Secure GDoF of the Z-channel with Finite Precision CSIT: How Robust are Structured Codes?

Yao-Chia Chan and Syed A. Jafar
Center for Pervasive Communications and Computing (CPCC)
University of California Irvine, Irvine, CA 92697
Email: {*yaochic, syed*}*@uci.edu*

Abstract

Under the assumption of perfect channel state information at the transmitters (CSIT), it is known that structured codes offer significant advantages for secure communication in an interference network, e.g., structured jamming signals based on lattice codes may allow a receiver to decode the sum of the jamming signal and the signal being jammed, even though they cannot be separately resolved due to secrecy constraints, subtract the aggregate jammed signal, and then proceed to decode desired codewords at lower power levels. To what extent are such benefits of structured codes fundamentally limited by uncertainty in CSIT? To answer this question, we explore what is perhaps the simplest setting where the question presents itself — a Z interference channel with secure communication. Using sum-set inequalities based on Aligned Images bounds we prove that the GDoF benefits of structured codes are lost completely under finite precision CSIT. The secure GDoF region of the Z interference channel is obtained as a byproduct of the analysis.

This work is supported by NSF grants CCF-1617504 and CNS-1731384, ARO grant W911NF-19-1-0344 and ONR grant N00014-18-1-2057. It was presented in part at the 2020 IEEE International Symposium on Information Theory [1].

1 Introduction

The capacity of wireless networks, as evident from recent Degrees of Freedom (DoF) [2] and Generalized Degrees of Freedom (GDoF) [3] studies, depends rather strongly on the underlying assumptions about the availability of channel state information at the transmitter(s) (CSIT). Zero forcing [4, 5], interference alignment [6–9] — structured codes [10, 11] 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 [12, 13]. 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? The question is important from both practical and theoretical perspectives. The emphasis on finite precision CSIT brings theory closer to practice, which is a worthy goal in itself. In addition, even if we set practical concerns aside, there is another motivation for the emphasis on robustness — if the benefits of structured codes are indeed lost under finite precision CSIT, then perhaps 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.

Under perfect CSIT the challenge in GDoF studies is the crafting of powerful achievable schemes. Finite precision CSIT shifts the challenge to *outer bounds*. Indeed, optimal schemes under finite precision CSIT tend to be classical random coding schemes that are well understood. What is difficult is to prove that these schemes are *optimal*, e.g., that alignment is not possible, that *nothing* more powerful exists (in the GDoF sense) under finite precision CSIT. Another motivation for the focus on GDoF outer bounds is that unlike inner bounds that are inherently cumbersome as they depend on numerous design choices, e.g., number of layers of rate-splitting for each user, the rates and power levels assigned to each layer, and various choices of spatial and temporal beamforming, GDoF outer bounds tend to be *much* more compact, depending only on the channel parameters.

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 [14–26]. 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. With the exception of 'Aligned Images (AI)' bounds [13], 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 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 [13]. In fact even if all the transmitters cooperate fully the resulting K user MISO BC still has only 1 DoF (thus resolving a conjecture by Lapidoth, Shamai and Wigger [12]). AI bounds have been similarly essential to robust GDoF characterizations of various interference and broadcast settings, such as the symmetric K user IC [27], the 2-user MIMO IC with arbitrary levels of CSIT [28], the 3 user MISO BC [29], and the 2-user MIMO BC with arbitrary levels of CSIT, [30, 31]. Robust GDoF characterizations have also been found using AI bounds for various intermediate levels of transmitter cooperation in [32–34].

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.

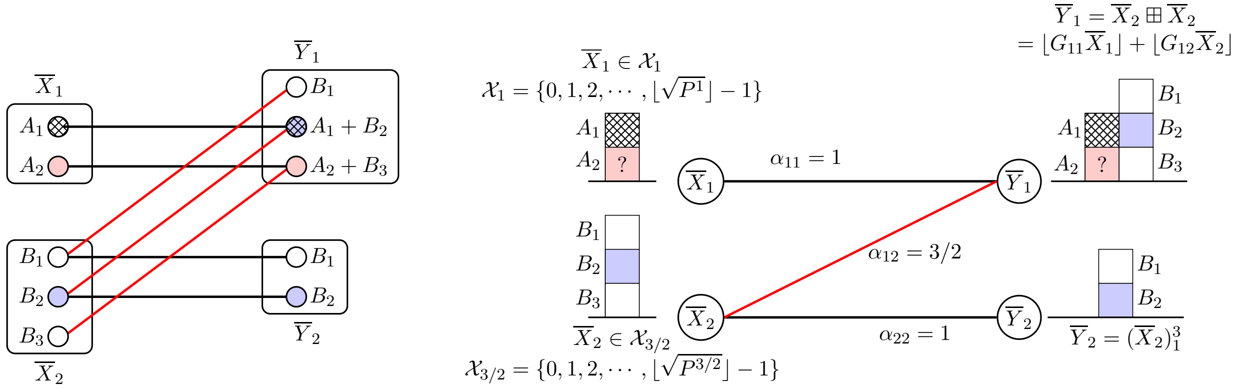

$\overline{X}_1$
A_1
A_2
$\overline{Y}_1$
B_1
$A_1 + B_2$
$A_2 + B_3$
B_1
B_2
B_3
$\overline{X}_2$
B_1
B_2
$\overline{Y}_2$
$\overline{X}_1 \in \mathcal{X}_1$
$\mathcal{X}_1 = \{0, 1, 2, \cdots, \lfloor\sqrt{P^1}\rfloor - 1\}$
A_1
A_2
?
B_1
B_2
B_3
$\overline{X}_2 \in \mathcal{X}_{3/2}$
$\mathcal{X}_{3/2}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

Figure 1: *A toy example. On the left is the ADT deterministic model CSIT 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 work that the GDoF tuple* $(\delta, 1/2)$ *is not achievable for any* $\delta > 0$*. This can be seen from Theorem 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 5.*

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 [35]. Exploring applications of these increasingly sophisticated sumset inequalities is another motivation for our work in this paper.

With the aid of sumset inequalities we wish to explore the robustness of structured codes for secure communication [16,18–20,24,26,36–40]. In particular, one powerful idea that is made possible by structured codes is the aggregate decoding and cancellation[1] of jammed signals [16,24,26,38–40]. 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 [41] 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 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 [42–46].

As a motivating example, consider the toy setting of a Z channel illustrated in Figure 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

[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*.

the capacity of the point to point Gaussian channel between Transmitter j and Receiver i, then we have $C_{11} : C_{12} : C_{22} = 2 : 3 : 2$ for this toy example. Note that the ratios of link capacities correspond to the α_{ij} values in the GDoF model, and that only the relative values of α_{ij} matter[2] for the GDoF metric. Throughout this paper we will normalize α_{22} to unity. In the figure[3] we see both the ADT deterministic model [47] (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. 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 coding schemes, yet to be discovered, that could overcome such limitations? These are the fundamental questions that motivate this work. What we find, using Aligned Images bounds and sum-set inequalities [35], 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

[2] It follows from the definition of GDoF that if all α_{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.

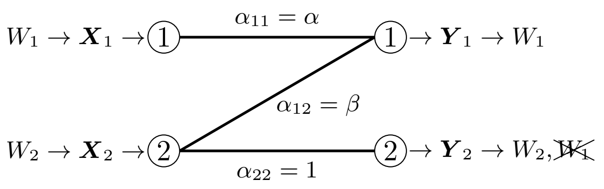

$W_1 \rightarrow \boldsymbol{X}_1 \rightarrow$ 1
$\alpha_{11} = \alpha$
1 $\rightarrow \boldsymbol{Y}_1 \rightarrow W_1$
$\alpha_{12} = \beta$
$W_2 \rightarrow \boldsymbol{X}_2 \rightarrow$ 2
2 $\rightarrow \boldsymbol{Y}_2 \rightarrow W_2, \cancel{W_1}$
$\alpha_{22} = 1$

Figure 2: *The Gaussian Z Interference Channel (ZIC).*

allowing perfect CSIT, then the problem has been studied in [42,43], and since channel uncertainty is not a concern, ADT models can be used to construct powerful lattice alignment solutions as shown in Figure 1. If we do not insist on information theoretic optimality then achievable schemes are easily developed, say from [48]. 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 [49]. Furthermore, the 2 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 [35]. Remarkably, despite its simplicity, the 2-user Z-channel is not far from exhausting the scope of known sum-set inequalities. It is noted recently in [50] that even if we introduce just one more user, which changes the 2-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 this work, e.g., deterministic encoders [44], cooperation between transmitters [45], cooperation between receivers [51], binary alphabet [46], and lack of coordination/trust between transmitters [52].

The rest of this paper is organized as follows. The system model is presented in the next section. The main result, i.e., the secure GDoF region is presented in Section 3. The achievability proof of the main result appears in Section 4, and the conserve proof follows in Section 5 along with a brief review of AI bounds. In Section 6 we present the conclusion.

Notation: For a positive integer n, denote $[n] = \{1, 2, \cdots, n\}$. The set $\{X(t) : t \in [n]\}$ is denoted as $\boldsymbol{X}$. For two functions $f(x)$ and $g(x)$, denote $f(x) = o(g(x))$ if $\limsup_{x\to\infty} f(x)/g(x) = 0$, and $f(x) = O(g(x))$ if $\limsup_{x\to\infty} f(x)/g(x) = c$ for some constant $c > 0$. For random variables X, Y and Z, and a set $\mathcal{G}$, define $H_{\mathcal{G}}(X|Y) = H(X|Y, \mathcal{G})$, and $I_{\mathcal{G}}(X; Y|Z) = I(X; Y|Z, \mathcal{G})$. All logarithms are to the base 2.

2 System Model

2.1 The Gaussian Z Interference Channel (ZIC)

We consider the two user Gaussian Z Interference Channel depicted in Figure 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

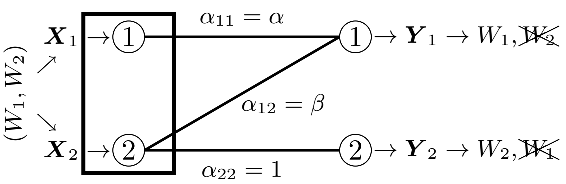


Figure 3: *The Gaussian Z Broadcast Channel (ZBC).*

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 $\boldsymbol{X}_i = \big(X_i(t)\big)_{t\in[n]} \in \mathbb{R}^n$ 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, θ_i is private randomness available only to Transmitter i, and $I(\theta_1, W_1; \theta_2, W_2) = 0$.

2.2 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 3, which is identical to the ZIC in every regard except that in the ZBC the transmitters are allowed to cooperate 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.

2.3 The GDoF Framework

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

$$Y_1(t) = G_{11}(t)\sqrt{P^{\alpha_{11}}}X_1(t) + G_{12}(t)\sqrt{P^{\alpha_{12}}}X_2(t) + Z_1(t), \tag{1}$$

$$Y_2(t) = G_{22}(t)\sqrt{P^{\alpha_{22}}}X_2(t) + Z_2(t), \tag{2}$$

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. Without loss of generality,[5] let us normalize the α_{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 α_{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 under the GDoF framework in (1) and (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 (5)). It is noteworthy that the deterministic models of [47], which

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

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.

