to what the transmitters expect; meanwhile it finds the other codewords shifted downward in power. As a result, the desired message remains decodable while the other messages remain secure.

# Chapter 4

# The Robustness of Structured Codes: Secure GDoF of $Z$ Channels

## 4.1 Benefits of Structured Codes

The capacity of wireless networks, as evident from recent Degrees of Freedom (DoF) [4] and Generalized Degrees of Freedom (GDoF) [7] studies, depends rather strongly on the underlying assumptions about the availability of channel state information at the transmitter(s) (CSIT). Zero forcing [2, 102], interference alignment [9–12] — structured codes [103, 104] in general — are powerful ideas; nevertheless their benefits can quickly disappear under even moderate amounts of channel uncertainty. Robustness is paramount, and it is enforced in GDoF studies by limiting CSIT to finite precision [17, 20]. This leads naturally to a crucial question: how robust are structured codes? Specifically, to what extent does finite precision CSIT fundamentally limit the benefits of structured coding schemes?

Accounting for arbitrary structure is essential because, unlike random noise, interference can be arbitrarily structured. It is the structure of the codes that decides how the signals align with each other, how many signal dimensions they occupy together, whether they add constructively or destructively, whether they can be collectively or individually decoded [53, 89, 94, 105–114]. Accounting for structure, even from the coarse GDoF perspective, turns out to be difficult, perhaps because structured codes are inherently combinatorial objects. This is especially the case for *robust* GDoF studies (e.g., with CSIT limited to finite precision), where it is increasingly evident that classical information theoretic tools are lacking.

### 4.1.1 Bounding Structure Benefits by Aligned Images

With the exception of 'Aligned Images (AI)' bounds [20], there are no alternatives, to our knowledge, that have been found to be capable of bounding the benefits of structure under non-trivial channel uncertainty. For example, aside from the combinatorial approach of AI bounds, there still is no other argument to *prove* that the $K$ user interference channel (IC) has *any* less than a total of $K/2$ DoF under finite precision CSIT. Note that Aligned Images bounds can prove something *much* stronger — that it has only a total of 1 DoF [20]. In fact even if all the transmitters cooperate fully the resulting $K$ user multiple-input single-output (MISO) broadcast channel (BC) still has only 1 DoF (thus resolving a conjecture by Lapidoth, Shamai and Wigger [17]). AI bounds have been similarly essential to robust GDoF characterizations of various interference and broadcast settings, such as the symmetric $K$ user IC [25], the two user MIMO IC with arbitrary levels of CSIT [33], the 3 user MISO BC [36], and the two user MIMO BC with arbitrary levels of CSIT, [26, 31]. Robust GDoF characterizations have also been found using AI bounds for various intermediate levels of transmitter cooperation in [28, 62, 63].

Aligned Images bounds are so called because they are based on counting the expected number of codewords that can cast 'aligned images' at one receiver while casting resolvable images at another. Because of their essentially combinatorial character, derivations of AI bounds can be somewhat tedious. Yet, the lack of alternatives thus far makes these bounds indispensable to the goal of developing a robust understanding of the capacity limits of wireless networks. In order to make further progress in this direction, it is important to explore and expand the scope of AI bounds. Notably, the class of AI bounds was recently expanded significantly into a broad class of sum-set inequalities in [24]. Exploring applications of these increasingly sophisticated sumset inequalities is another motivation for our work in this chapter.

## 4.2 Problem Statement and Contributions

### 4.2.1 Robustness of Structured Jamming

With the aid of sum-set inequalities we wish to explore the robustness of structured codes for secure communication [89, 94, 107–109, 113, 115–119]. In particular, one powerful idea that is made possible by structured codes is the aggregate decoding and cancellation[1] of jammed signals [89, 94, 113, 117–119]. Lattice-coded jamming signals are sometimes used to guarantee the secrecy of a message that is itself encoded with a compatible lattice code. A key advantage of structured codes in such settings is that even though neither the jamming noise nor the message is individually decodable, their sum can still be 'decoded' and cancelled. Intuitively, this is because the sum of lattice points is still a valid lattice point. The ability to decode and cancel jammed signals in aggregate is important because it then allows a receiver to successively decode [56] desired signals at lower power levels. However, this ability may not be robust to channel uncertainty, which is especially a concern for secure communication applications where robustness is paramount. The question is fundamental

[1] 'Aggregate decoding and cancellation' is used loosely here to refer to any means by which the interference from jammed signals at higher power levels to the desired signals at lower power levels can be mitigated. The focus is on mitigating the residual interference to lower power levels, and not on the aggregate decoding of higher levels *per se*.

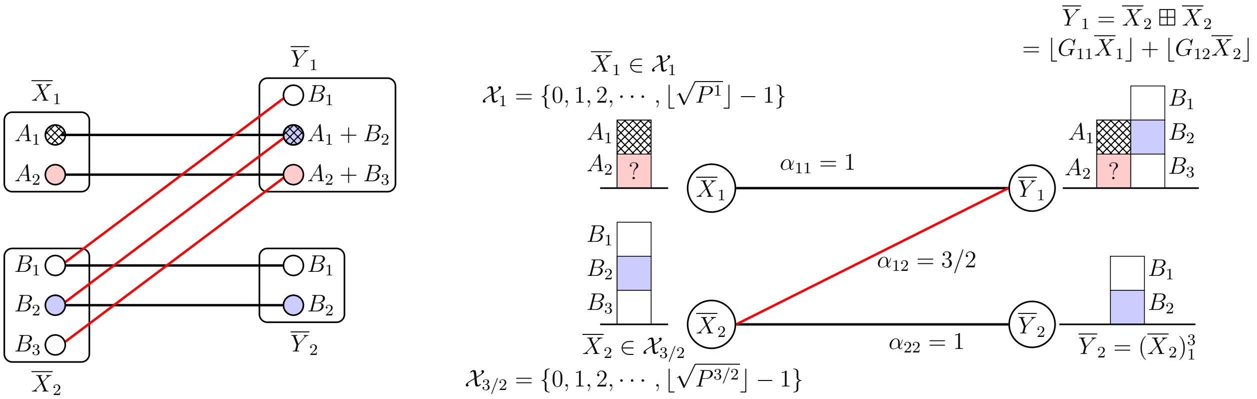

$\overline{X}_1$
$A_1$
$A_2$
$\overline{Y}_1$
$B_1$
$A_1 + B_2$
$A_2 + B_3$
$B_1$
$B_2$
$B_3$
$\overline{X}_2$
$B_1$
$B_2$
$\overline{Y}_2$
$\overline{X}_1 \in \mathcal{X}_1$
$\mathcal{X}_1 = \{0, 1, 2, \cdots, \lfloor\sqrt{P^1}\rfloor - 1\}$
$A_1$
$A_2$
?
$\overline{X}_1$
$\alpha_{11} = 1$
$\overline{Y}_1$
$\overline{Y}_1 = \overline{X}_2 \boxplus \overline{X}_2$
$= \lfloor G_{11}\overline{X}_1\rfloor + \lfloor G_{12}\overline{X}_2\rfloor$
$A_1$
$A_2$
?
$B_1$
$B_2$
$B_3$
$B_1$
$B_2$
$B_3$
$\alpha_{12} = 3/2$
$\overline{X}_2$
$\alpha_{22} = 1$
$\overline{Y}_2$
$B_1$
$B_2$
$\overline{X}_2 \in \mathcal{X}_{3/2}$
$\mathcal{X}_{3/2} = \{0, 1, 2, \cdots, \lfloor\sqrt{P^{3/2}}\rfloor - 1\}$
$\overline{Y}_2 = (\overline{X}_2)_1^3$

Figure 4.1: A toy example. On the left is the ADT deterministic model which shows that under perfect CSIT the secure GDoF tuple $(1/2, 1/2)$ is achievable (needs lattice alignment between structured codes $B_2$ and $A_1$). On the right is the corresponding channel model under finite precision CSIT, for which we prove in this chapter that the GDoF tuple $(\delta, 1/2)$ is not achievable for any $\delta > 0$. This can be seen from Theorem 4.1 by substituting $\beta = 3/2, d_2 = 3/2$ in Case 2, which yields $d_1 \leq 0$. Some of the notations are defined in Section 4.6.

and therefore broadly relevant, but in order to minimize distractions we study what is perhaps the simplest scenario where the question presents itself — a $Z$ interference channel with secrecy constraints [120–124].

### 4.2.2 A Toy Example

As a motivating example, consider the toy setting of a $Z$ channel illustrated in Figure 4.1 where the two transmitters wish to send independent secret messages to their respective receivers, and only Receiver 1 experiences interference. The desired links of each user by themselves are capable of carrying 1 GDoF, while the cross-link has 3/2 GDoF. Intuitively, if we think of $C_{ij}$ as representing the capacity of the point-to-point channel between Transmitter $j$ and Receiver $i$, then the capacities are in the ratio $C_{11} : C_{12} : C_{22} = 2 : 3 : 2$ for this toy example. Note that the ratios of link capacities correspond to the $\alpha_{ij}$ values in the GDoF model, and that only the relative values of $\alpha_{ij}$ matter[2] for the GDoF metric. Throughout this chapter we will normalize $\alpha_{22}$ to unity. In the figure[3] we see both the ADT deterministic model [8] (on the left), which implies *perfect* CSIT, as well as the more general deterministic[4] model (on the right) that allows us to study finite precision CSIT. Similar to the normalization, $\alpha_{22} = 1$, all channel capacities are normalized by the capacity of the channel between Transmitter 2 and Receiver 2 in the ADT model, so that after the normalization we have $(C_{11}, C_{12}, C_{22}) = (1, 3/2, 1)$. The ADT model shows, intuitively, how it is possible with perfect CSIT to achieve the GDoF tuple $(1/2, 1/2)$. Since communication must be secure and the top signal level $B_1$ is fully exposed to the undesired receiver, while the bottom signal level $B_3$ cannot be heard by the desired receiver (below the noise floor) this leaves Transmitter 2 only $B_2$ to achieve its 1/2 GDoF. Transmitter 1 sends a jamming signal $A_1$ to secure $B_2$ from Receiver 1. The most important aspect of this toy example is the alignment that takes place between $A_1$ and $B_2$, both of which are structured (lattice) codes, so that the sum $A_1 + B_2$ also has a lattice structure. This allows Receiver 1 to 'decode' the sum $A_1 + B_2$ (without being able to decode $A_1$ or $B_2$ separately, which would violate secrecy), subtract it from the received signal and then decode its desired signal $A_2$ in order to simultaneously achieve 1/2 GDoF. Now consider the same problem under finite precision CSIT, which poses obstacles for lattice alignment. If lattice alignment is restricted then so is the ability of Receiver 1 to 'decode' the linear combination of signals $A_1$ and $B_2$, which in turn limits the potential for decoding the desired signal $A_2$ that appears at a lower power level. But how strong are these restrictions? Is it still possible to partially mitigate interference from aligned signals at higher power levels to allow decoding of desired signals at lower power levels? Are these restrictions fundamental — could there be other structured

[2] It follows from the definition of GDoF that if all $\alpha_{ij}$ values are scaled by the same constant then the GDoF value is scaled by that constant as well.

[3] Intuitively, $\overline{X}_1$, $\overline{X}_2$ are non-negative integers that can be (approximately) expressed in $\lfloor\sqrt{P^{1/2}}\rfloor$-ary symbols as $\overline{X}_1 = A_1A_2$ and $\overline{X}_2 = B_1B_2B_3$.

[4] The model is not fully *deterministic* in a strict sense, because the channel coefficients are not perfectly known to the transmitters. The nomenclature comes from the fact that the Gaussian noise is removed in this model.

coding schemes, yet to be discovered, that could overcome such limitations? These are the fundamental questions that motivate the work in this chapter.

### 4.2.3 Secure Robust GDoF of the $Z$ Channel

What we find, using Aligned Images sum-set inequalities [24], is that indeed the limitations imposed on structured codes by finite precision CSIT, are both strong and fundamental. In the specific context of this toy example, we prove that the GDoF tuple $(\delta, 1/2)$ is not achievable for any $\delta > 0$. Thus, the GDoF benefits of lattice alignment, aggregate decoding and cancellation are all lost under finite precision CSIT, underscoring their fragile nature. Moreover, because the bound is information theoretic, no better alternative can exist. Beyond the toy example, the general proof formalizes the intuition that under finite precision CSIT, lower layers cannot be decoded without decoding higher layers, and higher layers cannot be decoded in aggregate if they cannot be decoded separately. As a byproduct of this analysis, we fully characterize the secure GDoF region of the $Z$ channel under finite precision CSIT.

Since the $Z$ interference channel is a canonical setting that has been extensively studied under a variety of assumptions, let us note that there are three essential distinguishing aspects of our work: 1) robustness, 2) information theoretic optimality in the GDoF sense, and 3) security. It is the combination of these 3 aspects that makes our setting uniquely challenging and allows us to explore the limitations of aggregate decoding for structured jamming under channel uncertainty. In fact it is arguably the simplest problem that allows us to do so. For example, if we relax any of these three constraints then there would be no need for AI bounds. If we relax the robustness constraint by allowing perfect CSIT, then the problem has been studied in [120,121], and since channel uncertainty is not a concern, ADT models can be used to construct powerful lattice alignment solutions as shown in Figure 4.1. If we do not insist on information theoretic optimality then achievable schemes are easily developed, say from [80]. If we stop short of GDoF, e.g., only ask for DoF (degrees of freedom) by restricting $\alpha = \beta = 1$, then the problem becomes trivial because the DoF region is the simplex bounded by $d_1 + d_2 \leq 1$ even with perfect CSIT, which is also achievable with finite precision CSIT. If we relax the security constraint, then there is no need for structured codes (e.g., lattice alignment) and the capacity has been characterized within a gap of a constant number of bits in [125]. Furthermore, the two user $Z$ interference channel with secrecy constraint is especially appealing because it has very few channel parameters, which allows us to seek a comprehensive GDoF characterization for the entire parameter space without any assumptions of symmetry, and at the same time the secrecy constraint ensures that the problem is non-trivial and allows room to explore sophisticated applications of the new sumset inequalities [24].

Remarkably, despite its simplicity, the two user $Z$ channel is not far from exhausting the scope of known sum-set inequalities. It is noted recently in [30] that even if we introduce just one more user, which changes the two user $Z$ channel into a 3-to-1 interference channel (only Receiver 1 experiences interference), then the problem of characterizing the secure GDoF region under robust CSIT assumptions may be beyond the reach of known sum-set inequalities. Finally, let us note that the $Z$ interference channel has also been explored under other assumptions that are not so closely related to the work in this chapter, e.g., deterministic encoders [122], cooperation between transmitters [123], cooperation between receivers [126], binary alphabet [124], and lack of coordination/trust between transmitters [127].

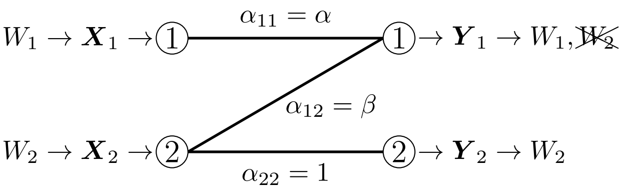

$W_1 \to \boldsymbol{X}_1 \to$ 1
$\alpha_{11} = \alpha$
1 $\to \boldsymbol{Y}_1 \to W_1, \cancel{W_2}$
$\alpha_{12} = \beta$
$W_2 \to \boldsymbol{X}_2 \to$ 2
2 $\to \boldsymbol{Y}_2 \to W_2$
$\alpha_{22} = 1$

Figure 4.2: The Gaussian $Z$ interference channel (ZIC).

## 4.3 System Model

### 4.3.1 The Gaussian $Z$ Interference Channel (ZIC)

We consider the two user Gaussian $Z$ Interference Channel depicted in Figure 4.2, which consists of two transmitters and two receivers, each equipped with a single antenna. As shown in the figure, the network has a $Z$ topology, so both transmitters are heard by Receiver 1, while only Transmitter 2 is heard by Receiver 2. There are two independent messages $W_1$ and $W_2$, that originate at Transmitter 1 and Transmitter 2 and are desired by Receiver 1 and Receiver 2, respectively. Message $W_i$ is uniformly distributed over the set $\mathcal{W}_i$. The messages are encoded into codewords $\boldsymbol{X}_1, \boldsymbol{X}_2$, where $\boldsymbol{X}_i = \{X_i(t) : t \in [n]\} \in \mathbb{R}^n$ is a codeword spanning $n$ channel uses that is sent from Transmitter $i$, and satisfies a unit transmit power constraint, $\frac{1}{n}\sum_{t\in[n]}\mathbb{E}[|X_i(t)|^2] \leq 1$, $i = 1, 2$. The messages are encoded separately and there is no common randomness shared between transmitters; i.e., $\boldsymbol{X}_i = f_{i,n}(W_i, \theta_i)$, where $f_{i,n}(.)$, $i = 1, 2$ are encoding functions, $\theta_i$ is private randomness available only to Transmitter $i$, and $I(\theta_1, W_1; \theta_2, W_2) = 0$.

### 4.3.2 The Gaussian $Z$ Broadcast Channel (ZBC)

While our focus is primarily on the ZIC, as a useful point of reference let us also define the corresponding Gaussian $Z$ Broadcast Channel (ZBC), shown in Figure 4.3, which is identical to the ZIC in every regard except that in the ZBC the transmitters are allowed to cooperate

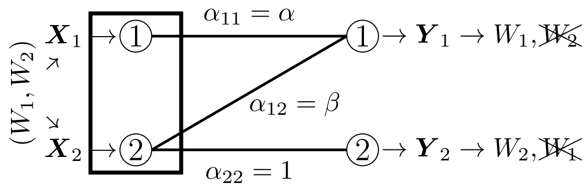


Figure 4.3: The Gaussian $Z$ broadcast channel (ZBC).

fully to jointly encode the messages; i.e., $(\boldsymbol{X}_1, \boldsymbol{X}_2) = f_{0,n}(W_1, W_2, \theta_1, \theta_2)$, where $f_{0,n}$ is the encoding function.

### 4.3.3 The GDoF framework

Within the GDoF framework, the received signals in the $t$-th channel use are described as

$$Y_1(t) = G_{11}(t)\sqrt{P^{\alpha_{11}}}X_1(t) + G_{12}(t)\sqrt{P^{\alpha_{12}}}X_2(t) + Z_1(t), \tag{4.1}$$

$$Y_2(t) = G_{22}(t)\sqrt{P^{\alpha_{22}}}X_2(t) + Z_2(t), \tag{4.2}$$

where $P$ is a nominal variable (referred to as *power*) whose asymptotic limit, i.e., $P \to \infty$, will be used to define the GDoF metric. $Z_i(t), i = 1, 2$, are the zero-mean unit-variance additive white Gaussian noise terms. $X_i(t), i = 1, 2$, are the signals sent from the two transmitters, each of which is subject to a unit transmit power constraint. All symbols are real-valued. $\alpha_{ij} \geq 0$ $(i, j = 1, 2)$ are channel strength parameters for the link from Transmitter $j$ to Receiver $i$. Without loss of generality,[5] let us normalize the $\alpha_{ij}$ parameters so that $\alpha_{22} = 1, \alpha_{12} = \beta$ and $\alpha_{11} = \alpha$.

Let us briefly recall the motivation behind the GDoF framework. The channel strength parameters $\alpha_{ij}$ correspond (approximately) to the capacity of the corresponding point-to-point Gaussian channel between Transmitter $j$ and Receiver $i$. Specifically, note that the links

[5] There is no loss of generality in this assumption because from the definition of GDoF in (4.5) it is obvious that any normalization of $\alpha_{ij}$ parameters results in simply the same normalization factor appearing in the GDoF value.

under the GDoF framework in (4.1) and (4.2) have approximate point-to-point capacities $\alpha_{ij}\Big(\frac{1}{2}\log(P)\Big)$. Here $\frac{1}{2}\log(P)$ may be viewed as a nominal scaling factor that is applied to proportionately scale the capacity of every link. The intuition behind this scaling is that as the capacity of every link is scaled by the same factor, the network capacity should scale by approximately the same factor as well. Therefore, normalizing all rates by $\frac{1}{2}\log(P)$ yields an approximation to the capacity of the network. Letting $P$ approach infinity makes the problem amenable to asymptotic analysis, which indeed gives us the definition of GDoF (See equation (4.5)). It is noteworthy that the deterministic models of [8], which have been the key to numerous capacity approximations over the last decade, are specializations of the GDoF framework under perfect CSIT. For robust GDoF studies, however, we need to limit CSIT to finite precision.

### 4.3.4 Finite Precision CSIT

Following in the footsteps of [20], let us define $\mathcal{G}$ as a set of random variables that satisfy the bounded density assumption of [20] (replicated as Definition 4.3 in Section 4.6.1 of this chapter). Elements of $\mathcal{G}$ may be viewed as random perturbation factors that are introduced into the model primarily to limit CSIT to finite precision, thus their realizations are assumed to be known perfectly to the receivers but not to the transmitters. Formally,

$$I(W_1, W_2, \theta_1, \theta_2, \boldsymbol{X}_1, \boldsymbol{X}_2; \mathcal{G}) = 0. \tag{4.3}$$

Specifically, the channel coefficients $G_{ij}(t)$ are distinct elements of $\mathcal{G}$ for all $t \in [n], i = 1, 2$.

### 4.3.5 Perfect CSIT

While our focus in this chapter is primarily on finite precision CSIT, as a useful point of reference let us also introduce the perfect CSIT assumption, which implies that the channel coefficients $G_{ij}(t)$ are perfectly known not only to both receivers but to both transmitters as well. The constraint (4.3) does not hold under perfect CSIT, and the coding functions may depend on the channel realizations. Thus, $\boldsymbol{X}_i = f_{i,n}(W_i, \theta_i, \mathcal{G})$, $i = 1, 2$ for the ZIC under perfect CSIT, and $(\boldsymbol{X}_1, \boldsymbol{X}_2) = f_{0,n}(W_1, W_2, \theta_1, \theta_2, \mathcal{G})$ for the ZBC under perfect CSIT.

### 4.3.6 Achievable Rates and Secrecy Constraints

A rate tuple $(R_1, R_2)$ is achievable subject to the secrecy constraint if, for all $\epsilon > 0$, there exist $n$-length codes for some $n > 0$ such that (i) the size of each message set $|\mathcal{W}_i| \geq 2^{nR_i}$; (ii) the decoding error probabilities at both users are no larger than $\epsilon$; and (iii) the following secrecy constraint is satisfied

$$\frac{1}{n} I(W_j; \boldsymbol{Y}_i \mid \mathcal{G}) \leq \epsilon \qquad\qquad \forall i, j \in \{1, 2\}, i \neq j. \tag{4.4}$$

Note that the secrecy constraint (4.4) is defined in the weak sense (normalized by $n$) [128]. The secure capacity region $\mathcal{C}_P$ is the closure of the set of all achievable secure rate tuples.

### 4.3.7 Secure GDoF Region

The secure GDoF region $\mathcal{D}$ is defined as

$$\mathcal{D} \triangleq \left\{ (d_1, d_2) \in \mathbb{R}_+^2 \middle| \exists (R_1(P), R_2(P)) \in \mathcal{C}_P, d_i = \lim_{P \to \infty} \frac{R_i(P)}{\frac{1}{2} \log P}, \forall i \in \{1, 2\} \right\}. \tag{4.5}$$

We will use subscripts to distinguish ZIC from ZBC, and superscripts to distinguish finite precision CSIT from perfect CSIT, so for example, $\mathcal{D}^{\text{f.p.}}_{\text{IC}}$ symbolizes the GDoF region for the ZIC under finite precision CSIT, and $\mathcal{D}^{\text{p}}_{\text{BC}}$ is the GDoF region for the ZBC under perfect CSIT.

## 4.4 Results

In order to answer our titular question about the robustness of structured codes, we will compare the GDoF region of the ZIC under perfect CSIT with the GDoF region of the ZIC under finite precision CSIT, i.e., $\mathcal{D}^{\text{p}}_{\text{IC}}$ versus $\mathcal{D}^{\text{f.p.}}_{\text{IC}}$. These are characterized below in Lemma 4.1 and Theorem 4.1, respectively.

### 4.4.1 Secure GDoF of the ZIC With Perfect CSIT

**Lemma 4.1.** *The secure GDoF region of the ZIC under perfect CSIT is characterized as*

$$\mathcal{D}^{p}_{IC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \middle| \begin{array}{l} d_1 \leq \alpha, d_2 \leq \min\{1, (1+\alpha-\beta)^+\}, \\ d_1 + d_2 \leq \alpha + (1-\beta)^+ \end{array} \right\}, \tag{4.6}$$

*where $\alpha, \beta \geq 0$ are defined in Figure 4.2.*

While a direct statement of Lemma 4.1 does not appear in prior literature to our knowledge, the lemma essentially follows from known results and arguments. For the sake of completeness, these arguments are summarized in Appendix C.1.

