# POLITECNICO DI TORINO

**Master's Degree in Communications and Computer Networks Engineering**


**Master's Degree Thesis**

# Analysis and implementation of a multi-user wireless Non-Orthogonal Multiple Access (NOMA) system

**Supervisor**

**Prof. Giorgio Taricco**

**Candidate**

**Alessandro Compagnoni**

**October 2023**

**Abstract**

This essay aims to simulate a NOMA downlink system in the power domain and evaluate its performance in terms of information rate. Non-Orthogonal Multiple Access (NOMA) systems have attracted significant interest in the context of next-generation networks for their potential to accommodate a large number of users and theoretically offer superior spectral efficiency compared to traditional Orthogonal Multiple Access (OMA) systems.

Our primary goal is to evaluate the simulated system's performance in relation to the Shannon capacity region, which represents the theoretical upper limit of reliable information transmission. Specifically, throughout this work, we demonstrate how closely we can approach the Shannon theoretical limit by implementing M-QAM and turbo codes MODCODs, while maintaining a target frame error rate of $10^{-3}$.

The entire analysis is conducted under the assumption of a discrete memoryless static channel approximation. It includes not only a comparison with the system's capacity region but also a comparison with the theoretical sum-rate bound and the corresponding theoretical rate limit of an OMA system, along with an analysis of the max-min operating points.

Finally, a discussion on the reliability of the results is also included, taking into account the implemented algorithms and their assumptions.

# Acknowledgements

I would like to express my sincere gratitude to my supervisor, Giorgio Taricco, for his patience and guidance throughout this work. His valuable directions have greatly contributed to the successful completion of this project.

Furthermore, I extend my appreciation to all the professors who have served as a continuous source of knowledge and inspiration throughout my academic journey. In particular, I am grateful to Gianluca Piccinini, Roberto Garello, Silvio Mercadante, Renato Gonnelli, Andrea Lavagno, Lorenzo Galleani, Franco Pellerey, and Fabrizio Pirri.

Lastly, I would like to thank my family for providing me with the opportunity to pursue my studies at the university.

*Virtus numquam infirmitas*

# Table of Contents

# List of Tables

# List of Figures

# Acronyms

**NOMA**
Non-Orthogonal Multiple Access

**SIC**
successive interference cancellation

**FER**
frame error rate

**QAM**
quadrature amplitude modulation

**SNR**
signal to noise ratio

**SINR**
signal to interference plus noise ratio

**r.v.**
random variable

**i.i.d.**
independent identical distributed

**AEP**
asymptotic equipartition property

**DMC**
discrete memoryless channel

**pdf**

probability density function

**CDF**

cumulative distribution function

**AWGN**

additive white gaussian noise

**ML**

maximum likelihood

**CLT**

central limit theorem

**Q.E.D.**

Quod Erat Demonstrandum

# Chapter 1

# Introduction

With the increasing demand for mobile communication and the Internet of Things, the future of advanced wireless networks relies on achieving better spectrum efficiency, handling more connected devices, and reducing latency [1]. In this evolving scenario, adopting Non-Orthogonal Multiple Access (NOMA) systems can play an important role in achieving the objectives of next-generation networks. NOMA allows multiple users to efficiently share the channel resources, offering the potential for massive connectivity and high spectral efficiency.

In the following sections of this work, we are going to discuss a possible implementation of a downlink Non-Orthogonal Multiple Access (NOMA) system in the power domain. This implementation will incorporate M-QAM modulation and turbo code MODCODs. Our primary objective is to compare MODCODs information rate performance with the theoretical limits determined by the capacity region of the Gaussian Broadcast channel. As a matter of fact, it should be noted that NOMA systems are generally studied from an information-theoretical perspective, which assumes the use of infinite-length codes capable of achieving capacity. However, the implementation of MODCODs with finite-length codes unavoidably degrades performance. In this work, we examine and quantify how the use of finite-length codes affects performance, fixed a target frame error rate.

The content of the thesis consists of the following chapters:

- Chapter 2 presents the notion of non-orthogonal multiple access (NOMA), with particular attention on the two-user downlink scenario.

- Chapter 3 concerns the simulation of a two-user downlink NOMA in static channel condition: we start from the mathematical model description, then we move on the FER vs. SNRs analysis; finally we study the rates of the implemented MODCODs and compare them with the Capacity region and orthogonal multiple access (OMA) performances.

- Chapter 4 delves into potential future directions for the thesis. Specifically, we are considering moving from a static channel model to one that incorporates a time-varying channel, including fast-fading and block-fading approximations. Additionally, we discuss other possible ways to enhance the quality of the results.
- Appendixes A and B summarize all the Information Theory notions necessary to deeply understand the meaning of the results achieved in the thesis, with a particular focus on the multi-user theory.

# Chapter 2

# Non-Orthogonal Multiple Access: overview

## 2.1 Introduction

In this chapter we briefly introduce the theoretical aspects of a NOMA system. In general, a NOMA system is a multiple access scheme in which radio resources (time, frequency, codes) are shared non-orthogonally between different users; that is multiple users signals are superimposed and the receiver should separate them in order to perform decoding.

There are different types of NOMA schemes from different classification prospectives, some of them include:

- Downlink NOMA and uplink NOMA.
- Power domain NOMA and Code domain NOMA.
- Single-carrier NOMA and multi-carrier NOMA.
- SISO-NOMA, SIMO-NOMA and MIMO-NOMA.
- Cooperative NOMA: involving cooperation among NOMA users or by means of dedicated relays.

A detailed theoretical review of NOMA is not the purpose of this thesis, therefore we will only focus on the two-user downlink power domain scenario, which is the object of our subsequent analysis; to learn more about NOMA theoretical aspects refer to [2] and [3].

## 2.2 Downlink NOMA in power domain

We consider a base station transmitting a superimposed signal to multiple users in the same channel resource block. In the case of a two-user NOMA scheme, the user close to the base station is named "Near user", instead, the user far from the base station is the "Far user". The notions of "near" and "far" do not strictly depend on the distance between users and base station, but actually they depend on the users' channel gains (the one who has the lower attenuation is the near user, the other is the far user).

Figure 2.1 summarizes this scenario. It can be noticed that more power is allocated to the far user signal.

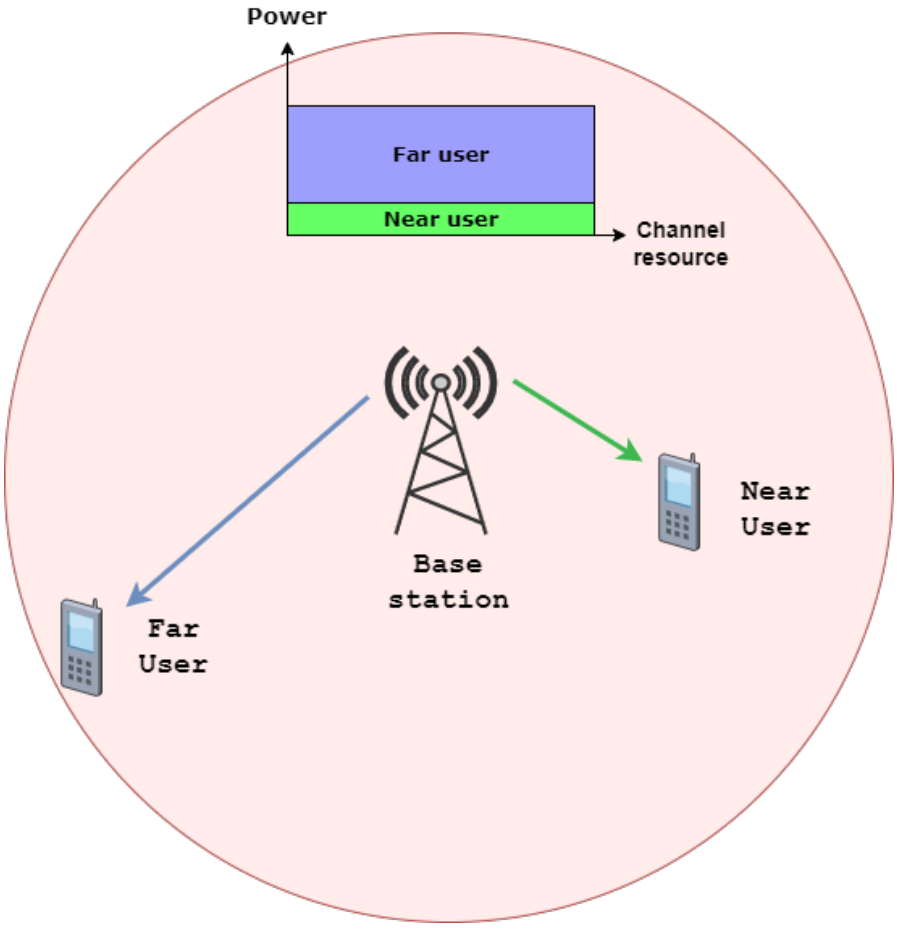



**Figure 2.1:** Two-user downlink NOMA in power domain (mentioned on p. 6)

In order to separate the signals:

- The Far user directly decodes its own signal (considering the near user signal

as interference noise).

- The Near user implements a successive interference cancellation (SIC) procedure: as a first step he decodes the far user signal, subtracts it from the superimposed signal and finally decodes its own signal.

It is useful to note that both the near user and the far user as a first step decode the far user signal, i.e. the one having the most power allocated. More theoretical details concerning SIC are discussed in Section 3.2. In Section 3.5.4, we show how SIC is implemented in our simulation setup.

Figure 2.2 shows the decoding block scheme at both users' receivers. In Section 3.2 we describe a mathematical model of the communication scheme.

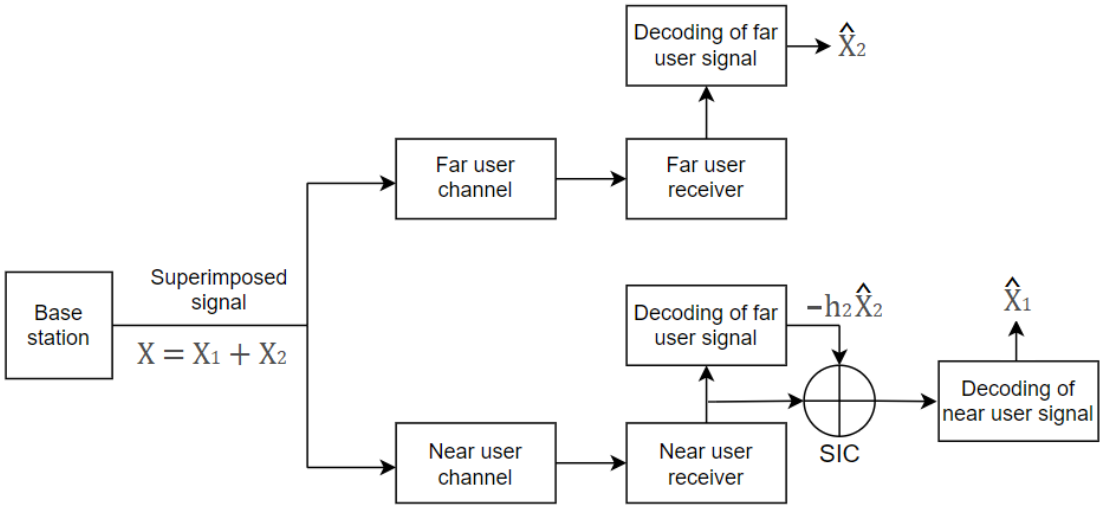



**Figure 2.2:** Decoding scheme (mentioned on p. 7)

# Chapter 3

# Simulated information rate of a downlink NOMA in Static channel approximation

## 3.1 Introduction

In this chapter we study the information rate performances of a two-user NOMA downlink system over $AWGN$ channel in static conditions. Different MODCODs are implemented and their achieved rates for a fixed target FER are compared against the information theoretical limits, i.e. against the capacity region of the Gaussian broadcast channel (B.3).

- In Section 3.2 we describe the communication mathematical model.

- In Section 3.3 we show some results concerning the FER Vs. SNRs performances of the system.

- In Section 3.4 the MODCODs performances are analyzed and compared with the capacity region for different power allocation factors. A sum-rate and a MAX-MIN analysis are also performed and a comparison with OMA performances is included.

## 3.2 Mathematical model description

A discrete memory-less $AWGN$ channel is considered in this model. The entire analysis involves only two users, which can be considered the simplest model describing a broadcast channel with $m > 1$ users. User-1 is the "Near user", instead, User-2 is the "Far user". According to the previous assumption, we have $|h_1| > |h_2|$, where $h_1$ and $h_2$ are the channel coefficients of User-1 and User-2, respectively. We define the frame size parameters:

- $f_{size-U1} \equiv$ "Frame length of User-1" $[^{information\ bits}/_{frame}]$
- $f_{size-U2} \equiv$ "Frame length of User-2" $[^{information\ bits}/_{frame}]$

The simulated MODCODs are realized by means of M-QAM modulation and Turbo Code. The M-QAM modulation scheme presents different cardinality $M_1 = 2^{m_1}$ and $M_2 = 2^{m_2}$ for User-1 and User-2 respectively; where $m_i$ represents the modulation efficiency $[^{bits}/_{symbol}]$ for User-i. The $UMTS$ Turbo encoding system [4] has the following tunable parameters:

- $R_{C-U1} \equiv$ "Code rate of User-1" (tunable by puncturing)
- $R_{C-U2} \equiv$ "Code rate of User-2" (tunable by puncturing)
- $N_{iter} \equiv$ "Number of decoding iterations"
- $P_{U1} \equiv$ "Puncturing pattern for User-1"
- $P_{U2} \equiv$ "Puncturing pattern for User-2"

Where the puncturing pattern matrices are exploited to adjust the users' rates.

The modulated signals $X_1$ and $X_2$, for User-1 and for User-2, respectively, have zero average. The power assigned to each signal is determined by the power allocation factor:

- $E[X_1] = 0$, $E[|X_1|^2] = P_1 = \alpha_1 P = \alpha P$
- $E[X_2] = 0$, $E[|X_2|^2] = P_2 = \alpha_2 P = (1 - \alpha) P$

Where $P$ is the total transmitted power and $\alpha \in (0,1)$ is the power allocation factor.

The transmitted superimposed signal is:

$$X = X_1 + X_2 \tag{3.1}$$

User-1 and User-2 receive:

$$\begin{cases} Y_1 = h_1 X + Z_1 = h_1 X_1 + h_1 X_2 + Z_1 \\ Y_2 = h_2 X + Z_2 = h_2 X_1 + h_2 X_2 + Z_2 \end{cases} \tag{3.2}$$

Where $Z_i \sim \mathcal{CN}(0, N)$ is the noise signal at User-i receiver; $i \in \{1,2\}$.

In a generic $m$-user NOMA system, each receiver employs the Successive Interference Cancellation (SIC) [5] technique, decoding and subtracting the strongest signal first. Then, the receiver continues to decode and subtract all the other user signals, from the strongest to the weakest, in an iterative fashion until it decodes its own signal. In the following steps, we are going to explain and justify the decoding strategy adopted by the two users. We denote by $SINR_{(i,r)}$ the SINR experienced by User-$r$ when decoding signal of User-i. Suppose User-2 directly demodulates its own signal by considering User-1 signal as interference noise; therefore, starting from Equation (3.2), we can write the corresponding SINR as:

$$\begin{aligned} SINR_{(1,2)} &= \frac{E[|h_2 X_2|^2]}{E[|h_2 X_1 + Z_2|^2]} \\ &= \frac{|h_2|^2 E[|X_2|^2]}{|h_2|^2 E[|X_1|^2] + h_2^* E[X_1^* Z_2] + h_2 E[X_1 Z_2^*] + E[|Z_2|^2]} \\ &= \frac{|h_2|^2 (1-\alpha) P}{|h_2|^2 E[|X_1|^2] + h_2^* E[X_1^*] E[Z_2] + h_2 E[X_1] E[Z_2^*] + E[|Z_2|^2]} \\ &= \frac{|h_2|^2 (1-\alpha) P}{|h_2|^2 E[|X_1|^2] + E[|Z_2|^2]} \\ &= \frac{|h_2|^2 (1-\alpha) P}{|h_2|^2 \alpha P + N} \\ &= \frac{|h_2|^2 P_2}{|h_2|^2 P_1 + N} \end{aligned} \tag{3.3}$$

Where user signals ($X_1$, $X_2$) and noise signals ($Z_1$, $Z_2$) are statistically independent and have zero expected values, justifying the intermediate steps in the previous derivation.

Equation (3.3) can be extended to the generic $m$-user scenario. Suppose User-$r$ is performing its $n$-th SIC iteration. We define:

**Definition 3.2.1.** $I_r(n) \equiv$ "Set of indices corresponding to users whose signal has not been decoded yet by User-$r$ at iteration $n$".

The following holds: $I_r(n) \subseteq \{1, ..., m\}$. We denote by $SINR_{(i,r;n)}$ the SINR experienced by User-$r$ when decoding signal of User-i at iteration $n$. Assuming all previous SIC iterations have been executed without any residual uncertainty (ideal SIC), the result derived in Equation (3.3) can be generalized as:

$$SINR_{(i,r;n)} = \frac{|h_r|^2 P_i}{|h_r|^2 \sum_{j \in I_r(n) \setminus i} P_j + N} \tag{3.4}$$

At the $n$-th SIC iteration, among the remaining users' signals, User-$r$ decodes the one whose corresponding SINR is maximum. So, the optimal choice is as follows:

$$\begin{aligned} i_{opt,r;n} &= \underset{i \in I_r(n)}{\operatorname{argmax}} SINR_{(i,r;n)} \\ &= \underset{i \in I_r(n)}{\operatorname{argmax}} \frac{|h_r|^2 P_i}{|h_r|^2 \sum_{j \in I_r(n) \setminus i} P_j + N} \\ &= \underset{i \in I_r(n)}{\operatorname{argmax}} \frac{P_i}{\sum_{j \in I_r(n) \setminus i} P_j + {}^{N}\!/_{|h_r|^2}} \end{aligned} \tag{3.5}$$

We define:

$$P_n \triangleq \sum_{k \in I_r(n)} P_k$$

This way we have:

$$\frac{P_i}{\sum_{j \in I_r(n) \setminus i} P_j + {}^{N}\!/_{|h_r|^2}} = \frac{P_i}{P_n - P_i + {}^{N}\!/_{|h_r|^2}} \tag{3.6}$$

Since $P_n \geq P_i$, $\forall i$ and ${}^{N}\!/_{|h_r|^2} > 0$, the denominator of the previous expression is always positive. Therefore, the original maximization problem reduces to maximize $P_i$:

$$i_{opt,r;n} = \underset{i \in I_r(n)}{\operatorname{argmax}} P_i \tag{3.7}$$

It's interesting to observe that Equation (3.7) does not depend on index $r$. Hence, each User-$r$, at the $n$-th iteration, will decode the signal (among the available ones at the $n$-th iteration) with the highest allocated power. If we assume $|h_1| > |h_2| > ... > |h_m|$, and so we choose a power allocation policy such that $P_1 < P_2 < ...P_m$, User-$r$ will perform SIC according to the following decoding order: $X_m, X_{m-1}, ..., X_r$.

In our 2-user system, we have $|h_1| > |h_2|$ and $P_1 < P_2$, hence User-1 will decode and subtract $X_2$ before decoding $X_1$, instead User-2 will directly decode $X_2$. If we assume User-1 performs an ideal SIC:

$$Y_1 = h_1 X_1 + h_1 X_2 + Z_1 \xrightarrow{(ideal)\ SIC} \tilde{Y}_1 = Y_1 - h_1 X_2 = h_1 X_1 + Z_1 \tag{3.8}$$

We can write the SINR for User-1 and for User-2 accordingly to Equation (3.4).

For User-1:

$$\begin{cases} SINR_{(2,1;1)} = \frac{|h_1|^2(1-\alpha)P}{|h_1|^2 \alpha P + N} \ \text{(1st iteration)} \\ \\ SINR_{(1,1;2)} = \frac{|h_1|^2 \alpha P}{N} \ \text{(2nd iteration)} \end{cases} \tag{3.9}$$

For User-2:

$$\left\{SINR_{(2,2;1)} = \frac{|h_2|^2(1-\alpha)P}{|h_2|^2\alpha P+N} \right. \tag{3.10}$$

The ideal SIC assumption is used to derive the capacity region shown in Equation (3.14), however our simulations will keep into account the propagation of the SIC error (see Section 3.5.4 for further details).

