On Deterministic Models for Capacity Approximations in Interference Networks and Information Theoretic Security

vorgelegt von
Rick Fritschek, M.Sc.
geb. in Schmalkalden

von der Fakultät IV - Elektrotechnik und Informatik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades

Doktor der Ingenieurwissenschaften
- Dr.-Ing. -

genehmigte Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr.-Ing. Rafael Schaefer
Gutachter: Prof. Giuseppe Caire, Ph.D.
Gutachter: Prof. Suhas Diggavi, Ph.D.
Gutachter: PD Dr.-Ing. Gerhard Wunder

Tag der wissenschaftlichen Aussprache: 13. Juni, 2018

Berlin 2018

Abstract

This work considers two major challenges of modern wireless communication. The first challenge is the analysis and management of interference in multi-user wireless channels. The other challenge is to provide information-theoretic security for future wireless networks. The second chapter considers the first challenge, in particular, the Gaussian interfering multiple access channel (G-IMAC). This channel model is an example of a multi-user interference-affected network. However, even for more simple models, such as the Gaussian interference channel, it is hard to derive good upper bounds and develop achievable schemes to show information-theoretic capacity results. In fact, a complete solution of that channel model is an open problem for over 40 years. However, recent developments have shown that deterministic models can approximate these Gaussian models within a constant-bit gap. These deterministic models view input signals as binary expansion and cut-off the bits which are corrupted by noise. They, therefore, yield insights into the high signal-to-noise regime, where the noise effected signal part has just a minor contribution to the overall capacity and emphasizes the contribution of interference. We, therefore, use the same strategy and look into deterministic approximations of the G-IMAC. We find achievable schemes and converse bounds for arbitrary interference strength and some channel-gain symmetry assumptions. Moreover, we transfer those approximate results to the G-IMAC and show a constant-gap capacity result for this channel model. The most interesting outcome of this work is, that the G-IMAC has multi-user gain. This means that for two users in each cell, half of the interference strength can be used for communication. This is in contrast to the classical Gaussian interference channel (G-IC), where for example treating interference as noise (TIN) is optimal under certain conditions. The G-IMAC, therefore, has an increase in degrees-of-freedom, compared to the G-IC. Chapter 3 considers the second challenge, where we look into the Gaussian multiple access wiretap channel. Here we use similar techniques, namely deterministic approximations, to develop achievable schemes which hold for asymmetric channel gain configurations. Moreover, we develop novel upper bounds, again based on previous insights from the G-IMAC, which are within a constant-gap for certain interference regimes. We then transfer those results to the Gaussian multiple access wiretap channel. For the upper bound of the Gaussian model, we use an in-between approximation and some recent results to provide a bridge between the

techniques for the Gaussian model and the linear deterministic model. In Chapter 4 we also consider wireless security, but this time we look into key generation scenarios. We develop a novel deterministic model for key generation with is based on the linear deterministic and the lower triangular deterministic model. It incorporates the key generation viewpoint, i.e. the channel gain is used as a source of randomness for key generation and recovers known results without the tedious state-of-the-art methods. We show that this model gives insights into the previously challenging task of analysing new key generation techniques. Moreover, it can help to communicate the results of information theoretic secrecy analysis with cryptography experts.

Zusammenfassung

Diese Arbeit behandelt zwei wichtige Herausforderungen der modernen drahtlosen Kommunikation. Die erste Herausforderung ist die Analyse und Handhabung von Interferenz in drahtlosen Mehrnutzerkanälen. Die andere Herausforderung ist informationstheoretische Sicherheit für moderne drahtlose Netzwerke zu schaffen. Das zweite Kapitel behandelt die erste Herausforderung und im speziellen den Gaussschen Interferenz Mehrfachzugriffskanal (Gaussian interfering multiple access channel - G-IMAC). Dieses Kanalmodell ist ein Beispiel für Interferenz behaftete Mehrnutzerkanäle. Jedoch stellt schon die Analyse der Kanalkapazität und damit der Beweis von oberen Schranken und die Entwicklung von Erreichbarkeitsresultaten für einfachere Modelle wie den Interferenzkanal ein Problem dar. Tatsächlich ist die allumfassende Kapazitätsanalyse des Interferenzkanals seit über 40 Jahren ungelöst. Jedoch haben aktuelle Entwicklungen gezeigt, dass deterministische Modelle Näherungslösungen für diese Gaussian Modelle generieren können. Die deterministischen Modelle betrachtet dabei die Eingangssignale in ihrer Binärentwicklung und schneiden die Bits, oder Stellen, welche rauschbehaftet sind, ab. Diese Methode gibt damit Einsicht in den Signalbereich welcher durch ein hohes Signal-zu-Rausch Verhältnis gekennzeichnet ist. In diesen Bereich spielt der Signalteil, welcher rauschbehaftet ist, nur eine untergeordnete Rolle in Bezug auf die Kapazität und die Wirkung der Interferenz wird in den Vordergrund gerückt. Demzufolge ist es naheliegend die gleichen deterministischen Näherungen für den G-IMAC zu verwenden. Darauf aufbauend können in dieser Arbeit Erreichbarkeitsresultate und obere Schranken für beliebige Interferenzstärken und spezielle Symmetrieannahmen gezeigt werden. Außerdem werden diese Näherungsresultate auf den Gausschen IMAC übertragen was zu einer Kapazitätsnäherung führt, welche innerhalb einer Konstante zu der tatsächlichen Kapazität liegt. Das interessante Resultat dieser Arbeit ist, dass der G-IMAC von den Mehrfachzugriff profitiert. Im Speziellen, für zwei Nutzer in jeder Zelle, kann die Hälfte der Interferenzstärke für Kommunikation benutzt werden. Im Gegensatz dazu steht der klassische Gausssche Interferenz Kanal (G-IC), bei dem *treating interference as noise* unter gewissen Voraussetzungen optimal ist und somit der Interferenzbereich nicht genutzt werden kann beziehungsweise wie Rauschen betrachtet wird. Der G-IMAC hat somit mehr Freiheitsgrade als der G-IC. Das dritte Kapitel behandelt die zweite Herausforderung der Sicherheit für drahtlose Kanäle und im speziellen den Gausschen

Mehrfachzugriffsabhörkanal (Gaussian multiple access wiretap channel - G-MAC-WT). Hier werden ähnliche Techniken benutzt, das heißt deterministische Näherungsverfahren, um Erreichbarkeitsresultate für asymmetrische Kanalstärken zu zeigen. Weiterhin werden neue obere Schranken entwickelt, basierend auf den vorherigen Resultaten, welche innerhalb einer Konstante zu den Erreichbarkeitsresultaten liegen. Diese Resultate werden dann wieder auf den Gausschen Fall übertragen und schaffen eine Kapazitätsnäherung innerhalb einer Konstante. Dafür wird ein Zwischennäherungsmodell eingeführt und aktuelle Techniken aus der Literatur verwendet, um eine Brücke zwischen den Techniken für das lineare deterministische Modell und den Gausschen Modell zu schaffen. Das vierten Kapitel behandelt die sichere Schlüsselgenerierung in drahtlosen Netzwerken. Es wird ein neues deterministisches Modell für die Schlüsselgenerierung entwickelt, welches auf den linearen deterministischen und den unteren dreieckigen deterministischen Modell basiert. Es inkludiert die Schlüsselgenerierungssichtweise, i.e. der Kanalfaktor wird als Quelle für den Zufall für die Schlüsselgenerierung benutzt. Das Modell liefert bekannte Resultate ohne die langwierigen State-of-the-Art Techniken benutzen zu müssen. Weiterhin ist es in der Lage Erkenntnisse zu generieren, welche mit Standardmethoden eine Herausforderung darstellten. Somit ist es damit möglich, Schlüsseltausch Szenarien zu analysieren welche mit Standardmethoden nicht bearbeitet werden konnten.

Acknowledgements

First of all, I want to thank my advisor Dr. Gerhard Wunder for giving me the opportunity to work with him. I am grateful for the scientific freedom and support during my time at the Technische Universität Berlin and the Freie Universität Berlin. I am also grateful to Prof. Giuseppe Caire and Prof. Suhas Diggavi for serving as referees of this dissertation. Moreover, I would like to thank Prof. Rafael Schaefer for serving as the chairman of the dissertation committee.

I want to thank all my friends and colleagues at the Technische Universität Berlin and the Freie Universität Berlin. In particular, I enjoyed the many conversations and discussions about science and life in general.

Moreover, I want to thank all my friends and family. I am grateful beyond words to my parents, Carina and Jens, for their constant unquestioning support, and encouragement. Finally, my deepest gratitude goes to Hannah for her endless love, encouragement, patience and emotional support.

Contents

1. Introduction

1.1. Motivation

The information age is the prevalent period of human history. It is arguably characterized by advances in storing, processing and transmission of data and therefore information. The transmission of information is growing, and the global IP traffic is projected to increase nearly threefold between 2016 and 2021 [Cis17]. The transmission of information is mainly divided between wireless and optical transport media. However, due to the smartphone revolution, wireless and smartphone traffic is expected to exceed PC traffic by 2021 [Cis17]. This motivates ongoing research and development to advance information transmission capabilities of wireless networks. Currently, economic driven research is focusing on the next wireless systems standard 5G (5-th Generation), which has a target goal of a 1000× increase in total data, which the network can serve, from 4G (LTE-A) to 5G [ABC$^+$14].
The two fundamental key challenges of wireless networks are *fading* and *interference*. Fading is a variation of the channel gain strengths due to multipath signal propagation, distance attenuation and shadowing by obstacles. While the traditional point of view was that fading is a harmful phenomenon, it has been shifted and nowadays its been seen as opportunity [TV05]. An example for this, is its use in physical layer security, which plays a key role in Chapter 4. The other key challenge is interference. This phenomenon is due to the inherent nature of wireless communication channels being a shared communication medium.

Interference networks. Throughout the last decades, extensive research was conducted to illuminate the impact of interference on the capacity of wireless networks. However, even for the simplest inference channel model, the two-user interference channel (IC), a complete capacity characterisation remains an unsolved problem for over 40 years. One of the major breakthroughs in recent time was an one bit capacity approximation of the Gaussian IC in [ETW08]. As a by-product, they defined the notion of *generalized degrees of freedom* (GDoF), which can be thought as interference dependent degrees-of-freedom (DoF). This notion will play a key role in Chapter 2 and Chapter 3. The result motivated a series of investigations towards constant-gap approximations of more complex models, e.g. [AST08], [BPT10], [NCL10], [ST11], [OEN14]. However, even constant-gap capacity

approximations seemed to be out-of-sight for most other Gaussian channel models, due to the noise properties. Those networks can be substantially simplified by removing the noise, in an appropriate way, which results in deterministic models. Those deterministic models can provide insights into the nature of the channel model, which in turn can lead to achievable schemes and upper bounds for the Gaussian equivalents. Two recent examples are the *linear deterministic model* (LDM), which emerged with the work of Avestimehr, Diggavi and Tse in [ADT07,ADT11] and the *lower triangular deterministic model* (LTDM), from [NMA13]. This thesis makes extensive use of those models, and a short introduction is therefore provided in Section 1.4. Another key technique for interference networks is the so-called *interference alignment* (IA), introduced in [MAMK08], [CJ08] and [JS08]. It was subsequently used for example in [MOGMAK14], which introduced *real* IA, using scaled integer lattices. Moreover, it was used in [ST08] for cellular models, introducing the Gaussian interfering multiple access channel and for example in [MAT10] and [AGK13] for different assumptions on the channel state information. The goal of IA is to align interfering signal parts in some dimension to maximize the interference-free signalling dimensions. These methods can be broadly categorized into two classes: vector-space alignment and signal-space alignment [NMA13]. Vector-space alignment refers to alignment in classical signalling dimensions such as time, frequency or multiple antennas. There, channel coefficients need to show enough variation in the specified dimension to enable those techniques. If the channel has only a single antenna on both ends and is time-invariant and frequency-flat, classical IA schemes do not work anymore. In those cases, signal-scale alignment methods need to be used. These techniques use for example lattice coding to split the channel in several power levels, which allow for an alignment on those levels. This thesis makes use of signal-scale alignment in Chapter 2 and Chapter 3.

Security. The technological advances in the information age also gave rise to the emerging challenge of security. Furthermore, new application scenarios such as the internet of things and others reinforce the need for security methods. Advances in processing speed and quantum computation research emphasize the need for security methods which are unconditional on the capabilities of an potential attacker[1]. This requirement is fulfilled by information theoretic security, pioneered by Claude Shannon in [Sha49], with the definition of perfect security. The simplest method is to use a one-time pad along with a key to encrypt and decrypt the message. However, this result had the practical disadvantage, that it needs long keys. The next breakthrough was made by Wyner in [Wyn75], in which he defined the wiretap channel and showed secrecy results under a new weaker asymptotic definition of secrecy. The used methods utilize inherent channel properties such as noise to secure communication and are therefore independent of key length. Recent studies defined

[1] unlike standard encryption methods, which build on computational complexity

a multi-user case of the wiretap channel, coined multiple-access wiretap channel (MAC-WT) in [TY08a], which will be analysed in Chapter 3. Moreover, Ahlswede and Csiszár introduced an alternate view of information theoretic security by defining a source model for secret key agreement in [AC93]. Wiretap type models and key-agreement models have a strong relationship since the capacity of the former is generally bigger or equal than the latter. These key-agreement models assume that both communication ends share a source of common randomness. Recent results in [YRS06] and [WTS07] have shown that the wireless channel can be exploited to generate a source of common randomness. The idea revolves around the phenomenon of reciprocity, which states that the varying channel gains[2], are the same in both communication directions. Chapter 4 analysis those scenarios by introducing a novel deterministic model.

1.2. Contributions and Outline of the Thesis

This thesis analyses and builds on the aforementioned points under the umbrella of using deterministic approximations of Gaussian networks to establish intuition and new results. The linear deterministic model, as well as the lower triangular deterministic model, will be for example used on the interfering multiple-access channel, which is the topic of Chapter 2. This channel can be thought of as two multiple-access channels which are interfering each other. Surprisingly, similar techniques can be used to analyse the multiple-access wiretap channel, which is part of Chapter 3. There, we also use the linear deterministic model as a first approximation. Moreover, we present a novel deterministic model, which builds on the LDM and LDTM to analyse key-generation models in Chapter 4.

In **Chapter 2** we analyse the Gaussian interfering multiple access channel (G-IMAC). We start by looking into the deterministic approximation of the model, denoted by LD-IMAC. We show achievable schemes and provide converse proofs for upper bounds in the weak interference regime. The achievable schemes can be seen as a form of signal-scale alignment which acts on the bit-levels of the approximation model and aligns them orthogonally. We will see that these methods do not lead to constant-gap results. There is a power dependent gap at certain channel gain parameters, due to the structure of the scheme. Transferring the achievable schemes to the Gaussian case via layered lattice codes also transfers this gap, which shows that the mentioned orthogonal bit-level coding strategies are not strong enough. The lower triangular deterministic model provides an alternative approximation model, where the fine channel gain is included. This yields an approximation where the bit-levels are mutually dependent, depending on the resulting lower triangular channel gain matrices. We will see, that this improved model (LTD-

[2] which is due to fading

IMAC) will lead to achievable schemes which reach the converse bound from the previous LD-IMAC considerations. Moreover, the achievable schemes lead to achievable schemes in the Gaussian case and we can show a constant-gap capacity result for the whole interference regime within a certain computable non-outage channel gain set. To limit the number of cases, all results were proved for the symmetrical case. Moreover, we will shed some light on the connection between the two approximation models.

The work presented in Chapter 2 has been published in [FW14a, FW14b, FW15a, FW15b, FW16b] and should be published in [FW17c].

In **Chapter 3** we study the Gaussian two-user multiple access wiretap channel (G-MAC-WT) and the Gaussian wiretap channel with a helper (G-WT-H). Previous results on both models were limited to *secure* DoF (SDoF) results, which were obtained by IA methods, in particular, real interference alignment. However, real IA is limited to asymptotic results and has the disadvantage of being limited to certain non-computable channel gain parameters and symmetry of the channel gains. We start again by approximating the models, with the LDM and use bit-level alignment methods, similar to the ones used for the LD-IMAC. These methods yield achievable schemes which are independent of the channel gains and give insights into the scaling of the secure rate for asymmetrical channel gains. One could view the results as *generalized* SDoF. We can show that the resulting achievable secrecy rates tend to the s.d.o.f. for vanishing channel gain differences. We present these achievable schemes for both models and show that they can be transferred to the Gaussian model with layered lattice codes. Here, the security property stems from an application of the crypto-lemma to lattices and so-called cooperative jamming. In cooperative jamming, signals are specifically designed and transmitted such that they minimally overlap at the legitimate receiver, while aligning at the attacker. Moreover, we will present new converse bounds for both models. We also present a framework within which we can transfer the converse bounds of the deterministic model to the Gaussian model.

The work presented in Chapter 3 has been published in [FW16a] and should be published in [FW17d].

In **Chapter 4** we analyse the problem of generating a common secret key between two legitimate communication partners. It is well-known that wireless channel reciprocity together with fading can be exploited, by sending known pilot signals back and forth between the partners to estimate the channel gain. However, the resulting channel gain can lack sufficient entropy due to insufficient randomness of the fading gains. The idea of product signalling [WFK16] could provide a remedy, where local sources of randomness are utilized. However, capacity calculations could not be obtained for the Gaussian channels. We, therefore, provide a novel deterministic key generation model, which is closely related to the LTDM. This new model can incorporate pilot and product signalling and recovers

known capacity results for the high-SNR regime. We derive analytical results for product signalling with certain channel gain scenarios for the half- and full-duplex case. We see that the full-duplex case directly connects to previous two-way wiretap results for specific channel gain scenarios.

The work presented in Chapter 4 has been published in [FW17a] and [FW17b].

Further Results which are not Part of this Thesis:

- The publication [FW14a] also includes results on the linear deterministic interfering broadcast channel (LD-IBC), which consists of two broadcast channels with mutual interference. There, we presented an achievable scheme and converse bounds for the LD-IBC. Moreover, we have shown results for the K-user LD-IMAC, which shows that for some channel gain configurations, the harmful interference gets divided by the number of users. The results for the 2-user LD-IBC channel were later transferred to the Gaussian case in [FW14b]. There we also used layered lattice codes to prove that the same achievable rates, within a bit-gap, can be achieved in the Gaussian IBC.

- In a co-authored work with Gerhard Wunder and Reaz Kahn [WFK16] we looked into secure key generation. In particular, we presented a key generation scheme, which utilizes the local randomness between two transceivers, coined product signalling. This is in contrast to state-of-the art techniques, which utilize pilot signalling, i.e. sending pre-defined pilot signals to measure the channel gain in both directions and estimate the channel gain between both transceivers for key generation. We present a short information-theoretical analysis and a practical implementation of a new algorithm for key exchange. Unfortunately, a thorough information-theoretical analysis, i.e closed form solutions for the rate-terms, was out-of-reach within the Gaussian model, which motivated the subsequent works for Chapter 3 in [FW17a] and [FW17b].

- In a co-authored work with Gerhard Wunder, Ingo Roth and Jens Eisert [WRFE17], the recently proposed Hierarchical Hard Thresholding Pursuit (HiHTP) algorithm [RKWE16] was analysed under noise constraints for user activity detection in wireless systems. Moreover, a performance analysis compares the method with the classical block correlation detector. The work provides an upper bound for the missed detection probability and compares the asymptotic behaviour between the new and the classical method. Moreover, simulations for the probability of identification failure were performed.

Copyright Information

1.3. Notation, Abbreviations and Definitions

We denote scalars, vectors, matrices and sets by lower case letters, lower case bold letters, upper case bold letters and calligraphic letters, i.e., x, $\mathbf{x}$, $\mathbf{X}$, $\mathcal{X}$, respectively. For two vectors $\mathbf{a}$ and $\mathbf{b}$, we denote by $[\mathbf{a};\mathbf{b}]$ the vector that is obtained by stacking $\mathbf{a}$ over $\mathbf{b}$. To specify a particular range of elements in a vector, we use the notation $\mathbf{a}_{[i:j]}$ to indicate that $\mathbf{a}$ is restricted to the elements i to j. If $i = 1$, it will be omitted $\mathbf{a}_{[:j]}$, the same for $j = n$ $\mathbf{a}_{[i:]}$. We use upper case letters X, Y, ... to denote random variables which take values from finite sets $\mathcal{X}, \mathcal{Y}, \ldots$ or from infinite sets, e.g. $\mathbb{R}$. We denote the probability mass function as $p(x) = \Pr(X = x)$, for x in (element of) $\mathcal{X}$ (discrete) and the probability density function as $f_X(x)$ (continuous). Moreover, we use:

Notation	
$\mathcal{N}(\mu, \sigma)$	Gaussian (normal) distribution with mean μ and variance σ
Unif$[a, b]$	Continues uniform distribution between a and b
var(X)	Variance of the real-valued random variable X
$x \in \mathcal{X}$	x is an element of $\mathcal{X}$
$\mathcal{X} \times \mathcal{Y}$	Cartesian product of the sets $\mathcal{X}$ and $\mathcal{Y}$
$\mathcal{X}^n$	n-th Cartesian product of $\mathcal{X}$
$\mathbb{E}[X]$	The expected value of X: $\sum_{x\in\mathcal{X}} xp(x)$
$\min \mathcal{A}$, $\max \mathcal{A}$	The smallest and the largest number of the set
$(\cdot)^+$	$\max\{0, \cdot\}$
$\lvert\cdot\rvert$	The absolute value or the cardinality, distinction is made clear in context
$\lfloor r \rfloor$	Greatest integer not exceeding r, $\max\{m \in \mathbb{Z} \lvert m \leq r\}$
$\lceil r \rceil$	The smallest integer greater than or equal to r, $\min\{m \in \mathbb{Z} \lvert m \geq r\}$
$\log(\cdot)$	The base 2 logarithm $\log_2(\cdot)$
$\oplus$	Binary addition (addition in $\mathbb{F}_2$)
$[x]_i$	The i-th binary digit of the binary expansion of x, $x = \sum_{-\infty}^{\infty} [x]_i 2^{-i}$
(a, b), $[a, b]$	An open and a closed interval, respectively
$(a, b]$, $[a, b)$	Half-open intervals, which do not contain a or b, respectively
iff	if and only if
w.l.o.g.	without loss of generality
$:=$	equal by definition

Abbreviations

SNR	signal to noise ratio
LDM	linear deterministic model
LTDM	lower triangular deterministic model
IMAC	interfering multiple access channel
G-IC	Gaussian interference channel
G-IMAC	Gaussian IMAC
LD-IMAC	linear deterministic IMAC
LTD-IMAC	lower triangular deterministic IMAC
MAC-WT	multiple access wiretap channel
G-MAC-WT	Gaussian MAC-WT
LD-MAC-WT	linear deterministic MAC-WT
G-WT-H	Gaussian wiretap channel with a helper
LD-WT-H	linear deterministic wiretap channel with a helper
DoF	degrees of freedom
GDoF	generalized DoF
SDoF	secure DoF
GSDof	generalized SDoF
IC	interference channel
MAC-P2P	multiple access channel interfering with a point-to-point link

Definition 1.1. The entropy $H(X)$ of a discrete random variable X is defined by

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log p(x).$$

Some properties of the entropy $H(X)$ are:

- Entropy is non-negative and bounded from above: $0 \leq H(X) \leq \log|\mathcal{X}|$
- Conditioning reduces entropy: $H(X|Y) \leq H(X)$
- $H(X_1,\dots X_n) \leq \sum_{i=1}^{\infty} H(X_i)$ with equality iff the random variables X_i are independent

Definition 1.2. The joint entropy $H(X,Y)$ of a pair of discrete random variables (X,Y), with a joint distribution $p(x,y)$ is defined by

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log p(x,y).$$

Definition 1.3. The conditional entropy $H(X|Y)$ of a pair of discrete random variables (X, Y), with a joint distribution $p(x, y)$ is defined by

$$H(X|Y) = \sum_{y \in \mathcal{Y}} p(y) H(Y|X = x) = -\sum_{y \in \mathcal{Y}} p(y) \sum_{x \in \mathcal{X}} p(x|y) \log p(x|y).$$

Theorem 1.4 (Chain rule)**.**

$$H(X, Y) = H(X) + H(Y|X).$$

Definition 1.5. The mutual information between two discrete random variables X and Y, with a joint distribution $p(x, y)$, and marginal distributions $p(x)$ and $p(y)$, is defined by

$$I(X; Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x)p(y)}.$$

Some properties of the mutual information $I(X)$ are:

- Mutual information is non-negative
- $I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X, Y)$
- $I(X_1, \ldots, X_n) = \sum_{i=1}^{n} I(X_i; Y|X_{i-1}, \ldots, X_1)$ (Chain rule for mutual information)

Definition 1.6. The conditional mutual information between two discrete random variables X and Y, given Z, is defined by

$$I(X; Y|Z) = H(X|Z) - H(X|Y, Z).$$

Definition 1.7. The differential entropy $h(X)$ of a continuous random variable X with a density $f(x)$ is defined by

$$h(X) = -\int_S f(x) \log f(x) dx,$$

where S is the support set of the random variable.

Definition 1.8. The mutual information $I(X; Y)$ between two random variables with joint density $f(x, y)$ is defined by

$$I(X; Y) = \int f(x, y) \log \frac{f(x, y)}{f(x)f(y)} dx dy.$$

Theorem 1.9 (Data processing inequality). *If $W \to X \to Y \to Z$ forms a Markov chain, then*

$$I(W;Z) \leq I(X;Y).$$

Theorem 1.10 (Fano's inequality). *Let $P_e = Pr\{g(Y) \neq X\}$, where g is any function on Y. Then*

$$H(P_e) + P_e \log(|\mathcal{X} - 1|) \geq H(X|Y).$$

All of the proofs for the theorems and results above, along with further details on (multi-user) information theory can be found in standard text books, for example by Cover and Thomas [CT91], El Gamal and Kim [EGK11], Csiszar and Körner [CK11] or Gallager [Gal68]. The text books [LPS09] and [BB11] cover the topic of information-theoretic security.

1.4. Approximation Models

In this section we want to examine the approximation models, which we use in this thesis, in closer detail. In particular we will introduce the linear deterministic model and the lower triangular deterministic model.

1.4.1. The linear deterministic model

To introduce the linear deterministic model (LDM) [ADT11], let us consider a single-user Gaussian point-to-point channel for a fixed time-slot

$$Y = Xh' + Z,$$

where $Z \sim \mathcal{N}(0,1)$ is additive Gaussian noise. Moreover, the average signal input power is normalized to one $\mathbb{E}[|X|^2] \leq 1$, and we therefore have that the channel gain represents the signal-to-noise ratio, $h' = \sqrt{\text{SNR}}$. If we now assume that the input power and the noise power have a *peak* power of one, we can represents them in the following way

$$X := \sum_{i=1}^{\infty} [X]_i 2^{-i} = 0.[X]_1[X]_2[X]_3 \ldots$$
$$Z := \sum_{i=1}^{\infty} [Z]_i 2^{-i} = 0.[Z]_1[Z]_2[Z]_3 \ldots,$$

as binary expansion, where $[X]_i, [Z]_i \in \{0, 1\}$. Plugging these into our system model yields

$$Y = 2^{\frac{1}{2}\log \mathrm{SNR}} \sum_{i=1}^{\infty} [X]_i 2^{-i} + \sum_{i=1}^{\infty} [Z]_i 2^{-i}.$$

Note that we can write $h' = h2^n$, where $n \in \mathbb{N}$ and $h \in [1, 2)$. We can therefore write any channel gain (and in this case SNR) greater than one as the product of a *fine* channel gain h and *coarse* channel gain 2^n. For the linear deterministic model we now approximate the channel gain by $h' \approx 2^n$ with the equivalence $n = \lfloor \frac{1}{2} \log \mathrm{SNR} \rfloor$, and therefore approximate the fine channel gain by one. This yields

$$\begin{aligned} Y &\approx 2^n \sum_{i=1}^{\infty} [X]_i 2^{-i} + \sum_{i=1}^{\infty} [Z]_i 2^{-i} \\ &= \sum_{i=1}^{n} [X]_i 2^{n-i} + \sum_{i=1}^{\infty} ([X]_{i+n} + [Z]_i) 2^{-i}. \end{aligned}$$

Observe that the channel gain 2^n shifts the bits of a scalar $x = 0.b_1 b_2 b_3 \ldots$ for n-position over the decimal point, such that we have $2^n x = b_1 b_2 \ldots b_n . b_{n+1} b_{n+2} \ldots$. The noise only affects the bits on the right side of the decimal point $2^n x + z = b_1 b_2 \ldots b_n . \tilde{b}_{n+1} \tilde{b}_{n+2} \ldots$ denoted as $\tilde{b}_{n+i}$. We can now approximate the model by cutting of the noise effected bits after the shift, which results in $y \approx b_1 b_2 \ldots b_n$ or equivalently

$$Y \approx \sum_{i=1}^{n} [X]_i 2^{n-i},$$

setting $\sum_{i=1}^{\infty} ([X]_{i+n} + [Z]_i) 2^{-i} = 0$ and ignoring the 1-bit carry over. We therefore approximated the noise-effected Gaussian point-to-point channel by a deterministic channel model. Note that we now have an input vector of bits. We will refer to those bits as *bit-levels*, and count those bit-levels from the top, i.e. most-significant bit, downwards. Superposition in multi-user scenarios is modelled by addition in $\mathbb{F}_2$ (modulo two)

$$\mathbf{y} = \mathbf{S}^{q-n_1} \mathbf{x}_1 \oplus \mathbf{S}^{q-n_2} \mathbf{x}_2,$$

where addition is therefore limited to the bit-levels, enhancing the tractability of the model. Moreover, we see that the model can be written in an algebraic fashion where $\mathbf{x} \in \mathbb{F}_2^q$ is an

input bit vector and $\mathbf{S}^{q-n}$ is a $q \times q$ shift matrix

$$\mathbf{S} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

which shifts an incoming bit vector for $q-n$ positions, where $q := \max\{n_1, n_2\}$. The model can be extended to an arbitrary number of users.

1.4.2. The lower triangular deterministic model

The lower triangular deterministic model, introduced by [NMA13], incorporates the fine channel gain $h \in [1, 2)$ into the model. Note that in the previous, linear deterministic model, the fine channel gain was approximated by one and had no influence in the channel. Here, instead, the fine channel gain is represented by a binary expansion

$$h = \sum_{j=0}^{\infty} [h]_j 2^{-j} = [h]_0.[h]_1[h]_2[h]_3 \ldots$$

where $h_0 = 1$ due to $h \in [1, 2)$. Plugging this in the system model yields

$$\begin{aligned} Y &= 2^n \left(\sum_{i=0}^{\infty} [h]_i 2^{-i} \right) \left(\sum_{i=1}^{\infty} [X]_i 2^{-i} \right) + \sum_{j=1}^{\infty} [Z]_j 2^{-j} \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{j} [X]_i [h]_{j-i} \right) 2^{n-j} + \sum_{j=1}^{\infty} \left(\sum_{i=1}^{j+n} [X]_i [h]_{j+n-i} + [Z]_j \right) 2^{-j} \\ &\approx \sum_{j=1}^{n} \left(\sum_{i=1}^{j} [X]_i [h]_{j-i} \right) 2^{n-j}, \end{aligned}$$

where we used the Cauchy product in the second line, and eliminated the noise effected part by setting $\sum_{j=1}^{\infty} \left(\sum_{i=1}^{j+n} [X]_i [h]_{j+n-i} + [Z]_j \right) 2^{-j} = 0$ in the last line. We see that the received bits are the result of a discrete convolution between the bits of X and h. We can therefore write the received bit vector as $\mathbf{Hx}$, where $\mathbf{x} \in \mathbb{F}_2^q$ and $\mathbf{H}$ is a lower triangular

matrix defined as

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ [h]_1 & 1 & 0 & \cdots & 0 \\ [h]_2 & [h]_1 & 1 & & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ [h]_{q-1} & [h]_{q-2} & \cdots & [h]_1 & 1 \end{pmatrix},$$

with $[h]_j$ representing the j-th bit in the binary expansion of h. Multi-user channels can be represented by modelling the superposition as binary addition $\oplus$ on the bit-levels:

$$\mathbf{y} = \mathbf{S}^{q-n_1}\mathbf{H}_1\mathbf{x}_1 \oplus \mathbf{S}^{q-n_2}\mathbf{H}_2\mathbf{x}_2,$$

where $\mathbf{x}_1$, $\mathbf{x}_2 \in \mathbb{F}_2^q$, $\mathbf{S}^{q-n}$ the $q \times q$ shift matrices. Thus, we keep the level-wise superposition of the LDM channel and the algebraic notation.

2. The Gaussian Interfering Multiple Access Channel

2.1. Introduction

One of the main limiting factors of cellular networks is interference. Throughout the last decades, research was conducted to investigate the role of interference in information theory. Several channel models were proposed, in which interference is one of the main limiting factors. But even for the simplest one, the two-user inference channel (IC), the capacity characterisation is an unsolved problem for more than 40 years. However, Etkin, Tse and Wang [ETW08] have achieved a major breakthrough, a capacity result to within one bit. They used a fundamental principle: if something is too hard to solve as one, you need to divide it into smaller simpler parts. And in the course of their investigation, defined the concept of *generalized degrees of freedom* (GDoF)

$$d_{\mathrm{sym}}(\alpha) := \lim_{\mathrm{SNR},\mathrm{INR}\to\infty;\frac{\log \mathrm{INR}}{\log \mathrm{SNR}}=\alpha} \frac{C_{\mathrm{sym}}(\mathrm{INR},\mathrm{SNR})}{C_{\mathrm{awgn}}(\mathrm{SNR})},$$

which can be viewed as an interference dependent notion of degrees of freedom (DoF). This achievement motivated a series of investigations of more complex channel models (e.g. [BPT10]), towards constant-gap capacity approximations. However, even constant-gap capacity results were hard to obtain, due to noise properties of the Gaussian channel models. A branch of research, therefore, investigated deterministic models. In particular, the so-called linear deterministic model (LDM) emerged with the work of Avestimehr, Diggavi and Tse [ADT07, ADT11]. The LDM approximates the channel by the binary expansion of the real signals. The coefficients of this binary expansion are viewed as bit-vectors and positions within these vectors are called levels. These bit-vectors are truncated at the noise level, such that the noise-corrupted bits are removed from the channel model, resulting in a deterministic approximation. Moreover, channel gain is approximated by a power of two 2^n, $n = \left\lfloor \frac{1}{2} \log \mathrm{SNR} \right\rfloor$, which results in a downshift of the bit-vector. Superposition is modelled as level-wise binary addition. Surprisingly, this rather simple model results in capacity approximations to within a constant bit-gap of the corresponding Gaussian chan-

nel models, e.g. a 42-bit gap for the deterministic two-user IC [BT08]. Another research branch investigated the concept of interference alignment, introduced in [MAMK08], [CJ08] and [JS08]. Interference alignment methods align interfering signal parts in some dimension and therefore make more interference-free dimensions available. These methods can be broadly categorized into two classes: vector-space alignment and Signal-space alignment [NMA13]. In vector-space alignment methods, the dimensions of multiple antennas, time and frequency are used to align interfering signal parts into some sub-spaces. However, in single-antenna, time-invariant, frequency-flat channel models, these methods fail and the class of signal-scale alignment methods needs to be used. In these methods, techniques such as lattice coding, split the channel into several power layers, allowing for alignment of interference. It was shown in recent investigations, that LDM solutions are the basis for the corresponding signal-scale alignment methods and therefore provide a stepping-stone for constant bit-gap capacity results, see for example [SJV$^+$08], [BPT10], [SB11], [ST11]. An interesting application of interference alignment is its use for the interfering multiple access channel (IMAC) in [ST08]. In this investigation, the interfering MAC (IMAC) serves as a general simple model for cellular networks. It was shown that multiuser gain, in form of additional DoF, can be enabled by vector-space alignment using frequency and delay properties of the channel. The question is now, if a multiuser gain is still present in the single-antenna, time-invariant, frequency-flat cellular networks, especially the IMAC as the simplest model.

2.2. Contributions and Outline of the Results

We investigate the single-antenna, time-invariant, frequency-flat Gaussian IMAC (G-IMAC). To make progress on this front, we start by investigating the linear deterministic approximation of the G-IMAC named LD-IMAC. We show that basic achievability schemes from the linear deterministic MAC-P2P [BW12] can be extended towards the LD-IMAC. In those schemes, the orthogonality of bit-levels in the LDM bit-vectors is used to exploit the signal-scale shift between two cells. This results in the alignment of the interference in half of its bit-levels, effectively reducing the interference by half in the weak interference regime. Due to a coupling of both cells, the achievable schemes are limited to the weak interference regime. Moreover, due to dependence on the ratio of interference-to-direct signal strength α, the achievable sum-rate has a step-like curve. However, converse proofs cannot assume orthogonality of bit-levels, which would mean a uniform distribution of the real signals and therefore results in a loose upper bound for certain values of α. This yields a sum-capacity for just certain discrete points depending on α. Using signal-scale alignment methods, i.e. layered lattice codes, we transfer the achievable scheme and the result to the Gaussian

IMAC. Extending techniques of [BT08], one can show that the LD-IMAC bounds are actually within a constant bit-gap of the Gaussian IMAC bounds. This yields a constant bit-gap sum-capacity result for the G-IMAC at discrete points, again depending on the channel gains. This shows that the schemes stemming from the LD-IMAC and the LDM itself is a sub-optimal approximation, which is also sub-optimal as an approximation of the sum-rate of the G-IMAC. As we later show, this sub-optimality stems from the LD models property of just allowing orthogonal bit-level assignment schemes. Interestingly, a new deterministic model was introduced in [NMA13], coined the lower triangular deterministic model (LTDM). In this model, the channel gain is not approximated by 2^n anymore, but the remainder incorporated as binary expansion. This results in a discrete convolution between the bits of the channel gain and the bits of the real signal and therefore yields a dependence between the bit-levels. This means that the model allows a broader form of achievable schemes, where the bit-levels do not need to be orthogonal. Since the problems with the LDM stem exactly from this necessity, an LTDM scheme could improve upon prior results. We show LTD-IMAC schemes for the whole interference range, which (completely) reach the LDM upper bounds in the weak interference case and hence improve upon prior results. Moreover, we transform the bounds towards the LTDM channel and develop new upper bounds for the remaining interference ranges. We, therefore, show the deterministic approximation of the sum-capacity of the LTD-IMAC to within a constant bit-gap. Extending the proof methods of [NMA13] towards the structure of our achievable scheme, we can use them to transfer the constant-gap results from the LTD-IMAC to the G-IMAC. This yields a constant-gap capacity approximation of the symmetric G-IMAC in the whole interference range.

2.3. System Model

2.3.1. The Gaussian Interfering Multiple Access Channel

We consider the Gaussian interfering multiple access channel (IMAC), in which there are two Gaussian multiple access channels (MACs) interfering with each other. Therefore, the system consists of 4 transmitters and 2 receivers. Transmitters X_{11} and X_{12} together with the receiver Y^1 and X_{21}, X_{22} with Y^2 each form a MAC and both are interfering with each other (see Fig. 2.1). We use the notation of h_{ik}^j, where the superscript j represents the receiver cell, and the subscripts i and k the transmitter cell and user, respectively.

The channel equations for a fixed time slot are given by

$$Y^1 = h_{11}^1 2^{n_{11}^1} X_{11} + h_{12}^1 2^{n_{12}^1} X_{12} + h_{21}^1 2^{n_{21}^1} X_{21} + h_{22}^1 2^{n_{22}^1} X_{22} + Z^1 \tag{2.1}$$

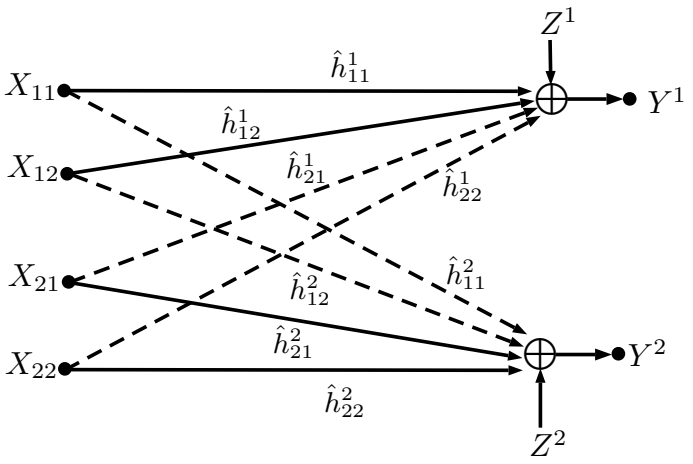

Figure 2.1.: Illustration of the Gaussian IMAC, we denote $\hat{h}^j_{ik} := h^j_{ik} 2^{n^j_{ik}}$. Direct links are represented as normal arrows, whereas interference links are represented as dashed arrows.

$$Y^2 = h^2_{21} 2^{n^2_{21}} X_{21} + h^2_{22} 2^{n^2_{22}} X_{22} + h^2_{11} 2^{n^2_{11}} X_{11} + h^2_{12} 2^{n^2_{12}} X_{12} + Z^2, \tag{2.2}$$

where $Z^j \sim \mathcal{N}(0,1)$ is assumed to be zero mean and unit variance Gaussian noise. Also, each transmitted signal has an associated unit average power constraint $\mathbb{E}[X^2_{ik}] \leq 1$. The channel gains are composed of two parts. A coarse channel gain, 2^n with $n \in \mathbb{N}$ and a fine channel gain $h \in [1,2)$. However, both parts can model any real channel gain greater than 1, which is sufficient for a constant-gap analysis. We choose this channel notation following the notation of [NMA13] to get a clear integration of linear deterministic and lower triangular deterministic ideas in the following investigation of the model. It is assumed that $n^1_{21} = n^1_{22} =: n^1_2$, $n^2_{11} = n^2_{12} =: n^2_1$, stating that the total interference strength caused by X_{ij} at the receivers is the same[1]. Note that the restriction for the coarse gain is justified in the case when the distance between the two cells is significantly larger than the cell dimension itself. However, for the fine channel gains of the interfering signals, we consider a simple modulation scheme. We take a similar approach as in [NMA13], to form the channel input such that the fine channel gains of the interfering signals coincide.

Each transmitter has one message to communicate to his receiver. As in the X-channel, we have 4 independent messages w_{ik}. Assume that each message w_{ik} is modulated into the signal U_{ik}. The transmitters can now form the channel input such that

$$X_{11} := h^2_{12} U_{11} \tag{2.2a}$$

[1]This assumption is not necessary for the techniques to work. In fact, we just need a difference in the ratios of both direct links and both interference links, which we call shift-property. However, it simplifies the investigation, since the shift-property gets simpler.

$$X_{12} := h_{11}^2 U_{12} \tag{2.2b}$$
$$X_{21} := h_{22}^1 U_{21} \tag{2.2c}$$
$$X_{22} := h_{21}^1 U_{22}. \tag{2.2d}$$

We, therefore, see the following signals at the receiver side

$$Y^1 = h_{11}^1 h_{12}^2 2^{n_{11}^1} U_{11} + h_{12}^1 h_{11}^2 2^{n_{12}^1} U_{12} + h_{21}^1 h_{22}^1 2^{n_2^1}(U_{21} + U_{22}) + Z^1 \tag{2.3}$$
$$Y^2 = h_{21}^2 h_{22}^1 2^{n_{21}^2} U_{21} + h_{22}^2 h_{22}^1 2^{n_{22}^2} U_{22} + h_{11}^2 h_{12}^2 2^{n_1^2}(U_{11} + U_{12}) + Z^2. \tag{2.4}$$

Notice that we have modulated the signals in a way, such that the interference parts align at the unintended receiver, reproducing a similar structure as in the X-channel[2]. Now we can define

$$\begin{aligned} g_{11}^1 &:= h_{11}^1 h_{12}^2, & g_{21}^2 &:= h_{21}^2 h_{22}^1 \\ g_{12}^1 &:= h_{12}^1 h_{11}^2, & g_{22}^2 &:= h_{22}^2 h_{21}^1 \\ g_2^1 &:= h_{21}^1 h_{22}^1, & g_1^2 &:= h_{11}^2 h_{12}^2, \end{aligned}$$

where $g_{ik}^j \in (1, 4]$ and we can rewrite (2.3)-(2.4) as

$$Y^1 = g_{11}^1 2^{n_{11}^1} U_{11} + g_{12}^1 2^{n_{12}^1} U_{12} + g_2^1 2^{n_2^1}(U_{21} + U_{22}) + Z^1 \tag{2.5}$$
$$Y^2 = g_{21}^2 2^{n_{21}^2} U_{21} + g_{22}^2 2^{n_{22}^2} U_{22} + g_1^2 2^{n_1^2}(U_{11} + U_{12}) + Z^2. \tag{2.6}$$

Moreover, we assume w.l.o.g. that $n_{11}^1 \geq n_{12}^1$, $n_{21}^2 \geq n_{22}^2$. The difference between the two coarse channel gains is denoted as $\Delta_1 := n_{11}^1 - n_{12}^1$ and $\Delta_2 := n_{21}^2 - n_{22}^2$.

2.3.2. Linear Deterministic IMAC

To simplify the Gaussian IMAC model and get some intuition for achievable schemes and upper bounds, we chose the LDM[3] as a first approximation, see [ADT11] for a thorough exposition. This enables schemes where certain bits, also called bit-levels, can be used independently. This property enables a form of bit-level alignment, which is used by our schemes. The channel gain is represented by n_{ik}^j-bit levels which correspond to $\lfloor \frac{1}{2} \log \mathrm{SNR} \rfloor$ of the original channel. We, therefore, approximate the fine channel gain by one. With

[2] Note that the difference lies in the coarse channel gains, in particular those of the aligning parts. The only case, where both structures are equal, is when *all* coarse channel gains are equal. In that case, both channel models reach $\frac{4}{3}$ DoF.

[3] see section 1.4.1

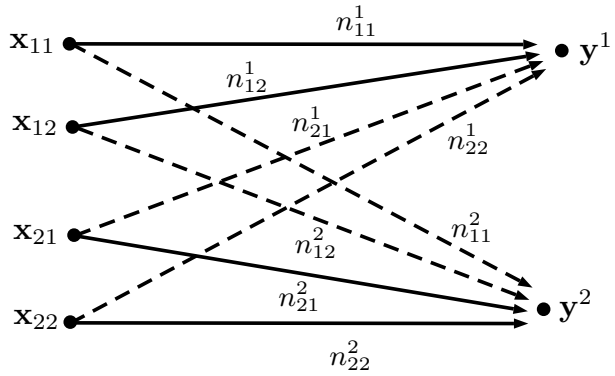

Figure 2.2.: Illustration of the LD-IMAC. Direct links are represented as normal arrows, whereas interference links are represented as dashed arrows.

this definitions the model can be written as

$$\mathbf{y}^1 = \mathbf{S}^{q-n_{11}^1}\mathbf{x}_{11} \oplus \mathbf{S}^{q-n_{12}^1}\mathbf{x}_{12} \oplus \mathbf{S}^{q-n_2^1}(\mathbf{x}_{21} \oplus \mathbf{x}_{22}) \tag{2.7}$$

$$\mathbf{y}^2 = \mathbf{S}^{q-n_{11}^2}\mathbf{x}_{11} \oplus \mathbf{S}^{q-n_{12}^2}\mathbf{x}_{12} \oplus \mathbf{S}^{q-n_2^2}(\mathbf{x}_{21} \oplus \mathbf{x}_{22}). \tag{2.8}$$

2.3.3. Lower Triangular Deterministic IMAC

We use the LTDM[4] as a second approximation, which enables a broader view on schemes fro achievable rates. In contrast to the LDM, the fine channel gain h is also written as a binary expansion, and not approximated by one, resulting in a discrete convolution between the bits of h and x, see [NMA13] for a thorough exposition.

Thus, the LTD-IMAC channel model is governed by the following equations

$$\mathbf{y}^1 = \mathbf{S}^{q-n_{11}^1}\mathbf{H}_{11}^1\mathbf{x}_{11} \oplus \mathbf{S}^{q-n_{12}^1}\mathbf{H}_{12}^1\mathbf{x}_{12} \oplus \mathbf{S}^{q-n_2^1}\mathbf{H}_2^1\left(\mathbf{x}_{21} \oplus \mathbf{x}_{22}\right) \tag{2.9}$$

$$\mathbf{y}^2 = \mathbf{S}^{q-n_{21}^2}\mathbf{H}_{21}^2\mathbf{x}_{21} \oplus \mathbf{S}^{q-n_{22}^2}\mathbf{H}_{22}^2\mathbf{x}_{22} \oplus \mathbf{S}^{q-n_1^2}\mathbf{H}_1^2(\mathbf{x}_{11} \oplus \mathbf{x}_{12}). \tag{2.10}$$

Note that we used the specific modulation of (2.3), to group the interference signal parts. The bits of the channel matrices correspond to the real values of g_{ik}^j, defined above. Moreover, we will use the notation that $\bar{\mathbf{x}}_{ik} := \mathbf{S}^{q-n_{ik}^j}\mathbf{x}_{11}$ and $\bar{\mathbf{x}}_{ik}^c := \mathbf{S}^{q-n_{ik}^j}\mathbf{x}_{ik}$ for $i \neq j$ for a simple distinction between direct and interference signals.

[4] see section 1.4.2

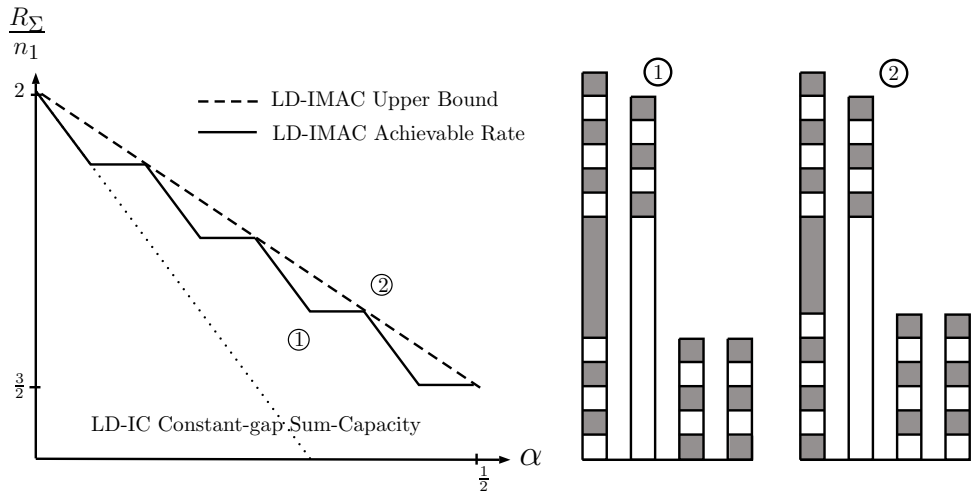

Figure 2.3.: GDoF of the LD-IMAC and LD-IBC in the weak interference regime in comparison to the LD-IC channel. The first part of the w-curve is depicted. Multiuser gain be seen, as a second user in each cell provides a DoF-wise gain of one-half of the interference strength in each cell.

2.4. Main Results for the IMAC

In the following section, we give an overview of the main results of this section. We start by presenting the results for the linear deterministic approximation of the IMAC. We will see that the LDM approximation is insufficient in a sense, that the achievable sum rate of any orthogonal bit-alignment scheme cannot achieve the upper bound at all points. note, that this excludes bit-copy schemes, which can be seen as an intermediate form between LDM and LTDM schemes. Moreover, we show that a transfer from orthogonal bit-alignment strategies to the Gaussian IMAC also inherit the problems. We will therefore turn to the lower triangular deterministic model and show that it captures schemes which can achieve the upper bound and therefore establish the possibility of a constant-gap capacity result. In the last part we present the constant-gap capacity result for the G-IMAC.

2.4.1. Approximate Capacity for the LD-IMAC

In section 2.5, we will show the achievable sum rate in the weak interference regime. We define the weak interference regime as

$$n_j^i + n_i^j \leq \min\{n_{12}^1, n_{22}^2\}.$$

This means that the sum of both interference link strength values is smaller than the weakest direct link strength of both cells. In this regime, the LD system model can be de-

composed into two sub channels (see section 2.5) which simplifies the analysis. We provide a narrow analysis of the LD-IMAC, since we only want to demonstrate its shortcomings. Later analysis of the LTD model will treat the general interference case. Note, that we will identify a larger weak interference regime for the LTD-IMAC and the Gaussian IMAC with $n_j^i + n_i^j \leq \min\{n_{11}^1, n_{21}^2\}$. The achievable sum-rate depends on the strength, or coarse channel gain, of the weaker user, which results in three sub-cases per cell i. If the coarse channel gain n_{i2}^i of the weaker link signal x_{i2}^i is smaller than the coarse interference channel gain n_j^i in cell i, the IMAC sum-rate falls back to the IC sum-rate. Above this threshold, multiuser gain will increase along with n_{i2}^i until it reaches the maximum multiuser gain. In the following we will briefly introduce the results for the last case, where the full multi-user gain can be achieved simultaneously in both cells.

Theorem 2.1. *An achievable sum-rate for the linear deterministic interfering multiple access channel (LD-IMAC) in the weak interference regime, is*

$$R_\Sigma \leq n_{12}^1 + n_{22}^2 - n_2^1 - n_1^2 + \phi(n_2^1, \Delta_1) + \phi(n_1^2, \Delta_2)$$

with the function ϕ for $p, q \in \mathbb{N}_0$, following the notation of [BW11], defined as

$$\phi(p,q) := \begin{cases} q + \frac{l(p,q)q}{2} & \text{if } l(p,q) \text{ is even,} \\ p - \frac{(l(p,q)-1)q}{2} & \text{if } l(p,q) \text{ is odd,} \end{cases}$$

where $l(p,q) := \lfloor \frac{p}{q} \rfloor$ for $q > 0$ and $l(p,0) = 0$.

ϕ is essentially composed of the multiuser gain and the difference of the coarse channel gain of both users in the corresponding cell. The proof of the theorem can be found in section 2.5.1. We note, that the achievable scheme would have a singularity point for the case that all coarse channel gains are equal, which is outside the weak interference regime. This collapse of d.o.f. is a known phenomenon, which also occurs in other channel models. It was shown in [CJW10], that asymmetric complex signalling can overcome this collapse of d.o.f. The LTDM includes this point as outage, and we therefore do not consider it further. To provide a result about the optimality of this sum-rate, the next lemma will give an upper bound for the aforementioned model.

Theorem 2.2. *The sum rate for the linear deterministic interfering multiple access channel (LD-IMAC) in the weak interference regime can be bounded from above by*

$$R_\Sigma \leq n_{11}^1 + n_{21}^2 - \frac{n_1^2}{2} - \frac{n_2^1}{2}.$$

We remark, that the LD model can be regarded as a special case of the LTD model, where the lower triangular matrix is the identity matrix. The upper bound for the weak interference part of the LTD-IMAC therefore also provides an upper bound for the LD-model. The proof can be found in section 2.6.2. A graphical comparison by means of GDoF shows, that the achievable sum-rate of Theorem 2.1 reaches the upper bound at the α values at which the scheme has an even number of layers (see Fig. 2.3). However, in between those points, the upper bound cannot be reached. The reason for this behaviour is the structure of the scheme which originates from the approximation model. Later, we will show that the lower triangular deterministic model eliminates this problem. By utilizing layered lattice coding schemes as in e.g. [SJV$^+$08], [NCL10], [SB11], [BPT10] and [NCNC16], we can transfer the LD achievable sum-rate to the Gaussian channel, which yields the following theorem.

Theorem 2.3. *An achievable sum-rate for the Gaussian interfering multiple access channel (G-IMAC) in the weak interference regime, is*

$$\begin{aligned} R_\Sigma > & \tfrac{1}{2}\log SNR_{11}^{\beta_1} - \tfrac{1}{2}\log SNR_{11}^{\alpha_1} + \tfrac{1}{2}\log SNR_{21}^{\beta_2} - \tfrac{1}{2}\log SNR_{21}^{\alpha_2} \\ & + \phi(\tfrac{1}{2}\log SNR_{21}^{\alpha_2}, \tfrac{1}{2}\log SNR_{11}^{(1-\beta_1)}) \\ & + \phi(\tfrac{1}{2}\log SNR_{11}^{\alpha_1}, \tfrac{1}{2}\log SNR_{21}^{(1-\beta_2)}) - 3 - 2.5(\lfloor L_2 \rfloor + \lfloor L_1 \rfloor) \end{aligned}$$

with ϕ defined as in (2.1). Note that l(p,q) is equivalent to $\lfloor L_i \rfloor$, which basically counts the layers of lattice codes. The proof for the theorem is provided in section 2.5.2. Observe that the sum-rate has the same structure as in Theorem 2.1 with the correspondence $n_{ik}^j = \lfloor \frac{1}{2}\log |h_{ik}^j|^2 P \rfloor$. We, therefore, need to prove an equivalent version of the bound in Theorem 2.2 for the Gaussian case. By extending proof methods of [BT08] we can show the following result.