### 4.4.2 Secure GDoF of the ZIC With Finite Precision CSIT

**Theorem 4.1.** *The secure GDoF region of the ZIC under finite precision CSIT is characterized as,*

1. *Regime 1:* $1 < \beta < \alpha$

$$\mathcal{D}_{IC}^{\text{f.p.}} = \left\{(d_1, d_2) \in \mathbb{R}_+^2 \middle| d_2 \le 1, d_1 + \beta d_2 \le \alpha\right\}, \tag{4.7}$$

2. *Regime 2:* $1 < \beta$ *and* $\beta - 1 < \alpha \le \beta$

$$\mathcal{D}_{IC}^{\text{f.p.}} = \left\{(d_1, d_2) \in \mathbb{R}_+^2 \middle| \frac{d_1}{\alpha} + \frac{d_2}{1 + \alpha - \beta} \le 1\right\}, \tag{4.8}$$

3. *Regime 3:* $1 < \beta$ *and* $\alpha \le \beta - 1$

$$\mathcal{D}_{IC}^{\text{f.p.}} = \left\{(d_1, d_2) \in \mathbb{R}_+^2 \middle| d_1 \le \alpha, d_2 = 0\right\}, \tag{4.9}$$

4. *Regime 4:* $0 \le \beta \le 1$

$$\mathcal{D}_{IC}^{\text{f.p.}} = \left\{(d_1, d_2) \in \mathbb{R}_+^2 \middle| \begin{array}{l} d_1 \le \alpha, d_2 \le 1, \\ d_1 + d_2 \le 1 + \alpha - \beta \end{array}\right\}, \tag{4.10}$$

*where* $\alpha, \beta \ge 0$ *are defined in Figure 4.2.*

The proof of Theorem 4.1 appears in Section 4.5 and 4.6. The main contribution of this chapter is the proof of Theorem 4.1 for Regimes 1 and 2. Regime 3 lies in the very strong interference regime defined in [7], where Receiver 1 can decode whatever Receiver 2 can decode in the GDoF sense, and hence the GDoF value is trivial in this regime under secrecy. Regime 4 lies in the STIN regime defined in [129], where optimal secure GDoF are achieved

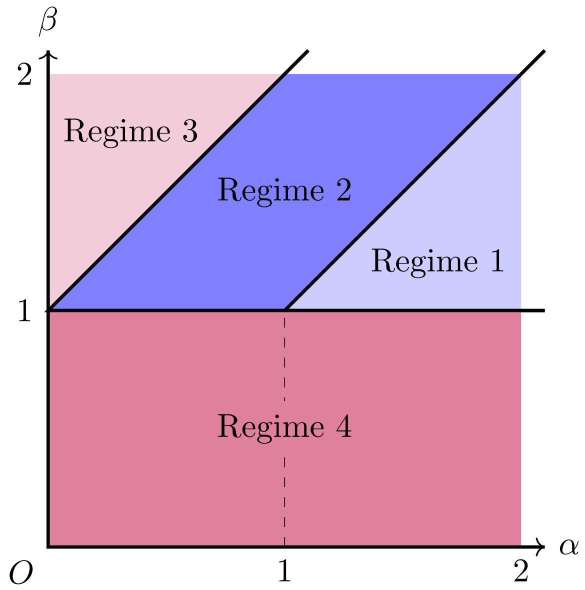


Figure 4.4: The parameter regimes corresponding to the four cases in Theorem 4.1.

with jammers, power control and treating interference as noise. The converse proofs for Regimes 1 and 2 rely on various sum-set inequalities of [24], and are central to the thesis of this chapter, that the benefits of structured jamming are not robust to finite precision CSIT in the GDoF sense.

### 4.4.3 How Robust Are Structured Codes?

With the help of Lemma 4.1 and Theorem 4.1, we are ready to explore the robustness of the GDoF gains from structured codes through the following observations.

1. There are 4 parameter regimes identified in Theorem 4.1. These regimes are shown in Figure 4.4. Our first observation is that in regimes 3 and 4, we have $\mathcal{D}_{\text{IC}}^{\text{p}} = \mathcal{D}_{\text{IC}}^{\text{f.p.}}$, i.e., there is no loss of GDoF from limiting CSIT to finite precision. However, this is not because structured codes are robust to finite precision CSIT. Upon inspection of the achievable scheme, it is evident that these are the regimes where structured codes are not needed even with perfect CSIT. In Regime 3 we only need to switch off Transmitter 2, thus allowing

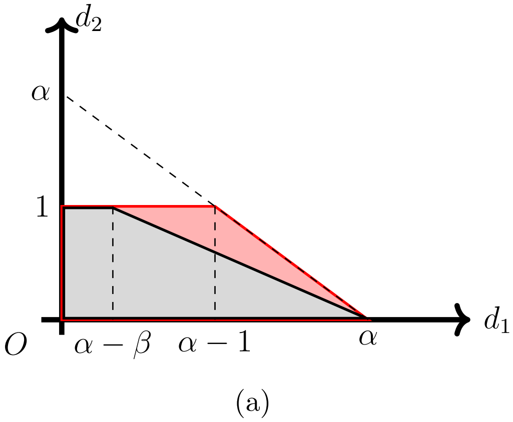


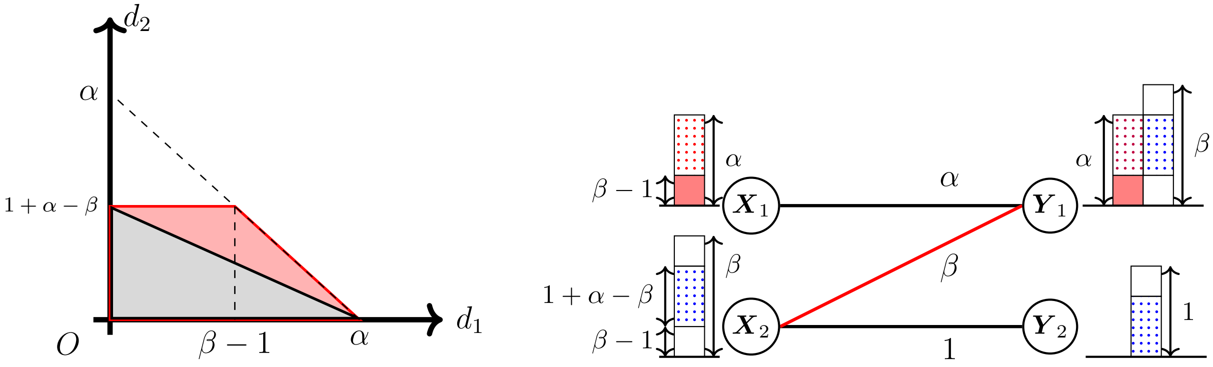
Figure 4.5: (a) $\mathcal{D}_{\text{IC}}^{\text{p}}$ (in red) and $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ (in grey) are shown for Regime 1 (where $1<\beta<\alpha$). (b) The achievability of $(d_1^{**},d_2^*)=(\alpha-1,1)$ under perfect CSIT is illustrated. In particular, aggregate decoding and cancellation of lattice-aligned signals (blue and red dotted portions) is required, which is possible only under perfect CSIT. Signal levels shown in plain white are empty.

User 1 to achieve $\alpha$ GDoF. It is not possible for User 2 to achieve any positive GDoF value in Regime 3 without violating the secrecy constraint because the signal from Transmitter 2 appears at Receiver 1 with so much strength ($\beta \geq \alpha+1$), that even if Transmitter 1 uses all its power to only transmit noise, thus maximally elevating the noise floor at Receiver 1, the interfering signal that appears above the noise floor at Receiver 1 still reveals everything that is visible to Receiver 2. In Regime 4 we adjust the power used by Transmitter 2 to send its own message, which will cause interference at Receiver 1. To keep it secure, all we need for Transmitter 1 is to transmit enough noise (jamming) to elevate the noise floor at Receiver 1 to the level of the interfering signal, and then send its desired message above the new noise floor. The jamming guarantees security, and the desired signal is decoded by Receiver 1 simply by treating everything else as noise. Thus, there is no need for structured codes to allow alignment or aggregate decoding of signals.

2. In regimes 1 and 2 a gap appears between $\mathcal{D}_{\text{IC}}^{\text{p}}$ and $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$. Indeed, these regimes are central to the work in this chapter, as they reveal the fragility of structured codes. First let us consider Regime 1. The GDoF regions, $\mathcal{D}_{\text{IC}}^{\text{p}}$ and $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ for this regime are illustrated in Figure 4.5(a). Let $d_2^*$ denote the maximal value of $d_2$. According to Figure 4.5(a), $d_2^*=1$.

Conditioned on $d_2 = d_2^*$, let $d_1^{**}$ denote the maximum value of $d_1$. We note that under perfect CSIT we have $(d_1^{**}, d_2^*) = (\alpha - 1, 1)$ but under finite precision CSIT we only have $(d_1^{**}, d_2^*) = (\alpha - \beta, 1)$. This loss of GDoF reveals the fragility of aggregate decoding of structured codes. For an intuitive explanation, consider Figure 4.5(b) which shows how $(d_1^{**}, d_2^*) = (\alpha - 1, 1)$ is achieved under perfect CSIT, by lattice alignment between the dotted portions of signals seen at Receiver 1. This lattice alignment ensures the secrecy of $W_2$ from Receiver 1, while simultaneously allowing Receiver 1 to decode the sum of lattice points as a valid codeword. Indeed, while the top $\alpha - \beta$ GDoF (shown in light red) of desired message can be decoded by Receiver 1 without any need for alignment, it is the aggregate decoding of aligned signals that allows Receiver 1 to decode the additional bottom $\beta - 1$ GDoF (shown in dark red) of desired message, thus achieving a total of $d_1^{**} = (\alpha - \beta) + (\beta - 1) = \alpha - 1$ GDoF. Intuitively, under finite precision CSIT, aggregate decoding and cancellation are not possible, thus Receiver 1 is only able to decode the top $\alpha - \beta$ GDoF of desired message, i.e., $d_1^{**} = \alpha - \beta$. The main technical challenge in this chapter is to prove this intuition, i.e., to show that aggregate decoding or any other structured jamming scheme that even partially retains the GDoF benefits of aggregate decoding and cancellation, is not possible under finite precision CSIT.

3. Now let us consider Regime 2, for which the GDoF regions $\mathcal{D}_{\text{IC}}^{\text{p}}$ and $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ are illustrated in Figure 4.6(a). In this case the loss of GDoF is even more severe as we have $(d_1^{**}, d_2^*) = (\beta - 1, 1 + \alpha - \beta)$ under perfect CSIT, and only $(d_1^{**}, d_2^*) = (0, 1 + \alpha - \beta)$ under finite precision CSIT. The loss of GDoF is once again attributable to the fragility of aggregate decoding, as illustrated in Figure 4.6(b). Aggregate decoding and cancellation of lattice-aligned signals allows Receiver 1 to decode the bottom $\beta - 1$ GDoF of desired message under perfect CSIT, thus achieving $d_1^{**} = \beta - 1$. Intuitively, under finite precision CSIT, Receiver 1 is no longer able to decode the aggregate signal, indeed $d_1^{**} = 0$. Once again, the challenge is to formalize and prove this intuition, for which we will rely on sum-set inequalities of [24].



(a)

(b)

Figure 4.6: (a) $\mathcal{D}_{\text{IC}}^{\text{p}}$ (in red) and $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ (in grey) are shown for Regime 2 (where $1 < \beta$ and $\beta - 1 < \alpha \leq \beta$). (b) The achievability of $(d_1^{**}, d_2^*) = (\beta - 1, 1 + \alpha - \beta)$ under perfect CSIT is illustrated. In particular, aggregate decoding of lattice-aligned signals (blue and red dotted portions) is required, which is possible only under perfect CSIT. Signal levels shown in plain white are empty.

4. The loss of GDoF in terms of $d_1^{**}$ values is illustrated for the entirety of Regimes $1, 2, 3$ in Figure 4.7. As noted, there is no loss in Regime 3, and Regime 4 is omitted to avoid clutter. Regime 2 is particularly striking because $d_1^{**} = 0$ under finite precision CSIT. The discontinuity between Regime 2 and Regime 3 is interesting, because it shows the tremendous cost for securing $W_2$ that is incurred in Regime 2 where $d_2^* > 0$. Note that this cost disappears in Regime 3 where $d_2^* = 0$.

5. While the previous observations emphasized the loss of GDoF, let us now provide a counterpoint to show that the loss is bounded. As another measure of the loss of GDoF, consider an arbitrary weighted sum of GDoF values, say $d(w_1, w_2) = w_1 d_1 + w_2 d_2$. Let us denote the maximal value of $d(w_1, w_2)$ for the ZIC under finite precision CSIT as $d_{\text{IC}}^{\text{f.p.}}(w_1, w_2) = \max_{(d_1,d_2) \in \mathcal{D}_{\text{IC}}^{\text{f.p.}}} w_1 d_1 + w_2 d_2$. Similarly, for perfect CSIT we have $d_{\text{IC}}^{\text{p}}(w_1, w_2) = \max_{(d_1,d_2) \in \mathcal{D}_{\text{IC}}^{\text{p}}} w_1 d_1 + w_2 d_2$. Based on Lemma 4.1 and Theorem 4.1, it is not difficult to verify that the extremal value,

$$\inf_{(\alpha,\beta) \in \mathbb{R}_2^+} \inf_{(w_1,w_2) \in \mathbb{R}_2^+} \frac{d_{\text{IC}}^{\text{f.p.}}(w_1, w_2)}{d_{\text{IC}}^{\text{p}}(w_1, w_2)} = \frac{1}{2}. \tag{4.11}$$

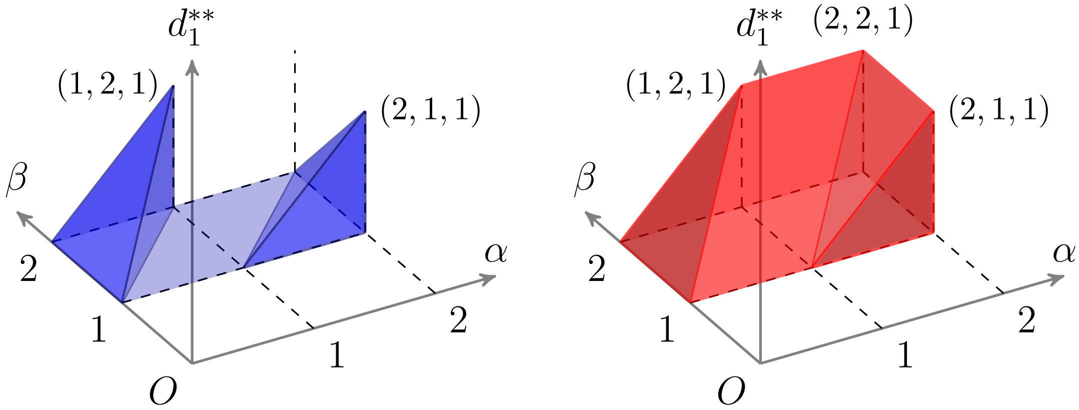


Figure 4.7: $d_1^{**}$ under finite precision CSIT (left) and perfect CSIT (right) in the parameter regimes $1,2,3$. Regime 4 is omitted. Peak vertices are labeled as $(\alpha,\beta,d_1^{**})$ tuples.

In other words, looking out from the origin, the GDoF region $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ is *at least* half as large in every direction as the GDoF region $\mathcal{D}_{\text{IC}}^{\text{p}}$. It is also easy to see that the bound is asymptotically tight because, e.g., in Figure 4.5(a), if we let $\beta \to \alpha$ from below and $\alpha \to \infty$, then $\mathcal{D}_{\text{IC}}^{\text{p}}$ approaches an almost-rectangular shape (with vertices $(0,0),(\alpha,0),(\alpha-1,1),(0,1)$) and $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ approaches the lower left half triangle created by a diagonal-wise partitioning of the rectangle (with vertices $(0,0),(\alpha,0),(0,1)$). Looking out along the other diagonal (the ray that passes through the origin and $(\alpha-1,1)$) we note that $\mathcal{D}_{\text{IC}}^{\text{f.p.}}$ is (asymptotically) only half as large as $\mathcal{D}_{\text{IC}}^{\text{p}}$. Note that this corresponds to $(w_1,w_2)=(\alpha-1,1)$.

6. Note that in the absence of secrecy constraints, the GDoF of the ZIC shown in Figure 4.2 under both CSIT assumptions can be found from [7] as

$$\widetilde{\mathcal{D}}_{\text{IC}}^{\text{p}} = \widetilde{\mathcal{D}}_{\text{IC}}^{\text{f.p.}} = \left\{ (d_1,d_2)\in\mathbb{R}_+^2 \;\middle|\; \begin{aligned} & d_1 \le \alpha, d_2 \le 1, \\ & d_1+d_2 \le \max\{\alpha,\beta\} + (1-\beta)^+ \end{aligned} \right\}. \tag{4.12}$$

### 4.4.4 Secure GDoF of the ZBC With Perfect and Finite Precision CSIT

The ZBC setting is less of our focus because even under perfect CSIT, the ZBC does not require lattice codes or aggregate decoding and cancellation of jammed signals for secure communication. Instead, it achieves secure communication through zero-forcing, which is conceptually much more straightforward. Nevertheless, it is also not robust under channel uncertainty. Moreover, the loss of GDoF in the ZBC under finite precision CSIT is also implied, as a byproduct of our analysis of the ZIC. This is because, remarkably, our converse proofs for Regimes $1, 2$ in Theorem 4.1 hold even if we allow full cooperation among transmitters. Therefore, as our final result let us present the GDoF characterization of the ZBC under both perfect and finite precision CSIT.

**Theorem 4.2.** *The secure GDoF region of the ZBC under perfect CSIT, $\mathcal{D}^{p}_{BC}$, and under finite precision CSIT, $\mathcal{D}^{\text{f.p.}}_{BC}$, are characterized as*

$$\mathcal{D}^{p}_{BC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \;\middle|\; \begin{array}{l} d_1 \leq \max\{\alpha, \beta - 1\}, \\ d_2 \leq (1 - (\beta - \alpha)^+)^+ \end{array} \right\}, \tag{4.13}$$

$$\mathcal{D}^{\text{f.p.}}_{BC} = \begin{cases} \left\{(d_1, d_2) \in \mathbb{R}^2_+ \middle| d_1 \leq \beta - 1, d_2 = 0\right\} & \text{if } 1 < \beta \text{ and } \alpha \leq \beta - 1, \\ \mathcal{D}^{\text{f.p.}}_{IC} & \text{otherwise,} \end{cases} \tag{4.14}$$

*where $\alpha, \beta \geq 0$ are defined in Figure 4.3.*

The proof of Theorem 4.2 is presented in Appendix C.2.

## 4.5 Proof of Theorem 4.1: Achievability

As noted previously, Regime 3 in Theorem 4.1 is trivial and Regime 4 already follows from [129]. Thus we only need the proof for Regimes 1 and 2. In this section we provide the proof of achievability which is quite straightforward.

For Regimes 1 and 2 it suffices to find schemes for the respective corner points and complete the regions by time-sharing. The tuple $(d_1, d_2) = (\alpha, 0)$ is one of the corner points for both cases, and is trivial. For Regime 1 it remains to find an achievable scheme for the other corner point, $(\alpha - \beta, 1)$. This is easily seen by modifying the scheme of Figure 4.5(b), such that Transmitter 1 sends his desired message only in the top $\alpha - \beta$ levels, i.e., and only a jamming signal (Gaussian noise) below that. Thus the noise floor at Receiver 1 is elevated to strength $\beta$, i.e., as high as the interfering signal, which guarantees security. Meanwhile, we let Transmitter 2 transmit at full power. This creates a point-to-point channel for Transmitter 1 where the desired link to Receiver 1 has $\alpha - \beta$ GDoF, and creates a wiretap channel for Transmitter 2 where the desired link to Receiver 2 has 1 GDoF and the eavesdropper link to Receiver 1 has 0 GDoF. Employing a Gaussian codebook in the first point-to-point channel and a wiretap codebook in the second, we achieve $\alpha - \beta$ SGDoF for User 1 and 1 SGDoF for User 2.

For Regime 2 the other corner point is $(0, 1-\alpha+\beta)$. This is also easily achieved by modifying the scheme of Figure 4.6(b), such that Transmitter 1 sends only a jamming signal (Gaussian noise) with its full power. This raises the noise floor at Receiver 1 to power level $\alpha$. As in Figure 4.6(b), we reduce the transmit power at Transmitter 2 so that the top $\beta - \alpha$ levels are empty, i.e., instead of the unit power constraint, Transmitter 2 only transmits with power $P^{-(\beta-\alpha)}$. This creates a wiretap channel for Transmitter 2, where the desired link to Receiver 2 has $1 + \alpha - \beta$ GDoF, and the eavesdropper link to Receiver 1 has 0 GDoF. A wiretap codebook achieves $1 + \alpha - \beta$ SGDoF for User 2 and 0 for User 1.

## 4.6 Proof of Theorem 4.1: Converse

The single user bound, $d_2 \leq 1$, in Regime 1 is trivial. Before presenting the proof of the weighted sum bounds, as preliminary background we need to introduce some definitions, sum-set inequalities, and a deterministic model, all of which originate in prior works on Aligned Images bounds.

### 4.6.1 Preliminaries

#### Definitions

**Definition 4.1** (Power levels)**.** *For $\lambda, P > 0$, define $\bar{P}^{\lambda} \triangleq \left\lfloor \sqrt{P}^{\lambda} \right\rfloor$, and a set $\mathcal{X}_{\lambda}$ as*

$$\mathcal{X}_{\lambda} = \left\{0, 1, 2, \cdots, \bar{P}^{\lambda} - 1\right\}, \tag{4.15}$$

*We refer to $P$ as* power*, and $\lambda$ as* power level *of $X \in \mathcal{X}_{\lambda}$. For simplicity, we denote $\bar{P}^1 = \bar{P}$.*

**Definition 4.2.** *For non-negative real numbers $X$, $\lambda_1$ and $\lambda_2$, where $\lambda_2 \geq \lambda_1 \geq 0$, we define a* sub-section *of $X$ corresponding to* interval *$(\lambda_1, \lambda_2)$, $(X)_{\lambda_1}^{\lambda_2}$, as*

$$(X)_{\lambda_1}^{\lambda_2} \triangleq \left\lfloor \frac{X - \bar{P}^{\lambda_2} \left\lfloor \frac{X}{\bar{P}^{\lambda_2}} \right\rfloor}{\bar{P}^{\lambda_1}} \right\rfloor. \tag{4.16}$$

*We say that the $(X)_{\lambda_1}^{\lambda_2}$ is a section of $X$ that sits at level $\lambda_1$, denoted as $\ell\left((X)_{\lambda_1}^{\lambda_2}\right) = \lambda_1$, and has* height *$\lambda_2 - \lambda_1$, denoted as $\mathcal{T}\left((X)_{\lambda_1}^{\lambda_2}\right) = \lambda_2 - \lambda_1$. Sub-sections $(X)_{\lambda_1}^{\lambda_2}$ and $(X)_{\lambda_1'}^{\lambda_2'}$ of $X \in \mathcal{X}_{\lambda}$ are* disjoint *if intervals $(\lambda_1, \lambda_2)$ and $(\lambda_1', \lambda_2')$ are disjoint.*

Similarly, for a set of non-negative real numbers $\boldsymbol{X} = \{X(t) : \ t \in [n]\}$, we define a sub-section $(\boldsymbol{X})_{\lambda_1}^{\lambda_2}$ as

$$(\boldsymbol{X})_{\lambda_1}^{\lambda_2} \triangleq \left\{(X(t))_{\lambda_1}^{\lambda_2} :\ t \in [n]\right\}. \tag{4.17}$$

Note that the same partitioning is applied to every element in the set. Levels and heights are similarly defined; i.e., $\ell\left((\boldsymbol{X})_{\lambda_1}^{\lambda_2}\right) = \lambda_1$, and $\mathcal{T}\left((\boldsymbol{X})_{\lambda_1}^{\lambda_2}\right) = \lambda_2 - \lambda_1$. Sub-section sets $(\boldsymbol{X})_{\lambda_1}^{\lambda_2}$ and $(\boldsymbol{X})_{\lambda_1'}^{\lambda_2'}$ are disjoint if intervals $(\lambda_1, \lambda_2)$ and $(\lambda_1', \lambda_2')$ are disjoint.

Figure 4.8 illustrates this partitioning of $X$ into various sub-sections. A further interpretation for sub-sections is by expressing numbers with base $\bar{P}$. For $X \in \mathcal{X}_\lambda$ and $\lambda \geq \lambda_2 \geq \lambda_1 \geq 0$, sub-section $(X)_{\lambda_1}^{\lambda_2}$ can be loosely interpreted in terms of the $\bar{P}$-ary expansion of $X$. The $\bar{P}$-ary expansion of $X$ is represented as $X = x_\lambda x_{\lambda-1} \cdots x_2 x_1$, which is equivalent to a string of length $\lambda$ in which each symbol $x_i \in \{0, 1, \cdots, \bar{P} - 1\}$. In this sense, what $(X)_{\lambda_1}^{\lambda_2}$ retrieves from $X$ is a sub-string $x_{\lambda_2} x_{\lambda_2 - 1} \cdots x_{\lambda_1 + 1}$ in the middle of $X$. A case that appears frequently in this chapter is $\lambda_2 = \lambda$ and $\lambda_1 = \lambda - \mu$. The corresponding sub-section $(X)_{\lambda-\mu}^{\lambda}$, denoted as $(X)^\mu$ and referred to as top-$\mu$ sub-section of $X$, retrieves from $X$ the leftmost length-$\mu$ sub-string $x_\lambda x_{\lambda-1} \cdots x_{\lambda-\mu+1}$ comprised of the first $\mu$ most significant symbols in $X$. Similar to (4.17), for a set of non-negative real numbers $\boldsymbol{X}$ with each element in $\mathcal{X}_\lambda$, we define $(\boldsymbol{X})^\mu = \{(X)^\mu :\ X \in \boldsymbol{X}\}$. While this interpretation is helpful, the coarse understanding is an oversimplification, as indeed all $\lambda, \lambda_1$ and $\lambda_2$ can take arbitrary non-negative real values. Such partitioning is essentially a generalization of the original symbol partitioning with binary representations that appeared in the ADT model in [8]. The generalization is needed because of our focus on finite precision CSIT.

**Definition 4.3** (Bounded density assumption)**.** *We define $\mathcal{G}$ as a set of real-valued random variables that satisfies the following conditions (collectively referred to as the bounded density assumption),*

1. *The magnitudes of all random variables in $\mathcal{G}$ are bounded away from infinity and zero;*

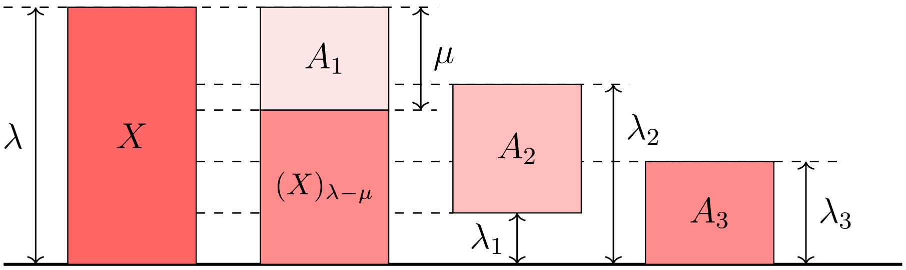


Figure 4.8: An illustration of Definition 4.2. The number $X$ can be decomposed into $X = \bar{P}^{\lambda-\mu}A_1 + (X)_{\lambda-\mu}$. Sub-section $A_1 = (X)_{\lambda-\mu}^{\lambda}$ has level $\ell(A_1) = \lambda - \mu$ and height $\mathcal{T}(A_1) = \mu$. Sub-section $A_2 = (X)_{\lambda_1}^{\lambda_2}$ has level $\ell(A_2) = \lambda_1$ and height $\mathcal{T}(A_2) = \lambda_2 - \lambda_1$. Sub-section $A_3 = (X)_0^{\lambda_3}$ has level $\ell(A_3) = 0$ and height $\mathcal{T}(A_3) = \lambda_3$. Note that $A_1$ and $A_3$ are disjoint when $\lambda - \mu \geq \lambda_3$.