To ensure the system operates correctly, $SINR_{(2,1;1)}$, $SINR_{(1,1;2)}$, $SINR_{(2,2;1)}$ must each exceed a respective threshold. However, it can be shown that:

$$SINR_{(2,1;1)} > SINR_{(2,2;1)}$$

Therefore, the threshold constraints apply only to $SINR_{(1,1;2)}$ and $SINR_{(2,2;1)}$.

To simplify the notation we set:

$$\begin{cases} SNR_{(1)} \triangleq SINR_{(1,1;2)} \\ SINR_{(2)} \triangleq SINR_{(2,2;1)} \end{cases} \tag{3.11}$$

We notice that:

- User-1 equivalent channel is $AWGN$ with $SNR = SNR_{(1)}$
- User-2 equivalent channel is $AWGN$ with $SNR = SINR_{(2)}$

Therefore, considering the $AWGN$ channel capacity formula (A.6), we get:

$$\begin{cases} R_1 \leq \log_2(1 + SNR_{(1)}) = \log_2(1 + \frac{|h_1|^2\alpha P}{N}) \\ \\ R_2 \leq \log_2(1 + SINR_{(2)}) = \log_2(1 + \frac{|h_2|^2(1-\alpha)P}{|h_2|^2\alpha P+N}) \end{cases} \tag{3.12}$$

The set of achievable rate pairs $(R_1, R_2)$ describes the capacity region of a Gaussian broadcast channel (see appendix B.3 for a formal explanation).

We define the following two SNRs parameters with respect to the total transmitted power $P$:

$$\begin{cases} \rho_1 \triangleq |h_1|^2 \frac{P}{N} \\ \\ \rho_2 \triangleq |h_2|^2 \frac{P}{N} \end{cases} \tag{3.13}$$

The achievable rates inequalities can be re-written as:

$$\begin{cases} R_1 \leq \log_2(1 + \alpha\rho_1) \\ \\ R_2 \leq \log_2\left(1 + \frac{(1-\alpha)\rho_2}{1+\alpha\rho_2}\right) \end{cases} \tag{3.14}$$

Figure 3.1 shows the achievable rates as a function of the parameter $\alpha$, fixed $\rho_1 = 13\,dB$ and $\rho_2 = 10\,dB$.

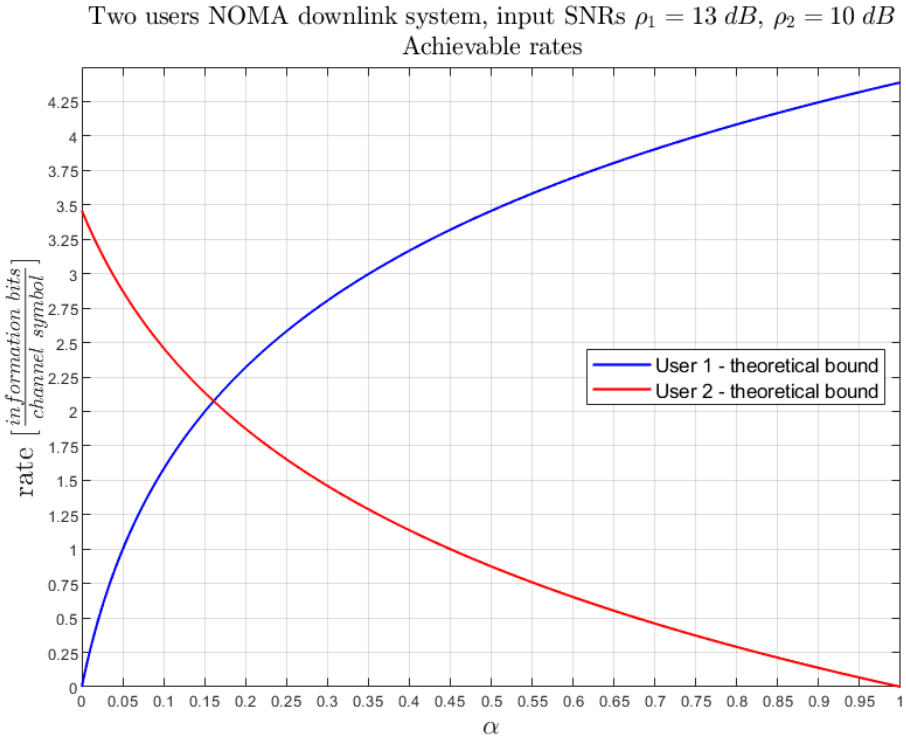



**Figure 3.1:** Two-user NOMA *AWGN* downlink system - achievable rates (mentioned on p. 13)

## 3.3 FER Vs. SNR simulation

In this analysis we fix the following input parameters:

- $min\{\rho_2\} = -3\ dB$
- $\frac{|h_1|^2}{|h_2|^2} = 5 \rightarrow \rho_1 \simeq \rho_2 + 7\ dB$
- $\alpha = 0.2$
- $m_1 = 8\ {}^{bits}/_{symbol}$
- $m_2 = 2\ {}^{bits}/_{symbol}$
- $N_{iter} = 7$
- $R_{C-U1} = R_{C-U2} = R_C \simeq {}^1/_3$ (unpunctured configuration)

The simulation is performed by increasing the $\rho_2$ value step by step. For each $\rho_2$ value, we collect 500 wrong frames. The overall simulation finally stops when the frame error rate (FER) of both users goes below $10^{-2}$.

Figure 3.2, 3.3 and 3.4 show the results of the simulations for different values of $f_{size-U1}$ and $f_{size-U2}$.

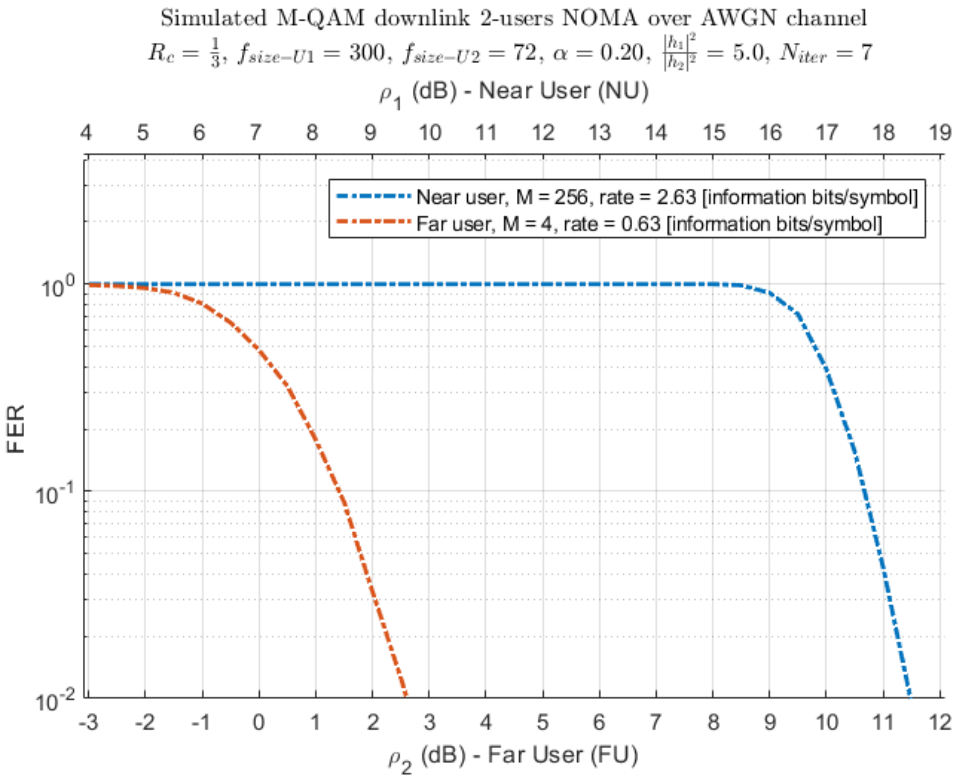



**Figure 3.2:** Two-user downlink NOMA - FER Vs. SNRs, $f_{size-U1} = 300$ bits (mentioned on p. 15)

As expected, by increasing the frame length the performance of the turbo decoder improves; however, further increasing the frame length over a certain threshold does not lead to a significant reduction of the FER, as it soon tends to be saturated. From this analysis, we concluded that choosing a frame size around 600 represents a good compromise between decoding performance and computational cost; more details about the performance of the UMTS turbo code for different input frame sizes can be found in [6].

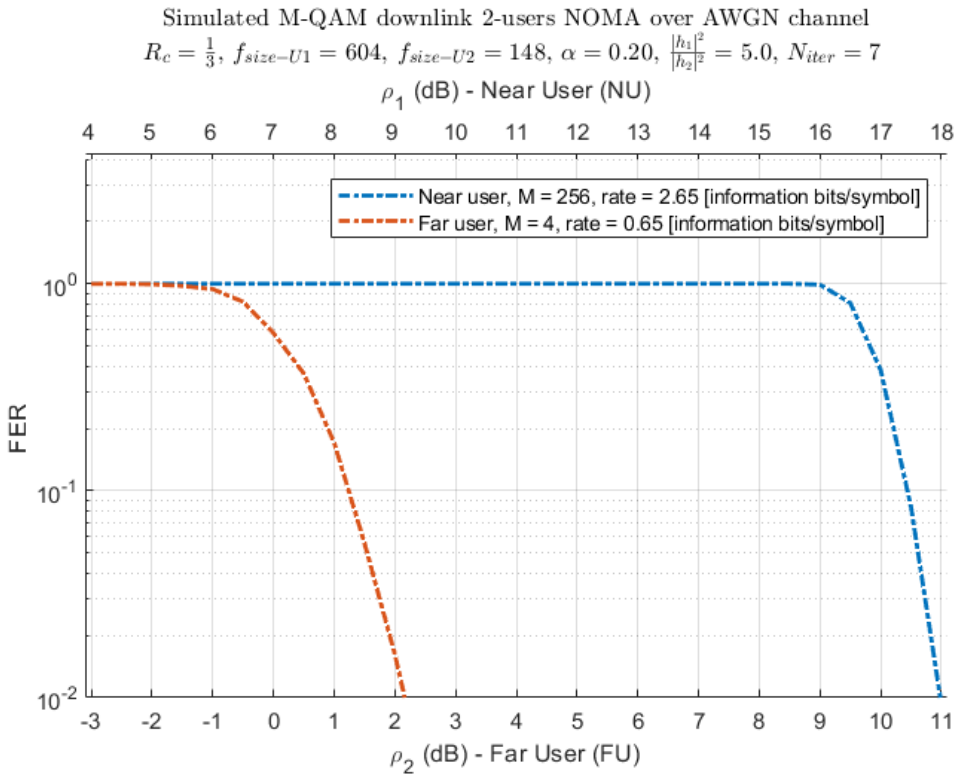



**Figure 3.3:** Two-user downlink NOMA - FER Vs. SNRs, $f_{size-U1} = 604$ bits (mentioned on p. 15)

## 3.4 MODCODs Vs. capacity region

### 3.4.1 Achievable rates analysis

In the following analysis:

- We fix the user SNRs
  - $\rho_1 = 13\ dB$
  - $\rho_2 = 10\ dB$
- $N_{iter} = 13$
- We consider a subset of $\alpha$ values $\in \{0,0.5\}$
- For each value of $\alpha$ we vary the modulation cardinality of users and their puncturing patterns until we find and store:

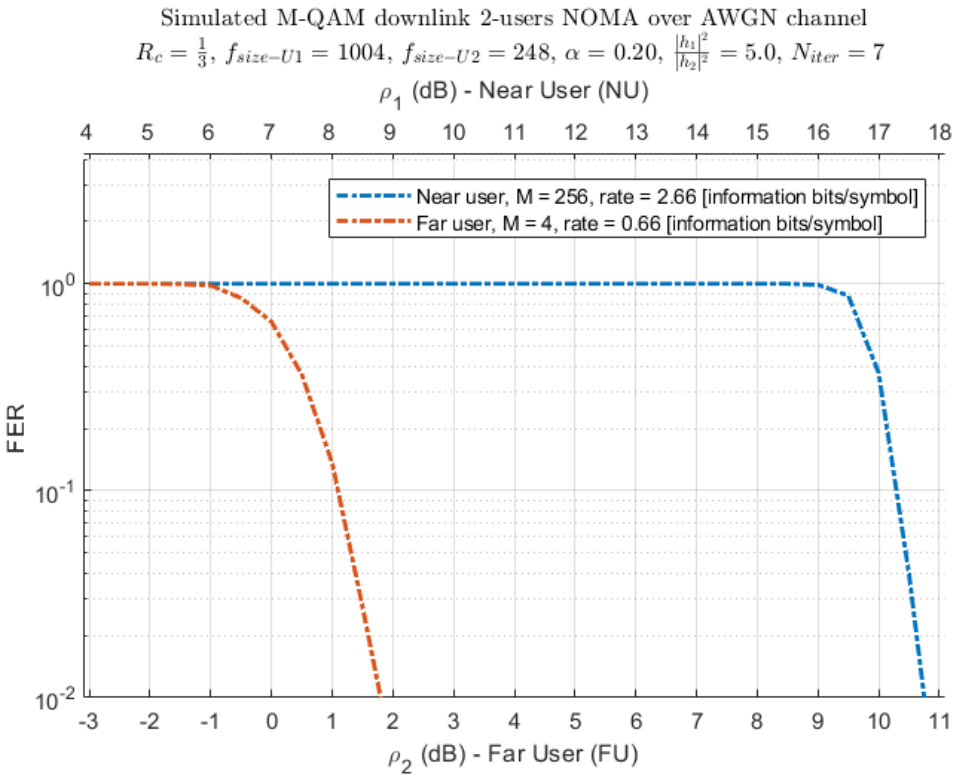



**Figure 3.4:** Two-user downlink NOMA - FER Vs. SNRs, $f_{size-U1} = 1004$ bits (mentioned on p. 15)

  - A pair of two MODCODs; the first of User-1 and the second of User-2, corresponding to a FER slightly below $10^{-3}$ for both users.
  - Another pair of two MODCODs; the first of User-1 and the second of User-2, corresponding to a FER slightly above $10^{-3}$ for both users.

- We interpolate the information rates ($r_{-U1}$ and $r_{-U2}$) corresponding to the pair of MODCODs with FER below $10^{-3}$ with the ones corresponding to the pair of MODCODs with FER above $10^{-3}$; finally we compute the corresponding rates, for both users, evaluated at $FER = 10^{-3}$

Before continuing with the simulation analysis, it is appropriate to list some important comments concerning the reliability of the obtained results.

- User-1 frame size ($f_{size-U1}$) has been fixed around 600 bits (independently from the considered value of $\alpha$) instead, User-2 frame size ($f_{size-U2}$) varies according to the ratio between the modulation cardinality of the two users.

Notice that, since simulations are taken frame by frame, the user with the lowest rate will also have a smaller information frame size. Smaller frame sizes imply:

  - An intrinsic reduction of the code rate due to the fixed overhead of the turbo encoding system (12 tail bits independently from the frame size).
  - A worst performance of the turbo decoder as we previously discussed and shown in Section 3.4.

- The chosen puncturing patterns are not optimal. In [7] has been proposed an algorithm to find optimal rate-compatible punctured turbo codes (RPTC) patterns, whose parameters include the information sizes and the puncturing period. In our work we do not apply the proposed algorithm but we choose the puncturing patterns presented in [7] corresponding to the ones which are found for information size equal to 320 and puncturing period equal to 8 (Table 3.1). However, as said before, our analysis include different frame sizes for every $\alpha$ and for every user; therefore a puncturing pattern (which is optimized for frame lengths equal to 320) can perform better or worse depending on the considered frame length. In this work we do not quantify the impact of non-optimal puncturing on the achieved performances.

  To learn more about the notion of rate-compatible codes refer to [8], then see [9], [10] and [7] for their extensions to turbo code.

- As can be seen in the tables below, the FER values of the MODCODs used for interpolation are often relatively far from $10^{-3}$. This spreading leads to less interpolation accuracy and consequently some results may be less reliable than others.

| Pattern index | Code Rate | Systematic part | First encoder | Second encoder |
|---|---|---|---|---|
| 1 | $1/3$ | 11111111 | 11111111 | 11111111 |
| 2 | $4/11$ | 11111111 | 11011101 | 11111111 |
| 3 | $2/5$ | 11111111 | 01010101 | 11111111 |
| 4 | $4/9$ | 11111111 | 01010101 | 11110011 |
| 5 | $1/2$ | 11111111 | 01010001 | 10110011 |
| 6 | $4/7$ | 11111111 | 01000001 | 10110001 |
| 7 | $2/3$ | 11111111 | 01000001 | 00010001 |
| 8 | $4/5$ | 11111111 | 01000000 | 00000001 |

**Table 3.1:** Puncturing patterns (mentioned on pp. 18, 19)

Table 3.2 shows the pairs of MODCODs that achieve a FER immediately below $10^{-3}$; on the other hand, Table 3.3 shows the pairs of MODCODs that

achieve a FER immediately above $10^{-3}$. The rates of User-1 and User-2 ($r_{-U1}$ and $r_{-U2}$) are expressed in information bits per channel symbol. $m_i$ and $P_{Ui}$ indicate for User-$i \in \{1,2\}$ the modulation efficiency and the puncturing pattern index respectively. We ordered the puncturing pattern indexes in such a way that higher indexes correspond to higher code rate patterns; in Table 3.1 all the implemented puncturing patterns are shown in detail.

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.05 | 600 | 1804 | (2,1) | (4,5) | 5.0e-04 | 7.4e-04 | 0.6623 | 1.9912 |
| 0.10 | 600 | 964 | (2,5) | (4,3) | 1.8e-04 | 2.6e-04 | 0.9901 | 1.5908 |
| 0.15 | 600 | 654 | (4,1) | (4,2) | 3.2e-04 | 4.2e-04 | 1.3245 | 1.4437 |
| 0.20 | 608 | 428 | (4,3) | (2,6) | 8.7e-04 | 1.6e-04 | 1.5875 | 1.1175 |
| 0.25 | 602 | 336 | (4,4) | (2,5) | 3.5e-04 | 6.8e-05 | 1.7602 | 0.9825 |
| 0.30 | 602 | 336 | (4,4) | (2,5) | 9.4e-05 | 5.8e-04 | 1.7602 | 0.9825 |
| 0.35 | 600 | 264 | (4,5) | (2,4) | 3.3e-04 | 4.6e-04 | 1.9802 | 0.8713 |
| 0.40 | 602 | 216 | (6,1) | (2,2) | 9.5e-04 | 3.3e-04 | 1.9868 | 0.7129 |
| 0.44 | 604 | 182 | (6,2) | (2,1) | 7.8e-04 | 7.4e-04 | 2.1649 | 0.6523 |

**Table 3.2:** Pairs of MODCODs for User-1 and User-2 @$FER < 10^{-3}$ (mentioned on p. 18)

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.05 | 602 | 1898 | (2,2) | (4,6) | 2.1e-03 | 4.1e-03 | 0.7218 | 2.2758 |
| 0.10 | 600 | 1056 | (2,6) | (4,5) | 3.3e-03 | 4.2e-02 | 1.1299 | 1.9887 |
| 0.15 | 608 | 668 | (4,2) | (4,3) | 2.9e-03 | 5.9e-03 | 1.4442 | 1.5867 |
| 0.20 | 602 | 452 | (4,4) | (4,1) | 1.2e-02 | 2.6e-03 | 1.7602 | 1.3216 |
| 0.25 | 600 | 394 | (4,5) | (2,7) | 2.1e-02 | 2.6e-02 | 1.9802 | 1.3003 |
| 0.30 | 600 | 338 | (4,5) | (2,6) | 1.9e-03 | 1.8e-02 | 1.9802 | 1.1155 |
| 0.35 | 600 | 296 | (6,1) | (2,5) | 6.9e-03 | 2.2e-02 | 1.9868 | 0.9801 |
| 0.40 | 604 | 218 | (6,2) | (2,3) | 1.5e-03 | 2.8e-03 | 2.1649 | 0.7814 |
| 0.44 | 604 | 180 | (6,3) | (2,2) | 7.3e-03 | 6.8e-03 | 2.3780 | 0.7087 |

**Table 3.3:** Pairs of MODCODs for User-1 and User-2 @$FER > 10^{-3}$ (mentioned on p. 18)

Finally, Table 3.4 shows the interpolated results from the previous tables evaluated at $FER = 10^{-3}$.