2.4 Finite Precision CSIT

Following in the footsteps of [13], let us define $\mathcal{G}$ as a set of random variables that satisfy the bounded density assumption of [13] (replicated as Definition 3 in Section 5.1.1 of this paper). 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,

$$I(W_1, W_2, \theta_1, \theta_2, \boldsymbol{X}_1, \boldsymbol{X}_2; \mathcal{G}) = 0. \tag{3}$$

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

2.5 Perfect CSIT

While our focus in this work 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 (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.

2.6 Achievable Rates under Secrecy Constraint

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 ϵ; and (iii) the following secrecy constraint is satisfied

$$\frac{1}{n} I(W_j; \boldsymbol{Y}_i \mid \mathcal{G}) \leq \epsilon \qquad\qquad \forall i, j \in \{1, 2\}, i \neq j. \tag{4}$$

The secure capacity region $\mathcal{C}_P$ is the closure of the set of all achievable secure rate tuples.

2.7 Secure GDoF Region

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

$$\mathcal{D} \triangleq \left\{ (d_1, d_2) \middle| \begin{array}{c} \forall i \in \{1, 2\} \\ \exists (R_1(P), R_2(P)) \in \mathcal{C}_P \end{array}, d_i = \lim_{P \to \infty} \frac{R_i(P)}{\frac{1}{2} \log P} \right\}. \tag{5}$$

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

3 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., $\mathcal{D}^{p}_{\mathrm{IC}}$ versus $\mathcal{D}^{f.p.}_{\mathrm{IC}}$. These are characterized below in Lemma 1 and Theorem 1, respectively.

3.1 Secure GDoF of the ZIC with Perfect CSIT

Lemma 1. *The secure GDoF region of the ZIC under perfect CSIT is characterized as*

$$\mathcal{D}^{p}_{IC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \middle| \begin{array}{l} d_1 \leq \alpha \\ d_2 \leq \min\{1, (1+\alpha-\beta)^+\} \\ d_1 + d_2 \leq \alpha + (1-\beta)^+ \end{array} \right\}. \tag{6}$$

While a direct statement of Lemma 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 A.

3.2 Secure GDoF of the ZIC with Finite Precision CSIT

Theorem 1. *The secure GDoF region of the ZIC under finite precision CSIT is characterized as,*

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

$$\mathcal{D}^{f.p.}_{IC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \middle| \begin{array}{l} d_2 \leq 1, \\ d_1 + \beta d_2 \leq \alpha \end{array} \right\}. \tag{7}$$

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

$$\mathcal{D}^{f.p.}_{IC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \middle| \frac{d_1}{\alpha} + \frac{d_2}{1+\alpha-\beta} \leq 1 \right\}. \tag{8}$$

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

$$\mathcal{D}^{f.p.}_{IC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \middle| \, d_1 \leq \alpha, d_2 = 0 \right\}. \tag{9}$$

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

$$\mathcal{D}^{f.p.}_{IC} = \left\{ (d_1, d_2) \in \mathbb{R}^2_+ \middle| \begin{array}{l} d_1 \leq \alpha, d_2 \leq 1 \\ d_1 + d_2 \leq 1 + \alpha - \beta \end{array} \right\}. \tag{10}$$

The proof of Theorem 1 appears in Section 4 and 5. The main contribution of this work is the proof of Theorem 1 for Regimes 1 and 2. Indeed, Regime 3 is trivial and Regime 4 already follows from [53]. The converse proofs for Regimes 1 and 2 rely on various sum-set inequalities of [35], and are central to the thesis of this work, that the benefits of structured jamming are not robust to finite precision CSIT in the GDoF sense.

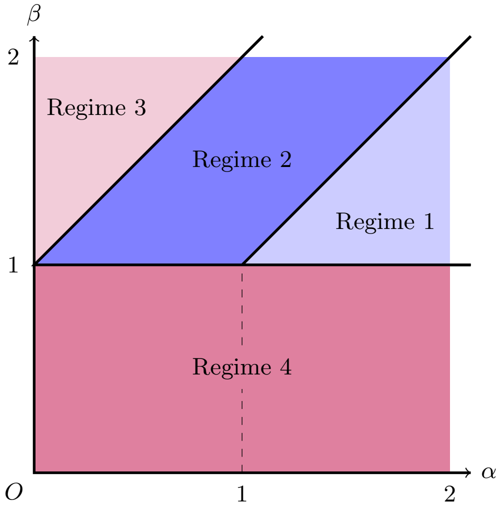


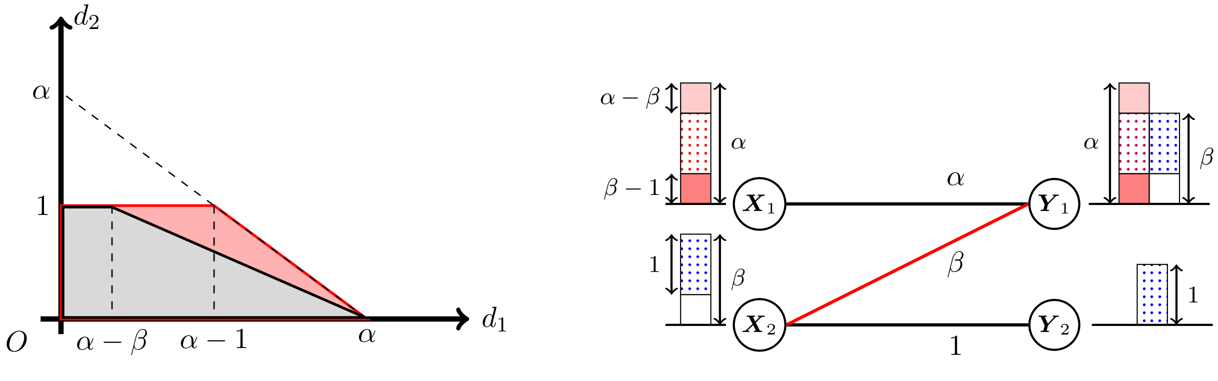
Figure 4: The parameter regimes corresponding to the four cases in Theorem 1.

3.3 How Robust are Structured Codes?

With the help of Lemma 1 and Theorem 1, we are ready to explore the robustness of the GDoF gains from structured codes through the following observations.

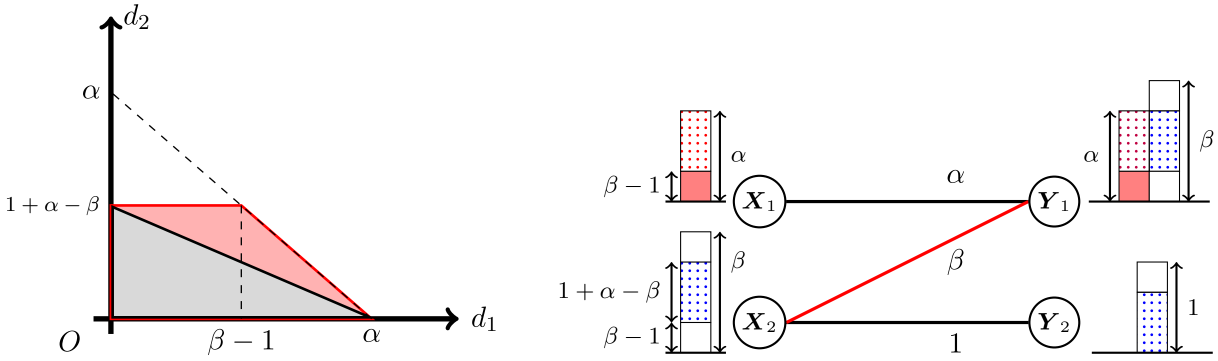
1. There are 4 parameter regimes identified in Theorem 1. These regimes are shown in Figure 4. Our first observation is that in regimes 3 and 4, we have $\mathcal{D}_{\rm IC}^{p}=\mathcal{D}_{\rm IC}^{f.p.}$, i.e., there is no loss of GDoF from limiting CSIT to finite precision. However, this is not 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 User 1 to achieve α 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 (see [53]) all we need is for Transmitter 1 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 $\mathcal{D}_{\rm IC}^{p}$ and $\mathcal{D}_{\rm IC}^{f.p.}$. Indeed, these regimes are central to this work, as they reveal the fragility of structured codes. First let us consider Regime 1. The GDoF regions, $\mathcal{D}_{\rm IC}^{p}$ and $\mathcal{D}_{\rm IC}^{f.p.}$ for this regime are illustrated in Figure 5(a). Let d_2^* denote the maximal value of d_2. According to Figure 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 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



(a) (b)

Figure 5: (a) $\mathcal{D}_{\text{IC}}^{p}$ (in red) and $\mathcal{D}_{\text{IC}}^{f.p.}$ (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 only possible under perfect CSIT. Signal levels shown in plain white are empty.



(a) (b)

Figure 6: (a) $\mathcal{D}_{\text{IC}}^{p}$ (in red) and $\mathcal{D}_{\text{IC}}^{f.p.}$ (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 only possible under perfect CSIT. Signal levels shown in plain white are empty.

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 work 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 $\mathcal{D}_{\text{IC}}^{p}$ and $\mathcal{D}_{\text{IC}}^{f.p.}$ are illustrated in Figure 6(a). In this case the loss of GDoF is even more severe as we have $(d_1^{**}, d_2^*) = (\beta - 1, 1 + \alpha - \beta)$

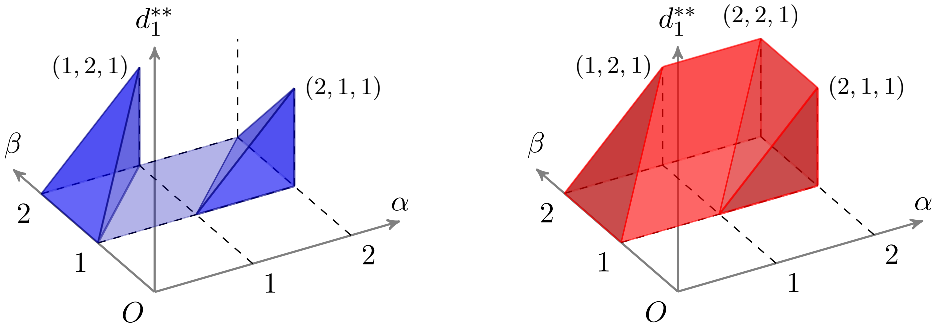


Figure 7: d_1^{**} under finite precision CSIT (blue) and perfect CSIT (red) in the parameter regimes $1, 2, 3$. Regime 4 is omitted. Peak vertices are labeled as $(\alpha, \beta, d_1^{**})$ tuples.

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 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 [35].