*i.e., there exists a constant $\Delta > 1$ such that $|g| \in \left(\frac{1}{\Delta}, \Delta\right)$ for all $g \in \mathcal{G}$.*

2. *There exists a finite constant $f_{max} > 0$, such that for all finite disjoint subsets $\mathcal{G}_1$, $\mathcal{G}_2$ of $\mathcal{G}$, the joint probability density function of the random variables in $\mathcal{G}_1$, conditioned on the random variables in $\mathcal{G}_2$, exists and is bounded above by $f_{max}^{|\mathcal{G}_1|}$.*

**Definition 4.4** (Finite-precision linear combination)**.** *For $X_1 \in \mathcal{X}_{\eta_1}$ and $X_2 \in \mathcal{X}_{\eta_2}$, define $X_1 \boxplus_{\mathcal{G}} X_2$ as*

$$X_1 \boxplus_{\mathcal{G}} X_2 \triangleq \lfloor G_1 X_1 \rfloor + \lfloor G_2 X_2 \rfloor , \tag{4.18}$$

*where $G_i$ are distinct random variables in $\mathcal{G}$ satisfying the bounded density assumption. For two sets of random variables of the same cardinality, $\boldsymbol{X}_1 = \{X_1(t) \in \mathcal{X}_{\eta_1} :\ t \in [n]\}$ and $\boldsymbol{X}_2 = \{X_2(t) \in \mathcal{X}_{\eta_2} :\ t \in [n]\}$ , we define $\boldsymbol{X}_1 \boxplus_{\mathcal{G}} \boldsymbol{X}_2$ as*

$$\boldsymbol{X}_1 \boxplus_{\mathcal{G}} \boldsymbol{X}_2 \triangleq \{\lfloor G_1(t) X_1(t) \rfloor + \lfloor G_2(t) X_2(t) \rfloor :\ t \in [n]\} , \tag{4.19}$$

*where $G_i(t)$ are distinct random variables in $\mathcal{G}$ satisfying the bounded density assumption. The subscript $\mathcal{G}$ of operator $\boxplus$ may be omitted if no ambiguity arises.*

**Key Sum-set Inequalities**

Our proof leans heavily on the sum-set inequalities based on Aligned Images sets from [24, Theorem 4]. While [24] presents these sum-set inequalities in generalized forms, the following simplified forms of those inequalities, taken from [28, Lemma 1], will be useful for our purpose.

**Lemma 4.2.** *Let $\mu, \nu > 0$, $T(t) \in \mathcal{X}_\mu$, $U(t) \in \mathcal{X}_\nu$ for $t \in [n]$, and $\boldsymbol{T} = \{T(t) : t \in [n]\}, \boldsymbol{U} = \{U(t) : t \in [n]\}$. Let $\boldsymbol{\mathcal{S}}_T$ and $\boldsymbol{\mathcal{S}}_U$ be sets of finitely many disjoint sub-sections, respectively, of $\boldsymbol{T}$ and $\boldsymbol{U}$, and let $\{\boldsymbol{S}_1, \boldsymbol{S}_2, \cdots, \boldsymbol{S}_M\}$ be a subset of $\boldsymbol{\mathcal{S}}_T \cup \boldsymbol{\mathcal{S}}_U$. Let $\boldsymbol{V} = \boldsymbol{T} \boxplus_{\mathcal{G}} \boldsymbol{U}$. Then*

$$H_{\mathcal{G}}\left(\boldsymbol{V}|\mathcal{W}\right) \geq H_{\mathcal{G}}\left(\boldsymbol{S}_1, \boldsymbol{S}_2, \cdots, \boldsymbol{S}_M|\mathcal{W}\right) + no(\log \bar{P}), \tag{4.20}$$

*where $\mathcal{W}$ is a set of random variables satisfying $I(\mathcal{W}, \boldsymbol{T}, \boldsymbol{U}; \mathcal{G}) = 0$, and the following constraints on the levels and heights of $\boldsymbol{S}_i$ hold for $i = 2, 3, \cdots, M$:*

$$\ell(\boldsymbol{S}_i) \geq \mathcal{T}(\boldsymbol{S}_1) + \mathcal{T}(\boldsymbol{S}_2) + \cdots + \mathcal{T}(\boldsymbol{S}_{i-1}). \tag{4.21}$$

Constraint (4.21) in Lemma 4.2 has a box-stacking interpretation that appeared previously in [24, Section IV] and [28, Section IV], but we tailor it as follows to fit the settings in Lemma 4.2. Let's consider the $t$-th channel use only and drop the index for simplicity. We can imagine these random variable sub-sections as boxes with labels $S_1, S_2, \cdots, S_M$; box $S_i$ has height $\mathcal{T}(S_i)$ and originally sits on level $\ell(S_i)$ in either $T$ or $U$. Then we stack the boxes in the index order of $S_1, S_2, \cdots, S_M$ from the ground. Now in this stack box $S_i$ sits above boxes $S_1, S_2, \cdots, S_{i-1}$, therefore it sits at level $\tilde{\ell}(S_i) = \mathcal{T}(S_1) + \mathcal{T}(S_2) + \cdots + \mathcal{T}(S_{i-1})$. Constraint (4.21) says that the new level $\tilde{\ell}(S_i)$ cannot be higher than the level at which box $S_i$ originally sits in $T$ or $U$, which is $\ell(S_i)$. In other words, constraint (4.21) is satisfied if, during retrieving these boxes in $T$ or $U$ and stacking them up from ground, there is no need to elevate any of

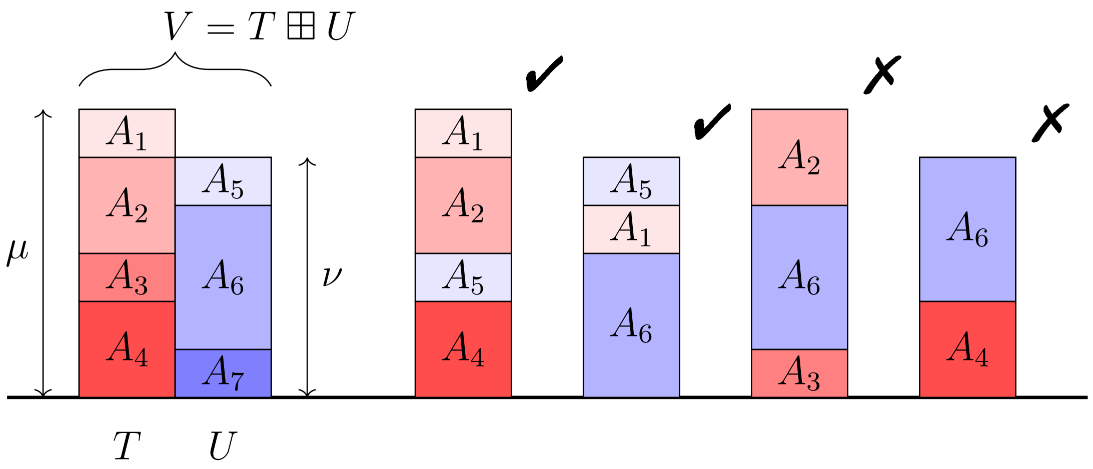


Figure 4.9: An illustration of the box-stacking interpretation of Lemma 4.2. The bounds $H_{\mathcal{G}}(V|\mathcal{W}) \geq H_{\mathcal{G}}(A_1, A_2, A_4, A_5|\mathcal{W})$ and $H_{\mathcal{G}}(V|\mathcal{W}) \geq H_{\mathcal{G}}(A_1, A_5, A_6|\mathcal{W})$ are implied by Lemma 4.2 in the GDoF sense because the boxes appearing in these inequalities can be stacked without elevating any of them above their original levels in $T$ or $U$, as illustrated in the two stacks marked with a ✓. On the other hand, Lemma 4.2 implies neither the bound $H_{\mathcal{G}}(V|\mathcal{W}) \geq H_{\mathcal{G}}(A_2, A_3, A_6|\mathcal{W})$ nor $H_{\mathcal{G}}(V|\mathcal{W}) \geq H_{\mathcal{G}}(A_4, A_6|\mathcal{W})$, because there is no way to stack the boxes appearing in these inequalities without elevating some of them above their original level in $T$ or $U$, as shown in the two stacks marked with a ✗.

them above their original level. Note that while constraints (4.21) seem to fix the stacking order according to the indices of the sub-sections, on the right-hand-side of (4.20) the entropy of the sub-sections does not depend on the index ordering. So one can arbitrarily rearrange the indices of the sub-sections and test the constraints in (4.21) with the permuted ordering. In other words, if there exists a stacking order of these boxes with no need to lift up any of them during stacking, then the sum-set inequality (4.20) holds. Figure 4.9 and 4.10 illustrate some ways to stack the boxes (sub-sections) which satisfy or violate constraints (4.21). Note that different choices of $\{S_1, S_2, \cdots, S_M\}$ lead to different stacks of boxes. For example, in Figure 4.9 the choice of $M = 4$ and $(S_1, S_2, S_3, S_4) = (A_4, A_5, A_2, A_1)$ gives us the checked (✓) stack on the left, while the choice of $M = 3$ and $(S_1, S_2, S_3) = (A_6, A_1, A_5)$ produces the checked stack on the right.

### Deterministic Model

To facilitate the use of Aligned Images bounds, we define a deterministic model as in [20]. In this deterministic model, the inputs are

$$A(t) = \left\lfloor \bar{P}^{\alpha} X_1(t) \right\rfloor \mod \bar{P}^{\alpha}, \tag{4.22}$$

$$B(t) = \left\lfloor \bar{P}^{\max\{1,\beta\}} X_2(t) \right\rfloor \mod \bar{P}^{\max\{1,\beta\}}, \tag{4.23}$$

and the outputs are

$$\overline{Y}_1(t) = \lfloor G_{11}(t) A(t) \rfloor + \left\lfloor G_{12}(t) \bar{P}^{\beta - \max\{1,\beta\}} B(t) \right\rfloor, \tag{4.24}$$

$$\overline{Y}_2(t) = \left\lfloor G_{22}(t) \bar{P}^{1 - \max\{1,\beta\}} B(t) \right\rfloor. \tag{4.25}$$

Note that $A(t) \in \mathcal{X}_{\alpha}$ and $B(t) \in \mathcal{X}_{\max\{1,\beta\}}$. Let $\boldsymbol{A} = \{A(t) : t \in [n]\}$, and $\boldsymbol{B} = \{B(t) : t \in [n]\}$, and $\overline{\boldsymbol{Y}}_i = \{\overline{Y}_i(t) : t \in [n]\}$ for $i = 1, 2$. It can be shown that the GDoF of the Gaussian model are bounded above by the GDoF of the deterministic model, accounting for both decoding and secrecy constraints, as described by the following lemma.

**Lemma 4.3.**

$$I_{\mathcal{G}}(W_i; \boldsymbol{Y}_i) \leq I_{\mathcal{G}}(W_i; \overline{\boldsymbol{Y}}_i) + no(\log \bar{P}) \qquad \forall i = 1, 2, \tag{4.26}$$

$$I_{\mathcal{G}}(W_j; \overline{\boldsymbol{Y}}_i) \leq I_{\mathcal{G}}(W_j; \boldsymbol{Y}_i) + no(\log \bar{P}) \qquad \forall i, j = 1, 2, i \neq j. \tag{4.27}$$

The proof of Lemma 4.3 is identical to that of Lemma 5.1 in [129].

### 4.6.2 Useful Lemmas

With the preliminaries in place, we now proceed to the task of proving the converse for Theorem 4.1, starting with the following lemmas. The first lemma is a straightforward consequence of the secrecy constraint (4.27). In the statement of the lemma, note that $(\boldsymbol{B})^{\overline{\mu}} = (\boldsymbol{B})^{\beta-\alpha}$ is the part of $\boldsymbol{B}$ that is received above $\boldsymbol{A}$ at Receiver 1 when $\beta > \alpha$, and similarly, $(\boldsymbol{A})^{\underline{\mu}} = (\boldsymbol{A})^{\alpha-\beta}$ is the part of $\boldsymbol{A}$ that is received above $\boldsymbol{B}$ at Receiver 1 when $\alpha > \beta$. The lemma essentially says that in terms of GDoF, neither of these exposed sections should reveal information about $W_2$ to Receiver 1, which already has $W_1$ and $\overline{\boldsymbol{Y}}_1$ available to it.

**Lemma 4.4.** *Let $\overline{\mu} = (\beta - \alpha)^+$ and $\underline{\mu} = (\alpha - \beta)^+$. Then we have,*

$$I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1) = no(\log \bar{P}), \tag{4.28}$$

$$I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_2 | W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) = no(\log \bar{P}), \tag{4.29}$$

$$I_{\mathcal{G}}(W_2; W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) = no(\log \bar{P}). \tag{4.30}$$

*Proof.*

$$I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1)$$

$$= I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1) + I_{\mathcal{G}}(W_2; W_1 | \overline{\boldsymbol{Y}}_1) \tag{4.31}$$

$$\leq I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1) + H_{\mathcal{G}}(W_1 | \overline{\boldsymbol{Y}}_1) \tag{4.32}$$

$$\leq I_{\mathcal{G}}(W_2; \boldsymbol{Y}_1) + H_{\mathcal{G}}(W_1 | \boldsymbol{Y}_1) + no(\log \bar{P}) \tag{4.33}$$

$$= no(\log \bar{P}). \tag{4.34}$$

We apply the chain rule to get (4.31), and the definition of mutual information to obtain (4.32). Next, we obtain (4.33) by applying (4.26) and (4.27). Finally, we apply the secrecy constraint (4.4) and Fano's inequality to obtain (4.34).

To show equality (4.29) and (4.30), we note that from $\overline{\boldsymbol{Y}}_1$ one can obtain $(\boldsymbol{A})^{\underline{\mu}}$ and $(\boldsymbol{B})^{\overline{\mu}}$, and then apply the chain rule; more specifically,

$$
\begin{aligned}
no(\log \bar{P}) &= I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1) && (4.35)\\
&= I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) && (4.36)\\
&= I_{\mathcal{G}}(W_2; W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}})\\
&\quad + I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1 | W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}). && (4.37)
\end{aligned}
$$

Equality (4.29) and (4.30) thus hold as mutual information is non-negative. □

The following lemma bounds from above the entropy difference, in the GDoF sense, of finite-precision linear combinations of random variables in terms of their power levels. It is adapted from Lemma 1 of [33] and hence its proof is omitted.

**Lemma 4.5.** *Let $\mu = \max_{i=1,2}\{\mu_i\}$ and $\nu = \max_{i=1,2}\{\nu_i\}$, where $\mu_i, \nu_i > 0, i = 1, 2$. Let $T(t) \in \mathcal{X}_\nu$ and $U(t) \in \mathcal{X}_\mu$ for $t \in [n]$; $\boldsymbol{T} = \{T(t) : \ t \in [n]\}$ and $\boldsymbol{U} = \{U(t) : \ t \in [n]\}$. Let $\boldsymbol{V}_i = (\boldsymbol{T})^{\mu_i} \boxplus_{\mathcal{G}_i} (\boldsymbol{U})^{\nu_i}$, where $i = 1, 2$, and $\mathcal{G} = \mathcal{G}_1 \cup \mathcal{G}_2$ is a set of random variables satisfying the bounded density assumption. Then*

$$
\begin{aligned}
&H_{\mathcal{G}}(\boldsymbol{V}_1 | \mathcal{W}) - H_{\mathcal{G}}(\boldsymbol{V}_2 | \mathcal{W})\\
&\leq \max\{\mu_1 - \mu_2, \nu_1 - \nu_2\}^+ \log \bar{P} + no(\log \bar{P}), && (4.38)
\end{aligned}
$$

*where $\mathcal{W}$ is a set of random variables satisfying $I(\mathcal{W}, \boldsymbol{T}, \boldsymbol{U}; \mathcal{G}) = 0$.*

An important issue that arises in applications of Aligned Images bounds is that of translating between 'linear combinations of sub-sections' on one hand, and 'sub-sections of linear combinations' on the other. Sum-set inequalities are formulated in [24] in terms of linear combinations of various sub-sections of input signals, but converse arguments often involve sub-sections of *output* signals, i.e., sub-sections of linear combinations of input signals. Understanding the extent to which these two notions can be related remains an open problem in general [30]. For our present purpose, however, because we only need the 'top' sub-sections, such a relationship is obtained in the following lemma.

**Lemma 4.6.** *Let $\lambda, \mu, \nu$ be real numbers satisfying $\lambda \geq \mu > 0$ and $\nu \geq 0$. Let $T \in \mathcal{X}_{\nu+\lambda}$ and $U \in \mathcal{X}_{\nu+\mu}$. Then*

$$H_{\mathcal{G}}((T \boxplus U)^{\lambda}) = H_{\mathcal{G}}((T)^{\lambda} \boxplus (U)^{\mu}) + O(1), \tag{4.39}$$

*where $\mathcal{G}$ is a set of random variables satisfying the bounded density assumption.*

Lemma 4.6 compares the entropy of a top sub-section of linear combination of two signals versus the entropy of a linear combination of the top sub-sections. Intuitively, the difference of these entropies is bounded within a constant because in the linear combination of two signals, the terms carried over from lower levels do not not scale with $P$. Such a relationship is referred to as being "within bounded distortion". The proof of Lemma 4.6 appears in Appendix C.3.

The next lemma provides an important lower bound on the entropy of a finite-precision linear combination of random variables based on Lemma 4.2 and the submodularity of entropy.

**Lemma 4.7.** *Let $P, \mu, \nu \geq 0$, and let $p, q > 0$ satisfy $\frac{1}{2} \leq \frac{p}{q} \leq 1$ and $\frac{p}{q} \in \mathbb{Q}$. Let $T(t) \in \mathcal{X}_{q+\mu}$ and $U(t) \in \mathcal{X}_{q+\nu}$ for $t \in [n]$; $\boldsymbol{T} = \{T(t) : \ t \in [n]\}$ and $\boldsymbol{U} = \{U(t) : t \in [n]\}$. Let $\boldsymbol{V} = \boldsymbol{T} \boxplus_{\mathcal{G}} \boldsymbol{U}$, where $\mathcal{G}$ is a set of random variables satisfying the bounded density assumption. Then*

$$\begin{aligned} &2pH_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \\ &\geq qH_{\mathcal{G}}((\boldsymbol{T})^{p+\mu}, (\boldsymbol{U})^{p+\nu}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) + no(\log \bar{P}), \end{aligned} \tag{4.40}$$

*where $\mathcal{W}$ is a set of random variables satisfying $I(\mathcal{W}, \boldsymbol{T}, \boldsymbol{U}; \mathcal{G}) = 0$.*

*Proof.* Since $\frac{p}{q} \in \mathbb{Q}$, there exists $\ell \in \mathbb{R}$ and $\tilde{p}$, $\tilde{q} \in \mathbb{N}$, such that $p = \tilde{p}\ell$ and $q = \tilde{q}\ell$. For all $t \in [n]$, define sub-sections of $T(t)$ and $U(t)$ as

$$A_i(t) = \begin{cases} (T(t))_{q-i\ell}^{q-(i-1)\ell} & \text{if } 1 \leq i \leq \tilde{p}, \\ (U(t))_{q-(i-\tilde{p})\ell}^{q-(i-\tilde{p}-1)\ell} & \text{if } \tilde{p}+1 \leq i \leq 2\tilde{p}, \end{cases} \tag{4.41}$$

and $\boldsymbol{A}_i = \{A_i(t) : \ t \in [n]\}$ for $i \in [2\tilde{p}]$. Then by Lemma 4.2, for $i \in [2\tilde{p}]$ the following holds:

$$\begin{aligned} &H_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \\ &\geq H_{\mathcal{G}}(\boldsymbol{A}_i, \boldsymbol{A}_{i+1}, \cdots, \boldsymbol{A}_{i+q-1}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}), \end{aligned} \tag{4.42}$$

where we omit $no(\log \bar{P})$ for brevity, and implicitly use modulo-$2\tilde{p}$ arithmetic in the indices; e.g., $i_0 = i_{2\tilde{p}}$. Lemma 4.2 is applied in the following way. After removing the top-$\mu$ sub-section of $\boldsymbol{T}$ and top-$\nu$ sub-section of $\boldsymbol{U}$, we take the top-$p$ sub-section of the remaining $\boldsymbol{T}$ and $\boldsymbol{U}$, and evenly slice them into $\tilde{p}$ boxes, each of which has height $\ell$. The boxes in $\boldsymbol{T}$ are then indexed from top to bottom with 1 to $\tilde{p}$, and those in $\boldsymbol{U}$ are indexed likewise with $\tilde{p}+1$ to $2\tilde{p}$. Conditioned on the top-$\mu$ sub-section of $\boldsymbol{T}$ and the top-$\nu$ sub-section of $\boldsymbol{U}$, Lemma 4.2 implies that the entropy of $\boldsymbol{T} \boxplus_{\mathcal{G}} \boldsymbol{U}$ is no less than the joint entropy of the boxes whose indices are within a circular sliding window of size $\tilde{q}$. This can be verified with the box-stacking interpretation of Lemma 4.2. See Figure 4.10 for an illustration of the procedure above.

Adding up (4.42) for all $i \in [2\tilde{p}]$, we have

$$\begin{aligned} &2pH_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \\ &= \ell 2\tilde{p}H_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \end{aligned} \tag{4.43}$$

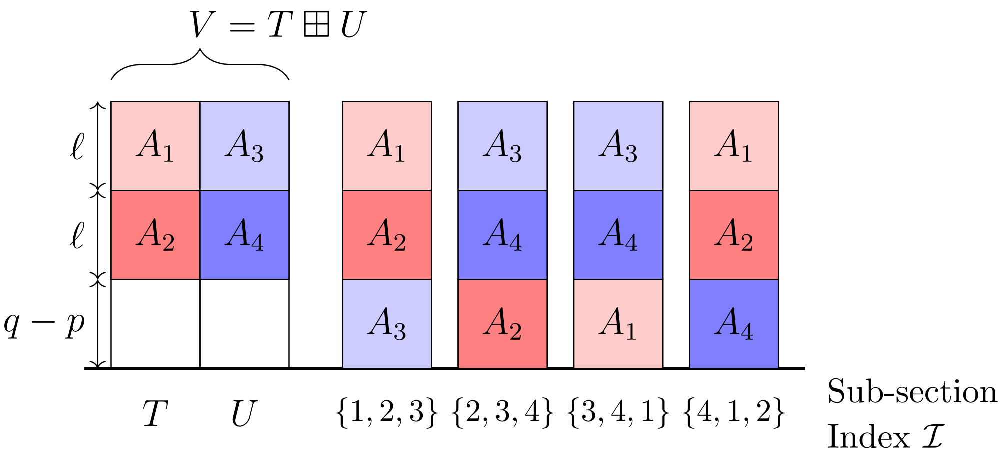


Figure 4.10: An illustration of how the sum-set inequality in Lemma 4.2 is applied to the proof of Lemma 4.7. In this case, $\mu = \nu = 0$, $p = 2$, and $q = 3$, which implies that $\ell = 1$, $\tilde{p} = 2$ and $\tilde{q} = 3$. The left most consecutive bars shows $\boldsymbol{V} = \boldsymbol{T} \boxplus_{\mathcal{G}} \boldsymbol{U}$ and some sub-sections of $\boldsymbol{T}$ and $\boldsymbol{U}$ taken by (4.41). The right four bars list all possible sub-section index sets obtained by a circular sliding window of size $q = 3$. Seeing that all sub-sections in each index set satisfy the box-stacking interpretation (All boxes can be stacked without elevating any above their original levels), Lemma 4.2 implies that $H_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}) \geq H_{\mathcal{G}}(\boldsymbol{A}_{\mathcal{I}}|\mathcal{W})$, where $\mathcal{I}$ is one of the sub-section index sets, and $\boldsymbol{A}_{\mathcal{I}} = \{A_i : \; i \in \mathcal{I}\}$. Summing up these inequalities and applying the submodularity of entropy, one can obtain (4.40).

$$\geq \ell \sum_{i=1}^{2\tilde{p}} H_{\mathcal{G}}(\boldsymbol{A}_i, \boldsymbol{A}_{i+1}, \cdots, \boldsymbol{A}_{i+\tilde{q}-1}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \tag{4.44}$$

$$\geq \ell\tilde{q} H_{\mathcal{G}}(\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_{2\tilde{p}}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \tag{4.45}$$

$$\geq q H_{\mathcal{G}}((\boldsymbol{T})^{p+\mu}, (\boldsymbol{U})^{p+\nu}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}). \tag{4.46}$$

Step (4.43) holds since $p = \tilde{p}\ell$. Step (4.45) follows from the submodularity[6] of entropy, and (4.46) holds because $q = \tilde{q}\ell$, and one can recover $(\boldsymbol{T})^{\mu+p}$ and $(\boldsymbol{U})^{\nu+p}$ from $\{\boldsymbol{A}_i : i \in [2\tilde{p}]\}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}$, and $\mathcal{G}$ within bounded distortion. □

[6] Let $\{X_1, X_2 \cdots, X_n\}$ be a set of random variables, then for $1 \leq k \leq n$, the submodularity of entropy implies:

$$\sum_{i=1}^{n} H(X_i, X_{i+1}, \cdots, X_{i+k-1}) \geq kH(X_1, X_2, \cdots, X_n), \tag{4.47}$$

where modulo-$n$ arithmetic is implicitly used in the indices. For example, if $k = 2, n = 3$, then $H(X_1, X_2) + H(X_2, X_3) + H(X_3, X_1) \geq 2H(X_1, X_2, X_3)$.

### 4.6.3 The Weighted-sum Bounds in Regime 1 and 2

We break down the proof into the following three lemmas. Throughout this section, we define $\mu = \beta - \alpha, \overline{\mu} = (\mu)^+$, $\underline{\mu} = (-\mu)^+$, and $\mathcal{W} = \{W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}\}$. Note that in both Regime 1 and 2, we have $\overline{\mu} < 1$. These three lemmas provides lower bounds on the entropy of the signals and codewords, which are expressed in terms of the model parameters. To make these bounds more accessible, after each of the following lemmas we explain their intuitions with an instance of ZIC in Figure 4.2, where $\alpha = 1$ and $\beta = \frac{8}{5}$, and demonstrate how they may be used. For this instance, $\mu = \overline{\mu} = \frac{3}{5}$, $\underline{\mu} = 0$, and $\mathcal{W} = \{W_1, (\boldsymbol{B})^{\frac{3}{5}}\}$.