Theorem 2.4. *The sum-rate for the Gaussian IMAC can be upper bounded by the corresponding LD-IMAC upper bound, within a constant number of bits. The G-IMAC in the weak interference regime is therefore bounded from above by*

$$R_\Sigma \leq n_{11}^1 + n_{21}^2 - \frac{n_1^2}{2} - \frac{n_2^1}{2} + c_1,$$

where c_1 is a constant. Therefore the two theorems 2.3 and 2.4 show, that the transfer of the results from the linear deterministic scheme to the Gaussian IMAC is possible. However, the achievable scheme inherits the same structure as in the LD model and therefore also the problems with the step-like achievability curve. These problems are related to the

fact, that the LD schemes are constrained to an orthogonal usage of bit-levels. Assuming independence of bit-levels would yield a tight upper bound. But we would therefore need to proof the optimality of a uniform input distribution. However, a result along these lines would be restricted to the linear deterministic model and does not extend to the general Gaussian case. Instead, one can use a more complex model, which enables schemes beyond an orthogonal usage of bit-levels. The lower triangular deterministic model is such a model and we will now describe the results for this model.

2.4.2. Approximate Constant-Gap Sum Capacity for the LTD-IMAC

We start with a theorem about the constant-gap sum capacity for the deterministic LTD-IMAC in a weak interference regime, defined by $n_2^1 + n_1^2 \leq \min\{n_{11}^1, n_{21}^2\}$, with arbitrary channel gains.

Theorem 2.5. *For every $\delta \in (0,1]$, n_{k1}^k, n_{k2}^k, $n_l^k \in \mathbb{N}$ such that $n_{k1}^k \geq n_{k2}^k \geq n_l^k$ and $n_2^1 + n_1^2 \leq \min\{n_{11}^1, n_{21}^2\}$ with $k, l \in \{1,2\}$, $k \neq l$, there exists a set $B \subset (1,2]^{2\times 3}$ of Lebesgue measure at most δ such that for all channel gains $g_{ik}^j \in (1,2]^{2\times 3} \setminus B$, the sum capacity $C_{\text{LTD-IMAC}}$ of the lower triangular deterministic interfering multiple access channel satisfies*

$$D - 2\log(c/\delta) \leq C_{\text{LTD-IMAC}} \leq D$$

with $D := \min\{D_1, D_2, D_3, D_4\}$ and

$$\begin{aligned}
D_1 &:= \max\{(n_{11}^1 - n_1^2), n_{12}^1\} + \max\{(n_{21}^2 - n_2^1), n_{22}^2\} \\
D_2 &:= \max\{(n_{11}^1 - n_1^2), n_{12}^1\} + n_{21}^2 - \tfrac{1}{2}n_2^1 \\
D_3 &:= n_{11}^1 - \tfrac{1}{2}n_1^2 + \max\{(n_{21}^2 - n_2^1), n_{22}^2\} \\
D_4 &:= n_{11}^1 - \tfrac{1}{2}n_1^2 + n_{21}^2 - \tfrac{1}{2}n_2^1,
\end{aligned}$$

for some constant c, independent of the channel gain.

The proof is provided in section 2.6. Recall that n_2^1 is the coarse interference strength of both users from cell 2 to cell 1, and equally, n_1^2 from cell 2 to cell 1. This means that the assumption $n_2^1 + n_1^2 \leq \min\{n_{11}^1, n_{21}^2\}$, states that the sum of the interference strengths is smaller than the minimum of n_{11}^1 and n_{21}^2, which are the two coarse channel gains of the stronger users in each cell. For a symmetric setting, the assumption becomes $\alpha = \frac{n_i}{n_1} \leq \frac{1}{2}$ and corresponds to the first part of the weak interference regime of the IC-channel. The δ in the gap $2\log(c/\delta)$ can be seen as a fixed trade-off factor. If δ is chosen to be large, the gap would become small. The achievable sum-rate would get closer to the bound. But δ is also the bound for the measure of the outage set B and a large bound would mean,

that the result would hold for a smaller set of channel gain configurations. On the other hand, a small δ would mean, that the result holds for a large set of channel gains but at the same time induce a bigger gap towards the upper bound. Due to a large number of cases for arbitrary channel gains and arbitrary interference regimes, we have limited the investigation of arbitrary regimes to symmetric channel gain configurations. The following theorem shows the result for the deterministic IMAC.

Theorem 2.6. *For every $\delta \in (0,1]$, n_1, n_2, $n_i \in \mathbb{N}$ such that $n_1 \geq n_2$, there exists a set $B \subset (1,2]^{2\times 3}$ of Lebesgue measure at most δ such that for all channel gains $g_{ik}^{j} \in (1,2]^{2\times 3} \setminus B$, the sum capacity $C_{LTD\text{-}IMAC}$ of the lower triangular deterministic symmetric interfering multiple access channel satisfies*

$$D - 2\log(c/\delta) \leq C_{LTD\text{-}IMAC} \leq D$$

with $D := \min\{D_1, D_2, D_3, D_4, D_5\}$ and

$$\begin{aligned}
D_1 &:= 2\max((n_1 - n_i)^+, n_i) + \min((n_1 - n_i)^+, n_i),\\
D_2 &:= \tfrac{2}{3}(2\max(n_1, n_i) + (n_1 - n_i)^+),\\
D_3 &:= 2n_1,\\
D_4 &:= \max(2n_2, 2(n_1 - n_i)^+, 2n_i),\\
D_5 &:= \max(n_1, n_i) + \max(n_2, (n_1 - n_i)^+).
\end{aligned}$$

for some constant c, independent of the channel gain

This result shows the constant-gap result for the symmetrical LTD-IMAC for the whole interference regime. One can see that the symmetrical weak interference cases D_1 and D_4 are reflected in D_4 and D_1, respectively. The cases D_2, D_3, D_5 and parts of D_4 and D_1 represent additional bounds for the cases with interference $\alpha > \frac{1}{2}$. As in the weak interference case, one can see that the gap is constant and can be seen as a fixed trade-off factor between rate-gap and quantity of supported channel gains. In the next sub section we will show, that this result can be extended to the Gaussian IMAC.

2.4.3. Constant-Gap Sum Capacity for the Gaussian IMAC

For the Gaussian case, extensions of the methods developed in [NMA13] show that the achievable schemes can be transferred to the Gaussian IMAC. In this process, the constant-gap gets larger buts stays constant in relation to the channel gain. Moreover, previously used techniques can show that the LTD-IMAC bounds can be used as a bound for the

G-IMAC by introducing another constant-gap. This yields the following constant-gap capacity approximation of the G-IMAC.

Theorem 2.7. *For every $\delta \in (0,1]$, n_1, n_2, $n_i \in \mathbb{N}$ such that $n_1 \geq n_2$, there exists a set $B \subset (1,2]^{2\times 4}$ of Lebesgue measure at most δ such that for all channel gains $h_{ik}^{j} \in (1,2]^{2\times 4} \setminus B$, the sum capacity $C_{G\text{-}IMAC}$ of the Gaussian symmetric interfering multiple access channel satisfies*

$$D - 2\log(c_2/\delta) \leq C_{G\text{-}IMAC} \leq D + c_3,$$

with $D := \min\{D_1, D_2, D_3, D_4, D_5\}$ and

$$\begin{aligned}
D_1 &:= 2\max((n_1 - n_i)^+, n_i) + \min((n_1 - n_i)^+, n_i),\\
D_2 &:= \tfrac{2}{3}(2\max(n_1, n_i) + (n_1 - n_i)^+),\\
D_3 &:= 2n_1,\\
D_4 &:= \max(2n_2, 2(n_1 - n_i)^+, 2n_i),\\
D_5 &:= \max(n_1, n_i) + \max(n_2, (n_1 - n_i)^+).
\end{aligned}$$

and c_2, c_3 are constants.

The proof for the achievability can be found in Section 2.7. It makes use of the scheme for the lower triangular deterministic model and uses a result from number theory, the Khintchine-Groshev Theorem, as well as techniques developed in [NMA13] and new techniques tailored towards the G-IMAC model. The proof of the upper bound is in the Appendix 2.10.1 and utilizes the upper bound of Theorem 2.5. Note that, as in the two theorems for the LTD channel model, we have a constant-gap result. This is because c_2 and c_3 are constants which are independent of the channel gain and δ is a trade-of factor in the same fashion as those in the previous results. This means that a bigger δ corresponds to a smaller gap but increases the outage set of channel gains for which the method does not work. In the following section, we will go into the details of the analysis and provide the proofs for the stated theorems.

2.5. Analysis of the LD-IMAC

2.5.1. Achievable Scheme for Theorem 2.1

The achievability scheme for the IMAC is basically an extended version of the scheme already used for the MAC-P2P in [BW11]. Like in the MAC-P2P we split the system (2.8) into two sub systems, $\mathcal{R}_{ach}^{(1)}$ and $\mathcal{R}_{ach}^{(2)}$, see Figure 2.4. Unlike in [BW11], both of our

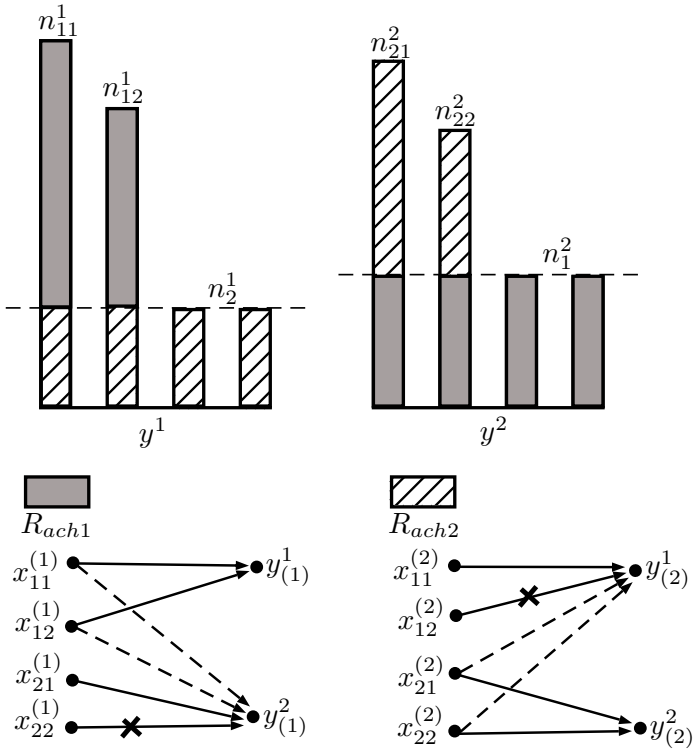

Figure 2.4.: Illustration of the split into two subsystems. The two models at the bottom show that letting the weaker user be silent (illustrated as crossed out arrows in each sub-system) results in a one-sided interference MAC-P2P model. The direct links are shown as normal arrows, whereas the interference links as shown as dashed arrows. We can therefore utilize the achievable scheme of the MAC-P2P for both sub-systems which leads to our overall achievable sum-rate.

sub-systems are identical. The sum of the achievable rates of these two sub systems will constitute the overall sum rate. The sub systems are given by the equations

$$\begin{aligned}\mathbf{y}_1^{(1)} &= \mathbf{S}^{q^{(1)}-(n_{11}^1-n_2^1)}\mathbf{x}_{11}^{(1)} \oplus \mathbf{S}^{q^{(1)}-(n_{12}^1-n_2^1)}\mathbf{x}_{12}^{(1)} \\ \mathbf{y}_2^{(1)} &= \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{11}^{(1)} \oplus \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{12}^{(1)} \oplus \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{21}^{(1)} \oplus \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{22}^{(1)}\end{aligned}$$

for $\mathcal{R}_{ach}^{(1)}$ and for $\mathcal{R}_{ach}^{(2)}$ we have:

$$\begin{aligned}\mathbf{y}_2^{(2)} &= \mathbf{S}^{q^{(2)}-(n_{21}^2-n_1^2)}\mathbf{x}_{21}^{(2)} \oplus \mathbf{S}^{q^{(2)}-(n_{22}^2-n_1^2)}\mathbf{x}_{22}^{(2)} \\ \mathbf{y}_1^{(2)} &= \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{11}^{(2)} \oplus \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{12}^{(2)} \oplus \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{21}^{(2)} \oplus \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{22}^{(2)}.\end{aligned}$$

Examining the resulting sub-systems, one can see that leaving one private part, at the side of the interference silent, results in a sub-system equal to $\mathcal{R}_{ach}^{(2)}$ in [BW11]. In particular

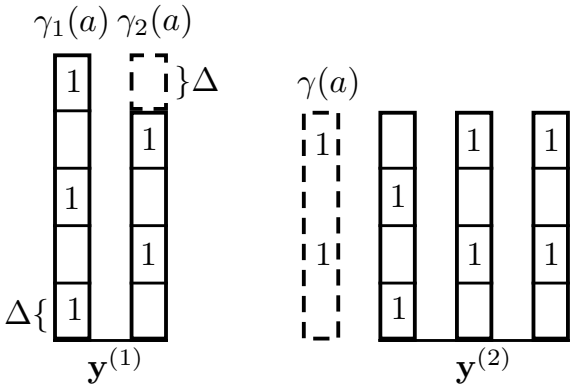

Figure 2.5.: Illustration of the γ-functions.

we choose $\mathbf{x}_{22}^{(1)} := \mathbf{0}$ and $\mathbf{x}_{12}^{(2)} := \mathbf{0}$ resulting in

$$\mathbf{y}_1^{(1)} = \mathbf{S}^{q^{(1)}-(n_{11}^1-n_2^1)}\mathbf{x}_{11}^{(1)} \oplus \mathbf{S}^{q^{(1)}-(n_{12}^1-n_2^1)}\mathbf{x}_{12}^{(1)}$$
$$\mathbf{y}_2^{(1)} = \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{11}^{(1)} \oplus \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{12}^{(1)} \oplus \mathbf{S}^{q^{(1)}-n_1^2}\mathbf{x}_{21}^{(1)}$$

for $\mathcal{R}_{ach}^{(1)}$ and for $\mathcal{R}_{ach}^{(2)}$ we have:

$$\mathbf{y}_2^{(2)} = \mathbf{S}^{q^{(2)}-(n_{21}^2-n_1^2)}\mathbf{x}_{21}^{(2)} \oplus \mathbf{S}^{q^{(2)}-(n_{22}^2-n_1^2)}\mathbf{x}_{22}^{(2)}$$
$$\mathbf{y}_1^{(2)} = \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{11}^{(2)} \oplus \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{21}^{(2)} \oplus \mathbf{S}^{q^{(2)}-n_2^1}\mathbf{x}_{22}^{(2)}.$$

The achievable sum rates for the systems are defined as

$$R_\Sigma^{(1)} \leq n_1^2 + \zeta^{(1)} + \phi(n_2^1, \Delta_1)$$

$$R_\Sigma^{(2)} \leq n_2^1 + \zeta^{(2)} + \phi(n_1^2, \Delta_2).$$

Where $\zeta^{(1)} := n_{12}^1 - n_2^1 - n_1^2$, $\zeta^{(2)} := n_{22}^2 - n_2^1 - n_1^2$ and the function ϕ as in 2.1. It suffices to show the achievability of one sub-system, the results for the other sub-systems follows by symmetry. Consider the sum rate $R_\Sigma^{(1)}$, let $\mathbf{a} \in \mathbb{F}_2^{n_1^2}$ specify the levels used for encoding the interference affected part of $\mathbf{x}_{21}$, where $a_i = 1$ if level i is used and $a_i = 0$ otherwise. Define $\gamma(\mathbf{a}) := \mathbf{1}_{n_1^2} - \mathbf{a}$, $\gamma_1(\mathbf{a}) := (\gamma(\mathbf{a}); \mathbf{1}_{\Delta_1})$ and $\gamma_2(\mathbf{a}) := [\mathbf{0}_{\Delta_1}; \gamma(\mathbf{a})]$, see Fig. 2.5. Then we can achieve

$$R_\Sigma^{(1)} \leq |\gamma_1(\mathbf{a})| + |\gamma_2(\mathbf{a})| - \rho(|\mathbf{a}|) + |\mathbf{a}|$$

where

$$\rho(x) := \min_{\mathbf{a} \in \mathbb{F}_2^{n_1^2} : |\mathbf{a}| = x} \gamma_1(\mathbf{a})^T \gamma_2(\mathbf{a})$$

is indicating how many used bit-levels between the common signal parts of $\mathbf{x}_{11}$ and $\mathbf{x}_{12}$ are overlapping. Minimizing $\rho(x)$, with a per-definition non-overlapping $\gamma(\mathbf{a})$ gives a solution with maximal direct rate and minimal interference. A solution for the assignment vector $\mathbf{a}$ with a given x can be shown to be of the following form. As in [BW11] we denote $l = n_1^2 \operatorname{div} \Delta_1$ and $Q = n_1^2 \bmod \Delta_1$, i.e., $n_1^2 = l\Delta_1 + Q$. We also subdivide $\mathbf{a}$ into $l\Delta_1$ blocks of length Δ_1, with one remainder block of length Q. Now, we distribute ones over all even-numbered blocks of $\mathbf{a}$, which means that those blocks are used for communication. Moreover, we distribute ones over the remainder block. The exact solution for the case that l is even, was given in [BW11] as

$$\mathbf{A}_{\text{even}} = \left(\mathbf{0}_{1\times\frac{l}{2}}; \mathbf{e}_k\right)_{k=1}^{l/2} \otimes \mathbf{I}_{\Delta_1},$$
$$\mathbf{A}_{\text{odd}} = \left(\mathbf{e}_k; \mathbf{0}_{1\times\frac{l}{2}}\right)_{k=1}^{l/2} \otimes \mathbf{I}_{\Delta_1}$$

and

$$\mathbf{A}_{\text{even}} = \left[\left(\mathbf{0}_{1\times\frac{(l-1)}{2}}; \mathbf{e}_k\right)_{k=1}^{(l-1)/2}; \mathbf{0}_{1\times\frac{l-1}{2}}\right] \otimes \mathbf{I}_{\Delta_1},$$
$$\mathbf{A}_{\text{odd}} = \mathbf{M}_{l\Delta_1}\left(\left[\left(\mathbf{e}_k; \mathbf{0}_{1\times\frac{(l+1)}{2}}\right)_{k=1}^{(l-1)/2}; \mathbf{e}_{\frac{l+1}{2}}\right] \otimes \mathbf{I}_{\Delta}\right)$$

for odd l. Here, $\otimes$ denotes the Kronecker product, $\mathbf{e}_k$ the unit row vector of appropriate size with 1 at position k and $\mathbf{M}_N = (\mathbf{e}_{N-k+1})_{k=1}^N$ is the flip matrix. Then the matrix

$$\mathbf{P} = \left[\mathbf{A}_{\text{even}} | \mathbf{0}_{l\Delta\times Q} | \mathbf{A}_{\text{odd}}\right],$$

gives an optimal assignment vector $\mathbf{a}$ by setting $\mathbf{a} = \mathbf{P}[\mathbf{1}_x; \mathbf{0}_{n_1^2-x}]$.

Now, the overall sum rate for the LD-IMAC system can be obtained by adding the rates of the sub systems: $R_\Sigma^{(1)} + R_\Sigma^{(2)} = R_\Sigma$

$$\begin{aligned} R_\Sigma &\le n_1^2 + \zeta^{(1)} + \phi(n_2^1, \Delta_1) + n_2^1 + \zeta^{(2)} + \phi(n_1^2, \Delta_2) \\ &= n_{12} + n_{22} - n_2^1 - n_1^2 + \phi(n_2^1, \Delta_1) + \phi(n_1^2, \Delta_2). \end{aligned} \tag{2.11}$$

■

2.5.2. Transfer from LD-IMAC to G-IMAC

In this section we prove Theorem 2.3, and therefore show the achievable sum-rate for the G-IMAC based on lattice coding schemes with an inherited structure of the linear deterministic schemes.

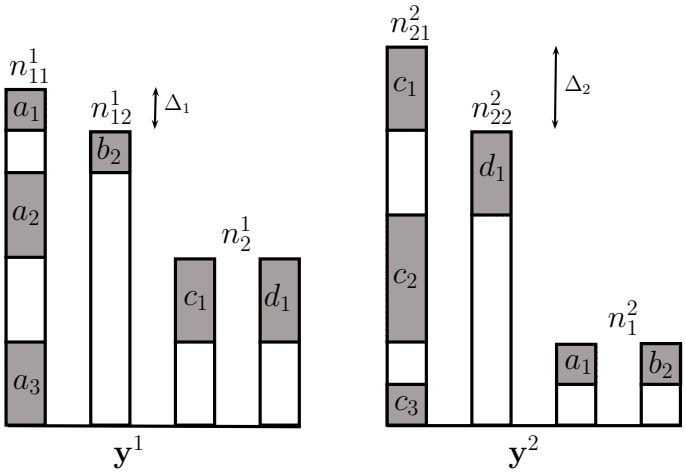

Figure 2.6.: An example for a scheme which achieves the upper bound is presented in the figure. The MAC-cell 1 has n_{11}^1 and n_{12}^1 bit levels in the direct paths and generates interference, at the other cell, of n_1^2 bit levels. Whereas the MAC cell 2 has n_{21}^2 and n_{22}^2 bit levels in the direct path and generates n_2^1 bit levels interference. It can be seen that the scheme utilizes the full bit-level range of the receivers except for half of the incoming interference effected bit-levels and therefore reaches the upper bound $R_\Sigma \leq n_{11}^1 + n_{21}^2 - \frac{1}{2}n_1^2 - \frac{1}{2}n_2^1$.

Weak Interference Regime

For this part, we assume w.l.o.g. that $h_{i1}^j \geq h_{i2}^j$ for $i = j$. This means that the first direct path is stronger or equal than the second direct path in each cell. Also, remember that we have equal (coarse) interference strength at the receivers. With the specific modulation from (2.5), we can assume that

$$h_{i1}^j = h_{i2}^j \text{ for } i \neq j. \tag{2.12}$$

Furthermore we define two expressions, the signal-to-noise ratio and the interference-to-noise ratio as:

$$|h_{ik}^j|^2 P = \begin{cases} \mathrm{SNR}_{ik} & \text{if } i = j \\ \mathrm{INR}_i^j & \text{if } i \neq j. \end{cases}$$

We also introduce two parameters α_i, β_i which combine these ratios with $\mathrm{SNR}_{i2} = \mathrm{SNR}_{i1}^{\beta_i}$ and $\mathrm{INR}_j^i = \mathrm{SNR}_{i1}^{\alpha_i}$. These parameters correspond to α, β which are used in the LDM channel model [FW14a] and in GDoF considerations. Now we can restrict the investigation to the weak interference regime defined through

$$\mathrm{INR}_1^2 + \mathrm{INR}_2^1 \leq \min\{\mathrm{SNR}_{12}, \mathrm{SNR}_{22}\}. \tag{2.13}$$

We assume that $\mathrm{SNR}_{ik} > 1$, otherwise the user can be left silent which results in a 1 bit penalty of the sum-rate. For convenience we use the standard terms: common and private signal, for the part which is seen at both cells and the part which is only received in the intended cell, respectively. Also note that the following techniques work for all channel parameters in the defined regime, except for a singularity at $\beta_i = 1$ in which the additional gain for that corresponding cell will be zero. These techniques are therefore not limited to any kind of rational numbers set, as alignment comes naturally due to the LDM schemes and the assumption (2.12).

Power Partitioning

The power as observed at each receiver is partitioned into intervals. The number of partitions is depended on the channel structure, in particular the β_i, α_i-parameters. These partitions play the role of intervals of bit levels in the LDM. The common signal part of cell i is partitioned into

$$\lfloor L_i \rfloor = \left\lfloor \frac{\log \mathrm{SNR}_{j1}^{\alpha_j}}{\log \mathrm{SNR}_{i1}^{(1-\beta_i)}} \right\rfloor$$

intervals. Moreover, there is an additional reminder block. The private signal part consists of an interference effected part, which is partitioned into $\lfloor L_j \rfloor$ intervals with an additional reminder part, as well as an interference free part. We, therefore, have a total of $l_{\max} \leq \lfloor L_i \rfloor + \lfloor L_j \rfloor + 3$ power partitions, depending on the number of non-zero reminder parts and if there is an additional interference free private signal part. Signal power is defined as

$$\theta_{il} = \begin{cases} \mathrm{SNR}_{i1}^{1-(l-1)(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-l(1-\beta_i)} & \text{for } 1 \leq l \leq \lfloor L_i \rfloor \\ \mathrm{SNR}_{i1}^{1-\lfloor L_i \rfloor(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-(\lfloor L_i \rfloor+1)(1-\beta_i)} & \text{for } l = \lfloor L_i \rfloor + 1 \\ \mathrm{SNR}_{i1}^{1-(\lfloor L_i \rfloor+1)(1-\beta_i)} - \mathrm{SNR}_{i1}^{\alpha_i} & \text{for } l = \lfloor L_i \rfloor + 2 \\ \frac{\mathrm{SNR}_{i1}^{\alpha_i}}{\mathrm{SNR}_{j1}^{(l-\lfloor L_i \rfloor-2)(1-\beta_j)}} - \frac{\mathrm{SNR}_{i1}^{\alpha_i}}{\mathrm{SNR}_{j1}^{(l-\lfloor L_i \rfloor-1)(1-\beta_j)}} & \text{for } \lfloor L_i \rfloor + 2 \leq l \\ & \leq \lfloor L_i \rfloor + \lfloor L_j \rfloor + 2 \\ \mathrm{SNR}_{i1}^{\alpha_i} \mathrm{SNR}_{j1}^{-\lfloor L_j \rfloor(1-\beta_j)} - 1 & \text{for } l = l_{\max} \end{cases} \tag{2.14}$$

with l indicating the specific partition (Fig. 2.7). Note that this is for the cases where $\lfloor L_i \rfloor$ = odd. The additional remainder term at $l = \lfloor L_i \rfloor + 1$ vanishes for $\lfloor L_i \rfloor$ = even, because it can be merged with the subsequent partition. In that case, all following powerlevels need to be changed accordingly. Each user k of cell i decomposes its signal into a sum of independent sub-signals

$$\mathbf{x}_{ik} = \sum_{l=1}^{l_{\max}} \mathbf{x}_{ik}(l).$$

This decomposition can be seen as a message split, where every message is separately encoded by a lattice code. Note that user 2 can only send at power levels $l > 1$, due to its power constrains.

Layered Nested Lattice Codes

Instead of the Loeliger-type [Loe97] lattice codes, used in [FW14b], we will use the nested lattice codes introduced in [UZ04] which can achieve capacity in the AWGN single-user channel. This results in a slightly lower gap in the overall rate terms. A lattice Λ is a discrete subgroup of $\mathbb{R}^n$ which is closed under real addition and reflection. Moreover, denote the nearest neighbour quantizer by

$$Q_\Lambda(\mathbf{x}) := \arg\min_{\mathbf{t}\in\Lambda} ||\mathbf{x} - \mathbf{t}||.$$

The fundamental Voronoi region $\mathcal{V}(\Lambda)$ of a lattice Λ consists of all points which get mapped or quantized to the zero vector. The modulo operation is defined as

$$[\mathbf{x}] \mod \Lambda := \mathbf{x} - Q_\Lambda(\mathbf{x}).$$

A nested lattice code is composed of a pair of lattices $(\Lambda_{\text{fine}}, \Lambda_{\text{coarse}})$, where $\mathcal{V}(\Lambda_{\text{coarse}})$ is the fundamental Voronoi region of the coarse lattice and operates as a shaping region for the corresponding fine lattice Λ_{fine}. It is therefore required that $\Lambda_{\text{coarse}} \subset \Lambda_{\text{fine}}$. Such a code has a corresponding rate R equal to the log of the nesting ratio. A part of the split message is now mapped to the corresponding codeword $\mathbf{u}_{ik}(l) \in \Lambda_{\text{fine},l-1} \cap \mathcal{V}(\Lambda_{\text{coarse},l})$, which is a point of the fine lattice inside the fundamental Voronoi region of the coarse lattice. Note that $\Lambda_{l_{max}} \subset \cdots \subset \Lambda_1$. The code is chosen such that it has a power of θ_{il}. The codeword $\mathbf{x}_{ik}(l)$ is now given as

$$\mathbf{x}_{ik}(l) = [\mathbf{u}_{ik} - \mathbf{d}_{ik}] \mod \Lambda_l,$$

where we dither (shift) with $\mathbf{d}_{ik} \sim \text{Unif}(\mathcal{V}(\Lambda_l))$ and reduce the result modulo-Λ_l. Transmitter ik now sends a scaled $\mathbf{x}_{ik}$ over the channel, such that the power per sub-signal $\mathbf{x}_{ik}(l)$ is $\frac{\theta_{il}}{|h^i_{ik}|^2}$ and receivers see a power of θ_{il}. Due to the partitioning construction, the $\mathbf{x}_{ik}$ satisfy the power restriction of P for user 1,

$$\sum_{l=1}^{l_{\max}} \frac{\theta_{il}}{|h^i_{i1}|^2} \leq \frac{\text{SNR}_{i1}}{|h^i_{i1}|^2} = P$$

and user 2

$$\sum_{l=2}^{l_{\max}} \frac{\theta_{il}}{|h_{i2}^i|^2} \leq \frac{\mathrm{SNR}_{i2}}{|h_{i2}^i|^2} = P$$

in each cell i.

Moreover, aligning sub-signals use the same code (with independent shifts).

In [UZ04] it was shown that nested lattice codes can achieve the capacity of the AWGN single-user channel with vanishing error probability. Viewing each of our power intervals as a channel, we therefore have that

$$R(l) \leq \tfrac{1}{2} \log \left(1 + \frac{\theta_{il}}{N_i(l)}\right), \tag{2.15}$$

where $N_i(l)$ denotes the noise variance per dimension of the subsequent levels. If a sum of K lattice points gets aligned at a power level θ_{il} and we want to decode the lattice point corresponding to this sum, then the achievable rate is given by

$$R(l) \leq \tfrac{1}{2} \log \left(\tfrac{1}{K} + \frac{\theta_{il}}{N_i(l)}\right), \tag{2.16}$$

which is obtained through minimization of the denominator in [NG11, Theorem 1] and MMSE scaled decoding.

Lattice Code Alignment

Due to the construction, shifted codewords $\mathbf{x}_{i1}(l)$ and $\mathbf{x}_{i2}(l+1)$ are received on separate power levels at the intended receiver and align on the same power level at the unintended receiver. As an example we look at the codewords $\mathbf{x}_{11}(2)$ and $\mathbf{x}_{12}(3)$. They are transmitted from the first and second transmitter of cell 1, with a scaled power of $\frac{\theta_{12}}{|h_{11}^1|^2}$ and $\frac{\theta_{13}}{|h_{12}^1|^2}$, respectively. This means that receiver 1 sees them with power

$$E(||h_{11}^1|\mathbf{x}_{11}(2)|^2) = \tfrac{\theta_{12}|h_{11}^1|^2}{|h_{11}^1|^2} = \theta_{12}.$$

assuming that level 2 and 3 are within the common signal part we have that $\theta_{12} = (|h_{11}^1|^2 P)^{1-1(1-\beta_1)} - (|h_{11}^1|^2 P)^{1-2(1-\beta_1)}$ and

$$E(||h_{12}^1|\mathbf{x}_{12}(3)|^2) = \tfrac{\theta_{13}|h_{12}^1|^2}{|h_{12}^1|^2} = \theta_{13}.$$

with $\theta_{13} = (|h_{11}^1|^2 P)^{1-2(1-\beta_1)} - (|h_{11}^1|^2 P)^{1-3(1-\beta_1)}$. Clearly both codewords are received on different levels as long as $\beta_1 \neq 1$. For the unintended receiver 2, these codewords are

received with power

$$E(||h_{11}^2|\mathbf{x}_{11}(2)|^2) = \frac{\theta_{12}|h_{11}^2|^2}{|h_{11}^1|^2}. \tag{2.17}$$

and

$$E(||h_{12}^2|\mathbf{x}_{12}(2)|^2) = \frac{\theta_{13}|h_{12}^2|^2}{|h_{12}^1|^2}. \tag{2.18}$$

Now we need to show that (2.17) and (2.18) are the same. For (2.17) we have that

$$\begin{aligned}
\frac{\theta_{12}|h_{11}^2|^2}{|h_{11}^1|^2} &= \left(\mathrm{SNR}_{11}^{1-1(1-\beta_1)} - \mathrm{SNR}_{11}^{1-2(1-\beta_1)}\right) \frac{|h_{11}^2|^2}{|h_{11}^1|^2} \\
&= \left(\frac{\mathrm{SNR}_{11}}{\mathrm{SNR}_{11}^{(1-\beta_1)}} - \frac{\mathrm{SNR}_{11}}{\mathrm{SNR}_{11}^{2(1-\beta_1)}}\right) \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{11}} \\
&= \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{11}^{(1-\beta_1)}} - \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{11}^{2(1-\beta_1)}}.
\end{aligned}$$

For (2.18) we have that

$$\begin{aligned}
\frac{\theta_{13}|h_{11}^2|^2}{|h_{11}^1|^2} &= \left(\mathrm{SNR}_{11}^{1-2(1-\beta_1)} - \mathrm{SNR}_{11}^{1-3(1-\beta_1)}\right) \frac{|h_{11}^2|^2}{|h_{12}^1|^2} \\
&= \left(\frac{\mathrm{SNR}_{11}}{\mathrm{SNR}_{11}^{2(1-\beta_1)}} - \frac{\mathrm{SNR}_{11}}{\mathrm{SNR}_{11}^{3(1-\beta_1)}}\right) \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{12}} \\
&= \left(\frac{\mathrm{SNR}_{11}^{\beta_1+(1-\beta_1)}}{\mathrm{SNR}_{11}^{2(1-\beta_1)}} - \frac{\mathrm{SNR}_{11}^{\beta_1+(1-\beta_1)}}{\mathrm{SNR}_{11}^{3(1-\beta_1)}}\right) \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{12}} \\
&= \left(\frac{\mathrm{SNR}_{11}^{\beta_1}}{\mathrm{SNR}_{11}^{(1-\beta_1)}} - \frac{\mathrm{SNR}_{11}^{\beta_1}}{\mathrm{SNR}_{11}^{2(1-\beta_1)}}\right) \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{12}} \\
&= \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{11}^{(1-\beta_1)}} - \frac{\mathrm{INR}_1^2}{\mathrm{SNR}_{11}^{2(1-\beta_1)}}
\end{aligned}$$

where we used that $\mathrm{SNR}_{11}^{\beta_1} = \mathrm{SNR}_{12}$ as defined.

Decoding Procedure

Decoding occurs per level, treating subsequent levels as noise. Due to the use of nested lattice codes, a sub-signal $\mathbf{u}_{ik} \mod \Lambda_l$ gets decoded, from which the original sub-signal $\mathbf{x}_{ik}$ can be reconstructed. The reconstructed signal then gets subtracted from the total received signal, leaving the noise part. The noise part constitutes the next level and the process continues. In case of an interference-affected level, only the sum of both sub-signals gets decoded $[\mathbf{u}_{ik}(l) + \mathbf{u}_{ik}(l+1)] \mod \Lambda_l$. From the sum, the original sum can be reconstructed and subtracted from the received signal. It is therefore a successive decoding scheme, which was proven to work for nested lattice codes in [Naz12] and recently applied in [CS16]. Therefore, each level is treated as a Gaussian point-to-point channel, and decodability is assured providing that the lattice rate is chosen appropriately according to (2.15) or (2.16), depending on the specific case. With a signal power of θ_{il}, it only remains

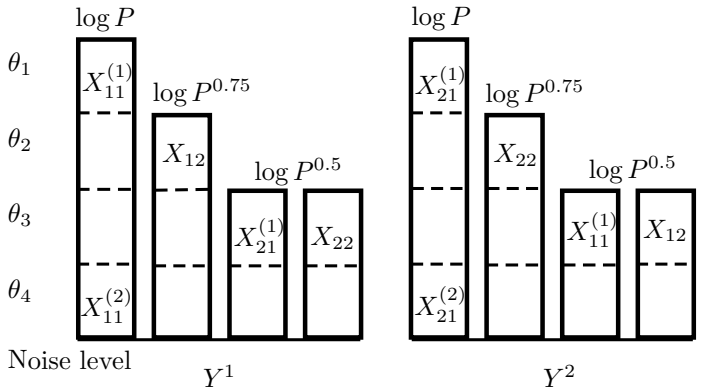

Figure 2.7.: Example of the symmetric restricted IMAC: Illustration of power partitioning, with the resulting 4 signal power levels and level use for coding

to specify the total noise of each level, consisting of the Gaussian noise at the receiver and the signal power of all subsequent levels, including the interference. The total achievable sum-rate is then given as the sum of all $R_{ik}(l)$ of the used direct levels.

Example of the symmetric restricted IMAC

In this example we consider the fairly restricted symmetric IMAC channel, where $\alpha = 0.5$ and $\beta = 0.75$. Note that this example is technically not in the weak interference regime (2.13) any more. However, the alignment strategies of this section can be applied to channels with the relaxed condition $\mathrm{INR}_1^2 + \mathrm{INR}_2^1 \leq \min\{\mathrm{SNR}_{11}, \mathrm{SNR}_{21}\}$ by careful handling of certain cases. This condition becomes $\alpha \leq 0.5$ in our symmetrical example. The symmetry assumption yields that $\mathrm{SNR}_{11} = \mathrm{SNR}_{21} = P$, $\mathrm{SNR}_{12} = \mathrm{SNR}_{22} = P^\beta$ and $\mathrm{INR}_1^2 = \mathrm{INR}_2^1 = P^\alpha$. Therefore we have that $L_i = \lfloor L_i \rfloor = \lfloor \frac{\alpha}{1-\beta} \rfloor = 2$. The scheme (2.14) yields $l_{\max} = 4$ levels with $\theta_1 = P - P^\beta$, $\theta_2 = P^\beta - P^\alpha$, $\theta_3 = P^\alpha - P^{0.25}$ and $\theta_4 = P^{0.25} - 1$. Moreover, we have the following noise powers per level, $N(1) = 1 + (P^{0.75} - 1) + \theta_3$, $N(2) = 1 + (P^{0.5} - 1) + \theta_3$, $N(3) = 1 + (P^{0.25} - 1)$ and $N(4) = 1$. We, therefore, have the following decoding bounds for both cells:

$$\begin{aligned} \{\mathbf{x}_{11}(1), \mathbf{x}_{21}(1)\} : &\qquad R(1) \leq \min\{r_1, r_3\} \\ \{\mathbf{x}_{12}(2), \mathbf{x}_{22}(2)\} : &\qquad R(2) \leq \min\{r_2, r_3\} \\ \{\mathbf{x}_{11}(4), \mathbf{x}_{21}(4)\} : &\qquad R(4) \leq r_4 \end{aligned}$$

with

$$r_1 = \tfrac{1}{2} \log\left(1 + \frac{P - P^{0.75}}{P^{0.75} + \theta_3}\right),$$

$$
\begin{aligned}
r_2 &= \tfrac{1}{2}\log\left(1+\frac{P^{0.75}-P^{0.5}}{P^{0.5}+\theta_3}\right),\\
r_3 &= \tfrac{1}{2}\log\left(\tfrac{1}{2}+\frac{P^{0.5}-P^{0.25}}{P^{0.25}}\right)^{+},\\
r_4 &= \tfrac{1}{2}\log\left(1+\frac{P^{0.25}-1}{1}\right).
\end{aligned}
$$

where the minima are necessary, because $\mathbf{x}_{11}(1), \mathbf{x}_{12}(2)$ and $\mathbf{x}_{21}(1), \mathbf{x}_{22}(2)$ need to be decodable at both receivers. Moreover, neither cell can send on level 3, since all interference is aligned at that level. The total achievable rate is the summation over all levels

$$R_\Sigma = 2R(1) + 2R(2) + 2R(4).$$

Moreover, we can show that

$$
\begin{aligned}
r_1 &= \tfrac{1}{2}\log\left(1+\frac{P-P^{0.75}}{P^{0.75}+\theta_3}\right)\\
&> \tfrac{1}{2}\log\left(\frac{P+\theta_3}{P^{0.75}+\theta_3}\right)\\
&> \tfrac{1}{2}\log\left(\frac{P}{P^{0.75}+\theta_3}\right)\\
&> \tfrac{1}{2}\log\left(\frac{P}{2P^{0.75}}\right)\\
&= \tfrac{1}{2}\log P^{0.25} - \tfrac{1}{2},
\end{aligned}
$$

where the last inequality follows from the fact that $P^{0.75} > \theta_3$ because of $P > 1$. Similarly, we can show that

$$
\begin{aligned}
r_2 &> \tfrac{1}{2}\log P^{0.25} - \tfrac{1}{2},\\
r_3 &> \tfrac{1}{2}\log P^{0.25} - 1,\\
r_4 &= \tfrac{1}{2}\log P^{0.25}.
\end{aligned}
$$

The total achievable rate is therefore

$$R_\Sigma = 2R(1) + 2R(2) + 2R(4) = 8\tfrac{1}{2}\log P^{0.25} - 2\tfrac{1}{2}\log P^{0.25} - 4 = 2\tfrac{1}{2}\log P - \tfrac{1}{2}\log P^{0.5} - 4$$

With the definition of $\alpha = 0.5$, $n_1 = \lfloor \frac{1}{2}\log P \rfloor$ and $n_i = \lfloor \frac{1}{2}\log P^{0.5} \rfloor$ one can see, that the proposed scheme can achieve the upper bound within a constant gap of 4 Bits.

Achievable Rate: The general (weak) interference case

Henceforth, we define $i \neq j$ for $i, j \in \{1, 2\}$ in all equations. In the general case, β_i and α_i can be any value in the defined regime and therefore any number of levels can be needed. The power splitting is done as in the example where signal power is given by (2.14). The choice of codeword decomposition and level usage is dependent on the underlying LDM scheme. We use the power partitions of θ_{il} in the same way as the Δ_i blocks in the LDM. However, instead of filling the $l-$th Δ_i-block with bits, we use the specific power partition interval θ_{il} to transmit a sub-signal lattice codeword. As in the previous example, the sub-signal codewords can be decoded providing a rate of (2.15) and (2.16), depending on the number of aligning signals. It remains to specify the effective noise per level. The general noise structure is

$$N_i(l) = 1 + \sum_{\text{used levels}} \theta_{l+1},$$

we the levels of aligned interference are counted twice. We have to distinguish three different rate-term structures for cell i, see Fig. 2.8. The first one is the common signal part R_{IC_i}. Here we need decoding bounds $R_{\mathrm{IC}_i}(l)$ per power-partition, which are also received as interference and therefore need to obey two decoding conditions. One decoding bound stems from the direct path utilizing bound (2.15). The other decoding bound stems from the fact that our successive decoding scheme needs to decode the sum of two interfering bit-levels at every odd bit-level and therefore needs to obey (2.16). We show in the Appendix 2.10.2, that we can achieve

$$\bar{R}_{\mathrm{IC}_i}(l) > \tfrac{1}{2} \log \mathrm{SNR}_{i1}^{(1-\beta_i)} - 1$$

which is the minimum of both bounds for the common part per power partition. The second term is the private part R_{P_i} which is not interference affected, therefore outside the alignment structures. We need to distinguish the two cases $\lfloor L_i \rfloor = \text{odd}$ and $\lfloor L_i \rfloor = \text{even}$. For $\lfloor L_i \rfloor = \text{odd}$, we have a remainder term with power

$$\mathrm{SNR}_{i1}^{1-\lfloor L_i \rfloor (1-\beta_i)} - \mathrm{SNR}_{i1}^{1-(\lfloor L_i \rfloor + 1)(1-\beta_i)},$$

and the regular private term with power

$$\mathrm{SNR}_{i1}^{1-(\lfloor L_i \rfloor + 1)(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-\alpha_i(1-\beta_i)}.$$

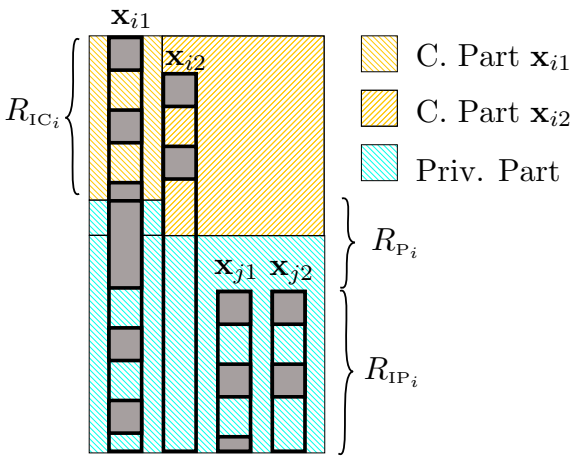

Figure 2.8.: Illustration of the three rate term structures. R_{IC_i} is the alignment structure of the common part. Note that the common part of $\mathbf{x}_{i2}$ is down shifted by exactly one power partition. Moreover, we illustrate the private signal parts, with and without interference.

For $\lfloor L_i \rfloor$ = even, we have a remainder term of power $\mathrm{SNR}_{i1}^{1-\lfloor L_i \rfloor(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-L_i(1-\beta_i)}$ and a private term of power $\mathrm{SNR}_{i1}^{1-L_i(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-\alpha_i(1-\beta_i)}$, which is depicted in Fig. 2.8. Note that for $\lfloor L_i \rfloor = L_i$ = even, the remainder term is zero. Let us choose the case $\lfloor L_i \rfloor$ = odd as an example. Here we have the remainder term and the private part term. The remainder term has the same analysis as the terms of R_{IC_i} in Appendix 2.10.2. Considering the new power partition, we get a rate of

$$R_{\mathrm{P}_{1i}} > \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{1-\lfloor L_i \rfloor(1-\beta_i)} - \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{1-(\lfloor L_i \rfloor+1)(1-\beta_i)} - 1.$$

For the private part, we only have to consider the direct rate, and do not need the minimisation over both decoding bounds which results in a smaller bit-gap

$$R_{\mathrm{P}_{2i}} > \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{1-(\lfloor L_i \rfloor+1)(1-\beta_i)} - \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{\alpha_i} - \tfrac{1}{2}.$$

The total rate of the private part is therefore

$$R_{\mathrm{P}_i} > \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{1-\lfloor L_i \rfloor(1-\beta_i)} - \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{\alpha_i} - 2.$$

Note that this is also achievable for the cases with $\lfloor L_i \rfloor$ = odd. The only difference is the location of the power split. Note that in our weak interference regime (2.13), we have that $1 - \lfloor L_i \rfloor(1-\beta_i) \geq \alpha_i$, since $1 - L_i(1-\beta_i) \geq \alpha_i$ which can be shown in the following way.

Plugging in the definition of L_i, we get

$$\begin{aligned} & 1 - \frac{\log \mathrm{SNR}_{j1}^{\alpha_j}}{\log \mathrm{SNR}_{i1}^{(1-\beta_i)}}(1-\beta_i) \geq \alpha_i \\ \Leftrightarrow \quad & 1 - \frac{\log \mathrm{SNR}_{j1}^{\alpha_j}}{\log \mathrm{SNR}_{i1}} \geq \alpha_i \\ \Leftrightarrow \quad & \log \mathrm{SNR}_{i1} - \log \mathrm{SNR}_{j1}^{\alpha_j} \geq \alpha_i \log \mathrm{SNR}_{i1} \\ \Leftrightarrow \quad & \log \mathrm{SNR}_{i1} \geq \log \mathrm{SNR}_{i1}^{\alpha_i} + \log \mathrm{SNR}_{j1}^{\alpha_j} \\ \Leftrightarrow \quad & \log \mathrm{SNR}_{i1} \geq \log \mathrm{INR}_2^1 + \log \mathrm{SNR}_1^2 \end{aligned}$$

which is true, since $\min\{\mathrm{SNR}_{12}, \mathrm{SNR}_{22}\} \leq \mathrm{SNR}_{i1}$.

The third rate term structure is the private rate part, which is affected by the interference. For every power partition, we can achieve a rate

$$\bar{R}_{\bar{\mathrm{IP}}_i}(l) > \tfrac{1}{2} \log \mathrm{SNR}_{j1}^{(1-\beta_j)} - \tfrac{1}{2},$$

which is shown in the Appendix 2.10.2.

Furthermore, if $L_j \neq \lfloor L_j \rfloor$ = even, the private part rate $R_{\bar{\mathrm{IP}}_i}$ has a remainder term allocated at the lowest power level. The lowest level has a noise term of 1 and a power of $\mathrm{SNR}_{i1}^{\alpha_i} \mathrm{SNR}_{j1}^{-\lfloor L_j \rfloor (1-\beta_j)} - 1$. We only need to decode the direct rate term and therefore get a decoding bound of

$$R_{\mathrm{IP}_{i,\mathrm{rem}}} \leq \tfrac{1}{2} \log \mathrm{SNR}_{i1}^{\alpha_i} \mathrm{SNR}_{j1}^{-\lfloor L_j \rfloor (1-\beta_j)}.$$

The total achievable sum rate is the summation over all three rate term structures $\bar{R}_{\mathrm{IC}_i}$, $\bar{R}_{\mathrm{IP}_i}$, and R_{P_i} including the remainder parts. Moreover, we need to sum over all individual partitions. This means that

$$\bar{R}_{\mathrm{IC}_i} > \sum_{l}^{\lfloor L_i \rfloor} \tfrac{1}{2} \log \mathrm{SNR}_{i1}^{(1-\beta_i)} - 1,$$

and

$$\bar{R}_{\mathrm{IP}_i} > \sum_{\substack{l=1 \\ l \text{ odd}}}^{\lfloor L_j \rfloor} \tfrac{1}{2} \log \mathrm{SNR}_{j1}^{(1-\beta_j)} - \tfrac{1}{2}.$$

We show the proof exemplary for the case that $L_i = \lfloor L_i \rfloor$ = even. Here we have an achievable sum-rate of:

$$R_\Sigma = \sum_{i}^{2} \bar{R}_{\mathrm{IC}_i} + \bar{R}_{\mathrm{P}_i} + \bar{R}_{\mathrm{IP}_i}$$

$$
\begin{aligned}
&> \sum_{l}^{\lfloor L_2 \rfloor} (\tfrac{1}{2}\log \mathrm{SNR}_{21}^{(1-\beta_2)} - 1) + \sum_{\substack{l=1 \\ l \text{ even}}}^{\lfloor L_2 \rfloor} (\tfrac{1}{2}\log \mathrm{SNR}_{21}^{(1-\beta_2)} - \tfrac{1}{2}) + \tfrac{1}{2}\log \mathrm{SNR}_{21}^{1-\lfloor L_2 \rfloor (1-\beta_2)} \\
&\quad + \sum_{l}^{\lfloor L_1 \rfloor} (\tfrac{1}{2}\log \mathrm{SNR}_{11}^{(1-\beta_1)} - 1) + \sum_{\substack{l=1 \\ l \text{ even}}}^{\lfloor L_1 \rfloor} (\tfrac{1}{2}\log \mathrm{SNR}_{11}^{(1-\beta_1)} - \tfrac{1}{2}) + \tfrac{1}{2}\log \mathrm{SNR}_{11}^{1-\lfloor L_1 \rfloor (1-\beta_1)} \\
&\quad - \tfrac{1}{2}\log \mathrm{SNR}_{11}^{\alpha_1} - \tfrac{1}{2}\log \mathrm{SNR}_{21}^{\alpha_2} - 3 \\
&= \lfloor L_2 \rfloor \tfrac{1}{2}\log \mathrm{SNR}_{21}^{(1-\beta_2)} + \frac{\lfloor L_2 \rfloor}{2}\tfrac{1}{2}\log \mathrm{SNR}_{21}^{(1-\beta_2)} + \tfrac{1}{2}\log \mathrm{SNR}_{21}^{1-\lfloor L_2 \rfloor (1-\beta_2)} \\
&\quad + \lfloor L_1 \rfloor \tfrac{1}{2}\log \mathrm{SNR}_{11}^{(1-\beta_1)} + \frac{\lfloor L_1 \rfloor}{2}\tfrac{1}{2}\log \mathrm{SNR}_{11}^{(1-\beta_1)} + \tfrac{1}{2}\log \mathrm{SNR}_{11}^{1-\lfloor L_1 \rfloor (1-\beta_1)} \\
&\quad - 2.5(\lfloor L_1 \rfloor + \lfloor L_2 \rfloor) - \tfrac{1}{2}\log \mathrm{SNR}_{11}^{\alpha_1} - \tfrac{1}{2}\log \mathrm{SNR}_{21}^{\alpha_2} - 3 \\
&= \tfrac{1}{2}\log \mathrm{SNR}_{11} + \frac{\lfloor L_2 \rfloor}{2}\tfrac{1}{2}\log \mathrm{SNR}_{21}^{(1-\beta_2)} + \tfrac{1}{2}\log \mathrm{SNR}_{21} + \frac{\lfloor L_1 \rfloor}{2}\tfrac{1}{2}\log \mathrm{SNR}_{11}^{(1-\beta_1)} \\
&\quad - \tfrac{1}{2}\log \mathrm{SNR}_{11}^{\alpha_1} - \tfrac{1}{2}\log \mathrm{SNR}_{21}^{\alpha_2} - 3 - 2.5(\lfloor L_2 \rfloor + \lfloor L_1 \rfloor) \\
&= \tfrac{1}{2}\log \mathrm{SNR}_{11}^{\beta_1} - \tfrac{1}{2}\log \mathrm{SNR}_{11}^{\alpha_1} + \tfrac{1}{2}\log \mathrm{SNR}_{21}^{\beta_2} - \tfrac{1}{2}\log \mathrm{SNR}_{21}^{\alpha_2} \\
&\quad + \phi(\tfrac{1}{2}\log \mathrm{SNR}_{21}^{\alpha_2}, \tfrac{1}{2}\log \mathrm{SNR}_{11}^{(1-\beta_1)}) \\
&\quad + \phi(\tfrac{1}{2}\log \mathrm{SNR}_{11}^{\alpha_1}, \tfrac{1}{2}\log \mathrm{SNR}_{21}^{(1-\beta_2)}) - 3 - 2.5(\lfloor L_2 \rfloor + \lfloor L_1 \rfloor),
\end{aligned}
$$

where the last step follows from the definition of $\phi(p,q)$ in (2.1). We have that $\phi(p,q) = q + \frac{l(p,q)q}{2}$ for $l(p,q) = \text{even}$. Plugging in $p = \frac{1}{2}\log \mathrm{SNR}_{i1}^{\alpha_i}$ and $q = \frac{1}{2}\log \mathrm{SNR}_{j1}^{(1-\beta_j)}$, shows that $l(\frac{1}{2}\log \mathrm{SNR}_{i1}^{\alpha_i}, \frac{1}{2}\log \mathrm{SNR}_{j1}^{(1-\beta_j)}) = \lfloor L_j \rfloor$ and the result follows. ∎

One can see that the achievable rate of the Gaussian channel is within a constant-gap of $3 + 2.5(\lfloor L_2 \rfloor + \lfloor L_1 \rfloor)$bits of the LDM rate using the correspondence $n_{ik}^j = \lfloor \frac{1}{2}\log |h_{ik}^j|^2 P \rfloor$.

2.6. Analysis of the LTD-IMAC

In this section we prove the two theorems, Theorem 2.5 and Theorem 2.6. In particular, we will first show the achievability in Section 2.6.1 and then in Section 2.6.2 the upper bound, for the theorems.

2.6.1. Achievable Schemes

We start with two lemmas, which provide the bases for the achievable rate in the LTD model in the general symmetric setting and in a weak interference general setting, respectively. Afterwards we discuss two lemmas which are necessary to prove that the codewords in the schemes can be decoded.