Figure 3.5 shows the MODCODs performances against the capacity region.

As expected, the dashed curves corresponding to the implemented MODCODs are below the capacity region. It is interesting to observe that, as the information theoretical limit increases, it becomes more and more difficult to find a MODCOD capable of approaching it.

| $\alpha$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|
| 0.05 | 0.6907 | 2.0419 |
| 0.10 | 1.0724 | 1.6952 |
| 0.15 | 1.3860 | 1.4905 |
| 0.20 | 1.5969 | 1.2506 |
| 0.25 | 1.8173 | 1.1263 |
| 0.30 | 1.9336 | 1.0033 |
| 0.35 | 1.9826 | 0.8929 |
| 0.40 | 2.0092 | 0.7479 |
| 0.44 | 2.1890 | 0.6598 |

**Table 3.4:** Interpolated rates for User-1 and User-2 @$FER = 10^{-3}$ (mentioned on p. 19)

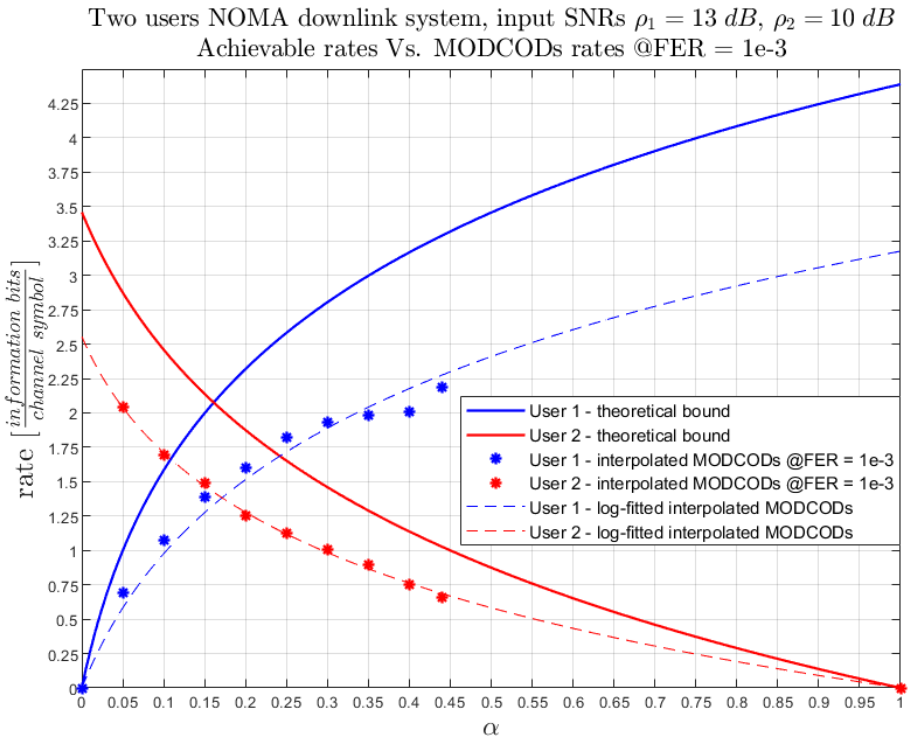



**Figure 3.5:** Two-user NOMA *AWGN* downlink system - MODCODs Vs. achievable rates (mentioned on p. 19)

### 3.4.2 Sum-rate analysis

The sum-rate theoretical bound is given by:

$$R_{sum-bound} = \log_2(1+\alpha\rho_1) + \log_2\left(1+\frac{(1-\alpha)\rho_2}{1+\alpha\rho_2}\right) \tag{3.15}$$

If we consider an orthogonal multiple access system (OMA), a fraction $\alpha$ of the channel resources is exclusively assigned to User-1, instead a fraction $1-\alpha$ is assigned to User-2. Each user has all the available power $P$ for transmission, this way (fixed the same input SNRs $\rho_1$ and $\rho_2$) the OMA rate limits are given by:

$$\begin{cases} R_{1-OMA} \leq \alpha\log_2(1+\rho_1) \\ R_{2-OMA} \leq (1-\alpha)\log_2(1+\rho_2) \end{cases} \tag{3.16}$$

And the corresponding sum-rate limit is:

$$R_{sum-OMA} = \alpha\log_2(1+\rho_1) + (1-\alpha)\log_2(1+\rho_2) \tag{3.17}$$

Figure 3.6 shows the sum-rate performances of the interpolated MODCODs evaluated at $FER = 10^{-3}$ (black dashed curve) against the sum-rate given by the capacity region (red curve) and the sum-rate limit given by an orthogonal multiple access (OMA) system with the same input SNRs (13,10) $dB$ (blue curve).

As expected the sum-rate of the capacity region is the highest; instead, for this particular SNRs pair, the sum-rate of the interpolated MODCODs is even below the one of the OMA system.

### 3.4.3 Operating point: MAX-MIN approach

In [11], [12] different types of power allocation for a NOMA system are analyzed. In particular they focused on the MAX-MIN approach under proportional fairness constraints, which provides very good results in terms of proportional fairness and transmission rate variation. We limit our analysis on the simple MAX-MIN approach (which may penalizes the user with highest SNR). Figure 3.7 shows different curves representing the minimum between the rate of User-1 and User-2; in particular they refer to the capacity region (red curve), to the OMA system (blue curve) and to the interpolated MODCODs evaluated at $FER = 10^{-3}$ (black dashed curve).

Please notice that the dashed lines indicate the MAX-MIN rate and the corresponding alpha value (operating point); obviously the MAX-MIN rate is the same for both users. As expected, the capacity region provides a MAX-MIN operating point with higher rate in respect to the OMA system one; instead, the MAX-MIN operating point of the interpolated MODCODs has the lowest rate.

Notice that the NOMA operating point is lower than the OMA one ($\alpha = 0.15$ Vs. $\alpha = 0.44$).

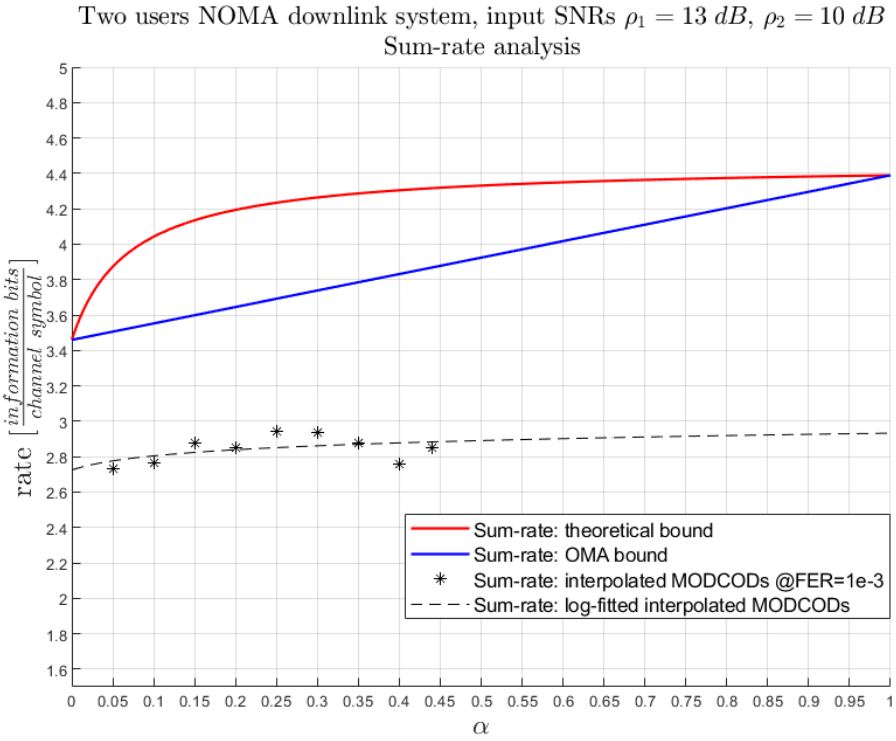



**Figure 3.6:** Two-user NOMA *AWGN* downlink system - Sum rate analysis (mentioned on p. 21)

### 3.4.4 Results for different input SNRs

The entire analysis has been repeated for other input SNR pairs:

- $(\rho_1 = 13, \rho_2 = 10)\ dB$ (previously tested)
- $(\rho_1 = 15, \rho_2 = 12)\ dB$
- $(\rho_1 = 20, \rho_2 = 10)\ dB$

In the following sections we report all the results concerning all the SNR pairs. For simplicity, captions of tables and figures are abbreviated; please refer to the figures and tables above for the full name.

### 3.4.5 Results: MODCODs with FER below $10^{-3}$

The following tables show the MODCODs with $FER < 10^{-3}$

- Table 3.5 for input SNRs (13,10) $dB$

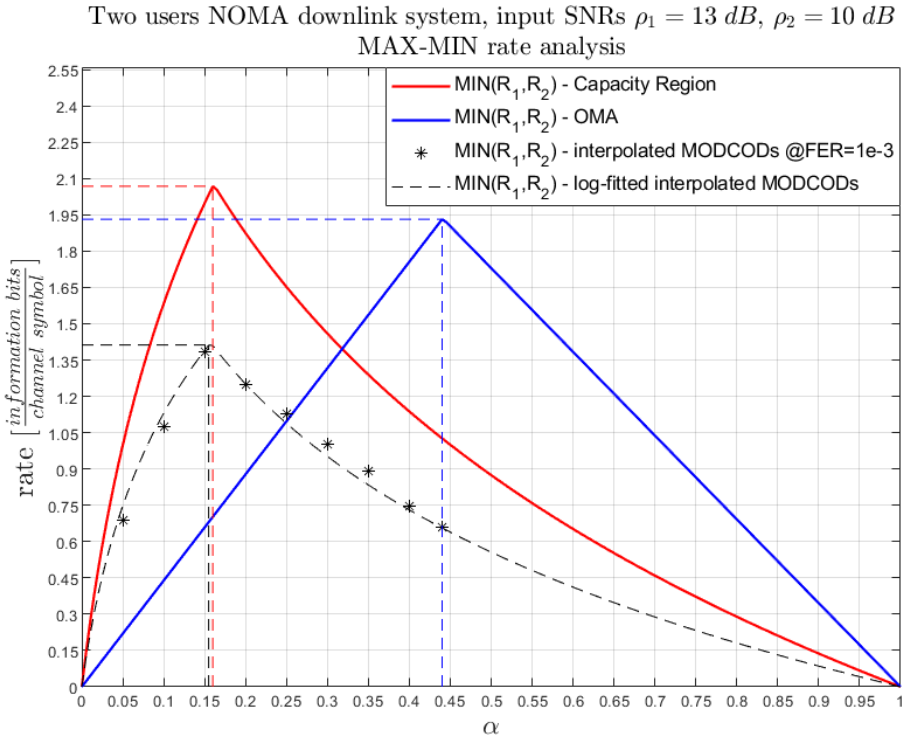



**Figure 3.7:** Two-user NOMA $AWGN$ downlink system - MAX MIN rate analysis (mentioned on p. 21)

- Table 3.6 for input SNRs (15,12) $dB$
- Table 3.7 for input SNRs (20,10) $dB$

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.05 | 600 | 1804 | (2,1) | (4,5) | 5.0e-04 | 7.4e-04 | 0.6623 | 1.9912 |
| 0.10 | 600 | 964 | (2,5) | (4,3) | 1.8e-04 | 2.6e-04 | 0.9901 | 1.5908 |
| 0.15 | 600 | 654 | (4,1) | (4,2) | 3.2e-04 | 4.2e-04 | 1.3245 | 1.4437 |
| 0.20 | 608 | 428 | (4,3) | (2,6) | 8.7e-04 | 1.6e-04 | 1.5875 | 1.1175 |
| 0.25 | 602 | 336 | (4,4) | (2,5) | 3.5e-04 | 6.8e-05 | 1.7602 | 0.9825 |
| 0.30 | 602 | 336 | (4,4) | (2,5) | 9.4e-05 | 5.8e-04 | 1.7602 | 0.9825 |
| 0.35 | 600 | 264 | (4,5) | (2,4) | 3.3e-04 | 4.6e-04 | 1.9802 | 0.8713 |
| 0.40 | 602 | 216 | (6,1) | (2,2) | 9.5e-04 | 3.3e-04 | 1.9868 | 0.7129 |
| 0.44 | 604 | 182 | (6,2) | (2,1) | 7.8e-04 | 7.4e-04 | 2.1649 | 0.6523 |

**Table 3.5:** SNRs (13,10) $dB$ @$FER < 10^{-3}$ (mentioned on p. 22)

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.045 | 602 | 1636 | (2,4) | (6,3) | 6.6e-04 | 8.0e-04 | 0.8801 | 2.3918 |
| 0.10 | 622 | 856 | (4,2) | (4,5) | 7.4e-04 | 8.7e-04 | 1.4432 | 1.9861 |
| 0.15 | 612 | 552 | (4,4) | (4,3) | 6.8e-04 | 8.7e-04 | 1.7586 | 1.5862 |
| 0.20 | 600 | 400 | (4,5) | (4,1) | 7.8e-04 | 4.4e-04 | 1.9802 | 1.3201 |
| 0.25 | 600 | 338 | (4,5) | (2,6) | 1.1e-04 | 9.4e-05 | 1.9802 | 1.1155 |
| 0.30 | 602 | 272 | (6,2) | (2,5) | 3.0e-04 | 1.5e-04 | 2.1655 | 0.9784 |
| 0.35 | 604 | 242 | (6,2) | (2,4) | 1.5e-04 | 1.2e-04 | 2.1649 | 0.8674 |
| 0.40 | 600 | 196 | (6,3) | (2,3) | 7.4e-04 | 5.8e-04 | 2.3810 | 0.7778 |
| 0.45 | 602 | 148 | (6,4) | (2,1) | 2.3e-04 | 4.6e-04 | 2.6404 | 0.6491 |

**Table 3.6:** SNRs (15,12) $dB$ @$FER < 10^{-3}$ (mentioned on p. 23)

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.025 | 600 | 1204 | (2,6) | (4,6) | 2.3e-04 | 4.8e-04 | 1.1299 | 2.2674 |
| 0.05 | 602 | 676 | (4,4) | (4,5) | 3.6e-04 | 9.2e-04 | 1.7602 | 1.9766 |
| 0.10 | 602 | 440 | (6,2) | (4,3) | 2.2e-04 | 3.6e-04 | 2.1655 | 1.5827 |
| 0.15 | 602 | 300 | (6,4) | (4,1) | 1.0e-04 | 2.5e-04 | 2.6404 | 1.3158 |
| 0.20 | 612 | 234 | (8,2) | (2,6) | 9.6e-05 | 1.2e-04 | 2.8868 | 1.1038 |
| 0.25 | 612 | 186 | (8,3) | (2,5) | 2.3e-04 | 8.1e-05 | 3.1710 | 0.9637 |
| 0.30 | 600 | 162 | (8,3) | (2,4) | 5.8e-05 | 1.0e-04 | 3.1746 | 0.8571 |
| 0.35 | 616 | 144 | (10,1) | (2,3) | 7.0e-04 | 2.6e-04 | 3.3118 | 0.7742 |
| 0.40 | 606 | 118 | (10,1) | (2,1) | 9.5e-05 | 6.8e-04 | 3.3115 | 0.6448 |

**Table 3.7:** SNRs (20,10) $dB$ @$FER < 10^{-3}$ (mentioned on p. 23)

### 3.4.6 Results: MODCODs with FER above $10^{-3}$

The following tables show the MODCODs with $FER > 10^{-3}$

- Table 3.8 for input SNRs (13,10) $dB$
- Table 3.9 for input SNRs (15,12) $dB$
- Table 3.10 for input SNRs (20,10) $dB$

### 3.4.7 Results: interpolated MODCODs @$FER = 10^{-3}$

The following tables show the interpolated MODCODs' performances evaluated at $FER = 10^{-3}$

- Table 3.11 for input SNRs (13,10) $dB$
- Table 3.12 for input SNRs (15,12) $dB$

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.05 | 602 | 1898 | (2,2) | (4,6) | 2.1e-03 | 4.1e-03 | 0.7218 | 2.2758 |
| 0.10 | 600 | 1056 | (2,6) | (4,5) | 3.3e-03 | 4.2e-02 | 1.1299 | 1.9887 |
| 0.15 | 608 | 668 | (4,2) | (4,3) | 2.9e-03 | 5.9e-03 | 1.4442 | 1.5867 |
| 0.20 | 602 | 452 | (4,4) | (4,1) | 1.2e-02 | 2.6e-03 | 1.7602 | 1.3216 |
| 0.25 | 600 | 394 | (4,5) | (2,7) | 2.1e-02 | 2.6e-02 | 1.9802 | 1.3003 |
| 0.30 | 600 | 338 | (4,5) | (2,6) | 1.9e-03 | 1.8e-02 | 1.9802 | 1.1155 |
| 0.35 | 600 | 296 | (6,1) | (2,5) | 6.9e-03 | 2.2e-02 | 1.9868 | 0.9801 |
| 0.40 | 604 | 218 | (6,2) | (2,3) | 1.5e-03 | 2.8e-03 | 2.1649 | 0.7814 |
| 0.44 | 604 | 180 | (6,3) | (2,2) | 7.3e-03 | 6.8e-03 | 2.3780 | 0.7087 |

**Table 3.8:** SNRs (13,10) $dB$ @$FER > 10^{-3}$ (mentioned on p. 24)

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.045 | 600 | 1610 | (2,5) | (6,4) | 2.5e-02 | 1.9e-01 | 0.9901 | 2.6568 |
| 0.10 | 604 | 864 | (4,3) | (4,6) | 6.1e-02 | 1.7e-01 | 1.5853 | 2.2677 |
| 0.15 | 600 | 532 | (4,5) | (4,4) | 4.9e-02 | 7.7e-03 | 1.9802 | 1.7558 |
| 0.20 | 602 | 384 | (4,6) | (4,2) | 2.8e-02 | 4.7e-03 | 2.2547 | 1.4382 |
| 0.25 | 602 | 346 | (4,6) | (2,7) | 1.6e-03 | 1.4e-03 | 2.2547 | 1.2959 |
| 0.30 | 602 | 278 | (6,3) | (2,6) | 3.2e-03 | 2.4e-03 | 2.3794 | 1.0988 |
| 0.35 | 600 | 244 | (6,3) | (2,5) | 1.6e-03 | 2.7e-03 | 2.3810 | 0.9683 |
| 0.40 | 602 | 196 | (6,4) | (2,4) | 1.4e-03 | 8.8e-03 | 2.6404 | 0.8596 |
| 0.45 | 628 | 168 | (8,1) | (2,2) | 1.2e-03 | 3.1e-03 | 2.6498 | 0.7089 |

**Table 3.9:** SNRs (15,12) $dB$ @$FER > 10^{-3}$ (mentioned on p. 24)

- Table 3.13 for input SNRs (20,10) $dB$

### 3.4.8 Results: interpolated MODCODs Vs. capacity region

The following figures show the interpolated MODCODs' performances evaluated at $FER = 10^{-3}$ against the capacity region of the Gaussian broadcast channel.