**Lemma 4.8.** *For $\lambda \geq 1 - \mu$ and $\overline{\mu} \leq 1$, we have*

$$H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda}|\mathcal{W}) \geq nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}|\mathcal{W}) + no(\log \bar{P}). \tag{4.48}$$

**Remark 4.1.** *To gain an intuitive understanding of the significance of Lemma 4.8, let us see how it is useful for our example. For the ZIC in Figure 4.2 with $\alpha = 1$ and $\beta = \frac{8}{5}$, we choose $\lambda = \frac{8}{5}$ and plug it in Lemma 4.8 to obtain the following lower bound:*

$$\begin{aligned} & H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\frac{8}{5}}|W_1, (\boldsymbol{B})^{\frac{3}{5}}) \\ & \geq nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\frac{6}{5}}|W_1, (\boldsymbol{B})^{\frac{3}{5}}) + no(\log \bar{P}) && (4.49) \\ \Rightarrow & H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\frac{8}{5}}|W_1, (\boldsymbol{B})^{\frac{3}{5}}, (\overline{\boldsymbol{Y}}_1)^{\frac{6}{5}}) \geq nR_2 + no(\log \bar{P}) && (4.50) \\ \Rightarrow & H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\frac{8}{5}}|W_1, (\overline{\boldsymbol{Y}}_1)^{\frac{6}{5}}) \geq nR_2 + no(\log \bar{P}). && (4.51) \end{aligned}$$

*In* (4.50) *we used the general property that $H(X \mid Y) \geq H(X) - H(Y)$, and in* (4.51) *we used the fact that the top-*3/5 *sub-section of $\boldsymbol{B}$ is exposed in the top-*3/5 *sub-section of $\overline{\boldsymbol{Y}}_1$ which is already included in the top-*6/5 *sub-section of $\overline{\boldsymbol{Y}}_1$. Note that after the conditioning, what remains on the LHS of* (4.51) *is the bottom-*2/5 *sub-section of $\overline{\boldsymbol{Y}}_1$, and* (4.51) *tells us that its entropy should be at least as large as $d_2$ in the GDoF sense. This is a key insight that may* *be understood intuitively as follows. First, note that $d_2 \leq 2/5$, because out of the top-$1$ sub-section of $\boldsymbol{B}$ that is visible to Receiver $2$, the top-$3/5$ sub-section is also directly exposed to Receiver $1$ and cannot directly carry information about $W_2$ due to secrecy constraints. Now, the key intuition is that under finite precision CSIT, signals sent at higher levels cannot be prevented from impacting lower levels, and thus leaking information through them. This insight is affirmed by* (4.50)*, which shows that after the conditioning, the lowest $2/5$ levels of $\overline{\boldsymbol{Y}}_1$ must still contain at least as much entropy (essentially due to jamming noise) as $W_2$, otherwise the impact of $W_2$ on lower digits of $\overline{\boldsymbol{Y}}_1$ would reveal something about $W_2$.*

*Proof of Lemma 4.8.*

$$
\begin{aligned}
&H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda}|\mathcal{W}) \\
&= H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-\overline{\mu}} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}|\mathcal{W}) + no(\log \bar{P}) && (4.52)\\
&\geq H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}|\mathcal{W}) + no(\log \bar{P}) && (4.53)\\
&= H_{\mathcal{G}}(W_2|\mathcal{W}) + H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}})|\mathcal{W}, W_2) \\
&\qquad - H_{\mathcal{G}}(W_2|\mathcal{W}, (\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}) + no(\log \bar{P}) && (4.54)\\
&= H(W_2) + H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}|\mathcal{W}, W_2) + no(\log \bar{P}) && (4.55)\\
&\geq nR_2 + H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-1+\mu}|\mathcal{W}, W_2) + no(\log \bar{P}) && (4.56)\\
&= nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}|\mathcal{W}, W_2) + no(\log \bar{P}) && (4.57)\\
&= nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}|\mathcal{W}) + no(\log \bar{P}). && (4.58)
\end{aligned}
$$

First, equality (4.52) holds because by Lemma 4.6 one can recover $(\boldsymbol{A})^{\lambda-\overline{\mu}} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}$ from $(\overline{\boldsymbol{Y}}_1)^{\lambda}$ within bounded distortion. Then we apply Lemma 4.5 to obtain (4.53), and apply the chain rule to obtain (4.54). Equality (4.55) holds for the following reasons: (a) equality (4.30) implies the first entropy term; (b) the last entropy term is of order $no(\log \bar{P})$ is because, from $(\boldsymbol{A})^{\underline{\mu}}$ and $(\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}$, by Lemma 4.6 one can recover $(\boldsymbol{B})^{1}$ within bounded distortion, which one can decode for $W_2$. Then we apply $nR_2 = H(W_2)$ and

Lemma 4.5 to obtain (4.56). Note that Lemma 4.5 is applicable because in Regimes 1 and 2, $1-\mu = 1+\alpha-\beta \geq (\alpha-\beta)^+ = \underline{\mu}$. Equality (4.57) holds because by Lemma 4.6, $(\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}$ can be recovered from $(\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-1+\mu}$ within bounded distortion. Finally, we arrive at (4.58) due to (4.29). □

In the next lemma, we show that the part of codeword $\boldsymbol{A}$ corresponding to the same power levels as the part of $\boldsymbol{B}$ carrying $W_2$ has entropy no less than $H(W_2) = nR_2$. Intuitively, this must be so because $W_2$ needs to be hidden from Receiver 1, and for this the 'jamming signal' must be at least as big as $W_2$.

**Lemma 4.9.**

$$H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}|\mathcal{W}, (\boldsymbol{B})^1) \geq nR_2 + no(\log \bar{P}). \tag{4.59}$$

**Remark 4.2.** *For the ZIC in Figure 4.2 with $\alpha = 1$ and $\beta = \frac{8}{5}$, Lemma 4.9 becomes*

$$H_{\mathcal{G}}((\boldsymbol{A})^{\frac{2}{5}}|W_1, (\boldsymbol{B})^1) \geq nR_2 + no(\log \bar{P}). \tag{4.60}$$

*This inequality suggests that, after removing $W_1$ and $(\boldsymbol{B})^1$, the entropy of $(\boldsymbol{A})^{\frac{2}{5}}$, which is the sub-section of $\boldsymbol{A}$ sitting at the same level as $(\boldsymbol{B})^1$, should be at least $nR_2 = H(W_2)$ in the GDoF sense. This is a direct consequence of (4.29), because intuitively, if the signal in $(\boldsymbol{A})^{\frac{2}{5}}$ contains less than $W_2$ in entropy, there is no way to fully hide $W_2$ away and keep it secret. This is illustrated in Figure 4.11, where $(\boldsymbol{A})^{\frac{2}{5}}$ contains a jamming signal of full entropy.*

*Proof of Lemma 4.9.*

$$\begin{aligned}
&H_{\mathcal{G}}((\boldsymbol{B})^1|\mathcal{W}) \\
&\leq H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{1+\underline{\mu}}|\mathcal{W}) + no(\log \bar{P}) && (4.61) \\
&= H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{1+\underline{\mu}}|\mathcal{W}, W_2) + no(\log \bar{P}) && (4.62)
\end{aligned}$$

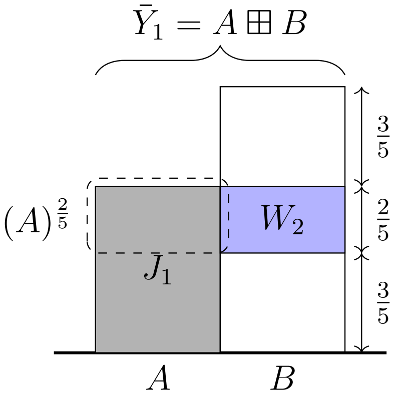


Figure 4.11: An illustration for Lemma 4.9. $\bar{Y}_1$ is the output of the ZIC in Figure 4.2 with $(\alpha, \beta) = (1, \frac{8}{5})$, and contains a scheme achieving $(d_1, d_2) = (0, \frac{2}{5})$.

$$\leq H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}, (\boldsymbol{B})^1 | \mathcal{W}, W_2) + no(\log \bar{P}) \tag{4.63}$$

$$= H_{\mathcal{G}}((\boldsymbol{B})^1 | \mathcal{W}, W_2) + H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu} | \mathcal{W}, W_2, (\boldsymbol{B})^1) + no(\log \bar{P}) \tag{4.64}$$

$$\leq H_{\mathcal{G}}((\boldsymbol{B})^1 | \mathcal{W}, W_2) + H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu} | \mathcal{W}, (\boldsymbol{B})^1) + no(\log \bar{P}). \tag{4.65}$$

First, we apply Lemma 4.5 to obtain inequality (4.61). Note that $(\overline{\boldsymbol{Y}}_1)^{1+\underline{\mu}}$ is well-defined because $\beta > 1$ in Regime 1 and 2, and implies that $\max\{\alpha, \beta\} > 1 + \underline{\mu}$. Equality (4.62) holds due to (4.29). Inequality (4.63) is true because $\mu = \beta - \alpha < 1$ in Regime 1 and 2, and $(\overline{\boldsymbol{Y}}_1)^{1+\underline{\mu}}$ can be recovered by Lemma 4.6 within bounded distortion from $(\boldsymbol{A})^{1-\mu} \boxplus (\boldsymbol{B})^1$, which is a function of $(\boldsymbol{A})^{1-\mu}$ and $(\boldsymbol{B})^1$. Then we apply the chain rule to obtain (4.64), and apply the fact that conditioning reduces entropy to obtain (4.65).

By swapping terms in (4.65), we have

$$H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu} | \mathcal{W}, (\boldsymbol{B})^1)$$

$$\geq H_{\mathcal{G}}((\boldsymbol{B})^1 | \mathcal{W}) - H_{\mathcal{G}}((\boldsymbol{B})^1 | \mathcal{W}, W_2) + no(\log \bar{P}) \tag{4.66}$$

$$= I_{\mathcal{G}}((\boldsymbol{B})^1; W_2 | \mathcal{W}) + no(\log \bar{P}) \tag{4.67}$$

$$= I_{\mathcal{G}}((\boldsymbol{B})^1, \mathcal{W}; W_2) - I(\mathcal{W}; W_2) + no(\log \bar{P}) \tag{4.68}$$

$$= I_{\mathcal{G}}((\boldsymbol{B})^1, \mathcal{W}; W_2) + no(\log \bar{P}) \tag{4.69}$$

$$\geq I_{\mathcal{G}}((\boldsymbol{B})^1; W_2) + no(\log \bar{P}) \tag{4.70}$$

$$\geq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2; W_2) + no(\log \bar{P}) \tag{4.71}$$

$$\geq nR_2 + no(\log \bar{P}). \tag{4.72}$$

We apply the definition of mutual information to obtain (4.67), the chain rule to obtain (4.68), and (4.30) to obtain (4.69). Then we remove $\mathcal{W}$ to obtain (4.70). Finally, we apply data processing inequality to obtain (4.71), and Fano's inequality to obtain (4.72). □

The third lemma is a lower bound for the entropy $H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|\mathcal{W})$.

**Lemma 4.10.** *For $\overline{\mu} < 1$, we have*

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|\mathcal{W}) \geq \frac{\min\{\beta, \alpha\}}{1-\overline{\mu}} nR_2 + no(\log \bar{P}). \tag{4.73}$$

**Remark 4.3.** *With $\alpha = 1$ and $\beta = \frac{8}{5}$, Lemma 4.10 becomes*

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_1, (\boldsymbol{B})^{\frac{3}{5}}) \geq \frac{5}{2} nR_2 + no(\log \bar{P}). \tag{4.74}$$

*Figure 4.11 provides an intuition of this lower bound. But instead of resorting to the illustration only, we provide a sketch of its proof as follows. First we apply (4.49) to the left-hand side of (4.74).*

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_1, (\boldsymbol{B})^{\frac{3}{5}})$$

$$\geq nR_2 + H_{\mathcal{G}}\left((\overline{\boldsymbol{Y}}_1)^{\frac{6}{5}}|W_1, (\boldsymbol{B})^{\frac{3}{5}}\right) + no(\log \bar{P}) \tag{4.75}$$

$$\geq nR_2 + \frac{3}{4} H_{\mathcal{G}}\left((\boldsymbol{A})^{\frac{2}{5}}, (\boldsymbol{B})^1|W_1, (\boldsymbol{B})^{\frac{3}{5}}\right) + no(\log \bar{P}) \tag{4.76}$$

$$= nR_2 + \frac{3}{4}\Big[H_{\mathcal{G}}\left((\boldsymbol{A})^{\frac{2}{5}}|W_1, (\boldsymbol{B})^1\right) + H_{\mathcal{G}}\left((\boldsymbol{B})^1|W_1, (\boldsymbol{B})^{\frac{3}{5}}\right)\Big] + no(\log \bar{P}) \tag{4.77}$$

$$\geq \frac{5}{2} nR_2 + no(\log \bar{P}). \tag{4.78}$$

*To obtain (4.76), we apply Lemma 4.7 by plugging in* $p = 2, q = 3, \mu = 0, \nu = \frac{3}{5}$ *and* $\mathcal{W} = W_1$ *therein. Equation (4.77) follows by the chain rule, and the fact that* $(\boldsymbol{B})^{\frac{3}{5}}$ *can be obtained from* $(\boldsymbol{B})^1$*. Finally, we arrive at (4.78) by bounding the first entropy term in (4.77) from below by* $nR_2$ *with (4.60), and bounding the second from below with (4.30). Note that the arguments above are a mere sketch of proof. We relegate the missing details, as well as the continuity argument when* $\alpha$ *or* $\beta$ *is irrational, to the formal proof of Lemma 4.10.*

*Proof of Lemma 4.10.* Let $\min\{\beta, \alpha\} = k(1 - \overline{\mu}) + \gamma$, where $k$ is a non-negative integer, and $\gamma$ satisfies either $\gamma = 0$ or $1 - \overline{\mu} < \gamma < 2(1 - \overline{\mu})$.[7] As an intermediate result, we claim that

$$H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\gamma+|\mu|}|\mathcal{W}) \geq \frac{\gamma}{1-\overline{\mu}} nR_2 + no(\log \bar{P}). \tag{4.79}$$

The inequality is trivial when $\gamma = 0$. If $\gamma \neq 0$, we can find a non-decreasing sequence $\{r_i\}$ with $r_i \in \mathbb{Q}$ and $\lim_{i\to\infty} r_i = \gamma$, and a non-increasing sequence $\{m_i\}$ with $m_i \in \mathbb{Q}$ and $\lim_{i\to\infty} m_i = 1 - \overline{\mu}$.[8] Let $N = \min\left\{i \middle| \frac{m_i}{r_i} < 1\right\}$. Such $N$ exists, because as $i \to \infty$, we have $r_i \to \gamma$, $m_i \to 1 - \overline{\mu}$, and $\frac{1}{2} < \frac{1-\overline{\mu}}{\gamma} < 1$.

For $i \geq N$, we have

$$H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\gamma+|\mu|}|\mathcal{W}) \tag{4.80}$$
$$\geq H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{r_i+|\mu|}|\mathcal{W}) + no(\log \bar{P}) \tag{4.81}$$
$$= \frac{1}{2m_i}\left(2m_i H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{r_i+|\mu|}|\mathcal{W})\right) + no(\log \bar{P}) \tag{4.82}$$
$$\geq \frac{r_i}{2m_i} H_{\mathcal{G}}((\boldsymbol{A})^{m_i+\underline{\mu}}, (\boldsymbol{B})^{m_i+\overline{\mu}}|\mathcal{W}) + no(\log \bar{P}) \tag{4.83}$$

[7] The existence of such $k$ and $\gamma$ can be shown as follows. In Regime 1, since $\beta > 1$, we can find $k, \gamma$, where either $\gamma = 0$ or $1 < \gamma < 2$, such that $\beta = k + \gamma$. On the other hand, in Regime 2, since $\alpha > 1 + \alpha - \beta$, we can find $k, \gamma$ such that $\alpha = k(1 + \alpha - \beta) + \gamma$ with either $\gamma = 0$ or $1 + \alpha - \beta < \gamma < 2(1 + \alpha - \beta)$.

[8] Such a non-increasing sequence $\{m_i\}$ and a non-increasing sequence $\{r_i\}$ can be constructed by the decimal representation of $1 - \overline{\mu}$ and $\gamma$, respectively. For example, let $0.\mu_1\mu_2\cdots\mu_i$ be the $i-$decimal of $1 - \overline{\mu}$, where $\mu_j \in \{0, 1, \cdots, 9\}$ for $j \in [i]$. We may let $m_i = 0.\mu_1\mu_2\cdots\mu_i + 10^{-i} = \left(\lfloor(1 - \overline{\mu}) \times 10^i\rfloor + 1\right) \times 10^{-i}$, which is a rational number no less than $1 - \overline{\mu}$. On the other hand, let $0.\gamma_1\gamma_2\cdots\gamma_i$ be the $i-$decimal of $\gamma$, where $\gamma_j \in \{0, 1, \cdots, 9\}$ for $j \in [i]$. We may let $r_i = 0.\gamma_1\gamma_2\cdots\gamma_i = \lfloor\gamma \times 10^i\rfloor \times 10^{-i}$, which is a rational number no greater than $\gamma$.

$$\geq \frac{r_i}{2m_i} H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}, (\boldsymbol{B})^{1}|\mathcal{W}) + no(\log \bar{P}) \tag{4.84}$$

$$= \frac{r_i}{2m_i} \Big[ H_{\mathcal{G}}((\boldsymbol{B})^{1}|\mathcal{W}) + H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}|\mathcal{W}, (\boldsymbol{B})^{1}) \Big] + no(\log \bar{P}) \tag{4.85}$$

$$\geq \frac{r_i}{2m_i} \Big[ H_{\mathcal{G}}(W_2|\mathcal{W}) + H_{\mathcal{G}}((\boldsymbol{B})^{1}|\mathcal{W}, W_2) - H_{\mathcal{G}}(W_2|\mathcal{W}, (\boldsymbol{B})^{1}) + nR_2 \Big] + no(\log \bar{P}) \tag{4.86}$$

$$\geq \frac{r_i}{m_i} nR_2 + no(\log \bar{P}). \tag{4.87}$$

Inequality (4.81) holds because of Lemma 4.5 and the fact that $r_i \leq \gamma$. Then we multiply and divide the entropy term by $2m_i$ to get (4.82), and apply[9] Lemma 4.7 to obtain (4.83). Inequality (4.84) holds because of Lemma 4.5 and the fact that $m_i + \underline{\mu} \geq 1 - \overline{\mu} + \underline{\mu} = 1 - \mu$, and $m_i + \overline{\mu} \geq 1$. Next we apply the chain rule to get (4.85), and apply the chain rule and Lemma 4.9 to get (4.86). Equality (4.87) follows from (4.86) due to the following reasons: (a) we apply (4.30) and $nR_2 = H(W_2)$ to the first entropy term; (b) the second entropy term is non-negative; and (c) $W_2$ can be decoded from $(\boldsymbol{B})^1$, which makes the third entropy term $no(\log \bar{P})$. Since inequality (4.87) is valid for all $i \geq N$, we have

$$H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\gamma+|\mu|}|\mathcal{W}) \geq \lim_{i\to\infty} \frac{r_i}{m_i} nR_2 + no(\log \bar{P}) = \frac{\gamma}{1-\overline{\mu}} nR_2 + no(\log \bar{P}). \tag{4.88}$$

Next, based on the intermediate result (4.79), we show the following lower bound.

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|\mathcal{W}) \geq knR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{|\mu|+\gamma}|\mathcal{W}) + no(\log \bar{P}). \tag{4.89}$$

This bound is reduced to (4.79) when $k = 0$ because of the following identity

$$\max\{\beta, \alpha\} = |\mu| + \min\{\beta, \alpha\} = |\mu| + k(1 - \overline{\mu}) + \gamma. \tag{4.90}$$

[9] To apply Lemma 4.7, we define $\boldsymbol{T} = (\boldsymbol{A})^{r_i+\underline{\mu}} \in \mathcal{X}_{r_i+\underline{\mu}}, \boldsymbol{U} = (\boldsymbol{B})^{r_i+\overline{\mu}} \in \mathcal{X}_{r_i+\overline{\mu}}, p = m_i$, and $q = r_i$. This leads to $\boldsymbol{V} = (\boldsymbol{A})^{r_i+\underline{\mu}} \boxplus (\boldsymbol{B})^{r_i+\overline{\mu}}$, which by Lemma 4.6 can be recovered from $(\overline{\boldsymbol{Y}}_1)^{r_i+|\mu|}$ within bounded distortion.

On the other hand, when $k \geq 1$, we apply Lemma 4.8 and omit $no(\log \bar{P})$ for brevity as follows.

$$
\begin{aligned}
& H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|\mathcal{W}) \\
& \geq nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\max\{\beta,\alpha\}-(1-\overline{\mu})}|\mathcal{W}) && (4.91) \\
& \geq 2nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\max\{\beta,\alpha\}-2(1-\overline{\mu})}|\mathcal{W}) && (4.92) \\
& \qquad\qquad\qquad \vdots \\
& \geq knR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\max\{\beta,\alpha\}-k(1-\overline{\mu})}|\mathcal{W}) && (4.93) \\
& = knR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{|\mu|+\gamma}|\mathcal{W}). && (4.94)
\end{aligned}
$$

Lemma 4.8 can be applied to (4.91) – (4.93) because in both Regime 1 and 2, we have $\overline{\mu} < 1$ and $\max\{\alpha, \beta\} - (k-1)(1-\overline{\mu}) \geq 1 - \mu$.[10] Next we apply (4.90) to obtain (4.94).

Finally, we plug (4.79) into (4.89), and get

$$
\begin{aligned}
H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|\mathcal{W}) & \geq knR_2 + \frac{\gamma}{1-\overline{\mu}} nR_2 + no(\log \bar{P}) && (4.95) \\
& = \frac{\min\{\beta,\alpha\}}{1-\overline{\mu}} nR_2 + no(\log \bar{P}), && (4.96)
\end{aligned}
$$

where equality (4.96) holds by applying the identity $\min\{\beta, \alpha\} = k(1-\overline{\mu}) + \gamma$. □

To finish the proof of the weighted-sum bound, we start by applying Fano's inequality as follows.

$$
\begin{aligned}
& nR_1 \\
& \leq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1) + no(\log \bar{P}) && (4.97) \\
& \leq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1, (\boldsymbol{B})^{\overline{\mu}}; W_1) + no(\log \bar{P}) && (4.98)
\end{aligned}
$$

[10] This can be seen by the following. First by (4.90) we have $\max\{\alpha, \beta\} - (k-1)(1-\overline{\mu}) = 1 - \overline{\mu} + \gamma + |\mu| = 1 + \gamma + \underline{\mu}$. In Regime 1, we have $1 + \gamma + \underline{\mu} \geq 1 + \underline{\mu} = 1 - \mu$, while in Regime 2, we have $1 + \gamma + \underline{\mu} \geq 1 \geq 1 - \mu$.

$$= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\boldsymbol{B})^{\overline{\mu}}) + I_{\mathcal{G}}((\boldsymbol{B})^{\overline{\mu}}; W_1) + no(\log \bar{P}) \tag{4.99}$$

$$= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\boldsymbol{B})^{\overline{\mu}}) + I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_2)^{\overline{\mu}}; W_1) + no(\log \bar{P}) \tag{4.100}$$

$$= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\boldsymbol{B})^{\overline{\mu}}) + no(\log \bar{P}) \tag{4.101}$$

$$\leq H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | (\boldsymbol{B})^{\overline{\mu}}) - H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | \mathcal{W}) + no(\log \bar{P}) \tag{4.102}$$

$$\leq \alpha n \log \bar{P} - \frac{\min\{\beta, \alpha\}}{1 - \overline{\mu}} n R_2 + no(\log \bar{P}). \tag{4.103}$$

Inequality (4.98) holds because adding $(\boldsymbol{B})^{\overline{\mu}}$ does not hurt the mutual information. Then we apply the chain rule to get (4.99). Since $\overline{\mu} < 1$ in Regime 1 and 2, $(\boldsymbol{B})^{\overline{\mu}}$ can be converted into $(\overline{\boldsymbol{Y}}_2)^{\overline{\mu}}$ within bounded distortion by Lemma 4.6, and as a result we have (4.100). Equality (4.101) holds due to (4.27) and the secrecy constraint (4.4), and the fact that $\overline{\mu} < 1$. Then seeing that $\{(\boldsymbol{B})^{\overline{\mu}}\} \subset \mathcal{W}$, inequality (4.102) is obtained by applying the fact that conditioning reduces entropy. To obtain inequality (4.103), first we apply the uniform bound to the first entropy in (4.102) as follows:

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | (\boldsymbol{B})^{\overline{\mu}}) \leq H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)_0^{\alpha}) \leq \alpha n \log P + no(\log \bar{P}). \tag{4.104}$$

And then we apply Lemma 4.10 to the second entropy in (4.102). Note that Lemma 4.10 is applicable since $\overline{\mu} < 1$ in Regime 1 and 2.

Finally by applying the definition of GDoF, we get

$$d_1 + \frac{\min\{\beta, \alpha\}}{1 - \overline{\mu}} d_2 = \lim_{P \to \infty} \frac{R_1 + \frac{\min\{\beta,\alpha\}}{1-\overline{\mu}} R_2}{\frac{1}{2}\log P} \leq \alpha \tag{4.105}$$

$$\Longrightarrow \begin{cases} d_1 + \beta d_2 \leq \alpha & \text{if } \alpha > \beta \\ \frac{d_1}{\alpha} + \frac{d_2}{1+\alpha-\beta} \leq 1 & \text{if } \beta - 1 < \alpha \leq \beta \end{cases}. \tag{4.106}$$

Inequalities (4.106) are the desired weighted-sum bounds for the respective Regime 1 and 2. Thus, we complete the proof. □

## 4.7 Summary

Motivated by robustness concerns that are paramount in secure communications, in this chapter we study the robust GDoF of secure communication over a two user $Z$ interference channel. The combination of security, robustness and GDoF optimality makes this problem uniquely challenging relative to prior work, while the $Z$ channel setting limits the number of parameters sufficiently to allow a GDoF characterization for all parameter regimes. In the process we also explore the scope of sum-set inequalities based on Aligned Image principles that were recently introduced in [24], which involve joint entropies of various sub-sections of input signals. We found that these new sum-set inequalities, combined with sub-modularity properties of entropy, are sufficient to characterize the robust secure GDoF region of a $Z$ interference channel (as well as a further generalization to the corresponding broadcast channel setting). The result shows that the GDoF benefits of structured jamming, e.g., aggregate decoding and cancellation of jammed signals, are entirely lost under finite precision CSIT. The result reaffirms the hypothesis that random codes may be enough for approximate capacity characterizations under robust assumptions. Thus, while the fundamental limits of structured codes under ideal assumptions remain both practically fragile and theoretically intractable, there remains hope that continued advances in Aligned Images converse bounds may eventually place within reach a robust network information theory of wireless networks, based on the understanding of the fundamental limits of random codes.