Lemma 2.8 (*general interference, symmetry*). *For every $\delta \in (0,1]$ and n_1, n_2, $n_i \in \mathbb{N}$ such that $n_1 \geq n_2$ there exists a set $B \subset (1,2]^{2\times 3}$ of Lebesgue measure $\mu(B) \leq \delta$ such that*

for all channel gains $g_{ik}^{j} \in (1,2]^{2\times 3} \setminus B$ *an achievable sum rate for the IMAC system model is:*

$$R_{\Sigma} \geq \min\{R_{ach,1}, R_{ach,2}, R_{ach,3}, R_{ach,4}, R_{ach,5}\} - 2\log(c/\delta)$$

with

$$R_{ach,1} := 2\max((n_1 - n_i)^+, n_i) + \min((n_1 - n_i)^+, n_i), \tag{2.18a}$$
$$R_{ach,2} := \tfrac{2}{3}(2\max(n_1, n_i) + (n_1 - n_i)^+), \tag{2.18b}$$
$$R_{ach,3} := 2n_1, \tag{2.18c}$$
$$R_{ach,4} := \max(2n_2, 2(n_1 - n_i)^+, 2n_i), \tag{2.18d}$$
$$R_{ach,5} := \max(n_1, n_i) + \max(n_2, (n_1 - n_i)^+). \tag{2.18e}$$

Lemma 2.9 (*weak interference*)**.** *For every* $\delta \in (0,1]$ *and* n_{k1}^{k}, n_{k2}^{k}, $n_{l}^{k} \in \mathbb{N}$ *such that* $n_{k1}^{k} \geq n_{k2}^{k} > n_{l}^{k}$ *and* $n_2^1 + n_1^2 < \min\{n_{11}^1, n_{21}^2\}$*, there exists a set* $B \subset (1,2]^{2\times 3}$ *of Lebesgue measure* $\mu(B) \leq \delta$ *such that for all channel gains* $g_{ik}^{j} \in (1,2]^{2\times 3} \setminus B$ *an achievable sum rate for the IMAC system model is:*

$$R_{\Sigma} \geq \min\{R_{ach,1}, R_{ach,2}, R_{ach,3}, R_{ach,4}\} - 2\log(c/\delta)$$

with

$$R_{ach,1} := \max\{(n_{11}^1 - n_1^2), n_{12}^1\} + \max\{(n_{21}^2 - n_2^1), n_{22}^2\} \tag{2.18f}$$
$$R_{ach,2} := \max\{(n_{11}^1 - n_1^2), n_{12}^1\} + n_{21}^2 - \tfrac{1}{2}n_2^1 \tag{2.18g}$$
$$R_{ach,3} := n_{11}^1 - \tfrac{1}{2}n_1^2 + \max\{(n_{21}^2 - n_2^1), n_{22}^2\} \tag{2.18h}$$
$$R_{ach,4} := n_{11}^1 - \tfrac{1}{2}n_1^2 + n_{21}^2 - \tfrac{1}{2}n_2^1, \tag{2.18i}$$

Proof. To prove the lemmas we first need to show under which conditions a rate allocation scheme yields linear independence of the used **H** columns and therefore allows successful decoding. For the interference range $\alpha \geq \frac{1}{2}$, we can use the lemma 11 of [NMA13], with a re-labelling such that it fits our case. The following lemma shows the modified version.

Lemma 2.10 ([NMA13, Lemma 11 (modified)])**.** *Let* $\delta \in (0,1]$ *and* n_1, n_2, $n_i \in \mathbb{N}$ *such that* $n_1 \geq n_2 \geq n_i$*, and* $2n_i \geq n_1$*, and let* R_{k1}^{c}, R_{k1}^{p1}, R_{k1}^{p2}, $R_{k2}^{c} \in \mathbb{N}$ *with* $k, l \in \{1,2\}$ *and* $l \neq k$ *satisfy,*

$$R_{k1}^{c} + R_{k2}^{c} + \max\{R_{l1}^{c}, R_{l2}^{c}\} + R_{k1}^{p1} \leq n_1 - \log\left(\tfrac{32}{\delta}\right)$$

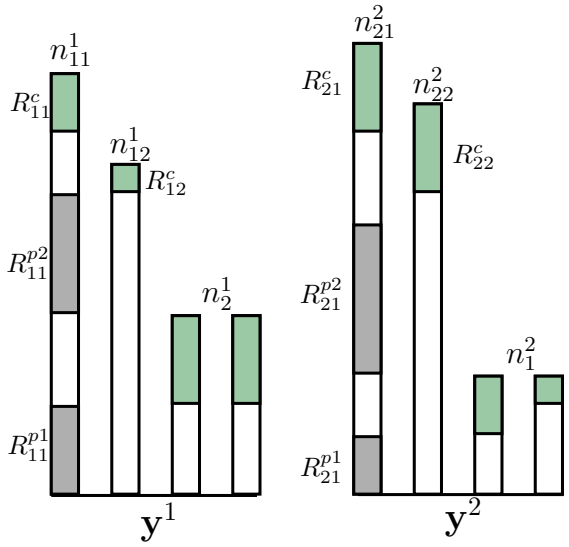

Figure 2.9.: Illustration of the achievable scheme and rate allocations in the range $\alpha < \frac{1}{2}$. The figure shows an asymmetric coarse channel gain example, where the received signal $\mathbf{y}^1$ has $\frac{1}{2}n_i < \Delta < n_i$ (case I.2) and the received signal $\mathbf{y}^2$ has $\Delta \leq \frac{1}{2}n_i$ (case I.3) .

$$R_{k2}^c + \max\{R_{l1}^c, R_{l2}^c\} + R_{k1}^{p1} \leq n_2 - \log\left(\tfrac{32}{\delta}\right)$$
$$\max\{R_{l1}^c, R_{l2}^c\} + R_{k1}^{p1} \leq n_i$$

Then, the bit allocation [...] for the (modulated) deterministic X-channel allows successful decoding at both receivers for all channel gains ($g_{ik}^j \in (1,2]^{2\times 3}$) except for a set $B \subset (1,2]^{2\times 3}$ of Lebesgue measure $\mu(B) \leq \delta$.

For the range of $\alpha < \frac{1}{2}$, our achievable scheme gets a second private signal part between the common and the private signal of the stronger user (see for example Fig. 2.9, R_{11}^{p2}). Therefore, Lemma 2.10 is not applicable anymore. However, due to the special structure of the achievable scheme, we can modify the proof to show a similar result.

Lemma 2.11. *Let $\delta \in (0,1]$ and n_{k1}^k, n_{k2}^k, $n_l^k \in \mathbb{N}$ such that $n_{k1}^k \geq n_{k2}^k > n_l^k$ and $n_2^1 + n_1^2 < \min\{n_{11}^1, n_{21}^2\}$, and let R_{k1}^c, R_{k1}^{p1}, R_{k1}^{p2}, R_{k2}^c, $R_{21}^c \in \mathbb{N}$, with $k,l \in \{1,2\}, k \neq l$ satisfy,*

$$R_{k1}^c + R_{k1}^{p1} + R_{k1}^{p2} + R_{k2}^c + \max\{R_{l2}^c, R_{l1}^c\} \leq n_{k1}^k - \log\left(\tfrac{8}{\delta}\right)$$
$$R_{k1}^{p1} + R_{k1}^{p2} + R_{k2}^c + \max\{R_{l1}^c, R_{l2}^c\} \leq n_{k2}^k$$
$$R_{k1}^{p2} + R_{k1}^{p1} + \max\{R_{l1}^c, R_{l2}^c\} \leq (n_{k1}^k - n_k^l)$$

$$R_{k1}^{p1} + \max\{R_{l1}^{c}, R_{l2}^{c}\} \leq n_l^k$$

Then, a bit allocation, chosen such that the conditions are satisfied, allows successful decoding at both receivers for all channel gains except for an outage set $B \subset (1,2]^{2\times 3}$ *of Lebesgue measure* $\mu(B) \leq \delta$.

Proof: The proof for Lemma 2.10 can be found in [NMA13] and the proof for Lemma 2.11 is in the same fashion but exploits the non-overlapping coding structure between $R_{k1}^{p1}, \max\{R_{l1}^{c}, R_{l2}^{c}\}$ and R_{11}^{p2} in the weak interference case, see Appendix 2.10.3. A similar method is used in Section 2.7, where the Gaussian equivalent of this modification is used. ■

The last two lemmas tell us that for all rates which obey the stated conditions, the spanned subspaces are independent except for a small set of measure $\mu(B) \leq \delta$. This means that there exists a unique solution and the signals can be decoded. Hence, any proposed scheme needs to be checked if it obeys these conditions and therefore allows for successful decoding. The conditions of the following schemes are checked in the appendix. It then remains to show that the proposed schemes achieve the rates in the theorem.

We have to choose different schemes for the cases

$$\begin{aligned} \text{I}: \ \alpha \in [0, \tfrac{1}{2}], \ \text{II}: \ \alpha \in (\tfrac{1}{2}, \tfrac{3}{5}), \ \text{III}: \ \alpha \in [\tfrac{3}{5}, 1] \\ \text{IV}: \ \alpha \in (1, \tfrac{3}{2}], \ \text{V}: \ \alpha \in (\tfrac{3}{2}, \infty). \end{aligned}$$

We indicated the common and private signal parts with the superscript c and p respectively. We therefore have that $\bar{\mathbf{x}} = [\bar{\mathbf{x}}^c; \bar{\mathbf{x}}^p]$.

The private parts of the signal can be used to communicate solely to the intended receiver, without affecting the other cell. We dedicate the R_{ik}^{c} most significant bits, and the $R_{i1}^{p_1}$ least significant bits of $\bar{\mathbf{x}}_{i1}$ to carry information. For the weak interference cases $\alpha < \frac{1}{2}$, the private part of $\bar{\mathbf{x}}$ has another bit-level allocation. There we dedicate the $R_{i1}^{p_2}$ most significant bits of the private part $\bar{\mathbf{x}}^p$ to carry information, see Figure 2.9. We now have to choose the scheme, and therefore how many bit-levels we give to each of the allocation rates, which we just introduced. We start with the weak interference case.

Case I: ($0 \leq \alpha \leq \frac{1}{2}$): We use the fact, that the model can be split into two sub-models, similar to the LD-Model (see Figure 2.4). This means that scheme differences for the bit-levels above the interference-level of one cell, do not influence the other cell. Hence, we can consider them separately and without loss of generality restrict the case analysis to symmetric cases. However, this is only possible for the weak interference model, which is why we consider the symmetrical model for higher interference regimes. For $k, l \in \{1, 2\}$

and $k \neq l$ we set

$$R_{k1}^{c} := \left\lfloor \tfrac{1}{2} n_k^l \right\rfloor, R_{k2}^{c} := \min\{ \left\lceil \tfrac{1}{2} n_k^l \right\rceil, (n_{k2}^k - (n_{k1}^k - n_k^l))^+ \}$$
$$R_{k1}^{p1} := \left\lfloor \tfrac{1}{2} n_l^k \right\rfloor, R_{k1}^{p2} := n_{k1}^k - n_k^l - n_l^k.$$

Multiuser gain in the IMAC model is dependent of the strength of the second user in each cell. This is also true in the weak interference case, where we differentiate between three sub-cases (of nine in total), dependent on n_{k2}^k.
Case I.1: The first sub-case is when $n_{k2}^k \leq n_{k1}^k - n_k^l$. In this case, the second user is useless for the channel, since the private rate $R_{i1}^{p_2}$ of user 1 can serve the same purpose. There is no multi-user gain in this regime and the achievable rate is limited to the IC sum rate.

$$\begin{aligned} R_\Sigma &= R_{11}^c + R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + R_{21}^c + R_{21}^{p1} + R_{21}^{p2} + R_{22}^c \\ &= 2 \left\lfloor \tfrac{1}{2} n_1^2 \right\rfloor + 2 \left\lfloor \tfrac{1}{2} n_2^1 \right\rfloor + n_{11}^1 + n_{21}^2 - 2n_1^2 - 2n_2^1 \\ &\geq (n_{11}^1 - n_1^2) + (n_{21}^2 - n_2^1) - 4. \end{aligned}$$

We remark that the achievable rate for one cell and this scheme is $(n_{k1}^k - \frac{1}{2} n_k^l - \frac{1}{2} n_l^k)$. This might be against the intuition from the IC model, where it is $((n_{k1}^k - n_l^k)$ resulting from a scheme similar to treating interference as noise. However, considering the sum rate of both cells in our scheme, we get back to the IC-rate. The following cases, where the second user of one or both cells is stronger, results in an *additional* rate part on top of the IC sum-rate. In the symmetrical case, we see that the conditions lead to a minimum of $R_{\text{ach},4}$ in Lemma 2.8, which can be reached by the allocation.
Case I.2: The second sub-case is when $n_{k1}^k - n_k^l < n_{k2}^k \leq n_{k1}^k - \frac{1}{2} n_k^l$. In this range, the upper part of the second user becomes useful as the top bit-level reaches above the part $R_{i1}^{p_2}$, and makes bit-level alignment possible. This part has a rising multiuser gain and is no longer limited to the IC sum rate.

$$\begin{aligned} R_\Sigma &= R_{11}^c + R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + R_{21}^c + R_{21}^{p1} + R_{21}^{p2} + R_{22}^c \\ &= 2 \left\lfloor \tfrac{1}{2} n_1^2 \right\rfloor + 2 \left\lfloor \tfrac{1}{2} n_2^1 \right\rfloor + n_{11}^1 + n_{21}^2 - 2n_1^2 - 2n_2^1 \\ &\quad + (n_{12}^1 - (n_{11}^1 - n_1^2)) + (n_{22}^2 - (n_{21}^2 - n_2^1)) \\ &\geq n_{22}^2 + n_{12}^1 - 4 \end{aligned}$$

The $n_{k2}^k - (n_{k1}^k - n_k^l)$ terms represent the additional rate of the second user and thus the multiuser gain. We achieve the active bound $R_{ach,4}$ in the symmetrical setting.
Case I.3: The last sub-case is for $n_{k1}^k - \frac{1}{2} n_k^l < n_{k2}^k \leq n_{k1}^k$, here the second user can be fully utilized to provide one half of the interference strength at the opposite cell. The multiuser

gain becomes half of the interference and the achievable sum rate reaches the main upper bound.

$$\begin{aligned}
R_\Sigma &= R_{11}^c + R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + R_{21}^c + R_{21}^{p1} + R_{21}^{p2} + R_{22}^c \\
&= 2\left\lfloor \tfrac{1}{2} n_1^2 \right\rfloor + 2\left\lfloor \tfrac{1}{2} n_2^1 \right\rfloor + n_{11}^1 + n_{21}^2 - 2n_1^2 - 2n_2^1 + \tfrac{1}{2}\left(\left\lceil n_1^2 \right\rceil + \left\lceil n_2^1 \right\rceil\right) \\
&= n_{11}^1 + n_{21}^2 - \left\lceil \tfrac{1}{2} n_1^2 \right\rceil - \left\lceil \tfrac{1}{2} n_2^1 \right\rceil \\
&\geq (n_{11}^1 - \tfrac{1}{2} n_1^2) + (n_{21}^2 - \tfrac{1}{2} n_2^1) - 2.
\end{aligned}$$

Here we see that the multiuser gain is $\frac{1}{2} n_k^l$ for cell k. Intuitively this means, that we can use the aligned part as additional rate. The combination of the cell rates (I.1:) $n_{11}^1 - n_1^2$, (I.2:) n_{k2}^k, (I.3:) $n_{11}^1 - \frac{1}{2} n_1^2$ leads to nine different cases. If a cell satisfies condition (I.1:) $n_{k2}^k \leq n_{k1}^k - n_k^l$, the $n_{k1}^k - n_k^l$ terms in the max of (2.19)-(2.18h) are active. Furthermore the max terms are smaller than $n_{k1}^k - n_k^l$ and the bound is reached. For condition (I.2:) $n_{k1}^k - n_k^l < n_{k2}^k \leq n_{k1}^k - \frac{1}{2} n_k^l$ yields activation of n_{k2}^k inside the max terms, and on the other hand, n_{k2}^k is weaker than $n_{k1}^k - \frac{1}{2} n_k^l$ proving the remaining bounds. The decoding conditions of lemma 2.11 are checked in the appendix. Considering a bit-gap of at most $2\log(16/\delta)$ from the decoding conditions and at most 4-bit from the use of fractional terms, results in a total gap of at most $2\log(c/\delta)$ with $c = 64$. This proves lemma 2.9. ■

We continue with the proof for lemma 2.8. From now on we confine the analysis to the symmetrical case, meaning that $n_{11}^1 = n_{21}^2 := n_1$, $n_{12}^1 = n_{22}^2 := n_2$, $n_1^2 = n_2^1 = n_i$. Sum rates for the weak interference case of the symmetric model are already shown as part of lemma 2.9, we therefore go on with the remaining regimes.

Case II ($\frac{1}{2} < \alpha < \frac{3}{5}$): For $k \in \{1, 2\}$ we set

$$\begin{aligned}
R_{k1}^c &:= \left\lfloor \tfrac{1}{2}(n_1 - n_i) \right\rfloor, \; R_{k2}^c := \min\{\left\lfloor \tfrac{1}{2}(n_1 - n_i) \right\rfloor, (n_2 - n_i)\} \\
R_{k1}^{p1} &:= n_i - \left\lfloor \tfrac{1}{2}(n_1 - n_i) \right\rfloor.
\end{aligned}$$

One can see the reason for this rate allocation scheme intuitively considering the interference at both cells. First of all, at $\alpha > \frac{1}{2}$, the interference is strong enough to "reach" into the common part of the signal $\bar{\mathbf{x}}_{k1}$ in cell k (see Fig. 2.10). Therefore, the additional private part bit allocation R_{k1}^{p2} of the weak interference case is zero and we can use the decoding lemma 2.10 from now on. Note that lemma 2.10, and therefore a bigger gap, is needed because of overlapping signal parts. Moreover, as a result of this new regime, the signal $\bar{\mathbf{x}}_{k2}$ in each cell k can support multiuser gain as long as $n_2 > n_i$. The previous rate allocation scheme ($\left\lfloor \frac{1}{2} n_i \right\rfloor$ for common parts) fails to satisfy the first equation of lemma 2.10, since there are less than n_i interference unaffected bit-levels for both users in a cell. The new allocation needs to fit into $(n_1 - n_i)$ bit-levels and an obvious choice is $\frac{1}{2}(n_1 - n_i)$. This way

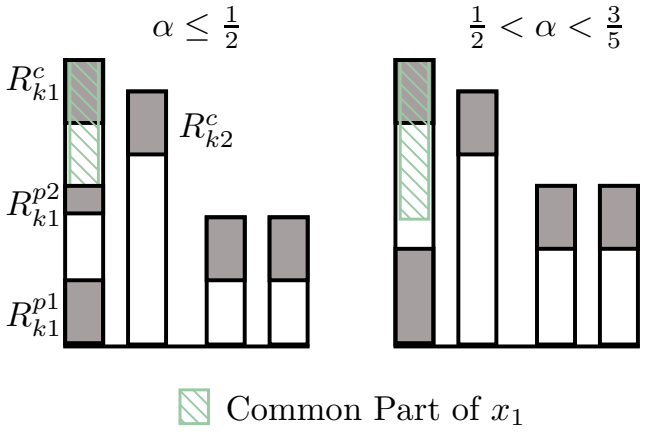

Figure 2.10.: Illustration of the scheme and rate allocations for the range $\frac{1}{2} < \alpha < \frac{3}{5}$ with $\alpha = \frac{4}{7}$ on the right hand side. The left hand side shows an illustration of the scheme in the previous regime. Both figures show the problem with the overlapping common part on the stronger signal.

we can use the whole bit-levels available and at the same time maximize the alignment at the other cell. The private part allocates the available rest, satisfying the third equation of lemma 2.10. See Figure 2.10 for an illustration. As in the weak interference case, we need to differentiate between sub-cases, depending on the strength of the signals $\bar{\mathbf{x}}_{k2}$.

Case II.1: The first sub-case is when $n_2 \geq n_i + \lfloor \frac{1}{2}(n_1 - n_i) \rfloor$. Therefore $\lfloor \frac{1}{2}(n_1 - n_i) \rfloor \leq (n_2 - n_i)$ and $R_{k2}^{c} := \lfloor \frac{1}{2}(n_1 - n_i) \rfloor$. The second direct signal has enough bit-levels to support the full multiuser gain. The sum-rate becomes

$$R_{\Sigma} = 4 \lfloor \tfrac{1}{2}(n_1 - n_i) \rfloor + 2(n_i - \lfloor \tfrac{1}{2}(n_1 - n_i) \rfloor) \geq n_1 + n_i - 2.$$

Regarding Lemma 2.8, the sub-case implies that $n_2 \geq n_i$ and it therefore follows from $n_i > (n_1 - n_i)$, that $n_2 > (n_1 - n_i)$. Moreover, one can see from $n_2 \geq n_i + \lfloor \frac{1}{2}(n_1 - n_i) \rfloor$ and $\alpha < \frac{3}{5}$, that $R_{\text{ach},1}$ gets activated and is the minimum of all bounds.

Case II.2: On the contrary, for $n_2 < n_i + \lfloor \frac{1}{2}(n_1 - n_i) \rfloor$, $R_{k2}^{c} := (n_2 - n_i)$ because the second direct signal cannot support the full previous rate allocation without violating the second decoding condition of lemma 2.10. The sum-rate is

$$R_{\Sigma} = 2(n_2 - n_i) + 2n_i = 2n_2.$$

And for $n_2 < n_i$ the IMAC collapses to the IC-model and yields the known $2n_i$ as sum rate. Note that $R_{ach,4}$ gets activated, and is also achieved, in the last two cases.

Case III ($\frac{3}{5} \leq \alpha \leq 1$): For case 3, we have the special situation, that the α-range needs to be subdivided to account for different sub-ranges. Still, due to the full multi-user gain

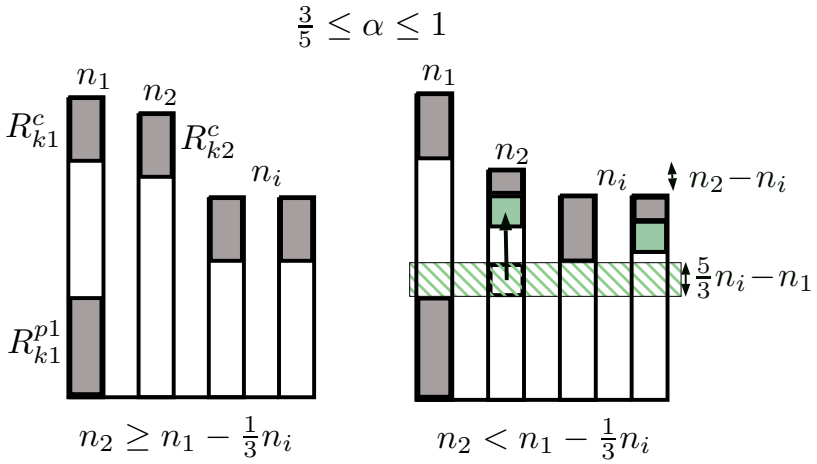

Figure 2.11.: Illustration of the achievable scheme and rate allocations in the range $\frac{3}{5} \leq \alpha \leq 1$ with $\alpha = \frac{2}{3}$. The left hand side shows the rate allocation for the case $n_2 \geq n_1 - \frac{1}{3}n_i$, while the right hand side shows the case $n_2 < n_1 - \frac{1}{3}n_i$.

sum-rate being the same over the whole range $\frac{3}{5} \leq \alpha \leq 1$ justifies analysing those as part of one case, see fig. 2.12.

Case III.A ($\frac{3}{5} \leq \alpha \leq \frac{2}{3}$): For $k \in \{1, 2\}$ we set

$$\begin{aligned} R_{k1}^c &:= \left\lfloor \tfrac{1}{3}n_i \right\rfloor, \\ R_{k2}^c &:= \min\{\left\lfloor \tfrac{1}{3}n_i \right\rfloor, \left\lfloor ((n_2 - n_i)^+ + \tfrac{5}{3}n_i - n_1) \right\rfloor\}, \\ R_{k1}^{p1} &:= n_1 - n_i. \end{aligned}$$

The change of the previous rate allocation is necessary because the common part drops in the range where we allocated the private part in the previous case. Therefore, the allocation of the private part needs to be changed accordingly. Due to this change, we have n_i bit-levels to allocate two common part allocations plus the aligned interference of the other cell. Due to the symmetry, an obvious choice is to use $\frac{1}{3}n_i$ for every common part allocation to maximise bit-level usage without violating the constraints. This scheme ensures that condition 1 from lemma 2.10 holds. We need to make sure, that also condition 2 and 3 hold. Condition 3 holds independently of n_2 due to the scheme design. For condition 2 the user of $\bar{\mathbf{x}}_{k2}$ needs to be strong enough to support the allocation of $\frac{1}{3}n_i$ bit-levels and therefore $n_2 \geq n_1 - \frac{1}{3}n_i$, which is the condition for the sub-case III.A.1. For $n_1 - \frac{1}{3}n_i > n_2 > n_i$ we reach the sub-case III.A.2, where the signal $\bar{\mathbf{x}}_{k2}$ can support an allocation of $(n_2 - n_i)^+ + \frac{5}{3}n_i - n_1$ bit-levels. For $n_2 \leq n_i$ the scheme cannot support multi-user gain any more, the LTD-IMAC falls back to the LTD-IC and one strategy is to leave the weak user of signal $\bar{\mathbf{x}}_{k2}$ silent and use IC techniques. We, therefore, have two

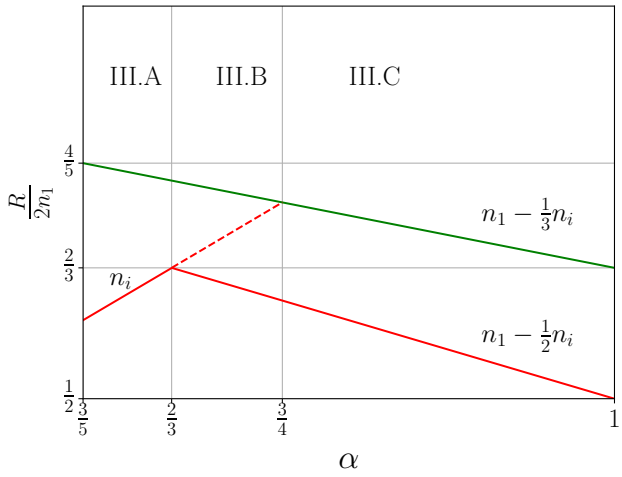

Figure 2.12.: Illustration of the full multi-user gain sum-rate (green) and the IC sum-rate (red) in the three α sub-ranges of case III. For varying strength of the weaker users signal $\bar{\mathbf{x}}_{k2}$ in each cell k, the achieved sum-rate can lie in between both curves.

sub-cases, where only for $n_2 \geq n_1 - \frac{1}{3}n_i$ (III.A.1) full multi-user gain can be achieved and at $n_2 = n_1 - \frac{1}{3}n_i$ is a transition to case III.A.2, which still yields multi-user gain as long as $n_2 > n_i$. We remark that as long as n_2 is larger than the private part $n_1 - n_i$, it can be used to achieve the same sum-rate as IC-techniques. For achieving n_i in the range $n_2 < n_i$, R_{k1}^c would need a larger allocation, which will be used in case III.B.

Sum Rate: The sum rate for the case III.A.1 is

$$R_\Sigma = 4\left\lfloor \tfrac{1}{3}n_i \right\rfloor + 2(n_1 - n_i) \geq 2n_1 - \tfrac{2}{3}n_i - 4,$$

where $R_{ach,2}$ is active and for the case III.A.2 ($n_2 > n_i$) it is

$$R_\Sigma = 2(\tfrac{1}{3}n_i + (n_1 - n_i) + ((n_2 - n_i)^+ + \tfrac{5}{3}n_i - n_1) - 2 \geq 2n_2 - 2,$$

where the rate term $R_{ach,4}$ is active.

Case III.B ($\frac{2}{3} < \alpha \leq \frac{3}{4}$): For $k \in \{1, 2\}$ we set

$$\begin{aligned}
R_{k1}^c &:= \left\lfloor \tfrac{1}{3}n_i \right\rfloor + \min\{\left\lfloor (\tfrac{2}{3}n_i - n_2)^+ \right\rfloor, \left\lfloor (n_1 - \tfrac{4}{3}n_i)^+ + \tfrac{1}{2}(2n_i - n_2 - n_1)^+ \right\rfloor\}, \\
R_{k2}^c &:= \min\{\left\lfloor \tfrac{1}{3}n_i \right\rfloor, \left\lfloor ((n_2 - n_i)^+ + (\tfrac{5}{3}n_i - n_1)^+) \right\rfloor, (n_2 - (n_1 - n_i))^+\}, \\
R_{k1}^{p1} &:= n_1 - n_i.
\end{aligned}$$

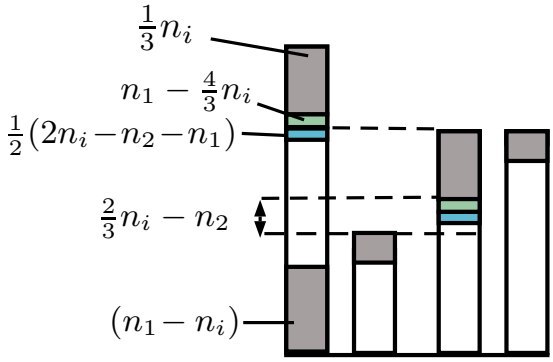

Figure 2.13.: Illustration of the scheme for case III.B.4. The goal is to allocate as many as possible bits of $\bar{\mathbf{x}}_{k1}$, to fill the free (allocatable) space $\frac{2}{3}n_i - n_2$ between the interference and R^c_{k2}, R^{p1}_{k1}. The obvious action is to allocate more bit-levels at $\bar{\mathbf{x}}_{k1}$, however, there are just $n_1 - \frac{4}{3}n_i$ freely allocatable (i.e. which do not overlap with other signals) bits. The remaining $2n_i - n_2 - n_1$ bits overlap with the aligned interference and one can allocate only half of the available bit-levels in order to stay within decoding conditions.

As in case III.A, only for $n_2 \geq n_1 - \frac{1}{3}n_i$ (III.B.1) full multi-user gain can be achieved and at $n_2 = n_1 - \frac{1}{3}n_i$ is a transition to case III.B.2. However, due to the fact that n_i gets bigger than $n_1 - \frac{1}{2}n_i$ for $\alpha > \frac{2}{3}$ (see fig. 2.12), the scheme still yields multi-user gain as long as $n_2 > n_1 - n_i$. This means that we still have multi-user gain as long as the signal bit vector $\bar{\mathbf{x}}_{k2}$ is larger than the private part of $\bar{\mathbf{x}}_{k1}$. We, therefore, have two additional sub-cases for $n_1 - n_i < n_2 < n_i$. The first sub-case III.B.3 is for $\frac{2}{3}n_i \leq n_2 < n_i$, where we use the same strategy as in III.B.2, but can only support a free allocation below n_i at $\bar{\mathbf{x}}_{k2}$. This means that the part $(n_2 - n_i)^+$ will be zero, resulting in a sum-rate of $2n_i$ instead of $2n_2$. The second sub-case III.B.4 is in the range $n_1 - n_i < n_2 < \frac{2}{3}n_i$. For this sub-case, the signal $\bar{\mathbf{x}}_{k2}$ cannot support the $\frac{5}{3}n_i - n_1$ bit-level allocation anymore. The allocation $n_2 - (n_1 - n_i)$ gets active, which uses a maximum of bit-levels without overlapping with the private part of $\bar{\mathbf{x}}_{k1}$. The low number of bit levels of $\bar{\mathbf{x}}_{k2}$ results in a gap of $(\frac{2}{3}n_i - n_2)^+$ bits between the interference signal allocation and the bit allocations of R^c_{k2} and R^{p1}_{k1}. One therefore needs to allocate more bit levels at $\bar{\mathbf{x}}_{k1}$ to compensate. However, due to $\frac{3}{4} \geq \alpha > \frac{2}{3}$ we have that $n_1 - n_i < 2n_i - n_1 \leq \frac{2n_i}{3}$. Therefore, n_2 can fall into a range $(n_2 < 2n_i - n_1)$, where the missing bit-levels $(\frac{2}{3}n_i - n_2)^+$ are more than the freely allocatable space above n_i, which is $n_1 - \frac{4}{3}n_i$ bit-levels. Therefore, only $n_1 - \frac{4}{3}n_i$ bit-levels can be allocated without penalty, and another $\frac{1}{2}(2n_i - n_2 - n_1)^+$ for half of the remaining space (see fig. 2.13). Note that case III.B.3 and II.B.4 is in the range $n_2 < n_i$. One therefore needs to switch the signal $\bar{\mathbf{x}}_{k2}$ with the interfering signal in the decoding lemma, which yields the third condition that $R^c_{k2} + R^{p1}_{k1} \leq n_2$ and in condition 2, n_2 gets replaced with n_i.

Sum Rate: The sum rate for the case III.B.1 is

$$R_\Sigma = 4\left\lfloor \tfrac{1}{3}n_i \right\rfloor + 2(n_1 - n_i) \geq 2n_1 - \tfrac{2}{3}n_i - 4,$$

where $R_{ach,2}$ is active. For the case III.B.2 and $n_2 \geq n_i$ the sum rate is

$$R_\Sigma = 2(\tfrac{1}{3}n_i + (n_1 - n_i) + ((n_2 - n_i)^+ + \tfrac{5}{3}n_i - n_1) - 2 \geq 2n_2 - 2,$$

and for $\frac{2}{3}n_i \leq n_2 < n_i$ (case III.B.3) it is

$$R_\Sigma = 2(\tfrac{1}{3}n_i + (n_1 - n_i) + (\tfrac{5}{3}n_i - n_1)) - 2 \geq 2n_i - 2,$$

where the term $R_{ach,4}$ is active in the last two cases.

For case III.B.4 $(n_1 - n_i) < n_2 < \frac{2}{3}n_i$,

as long as $n_2 > 2n_i - n_1$ we have that $R^c_{k1} = \left\lfloor \frac{1}{3}n_i \right\rfloor + \left\lfloor (\frac{2}{3}n_i - n_2)^+ \right\rfloor$, while $R^c_{k2} = (n_2 - (n_1 - n_i))^+$ and the sum rate is $2n_i - 2$. If $n_2 \leq 2n_i - n_1$, the allocation of R^c_{k1} changes and the sum rate becomes

$$\begin{aligned} R_\Sigma = 2(&\tfrac{1}{3}n_i + \left\lfloor (n_1 - \tfrac{4}{3}n_i) + \tfrac{1}{2}(2n_i - n_2 - n_1) \right\rfloor \\ &+ (n_1 - n_i) + (n_2 - (n_1 - n_i))^+ - 2 \geq n_2 + n_1 - 2, \end{aligned}$$

where the rate term $R_{ach,5}$ gets active.

Case III.C ($\frac{3}{4} \leq \alpha \leq 1$): For $k \in \{1, 2\}$ we set

$$\begin{aligned} R^c_{k1} &:= \left\lfloor \tfrac{1}{3}n_i \right\rfloor + \left\lfloor \tfrac{1}{2}\left[\tfrac{1}{3}n_i - (n_2 - (n_1 - n_i))^+ \right]^+ \right\rfloor, \\ R^c_{k2} &:= \min\{ \left\lfloor \tfrac{1}{3}n_i \right\rfloor, (n_2 - (n_1 - n_i))^+ \}, \\ R^{p1}_{k1} &:= n_1 - n_i. \end{aligned}$$

For $\alpha \geq \frac{3}{4}$ we have $n_1 - \frac{1}{3}n_i \leq n_i$ which means that R^c_{k1} drops below interference level and therefore overlaps with R^c_{l1} and R^c_{l2}, the aligned interference signals of the other cell. Additionally, more than $\frac{1}{3}n_i$ free bit-levels are available between the private part R^{p1}_{k1} and the aligned interference (R^c_{l1} and R^c_{l2}). This means, that full multi-user gain can be supported even if $n_2 < n_1 - \frac{1}{3}n_i$ for as long as $n_2 \geq n_1 - \frac{2}{3}n_i$ (III.C.1). If $n_2 < n_1 - \frac{2}{3}n_i$, $\bar{\mathbf{x}}_{k2}$ is not strong enough to support full multi-user gain, and the allocation $R^c_{k2} := n_2 - (n_1 - n_i)$ gets active, resulting in case III.C.2. As in the previous sub-case III.B, $\bar{\mathbf{x}}_{k1}$ gets active and can allocate half of the available difference of $(n_1 - n_i) + \frac{1}{3}n_i - n_2$ bit-levels. Note that one cannot use all of the bit-levels between n_2 and $n_i - \frac{1}{3}n_i$ which are $\frac{2}{3}n_i - n_2$, because it would violate decoding condition 1 for $\alpha > \frac{3}{4}$. As in the previous case, the decoding

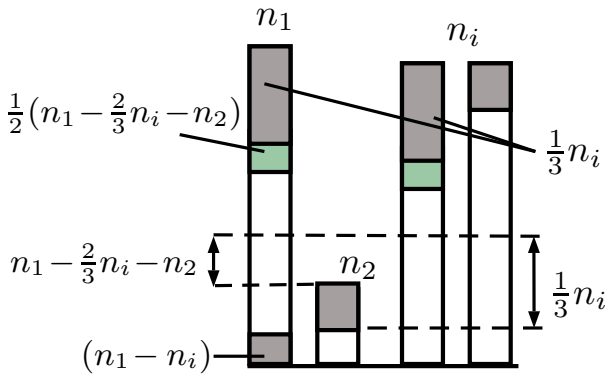

Figure 2.14.: Illustration of the scheme for the case III.C.2. In this case, n_2 is too weak to support the full $\frac{n_i}{3}$ bit-levels. It can support a maximum of $n_2-(n_1-n_i)$ bit-levels. The remaining free $n_1-\frac{2n_i}{3}-n_2$ bit-levels can be added at $\bar{\mathbf{x}}_{k1}$. However, since every additional bit generates additional interference (both green parts), we can only allocate half of the remaining bits to stay within decoding conditions.

lemma needs to be adjusted for $n_2 < n_i$. There is multi-user gain in this case, as long as $n_2 > n_1 - n_i$, below the LTD-IMAC falls back to the LTD-IC.

Sum Rate: The sum rate for the case III.C.1 is

$$R_\Sigma = 4\left\lfloor \tfrac{1}{3}n_i \right\rfloor + 2(n_1-n_i) \geq 2n_1 - \tfrac{2}{3}n_i - 4,$$

where $R_{ach,2}$ is active. For the case III.C.2

$$\begin{aligned} R_\Sigma &= 2(\tfrac{1}{3}n_i + (n_1-n_i) + (n_2-(n_1-n_i))^+ + \tfrac{1}{2}(\tfrac{1}{3}n_i - (n_2-(n_1-n_i))^+) - 2 \\ &\geq n_2 + n_1 - 2, \end{aligned}$$

the scheme reaches $R_{ach,5}$.

Case IV ($1 < \alpha < \frac{3}{2}$): For the range $\alpha > 1$ the decoding lemma needs to be adjusted. A simple reassignment of the corresponding rates solves this problem. We can set

$$R_{k1}^c := \left\lfloor \tfrac{1}{3}n_i \right\rfloor + \left\lfloor \tfrac{1}{2}(\tfrac{1}{3}n_i - n_2)^+ \right\rfloor, R_{k2}^c := \min\{\left\lfloor \tfrac{1}{3}n_i \right\rfloor, n_2\}.$$

Since the interfering signal is stronger than both users, the private part of $\bar{\mathbf{x}}_{k1}$ vanishes completely. We have to analyse two sub-cases: Case IV.1: This sub-case is in the range $n_2 \geq \left\lfloor \frac{1}{3}n_i \right\rfloor$. Here, $R_{k2}^c := \left\lfloor \frac{1}{3}n_i \right\rfloor$, and the multi-user gain can be completely supported by the weaker users signal $\bar{\mathbf{x}}_{k2}$. Case IV.2: For $n_2 < \left\lfloor \frac{1}{3}n_i \right\rfloor$, the multi-user gain cannot be fully supported. We have $R_{k2}^c := n_2$ and for $n_2 = 0$, the channel falls back to the IC sum-rate.

Sum Rate: The sum rate for the cases IV.1 and IV.2 is $R_\Sigma \geq \frac{4}{3}n_i - 4$ and $R_\Sigma \geq n_i + n_2 - 2$, respectively. In case IV.1, $R_{ach,2}$ is active, and for case IV.2, $R_{ach,5}$ is active.

Case V ($\frac{3}{2} \leq \alpha < \infty$): At $\alpha = \frac{3}{2}$, we have that $n_1 = \frac{2}{3}n_i$ and therefore reached the maximum allocatable rate point which satisfies all decoding conditions with the previous rate allocation. Since n_i keeps growing, the strategy is to use half of n_1 as allocation and we set

$$R_{k1}^c := \max\{\left\lfloor \tfrac{1}{2}n_1 \right\rfloor, \left\lfloor \tfrac{1}{2}n_i - \tfrac{1}{2}n_2 \right\rfloor, n_1 - n_2\},$$
$$R_{k2}^c := \min\{\left\lfloor \tfrac{1}{2}n_1 \right\rfloor, n_2\}.$$

Once again, multi-user gain is dependent on the strength of n_2. For $n_2 \geq \left\lfloor \frac{1}{2}n_1 \right\rfloor$ (case V.I), the second user can fully support the gain but for $n_2 < \left\lfloor \frac{1}{2}n_1 \right\rfloor$ just $R_{k2}^c := n_2$. For this case, we have $R_{k1}^c := n_1 - n_2$ as long as $2n_1 < n_i + n_2$ and get the full sum-rate. Otherwise, full multi-user gain cannot be supported and we have $R_{k1}^c := \left\lfloor \frac{1}{2}n_i - \frac{1}{2}n_2 \right\rfloor$ and reach the case V.2.

Sum Rate: The sum rate for the cases V.1 and V.2 is $R_\Sigma \geq 2n_1 - 4$ and $R_\Sigma \geq n_i + n_2 - 2$, respectively.

As in [NMA13], we have ignored the $\log(32/\delta)$ terms from the decoding lemma, and add a reduction in the overall sum-rate of $2\log(32/\delta)$. Together with a bit-gap of at most 4, we get the overall gap $2\log(128/\delta)$. □

2.6.2. Upper Bounds

Theorem 2.12. *The sum rate for the symmetric LTD-IMAC system model can be bounded from above by*

$$R_\Sigma \leq \min\{D_1, D_2, D_3, D_4, D_5\}$$

with

$$D_1 := 2\max((n_1 - n_i)^+, n_i) + \min((n_1 - n_i)^+, n_i), \tag{2.18j}$$
$$D_2 := \tfrac{2}{3}(2\max(n_1, n_i) + (n_1 - n_i)^+), \tag{2.18k}$$
$$D_3 := 2n_1, \tag{2.18l}$$
$$D_4 := \max(2n_2, 2(n_1 - n_i)^+, 2n_i), \tag{2.18m}$$
$$D_5 := \max(n_1, n_i) + \max(n_2, (n_1 - n_i)^+). \tag{2.18n}$$

Proof. Considering Fano's inequality and the Data Processing inequality one can establish the following bounds:

$$\begin{aligned}
&n(R_{11}^1 + R_{21}^1 + R_{21}^2 + R_{22}^2) \\
&\leq I(\mathbf{x}_{11}^n, \mathbf{x}_{12}^n; (\mathbf{y}^1)^n) + I(\mathbf{x}_{21}^n, \mathbf{x}_{22}^n; (\mathbf{y}^2)^n) + n(\epsilon_{n,12} + \epsilon_{n,34}) \\
&= H((\mathbf{y}^1)^n) - H((\mathbf{y}^1)^n | \mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + H((\mathbf{y}^2)^n) \\
&\quad - H((\mathbf{y}^2)^n | \mathbf{x}_{21}^n, \mathbf{x}_{22}^n) + n(\epsilon_{n,12} + \epsilon_{n,34}).
\end{aligned}$$

We denote $(\mathbf{y}^j)^{n,\uparrow} := (\mathbf{y}^j)_{[\eta+1:n_1]}^n$ and $(\mathbf{y}^j)^{n,\downarrow} := (\mathbf{y}^j)_{[1:\eta]}^n$ with $\eta := \max((n_1 - n_i)^+, n_i)$ and show that

$$\begin{aligned}
&2n(R_\Sigma - \epsilon_{n,\Sigma}) \\
&\leq 2H((\mathbf{y}^1)^n) - 2H((\mathbf{y}^1)^n | \mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + 2H(\mathbf{y}_{12}^n) - 2H((\mathbf{y}^2)^n | \mathbf{x}_{21}^n, \mathbf{x}_{22}^n) \\
&\leq 2H((\mathbf{y}^1)^{n,\downarrow}) + 2H((\mathbf{y}^1)^{n,\uparrow}) - 2H(\mathbf{H}_2^1((\bar{\mathbf{x}}_{21}^c)^n \oplus (\bar{\mathbf{x}}_{22}^c)^n)) \\
&\quad + 2H((\mathbf{y}^2)^{n,\downarrow}) + 2H((\mathbf{y}^2)^{n,\uparrow}) - 2H(\mathbf{H}_1^2((\bar{\mathbf{x}}_{11}^c)^n \oplus (\bar{\mathbf{x}}_{12}^c)^n)) \\
&\overset{(a)}{\leq} 4n \max((n_1 - n_i)^+, n_i) + H((\mathbf{y}^1)^{n,\uparrow}) + H((\mathbf{y}^2)^{n,\uparrow}) \\
&\leq 4n \max((n_1 - n_i)^+, n_i) + 2n \min((n_1 - n_i)^+, n_i)
\end{aligned}$$

where (a) follows from $H((\mathbf{y}^j)^{n,\downarrow}) \leq n\eta$ and

$$\begin{aligned}
&H((\mathbf{y}^1)^{n,\uparrow}) - 2H(\mathbf{H}_1^2((\bar{\mathbf{x}}_{11}^c)^n \oplus (\bar{\mathbf{x}}_{12}^c)^n)) \\
&\leq H((\mathbf{y}^1)^{n,\uparrow}) - H(\mathbf{H}_1^2((\bar{\mathbf{x}}_{11}^c)^n \oplus (\bar{\mathbf{x}}_{12}^c)^n) | (\bar{\mathbf{x}}_{11}^c)^n) - H(\mathbf{H}_1^2((\bar{\mathbf{x}}_{11}^c)^n \oplus (\bar{\mathbf{x}}_{12}^c)^n) | (\bar{\mathbf{x}}_{12}^c)^n) \\
&= H((\mathbf{y}^1)^{n,\uparrow}) - H((\bar{\mathbf{x}}_{11}^c)^n) - H((\bar{\mathbf{x}}_{12}^c)^n) \\
&\leq 0.
\end{aligned}$$

Here we used in the second last step, that the $\mathbf{H}$ matrices are lower uni-triangular matrices. This means that they are invertible, hence are bijective mappings. By symmetry is also holds that

$$H((\mathbf{y}^2)^{n,\uparrow}) - 2H(\mathbf{H}_2^1((\bar{\mathbf{x}}_{21}^c)^n \oplus (\bar{\mathbf{x}}_{22}^c)^n)) \leq 0.$$

Dividing both sides by $2n$ and taking $n \to \infty$ yields the upper bound (2.18j).

We now establish the bound (2.18k). Therefore we show that

$$\begin{aligned}
&3n(R_{11}^1 + R_{21}^1 + R_{21}^2 + R_{22}^2 - \epsilon) \\
&\leq 3I(\mathbf{x}_{11}^n, \mathbf{x}_{12}^n; (\mathbf{y}^1)^n) + 3I(\mathbf{x}_{21}^n, \mathbf{x}_{22}^n; (\mathbf{y}^2)^n) \\
&\leq 2H((\mathbf{y}^1)^n) - 2H((\mathbf{y}^1)^n | \mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + 2H((\mathbf{y}^2)^n)
\end{aligned}$$

$$
\begin{aligned}
&\quad - 2H((\mathbf{y}^2)^n|\mathbf{x}_{21}^n, \mathbf{x}_{22}^n) + H(\bar{\mathbf{x}}_{11}^n \oplus \bar{\mathbf{x}}_{12}^n) + H(\bar{\mathbf{x}}_{21}^n \oplus \bar{\mathbf{x}}_{22}^n). \\
&\leq 2H((\mathbf{y}^1)^n) + 2H((\mathbf{y}^2)^n) + 2n(n_1 - n_i)^+
\end{aligned}
$$

with

$$
\begin{aligned}
&H(\bar{\mathbf{x}}_{i1}^n \oplus \bar{\mathbf{x}}_{i2}^n) - 2H(\mathbf{H}_i^{i^c}((\bar{\mathbf{x}}_{i1}^c)^n \oplus (\bar{\mathbf{x}}_{i2}^c)^n)) \\
&\leq H(\bar{\mathbf{x}}_{i1}^n \oplus \bar{\mathbf{x}}_{i2}^n) - H(\mathbf{H}_i^{i^c}((\bar{\mathbf{x}}_{i1}^c)^n \oplus (\bar{\mathbf{x}}_{i2}^c)^n)|(\bar{\mathbf{x}}_{i1}^c)^n) - H(\mathbf{H}_i^{i^c}((\bar{\mathbf{x}}_{i1}^c)^n \oplus (\bar{\mathbf{x}}_{i2}^c)^n)|(\bar{\mathbf{x}}_{i2}^c)^n) \\
&= H(\bar{\mathbf{x}}_{i1}^n \oplus \bar{\mathbf{x}}_{i2}^n) - H((\bar{\mathbf{x}}_{i1}^c)^n) - H((\bar{\mathbf{x}}_{i2}^c)^n) \\
&\leq H((\bar{\mathbf{x}}_{i1}^n \oplus \bar{\mathbf{x}}_{i2}^n)_{[1:(n_1-n_i)^+]}) \\
&\leq n(n_1 - n_i)^+
\end{aligned}
$$

for $i \in \{1, 2\}$ in all[5] $\bar{\mathbf{x}}_{i1}^n$ and $\bar{\mathbf{x}}_{i2}^n$ and therefore

$$
\begin{aligned}
&n(R_\Sigma - \epsilon) \\
&\leq \tfrac{2n}{3}(2\max(n_1, n_i) + (n_1 - n_i)^+),
\end{aligned}
$$

which shows the upper bound (2.18k) for $n \to \infty$. We now establish the bound (2.18l). We can show that

$$
\begin{aligned}
&n(R_{11}^1 + R_{21}^1 + R_{21}^2 + R_{22}^2 - \epsilon) \\
&\leq I(\mathbf{x}_{11}^n, \mathbf{x}_{12}^n; (\mathbf{y}^1)^n, \mathbf{x}_{21}^n, \mathbf{x}_{22}^n) + I(\mathbf{x}_{21}^n, \mathbf{x}_{22}^n; (\mathbf{y}^2)^n, \mathbf{x}_{11}^n, \mathbf{x}_{12}^n) \\
&= I(\mathbf{x}_{11}^n, \mathbf{x}_{12}^n; (\mathbf{y}^1)^n|\mathbf{x}_{21}^n, \mathbf{x}_{22}^n) + I(\mathbf{x}_{21}^n, \mathbf{x}_{22}^n; (\mathbf{y}^2)^n|\mathbf{x}_{11}^n, \mathbf{x}_{12}^n) \\
&= H((\mathbf{y}^1)^n|\mathbf{x}_{21}^n, \mathbf{x}_{22}^n) + H((\mathbf{y}^2)^n|\mathbf{x}_{11}^n, \mathbf{x}_{12}^n) \\
&\leq 2nn_1.
\end{aligned}
$$

Dividing by n shows the upper bound (2.18l) for $n \to \infty$. Now, we show the upper bound (2.18m). One can show that:

$$
\begin{aligned}
&n(R_{11}^1 + R_{21}^1 + R_{21}^2 + R_{22}^2 - \epsilon_{n,\Sigma}) \\
&\leq H((\mathbf{y}^1)^n) - H((\mathbf{y}^1)^n|\mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + H((\mathbf{y}^2)^n) - H((\mathbf{y}^2)^n|\mathbf{x}_{21}^n, \mathbf{x}_{22}^n) \\
&= H((\mathbf{y}^1)^n) - H(\mathbf{H}_2^1((\bar{\mathbf{x}}_{21}^c)^n \oplus (\bar{\mathbf{x}}_{22}^c)^n)) + H((\mathbf{y}^2)^n) - H(\mathbf{H}_1^2((\bar{\mathbf{x}}_{11}^c)^n \oplus (\bar{\mathbf{x}}_{12}^c)^n)) \\
&\leq H((\mathbf{y}^1)^n) - H(\mathbf{H}_2^1(\bar{\mathbf{x}}_{21}^c)^n) + H((\mathbf{y}^2)^n) - H(\mathbf{H}_1^2(\bar{\mathbf{x}}_{11}^c)^n) \\
&\leq 2n\max(n_2, (n_1 - n_i)^+, n_i)
\end{aligned}
$$

[5] Note that the index i at the signals identifies the MAC-cell and has nothing to do with the i at n_i which stands for *interference*.

Dividing by n and letting $n \to \infty$ shows the bound (2.18m).

We now establish the bound (2.18n). We can show that

$$\begin{aligned}
&n(R_\Sigma - \epsilon_{n,\Sigma}) \\
&\leq H((\mathbf{y}^1)^n) - H((\mathbf{y}^1)^n|\mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + H((\mathbf{y}^2)^n) - H((\mathbf{y}^2)^n|\mathbf{x}_{21}^n, \mathbf{x}_{22}^n) \\
&\leq H((\mathbf{y}^1)^n) - H((\mathbf{y}^1)^n|\mathbf{x}_{11}^n, \mathbf{x}_{12}^n, \mathbf{x}_{22}^n) + H((\mathbf{y}^2)^n) - H((\mathbf{y}^2)^n|\mathbf{x}_{21}^n, \mathbf{x}_{22}^n) \\
&\leq H((\mathbf{y}^1)^n) - H(\bar{\mathbf{x}}_{21}^n) + H((\mathbf{y}^2)^n) - H(\bar{\mathbf{x}}_{11}^n \oplus \bar{\mathbf{x}}_{12}^n) \\
&\leq H((\mathbf{y}^1)^n) + n \max(n_2, (n_1 - n_i)^+) \\
&\leq n \max(n_1, n_i) + n \max(n_2, (n_1 - n_i)^+).
\end{aligned}$$

Dividing both sides by n and taking $n \to \infty$ yields the desired upper bound.

□

Corollary 2.13. *If the weaker user is strong enough to support full multi-user gain, the sum rate for the symmetric LTD-IMAC system model can be bounded from above by*

$$R_\Sigma \leq \begin{cases} 2(n_1 - \frac{1}{2}n_i) & \text{for } 0 \leq \alpha \leq \frac{1}{2} \\ 2(\frac{1}{2}n_1 + \frac{1}{2}n_i) & \text{for } \frac{1}{2} \leq \alpha \leq \frac{3}{5} \\ 2(n_1 - \frac{1}{3}n_i) & \text{for } \frac{3}{5} \leq \alpha \leq 1 \\ \frac{4}{3}n_i & \text{for } 1 \leq \alpha \leq \frac{3}{2} \\ 2n_1 & \text{for } \frac{3}{2} \leq \alpha \leq \infty. \end{cases}$$

Proof. Follows immediately from Theorem 2.6.2 by investigation of the active bounds in the corresponding regimes. □

Remark 2.14. The upper bounds for the weak interference asymmetric cases can be found in [FW15a]. Upper bounds for weak symmetric cases correspond to the specific achievable schemes. Since the model can be split in the weak interference regime, the symmetric upper bounds can be split and mixed as well and show the asymmetric bounds as well.