4. The loss of GDoF in terms of d_1^{**} values is illustrated for the entirety of Regimes $1, 2, 3$ in Figure 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 $d_{\mathrm{IC}}^{f.p.}(w_1, w_2) = \max_{(d_1,d_2)\in\mathcal{D}_{\mathrm{IC}}^{f.p.}} w_1 d_1 + w_2 d_2$. Similarly, for perfect CSIT we have $d_{\mathrm{IC}}^{p}(w_1, w_2) = \max_{(d_1,d_2)\in\mathcal{D}_{\mathrm{IC}}^{p}} w_1 d_1 + w_2 d_2$. Based on Lemma 1 and Theorem 1, it is not difficult to verify that the extremal value,

$$\inf_{(\alpha,\beta)\in\mathbb{R}_2^+} \inf_{(w_1,w_2)\in\mathbb{R}_2^+} \frac{d_{\mathrm{IC}}^{f.p.}(w_1, w_2)}{d_{\mathrm{IC}}^{p}(w_1, w_2)} = \frac{1}{2}. \tag{11}$$

In other words, looking out from the origin, the GDoF region $\mathcal{D}_{\mathrm{IC}}^{f.p.}$ is *at least* half as large in every direction as the GDoF region $\mathcal{D}_{\mathrm{IC}}^{p}$. It is also easy to see that the bound is asymptotically tight because, e.g., in Figure 5(a), if we let $\beta \to \alpha$ from below and $\alpha \to \infty$, then $\mathcal{D}_{\mathrm{IC}}^{p}$ approaches an almost-rectangular shape (with vertices $(0,0), (\alpha,0), (\alpha-1,1), (0,1)$) and $\mathcal{D}_{\mathrm{IC}}^{f.p.}$ 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 $\mathcal{D}_{\mathrm{IC}}^{f.p.}$ is (asymptotically) only half as large as $\mathcal{D}_{\mathrm{IC}}^{p}$. Note that this corresponds to $(w_1, w_2) = (\alpha - 1, 1)$.

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

$$\mathcal{D}_{BC}^{p} = \left\{(d_1, d_2,) \in \mathbb{R}_+^2 \middle| d_1 \leq \max\{\alpha, \beta - 1\},\ d_2 \leq (1 - (\beta - \alpha)^+)^+\right\}, \tag{12}$$

$$\mathcal{D}_{BC}^{f.p.} = \begin{cases} \left\{(d_1, d_2) \in \mathbb{R}_+^2 \middle| d_1 \leq \beta - 1, d_2 = 0\right\} & \text{if } 1 < \beta \text{ and } \alpha \leq \beta - 1, \\ \mathcal{D}_{IC}^{f.p.} & \text{otherwise.} \end{cases} \tag{13}$$

The proof of Theorem 2 is presented in Appendix B.

4 Proof of Theorem 1: Achievability

As noted previously, Regime 3 in Theorem 1 is trivial and Regime 4 already follows from [53]. 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 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 β, 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 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 α. As in Figure 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.

5 Proof of Theorem 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.

5.1 Preliminaries from Prior Work

The following definitions are inherited from [13, 35].

5.1.1 Definitions

Definition 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*

$$\mathcal{X}_{\lambda} = \left\{0, 1, 2, \cdots, \bar{P}^{\lambda} - 1\right\}, \tag{14}$$

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

Definition 2. *For non-negative real numbers X, λ_1 and λ_2, where $\lambda_2 \geq \lambda_1 \geq 0$, we define a* sub-section *of X corresponding to* interval (λ_1, λ_2)*, $(X)_{\lambda_1}^{\lambda_2}$, as*

$$(X)_{\lambda_1}^{\lambda_2} \triangleq \left\lfloor \frac{X - \bar{P}^{\lambda_2} \left\lfloor \frac{X}{\bar{P}^{\lambda_2}} \right\rfloor}{\bar{P}^{\lambda_1}} \right\rfloor. \tag{15}$$

We say that the $(X)_{\lambda_1}^{\lambda_2}$ is a section of X that sits at level λ_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 (λ_1, λ_2) and (λ_1', λ_2') are disjoint.*

Figure 8 illustrates this partitioning of X into various sub-sections. 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

$$(\boldsymbol{X})_{\lambda_1}^{\lambda_2} \triangleq \{(X(t))_{\lambda_1}^{\lambda_2} : t \in [n]\}. \tag{16}$$

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 (λ_1, λ_2) and (λ_1', λ_2') are disjoint.

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 λ 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 work 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-μ sub-section of X, retrieves from X the leftmost length-μ sub-string $x_{\lambda} x_{\lambda-1} \cdots x_{\lambda-\mu+1}$ comprised of the first μ most significant symbols in X. Similar to (16), 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 λ, λ_1 and λ_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 [47]. The generalization is needed because of our focus on finite precision CSIT.

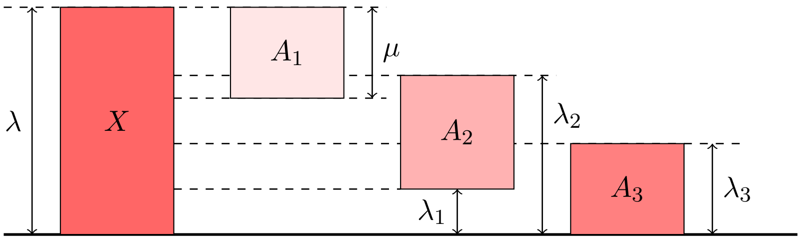


Figure 8: *An illustration of Definition 2. Sub-section* $A_1 = (X)_{\lambda-\mu}^{\lambda}$ *has level* $\ell(A_1) = \lambda - \mu$ *and height* $\mathcal{T}(A_1) = \mu$*. Sub-section* $A_2 = (X)_{\lambda_1}^{\lambda_2}$ *has level* $\ell(A_2) = \lambda_1$ *and height* $\mathcal{T}(A_2) = \lambda_2 - \lambda_1$*. 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* $\lambda - \mu \geq \lambda_3$*.*

Definition 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; 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 (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*

$$X_1 \boxplus_{\mathcal{G}} X_2 \triangleq \lfloor G_1 X_1 \rfloor + \lfloor G_2 X_2 \rfloor, \tag{17}$$

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*

$$\boldsymbol{X}_1 \boxplus_{\mathcal{G}} \boldsymbol{X}_2 \triangleq \{\lfloor G_1(t) X_1(t) \rfloor + \lfloor G_2(t) X_2(t) \rfloor : \ t \in [n]\}, \tag{18}$$

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.*

5.1.2 Key Sumset Inequalities

Our proof leans heavily on the sum-set inequalities based on Aligned Image sets from [35, Theorem 4]. While [35] presents these sum-set inequalities in generalized forms, the following simplified forms of those inequalities, taken from [34, Lemma 1], will be useful for our purpose.

Lemma 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* S_T *and* S_U *be sets of finitely many disjoint sub-sections respectively of* $\boldsymbol{T}$ *and* $\boldsymbol{U}$*, and let* $\{\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_M\}$ *be a subset of* $S_T \cup S_U$*. Let* $\boldsymbol{V} = \boldsymbol{T} \boxplus_{\mathcal{G}} \boldsymbol{U}$*. Then*

$$H_{\mathcal{G}}\left(\boldsymbol{V}|\mathcal{W}\right) \geq H_{\mathcal{G}}\left(\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_M|\mathcal{W}\right) + no(\log \bar{P}), \tag{19}$$

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* $\boldsymbol{A}_i$ *hold for* $i = 2, 3, \cdots, M$*:*

$$\ell(\boldsymbol{A}_i) \geq \mathcal{T}(\boldsymbol{A}_1) + \mathcal{T}(\boldsymbol{A}_2) + \cdots + \mathcal{T}(\boldsymbol{A}_{i-1}). \tag{20}$$

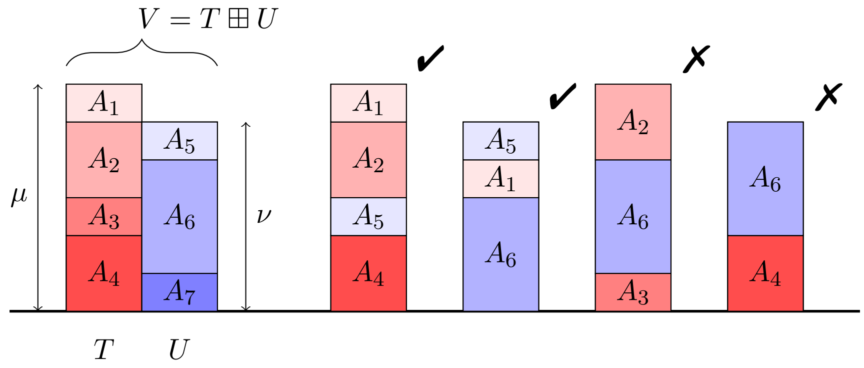


Figure 9: *An illustration of the box-stacking interpretation of Lemma 2. The bounds $H_{\mathcal{G}}(V|\mathcal{W}) \geq H_{\mathcal{G}}(A_1, A_2, A_4, A_5|\mathcal{W})$ and $H_{\mathcal{G}}(V|\mathcal{W}) \geq H_{\mathcal{G}}(A_1, A_5, A_6|\mathcal{W})$ are implied by Lemma 2 in the GDoF sense because 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 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 ✗.*

Constraint (20) in Lemma 2 has the following box-stacking interpretation. 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 $A_1, A_2, \cdots, A_M$; box A_i has height $\mathcal{T}(A_i)$ and originally sits on level $\ell(A_i)$ in either T or U. Then we stack the boxes in the index order of $A_1, A_2, \cdots, A_M$ from the ground. Now in this stack box A_i sits above boxes $A_1, A_2, \cdots, A_{i-1}$, therefore it sits at level $\tilde{\ell}(A_i) = \mathcal{T}(A_1) + \mathcal{T}(A_2) + \cdots + \mathcal{T}(A_{i-1})$. Constraint (20) says that the new level $\tilde{\ell}(A_i)$ cannot be higher than the level at which box A_i originally sits in T or U, which is $\ell(A_i)$. In other words, constraint (20) 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 them above their original level. Note that while constraints (20) seem to fix the stacking order according to the indices of the sub-sections, on the right-hand-side of (19) 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 (20) with the 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 (19) holds. Figure 9 and 10 illustrate some ways to stack the boxes (sub-sections) which satisfy or violate constraints (20).