# Chapter 5

# Conclusion

This dissertation explores different approaches to characterize the capacity of large wireless networks with high SNR asymptotoics under the robust assumption of channel information. We apply extremal analysis to characterize the benefit of transmitter cooperation, find sharp GDoF characterizations of secure networks in broadly larger parameter regimes, and show the fundamental fragility of structured codes in secure communications. These optimality results are based on the use of Aligned Image sum-set inequalities. The key contributions are summarized as follows.

- In chapter 2 we demonstrate the feasibility of an extremal netowrk theory by finding the extremal sum-GDoF gain that transmitter cooperation can bring to $K$ user interference channel in weak interference regimes, as a preliminary attempt to apply an extremal network theory. Taking treating interference as noise as the baseline for GDoF comparison, we find the extremal gain within the TIN and CTIN regime respectively as 1.5 and $2-\frac{1}{K}$, which is a constant with respect to $K$, while the extremal gain within the SLS regime is found to be $\Theta(\log_2 K)$, which grows logrithmatically with $K$.
- In chapter 3 we take another path to characterize the GDoF of large wireless networks

with an arbitrary number of users. With secrecy constraints added, we discover the largest parameter regimes known so far: the STIN regime for interference networks and the SLS regime for the broadcast networks. In both network settings, a secure version of TIN achieves the GDoF optimal.

- In chapter 4 we study the robustness of structured codes under finite precision CSIT with an instance of structured jamming based on lattice codes. We show that in a two user $Z$ secure interference channel, the structured jamming loses its GDoF benefit under finite precision CSIT. As a byproduct, the secure GDoF regions of the $Z$ channels are fully characterized.

**Open problems and Future Directions**

The results of extremal gain from transmitter cooperation open the door to a number of intriguing questions where extremal analysis could be useful to gain a deeper understanding of the benefits of transmitter cooperation. Some of them are listed as follows:

- Is it possible to achieve more than logarithmic GDoF gain by transmitter cooperation over TIN in a general weak interference regime where the only constraint is that the direct links are stronger than cross links?

- What is the maximum possible sum-GDoF gain of a $K$ user MISO BC over the corresponding $K$ user IC in the general weak interference regime? Or, even in the SLS-regime?

- Seeing that with the secrecy constraints the extremal gain in the STIN regime is unbounded while the extremal gain is 1 in the SLS regime, what are the parameter regimes lying between, such that the extremal gain shows interesting scaling behavior with $K$?

In general, it seems extremal analysis may be useful to gauge the potential benefits of a myriad of factors such as multiple antennas, power control, rate-splitting, space-time multiplexing, network coherence, robustness of CSIT and secrecy – all intriguing issues for which the current understanding is extremely limited.

While the extremal network theory points out a novel workaround to bypass the curse of dimensionality embedded in large wireless networks, another direction is to search for new schemes and develop new upper bounds. This direction might seem conventional, but it leads to new tools empowering us to go beyond the known parameter regimes and perform the extremal analysis in the known regimes as well. One example of new schemes that help the extremal analysis is the ones found in the study the SGDoF of the $K$ user MISO BC in the STIN regime. Such schemes, as exemplified in Figure 3.5, combine secret sharing and simple layered superposition (SLS). Their potential is yet to be explored and appears to be a promising ingredient for complete secure GDoF characterizations when we go beyond the SLS regime. Another example appears in [30], where we go beyond the $Z$ networks to the 3-to-1 interference networks. Under finite precision CSIT and secrecy, we identify a parameter regime where the problem of characterizing secure GDoF region is beyond the reach of the known Aligned Image sum-set inequalities. We conjecture a generalized class of sum-set inequalities which may help provide tight GDoF bounds. Its validity is currently an open problem.

# Bibliography

[1] H. H.-J. Liao, "Multiple access channels.," tech. rep., 1972.

[2] H. Weingarten, Y. Steinberg, and S. S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Transactions on Information Theory*, vol. 52, pp. 3936–3964, Sep. 2006.

[3] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[4] L. Zheng and D. Tse, "Diversity and multiplexing : A fundamental tradeoff in multiple-antenna channels," *IEEE Trans. on Info. Theory*, vol. 49, pp. 1073–1096, May 2003.

[5] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pp. 2065–2069, 2005.

[6] S. Jafar and M. Fakhereddin, "Degrees of freedom for the MIMO interference channel," *IEEE Transactions on Information Theory*, vol. 53, pp. 2637–2642, July 2007.

[7] R. Etkin, D. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5534–5562, 2008.

[8] A. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow: A deterministic approach," *IEEE Trans. on Inf. Theory*, vol. 57, pp. 1872–1905, 2011.

[9] S. Jafar and S. Shamai, "Degrees of freedom region for the MIMO X channel," *IEEE Trans. on Information Theory*, vol. 54, pp. 151–170, Jan. 2008.

[10] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of the $K$ user interference channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 3425–3441, Aug. 2008.

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

[12] S. Jafar, "Interference Alignment: A New Look at Signal Dimensions in a Communication Network," in *Foundations and Trends in Communication and Information Theory*, pp. 1–136, 2011.

[13] N. Jindal, "MIMO broadcast channels with finite-rate feedback," *IEEE Transactions on Information Theory*, vol. 52, no. 11, pp. 5045–5060, 2006.

[14] G. Caire, N. Jindal, and S. Shamai, "On the required accuracy of transmitter channel state information in multiple antenna broadcast channels," in *Proceedings of the Asilomar Conference on Signals, Systems and Computers*, 2007.

[15] C. Huang, S. A. Jafar, S. Shamai, and S. Vishwanath, "On Degrees of Freedom Region of MIMO Networks without Channel State Information at Transmitters," *IEEE Transactions on Information Theory*, pp. 849–857, Feb. 2012.

[16] C. S. Vaze and M. K. Varanasi, "The degree-of-freedom regions of MIMO broadcast, interference, and cognitive radio channels with no CSIT," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5354–5374, 2012.

[17] A. Lapidoth, S. Shamai, and M. Wigger, "On the capacity of fading MIMO broadcast channels with imperfect transmitter side-information," in *Proceedings of 43rd Annual Allerton Conference on Communications, Control and Computing*, Sep. 28-30, 2005.

[18] C. Hao, B. Rassouli, and B. Clerckx, "Degrees-of-freedom region of MISO-OFDMA broadcast channel with imperfect CSIT," *arXiv:1310.6669*, October 2013.

[19] H. Weingarten, S. Shamai, and G. Kramer, "On the compound MIMO broadcast channel," in *Proceedings of Annual Information Theory and Applications Workshop UCSD*, Jan 2007.

[20] A. Gholami Davoodi and S. A. Jafar, "Aligned image sets under channel uncertainty: Settling conjectures on the collapse of degrees of freedom under finite precision CSIT," *IEEE Trans. on Information Theory*, vol. 62, no. 10, pp. 5603–5618, 2016.

[21] R. Tandon, S. A. Jafar, S. Shamai, and H. V. Poor, "On the synergistic benefits of alternating CSIT for the MISO BC," *IEEE Transactions on Information Theory*, vol. 59, pp. 4106–4128, July 2013.

[22] N. Naderializadeh and A. S. Avestimehr, "Interference networks with no CSIT: Impact of topology," *IEEE Transactions on Information Theory*, vol. 61, no. 2, pp. 917–938, 2015.

[23] A. G. Davoodi and S. A. Jafar, "Network coherence time matters – Aligned image sets and the degrees of freedom of interference networks with finite precision CSIT and perfect CSIR," *IEEE Transactions on Information Theory*, vol. 64, pp. 7780–7791, Dec 2018.

[24] A. G. Davoodi and S. A. Jafar, "Sum-set inequalities from aligned image sets: Instruments for robust GDoF bounds," *IEEE Transactions on Information Theory*, vol. 66, no. 10, pp. 6458–6487, 2020.

[25] A. Gholami Davoodi and S. A. Jafar, "Generalized degrees of freedom of the symmetric $K$-user interference channel under finite precision CSIT," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6561–6572, 2017.

[26] A. Gholami Davoodi and S. Jafar, "Degrees of freedom region of the $(M, N_1, N_2)$ MIMO broadcast channel with partial CSIT: An application of sum-set inequalities based on aligned image sets," *IEEE Transactions on Information Theory*, vol. 66, no. 10, pp. 6256–6279, 2020.

[27] H. Joudeh and B. Clerckx, "On the separability of parallel MISO broadcast channels under partial CSIT: A degrees of freedom region perspective," *IEEE Transactions on Information Theory*, vol. 66, no. 7, pp. 4513–4529, 2020.

[28] J. Wang, B. Yuan, L. Huang, and S. A. Jafar, "Sum-GDoF of 2-user interference channel with limited cooperation under finite precision CSIT," *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 6999–7021, 2020.

[29] Y.-C. Chan and S. A. Jafar, "Secure GDoF of the $Z$-channel with finite precision CSIT: How robust are structured codes?," *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2410–2428, 2022.

[30] Y.-C. Chan and S. A. Jafar, "Exploring aligned-images bounds: Robust secure GDoF of 3-to-1 interference channel," in *ICC 2021 - IEEE International Conference on Communications*, pp. 1–6, 2021.

[31] A. Gholami Davoodi, B. Yuan, and S. A. Jafar, "GDoF region of the MISO BC: Bridging the gap between finite precision and perfect CSIT," *IEEE Transactions on Information Theory*, vol. 64, pp. 7208–7217, Nov. 2018.

[32] A. G. Davoodi and S. A. Jafar, "$K$-user symmetric $M \times N$ MIMO interference channel under finite precision CSIT: A GDoF perspective," *IEEE Transactions on Information Theory*, vol. 65, pp. 1126–1136, Feb. 2019.

[33] A. Gholami Davoodi and S. Jafar, "Aligned image sets and the generalized degrees of freedom of symmetric MIMO interference channel with partial CSIT," *IEEE Transactions on Information Theory*, vol. 65, pp. 406–417, Jan 2019.

[34] C. Geng, N. Naderializadeh, S. Avestimehr, and S. Jafar, "On the optimality of treating interference as noise," *IEEE Transactions on Information Theory*, vol. 61, pp. 1753 – 1767, April 2015.

[35] X. Yi and G. Caire, "Optimality of treating interference as noise: A combinatorial perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4654–4673, 2016.

[36] A. Gholami Davoodi and S. Jafar, "Optimality of simple layered superposition coding in the 3 user MISO BC with finite precision CSIT," *IEEE Transactions on Information Theory*, vol. 65, pp. 7181–7207, Nov 2019.

[37] H. Sun and S. A. Jafar, "On the optimality of treating interference as noise for $K$ user parallel Gaussian interference networks," *IEEE Transactions on Information Theory*, vol. 62, pp. 1911–1930, April, 2016.

[38] C. Geng, H. Sun, and S. Jafar, "On the optimality of treating interference as noise: General message sets," *IEEE Transactions on Information Theory*, vol. 61, pp. 3722–3736, July 2015.

[39] C. Geng and S. Jafar, "On the optimality of treating interference as noise: Compound interference networks," *IEEE Transactions on Information Theory*, vol. 62, pp. 4630–4653, Aug. 2016.

[40] S. Gherekhloo, A. Chaaban, and A. Sezgin, "Expanded GDoF-optimality regime of treating interference as noise in the $M \times 2$ X-channel," *IEEE Transactions on Information Theory*, vol. 63, pp. 355–376, Jan. 2017.

[41] S. Gherekhloo, A. Chaaban, C. Di, and A. Sezgin, "(Sub-)optimality of treating interference as noise in the cellular uplink with weak intererence," *IEEE Transactions on Information Theory*, vol. 62, pp. 322–356, Jan. 2016.

[42] C. Geng and S. A. Jafar, "Secure GDoF of $K$-user Gaussian interference channels: When secrecy incurs no penalty," *IEEE Communications Letters*, vol. 19, pp. 1287–1290, Aug 2015.

[43] X. Yi and H. Sun, "Opportunistic treating interference as noise," *arXiv preprint arXiv:1808.08926*, 2018.

[44] H. Joudeh and B. Clerckx, "On the optimality of treating inter-cell interference as noise in uplink cellular networks," *arXiv preprint arXiv:1809.03309*, 2018.

[45] H. Joudeh, X. Yi, and B. Clerckx, "On multi-cell uplink-downlink duality with treating inter-cell interference as noise," *arXiv preprint arXiv:1901.05747*, 2019.

[46] X. Yi, H. Sun, S. Jafar, and D. Gesbert, "TDMA is optimal for all-unicast DoF region of TIM if and only if topology is chordal bipartite," *IEEE Transactions on Information Theory*, vol. 64, pp. 2065 – 2076, March 2018.

[47] S. A. Jafar, "Topological interference management through index coding," *IEEE Transactions on Information Theory*, vol. 60, pp. "529–568", Jan. 2014.

[48] C. Suh and D. Tse, "Feedback capacity of the Gaussian interference channel to within 1.7075 bits: the symmetric case," *ArXiv:0901.3580*, vol. abs/0901.3580, 2009.

[49] T. Gou and S. A. Jafar, "Capacity of a class of symmetric SIMO Gaussian interference channels within O (1)," *IEEE Trans. on Information Theory*, vol. 57, pp. 1932–1958, April 2011.

[50] S. Rini, D. Tuninetti, and N. Devroye, "State of the cognitive interference channel: a new unified inner bound, and capacity to within 1.87 bits," *CoRR*, vol. abs/0910.3028, 2009.

[51] S. Karmakar and M. K. Varanasi, “Capacity of the MIMO interference channel to within a constant gap,” *ArXiv:1102.0267*, vol. abs/1102.0267, 2011.

[52] S. Avestimehr, A. Sezgin, and D. Tse, “Capacity of the two way relay channel within a constant gap,” *European Transactions on Telecommunications*, vol. 21, pp. 363 – 374, April 2010.

[53] R. Etkin and E. Ordentlich, “The degrees-of-freedom of the $K$-User Gaussian interference channel is discontinuous at rational channel coefficients,” *IEEE Trans. on Information Theory*, vol. 55, pp. 4932–4946, Nov. 2009.

[54] B. Clerckx, H. Joudeh, C. Hao, M. Dai, and B. Rassouli, “Rate splitting for MIMO wireless networks: A promising PHY-layer strategy for LTE evolution,” *IEEE Communications Magazine*, pp. 98–105, May 2016.

[55] B. Yuan and S. Jafar, “Elevated multiplexing and signal space partitioning in the 2 user MIMO IC with partial CSIT,” *IEEE Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2016.

[56] T. M. Cover, “Broadcast channels,” *IEEE Transactions on Information Theory*, vol. 18, pp. 2–14, Jan. 1972.

[57] V. Annapureddy and V. Veeravalli, “Gaussian interference networks: Sum capacity in the low interference regime and new outer bounds on the capacity region,” *IEEE Trans. on Information Theory*, pp. 3032–3050, July 2009.

[58] X. Shang, G. Kramer, and B. Chen, “A new outer bound and the noisy-interference sum-rate capacity for Gaussian interference channels,” *IEEE Transactions on Information Theory*, vol. 55, pp. 689–699, Feb. 2009.

[59] A. Motahari and A. Khandani, “Capacity bounds for the Gaussian interference channel,” *IEEE Transactions on Information Theory*, vol. 55, pp. 620–643, Feb. 2009.

[60] N. Naderializadeh and A. S. Avestimehr, “ITLinQ: A new approach for spectrum sharing in device-to-device communication systems,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1139–1151, 2014.

[61] X. Yi and G. Caire, “ITLinQ+: An improved spectrum sharing mechanism for device-to-device communications,” *49th Asilomar Conference on Signals, Systems and Computers*, pp. 1310 – 1314, 2015.

[62] Y. Chan, J. Wang, and S. A. Jafar, “Toward an extremal network theory – robust GDoF gain of transmitter cooperation over TIN,” *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3827–3845, 2020.

[63] A. Gholami Davoodi and S. A. Jafar, “Transmitter cooperation under finite precision CSIT: A GDoF perspective,” *IEEE Trans. on Information Theory*, vol. 63, no. 9, pp. 6020–6030, 2017.

[64] H. Joudeh and G. Caire, "Cellular networks with finite precision CSIT: GDoF optimality of multi-cell TIN and extremal gains of multi-cell cooperation," *IEEE Transactions on Information Theory*, pp. 1–1, 2021.

[65] J. Wang and S. A. Jafar, "Sum-GDoF of symmetric multi-hop interference channel under finite precision CSIT using aligned-images sum-set inequalities," *IEEE Transactions on Information Theory*, vol. 68, no. 7, pp. 4470–4490, 2022.

[66] Y.-C. Chan, P. Pezeshkpour, C. Geng, and S. A. Jafar, "The extremal GDoF gain of optimal versus binary power control in $K$ user interference networks is $\Theta(\sqrt{K})$," *arXiv e-prints*, p. arXiv:2205.02216, May 2022.

[67] H. Joudeh and B. Clerckx, "On the optimality of treating inter-cell interference as noise in uplink cellular networks," *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7208–7232, 2019.

[68] H. Joudeh, X. Yi, B. Clerckx, and G. Caire, "On the optimality of treating inter-cell interference as noise: Downlink cellular networks and uplink-downlink duality," *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 6939–6961, 2020.

[69] C. Geng and S. A. Jafar, "Power control by GDoF duality of treating interference as noise," *IEEE Communications Letters*, vol. 22, no. 2, pp. 244–247, 2018.

[70] C. Geng, H. Sun, and S. A. Jafar, "Multilevel topological interference management: A TIM-TIN perspective," *IEEE Transactions on Communications*, pp. 1–1, 2021.

[71] C. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, Oct 1949.

[72] A. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[73] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[74] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[75] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[76] H. D. Ty, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 56, pp. 5477–5487, Nov 2010.

[77] R. Liu and V. Poor, "Secrecy capacity region of a multiple antenna Gaussian broadcast channel with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, pp. 1235–1249, March 2009.

[78] Y. Liang and H. Poor, "Multiple access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, pp. 976–1002, March 2008.

[79] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, pp. 2083–2114, April 2011.

[80] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, pp. 2493–2507, June. 2008.

[81] Y. Liang, A. Somekh-Baruch, V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Transactions on Information Theory*, vol. 55, pp. 604–619, Feb. 2009.

[82] G. Bagherikaram, A. Motahari, and A. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Transactions on Information Theory*, vol. 59, pp. 2673–2682, 5 2013.

[83] J. Xu, Y. Cao, and B. Chen, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, pp. 2453–2469, June 2008.

[84] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, pp. 2735–2751, June 2008.

[85] E. Tekin and A. Yener, "The Gaussian multiple access wiretap channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 5747–5755, Dec. 2008.

[86] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, pp. 4529–4542, Oct. 2009.

[87] R. Yates, D. Tse, and Z. Li, "Secret communication over interference channels," *Proceedings of IEEE ISIT 2008.*

[88] R. Liu, T. Liu, H. Poor, and S. Shamai, "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 56, pp. 4215–4227, Sep. 2010.

[89] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messagess," *IEEE Transactions on Information Theory*, vol. 57, pp. 2730 – 2745, May 2011.

[90] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Transactions on Information Theory*, vol. 57, pp. 3323–3332, Jun. 2011.

[91] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Transactions on Information Theory*, vol. 60, pp. 3359–3378, June 2014.

[92] J. Xie and S. Ulukus, “Secure degrees of freedom of $K$-user Gaussian interference channels: A unified view,” *IEEE Transactions on Information Theory*, vol. 61, pp. 2647–2661, May 2015.

[93] T. Gou and S. A. Jafar, “On the secure degrees of freedom of wireless X networks,” in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 826–833, 2008.

[94] J. Chen, “Secure communication over interference channel: To jam or not to jam?,” *IEEE Transactions on Information Theory*, vol. 66, no. 5, pp. 2819–2841, 2020.

[95] X. He, A. Khisti, and A. Yener, “MIMO broadcast channel with an unknown eavesdropper: Secrecy degrees of freedom,” *IEEE Transactions on Communications*, vol. 62, no. 1, pp. 246–255, 2014.

[96] P. Mukherjee, J. Xie, and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT,” *IEEE Transactions on Information Theory*, vol. 63, pp. 1898–1922, Mar. 2017.

[97] S. Lashgari and A. S. Avestimehr, “Secrecy DoF of blind MIMOME wiretap channel with delayed CSIT,” *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 478–489, Feb 2018.

[98] S. Lee and A. Khisti, “The wiretapped diamond-relay channel,” *IEEE Transactions on Information Theory*, vol. 64, pp. 7194–7207, Nov 2018.

[99] J. Chen and C. Geng, “Optimal secure GDoF of symmetric gaussian wiretap channel with a helper,” *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2334–2352, 2021.

[100] J. Chen and F. Li, “Adding a helper can totally remove the secrecy constraints in a two-user interference channel,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3126–3139, 2019.

[101] Y. Liang, G. Kramer, and H. V. Poor, “Compound wiretap channels,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–12, 2009.

[102] G. Caire and S. Shamai, “On the achievable throughput of a multiantenna Gaussian broadcast channel,” *IEEE Transactions on Information Theory*, vol. 49, pp. 1691–1706, July 2003.

[103] G. Bresler, A. Parekh, and D. N. C. Tse, “The approximate capacity of the many-to-one and one-to-many Gaussian interference channels,” *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4566–4592, 2010.

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

[105] S. Jafar and S. Vishwanath, "Generalized degrees of freedom of the symmetric Gaussian $K$ user interference channel," *IEEE Transactions on Information Theory*, vol. 56, pp. 3297–3303, July 2010.

[106] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Transactions on Information Theory*, vol. 60, pp. 2121–2138, April 2014.

[107] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. on Information Theory*, vol. 60, pp. 3359–3378, June 2014.

[108] J. Xie and S. Ulukus, "Secure degrees of freedom of $K$-user Gaussian interference channels: A unified view," *IEEE Trans. on Information Theory*, vol. 61, pp. 2647–2661, May 2015.

[109] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Trans. on Information Theory*, vol. 63, pp. 1898–1922, March 2017.

[110] P. Mukherjee and S. Ulukus, "Secure degrees of freedom of the multiple access wiretap channel with multiple antennas," *IEEE Transactions on Information Theory*, vol. 64, pp. 2093–2103, March 2018.

[111] K. Banawan and S. Ulukus, "Secure degrees of freedom in networks with user misbehavior," *Entropy*, vol. 21, no. 10, 2019.

[112] J. Chen and C. Geng, "Optimal secure GDoF of symmetric Gaussian wiretap channel with a helper," *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2334–2352, 2021.

[113] J. Chen and F. Li, "Adding a helper can totally remove the secrecy constraints in a two-user interference channel," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 3126–3139, Dec 2019.

[114] F. Li and J. Chen, "Adding common randomness can remove the secrecy penalty in GDoF," *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2308–2333, 2021.

[115] D. A. Karpuk and A. Chorti, "Perfect secrecy in physical-layer network coding systems from structured interference," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1875–1887, 2016.

[116] K. Banawan and S. Ulukus, "Secure degrees of freedom region of static and time-varying Gaussian MIMO interference channel," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 444–461, 2019.

[117] P. Babaheidarian, S. Salimi, and P. Papadimitratos, "Towards Scalable Security in Interference Channels With Arbitrary Number of Users," *arXiv e-prints*, p. arXiv:2004.06588, Apr. 2020.

[118] Z. Wang, M. Xiao, M. Skoglund, and H. V. Poor, "Secrecy degrees of freedom of the two-user MISO broadcast channel with mixed CSIT," in *2015 IEEE Information Theory Workshop (ITW)*, pp. 1–5, 2015.

[119] C. Geng, R. Tandon, and S. A. Jafar, "On the symmetric 2-user deterministic interference channel with confidential messages," in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, Dec 2015.

[120] Zang Li, R. D. Yates, and W. Trappe, "Secrecy capacity region of a class of one-sided interference channel," in *2008 IEEE International Symposium on Information Theory*, pp. 379–383, July 2008.

[121] X. He and A. Yener, "A new outer bound for the Gaussian interference channel with confidential messages," in *2009 43rd Annual Conference on Information Sciences and Systems*, pp. 318–323, March 2009.

[122] R. Bustin, M. Vaezi, R. F. Schaefer, and H. V. Poor, "On the secrecy capacity of the Z-interference channel," in *24th International Zurich Seminar on Communications (IZS)*, ETH-Zürich, 2016.

[123] P. Mohapatra, C. R. Murthy, and J. Lee, "On the secrecy capacity region of the two-user symmetric Z interference channel with unidirectional transmitter cooperation," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 572–587, March 2017.

[124] S. Karmakar and A. Ghosh, "Secrecy capacity region of fading binary Z interference channel with statistical CSIT," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 848–857, April 2019.

[125] Y. Zhu and D. Guo, "Ergodic fading Z-interference channels without state information at transmitters," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2627–2647, 2011.

[126] A. Fayed, T. Khattab, and L. Lai, "Secret communication on the Z-channel with cooperative receivers," in *2016 50th Asilomar Conference on Signals, Systems and Computers*, pp. 909–914, Nov 2016.

[127] Jianwei Xie and S. Ulukus, "Secrecy games on the one-sided interference channel," in *2011 IEEE International Symposium on Information Theory Proceedings*, pp. 1245–1249, July 2011.

[128] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology — EUROCRYPT 2000*, pp. 351–368, Springer Berlin Heidelberg, 2000.

[129] Y.-C. Chan, C. Geng, and S. A. Jafar, "Robust optimality of secure TIN," *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3071–3082, 2022.