2.7. Transfer from LTD-IMAC to G-IMAC

2.7.1. Achievability for the G-IMAC

In this part, we prove the achievability for the Gaussian IMAC. We will show, that the lower-triangular scheme directly guides the constant-gap capacity achieving Gaussian scheme. The analysis is done in the same fashion as in [NMA13]. We assume perfect

knowledge of the channel gains h_{ik}^j. However, the same techniques as in [NMA13] can be applied to show, that a max n_{ik}^j-bit quantisation of h_{ik}^j is sufficient for the achievability. Remember that the input signals are constructed such that

$$x_{11} := h_{12}^2 u_{11} \tag{2.18o}$$

$$x_{12} := h_{11}^2 u_{12} \tag{2.18p}$$

$$x_{21} := h_{22}^1 u_{21} \tag{2.18q}$$

$$x_{22} := h_{21}^1 u_{22}. \tag{2.18r}$$

Observe, that this results in (2.5), where the new channel gains are $g_{ik}^j \in (1, 4]$. Due to this modulation, the first two bits of u_{ik} are set to zero i.e.,

$$u_{ik} := \sum_{j=3}^{n_{i1}} [u_{ik}]_j 2^{-j},$$

where $[u_{ik}]_j \in \{0, 1\}$ represents the bits of the binary expansion of u_{ik}. This ensures that $|u_{ik}| \leq \frac{1}{4}$ and therefore $|g_{ik}^j u_{ik}| \leq 1$. Moreover, the u_{ik}-inputs are chosen such that the corresponding $[u_{ik}]_j$-bits obey the design criteria of the LTD scheme in 2.6.1. In particular, the places where the binary vectors of the LTD model are forced to be zero, need to be zero in the Gaussian scheme as well. Therefore, the u_{i1}-inputs will be also decomposed into common and private signal parts i.e.,

$$u_{i1} = u_{i1}^P + u_{i1}^C.$$

Where the private part $u_{i1}^P := u_{i1}^{P_1} + u_{i1}^{P_2}$ is decomposed again into two parts for the weak interference regime i.e., $\frac{n_i}{n_1} \leq \frac{1}{2}$. In the following, we analyse the receiver one exemplary. By symmetry, all results for receiver one apply for receiver two as well. The channel equation for receiver one is

$$y^1 = g_{11}^1 2^{n_{11}^1} u_{11} + g_{12}^1 2^{n_{12}^1} u_{12} + g_2^1 2^{n_2^1} (u_{21}^C + u_{22}^C) + (g_2^1 2^{n_2^1} u_{21}^P + z^1). \tag{2.19}$$

Observe that the private part u_{21}^P of transmitter two is grouped with the Gaussian noise. The purpose of the private part is, that it is received below the noise floor of the unintended receiver. By the specific structure of the LTD scheme, the private part is given by

$$u_{i1}^P := \sum_{j=n_2^1+3}^{n_{i1}} [u_{i1}]_j 2^{-j},$$

where the two first bits are set to zero. Therefore we have $|2^{n_2^1}u_{21}^P| \leq \frac{1}{4}$ and $|g_2^1 2^{n_2^1}u_{21}^P| \leq 1$. It follows, that the last parts of the received signal $(g_2^1 2^{n_2^1}u_{21}^P + z^1)$ can be treated as noise. Moreover, one can see that the two interfering signals from receiver two u_{21}^C and u_{22}^C are received with the same channel gain and therefore align at receiver one. Once again following the notation of [NMA13], we can write the received signal parts above noise as

$$s_{11} := 2^{n_{11}^1}u_{11} \tag{2.19a}$$

$$s_{12} := 2^{n_{12}^1}u_{12} \tag{2.19b}$$

$$s_2^1 := 2^{n_2^1}(u_{21}^C + u_{22}^C). \tag{2.19c}$$

The decoder at receiver one tries to find estimates $\hat{s}_{11}$, $\hat{s}_{12}$, $\hat{s}_2^1$ for the received signal parts. Therefore, it is only interested in the sum of both interfering signals. The goal is to find the specific $\hat{s}_{11}$, $\hat{s}_{12}$, $\hat{s}_2^1$ which minimize the distance to the received signal, i.e.

$$|y_1 - g_{11}^1\hat{s}_{11} - g_{12}^1\hat{s}_{12} - g_2^1\hat{s}_2^1|.$$

An error can occur, if the distance between y_1 and any other triple $(\hat{s}_{11},\ \hat{s}_{12},\ \hat{s}_2^1)$ has a smaller distance than the noise. Therefore we need to investigate the minimum distance between the received signal parts and any other triple, which is

$$d := \min_{(s_{11},s_{12},s_2^1)\neq(\hat{s}_{11},\hat{s}_{12},\hat{s}_2^1)} |g_{11}^1(s_{11} - \hat{s}_{11}) - g_{12}^1(s_{12} - \hat{s}_{12}) - g_2^1(s_2^1 - \hat{s}_2^1)|.$$

Observe that the structure of the problem is exactly the same as in [NMA13, p. 4869], although the network model is different[6]. For the interference regime where $\alpha \geq \frac{1}{2}$, we can use a Lemma which was proved in [NMA13].

Lemma 2.15 ([NMA13, Lemma 9, (modified for the G-IMAC)]). *Let $\delta \in (0,1]$ and n_1, n_2, $n_i \in \mathbb{N}$, $n_1 \geq n_2$ and $\frac{n_i}{n_1} \geq \frac{1}{2}$. Assume R_{11}^P, R_{11}^C, R_{12}, R_{21}, R_{22}^P, $R_{22}^C \in \mathbb{Z}_+$ satisfy,*

$$\begin{aligned} R_{11}^C + R_{12}^C + R_{21}^C + R_{11}^P &\leq n_1 - \log\left(\tfrac{c}{\delta}\right) \\ R_{12}^C + R_{21}^C + R_{11}^P &\leq n_2 - \log\left(\tfrac{c}{\delta}\right) \\ R_{21}^C + R_{11}^P &\leq n_i - 6 \end{aligned}$$

and

$$\begin{aligned} R_{21}^C + R_{22}^C + R_{11}^C + R_{22}^P &\leq n_1 - \log\left(\tfrac{c}{\delta}\right) \\ R_{22}^C + R_{11}^C + R_{22}^P &\leq n_2 - \log\left(\tfrac{c}{\delta}\right) \end{aligned}$$

[6] In particular the coarse channel gain of the aligning signals, and therefore the form of s_2^1

$$R_{11}^C + R_{22}^P \leq n_i - 6$$

where $c := 13104$ *and* R_{ik} *is the rate of the signal* u_{ik}*. Then, the bit allocation of the LTD-IMAC applied to the Gaussian IMAC results in a minimum constellation distance* $d \geq 32$ *at each receiver for all channel gains (*$h_{mk} \in (1,2]^{2\times 2}$*) except for a set* $B \subset (1,2]^{2\times 2}$ *of Lebesgue measure* $\mu(B) \leq \delta$*.*

Since the structure of the conditions is the same as in the LTD-IMAC case (Lemma 2.10), we see that the G-IMAC can achieve the sum rate of Lemma 2.8 (with appropriate adjustment of the constants) with small probability of error. However, note that we cannot apply this Lemma to our weak interference case. This is due to the private part, which is composed of the two private signals $u_{11}^{P_1}, u_{11}^{P_2}$. We provide the proof for an adjusted Lemma in Appendix 2.10.4. Moreover, Lemma 2.15 only provides conditions for the decoding error to be small. As in [NMA13], it can be shown that an outer code over the modulated channel results in a vanishing error probability. Due to the structural similarities between the X-channel and the IMAC, all results in [NMA13] regarding vanishing error probability also apply for the IMAC. In particular, for an outer code with rate R'_{ik} and a modulation rate of R_{ik} it holds that

$$\begin{aligned} R'_{ik} &= I(u_{ik}; \hat{s}_{11}, \hat{s}_{12}, \hat{s}_2^1) \\ &= I(s_{ik}; \hat{s}_{11}, \hat{s}_{12}, \hat{s}_2^1) \\ &\geq R_{ik} - 1.5, \end{aligned} \tag{2.20}$$

which uses the bound

$$H(s_{11}, s_{12}, s_2^1 | \hat{s}_{11}, \hat{s}_{12}, \hat{s}_2^1) \leq 1.5,$$

proven in [NMA13], under usage of the conclusions of Lemma 2.15. This can be shown for each signal. The sum of the lower bounds then shows, that an outer code can achieve the previous sum rate with a vanishing error probability within a constant gap of six bits.

2.8. On The Difference between the LD Model and the LTD Model

Let us look at a specific example for both models. Assume we have a symmetrical channel, such that

$$\begin{aligned} n_{11}^1 = n_{21}^2 = n_1 = 11 \times \Delta \text{ bits} \\ n_{12}^1 = n_{22}^2 = n_2 = 10 \times \Delta \text{ bits} \end{aligned}$$

$$n_{21}^1 = n_{22}^1 = n_{11}^2 = n_{12}^2 = n_i = 5 \times \Delta \text{ bits.}$$

The parameters are $\alpha_1 = \alpha_2 = \frac{5}{11}$ and $\beta_1 = \beta_2 = \frac{10}{11}$. Figure 2.15 shows the achievable strategy for the LD model. We partition the common part of the signal in Δ-bit partitions such that we have maximal direct bit-rate while minimizing the aligning interference. This results in an achievable bit-rate of 8Δ (sum rate of 16Δ) bits using an orthogonal alignment scheme, where bit-levels are used independently. Let's assume the optimal input distribution in the IMAC setting is uniform. If $X \sim$ Unif[0,1] we have that the binary expansion $X = \sum_{n=1}^{\infty} x_n 2^{-n}$ yields i.i.d. Bern($\frac{1}{2}$) x_n. Which would mean that the bits of the binary received vector $\mathbf{y}$ are also i.i.d. Bern($\frac{1}{2}$). Hence, we could show the following converse bound

$$\begin{aligned} n(\sum R - \epsilon) &\leq I(\mathbf{x}_{11}^n, \mathbf{x}_{12}^n; \mathbf{y}_1^n) + I(\mathbf{x}_{21}^n, \mathbf{x}_{22}^n; \mathbf{y}_2^n) \\ &\leq H(\mathbf{y}_1^n) - H(\mathbf{y}_1^n | \mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + H(\mathbf{y}_2^n) - H(\mathbf{y}_2^n | \mathbf{x}_{21}^n, \mathbf{x}_{22}^n) \\ &\leq H(\mathbf{y}_1^{\uparrow,n}) + H(\mathbf{y}_1^{\downarrow,n}) - H(\mathbf{y}_1^n | \mathbf{x}_{11}^n, \mathbf{x}_{12}^n) + H(\mathbf{y}_2^{\uparrow,n}) + H(\mathbf{y}_2^{\downarrow,n}) - H(\mathbf{y}_2^n | \mathbf{x}_{21}^n, \mathbf{x}_{22}^n). \end{aligned}$$

Now we can upper bound $H(\mathbf{y}_1^{\downarrow,n})$ and $H(\mathbf{y}_2^{\downarrow,n})$ by $n6\Delta$ bits. Moreover, we can split

$$H(\mathbf{y}_1^{\uparrow,n}) - H(\mathbf{y}_2^n | \mathbf{x}_{21}^n, \mathbf{x}_{22}^n) = \sum_{\Delta} H(\mathbf{y}_{\Delta,1}^{\uparrow,n}) - H(\mathbf{y}_{\Delta,2} | \mathbf{x}_{21,\Delta}^n, \mathbf{x}_{22,\Delta}^n)$$

in Δ partitions, which is possible due to the bits of $\mathbf{y}$ being independent as assumed. Now one can condition the term $H(\mathbf{y}_{\Delta,2} | \mathbf{x}_{21,\Delta}^n, \mathbf{x}_{22,\Delta}^n)$ alternately on $\mathbf{x}_{11,\Delta}^n$ and $\mathbf{x}_{12,\Delta}^n$, starting with the latter, which results in

$$H(\mathbf{y}_1^{\uparrow,n}) - H(\mathbf{y}_2^n | \mathbf{x}_{21}^n, \mathbf{x}_{22}^n) \leq n2\Delta.$$

The same can be done with $H(\mathbf{y}_2^{\uparrow,n}) - H(\mathbf{y}_1^n | \mathbf{x}_{11}^n, \mathbf{x}_{12}^n)$ resulting in an overall bound of

$$R_\Sigma \leq 16\Delta \text{ bits.}$$

However, without any $\mathbf{y}$ distribution assumption we can get the bound of theorem 2.2

$$R_\Sigma \leq n_{11}^1 + n_{21}^2 - \frac{n_1^2}{2} - \frac{n_2^1}{2}$$

and therefore $R_\Sigma \leq 17\Delta$ bits. Those 17Δ bits are achievable by using the LTD model and an achieving strategy for our example is given in Fig. 2.16. The difference in the LTD model is, that a dependence of the bit-levels at the receiver is introduced by taking the binary expansion of the channel gain into account.

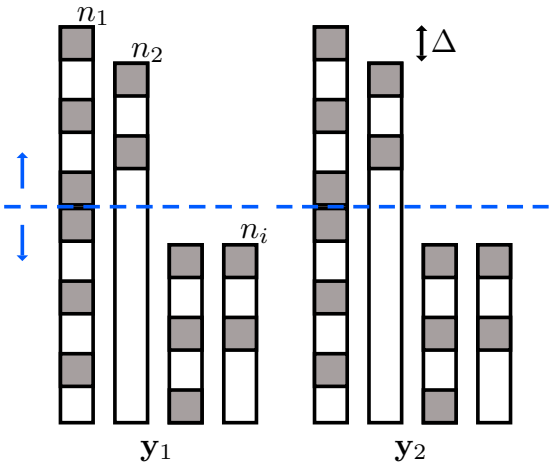

Figure 2.15.: Achievable strategy for the LDM in the exemplary setting. We have illustrated the parts of $\mathbf{y}_1^{\uparrow,n}$, $\mathbf{y}_2^{\uparrow,n}$ and $\mathbf{y}_1^{\downarrow,n}$, $\mathbf{y}_2^{\downarrow,n}$ with blue arrows. Every grey box corresponds to a $\Delta-$bit allocation.

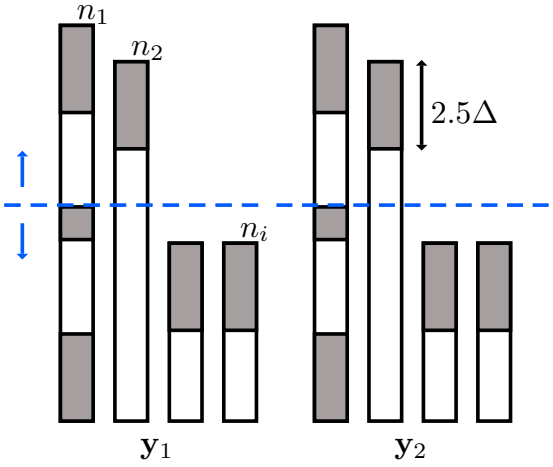

Figure 2.16.: Achievable strategy for the LTDM in the exemplary setting. We have illustrated the parts of $\mathbf{y}_1^{\uparrow,n}$, $\mathbf{y}_2^{\uparrow,n}$ and $\mathbf{y}_1^{\downarrow,n}$, $\mathbf{y}_2^{\downarrow,n}$ with blue arrows. The aligning blocks have 2.5Δ bits. The block in the middle, under the blue split, has Δ bits.

2.9. Conclusions

In this paper we have investigated the Gaussian interfering multiple access channel (G-IMAC). We used the linear deterministic model (LDM) of the IMAC (coined LD-IMAC) as a first approximation to gain new insights. These insights show that with the help of interference alignment techniques in the signal-scale, up to half of the interference can be aligned and the other half can be therefore made available for communication. Moreover, we have shown upper bounds which coincide with the achievable rates for certain interference-to-signal ratios (see Fig. 2.3) and are within a certain gap of all other points. We conjectured that the gap is due to the over simplification of the LDM. Subsequently, lattice codes were used to convert the bit-level alignment schemes from the LD-IMAC to the G-IMAC. However, the gap towards the upper bounds consisted due to the fact that the lattice codes schemes were modelled after the bit-alignment strategies of the LD-IMAC, therefore inheriting the suboptimal structure. To overcome this gap, an approximation was needed which lies between the standard G-IMAC and the LD-IMAC. The new approximation model of [NMA13], the lower triangular deterministic model (LTDM), was a promising approach. Instead of setting the fine channel gain to one (as in the LDM case), this new model integrated the channel gain by another binary expansion. Taking the fine channel gain into account enables a new class of achievable schemes which are not limited to orthogonal bit alignment. It turned out, that this was also the limiting factor in the previous LDM achievable schemes. We have shown that the IMAC approximated by the LTDM (LTD-IMAC) can achieve the previous upper bounds in the whole interference regime, within a *constant* gap. Moreover, techniques from [NMA13] could be modified in a way to show a constant gap capacity approximation of the G-IMAC, thereby porting the LTDM schemes to the Gaussian model. As a by-product this shows, that the GDoF of the IMAC is indeed as pictured in Fig. 2.17. This shows that in the IMAC considerable gains can be achieved via signal scale alignment methods. Above $\frac{3}{2}$ interference-to-signal ratio, the harmful effects of interference can be completely cancelled. Note that we only treated the case of equal interference strength at the receivers. This assumption is only for simplification of the analysis. However, one needs a difference in the ratio of both direct link gains in comparison to the interference link gains in order to enable the signal scale alignment and get multi-user gain. We call this difference the shift-property.

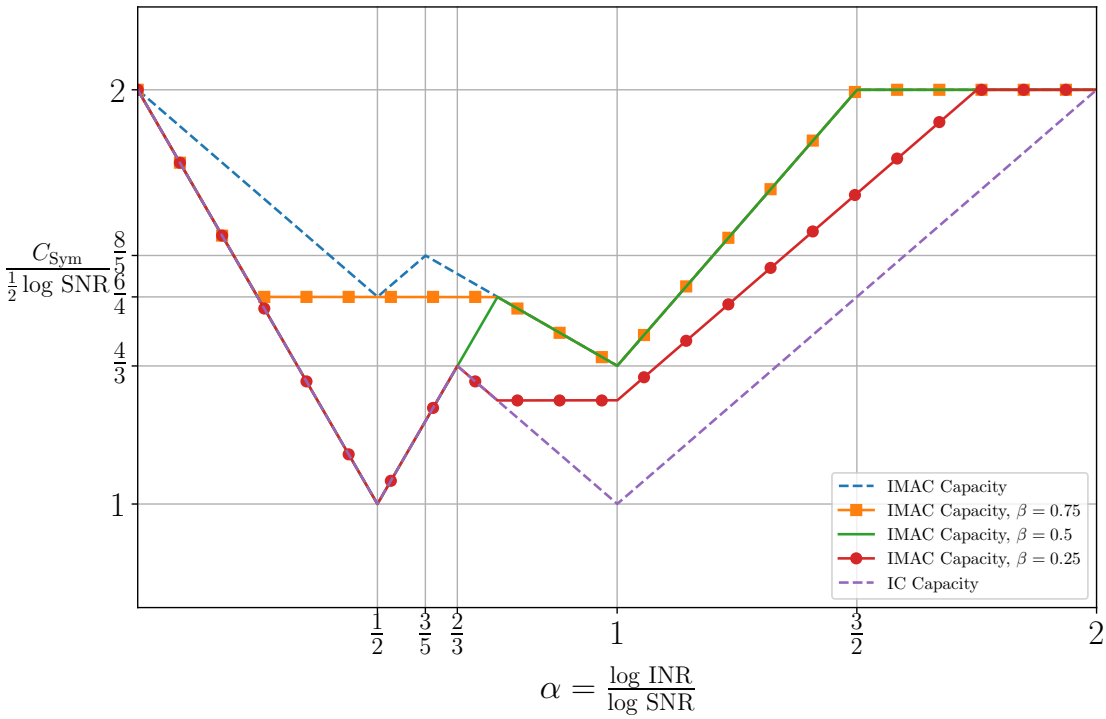

Figure 2.17.: The GDoF "W" curve for the Gaussian IMAC, for various β, which are the defined as the channel strength ratio between the two direct links $\text{SNR}_{i2} = \text{SNR}_{i1}^{\beta}$, or equivalently $\beta = \frac{n_2}{n_1}$ if fine gains are neglected. All curves are based on a symmetric channel. One can see that β controls the multi-user gain dependent on α. Moreover, one can see that for certain parameter ranges, the capacity is independent of differences in α, which results in horizontal lines. The first two (from the left) show 2β, the third shows $1 + \beta$.

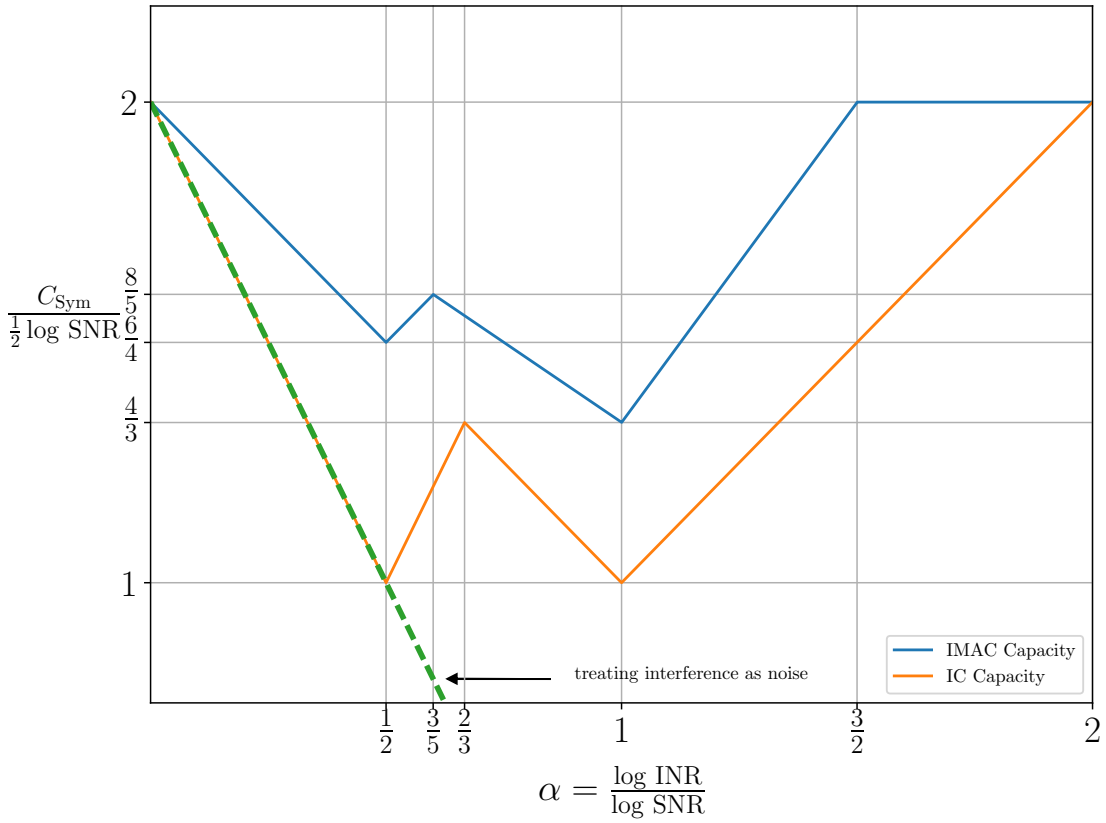

Figure 2.18.: The GDoF "W" curve for the symmetric Gaussian IC and the symmetric Gaussian IMAC. In the case of the IMAC, the SNR is the signal-noise-ratio of the strong direct links (associated with the coarse channel gain 2^{n_1}). Moreover, the curve shows the case that the weaker direct links (associated with coarse channel gain 2^{n_2}) are *strong enough* to support full multi-user gain.

2.10. Proofs

2.10.1. Proof of Theorem 2.4 and 2.7

Proof. A part of this proof follows closely the method of [BT08] for the Gaussian 2-user IC and applies it to the IMAC setting. The mutual information terms of the Gaussian channel will be transformed into a deterministic form in two steps. Each step will introduce a bit penalty which contributes to the overall gap between both bounds. Step 1 will transform the average power constraint to a peak power constraint. Step 2 truncates the signals at the noise level and removes the noise.

Step 1: average power constraint to peak power constraint. The channel equation for the Gaussian IMAC is

$$y^1 = h_{11}^1 2^{n_{11}^1} x_{11} + h_{12}^1 2^{n_{12}^1} x_{12} + h_{21}^1 2^{n_{21}^1} x_{21} + h_{22}^1 2^{n_{22}^1} x_{22} + z^1$$
$$y^2 = h_{11}^2 2^{n_{11}^2} x_{11} + h_{12}^2 2^{n_{12}^2} x_{12} + h_{21}^2 2^{n_{21}^2} x_{21} + h_{22}^2 2^{n_{22}^2} x_{22} + z^2,$$

Recall that we assume without loss of generality that the Gaussian IMAC inputs have a unit average power constraint. We have to split the input signals into two parts, where one part is not exceeding the unit peak power constraint. We can write the binary expansion of the input signals as

$$x_{ik} = \sum_{b=-\infty}^{\infty} [x_{ik}]_b 2^{-b}.$$

Now we can write the part which exceeds the peak power constraint as

$$\hat{x}_{ik} := sign(x_{ik}) \sum_{b=-\infty}^{0} [x_{ik}]_b 2^{-b}$$

and let the remaining part be

$$\bar{x}_{ik} := x_{ik} - \hat{x}_{ik} = sign(x_{ik}) \sum_{b=1}^{\infty} [x_{ik}]_b 2^{-b}.$$

Therefore, we can rewrite the channel equations such that all signals have a peak power constraint.

$$\bar{y}^1 = h_{11}^1 2^{n_{11}^1} \bar{x}_{11} + h_{12}^1 2^{n_{12}^1} \bar{x}_{12} + h_{21}^1 2^{n_{21}^1} \bar{x}_{21} + h_{22}^1 2^{n_{22}^1} \bar{x}_{22} + z^1$$
$$\bar{y}^2 = h_{11}^2 2^{n_{11}^2} \bar{x}_{11} + h_{12}^2 2^{n_{12}^2} \bar{x}_{12} + h_{21}^2 2^{n_{21}^2} \bar{x}_{21} + h_{22}^2 2^{n_{22}^2} \bar{x}_{22} + z^2,$$

and let

$$\hat{y}^1 = y^1 - \bar{y}^1$$
$$\hat{y}^2 = y^2 - \bar{y}^2,$$

be the receiver-side which exceeds the constraints. Each transmitter encodes a codeword $x_{ik}^n(w_{ik})$ based on the message w_{ik} with message rate R_{ik} for cell i and user k. We can therefore write the mutual information term for cell i in the following way

$$\begin{aligned}
&I(w_{i1}, w_{i2}; (y^i)^n) \\
&\overset{(a)}{\leq} I(w_{i1}, w_{i2}; (\bar{y}^i)^n, (\hat{y}^i)^n) \\
&= I(w_{i1}, w_{i2}; (\bar{y}^i)^n) + I(w_{i1}, w_{i2}; (\hat{y}^i)^n | (\bar{y}^i)^n) \\
&\leq I(w_{i1}, w_{i2}; (\bar{y}^i)^n) + H((\hat{y}^i)^n) \\
&\overset{(b)}{\leq} I(w_{i1}, w_{i2}; (\bar{y}^i)^n) + \sum_{i=1}^{2} H(\hat{x}_{i1}^n) + H(\hat{x}_{i2}^n) \\
&\overset{(c)}{\leq} I(w_{i1}, w_{i2}; (\bar{y}^i)^n) + 8n
\end{aligned}$$

where (a) follows with the data processing inequality $(y^i)^n = (\bar{y}^i)^n + (\hat{y}^i)^n = f((\bar{y}^i)^n, (\hat{y}^i)^n)$, (b) follows since $(\hat{y}^i)^n = \hat{x}_{i1}^n + \hat{x}_{i2}^n$ and (c) is a consequence of Lemma 6 in [BT08].

Step 2: truncate at the noise level and remove the noise Recall that the input is purely made of peak-power constraint signals due to step 1. Moreover, the channel gain is represented as $h2^n$, where $h \in (1, 2]$, $n \in \mathbb{N}$.

$$x_{ik} = sign(x_{ik}) \sum_{b=1}^{\infty} [x_{ik}]_b 2^{-b}.$$

We will now split the terms $h_{ik}2^{n_{ik}^j} x_{ik}$ in parts above the noise level and below the noise level. The part above the noise level can be written as

$$h_{ik}2^{n_{ik}^j} sign(x_{ik}) \sum_{b=1}^{n_{ik}^j} [x_{ik}]_b 2^{-b}.$$

The part below the noise level can be bounded from above by

$$|h_{ik}2^{n_{ik}^j} \sum_{b=n_{ik}^j+1}^{\infty} [x_{ik}]_b 2^{-b}| \leq 2^{n_{ik}^j+1}2^{-n_{ik}^j} \leq 2.$$

Therefore, we can write the truncated output equations without noise as

$$\tilde{y}^j = \sum_i \sum_k \left\lfloor 2^{n_{ik}^j} \sum_{b=1}^{n_{ik}^j} [x_{ik}]_b 2^{-b} \right\rfloor,$$

where $i, k \in \{1, 2\}$. Following the proof method, we define

$$\begin{aligned}
\epsilon^j := \hat{y}^j - \tilde{y}^j = \sum_i \sum_k \Bigg[& h_{ik}2^{n_{ik}^j} \sum_{b=n_{ik}^j+1}^{\infty} [x_{ik}]_b 2^{-b} \\
& + (h_{ik}^j - 1) \sum_{b=1}^{n_{ik}^j} [x_{ik}]_b 2^{-b} + \text{frac}\left(2^{n_{ik}^j} \sum_{b=1}^{n_{ik}^j} [x_{ik}]_b 2^{-b}\right) \Bigg] \\
& + z^j \\
= \sum_i \sum_k x_{ik}^* + z^j,
\end{aligned}$$

where the first part in the sum accounts for the terms below the noise level, the second part includes the fractional channel gain h and the last part is for the fractional terms due to the floor function. Now we can transform the mutual information terms into the final linear deterministic mutual information terms

$$\begin{aligned}
& I(w_{i1}, w_{i2}; (\bar{y}^i)^n) \\
& \leq I(w_{i1}, w_{i2}; (\tilde{y}^j)^n, (\epsilon^j)^n) \\
& = I(w_{i1}, w_{i2}; (\tilde{y}^j)^n) + I(w_{i1}, w_{i2}; (\epsilon^j)^n | (\tilde{y}^j)^n) \\
& = I(w_{i1}, w_{i2}; (\tilde{y}^j)^n) + h((\epsilon^j)^n | (\tilde{y}^j)^n) - h((\epsilon^j)^n | (\tilde{y}^j)^n, w_{i1}, w_{i2}) \\
& \leq I(w_{i1}, w_{i2}; (\tilde{y}^j)^n) + h((\epsilon^j)^n) - h(z^j) \\
& = I(w_{i1}, w_{i2}; (\tilde{y}^j)^n) + I(x_{11}^*, x_{12}^*, x_{21}^*, x_{22}^*; (\epsilon^j)^n) \\
& \overset{(a)}{<} I(w_{i1}, w_{i2}; (\tilde{y}^j)^n) + 3.1n,
\end{aligned}$$

where (a) is due to the fact that $(x_{11}^*, x_{12}^*, x_{21}^*, x_{22}^*) \mapsto \epsilon^j$ forms a 4-user MAC channel. With (2.10.1) and $|(h_{ik}^j - 1)x_{ik}| \leq 1$, one can see that $|x_{ik}^*| \leq 4$ and therefore $\frac{1}{n} I(x_{11}^*, x_{12}^*, x_{21}^*, x_{22}^*; (\epsilon^j)^n) \leq \frac{1}{2}\log(1 + 4(16)) + \epsilon_n < 3.1n$ for $n \to \infty$.

Therefore, we have shown that we can bound the Gaussian IMAC mutual information terms from above with deterministic mutual information terms within a constant gap of 11.1 bits.

$$\begin{aligned} I(w_{i1}, w_{i2}; (y^i)^n) &\overset{\text{Step 1}}{\leq} I(w_{i1}, w_{i2}; (\bar{y}^i)^n) + 8n \\ &\overset{\text{Step 2}}{\leq} I(w_{i1}, w_{i2}; (\tilde{y}^j)^n) + 11.1n. \end{aligned}$$

Note that the LD-IMAC and the LTD-IMAC models are restricted to positive inputs. However, capacity is only a function of the magnitude of the channel gains, and additional negative inputs would only result in an additional constant number of bits. Moreover, addition over $\mathbb{F}_2$ also costs only a constant number of bits (the missing carry over) and can be neglected for high SNR regimes as well. We can therefore upper bound the mutual information of the Gaussian model, with the terms of the deterministic model plus a constant number of bits. Furthermore, we can upper bound the deterministic model terms with Theorem 2.6.2, which yields an upper bound for the Gaussian model. □

Remark 2.16. An alternative way to prove those bounds is to directly bound the Gaussian mutual information terms by using smart genies and the fact that conditional differential entropy is maximised by Gaussian random variables. In particular, the genie must be chosen such that it mimics the cuts in the proof of Theorem 2.6.2. The main challenges here are the first two bounds, D_1 and D_2. Both bounds rely on a cut of the received *sum* of signals y. We remark that a simple genie which provides for example the interference of the users in cell 1 at receiver 2 plus noise (i.e. $s_1 = h_{11}^2 2^{n_{11}^2} x_{11} + h_{12}^2 2^{n_{12}^2} x_{12} + z^2$), to receiver 1 is not sufficient for a good bound. Instead, one needs to provide a genie, where the sum of both signals has the same relative shift as the received signals. Lets say we provide the following genie information to receiver 1: $s_1 = ax_{11} + bx_{12} + z^2$, then a and b need to obey $h_{11}^1 2^{n_{11}^1} b = h_{12}^1 2^{n_{12}^1} a$. This property allows an elimination of an additional term inside the log variance term resulting from the Gaussian conditional entropy minus noise. in the following way: Let the received signal be given as $Y = aX_1 + bX_2 + cX_3 + dX_4 + Z_1$. Moreover, we define a genie signal as $S = a'X_1 + b'X_2 + Z_2$. We now want to bound the term $h(Y|S) - h(Z_1)$ from above. Using the fact that conditional differential entropy is maximised by Gaussian random variables, we have that

$$h(Y|S) - h(Z_1) \leq h(Y_G|S_G) - h(Z_1) = h(Y_G, S_G) - h(S_G) - h(Z_1).$$

We know that

$$\mathrm{Var}(Y_G, S_G) = E[Y_G^2]E[S_G^2] - (E[Y_G S_G])^2$$

and we therefore get

$$h(Y_G, S_G) - h(S_G) - h(Z_1) = \tfrac{1}{2}\log\left[\frac{E[Y_G^2]E[S_G^2] - (E[Y_G S_G])^2}{E[S_G^2]E[Z_1^2]}\right],$$

where we used that for a Gaussian random variable X, $h(X) = \frac{1}{2}\log 2\pi\epsilon\mathrm{Var}(X)$. Notice, that in our model, the noise is limited to one. We can therefore write the term as

$$\begin{aligned}
&\tfrac{1}{2}\log\left[\frac{E[Y_G^2]E[S_G^2] - (E[Y_G S_G])^2}{E[S_G^2]E[Z^2]}\right] \\
&= \tfrac{1}{2}\log\left[E[Y_G^2] - \frac{(E[Y_G S_G])^2}{E[S_G^2]}\right] \\
&= \tfrac{1}{2}\log\left[a^2 + b^2 + c^2 + d^2 + 1 - \frac{(aa')^2 + 2aa'bb' + (bb')^2}{(a')^2 + (b')^2 + 1}\right] \\
&= \tfrac{1}{2}\log\left[c^2 + d^2 + 1 + \frac{(a^2 + b^2) - (ab' - a'b)^2}{(a')^2 + (b')^2 + 1}\right] \\
&\overset{(b)}{=} \tfrac{1}{2}\log\left[c^2 + d^2 + 1 + \frac{a^2 + b^2}{(a')^2 + (b')^2 + 1}\right],
\end{aligned}$$

where we used in (b), that the genie provides the side-information with $\frac{a}{b} = \frac{a'}{b'}$.

Now one can scale a and b appropriately as in the proof of Theorem 2.6.2. Since the genie information is now a shifted version of the interference terms, one needs to use the same trick as in the deterministic case to handle the remaining parts $h(S_1) - h(Y^1|S_2, w_{11}, w_{12})$ and $h(S_2) - h(Y^2|S_1, w_{21}, w_{22})$ to show the bound.

2.10.2. Bound on Alignment Structure Rate Term

We look into the lattice decoding bounds and develop lower bounds on the maximum achievable rates R_{I_i} for the possible rate expressions inside the alignment structure for cell i and bit-level l. The achievable rate for the alignment structure is divided into three parts. We have two common signal parts, which are also received at cell j and one private signal part which is just received in cell i. The common signal parts need to obey two different decoding bounds, where one bound is for the decodability in cell i and one is for the decodability in cell j.

Common Signal Parts

For the direct path we have the decoding bound (2.15) with an equivalent noise

$$N_i(l) = 1 + \sum_{\text{used levels}} \theta_{l+1}$$

$$= \mathrm{SNR}_{i1}^{1-l(1-\beta_i)} + \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor L_j \rfloor} \frac{\mathrm{INR}_j^i}{\mathrm{SNR}_{j1}^{(m-1)(1-\beta_j)}} - \frac{\mathrm{INR}_j^i}{\mathrm{SNR}_{j1}^{m(1-\beta_j)}},$$

because every partition, starting at level l, is used atleast once, the middle terms of the sum vanish and we have $\mathrm{SNR}_{i1}^{1-l(1-\beta_i)} - 1$ left. Moreover, due to the overlapping of the interference, we have a sum over the odd bit-levels of the interference affected part. Together with the general noise of 1, we get the expression above. The decoding bound is therefore given as

$$\begin{aligned} R_{\mathrm{IC}_i}(l) &\leq \tfrac{1}{2} \log \left(1 + \frac{\mathrm{SNR}_{i1}^{1-(l-1)(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-l(1-\beta_i)}}{\mathrm{SNR}_{i1}^{1-l(1-\beta_i)} + \nu} \right) \\ &= \bar{R}_{\mathrm{IC}_i'}(l), \end{aligned}$$

where we denote $\nu = \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor L_j \rfloor} \frac{\mathrm{INR}_j^i}{\mathrm{SNR}_{j1}^{(m-1)(1-\beta_j)}} - \frac{\mathrm{INR}_j^i}{\mathrm{SNR}_{j1}^{m(1-\beta_j)}}$. Now we can lower bound $\bar{R}_{\mathrm{I}_i}(l)$ and show that

$$\begin{aligned} \bar{R}_{\mathrm{IC}_i'}(l) &= \tfrac{1}{2} \log \left(1 + \frac{\mathrm{SNR}_{i1}^{1-(l-1)(1-\beta_i)} - \mathrm{SNR}_{i1}^{1-l(1-\beta_i)}}{\mathrm{SNR}_{i1}^{1-l(1-\beta_i)} + \nu} \right) \\ &= \tfrac{1}{2} \log \left(\frac{\mathrm{SNR}_{i1}^{1-(l-1)(1-\beta_i)} + \nu}{\mathrm{SNR}_{i1}^{1-l(1-\beta_i)} + \nu} \right) \\ &> \tfrac{1}{2} \log \left(\frac{\mathrm{SNR}_{i1}^{1-(l-1)(1-\beta_i)}}{\mathrm{SNR}_{i1}^{1-l(1-\beta_i)} + \nu} \right) \\ &> \tfrac{1}{2} \log \left(\frac{\mathrm{SNR}_{i1}^{1-(l-1)(1-\beta_i)}}{2\mathrm{SNR}_{i1}^{1-l(1-\beta_i)}} \right) \\ &= \tfrac{1}{2} \log \mathrm{SNR}_{i1}^{1-\beta_i} - \tfrac{1}{2}, \end{aligned}$$

where we used that $\mathrm{SNR}_{i1}^{1-l(1-\beta_i)} > \nu$. The decoding bound is different in the interference path, because we need to decode the sum of two bit-levels. A sum of K signals needs to obey the decoding bound (2.16) with an equivalent noise of

$$\begin{aligned} N_j(l) &= 1 + \sum_{\text{used levels}} \theta_{l+1} \\ &= \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{l(1-\beta_i)}} + \sum_{\substack{m=l+1 \\ m \text{ odd}}}^{\lfloor L_i \rfloor} \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{(m-1)(1-\beta_i)}} - \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{m(1-\beta_i)}} \end{aligned}$$

$$= \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{l(1-\beta_i)}}(1 + \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor L_i \rfloor} \mathrm{SNR}_{i1}^{(1-m)(1-\beta_i)} - \mathrm{SNR}_{i1}^{-m(1-\beta_i)})$$
$$= \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{l(1-\beta_i)}}(1+\nu_2).$$

Note that an signal directed to level l with an received power of θ_l at cell i gets received at cell j with power

$$\theta_l \frac{|h_{ik}^j|^2}{|h_{ik}^i|^2} = \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{(l-1)(1-\beta_i)}} - \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{l(1-\beta_i)}} = \frac{\mathrm{INR}_i^j}{\mathrm{SNR}_{i1}^{l(1-\beta_i)}}(\mathrm{SNR}_{i1}^{(1-\beta_i)} - 1).$$

We, therefore, have the second decoding bound with

$$R_{\mathrm{CI}_i}(l) \leq \tfrac{1}{2}\log\left(\frac{1}{2} + \frac{\mathrm{SNR}_{i1}^{(1-\beta_i)} - 1}{1+\nu_2}\right) = \bar{R}_{\mathrm{IC}_i''}(l).$$

We can now lower bound the rate $\bar{R}_{\mathrm{IC}_i''}(l)$ and show that

$$\begin{aligned}
\bar{R}_{\mathrm{IC}_i''}(l) &= \tfrac{1}{2}\log\left(\frac{1}{2} + \frac{\mathrm{SNR}_{i1}^{(1-\beta_i)} - 1}{1+\nu_2}\right) \\
&> \tfrac{1}{2}\log\left(1 + \frac{\mathrm{SNR}_{i1}^{(1-\beta_i)} - 1}{1+\nu_2}\right) - \tfrac{1}{2} \\
&= \tfrac{1}{2}\log\left(\frac{\mathrm{SNR}_{i1}^{(1-\beta_i)} + \nu_2}{1+\nu_2}\right) - \tfrac{1}{2} \\
&> \tfrac{1}{2}\log\left(\frac{\mathrm{SNR}_{i1}^{(1-\beta_i)}}{1+\nu_2}\right) - \tfrac{1}{2} \\
&> \tfrac{1}{2}\log\left(\mathrm{SNR}_{i1}^{(1-\beta_i)}\right) - 0.5\log(2) - \tfrac{1}{2} \\
&= \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{(1-\beta_i)} - 1
\end{aligned}$$

where we used the fact that $\nu_2 < 1$ since $\mathrm{SNR}_{i1} > 1$ and the weak interference regime. Note that we need to obey both decoding bounds such that our common signal parts are decodable at the legitimate receiver, and also as part of the lattice sum at the unintended receiver. The latter is important for the successive decoding scheme in which we need to subtract the interference sum to be able to decode the following bit-levels. We, therefore, use the minimum of both and the achievable rate is therefore

$$\bar{R}_{\mathrm{IC}_i}(l) = \min\{\bar{R}_{\mathrm{IC}_i'}(l), \bar{R}_{\mathrm{IC}_i''}(l)\} > \tfrac{1}{2}\log \mathrm{SNR}_{i1}^{(1-\beta_i)} - 1.$$

Private Signal Parts

Here we just need to look into the direct path where we have the decoding bound (2.15) with an equivalent noise

$$N_i(l) = 1 + \sum_{\text{used levels}} \theta_{l+1} = \frac{\text{INR}_j^i}{\text{SNR}_{j1}^{l(1-\beta_j)}}(1+\nu_3),$$

where

$$\nu_3 = \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor L_j \rfloor} \text{SNR}_{j1}^{(1-m)(1-\beta_j)} - \text{SNR}_{j1}^{-m(1-\beta_j)}.$$

Note that this is the equivalent of $N_j(l)$ in the bound for $R_{IC_i''}$. Moreover, the bound is similar, except that we now just need to decode one codeword and therefore get the bound

$$R_{\text{IP}_i}(l) \leq \tfrac{1}{2}\log\left(1 + \frac{\text{SNR}_{j1}^{(1-\beta_j)} - 1}{1+\nu_3}\right) = \bar{R}_{\text{IP}_i}(l).$$

Now we can lower bound $\bar{R}_{\text{I}_i}(l)$ by

$$\bar{R}_{\text{IP}_i}(l) > \tfrac{1}{2}\log \text{SNR}_{j1}^{(1-\beta_j)} - \tfrac{1}{2},$$

using the same steps as for $\bar{R}_{\text{IC}_i}$. This rate depends on the ratio of the direct signals of cell j, since this ratio gives the size of the interference alignment blocks and therefore the size of the interference-free slots which cell i can use for communication.

Remark 2.17. We did not discuss the case where $\lfloor Li \rfloor \neq Li$, which results in remainder terms for certain cases in the alignment structures. The transmission power is not affected, but the noise term would be slightly different. However, the noise term would only change in the ν-terms but still obey our conditions. This means that all results above apply to these cases as well.

2.10.3. Proof of Lemma 4

We have three bit vectors $\bar{\mathbf{u}}_1^{'} = \bar{\mathbf{u}}_1 \oplus \bar{\mathbf{u}}_4 \oplus \bar{\mathbf{u}}_5$, $\bar{\mathbf{u}}_2$ and $\bar{\mathbf{u}}_3$, which are multiplied by the matrices $\bar{\mathbf{G}}_1$, $\bar{\mathbf{G}}_2$ and $\bar{\mathbf{G}}_3$, respectively. Here, $\bar{\mathbf{u}}_1^{'}$ corresponds to the wanted received signal x_{i1}, $\bar{\mathbf{u}}_2$ to x_{i2} and $\bar{\mathbf{u}}_3$ to the sum of both interference bit vectors. One can view the signals $\bar{\mathbf{u}}_4$ and $\bar{\mathbf{u}}_5$ as the private parts of $\bar{\mathbf{u}}_1^{'}$. We use the same framework as in [NMA13] to analyse this setting, i.e we use the notation

$$\mathcal{U}(n^-, n^+) := \{\bar{\mathbf{u}} \in \{0,1\}^{n_1} : \bar{u}_i = 0 \ \forall i \in \{1, \ldots, n_1 - n^-\} \cup \{n_1 - n^+ + 1, \ldots, n_1\}\}$$

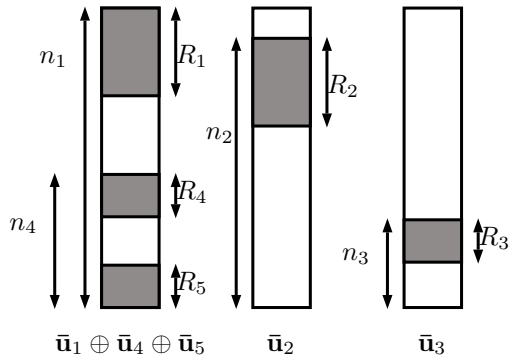

Figure 2.19.: Illustration of the received bit-vectors at one receiver. A blank region corresponds to bits which are set to zero, i.e. unused bits. And grey regions correspond to used bit-levels. Observe that there are 5 used regions, which correspond to the weak interference case and our proposed scheme.

where n^- and n^+ are nonnegative integers such that $n^- \geq n^+$. Such that we can consider bit vectors ($\bar{\mathbf{u}}_1$, $\bar{\mathbf{u}}_2$, $\bar{\mathbf{u}}_4$, $\bar{\mathbf{u}}_3$, $\bar{\mathbf{u}}_5$) in

$$\mathcal{U} := \mathcal{U}(n_1, n_1 - R_1) \times \mathcal{U}(n_2, n_2 - R_2) \times \mathcal{U}(n_4, n_4 - R_4) \times \mathcal{U}(n_3, n_3 - R_3) \times \mathcal{U}(R_5, 0),$$

with $n_1 \geq n_2 \geq n_4 \geq n_3$, see Fig 2.19. Note that due to our scheme, we have a few assumptions on $R_{k'}$, $k' \in \{1, \ldots, 5\}$, namely that $\bar{\mathbf{u}}_4$, $\bar{\mathbf{u}}_3$ and $\bar{\mathbf{u}}_5$ do not overlap, and $\bar{\mathbf{u}}_1$ and $\bar{\mathbf{u}}_2$ do not overlap with those three signals, too. This yields the following equations

$$\begin{aligned} R_1 + R_4 + R_3 + R_5 &\leq n_1 \\ R_2 + R_4 + R_3 + R_5 &\leq n_2 \\ R_4 + R_3 + R_5 &\leq n_4 \\ R_3 + R_5 &\leq n_3. \end{aligned}$$

We introduce the rate $R_{\text{Fix}} := R_3 + R_4 + R_5$ to denote the sum of the bit-level rates which are fixed by the scheme, i.e. do not overlap. Therefore, we have that

$$\begin{aligned} R_1 &\leq n_1 - R_{\text{Fix}} \\ R_2 + n_1 - n_2 &\leq n_1 - R_{\text{Fix}} \end{aligned}$$

and it follows that $n(\bar{\mathbf{u}}_k) \leq n_1 - R_{\text{Fix}}$, for $k \in \{1,2\}$, $\bar{\mathbf{u}}_k \neq 0$ and $n(\bar{\mathbf{u}})$ which gives the smallest index i, such that $\bar{u}_i = 1$, and $n(\mathbf{0}) = \infty$. This means we have that

$$\min\{n(\bar{\mathbf{u}}_4), n(\bar{\mathbf{u}}_5), n(\bar{\mathbf{u}}_3)\} > n_1 - R_{\text{Fix}}.$$

We can now remove the dependence of the outage set on the signals $\bar{\mathbf{u}}_4$, $\bar{\mathbf{u}}_5$, $\bar{\mathbf{u}}_3$. Note that we have $n(\bar{\mathbf{G}}\bar{\mathbf{u}}) = n(\bar{\mathbf{u}})$, since the matrices $\bar{\mathbf{G}}$ are unit lower triangular and therefore down-shift (to bigger indices) the signal $\bar{\mathbf{u}}$[7]. We therefore have that

$$\bar{\mathbf{G}}_1(\bar{\mathbf{u}}_1 \oplus \bar{\mathbf{u}}_4 \oplus \bar{\mathbf{u}}_5) \oplus \bar{\mathbf{G}}_2\bar{\mathbf{u}}_2 \oplus \bar{\mathbf{G}}_3\bar{\mathbf{u}}_3 = \mathbf{0}$$

only if

$$\begin{aligned} n\left(\bar{\mathbf{G}}_1\bar{\mathbf{u}}_1 \oplus \bar{\mathbf{G}}_2\bar{\mathbf{u}}_2\right) &= n\left(\bar{\mathbf{G}}_1(\bar{\mathbf{u}}_4 \oplus \bar{\mathbf{u}}_5) + \bar{\mathbf{G}}_3\bar{\mathbf{u}}_3\right) \\ &\geq \min\{n(\bar{\mathbf{G}}_1(\bar{\mathbf{u}}_4 \oplus \bar{\mathbf{u}}_5)), n(\bar{\mathbf{G}}_3\bar{\mathbf{u}}_3)\} \\ &= \min\{n(\bar{\mathbf{u}}_4 \oplus \bar{\mathbf{u}}_5), n(\bar{\mathbf{u}}_3)\} \\ &= \min\{\min\{n(\bar{\mathbf{u}}_4), n(\bar{\mathbf{u}}_5)\}, n(\bar{\mathbf{u}}_3)\} \\ &= \min\{n(\bar{\mathbf{u}}_4), n(\bar{\mathbf{u}}_5), n(\bar{\mathbf{u}}_3)\} \\ &> n_1 - R_{\text{Fix}}. \end{aligned}$$

Also, we have for $(\bar{\mathbf{u}}_4, \bar{\mathbf{u}}_3, \bar{\mathbf{u}}_5) \neq (\mathbf{0}, \mathbf{0}, \mathbf{0})$ that

$$\bar{\mathbf{G}}_1(\bar{\mathbf{u}}_1 \oplus \bar{\mathbf{u}}_4 \oplus \bar{\mathbf{u}}_5) \oplus \bar{\mathbf{G}}_2\bar{\mathbf{u}}_2 \oplus \bar{\mathbf{G}}_3\bar{\mathbf{u}}_3 = \mathbf{0}$$

can hold only if $(\bar{\mathbf{u}}_1, \bar{\mathbf{u}}_2) \neq (\mathbf{0}, \mathbf{0})$, again due to the non-overlapping property of the signals $\bar{\mathbf{u}}_4, \bar{\mathbf{u}}_3$ and $\bar{\mathbf{u}}_5$. Define the sets

$$\begin{aligned} B'(\bar{\mathbf{u}}_0, \bar{\mathbf{u}}_1, \bar{\mathbf{u}}_2) := \{&(g_0, g_1, g_2) \in (1,2]^3 : \\ &n\left(\bar{\mathbf{G}}_0\bar{\mathbf{u}}_0 \oplus \bar{\mathbf{G}}_1\bar{\mathbf{u}}_1 \oplus \bar{\mathbf{G}}_2\bar{\mathbf{u}}_2\right) > n_1 - R_{\text{Fix}}\} \end{aligned}$$

and

$$\mathcal{U} := \mathcal{U}(n_0, n_0 - R_0) \times \mathcal{U}(n_1, n_1 - R_1) \times \mathcal{U}(n_2, n_2 - R_2).$$

[7] We have = instead of $\leq$, due to the unit diagonal.

with the outage set

$$B \subset B' := \bigcup_{(\bar{\mathbf{u}}_0,\bar{\mathbf{u}}_1,\bar{\mathbf{u}}_2)\in\mathcal{U}\setminus\{(\mathbf{0},\mathbf{0},\mathbf{0})\}} B'(\bar{\mathbf{u}}_0,\bar{\mathbf{u}}_1,\bar{\mathbf{u}}_2).$$

Observe that this corresponds to our case for $\bar{\mathbf{u}}_0 = \mathbf{0}$ and $R_0 = 0$. It was shown in [NMA13, Proof of Lemma 11], that the measure of the set

$$B \subset B' := \bigcup_{(\bar{\mathbf{u}}_0,\bar{\mathbf{u}}_1,\bar{\mathbf{u}}_2)\in\mathcal{U}\setminus\{(\mathbf{0},\mathbf{0},\mathbf{0})\}} B'(\bar{\mathbf{u}}_0,\bar{\mathbf{u}}_1,\bar{\mathbf{u}}_2)$$

can be bounded by

$$\mu(B) \leq \delta$$

if

$$\begin{aligned} R_1 + R_0 + R_2 + R_{\text{Fix}} &\leq n_1 - \log(16/\delta) \\ R_0 + R_2 + R_{\text{Fix}} &\leq n_0 - \log(16/\delta) \\ R_2 + R_{\text{Fix}} &\leq n_2. \end{aligned}$$

If we plug-in $\bar{\mathbf{u}}_0 = \mathbf{0}$ and go through the proof, one can see that this reduces the number of cases from four to one, which results in a lower gap and just two conditions, namely

$$\begin{aligned} R_1 + R_2 + R_{\text{Fix}} &\leq n_1 - \log(4/\delta) \\ R_2 + R_{\text{Fix}} &\leq n_2. \end{aligned}$$

Together with our conditions for the fixed, non-overlapping parts, we have that

$$\begin{aligned} R_1 + R_2 + R_4 + R_3 + R_5 &\leq n_1 - \log(4/\delta) \\ R_2 + R_4 + R_3 + R_5 &\leq n_2 \\ R_4 + R_3 + R_5 &\leq n_4 \\ R_3 + R_5 &\leq n_3. \end{aligned}$$

Now we can set

$$\begin{aligned} R_1 &:= R_{k1}^c & n_1 &:= n_{k1}^k \\ R_2 &:= R_{k2}^c & n_2 &:= n_{k2}^k \\ R_3 &:= \max\{R_{l2}^c, R_{l1}^c\} & n_4 &:= (n_{k1}^k - n_l^k) \\ R_4 &:= R_{k1}^{p2} & n_3 &:= n_k^l \end{aligned}$$

$$R_5 := R_{k1}^{p1}.$$

and replace δ with $\delta/2$ to account for the measure of the overall outage set (over both receivers) which concludes the proof of Lemma 2.11.