5.1.3 Deterministic Model

To facilitate the use of Aligned Images bounds, we define a deterministic model as in [13]. In this deterministic model, the inputs are

$$A(t) = \left\lfloor \bar{P}^{\alpha} X_1(t) \right\rfloor \mod \bar{P}^{\alpha}, \tag{21}$$

$$B(t) = \left\lfloor \bar{P}^{\max\{1,\beta\}} X_2(t) \right\rfloor \mod \bar{P}^{\max\{1,\beta\}}, \tag{22}$$

and the outputs are

$$\overline{Y}_1(t) = \lfloor G_{11}(t)A(t) \rfloor + \left\lfloor G_{12}(t)\bar{P}^{-(1-\beta)^+} B(t) \right\rfloor, \tag{23}$$

$$\overline{Y}_2(t) = \left\lfloor G_{22}(t)\bar{P}^{-(\beta-1)^+} B(t) \right\rfloor. \tag{24}$$

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 3.

$$
\begin{aligned}
I_{\mathcal{G}}(W_i; \boldsymbol{Y}_i) &\leq I_{\mathcal{G}}(W_i; \overline{\boldsymbol{Y}}_i) + no(\log P) && \forall i = 1, 2, && (25)\\
I_{\mathcal{G}}(W_j; \overline{\boldsymbol{Y}}_i) &\leq I_{\mathcal{G}}(W_j; \boldsymbol{Y}_i) + no(\log P) && \forall i, j = 1, 2, i \neq j. && (26)
\end{aligned}
$$

The proof of Lemma 3 is identical to that of Lemma 5.1 in [53].

5.2 Useful Lemmas

With the preliminaries in place, we now proceed to the task of proving the converse for Theorem 1, starting with the following lemmas. The first lemma is a straightforward consequence of the secrecy constraint (26).

Lemma 4. *Let $\overline{\mu} = (\beta - \alpha)^+$ and $\underline{\mu} = (\alpha - \beta)^+$. Then we have,*

$$
\begin{aligned}
I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1) &= no(\log \bar{P}), && (27)\\
I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_2 | W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) &= no(\log \bar{P}), && (28)\\
I_{\mathcal{G}}(W_2; W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) &= no(\log \bar{P}). && (29)
\end{aligned}
$$

Proof.

$$
\begin{aligned}
I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1) &= I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1) + I_{\mathcal{G}}(W_2; W_1 | \overline{\boldsymbol{Y}}_1) && (30)\\
&\leq I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1) + H_{\mathcal{G}}(W_1 | \overline{\boldsymbol{Y}}_1) && (31)\\
&\leq I_{\mathcal{G}}(W_2; \boldsymbol{Y}_1) + H_{\mathcal{G}}(W_1 | \boldsymbol{Y}_1) + no(\log \bar{P}) && (32)\\
&= no(\log \bar{P}). && (33)
\end{aligned}
$$

We apply the chain rule to get (30), and the definition of mutual information to obtain (31). Next, we obtain (32) by applying (25) and (26). Finally, we apply the secrecy constraint (4) and Fano's inequality to obtain (33).

To show equality (28) and (29), 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,

$$
\begin{aligned}
no(\log \bar{P}) &= I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1) && (34)\\
&= I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1, W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) && (35)\\
&= I_{\mathcal{G}}(W_2; W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}) + I_{\mathcal{G}}(W_2; \overline{\boldsymbol{Y}}_1 | W_1, (\boldsymbol{A})^{\underline{\mu}}, (\boldsymbol{B})^{\overline{\mu}}). && (36)
\end{aligned}
$$

Equality (28) and (29) 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 [28] and hence its proof is omitted.

Lemma 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*

$$H_{\mathcal{G}}(\boldsymbol{V}_1|\mathcal{W}) - H_{\mathcal{G}}(\boldsymbol{V}_2|\mathcal{W}) \leq \max\{\mu_1 - \mu_2, \nu_1 - \nu_2\}^+ \log P + no(\log \bar{P}), \tag{37}$$

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 [35] 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 [50]. For our present purpose, however, because we only need the 'top' sub-sections, such a relationship is obtained in the following lemma.

Lemma 6. *Let λ, μ, ν 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*

$$H_{\mathcal{G}}((T \boxplus U)^\lambda) = H_{\mathcal{G}}((T)^\lambda \boxplus (U)^\mu) + O(1), \tag{38}$$

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

The proof of Lemma 6 is relegated to Appendix C.

The next lemma provides an important lower bound on the entropy of a finite-precision linear combination of random variables based on Lemma 2 and the submodularity of entropy.

Lemma 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*

$$2pH_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^\mu, (\boldsymbol{U})^\nu) \geq qH_{\mathcal{G}}((\boldsymbol{T})^{p+\mu}, (\boldsymbol{U})^{p+\nu}|\mathcal{W}, (\boldsymbol{T})^\mu, (\boldsymbol{U})^\nu) + no(\log \bar{P}), \tag{39}$$

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

$$A_i(t) = \begin{cases} (T(t))_{q-i\ell}^{q-(i-1)\ell} & \text{if } 1 \leq i \leq \tilde{p} \\ (U(t))_{q-(i-\tilde{p})\ell}^{q-(i-\tilde{p}-1)\ell} & \text{if } \tilde{p}+1 \leq i \leq 2\tilde{p} \end{cases}, \tag{40}$$

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

$$H_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^\mu, (\boldsymbol{U})^\nu) \geq H_{\mathcal{G}}(\boldsymbol{A}_i, \boldsymbol{A}_{i+1}, \cdots, \boldsymbol{A}_{i+q-1}|\mathcal{W}, (\boldsymbol{T})^\mu, (\boldsymbol{U})^\nu) + no(\log \bar{P}), \tag{41}$$

where we implicitly use modulo-$2\tilde{p}$ arithmetic in the indices; e.g., $i_0 = i_{2\tilde{p}}$. Lemma 2 is applied in the following way. After removing top-μ sub-section of $\boldsymbol{T}$ and top-ν 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 ℓ. 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-μ sub-section of $\boldsymbol{T}$ and the top-ν

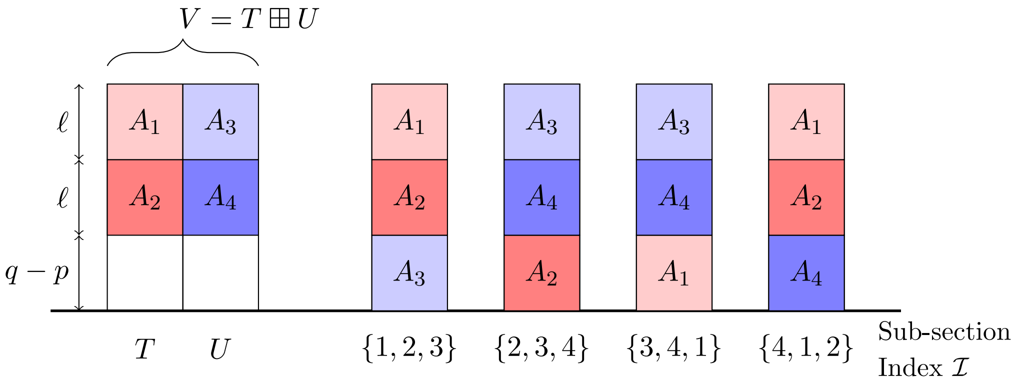


Figure 10: *An illustration of how the sum-set inequality in Lemma 2 is applied to the proof of Lemma 7. In this case, $\mu = \nu = 0$, $p = 2$, and $q = 3$, which implies that $\ell = 1$, $\tilde{p} = 2$ and $\tilde{q} = 3$. The left most consecutive bars shows $\boldsymbol{V} = \boldsymbol{T} \boxplus_{\mathcal{G}} \boldsymbol{U}$ and some sub-sections of $\boldsymbol{T}$ and $\boldsymbol{U}$ taken by (40). 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 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 (39).*

sub-section of $\boldsymbol{U}$, Lemma 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 2. See Figure 10 for an illustration of the procedure above.

Adding up (41) for all $i \in [2\tilde{p}]$, we have

$$\begin{aligned}
&2pH_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) \\
&= \ell 2\tilde{p} H_{\mathcal{G}}(\boldsymbol{V}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) && (42) \\
&\geq \ell \sum_{i=1}^{2\tilde{p}} H_{\mathcal{G}}(\boldsymbol{A}_i, \boldsymbol{A}_{i+1}, \cdots, \boldsymbol{A}_{i+\tilde{q}-1}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) + no(\log \bar{P}) && (43) \\
&\geq \ell \tilde{q} H_{\mathcal{G}}(\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_{2\tilde{p}}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) + no(\log \bar{P}) && (44) \\
&\geq qH_{\mathcal{G}}((\boldsymbol{T})^{p+\mu}, (\boldsymbol{U})^{p+\nu}|\mathcal{W}, (\boldsymbol{T})^{\mu}, (\boldsymbol{U})^{\nu}) + no(\log \bar{P}). && (45)
\end{aligned}$$

Step (42) holds since $p = \tilde{p}\ell$. Step (44) follows from the sub-modularity [6] of entropy, and (45) 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. □

5.3 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 $\overline{\mu} \leq 1$.

[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:

$$\sum_{i=1}^{n} H(X_i, X_{i+1}, \cdots, X_{i+k-1}) \geq kH(X_1, X_2, \cdots, X_n), \quad (46)$$

where modulo-n arithmetic is implicitly used in the inidices, e.g., $i_0 = i_n$.

Lemma 8. *For $\lambda \geq 1-\mu$ and $\overline{\mu} \leq 1$, we have*

$$H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda}|\mathcal{W}) \geq nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}|\mathcal{W}) + no(\log \bar{P}). \tag{47}$$

Proof.

$$\begin{aligned}
H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda}|\mathcal{W}) &= H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-\overline{\mu}} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}|\mathcal{W}) + no(\log \bar{P}) && (48)\\
&\geq H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}|\mathcal{W}) + no(\log \bar{P}) && (49)\\
&= H_{\mathcal{G}}(W_2|\mathcal{W}) + H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}})|\mathcal{W}, W_2)\\
&\qquad - H_{\mathcal{G}}(W_2|\mathcal{W}, (\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}) + no(\log \bar{P}) && (50)\\
&= H(W_2) + H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}|\mathcal{W}, W_2) + no(\log \bar{P}) && (51)\\
&\geq nR_2 + H_{\mathcal{G}}((\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-1+\mu}|\mathcal{W}, W_2) + no(\log \bar{P}) && (52)\\
&= nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}|\mathcal{W}, W_2) + no(\log \bar{P}) && (53)\\
&= nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\lambda-(1-\overline{\mu})}|\mathcal{W}) + no(\log \bar{P}). && (54)
\end{aligned}$$

First, equality (48) holds because by Lemma 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 5 to obtain (49), and apply the chain rule to obtain (50). Equality (51) holds for the following reasons: (a) equality (29) implies the first entropy term; (b) the last entropy term is of $no(\log \bar{P})$ is because, from $(\boldsymbol{A})^{\underline{\mu}}$ and $(\boldsymbol{A})^{\lambda-1} \boxplus (\boldsymbol{B})^{\lambda-\underline{\mu}}$, by Lemma 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 5 to obtain (52). Note that Lemma 5 is applicable because in Regimes 1 and 2, $1-\mu = 1+\alpha-\beta \geq (\alpha-\beta)^+ = \underline{\mu}$. Equality (53) holds because by Lemma 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 (54) due to (28). □

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 9.

$$H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}|\mathcal{W}, (\boldsymbol{B})^1) \geq nR_2 + no(\log \bar{P}). \tag{55}$$

Proof.

$$\begin{aligned}
H_{\mathcal{G}}((\boldsymbol{B})^1|\mathcal{W}) &\leq H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{1+\underline{\mu}}|\mathcal{W}) + no(\log \bar{P}) && (56)\\
&= H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{1+\underline{\mu}}|\mathcal{W}, W_2) + no(\log \bar{P}) && (57)\\
&\leq H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}, (\boldsymbol{B})^1|\mathcal{W}, W_2) + no(\log \bar{P}) && (58)\\
&= H_{\mathcal{G}}((\boldsymbol{B})^1|\mathcal{W}, W_2) + H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}|\mathcal{W}, W_2, (\boldsymbol{B})^1) + no(\log \bar{P}) && (59)\\
&\leq H_{\mathcal{G}}((\boldsymbol{B})^1|\mathcal{W}, W_2) + H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}|\mathcal{W}, (\boldsymbol{B})^1) + no(\log \bar{P}). && (60)
\end{aligned}$$

First, we apply Lemma 5 to obtain inequality (56). 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 (57) holds due to (28). Inequality (58) 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 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 (59), and apply the fact that conditioning reduces entropy to obtain (60).