# Appendix A

# Appendix for Chapter 2

## A.1 Optimality of Cyclic Partition for Polyhedral TIN in SLS Regime

**Theorem A.1.** *If $[\alpha]_{K\times K} \in \mathcal{A}_{\text{SLS}}$, then for any subset of users, $S$, $S \subset [K]$, there exists a p-optimal cyclic partition of $S$.*

### A.1.1 Proof of Theorem A.1

Without loss of generality we will prove the lemma for $S = [K]$, since the same proof works for any $S \subset [K]$ as well. Let us start with arbitrary $[\alpha]_{K\times K}$, i.e., not necessarily in the SLS regime. The sum-GDoF value in the polyhedral region, $\mathcal{D}_{\Sigma,\text{P-TIN}}$ is the solution to the following linear program,

$$(LP_1) \qquad \mathcal{D}_\Sigma = \max d_1 + d_2 + \cdots + d_K \tag{A.1}$$

$$\text{such that} \sum_{k\in\{\pi\}} d_k \le \sum_{k\in\{\pi\}} \alpha_{kk} - w(\pi), \quad \forall \pi \in \Pi, \tag{A.2}$$

$$d_k \ge 0, \quad \forall k \in [K], \tag{A.3}$$

and can be equivalently expressed by the following dual linear program.

$$(LP_2) \qquad \mathcal{D}_\Sigma = \min \sum_{\pi\in\Pi} \lambda_\pi \left( \sum_{k\in\{\pi\}} \alpha_{kk} - w(\pi) \right) \tag{A.4}$$

$$\text{such that} \sum_{\pi\in\Pi} \lambda_\pi 1(k \in \{\pi\}) \ge 1, \quad \forall k \in [K], \tag{A.5}$$

$$\lambda_\pi \ge 0, \quad \forall \pi \in \Pi, \tag{A.6}$$

where $1(\cdot)$ is the indicator function that returns the values 1 or 0 when the argument to the function is true or false, respectively.

For all $\pi \in \Pi$, let us define $\lambda^*_\pi$ as the optimizing values of $\lambda_\pi$ for $LP_2$. Let the corresponding optimal values for $LP_1$ be $d^*_k$ for all $k \in [K]$. Because a solution must exist, by the strong-duality of linear programming, the optimal $D_\Sigma$ for $LP_2$ is the same as the optimal $D_\Sigma$ for $LP_1$. Therefore, the following conditions are implied.

$$D_\Sigma = d^*_1 + d^*_2 + \cdots + d^*_K = \sum_{\pi\in\Pi} \lambda^*_\pi \left( \sum_{k\in\{\pi\}} \alpha_{kk} - w(\pi) \right), \tag{A.7}$$

$$\sum_{k\in\{\pi\}} \alpha_{kk} - w(\pi) \ge \sum_{k\in\{\pi\}} d^*_k, \qquad \forall \pi \in [\Pi], \tag{A.8}$$

$$\lambda^*_\pi \ge 0, \qquad \forall \pi \in [\Pi], \tag{A.9}$$

$$d^*_k \ge 0, \qquad \forall k \in [K]. \tag{A.10}$$

**Definition A.1** (Set of Active Cycles, $\Pi^*$)**.** *Based on the optimizing solution to $LP_2$, define*

$$\Pi^* = \{\pi \in \Pi : \lambda^*_\pi > 0\}. \tag{A.11}$$

This is called the set of active cycles, because the corresponding cycle bounds are active (i.e., tight) in the solution to $LP_2$ (see Lemma A.1).

**Definition A.2** (Set of Inactive Users, $\mathcal{K}_o$)**.** *Define* $\mathcal{K}_o \subset [K]$ *as the set of all users* $k$ *for which the inequality in* (A.5) *is strict. Thus,*

$$\mathcal{K}_o = \left\{ k \in [K] : \sum_{\pi \in \Pi} \lambda_\pi^* 1(k \in \{\pi\}) > 1 \right\}. \tag{A.12}$$

This is called the set of inactive users because for each of these users, we must have $d_k^* = 0$ (see Lemma A.1).

**Lemma A.1.**

$$\forall k \in \mathcal{K}_o \qquad \textit{we must have} \qquad d_k^* = 0, \tag{A.13}$$

$$\text{and } \forall \pi \in \Pi^* \qquad \textit{we must have} \qquad \sum_{k \in \{\pi\}} d_k^* = \sum_{k \in \{\pi\}} \alpha_{kk} - w(\pi). \tag{A.14}$$

Note that the conditions are simply complementary slackness conditions. Therefore Lemma A.1 holds for arbitrary channel parameters, i.e., even if $[\alpha]_{K \times K} \notin \mathcal{A}_{\text{SLS}}$. For the sake of completeness, a proof of Lemma A.1 appears in Appendix A.1.2.

Henceforth, let us restrict our attention to the SLS regime. In fact, let us define a *strict* SLS regime as

$$\bar{\mathcal{A}}_{\text{SLS}} = \{[\alpha]_{K \times K} \in \mathbb{R}_+^{K \times K} : \alpha_{ii} > \max(\alpha_{ij}, \alpha_{ki}, \alpha_{ik} + \alpha_{ji} - \alpha_{jk}),\ \forall i, j, k \in [K], i \notin \{j, k\}\}. \tag{A.15}$$

Note that the only difference between $\mathcal{A}_{\text{SLS}}$ and $\bar{\mathcal{A}}_{\text{SLS}}$ is that the defining inequalities in the latter are all strict inequalities. Note that all $\alpha_{ii}$ and $\delta_{ij}$ are strictly positive in the strict SLS regime. Following the same reasoning as the proof of Lemma A.3, in the strict SLS regime, for distinct $i, j, k \in [K]$, we must have

$$[\alpha]_{K\times K} \in \bar{\mathcal{A}}_{\text{SLS}} \qquad \Longrightarrow \qquad \delta_{ki} + \delta_{ij} > \delta_{kj}. \tag{A.16}$$

Note that the inequality is strict here as well. This is important for the proof.

We will first prove Theorem A.1 for the strict SLS regime and later use a continuity argument (identical to the continuity argument in the last paragraph of the proof of Theorem 3 in [37]) to show that the result holds even when the inequalities are relaxed to include equalities. The shell of the proof is identical to the proof of Theorem 3 in [37]. The main step that connects the two proofs is Lemma A.2.

Now define the following linear program.

$$(LP_3) \qquad \mathcal{D}_\Sigma = \min \sum_{\pi\in\Pi} \lambda_\pi \left( \sum_{k\in\{\pi\}} \alpha_{kk} - w(\pi) \right) \tag{A.17}$$

$$\text{such that} \sum_{\pi\in\Pi} \lambda_\pi 1(k \in \{\pi\}) = 1, \quad \forall k \in [K], \tag{A.18}$$

$$\lambda_\pi \geq 0, \quad \forall \pi \in \Pi. \tag{A.19}$$

Note that the only difference between $LP_2$ and $LP_3$ is that the inequality in (A.5) has been replaced with the equality in (A.18). The following lemma is the most critical part of the proof, as it shows that this change does not matter in the strict SLS regime, thereby reducing the problem to another problem that is already solved in [37].

**Lemma A.2.**

$$[\alpha]_{K\times K} \in \bar{\mathcal{A}}_{SLS} \qquad \Longrightarrow \qquad LP_2 \equiv LP_3. \tag{A.20}$$

The proof of Lemma A.2 appears in Appendix A.1.3.

Following Lemma A.2, $LP_3$ is identical to the $LP_3$ in [37] and the rest of the proof is identical to the proof of Theorem 3 in [37]. Thus, the proof of Theorem A.1 is complete. □

*Remark: Note that Lemma A.2 does not follow from [37]. Only after Lemma A.2 do the two proofs become identical. In [37], the equivalence of $LP_2$ and $LP_3$ is proved for a strict TIN regime. However, that proof does not hold in the strict SLS regime, and this distinction is quite important. In both cases (strict TIN regime and the strict SLS regime), we need to prove that all the constraints in* (A.5) *are tight. In the strict TIN regime, [37] accomplishes this by first proving that all $d_i^*$ that optimize the sum-GDoF must be strictly positive, so that it follows from complementary slackness that the constraints in* (A.5) *must be tight. However, in the strict SLS regime, unfortunately it is not true that all $d_i^*$* must *be strictly positive. A simple counterexample is the two user IC with $\alpha_{11} = \alpha_{22} = 1, \alpha_{12} = \alpha_{21} = 1/2$ which is in the strict SLS regime but not the strict TIN regime, and has $\mathcal{D}_{\Sigma,\text{TINA}} = 1$ which can be achieved with $(d_1^*, d_2^*) = (1, 0)$. Therefore, Lemma A.2 in the strict SLS regime needs a different argument that proves directly that all conditions in* (A.5) *are tight without relying on strict positivity of all the $d_i^*$ that optimize the sum-GDoF. Such an argument is presented in Appendix A.1.3.*

### A.1.2 Proof of Lemma A.1

$$0 = \sum_{\pi\in\Pi} \lambda_\pi^* \left( \sum_{k\in\{\pi\}} \alpha_{kk} - w(\pi) \right) - D_\Sigma \tag{A.21}$$

$$\geq \sum_{\pi\in\Pi} \lambda_\pi^* \left( \sum_{k\in\{\pi\}} d_k^* \right) - D_\Sigma \tag{A.22}$$

$$= \sum_{k\in[K]} \left( d_k^* \left( \sum_{\pi\in[\Pi]} \lambda_\pi^* 1(k \in \{\pi\}) \right) \right) - D_\Sigma \tag{A.23}$$

$$= \sum_{k\in[K]\backslash\mathcal{K}_o} d_k^* + \sum_{k\in\mathcal{K}_o} c_k d_k^* - D_\Sigma \tag{A.24}$$

$$= \sum_{k\in[K]\backslash\mathcal{K}_o} d_k^* + \sum_{k\in\mathcal{K}_o} c_k d_k^* - \sum_{k\in[K]} d_k^* \tag{A.25}$$

$$= \sum_{k\in\mathcal{K}_o} (c_k - 1) d_k^* \tag{A.26}$$

$$\geq 0, \tag{A.27}$$

because $c_k \triangleq \sum_{\pi\in\Pi} \lambda_\pi^* 1(k \in \pi) > 1$ for all $k \in \mathcal{K}_o$, and $d_k^* \geq 0$ for all $k \in [K]$. Since we started and ended with 0, all steps from (A.21) to (A.27) must be equalities. Thus, the proof of Lemma A.1 is complete. □

### A.1.3 Proof of Lemma A.2

We need to prove that the set $\mathcal{K}_o$ is empty. Suppose, on the contrary, that there exists $k_o \in \mathcal{K}_o$. According to Lemma A.1 the user $k_o$ must be inactive, i.e., $d_{k_o}^* = 0$. Let $\pi_o = (i_1 \to i_2 \to \cdots \to i_M \Lsh)$ be an active cycle that includes User $k_o$. Without loss of generality, suppose $k_o = i_M$. We will consider 3 cases.

1. **Case 1:** $(M > 2)$

   Suppose the length of the cycle is greater than 2. Since $\pi_o$ is an active cycle, according to Lemma A.1,

$$\sum_{k\in\{\pi_o\}} d_k^* = \sum_{k\in\{\pi_o\}} \alpha_{kk} - w(\pi_o) \tag{A.28}$$

$$\implies d_{i_1}^* + d_{i_2}^* + \cdots + d_{i_M}^* = \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-1} i_M} + \delta_{i_M i_1}. \tag{A.29}$$

But since $k_o \in \mathcal{K}_o$, according to Lemma A.1 we must have $d^*_{k_o} = d^*_{i_M} = 0$. Therefore,

$$d^*_{i_1} + d^*_{i_2} + \cdots + d^*_{i_{M-1}} = \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-2} i_{M-1}} + \delta_{i_{M-1} i_M} + \delta_{i_M i_1}. \quad \text{(A.30)}$$

But now consider the cycle $\pi' = (i_1 \to i_2 \cdots \to i_{M-1} \underline{\Lsh} )$. This may or may not be an active cycle. Regardless, the following bound must hold.

$$d^*_{i_1} + d^*_{i_2} + \cdots + d^*_{i_{M-1}} \leq \delta_{i_1 i_2} + \delta_{i_2 i_3} + \cdots + \delta_{i_{M-2} i_{M-1}} + \delta_{i_{M-1} i_1}. \quad \text{(A.31)}$$

Subtracting (A.30) from (A.31) we have

$$0 \leq \delta_{i_{M-1} i_1} - \delta_{i_{M-1} i_M} - \delta_{i_M i_1} \quad \text{(A.32)}$$

$$\implies \delta_{i_{M-1} i_M} + \delta_{i_M i_1} \leq \delta_{i_{M-1} i_1}. \quad \text{(A.33)}$$

But this is a contradiction because under strict SLS condition, according to (A.16),

$$\delta_{i_{M-1} i_M} + \delta_{i_M i_1} > \delta_{i_{M-1} i_1}. \quad \text{(A.34)}$$

2. **Case 2:** $(M = 1)$

   The length of the cycle, $M$, cannot be 1 because then Lemma A.1 would imply that the single user bound is active, i.e., $d^*_{k_o} = \alpha_{k_o k_o}$, but $\alpha_{k_o k_o} > 0$ in the strict SLS regime, so user $k_o$ must be active, i.e., we would have a contradiction. This leaves us with the only possibility, $M = 2$.

3. **Case 3:** $(M = 2)$

   Now suppose the length of the cycle $\pi_o$ is $M = 2$. Then we have

$$d^*_{i_1} + d^*_{i_M} = \delta_{i_1 i_M} + \delta_{i_M i_1}, \quad \text{(A.35)}$$

and since $k_o = i_M \in \mathcal{K}_o$ according to Lemma A.1 we have $d^*_{i_M} = 0$. Therefore,

$$d^*_{i_1} = \delta_{i_1 i_M} + \delta_{i_M i_1}. \tag{A.36}$$

Consider the following two subcases.

(a) **Subcase 1: $\pi_o$ is the only active bound that includes user $k_o$**

Then $\lambda_{\pi_o} > 1$. But this would mean that user $i_1$ also belongs to $\mathcal{K}_o$, because the sum of weights of active cycles that include user $i_1$ must be greater than 1 as well. However, if both user $i_1$ and user $i_M$ are in $\mathcal{K}_o$, then they must both be inactive. This is a contradiction, because $d^*_{i_1} + d^*_{i_M} = \delta_{i_1 i_M} + \delta_{i_M i_1} > 0$.

(b) **Subcase 2: There is another active bound, $\pi_1 \neq \pi_o$ that includes user $k_o$**

Now, $\pi_1$ must also have length $M = 2$ because, as we have already established, any other possibility leads to a contradiction. Since $\pi_1$ is different from $\pi_o$ it must involve a user other than $i_1$ in addition to user $i_M$. Let's call this user $i_2$. Then, proceeding similarly as in the case of $\pi_o$ we find that we must have

$$d^*_{i_2} = \delta_{i_2 i_M} + \delta_{i_M i_2}. \tag{A.37}$$

But we also know that the following bound must hold

$$d^*_{i_1} + d^*_{i_2} \leq \delta_{i_1 i_2} + \delta_{i_2 i_1}. \tag{A.38}$$

Subtracting (A.36) and (A.37) from (A.38) we have,

$$\begin{aligned} 0 &\leq \delta_{i_1 i_2} + \delta_{i_2 i_1} - \delta_{i_1 i_M} - \delta_{i_M i_1} - \delta_{i_2 i_M} - \delta_{i_M i_2} && \text{(A.39)} \\ &< (\delta_{i_1 i_M} + \delta_{i_M i_2}) + (\delta_{i_2 i_M} + \delta_{i_M i_1}) - \delta_{i_1 i_M} - \delta_{i_M i_1} - \delta_{i_2 i_M} - \delta_{i_M i_2} && \text{(A.40)} \\ &= 0, && \text{(A.41)} \end{aligned}$$

which is a contradiction. Note that we used (A.16) in (A.39).

Thus, we have a contradiction in every case, so there cannot be any such $k_o \in \mathcal{K}_o$, which implies that $\mathcal{K}_o$ is empty, and the proof is complete. □

## A.2 Other Useful Lemmas

### A.2.1 A condition on $\delta_{ij}$ in the SLS Regime

**Lemma A.3.** *For all $i, j, k \in [K]$,*

$$[\alpha]_{K\times K} \in \mathcal{A}_{SLS} \qquad \Longrightarrow \qquad \delta_{ki} + \delta_{ij} \geq \delta_{kj}. \tag{A.42}$$

### Proof of Lemma A.3

*Proof:* $\delta_{ki} + \delta_{ij} - \delta_{kj} = \alpha_{kk} - \alpha_{ik} + \alpha_{ii} - \alpha_{ji} - \alpha_{kk} + \alpha_{jk} = \alpha_{ii} + \alpha_{jk} - \alpha_{ik} - \alpha_{ji}$ which, by definition, is non-negative in $\mathcal{A}_{\text{SLS}}$. □

### A.2.2 Trivial cycles in the SLS Regime

**Lemma A.4.** *If $[\alpha]_{K\times K} \in \mathcal{A}_{\text{SLS}}$, then for every $\mathcal{S} \subset [K]$ there exists a p-optimal cyclic partition containing at most one trivial cycle.*

### Proof of Lemma A.4

Let $\{\pi_i\}_{i=1}^N$ be a p-optimal cyclic partition for $\mathcal{S}$. Suppose there is more than one trivial cycle in a p-optimal cyclic partition, we claim that they can be combined into one cycle, and the resulting partition is still p-optimal and free of trivial cycles. Let $\pi_1 = (i_1 \circlearrowleft), \pi_2 = (i_2 \circlearrowleft), \cdots, \pi_j = (i_j \circlearrowleft)$, $2 \leq j \leq N$, be all the trivial cycles in $\{\pi_i\}_{i=1}^N$. These trivial cycles can be combined into $\pi_{1,2,\cdots,j} = (\pi_1 \to \pi_2 \to \cdots \to \pi_j \circlearrowleft)$. Since $\pi_{1,2,\cdots,j}$ and all the other cycles are disjoint, $\{\pi_{1,2,\cdots,j}, \pi_{j+1}, \cdots, \pi_N\}$ is a cyclic partition. Moreover,

$$\Delta_{\pi_{1,2,\cdots,j}} = \sum_{m=1}^{j} \delta_{i_m,i_{m+1}} \leq \sum_{m=1}^{j} \alpha_{i_m i_m} = \sum_{m=1}^{j} \Delta_{\pi_m}, \tag{A.43}$$

where $\delta_{i_j,i_{j+1}} = \delta_{i_j,i_1}$. As a result, $\{\pi_{1,2,\cdots,j}, \pi_{j+1}, \cdots, \pi_N\}$ is also p-optimal, and contains no trivial cycles. □

### A.2.3 Combining Disjoint Cycles in the SLS Regime

**Lemma A.5.** *If $[\alpha]_{K\times K} \in \mathcal{A}_{\text{SLS}}$, $\pi_1, \pi_2, \cdots, \pi_n$ are $n > 1$ disjoint cycles, and*

$$\pi_{1,2,\cdots,n} = (\pi_1 \to \pi_2 \to \cdots \to \pi_n \circlearrowleft) \tag{A.44}$$

*is their combination, then*

$$\Delta_{\pi_{1,2,\cdots,n}} \leq \Delta_{\pi_1} + \Delta_{\pi_2} + \cdots + \Delta_{\pi_n} + \Delta_{\pi}, \tag{A.45}$$

*where $\pi = (\pi_1(1) \to \pi_2(1) \to \cdots \to \pi_n(1) \circlearrowleft)$.*

### Proof of Lemma A.5

Let us represent the cycles explicitly as

$$
\begin{aligned}
\pi_1 &= (i_{1,1} \to \cdots \to i_{1,m_1} \circlearrowleft), && \text{(A.46)}\\
\pi_2 &= (i_{2,1} \to \cdots \to i_{2,m_2} \circlearrowleft), && \text{(A.47)}\\
&\vdots \\
\pi_n &= (i_{n,1} \to \cdots \to i_{n,m_n} \circlearrowleft), && \text{(A.48)}\\
\pi_{1,2,\cdots,n} &= (i_{1,1} \to \cdots \to i_{1,m_1} \to i_{2,1} \to \cdots \to i_{2,m_2} \to \cdots \to i_{n,m_n} \circlearrowleft). && \text{(A.49)}
\end{aligned}
$$

Then we have

$$
\begin{aligned}
\Delta_{\pi_{1,2,\cdots,n}} &\leq (\Delta_{\pi_1} - \delta_{i_{1,m_1} i_{1,1}}) + (\Delta_{\pi_2} - \delta_{i_{2,m_2} i_{2,1}}) + \cdots + (\Delta_{\pi_n} - \delta_{i_{n,m_n} i_{n,1}}) \\
&\qquad + \delta_{i_{1,m_1} i_{2,1}} + \delta_{i_{2,m_2} i_{3,1}} + \cdots + \delta_{i_{n-1,m_{n-1}} i_{n,1}} + \delta_{i_{n,m_n} i_{1,1}} && \text{(A.50)}\\
&\leq \Delta_{\pi_1} + \delta_{i_{1,1} i_{2,1}} + \Delta_{\pi_2} + \delta_{i_{2,1} i_{3,1}} + \cdots + \Delta_{\pi_n} + \delta_{i_{n,1} i_{1,1}} && \text{(A.51)}\\
&= \Delta_{\pi_1} + \Delta_{\pi_2} + \cdots + \Delta_{\pi_n} + \Delta_{\pi}. && \text{(A.52)}
\end{aligned}
$$

Note that in (A.51) we used the fact that since $[\alpha]_{K \times K} \in \mathcal{A}_{\text{SLS}}$, we must have $\delta_{ij} + \delta_{jk} \geq \delta_{ik}$. □

### A.2.4 Connecting BC Bounds to Cycle Bounds in the SLS Regime

**Lemma A.6.** *In the SLS regime, for any cycle $\pi \in \Pi$,*

$$
\pi = (i_1 \to i_2 \to \cdots \to i_M \circlearrowleft), \tag{A.53}
$$

*we have the following bound on the sum-GDoF of the BC restricted to the users involved in the cycle* $\pi$*,*

$$\mathcal{D}_{\Sigma,\mathrm{BC}}(\{\pi\}) \leq \Delta_{\pi} + \alpha_{i_{m+1}i_m}, \tag{A.54}$$

*for any* $m \in [1:M]$*, with* $i_{M+1} = i_1$*. Furthermore,*

$$\mathcal{D}_{\Sigma,\mathrm{BC}}(\{\pi\}) \leq \Delta_{\pi} + \mathcal{D}_{\Sigma,\mathrm{TINA}}. \tag{A.55}$$

## Proof of Lemma A.6

Lemma A.6 follows directly as a special case of the results presented in [36]. For the sake of completeness we present a self-contained proof here. The proof is trivial for cycles of length $M = 1$, because the single-user bound implies $\mathcal{D}_{\Sigma,\mathrm{BC}}(\{\pi\}) \leq \alpha_{i_1i_1} \leq \Delta_{\pi} + \alpha_{i_1i_1}$. To prove Lemma A.6 for $M \geq 2$, let us give to each receiver $i_m, m \in [M]$, the messages $W_{[m+1:M]} \triangleq (W_{i_{m+1}}, W_{i_{m+2}}, \cdots, W_{i_M})$ as side information. This can only help, so the converse for the genie-aided channel is still a converse for the original channel. Note that no messages are given as side information to receiver $M$. Now, applying Fano's inequality within the deterministic model (Section 2.3.1) of the $K$ user MISO broadcast channel, and omitting $o(\log(P))$ terms we have,

$$\begin{aligned} TR_{i_1} &\leq I(W_{i_1}; (\bar{Y}_{i_1}(t))^{[1:T]} | \mathcal{G}, W_{[2:M]}) && \text{(A.56)}\\ &\leq H((\bar{Y}_{i_1}(t))^{[1:T]} | \mathcal{G}, W_{[2:M]}) && \text{(A.57)}\\ TR_{i_m} &\leq I(W_{i_m}; (\bar{Y}_{i_m}(t))^{[1:T]} | \mathcal{G}, W_{[m+1:M]}) && \text{(A.58)}\\ &= H((\bar{Y}_{i_m}(t))^{[1:T]} | \mathcal{G}, W_{[m+1:M]}) - H((\bar{Y}_{i_m}(t))^{[1:T]} | \mathcal{G}, W_{[m:M]}), \quad \forall m \in [2:M]. && \text{(A.59)} \end{aligned}$$

Adding these inequalities we get,

$$
\begin{aligned}
& T\sum_{m=1}^{M} R_{i_m} \\
\leq & \sum_{m=1}^{M-1} \left[H\left((\bar{Y}_{i_m}(t))^{[1:T]}|\mathcal{G}, W_{[m+1:M]}\right) - H\left((\bar{Y}_{i_{m+1}}(t))^{[1:T]}|\mathcal{G}, W_{[m+1:M]}\right)\right] + H((\bar{Y}_{i_M}(t))^{[1:T]}|\mathcal{G}) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(A.60)} \\
\leq & \sum_{m=1}^{M-1} \Big[\mathbb{H}_g\left([\alpha_{i_m1}, \alpha_{i_m2}, \cdots, \alpha_{i_mK}] \mid W_{[m+1:M]}\right) - \mathbb{H}_g\left([\alpha_{i_{m+1}1}, \alpha_{i_{m+1}2}, \cdots, \alpha_{i_{m+1}K}] \mid W_{[m+1:M]}\right)\Big] \\
& \qquad + \alpha_{i_Mi_M} T\log(P) && \text{(A.61)} \\
\leq & \sum_{m=1}^{M-1} \max_{\ell\in[K]} \left(\alpha_{i_m\ell} - \alpha_{i_{m+1}\ell}\right)^+ T\log(P) + \alpha_{i_Mi_M} T\log(P) && \text{(A.62)} \\
\leq & \sum_{m=1}^{M-1} \left(\alpha_{i_mi_m} - \alpha_{i_{m+1}i_m}\right) T\log(P) + \alpha_{i_Mi_M} T\log(P) && \text{(A.63)} \\
\leq & \sum_{m=1}^{M} \left(\alpha_{i_mi_m} - \alpha_{i_{m+1}i_m}\right) T\log(P) + \alpha_{i_1i_M} T\log(P) && \text{(A.64)} \\
= & \left(\sum_{m=1}^{M} \delta_{i_mi_{m+1}}\right) T\log(P) + \alpha_{i_1i_M} T\log(P) && \text{(A.65)} \\
= & (\Delta_\pi + \alpha_{i_1i_M}) T\log(P). && \text{(A.66)}
\end{aligned}
$$