- Figure 3.8 for input SNRs (13,10) $dB$
- Figure 3.9 for input SNRs (15,12) $dB$
- Figure 3.10 for input SNRs (20,10) $dB$

In general it can be observed that the rate performance of the implemented MODCODs follows the bound of the capacity region related to the particular pair of SNRs under analysis and give us an idea on the achievable performances with M-QAM and Turbo Code in static channel conditions.

| $\alpha$ | $f_{size-U1}$ | $f_{size-U2}$ | $(m_1, P_{U1})$ | $(m_2, P_{U2})$ | $FER_{-U1}$ | $FER_{-U2}$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|---|---|---|---|---|---|
| 0.025 | 600 | 1208 | (2,7) | (4,7) | 4.5e-03 | 1.2e-01 | 1.3158 | 2.6491 |
| 0.05 | 608 | 692 | (4,5) | (4,6) | 1.8e-02 | 1.7e-02 | 1.9805 | 2.2541 |
| 0.10 | 600 | 400 | (4,7) | (4,4) | 3.5e-03 | 1.4e-03 | 2.6316 | 1.7544 |
| 0.15 | 604 | 292 | (6,5) | (4,2) | 3.9e-03 | 1.1e-03 | 2.9608 | 1.4314 |
| 0.20 | 600 | 242 | (8,3) | (2,7) | 5.6e-03 | 1.3e-03 | 3.1746 | 1.2804 |
| 0.25 | 612 | 192 | (8,4) | (2,6) | 2.0e-02 | 1.5e-03 | 3.5172 | 1.1034 |
| 0.30 | 612 | 192 | (8,4) | (2,6) | 1.1e-03 | 4.4e-02 | 3.5172 | 1.1034 |
| 0.35 | 606 | 144 | (10,2) | (2,4) | 2.9e-03 | 2.7e-03 | 3.6071 | 0.8571 |
| 0.40 | 614 | 108 | (10,3) | (2,2) | 7.4e-02 | 3.6e-03 | 3.9613 | 0.6968 |

**Table 3.10:** SNRs (20,10) $dB$ @$FER > 10^{-3}$ (mentioned on p. 24)

| $\alpha$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|
| 0.05 | 0.6907 | 2.0419 |
| 0.10 | 1.0724 | 1.6952 |
| 0.15 | 1.3860 | 1.4905 |
| 0.20 | 1.5969 | 1.2506 |
| 0.25 | 1.8173 | 1.1263 |
| 0.30 | 1.9336 | 1.0033 |
| 0.35 | 1.9826 | 0.8929 |
| 0.40 | 2.0092 | 0.7479 |
| 0.44 | 2.1890 | 0.6598 |

**Table 3.11:** SNRs (13,10) $dB$ - interpolated rates @$FER = 10^{-3}$ (mentioned on p. 24)

### 3.4.9 Results: sum-rate analysis

The following figures show the sum-rate analysis.

- Figure 3.11 for input SNRs (13,10) $dB$
- Figure 3.12 for input SNRs (15,12) $dB$
- Figure 3.13 for input SNRs (20,10) $dB$

It is interesting to observe that in the case of input SNRs (20,10) $dB$ the sum-rate of the interpolated MODCODs is, for some alpha, higher than the maximum sum-rate achivable by an OMA system with same SNRs. As the difference between the two users' SNRs decreases, the advantage of implementing a NOMA system with respect to an OMA decreases as well.

| $\alpha$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|
| 0.045 | 0.8928 | 2.4029 |
| 0.10 | 1.4529 | 1.9938 |
| 0.15 | 1.7785 | 1.5974 |
| 0.20 | 1.9994 | 1.3608 |
| 0.25 | 2.2045 | 1.2729 |
| 0.30 | 2.2736 | 1.0606 |
| 0.35 | 2.3374 | 0.9359 |
| 0.40 | 2.4981 | 0.7941 |
| 0.45 | 2.6489 | 0.6736 |

**Table 3.12:** SNRs (15,12) $dB$ - interpolated rates @$FER = 10^{-3}$ (mentioned on p. 24)

| $\alpha$ | $r_{-U1}$ | $r_{-U2}$ |
|---|---|---|
| 0.025 | 1.2221 | 2.3185 |
| 0.05 | 1.8182 | 1.9850 |
| 0.10 | 2.4225 | 1.7128 |
| 0.15 | 2.8417 | 1.4229 |
| 0.20 | 3.0525 | 1.2632 |
| 0.25 | 3.2859 | 1.0851 |
| 0.30 | 3.5030 | 0.9504 |
| 0.35 | 3.5218 | 0.8216 |
| 0.40 | 3.5411 | 0.6567 |

**Table 3.13:** SNRs (20,10) $dB$ - interpolated rates @$FER = 10^{-3}$ (mentioned on p. 25)

### 3.4.10 Results: MAX-MIN rate analysis

The following figures show the MAX-MIN rate analysis.

- Figure 3.14 for input SNRs (13,10) $dB$
- Figure 3.15 for input SNRs (15,12) $dB$
- Figure 3.16 for input SNRs (20,10) $dB$

Concerning the MAX-MIN rate, as in the case of sum-rate analysis, the advantage of a NOMA system over an OMA system is greater when the difference between the input SNRs of the two users is larger.

The MAX-MIN operating points of the implemented MODCODs are:

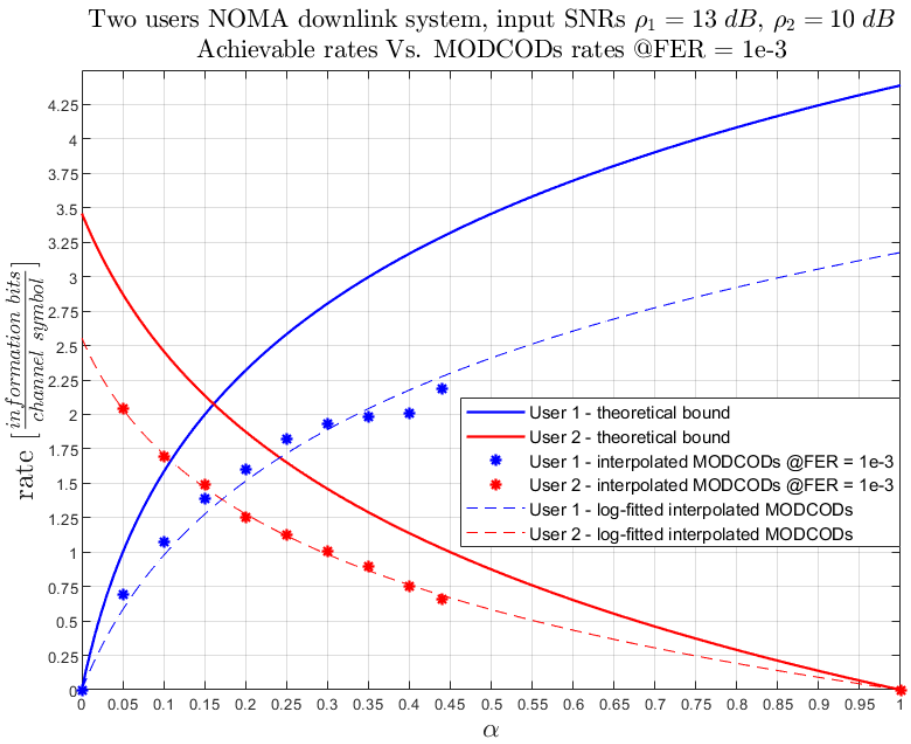



**Figure 3.8:** SNRs (13,10) *dB* - MODCODs Vs. achievable rates (mentioned on p. 25)

- $\alpha = 0.15$ for SNRs (13,10)
- $\alpha = 0.14$ for SNRs (15,12)
- $\alpha = 0.07$ for SNRs (20,10)

## 3.5 Simulation specifications

In this section we provide some further details concerning the simulation setup and algorithms.

- In Section 3.5.1 we describe the MODCODs interpolation functions.
- In Section 3.5.2 we show the pseudo codes of puncturing and "reverse" puncturing algorithms.
- In Section 3.5.3 the algorithm to determine the frame size of the two users is presented.

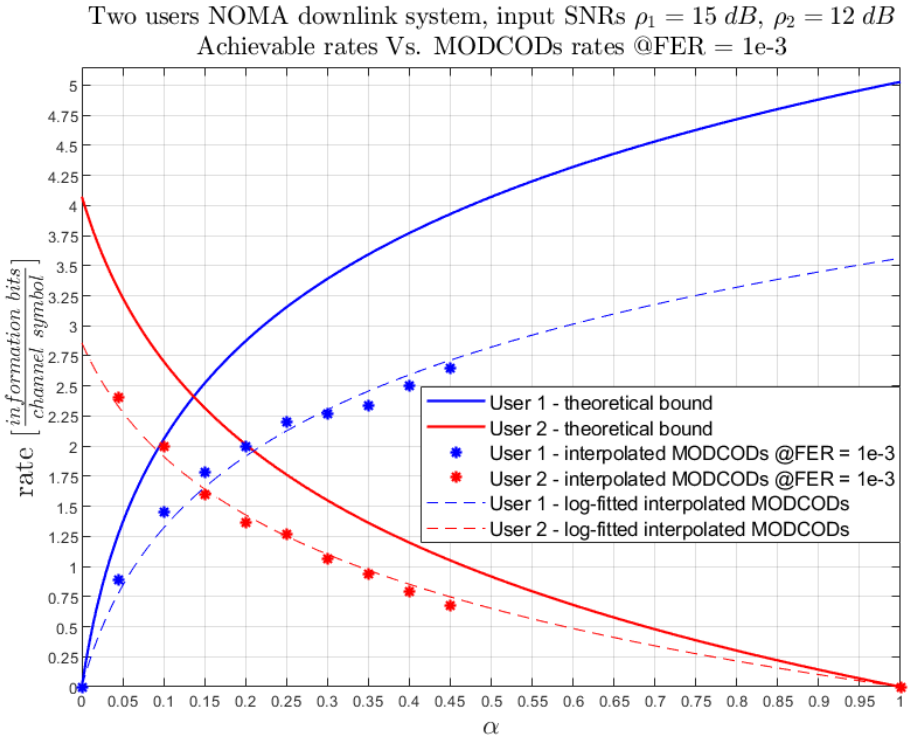



**Figure 3.9:** SNRs (15,12) $dB$ - MODCODs Vs. achievable rates (mentioned on p. 25)

### 3.5.1 Interpolation functions

Fixed $\alpha$, MODCODs corresponding to a FER above $10^{-3}$ are logarithmically interpolated with the ones corresponding to a FER below $10^{-3}$. We define:

- $r_{-Ui}(1) \equiv$ "rate of User-i corresponding to $FER_{-Ui}(1) < 10^{-3}$"
- $r_{-Ui}(2) \equiv$ "rate of User-i corresponding to $FER_{-Ui}(2) > 10^{-3}$"
- $r_{-Ui} \equiv$ "rate of User-i evaluated at target $FER = 10^{-3}$"

Then:

$$r_{-Ui} = r_{-Ui}(2) + \left( \frac{\log 10^{-3} - \log FER_{-Ui}(2)}{\log FER_{-Ui}(1) - \log FER_{-Ui}(2)} \right) (r_{-Ui}(1) - r_{-Ui}(2)) \quad (3.18)$$

The obtained interpolated rates at $FER = 10^{-3}$ are interpolated each others for different value of $\alpha$ using the following functions:

$$\begin{cases} y_1 = b_1 \log(c_1 x_1 + 1), \text{ for User-1} \\ y_2 = b_2 \log(c_2 x_2 + 1) - b_2 \log(c_2 + 1), \text{ for User-2} \end{cases} \quad (3.19)$$

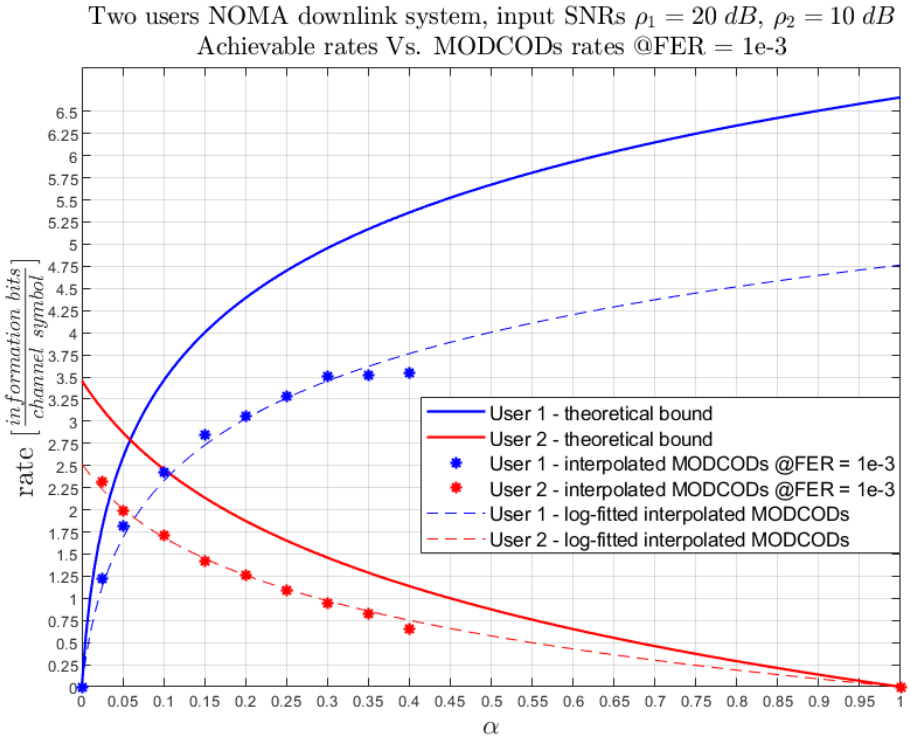



**Figure 3.10:** SNRs (20,10) *dB* - MODCODs Vs. achievable rates (mentioned on p. 25)

Where:

- ($x_1$,$x_2$) independent variables.
- ($y_1$,$y_2$) dependent variables.
- ($b_1$,$b_2$) interpolation coefficients.
- ($c_1$,$c_2$) tunable parameters.

### 3.5.2 Puncturing algorithms

In this section we describe the implemented puncturing algorithms. Algorithm 1 is performed at the transmitter side after turbo encoding. The purpose of this algorithm is to remove some bits (the ones indicated by the puncturing matrix) before transmission in order to increase the code rate. Algirithm 2 is performed after signal demodulation and right before soft decoding: it adds zero symbols in the puncturing positions in order to perform decoding.

**Algorithm 1:** Puncturing (performed at TX) (mentioned on p. 30)

**Input :**

- UserCodedBlock: user coded block after turbo encoding
- P: puncturing pattern matrix
- FrameLength: information frame size
- BlockLength: expected coded block length after puncturing

**Output :**

- $UserPuncturedBlock$: user punctured code block

```
// Remove the 12 tail bits
UserCodedBlock-No-Tail ← UserCodedBlock
// Extract systematic and constituent encoder parts
Systematic-part ← UserCodedBlock-No-Tail
1st-encoder-part ← UserCodedBlock-No-Tail
2nd-encoder-part ← UserCodedBlock-No-Tail
// Compute the number of periods that fit in the frame size
Nperiods = ⌊FrameLength / RowLength(P)⌋
// Initialize the punctured block
UserPuncturedBlock ← initialization(BlockLength)
// Bit assignment:  If P(j) = 1 → the bit is not punctured
for i ← 1 to Nperiods do
    for j ← 1 to RowLength(P) do
        if systematic(P(j)) == 1 (not punctured) then
            UserPuncturedBlock ← add systematic bit
        end if
        if 1stEncoder(P(j)) == 1 (not punctured) then
            UserPuncturedBlock ← add 1st encoder bit
        end if
        if 2ndEncoder(P(j)) == 1 (not punctured) then
            UserPuncturedBlock ← add 2nd encoder bit
        end if
    end for
end for
UserPuncturedBlock ← add the remaining bits and tail bits
return UserPuncturedBlock
```

**Algorithm 2:** Reverse puncturing (performed at RX) (mentioned on p. 30)

**Input :**

- Y-demod: demodulated signal
- P: puncturing pattern matrix
- FrameLength: information frame size

**Output :**

- $Y\text{-}filled$: signal with zero-symbols inserted in puncturing positions

```
// Initialize the systematic, 1st encoder and 2nd encoder parts
// Notice that they are initialized with all zero symbols as if they were all punctured
SystematicPart ← zero-initialization(FrameLength)
1stEncoderPart ← zero-initialization(FrameLength)
2ndEncoderPart ← zero-initialization(FrameLength)
// Compute the number of periods that fit in the frame size
Nperiods = ⌊FrameLength / RowLength(P)⌋
// Replace the zero symbols with demodulated symbols in the unpunctured positions
for i ← 1 to Nperiods do
    for j ← 1 to RowLength(P) do
        if systematic(P(j)) == 1 (not punctured) then
            // Replace the zero symbol in the systematic part
            SystematicPart ← addsymbol(Y-demod)
        end if
        if 1stEncoder(P(j)) == 1 (not punctured) then
            // Replace the zero symbol in the 1st encoder part
            1stEncoderPart ← addsymbol(Y-demod)
        end if
        if 2ndEncoder(P(j)) == 1 (not punctured) then
            // Replace the zero symbol in the 2nd encoder part
            2ndEncoderPart ← addsymbol(Y-demod)
        end if
    end for
end for
// Parallel to serial conversion
Y-filled ← PTS(SystematicPart,1stEncoderPart,2ndEncoderPart)
Y-filled ← add the remaining symbols and tail symbols
return Y-filled
```

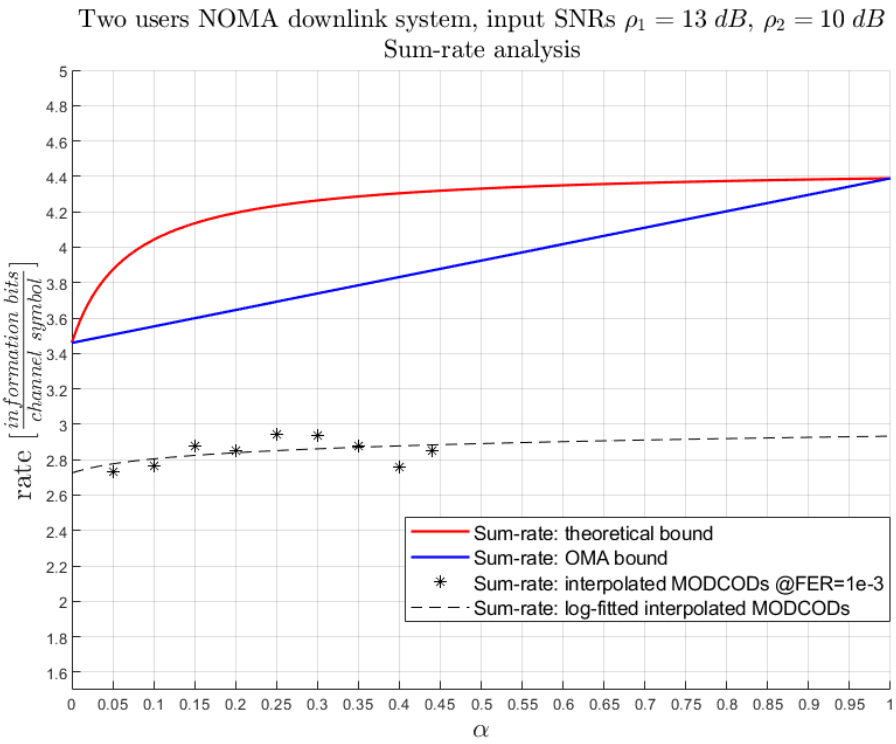



**Figure 3.11:** SNRs (13,10) $dB$ - Sum rate analysis (mentioned on p. 26)

### 3.5.3 FrameLength setting algorithm

As previously explained in Section 3.4, the frame size of User-1 is fixed at approximately 600 bits, whereas the frame size of User-2 will vary according to the ratio between the modulation cardinality of the two users (and their puncturing matrix rates).

We define:

- Nsymbols-U1 ≡ "total number of transmitted symbols per block for User-1"
- Nsymbols-U2 ≡ "total number of transmitted symbols per block for User-2"

Since the simulation is taken block by block, the frame size of the two users must respect the following constraint:

- Nsymbols-U1 = Nsymbols-U2
  → BlockLength-U1 / $m_1$ = BlockLength-U2 / $m_2$

Algorithm 3 is built in order to satisfy this constraint. In words: we start from $f_{size-U1} = 600$, we check if there exists a $f_{size-U2}$ that satisfies the constraint, if not we increase $f_{size-U1}$ and we repeat the procedure until the constraint is satisfied.