By swapping terms in (60), we have

$$\begin{aligned}
H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}|\mathcal{W},(\boldsymbol{B})^1) &\geq H_{\mathcal{G}}((\boldsymbol{B})^1|\mathcal{W}) - H_{\mathcal{G}}((\boldsymbol{B})^1|\mathcal{W},W_2) + no(\log\bar{P}) && (61)\\
&= I_{\mathcal{G}}((\boldsymbol{B})^1;W_2|\mathcal{W}) + no(\log\bar{P}) && (62)\\
&= I_{\mathcal{G}}((\boldsymbol{B})^1,\mathcal{W};W_2) - I(\mathcal{W};W_2) + no(\log\bar{P}) && (63)\\
&= I_{\mathcal{G}}((\boldsymbol{B})^1,\mathcal{W};W_2) + no(\log\bar{P}) && (64)\\
&\geq I_{\mathcal{G}}((\boldsymbol{B})^1;W_2) + no(\log\bar{P}) && (65)\\
&\geq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2;W_2) + no(\log\bar{P}) && (66)\\
&= nR_2 + no(\log\bar{P}). && (67)
\end{aligned}$$

We apply the definition of mutual information to obtain (62), the chain rule to obtain (63), and (29) to obtain (64). Then we remove $\mathcal{W}$ to obtain (65). Finally, we apply data processing inequality to obtain (66), and Fano's inequality to obtain (67). □

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

Lemma 10. *For $\overline{\mu} \leq 1$, we have*

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|\mathcal{W}) \geq \frac{\min\{\beta,\alpha\}}{1-\overline{\mu}} nR_2 + no(\log\bar{P}). \tag{68}$$

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

$$H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\gamma+|\mu|}|\mathcal{W}) \geq \frac{\gamma}{1-\overline{\mu}} nR_2 + no(\log\bar{P}). \tag{69}$$

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

$$\begin{aligned}
&H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\gamma+|\mu|}|\mathcal{W}) && (70)\\
&\geq H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{r_i+|\mu|}|\mathcal{W}) + no(\log\bar{P}) && (71)\\
&= \frac{1}{2m_i}\left(2m_i H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{r_i+|\mu|}|\mathcal{W})\right) + no(\log\bar{P}) && (72)\\
&\geq \frac{r_i}{2m_i} H_{\mathcal{G}}((\boldsymbol{A})^{m_i+\underline{\mu}},(\boldsymbol{B})^{m_i+\overline{\mu}}|\mathcal{W}) + no(\log\bar{P}) && (73)
\end{aligned}$$

[7] The existence of such k and γ can be shown as follows. In Regime 1, since $\beta > 1$, we can find k,γ, 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,γ 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 γ, 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 γ, 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 γ.

$$
\begin{aligned}
&\geq \frac{r_i}{2m_i} H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu}, (\boldsymbol{B})^1 | \mathcal{W}) + no(\log \bar{P}) && (74)\\
&= \frac{r_i}{2m_i} \big(H_{\mathcal{G}}((\boldsymbol{B})^1 | \mathcal{W}) + H_{\mathcal{G}}((\boldsymbol{A})^{1-\mu} | \mathcal{W}, (\boldsymbol{B})^1) \big) + no(\log \bar{P}) && (75)\\
&\geq \frac{r_i}{2m_i} \big(H_{\mathcal{G}}(W_2 | \mathcal{W}) + H_{\mathcal{G}}((\boldsymbol{B})^1 | \mathcal{W}, W_2) - H_{\mathcal{G}}(W_2 | \mathcal{W}, (\boldsymbol{B})^1) + nR_2 \big) + no(\log \bar{P}) && (76)\\
&\geq \frac{r_i}{m_i} nR_2 + no(\log \bar{P}). && (77)
\end{aligned}
$$

Inequality (71) holds because of Lemma 5 and the fact that $r_i \leq \gamma$. Then we multiply and divide the entropy term by $2m_i$ to get (72), and apply[9] Lemma 7 to obtain (73). Inequality (74) holds because of Lemma 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 (75), and apply the chain rule and Lemma 9 to get (76). Equality (77) follows from (76) due to the following reasons: (a) we apply (29) 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 (77) is valid for all $i \geq N$, we have

$$
H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\gamma + |\mu|} | \mathcal{W}) \geq \lim_{i \to \infty} \frac{r_i}{m_i} nR_2 + no(\log \bar{P}) = \frac{\gamma}{1 - \overline{\mu}} nR_2 + no(\log \bar{P}). \tag{78}
$$

Next, based on the intermediate result (69), we show the following lower bound.

$$
H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | \mathcal{W}) \geq knR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{|\mu| + \gamma} | \mathcal{W}) + no(\log \bar{P}). \tag{79}
$$

This bound is reduced to (69) when $k = 0$ because of the following identity

$$
\max\{\beta, \alpha\} = |\mu| + \min\{\beta, \alpha\} = |\mu| + k(1 - \overline{\mu}) + \gamma. \tag{80}
$$

On the other hand, when $k \geq 1$, we apply Lemma 8 as follows.

$$
\begin{aligned}
H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | \mathcal{W}) &\geq nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\max\{\beta,\alpha\} - (1 - \overline{\mu})} | \mathcal{W}) + no(\log \bar{P}) && (81)\\
&\geq 2nR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\max\{\beta,\alpha\} - 2(1 - \overline{\mu})} | \mathcal{W}) + no(\log \bar{P}) && (82)\\
&\geq \cdots\\
&\geq knR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\max\{\beta,\alpha\} - k(1 - \overline{\mu})} | \mathcal{W}) + no(\log \bar{P}) && (83)\\
&= knR_2 + H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{|\mu| + \gamma} | \mathcal{W}) + no(\log \bar{P}). && (84)
\end{aligned}
$$

Lemma 8 can be applied to (81) – (83) because in both Regime 1 and 2, we have $\overline{\mu} \leq 1$ and $\max\{\alpha, \beta\} - (k-1)(1 - \overline{\mu}) \geq 1 - \mu$ [10]. Next we apply (80) to obtain (84).

Finally, we plug (69) into (79), and get

$$
\begin{aligned}
H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | \mathcal{W}) &\geq knR_2 + \frac{\gamma}{1 - \overline{\mu}} nR_2 + no(\log \bar{P}) && (85)\\
&= \frac{\min\{\beta, \alpha\}}{1 - \overline{\mu}} nR_2 + no(\log \bar{P}), && (86)
\end{aligned}
$$

where equality (86) holds by applying the identity $\min\{\beta, \alpha\} = k(1 - \overline{\mu}) + \gamma$. □

[9] To apply Lemma 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 6 can be recovered from $(\overline{\boldsymbol{Y}}_1)^{r_i + |\mu|}$ within bounded distortion.

[10] This can be seen by the following. First by (80) 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 $1 + \gamma + \underline{\mu} \geq 1 \geq 1 - \mu$.

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

$$\begin{aligned}
nR_1 &\le I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1) + no(\log \bar{P}) && (87)\\
&\le I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1, (\boldsymbol{B})^{\overline{\mu}}; W_1) + no(\log \bar{P}) && (88)\\
&= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\boldsymbol{B})^{\overline{\mu}}) + I_{\mathcal{G}}((\boldsymbol{B})^{\overline{\mu}}; W_1) + no(\log \bar{P}) && (89)\\
&= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\boldsymbol{B})^{\overline{\mu}}) + I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_2)^{\overline{\mu}}; W_1) + no(\log \bar{P}) && (90)\\
&= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\boldsymbol{B})^{\overline{\mu}}) + no(\log \bar{P}) && (91)\\
&\le H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | (\boldsymbol{B})^{\overline{\mu}}) - H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | \mathcal{W}) + no(\log \bar{P}) && (92)\\
&\le \alpha n \log \bar{P} - \frac{\min\{\beta, \alpha\}}{1-\overline{\mu}} nR_2 + no(\log \bar{P}) && (93)
\end{aligned}$$

Inequality (88) holds because adding $(\boldsymbol{B})^{\overline{\mu}}$ does not hurt the mutual information. Then we apply the chain rule to get (89). Since $\overline{\mu} \le 1$ in Regime 1 and 2, $(\boldsymbol{B})^{\overline{\mu}}$ can be converted into $(\overline{\boldsymbol{Y}}_2)^{\overline{\mu}}$ within bounded distortion by Lemma 6, and as a result we have (90). Equality (91) holds due to (26) and the secrecy constraint (4), and the fact that $\overline{\mu} \le 1$. Then seeing that $\{(\boldsymbol{B})^{\overline{\mu}}\} \subset \mathcal{W}$, inequality (92) is obtained by applying the fact that conditioning reduces entropy. To obtain inequality (93), first we apply the uniform bound to the first entropy in (92) as follows:

$$H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | (\boldsymbol{B})^{\overline{\mu}}) \le H_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)_0^{\alpha}) \le \alpha n \log P + no(\log \bar{P}). \tag{94}$$

And then we apply Lemma 10 to the second entropy in (92) . Note that Lemma 10 is applicable since $\overline{\mu} \le 1$ in Regime 1 and 2.

Finally by applying the definition of GDoF, we get

$$d_1 + \frac{\min\{\beta, \alpha\}}{1-\overline{\mu}} d_2 = \lim_{P\to\infty} \frac{R_1 + \frac{\min\{\beta,\alpha\}}{1-\overline{\mu}} R_2}{\frac{1}{2}\log P} \le \alpha \tag{95}$$

$$\implies \begin{cases} d_1 + \beta d_2 \le \alpha & \text{if } \alpha > \beta \\ \frac{d_1}{\alpha} + \frac{d_2}{1+\alpha-\beta} \le 1 & \text{if } \beta - 1 < \alpha \le \beta \end{cases}. \tag{96}$$

Inequalities (96) are the desired weighted-sum bounds for the respective Regime 1 and 2. Thus, we complete the proof. □

6 Conclusion

Motivated by robustness concerns that are paramount in secure communications, in this work we study the robust GDoF of secure communication over a 2 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 Images bounds that were recently introduced in [35], 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.