Note that Lemma 2.1 was used in (A.62), and the definition of the SLS regime was used in (A.63) to conclude that

$$\alpha_{i_mi_m} - \alpha_{i_{m+1}i_m} \geq \alpha_{i_m,\ell} - \alpha_{i_{m+1},\ell}. \tag{A.67}$$

From (A.66) we have in the GDoF limit,

$$\mathcal{D}_{\Sigma,\mathrm{BC}}(\{\pi\}) \leq \Delta_\pi + \alpha_{i_1i_M} = \Delta_\pi + \alpha_{\pi(M+1)\pi(M)}. \tag{A.68}$$

Next, note that if we go through the same steps starting with a shifted representation of the cycle $\pi$, e.g.,

$$\pi^j = (\pi(1+j) \to \pi(2+j) \to \cdots \to \pi(M+j) \circlearrowleft), \tag{A.69}$$

then we obtain

$$\mathcal{D}_{\Sigma,\text{BC}}(\{\pi^j\}) = \mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq \Delta_\pi + \alpha_{\pi(M+1+j)\pi(M+j)}, \tag{A.70}$$

and in particular for $j = m + M$, we have the bound $\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq \Delta_\pi + \alpha_{\pi(m+1)\pi(m)} = \Delta_\pi + \alpha_{i_{m+1}i_m}$ for any $m \in [1:M]$, as desired. Finally, seeing that $\alpha_{ij} \leq \alpha_{ii} \leq \mathcal{D}_{\Sigma,\text{TINA}}(\{\pi\})$ for all $i, j \in \{\pi\}$ in the SLS regime, we have

$$\mathcal{D}_{\Sigma,\text{BC}}(\{\pi\}) \leq \Delta_\pi + \mathcal{D}_{\Sigma,\text{TINA}}(\{\pi\}). \tag{A.71}$$

This completes the proof of Lemma A.6. □

# Appendix B

# Appendix for Chapter 3

## B.1 Proof of Lemma 3.3

The proof of (3.23) is identical to the one in [20, Appendix] and is not repeated here. In the following we prove (3.24) only. Define for all $k, i \in [K]$ with the channel use index $t$ suppressed:

$$\begin{aligned}
\tilde{X}_i &= \bar{P}^{\alpha_{ii}} X_i, & \tilde{Y}_k &= \sum_{i=1}^{K} \left\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \left\lceil \tilde{X}_i \right\rceil \right\rceil, \\
\hat{X}_i &= \left\lceil \tilde{X}_i \right\rceil - \bar{X}_i, & \bar{\epsilon}_{ki} &= G_{ki} \bar{P}^{\alpha'_{ki}} \bar{X}_i - \left\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \bar{X}_i \right\rceil, \\
\Delta_k &= Y_k - \lceil Y_k \rceil, & \epsilon_{ki} &= \left\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \left\lceil \tilde{X}_i \right\rceil \right\rceil - G_{ki} \bar{P}^{\alpha'_{ki}} \left\lceil \tilde{X}_i \right\rceil, \\
\delta_i &= \left\lceil \tilde{X}_i \right\rceil - \tilde{X}_i, & \hat{\delta}_{ki} &= \bar{P}^{\alpha'_{ki}} \hat{X}_i - \left\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \right\rceil.
\end{aligned}$$

Now we proceed to the proof of (3.24).

$$I_{\mathcal{G}}(W_{-k}^{K}; \bar{Y}_k^n)$$

$$\begin{aligned}
&\leq I_{\mathcal{G}}(W_{-k}^K; \bar{Y}_k^n, \tilde{Y}_k^n, Y_k^n) && \text{(B.1)}\\
&\leq I_{\mathcal{G}}(W_{-k}^K; Y_k^n) + I_{\mathcal{G}}(W_{-k}^K; \tilde{Y}_k^n \mid Y_k^n) + I_{\mathcal{G}}(W_{-k}^K; \bar{Y}_k^n \mid Y_k^n, \tilde{Y}_k^n) && \text{(B.2)}\\
&\leq I_{\mathcal{G}}(W_{-k}^K; Y_k^n) + H_{\mathcal{G}}(\tilde{Y}_k^n \mid Y_k^n) + H_{\mathcal{G}}(\bar{Y}_k^n \mid Y_k^n, \tilde{Y}_k^n) && \text{(B.3)}\\
&\leq I_{\mathcal{G}}(W_{-k}^K; Y_k^n) + H_{\mathcal{G}}(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil) + H_{\mathcal{G}}(\bar{Y}_k^n \mid \tilde{Y}_k^n), && \text{(B.4)}
\end{aligned}$$

where (B.4) holds because $\lceil Y_k^n \rceil$ is a function of $Y_k^n$, and $H(X \mid f(Y)) \geq H(X \mid Y)$ for any function $f$ and random variables $X, Y$. Next we show that $H_{\mathcal{G}}(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil)$ and $H_{\mathcal{G}}(\bar{Y}_k^n \mid \tilde{Y}_k^n)$ in (B.4) is bounded above by $no(\log P)$. For $H_{\mathcal{G}}(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil)$, we note that for all $k \in [K]$, (with the channel use index $t$ suppressed,)

$$\tilde{Y}_k = \lceil Y_k \rceil + \Delta_k + \textstyle\sum_{i=1}^K \left( G_{ki} \bar{P}^{\alpha'_{ki}} \delta_i + \epsilon_{ki} \right), \tag{B.5}$$

and both $\tilde{Y}_k$ and $\lceil Y_k \rceil$ take integer values in their respective real and imaginary part. The sum of the truncation errors $\Delta_k + \sum_{i=1}^K G_{ki} \bar{P}^{\alpha'_{ki}} \delta_i + \epsilon_{ki}$ has its real and imaginary part taking an integer value in $(-1 - 2K\Delta, K(1 + 2\Delta))$. Therefore, we have

$$\begin{aligned}
H_{\mathcal{G}}(\tilde{Y}_k^n \mid \lceil Y_k^n \rceil) &\leq H(\{\Delta_k + \sum_{i=1}^K \left( G_{ki} \bar{P}^{\alpha'_{ki}} \delta_i + \epsilon_{ki} \right)\}_{t=1}^n) && \text{(B.6)}\\
&\leq n2 \log_2 \left( 2 \lceil K(1 + 2\Delta) \rceil \right) = no(\log P). && \text{(B.7)}
\end{aligned}$$

For $H_{\mathcal{G}}(\bar{Y}_k^n \mid \tilde{Y}_k^n)$ in (B.4), we note that for all $k \in [K]$, (with the channel use index $t$ supressed,)

$$\tilde{Y}_k = \bar{Y}_k + \sum_{i=1}^K G_{ki} \left\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \right\rceil + \sum_{i=1}^K \left( G_{ki} \hat{\delta}_{ki} + \bar{\epsilon}_{ki} + \epsilon_{ki} \right). \tag{B.8}$$

Since $\tilde{Y}_k, \tilde{Y}_k$ and $\lceil G_{ki} \bar{P}^{\alpha'_{ki}} \hat{X}_i \rceil$ take integer values in their respective real and imaginary part, the sum of the truncation errors $\sum_{i=1}^K G_{ki} \hat{\delta}_{ki} + \bar{\epsilon}_{ki} + \epsilon_{ki}$ must be an integer in $(-2K(1+$

$\Delta), 2K(1+\Delta))$ in its real and imaginary part. Therefore,

$$
\begin{aligned}
& H_{\mathcal{G}}(\bar{Y}_k^n \mid \tilde{Y}_k^n) \\
& \le \sum_{i=1}^{K} H_{\mathcal{G}}(\{\left\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \right\rceil\}_{t=1}^n) + H(\{\sum_{i=1}^{K} \left( G_{ki}\hat{\delta}_{ki} + \bar{\epsilon}_{ki} + \epsilon_{ki} \right)\}_{t=1}^n) && \text{(B.9)} \\
& \le \sum\nolimits_{i=1}^{K} H_{\mathcal{G}}(\{\hat{X}_i\}_{t=1}^n) + n2\log_2\left(2\left\lceil 2K(1+\Delta)\right\rceil\right), && \text{(B.10)}
\end{aligned}
$$

where (B.10) is because $\lceil \bar{P}^{\alpha'_{ki}} \hat{X}_i \rceil$ is a function of $\hat{X}_i$. Finally, seeing that $\mathbb{E}[|\lceil \tilde{X}_i \rceil|^2] \le \mathbb{E}[|2\tilde{X}_i|^2] \le 4P^{-\alpha_{ii}}$, we can further bound $H(\hat{X}_i(t))$ above with a constant by following the same procedure in [20, (130) – (149), Appendix]. Now $H_{\mathcal{G}}(\bar{Y}_k^n \mid \tilde{Y}_k^n)$ in (B.4) is bounded by $no(\log P)$, and (3.24) is therefore established.

## B.2 Proof of Theorem 3.2: Case $K = 2$

It suffices to show $SGDoF_{BC}^{f.p.}([\boldsymbol{\alpha}]) = \mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ for all $[\boldsymbol{\alpha}]$ in the STIN regime. From Theorem 3 this holds for all $[\boldsymbol{\alpha}]$ in the SLS regime. So the remaining cases to be tackled are (i) $\alpha_{11} \ge \alpha_{21} \ge \alpha_{22} \ge \alpha_{12}$, and (ii) $\alpha_{22} \ge \alpha_{12} \ge \alpha_{11} \ge \alpha_{21}$, and it suffices to consider case (i) due to symmetry. In the remainder of this section we assume case (i), where $\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}])$ is characterized as

$$
\mathtt{TIN}_{\mathcal{P}}([\boldsymbol{\alpha}]) = \left\{ (d_1, d_2) \in \mathbb{R}_+^2 \;\middle|\; \begin{array}{l} d_1 \le \alpha_{11}, d_2 \le \alpha_{22} \\ d_1 + d_2 \le \alpha_{11} + \alpha_{22} - \alpha_{21} - \alpha_{12} \end{array} \right\}. \tag{B.11}
$$

The single user bound $d_1 \le \alpha_{11}$ and the sum bound follow the proof for Theorem 3, so it only remains to show the bound $d_2 \le \alpha_{22}$. To do so, we cast $Y_2^n$ into the deterministic model $\bar{Y}_2^n$ in the same way as is done in (3.21), and define $(X)^{\mu} \triangleq \left\lceil X/\bar{P}^{\alpha-\mu} \right\rceil$ for a real value $X = O(\bar{P}^{\alpha})$ and $0 \le \mu \le \alpha$. First we apply Fano's inequality to bound $R_2$ from above (with

$no(\log P)$ omitted):

$$\begin{aligned}
nR_2 &\leq I_{\mathcal{G}}(\bar{Y}_2^n; W_2) && \text{(B.12)}\\
&= H_{\mathcal{G}}(\bar{Y}_2^n) - H_{\mathcal{G}}(\bar{Y}_2^n|W_2) && \text{(B.13)}\\
&\leq H_{\mathcal{G}}(\bar{Y}_2^n) - H_{\mathcal{G}}((\bar{X}_1^n)^{\alpha_{21}-\alpha_{22}}|W_2) && \text{(B.14)}\\
&= H_{\mathcal{G}}(\bar{Y}_2^n) - H_{\mathcal{G}}((\bar{X}_1^n)^{\alpha_{21}-\alpha_{22}}) && \text{(B.15)}\\
&\leq \alpha_{22} n \log P && \text{(B.16)}
\end{aligned}$$

To obtain (B.14), we find $(\bar{Y}_2^n)^{\alpha_{21}-\alpha_{22}}$, a function of $\bar{Y}_2^n$, is within bounded distortion of $(\bar{X}_1^n)^{\alpha_{21}-\alpha_{22}}$, due to $\alpha_{21} \geq \alpha_{22}$. Next, inequality (B.15) holds, because $I((\bar{Y}_1^n)^{\alpha_{21}-\alpha_{22}}; W_2) \leq no(\log P)$, and $(\bar{Y}_1^n)^{\alpha_{21}-\alpha_{22}}$ is within bounded distortion of $(\bar{X}_1^n)^{\alpha_{21}-\alpha_{22}}$. The former is due to Lemma 4 and the chain rule, and the latter is because $\alpha_{21} - \alpha_{22} \leq \alpha_{11} - \alpha_{12}$, as implied by case (i). Finally, we apply Lemma 5 to obtain (B.16). By dividing both sides of (B.16) by $n \log P$ and applying the GDoF limit, we get the desired bound $d_2 \leq \alpha_{22}$, which concludes the proof.

# Appendix C

# Appendix for Chapter 4

## C.1 Proof of Lemma 4.1

Here we present the proof of the SGDoF region $\mathcal{D}_{\text{IC}}^{\text{p}}$. The converse bounds are available from Lemma 8 of [94] (for single-user bound) and Lemma 2 of [121] (for the sum bound). The converse bounds are tight in Regime 3 and 4 defined in Theorem 4.1, as $\mathcal{D}_{\text{IC}}^{\text{p}} = \mathcal{D}_{\text{IC}}^{\text{f.p.}}$ in these regimes, and the schemes for finite precision CSIT also apply to the case with perfect CSIT. The remaining part to be shown is the achievability of $\mathcal{D}_{\text{IC}}^{\text{p}}$ in Regime 1 and 2.

In the following presentation of the schemes, without loss of generality we work on the simplified ZIC with all channel gains normalized to be 1; i.e.,

$$Y_1(t) = \sqrt{P^\alpha} X_1(t) + \sqrt{P^\beta} X_2(t) + Z_1(t), \tag{C.1}$$

$$Y_2(t) = \sqrt{P} X_2(t) + Z_2(t), \tag{C.2}$$

where $t \in [n]$, $Z_1(t), Z_2(t) \sim \mathcal{N}(0,1)$ and $X_1(t), X_2(t)$ are subject to unit input power constraint. This can be done by normalizing the inputs and the outputs of the original model (4.1) and (4.2) with the channel coefficients, which are known at both sides. Also we set the noise variances to unity since they are inconsequential to the GDoF analysis.

### C.1.1 The Achievability in Regime 1

The corner points of $\mathcal{D}_{\mathrm{IC}}^{\mathrm{p}}$ in Regime 1 are $(d_1, d_2) = (\alpha, 1)$ and $(\beta - 1, 1)$. The former is trivial, and time sharing achieves all tuples on the line segment between these two point. So we show the tuple $(\beta - 1, 1)$ is achievable with a scheme based on lattice alignment and aggregate decoding.

We first present the coding scheme, and then specify the alphabet design for the respective codebooks later. Message $W_1$ is split into two parts, and they are respectively encoded into codewords $\boldsymbol{V}_{11} = \{V_{11}(t) : t \in [n]\}$ and $\boldsymbol{V}_{12} = \{V_{12}(t) : t \in [n]\}$ with codebooks generated respectively by distribution $P_{V_{11}}$ on alphabet $\Gamma_{11}$, and by $P_{V_{12}}$ on $\Gamma_{12}$. Message $W_2$ is encoded into $\boldsymbol{V}_2 = \{V_2(t) : t \in [n]\}$ with a wiretap codebook generated by distribution $P_{V_2}$ on alphabet $\Gamma_2$. Let $X_1(t) = V_{11}(t) + J_1(t) + V_{12}(t)$ and $X_2(t) = V_2(t)$, where $J_1(t) \in \Gamma_J$ follows distribution $P_J$. For the channel (C.1) and (C.2), the following rates in single-letter form are achievable under secrecy constraints:

$$R_1 = I(Y_1; V_{11}, V_{12}), \tag{C.3}$$

$$R_2 = I(Y_2; V_2) - I(Y_1; V_2 | V_{11}, V_{12}). \tag{C.4}$$

$R_1$ is achievable because there is no information leakage link. $R_2$ is achievable because after $V_{11}$ and $V_{12}$ are decoded and removed from $Y_1$, what remains is the classical wiretap channel [72].

To show the desired GDoF tuple is achievable with the rate (C.3) and (C.4), next we specify the design of the alphabets $\Gamma_{11}, \Gamma_J, \Gamma_{12}$, and $\Gamma_2$. Let $Q \triangleq \left\lfloor \sqrt{P^{\alpha-\epsilon}} \right\rfloor$, $Q_J \triangleq \left\lfloor \sqrt{P^{\alpha-1-\epsilon}} \right\rfloor$, and

$A = 8\sqrt{P^{2\epsilon}}$, where $\epsilon > 0$. We define the alphabets (referred to as lattices in the following discussion) as

$$V_{11} \in \Gamma_{11} \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm Q, \pm 2Q, \cdots, \pm \left\lfloor \sqrt{P^{\beta-\alpha-\epsilon}} \right\rfloor Q\right\}, \tag{C.5}$$

$$J_1 \in \Gamma_J \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm Q_J, \pm 2Q_J, \cdots, \pm \left(\left\lfloor \tfrac{1}{8}\sqrt{P^{1-\epsilon}} \right\rfloor - 1\right) Q_J\right\}, \tag{C.6}$$

$$V_{12} \in \Gamma_{12} \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm 1, \pm 2, \cdots, \pm \left(\left\lfloor \tfrac{1}{4}\sqrt{P^{\alpha-1-2\epsilon}} \right\rfloor - 1\right)\right\}, \tag{C.7}$$

$$V_2 \in \Gamma_2 \triangleq A\sqrt{P^{-\alpha}} \times \left\{0, \pm Q_J, \pm 2Q_J, \cdots, \pm \left(\left\lfloor \tfrac{1}{8}\sqrt{P^{1-\epsilon}} \right\rfloor - 1\right) Q_J\right\}, \tag{C.8}$$

where for a real number $\xi$ and a finite set of integers $\{x_1, x_2, \cdots, x_n\}$, we define their product $\xi \times \{x_1, x_2, \cdots, x_n\} \triangleq \{\xi x_1, \xi x_2, \cdots, \xi x_n\}$. Note that such a choice of $A, Q, Q_J$, along with the lattices $\Gamma_{11}, \Gamma_J, \Gamma_{12}$ and $\Gamma_2$, satisfies the unit input power constraint for channel (C.1) and (C.2).

Let $V_{11}, V_{12}, J_1$ and $V_2$ be independent and uniformly distributed in their respective lattices. Now we can follow the argument from [103, 107] to bound (C.3) and (C.4) from below. The following lemma works as a common tool of the argument. Its proof is straightforward, by directly applying Fano's inequality to the achievable rate $R = I(X;Y)$.[1]

**Lemma C.1.** *Consider a channel with input $X$ and output $Y$, whose values are taken from finite alphabet $\mathcal{X}$. If $X$ is uniformly distributed in $\mathcal{X}$, and* $\Pr[X \neq Y] \leq \epsilon$, $0 \leq \epsilon \leq 1$, *then the mutual information $I(X;Y)$ can be bounded from below as $I(X;Y) \geq H(X)(1-\epsilon) - 1$.*

Now we bound the mutual information terms in (C.3) and (C.4). First we bound (C.3) from below. This is done firstly by attaching the nearest-neighbor symbol detectors $\hat{V}_{11}$ and $\hat{V}_{12}$ to $Y_1$, where

$$\hat{V}_{11} \triangleq \arg\min_{V_{11} \in \Gamma_{11}} \left| Y_1 - \sqrt{P^{\beta}} V_{11} \right|, \tag{C.9}$$

[1] By Fano's inequality, we have $H(X|Y) \leq 1 + \Pr[X \neq Y] \log|\mathcal{X}| \leq 1 + \epsilon H(X)$, where the last inequality holds because $\Pr[X \neq Y] \leq \epsilon$ and $X$ is uniformly distributed in $\mathcal{X}$. By plugging this bound in $I(X;Y) = H(X) - H(X|Y)$ we get the desired lower bound.

$$\hat{V}_{12} \triangleq \arg \min_{V_{12}\in\Gamma_{12}} \left| \tilde{Y}_1 - AQ_J \left[ \frac{\tilde{Y}_1}{AQ_J} \right] - \sqrt{P^\beta} V_{12} \right|, \tag{C.10}$$

where $\tilde{Y}_1 \triangleq Y_1 - \sqrt{P^\beta}\hat{V}_{11}$, and $[x]$ rounds $x$ to its nearest integer for all $x \in \mathbb{R}$. This encloses the original channel and equivalently creates a new channel of finite-alphabet input and output. Then we apply the data processing inequality and Lemma C.1 as follows.

$$\begin{aligned}
&I(Y_1; V_{11}, V_{12}) \\
&\geq I(\hat{V}_{11}, \hat{V}_{12}; V_{11}, V_{12}) && \text{(C.11)}\\
&\geq (\log|\Gamma_{11}| + \log|\Gamma_{12}|) \times \left(1 - \Pr\left[(\hat{V}_{11}, \hat{V}_{12}) \neq (V_{11}, V_{12})\right]\right) - 1 && \text{(C.12)}\\
&\geq (\beta - 1 - 3\epsilon)\log \bar{P} \times \left(1 - \Pr\left[(\hat{V}_{11}, \hat{V}_{12}) \neq (V_{11}, V_{12})\right]\right) - 3, && \text{(C.13)}
\end{aligned}$$

where inequality (C.13) holds for $P$ large enough because for $x \geq 2$, we have $\log(2\lfloor x \rfloor - 1) \geq \log x$.

Then by following the same steps in (C.12) and (C.13), we can bound the first term in (C.4) as

$$I(Y_2; V_2) \geq (1 - \epsilon)\log \bar{P}\left(1 - \Pr\left[\hat{V}_2 \neq V_2\right]\right) - 4, \tag{C.14}$$

where

$$\hat{V}_2 \triangleq \arg \min_{V_2\in\Gamma_2} \left| Y_2 - \sqrt{P^\alpha} V_2 \right|. \tag{C.15}$$

The second term in (C.4) can be bounded above by a constant as follows:

$$\begin{aligned}
&I(Y_1; V_2 | V_{11}, V_{12}) \\
&\leq I(Y_1; V_2 | V_{11}, V_{12}, Z_1) && \text{(C.16)}\\
&= I(\sqrt{P^\beta} J_1 + \sqrt{P^\alpha} V_2; V_2) && \text{(C.17)}
\end{aligned}$$

$$
\begin{aligned}
&= H(\sqrt{P^{\beta}}J_1 + \sqrt{P^{\alpha}}V_2) - H(\sqrt{P^{\beta}}J_1) && \text{(C.18)}\\
&\leq \log\left(4\left\lfloor \tfrac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 3\right) - \log\left(2\left\lfloor \tfrac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 1\right) && \text{(C.19)}\\
&\leq 1. && \text{(C.20)}
\end{aligned}
$$

Inequality (C.16) holds since $Z_1$ is independent of $V_2$, and (C.17) follows because $(V_{11}, V_{12}, Z_1)$ is independent of $(J_1, V_2)$. Inequality (C.19) is true by applying the uniform bound on the set $AQ_J \times \left\{0, \pm 1, \pm 2, \cdots, \pm 2\left(\left\lfloor \frac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 1\right)\right\}$, from which $\sqrt{P^{\beta}}J_1 + \sqrt{P^{\alpha}}V_2$ takes value. Finally (C.20) holds when $P$ is large enough.

It remains to find upper bounds of $\Pr[(\hat{V}_{11}, \hat{V}_{12}) \neq (V_{11}, V_{12})]$ in (C.13) and $\Pr[\hat{V}_2 \neq V_2]$ in (C.14). They vanish as $P$ goes to infinity, as stated in the following lemma, whose proof is relegated to Appendix C.1.3.

**Lemma C.2.** *Given $\hat{V}_{11}, \hat{V}_{12}$, and $\hat{V}_2$ are respectively defined in (C.9), (C.10) and (C.15), we have*

$$
\begin{aligned}
&\lim_{P\to\infty} \Pr[(\hat{V}_{11}, \hat{V}_{12}) \neq (V_{11}, V_{12})] = 0, && \text{(C.21)}\\
&\lim_{P\to\infty} \Pr[\hat{V}_2 \neq V_2] = 0. && \text{(C.22)}
\end{aligned}
$$

Finally, by respectively plugging (C.13) into (C.3), and plugging (C.14) and (C.20) into (C.4), we get

$$
\begin{aligned}
&R_1 \geq (\beta - 1 - 3\epsilon)\,\tfrac{1}{2}\log P + o(\log \bar{P}) = (\beta - 1)\,\tfrac{1}{2}\log P + o(\log \bar{P}), && \text{(C.23)}\\
&R_2 \geq (1 - \epsilon)\,\tfrac{1}{2}\log P + o(\log \bar{P}) = \tfrac{1}{2}\log P + o(\log \bar{P}). && \text{(C.24)}
\end{aligned}
$$

We arrive at $d_1 = \lim_{P\to\infty} \frac{R_1}{\frac{1}{2}\log P} \geq \beta - 1$, and $d_2 = \lim_{P\to\infty} \frac{R_1}{\frac{1}{2}\log P} \geq 1$. Thus the secure GDoF tuple $(d_1, d_2) = (\beta - 1, 1)$ is achievable with this scheme based on lattice alignment and aggregate decoding.

### C.1.2 The Achievability in Regime 2

The corner points of $\mathcal{D}_{\text{IC}}^{\text{p}}$ in Regime 1 are $(d_1, d_2) = (\alpha, 0)$ and $(\beta - 1, 1 + \alpha - \beta)$. Following the same reason for the corner points of Regime 1, it remains to show $(\beta - 1, 1 + \alpha - \beta)$ is achievable, which is done with lattice alignment and aggregate decoding as well.