2.10.4. Proof of the Decoding Lemma for the Weak Interference Case

In order to get a similar result as in Lemma 2.15 for the weak interference case, we need to prove a modified version of [NMA13, Lemma 12], which is

Lemma 2.18. *Let* n_3, n_1, $n_2 \in \mathbb{Z}_+$ *such that* $n_1 \geq n_2 \geq n_3$ *and* $\frac{n_3}{n_1} < \frac{1}{2}$, *and let* $R_1, R_2, R_3, R_4, R_5 \in \mathbb{Z}_+$. *Define the event*

$$B(u_1, u_2, u_3, u_4, u_5) := \{(g_1, g_2, g_3) \in (1, 4]^3 : \ |g_2 u_2 + g_1(u_1 + u_4 + u_5) + g_3 u_3| \leq 2^{5-n_1}\}$$

and set

$$B := \bigcup_{(u_1,u_2,u_3,u_4,u_5) \in \mathcal{U} \setminus \{(0,0,0,0)\}} B(u_1, u_2, u_3, u_4, u_5).$$

For any $\delta \in (0, 1]$ *satisfying*

$$\begin{aligned} R_1 + R_2 + R_5 + R_4 + R_3 &\leq n_1 - 6 - \log(1008/\delta) \\ R_2 + R_5 + R_4 + R_3 &\leq n_2 - 6 \\ R_5 + R_4 + R_3 &\leq (n_1 - n_3) \\ R_4 + R_3 &\leq n_3 \end{aligned}$$

we have $\mu(B) \leq \delta$.

Where the set $\mathcal{U}$ is defined as

$$\mathcal{U}(n^-, n^+) := \{u \in [-1, 1] : [u]_i = 0 \ \forall i \in \{1, \ldots, n_1 - n^-\} \cup \{n_1 - n^+ + 1, \ldots\}\}$$

and

$$\begin{aligned} \mathcal{U} := &\mathcal{U}(n_1, n_1 - R_1) \times \mathcal{U}(n_2, n_2 - R_2) \times \mathcal{U}((n_1 - n_3), (n_1 - n_3) - R_5) \times \\ &\times \mathcal{U}(n_3, n_3 - R_3) \times \mathcal{U}(R_4, 0). \end{aligned}$$

This means that $\mathcal{U}$ represents the set of possible inputs, if constrained to the specific bit-structure of the LTDM scheme.

Proof. The proof follows closely the one from [NMA13]. We will therefore just point out the main differences and refer the reader to the original proof for a more detailed exposition. First of all, note that due to the specific scheme in the LTD model we have the equations

$$R_5 + R_4 + R_3 \leq (n_1 - n_i)$$
$$R_4 + R_3 \leq n_i.$$

This is because the parts R_5, R_4, R_3 are constructed such that they do not overlap (except the aligning interference signals), see Fig. 2.9. We now represent the outage event as

$$B(u_1, u_2, u_3, u_4, u_5) := \{(g_1, g_2, g_3) \in (1, 4]^3 : \\ |g_2 2^{n_1} u_2 + g_1 2^{n_1}(u_1 + u_4 + u_5) + 2^{n_1} g_3 u_3| \leq 2^5\}$$

and decomposes the shifted signals as

$$2^{n_1} u_2 = A_2 q_2 \tag{2.20a}$$
$$2^{n_1} u_1 = A_1 q_1 \tag{2.20b}$$
$$2^{n_1} u_3 = A_3 q_3 \tag{2.20c}$$
$$2^{n_1} u_4 = q_4 \tag{2.20d}$$
$$2^{n_1} u_5 = A_5 q_5 \tag{2.20e}$$

with a bit-offset at the receiver of $A_k := 2^{n_k - R_k}$ for $k \in 1, 2, 3, 5$ and a used number of bits

$$q_k \in \{-Q_k, -Q_k + 1, \ldots, Q_k - 1, Q_k\}$$

for $k \in \{1, 2, 3, 4, 5\}$ and $Q_k := 2^{R_k}$. Observe that our set B has the same structure as the one in [NMA13], but with an additional variable attached to the aligning part g_1. To solve it in the same fashion, we would need to proof a generalization of [NMA13, Lemma 14]. However, we can circumvent this by exploiting the structure of the weak interference case. We can use that the private allocations of the stronger user are not overlapping with the aligned interference parts. This enables a bound on those parts, which simplifies the analysis and lets us apply [NMA13, Lemma 14] as it is. The following Lemma introduces this idea.

Lemma 2.19. *For $g_1, g_2 \in (1, 4]$, A_k and q_k as defined above, it holds that*

$$|g_1(q_4 + A_5 q_5) + g_3 A_3 q_3| \leq 2^{R_3 + R_4 + R_5 + 2}.$$

Proof. Observe that due to the specific structure of the parts u_3, u_4, u_5 in $\mathcal{U}$ which is

$$\begin{aligned}
u_5 &= b_1 2^{-(n_1-(n_1-n_3))-1} + \cdots + b_{R_5} 2^{-(n_1-((n_1-n_3)-R_5))} \\
u_3 &= b_1 2^{-(n_1-n_3)-1} + \cdots + b_{R_3} 2^{-(n_1-(n_3-R_3))} \\
u_4 &= b_1 2^{-(n_1-R_4)-1} + \cdots + b_{R_4} 2^{-n_1}
\end{aligned}$$

with $b_i \in \{0,1\}$ and the LTD scheme constraints such that $R_5 \leq (n_1 - 2n_3)$, $R_3 \leq \frac{n_3}{2}$ and $R_4 \leq \frac{n_3}{2}$ we can rewrite the sum

$$A_3 q_3^+ + q_4^+ + A_5 q_5^+ = q_6^+ \tag{2.21}$$

where $R_6 := R_3 + R_4 + R_5$ and $q_k^+ \in \{0, \ldots, Q_k - 1, Q_k\}$ for $k \in \{3,4,5,6\}$ and $Q_k := 2^{R_k}$. In particular this means that

$$R_5 + R_4 + R_3 \leq (n_1 - n_3) \tag{2.22}$$

$$R_4 + R_3 \leq n_3, \tag{2.23}$$

establishing two of the inequalities. We can now show that

$$\begin{aligned}
|g_1(q_4 + A_5 q_5) + g_3 A_3 q_3| &\leq |g_1 q_4| + |g_1 A_5 q_5| + |g_3 A_3 q_3| \\
&\leq |g_1||q_4| + |g_1||A_5 q_5| + |g_3||A_3 q_3| \\
&\leq 2^2 (q_4^+ + A_5 q_5^+ + A_3 q_3^+) \\
&= 2^{R_3+R_4+R_5+2},
\end{aligned}$$

where we used (2.21). □

We can further rewrite B using the triangle inequality and in addition use Lemma 2.19 such that

$$\begin{aligned}
&B(u_1, u_2, u_3, u_4, u_5) \\
&= \{|g_2 A_2 q_2 + g_1(A_1 q_1 + q_4 + A_5 q_5) + g_3 A_3 q_3| \leq 2^5\} \\
&\subseteq \{|g_2 A_2 q_2 + g_1 A_1 q_1| \leq 2^5 + |g_1(q_4 + A_5 q_5) + g_3 A_3 q_3|\} \\
&\subseteq \{|g_2 A_2 q_2 + g_1 A_1 q_1| \leq 2^5 + 2^{R_3+R_4+R_5+2}\} \\
&\subseteq \{|g_2 A_2 q_2 + g_1 A_1 q_1| \leq \beta\} := B'(q_2, q_1)
\end{aligned}$$

where $\beta := 2^{R_3+R_4+R_5+6}$. Now we can apply Groshev's theorem. In particular, we need a generalisation of the theorem for an asymmetric and non-asymptotic setting, which was

proven in [NMA13, Lemma 14] and builds on a technique from [Dod07]. In particular we need just the special case of two parameters of the Lemma:

Lemma 2.20. *Let* $\beta \in (0,1]$, $A_2 \in \mathbb{N}$, *and* $Q_1, Q_2 \in \mathbb{N}$. *Define the event*

$$B(q_1,q_2) := \{(g_1,g_2) \in (1,4]^2 : |g_1 q_1 + A_2 g_2 q_2| < \beta\}$$

and set

$$B := \bigcup_{\substack{q_1,q_2 \in \mathbb{Z} \\ q_1,q_2 \neq \mathbf{0}, \\ |q_k| \leq Q_k \forall k}} B(q_1,q_2).$$

Then

$$\mu(B) \leq 1008\beta \left(\min \left\{ Q_2, \frac{Q_1}{A_2} \right\} \right).$$

Now we can continue with the proof of Lemma 2.18. We need to normalize

$$|g_2 A_2 q_2 + g_1 A_1 q_1| < \beta$$

in order to fit Lemma 2.20. We first assume that $A_1 \leq A_2$. Define

$$\begin{aligned} A_1' &:= 1 \\ A_2' &:= \tfrac{A_2}{A_1} = 2^{-n_1+n_2-R_2+R_1} \\ \beta' &:= \tfrac{\beta}{A_1} = 2^{R_1+R_3+R_4+R_5+6-n_1} \end{aligned}$$

Now, observe that we need $\beta' \in (0,1]$ and we therefore have the inequality

$$R_1 + R_3 + R_4 + R_5 \leq n_1 - 6. \tag{2.24}$$

Since we know that $n_1 \geq n_2$, we also know

$$Q_1 = 2^{R_1} \geq 2^{R_1+n_2-n_1} = A_2' Q_2.$$

We therefore have

$$\mu(B') \leq 1008\beta' Q_2.$$

Substituting the definitions yields

$$\mu(B') \leq 1008 \cdot 2^{R_1+R_2+R_2+R_3+R_4+R_5+6-n_1}.$$

Combined with (2.25), this shows that if

$$\begin{aligned} R_1 + R_2 + R_5 + R_4 + R_3 &\leq n_1 - 6 - \log(1008/\delta), \\ R_1 + R_5 + R_4 + R_3 &\leq n_1 - 6, \end{aligned}$$

we have $\mu(B') \leq \delta$. The case for $A_2 \leq A_1$ is done in the same fashion with appropriate index switching. For β' it gives the condition

$$R_2 + R_3 + R_4 + R_5 \leq n_2 - 6, \tag{2.25}$$

which is stronger than (2.24). Furthermore, it yields the bound

$$\mu(B') \leq 1008\beta' \frac{Q_2}{A_1'},$$

which gives again

$$\mu(B') \leq 1008 \cdot 2^{R_1+R_2+R_3+R_4+R_5+6-n_1}.$$

We therefore have that the above equations, together with (2.22) yields

$$\begin{aligned} R_1 + R_2 + R_5 + R_4 + R_3 &\leq n_1 - 6 - \log(1008/\delta), \\ R_2 + R_5 + R_4 + R_3 &\leq n_2 - 6, \\ R_5 + R_4 + R_3 &\leq (n_1 - n_3), \\ R_4 + R_3 &\leq n_3, \end{aligned}$$

which results in $\mu(B') \leq \delta$. This completes the proof of Lemma 2.18 and it can be used to show the following result:

Lemma 2.21. *Let* $\delta \in (0, 1]$ *and* n_1, n_2, $n_i \in \mathbb{N}$, $n_1 \geq n_2 \geq n_i$ *and* $\frac{n_i}{n_1} < \frac{1}{2}$. *Assume* R_{11}^P, R_{11}^C, R_{12}, R_{21}, R_{22}^P $R_{22}^C \in \mathbb{Z}_+$ *satisfy,*

$$\begin{aligned} R_{11}^C + R_{12}^C + R_{21}^C + R_{11}^{P_1} + R_{11}^{P_2} &\leq n_1 - \log\left(\tfrac{c}{\delta}\right) \\ R_{12}^C + R_{21}^C + R_{11}^{P_1} + R_{11}^{P_2} &\leq n_2 - 6 \\ R_{21}^C + R_{11}^{P_1} + R_{11}^{P_2} &\leq (n_1 - n_i) \\ R_{21}^C + R_{11}^{P_2} &\leq n_i \end{aligned}$$

and

$$R_{21}^C + R_{22}^C + R_{11}^C + R_{22}^{P_1} + R_{22}^{P_2} \leq n_1 - \log\left(\tfrac{c}{\delta}\right)$$

$$\begin{aligned} R_{22}^{C} + R_{11}^{C} + R_{22}^{P_1} + R_{22}^{P_2} &\leq n_2 - 6 \\ R_{11}^{C} + R_{22}^{P_1} + R_{22}^{P_2} &\leq (n_1 - n_i) \\ R_{11}^{C} + R_{22}^{P_2} &\leq n_i \end{aligned}$$

where $c := 2016$ *and* R_{ik} *is the rate of the signal* u_{ik}*. Then, the bit allocation of the LTD-IMAC applied to the Gaussian IMAC results in a minimum constellation distance* $d \geq 32$ *at each receiver for all channel gains* ($g_{ik}^{j} \in (1,2]^{2\times 2}$) *except for a set* $B \subset (1,2]^{2\times 2}$ *of Lebesgue measure* $\mu(B) \leq \delta$*.*

□

2.10.5. Verification of Decoding Conditions on LTDM Schemes

We check the cases

$$\begin{aligned} \text{I}: \ \alpha \in [0, \tfrac{1}{2}], \ \text{II}: \ \alpha \in (\tfrac{1}{2}, \tfrac{3}{5}), \ \text{III}: \ \alpha \in [\tfrac{3}{5}, 1] \\ \text{IV}: \ \alpha \in (1, \tfrac{3}{2}], \ \text{V}: \ \alpha \in (\tfrac{3}{2}, \infty) \end{aligned}$$

separately. We restrict the following section on cell 1. The corresponding cases for cell 2 can be checked accordingly with adjusted indices.

Case I.1 ($n_i^{j\neq i} \leq \Delta_i$)**:** In this case, $R_{12}^{c} = \min\{\lceil \frac{1}{2} n_1^2 \rceil, (n_{12}^1 - (n_{11}^1 - n_1^2))^+\} = (n_{12}^1 - (n_{11}^1 - n_1^2))^+ = 0$. This is in accordance with the discussion above. We note that this case is outside of the conditions of the decoding lemma. Here, the bound of the second condition needs to be switched with the bound of the third condition. This means that the second condition is bounded by $n_{k1}^k - n_k^l$, for this particular case. For the first restriction we have:

$$\begin{aligned} &R_{11}^{c} + R_{11}^{p1} + R_{11}^{p2} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \\ &\quad = \lfloor \tfrac{1}{2} n_1^2 \rfloor + \lceil \tfrac{1}{2} n_2^1 \rceil + \lfloor \tfrac{1}{2} n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 \\ &\quad = n_{11} - \lceil \tfrac{1}{2} n_1^2 \rceil \leq n_{11} \end{aligned}$$

The second one gives:

$$\begin{aligned} &R_{11}^{p1} + R_{11}^{p2} + R_{12}^{c} + \max\{R_{21}^{c}, R_{22}^{c}\} \\ &\quad = \lceil \tfrac{1}{2} n_2^1 \rceil + \lfloor \tfrac{1}{2} n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 \\ &\quad = n_{11}^1 - n_1^2. \end{aligned}$$

Case I.2 ($\frac{1}{2}n_i^{j\neq i} < \Delta_i < n_i^{j\neq i}$): Here, $R_{12}^c = \min\{\lceil \frac{1}{2}n_1^2 \rceil, (n_{12}^1 - (n_{11}^1 - n_1^2))^+\} = n_{12}^1 - (n_{11}^1 - n_1^2) > 0$. R^c becomes valuable, and multi-user gain starts increasing.

$$\begin{aligned} &R_{11}^c + R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &\quad = n_{12}^1 - (n_{11}^1 - n_1^2) + \lfloor \tfrac{1}{2}n_1^2 \rfloor + \lceil \tfrac{1}{2}n_2^1 \rceil + \lfloor \tfrac{1}{2}n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 \\ &\quad = n_{12}^1 + \lfloor \tfrac{1}{2}n_1^2 \rfloor \leq n_{12}^1 + \Delta_1 = n_{11}^1. \end{aligned}$$

The next conditions result in:

$$\begin{aligned} &R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + \max\{R_{21}^c, R_{22}^c\} \\ &\quad = n_{12}^1 - (n_{11}^1 - n_1^2) + \lceil \tfrac{1}{2}n_2^1 \rceil + \lfloor \tfrac{1}{2}n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 = n_{12}^1, \end{aligned}$$

which obeys the restriction since $n_{11}^1 - n_1^2 < n_{11}^1 - \Delta_1 = n_{12}^1$.
Case I.3 ($\Delta_i \leq \frac{1}{2}n_i^{j\neq i}$): In this case, $R_{12}^c = \min\{\lceil \frac{1}{2}n_1^2 \rceil, (n_{12}^1 - (n_{11}^1 - n_1^2))^+\} = \lceil \frac{1}{2}n_1^2 \rceil$. R^c is fully valuable, and multi-user gain is at maximum.

$$\begin{aligned} &R_{11}^c + R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &\quad = \lfloor \tfrac{1}{2}n_1^2 \rfloor + \lceil \tfrac{1}{2}n_1^2 \rceil + \lceil \tfrac{1}{2}n_2^1 \rceil + \lfloor \tfrac{1}{2}n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 = n_{11}^1. \end{aligned}$$

The second condition results in

$$\begin{aligned} &R_{11}^{p1} + R_{11}^{p2} + R_{12}^c + \max\{R_{21}^c, R_{22}^c\} = \lceil \tfrac{1}{2}n_1^2 \rceil + \lceil \tfrac{1}{2}n_2^1 \rceil + \lfloor \tfrac{1}{2}n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 \\ &\quad = n_{11}^1 - \lfloor \tfrac{1}{2}n_1^2 \rfloor \end{aligned}$$

which obeys the restriction since we need to re-index $n_{11}^1 - \lfloor \frac{1}{2}n_1^2 \rfloor \leq n_{11}^1 - \Delta_1 = n_{12}^1$. For the last two conditions we have

$$\begin{aligned} &R_{11}^{p1} + R_{11}^{p2} + \max\{R_{22}^c, R_{21}^c\} = \lceil \tfrac{1}{2}n_2^1 \rceil + \lfloor \tfrac{1}{2}n_2^1 \rfloor + n_{11}^1 - n_1^2 - n_2^1 \\ &\quad = n_{11}^1 - n_1^2. \end{aligned}$$

Furthermore,

$$R_{11}^{p1} + \max\{R_{22}^c, R_{21}^c\} = \lceil \tfrac{1}{2}n_2^1 \rceil + \lfloor \tfrac{1}{2}n_2^1 \rfloor = n_2^1.$$

which is applicable to the cases I.1-3.
Case II.1 : The first sub-case is when $n_2 \geq n_i + \lfloor \frac{1}{2}(n_1 - n_i) \rfloor$. Therefore $\lfloor \frac{1}{2}(n_1 - n_i) \rfloor \leq (n_2 - n_i)$ and $R_{k2}^c := \lfloor \frac{1}{2}(n_1 - n_i) \rfloor$. The second direct signal has enough power to provide

the full multi-user gain.

$$\begin{aligned} R_{11}^c + R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} &= 3\left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor + n_i - \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor \\ &\leq n_i + 2(\tfrac{1}{2}(n_1 - n_i)) = n_1. \end{aligned}$$

$$R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 2\left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor + n_i - \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor \leq n_2.$$

$$R_{11}^{p1} + \max\{R_{22}^c, R_{21}^c\} = \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor + n_i - \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor = n_i.$$

Case II.2 : The second sub-case is when $n_2 < n_i + \left\lfloor \frac{1}{2}(n_1 - n_i)\right\rfloor$. Therefore $\left\lfloor \frac{1}{2}(n_1 - n_i)\right\rfloor > (n_2 - n_i)$ and $R_{k2}^c := (n_2 - n_i)$. The weaker user has not enough power to provide the full multi-user gain.

$$\begin{aligned} R_{11}^c + R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} &= 2\left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor + n_i - \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor + (n_2 - n_i) \\ &\leq \tfrac{1}{2}n_1 + n_2 - \tfrac{1}{2}n_i < \tfrac{1}{2}n_1 + n_i + \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor - \tfrac{1}{2}n_i \leq n_1. \end{aligned}$$

$$R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = n_i - \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor + (n_2 - n_i) + \left\lfloor \tfrac{1}{2}(n_1 - n_i)\right\rfloor = n_2.$$

The last condition follows from case II.1.

Case III.A.1 (B.1) : The cases are active for $n_2 > n_1 - \frac{1}{3}n_i$. Therefore, we have $\left\lfloor (n_2 + \frac{2}{3}n_i - n_1)\right\rfloor \geq \left\lfloor \frac{1}{3}n_i\right\rfloor$ and $R_{k2}^c := \left\lfloor \frac{1}{3}n_i\right\rfloor$. Full multi-user gain can be achieved.

$$R_{11}^c + R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 3\left\lfloor \tfrac{1}{3}n_i\right\rfloor + (n_1 - n_i) \leq n_1.$$

$$R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 2\left\lfloor \tfrac{1}{3}n_i\right\rfloor + (n_1 - n_i) \leq n_1 - \tfrac{1}{3}n_i < n_2.$$

$$R_{11}^{p1} + \max\{R_{22}^c, R_{21}^c\} = \left\lfloor \tfrac{1}{3}n_i\right\rfloor + (n_1 - n_i) \leq n_1 - \tfrac{2}{3}n_i \overset{\left(\frac{3}{5} \leq \alpha\right)}{\leq} n_i.$$

Note that case III.C.1 follows on the same lines for $n_2 \geq n_1 - \frac{2}{3}n_i$ by careful evaluation of the decoding bounds, and re-indexing for $n_2 \leq n_i$.

Case III.B.2 : The second sub-case of B is when $n_i < n_2 \leq n_1 - \frac{1}{3}n_i$. Therefore $R_{k1}^c := \left\lfloor \frac{1}{3}n_i\right\rfloor$ and $R_{k2}^c := \left\lfloor ((n_2 - n_i)^+ + \frac{5}{3}n_i - n_1)^+\right\rfloor$.

$$R_{11}^c + R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \leq \tfrac{2}{3}n_i + (n_1 - n_i) + n_2 - n_i + \tfrac{5}{3}n_i - n_1$$

$$\leq \tfrac{1}{3}n_i + n_2 < \tfrac{1}{3}n_i + n_1 - \tfrac{1}{3}n_i = n_1.$$

$$R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \leq \tfrac{1}{3}n_i + (n_1 - n_i) + n_2 - n_i + \tfrac{5}{3}n_i - n_1 = n_2.$$

The last case follows from III.B.1.

Case III.B.3 : The third sub-case is for $n_i \geq n_2 > \frac{2}{3}n_i$ and $\frac{2}{3} < \alpha \leq \frac{3}{4}$. Therefore $R_{k1}^{c} := \lfloor \frac{1}{3}n_i \rfloor$ and $R_{k2}^{c} := \lfloor (\frac{5}{3}n_i - n_1)^+ \rfloor$. We have that

$$R_{11}^{c} + R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \leq \tfrac{2}{3}n_i + (n_1 - n_i) + \tfrac{5}{3}n_i - n_1 = \tfrac{4}{3}n_i \overset{\alpha \leq \frac{3}{4}}{\leq} n_1.$$

$$R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \leq \tfrac{1}{3}n_i + (n_1 - n_i) + \tfrac{5}{3}n_i - n_1 = n_i.$$

The last condition follows from B.1 by re-indexing (switching n_2 with n_i).

Case III.B.4 : The last sub-case of III.B is for $\frac{2}{3}n_i \geq n_2 > n_1 - n_i$ and again $\frac{2}{3} < \alpha \leq \frac{3}{4}$. Therefore $R_{k1}^{c} := \lfloor \frac{1}{3}n_i \rfloor + \min\{ \lfloor (\frac{2}{3}n_i - n_2)^+ \rfloor , \lfloor (n_1 - \frac{4}{3}n_i)^+ + \frac{1}{2}(2n_i - n_2 - n_1)^+ \rfloor \}$ and $R_{k2}^{c} := (n_2 - (n_1 - n_i))^+$. For $n_2 \geq 2n_i - n_1$ we have $R_{k1}^{c} := \lfloor \frac{1}{3}n_i \rfloor + \lfloor (\frac{2}{3}n_i - n_2)^+ \rfloor$ which results in

$$\begin{aligned} &R_{11}^{c} + R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \\ &\quad \leq \tfrac{2}{3}n_i + (\tfrac{4}{3}n_i - 2n_2)^+ + (n_1 - n_i) + (n_2 - (n_1 - n_i))^+ = 2n_i - n_2 \leq n_1. \end{aligned}$$

$$\begin{aligned} &R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \\ &\quad \leq \tfrac{1}{3}n_i + (\tfrac{2}{3}n_i - n_2)^+ + (n_1 - n_i) + (n_2 - (n_1 - n_i))^+ = n_i. \end{aligned}$$

For $n_2 < 2n_i - n_1$ we have $R_{k1}^{c} := \lfloor \frac{1}{3}n_i \rfloor + \lfloor (n_1 - \frac{4}{3}n_i)^+ + \frac{1}{2}(2n_i - n_2 - n_1)^+ \rfloor$ which results in

$$\begin{aligned} &R_{11}^{c} + R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \\ &\quad \leq \tfrac{2}{3}n_i + 2(n_1 - \tfrac{4}{3}n_i)^+ + (2n_i - n_2 - n_1)^+ + (n_1 - n_i) + (n_2 - (n_1 - n_i))^+ = n_1. \end{aligned}$$

$$\begin{aligned} &R_{11}^{p1} + R_{12}^{c} + \max\{R_{22}^{c}, R_{21}^{c}\} \\ &\quad \leq \tfrac{1}{3}n_i + (n_1 - \tfrac{4}{3}n_i)^+ + \tfrac{1}{2}(2n_i - n_2 - n_1)^+ + (n_1 - n_i) + (n_2 - (n_1 - n_i))^+ \\ &\quad = \tfrac{n_2}{2} + \tfrac{n_1}{2} < n_i. \end{aligned}$$

The last condition follows from III.B.1.

Case III.A.2 : The second sub-case is when $n_i \leq n_2 < n_1 - \frac{1}{3}n_i$ and $\alpha < \frac{2}{3}$. Therefore $\left\lfloor (n_2 + \frac{2}{3}n_i - n_1) \right\rfloor < \left\lfloor \frac{1}{3}n_i \right\rfloor$ and $R_{k2}^c := \left\lfloor (n_2 + \frac{2}{3}n_i - n_1) \right\rfloor$. The weaker user has not enough power to provide the full multi-user gain.

$$\begin{aligned} &R_{11}^c + R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &\quad = 2\left\lfloor \tfrac{1}{3}n_i \right\rfloor + (n_1 - n_i) + \left\lfloor (n_2 + \tfrac{2}{3}n_i - n_1) \right\rfloor \\ &\quad \leq \tfrac{2}{3}n_i + (n_1 - n_i) + (n_2 + \tfrac{2}{3}n_i - n_1) = \tfrac{1}{3}n_i + n_2 < n_1. \end{aligned}$$

$$\begin{aligned} &R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &\quad = \left\lfloor \tfrac{1}{3}n_i \right\rfloor + (n_1 - n_i) + \left\lfloor (n_2 + \tfrac{2}{3}n_i - n_1) \right\rfloor \leq n_2. \end{aligned}$$

The last condition follows from case III.A.1.

Case III.C.2 : This sub-case is when $n_1 - n_i \leq n_2 < n_1 - \frac{2}{3}n_i$ and $\alpha > \frac{3}{4}$. Therefore $(n_2 - (n_1 - n_i))^+ < \left\lfloor \frac{1}{3}n_i \right\rfloor$ and $R_{k2}^c := n_2 - (n_1 - n_i)$. The weaker user has not enough power to provide the full multi-user gain.

$$\begin{aligned} &R_{11}^c + R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &\quad = 2\left\lfloor \tfrac{1}{3}n_i \right\rfloor + (n_1 - n_i) + n_2 - (n_1 - n_i) + [n_1 - n_2 - \tfrac{2}{3}n_i] \leq n_1. \end{aligned}$$

$$\begin{aligned} &R_{11}^{p1} + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &= \left\lfloor \tfrac{1}{3}n_i \right\rfloor + (n_1 - n_i) + n_2 - (n_1 - n_i) + \tfrac{1}{2}[n_1 - n_2 - \tfrac{2}{3}n_i] \\ &\leq \tfrac{n_1}{2} + \tfrac{n_2}{2} < \tfrac{1}{2}(n_1 - \tfrac{2}{3}n_i) + \tfrac{n_1}{2} \leq n_i. \end{aligned}$$

The last condition follows from case III.C.1.

Case IV.1 : The first sub-case is when $n_2 > \frac{1}{3}n_i$. Therefore $R_{k2}^c := \left\lfloor \frac{1}{3}n_i \right\rfloor$. Since we are in the range $\alpha \geq 1$, the private part vanishes. Furthermore, full multi-user gain can be achieved.

$$R_{11}^c + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 3\left\lfloor \tfrac{1}{3}n_i \right\rfloor \leq n_i.$$

$$R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 2\left\lfloor \tfrac{1}{3}n_i \right\rfloor \leq \tfrac{2}{3}n_i \overset{\left(\alpha \leq \frac{3}{2}\right)}{\leq} n_1.$$

Case IV.2 : The second sub-case is when $n_2 \leq \frac{1}{3}n_i$. Therefore $R_{k2}^c := n_2$, and the second term in $R_{k1}^c := \lfloor \frac{1}{3}n_i \rfloor + \lfloor \frac{1}{2}(\frac{1}{3}n_i - n_2)^+ \rfloor$ gets activated. The weaker user has not enough power to provide the full multi-user gain.

$$R_{11}^c + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 2(\lfloor \tfrac{1}{3}n_i \rfloor + \lfloor \tfrac{1}{2}(\tfrac{1}{3}n_i - n_2)^+ \rfloor) + n_2 \leq n_i.$$

$$\begin{aligned} R_{12}^c + \max\{R_{22}^c, R_{21}^c\} &= \lfloor \tfrac{1}{3}n_i \rfloor + \lfloor \tfrac{1}{2}(\tfrac{1}{3}n_i - n_2)^+ \rfloor + n_2 \\ &\leq \tfrac{1}{2}n_i - \tfrac{1}{2}n_2 \overset{\left(\alpha \leq \frac{3}{2}\right)}{\leq} \tfrac{3}{4}n_1 - \tfrac{1}{2}n_2 < n_1. \end{aligned}$$

Case V.1.1 : The first sub-case is when $n_2 \geq \frac{1}{2}n_1$. Therefore $R_{k2}^c := \lfloor \frac{1}{2}n_1 \rfloor$. Full multi-user gain can be achieved.

$$R_{11}^c + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 3\lfloor \tfrac{1}{2}n_1 \rfloor \overset{\alpha \geq \frac{3}{2}}{\leq} n_i.$$

$$R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = 2\lfloor \tfrac{1}{2}n_1 \rfloor \leq n_1.$$

Case V.1.2 : The second sub-case is when $n_2 < \frac{1}{2}n_1$ but $2n_1 < n_i + n_2$. Therefore $R_{k2}^c := n_2$ and $R_{k1}^c := n_1 - n_2$. Full multi-user gain can be achieved.

$$R_{11}^c + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = n_2 + 2(n_1 - n_2) = 2n_1 - n_2 < n_i.$$

$$R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = n_1.$$

Case V.2 : The third sub-case is when $n_2 < \frac{1}{2}n_1$ and $2n_1 \geq n_i + n_2$. Therefore $R_{k2}^c := n_2$ and $R_{k1}^c := \lfloor \frac{1}{2}n_i - \frac{1}{2}n_2 \rfloor$. The weaker user has not enough power to provide the full multi-user gain.

$$R_{11}^c + R_{12}^c + \max\{R_{22}^c, R_{21}^c\} = n_2 + 2(\lfloor \tfrac{1}{2}n_i - \tfrac{1}{2}n_2 \rfloor) \leq n_i.$$

$$\begin{aligned} &R_{12}^c + \max\{R_{22}^c, R_{21}^c\} \\ &\quad = n_2 + \lfloor \tfrac{1}{2}n_i - \tfrac{1}{2}n_2 \rfloor \leq \tfrac{1}{2}n_i + \tfrac{1}{2}n_2 \leq \tfrac{1}{2}n_i + \tfrac{1}{2}(2n_1 - n_i) = n_1. \end{aligned}$$

3. The Multiple Access Wiretap Channel

3.1. Introduction

The wiretap channel was first proposed by Wyner in [Wyn75], and solved in its degraded version. This result was later extended to the general wiretap channel by Csiszar and Körner in [CK78]. Moreover, the Gaussian equivalent was studied by Leung-Yan-Cheon and Hellman in [LYCH78]. The wiretap channel and its modified version served as an archetypical channel for physical-layer security investigations. However, in recent years, the network nature of communication, i.e. support of multiple users, became increasingly important. A straightforward extension of the wiretap channel to multiple users was done in [TY08a], where the Gaussian multiple access wiretap channel (G-MAC-WT) was introduced. A general solution for the secure capacity of this multi-user wiretap set-up was out of reach and investigations focused on the secure degrees of freedom (s.d.of.) of these networks. Degrees of freedom are used to gain insights into the scaling behaviour of multi-user channels. They measure the capacity of the network, normalized by the single-link capacity, as power goes to infinity. This also means that the d.o.f. provide an asymptotic view on the problem at hand. This simplifies the analysis and enables asymptotic solutions of channel models where no finite power capacity results could be found. An example of a technique, which yields d.o.f. results, is real interference alignment. It uses integer lattice transmit constellations which are scaled such that alignment can be achieved. The intended messages are recovered by minimum-distance decoding and the error probability is bounded by usage of the Khintchine-Groshev theorem of Diophantine approximation theory. The disadvantage of the method is that these results only hold for almost all channel gains. This is unsatisfying for secrecy purposes since it leaves an infinite amount of cases where the schemes do not work, e.g. rational channel gains. Moreover, secrecy should not depend on the accuracy of channel measurements. Real interference alignment is part of a broader class of interference alignment strategies. Interference alignment (IA) was introduced in [CJ08] and [MAMK08], among others, and its main idea is to design signals such that the caused interference overlaps(aligns) and therefore uses fewer signal dimensions. The resulting interference-free signal dimensions can be used for communication. IA methods can be divided into two categories, namely the vector-space alignment approach

and the signal-scale alignment approach [NMA13]. The former uses the classical signalling dimensions time, frequency and multiple-antennas for the alignment, while the latter uses the signal strength for alignment. Real interference alignment and signal-strength deterministic models are examples for signal-scale alignment. Signal-strength deterministic models are based on an approximation of the Gaussian channel. An example for such an approximation is the linear deterministic model (LDM), introduced by Avestimehr et al. in [ADT07]. It is based on a binary expansion of the transmit signal, and an approximation of the channel gain to powers of two. The resulting binary expansion gets truncated at the noise level which yields a noise-free binary signal vector and makes the model deterministic. It has been shown that various Gaussian channels (i.e. [BT08], [BPT10], [SB11], [FW17c]) can be approximated by the LDM such that the deterministic capacity is within a constant bit-gap of the Gaussian channel. Moreover, layered lattice coding schemes can be used to transfer the achievable scheme or rather the level structure to the Gaussian model, see for example [SJV$^+$08], [NCL10], [SB11], [BPT10] and [NCNC16].

Previous work and Contributions: Previous work on the wiretap channel in multi-user settings mainly utilized the real IA approach in addition to cooperative jamming, introduced in [TY08b]. The idea of using IA in a secrecy context is to cooperatively jam the eavesdropper, while aligning the jamming signal in a small subspace at the legitimate receiver. This resulted in a sum s.d.o.f characterization of $\frac{K(K-1)}{K(K-1)+1}$ for the K-user case in [XU14]. The idea is that the users can allocate a small part of the signalling dimensions with uniformly distributed random bits. Those random bits are sent such that they occupy a small space at the legitimate receiver, while overlapping with the signals at the eavesdropper. A specialized model is the wiretap channel with a helper. This model consists of the standard wiretap channel model, with a second independent user, whose only purpose is to jam the eavesdropper. The authors in [HY14] showed that using structured codes provides strictly positive s.d.o.f for this model. In [XU12] and [XU13], the real IA approach was used on the wiretap channel with a helper (with and without CSIT, respectively) to investigate the s.d.o.f, therefore achieve results for the infinite SNR regime. Another branch of recent work [BSP15] approached the problem, using a compute-and-forward decoding strategy, which leads to results for the finite regime that are optimal in a s.d.o.f sense. The next step is to transition from the s.d.o.f. results, to a secure constant-gap capacity result. We take a different approach and study the linear deterministic approximations of both models to gain insights leading to constant-gap capacity approximations. This approach has been used for example for wiretap channels in [EHLGS12], [CVS14], for relay networks [PDT09] and for IC channels [MM13], [VAS16]. It was also recently used in [LZK17] for an s.d.o.f. analysis of the Gaussian diamond-wiretap channel, which is a multi-hop version of the G-MAC-WT. We show that the previously known $\frac{1}{2}$ d.o.f. result of the wiretap

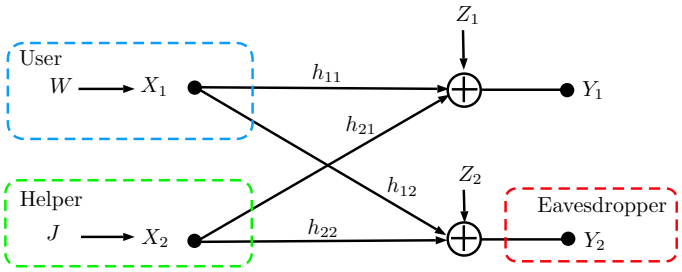

Figure 3.1.: Gaussian wiretap channel with one helper.

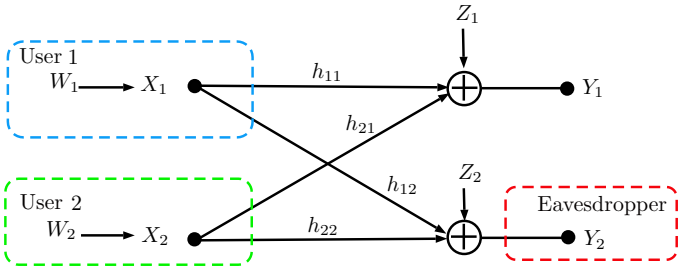

Figure 3.2.: The Gaussian multiple access Wiretap channel.

channel with a helper [XU14] can be extended to a general (asymmetric) and finite but high-SNR regime. Moreover, we develop a converse proof which shows a constant-gap for certain channel gain values. The converse proof converges to the d.o.f bound for vanishing channel gain differences. Furthermore, we use the same alignment methods to present an achievable scheme for the linear deterministic MAC-WT (LD-MAC-WT) and show that here, a rate can be achieved, which converges to $\frac{2}{3}$ d.o.f., for vanishing receive signal power differences. We also extend the converse proof of [XU14], which is partly based on [Khi11], for the MAC-WT towards general receive signal powers, to match our achievable scheme for certain channel parameters. Moreover, we show that both achievable schemes can be translated to the Gaussian channel models, by using layered lattice codes to imitate bit-levels. We also combine previous techniques with new novel techniques to translate the results of both converse proofs to the Gaussian channel.

3.2. System Model

The Gaussian multiple access wiretap channel (G-MAC-WT) and the Gaussian wiretap channel with one helper (G-WT-H) are defined as a system consisting of 2 transmitters and 2 receivers, as shown in Fig. 3.1 and Fig. 3.2, where $X_1, X_2 \in \mathbb{R}$ are the channel inputs of both users, communicating with the legitimate receiver with channel output Y_1 or jamming the eavesdropper, with channel output Y_2. The channel itself is modelled with

additive white Gaussian noise, $Z_1, Z_2 \sim \mathcal{N}(0,1)$. Therefore, the system equations can be written as

$$Y_1 = h_{11}X_1 + h_{21}X_2 + Z_1, \tag{3.0a}$$

$$Y_2 = h_{22}X_2 + h_{12}X_1 + Z_2, \tag{3.0b}$$

where the channel inputs satisfy an average transmit power constraint $E\{X_i^2\} \leq P_i$ for each i. The channel gains from user i to receiver k are denoted by h_{ik}. Let $|h_{11}|^2 P_1 = \mathrm{SNR}_1$ and $|h_{21}|^2 P_2 = \mathrm{SNR}_2$ represent the received average power at Y_1 of both direct signals. We assume that both signals are received at Y_2 with the same average power and therefore $h_{12} = h_{22} = h_E$ and $P_1 = P_2 = P$ which gives $|h_E|^2 P = \mathrm{SNR}_E$.[1] We introduce the two parameters β_1 and β_2, which connect the SNR ratios with $\mathrm{SNR}_2 = \mathrm{SNR}_1^{\beta_1}$ and $\mathrm{SNR}_E = \mathrm{SNR}_1^{\beta_2}$. The difference between the G-MAC-WT and G-WT-H is, that in case of the G-WT-H, user 2 is just helping user 1 by independently jamming both receivers to achieve a secure communication. In the case of the G-MAC-WT model, both users want to transmit information to Y_1 and are able to use jamming.

G-WT-H

A $(2^{nR}, n)$ code will consist of an encoding and a decoding function. The encoder assigns a codeword $x_1^n(w)$ to each message w, where W is uniformly distributed over the set $[1 : 2^{nR}]$, and the associated decoder assigns an estimate $\hat{w} \in [1 : 2^{nR}]$ to each observation of Y_1^n. A secure rate R is said to be achievable if there exist a sequence of $(2^{nR}, n)$ codes which satisfy a probability of error constraint $P_e^{(n)} = P(\hat{W} \neq W) \leq \epsilon$ as well as a secrecy constraint

$$\tfrac{1}{n} H(W|Y_2^n) \geq \tfrac{1}{n} H(W) - \epsilon, \tag{3.1}$$

which gives $I(W; Y_2^n) \leq \epsilon n$ where $\epsilon \to 0$ for $n \to \infty$. A message W is therefore information-theoretically secure if the eavesdropper cannot reconstruct it from the channel observation Y_2^n. This means that the uncertainty of the message is almost equal to its entropy, given the channel observation.

G-MAC-WT

A $(2^{nR_1}, 2^{nR_2}, n)$ code for the multiple access wiretap channel will consist of a message pair (W_1, W_2) uniformly distributed over the message set $[1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ with a decoding and two randomized encoding functions. Encoder 1 assigns a codeword $X_1^n(w_1)$

[1] This will reduce the number of cases and therefore simplify the analysis. However, the following techniques also work without this assumption. See also remark 3.

to each message $w_1 \in [1 : 2^{nR_1}]$, while the encoder 2 assigns a codeword $X_2^n(w_2)$ to each message $w_2 \in [1 : 2^{nR_2}]$. The decoder assigns an estimate $(\hat{w}_1, \hat{w}_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ to each observation of Y_1^n. A secure rate pair (R_1, R_2) is said to be achievable if there exist a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes, which satisfy a reliability constraint, i.e. probability of error such that: $P_e^{(n)} = P[(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)] \leq \epsilon$ and a security constraint for both messages W_1, W_2:

$$\tfrac{1}{n} H(W_1, W_2 | Y_2^n) \geq \tfrac{1}{n} H(W_1, W_2) - \epsilon,$$

which gives $I(W_1, W_2; Y_2^n) \leq \epsilon n$, where $\epsilon \to 0$ for $n \to \infty$. In particular, for the G-MAC-WT model, we are interested in the secure *sum*-rate $R_\Sigma := R_1 + R_2$.

3.3. The Linear Deterministic Model System

3.3.1. LD Wiretap with a Helper and LD-MAC-WT

As simplification, we will investigate the corresponding linear deterministic model (LDM) of the system models as an intermediate step. The LDM models the signals of the channel as bit-vectors $\mathbf{x}$, which is achieved by a binary expansion of the input signal X. We refer the reader to Section 1.4.1, for an introduction to this model. The model can be written as

$$\mathbf{Y}_1 = \mathbf{S}^{q-n_{11}} \mathbf{X}_1' \oplus \mathbf{S}^{q-n_{21}} \mathbf{X}_2', \tag{3.1a}$$

$$\mathbf{Y}_2 = \mathbf{S}^{q-n_{22}} \mathbf{X}_2' \oplus \mathbf{S}^{q-n_{12}} \mathbf{X}_1', \tag{3.1b}$$

where $q := \max\{n_{11}, n_{12}, n_{21}, n_{22}\}$. For ease of notation, we denote $\mathbf{X}_1 = \mathbf{S}^{q-n_{11}} \mathbf{X}_1'$ and $\mathbf{X}_2 = \mathbf{S}^{q-n_{21}} \mathbf{X}_2'$. Furthermore, we denote $\mathbf{S}^{q-n_{22}} \mathbf{X}_2'$ and $\mathbf{S}^{q-n_{12}} \mathbf{X}_1'$ by $\bar{\mathbf{X}}_2$ and $\bar{\mathbf{X}}_1$, respectively. We also include the assumption on the symmetry in the channel gains at the eavesdropper, which leads to $n_{22} = n_{12} =: n_E$, and denote $|n_1 - n_2| =: n_\Delta$ with $n_{11} =: n_1$ and $n_{21} =: n_2$. We can therefore rewrite the deterministic channel model as

$$\mathbf{Y}_1 = \mathbf{S}^{q-n_1} \mathbf{X}_1' \oplus \mathbf{S}^{q-n_2} \mathbf{X}_2' = \mathbf{X}_1 \oplus \mathbf{X}_2, \tag{3.1c}$$

$$\mathbf{Y}_2 = \mathbf{S}^{q-n_E} \mathbf{X}_2' \oplus \mathbf{S}^{q-n_E} \mathbf{X}_1' = \bar{\mathbf{X}}_2 \oplus \bar{\mathbf{X}}_1. \tag{3.1d}$$

The resulting received bit-vectors of the channel model can be illustrated as shown in Fig. 3.3. There, one can see that for example the two bit-vectors $\mathbf{X}_1$ and $\mathbf{X}_2$ are received at $\mathbf{Y}_1$ with n_1 and n_2 bit-levels, respectively. The highest bit is at the top of the boxes, while the lowest bit is just above the noise level. All schemes rely on a partition of the received signal of the legitimate receiver into a common ($\mathbf{Y}_{1,c}$) and a private ($\mathbf{Y}_{1,p}$) part.

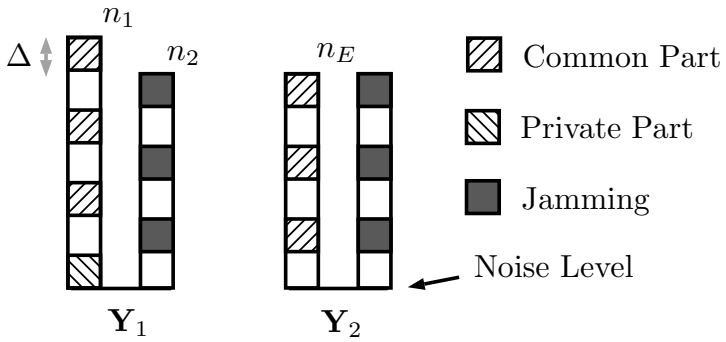

Figure 3.3.: The Gaussian wiretap channel with a helper in the linear deterministic model. The helper utilizes jamming, such that all used signal parts align with the jamming at the attacker (Y_2).

The common bits are the top

$$n_c := \min\{n_E + n_\Delta, \max\{n_1, n_2\}\} \tag{3.2}$$

bits of $\mathbf{Y}_1$. And the private part consists of the bottom

$$n_p := (\max\{n_1, n_2\} - n_c)^+$$

bits of $\mathbf{Y}_1$. We note that due to the bit-level shift, the last n_Δ bits of $\mathbf{X}_1$ in $\mathbf{Y}_{1,c}$ are actually private, see Remark 3.5 and Fig. 3.3. To specify a particular range of elements in a bit-level vector we use the notation $\mathbf{a}_{[i:j]}$ to indicate that $\mathbf{a}$ is restricted to the bit-levels i to j. Bit-levels are counted from top, most significant bit in the expansion, to bottom. If $i = 1$, it will be omitted $\mathbf{a}_{[:j]}$, the same for $j = n$ $\mathbf{a}_{[i:]}$. We define the modulo operation as $a \bmod n := a - \lfloor \frac{a}{n} \rfloor n$.

Remark 3.1. The assumption that $n_{22} = n_{12} = n_E$, i.e. the eavesdropper receives the signals with equal strength, does not influence the achievable secrecy sum-rate. Consider a channel with $n_{22} \neq n_{12}$, for example $n_{22} > n_{12}$. The part of $\mathbf{x}_2'$ which is received above n_{12} at the eavesdropper, $\bar{\mathbf{x}}_{2,[:n_{22}-n_{12}]}$, cannot be utilized since it cannot be jammed. One can therefore achieve the same rate by ignoring the top $n_{22} - n_{12}$ bits of $\mathbf{x}_2'$. The same argument holds for $n_{12} > n_{22}$.

3.3.2. Achievable Scheme for the Wiretap Channel with a Helper

We partition the received signal of the legitimate receiver into a common ($\mathbf{y}_{1,c}$) and a private ($\mathbf{y}_{1,p}$) part. Note that we need to differentiate between the cases that $n_1 \geq n_2$ and $n_1 < n_2$, since the user and the helper have different roles and those cases therefore lead

to different schemes. The main idea is to deploy a jamming scheme such that the jamming signal parts of the helper overlap (align) with the used signal parts of the user at $\mathbf{y}_2$, while minimizing the overlap at the legitimate receiver $\mathbf{y}_1$. This leads to the following result:

Theorem 3.2. *An achievable secrecy rate of the linear deterministic wiretap channel with a helper is*

$$R_{ach} = n_p + \left\lfloor \frac{n_c}{2n_\Delta} \right\rfloor n_\Delta + Q$$

where

$$Q = \begin{cases} n_Q & \text{for } n_Q < n_\Delta, n_1 \geq n_2 \\ n_\Delta & \text{for } n_Q \geq n_\Delta, n_1 \geq n_2 \\ 0 & \text{for } n_Q < n_\Delta, n_1 < n_2 \\ n_Q - n_\Delta & \text{for } n_Q \geq n_\Delta, n_1 < n_2 \end{cases} \tag{3.3}$$

with $n_Q = n_c \bmod 2n_\Delta$.

Proof. **Case 1** ($n_1 \geq n_2$)

We denote the part of $\mathbf{x}_1$ and $\mathbf{x}_2$ in $\mathbf{y}_{1,c}$ by $\mathbf{x}_{1,c}$ and $\mathbf{x}_{2,c}$, respectively. Moreover, we partition these common parts of the signals into $2n_\Delta$-bits partitions. We now utilize the first n_Δ bits of every *full* partition in $\mathbf{x}_{1,c}$ for messages and leave the remainder free. And for $\mathbf{x}_{2,c}$ we utilize the first n_Δ-bits of every partition for jamming, while the rest is free. After partitioning, $\mathbf{y}_{1,c}$ has a remainder part with

$$n_Q = n_c \bmod 2n_\Delta \text{ bits.} \tag{3.4}$$

bit-levels. The user signal in this remainder part follows the same rules as before, while the helper lets the first n_Δ bits free and only utilizes the bits afterwards for jamming, until we have filled all n_Q bits. The private part $\mathbf{y}_{1,p}$ can be used completely by the user, and all of $\mathbf{x}_1$ in this part can be used for messaging. The total achievable rate is the private rate $r_p = n_p$ plus the common rate

$$r_c = \frac{1}{2}\left(\left\lfloor \frac{n_c}{2n_\Delta} \right\rfloor 2n_\Delta \right) + Q,$$

where Q is defined as in the theorem. The common rate follows from the fact, that we utilize half of the bits of all $2n_\Delta$ partitions, along with a remainder part Q. In the remainder, we utilize every bit, as long as n_Q is smaller than n_Δ. If n_Q is larger than n_Δ, we only utilize the first n_Δ bits.

Case 2 ($n_1 < n_2$)

We use the same strategy as before, except for the remainder part n_Q (3.4) of $\mathbf{y}_{1,c}$. In the remainder part, the first n_Δ bits of the user are left free, and all bits afterwards are used for messaging, while the helper only jams the first n_Δ bits. The strategy is, therefore, the opposite as before. This yields a different Q-term, where for $n_Q < n_\Delta$ no rate is achieved, and for $n_Q \geq n_\Delta$ one can use $n_Q - n_\Delta$ bits for messaging.

We note that the secrecy is provided by the (Crypto-) lemma 3.3 and the fact that we use binary addition on each level as well as jamming signals chosen such that each bit is Bern($\frac{1}{2}$) distributed. And we therefore have that $I(\mathbf{x}_1^n; \mathbf{y}_2^n) = 0$. □

Lemma 3.3 (Crypto-Lemma, [FJ04]). *Let G be a compact abelian group with group operation $+$, and let $Y = X + N$, where X and N are random variables over G and N is independent of X and uniform over G. Then Y is independent of X and uniform over G.*

3.3.3. Achievable Scheme for the LD-MAC-WT

We use the same common and private part definitions as in the LD-WT with a helper case. However, there are some important differences. Note that the channel is symmetrical, i.e. both users can send messages and jam and we can therefore assume w.l.o.g that $n_1 \geq n_2$. We can show the following result:

Theorem 3.4. *An achievable secrecy sum-rate R_Σ of the linear deterministic multiple access wiretap channel with symmetric channel gains at the eavesdropper is*

$$R_\Sigma = \lfloor \tfrac{n_c}{3n_\Delta} \rfloor 2n_\Delta + n_p + Q.$$

where $n_c = \min\{n_E + n_\Delta, n_1\}$, $n_p = n_1 - n_c$ and

$$Q = \begin{cases} q & \text{for } n_Q < n_\Delta \\ n_\Delta & \text{for } 2n_\Delta > n_Q \geq n_\Delta \\ n_\Delta + q & \text{for } n_Q \geq 2n_\Delta, \end{cases}$$

with $n_Q = n_c \bmod 3n_\Delta$ and $q = n_Q \bmod n_\Delta$.

Proof. First of all, we look at the case that $n_2 \geq n_E$. Our strategy is the same as before, i.e. to deploy a cooperative jamming scheme such that minimal jamming is done to $\mathbf{y}_{1,c}$, while maximal jamming is received at $\mathbf{y}_2$. We partition the common signals, $\mathbf{x}_{1,c}$ and $\mathbf{x}_{2,c}$, into $3n_\Delta$-bit parts and partition these parts again into n_Δ-bit parts. For $\mathbf{x}_{1,c}$, in every

$3n_\Delta$-bit part we use the first n_Δ bits for the message and the next n_Δ bits for jamming, while the last n_Δ bits will not be used. For $\mathbf{x}_{2,c}$, in every $3n_\Delta$-bit part, the first n_Δ bits will be used for jamming. The next n_Δ bits will be used for the message and the last n_Δ bits left free. There will be a remainder part with

$$n_Q = n_c \bmod 3n_\Delta \text{ bits.}$$

The remainder part follows the same design rules as the $3n_\Delta$ parts, except that $\mathbf{x}_{2,c}$ leaves the first n_Δ bits free, then uses jamming on the next n_Δ bits and utilizes the last n_Δ bits for messaging, until n_Q bits are allocated. The scheme is designed such that the jamming parts of $\mathbf{x}_{1,c}$ and $\mathbf{x}_{2,c}$ overlap at $\mathbf{y}_{1,c}$, while the message parts of one signal overlap with the non-used part of the other signal. However, due to the signal strength difference n_Δ, the jamming parts overlap with the messages at $\mathbf{y}_2$, see Fig. 3.4. Secure communication is, therefore, provided by the Crypto-lemma, as long as we use a Bern($\frac{1}{2}$) distribution for the jamming bits. The whole private part can be used for messaging and its sum-rate is therefore $r_p = n_p$. The achievable secure rate for the common part consists of the rate for the $3n_\Delta$ partitions and the remainder part. It can be seen that every $3n_\Delta$-part of $\mathbf{y}_{1,c}$ allocates $2n_\Delta$ bits for the messages. This results in the common secrecy rate

$$r_c = (\lfloor \tfrac{n_c}{3n_\Delta} \rfloor 3n_\Delta)\tfrac{2}{3} + Q,$$

where Q specifies the rate part of the remainder term. In the remainder part we allocate all remaining bits as message bits, as long as $n_Q < n_\Delta$. For $2n_\Delta > n_Q \geq n_\Delta$, we allocate the first n_Δ bits of n_Q for the message. And for $n_Q \geq 2n_\Delta$, we allocate the first n_Δ bits as well as the last q bits, where q is defined as

$$q = n_Q \bmod n_\Delta.$$

This results in

$$Q = \begin{cases} q & \text{for } n_Q < n_\Delta \\ n_\Delta & \text{for } 2n_\Delta > n_Q \geq n_\Delta \\ n_\Delta + q & \text{for } n_Q \geq 2n_\Delta. \end{cases}$$

Together with the private rate term, we achieve

$$R = \tfrac{2}{3}(\lfloor \tfrac{n_c}{3n_\Delta} \rfloor 3n_\Delta) + n_p + Q.$$

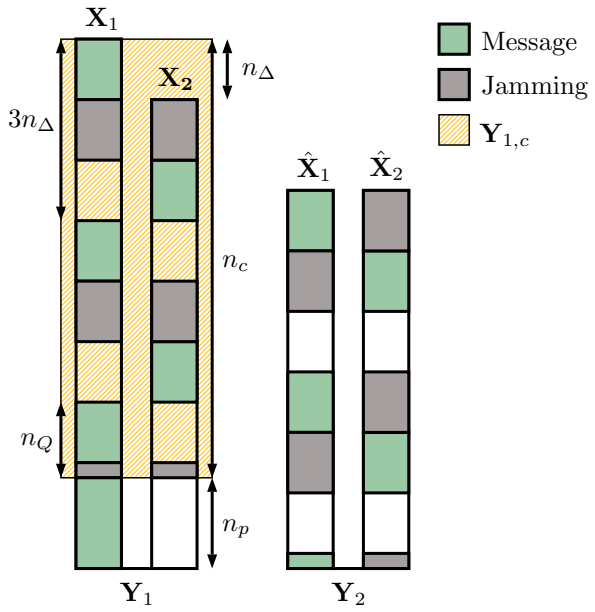

Figure 3.4.: Illustration of the achievable scheme. The private part $\mathbf{y}_{1,p}$ can be used freely and is, in this case, allocated by User 1. The common part $\mathbf{y}_{1,c}$ uses our alignment strategy. The strategy exploits the channel gain difference between both signals, to minimize the effect of jamming at the receiver $\mathbf{y}_1$, while jamming all signal parts at the eavesdropper $\mathbf{y}_2$.