**Algorithm 3:** Compute users' frame size (mentioned on p. 33)

**Input :**

- $m_1$: modulation efficiency of User-1
- $m_2$: modulation efficiency of User-2
- $P_{U1}$: puncturing pattern matrix of User-1
- $P_{U2}$: puncturing pattern matrix of User-2

**Output :**

- $f_{size-U1}$
- $f_{size-U2}$

```
// Initialize the frame size of User-1 to 599
f_size-U1 ← 599
while 1 do
    f_size-U1 ← f_size-U1 + 1
    // Compute the block length (after puncturing) as a function of
       the frame size and the puncturing pattern matrix
    BlockLength-U1 ← ComputeLength(f_size-U1,P_U1)
    // Compute the block length of User-2 such that Nsymbols-U1 =
       Nsymbols-U2 is satisfied
    BlockLength-U2 ← (m2/m1)·BlockLength-U1
    // Check if implicit constraints are satisfied
    if BlockLength-U1/m1 AND BlockLength-U2 are integer then
        // Find a f_size-U2 value that fits P_U2 and BlockLength-U2
        f_size-U2 ← FindSize(BlockLength-U2,P_U2)
        // Check if the found value is a valid integer number
        if f_size-U2 is integer then
            break while (algorithm end)
        end if
    end if
end while
return f_size-U1, f_size-U2
```

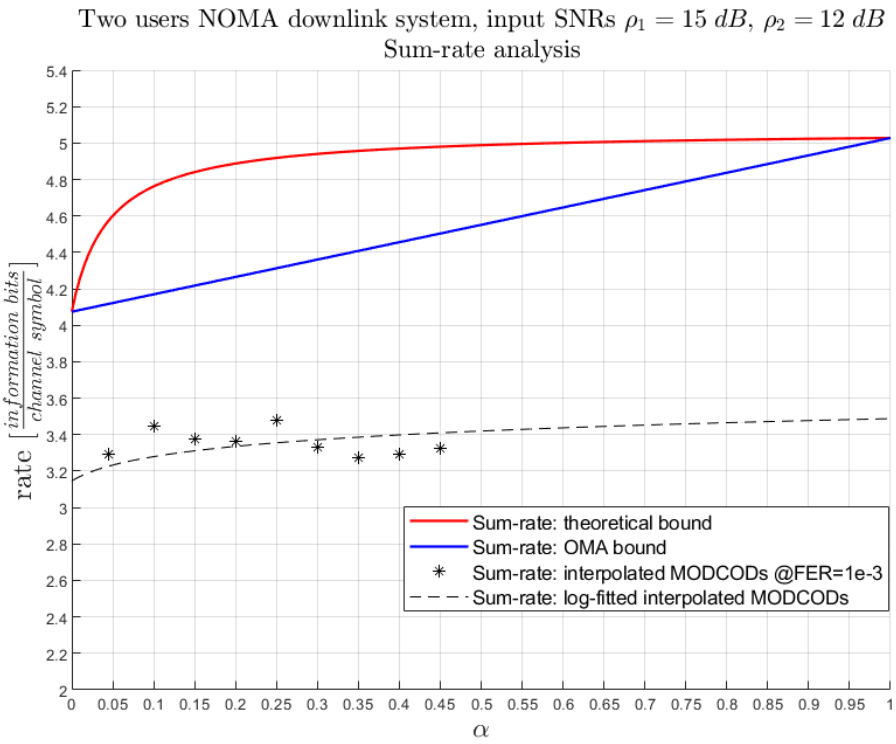



**Figure 3.12:** SNRs (15,12) $dB$ - Sum rate analysis (mentioned on p. 26)

### 3.5.4 Successive interference cancellation (SIC)

Concerning the SIC implementation, we have assumed a complete channel state information at both transmitter and receiver sides; therefore the receiver knows the following parameters:

- Total transmitted power: $P$
- Power allocation factor: $\alpha$
- Users' channel gains: $h_1$,$h_2$
- Additive white Gaussian Noise Variance: $N$

Both User-1 and User-2 demodulate the signals as log-likelihood-ratio (LLR) output type (in order to perform soft decoding later). To achieve a LLR output type, the Noise Variance information is needed by the receiver. In case of User-2, when he decodes its own signal from the superimposed signal, we have already seen in Section 3.2 that the Noise Variance is given by:

$$N_{U2} = |h_2|^2 \alpha P + N \tag{3.20}$$

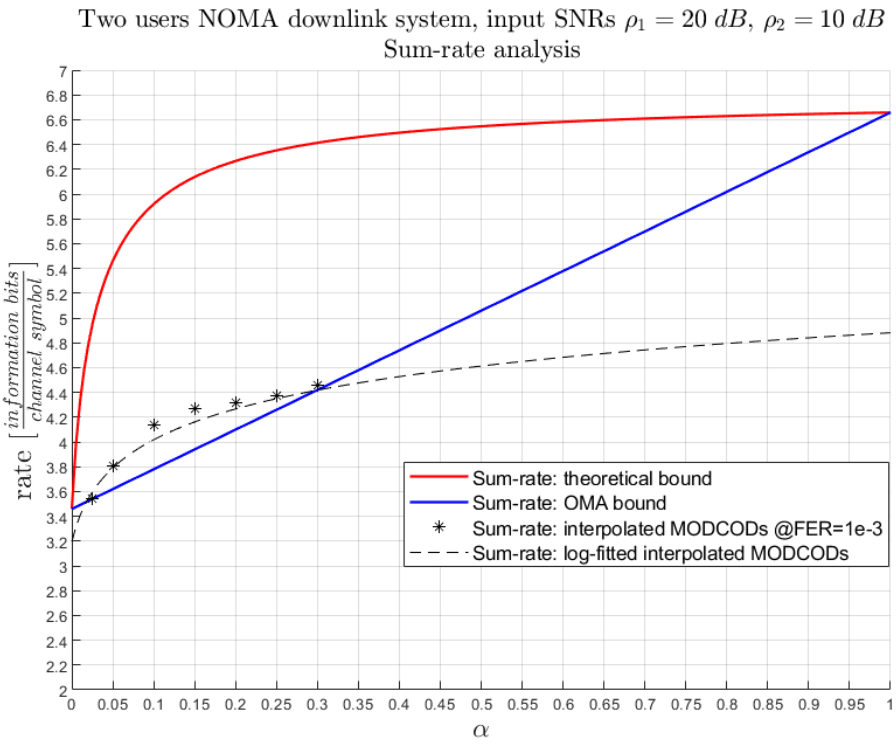



**Figure 3.13:** SNRs (20,10) $dB$ - Sum rate analysis (mentioned on p. 26)

Instead from the User-1 perspective (the user who performs SIC), when he decodes the User-2 signal, the Noise Variance is:

$$N_{U2|U1} = |h_1|^2 \alpha P + N \tag{3.21}$$

(Where $N_{Ui|Uj}$ is the Noise Variance observed by User-j when he decodes the User-i signal).

Once the User-2 signal has been decoded from User-1 receiver as $\hat{X}_2$, User-1 subtract it from the superimposed signal:

$$\tilde{Y_1} = h_1 X_1 + Z_1 - h_1(X_2 - \hat{X}_2) \tag{3.22}$$

Therefore, when User-1 decodes its own signal, the Noise Variance is given by:

$$N_{U1} = E\left[|Z_1 - h_1(X_2 - \hat{X}_2)|^2\right] \tag{3.23}$$

Unfortunately Equation (3.23) is difficult to solve; hence User-1, in order to compute it, performs the following approximation:

$$\hat{X}_2 = X_2$$

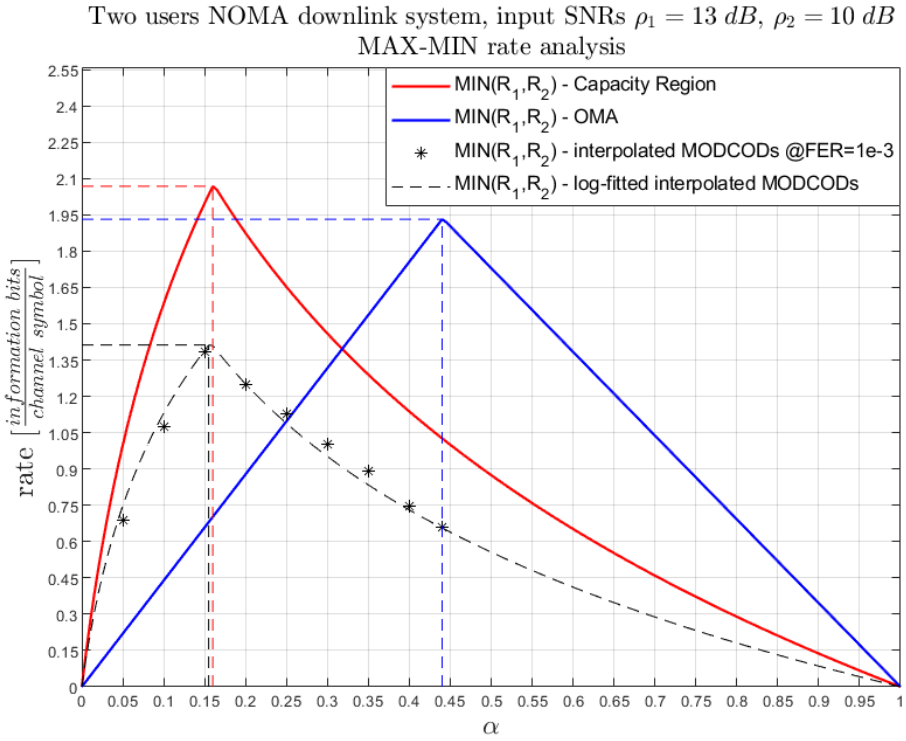



**Figure 3.14:** SNRs (13,10) *dB* - MAX-MIN rate analysis (mentioned on p. 27)

This way Equation (3.23) becomes:

$$N_{U1} = E\left[|Z_1|^2\right] = N \tag{3.24}$$

The previous assumption simplifies the model but makes the Noise Variance estimation worse, so the decoding performances (in terms of frame error rate) get slightly worse as well.

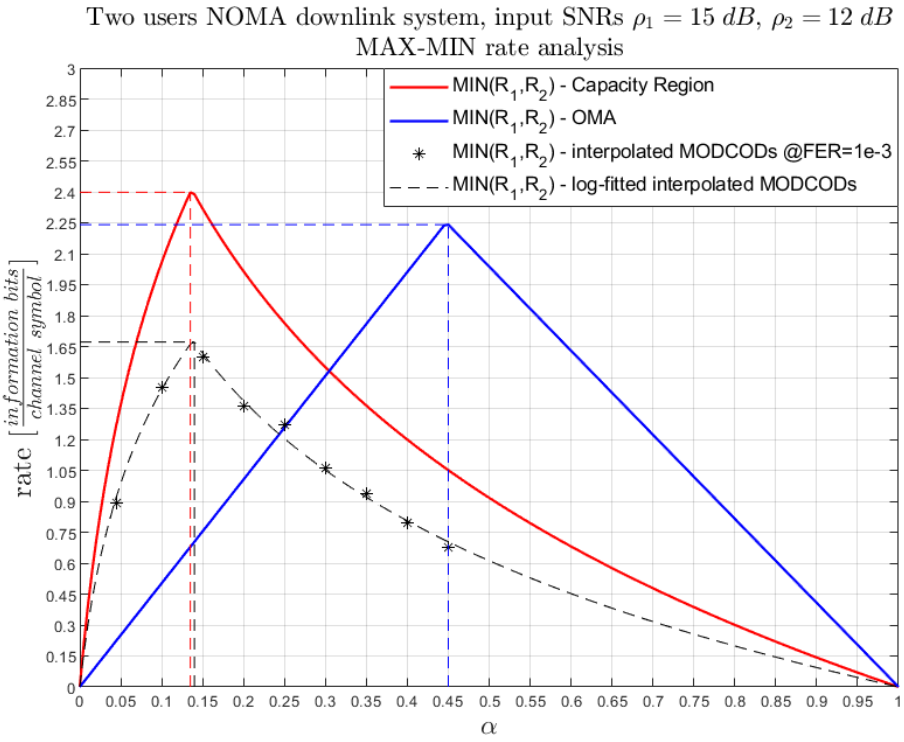



**Figure 3.15:** SNRs (15,12) *dB* - MAX-MIN rate analysis (mentioned on p. 27)

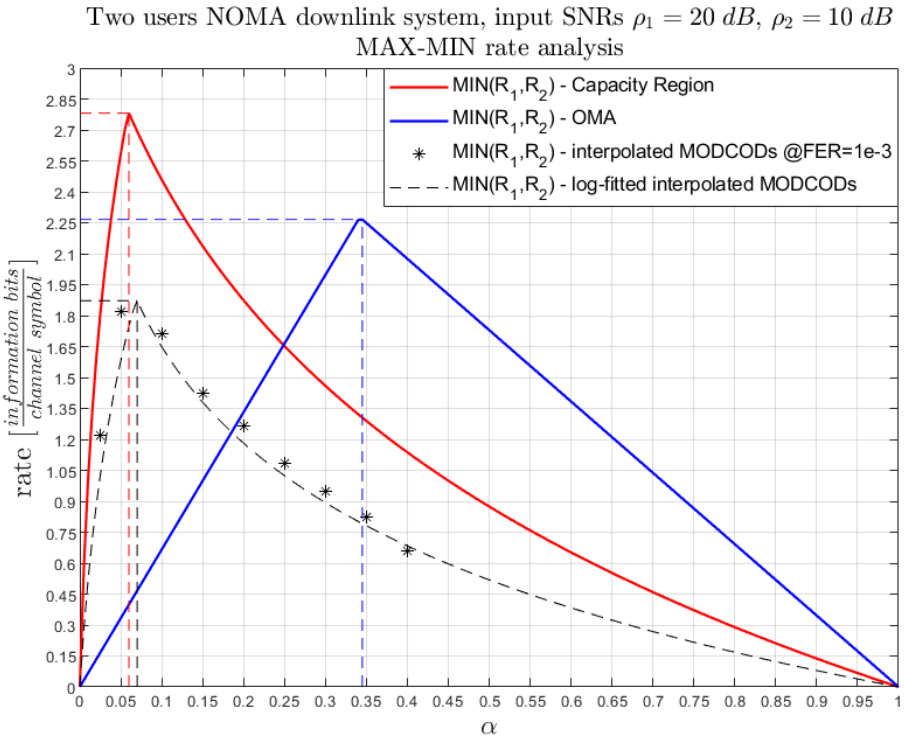



**Figure 3.16:** SNRs (20,10) $dB$ - MAX-MIN rate analysis (mentioned on p. 27)

# Chapter 4

# Epilogue

## 4.1 Conclusions

Through this work, it has been shown how closely M-QAM and turbo code-based MODCODs can approach the theoretical transmission rate limits in a NOMA system. Different analyses have been involved, starting with a comparison to the capacity region of a Gaussian broadcast channel, followed by an evaluation of sum-rate performance and MAX-MIN operating points, and comparing them with OMA performance limits. The capacity region can theoretically be approached using an infinite-length code; consequently, we examined and quantified the impact of employing finite-length codes on performance while maintaining a fixed target frame error rate.

## 4.2 Future Works

In the remaining part of the chapter, we present some potential future research directions for this thesis. Our main goal is to repeat the entire analysis within a fading channel and improve the simulation accuracy.

- In Section 4.2.1, we discuss a possible future study focusing on the analysis of a NOMA system under fading conditions.

- In Section 4.2.2, we outline various improvements that can be implemented in the current work, with a specific emphasis on enhancing the reliability of simulation results.

### 4.2.1 Fading channel approximation

So far, we have approximated the channel gain to be static. Now, let's consider the channel gain affected by a time-varying gain.

#### Fast Fading

In a fast-fading channel, each transmitted codeword is affected by multiple channel coefficients [13], drawn according to a given probability distribution. If the code is sufficiently long, we can assume that all the possible channel coefficients affect the entire transmitted codeword. Under this condition, in principle, we can reliably transmit information at a rate equal to or less than the ergodic capacity. The following definitions regarding the ergodic capacity and the ergodic capacity region have been taken from the book "Wireless Communications" by A. Goldsmith [14]. The ergodic capacity, assuming known channel state information (CSI) at the receiver, and in the absence of power adaptation, is given by the following formula:

$$C_{ergodic} = E_{f(\gamma)}[\log_2(1+\gamma)] = \int_0^\infty d\gamma \log_2(1+\gamma) f(\gamma) \tag{4.1}$$

Where $\gamma$ is the instantaneous SNR, and $f(\gamma)$ is its corresponding distribution defined by the fading model.

Starting from Equation (3.12), the ergodic capacity region of our NOMA downlink system becomes:

$$\begin{cases} R_1 \leq E_{f(|h_1|)}[\log_2(1+\frac{|h_1|^2\alpha P}{N})] \\ R_2 \leq E_{f(|h_2|)}[\log_2(1+\frac{|h_2|^2(1-\alpha)P}{|h_2|^2\alpha P+N})] \end{cases} \tag{4.2}$$

As an example, we can consider a very typical fading model, commonly used to model multipath fading phenomena, which is Rayleigh Fading [15]. In this model, we have:

$$\begin{cases} h_i \sim \mathcal{CN}(0, \sigma_i^2) \\ i \in \{1,2\} \end{cases} \tag{4.3}$$

As a consequence, the channel gains' magnitude is Rayleigh distributed:

$$\begin{cases} f(|h_i|) = \frac{|h_i|}{\sigma_i^2} \exp\left\{-\frac{|h_i|^2}{2\sigma_i^2}\right\} \\ i \in \{1,2\} \end{cases} \tag{4.4}$$

Equation (4.2) becomes:

$$\begin{cases} R_1 \leq \int_0^\infty d|h_1| \log_2(1+\frac{|h_1|^2\alpha P}{N}) \frac{|h_1|}{\sigma_1^2} \exp\left\{-\frac{|h_1|^2}{2\sigma_1^2}\right\} \\ \\ R_2 \leq \int_0^\infty d|h_2| \log_2(1+\frac{|h_2|^2(1-\alpha)P}{|h_2|^2\alpha P+N}) \frac{|h_2|}{\sigma_2^2} \exp\left\{-\frac{|h_2|^2}{2\sigma_2^2}\right\} \end{cases} \tag{4.5}$$

We introduce the input average-SNR parameters:

$$\begin{cases} E[\rho_1] \triangleq E[|h_1|^2]\frac{P}{N} \\ \\ E[\rho_2] \triangleq E[|h_2|^2]\frac{P}{N} \end{cases} \tag{4.6}$$

From the Rayleigh distribution, we know:

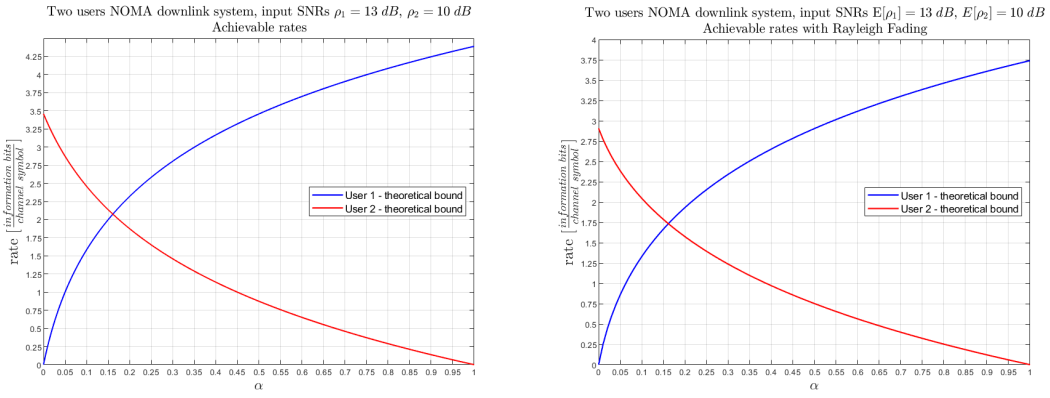
$$\begin{cases} E[|h_i|^2] = 2\sigma_i^2 \\ i \in \{1,2\} \end{cases} \tag{4.7}$$

So we can derive the $\sigma_i$ parameters:

$$\begin{cases} \sigma_i = \sqrt{\frac{1}{2}E[|h_i|^2]} \\ i \in \{1,2\} \end{cases} \tag{4.8}$$

By looking at Figure 4.1, we can observe that the capacity region, fixed the same SNRs, decreases due to the fading effect. This result is expected from the Jensen inequality:

$$E[\log_2(1+\gamma)] \leq \log_2(1+E[\gamma]) \tag{4.9}$$




**(a)** SNRs (13,10) - Static

**(b)** SNRs (13,10) - Rayleigh Fading

**Figure 4.1:** Capacity region: Static Vs. Rayleigh fading (mentioned on p. 43)

In order to simulate a NOMA system under fast fading conditions using our simulation setup, we have to assume that the receiver knows all the channel gains of each transmitted symbol of each block, so that the phase can be synchronized. This, of course, is not feasible, hence one of our objectives is to implement a system from scratch where the ergodic capacity region can be used as a performance comparison metric.