A Proof of Lemma 1

In this section we present the proof of the SGDoF region $\mathcal{D}^{p}_{IC}$. The converse bounds are available from Lemma 8 of [26] (for single-user bound) and Lemma 2 of [43] (for the sum bound). The converse bounds are tight in Regime 3 and 4 defined in Theorem 1, as $\mathcal{D}^{p}_{IC} = \mathcal{D}^{f.p.}_{IC}$ 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 $\mathcal{D}^{p}_{IC}$ 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.,

$$Y_1(t) = \sqrt{P^{\alpha}}X_1(t) + \sqrt{P^{\beta}}X_2(t) + Z_1(t), \tag{97}$$

$$Y_2(t) = \sqrt{P}X_2(t) + Z_2(t), \tag{98}$$

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 (1) and (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.

A.1 The Achievability in Regime 1

The corner points of $\mathcal{D}^{p}_{IC}$ 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.

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 $\epsilon > 0$. In the following we suppress the channel-use index t for brevity. Define $X_1 = V_{11} + J_1 + V_{12}$ and $X_2 = V_2$, where V_{11}, J_1, V_{12}, V_2 are drawn respectively from the following sets (referred to as lattices):

$$V_{11} \in \Gamma_{11} \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm Q, \pm 2Q, \cdots, \pm \left\lfloor \sqrt{P^{\beta-\alpha-\epsilon}} \right\rfloor Q \right\}, \tag{99}$$

$$J_1 \in \Gamma_J \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm Q_J, \pm 2Q_J, \cdots, \pm \left(\left\lfloor \tfrac{1}{8}\sqrt{P^{1-\epsilon}} \right\rfloor - 1 \right) Q_J \right\}, \tag{100}$$

$$V_{12} \in \Gamma_{12} \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm 1, \pm 2, \cdots, \pm \left(\left\lfloor \tfrac{1}{4}\sqrt{P^{\alpha-1-2\epsilon}} \right\rfloor - 1 \right) \right\}, \tag{101}$$

$$V_2 \in \Gamma_2 \triangleq A\sqrt{P^{-\alpha}} \times \left\{0, \pm Q_J, \pm 2Q_J, \cdots, \pm \left(\left\lfloor \tfrac{1}{8}\sqrt{P^{1-\epsilon}} \right\rfloor - 1 \right) Q_J \right\}. \tag{102}$$

where for a real number ξ 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 Γ_2, satisfies the unit input power constraint.

Let V_{11}, V_{12}, J_1 and V_2 be independent and uniformly distributed in their respective lattices. Message W_1 is split into two parts, which are respectively encoded into V_{11} and V_{12}, and message W_2 is encoded into V_2, all with wiretap codebooks. The following rates are achievable under secrecy constraints [18, Theorem 4]:

$$R_1 \geq I(Y_1; V_{11}, V_{12}), \tag{103}$$

$$R_2 \geq I(Y_2; V_2) - I(Y_1; V_2|V_{11}, V_{12}). \tag{104}$$

We follow the argument in [18,54] to bound these rates from below. First we bound $I(Y_1; V_{11}, V_{12})$ from below as follows.

$$I(Y_1; V_{11}, V_{12}) \tag{105}$$

$$= H(V_{11}, V_{12}) - H(V_{11}, V_{12}|Y_1) \tag{106}$$

$$\geq (\log|\Gamma_{11}| + \log|\Gamma_{12}|)\left(1 - \Pr[\hat{V}_{11} \neq V_{11} \text{ or } \hat{V}_{12} \neq V_{12}]\right) - 1 \tag{107}$$

$$= \left(\log\left(2\left\lfloor\sqrt{P^{\beta-\alpha-\epsilon}}\right\rfloor + 1\right) + \log\left(2\left\lfloor\frac{1}{4}\sqrt{P^{\alpha-1-2\epsilon}}\right\rfloor - 1\right)\right)\left(1 - \Pr[\hat{V}_{11} \neq V_{11} \text{ or } \hat{V}_{12} \neq V_{12}]\right) - 1 \tag{108}$$

$$\geq (\beta - 1 - 3\epsilon)\log\bar{P}\left(1 - \Pr[\hat{V_{11}} \neq V_{11} \text{ or } \hat{V_{12}} \neq V_{12}]\right) - 3. \tag{109}$$

In (107), $\hat{V}_{11}$ and $\hat{V}_{12}$ follow the nearest-neighbor decoding rule and are respectively defined as

$$\hat{V}_{11} \triangleq \arg\min_{V_{11}\in\Gamma_{11}} \left|Y_1 - \sqrt{P^\beta}V_{11}\right|, \tag{110}$$

$$\hat{V}_{12} \triangleq \arg\min_{V_{12}\in\Gamma_{12}} \left|\tilde{Y}_1 - AQ_J\left[\frac{\tilde{Y}_1}{AQ_J}\right] - \sqrt{P^\beta}V_{12}\right|, \tag{111}$$

where $\tilde{Y}_1 \triangleq Y_1 - \sqrt{P^\beta}\hat{V}_{11}$, and $[x]$ rounds x to its nearest integer for all $x \in \mathbb{R}$. Inequality (107) holds due to Fano's inequality and the fact that V_{i1} is uniformly taken from Γ_{1i}, where $i = 1, 2$. Inequality (109) holds for P large enough because for $x \geq 2$, we have

$$\log(2\lfloor x\rfloor - 1) \geq \log x. \tag{112}$$

Next we follow steps similar to (106) – (109) to bound $I(Y_2; V_2)$ from below as follows

$$I(Y_2; V_2) = H(V_2) - H(V_2|Y_2) \tag{113}$$

$$= (\log|\Gamma_2|)\left(1 - \Pr[\hat{V}_2 \neq V_2]\right) - 1 \tag{114}$$

$$= \log\left(2\left\lfloor\frac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 1\right)\left(1 - \Pr[\hat{V}_2 \neq V_2]\right) - 1 \tag{115}$$

$$\geq (1 - \epsilon)\log\bar{P}\left(1 - \Pr[\hat{V}_2 \neq V_2]\right) - 4, \tag{116}$$

where in (114) $\hat{V}_2$ is defined as

$$\hat{V}_2 \triangleq \arg\min_{V_2\in\Gamma_2} \left|Y_2 - \sqrt{P^\alpha}V_2\right|, \tag{117}$$

As for the negative term in (104), $I(Y_1; V_2|V_{11}, V_{12})$, it is bounded above as follows.

$$I(Y_1; V_2|V_{11}, V_{12}) \leq I(Y_1; V_2|V_{11}, V_{12}, Z_1) \tag{118}$$

$$= I(\sqrt{P^\beta}J_1 + \sqrt{P^\alpha}V_2; V_2) \tag{119}$$

$$= H(\sqrt{P^\beta}J_1 + \sqrt{P^\alpha}V_2) - H(\sqrt{P^\beta}J_1) \tag{120}$$

$$\leq \log\left(4\left\lfloor\frac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 3\right) - \log\left(2\left\lfloor\frac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 1\right) \tag{121}$$

$$\leq 1. \tag{122}$$

Ineqaulity (118) holds since Z_1 is independent of V_2, and (119) follows because (V_{11}, V_{12}, Z_1) is independent of (J_1, V_2). Inequality (121) is true due to the uniform bound and the fact that $\sqrt{P^\beta}J_1 + \sqrt{P^\alpha}V_2$ takes value from the set $AQ_J \times \{0, \pm1, \pm2, \cdots, \pm2\left(\left\lfloor \frac{1}{8}\sqrt{P^{1-\epsilon}}\right\rfloor - 1\right)\}$. Finally (122) holds when P is large enough due to (112).

It remains to find upper bounds of $\Pr[\hat{V}_{11} \neq V_{11}$ or $\hat{V}_{12} \neq \hat{V}_{12}]$ in (109) and $\Pr[\hat{V}_2 \neq V_2]$ in (116). They vanish as P goes to infinity, as stated in the following lemma, whose proof is relegated to Appendix A.3.

Lemma 11. *Given $\hat{V}_{11}, \hat{V}_{12}$, and $\hat{V}_2$ are respectively defined in (110), (111) and (117), we have*

$$\lim_{P\to\infty} \Pr[\hat{V}_{11} \neq V_{11} \text{ or } \hat{V}_{12} \neq V_{12}] = 0, \tag{123}$$

$$\lim_{P\to\infty} \Pr[\hat{V}_2 \neq V_2] = 0. \tag{124}$$

Finally, by respectively plugging (109) into (103), and plugging (116) and (122) into (104), we get

$$R_1 \geq (\beta - 1 - 3\epsilon)\,\tfrac{1}{2}\log P + o(\log \bar{P}) = (\beta - 1)\,\tfrac{1}{2}\log P + o(\log \bar{P}) \tag{125}$$

$$R_2 \geq (1 - \epsilon)\,\tfrac{1}{2}\log P + o(\log \bar{P}) = \tfrac{1}{2}\log P + o(\log \bar{P}). \tag{126}$$

We arrive at $d_1 = \lim_{P\to\infty} \frac{R_1}{\frac{1}{2}\log P} = \beta - 1$, and $d_2 = \lim_{P\to\infty} \frac{R_1}{\frac{1}{2}\log P} = 1$. Thus the secure GDoF tuple $(d_1, d_2) = (\beta - 1, 1)$ is achievable with this scheme based on lattice alignment and aggregate decoding.

A.2 The Achievability in Regime 2

The corner points of $\mathcal{D}^p_{IC}$ 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.

Let $Q \triangleq \left\lfloor \sqrt{P^{\alpha-1-\epsilon}} \right\rfloor$ and $A \triangleq \sqrt{P^{2\epsilon}}$, where $\epsilon > 0$. In the following we suppress the channel-use index t for brevity. Define $X_1 = V_1 + J_1$ and $X_2 = V_2$, where

$$V_1 \in \Gamma_1 \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm1, \pm2, \cdots, \pm\left(\left\lfloor \tfrac{1}{2}\sqrt{P^{\alpha-1-2\epsilon}}\right\rfloor - 1\right)\right\}, \tag{127}$$

$$J_1 \in \Gamma_J \triangleq A\sqrt{P^{-\beta}} \times \left\{0, \pm Q, \pm 2Q, \cdots, \pm\left\lfloor \sqrt{P^{1-\alpha+\beta-\epsilon}}\right\rfloor Q\right\}, \tag{128}$$

$$V_2 \in \Gamma_2 \triangleq A\sqrt{P^{-\alpha}} \times \left\{0, \pm Q, \pm 2Q, \cdots, \pm\left\lfloor \sqrt{P^{1-\alpha+\beta-\epsilon}}\right\rfloor Q\right\}. \tag{129}$$

Note that such a choice of A, Q and the lattices Γ_1, Γ_J and Γ_2 satisfies the unit input power constraint.