For $n_2 \geq n_E$ the achievable scheme is the same, except that we do not have a private part. We therefore have an achievable rate of

$$R = \tfrac{2}{3}(\lfloor \tfrac{n_c}{3n_\Delta} \rfloor 3n_\Delta) + Q,$$

which completes the proof. □

Remark 3.5. The bit level shift between $\mathbf{y}_1$ and $\mathbf{y}_2$ of n_Δ bits makes it impossible to divide $\mathbf{y}_1$ in exclusively private and common parts. In our division, the bottom n_Δ bits of $\mathbf{x}_{1,c}$ are only received at $\mathbf{y}_1$ and therefore private. Hence, the common rate r_c is not purely made of common signal parts. Nevertheless, our choice of division reaches the upper bound and fits into the scheme.

Remark 3.6. Our scheme relies on the signal strength difference between both users. Our scheme would not work, if $n_1 = n_2$, while having equal channel gains at the eavesdropper. In that case we would not have any signal strength diversity to exploit which results in a singularity point where the secrecy rate is zero.

3.3.4. Converse for the LD-WT with a Helper

Theorem 3.7. *The secrecy rate R of the linear deterministic wiretap channel with one helper and symmetric channel gains at the wiretapper is bounded from above by*

$$R \leq \min\{r_{ub1}, r_{ub2}, r_{ub3}\}$$

with

$$\begin{aligned} r_{ub1} &= n_p + \tfrac{1}{2}n_c + \tfrac{1}{2}(n_1 - n_2)^+ \\ r_{ub2} &= n_1 \\ r_{ub3} &= n_2 + (n_1 - n_2 - n_E)^+ + [n_E - n_2 - (n_E - n_1 + n_2)^+]^+ \end{aligned}$$

Proof. The proof is in the same fashion as in the truncated deterministic model which is shown later and therefore deferred to the Appendix 3.7. □

3.3.5. Converse for the LD-MAC-WT

Theorem 3.8. *The secrecy sum-rate R_Σ of the linear deterministic multiple access wiretap channel with symmetric channel gains at the eavesdropper is bounded from above by*

$$R_\Sigma \leq \begin{cases} \frac{2}{3}n_c + n_p + \frac{1}{3}n_\Delta & \text{for } n_2 \geq n_E \\ \frac{2}{3}n_c + \frac{1}{3}n_\Delta & \text{for } n_E > n_2. \end{cases}$$

Proof. The proof is in the same fashion as in the truncated deterministic model which is shown later and therefore deferred to the Appendix 3.8. □

3.4. The Gaussian wiretap channel with a helper

In this section, we analyse the Gaussian wiretap channel with a helper. To get results we stick to the previously developed scheme in section 3.3.2, and we will transfer the alignment and jamming structure to its Gaussian equivalent with layered lattice codes. This will lead to an achievable rate which is directly based on the deterministic rate. Moreover, we will make use of results in [MXU17] to show that the mutual information of the Gaussian case can be upper bounded by an appropriate deterministic model. As a result, the deterministic bound in section 3.3.4 is a bound for the Gaussian model as well, with a constant bit-gap attached.

3.4.1. Achievable Scheme

Theorem 3.9. *An achievable secrecy rate of the Gaussian wiretap channel with a helper is*

$$R_{ach} = r^p + r^c + r^R$$

where $r^c := l_u(\frac{1}{2}\log SNR_1^{(1-\beta_1)} - \frac{1}{2})$, *with*

$$l_u := \left\lfloor \frac{\min\{1+\beta_2-\beta_1, 1\}}{2(1-\beta_1)} \right\rfloor,$$

$r^p := \frac{1}{2}\log(\max\{1, SNR_1^{\beta_1-\beta_2}\})$, *and*

$$r^R = \begin{cases} r^{R_1} & \text{for } r^{R_1} < r^{R_2}, SNR_1 \geq SNR_2 \\ r^{R_2} & \text{for } r^{R_1} \geq r^{R_2}, SNR_1 \geq SNR_2 \\ 0 & \text{for } r^{R_1} < r^{R_2}, SNR_2 \geq SNR_1 \\ r^{R_3} & \text{for } r^{R_1} \geq r^{R_2}, SNR_2 \geq SNR_1 \end{cases}$$

with

$$\begin{aligned} r^{R_1} &:= \tfrac{1}{2}\log SNR_1^{1-2l_u(1-\beta_1)} - \tfrac{1}{2}\log SNR_1^{\min\{\beta_1-\beta_2,0\}} - \tfrac{1}{2}, \\ r^{R_2} &:= \tfrac{1}{2}\log SNR_1^{(1-\beta_1)} - \tfrac{1}{2}, \\ r^{R_3} &:= r^{R_1} - r^{R_2}. \end{aligned}$$

Proof. In the following, we look into the case that $\mathrm{SNR}_1 \geq \mathrm{SNR}_2$. For the achievable scheme, we need to partition the available power into intervals. Each of these intervals plays the role of an $n_\Delta-$Interval of bit-levels in the linear deterministic scheme. Remember that we have $E\{X_i^2\} \leq P$ and $Z_1, Z_2 \sim \mathcal{N}(0,1)$, which means that $|h_{11}|^2P = \mathrm{SNR}_1$ and $|h_{21}|^2P = \mathrm{SNR}_2$ represent the power of both direct signals. As in the deterministic model, we assume that both signals at Y_2 are received with the same power and therefore $h_{12} = h_{22} = h_E$ which gives $|h_E|^2P = \mathrm{SNR}_E$. We also use the two parameters β_1 and β_2, which connects the SNR ratios with $\mathrm{SNR}_2 = \mathrm{SNR}_1^{\beta_1}$ and $\mathrm{SNR}_E = \mathrm{SNR}_1^{\beta_2}$. Now we can partition the received power at Y_1 into intervals of $\mathrm{SNR}_1^{(1-\beta_1)}$. Each of the intervals has therefore signal power θ_l which is defined as

$$\begin{aligned} \theta_l &= q_{l-1} - q_l \\ &= \mathrm{SNR}_1^{1-(l-1)(1-\beta_1)} - \mathrm{SNR}_1^{1-l(1-\beta_1)} \end{aligned} \tag{3.5}$$

with l indicating the specific level, similar to the technique in [BPT10]. The users decompose the signals X_i into a sum of independent sub-signals $X_i = \sum_{l=1}^{l_{max}} X_{il}$. We will use n-dimensional nested lattice codes introduced in [UZ04] which can achieve capacity in the AWGN single-user channel. A lattice Λ is a discrete subgroup of $\mathbb{R}^n$ which is closed under real addition and reflection. Moreover, denote the nearest neighbour quantizer by

$$Q_\Lambda(\mathbf{x}) := \arg\min_{\mathbf{t}\in\Lambda} ||\mathbf{x} - \mathbf{t}||.$$

The fundamental Voronoi region $\mathcal{V}(\Lambda)$ of a lattice Λ consists of all points which get mapped or quantized to the zero vector. The modulo operation for lattices defined as

$$[\mathbf{x}] \bmod \Lambda := \mathbf{x} - Q_\Lambda(\mathbf{x}).$$

Nested Lattice Codes

A nested lattice code is composed of a pair of lattices $(\Lambda_{\text{fine}}, \Lambda_{\text{coarse}})$, where $\mathcal{V}(\Lambda_{\text{coarse}})$ is the fundamental Voronoi region of the coarse lattice and operates as a shaping region for the corresponding fine lattice Λ_{fine}. It is therefore required that $\Lambda_{\text{coarse}} \subset \Lambda_{\text{fine}}$. Such a code has a corresponding rate R equal to the log of the nesting ratio. A part of the split message is now mapped to the corresponding codeword $\mathbf{u}_i(l) \in \Lambda_{\text{fine},l-1} \cap \mathcal{V}(\Lambda_{\text{coarse},l})$, which is a point of the fine lattice inside the fundamental Voronoi region of the coarse lattice. Note that $\Lambda_{l_{max}} \subset \cdots \subset \Lambda_1$. The code is chosen such that it has a power of θ_l. The codeword $\mathbf{x}_i(l)$ is now given as

$$\mathbf{x}_i(l) = [\mathbf{u}_i - \mathbf{d}_i] \bmod \Lambda_l,$$

where we dither (shift) with $\mathbf{d}_i \sim \text{Unif}(\mathcal{V}(\Lambda_l))$ and reduce the result modulo-Λ_l. Transmitter i now sends a scaled $\mathbf{x}_i$ over the channel, such that the power per sub-signal $\mathbf{x}_i(l)$ is $\frac{\theta_l}{|h_{i1}|^2}$ and receivers see a power of θ_l. Due to the partitioning construction, the $\mathbf{x}_i$ satisfy the power restriction of P for user 1,

$$\sum_{l=1}^{l_{\max}} \frac{\theta_l}{|h_{11}|^2} \leq \frac{\text{SNR}_1}{|h_{11}|^2} = P$$

and user 2

$$\sum_{l=2}^{l_{\max}} \frac{\theta_l}{|h_{21}|^2} \leq \frac{\text{SNR}_2}{|h_{21}|^2} = P.$$

Moreover, aligning sub-signals use the same code (with independent shifts). In [UZ04] it was shown that nested lattice codes can achieve the capacity of the AWGN single-user

channel with vanishing error probability. Viewing each of our power intervals as a channel, we therefore have that

$$R(l) \leq \tfrac{1}{2} \log \left(1 + \frac{\theta_l}{N(l)}\right), \tag{3.6}$$

where $N(l)$ denotes the noise variance per dimension of the subsequent levels. Now, X_1 is used for signal transmission, while X_2 is solely used for jamming. As in the deterministic case, the objective is to align the signal parts of X_1 with the jamming of X_2 at Y_2, while allowing decoding of the signal parts at Y_1. Due to the signal scale based coding strategy and the equal receive power at Y_2, an alignment is achieved with the proposed scheme. We use a jamming strategy, where the jamming sub-codeword is uniformly distributed on $\mathcal{V}$, therefore $\mathbf{x}_{2,\text{jam}}(l) \sim \text{Unif}(\mathcal{V}(\Lambda_l))$. Now, application of lemma 3.3 shows, that the received codeword $\mathbf{y} = [\mathbf{x}_1(l) + \mathbf{x}_{2,\text{jam}}(l)] \bmod \Lambda_l$ is independent of $\mathbf{x}_1(l)$, therefore providing secrecy. We therefore just need to prove, that the signal can be decoded at Y_1. The decoding is done level-wise, treating subsequent levels as noise. Every level is treated as a Gaussian point-to-point channel with power θ_l and noise $1 + \text{SNR}_1^{1-l(1-\beta_1)}$, which consists of the base noise N_1 at Y_1 and the power of all subsequent levels of both signals. Successful decoding can be assured with a rate limitation (see (3.6)) of

$$r_l \leq \tfrac{1}{2} \log \left(1 + \frac{\theta_l}{1 + \text{SNR}_1^{1-l(1-\beta_1)}}\right). \tag{3.7}$$

Achievable rate

As in the deterministic case, we have a private and common part. Common and private parts are defined as in the deterministic model. The common part depends on the strength of the received power at Eve (remember $n_c := \min\{n_E + n_\Delta, n_1\}$ for $n_1 \geq n_2$). The part $n_E + n_\Delta$ corresponds to $\text{SNR}_1^{\beta_2 + (1-\beta_1)}$ in the Gaussian model. The opposing remainder is therefore $\text{SNR}_1^{\beta_1 - \beta_2}$ and we get the common power as

$$P^c := \text{SNR}_1 - \max\{1, \text{SNR}_1^{\beta_1 - \beta_2}\},$$

while the private part has a power of

$$P^p := \max\{1, \text{SNR}_1^{\beta_1 - \beta_2}\} - 1.$$

The private part will not be partitioned further, since it can be used completely and without penalty. Moreover, it has only the base noise and a rate of $r^p = \frac{1}{2}\log(1 + P^p)$ can be achieved. For the common part, we also use the deterministic achievable scheme and need to partition the available power. All odd levels l of X_1 will be used for signal

transmission. Every level l can handle a rate of r_l. We can simplify the rate of (3.7) with

$$\log\left(1+\frac{a-b}{1+b}\right)=\log\left(\frac{a+1}{1+b}\right)\geq\log\left(\frac{a}{2b}\right)$$

where we used that $b>1$ to get $r_l\geq\frac{1}{2}\log\mathrm{SNR}_1^{(1-\beta_1)}-\frac{1}{2}$. Since we use the same scheme as in the deterministic case[2], we have a total of

$$l_{\mathrm{u}}:=\left\lfloor\frac{\min\{1+\beta_2-\beta_1,1\}}{2(1-\beta_1)}\right\rfloor$$

used levels in X_1, where the remainder term is not yet included. The alignment section of the common part has a total rate of

$$r^c=l_{\mathrm{u}}(\tfrac{1}{2}\log\mathrm{SNR}_1^{(1-\beta_1)}-\tfrac{1}{2}),$$

which corresponds to $\lfloor\frac{n_c}{2n_\Delta}\rfloor n_\Delta$ in the deterministic case. Moreover, we need to consider the remainder term, which is allocated between the alignment structure and the noise floor or the private part. Once again we use the deterministic scheme as a basis. We see in (3.3), that we have two cases for $n_1\geq n_2$, which corresponds to $\mathrm{SNR}_1\geq\mathrm{SNR}_2$. If the remainder has an available power of

$$P^R=\mathrm{SNR}_1^{1-2l_{\mathrm{u}}(1-\beta_1)}-\mathrm{SNR}_1^{\min\{\beta_1-\beta_2,0\}}<\mathrm{SNR}_1^{1-2l_{\mathrm{u}}(1-\beta_1)}-\mathrm{SNR}_1^{1-(2l_{\mathrm{u}}+1)(1-\beta_1)},$$

it can use the whole power and achieve a rate of

$$r^R\geq\tfrac{1}{2}\log\mathrm{SNR}_1^{1-2l_{\mathrm{u}}(1-\beta_1)}-\tfrac{1}{2}\log\mathrm{SNR}_1^{\min\{\beta_1-\beta_2,0\}}-\tfrac{1}{2}.$$

Otherwise, it can only use a full partition, which leads to

$$r^R\geq\tfrac{1}{2}\log\mathrm{SNR}_1^{(1-\beta_1)}-\tfrac{1}{2}.$$

We therefore get a total rate of

$$R_{\mathrm{ach}}=r^p+r^c+r^R.$$

The case of $\mathrm{SNR}_2>\mathrm{SNR}_1$ can be shown similarly. Note that we are therefore within a constant gap of the rates of the deterministic model (Theorem 3.2), by comparing via $n=\lfloor\frac{1}{2}\log\mathrm{SNR}\rfloor$. □

[2] I.e. use the odd partitions for messaging

3.4.2. Developing a Converse from LD-Bounds

For the converse of the Gaussian model, we want to make use of the converse for the linear deterministic model. The goal is to bound the Gaussian mutual information terms by the ones of the deterministic model. Since we have a bound for the deterministic model, we immediately have a bound for the Gaussian model. Due to the G-WT-H consisting of MAC channels with security constraint, one could try to use the constant-gap bound of [BT08]. Unfortunately, the result of [BT08, Thm.1] for the complex Gaussian IC, which shows that the capacity is within 42 bits of the deterministic IC capacity, depends on an assumption on the uniformity of the optimal input distribution to show that $I(W_1, W_2; \mathbf{y}^n_{2,\mathrm{LDM}}) \leq I(W_1, W_2; Y^n_{2,\mathrm{G}}) + cn$, where G stands for Gaussian model. We therefore need to introduce another approximation model first. It was shown in [MXU17] that the integer-input integer-output model of the MAC-WT and WT-H, is within a constant-gap of the G-MAC-WT and G-WT-H. The system equations for the integer-input integer-output model can be written as

$$\bar{Y}_{1,\mathrm{D}} = \lfloor h_{11}\bar{X}_{1,\mathrm{D}} \rfloor + \lfloor h_{21}\bar{X}_{2,\mathrm{D}} \rfloor \tag{3.7a}$$

$$\bar{Y}_{2,\mathrm{D}} = \lfloor h_{22}\bar{X}_{2,\mathrm{D}} \rfloor + \lfloor h_{12}\bar{X}_{1,\mathrm{D}} \rfloor, \tag{3.7b}$$

where the $\bar{X}_1^D \in \{0, 1, \ldots, \lfloor\sqrt{\mathrm{SNR}}\rfloor\}$. One can construct these codewords easily from a set of given codewords for the Gaussian case by $\lfloor X_{\mathrm{G}} \rfloor \bmod \lfloor\sqrt{P}\rfloor$. It was now shown in [MXU17], that the mutual information terms for the integer-input integer-output channel (3.8) are within a constant-gap[3] of the corresponding Gaussian model (3.1), which means that

$$I(W_1, W_2; Y^n_{1,\mathrm{G}}) \leq I(W_1, W_2; \bar{Y}^n_{1,\mathrm{D}}) + nc \tag{3.7c}$$

$$I(W_1, W_2; \bar{Y}^n_{2,\mathrm{D}}) \leq I(W_1, W_2; Y^n_{2,\mathrm{G}}) + nc, \tag{3.7d}$$

where c is a constant. We remark that these equations are for the MAC-WT models, the ones for the WT-H models can be shown similarly. The first equation follows from a proof in [BT08] and a more detailed version of the same ideas in [DJ16]. The second equation builds on lemmata and ideas from [BT08], [DJ16] and [ADT11]. For the G-WT-H, we therefore have that

$$nR = I(W; Y^n_{1,\mathrm{G}}) - I(W; Y^n_{2,\mathrm{G}}) + n\epsilon \tag{3.8}$$

$$\leq I(W; \bar{Y}^n_{1,\mathrm{D}}) - I(W; \bar{Y}^n_{2,\mathrm{D}}) + n(c + \epsilon), \tag{3.9}$$

[3] It was actually stated, that both terms are within $o(\log P)$. However, the proof results also satisfy the stronger notion of a constant-gap.

which shows that any bound for the integer-input integer-output model, can be used as an outer bound for the corresponding Gaussian model. Now, to bring the LDM ideas to the truncated model, we modify the form such that $\bar{X}_1^D$ is represented[4] as

$$X_{1,D} = 2^n \sum_{b=1}^{n} \tilde{X}_{1,b} 2^{-b} \in \{0, 1, \ldots, 2^n - 1\},$$

where $n = \lfloor \log \lfloor \sqrt{\mathrm{SNR}} \rfloor \rfloor$. Note that the floor function around the logarithm, i.e. the quantization from integers to powers of two, reduces the cardinality of the input constellation by at most half plus one-half, which results in a maximum bit-gap of 2 bits in the capacity results for high-SNR. We can therefore work with the model

$$Y_{1,\mathrm{D}} = \lfloor h_{11} X_{1,\mathrm{D}} \rfloor + \lfloor h_{21} X_{2,\mathrm{D}} \rfloor \tag{3.9a}$$

$$Y_{2,\mathrm{D}} = \lfloor h_{22} X_{2,\mathrm{D}} \rfloor + \lfloor h_{12} X_{1,\mathrm{D}} \rfloor, \tag{3.9b}$$

where $h_{ij} X_{i,D} = h_{ij} 2^{n_{ij}} \sum_{b=1}^{n_{ij}} \tilde{X}_{1,b} 2^{-b}$, $h_{ij} \in [1, 2)$ and the n_{ij} correspond to the bit-levels in the LD model. We therefore change the notation to include the assumption on equal received power at the wiretapper and write the model as

$$Y_{1,\mathrm{D}} = \lfloor h_1 X_{1,\mathrm{D}} \rfloor + \lfloor h_2 X_{2,\mathrm{D}} \rfloor \tag{3.9c}$$

$$Y_{2,\mathrm{D}} = \lfloor h_E X_{2,\mathrm{D}} \rfloor + \lfloor h_E X_{1,\mathrm{D}} \rfloor. \tag{3.9d}$$

We will call this model the truncated deterministic model (TDM). For the converse proofs we will also need the following lemmata. Note that the intuitive ideas were already used for results for example in the converse proof in [GSJ15], but without a proof. Moreover, the first lemma uses ideas from a proof in [BT08].

Lemma 3.10. *For an arbitrary signal $X_D \in \{0, 1, \ldots, 2^n - 1\}$, with $n \in \mathbb{N}$ and channel gain $h \in [1, 2)$ we have that*

$$H(\lfloor h X_D \rfloor) = H(\tilde{X}_1, \ldots, \tilde{X}_n),$$

where $\tilde{X}_i \in \mathbb{F}_2$ are such that $X_D = 2^n \sum_{i=1}^{n} \tilde{X}_i 2^{-i}$.

Proof. We denote the tuple $(\tilde{X}_1, \ldots, \tilde{X}_n) \in \mathbb{F}_2^n$ by $\tilde{\mathbf{x}}$. There is a bijection $f_1 : \mathbb{F}_2^n \to \{0, 1, \ldots, 2^n - 1\}$ which can be constructed as $f_1(\tilde{\mathbf{x}}) = 2^n \sum_{i=1}^{n} \tilde{X}_i 2^{-i}$. Now, the resulting integers are distance one apart. Therefore multiplying by $h \in [1, 2)$ does not lower the distance. Quantizing those scaled values to the integer part only introduces gaps in the

[4] For the time being, we use n as the index of the bit-level as well as the sequence index. This will be distinguishable later on, since the bit-level index will always have a subscript indicating the specific channel gain.

support, but does not reduce the cardinality. We therefore have that $f_2(X_D) = \lfloor hX_D \rfloor$ is again a bijection. Therefore, the composition of both functions $f_3 = f_2 \circ f_1$ is a bijection and we have that

$$H(f_3(\tilde{\mathbf{x}})) = H(\tilde{\mathbf{x}})$$

which shows the result. □

Lemma 3.11. *For an arbitrary signal* $X_D \in \{0, 1, \ldots, 2^n - 1\}$, *with* $n, m \in \mathbb{N}$, $m < n$, $X_D = 2^n \sum_{i=1}^{n} \tilde{X}_i 2^{-i}$, $\tilde{X} \in \mathbb{F}_2$ *and channel gain* $h \in [1, 2)$ *we have that*

$$H(\lfloor h2^n \sum_{i=1}^{n} \tilde{X}_i 2^{-i} \rfloor) = H(\lfloor h2^n \sum_{i=1}^{m} \tilde{X}_i 2^{-i} \rfloor + \lfloor h2^n \sum_{i=m+1}^{n} \tilde{X}_i 2^{-i} \rfloor)$$

Proof. The first entropy term contains $2^n \sum_{i=1}^{n} \tilde{X}_i 2^{-i} \in \{0, 1, \ldots, 2^n - 1\}$. As argued previously, the support has distance one, and multiplying by the channel gain and taking the integer part only introduces gaps in the support and scales the values up, but the cardinality stays the same. Therefore, $|\operatorname{supp}(X_D)| = |\operatorname{supp}(\lfloor hX_D \rfloor)| = 2^n$. Now, the same is true for

$$\underline{X}_D := 2^n \sum_{i=m+1}^{n} \tilde{X}_i 2^{-i} \in \{0, 1, \ldots, 2^{n-m} - 1\}.$$

It also holds for

$$\bar{X}_D := 2^n \sum_{i=1}^{m} \tilde{X}_i 2^{-i} \in \{0, 2^{n-m}, 2^{n-m+1}, 2^{n-m} + 2^{n-m+1}, \ldots, 2^n - 2^{n-m}\},$$

where the distance is $2^{n-m} > 1$, since $n > m$. Moreover, we have that $X_D = \bar{X}_D + \underline{X}_D$. The cardinality of the support of $\bar{X}_D$ is

$$\operatorname{supp}(\bar{X}_D) = \frac{2^n - 2^{n-m}}{2^{n-m}} + 1 = 2^m.$$

Now, due to the structure[5], the sum between $\underline{X}_D$ and $\bar{X}_D$ yields a Cartesian product between the support sets, and we therefore have that

$$|\operatorname{supp}(\underline{X}_D + \bar{X}_D)| = 2^n = 2^{n-m} 2^m = |\operatorname{supp}(\underline{X}_D)||\operatorname{supp}(\bar{X}_D)|,$$

for the support of the sum-set. The same holds for the scaled integer parts, since they have the same scaling and therefore

$$|\operatorname{supp}(\lfloor h(\underline{X}_D + \bar{X}_D) \rfloor)| = |\operatorname{supp}(\underline{X}_D + \bar{X}_D)|$$

[5] In particular because the biggest element of $\underline{X}_D$ is still smaller than the smallest distance in $\bar{X}_D$.

$$
\begin{aligned}
&= |\operatorname{supp}(\underline{X}_D)||\operatorname{supp}(\bar{X}_D)| \\
&= |\operatorname{supp}(\lfloor h\underline{X}_D \rfloor)||\operatorname{supp}(\lfloor h\bar{X}_D \rfloor)| \\
&= |\operatorname{supp}(\lfloor h\underline{X}_D \rfloor + \lfloor h\bar{X}_D \rfloor)|,
\end{aligned}
$$

which proves the result. □

Moreover, we introduce the function

$$f_{[a:b]}(\lfloor hX_D \rfloor) = (\lfloor hX_D \rfloor)_{[a:b]} = \lfloor h_{ij} 2^{n_{ij}} \sum_{k=a}^{b} \tilde{X}_k 2^{-k} \rfloor,$$

which restricts the exponents of the binary expansion inside the term to lie in the set of integers $\{a, a+1, \ldots, b\}$. The result of lemma 3.11 can then be written as

$$H(\lfloor hX_D \rfloor) = H((\lfloor hX_D \rfloor)_{[1:m]} + (\lfloor hX_D \rfloor)_{[m+1:n]}).$$

If the term is a sum of two signals, then both get restricted relative to the stronger part. Therefore, a signal

$$Y_D = \lfloor h_1 2^n \sum_{i=1}^{n} \tilde{X}_{1,i} 2^{-i} \rfloor + \lfloor h_2 2^m \sum_{i=1}^{m} \tilde{X}_{2,i} 2^{-i} \rfloor,$$

where $n > m$, can be restricted to

$$(Y_D)_{[1:a]} = \lfloor h_1 2^n \sum_{i=1}^{a} \tilde{X}_{1,i} 2^{-i} \rfloor + \lfloor h_2 2^m \sum_{i=1}^{a-(n-m)} \tilde{X}_{2,i} 2^{-i} \rfloor.$$

Moreover, we use the notation also on the bit-tuples to indicate that $(\tilde{X}_1, \ldots, \tilde{X}_n) \in \mathbb{F}_2^n$ by $\tilde{\mathbf{x}}$ is restricted to the bits a to b, such that $(\tilde{X}_a, \ldots, \tilde{X}_b)$ is denoted as $(\tilde{\mathbf{x}})_{[a:b]}$. The notation is, therefore, the same as for the bit-vectors in the linear deterministic model.

We can now show Theorem 3.7 for the TD model which yields the following Theorem for the Gaussian equivalent.

Theorem 3.12. *The secrecy rate R of the Gaussian wiretap channel with one helper and symmetric channel gains at the wiretapper is bounded from above by*

$$R \leq \min\{r_{ub1}, r_{ub2}, r_{ub3}\} + c$$

with

$$\begin{aligned} r_{ub1} &= n_p + \tfrac{1}{2}n_c + \tfrac{1}{2}(n_1 - n_2)^+ \\ r_{ub2} &= n_1 \\ r_{ub3} &= n_2 + (n_1 - n_2 - n_E)^+ + [n_E - n_2 - (n_E - n_1 + n_2)^+]^+, \end{aligned}$$

where c is a constant independent of the power P.

Proof. We start with equation (3.8) and convert the steps of the proof for the linear deterministic case to the truncated deterministic model.

$$\begin{aligned} n(R-\epsilon) &= I(W; Y_{1,\mathrm{G}}^n) - I(W; Y_{2,\mathrm{G}}^n) \\ &\leq I(W; Y_{1,\mathrm{D}}^n) - I(W; Y_{2,\mathrm{D}}^n) + nc \\ &\leq I(W; Y_{1,\mathrm{D}}^n) - I(W; (Y_{2,\mathrm{D}})_{[1:n_2]}^n) + nc \\ &= H(Y_{1,D}^n) - H(Y_{1,D}^n|W) - H((Y_{2,D}^n)_{[:n_2]}) + H((Y_{2,D}^n)_{[:n_2]}|W) + nc \\ &= H(Y_{1,D}^n) - H((Y_{2,D}^n)_{,[:n_2]}) + H((\lfloor h_E X_{2,D}^n \rfloor)_{[:n_2]}) - H(\lfloor h_2 X_{2,D}^n \rfloor) + nc, \end{aligned}$$

where Fanos inequality and the secrecy constraint was used. Moreover, we used the fact that $I(W; Y_{2,D}^n) \geq I(W; f(Y_{2,D}^n))$ for arbitrary functions f, due to the data processing inequality. Note that for $n_2 \geq n_E$, we have that $(Y_{2,D}^n)_{[:n_2]} = Y_{2,D}^n$. In the last line we used that $X_{1,D}$ is a function of W, and $X_{2,D}$ is independent of W, due to the helper model assumptions. We remark that the first property does not hold in general, since jamming through the first user would result in a stochastic function. Now, for $n_E \geq n_2$, both terms $\lfloor h_2 X_{2,D}^n \rfloor$ and $(\lfloor h_E X_{2,D}^n \rfloor)_{[:n_2]}$ have the same bits, and we can use lemma 3.10 to show that

$$H((\lfloor h_E X_{2,D}^n \rfloor)_{[:n_2]}) - H(\lfloor h_2 X_{2,D}^n \rfloor) = 0$$

and for $n_E < n_2$ the second term contains more bits, and we can therefore use the chain rule and lemma 3.10 and show that

$$H((\lfloor h_E X_{2,D}^n \rfloor)_{[:n_2]}) - H(\lfloor h_2 X_{2,D}^n \rfloor) = -H((\tilde{\mathbf{x}}_2^n)_{[n_E+1:]}|(\tilde{\mathbf{x}}_2^n)_{[:n_E]}). \tag{3.10}$$

We now split the received signals in common and private parts. Also, remember that n_c is defined in equation (3.2). We start by adding two of the terms and split them apart

$$\begin{aligned} &2(H(Y_{1,D}^n) - H((Y_{2,D}^n)_{[:n_2]})) \\ &\leq 2H((Y_{1,D}^n)_{[n_c+1:]}) + 2H((Y_{1,D}^n)_{[:n_c]}) - 2H((Y_{2,D}^n)_{[:n_2]}). \end{aligned}$$

Note that the private part $H((Y_{1,D}^n)_{[n_c+1:]})$ is zero for $n_1 \leq n_E$. Now, counting from top to bottom, for $n_1 \geq n_2$, $X_{1,D}^n$ has n_c bit-levels in $(Y_{1,D})_{[:n_c]}$, while $X_{2,D}^n$ has $\eta := \min\{n_E, \min\{n_1, n_2\}\} = n_c - n_\Delta$ bit-levels. Therefore, η represents the amount of bit-levels of the weaker signal in the common received signal part. Hence, for $n_2 > n_1$, $X_{1,D}^n$ and $X_{2,D}^n$ have η and n_c bit-levels in that term, respectively. We need to account for this switch of indexing in the next part, where we analyse the entropy difference. We will use a method inspired by [FW14a] to show the following (for $n_1 \geq n_2$)

$$
\begin{aligned}
&2(H(Y_{1,D}^n) - H((Y_{2,D}^n)_{[:n_2]}) \\
&\leq 2H((Y_{1,D}^n)_{[n_c+1:]}) + 2H((Y_{1,D}^n)_{[:n_c]}) - H((Y_{2,D}^n)_{[:n_2]}|\tilde{\mathbf{x}}_1^n) - H((Y_{2,D}^n)_{[:n_2]}|\tilde{\mathbf{x}}_2^n) \\
&= 2H((Y_{1,D}^n)_{[n_c+1:]}) + 2H((Y_{1,D}^n)_{[:n_c]}) - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) - H((\tilde{\mathbf{x}}_1^n)_{[:n_2]}) \\
&= 2H((Y_{1,D}^n)_{[n_c+1:]}) + H((Y_{1,D}^n)_{[:n_c]}) + H((f(\lfloor h_1 X_{1,\mathrm{D}}^n \rfloor, \lfloor h_2 X_{2,\mathrm{D}}^n \rfloor))_{[:n_c]}) \\
&\quad - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) - H((\tilde{\mathbf{x}}_1^n)_{[:n_2]}) \\
&\leq 2H((Y_{1,D}^n)_{[n_c+1:]}) + H((Y_{1,D}^n)_{[:n_c]}) + H((\lfloor h_2 X_{2,\mathrm{D}}^n \rfloor)_{[:\eta]}) + H((\lfloor h_1 X_{1,\mathrm{D}}^n \rfloor)_{[:n_c]}) \\
&\quad - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) - H((\tilde{\mathbf{x}}_1^n)_{[:n_2]}) \\
&= 2H((Y_{1,D}^n)_{[n_c+1:]}) + H((Y_{1,D}^n)_{[:n_c]}) + H((\tilde{\mathbf{x}}_2^n)_{[:\eta]}) + H((\tilde{\mathbf{x}}_1^n)_{[:n_c]}) \\
&\quad - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) - H((\tilde{\mathbf{x}}_1^n)_{[:n_2]}),
\end{aligned}
$$

We now have for $n_1 \geq n_2$ that

$$
H((\tilde{\mathbf{x}}_1^n)_{[:n_c]}) - H((\tilde{\mathbf{x}}_1^n)_{[:n_2]}) \leq n(n_c - \min\{n_2, n_E\})^+ \leq n n_\Delta,
$$

and

$$
H((\tilde{\mathbf{x}}_2^n)_{[:\eta]}) - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) \leq n(\eta - \min\{n_2, n_E\})^+ = 0.
$$

And for $n_2 > n_1$ we get

$$
H((\tilde{\mathbf{x}}_1^n)_{[:\eta]}) - H((\tilde{\mathbf{x}}_1^n)_{[:n_2]}) \leq n(\eta - \min\{n_2, n_E\})^+ = 0,
$$

and

$$
H((\tilde{\mathbf{x}}_2^n)_{[:n_c]}) - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) \leq n(n_c - \min\{n_2, n_E\})^+.
$$

We remark that the last term gets $(n_2 - n_E)^+$ for $n_1 < n_E < n_2$, in which case we can use (3.10), which has a length of $(n_2 - n_E)$ bit-levels. Also for $n_E < n_1 < n_2$ we have that $n(n_c - \min\{n_2, n_E\})^+ = n n_\Delta$, by using (3.10) again, we see that for $n_2 > n_1$

$$
H((\tilde{\mathbf{x}}_2^n)_{[:n_c]}) - H((\tilde{\mathbf{x}}_2^n)_{[:n_2]}) \leq n(n_c - \min\{n_2, n_E\})^+ = 0.
$$

We therefore have an additional term of nn_Δ for $n_1 \geq n_2$. Now one can divide all terms by two, resulting in

$$H(Y_{1,D}^n) - H((Y_{2,D}^n)_{[:n_2]}) \leq H((Y_{1,D}^n)_{[n_c+1:]}) + \frac{1}{2}H((Y_{1,D}^n)_{[:n_c]}) + \frac{n}{2}(n_1 - n_2)^+.$$

Plugging all the results into the first equation yields

$$n(R-\epsilon) \leq n(n_p + \tfrac{1}{2}n_c + \tfrac{1}{2}(n_1 - n_2)^+ + c).$$

dividing by n and letting $n \to \infty$ shows the result. For the case that $n_2 > 2n_1$ we have that

$$\begin{aligned} n(R-\epsilon) &\leq H(Y_{1,D}^n) - H(Y_{2,D}^n) + H(\lfloor h_E X_{2,D}^n \rfloor) - H(\lfloor h_2 X_{2,D}^n \rfloor) + nc \\ &\leq H(\lfloor h_1 X_{1,D}^n \rfloor) + H(\lfloor h_2 X_{2,D}^n \rfloor) - H(Y_{2,D}^n | \tilde{\mathbf{X}}_1^n) \\ &\quad - H(\lfloor h_2 X_{2,D}^n \rfloor) + H(\lfloor h_E X_{2,D}^n \rfloor) + nc \\ &= H(\lfloor h_1 X_{1,D}^n \rfloor) \leq nn_1 \end{aligned}$$

and for the case that $3n_2 < 2n_1$ we have that

$$\begin{aligned} nR &\leq I(W; Y_{1,D}^n) - I(W; Y_{2,D}^n) + n(\epsilon + c) \\ &\leq I(W; Y_{1,D}^n) - I(W; (Y_{2,D}^n)_{[:n_1-n_2]}) + n(\epsilon + c) \\ &\leq H(Y_{1,D}^n) - H((Y_{2,D}^n)_{[:n_1-n_2]}) + H((\lfloor h_E X_{2,D}^n \rfloor)_{[:n_1-n_2]}) - H(\lfloor h_2 X_{2,D}^n \rfloor) + n(\epsilon + c) \\ &\leq H((Y_{1,D}^n)_{[:(n_1-n_2)]}) + H((Y_{1,D}^n)_{[(n_1-n_2)+1:]} | (Y_{1,D}^n)_{[:(n_1-n_2)]}) - H((Y_{2,D}^n)_{[:n_1-n_2]} | \tilde{\mathbf{X}}_2^n) \\ &\quad + H((\lfloor h_E X_{2,D}^n \rfloor)_{[:n_1-n_2]}) - H(\lfloor h_2 X_{2,D}^n \rfloor) + n(\epsilon + c). \end{aligned}$$

One can show that

$$H((Y_{1,D}^n)_{[:(n_1-n_2)]}) - H((Y_{2,D}^n)_{[:n_1-n_2]} | \tilde{\mathbf{X}}_2^n) \leq n(n_1 - n_2 - n_E)^+$$

and

$$\begin{aligned} &H\left((\lfloor h_E X_{2,D}^n \rfloor)_{[:n_1-n_2]}\right) - H(\lfloor h_2 X_{2,D}^n \rfloor) \\ &\leq n(\min\{n_1 - n_2, n_E\} - n_2) = n[n_E - n_2 - (n_E - n_1 + n_2)^+]^+ \end{aligned}$$

and $H((Y_{1,D}^n)_{[(n_1-n_2)+1:]} | (Y_{1,D}^n)_{[:(n_1-n_2)]}) \leq nn_2$ which yields

$$nR \leq nn_2 + n(n_1 - n_2 - n_2)^+ + n[n_E - n_2 - (n_E - n_1 + n_2)^+]^+ + n(\epsilon + c)$$

dividing by n and letting $n \to \infty$ shows the result. □

3.5. The Gaussian Multiple-Access Wiretap Channel

In this section we analyse the Gaussian MAC-WT channel. As in the case of the WT channel with a Helper, we want to stick to the ideas of the corresponding linear deterministic model. This means we want to transfer the alignment and jamming structure to its Gaussian equivalent with layered lattice codes. This will lead to an achievable rate which is directly based on the deterministic rate. Moreover, we will make use of the previously developed ideas to convert the converse proof of the linear deterministic model, to the truncated model and therefore to the Gaussian model.

3.5.1. Achievable Scheme

Theorem 3.13. *An achievable secrecy sum-rate of the Gaussian multiple-access wiretap channel is*

$$R_\Sigma = r^p + r^c + r^R$$

where $r^c := l_u(\frac{1}{2}\log SNR_1^{(1-\beta_1)} - \frac{1}{2})$, *with*

$$l_u := 2\left\lfloor \frac{\min\{1+\beta_2-\beta_1, 1\}}{3(1-\beta_1)} \right\rfloor,$$

$r^p := \frac{1}{2}\log(\max\{1, SNR_1^{\beta_1-\beta_2}\})$, *and*

$$r^R = \begin{cases} r^{R_1} & \text{for } r^{R_1} < r^{R_2} \\ r^{R_2} & \text{for } 2r^{R_2} > r^{R_1} \geq r^{R_2} \\ r^{R_1} + r^{R_2} & \text{for } r^{R_1} \geq 2r^{R_2}. \end{cases}$$

with

$$r^{R_1} := \tfrac{1}{2}\log SNR_1^{1-\frac{3}{2}l_u(1-\beta_1)} - \tfrac{1}{2}\log SNR_1^{\min\{\beta_1-\beta_2,0\}} - \tfrac{1}{2}$$
$$r^{R_2} := \tfrac{1}{2}\log SNR_1^{(1-\beta_1)} - \tfrac{1}{2}.$$

Proof. We use the same framework as for the wiretap channel with a helper in section 3.4.1. We therefore partition the available power into intervals with power θ_l, see eq. (3.5), where l indicates the level. Each of these intervals plays the role of an n_Δ-Interval of bit-levels in the linear deterministic scheme. We have that $|h_1|^2P = \mathrm{SNR}_1$, $|h_2|^2P = \mathrm{SNR}_2$, as well as $h_{12} = h_{22} = h_E$ which gives $|h_E|^2P = \mathrm{SNR}_E$. We also use the two parameters

β_1 and β_2, which connects the SNR ratios with $\mathrm{SNR}_2 = \mathrm{SNR}_1^{\beta_1}$ and $\mathrm{SNR}_E = \mathrm{SNR}_1^{\beta_2}$. We therefore partition the received power at Y_1 into intervals $\mathrm{SNR}_1^{(1-\beta_1)}$. The users decompose the signals X_i into a sum of independent sub-signals $X_i = \sum_{l=1}^{l_{max}} X_{il}$. And each signal uses the layered lattice codes as defined in section 3.4.1.

Achievable rate

Note that, w.l.o.g we look at the case $\mathrm{SNR}_1 > \mathrm{SNR}_2$, which is $\beta_1 < 1$. Due to the symmetry of the users the case $\beta_1 \geq 1$ follows immediately by interchanging both signals. As in the deterministic case, we have a private and common part. The common part is defined as the bit-levels $n_c := \min\{n_E + n_\Delta, n_1\}$. The part $n_E + n_\Delta$ corresponds to $\mathrm{SNR}_1^{\beta_2+(1-\beta_1)}$ in the Gaussian model. The opposing remainder is, therefore, $\mathrm{SNR}_1^{\beta_1-\beta_2}$ and we get the common power as

$$P^c := \mathrm{SNR}_1 - \max\{1, \mathrm{SNR}_1^{\beta_1-\beta_2}\},$$

while the private part has a power of

$$P^p := \max\{1, \mathrm{SNR}_1^{\beta_1-\beta_2}\} - 1,$$

exactly as in the case of the wiretap channel with a helper. However, due to the modified scheme where both users jam and align their jamming signals at the legitimate receiver (see section 3.3.3) we have a different number of used levels for messaging. We have

$$l_\mathrm{u} := 2 \left\lfloor \frac{\min\{1 + \beta_2 - \beta_1, 1\}}{3(1-\beta_1)} \right\rfloor$$

used levels for messaging, where each one supports a rate of $r_l \geq \frac{1}{2} \log \mathrm{SNR}_1^{(1-\beta_1)} - \frac{1}{2}$. And we therefore have a sum rate of

$$r^c = l_\mathrm{u}(\tfrac{1}{2} \log \mathrm{SNR}_1^{(1-\beta_1)} - \tfrac{1}{2}),$$

for the whole common alignment part. Moreover, we need to consider the remainder term, which is allocated between the alignment structure and the noise floor or the private part. We see from the deterministic scheme that for

$$1 - (\tfrac{3}{2} l_\mathrm{u} + 1)(1-\beta_1) < \min\{\beta_1 - \beta_2, 0\}$$

we can achieve a rate of

$$r^R \geq \tfrac{1}{2} \log \mathrm{SNR}_1^{1-\frac{3}{2}l_\mathrm{u}(1-\beta_1)} - \tfrac{1}{2} \log \mathrm{SNR}_1^{\min\{\beta_1-\beta_2,0\}} - \tfrac{1}{2}.$$

Moreover, for

$$1-(\tfrac{3}{2}l_{\mathrm{u}}+2)(1-\beta_1)<\min\{\beta_1-\beta_2,0\}\leq 1-(\tfrac{3}{2}l_{\mathrm{u}}+1)(1-\beta_1)$$

we have

$$r^R\geq \tfrac{1}{2}\log \mathrm{SNR}_1^{(1-\beta_1)}-\tfrac{1}{2},$$

and for

$$\min\{\beta_1-\beta_2,0\}\leq 1-(\tfrac{3}{2}l_{\mathrm{u}}+2)(1-\beta_1)$$

we have

$$r^R\geq \tfrac{1}{2}\log \mathrm{SNR}_1^{(1-\beta_1)}+\tfrac{1}{2}\log \mathrm{SNR}_1^{1-\frac{3}{2}l_{\mathrm{u}}(1-\beta_1)}-\tfrac{1}{2}\log \mathrm{SNR}_1^{\min\{\beta_1-\beta_2,0\}}-1.$$

We therefore get a total rate of

$$r_{\mathrm{ach}}=r^p+r^c+r^R.$$

The case of $\mathrm{SNR}_2>\mathrm{SNR}_1$ can be shown similarly. Note that we are therefore within a gap of $1+\frac{l_{\mathrm{u}}}{2}$ bits at maximum, of the rates of the deterministic model, by comparing via $n_i=\lfloor\frac{1}{2}\log \mathrm{SNR}_i\rfloor$. □

3.5.2. Converse Bound for the G-MAC-WT

We use a similar approach as for the Gaussian WT with a helper, with the same framework developed in section 3.4.2. This means we also use the truncated deterministic model

$$Y_{1,\mathrm{D}}=\lfloor h_1X_{1,\mathrm{D}}\rfloor+\lfloor h_2X_{2,\mathrm{D}}\rfloor \tag{3.10a}$$

$$Y_{2,\mathrm{D}}=\lfloor h_EX_{2,\mathrm{D}}\rfloor+\lfloor h_EX_{1,\mathrm{D}}\rfloor, \tag{3.10b}$$

which can be shown to be within a constant gap to the Gaussian channel, see (3.8).

Theorem 3.14. *The secrecy sum-rate R_Σ of the Gaussian multiple access wiretap channel with symmetric channel gains at the eavesdropper is bounded from above by*

$$R_\Sigma\leq\begin{cases}\frac{2}{3}n_c+n_p+\frac{1}{3}n_\Delta+c & \text{for } n_2\geq n_E\\ \frac{2}{3}n_c+\frac{1}{3}n_\Delta+c & \text{for } n_E>n_2,\end{cases}$$

where c is a constant independent of the signal power P.

Proof. We begin with the following derivations

$$
\begin{aligned}
& n(R_\Sigma - \epsilon) && (3.11)\\
&\quad = I(W_1, W_2; Y_{1,\mathrm{G}}^n) - I(W_1, W_2; Y_{2,\mathrm{G}}^n)\\
&\quad \leq I(W_1, W_2; Y_{1,\mathrm{D}}^n) - I(W_1, W_2; Y_{2,\mathrm{D}}^n) + nc\\
&\quad \leq I(W_1, W_2; Y_{1,\mathrm{D}}^n) - I(W_1, W_2; Y_{2,\mathrm{D}}^n) + nc\\
&\quad \leq I(W_1, W_2; Y_{1,\mathrm{D}}^n, Y_{2,\mathrm{D}}^n) - I(W_1, W_2; Y_{2,\mathrm{D}}^n) + nc\\
&\quad \leq I(W_1, W_2; Y_{1,\mathrm{D}} | Y_{2,\mathrm{D}}) + nc\\
&\quad \leq I(X_{1,\mathrm{D}}^n, X_{2,\mathrm{D}}^n; Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}}^n) + nc\\
&\quad = H(Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}}^n) - H(Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}}^n, X_{1,\mathrm{D}}^n, X_{2,\mathrm{D}}^n) + nc\\
&\quad \overset{(b)}{=} H(Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}}^n) + nc\\
&\quad \overset{(c)}{\leq} H(Y_{1,\mathrm{D},c}^n | Y_{2,\mathrm{D}}) + H(Y_{1,\mathrm{D},p}^n | Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c}) + nc && (3.12)
\end{aligned}
$$

where we used basic techniques such as Fano's inequality and the chain rule. Step (a) introduces the secrecy constraint (3.1), while we used the chain rule, non-negativity of mutual information and the data processing inequality in the following lines. Step (b) follows from the fact that $Y_{1,\mathrm{D}}^n$ is a function of $(X_{1,\mathrm{D}}^n, X_{2,\mathrm{D}}^n)$. Note that due to the definition of the common and the private part[6] of $Y_{1,\mathrm{D}}^n$, it follows that $H(Y_{1,\mathrm{D},p}^n | Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c}) = 0$ for $n_E \geq n_2$. For step (c), we used lemma 3.11, the data-processing inequality and the chain-rule. We now extend the strategy of [XU14], of bounding a single signal part, to asymmetrical channel gains

$$
\begin{aligned}
nR_1 &= H(W_1)\\
&\leq I(W_1; Y_{1,\mathrm{D}}^n) - n\epsilon_3\\
&\leq I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D}}^n) - n\epsilon_3\\
&\leq I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},c}^n) + I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - n\epsilon_3\\
&= H(Y_{1,\mathrm{D},c}^n) - H(Y_{1,\mathrm{D},c}^n | X_{1,\mathrm{D}}^n) + I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - n\epsilon_3\\
&= H(Y_{1,\mathrm{D},c}^n) - H((\lfloor h_2 X_{2,\mathrm{D}}^n \rfloor)_{[:n_c]}) + I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - n\epsilon_3 && (3.13)
\end{aligned}
$$

and it therefore holds that

$$
H((\lfloor h_2 X_{2,\mathrm{D}}^n \rfloor)_{[:n_c]}) \leq H(Y_{1,\mathrm{D},c}^n) + I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - n(R_1 + \epsilon_3). \tag{3.14}
$$

[6] The common part is defined as $Y_{1,\mathrm{D},c}^n = (Y_{1,\mathrm{D}}^n)_{[:n_c]}$, and the private part as $Y_{1,\mathrm{D},p}^n = (Y_{1,\mathrm{D}}^n)_{[n_c+1:]}$.

The same can be shown for $H((\lfloor h_1 X_{1,\mathrm{D}}^n \rfloor)_{[:n_c]})$, where it holds that

$$H((\lfloor h_1 X_{1,\mathrm{D}}^n \rfloor)_{[:n_c]}) \leq H(Y_{1,\mathrm{D},c}^n) + I(X_{2,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - n(R_2 + \epsilon_3). \tag{3.15}$$

Moreover, we have that

$$\begin{aligned}
&I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) + I(X_{2,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) \\
&= 2H(Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - H(Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n, X_{1,\mathrm{D}}^n) - H(Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n, X_{2,\mathrm{D}}^n) \\
&= 2H(Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n) - H((\lfloor h_2 X_{2,\mathrm{D}}^n \rfloor)_{[n_c+1:]} | Y_{1,\mathrm{D},c}^n) - H((\lfloor h_1 X_{1,\mathrm{D}}^n \rfloor)_{[n_c+1:]} | Y_{1,\mathrm{D},c}^n) \\
&= H(Y_{1,\mathrm{D},p}^n | Y_{1,\mathrm{D},c}^n).
\end{aligned} \tag{3.16}$$

The key idea for the various cases is now to bound the term $H(Y_{1,\mathrm{D},c}^n | Y_{2,\mathrm{D}})$, or equivalently $H(Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}})$ for $n_E > n_2$, in an appropriate way, to be able to use (3.14) and (3.15) on (3.12). We start with the first case:

Case 1 ($n_2 \geq n_E$)

Here we have a none vanishing private part, due to the definition of $Y_{1,\mathrm{D},c}^n$ and therefore need to bound the term $H(Y_{1,\mathrm{D},c}^n | Y_{2,\mathrm{D}})$. Note that due to the definition of $Y_{1,\mathrm{D},c}^n$ and the specific case, we have that $H((\lfloor h_2 X_{2,\mathrm{D}}^n \rfloor)_{[:n_c]}) = H(\lfloor h_E X_{2,D}^n \rfloor)$. We look into the first term of equation (3.12) and show that

$$\begin{aligned}
&H(Y_{1,\mathrm{D},c}^n | Y_{2,\mathrm{D}}) \\
&\quad = H(Y_{1,\mathrm{D},c}^n, Y_{2,\mathrm{D}}) - H(Y_{2,\mathrm{D}}) \\
&\quad \leq H(Y_{1,\mathrm{D},c}^n, \lfloor h_E X_{2,\mathrm{D}} \rfloor, \lfloor h_E X_{1,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D}}) \\
&\quad = H(\lfloor h_E X_{2,\mathrm{D}} \rfloor, \lfloor h_E X_{1,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D}}) + H(Y_{1,\mathrm{D},c}^n | \lfloor h_E X_{2,\mathrm{D}} \rfloor, \lfloor h_E X_{1,\mathrm{D}} \rfloor) \\
&\quad \leq H(\lfloor h_E X_{1,\mathrm{D}} \rfloor) + H(\lfloor h_E X_{2,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D}} | X_{2,\mathrm{D}}) + H(Y_{1,\mathrm{D},c}^n | \lfloor h_E X_{2,\mathrm{D}} \rfloor, \lfloor h_E X_{1,\mathrm{D}} \rfloor) \\
&\quad = H(\lfloor h_E X_{2,\mathrm{D}} \rfloor) + H(Y_{1,\mathrm{D},c}^n | \lfloor h_E X_{2,\mathrm{D}} \rfloor, \lfloor h_E X_{1,\mathrm{D}} \rfloor).
\end{aligned} \tag{3.17}$$

Observe that the second term of equation (3.17) is dependent on the specific regime. We can bound this term by

$$H(Y_{1,\mathrm{D},c}^n | \lfloor h_E X_{2,\mathrm{D}} \rfloor, \lfloor h_E X_{1,\mathrm{D}} \rfloor) \leq n(n_c - n_E) = n n_\Delta.$$

Note that the choice of $\lfloor h_E X_{2,\mathrm{D}} \rfloor$ in (3.17) as remaining signal part was arbitrary due to our assumption that both signals $\lfloor h_E X_{1,\mathrm{D}} \rfloor$ and $\lfloor h_E X_{2,\mathrm{D}} \rfloor$ have the same signal strength.