### Block Fading

The block-fading approximation requires that the channel gain evolves according to a specific probability distribution for each transmitted code block, and remains constant throughout the transmission of the entire block. Additionally, the channel gains of different blocks are statistically independent of each other. An example of block-fading gain is given by the Shadowing gain. Shadowing refers to slowly time-varying phenomena [16] caused by the presence of obstacles in the channel, such as building walls, car bodies [17], trees, etc. In this model, the channel gain evolves following a log-normal distribution, which is well suited to describe the effects of shadowing. If $X$ is log-normally distributed with parameters $\mu$ and $\sigma$; i.e. $X \sim \mathcal{LN}(\mu, \sigma)$, its pdf is given by:

$$f(x) = \frac{1}{x\sqrt{2\pi}\sigma} \exp\left\{-\frac{(\ln x - \mu)^2}{2\sigma^2}\right\} \tag{4.10}$$

Where $\sigma$ values ranging from 5 to 12 $dB$ are commonly considered [18].

Differing from the fast-fading approximation, the block-fading approximation holds particular significance as it can provide a reliable representation of a real communication scenario where the channel evolves slowly enough to enable the receiver to estimate its coefficients. Developing an analysis that incorporates the block-fading approximation requires a comparison of performance with outage capacity and outage probability.

## 4.2.2 Other Improvements

As discussed in Section 3.4, there are reliability concerns regarding the precision of the results obtained. To address this issue, we would like to:

- Implement an algorithm for identifying optimal (or sub-optimal) puncturing patterns based on the input parameters. By doing so, we aim to achieve a higher information rate and eliminate the "random goodness" variable of the selected puncturing pattern; this way performances of various simulations with different parameters become more consistent with each other.
- Improve the interpolation functions.
- Improve the resolution of the rates associated with the MODCODs to be tested. This step will reduce the variation of the FER around the target FER, leading to a better interpolation accuracy.
- We would like to rerun the simulations on more powerful hardware. This would allow us to increase the length of the transmitted blocks and bring the performance of the MODCODs even closer to the theoretical capacity region.

# Appendices

# Appendix A

# Review of single-user Information theory

## A.1 Introduction

In this chapter we will review the elements of information theory concerning the transmission of information by a single sender to a single receiver, in particular:

- In Section A.2 we define and describe the properties of the information entropy, joint entropy and relative entropy.
- In Section A.3 we define and describe the notion of mutual information.
- In Section A.4 we introduce the AEP and the other definitions that are needed to prove the channel coding theorem.
- In Section A.5 we present the notion of Communication Channel, Channel Capacity, the Channel Coding Theorem and its proof using jointly typical decoding.
- In Section A.6 we extend the notion of entropy and mutual information to continuous random variables.
- In Section A.7 we introduce the AWGN channel, we derive its capacity and we introduce the maximum likelihood decoding.

The information theory results affect different areas, such as:

- Communication systems.
- Storage systems.

- Physics (statistical mechanics).
- Computer science (Kolmogorov Complexity).
- Mathematics.
- Philosphy of Science (Novacula Occami).
- Economics.

For the purpose of this essay, we will focus on communication system aspects only. Most of the contents related to this Appendix and Appendix B derives from Shannon results [19] and follows the order and notations presented in the book of Joy A. Thomas and Thomas M. Cover [20].

## A.2 Entropy

The information theory revolves around the Entropy, a quantity that describes the average uncertainty of a random variable, or, from another point of view, the expected information that we gain by observing an outcome of that variable.

Given a discrete r.v. $X$ with alphabet $\Omega_X$ and probability mass function:

$$p(x) = P(X = x), \;\; x \in \Omega_X, \;\; M = |\Omega_X|$$

Its entropy is defined as:

**Definition A.2.1** (Entropy)**.**

$$H(X) \triangleq -\sum_{x \in \Omega_X} p(x) \log_2 p(x) \qquad [bits]$$

Some of the entropy key properties are listed below:

- $H(X) \geq 0$
- $H(X) = H(p)$ (Label invariance)
- $H(X) = 0$ if $\exists!\; x \in \Omega_X : p(x) = 1$
- $H(X)$ is a concave function in $p$
- $\max H(X) = \log_2 M$, achieved if $p(x) = 1/M$, $\forall x \in \Omega_X$

All the above properties can be checked by observing Figure A.1 and Figure A.2, where the possible entropy values of a cardinality $M = 3$ random variable are displayed.

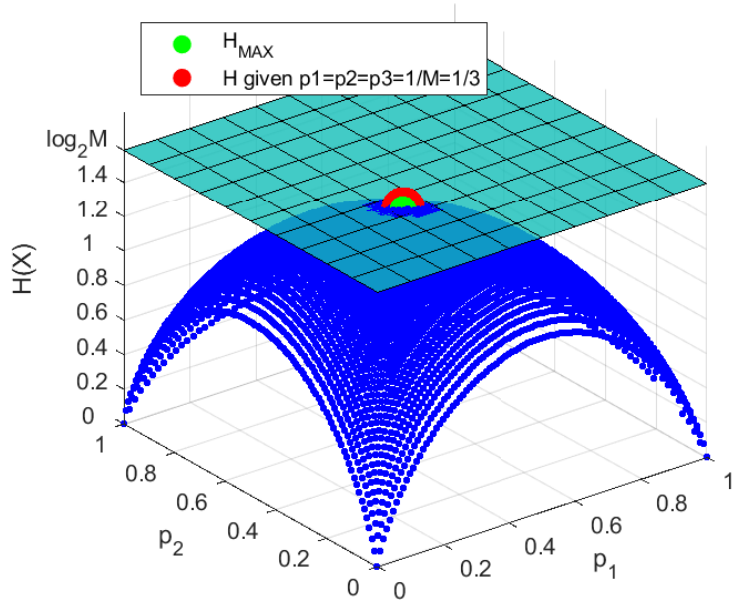



**Figure A.1:** Entropy, (3D) plot of a cardinality-three r.v. (mentioned on p. 48)

**Theorem A.2.1** (Averaging a subset of the probability vector always increases the entropy)**.** *Given the vector:*

$$p(X) = (p_1, ..., p_J, p_{J+1}, ..., p_M)$$

*We average a subset* $\Lambda \subseteq \Omega_X$ *with cardinality* $J = |\Lambda| < M$*. Suppose, for simplicity, that the averaged elements are the first* $J$ *of the probability vector* $p(X)$*:*

$$p \triangleq \frac{1}{J} \sum_{i=1}^{J} p_i$$

*This does not lead to a loss of generality, since the entropy is invariant to permutations in the probability vector. The resulting (partially) averaged probability vector is:*

$$p_{J-AVE}(X) = (p, ..., p, p_{J+1}, ..., p_M)$$

*Then the following in always true:*

$$H(p_{J-AVE}) \geq H(p), \quad \forall J \in \{2, ..., M\}$$

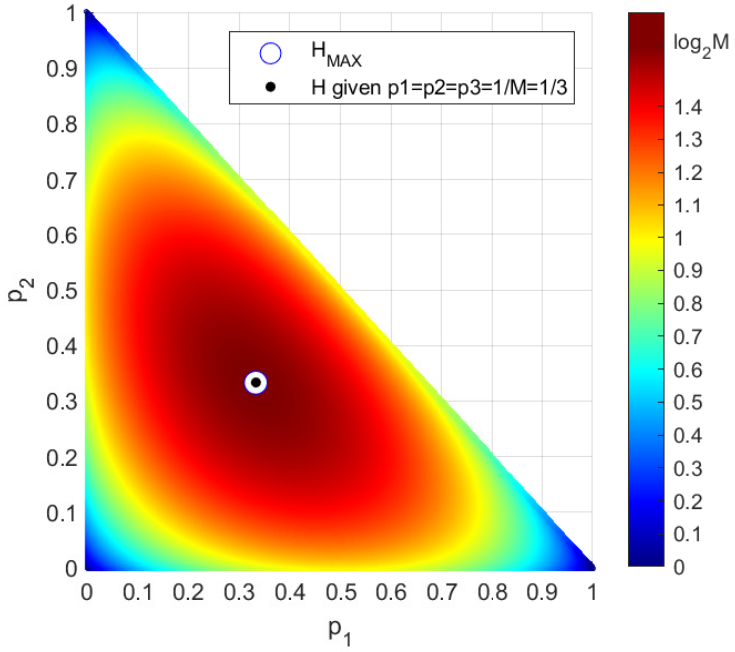



**Figure A.2:** Entropy, (color) plot of a cardinality-three r.v. (mentioned on p. 48)

In Figure A.3 is displayed an example where the entropy of a distribution

$$p(X) = (p_1, p_2, p_3)$$

is compared with the one of a partially averaged distribution, where the first two entries $p_1$ and $p_2$ are averaged. As can be seen, the achieved entropy is quite larger in respect to the original distribution. Intuitively, the average operation makes the overall probability mass to be distributed more uniformly among the possible outcomes in respect to the previous configuration; this leads to an increase of the outcome uncertainty and therefore the entropy increases as well.

The definition of entropy can be extended to a pair of random variables. Given two discrete random variables $X$ and $Y$, with, respectively, alphabets $\Omega_X$ and $\Omega_Y$, their joint entropy is defined as:

**Definition A.2.2** (Joint entropy)**.**

$$H(X,Y) \triangleq -\sum_{(x,y)\in\ \Omega_X\times\Omega_Y} p(x,y)\log_2 p(x,y) \qquad [bits]$$

The conditional entropy of the random variable $X$ given $Y$, instead, is defined as:

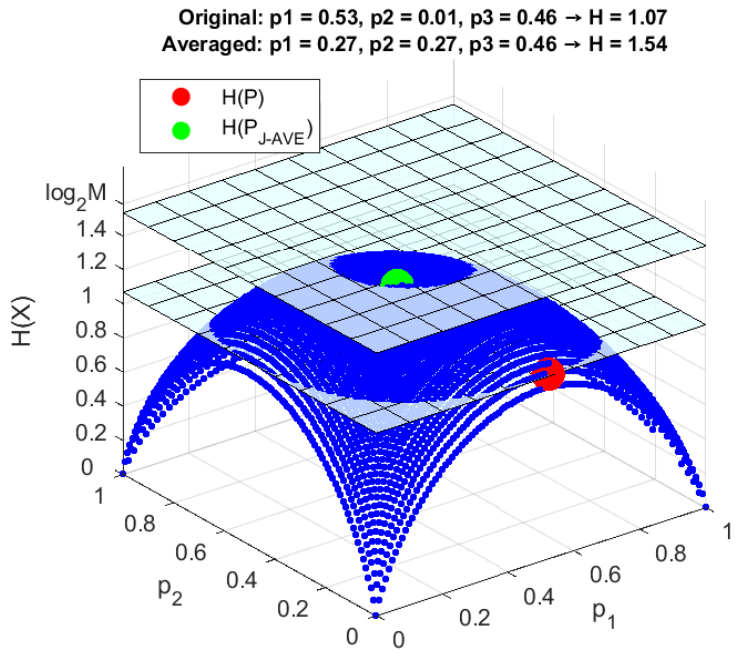



**Figure A.3:** Entropy, original vs. (partially) averaged distribution (mentioned on p. 50)

**Definition A.2.3** (Conditional entropy)**.**

$$H\left(X|\ Y\right) \triangleq \sum_{y\in\ \Omega_{\mathrm{Y}}} p\left(y\right) H\left(X|\ Y=y\right) \qquad [bits]$$

Definition A.2.3 describes the residual uncertainty of the random variable $X$ after $Y$ has been revealed. We can rewrite it as:

$$H(X|Y) = -\sum_{y\in\ \Omega_{\mathrm{Y}}} p\left(y\right) \sum_{x\in\ \Omega_{\mathrm{x}}} p\left(x|\ y\right) \log_2 p\left(x|\ y\right)$$

$$= -\sum_{(x,y)\in\ \Omega_{\mathrm{X}}\times\Omega_{\mathrm{Y}}} p\left(x,y\right) \log_2 p\left(x|\ y\right)$$

The following results are derived:

- $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$ (Chain Rule)
- $H(X,Y) \leq H(X) + H(Y)$, equality holds iff $X$ and $Y$ are independent.
- $H(X|Y) \leq H(X)$, equality holds iff $X$ and $Y$ are independent.

The chain rule for the entropy can be generalized for $n$ random variables as follows:

**Theorem A.2.2** (Chain rule for entropy)**.** *Given* $(X_1, ..., X_n) \sim p(x_1, ..., x_n)$*; then:*

$$H(X_1, ..., X_n) = H(X_1) + H(X_2|X_1) + ... + H(X_n|X_{n-1}, ..., X_1)$$

### A.2.1 Relative entropy

Given two probability mass functions $p(x)$ and $q(x)$, their relative entropy (or Kullback-Leibler divergence) is defined as:

**Definition A.2.4** (Relative entropy)**.**

$$D(p||q) \triangleq \sum_{x \in |\Omega_X|} p(x) \log_2 \frac{p(x)}{q(x)}$$

The relative entropy satisfies:

- $D(p||q) \geq 0$, with equality iff $q(x) = p(x)$
- $D(p||q) \neq D(q||p)$, unless $q(x) = p(x)$

The relative entropy can be considered as a sort of distance between the two distributions; it represents the amount of information that we loose by modelling $p(x)$ with $q(x)$.

An example is shown in Figure A.4, where a distribution $p(x)$ is modeled with two different binomial distributions, having different parameter p. The distribution in the figure on the right is clearly closer to the original, as a result it has a lower relative entropy (the corresponding values are displayed in the figure titles).

## A.3 Mutual information

Given two discrete random variables $X$ and $Y$, with, respectively, alphabets $\Omega_X$ and $\Omega_Y$, the mutual information $I(X;Y)$ is the Kullback-Leibler divergence between the joint distribution and the product of the marginal ones:

**Definition A.3.1** (Mutual information)**.**

$$I(X;Y) \triangleq D(p(x,y)||p(x)p(y)) = \sum_{(x,y) \in \ \Omega_X \times \Omega_Y} p(x,y) \log_2 \frac{p(x,y)}{p(x)\,p(y)}$$

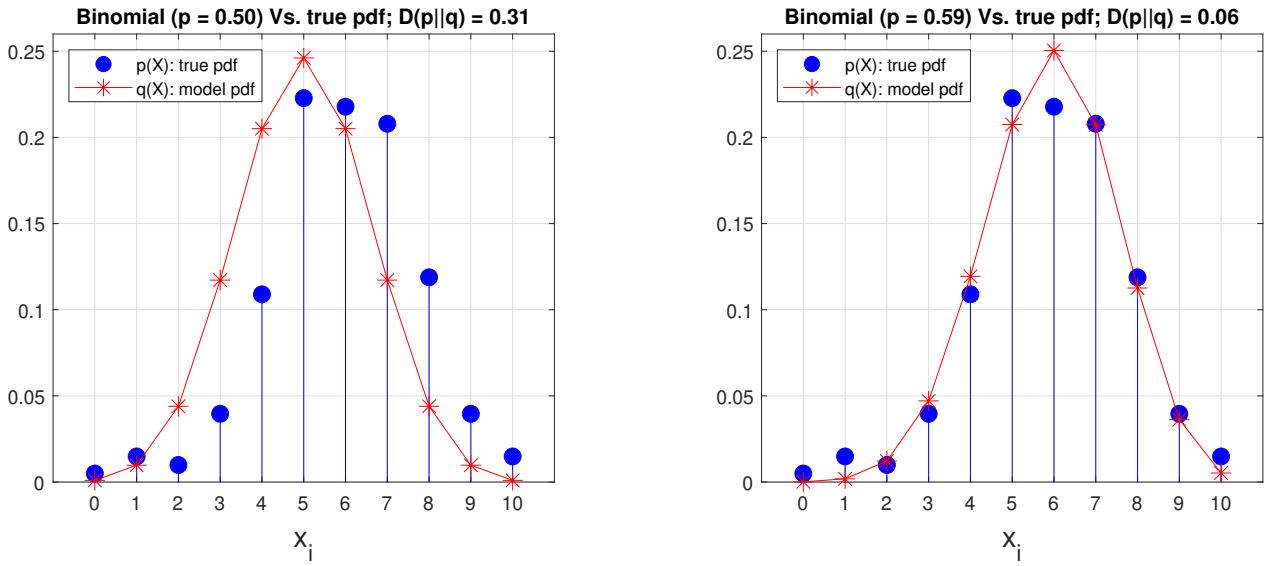



**Figure A.4:** Relative entropy, comparison between two different model distribution (mentioned on p. 52)

Starting from Definition A.3.1, we can easily show that:

$$I(X;Y) = H(X) - H(X|Y)$$

Therefore, the mutual information can be interpreted as the information that we gain on $X$ once $Y$ is revealed; or, from another perspective, the amount of uncertainty of $X$ that is removed once $Y$ is observed. From the results presented in Section A.2, we can derive the following properties:

- $I(X;Y) \geq 0$
- $I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y;X)$
- $I(X;Y) = H(X) + H(Y) - H(X,Y)$

The above results are summarized in the Venn diagram displayed in Figure A.5.

The mutual information satisfies the following chain rule.

**Theorem A.3.1** (Chain rule for mutual information)**.** *Given* $(X_1, ..., X_n, Y) \sim p(x_1, ..., x_n, y)$*; then:*

$$I(X_1, ..., X_n; Y) = I(X_1; Y) + I(X_2; Y|X_1) + ... + I(X_n; Y|X_{n-1}, ..., X_1)$$

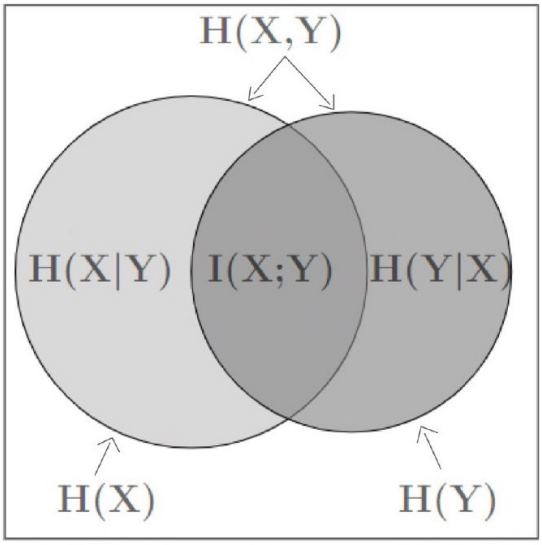



**Figure A.5:** Mutual information, Venn diagram (mentioned on p. 53)

*Equivalently:*

$$I(Y; X_1, ..., X_n) = I(Y; X_1) + I(Y; X_2|X_1) + ... + I(Y; X_n|X_{n-1}, ..., X_1)$$

*Where the conditional mutual information of $X$ and $Y$ given $Z$ is defined as:*

**Definition A.3.2** (Conditional mutual information)**.**

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

## A.4 Law of large numbers in information theory

### A.4.1 Asymptotic equipartition property (AEP)

We first recall the law of the large numbers.