Let V_1, J_1 and V_2 be independent and uniformly distributed in their respective lattices. Message W_1 and W_2 are respectively encoded into V_1 and V_2 with wiretap codebooks of rate R_1 and R_2. The following rates are achievable under the secrecy constraints [18, Theorem 4]:

$$R_1 \geq I(Y_1; V_1), \tag{130}$$

$$R_2 \geq I(Y_2; V_2) - I(Y_1; V_2|V_1). \tag{131}$$

To further bound these rates from below, we follow steps similar to (106) – (109) in Appendix A.1, and get a lower bound of $I(Y_1; V_1)$ as follows.

$$I(Y_1; V_1) \geq (\alpha - 1 - 2\epsilon)\,\tfrac{1}{2}\log P\left(1 - \Pr[\hat{V}_1 \neq V_1]\right) - 2. \tag{132}$$

where $\hat{V}_1$ is defined as

$$\hat{V}_1 = \arg\min_{V_1 \in \Gamma_1} \left| Y_1 - AQ \left[\frac{Y_1}{AQ} \right] - \sqrt{P^\beta} V_1 \right|. \tag{133}$$

To get a lower bound of $I(Y_2; V_2)$ we follow steps identical to (113) – (116)

$$I(Y_2; V_2) \geq (1 - \alpha + \beta - \epsilon) \tfrac{1}{2} \log P \left(1 - \Pr[\hat{V}_2 \neq V_2] \right) - 2, \tag{134}$$

where $\hat{V}_2$ is defined as

$$\hat{V}_2 = \arg\min_{V_2 \in \Gamma_2} \left| Y_2 - \sqrt{P} V_2 \right|. \tag{135}$$

And we can bound $I(Y_1; V_2|V_1)$ from above by following steps similar to (118) – (122)

$$I(Y_1; V_2|V_1) \leq 1. \tag{136}$$

With a similar reasoning to the one in Lemma 11, one can show that for both $i = 1, 2$, $\Pr[\hat{V}_i \neq V_i] \to 0$ as $P \to \infty$. Finally, by plugging (132) into (130), and by plugging (134) and (136) into (131), we get

$$R_1 \geq (\alpha - 1 - 2\epsilon) \tfrac{1}{2} \log P + o(\log \bar{P}) = (\alpha - 1) \tfrac{1}{2} \log P + o(\log \bar{P}), \tag{137}$$

$$R_2 \geq (1 - \alpha + \beta - \epsilon) \tfrac{1}{2} \log P + o(\log \bar{P}) = (1 - \alpha + \beta) \tfrac{1}{2} \log P + o(\log \bar{P}). \tag{138}$$

By applying the definition of GDoF we get $d_1 = \lim_{P \to \infty} \frac{R_1}{\frac{1}{2} \log P} = \alpha - 1$ and $d_2 = \lim_{P \to \infty} \frac{R_2}{\frac{1}{2} \log P} = 1 - \alpha + \beta$. Hence the GDoF tuple $(d_1, d_2) = (\alpha - 1, 1 - \alpha + \beta)$ is achievable with this scheme.

A.3 Proof of Lemma 11

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 (110), and seeing that $Z_1 \sim \mathcal{N}(0, 1)$, we have

$$\Pr[\hat{V}_{11} \neq V_{11}] \leq \Pr\{\mathcal{E}\} \leq 2 \exp\left(-\frac{1}{8} A^2 \right). \tag{139}$$

Next we move on and argue that V_{12} can be correctly decoded with (111) 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 $\sqrt{P^\beta} \times \Gamma_J + \sqrt{P^\alpha} \times \Gamma_2$. [11] 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

[11] For two sets Γ_1 and Γ_2, define $\Gamma_1 + \Gamma_2 \triangleq \{a + b | a \in \Gamma_1, b \in \Gamma_2\}$ as the sum set of Γ_1 and Γ_2.

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 (111) when $\mathcal{E}^c$ occurs and V_{11} is correctly decoded, and

$$Pr[\hat{V}_{12} \neq V_{12} | \hat{V}_{11} = V_{11}] \leq \Pr\{\mathcal{E}\} \leq 2\exp\left(-\frac{1}{8}A^2\right). \tag{140}$$

Finally we can bound $\Pr[\hat{V}_{11} \neq V_{11}$ or $\hat{V}_{12} \neq V_{12}]$ as follows.

$$\begin{aligned}
&\Pr[\hat{V}_{11} \neq V_{11} \text{ or } \hat{V}_{12} \neq V_{12}] && (141)\\
&\leq \Pr[\hat{V}_{11} \neq V_{11}] + \Pr[\hat{V}_{12} \neq V_{12}] && (142)\\
&\leq \Pr[\hat{V}_{11} \neq V_{11}] + \Pr[\hat{V}_{12} \neq V_{12} | \hat{V}_{11} = V_{11}] \Pr[\hat{V}_{11} = V_{11}] \\
&\qquad + \Pr[\hat{V}_{12} \neq V_{12} | \hat{V}_{11} \neq V_{11}] \Pr[\hat{V}_{11} \neq V_{11}] && (143)\\
&\leq \Pr[\hat{V}_{11} \neq V_{11}] + \Pr[\hat{V}_{12} \neq V_{12} | \hat{V}_{11} = V_{11}] + \Pr[\hat{V}_{11} \neq V_{11}] && (144)\\
&\leq 6\exp\left(-\frac{1}{8}A^2\right), && (145)
\end{aligned}$$

where we use the union bound in (142), and the law of total probability in (143). Inequality (145) holds because of (139) and (140). Since $A^2 = O(P^{2\epsilon})$ and $\epsilon > 0$, we have $\Pr[\hat{V}_{11} \neq V_{11}$ 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 (117) when $\mathcal{E}$ occurs, and

$$\Pr[\hat{V}_2 \neq V_2] \leq \Pr\{\mathcal{E}\} \leq 2\exp\left(-\tfrac{1}{8}A^2P^{1-\alpha}Q_J^2\right). \tag{146}$$

Note that $A^2P^{1-\alpha}Q_J^2 = O(P^{\alpha-1+\epsilon})$ 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.

B Proof of Theorem 2

In this section, we provide the proof of Theorem 2, which characterizes the SGDoF region of the ZBC with perfect and finite precision CSIT, respectively.

B.1 The SGDoF Region with Perfect CSIT

B.1.1 Converse

To show the converse part, we cast the Gaussian channel model into the deterministic model defined in Section 5.1.3. Lemma 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.

$$\begin{aligned}
nR_1 &\leq I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1) + no(\log\bar{P}) && (147)\\
&= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1, (\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}; W_1) + no(\log\bar{P}) && (148)\\
&= I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}; W_1) + I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1; W_1 | (\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}) + no(\log\bar{P}) && (149)\\
&\leq I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_2)^{\min\{(\beta-\alpha)^+,1\}}; W_1) + H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1 | (\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}) + no(\log\bar{P}) && (150)\\
&\leq n\left(\max\{\alpha,\beta\} - \min\{(\beta-\alpha)^+,1\}\right)\log\bar{P} + no(\log\bar{P}) && (151)\\
&= n\max\{\alpha,\beta-1\}\log\bar{P} + no(\log\bar{P}), && (152)
\end{aligned}$$

where $\overline{\boldsymbol{Y}}_1$ and $\boldsymbol{B}$ are defined in Section 5.1.3. Equality (148) 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 (149). Next we note that, since both $(\overline{\boldsymbol{Y}}_1)^{\min\{(\beta-\alpha)^+,1\}}$ and $(\overline{\boldsymbol{Y}}_2)^{\min\{(\beta-\alpha)^+,1\}}$ contain top $\min\{(\beta-\alpha)^+,1\}$ segment 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 (150). The first term in (150) is $no(\log \bar{P})$ due to Lemma 3, and we apply the uniform bound to obtain (151). Equality (152) 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

$$\begin{aligned}
nR_2 &\leq I(\overline{\boldsymbol{Y}}_2; W_2) + no(\log \bar{P}) && (153)\\
&= I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2, (\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}; W_2) + no(\log \bar{P}) && (154)\\
&= I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}; W_2) + I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2; W_2 | (\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}) + no(\log \bar{P}) && (155)\\
&\leq I_{\mathcal{G}}((\overline{\boldsymbol{Y}}_1)^{\min\{1,(\beta-\alpha)^+\}}; W_2) + H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2 | (\overline{\boldsymbol{Y}}_2)^{\min\{1,(\beta-\alpha)^+\}}) + no(\log \bar{P}) && (156)\\
&\leq n\left(1-(\beta-\alpha)^+\right)^+ \log \bar{P} + no(\log \bar{P}), && (157)
\end{aligned}$$

where $\overline{\boldsymbol{Y}}_2$ is defined in (24) in Section 5.1.3. Equality (154) 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 (155). Note that $(\overline{\boldsymbol{Y}}_1)^{\min\{1,(\beta-\alpha)^+\}}$ contains the top-$\min\{1,(\beta-\alpha)^+\}$ segment 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 (156). Finally we arrive at (157) by applying Lemma 3 and the secrecy constraint (4) to the first term in (156), and the uniform bound to the second term. Thus the bound $d_2 = \lim_{P\to\infty} \frac{nR_2}{n\frac{1}{2}\log P} \leq (1-(\beta-\alpha)^+)^+$.

B.1.2 Achievability

To show the achievability, we present two schemes respectively for the following two regimes: (a) Regime P1: $\beta - 1 \leq \alpha$, 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

$$\begin{bmatrix} X_1(t) \\ X_2(t) \end{bmatrix} = c_1(t) \begin{bmatrix} 1 \\ 0 \end{bmatrix} U_1(t) + c_2(t) \begin{bmatrix} -G_{12}(t)\sqrt{P^\beta} \\ G_{11}(t)\sqrt{P^\alpha} \end{bmatrix} U_2(t), \tag{158}$$

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

$$c_2(t) = \frac{1}{\sqrt{2\left(|G_{12}(t)|^2 P^\beta + |G_{11}(t)|^2 P^\alpha\right)}} \tag{159}$$

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 cross-link-free channel as follows.

$$Y_1(t) = \frac{1}{2} G_{11}(t)\sqrt{P^\alpha} U_1(t) + Z_1(t), \tag{160}$$

$$Y_2(t) = \frac{G_{22}(t)\sqrt{P^{1+\alpha}}}{\sqrt{2\left(|G_{12}(t)|^2 P^\beta + |G_{11}(t)|^2 P^\alpha\right)}} U_2(t) + Z_2(t). \tag{161}$$

Channel (160) allows GDoF α for W_1, and channel (161) allows $1+\alpha-\max\{\alpha,\beta\}=1-(\beta-\alpha)^+$ for W_2. Note that the secrecy constraint (4) 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 (4) satisfied in the mean time. Here we conclude the proof.