Moreover, it follows on the same lines that

$$H(Y_{1,\mathrm{D},c}^n|Y_{2,\mathrm{D}}) \leq H(\lfloor h_E X_{1,\mathrm{D}} \rfloor) + nn_\Delta.$$

Looking at this result, its intuitive that one can also show the stronger result

$$H(Y_{1,\mathrm{D},c}^n|Y_{2,\mathrm{D}}) \leq H((\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]})$$

for the case that $n_2 \geq n_E$. This can be shown by considering a similar strategy as in (3.17)

$$\begin{aligned}
&H(Y_{1,\mathrm{D},c}^n|Y_{2,\mathrm{D}}) \\
&\quad = H(Y_{1,\mathrm{D},c}^n, Y_{2,\mathrm{D}}) - H(Y_{2,\mathrm{D}}) \\
&\quad \leq H(Y_{2,\mathrm{D}}, (\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}, (\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]}) - H(Y_{2,\mathrm{D}}) \\
&\quad = H((\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}, (\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]}) + H(Y_{2,\mathrm{D}}|(\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}, (\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]}) \\
&\qquad -H(Y_{2,\mathrm{D}}) \\
&\quad \leq H((\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}) + H((\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]}) + H(Y_{2,\mathrm{D}}|(\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}, (\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]})) \\
&\qquad -H(Y_{2,\mathrm{D}}|X_{1,\mathrm{D}}) \\
&\quad = H((\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}) + H(Y_{2,\mathrm{D}}|(\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}, (\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]})),
\end{aligned} \tag{3.18}$$

where

$$H(Y_{2,\mathrm{D}}|(\lfloor h_1 X_{1,\mathrm{D}} \rfloor)_{[:n_c]}, (\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]})) \leq n(n_E - n_2)^+ = 0. \tag{3.19}$$

We combine one sum-rate inequality (3.12) with (3.17) and one with (3.18). Moreover, we plug (3.14) and (3.15) into the corresponding bound, which yields

$$n(2R_1 + R_2 - \epsilon_6) \leq H(Y_{1,\mathrm{D},c}^n) + I(X_{2,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n|Y_{1,\mathrm{D},c}^n) + H(Y_{1,\mathrm{D},p}^n|Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c})$$

and

$$n(R_1 + 2R_2 - \epsilon_7) \leq H(Y_{1,\mathrm{D},c}^n) + I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n|Y_{1,\mathrm{D},c}^n) + H(Y_{1,\mathrm{D},p}^n|Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c}) + nn_\Delta.$$

A summation of these results gives

$$\begin{aligned}
&3n(R_1 + R_2) - n\epsilon_8 \\
&\quad \leq 2H(Y_{1,\mathrm{D},c}^n) + I(X_{1,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n|Y_{1,\mathrm{D},c}^n) + I(X_{2,\mathrm{D}}^n; Y_{1,\mathrm{D},p}^n|Y_{1,\mathrm{D},c}^n) + nn_\Delta \\
&\qquad + 2H(Y_{1,\mathrm{D},p}^n|Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c})
\end{aligned}$$

$$= 2H(Y^n_{1,\mathrm{D},c}) + H(Y^n_{1,\mathrm{D},p}|Y^n_{1,\mathrm{D},c}) + 2H(Y^n_{1,\mathrm{D},p}|Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c}) + nn_\Delta,$$

where we used (3.16). Now, because $H(Y^n_{1,\mathrm{D},p}|Y_{2,\mathrm{D}}, Y_{1,\mathrm{D},c}) \leq nn_p$ and $H(Y^n_{1,\mathrm{D},p}|Y^n_{1,\mathrm{D},c}) \leq nn_p$, this results in

$$3n(R_1 + R_2) - n\epsilon_8 \leq 2H(Y^n_{1,\mathrm{D},c}) + 3nn_p + nn_\Delta \leq 2nn_c + 3nn_p + nn_\Delta.$$

Dividing by $3n$ and letting $n \to \infty$ shows the result.

Case 2 ($n_E > n_2$)

First, we assume that $n_E \geq n_1$, and include a short proof for $n_1 > n_E \geq n_2$ at the end of this subsection. For Case 2, the private part $Y^n_{1,\mathrm{D},p}$ is zero, due to the definition of the private part and $n_E > n_2$. It follows that (3.12) is

$$n(R_1 + R_2) \leq H(Y^n_{1,\mathrm{D}}|Y^n_{2,\mathrm{D}}). \tag{3.20}$$

Moreover, we have that

$$H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor) = H((\lfloor h_2 X_{2,\mathrm{D}} \rfloor)_{[:n_E]}) \leq H(\lfloor h_E X_{2,\mathrm{D}} \rfloor),$$

which is why we need to bound (3.20) by $H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor)$ and $H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor)$. We therefore modify (3.18) to fit our purpose in the following way

$$\begin{aligned}
&H(Y^n_{1,\mathrm{D}}|Y_{2,\mathrm{D}}) \\
&\quad = H(Y^n_{1,\mathrm{D}}, Y_{2,\mathrm{D}}) - H(Y_{2,\mathrm{D}}) \\
&\quad \leq H(Y_{2,\mathrm{D}}, \lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D}}) \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D}}) + H(Y_{2,\mathrm{D}}|\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H(Y^n_{2,\mathrm{D},c}|\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\qquad + H(Y^n_{2,\mathrm{D},p}|\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor, Y^n_{2,\mathrm{D},c}) - H(Y^n_{2,\mathrm{D},c}) - H(Y^n_{2,\mathrm{D},p}|Y^n_{2,\mathrm{D},c}) \\
&\quad \leq H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H(Y^n_{2,\mathrm{D},c}|\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y^n_{2,\mathrm{D},c}),
\end{aligned}$$

where $Y^n_{2,\mathrm{D},c} = (Y^n_{2,\mathrm{D}})_{[:n_1]}$ and $Y^n_{2,\mathrm{D},p} = (Y^n_{2,\mathrm{D}})_{[n_1+1:]}$. Now, we can show that

$$\begin{aligned}
&H(Y^n_{1,\mathrm{D}}|Y_{2,\mathrm{D}}) \\
&\quad \leq H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H(Y^n_{2,\mathrm{D},c}|\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y^n_{2,\mathrm{D},c}), \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y^n_{2,\mathrm{D},c}) + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]}|\lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\quad \leq H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) + H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y^n_{2,\mathrm{D},c}|X_{2,\mathrm{D}}) + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]}|\lfloor h_2 X_{2,\mathrm{D}} \rfloor)
\end{aligned}$$

$$
\begin{aligned}
&= H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\leq H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor) + n n_\Delta, \qquad (3.21)
\end{aligned}
$$

where the last inequality follows because we have that

$$
H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) = H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[n_2+1:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor), \qquad (3.22)
$$

due to lemma 3.10 and the chain-rule. Bounding $H(Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}})$ by $H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor)$ requires more work. We have a redundancy in the negative entropy terms, with which we can cancel the $H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor)$ term in the following way

$$
\begin{aligned}
&H(Y_{1,\mathrm{D}}^n | Y_{2,\mathrm{D}}) \\
&\quad \leq H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H(Y_{2,\mathrm{D},c}^n | \lfloor h_1 X_{1,\mathrm{D}} \rfloor, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D},c}^n), \\
&\quad \leq H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) + H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H((Y_{2,\mathrm{D},c}^n)_{[:n_2]} | X_{1,\mathrm{D}}) \\
&\qquad + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) - H((Y_{2,\mathrm{D},c}^n)_{[n_2+1:]} | X_{1,\mathrm{D}}, (Y_{2,\mathrm{D},c}^n)_{[:n_2]}) \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) - H((Y_{2,\mathrm{D},c}^n)_{[n_2+1:]} | X_{1,\mathrm{D}}, (Y_{2,\mathrm{D},c}^n)_{[:n_2]}) \\
&\qquad + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\quad \leq H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\qquad - H((Y_{2,\mathrm{D},c}^n)_{[n_2+1:]} | X_{1,\mathrm{D}}, (Y_{2,\mathrm{D},c}^n)_{[:n_2]}, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) - H((Y_{2,\mathrm{D},c}^n)_{[n_2+1:]} | X_{1,\mathrm{D}}, \lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) - H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[n_2+1:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) + H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]} | \lfloor h_2 X_{2,\mathrm{D}} \rfloor) \\
&\quad = H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor), \qquad (3.23)
\end{aligned}
$$

where the last step follows due to equation (3.22). Now we can bound one (3.20) with (3.21) and one with (3.23). Moreover, we use (3.14) and (3.15) on the result. Note that due to our regime, (3.14) becomes

$$
H(\lfloor h_2 X_{2,\mathrm{D}} \rfloor) \leq H(Y_{1,\mathrm{D}}^n) - n(R_1 + \epsilon_3),
$$

while (3.15) becomes

$$
H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) \leq H(Y_{1,\mathrm{D}}^n) - n(R_2 + \epsilon_4).
$$

Putting everything together results in

$$
3n(R_1 + R_2) - n\epsilon_8 \leq 2H(Y_{1,\mathrm{D}}^n) + n n_\Delta \leq 2n n_c + n n_\Delta.
$$

Dividing by $3n$ and letting $n \to \infty$ shows the result. We need to modify a bound on $H(Y_{1,\mathrm{D}}^n|Y_{2,\mathrm{D}})$, if the signal strength n_E lies in between n_1 and n_2. In (3.21), we see that

$$H(\lfloor h_1 X_{1,\mathrm{D}} \rfloor) - H(Y_{2,\mathrm{D},c}^n|X_{2,\mathrm{D}}) \leq n(n_1 - n_E)^+.$$

Moreover, we have that

$$H((\lfloor h_E X_{2,\mathrm{D}} \rfloor)_{[:n_1]}|\lfloor h_2 X_{2,\mathrm{D}} \rfloor) \leq n(n_E - n_2)^+.$$

Both changes cancel and we get the same result as (3.21). The result follows on the same lines as in the previous derivation. □

3.6. Conclusions

We have shown an achievable scheme for both, the Gaussian multiple-access wiretap channel and the Gaussian wiretap channel with a helper. We used the linear deterministic approximation of both models, to gain insights into the structure and devised novel achievable schemes based on orthogonal bit-level alignment to achieve secrecy. These techniques can be summarized as signal-scale alignment methods, where we used jamming alignment at the eavesdropper in the signal-scale, while minimizing the negative effect at the legitimate receiver. Both results were then transferred to the Gaussian model, by utilizing layered lattice coding. Moreover, we developed converse proofs for both models, which achieve a constant-gap bound for certain signal power regimes. Those converse techniques were developed for the LD model and then transferred to a truncated deterministic model, which in turn is within a constant-gap of the integer-input integer-output model. The integer-input integer-output model yields converse proofs for the Gaussian models, by invoking a result of [MXU17]. Since our results hold for asymmetrical channel gains and are dependent on those ratios, they can be seen as *generalized* s.d.o.f. and converge to the known s.d.o.f. results for the channel gain ratio approaching one. Looking into the figure 3.6, one can see the achievable rate normalized by the single-link channel, with varying parameter β_1, i.e. channel gain configurations. One can see that the figure shows the s.d.o.f of $\frac{1}{2}$ for the G-WT-H, and $\frac{2}{3}$ for the G-MAC-WT for $\beta_1 \to 1$, which agrees with the results of [XU12]. We can also see, that the achievable rate of both models fluctuates between the upper bound and a lower bound, for the part where the bit-level alignment scheme is dominant. We believe that this is a result of the orthogonal bit-level alignment techniques which get transferred to the Gaussian model. A deterministic model with inter-dependent bit-levels, like the one used in [NMA13], could help to completely reach the upper bound. This would give a constant-gap sum-capacity result for the whole range.

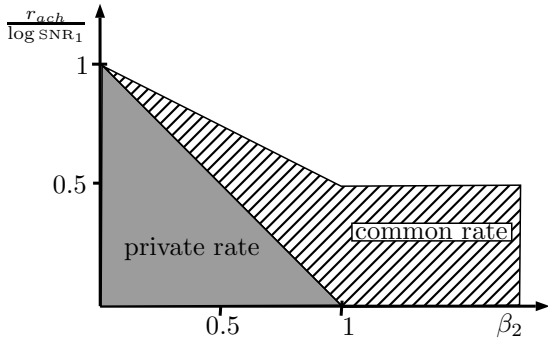

Figure 3.5.: Illustration of the achievable secrecy rate for the LD-WTH in relation to the single-link scenario, and variation in the β_2 parameter, while $\beta_1$is fixed at 0.75.

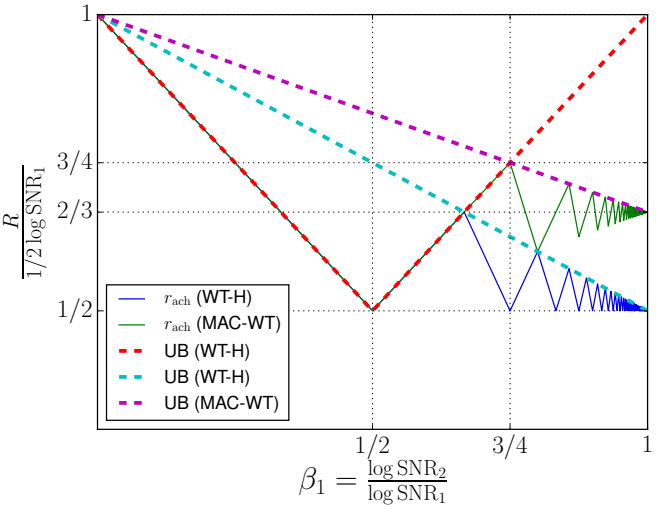

Figure 3.6.: Illustration of the achievable secrecy rates and upper bounds for the Gaussian WT-H and the Gaussian MAC-WT in relation to the single-link scenario, i.e. normalized by $\frac{1}{2} \log \mathrm{SNR}_1$, and variation in the β_1 parameter, while β_2 is fixed at 1, i.e. vanishing private part.

3.7. Proof of Theorem 3.7

Proof. We start as in [XU12] with the following procedure

$$\begin{aligned}
nR &= H(W|\mathbf{y}_1^n) + I(W;\mathbf{y}_1^n) \\
&\leq I(W;\mathbf{y}_1^n) + n\epsilon \\
&\leq I(W;\mathbf{y}_1^n) - I(W;\mathbf{y}_2^n) + n\epsilon_2 \\
&\leq I(W;\mathbf{y}_1^n) - I(W;\mathbf{y}_{2,[:n_2]}^n) + n\epsilon_2 \\
&= H(\mathbf{y}_1^n) - H(\mathbf{y}_1^n|W) - H(\mathbf{y}_{2,[:n_2]}^n) + H(\mathbf{y}_{2,[:n_2]}^n|W) + n\epsilon_2 \\
&= H(\mathbf{y}_1^n) - H(\mathbf{y}_{2,[:n_2]}^n) + H(\bar{\mathbf{x}}_{2,[:n_2]}^n) - H(\mathbf{x}_2^n) + n\epsilon_2
\end{aligned}$$

where Fanos inequality and the secrecy constraint was used. Moreover, we used the fact that $I(W;\mathbf{y}_2^n) \geq I(W;f(\mathbf{y}_2^n))$ for arbitrary functions f, due to the data processing inequality. Note that for $n_2 \geq n_E$, we have that $\mathbf{y}_{2,[:n_2]}^n = \mathbf{y}_2^n$. In the last line we used that X_1 is a function of W, and X_2 is independent of W. We remark that the first property does not hold in general, since jamming through the first user would result in a stochastic function. Now, for $n_E \geq n_2$, $\bar{\mathbf{x}}_{2,[:n_2]}^n = \mathbf{x}_2^n$ we have

$$H((\bar{\mathbf{x}}_2^n)_{[:n_2]}) - H(\mathbf{x}_2^n) = 0$$

and for $n_E < n_2$ we have $\bar{\mathbf{x}}_{2,[:n_2]}^n = \bar{\mathbf{x}}_2^n$ is a part of $\mathbf{x}_2^n$ and we can therefore show that

$$H(\bar{\mathbf{x}}_2^n) - H(\mathbf{x}_2^n) \leq -H((\mathbf{x}_2^n)_{[n_E+1:]}|(\mathbf{x}_2^n)_{[:n_E]}). \tag{3.24}$$

We now split the received signals in common and private parts. We start by adding two of the terms and show

$$\begin{aligned}
&2(H(\mathbf{x}_1^n \oplus \mathbf{x}_2^n) - H((\bar{\mathbf{x}}_1^n \oplus \bar{\mathbf{x}}_2^n)_{[:n_2]})) \\
&\leq 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[n_c+1:]}) + 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[:n_c]}) - 2H((\bar{\mathbf{x}}_1^n \oplus \bar{\mathbf{x}}_2^n)_{[:n_2]}).
\end{aligned}$$

Note that the private part $H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[n_c+1:]})$ is zero for $n_1 \leq n_E$. Now, counting from top to bottom, for $n_1 \geq n_2$, $\mathbf{x}_1^n$ has n_c bit-levels in $(\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[:n_c]}$, while $\mathbf{x}_2^n$ has $\eta := \min\{n_E, \min\{n_1, n_2\}\} = n_c - n_\Delta$ bit-levels. Therefore, η represents the amount of bit-levels of the weaker signal in the common received signal part. Hence, for $n_2 > n_1$, $\mathbf{x}_1^n$ and $\mathbf{x}_2^n$ have η and n_c bit-levels in that term, respectively. We need to account for this switch of indexing in the next part, where we analyse the entropy difference. We will use

a method inspired by [FW14a] to show the following (for $n_1 \geq n_2$)

$$\begin{aligned}
&2(H(\mathbf{x}_1^n \oplus \mathbf{x}_2^n) - H((\bar{\mathbf{x}}_1^n \oplus \bar{\mathbf{x}}_2^n))_{[:n_2]}) \\
&\leq 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[n_c+1:]}) + 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[:n_c]}) \\
&\quad - H((\bar{\mathbf{x}}_1^n \oplus \bar{\mathbf{x}}_2^n)_{[:n_2]}|\bar{\mathbf{x}}_1^n) - H((\bar{\mathbf{x}}_1^n \oplus \bar{\mathbf{x}}_2^n)_{[:n_2]}|\bar{\mathbf{x}}_2^n) \\
&= 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[n_c+1:]}) + 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[:n_c]}) - H((\bar{\mathbf{x}}_2^n)_{[:n_2]}) - H((\bar{\mathbf{x}}_1^n)_{[:n_2]}) \\
&\leq 2H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[n_c+1:]}) + H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[:n_c]}) + H(\mathbf{x}_{2,[:\eta]}^n) + H(\mathbf{x}_{1,[:n_c]}^n) \\
&\quad - H((\bar{\mathbf{x}}_2^n)_{[:n_2]}) - H((\bar{\mathbf{x}}_1^n)_{[:n_2]}),
\end{aligned}$$

We now have for $n_1 \geq n_2$ that

$$H(\mathbf{x}_{1,[1:n_c]}^n) - H((\bar{\mathbf{x}}_1^n)_{[:n_2]}) = n(n_c - \min\{n_2, n_E\})^+ \leq nn_\Delta,$$

and

$$H(\mathbf{x}_{2,[:\eta]}^n) - H((\bar{\mathbf{x}}_2^n)_{[:n_2]}) = n(\eta - \min\{n_2, n_E\})^+ = 0.$$

And for $n_2 > n_1$ we get

$$H(\mathbf{x}_{1,[1:\eta]}^n) - H((\bar{\mathbf{x}}_1^n)_{[:n_2]}) = n(\eta - \min\{n_2, n_E\})^+ = 0,$$

and

$$H(\mathbf{x}_{2,[:n_c]}^n) - H((\bar{\mathbf{x}}_2^n)_{[:n_2]}) = n(n_c - \min\{n_2, n_E\})^+. \tag{3.25}$$

We remark that the last term (3.25) gets $(n_2 - n_E)^+$ for $n_1 < n_E < n_2$, in which case we can use (3.24), which has a length of $(n_2 - n_E)$ bit-levels. Also for $n_E < n_1 < n_2$ we have that $n(n_c - \min\{n_2, n_E\})^+ = nn_\Delta$, by using (3.24) again, we see that for $n_2 > n_1$

$$H(\mathbf{x}_{2,[:n_c]}^n) - H((\bar{\mathbf{x}}_2^n)_{[:n_2]}) = n(n_c - \min\{n_2, n_E\})^+ = 0.$$

We therefore have an additional term of nn_Δ for $n_1 \geq n_2$. Now one can divide all terms by two, resulting in

$$\begin{aligned}
&H(\mathbf{y}_1^n) - H(\mathbf{y}_2^n) \\
&\leq H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[n_c+1:]}) + \frac{1}{2}H((\mathbf{x}_1^n \oplus \mathbf{x}_2^n)_{[:n_c]}) + \frac{n}{2}(n_1 - n_2)^+.
\end{aligned}$$

Plugging all the results into the first equation yields

$$\begin{aligned}
nR &\leq H(\mathbf{y}_1^n) - H(\mathbf{y}_2^n) + H(\bar{\mathbf{x}}_2^n) - H(\mathbf{x}_2^n) + n\epsilon_2 \\
&\leq n(n_p + \tfrac{1}{2}n_c + \tfrac{1}{2}(n_1 - n_2)^+ + \epsilon_2).
\end{aligned}$$

dividing by n and letting $n \to \infty$ shows the result. For the case that $n_2 > 2n_1$ we have that

$$\begin{aligned} n(R-\epsilon_2) &\leq H(\mathbf{y}_1^n) - H(\mathbf{y}_2^n) + H(\bar{\mathbf{x}}_2^n) - H(\mathbf{x}_2^n) \\ &\leq H(\mathbf{x}_1^n) + H(\mathbf{x}_2^n) - H(\mathbf{y}_2^n|\bar{\mathbf{x}}_1^n) + H(\bar{\mathbf{x}}_2^n) - H(\mathbf{x}_2^n) \\ &= H(\mathbf{x}_1^n) \leq nn_1 \end{aligned}$$

and for the case that $3n_2 < 2n_1$ we have that

$$\begin{aligned} nR &\leq I(W;\mathbf{y}_1^n) - I(W;\mathbf{y}_2^n) + n\epsilon_2 \\ &\leq I(W;\mathbf{y}_1^n) - I(W;\mathbf{y}_{2,[:n_1-n_2]}^n) + n\epsilon_2 \\ &\leq H(\mathbf{y}_1^n) - H(\mathbf{y}_{2,[:n_1-n_2]}^n) + H(\bar{\mathbf{x}}_{2,[:n_1-n_2]}^n) - H(\mathbf{x}_2^n) + n\epsilon_2 \\ &\leq H(\mathbf{y}_{1,[:(n_1-n_2)]}^n) + H(\mathbf{y}_{1,[n_1-n_2)+1:]}^n|\mathbf{y}_{1,[:n_1-n_2]}^n) \\ &\quad - H(\mathbf{y}_{2,[:n_1-n_2]}^n|\mathbf{x}_2^n) + H(\bar{\mathbf{x}}_{2,[:n_1-n_2]}^n) - H(\mathbf{x}_2^n) + n\epsilon_2 \end{aligned}$$

One can show that

$$H(\mathbf{y}_{1,[:n_1-n_2]}^n) - H(\mathbf{y}_{2,[:n_1-n_2]}^n|\mathbf{x}_2^n) \leq n(n_1-n_2-n_E)^+$$

and

$$\begin{aligned} &H(\bar{\mathbf{x}}_{2,[:n_1-n_2]}^n) - H(\mathbf{x}_2^n) \\ &\leq n(\min\{n_1-n_2, n_E\} - n_2) = n[n_E - n_2 - (n_E - n_1 + n_2)^+]^+ \end{aligned}$$

and $H(\mathbf{y}_{1,[(n_{11}-n_{21})+1:]}^n|\mathbf{y}_{1,[:(n_{11}-n_{21})]}^n) \leq nn_2$ which yields

$$nR \leq nn_2 + n(n_1-n_2-n_2)^+ + + n[n_E - n_2 - (n_E - n_1 + n_2)^+]^+ + n\epsilon_2$$

dividing by n and letting $n \to \infty$ shows the result. □

3.8. Proof of Theorem 3.8

Proof. We start with some general observations and derivations before handling the different cases explicitly. We begin with the following derivations

$$\begin{aligned} n(R_1+R_2) &= H(W_1,W_2) \\ &= H(W_1,W_2|\mathbf{y}_1^n) + I(W_1,W_2;\mathbf{y}_1^n) \end{aligned}$$

$$
\begin{aligned}
&\leq I(W_1, W_2; \mathbf{y}_1^n) + n\epsilon \\
&\overset{(a)}{\leq} I(W_1, W_2; \mathbf{y}_1^n) - I(W_1, W_2; \mathbf{y}_2^n) + n\epsilon_2 \\
&\leq I(W_1, W_2; \mathbf{y}_1^n, \mathbf{y}_2^n) - I(W_1, W_2; \mathbf{y}_2^n) + n\epsilon_2 \\
&\leq I(W_1, W_2; \mathbf{y}_1^n | \mathbf{y}_2^n) + n\epsilon_2 \\
&\leq I(\mathbf{x}_1^n, \mathbf{x}_2^n; \mathbf{y}_1^n | \mathbf{y}_2^n) + n\epsilon_2 \\
&= H(\mathbf{y}_1^n | \mathbf{y}_2^n) - H(\mathbf{y}_1^n | \mathbf{y}_2^n, \mathbf{x}_1^n, \mathbf{x}_2^n) + n\epsilon_2 \\
&\overset{(b)}{=} H(\mathbf{y}_1^n | \mathbf{y}_2^n) + n\epsilon_2 \\
&\leq H(\mathbf{y}_{1,c}^n | \mathbf{y}_2^n) + H(\mathbf{y}_{1,p}^n | \mathbf{y}_2^n, \mathbf{y}_{1,c}^n) + n\epsilon_2
\end{aligned} \tag{3.26}
$$

where we used basic techniques such as Fano's inequality and the chain rule. Step (a) introduces the secrecy constraint (3.1), while we used the chain rule, non-negativity of mutual information and the data processing inequality in the following lines. Step (b) follows from the fact that $\mathbf{y}_1^n$ is a function of $(\mathbf{x}_1^n, \mathbf{x}_2^n)$. Note that due to the definition of the common and the private part[7] of $\mathbf{y}_1^n$, it follows that $H(\mathbf{y}_{1,p}^n | \mathbf{y}_2^n, \mathbf{y}_{1,c}^n) = 0$ for $n_E \geq n_2$. We now extend the strategy of [XU14], of bounding a single signal part, to asymmetrical channel gains

$$
\begin{aligned}
nR_1 &= H(W_1) \\
&\leq I(W_1; \mathbf{y}_1^n) - n\epsilon_3 \\
&\leq I(\mathbf{x}_1^n; \mathbf{y}_1^n) - n\epsilon_3 \\
&= I(\mathbf{x}_1^n; \mathbf{y}_{1,c}^n) + I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n) - n\epsilon_3 \\
&= H(\mathbf{y}_{1,c}^n) - H(\mathbf{y}_{1,c}^n | \mathbf{x}_1^n) + I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n) - n\epsilon_3 \\
&= H(\mathbf{y}_{1,c}^n) - H(\mathbf{x}_{2,c}^n) + I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n) - n\epsilon_3
\end{aligned}
$$

and it therefore holds that

$$
H(\mathbf{x}_{2,c}^n) \leq H(\mathbf{y}_{1,c}^n) + I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n) - n(R_1 + \epsilon_3). \tag{3.27}
$$

The same can be shown for $H(\mathbf{x}_{1,c}^n)$, where it holds that

$$
H(\mathbf{x}_{1,c}^n) \leq H(\mathbf{y}_{1,c}^n) + I(\mathbf{x}_2^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n) - n(R_2 + \epsilon_4). \tag{3.28}
$$

Moreover, we have that

$$
I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n) + I(\mathbf{x}_2^n; \mathbf{y}_{1,p}^n | \mathbf{y}_{1,c}^n)
$$

[7] The common part is defined as $\mathbf{y}_{1,c}^n = \mathbf{y}_{1,[:n_c]}^n$, and the private part as $\mathbf{y}_{1,p}^n = \mathbf{y}_{1,[n_c+1:]}^n$.

$$
\begin{aligned}
&= 2H(\mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) - H(\mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n, \mathbf{x}_1^n) - H(\mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n, \mathbf{x}_2^n) \\
&= 2H(\mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) - H(\mathbf{x}_{2,p}^n|\mathbf{y}_{1,c}^n) - H(\mathbf{x}_{1,p}^n|\mathbf{y}_{1,c}^n) \\
&= H(\mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n). \qquad (3.29)
\end{aligned}
$$

The key idea for the various cases is now to bound the term $H(\mathbf{y}_{1,c}^n|\mathbf{y}_2^n)$, or equivalently $H(\mathbf{y}_1^n|\mathbf{y}_2^n)$ for $n_E > n_2$, in an appropriate way, to be able to use (3.27) and (3.28) on (3.26). We start with the first case:

Case 1 ($n_2 \geq n_E$)

Here we have a none vanishing private part, due to the definition of $\mathbf{y}_{1,c}^n$ and therefore need to bound the term $H(\mathbf{y}_{1,c}^n|\mathbf{y}_2^n)$. Note that due to the definition of $\mathbf{y}_{1,c}^n$ we have that $H(\mathbf{x}_{2,c}^n) = H(\bar{\mathbf{x}}_2^n)$. We look into the first term of equation (3.26) and show that

$$
\begin{aligned}
H(\mathbf{y}_{1,c}^n|\mathbf{y}_2^n) &= H(\mathbf{y}_{1,c}^n, \mathbf{y}_2^n) - H(\mathbf{y}_2^n) \\
&\leq H(\mathbf{y}_{1,c}^n, \bar{\mathbf{x}}_1^n, \bar{\mathbf{x}}_2^n) - H(\mathbf{y}_2^n) \\
&= H(\bar{\mathbf{x}}_1^n, \bar{\mathbf{x}}_2^n) + H(\mathbf{y}_{1,c}^n|\bar{\mathbf{x}}_1^n, \bar{\mathbf{x}}_2^n) - H(\mathbf{y}_2^n) \\
&\leq H(\bar{\mathbf{x}}_1^n) + H(\bar{\mathbf{x}}_2^n) - H(\mathbf{y}_2^n|\bar{\mathbf{x}}_2^n) + H(\mathbf{y}_{1,c}^n|\bar{\mathbf{x}}_1^n, \bar{\mathbf{x}}_2^n) \\
&= H(\bar{\mathbf{x}}_2^n) + H(\mathbf{y}_{1,c}^n|\bar{\mathbf{x}}_1^n, \bar{\mathbf{x}}_2^n). \qquad (3.30)
\end{aligned}
$$

Observe that the second term of equation (3.30) is depended on the specific regime. We can bound this term by

$$H(\mathbf{y}_{1,c}^n|\bar{\mathbf{x}}_1^n, \bar{\mathbf{x}}_2^n) \leq n(n_c - n_E) = nn_\Delta.$$

Note that the choice of $\bar{\mathbf{x}}_2^n$ in (3.30) as remaining signal part was arbitrary due to our assumption that both signals $\bar{\mathbf{x}}_1^n$ and $\bar{\mathbf{x}}_2^n$ have the same signal strength. Moreover, it follows on the same lines that

$$H(\mathbf{y}_{1,c}^n|\mathbf{y}_2^n) \leq H(\bar{\mathbf{x}}_1^n) + nn_\Delta.$$

Looking at this result, its intuitive that one can also show the stronger result

$$H(\mathbf{y}_{1,c}^n|\mathbf{y}_2^n) \leq H(\mathbf{x}_{1,c}^n)$$

for the case that $n_2 \geq n_E$. This can be shown by considering a similar strategy as in (3.30)

$$
\begin{aligned}
H(\mathbf{y}_{1,c}^n|\mathbf{y}_2^n) &= H(\mathbf{y}_{1,c}^n, \mathbf{y}_2^n) - H(\mathbf{y}_2^n) \\
&\leq H(\mathbf{y}_2^n, \mathbf{x}_{1,c}^n, \mathbf{x}_{2,c}^n) - H(\mathbf{y}_2^n)
\end{aligned}
$$

$$
\begin{aligned}
&= H(\mathbf{x}_{1,c}^n, \mathbf{x}_{2,c}^n) + H(\mathbf{y}_2^n|\mathbf{x}_{1,c}^n, \mathbf{x}_{2,c}^n) - H(\mathbf{y}_2^n) \\
&\leq H(\mathbf{x}_{1,c}^n) + H(\mathbf{x}_{2,c}^n) - H(\mathbf{y}_2^n|\mathbf{x}_{1,c}^n) + H(\mathbf{y}_2^n|\mathbf{x}_{1,c}^n, \mathbf{x}_{2,c}^n) \\
&= H(\mathbf{x}_{1,c}^n) + H(\mathbf{y}_2^n|\mathbf{x}_{1,c}^n, \mathbf{x}_{2,c}^n), \qquad (3.31)
\end{aligned}
$$

where

$$H(\mathbf{y}_2^n|\mathbf{x}_{1,c}^n, \mathbf{x}_{2,c}^n) \leq n(n_E - n_2)^+ = 0.$$

We combine one sum-rate inequality (3.26) with (3.30) and one with (3.31). Moreover, we plug (3.27) and (3.28) into the corresponding bound, which yields

$$n(2R_1 + R_2 - \epsilon_6) \leq H(\mathbf{y}_{1,c}^n) + I(\mathbf{x}_2^n; \mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) + H(\mathbf{y}_{1,p}^n|\mathbf{y}_2^n, \mathbf{y}_{1,c}^n)$$

and

$$n(R_1 + 2R_2 - \epsilon_7) \leq H(\mathbf{y}_{1,c}^n) + I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) + H(\mathbf{y}_{1,p}^n|\mathbf{y}_2^n, \mathbf{y}_{1,c}^n) + nn_\Delta.$$

A summation of these results gives

$$
\begin{aligned}
3n(R_1 + R_2) - n\epsilon_8 \leq\ & 2H(\mathbf{y}_{1,c}^n) + I(\mathbf{x}_1^n; \mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) + 2H(\mathbf{y}_{1,p}^n|\mathbf{y}_2^n, \mathbf{y}_{1,c}^n) \\
&+ I(\mathbf{x}_2^n; \mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) + nn_\Delta.
\end{aligned}
$$

Using (3.29), and the fact that $H(\mathbf{y}_{1,p}^n|\mathbf{y}_2^n, \mathbf{y}_{1,c}^n) \leq nn_p$ and $H(\mathbf{y}_{1,p}^n|\mathbf{y}_{1,c}^n) \leq nn_p$ results in

$$3n(R_1 + R_2) - n\epsilon_8 \leq 2H(\mathbf{y}_{1,c}^n) + 3nn_p + nn_\Delta \leq 2nn_c + 3nn_p + nn_\Delta.$$

Dividing by $3n$ and letting $n \to \infty$ shows the result.

Case 2 ($n_E > n_2$)

First, we assume that $n_E \geq n_1$, and include a short proof for $n_1 > n_E \geq n_2$ at the end of this subsection. For Case 2, the private part $\mathbf{y}_{1,p}$ is zero, due to the definition of the private part and $n_E > n_2$. It follows that (3.26) is

$$n(R_1 + R_2) \leq H(\mathbf{y}_1^n|\mathbf{y}_2^n). \qquad (3.32)$$

Moreover, $H(\mathbf{x}_2^n) = H(\mathbf{x}_{2,c}^n) \leq H(\bar{\mathbf{x}}_2^n)$, which is why we need to bound (3.32) by $H(\mathbf{x}_2^n)$ and $H(\mathbf{x}_1^n)$. We therefore modify (3.31) to fit our purpose in the following way

$$\begin{aligned}
H(\mathbf{y}_1^n|\mathbf{y}_2^n) &= H(\mathbf{y}_1^n, \mathbf{y}_2^n) - H(\mathbf{y}_2^n) \\
&\leq H(\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\mathbf{y}_2^n|\mathbf{x}_1^n, \mathbf{x}_2^n) - H(\mathbf{y}_2^n) \\
&= H(\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\mathbf{y}_{2,c}^n|\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\mathbf{y}_{2,p}^n|\mathbf{x}_1^n, \mathbf{x}_2^n, \mathbf{y}_{2,c}^n) \\
&\quad - H(\mathbf{y}_{2,c}^n) - H(\mathbf{y}_{2,p}^n|\mathbf{y}_{2,c}^n) \\
&\leq H(\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\mathbf{y}_{2,c}^n|\mathbf{x}_1^n, \mathbf{x}_2^n) - H(\mathbf{y}_{2,c}^n),
\end{aligned}$$

where $\mathbf{y}_{2,c}^n = \mathbf{y}_{2,[:n_1]}^n$ and $\mathbf{y}_{2,p}^n = \mathbf{y}_{2,[n_1+1:]}^n$. Now, we can show that

$$\begin{aligned}
H(\mathbf{y}_1^n|\mathbf{y}_2^n) &\leq H(\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\mathbf{y}_{2,c}^n|\mathbf{x}_1^n, \mathbf{x}_2^n) - H(\mathbf{y}_{2,c}^n) \\
&= H(\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) - H(\mathbf{y}_{2,c}^n) \\
&\leq H(\mathbf{x}_1^n) + H(\mathbf{x}_2^n) - H(\mathbf{y}_{2,c}^n|\mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \\
&= H(\mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \\
&\leq H(\mathbf{x}_2^n) + nn_\Delta. \qquad (3.33)
\end{aligned}$$

Bounding $H(\mathbf{y}_1^n|\mathbf{y}_2^n)$ by $H(\mathbf{x}_1^n)$ requires more work. We have a redundancy in the negative entropy terms, with which we can cancel the $H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n)$ term in the following way

$$\begin{aligned}
H(\mathbf{y}_1^n|\mathbf{y}_2^n) &\leq H(\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) - H(\mathbf{y}_{2,c}^n) \\
&\leq H(\mathbf{x}_1^n) + H(\mathbf{x}_2^n) - H(\mathbf{y}_{2,c,[:n_2]}^n|\mathbf{x}_1^n) \\
&\quad + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) - H(\mathbf{y}_{2,c,[n_2+1:]}^n|\mathbf{x}_1^n, \mathbf{y}_{2,c,[:n_2]}^n) \\
&= H(\mathbf{x}_1^n) - H(\mathbf{y}_{2,c,[n_2+1:]}^n|\mathbf{x}_1^n, \mathbf{y}_{2,c,[:n_2]}^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \\
&\leq H(\mathbf{x}_1^n) - H(\mathbf{y}_{2,c,[n_2+1:]}^n|\mathbf{x}_1^n, \mathbf{y}_{2,c,[:n_2]}^n, \mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \\
&= H(\mathbf{x}_1^n) - H(\mathbf{y}_{2,c,[n_2+1:]}^n|\mathbf{x}_1^n, \mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \\
&= H(\mathbf{x}_1^n) - H(\hat{\mathbf{x}}_{2,c,[n_2+1:]}^n|\mathbf{x}_2^n) + H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \\
&= H(\mathbf{x}_1^n). \qquad (3.34)
\end{aligned}$$

Now we can bound one (3.32) with (3.33) and one with (3.34). Moreover, we use (3.27) and (3.28) on the result. Note that due to our regime, (3.27) becomes

$$H(\mathbf{x}_2^n) \leq H(\mathbf{y}_1^n) - n(R_1 + \epsilon_3),$$

while (3.28) becomes

$$H(\mathbf{x}_1^n) \leq H(\mathbf{y}_1^n) - n(R_2 + \epsilon_4).$$

Putting everything together results in

$$3n(R_1 + R_2) - n\epsilon_8 \leq 2H(\mathbf{y}_1^n) + nn_\Delta \leq 2nn_c + nn_\Delta.$$

Dividing by $3n$ and letting $n \to \infty$ shows the result.

We need to modify a bound on $H(\mathbf{y}_1^n|\mathbf{y}_2^n)$, if the signal strength n_E lies in between n_1 and n_2. In (3.33), we see that

$$H(\mathbf{x}_1^n) - H(\mathbf{y}_{2,c}^n|\mathbf{x}_2^n) \leq n(n_1 - n_E)^+.$$

Moreover, we have that $H(\bar{\mathbf{x}}_2^n|\mathbf{x}_2^n) \leq n(n_E - n_2)^+$. Both changes cancel and we get the same result as (3.33). The result follows on the same lines as in the previous derivation. □

4. Key Generation using the Wireless Channel

4.1. Introduction

With the advance of technology, new application scenarios such as the Internet of Things and others reinforce the need for new security paradigms which are unconditional on the eavesdropper such as information-theoretic security, also called physical layer security [Muk15]. Resulting techniques can be used, for example, for secure key agreement over the wireless channel, assuming that both parties are already authenticated. Key-agreement between two parties is a well-investigated topic, dating back to first works on the subject by [AC93] and [Mau93]. Those works focused on upper and lower bounds for various models of key-agreement and laid out the foundations for a systematic analysis. In [AC93], the key-agreement problem was split into two general models, source-type model and the channel-type model. In the source-type model, both parties, in the following called Alice and Bob, have access to a source of common randomness. In the channel model, Alice can communicate over a discrete memoryless channel to Bob. In both cases, both parties have access to a public insecure communication channel, which can be used to generate a common key from their observations. It has been shown, that the wireless channel can be exploited to generate a source of common randomness for Alice and Bob. The first rigorous works in this direction were [YRS06] and [WTS07]. The idea evolves around the reciprocity of the wireless channel, which states that the varying (due to fading) wireless channel is nearly the same in both directions. Now, pilot signals can be send by both terminals, such that the receivers can estimate the channel gain. Due to reciprocity, the channel gain becomes a source of common randomness and both Alice and Bob can estimate it. Furthermore, the estimates do not need to be perfect. By invoking Slepian-Wolf coding schemes with side-information, a single transmission, via the public channel, from Alice to Bob is sufficient to generate a common key at both terminals (see [AC93]). The drawback for practical purposes is that the entropy and length of the key depends on the randomness of the channel gain, which is dependent on the coherence time. A slowly varying channel provides less key-rate, which can become zero in worst case scenarios. Some works there-

fore focused on relay assisted key generation, mixed source-channel type key generation in [LLPD13], [LLP12] and local randomness aided scenarios in [WFK16], to overcome this problem. The latter work utilizes local randomness with a novel product signalling scheme to enhance the key generation for periods of static channel gain. However, the resulting rate expressions are non-trivial and closed-form solutions could not be obtained. This motivates the development of an approximate key generation model, which can incorporate those special cases. Another line of research focused on the inclusion of full-duplex channel modes into the security models. Recent advances, e.g. [Kha13], [DDS12], [BMK13], have shown that full-duplex wireless is a viable and practical technique for future communication systems. This opens up an interesting possibility to use full-duplex aided methods in security scenarios. A general model for the full-duplex secret messaging scenario is the two-way wiretap channel, where the users communicate over a noisy bidirectional channel, while the eavesdropper observes interfering signals. This model was first investigated in [TY08c], and subsequently studied in [PB11] and [GKYG13]. Recently, the trade-off between half-duplex and full-duplex key generation for pilot signalling was investigated in [VS15], where also results on the trade-off between channel probing and reconciliation were shown.

Contributions: The following chapter will describe work, which was originally motived by the fact that we could not show closed-form results for product signalling in [WFK16]. So we developed a model, closely related to the linear deterministic model [ADT11] and the lower triangular deterministic model [NMA13], which abstracts from the Gaussian channel by looking at the binary expansion of the signals and truncating the resulting bit-sequence such that they are noise-free. Moreover, as in the LTDM, the channel gain bits, the fine channel gain, is included in the model, since those bits will provide the common randomness in the channel and are used for standard key generation. However, unlike in the LTDM, we view this fine channel gain as random and try to extract the randomness for key generation. We can show several results for special cases and also recover pilot-signalling results of high SNR regimes. Moreover, we view those systems in half and full-duplex scenarios. We analyse the trade-of between half and full-duplex in the deterministic setting and derive results for the high SNR scenario. The model also provides a look into a secret messaging scheme for long coherence block lengths which utilizes cooperative jamming on bit-levels. It therefore bridges the gap between the linear deterministic secret messaging scenarios, e.g. [FW17c], and key generation. We show that this new model provides a simple and intuitive way to analyse these problems. The new model has several advantages due to its properties, e.g. public communication being obsolete and build-in quantization. We believe that the model can be useful in other scenarios too, e.g multi-user key generation.

4.2. Gaussian System Model

We denote the channel gain from Alice to Bob with h_{ab} and from Bob to Alice with h_{ba}. We assume reciprocity, meaning that within one channel use i, both h_{ab} and h_{ba} are the same[1]. Moreover, we assume that the channel gain is a fading parameter, changing randomly with a Gaussian distribution $h_{ab} \sim \mathcal{N}(0, \sigma^2_{h_{ab}})$ after an coherence block of T channel uses. Alice and Bob have an additional local source of randomness, ω_a and ω_b, respectively, which can be used for the inputs. Both communication channels are in presence of a wire-tapper Eve, which can receive Alice's input through a channel h_{ae} and Bob's input through a channel h_{be}.

Half-Duplex System: Alice communicates with Bob in a two-way non-duplex fashion. Looking at n total channel uses, both alternate in receive and transmit mode such that Alice sends signals to Bob at the odd channel uses while, Bob utilizes the even channel uses. We can therefore write the channel equations in the following way

$$Y_b = H_{ab}X_a + Z_1$$
$$Y_a = H_{ba}X_b + Z_2$$

and

$$Y_e = \begin{cases} H_{ae}X_a & \text{for } n \text{ odd} \\ H_{be}X_b & \text{for } n \text{ even.} \end{cases}$$

The system model is illustrated in Fig. 4.1. The figure also depicts the public noiseless channels Φ and Ψ, which are available for both Alice and Bob. We have t time instances in which we use the wireless channels n times and the public noiseless channels $k = t - n$ times, where $n \leq t$.

Full-Duplex System: Alice communicates with Bob in a two-way duplex fashion. We can therefore write the channel equations in the following way

$$Y_a = H_{ba}X_b + H_{Ia}X_a + Z_1^{'}$$
$$Y_b = H_{ab}X_a + H_{Ib}X_b + Z_2^{'}$$
$$Y_e = H_{ae}X_a + H_{be}X_b + Z_3,$$

[1] In the *fine* scale, which will be explained later

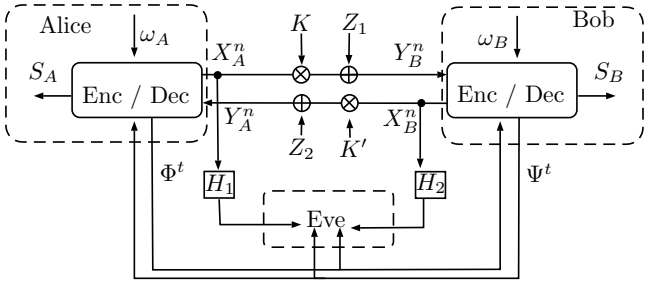

Figure 4.1.: Illustration of the half-duplex system model with (dashed communication) and without side information at Eve

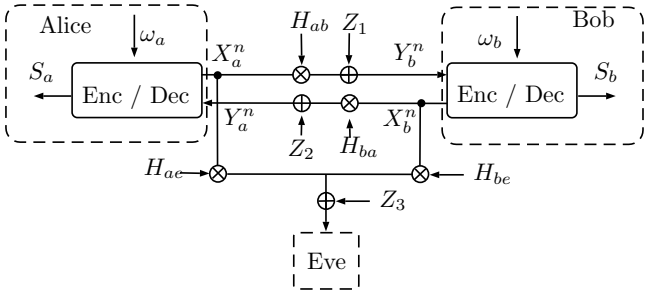

Figure 4.2.: Illustration of the full-duplex system model with (dashed communication) and without side information at Eve

where $Z_i' \sim \mathcal{N}(0,1)$ is Gaussian noise and H_{Ia}, H_{Ib} are the channel gains for the self-interference. Note that both nodes know their own codewords and can therefore cancel the self-interference [TY08c]. This leads to the following simplified model

$$\begin{aligned} Y_a &= H_{ba}X_b + Z_1 \\ Y_b &= H_{ab}X_a + Z_2 \\ Y_e &= H_{ae}X_a + H_{be}X_b + Z_3, \end{aligned}$$

with the Gaussian noise $Z_i \sim \mathcal{N}(0,1)$. The system model is illustrated in Fig. 4.2.

Key Generation and Secrecy Definitions There are n rounds of wireless communication, where in each round i Alice (Bob) sends a codeword $X_a(\omega_A, i)$ ($X_b(\omega_b, i)$) over the channel. We denote $X_a^n = (X_a(1), \cdots, X_a(n))$ and $X_b^n = (X_b(1), \cdots, X_b(n))$. We note that in the most general setting, there is also a public channel Φ^k and Ψ^k which can be used k times. This public channel can be used for key reconciliation, i.e. forging a shared key from two correlated random observations. Let f_a and f_b denote the key generation functions at Alice and Bob, respectively. We therefore have that the keys for Alice and Bob, are $S_a = f_a(X_a^n, Y_a^n, \Phi^k)$ and $S_b = f_b(X_b^n, Y_b^n, \Psi^k)$, respectively.

We define an achievable key rate R_{key} if for every $\epsilon > 0$ and sufficiently large n there exists a strategy such that S_a and S_b satisfy

$$\Pr\{S_a \neq S_b\} < \epsilon,$$

$$\tfrac{1}{n} I(\Phi^k, \Psi^k, Y_e^n; S_a) < \epsilon,$$

$$\tfrac{1}{n} H(S_a) > R_{key} - \epsilon,$$

$$\tfrac{1}{n} \log |S_a| < \tfrac{1}{n} H(S_a) + \epsilon,$$

where $|S_a|$ denotes the alphabet size of the discrete key random variable S_a, see also [AC93]. It was shown in [AC93] that if both terminals observe correlated source outputs X^n and Y^n from a discrete memoryless multiple source with generic sources (X, Y), a secrecy key rate of $I(X;Y)$ can be achieved. The proof uses only a single forward or backward transmission of the public channel along with an extended Slepian-Wolf coding scheme. Originally proved for discrete sources, this result can be extended to continuous sources as well [YRS06, Nit08]. Moreover, the result can be extended to the case of a pair of sources, for example (X_a, Y_a, X_b, Y_b). To see this, one can use the same idea as in [AC93], in conjunction with the Slepian-Wolf theorem for multiple sources.

Introducing Product Signalling: The idea in [WFK16] was to utilize the local randomness ω_A and ω_B such that Alice and Bob send random signals over the channel. Therefore, instead of measuring the channel gain H with pilot signalling alone, one gets a channel output Y_a and Y_b at Alice and Bob, respectively. Both of these are correlated via channel gain. To get some gain out of the local randomness, one also considers the local source of the sender. This means that Alice and Bob *virtually* receive (Y_a, X_a) and (Y_b, X_b), respectively. Now both sources are correlated in H, X_a and X_b. The main challenge was a practical way to reconcile observations of both Alice and Bob. A simple solution to this problem, also presented in [WFK16], was to multiply the observations to produce correlated observations of a source (X_aY_a, X_bY_b). This would yield a secure key rate of $I(Y_aX_a; Y_bX_b)$. However, exact calculation of the mutual information term $I(Y_aX_a; Y_bX_b)$ is involved, even for Gaussian signals. This is due to the multiplication operations which yield Bessel functions and to the best of our knowledge there is no known closed form solution for this term. However, we will approximate the term with the linear deterministic model to gain insights into its nature.

4.3. A Deterministic Model for Key Generation

We introduce a novel deterministic model for key generation, which is closely inspired by the linear deterministic [ADT11] and the lower triangular model [NMA13]. We refer the reader to section 1.4.1 and 1.4.2 for a short introduction to these approximation models. We assume that the input signals and the noise have a peak power constraint of one. That means, that the channel gains represent the signal-to-noise values and we therefore have the correspondence that $H = \sqrt{\text{SNR}}$. In the new model, all operations are over $\mathbb{F}_2$ and $\mathbf{x}_a, \mathbf{x}_b \in \mathbb{F}_2^q$ are the input bit vectors of Alice and Bob, which represent the first q bits of the binary expansion of the transmit signals X_a and X_b, where $q = \max\{N_{ab}, N_{ba}, N_{ae}, N_{ea}\}$. These bit vectors have a finite number of entries, since the noise effected bits are cut-off. Moreover, the channel gain is split into a coarse and a fine channel gain part, such that we have $H = 2^N h$, where $N \in \mathbb{N}$ and $h \in (1, 2]$, which can model any channel gain greater than one. Note, that we model reciprocity such that the channel gain is the same in the fine channel gain h, but differs in the coarse gain N. This allows us to model different signal scales for transmission, since signal transmit power induces the specific coarse gain. We use the function $T_{lt}(\mathbf{x}) = \mathbf{X}$ which maps a bit-vector $\mathbf{x}$ to its square lower triangular Toeplitz matrix $\mathbf{X}$:

$$T_{lt}(\mathbf{x}) = \mathbf{X} = \begin{pmatrix} [x]_1 & 0 & \cdots & 0 & 0 \\ [x]_2 & [x]_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ [x]_{q-1} & [x]_{q-2} & \cdots & [x]_1 & 0 \\ [x]_q & [x]_{q-1} & \cdots & [x]_2 & [x]_1 \end{pmatrix},$$

where $[x]_i$, for $i \in \{1, \cdots, q\}$, denotes the i-th bit of the binary expansion of X and therefore the i-th element of the bit-vector $\mathbf{x}$. Moreover, $T_{lt}^{-1}(\mathbf{X}) = \mathbf{X}\mathbf{e}_1 = \mathbf{x}$ maps a lower triangular Toeplitz matrix back to its vector

$$T_{lt}^{-1} \begin{bmatrix} [x]_1 & 0 & 0 & 0 \\ [x]_2 & [x]_1 & 0 & 0 \\ [x]_3 & [x]_2 & [x]_1 & 0 \\ [x]_4 & [x]_3 & [x]_2 & [x]_1 \end{bmatrix} = \begin{bmatrix} [x]_1 & 0 & 0 & 0 \\ [x]_2 & [x]_1 & 0 & 0 \\ [x]_3 & [x]_2 & [x]_1 & 0 \\ [x]_4 & [x]_3 & [x]_2 & [x]_1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} [x]_1 \\ [x]_2 \\ [x]_3 \\ [x]_4 \end{bmatrix}.$$

Here we used $\mathbf{e}_1$ to indicate the first column vector of the identity matrix with dimension q. The bits of h can then be represented in a lower uni-triangular[2] Toeplitz matrix $T_{lt}(\mathbf{h})$. Whereas the multiplication with the coarse gain 2^N is modelled algebraically by

[2]The resulting matrix is uni-triangular, i.e. all 1's on the diagonal, since $h \in (1, 2]$

the multiplication with an $q \times q$ down-shift matrix $\mathbf{S}^{q-N}$

$$\mathbf{S} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

which shifts a vector for $q - N$ position downwards. Note that we neglect channel gains smaller than one, which is sufficient for high SNR regimes. Our approximation model also aims for an analysis of the high SNR behaviour. Note that the correspondence towards the SNR for the deterministic models is $N = \lfloor \frac{1}{2} \log \mathrm{SNR} \rfloor$.

The full-duplex model can be written as

$$\begin{aligned} \mathbf{y}_a &= \mathbf{S}^{q-N_{ba}} \mathbf{H}_{ba} \mathbf{x}_b \\ \mathbf{y}_b &= \mathbf{S}^{q-N_{ab}} \mathbf{H}_{ab} \mathbf{x}_a \\ \mathbf{y}_e &= \mathbf{S}^{q-N_{ae}} \mathbf{H}_{ae} \mathbf{x}_a \oplus \mathbf{S}^{q-N_{be}} \mathbf{H}_{be} \mathbf{x}_b, \end{aligned}$$

while **the half-duplex model** can be written as

$$\begin{aligned} \mathbf{y}_b &= \mathbf{S}^{q-N_{ab}} \mathbf{H}_{ab} \mathbf{x}_a \\ \mathbf{y}_a &= \mathbf{S}^{q-N_{ba}} \mathbf{H}_{ba} \mathbf{x}_b \end{aligned}$$

Note that for the half-duplex system we assume a time division in which a transceiver can either receive or transmit. Both Alice and Bob alternate in receive and transmit mode. Alice uses the odd n channel uses for transmission, while Bob uses the even n channel uses for transmission. Therefore Eve observes

$$\mathbf{y}_e = \begin{cases} \mathbf{S}^{q-N_{ae}} \mathbf{H}_{ae} \mathbf{x}_a & \text{for } n \text{ odd} \\ \mathbf{S}^{q-N_{be}} \mathbf{H}_{be} \mathbf{x}_b & \text{for } n \text{ even.} \end{cases}$$

Secrecy Constraints: Due to the deterministic nature of the model for key exchange we can make simplifications on the security constraints. We define an achievable deterministic key rate R_d if for every $\epsilon > 0$ and sufficiently large n there exists a strategy such that both generated keys at Alice and Bob, denoted by $\mathbf{s}_A$ and $\mathbf{s}_B$, respectively, satisfy

$$\Pr\{\mathbf{s}_A \neq \mathbf{s}_B\} = 0,$$

$$\frac{1}{n}H(\mathbf{s}_A) > R_d - \epsilon,$$
$$\frac{1}{n}\log|\mathbf{s}_A| < \frac{1}{n}H(\mathbf{s}_A) + \epsilon,$$

where $|\mathbf{s}_A|$ counts the bits in the binary random vector $\mathbf{s}_A$. Moreover, we define a secure deterministic key rate R_{sd} as the key rate R_d with the following security constaint

$$\frac{1}{n}I(\mathbf{y}_E^n; \mathbf{s}_A) = 0. \tag{4.1}$$

Note that we put a stricter notion on the difference between both keys. Moreover, we do not need a public communication channel. At last, Eq. (4.1) evokes a so-called perfect security condition in contrast to weaker standard notions. All of these changes can be achieved with no further struggles due to the lack of noise in the model, which explains the modified security condition.