**Theorem A.4.1** (Weak law of the large numbers)**.** *Given a sequence of random variables: $X_1, X_2, ..., X_n$; such that each $X_i$ is i.i.d. with mean $\mu = E_{p(x)}[X_i]$; the weak law of large numbers states that, for any $\varepsilon > 0$:*

$$\lim_{n\to\infty} P\left(\left|\frac{1}{n}\sum_{i=1}^{n} X_i \ - \mu\right| < \varepsilon\right) = 1$$

We can derive an analogous law for the entropy. The entropy described in Definition A.2.1 can be re-written as:

$$H(X) = \sum_{x \in \Omega_X} p(x) \log_2 \frac{1}{p(x)} = E_{p(x)} \left[ \log_2 \frac{1}{p(x)} \right] \tag{A.1}$$

Considering an i.i.d. sequence $X_1, X_2, ..., X_n$; the corresponding sequence:

$$\log_2 \frac{1}{p(X_1)},\ \log_2 \frac{1}{p(X_2)},\ \ldots\ ,\ \log_2 \frac{1}{p(X_N)}$$

is also i.i.d.

Notice here that here $p(X_i)$ are i.i.d. random variables with alphabets: $\Omega_{p(X)} = \{p(X = x_1), ..., p(X = x_{|\Omega_X|})\}$.

By applying A.4.1, we get:

$$\lim_{n \to \infty} P \left( \left| \frac{1}{n} \sum_{i=1}^{n} \log_2 \frac{1}{p(X_i)} - H(X) \right| < \varepsilon \right) = 1$$

From the properties of logarithms and exploiting independence of $X_1, ..., X_n$ we can write:

$$\lim_{n \to \infty} P \left( \left| \frac{1}{n} \log_2 \frac{1}{p(X_1, X_2, ..., X_n)} - H(X) \right| < \varepsilon \right) = 1 \tag{A.2}$$

Equation (A.2) describes the asymptotic equipartition property (AEP), whose consequences are very surprising.

### A.4.2 Typical sequences

From AEP we can state that, for $n$ sufficiently large:

$$p(X_1, X_2, ..., X_n) \simeq 2^{-nH(X)}$$

In this respect, we define the typical set ${A_\varepsilon}^{(n)}$ as the set containing all the length-$n$ (typical) sequences whose probability is close to $2^{-nH(X)}$; more precisely:

**Definition A.4.1** (Typical set)**.**

$$\begin{aligned} A_\varepsilon^{(n)} &\triangleq \left\{ x^n = (x_1, ..., x_n) \in \Omega_X^n : 2^{-n(H(X)+\varepsilon)} \leq p(x^n) \leq 2^{-n(H(X)-\varepsilon)} \right\} \\ &= \left\{ x^n \in \Omega_X^n : H(X) - \varepsilon \leq -\frac{1}{n} \log_2 p(x^n) \leq H(X) + \varepsilon \right\} \end{aligned}$$

The following properties are satisfied; $\forall \varepsilon > 0$:

- $\exists n^*$ : if $n > n^*$, then $P(A_\varepsilon^{(n)}) > 1 - \varepsilon$
- $\left|A_\varepsilon^{(n)}\right| \leq 2^{n(H(X)+\varepsilon)}$
- $\exists n^*$ : if $n > n^*$, then $\left|A_\varepsilon^{(n)}\right| \geq (1-\varepsilon)2^{n(H(X)-\varepsilon)}$

As an example, let's consider the following cardinality four discrete r.v. $X$ with alphabet $\Omega_X = \{x_1, x_2, x_3, x_4\}$ and distribution $p_i = P(X = x_i)$, where:

- $p_1 = 0.2,\ \ p_2 = 0.3,\ \ p_3 = 0.1,\ \ p_4 = 0.4$
- $n = 10^4$ (sequence length)
- $n_{sim} = 20$ (number of simulations)

At each simulation we generate a length-$n$ sequence $x_1, ..., x_n$ where $x_i$ is a realization of $X$. We compute the corresponding estimated entropy: $H_{est} = \frac{1}{n}\sum_{i=1}^{n} \log_2 \frac{1}{p_i}$ and we compare it with the true entropy:
$H = -\sum_{i=1}^{4} p_i \log_2 p_i$. Figure A.6 shows that at each simulation the estimated entropy is very close to the true one, for example, if we set $\varepsilon = 0.02$, by looking the Figure we can check that all the $n_{sim} = 20$ sequences belong to $A_\varepsilon^{(n)}$.

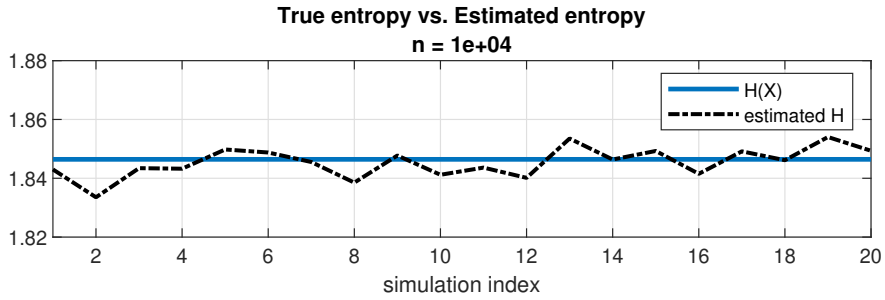



**Figure A.6:** True entropy vs. estimated entropy (mentioned on p. 56)

### A.4.3 Jointly typical sequences

Two sequences $X^n$ and $Y^n$ with joint distribution $p(x^n, y^n) = \prod_{i=1}^{n} p(x_i, y_i)$ are jointly typical if they are typical sequences and their empirical joint entropy is close to the true joint entropy. More precisely:

**Definition A.4.2** (Jointly typical set)**.**

$$\begin{aligned} A_\varepsilon^{(n)} \triangleq \{&(x^n, y^n) \in (\Omega_X^n, \Omega_Y^n) : \\ &| -1/n \log_2 p(x^n) - H(X)| < \varepsilon, \\ &| -1/n \log_2 p(y^n) - H(Y)| < \varepsilon, \\ &| -1/n \log_2 p(x^n, y^n) - H(X,Y)| < \varepsilon\} \end{aligned}$$

The following properties are satisfied; $\forall \varepsilon > 0$:

- $\exists n^* :$ if $n > n^*$, then $P((X^n, Y^n) \in A_\varepsilon^{(n)}) > 1 - \varepsilon$
- $\left|A_\varepsilon^{(n)}\right| \leq 2^{n(H(X,Y)+\varepsilon)}$
- $\exists n^* :$ if $n > n^*$, then $\left|A_\varepsilon^{(n)}\right| \geq (1-\varepsilon)2^{n(H(X,Y)-\varepsilon)}$

If we consider the pair of independent sequences $(\tilde{X}^n, \tilde{X}^n) \sim p(x^n)p(y^n)$, these properties hold:

- $P((\tilde{X}^n, \tilde{X}^n) \in A_\varepsilon^{(n)}) \leq 2^{-n(I(X;Y)-3\varepsilon)}$.
- $\exists n^* :$ if $n > n^*$, then $P((\tilde{X}^n, \tilde{X}^n) \in A_\varepsilon^{(n)}) \geq (1-\varepsilon)2^{-n(I(X;Y)+3\varepsilon)}$

# A.5 Channel coding theorem

## A.5.1 Communication channel

**Definition A.5.1.** A discrete channel $(\Omega_X, p(y|x), \Omega_Y)$ is a system with input alphabet $\Omega_X$ and output alphabet $\Omega_Y$, characterized by a probability transition matrix whose the generic element $p(y|x)$ represents the probability of observing $y \in \Omega_Y$ having transmitted the symbol $x \in \Omega_X$; $p(y|x)$ satisfies:

- $p(y|x) \geq 0, \ \ \forall x \in \Omega_X, \forall y \in \Omega_Y$
- $\sum_y p(y|x) = 1, \ \ \forall x \in \Omega_X$

We consider only memoryless channels (the output probability depends only on the input at that time and is conditionally independent on previous channels inputs and outputs).

**Definition A.5.2.** The n$^{th}$ extension of the discrete memoryless channel is given by $(\Omega_X^n, p(y^n|x^n), \Omega_Y^n)$; where the alphabets $\Omega_X^n$ and $\Omega_Y^n$ contains the $n$-symbols vectors:

- $x^n = (x_1, ..., x_n) \in \Omega_X^n$
- $y^n = (y_1, ..., y_n) \in \Omega_Y^n$

We suppose that the current input symbol does not depends on the previous input symbols; under this assumption we have: $p(y^n|x^n) = \prod_{i=1}^n p(y_i|x_i)$. An example of $p(y^n|x^n)$ of this form is given by the $AWGN$ channel discussed in Section A.7.

We want to transmit a message belonging to the message set, whose cardinality is $M$. Each message is mapped to the corresponding index in the index set $\{1,2,...,M\}$.

**Definition A.5.3.** An $(M, n)$ code with $M$ messages and $n$ symbols per message consists of:

- An encoding function $f^n : \{1, ..., M\} \to \Omega_X^n$
- $x^n(i) \in \Omega_X^n$ represents the codeword associated to the message $i$.
- The codebook is the set of all the codewords: $\mathcal{C} \triangleq \{x^n(1), ..., x^n(M)\}$
- A decoding function $g : \Omega_Y^n \to \{1, ..., M\}$.

We now put everything together to define the communication channel shown in Figure A.7.

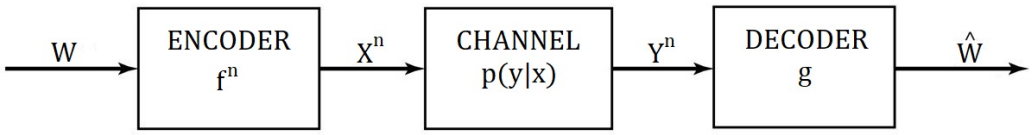



**Figure A.7:** Communication channel (mentioned on p. 58)

- A message $W$ with index $i$ is encoded to $X^n = x^n(i)$.
- $X^n$ is transmitted through the discrete channel.
- $Y^n$ is received.
- After decoding $Y^n$ we get a guess of the original transmitted message $i \to \hat{W}$.

We now list some definitions concerning the error probability.

**Definition A.5.4** (Conditional probability of error)**.**

$$\lambda_i \triangleq P(g(Y^n) \neq i | X^n = x^n(i)) = \sum_{y^n : g(y^n) \neq i} p(y^n | x^n(i))$$

**Definition A.5.5** (Maximal error probability)**.**

$$\lambda_{MAX} \triangleq \max_{i \in \{1,...M\}} \lambda_i$$

**Definition A.5.6** (Average error probability)**.**

$$\lambda_{AVE} \triangleq \frac{1}{M}\sum_{i=1}^{M}\lambda_i$$

If the index of $W$ is uniformly distributed the average error probability is equal to the overall error probability:

$$P_e \triangleq P(\hat{W} \neq W) = P(g(Y^n) \neq W) = \lambda_{AVE}$$

### A.5.2 Channel capacity

**Definition A.5.7.** The rate of a $(M, n)$ code is defined as:

$$R \triangleq \frac{\log_2 M}{n} \ [Information\ bits\ per\ symbol]$$

($\log_2 M$ is the number of bits per message and $n$ is the number of symbols per message). Notice that $M = \lceil 2^{nR} \rceil$ so a code is said to be a $(2^{nR}, n)$ code.

A rate $R$ is achievable if there exists a $(2^{nR}, n)$ code such that $\lambda_{MAX} \to 0$ as $n \to \infty$.

**Definition A.5.8.** The (operational) Channel Capacity is the supremum of all achievable rates; i.e. all the rates less than the Channel Capacity are achievable by means of a $(2^{nR}, n)$ code for $n$ sufficiently large.

**Definition A.5.9.** The Information Channel Capacity is given by:

$$C \triangleq max_{p(x)} I(X;Y)$$

where $X$ and $Y$ are random variables representing, respectively, the transmitted and the received symbol.

**Theorem A.5.1** (Channel coding theorem)**.** *The operational Channel Capacity is exactly equal to the Information Channel Capacity, i.e., given a discrete memoryless channel* $(\Omega_X^n, p(y^n|x^n), \Omega_Y^n)$ *and a rate* $R \leq C = max_{p(x)} I(X;Y)$*, there exists a* $(2^{nR}, n)$ *code achieving* $R$ *with* $\lambda_{MAX} \to 0$*. Conversely, any code achieving* $\lambda_{MAX} \to 0$ *must have* $R \leq C = max_{p(x)} I(X;Y)$*, where* $\lambda_{MAX}$ *is the maximal error probability defined in* $Def^n$ *A.5.5.*

Theorem A.5.1 is an essential result of information theory, therefore we present its proof.

*Proof.* We suppose the entire codebook to be random and represented by the $M \times n$ matrix displayed in Equation (A.3), where each row is a $n$-symbols codeword drawn according to $p(x^n) = \prod_{i=1}^{n} p(x_i)$.

$$\mathcal{C} = \begin{bmatrix} x_1(1) & x_2(1) & \cdots & x_n(1) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(M) & x_2(M) & \cdots & x_n(M) \end{bmatrix} \tag{A.3}$$

Each element of the matrix is *i.i.d.*, therefore the probability of a particular codebook $\mathcal{C}$ is given by:

$$P(\mathcal{C}) = \prod_{w=1}^{M} \prod_{i=1}^{n} p(x_i(w)) \tag{A.4}$$

1. The sender chooses a message with index $W = w$, where $P(W = w) = {}^1/_M, \forall w \in \{1, ..., M\}$ and encodes it to $X^n(w)$ (the $w^{th}$ row of $\mathcal{C}$).

2. The codeword $X^n(w)$ is transmitted through the channel; the receiver receives $Y^n$ according to $p(y^n|x^n(w)) = \prod_{i=1}^{n} p(y_i|x_i(w))$ and uses a decoding algorithm to guess $W$ as $\hat{W}(Y^n)$.

We now compute the average error probability in respect to the codebook and codewords (transmitted messages):

$$E_{[W,\mathcal{C}]}(e) \triangleq \sum_{\mathcal{C},w} P(\mathcal{C}, W = w) P(\hat{W}(Y^n) \neq w|\mathcal{C}, w)$$

$\mathcal{C}$ and $W$ are independent $\rightarrow P(\mathcal{C}, W = w) = P(\mathcal{C})P(W = w)$

$$E_{[W,\mathcal{C}]}(e) = \sum_{\mathcal{C}} P(\mathcal{C}) \sum_{w=1}^{M} P(W = w) P(\hat{W}(Y^n) \neq w|\mathcal{C}, w)$$

$$= \sum_{\mathcal{C}} P(\mathcal{C}) \frac{1}{M} \sum_{w=1}^{M} P(\hat{W}(Y^n) \neq w|\mathcal{C}, w)$$

By the symmetry of the codebook construction, the average error probability does not depend on the particular transmitted message $W$; in other words, as long as the codebook is not revealed, the probability of error is the same for any selected message (for any transmitted codeword); hence, for simplicity and without loss of generality, we suppose that the message $W = 1$ is selected:

$$\sum_{w=1}^{M} P(\hat{W}(Y^n) \neq w|\mathcal{C}, w) = M P(\hat{W}(Y^n) \neq 1|\mathcal{C}, W = 1)$$

$$\implies E_{[W,\mathcal{C}]}(e) = \sum_{\mathcal{C}} P(\mathcal{C}) P(\hat{W}(Y^n) \neq 1|\mathcal{C}, W = 1)$$

We consider the jointly typical decoding algorithm, which is asymptotically optimal:

- The receiver guess $\hat{W}$ iff $(X^n(\hat{W}), Y^n) \in A_\varepsilon^{(n)}$ and there is no other index $W' \neq \hat{W} : (X^n(W'), Y^n) \in A_\varepsilon^{(n)}$.

We consequently have a decoding error if one or more of the following events occur:

- $\mathcal{E}_1^c \equiv$ "$(X^n(1), Y^n) \notin A_\varepsilon^{(n)}$"
- $\mathcal{E}_2 \equiv$ "$(X^n(2), Y^n) \in A_\varepsilon^{(n)}$"

  $\vdots$
- $\mathcal{E}_M \equiv$ "$(X^n(M), Y^n) \in A_\varepsilon^{(n)}$"

The average probability of error becomes:

$$E_{[W,\mathcal{C}]}(e) = \sum_{\mathcal{C}} P(\mathcal{C}) P(\mathcal{E}_1^c \cup \mathcal{E}_2 \cup ... \cup \mathcal{E}_M | \mathcal{C}, W = 1)$$

From the union bound inequality we get:

$$P(\mathcal{E}_1^c \cup \mathcal{E}_2 \cup ... \cup \mathcal{E}_M | \mathcal{C}, W = 1) \leq P(\mathcal{E}_1^c | \mathcal{C}, W = 1) + \sum_{j=2}^{M} P(\mathcal{E}_j | \mathcal{C}, W = 1)$$

We start to consider $P(\mathcal{E}_1^c | \mathcal{C}, W = 1) = P((X^n(1), Y^n) \notin A_\varepsilon^{(n)} | \mathcal{C}, W = 1)$.

Since $p(y^n|x^n(1)) = \prod_{i=1}^n p(y_i|x_i(1))$, we have that:

$$p(y^n, x^n(1)) = p(x^n(1)) p(y^n|x^n(1)) = \prod_{i=1}^{n} p(x_i(1)) p(y_i|x_i(1)) = \prod_{i=1}^{n} p(y_i, x_i(1))$$

This last observation allows us to state that (from the $1^{st}$ property of jointly typical sequences presented in Section A.4.3) sequences $X^n(1)$ and $Y^n$ are jointly typical with probability close to 1, independently from the particular random codebook $\mathcal{C}$, provided that $n$ is sufficiently large; therefore we have:

$$P(\mathcal{E}_1^c | \mathcal{C}, W = 1) \leq \varepsilon$$

We now consider $P(\mathcal{E}_j | \mathcal{C}, W = 1) = P((X^n(j), Y^n) \in A_\varepsilon^{(n)} | \mathcal{C}, W = 1)$.