B.2 The SGDoF Region with Finite Precision CSIT

To show $\mathcal{D}_{BC}^{f.p.}$, we continue the definition of the channel regimes in Theorem 1, and further divide Regime 4 into the following two sub-regimes: (a) Regime 4.1, satisfying $\beta\le 1$ and $\beta\le\alpha$; and (b) Regime 4.2, satisfying $\beta\le 1$ 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 5.3 for the corresponding regimes, which still holds when full transmitter cooperation is allowed. The SGDoF region of Regime 3 is identical to $\mathcal{D}_{BC}^{p}$ of the same regime, and the a achievable scheme does not rely on the perfect CSIT assumption. So the proof in Appendix B.1 holds for finite precision CSIT. Finally, the proof for Regime 4.1 follows from the results in [53]. As a result, only the SGDoF region of Regime 4.2, which is $\{(d_1,d_2)\in\mathbb{R}_+^2:\ d_1\le\alpha, d_1+d_2\le 1+\alpha-\beta\}$, remains to be shown.

First let us consider the converse proof. The single-user bound $d_1\le\alpha$ follows from the proof in Appendix B.1 in the corresponding channel regime. To show the sum bound, $d_1+d_2\le 1+\alpha-\beta$, we cast the Gaussian ZBC model into the deterministic model defined in Section 5.1.3. Lemma 3 implies that this incurs no GDoF loss. Next we apply Fano's inequality, and get

$$\begin{aligned}
nR_1+nR_2 &\le I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1;W_1)+I_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2;W_2)+no(\log\bar{P}) && (162)\\
&\le H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1)-H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_1)+H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2)-H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2|W_2)+no(\log\bar{P}) && (163)\\
&= H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_2)-H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_1|W_1)+H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2|W_1)-H_{\mathcal{G}}(\overline{\boldsymbol{Y}}_2|W_2)+no(\log\bar{P}) && (164)\\
&\le \max\{1-\beta,-\alpha\}^+n\log P+\max\{\beta-1,\alpha\}^+n\log Pno(\log\bar{P}) && (165)\\
&= (1+\alpha-\beta)n\log P+no(\log\bar{P}), && (166)
\end{aligned}$$

where $\overline{\boldsymbol{Y}}_1$ and $\overline{\boldsymbol{Y}}_2$ are defined respectively in (23) and (24). We apply (26) and the secrecy constraint (4) to obtain (164). Inequality (165) holds due to Lemma 5. Since $\beta\le 1$ in this regime, we have (166), and in the GDoF limit we obtain the sum bound $d_1+d_2=\lim_{P\to\infty}\frac{R_1+R_2}{\frac{1}{2}\log P}\le 1+\alpha-\beta$.

Finally, let us consider the achievability. Since the 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 Proof of Lemma 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 λ sub-section of the random variables as follows:

$$(T)^\lambda=(T)_\nu^{\lambda+\nu}=\left\lfloor\frac{T-\bar{P}^{\lambda+\nu}\left\lfloor\frac{T}{\bar{P}^{\lambda+\nu}}\right\rfloor}{\bar{P}^\nu}\right\rfloor=\left\lfloor\frac{T}{\bar{P}^\nu}\right\rfloor, \tag{167}$$

$$(U)^{\mu} = (U)_{\nu}^{\mu+\nu} = \left\lfloor \frac{U - \bar{P}^{\mu+\nu}\left\lfloor \frac{U}{\bar{P}^{\mu+\nu}} \right\rfloor}{\bar{P}^{\nu}} \right\rfloor = \left\lfloor \frac{U}{\bar{P}^{\nu}} \right\rfloor, \tag{168}$$

$$(V)^{\lambda} = (T \boxplus U)_{\nu}^{\lambda+\nu} = \left\lfloor \frac{V - \bar{P}^{\lambda+\nu}\left\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \right\rfloor}{\bar{P}^{\nu}} \right\rfloor. \tag{169}$$

Note that the last equality of (167) and (168) holds because $\lfloor \frac{T}{\bar{P}^{\lambda+\nu}} \rfloor = \lfloor \frac{U}{\bar{P}^{\mu+\nu}} \rfloor = 0$.

Next we simplify (169) in the way as is done to (167) and (168). 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 $\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \rfloor$, which is a term appearing in the denominator of (169).

$$\frac{V}{\bar{P}^{\lambda+\nu}} = G_1 \frac{T}{\bar{P}^{\lambda+\nu}} + G_2 \frac{U}{\bar{P}^{\lambda+\nu}} + \frac{\eta_T + \eta_U}{\bar{P}^{\lambda+\nu}} \tag{170}$$

$$= \tilde{\eta}_1 + \tilde{\eta}_2 + \tilde{\eta}_3, \tag{171}$$

where $\tilde{\eta}_i$ is the i^{th} term in (170). It is obvious that $\tilde{\eta}_1, \tilde{\eta}_2 \in [-\Delta, \Delta]$, and $\tilde{\eta}_3 \in [0, 2]$. So $\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \rfloor$ 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 (169) further as follows.

$$(V)^{\lambda} = \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor + \underbrace{\left\lfloor -\bar{P}^{\lambda+\nu} \left\lfloor \frac{V}{\bar{P}^{\lambda+\nu}} \right\rfloor \right\rfloor + E}_{\tilde{E}} \tag{172}$$

$$= \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor + \tilde{E}, \tag{173}$$

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 $\delta_T = \frac{T}{\bar{P}^{\nu}} - (T)^{\lambda}$, $\delta_U = \frac{U}{\bar{P}^{\nu}} - (U)^{\lambda}$, $\epsilon_T = G_1 (T)^{\lambda} - \lfloor G_1 (T)^{\lambda} \rfloor$, $\epsilon_U = G_2 (U)^{\mu} - \lfloor G_2 (U)^{\mu} \rfloor$, and $\epsilon = \frac{V}{\bar{P}^{\nu}} - \lfloor \frac{V}{\bar{P}^{\nu}} \rfloor$, whose values are in $[0, 1)$. With these truncation terms, we relate Z with $(V)^{\lambda}$ as follows.

$$Z = \left\lfloor G_1 (T)^{\lambda} \right\rfloor + \lfloor G_2 (U)^{\mu} \rfloor \tag{174}$$

$$= G_1 (T)^{\lambda} + G_2 (U)^{\mu} - (\epsilon_T + \epsilon_U) \tag{175}$$

$$= G_1 \frac{T}{\bar{P}^{\nu}} + G_2 \frac{U}{\bar{P}^{\nu}} - (G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U) \tag{176}$$

$$= \frac{1}{\bar{P}^{\nu}} (\lfloor G_1 T \rfloor + \lfloor G_2 U \rfloor) - \left(\frac{\eta_T + \eta_U}{\bar{P}^{\nu}} + G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U \right) \tag{177}$$

$$= \left\lfloor \frac{V}{\bar{P}^{\nu}} \right\rfloor + \epsilon - \left(\frac{\eta_T + \eta_U}{\bar{P}^{\nu}} + G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U \right) \tag{178}$$

$$= (V)^{\lambda} - \tilde{E} - \underbrace{\left(\frac{\eta_T + \eta_U}{\bar{P}^{\nu}} + G_1 \delta_T + G_2 \delta_U + \epsilon_T + \epsilon_U - \epsilon \right)}_{E'} \tag{179}$$

$$= (V)^{\lambda} - \tilde{E} - E', \tag{180}$$

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_Σ 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 $H((T \boxplus U)^\lambda) = H((T)^\lambda \boxplus (U)^\lambda) + O(1)$.

References

[1] Y. C. Chan and S. A. Jafar, "Secure gdof of the z-channel with finite precision csit: How robust are structured codes?" in *2020 IEEE International Symposium on Information Theory (ISIT)*, 2020, pp. 1558–1563.

[2] Lizhong Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[3] 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.

[4] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Transactions on Information Theory*, vol. 49, no. 7, pp. 1691–1706, July 2003.

[5] 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, no. 9, pp. 3936–3964, Sep. 2006.

[6] S. Jafar and S. Shamai, "Degrees of freedom region for the MIMO X channel," *IEEE Trans. on Information Theory*, vol. 54, no. 1, pp. 151–170, Jan. 2008.

[7] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the k-user interference channel," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3425–3441, Aug 2008.

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

[9] A. S. Motahari, S. Oveis-Gharan, M. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4799–4810, 2014.

[10] 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.

[11] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6463–6486, Oct 2011.

[12] 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.

[13] 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.

[14] 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.

[15] S. Jafar and S. Vishwanath, "Generalized Degrees of Freedom of the Symmetric Gaussian K User Interference Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3297–3303, July 2010.

[16] X. He and A. Yener, "The Gaussian many-to-one interference channel with confidential messagess," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2730 – 2745, May 2011.

[17] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2121–2138, April 2014.

[18] 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.

[19] ——, "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.

[20] 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.

[21] 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, no. 3, pp. 2093–2103, March 2018.

[22] K. Banawan and S. Ulukus, "Secure degrees of freedom in networks with user misbehavior," *Entropy*, vol. 21, no. 10, 2019. [Online]. Available: https://www.mdpi.com/1099-4300/21/10/945

[23] J. Chen and C. Geng, "Optimal Secure GDoF of Symmetric Gaussian Wiretap Channel with a Helper," *arXiv e-prints*, p. arXiv:1812.10457, Dec 2018.

[24] 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, Dec 2019.

[25] F. Li and J. Chen, "Adding Common Randomness Can Remove the Secrecy Constraints in Communication Networks," *arXiv e-prints*, p. arXiv:1907.04599, Jul. 2019.

[26] 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.

[27] 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.

[28] 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, no. 1, pp. 406–417, Jan 2019.

[29] ——, "Optimality of simple layered superposition coding in the 3 user MISO BC with finite precision CSIT," *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7181–7207, Nov 2019.

[30] 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, no. 11, pp. 7208–7217, Nov. 2018.

[31] 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.

[32] 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.

[33] 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.

[34] J. Wang, B. Yuan, L. Huang, and S. A. Jafar, "GDoF of Interference Channel with Limited Cooperation under Finite Precision CSIT," *arXiv e-prints*, p. arXiv:1908.00703, Aug 2019.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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)*, 2015, pp. 1–5.

[40] 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)*, Dec 2015, pp. 1–6.

[41] T. Cover, "Broadcast channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 2–14, January 1972.

[42] 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*, July 2008, pp. 379–383.

[43] 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*, March 2009, pp. 318–323.

[44] 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.

[45] 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, no. 3, pp. 572–587, March 2017.

[46] 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, no. 4, pp. 848–857, April 2019.

[47] 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.

[48] 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, no. 6, pp. 2493–2507, June. 2008.

[49] 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.

[50] Y.-C. Chan and S. A. Jafar, “Exploring Aligned-Images Bounds: Robust Secure GDoF of 3-to-1 Interference Channel,” *Technical Report, https://escholarship.org/uc/item/8nh0m0qm*, October 2020.

[51] 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*, Nov 2016, pp. 909–914.

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

[53] Y.-C. Chan, C. Geng, and S. A. Jafar, “Robust optimality of TIN under secrecy constraints,” *Technical Report, https://escholarship.org/uc/item/4242x608*, October 2019.

[54] G. Bresler and D. Tse, “The two-user Gaussian interference channel: a deterministic view,” *European Transactions in Telecommunications*, vol. 19, no. 4, pp. 333–354, June 2008.