Remark 4.1. The coherence block length T is a rather coarse measure of the randomness and dynamics of the channel gain. The deterministic channel model can support a finer notion, where one can look at the correlation of each bit-level, instead of only the whole bit-vector. This would yield a smooth characterization of the transition from completely static channel gain, to a completely random channel gain.

Remark 4.2. Total independence of Eve's channel gain and the channel gain between Alice and Bob is an idealistic scenario. Realistic channel gain scenarios might be different, in the sense that both channel gains share some characteristics. This opens up attack scenarios, for example in case of insufficient quantization. Our model, which has the built-in quantization i.e. bit-levels, can help to analyse these scenarios. A possible constraint could be that the top m bit-levels have some correlation with Eve and should therefore be avoided for key generation.

4.4. Achievable Key Rates

In this section, we will analyse some secure key generation schemes for the full-duplex and the half-duplex channel settings within the deterministic channel model. Moreover we will see, that the most prominent advantage of full duplex is that we only need one channel use or time instance for a complete key exchange.

4.4.1. Pilot Signalling

The classical approach for key exchange within a wireless medium is to use pilot signalling. With this scheme, both users send a pre-defined pilot signal over the wireless channel to

each other. The idea is now, that the pilot signal measures the channel gain, which is a random variable in a fading environment that changes after a coherence block of T channel uses. Therefore, both users, Alice and Bob, receive the measured channel gain H and H', respectively. Note that we assume reciprocity, this means that both channel gains noisy versions of each other with high correlation. It was shown in [AC93], that these correlated random variables can be used to produce a common key with a rate of $I(H;H')$, by using a single reconciliation transmission over an insecure public channel. We can model pilot signalling by transmitting a basis vector $\mathbf{e}_1$ over the channel with power N. We therefore have that

$$\mathbf{y}_a = \mathbf{S}^{q-N_{ba}}\mathbf{H}_{ba}\mathbf{x}_b = \mathbf{S}^{q-N_{ba}}\mathbf{H}_{ba}\mathbf{e}_1$$

Notice that $\mathbf{H}_{ba}\mathbf{e}_1 = T_{lt}^{-1}(\mathbf{H}_{ba}) = \mathbf{h}_{ba}$ is a q-bit-vector containing the bits of h_{ba}, which gets downshifted by $q - N_{ba}$ bit-levels, resulting in N_{ba} received channel gain bits. Note that due to our assumptions on reciprocity, we have that $h_{ab} = h_{ba} = h$. Therefore, both users receive the same bit-vector, which is just differing in the number of bits N_{ab} and N_{ba}. Since both users have perfect channel gain knowledge of the coarse gains, they can extract the minimum mutually received channel gain bits. This yields a secure key rate of

$$R_{sd} = \frac{1}{T}\min\{N_{ba}, N_{ab}\},$$

in the full-duplex deterministic case. For the real Gaussian case, this would correspond to a rate of

$$R_{sd} = \tfrac{1}{2T}\min\{\log \mathrm{SNR}_{ba}, \log \mathrm{SNR}_{ab}\}.$$

For the half-duplex model we have a secure key rate of

$$R_{sd} = \tfrac{1}{2T}\min\{N_{ba}, N_{ab}\},$$

which introduces a factor of two since two channel uses are needed for the key exchange. If the general noise power does not increase, due to self-interference cancellation, than the full-duplex key rate is two times higher than the half-duplex secret key rate, which is expected. Note that we did not need to check the secrecy property 4.1, since the channel gain between Alice and Bob is assumed to be independent of Eves channel gain. This means that Eves received signal is also independent of the key. We see that using the deterministic model has two advantages. The first one is that due to the deterministic nature, no public communication is needed to reconcile the keys. The second advantage is that the binary expansion introduces a natural quantization which is fine enough to

combat the noise. As a result, the observations at Alice and Bob can be used as a key without further post-processing.

4.4.2. Key Exchange by Product Signalling

Assume that we do not send pilot signals over the channel, but generate a random number which is send over the channel. In that case both Alice and Bob receive a $\mathbf{y}$ which is the discrete convolution between the bits of a signal $\mathbf{x}$ and the bits of the channel gain $T_{lt}^{-1}(\mathbf{K})$. Generating a signal $\mathbf{x}_A$ and $\mathbf{x}_B$ and sending it over the respective channel produces two different observations $\mathbf{y}_A$ and $\mathbf{y_B}$. However, since the receivers Alice and Bob, know their own signal, they can multiply the observation from the left with $T_{lt}(\mathbf{x}_A)$ and $T_{lt}(\mathbf{x}_B)$, respectively. This yields the following two observations

$$T_{lt}(\mathbf{x}_a)\mathbf{y}_a = T_{lt}(\mathbf{x}_a)\mathbf{S}^{q-N_{ba}}\mathbf{H}_{ba}\mathbf{x}_b$$
$$T_{lt}(\mathbf{x}_b)\mathbf{y}_b = T_{lt}(\mathbf{x}_b)\mathbf{S}^{q-N_{ab}}\mathbf{H}_{ab}\mathbf{x}_a.$$

The following lemma will show, that both modified observations are the same.

Lemma 4.3. *For arbitrary binary vectors* $\mathbf{x}_A, \mathbf{y}_A \in \mathbb{F}_2^n$ *and* $\mathbf{x}_B, \mathbf{y}_B \in \mathbb{F}_2^m$*, and truncated vectors* $\bar{\mathbf{x}}_A, \bar{\mathbf{y}}_A, \bar{\mathbf{x}}_B, \bar{\mathbf{y}}_B \in \mathbb{F}_2^{\min\{n,m\}}$ *we have that*

$$T_{lt}(\bar{\mathbf{x}}_B)\bar{\mathbf{y}}_B = T_{lt}(\bar{\mathbf{x}}_A)\bar{\mathbf{y}}_A.$$

Proof. First of all we note that the product of a lower triangular Toeplitz matrix with a vector is commutative. The operation mimics the product of two polynomials, where the result follows from the commutativity of the product of polynomials. Alternatively, one can think about this product as a discrete convolution, which is also commutative. Truncating the matrix such that it has the same dimension as the vector squared does not change this fact. This means that for arbitrary binary vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^q$ we have that

$$T_{lt}(\mathbf{x})\mathbf{y} = T_{lt}(\mathbf{y})\mathbf{x}. \tag{4.2}$$

We know that $T_{lt}(\mathbf{x})\mathbf{y} = T_{lt}(\mathbf{x})T_{lt}(\mathbf{y})e_1$ and that $T_{lt}(\mathbf{y})\mathbf{x} = T_{lt}(\mathbf{y})T_{lt}(\mathbf{x})e_1$ and we therefore have that

$$T_{lt}(\mathbf{x})T_{lt}(\mathbf{y})e_1 = T_{lt}(\mathbf{y})T_{lt}(\mathbf{x})e_1,$$

which shows that

$$T_{lt}(\mathbf{x})T_{lt}(\mathbf{y}) = T_{lt}(\mathbf{y})T_{lt}(\mathbf{x}) \tag{4.3}$$

and therefore the commutativity of the squared lower triangular matrices. Now we can proceed to show the lemma. We have that

$$\begin{aligned} T_{lt}(\bar{\mathbf{x}}_B)\bar{\mathbf{y}}_B &= T_{lt}(\bar{\mathbf{x}}_B)\bar{\mathbf{H}}_{ab}\bar{\mathbf{x}}_A \\ &\overset{(a)}{=} T_{lt}(\bar{\mathbf{x}}_B)T_{lt}(\bar{\mathbf{x}}_A)T_{lt}^{-1}(\bar{\mathbf{H}}_{ab}) \\ &\overset{(b)}{=} T_{lt}(\bar{\mathbf{x}}_A)T_{lt}(\bar{\mathbf{x}}_B)T_{lt}^{-1}(\bar{\mathbf{H}}_{ab}) \\ &\overset{(c)}{=} T_{lt}(\bar{\mathbf{x}}_A)T_{lt}(\bar{\mathbf{x}}_B)T_{lt}^{-1}(\bar{\mathbf{H}}_{ba}) \\ &= T_{lt}(\bar{\mathbf{x}}_A)\bar{\mathbf{H}}_{ba}\bar{\mathbf{x}}_B \\ &= T_{lt}(\bar{\mathbf{x}}_A)\bar{\mathbf{y}}_A, \end{aligned}$$

where (a) is due to eq. (4.2), (b) is due to eq. (4.3) and (c) is due to reciprocity of the fine channel gain. Note that the coarse channel gains match as well, since we are looking at a truncated channel gain matrix. □

This lemma shows that cutting-off bits as needed for rescaling, results in a common bit-sequence which can be used as a key. We therefore have a key $\mathbf{y} = \mathbf{D}^{q-N}T_{lt}(\mathbf{x}_a)\mathbf{H}\mathbf{x}_b$, while Eve observes $\mathbf{z} = \mathbf{D}^{q-N_{ae}}\mathbf{H}_{ae}\mathbf{x}_a \oplus \mathbf{D}^{q-N_{be}}\mathbf{H}_{be}\mathbf{x}_b$, where $N := \min\{N_{ab}, N_{ba}\}$ and $\mathbf{H} := \mathbf{H}_{ab} = \mathbf{H}_{ba}$. An exact analysis of the scheme remains elusive, and we only see a possible gain in a mixed regime, where some channel gain bits are random and some are fixed. The following special case shows, that Eve can gain some information about the key in a purely fixed channel gain scenario:

Security for static channel gain scenarios

An intriguing scenario is the case that all channel gains are fixed, and the channel gain matrices can be represented by the identity matrix. Note that modelling the channel gain by the identity matrix does not change the entropy of the observations in comparison to a fixed (constant) one, since fixed lower triangular toeplitz matrices are bijective mappings.
Full Duplex: The model for the full duplex scenario is then

$$\begin{aligned} \mathbf{y}_a &= \mathbf{S}^{q-N_{ba}}\mathbf{I}_{ba}\mathbf{x}_b \\ \mathbf{y}_b &= \mathbf{S}^{q-N_{ab}}\mathbf{I}_{ab}\mathbf{x}_a \\ \mathbf{y}_e &= \mathbf{S}^{q-N_{ae}}\mathbf{I}_{ae}\mathbf{x}_a \oplus \mathbf{S}^{q-N_{be}}\mathbf{I}_{be}\mathbf{x}_b. \end{aligned}$$

If the channel to Eve is symmetric,i.e $N_{ae} = N_{be}$, she would observe the modulo two summation of both input signal vectors $\mathbf{x}_a$ and $\mathbf{x}_b$. Moreover, Alice and Bob can use product

signalling and get the discrete convolution of both signals $T_{lt}(\mathbf{x}_a)\mathbf{x}_b$. One might think to design two Bern(1/2) bit-strings, such that they jam each other, and use the product signalling approach to recover them. The question is now, is this key secure? We need to look into the mutual information between the key and Eves observation: $I(T_{lt}(\mathbf{x}_a)\mathbf{x}_b; \mathbf{x}_a \oplus \mathbf{x}_b)$. The first bit of the key is $x_{b,1}x_{a,1} =: y_{\odot}$, while the observation of Eve, about those bits, is $x_{b,1} \oplus x_{a,1} =: y_{\oplus}$. One can now calculate $I(y_{\oplus}; y_{\odot}) \approx 0.31 > 0$ and see that it is strictly greater than zero. We will show later, that in case of fixed channel gains, it is sufficient to utilize jamming on bit-levels together with secure messaging.

Half Duplex: The model for the half duplex scenario with identity matrix channel gain matrices is

$$\mathbf{y}_b = \mathbf{S}^{q-N_{ba}}\mathbf{I}_{ab}\mathbf{x}_a$$
$$\mathbf{y}_a = \mathbf{S}^{q-N_{ab}}\mathbf{I}_{ba}\mathbf{x}_b$$

and

$$\mathbf{y}_e = \begin{cases} \mathbf{S}^{q-N_{ae}}\mathbf{I}_{ae}\mathbf{x}_a & \text{for } n \text{ odd} \\ \mathbf{S}^{q-N_{be}}\mathbf{I}_{be}\mathbf{x}_b & \text{for } n \text{ even.} \end{cases}$$

We use product signalling, and Alice and Bob generate the keys $T_{lt}(\mathbf{x}_b)\mathbf{y}_b$ and $T_{lt}(\mathbf{x}_a)\mathbf{y}_a$, respectively. Both keys are the same due to Lemma (4.3). It can be easily seen that the deterministic key generation rate is

$$R_d = \tfrac{1}{2T}\min\{N_{ba}, N_{ab}\}.$$

However, Eve can also observe both signals. The secure key rate is therefore dependent on the channel gain to Eve and resembles a wiretap scenario. The secure rate is therefore only for the cases with $\min\{N_{ab}, N_{ba}\} - \min\{N_{ae}, N_{be}\} > 0$ positive. Both signal sources are needed to construct the key, and the difference is inherently included in the bit-levels. It is therefore easy to see that the secure key rate is

$$R_{sd} = \tfrac{1}{2T}(\min\{N_{ab}, N_{ba}\} - \min\{N_{ae}, N_{be}\}).$$

Linking the key rate to the Gaussian model gives

$$R_s = \tfrac{1}{4T}(\min\{\log \mathrm{SNR}_{ab}, \log \mathrm{SNR}_{ba}\} - \min\{\log \mathrm{SNR}_{ae}, \log \mathrm{SNR}_{be}\}),$$

where SNR_{ae} and SNR_{be} denotes the channel gain to Eve at odd and even time slots, respectively. Note, that the asymmetrical full duplex channel, which full-fills the assumption on the channel gains, achieves twice the key rate.

Static Channel Gain at Eve

A natural extension to the previous case is to look into a model where we have a random varying channel gain in the legitimate channel and a constant gain for Eve. This is the worst case scenario from a physical layer security perspective, since Eve can receive all communication in plain, while Alice and Bob need to handle the channel gain as well.
Half Duplex: The model is the following

$$\mathbf{y}_b = \mathbf{S}^{q-N_{ab}}\mathbf{H}_{ab}\mathbf{x}_a$$
$$\mathbf{y}_a = \mathbf{S}^{q-N_{ba}}\mathbf{H}_{ba}\mathbf{x}_b$$

and

$$\mathbf{y}_e = \begin{cases} \mathbf{S}^{q-N_{ae}}\mathbf{I}_{ae}\mathbf{x}_a & \text{for } n \text{ odd} \\ \mathbf{S}^{q-N_{be}}\mathbf{I}_{be}\mathbf{x}_b & \text{for } n \text{ even.} \end{cases}$$

It is easy to see that we cannot achieve a higher rate R_d than the previous cases with pilot signalling or static channel gain, since the maximum number of bits in the key vector is upper bounded by the mutual coarse channel gain $\min\{N_{ab}, N_{ba}\}$. However, calculating the secure key generation rate is more involved, and one needs to look into the term $I(\mathbf{y}_e^n; \mathbf{s}_a) = I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; T_{lt}(\mathbf{x}_b)\mathbf{y}_b)$. If we assume that $N_{ab} = N_{ba} = N_{ae} = N_{be}$, we can show that

$$\begin{aligned} I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; \mathbf{X}_b\mathbf{y}_b) &= h(\mathbf{X}_b\mathbf{y}_b) - h(\mathbf{X}_b\mathbf{y}_b|\mathbf{x}_b, \mathbf{x}_a) \\ &\overset{(a)}{=} h(\mathbf{X}_b\mathbf{y}_b) - h(\mathbf{X}_b\mathbf{X}_a T_{lt}^{-1}(\mathbf{H}_{ab})|\mathbf{x}_b, \mathbf{x}_a) \\ &= h(\mathbf{X}_b\mathbf{y}_b) - h(T_{lt}^{-1}(\mathbf{H}_{ab})) \\ &= h(\mathbf{X}_b\mathbf{X}_a T_{lt}^{-1}(\mathbf{H}_{ab})) - h(T_{lt}^{-1}(\mathbf{H}_{ab})) \\ &\leq h(\mathbf{X}_b\mathbf{X}_a, T_{lt}^{-1}(\mathbf{H}_{ab})) - h(T_{lt}^{-1}(\mathbf{H}_{ab})) \\ &= h(\mathbf{X}_b\mathbf{X}_a), \end{aligned}$$

where we denote $T_{lt}(\mathbf{x}_b) = \mathbf{X}_b$, $T_{lt}(\mathbf{x}_a) = \mathbf{X}_a$. Note that (a) is due to (4.2) and the assumptions on the coarse gains. The multiplication by $\mathbf{X}_b\mathbf{X}_a$ is a bijection in the case of fixed $\mathbf{x}_b$ and $\mathbf{x}_a$. In that case we would have that $I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; T_{lt}(\mathbf{x}_b)\mathbf{y}_b) = 0$, fulfilling the secrecy constraint if no local key bits are send to eve. This suggest a secrecy protocol which only uses local bit-levels as additional source of randomness, if those bit-levels are not received at Eve. For this purpose we can divide the local randomness vectors $\mathbf{x}_a$ and $\mathbf{x}_b$ in common and private parts, where the common part can be received by the legitimate receiver, as well as by Eve. The private part on the other hand is only received by the legitimate receiver. Both signals can then be partitioned into two parts $\mathbf{x}_a = \mathbf{x}_a^p + \mathbf{x}_a^c$

and $\mathbf{x}_b = \mathbf{x}_b^p + \mathbf{x}_b^c$, where $\mathbf{x}_a^p, \mathbf{x}_b^p > 0$ if and only if $N_{ab} > N_{ae}$ and $N_{ba} > N_{be}$. We can design the send signal such that we only use the private part of the signal to send random bits, and the common part for pilot signalling, for example

$$\mathbf{x}_a = \underbrace{100\cdots0\overbrace{b_1 b_2 \cdots b_{N_{ab}-N_{ae}}}^{\mathbf{x}_a^p}}_{N_{ab} \text{ bits}}.$$

Due to the lower triangular structure of the channel gain operation, the private bits only get down-shifted in the observations. One can then split $I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; T_{lt}(\mathbf{x}_b)\mathbf{y}_b)$ into a common $I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; \mathbf{H}^c)$ and a private part $I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; \mathbf{X}_B\mathbf{y}_B|\mathbf{H}^c)$ $= I(\mathbf{S}^{q-N_{ae}}\mathbf{x}_a, \mathbf{S}^{q-N_{be}}\mathbf{x}_b; (\mathbf{X}_B\mathbf{y}_B)^p)$ and show that both are zero. In this way we have exploited the structure of the deterministic model to design a scheme which uses a form of mixed signalling, where the common parts utilize pilot signalling and the private parts utilize product signalling. Due to the assumption that Eve has a static channel gain and can therefore see the local contribution in plain, we have obtained a worst-case scenario with a minimal achievable secure key rate.

Achievable Secure Key Generation Rate for a Symmetric Eve Scenario for Full Duplex

In this example we assume that Eve gets the same number of bit-levels N_e from both signals. Therefore Eve observes

$$\begin{aligned}\mathbf{y}_e &= \mathbf{S}^{q-N_e}\mathbf{H}_{ae}\mathbf{x}_a \oplus \mathbf{S}^{q-N_e}\mathbf{H}_{be}\mathbf{x}_b \\ &= \mathbf{S}^{q-N_e}\left(\mathbf{H}_{ae}\mathbf{x}_a \oplus \mathbf{H}_{be}\mathbf{x}_b\right) \\ &= \mathbf{S}^{q-N_e}\left(\mathbf{r}_a \oplus \mathbf{r}_b\right),\end{aligned}$$

where we denote $\mathbf{r}_a := \mathbf{H}_{ae}\mathbf{x}_a$ and $r_b := \mathbf{H}_{be}\mathbf{x}_b$ as the received bit vectors.

Large Coherence Block Length T For this case, pilot signalling returns a diminishing key rate with growing T. As long as the channel gain is fixed, we can use the two-way channel for message exchange and use a jamming scheme to utilize the full-duplex ability of the channel. Our scheme is the following: Alice and Bob design the first N_e bit-levels such that one transmitter sends jamming bits, while the other transmitter sends a key message, see Fig. 4.3. In this way, the common message, i.e. the top N_e bit-levels which are also seen by Eve, get jammed and the other message kept secret. Note that the jammed receiver (Bob, in Fig. 4.3) can recover the messages of the bit-levels below because (i) of the lower uni-triangular channel gain structure and (ii) the channel gain being fixed, so he can learn the channel gain. Bob can therefore successively decode the jamming and subtract it from the received signal to recover the lower message bit-levels. Moreover, this method does not

depend on the channel gain characteristics of Eve, which can be non-fixed. This can be seen by looking at the i-th bit of the bit-vector $\mathbf{r}_a$

$$r_{a,i} = x_{a,1}h_{ae,i-1} \oplus \ldots \oplus x_{a,i-1}h_{ae,1} \oplus x_{a,i}. \tag{4.4}$$

We know that the bits of $\mathbf{x}_a$ are i.i.d. Bern(1/2) since they are jamming bits and can therefore invoke the following lemma:

Lemma 4.4 (Crypto-Lemma, [FJ04]). *Let G be a compact abelian group with group operation $+$, and let $Y = X + N$, where X and N are random variables over G and N is independent of X and uniform over G. Then Y is independent of X and uniform over G.*

Identifying $x_{a,i}$ as independent of the other bits in (4.4) and Bern(1/2) shows that $r_{a,i}$ is independent of all previous bits $r_{a,j}$ for $1 \leq j < i$ and Bern(1/2) distributed. But this means, that every bit of $\mathbf{y}_e$ is independent of the message bits in $\mathbf{r}_b$, again by virtue of Lemma 4.4. Due to $\mathbf{r}_a$ and $\mathbf{r}_b$ occupying the same bit-levels at Eve, we see that one signal can jam the other and therefore provide secrecy. The achievable key rate is therefore

$$R_{sd} = (N_{ba} - N_e)^+ + (N_{ab} - N_e)^+ + N_e,$$

with $(\cdot)^+ := \min\{0, \cdot\}$. Interestingly, this simple scheme corresponds to

$$R_{sg} = \tfrac{1}{2}(\log \mathrm{SNR}_{ba} + \log \mathrm{SNR}_{ab} - \log \mathrm{SNR}_e)$$

in the high-SNR Gaussian case for $\min\{\mathrm{SNR}_{ba}, \mathrm{SNR}_{ab}\} \geq \mathrm{SNR}_e$ and therefore recovers the sum rate of [TY08c] in the high SNR regime:

$$\begin{aligned} R_\Sigma &= \tfrac{1}{2}(\log(1 + \mathrm{SNR}_{ba}) + \log(1 + \mathrm{SNR}_{ab}) \\ &\quad - \log(1 + 2\mathrm{SNR}_e)) \\ &\underset{\mathrm{SNR}\to\infty}{\approx} R_{sg}. \end{aligned}$$

A look into the proof of [HY13, Theorem 3] reveals, that the same techniques can be used, to show a sum-rate bound for the deterministic channel which leads to

$$\begin{aligned} R_{sd} \leq \min\{&I(\mathbf{x}_a; \mathbf{y}_b|\mathbf{y}_e, \mathbf{x}_b) + I(\mathbf{x}_b; \mathbf{y}_e, \mathbf{y}_a|\mathbf{x}_a), \\ &I(\mathbf{x}_b; \mathbf{y}_a|\mathbf{y}_e, \mathbf{x}_a) + I(\mathbf{x}_a; \mathbf{y}_e, \mathbf{y}_b|\mathbf{x}_b)\}, \end{aligned}$$

and shows, that the sum rate R_{sd} is in fact optimal. We note that the asymmetric channel gain configurations follow by carefully jamming exactly all overlapping bit-levels at Eve.

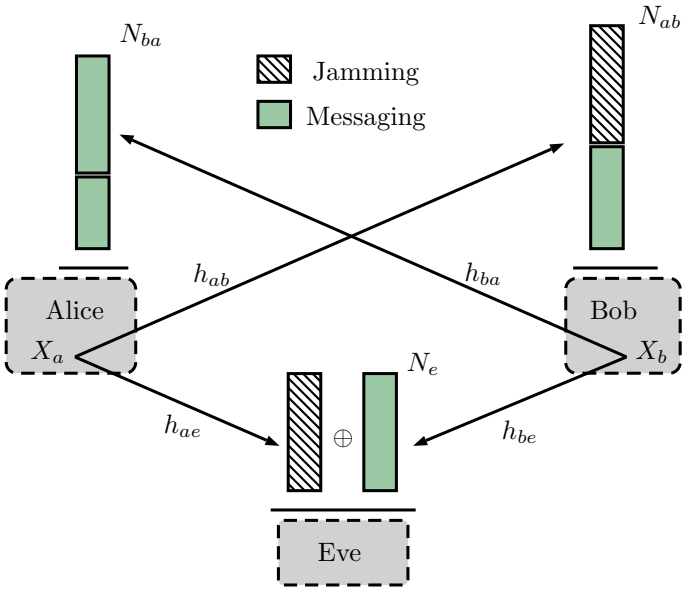

Figure 4.3.: A jamming scheme for the deterministic two-way channel (large T) with symmetric Eve observations. Since the channel gain h_{ba} is fixed, due to the long coherence block length T, the scheme uses secure messaging with cooperative jamming to establish a common secure key.

This scheme is therefore novel in the regard, that a user is not either messaging or jamming, but utilizing both methods.

Short Coherence Block Length T A short coherence block length means, that the channel gain is changing fast and we can use more channel-uses for pilot signalling. We can therefore achieve a key rate of

$$R_{sd} = \frac{1}{T} \min\{N_{ba}, N_{ab}\}.$$

4.4.3. Discussion

We have analysed both, the state-of-the-art pilot signalling scheme and the new product signalling with a deterministic model. We have shown that the general key generation rate is the same for both schemes for a perfect channel gain behaviour, i.e. uniformly distributed with short coherence time. This is due to the fact that the overall size of the bit-vectors stays the same. Therefore, product signalling would have no advantage compared to pilot signalling. Moreover, the secure key rate for product signalling can be even worse because Eve can listen to both Alice and Bob, and therefore gets parts of the local randomness sources. This means that there is a trade-off which closely resembles that of a wiretap scenario and we have proposed a scheme to exploit the created algebraic

structure. Product signalling begins to shine in cases with long coherence time. Here, one can compensate the lack of randomness in the channel gain, by feeding in the local sources. Product signalling would therefore yield a more robust key generation technique.

4.5. Conclusions

Motivated by an open problem in [WFK16], we have developed a deterministic model for secure key rate analysis of Gaussian models. The approximation is used to show secure key generation rate results on a product signalling scheme, developed in [WFK16]. The proposed approximate model provides insights which were out-of-reach within the classical Gaussian model. An advantage of the new model is that the key rate can be achieved without a public communication channel, due to its deterministic nature, i.e. absence of noise. Moreover, the model has an inherent quantization, which makes it possible to directly derive key rates from the equations. An interesting part is the additional algebraic structure. It was shown in the past, that algebraic structures can be exploited in several ways to gain unexpected results, especially for multi-user networks. Future research could therefore look into application of our model to analyse multi-user key generation scenarios. Furthermore, there is a need to investigate the exact gap between the approximate rate and the corresponding Gaussian model. We expect that this gap is within a few bits, due to similar results in several works on the linear deterministic model, e.g. [BT08]. Moreover, rate leakage in the noise effected part of the signal could lead to an adjustment of the secure key rate of the corresponding Gaussian model. Nonetheless, we believe that the proposed model can unlock some previously out-of-reach results and therefore act as a powerful tool for the analysis of secure key generation problems.

A. Diophantine Approximation & Constellation Distance

The field of Diophantine approximation studies the approximation of real numbers by rational numbers. It is a fact that the rational numbers are dense in the real numbers, which means that between any two real numbers is a rational one:

Theorem A.1. *If $x \in \mathbb{R}$, $y \in \mathbb{R}$, and $x < y$, then there exists a $p \in \mathbb{Q}$ such that $x < p < y$.*

Proof. See [Rud64]. □

Now it follows that for any real number x, and any positive ϵ, there exists a rational number $\frac{p}{q}$ such that

$$\left| x - \frac{p}{q} \right| < \epsilon.$$

Moreover, it is clear that $|qx - p| < 1$, since an arbitrary real number qx is always in proximity of 1 to an integer. This leads to the bound

$$\left| x - \frac{p}{q} \right| < \frac{1}{q}.$$

A better approximation was shown by Dirichlet:

Theorem A.2 (Dirichlet's Approximation Theorem). *If x is any real number, and n a positive integer, then there is an irreducible fraction $\frac{p}{q}$ satisfying $0 < q \leq n$ such that*

$$\left| x - \frac{p}{q} \right| < \frac{1}{qn}.$$

Proof. Dirichlet's Box Principle: Let $\lfloor x \rfloor$ be the integer part and $\{x\} := x - \lfloor x \rfloor$ the fractional part of x. Now divide the interval $[0, 1)$ in n sub-intervals, by setting each sub-interval $\left[\frac{k}{n}, \frac{k+1}{n}\right)$ for $k = 0, \ldots, n-1$. We therefore have constructed n intervals $\left[\frac{0}{n}, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right), \cdots \left[\frac{n-1}{n}, 1\right)$ of length $\frac{1}{n}$. If we now distribute $n+1$ numbers $\{rx\}$, for $r = 0, 1, \ldots, n$ into those bins, we see that two fall in the same bin. We therefore have that

$$|\{rx\} - \{r'x\}| = |rx - \lfloor rx \rfloor - r'x + \lfloor r'x \rfloor| = |qx - p| < \frac{1}{n},$$

where $q = r - r'$, $p = \lfloor rx \rfloor - \lfloor r'x \rfloor$ and $|q| \leq n$. □

Note that the equation $|qx - p| < \frac{1}{n}$ from above, suggest the convenient notation

$$||\theta|| := \min\{|\theta - k| : k \in \mathbb{Z}\} = \min\{\{\theta\}, 1 - \{\theta\}\} \tag{A.1}$$

and we can therefore present the result of Theorem A.2 as $||qx|| < \frac{1}{n}$. One can now consider a general approximation function $\psi(q) : \mathbb{N} \to (0, \infty)$ with $\lim_{q\to\infty} \psi(q) = 0$ and look into the solutions of $||qx|| < \psi(q)$ and say that a point x is ψ-approximable if that equation holds for infinitely many $q \in \mathbb{N}$. Notice that (A.1) is invariant under translation by integers and we can w.l.o.g constraint x to a unit interval such that $x \in [0, 1]$. The set of all $x \in [0, 1]$ satisfying the equation $||qx|| < \beta$ for some fixed $\psi(q) = \beta$ and q can be written as[1]

$$B(q, \beta) = \bigcup_{p=0}^{q} \left(\tfrac{p}{q} - \tfrac{\beta}{q}, \tfrac{p}{q} + \tfrac{\beta}{q}\right) \cap [0, 1].$$

We can now ask the question, how large is $|B(q, \beta)|$? Note that the set $B(q, \beta)$ is a β-neighbourhood of the resonant set

$$R_q := \{0, \tfrac{1}{q}, \ldots, \tfrac{p}{q}, \ldots, \tfrac{q-1}{q}, 1\}$$

and $B(q, \beta)$ can be visualised as shown in Figure A.1.

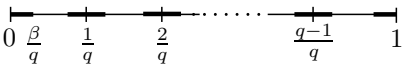

Figure A.1.: The set $B(q, \beta)$ in the line $[0, 1]$.

There, one can see that the set has $q - 1$ parts of length $\frac{2\beta}{q}$ and the two end parts of length $\frac{\beta}{q}$. Therefore, $B(q, \beta)$ has a length of

$$(q - 1)\tfrac{2\beta}{q} + \tfrac{2\beta}{q} = 2\beta.$$

Now, what can we say about the set of all $(x_1, x_2) \in [0, 1]^2$ satisfying the equation

$$||q_1 x_1 + q_2 x_2|| < \beta \tag{A.2}$$

for some tuple $(q_1, q_2) \in \mathbb{Z}^2$? One can use the idea of identifying the solution set with Torus geometry in the plane. Figure A.2 shows the solution set of equation (A.2). One can now imagine that one glues the left hand side of the square, to the right hand side,

[1] See [Dod07].

forming a cylinder. Now, gluing the top of the cylinder to its bottom forms a torus. All stripes which we see in the picture can be counted in this torus and we see that we have $|q_1|$ stripes in the x_1 direction, going from bottom to top. The red stripe, for example, starts at[2] $(0, 0)$ and goes to $(1, \frac{2}{|-3|})$, where it leaves the square and re-enters at $(0, \frac{2}{|-3|})$ and continues to the top, reaching its end (in the x_1 direction) at $(0.5, 1)$. One might also count the (same) stripes in the x_2 direction, counting $|q_2|$ full stripes, which go from the left to the right of the square.

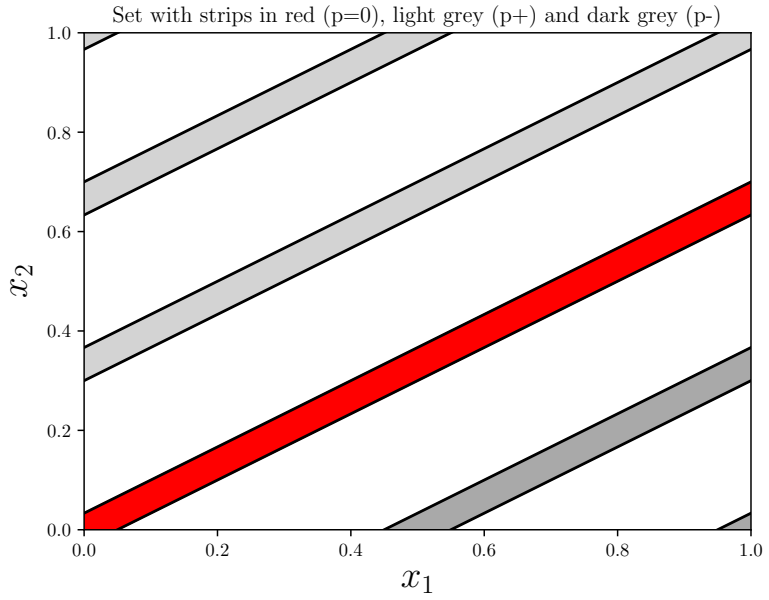

Figure A.2.: Solutions of the equation A.2 for $q_1 = -2$ and $q_2 = 3$. The stripes intersect with the x_2-axis at 0, $\frac{1}{|q_2|}$ and $\frac{2}{|q_2|}$. They intersect with the x_1-axis at 0 and $\frac{1}{|q_1|}$.

Those stripes have a width of $\frac{2\beta}{|q_i|}$ in the x_i direction for $i \in \{1, 2\}$. Now we can calculate the area of all stripes in the figure. We know that the area of a parallelogram (a stripe) is base width times height and therefore get $\frac{2\beta}{|q_i|}$ if seen in the x_i direction. Moreover, we have a total of $|q_i|$ stripes and therefore get a total area of 2β, independent of the direction in which we count. We therefore know, that the solution set of equation A.2 has a measure of 2β. Further details can be found in [Dod07] and [Dod93].

[2] And a bit at $(1, 0)$

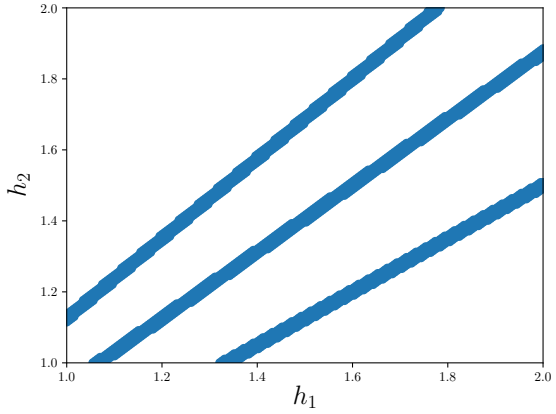

Figure A.3.: A scatter plot for equation (A.3), with the values $\bar{u}_1 = \{4/8, 5/8, 6/8\}$, which corresponds to the stripes from left to right, moreover we chose $\bar{u}_2 = -2/3$ and $n = 8$. The plot uses 40000 channel gain tuples.

Connection to Constellation Distance

To decode signals, we want the minimum distance between two points of the signal constellation to be atleast twice as large as the radius of the noise spheres around them. This enables successful decoding of the signal points with high probability. For example, look at the Gaussian multiple-access channel with input constellations $u_1 \in \{0, 1/8, \ldots, 7/8\}$ for transmitter one and $u_2 \in \{0, 1/3, 2/3\}$ for transmitter 2, which has additive Gaussian noise of unit variance. To have a received constellation distance of atleast twice the noise variance means that

$$\begin{aligned} 2^n|h_1u_1 + h_2u_2 - h_1u_1^{'} - h_2u_2^{'}| &= 2^n|h_1(u_1 - u_1^{'}) + h_2(u_2 - u_2^{'})| \\ &= 2^n|h_1\bar{u}_1 + h_2\bar{u}_2| \geq 2, \end{aligned}$$

for all $u_1, u_1^{'} \in \{0, 1/8, \ldots, 7/8\}$, $u_2, u_2^{'} \in \{0, 1/3, 2/3\}$, and $(u_1, u_2) \neq (u_2, u_2^{'})$. Or equivalently for all $\bar{u}_1 \in \{-7/8, \ldots, -1/8, 1/8, \ldots, 7/8\}$ and $\bar{u}_2 \in \{-2/3, -1/3, 1/3, 2/3\}$. We can now ask the question, how big is the outage set, i.e. for which channel gains h_1, h_2 do we have that

$$2^n|h_1\bar{u}_1 + h_2\bar{u}_2| < 2. \tag{A.3}$$

We show the set of all solutions for $h_1, h_2 \in [1, 2]$, $\bar{u}_1 = \{4/8, 5/8, 6/8\}$, $\bar{u}_2 = -2/3$ and $n = 8$ in Figure A.3. By identifying $2^n\bar{u}_i = q_i$, $h_i = x_i$, and $\beta = 2$, we see that this *outage* set, or rather one stripe (a fixed value of (q_1, q_2)) corresponds to the solutions of equation (A.2) for $p = 0$. Now, lets suppose we have three input constellation differences $(q_1, q_2, q_3) \in \mathbb{Z}^3$,

and each is bounded by a number $Q_i \in \mathbb{N}$ such that $q_i \in \{-Q_i, -Q_i+1, \ldots, Q_i-1, Q_i\}$. One can define the event

$$B(q_1, q_2, q_3) := \{(h_1, h_2, h_3) \in [1,2]^3 : |h_1 q_1 + h_2 q_2 + h_3 q_3| < \beta\}$$

and ask about the measure of $B(q_1, q_2, q_3)$ depending on q_i and β. One can transform this question into the form of equation (A.2) by identifying one q variable as p and fixing the corresponding channel gain value h such that

$$B_{h_1}(q_2, q_3) := \{(h_2, h_3) \in [1,2]^2 : (h_1, h_2, h_3) \in ||h_2 q_2 + h_3 q_3|| < \beta\}$$

for all $q_1 \in \mathbb{Z} : |q_1| \leq Q_1$. Now the set $B_{h_1}(q_2, q_3)$ looks the same as that of equation(A.2) in Figure A.2, except that the p value is bounded $|p| = |q_1| \leq Q_1$. We now have a maximum of $2Q_1 + 1 \leq 3Q_1$ stripes[3] for *every* tuple (h_2, h_3), and we therefore have at most $\min\{3Q_1, |q_2|\}$ stripes in $(h_2, h_3) \in [1,2]^2$ in the (exemplary) h_2 direction with a width of $\frac{2\beta}{|q_2|}$. We therefore get a measure of

$$\mu(B_{h_1}(q_2, q_3)) \leq \frac{2\beta}{|q_2|} \min\{3Q_1, |q_2|\} \leq 6\beta \min\left\{\frac{Q_1}{|q_2|}, 1\right\},$$

for all cases with $|q_1| \leq |q_2|$, the other cases can be shown similarly. The total outage set, over all values of q_1, q_2 and q_3 can then be shown to be

$$\mu(B(q_1, q_2, q_3)) \leq \sum_{\substack{q_2 \in \mathbb{Z}: \\ |q_2| \leq Q_2}} \sum_{\substack{q_1 \in \mathbb{Z}: \\ |q_3| \leq Q_3}} \int_{h_1=1}^{2} \mu(B_{h_1}(q_2, q_3)) dh_1.$$

The result is dependent on the maximum constellation size Q_1, Q_2 and Q_3 and we therefore have a quantity for the trade-of between achievable rate and size of the outage-set for which decoding is not possible. The previous ideas were first used in the proof of [NMA13, Lemma 14], which is a generalisation of the example above.

[3] one for every value of q_1, including $q_1 = 0$

Publication List

[FW14a] R. Fritschek and G. Wunder. Upper bounds and duality relations of the linear deterministic sum capacity for cellular systems. In *Proc. IEEE International Conference on Communications (ICC)*, Sydney, Australia, 2014.

[FW14b] R. Fritschek and G. Wunder. Enabling the multi-user generalized degrees of freedom in the gaussian cellular channel. In *Proc. IEEE Information Theory Workshop (ITW)*, Hobart, Australia, 2014.

[FW15a] R. Fritschek and G. Wunder. Deterministic imac revisited: Constant-gap capacity in the weak interference case. In *Proc. IEEE International Conference on Communications (ICC)*, London, UK, 2015.

[FW15b] R. Fritschek and G. Wunder. Constant-gap sum-capacity approximation of the deterministic interfering multiple access channel. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, Hong Kong, China, 2015.

[FW16a] R. Fritschek and G. Wunder. Towards a constant-gap sum-capacity result for the gaussian wiretap channel with a helper. In *Proc. IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, July 2016.

[WFK16] G. Wunder, R. Fritschek, and R. Khan. Recip: Wireless channel reciprocity restoration method for varying transmission power. In *Proc. IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016.

[FW16b] R. Fritschek and G. Wunder. Enabling the multi-user generalized degrees of freedom in cellular interference networks with multi-user coding. Chapter in *Communications in Interference Limited Networks*, pages 53–73, Springer, 2016.

[FW17a] R. Fritschek and G. Wunder. On-the-fly secure key generation with deterministic models. In *Proc. IEEE International Conference on Communications (ICC)*, Paris, France, 2017, accepted and presented.

[WRFE17] G. Wunder, I. Roth, R. Fritschek and J. Eisert. HiHTP: A custom-tailored hierarchical sparse detector for massive MTC. In *Proc. Asilomar Conference on Signals, Systems and Computers*, Pacific Groove, CA, 2017, accepted.

[FW17b] R. Fritschek and G. Wunder. On full-duplex secure key generation with deterministic models. In *Proc. IEEE Conference on Communications and Network Security (CNS '17) - 4th Workshop on Physical-Layer Methods for Wireless Security*, Las Vegas, Nevada, 2017, invited, accepted and presented.

[FW17c] R. Fritschek and G. Wunder. On multiuser gain and the constant-gap sum capacity of the Gaussian interfering multiple access channel. Submitted to IEEE Transactions on Information Theory.

[FW17d] R. Fritschek and G. Wunder. On the Gaussian multiple access wiretap channel and the Gaussian wiretap channel with a helper: Achievable schemes and upper bounds. Submitted to IEEE Transactions on Information Forensics and Security.

Bibliography

[ABC+14] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang. What will 5G be? *IEEE Journal on Selected Areas in Communications*, 32(6):1065–1082, June 2014.

[AC93] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, Jul 1993.

[ADT07] S. Avestimehr, S. Diggavi, and D. Tse. A deterministic approach to wireless relay networks. In *Proc. Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2007.

[ADT11] S. Avestimehr, S. Diggavi, and D. Tse. Wireless Network Information Flow: A Deterministic Approach. *IEEE Transactions on Information Theory*, 57(4):1872–1905, 2011.

[AGK13] M. J. Abdoli, A. Ghasemi, and A. K. Khandani. On the degrees of freedom of k-user siso interference and x channels with delayed csit. *IEEE Transactions on Information Theory*, 59(10):6542–6561, Oct 2013.

[AST08] A. Avestimehr, A. Sezgin, and D. Tse. Capacity of the two-way relay channel within a constant gap. *European Transactions on Telecommunications*, 19(4):333–354, 2008.

[BB11] M. Bloch and J. Barros. *Physical-layer security: From information theory to security engineering.* Cambridge University Press, 2011.

[BMK13] D. Bharadia, E. McMilin, and S. Katti. Full duplex radios. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, pages 375–386, 2013.

[BPT10] G. Bresler, A. Parekh, and D. Tse. The approximate capacity of the many-to-one and one-to-many Gaussian interference channels. *IEEE Transactions on Information Theory*, 56(9):4566–4592, 2010.

[BSP15] P. Babaheidarian, S. Salimi, and P. Papadimitratos. Finite-SNR regime analysis of the Gaussian wiretap multiple-access channel. In *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 307–314, Sept 2015.

[BT08] G. Bresler and D. Tse. The two-user Gaussian interference channel: a deterministic view. *European Transactions on Telecommunications*, 19(4):333–354, 2008.

[BW11] J. Bühler and G. Wunder. On interference alignment and the deterministic capacity for cellular channels with weak symmetric cross links. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, Saint-Petersburg, Russia, 2011.

[BW12] J. Bühler and G. Wunder. The multiple access channel interfering with a point to point link: Linear deterministic sum capacity. In *IEEE International Conference on Communications (ICC)*, Ottawa, Canada, 2012.

[Cis17] Cisco. Cisco visual networking index: Forecast and methodology, 2016-2021. *White paper*, June 2017.

[CJ08] V. Cadambe and S. Jafar. Interference alignment and degrees of freedom of the K-User interference channel. *IEEE Transactions on Information Theory*, 54(8):3425–3441, Aug 2008.

[CJW10] V. R. Cadambe, S. A. Jafar, and C. Wang. Interference alignment with asymmetric complex signaling-settling the Host-Madsen-Nosratinia conjecture. *IEEE Transactions on Information Theory*, 56(9):4552–4565, Sept 2010.

[CK78] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, May 1978.

[CK11] I. Csiszar and J. Körner. *Information theory: Coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[CS16] A. Chaaban and A. Sezgin. The approximate capacity region of the symmetric K-User Gaussian interference channel with strong interference. *IEEE Transactions on Information Theory*, 62(5):2592–2621, May 2016.

[CT91] T. M. Cover and J. A. Thomas. *Elements of Information Theory*, volume Wiley Series in Telecommunications. 1991.

[CVS14] Y. Chen, H. Vogt, and A. Sezgin. Gaussian wiretap channels with correlated sources: Approaching capacity region within a constant gap. In *2014 IEEE International Conference on Communications Workshops (ICC)*, pages 794–799, June 2014.

[DDS12] M. Duarte, C. Dick, and A. Sabharwal. Experiment-driven characterization of full-duplex wireless systems. *IEEE Transactions on Wireless Communications*, 11(12):4296–4307, December 2012.

[DJ16] A. G. 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 Transactions on Information Theory*, 62(10):5603–5618, Oct 2016.

[Dod93] M. M. Dodson. Geometric and probabilistic ideas in metric Diophantine approximation. *Russian Mathematical Surveys*, 48(5):73–102, 1993.

[Dod07] M. M. Dodson. Diophantine approximation, khintchine's theorem, torus geometry and hausdorff dimension. *ArXiv e-prints*, October 2007.

[EGK11] A. El Gamal and Y.-H. Kim. *Network information theory*. Cambridge university press, 2011.

[EHLGS12] M. El-Halabi, T. Liu, C. N. Georghiades, and S. Shamai. Secret writing on dirty paper: A deterministic view. *IEEE Transactions on Information Theory*, 58(6):3419–3429, June 2012.

[ETW08] R. Etkin, D. Tse, and H. Wang. Gaussian interference channel capacity to within one bit. *IEEE Transactions on Information Theory*, 54(12):5534–5562, 2008.

[FJ04] G. D. Forney Jr. On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener. *arXiv preprint cs/0409053*, 2004.

[Gal68] R. G. Gallager. *Information theory and reliable communication*, volume 2. Springer, 1968.

[GKYG13] A. E. Gamal, O. O. Koyluoglu, M. Youssef, and H. E. Gamal. Achievable secrecy rate regions for the two-way wiretap channel. *IEEE Transactions on Information Theory*, 59(12):8099–8114, Dec 2013.

[GSJ15] C. Geng, H. Sun, and S. A. Jafar. On the optimality of treating interference as noise: General message sets. *IEEE Transactions on Information Theory*, 61(7):3722–3736, July 2015.

[HY13] X. He and A. Yener. The role of feedback in two-way secure communications. *IEEE Transactions on Information Theory*, 59(12):8115–8130, Dec 2013.

[HY14] X. He and A. Yener. Providing secrecy with structured codes: Two-user gaussian channels. *IEEE Transactions on Information Theory*, 60(4):2121–2138, April 2014.

[JS08] S. Jafar and S. Shamai. Degrees of freedom region of the MIMO X channel. *IEEE Transactions on Information Theory*, 54(1):151–170, Jan 2008.

[Kha13] A. K. Khandani. Two-way (true full-duplex) wireless. In *2013 13th Canadian Workshop on Information Theory*, pages 33–38, June 2013.

[Khi11] A. Khisti. Interference alignment for the multiantenna compound wiretap channel. *IEEE Transactions on Information Theory*, 57(5):2976–2993, May 2011.

[LLP12] L. Lai, Y. Liang, and H. V. Poor. A unified framework for key agreement over wireless fading channels. *IEEE Transactions on Information Forensics and Security*, 7(2):480–490, April 2012.

[LLPD13] L.Lai, Y. Liang, H. Poor, and W. Du. *Key generation from wireless channels*, volume Physical Layer Security in Wireless Communications, CRC Press. 2013.

[Loe97] H.-A. Loeliger. Averaging bounds for lattices and linear codes. *IEEE Transactions on Information Theory*, 43(6), 1997.

[LPS09] Y. Liang, H. V. Poor, and S. S. (Shitz). Information theoretic security. *Foundations and Trends® in Communications and Information Theory*, 5(4-5):355–580, 2009.

[LYCH78] S. Leung-Yan-Cheong and M. Hellman. The Gaussian wire-tap channel. *Information Theory, IEEE Transactions on*, 24(4):451–456, Jul 1978.

[LZK17] S. H. Lee, W. Zhao, and A. Khisti. Secure degrees of freedom of the Gaussian diamond-wiretap channel. *IEEE Transactions on Information Theory*, 63(1):496–508, Jan 2017.

[MAMK08] M. Maddah-Ali, A. Motahari, and A. Khandani. Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis. *IEEE Transactions onInformation Theory*, 54(8):3457–3470, Aug 2008.

[MAT10] M. A. Maddah-Ali and D. Tse. Completely stale transmitter channel state information is still very useful. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1188–1195, Sept 2010.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, May 1993.

[MM13] P. Mohapatra and C. R. Murthy. Secrecy in the 2-user symmetric deterministic interference channel with transmitter cooperation. In *2013 IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 270–274, June 2013.

[MOGMAK14] A. S. Motahari, S. Oveis-Gharan, M. A. Maddah-Ali, and A. K. Khandani. Real interference alignment: Exploiting the potential of single antenna systems. *IEEE Transactions on Information Theory*, 60(8):4799–4810, Aug 2014.

[Muk15] A. Mukherjee. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10):1747–1761, Oct 2015.

[MXU17] P. Mukherjee, J. Xie, and S. Ulukus. Secure degrees of freedom of one-hop wireless networks with no eavesdropper CSIT. *IEEE Transactions on Information Theory*, 63(3):1898–1922, March 2017.

[Naz12] B. Nazer. Successive compute-and-forward. In *Proceedings of the 22nd Biennial International Zurich Seminar on Communication (IZS 2012)*, Zurich, Switzerland, 2012.

[NCL10] W. Nam, S. Y. Chung, and Y. H. Lee. Capacity of the gaussian two-way relay channel to within 1*over*2 bit. *IEEE Transactions on Information Theory*, 56(11):5488–5494, Nov 2010.

[NCNC16] B. Nazer, V. R. Cadambe, V. Ntranos, and G. Caire. Expanding the compute-and-forward framework: Unequal powers, signal levels, and multiple linear combinations. *IEEE Transactions on Information Theory*, 62(9):4879–4909, Sept 2016.

[NG11] B. Nazer and M. Gastpar. Compute-and-forward: Harnessing interference through structured codes. *IEEE Transactions on Information Theory*, 57(10):6463–6486, Oct 2011.

[Nit08] S. Nitinawarat. Secret key generation for correlated Gaussian sources. In *IEEE International Symposium on Information Theory*, pages 702–706, July 2008.

[NMA13] U. Niesen and M. Maddah-Ali. Interference alignment: From degrees of freedom to constant-gap capacity approximations. *IEEE Transactions on Information Theory*, 59(8):4855–4888, Aug 2013.

[OEN14] O. Ordentlich, U. Erez, and B. Nazer. The approximate sum capacity of the symmetric gaussian k -user interference channel. *IEEE Transactions on Information Theory*, 60(6):3450–3482, June 2014.

[PB11] A. J. Pierrot and M. R. Bloch. Strongly secure communications over the two-way wiretap channel. *IEEE Transactions on Information Forensics and Security*, 6(3):595–605, Sept 2011.

[PDT09] E. Perron, S. Diggavi, and E. Telatar. On cooperative wireless network secrecy. In *IEEE INFOCOM 2009*, pages 1935–1943, April 2009.

[RKWE16] I. Roth, M. Kliesch, G. Wunder, and J. Eisert. Reliable recovery of hierarchically sparse signals and application in machine-type communications. *arXiv preprint*, abs/1612.07806, 2016.

[Rud64] W. Rudin. *Principles of mathematical analysis*, volume 3. McGraw-hill New York, 1964.

[SB11] S. Saha and R. A. Berry. Sum-capacity of a class of K-user Gaussian interference channels within $o(k \log k)$ bits. *Allerton Conf. 2011*, 2011.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[SJV+08] S. Sridharan, A. Jafarian, S. Vishwanath, S. A. Jafar, and S. Shamai. A layered lattice coding scheme for a class of three user Gaussian interference channels. *Allerton Conf. 2008*, 2008.

[ST08] C. Suh and D. Tse. Interference alignment for cellular networks. In *Proc. Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2008.

[ST11] C. Suh and D. N. C. Tse. Feedback capacity of the gaussian interference channel to within 2 bits. *IEEE Transactions on Information Theory*, 57(5):2667–2685, May 2011.

[TV05] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[TY08a] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *Information Theory, IEEE Transactions on*, 54(12):5747–5755, Dec 2008.

[TY08b] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *Information Theory, IEEE Transactions on*, 54(6):2735–2751, June 2008.

[TY08c] E. Tekin and A. Yener. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.

[UZ04] U. Urez and R. Zamir. Achieving $\frac{1}{2}\log(1 + snr)$ on the AWGN channel with lattice encoding and decoding. *IEEE Transactions on Information Theory*, 50(10), 2004.

[VAS16] H. Vogt, Z. H. Awan, and A. Sezgin. On deterministic ic with common and private message under security constraints. In *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 947–952, Dec 2016.

[VS15] H. Vogt and A. Sezgin. Full-duplex vs. half-duplex secret-key generation. *CoRR*, abs/1506.08565, 2015.

[WTS07] R. Wilson, D. Tse, and R. A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *IEEE Transactions on Information Forensics and Security*, 2(3):364–375, Sept 2007.

[Wyn75] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[XU12] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers. In *Proc. Allerton Conference on Communication, Control, and Computing*, pages 193–200, Oct 2012.

[XU13] J. Xie and S. Ulukus. Secure degrees of freedom of the Gaussian wiretap channel with helpers and no eavesdropper CSI: Blind cooperative jamming. In *2013 47th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–5, March 2013.

[XU14] J. Xie and S. Ulukus. Secure degrees of freedom of one-hop wireless networks. *IEEE Transactions on Information Theory*, 60(6):3359–3378, June 2014.

[YRS06] C. Ye, A. Reznik, and Y. Shah. Extracting secrecy from jointly Gaussian random variables. In *IEEE International Symposium on Information Theory*, pages 2593–2597, July 2006.