We follow the same order as in Appendix $C$.1.1 by giving the coding scheme first and the alphabet design later. Message $W_1$ is encoded into $\boldsymbol{V}_1 = \{V_1(t) : t \in [n]\}$ with a codebook generated with alphabet $\Gamma_1$, and $W_2$ are encoded into $\boldsymbol{V}_2 = \{V_2(t) : t \in [n]\}$ with a wiretap codebook generated with alphabet $\Gamma_2$. Let $X_1(t) = V_1(t) + J_1(t)$ and $X_2(t) = V_2(t)$, where $J(t) \in \Gamma_J$. For the channel (C.1) and (C.2), the following rates in single-letter form are achievable under the secrecy constraints, for the reason similar to (C.3) and (C.4):

$$R_1 = I(Y_1; V_1), \tag{C.25}$$

$$R_2 = I(Y_2; V_2) - I(Y_1; V_2|V_1). \tag{C.26}$$

Next we specify the design of the alphabets $\Gamma_1, \Gamma_J$ and $\Gamma_2$. Let $Q \triangleq \left\lfloor \sqrt{P^{\alpha-1-\epsilon}} \right\rfloor$ and $A \triangleq \sqrt{P^{2\epsilon}}$, where $\epsilon > 0$. The alphabets (referred to as lattices in the following as well) are defined as

$$V_1 \in \Gamma_1 \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm 1, \pm 2, \cdots, \pm\left(\left\lfloor \tfrac{1}{2}\sqrt{P^{\alpha-1-2\epsilon}} \right\rfloor - 1\right)\right\}, \tag{C.27}$$

$$J_1 \in \Gamma_J \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm Q, \pm 2Q, \cdots, \pm \left\lfloor \sqrt{P^{1-\alpha+\beta-\epsilon}} \right\rfloor Q\right\}, \tag{C.28}$$

$$V_2 \in \Gamma_2 \triangleq A\sqrt{P^{-\alpha}} \times \left\{0, \pm Q, \pm 2Q, \cdots, \pm \left\lfloor \sqrt{P^{1-\alpha+\beta-\epsilon}} \right\rfloor Q\right\}. \tag{C.29}$$

Note that such a choice of $A, Q$ and the lattices $\Gamma_1, \Gamma_J$ and $\Gamma_2$ satisfies the unit input power constraint.

Finally we bound the rate (C.25) and (C.26) from below. Let $V_1, J_1$ and $V_2$ be independent and uniformly distributed in their respective lattices. By following the steps in Appendix C.1.1, we have

$$I(Y_1; V_1) \geq (\alpha - 1 - 2\epsilon) \times \tfrac{1}{2} \log P \left(1 - \Pr[\hat{V}_1 \neq V_1]\right) - 2, \tag{C.30}$$

$$I(Y_2; V_2) - I(Y_1; V_2|V_1) \geq (1 - \alpha + \beta - \epsilon) \tfrac{1}{2} \log P \left(1 - \Pr[\hat{V}_2 \neq V_2]\right) - 3, \tag{C.31}$$

where $\hat{V}_1$ and $\hat{V}_2$ are respectively defined as

$$\hat{V}_1 \triangleq \arg \min_{V_1 \in \Gamma_1} \left| Y_1 - AQ \left[\frac{Y_1}{AQ}\right] - \sqrt{P^\beta} V_1 \right|, \tag{C.32}$$

$$\hat{V}_2 \triangleq \arg \min_{V_2 \in \Gamma_2} \left| Y_2 - \sqrt{P} V_2 \right|. \tag{C.33}$$

With a similar reasoning to the one in Lemma C.2, one can show that for both $i = 1, 2$, $\Pr[\hat{V}_i \neq V_i] \to 0$ as $P \to \infty$, and

$$R_1 \geq (\alpha - 1 - 2\epsilon) \tfrac{1}{2} \log P + o(\log \bar{P}) = (\alpha - 1) \tfrac{1}{2} \log P + o(\log \bar{P}), \tag{C.34}$$

$$R_2 \geq (1 - \alpha + \beta - \epsilon) \tfrac{1}{2} \log P + o(\log \bar{P}) = (1 - \alpha + \beta) \tfrac{1}{2} \log P + o(\log \bar{P}). \tag{C.35}$$

By applying the definition of GDoF we get $d_1 = \lim_{P \to \infty} \frac{R_1}{\frac{1}{2} \log P} \geq \alpha - 1$ and $d_2 = \lim_{P \to \infty} \frac{R_2}{\frac{1}{2} \log P} \geq 1 - \alpha + \beta$. Hence the GDoF tuple $(d_1, d_2) = (\alpha - 1, 1 - \alpha + \beta)$ is achievable with this scheme.

### C.1.3 Proof of Lemma C.2

Let event $\mathcal{E} \triangleq \left\{Z_1 \middle| |Z_1| \geq \frac{A}{2}\right\}$, and its complement denoted as $\mathcal{E}^c = \left\{Z_1 \middle| |Z_1| < \frac{A}{2}\right\}$. Define $I_1 \triangleq \sqrt{P^\beta} V_{12} + Z_1$ and $I_2 \triangleq \sqrt{P^\beta} J_1 + \sqrt{P^\alpha} V_2 + I_1$. Note that $Y_1 = \sqrt{P^\beta} V_{11} + I_2$ is the sum of a lattice point $\sqrt{P^\beta} V_{11}$ and an offset $I_2$. The lattice point is taken from the lattice $\sqrt{P^\beta} \times \Gamma_{11}$ with the minimum spacing $AQ$, while the offset, $I_2$, takes value from $\left(-\frac{AQ}{2}, \frac{AQ}{2}\right)$ when $\mathcal{E}^c$ happens. So when $\mathcal{E}^c$ occurs, $V_{11}$ can be correctly decoded by (C.9), and seeing that $Z_1 \sim \mathcal{N}(0,1)$, we have

$$\Pr[\hat{V}_{11} \neq V_{11}] \leq \Pr\{\mathcal{E}\} \leq 2\exp\left(-\frac{1}{8}A^2\right). \tag{C.36}$$

Next we move on and argue that $V_{12}$ can be correctly decoded with (C.10) when $V_{11}$ is correctly decoded and $\mathcal{E}^c$ occurs. Suppose $V_{11}$ is correctly decoded and removed from $Y_1$, resulting in the remaining $\tilde{Y}_1 = I_2 = \sqrt{P^\beta}J_1 + \sqrt{P^\alpha}V_2 + I_1$. Note that $I_2$ is the sum of offset $I_1$ and a lattice point $\sqrt{P^\beta}J_1 + \sqrt{P^\alpha}V_2$, which is taken from lattice $\sqrt{P^\beta} \times \Gamma_J + \sqrt{P^\alpha} \times \Gamma_2$.[2] Such a lattice has the minimum spacing $AQ_J$. On the other hand, offset $I_1$ takes value from $\left(-\frac{AQ_J}{2}, \frac{AQ_J}{2}\right)$ when $\mathcal{E}^c$ happens. As a result, when $\mathcal{E}^c$ occurs, $\tilde{Y}_1 - AQ_J\left[\frac{\tilde{Y}_1}{AQ_J}\right] = I_1 = \sqrt{P^\beta}V_{12} + Z_1$. Note that, once again, $I_1$ is the sum a lattice point $\sqrt{P^\beta}V_{12}$, which is taken from lattice $\bar{P}^\beta \times \Gamma_{12}$ with the minimum spacing $A$, and an offset $Z_1$, which is in $\left(-\frac{A}{2}, \frac{A}{2}\right)$ if $\mathcal{E}^c$ happens. Therefore, $V_{12}$ can be correctly decoded by (C.10) when $\mathcal{E}^c$ occurs and $V_{11}$ is correctly decoded, and

$$Pr[\hat{V}_{12} \neq V_{12}|\hat{V}_{11} = V_{11}] \leq \Pr\{\mathcal{E}\} \leq 2\exp\left(-\frac{1}{8}A^2\right). \tag{C.37}$$

Finally we can bound $\Pr\left[(\hat{V}_{11}, \hat{V}_{12}) \neq (V_{11}, V_{12})\right]$ as follows.

$$\begin{aligned}
&\Pr\left[(\hat{V}_{11}, \hat{V}_{12}) \neq (V_{11}, V_{12})\right] \\
&\leq \Pr[\hat{V}_{11} \neq V_{11}] + \Pr[\hat{V}_{12} \neq V_{12}] && \text{(C.38)}\\
&= \Pr[\hat{V}_{11} \neq V_{11}] + \Pr[\hat{V}_{12} \neq V_{12}|\hat{V}_{11} = V_{11}]\Pr[\hat{V}_{11} = V_{11}] \\
&\qquad\qquad + \Pr[\hat{V}_{12} \neq V_{12}|\hat{V}_{11} \neq V_{11}]\Pr[\hat{V}_{11} \neq V_{11}] && \text{(C.39)}\\
&\leq \Pr[\hat{V}_{11} \neq V_{11}] + \Pr[\hat{V}_{12} \neq V_{12}|\hat{V}_{11} = V_{11}] + \Pr[\hat{V}_{11} \neq V_{11}] && \text{(C.40)}\\
&\leq 6\exp\left(-\frac{1}{8}A^2\right), && \text{(C.41)}
\end{aligned}$$

[2] For two sets $\Gamma_1$ and $\Gamma_2$, define $\Gamma_1 + \Gamma_2 \triangleq \{a + b | a \in \Gamma_1, b \in \Gamma_2\}$ as the sum set of $\Gamma_1$ and $\Gamma_2$.

where we apply the union bound in (C.38), and the law of total probability in (C.39). Inequality (C.41) holds because of (C.36) and (C.37). Since $A^2 = O(P^{2\epsilon})$ and $\epsilon > 0$, we have $\Pr[\hat{V}_{11} \neq V_{11} \text{ or } \hat{V}_{12} \neq V_{12}] \to 0$ as $P \to \infty$.

Note that $Y_2 = \sqrt{P}V_2 + Z_2$ is the sum of a lattice point $\sqrt{P}V_2$, which is taken from lattice $\sqrt{P} \times \Gamma_2$ with the minimum spacing $A\sqrt{P^{1-\alpha}}Q_J$, and an offset $Z_2$, which is in $\left(-\frac{A}{2}, \frac{A}{2}\right)$ if $\mathcal{E}^c$ happens. So $V_2$ can be correctly decoded by (C.15) when $\mathcal{E}$ occurs, and

$$\Pr[\hat{V}_2 \neq V_2] \leq \Pr\{\mathcal{E}\} \leq 2\exp\left(-\tfrac{1}{8}A^2 P^{1-\alpha} Q_J^2\right). \tag{C.42}$$

Note that $A^2 P^{1-\alpha} Q_J^2 = O(P^{\alpha-1+\epsilon})$ and $\alpha \geq 1$ in Regime 1, we have $\alpha - 1 + \epsilon > 0$, and $\Pr[\hat{V}_2 \neq V_2] \to 0$ as $P \to \infty$ as well. Here we conclude the proof.

## C.2 Proof of Theorem 4.2

In this section, we provide the proof of Theorem 4.2, which characterizes the SGDoF region of the ZBC with perfect and finite precision CSIT, respectively.

### C.2.1 The SGDoF Region with Perfect CSIT

**Converse**

To show the converse part, we cast the Gaussian channel model into the deterministic model defined in Section 4.6.1. Lemma 4.3 implies that the deterministic model incurs no loss in GDoF. To obtain the single-user bound for $d_1$, we apply Fano's inequality as follows.

$$nR_1$$

$$\leq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1) + no(\log \bar{P}) \tag{C.43}$$

$$= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1, (\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}; W_1) + no(\log \bar{P}) \tag{C.44}$$

$$= I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}; W_1) + I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}) + no(\log \bar{P}) \tag{C.45}$$

$$\leq I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_2)^{\min\{(\beta-\alpha)^+,1\}}; W_1) + H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | (\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}) + no(\log \bar{P}) \tag{C.46}$$

$$\leq n \left(\max\{\alpha, \beta\} - \min\{(\beta-\alpha)^+, 1\}\right) \log \bar{P} + no(\log \bar{P}) \tag{C.47}$$

$$= n \max\{\alpha, \beta - 1\} \log \bar{P} + no(\log \bar{P}), \tag{C.48}$$

where $\overline{\boldsymbol{Y}}_1$ and $\boldsymbol{B}$ are defined in Section 4.6.1. Equality (C.44) holds because $(\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}$ is a function of $\overline{\boldsymbol{Y}}_1$. Then we apply the chain rule to get (C.45). Next we note that, since both $(\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}$ and $(\overline{\boldsymbol{Y}}_2)^{\min\{(\beta-\alpha)^+,1\}}$ contain the top-$\min\{(\beta-\alpha)^+, 1\}$ subsection of $\boldsymbol{B}$ only, the latter can be obtained with the former within bounded distortion with $\mathcal{G}$ given. Applying this observation, and by the definition of mutual information, we get inequality (C.46). The first term in (C.46) is $no(\log \bar{P})$ due to Lemma 4.3, and we apply the uniform bound to obtain (C.47). Equality (C.48) then follows. Finally, we arrive at $d_1 = \lim_{P\to\infty} \frac{nR_1}{n\frac{1}{2}\log P} \leq \max\{\alpha, \beta - 1\}$.

Next we show the single-user bound for $d_2$ as follows. Starting by Fano's inequality, we get

$$nR_2$$

$$\leq I(\overline{\boldsymbol{Y}}_2; W_2) + no(\log \bar{P}) \tag{C.49}$$

$$= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2, (\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}; W_2) + no(\log \bar{P}) \tag{C.50}$$

$$= I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}; W_2) + I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2; W_2 | (\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}) + no(\log \bar{P}) \tag{C.51}$$

$$\leq I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\min\{1,(\beta-\alpha)^+\}}; W_2) + H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2 | (\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}) + no(\log \bar{P}) \tag{C.52}$$

$$\leq n \left(1 - (\beta-\alpha)^+\right)^+ \log \bar{P} + no(\log \bar{P}), \tag{C.53}$$

where $\overline{\boldsymbol{Y}}_2$ is defined in (4.25) in Section 4.6.1. Equality (C.50) holds because $(\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}$ is a function of $\overline{\boldsymbol{Y}}_2$. Then we apply the chain rule to get (C.51). Note that $(\overline{\boldsymbol{Y}}_1)^{\min\{1,(\beta-\alpha)^+\}}$

contains the top-$\min\{1,(\beta-\alpha)^+\}$ sub-section of codeword $\boldsymbol{B}$, so it can be obtained with $(\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}$ and $\mathcal{G}$ within bounded distortion. So we apply this observation, together with the definition of mutual information, to get (C.52). Finally we arrive at (C.53) by applying Lemma 4.3 and the secrecy constraint (3.2) to the first term in (C.52), and the uniform bound to the second term. Thus the bound $d_2 = \lim_{P\to\infty} \frac{nR_2}{n\frac{1}{2}\log P} \le (1-(\beta-\alpha)^+)^+$.

### Achievability

To show the achievability, we present two schemes respectively for the following two regimes: (a) Regime P1: $\beta - 1 \le \alpha$, and (b) Regime P2: $\alpha < \beta - 1$. For Regime P1, it suffices to achieve the corner point $(d_1, d_2) = (\alpha, 1-(\beta-\alpha)^+)$. It can be achieved by zero-forcing the cross link. More specifically, we define the input codeword $X_1(t)$ and $X_2(t)$ for $t \in [n]$ as

$$\begin{bmatrix} X_1(t) \\ X_2(t) \end{bmatrix} = c_1(t) \begin{bmatrix} 1 \\ 0 \end{bmatrix} U_1(t) + c_2(t) \begin{bmatrix} -G_{12}(t)\sqrt{P^\beta} \\ G_{11}(t)\sqrt{P^\alpha} \end{bmatrix} U_2(t), \tag{C.54}$$

where $U_1(t)$ and $U_2(t)$ are independent codewords encoded respectively from $W_1$ and $W_2$; $c_1(t) = \frac{1}{2}$ and

$$c_2(t) = \frac{1}{\sqrt{2\left(|G_{12}(t)|^2 P^\beta + |G_{11}(t)|^2 P^\alpha\right)}} \tag{C.55}$$

are chosen to satisfy the unit input power constraint. Such choice of $c_2(t)$ and the precoding vector is possible because of the perfect CSIT assumption. Note that the vector for $U_2(t)$ is chosen such that it zero-forces $U_2(t)$ at Receiver 1. Now the receivers respectively see the cross-link-free channel as follows.

$$Y_1(t) = \frac{1}{2} G_{11}(t)\sqrt{P^\alpha} U_1(t) + Z_1(t), \tag{C.56}$$

$$Y_2(t) = \frac{G_{22}(t)\sqrt{P^{1+\alpha}}}{\sqrt{2\left(|G_{12}(t)|^2 P^\beta + |G_{11}(t)|^2 P^\alpha\right)}} U_2(t) + Z_2(t). \tag{C.57}$$

Channel (C.56) allows GDoF $\alpha$ for $W_1$, and channel (C.57) allows $1+\alpha-\max\{\alpha,\beta\} = 1-(\beta-\alpha)^+$ for $W_2$. Note that the secrecy constraint (3.2) is satisfied, because undesired signals are zero forced and codewords $U_1(t)$ and $U_2(t)$ are independent.

On the other hand, for Regime P2, it suffices to achieve $(d_1,d_2)=(\beta-1,0)$. This can be done by setting $X_1(t)=0$ and $X_2(t)=\sqrt{P^{-1}}U_1(t)$, where $U_1(t)$ is encoded from $W_1$ with a wiretap codebook. With such a setting, the channel allows a GDoF $\beta-1$ for $W_1$ with the secrecy constraint (3.2) satisfied in the mean time. Here we conclude the proof.

### C.2.2 The SGDoF Region with Finite Precision CSIT

To show $\mathcal{D}_{\mathrm{BC}}^{\mathrm{f.p.}}$, we continue the definition of the channel regimes in Theorem 4.1, and further divide Regime 4 into the following two sub-regimes: (a) Regime 4.1, satisfying $\beta \leq 1$ and $\beta \leq \alpha$; and (b) Regime 4.2, satisfying $\beta \leq 1$ and $\alpha < \beta$. It remains to present the proof for Regime 4.2, as the proof for the other regimes is implied from the previous results.

More specifically, for Regime 1 and 2, their proofs follow from the proof in Section 4.6.3 for the corresponding regimes, which still holds when full transmitter cooperation is allowed. The SGDoF region of Regime 3 is identical to $\mathcal{D}_{\mathrm{BC}}^{\mathrm{p}}$ of the same regime, and the achievable scheme does not rely on the perfect CSIT assumption. So the proof in Appendix C.2.1 holds for finite precision CSIT. Finally, the proof for Regime 4.1 follows from the results in [129]. As a result, only the SGDoF region of Regime 4.2, which is $\{(d_1,d_2)\in\mathbb{R}_+^2 :\ d_1\leq\alpha, d_1+d_2\leq 1+\alpha-\beta\}$, remains to be shown.

First let us consider the converse proof. The single-user bound $d_1 \leq \alpha$ follows from the proof in Appendix C.2.1 in the corresponding channel regime. To show the sum bound, $d_1+d_2\leq 1+\alpha-\beta$, we cast the Gaussian ZBC model into the deterministic model defined in Section 4.6.1. Lemma 4.3 implies that this incurs no GDoF loss. Next we apply Fano's inequality, and get

$$
\begin{aligned}
&nR_1 + nR_2 \\
&\leq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1) + I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2; W_2) + no(\log \bar{P}) && \text{(C.58)} \\
&\leq H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1) - H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_1) + H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2) - H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2|W_2) + no(\log \bar{P}) && \text{(C.59)} \\
&= H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_2) - H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_1) + H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2|W_1) - H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2|W_2) + no(\log \bar{P}) && \text{(C.60)} \\
&\leq \max\{1-\beta, -\alpha\}^+ n \log \bar{P} + \max\{\beta - 1, \alpha\}^+ n \log \bar{P} + no(\log \bar{P}) && \text{(C.61)} \\
&= (1 + \alpha - \beta) n \log \bar{P} + no(\log \bar{P}), && \text{(C.62)}
\end{aligned}
$$

where $\overline{\boldsymbol{Y}}_1$ and $\overline{\boldsymbol{Y}}_2$ are defined respectively in (4.24) and (4.25). We apply (4.27) and the secrecy constraint (3.2) to obtain (C.60). Inequality (C.61) holds due to Lemma 4.5. Since $\beta \leq 1$ in this regime, we have (C.62), and in the GDoF limit we obtain the sum bound $d_1 + d_2 = \lim_{P\to\infty} \frac{R_1+R_2}{\frac{1}{2}\log P} \leq 1 + \alpha - \beta$.

Finally, let us consider the achievability. Since the SGDoF region of the ZBC in Regime 4.2 is identical to that of the ZIC in the same regime, the same achievable schemes apply. Thus, we obtain the SGDoF region of the ZBC with finite precision CSIT and conclude the proof.

## C.3 Proof of Lemma 4.6

We assume $G_1$ and $G_2$ are real random variables with $|G_i| \in (\frac{1}{\Delta}, \Delta)$ for $i = 1, 2$. For quick reference, we define $V = T \boxplus U$ and $Z = (T)^\lambda \boxplus (U)^\mu$, and summarize the definition of the top-$\lambda$ sub-section of the random variables as follows:

$$
(T)^\lambda = (T)_\nu^{\lambda+\nu} = \left\lfloor \frac{T - \bar{P}^{\lambda+\nu} \left\lfloor \frac{T}{\bar{P}^{\lambda+\nu}} \right\rfloor}{\bar{P}^\nu} \right\rfloor = \left\lfloor \frac{T}{\bar{P}^\nu} \right\rfloor, \tag{C.63}
$$

$$
(U)^\mu = (U)_\nu^{\mu+\nu} = \left\lfloor \frac{U - \bar{P}^{\mu+\nu} \left\lfloor \frac{U}{\bar{P}^{\mu+\nu}} \right\rfloor}{\bar{P}^\nu} \right\rfloor = \left\lfloor \frac{U}{\bar{P}^\nu} \right\rfloor, \tag{C.64}
$$

$$(V)^{\lambda} = (T \boxplus U)_{\nu}^{\lambda+\nu} = \left\lfloor \frac{V - \bar{P}^{\lambda+\nu} \left\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \right\rfloor}{\bar{P}^{\nu}} \right\rfloor. \tag{C.65}$$

Note that the last equality of (C.63) and (C.64) holds because $\left\lfloor \frac{T}{\bar{P}^{\lambda+\nu}} \right\rfloor = \left\lfloor \frac{U}{\bar{P}^{\mu+\nu}} \right\rfloor = 0$.

Next we simplify (C.65) in the way as is done to (C.63) and (C.64). Define $\eta_T = G_1 T - \lfloor G_1 T \rfloor$, and $\eta_U = G_2 U - \lfloor G_2 U \rfloor$. Note that $\eta_T, \eta_U \in [0, 1)$. Let us first estimate the size of the support of $\left\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \right\rfloor$, which is a term appearing in the denominator of (C.65).

$$\frac{V}{\bar{P}^{\lambda+\nu}} = G_1 \frac{T}{\bar{P}^{\lambda+\nu}} + G_2 \frac{U}{\bar{P}^{\lambda+\nu}} + \frac{\eta_T + \eta_U}{\bar{P}^{\lambda+\nu}} \tag{C.66}$$

$$= \tilde{\eta}_1 + \tilde{\eta}_2 + \tilde{\eta}_3, \tag{C.67}$$

where $\tilde{\eta}_i$ is the $i^{\text{th}}$ term in (C.66). It is obvious that $\tilde{\eta}_1, \tilde{\eta}_2 \in [-\Delta, \Delta]$, and $\tilde{\eta}_3 \in [0, 2]$. So $\left\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \right\rfloor$ is a random variable with support $\{-2\Delta, -2\Delta + 1 \cdots, 0, 1, \cdots, 2\Delta + 2\}$. Note that for real numbers $x, y$, we have $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + E$, where $E \in \{-1, 0, 1\}$. With this observation, we can expand $(V)^{\lambda}$ defined in (C.65) further as follows.

$$(V)^{\lambda} = \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor + \underbrace{\left\lfloor -\bar{P}^{\lambda+\nu} \left\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \right\rfloor \right\rfloor + E}_{\tilde{E}} \tag{C.68}$$

$$= \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor + \tilde{E}, \tag{C.69}$$

where $\tilde{E}$ is a random variable with support of size no greater than $3(4\Delta + 3)$.

Finally we relate $Z$ to $(V)^{\lambda}$. Define truncation terms $\delta_T = \frac{T}{\bar{P}^{\nu}} - (T)^{\lambda}$, $\delta_U = \frac{U}{\bar{P}^{\nu}} - (U)^{\lambda}$, $\epsilon_T = G_1 (T)^{\lambda} - \left\lfloor G_1 (T)^{\lambda} \right\rfloor$, $\epsilon_U = G_2 (U)^{\mu} - \lfloor G_2 (U)^{\mu} \rfloor$, and $\epsilon = \frac{V}{\bar{P}^{\nu}} - \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor$, whose values are in $[0, 1)$. With these truncation terms, we relate $Z$ with $(V)^{\lambda}$ as follows.

$$Z = \left\lfloor G_1 (T)^{\lambda} \right\rfloor + \lfloor G_2 (U)^{\mu} \rfloor \tag{C.70}$$

$$= G_1 (T)^{\lambda} + G_2 (U)^{\mu} - (\epsilon_T + \epsilon_U) \tag{C.71}$$

$$= G_1 \frac{T}{\bar{P}^{\nu}} + G_2 \frac{U}{\bar{P}^{\nu}} - (G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U) \tag{C.72}$$

$$= \frac{1}{\bar{P}^{\nu}}(\lfloor G_1 T \rfloor + \lfloor G_2 U \rfloor) - \left( \frac{\eta_T + \eta_U}{\bar{P}^{\nu}} + G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U \right) \tag{C.73}$$

$$= \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor + \epsilon - \left( \frac{\eta_T + \eta_U}{\bar{P}^{\nu}} + G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U \right) \tag{C.74}$$

$$= (V)^{\lambda} - \tilde{E} - \underbrace{\left( \frac{\eta_T + \eta_U}{\bar{P}^{\nu}} + G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U - \epsilon \right)}_{E'} \tag{C.75}$$

$$= (V)^{\lambda} - \tilde{E} - E', \tag{C.76}$$

where $E'$ is a random variable taking an integer value from $[-2\Delta - 1, 2\Delta + 4]$ and therefore has a support of size at most $4\Delta + 6$. As a result, $E_{\Sigma} = \tilde{E} + E'$ is a random variable with a support of size at most $3(4\Delta + 3)(4\Delta + 6)$, which is a constant with respect to $P$.

In summary, one can evaluate $Z = (T)^{\lambda} \boxplus (U)^{\lambda}$ from $(V)^{\lambda}$ once $E_{\Sigma}$ is known, which is a discrete random variable with a support of constant size invariant of $P$. By comparing the entropy of $Z$ and $(V)^{\lambda}$, we have $H(Z) - H(E_{\Sigma}) \leq H(Z|E_{\Sigma}) \leq H((V)^{\lambda}) \leq H(Z) + H(E_{\Sigma})$, and therefore establish $H((T \boxplus U)^{\lambda}) = H((T)^{\lambda} \boxplus (U)^{\lambda}) + O(1)$.