If $j \neq 1$, $X^n(j)$ and $X^n(1)$ are independent, so are $Y^n$ and $X^n(j)$; i.e.

$$(Y^n, X^n(j \neq 1)) \sim \prod_{i=1}^{n} p(y_i) p(x_i(j))$$

As a consequence, independently from the particular random codebook $\mathcal{C}$, $X^n(j)$ and $Y^n$ are jointly typical with probability equal or less than $2^{-n(I(X;Y)-3\varepsilon)}$; therefore we have:

$$P(\mathcal{E}_j | \mathcal{C}, W = 1) \leq 2^{-n(I(X;Y)-3\varepsilon)}, \;\; j = 2, ..., M$$

We combine the previous results:

$$P(\mathcal{E}_1^c \cup \mathcal{E}_2 \cup ... \cup \mathcal{E}_M|\mathcal{C}, W=1) \leq \varepsilon + (M-1)2^{-n(I(X;Y)-3\varepsilon)}$$

$$\rightarrow E_{[W,\mathcal{C}]}(e) \leq \sum_{\mathcal{C}} P(\mathcal{C})(\varepsilon + (M-1)2^{-n(I(X;Y)-3\varepsilon)})$$

Finally we get the following inequality:

$$E_{[W,\mathcal{C}]}(e) \leq \varepsilon + (M-1)2^{-n(I(X;Y)-3\varepsilon)} = \varepsilon + (2^{nR}-1)2^{-n(I(X;Y)-3\varepsilon)}$$

For $n$ sufficiently large we get:

$$E_{[W,\mathcal{C}]}(e) \leq \varepsilon + 2^{n(R-[I(X;Y)-3\varepsilon])}$$

Hence we can make $E_{[W,\mathcal{C}]}(e)$ arbitrarily small provided that $R < I(X;Y)$:

- Fixed $\epsilon > 0$
- $\exists n^* : E_{[W,\mathcal{C}]}(e) < \epsilon, \forall n > n^*$

Now we choose a distribution of $x$ which maximizes the mutual information. Given $(X^*, p(x^*)) : I(X;Y) = C$, we can make $E_{[W,\mathcal{C}]}(e)$ arbitrarily small provided that $R < C$. Since the average probability of error over all the codebooks and codewords is small, there exists at least one good codebook $\mathcal{C}^* = \{x^{*n}(1), ..., x^{*n}(M)\}$ such that $\lambda_{AVE}(\mathcal{C}^*)$ is small; where $\lambda_{AVE}$, defined in $Def^n$ A.5.6, is the average error probability in respect to the transmitted codeword:

$$\lambda_{AVE}(\mathcal{C}^*) = \frac{1}{M}\sum_{i=1}^{M} \lambda_i(\mathcal{C}^*) \leq \epsilon$$

Where $\lambda_i(\mathcal{C}^*)$ is the conditional error probability given the message $i$ is selected (the codeword $X^n(i) \in \mathcal{C}^*$ is transmitted). Suppose (without loss of generality) that the conditional probabilities are ordered: $\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_M$; we can write:

$$\lambda_{AVE}(\mathcal{C}^*) = \frac{1}{M}(\sum_{i=1}^{M/2} \lambda_i(\mathcal{C}^*) + \sum_{i=M/2+1}^{M} \lambda_i(\mathcal{C}^*))$$

We define the "good-half codebook" as the set of all codewords with index $i \leq M/2$; the "bad-half codebook" as the set of all the remaining codewords:

- $\mathcal{C}^*_{good} = \{x^{*n}(1), ..., x^{*n}(M/2)\}$
- $\mathcal{C}^*_{bad} = \{x^{*n}(M/2+1), ..., x^{*n}(M)\}$

We rewrite the average probability of error as:

$$\lambda_{AVE}(\mathcal{C}^*) = \frac{1}{M}(\sum_{i \in I(\mathcal{C}^*_{good})} \lambda_i(\mathcal{C}^*_{good}) + \sum_{i \in I(\mathcal{C}^*_{bad})} \lambda_i(\mathcal{C}^*_{bad}))$$

The minimum error probability of the "bad-half codebook" can not be smaller than the maximum error probability of the "good-half codebook":

$$\lambda_{AVE}(\mathcal{C}^*) \geq \frac{1}{M}(\sum_{i \in I(\mathcal{C}^*_{good})} \lambda_i(\mathcal{C}^*_{good}) + \frac{M}{2}\lambda_{MAX}(\mathcal{C}^*_{good}))$$

$$\implies \lambda_{AVE}(\mathcal{C}^*) - \frac{1}{2}\lambda_{MAX}(\mathcal{C}^*_{good}) \geq \frac{1}{M} \sum_{i \in I(\mathcal{C}^*_{good})} \lambda_i(\mathcal{C}^*_{good}) \geq 0$$

$$\implies \lambda_{MAX}(\mathcal{C}^*_{good}) \leq 2\lambda_{AVE}(\mathcal{C}^*) \leq 2\epsilon$$

Therefore there exists a good code with rate:

$$R' = \frac{\log_2 M/2}{n} = R - \frac{1}{n} \xrightarrow{n \to \infty} R$$

such that the maximum probability of error can be made arbitrarily small provided that $R \leq C$; this proves the channel coding theorem. □

## A.6 Differential entropy

In this section the differential entropy is defined. Its properties are very similar to the entropy of a discrete r.v. (Section A.2); hence to avoid repetition we will only focus on its peculiar properties.

**Definition A.6.1.** Given a continuous r.v. $X$ with probability density function $f(x)$, its differential entropy is defined as:

$$h(x) = \int_{S_X} dx f(x) \log_2 f(x)$$

Where $S_X$ is the support of $X$.

The following properties are satisfied.

- Given $c, a \in \mathbb{R}$:
  - $h(X + c) = h(X)$ (translations do not change the differential entropy)
  - $h(aX) = h(X) + \log_2 |a|$

- Given another continuous r.v. $Y$ with density $f(y)$:
  - $h(X,Y) = h(X) + h(X|Y) = h(Y) + h(Y|X)$ (Chain Rule)
  - $h(X,Y) \leq h(X) + h(Y)$, equality holds iff $X$ and $Y$ are independent
  - $h(X+Y|X) = h(Y)$, if $X$ and $Y$ are independent
- If $X_G \sim \mathcal{N}(\mu, \sigma_G^2)$
  - $h(X_G) = 1/2 \log_2(2\pi e\sigma^2)$
- If $X$ is any continuous r.v. with variance $\sigma_G^2$ (same as $X_G$), the following inequality holds:
  - $h(X) \leq h(X_G)$

**Definition A.6.2.** Given two densities $f(x)$ and $g(x)$, their relative entropy (or Kullback-Leibler distance) is defined as:

$$D(f||g) = \int dx f(x) \log_2 \frac{f(x)}{g(x)}$$

**Definition A.6.3.** The mutual information between two continuous r.v. $X$ and $Y$, with joint density $f(x,y)$, is defined as:

$$I(X;Y) = \int dxdy f(x,y) \log_2 \frac{f(x,y)}{f(x)f(y)}$$

From the definition it follows that:

- $I(X;Y) = h(X) - h(X|Y) = h(Y) - h(Y|X) = h(X) + h(Y) - h(X,Y)$
- $I(X;Y) = D(f(x,y)||f(x)f(y))$

## A.7 AWGN channel

Let us briefly describe the AWGN channel. In this model the noise is Gaussian distributed; this assumption is very simple but at the same time is used in many scenarios, as a matter of fact thanks to the CLT the overall sum of many random noise contributions tends to be Gaussian distributed.

**Definition A.7.1.** A $(S_X, f(y^n|x^n), S_Y)$ channel is AWGN if:

$$f(y^n|x^n) = \prod_{i=1}^{n} f(y_i|x_i) = \prod_{i=1}^{n} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(y_i - x_i)^2}{2\sigma^2}\right)$$

I.e. $f(y^n|x^n) \sim \mathcal{N}_n(x^n, \sigma^2 \mathbb{I}_n)$, where $\mathcal{N}_n$ denotes the multivariate Gaussian distribution of a $n$-dimensional random vector.

The generic received symbol $Y$ is equal to the input symbol plus a white noise added by the receiver side:

$$Y = X + Z$$

where $Z \sim \mathcal{N}(0, \sigma^2)$ is the white noise.

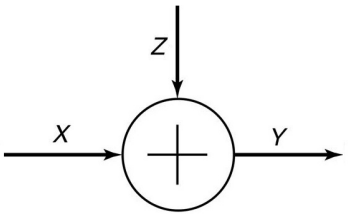



**Figure A.8:** AWGN channel

### A.7.1 AWGN Capacity

We can easily evaluate the channel capacity of the AWGN channel by exploiting the properties of differential entropy displayed in Section A.6; keeping into account that:

- $X$ and $Z$ are independent.
- $Z$ is Gaussian distributed with zero mean.

Therefore we get:

$$I(X;Y) = h(Y) - h(Y|X) = h(Y) - h(X+Z|X) = h(Y) - h(Z)$$

In order to find the maximum we exploit the following inequality:

$$h(Y) \leq h(Y_G) = 1/2 \log_2(2\pi e \sigma_Y^2)$$

I.e. the maximum entropy is achieved if $Y$ is Gaussian distributed:

$$Y = Y_G \longleftrightarrow Y \sim \mathcal{N}(\mu_Y, \sigma_Y^2)$$

Assuming the transmission power constraint $E[X^2] \leq P$, the previous condition is satisfied if $X \sim N(\mu_X, P - \mu_X^2) \Longleftrightarrow Y \sim \mathcal{N}(\mu_X, P - \mu_X^2 + \sigma^2)$

The variance is maximixed if $\mu_X = 0$, i.e. if $X \sim \mathcal{N}(0, P) \rightarrow Y \sim \mathcal{N}(0, P + \sigma^2)$

$$\rightarrow h(Y_G) = 1/2 \log_2(2\pi e(P + \sigma^2))$$

Since $C = max_{f(x)} I(X;Y)$, we finally get:

$$C_{AWGN} = 1/2 \log_2(2\pi e(P + \sigma^2)) - 1/2 \log_2(2\pi e \sigma^2) = \frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma^2}\right) \qquad \text{(A.5)}$$

If we transmit complex signals with in-phase and quadrature components the capacity is doubled:

$$C_{AWGN} = \log_2\left(1 + \frac{P}{\sigma^2}\right) = \log_2\left(1 + SNR\right) \tag{A.6}$$

Where SNR denotes the (useful) signal to noise power ratio. Similarly to what we saw in Section A.5, it can also be proven in the continuous case that any rate below capacity can be achieved with arbitrarily small probability of error.

# Appendix B

# Review of multi-user Information theory

## B.1 Jointly typical sequences (extension)

In this section, in order to analyze the multi-user channels, we extend the notion of typical sequences (Section A.4) to a collection of three random variables $X_A, X_B, Y$ with joint distribution:

- $p(x_A, x_B, y), (x_A, x_B, y) \in \Omega_{X_A} \times \Omega_{X_B} \times \Omega_Y$

Let's consider three $n$-sequences of that variables:

- $X_A^n = X_{A1}, ..., X_{An}$
- $X_B^n = X_{B1}, ..., X_{Bn}$
- $Y^n = Y_1, ..., Y_n$

So that the corresponding joint random vector can be written as:

- $(X_A^n, X_B^n, Y^n) = (X_{A1}, X_{B1}, Y_1), ..., (X_{An}, X_{Bn}, Y_n)$

drawn accordingly to:

- $p(x_A^n, x_B^n, y^n) = \prod_{i=1}^n p(x_{Ai}, x_{Bi}, y_i) = \prod_{i=1}^n P(X_{Ai} = x_{Ai}, X_{Bi} = x_{Bi}, Y_i = y_i)$

We derive the AEP by following the same logic presented in A.4:

$$-\frac{1}{n} \log_2 p((X_{A1}, X_{B1}, Y_1), ..., (X_{An}, X_{Bn}, Y_n)) = -\frac{1}{n} \sum_{i=1}^{n} \log_2 p(X_{Ai}, X_{Bi}, Y_i)$$

- $(X_{Ai}, X_{Bi}, Y_i)$ and $(X_{Aj}, X_{Bj}, Y_j), i \neq j$, are independent

- so are $\log_2 p(X_{Ai}, X_{Bi}, Y_i)$ and $\log_2 p(X_{Aj}, X_{Bj}, Y_j)$

Therefore by applying the weak law of the large numbers (Theorem A.4.1) we derive:

$$\lim_{n\to\infty} P\left(\left|-\frac{1}{n}\sum_{i=1}^{n}\log_2 p(X_{Ai}, X_{Bi}, Y_i) - H(X_A, X_B, Y)\right| < \varepsilon\right) = 1$$

Equivalently:

$$\lim_{n\to\infty} P\left(\left|-\frac{1}{n}\log_2 p((X_A^n, X_B^n, Y^n)) - H(X_A, X_B, Y)\right| < \varepsilon\right) = 1$$

I.e. for $n$ sufficiently large the following holds: $p(X_A^n, X_B^n, Y^n) \simeq 2^{-nH(X_A,X_B,Y)}$ In this respect sequences $X_A^n$, $X_B^n$ and $Y^n$ with joint distribution $p(x_A^n, x_B^n, y^n) = \prod_{i=1}^n p(x_{Ai}, x_{Bi}, y_i)$ are jointly typical if they are typical sequences and their empirical joint entropy is close to the true joint entropy. More precisely:

**Definition B.1.1** (Jointly typical set (extension))**.**

$$\begin{aligned} A_\varepsilon^{(n)} \triangleq \{\boldsymbol{x} = (x_A^n, x_B^n, y^n) \in (\Omega_{X_A}^n, \Omega_{X_B}^n, \Omega_Y^n) : \\ |-1/n \log_2 p(x_A^n) - H(X_A)| < \varepsilon, \\ |-1/n \log_2 p(x_B^n) - H(X_B)| < \varepsilon, \\ |-1/n \log_2 p(y^n) - H(Y)| < \varepsilon, \\ |-1/n \log_2 p(x_A^n, x_B^n, y^n) - H(X_A, X_B, Y)| < \varepsilon\} \end{aligned}$$

The following properties are satisfied. $\forall\varepsilon > 0$, $\exists n^*$ : if $n > n^*$, then:

1. $P((X_A^n, X_B^n, Y^n) \in A_\varepsilon^{(n)}) > 1 - \varepsilon$
2. $\boldsymbol{x} \in A_\varepsilon^{(n)} \Longrightarrow p(\boldsymbol{x}) \doteq 2^{-n(H(X_A,X_B,Y)\pm\varepsilon)}$
3. $\left|A_\varepsilon^{(n)}\right| \doteq 2^{n(H(X_A,X_B,Y)\pm 2\varepsilon)}$

   Where $a \doteq 2^{n(b\pm\varepsilon)}$ means $|\frac{1}{n}\log_2 a - b| < \varepsilon$

   Given $S_1, S_2 \subseteq \{X_A, X_B, Y\}$ we build their corresponding $n$-sequences:

   - $S_1^n = S_{11}, ..., S_{1n}$
   - $S_2^n = S_{21}, ..., S_{2n}$

   with distributions $p(\boldsymbol{s_1})$ and $p(\boldsymbol{s_2})$ respectively. The following holds:

4. If $(\boldsymbol{s_1}, \boldsymbol{s_2}) \in A_\varepsilon^{(n)}(S_1, S_2) \Longrightarrow p(\boldsymbol{s_1}|\boldsymbol{s_2}) \doteq 2^{-n(H(S_1|S_2)\pm 2\varepsilon)}$

   Where

$$\begin{aligned} A_\varepsilon^{(n)}(S_1, S_2) \triangleq \{&(\boldsymbol{s_1}, \boldsymbol{s_2}) : \\ &| -1/n \log_2 p(\boldsymbol{s_1}) - H(S_1)| < \varepsilon, \\ &| -1/n \log_2 p(\boldsymbol{s_2}) - H(S_2)| < \varepsilon, \\ &| -1/n \log_2 p(\boldsymbol{s_1}, \boldsymbol{s_2}) - H(S_1, S_2)| < \varepsilon\} \end{aligned}$$

   Considering again $S_1$ and $S_2$, let's suppose the $n$-sequence $S_2^n = \boldsymbol{s_2}$ has been revealed. We define $A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})$ as the set of $\boldsymbol{s_1}$ sequences that are jointly typical with $\boldsymbol{s_2}$, more precisely:

$$\begin{aligned} A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2}) \triangleq \{&\boldsymbol{s_1} : \\ &| -1/n \log_2 p(\boldsymbol{s_1}) - H(S_1)| < \varepsilon, \\ &| -1/n \log_2 p(\boldsymbol{s_1}, \boldsymbol{s_2}) - H(S_1, S_2)| < \varepsilon\} \end{aligned}$$

   If $\boldsymbol{s_2} \in A_\varepsilon^{(n)}$, the following hold:

5. $|A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})| \leq 2^{n(H(S_1|S_2)+2\varepsilon)}$

6. $(1-\varepsilon)2^{n(H(S_1|S_2)-2\varepsilon)} \leq \sum_{\boldsymbol{s_2}} p(\boldsymbol{s_2})|A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})|$

   We consider $S_1, S_2, S_3 \subseteq \{X_A, X_B, Y\}$ and $\tilde{S_1^n}, \tilde{S_2^n}, \tilde{S_3^n}$ such that:

$$P(\tilde{S_1^n} = \boldsymbol{s_1}, \tilde{S_2^n} = \boldsymbol{s_2}, \tilde{S_3^n} = \boldsymbol{s_3}) = \prod_{i=1}^{n} p(s_{3i}) p(s_{1i}|s_{3i}) p(s_{2i}|s_{3i})$$

   (I.e. $\tilde{S_1^n}$ and $\tilde{S_2^n}$ are conditionally independent given $\tilde{S_3^n}$ but with the same marginal as $S_1^n$ and $S_2^n$). The following property is satisfied:

7. $P((\tilde{S_1^n}, \tilde{S_2^n}, \tilde{S_3^n}) \in A_\varepsilon^{(n)}) \doteq 2^{-n(I(S_1;S_2|S_3)\pm 7\varepsilon)}$

*Proof.* We present the proof of the various properties listed above.

1. This follows directly from the definition of jointly typical set

2. Same as the first

3. The upper bound derives from:

$$\begin{aligned} 1 &\geq P((X_A^n, X_B^n, Y^n) \in A_\varepsilon^{(n)}) \\ &= \sum_{\boldsymbol{x} \in A_\varepsilon^{(n)}} p(\boldsymbol{x}) \geq |A_\varepsilon^{(n)}| min(p(\boldsymbol{x})) \\ &= |A_\varepsilon^{(n)}| 2^{-n(H(X_A, X_B, Y)+\varepsilon)} \\ &\rightarrow |A_\varepsilon^{(n)}| \leq 2^{n(H(X_A, X_B, Y)+\varepsilon)} \end{aligned}$$

   Instead, the lower bound follows from:

$$\begin{aligned} 1 - \varepsilon &\leq P((X_A^n, X_B^n, Y^n) \in A_\varepsilon^{(n)}) \\ &= \sum_{\boldsymbol{x} \in A_\varepsilon^{(n)}} p(\boldsymbol{x}) \leq |A_\varepsilon^{(n)}| max(p(\boldsymbol{x})) \\ &= |A_\varepsilon^{(n)}| 2^{-n(H(X_A, X_B, Y)-\varepsilon)} \\ &\rightarrow |A_\varepsilon^{(n)}| \geq (1-\varepsilon) 2^{n(H(X_A, X_B, Y)-\varepsilon)} \end{aligned}$$

   I.e. overall we have:

$$\left|A_\varepsilon^{(n)}\right| \doteq 2^{n(H(X_A, X_B, Y) \pm 2\varepsilon)}$$

   Q.E.D.

4. From the definition of $A_\varepsilon^{(n)}(S_1, S_2)$ it follows that:

   - $p(\boldsymbol{s_2}) \doteq 2^{-n(H(S_2) \pm \varepsilon)}$
   - $p(\boldsymbol{s_1}, \boldsymbol{s_2}) \doteq 2^{-n(H(S_1, S_2) \pm \varepsilon)}$

   Therefore:

$$p(\boldsymbol{s_1}|\boldsymbol{s_2}) = \frac{p(\boldsymbol{s_1}, \boldsymbol{s_2})}{p(\boldsymbol{s_2})} \doteq 2^{-n(H(S_1, S_2) - H(S_2) \pm 2\varepsilon)} \doteq 2^{-n(H(S_1|S_2) \pm 2\varepsilon)}$$

   Q.E.D.

5. We use the previous property:

$$\begin{aligned} 1 &\geq P(\boldsymbol{s_1} \in A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})) \\ &= \sum_{\boldsymbol{s_1} \in A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})} p(\boldsymbol{s_1}|\boldsymbol{s_2}) \geq |A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})| min(p(\boldsymbol{s_1}|\boldsymbol{s_2})) \\ &= |A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})| 2^{-n(H(S_1|S_2)+2\varepsilon)} \\ &\Longrightarrow |A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})| \leq 2^{n(H(S_1|S_2)+2\varepsilon)} \end{aligned}$$

   Q.E.D.

6. From the first property:

$$\begin{aligned}
1-\varepsilon &\leq P((S_1^n, S_2^n) \in A_\varepsilon^{(n)}) \\
&= \sum_{\boldsymbol{s_2}} p(\boldsymbol{s_2}) \sum_{\boldsymbol{s_1} \in A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})} p(\boldsymbol{s_1}|\boldsymbol{s_2}) \leq \sum_{\boldsymbol{s_2}} p(\boldsymbol{s_2}) |A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})| max(p(\boldsymbol{s_1}|\boldsymbol{s_2})) \\
&= \sum_{\boldsymbol{s_2}} p(\boldsymbol{s_2}) |A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})| 2^{-n(H(S_1|S_2)-2\varepsilon)} \\
&\implies (1-\varepsilon) 2^{n(H(S_1|S_2)-2\varepsilon)} \leq \sum_{\boldsymbol{s_2}} p(\boldsymbol{s_2}) |A_\varepsilon^{(n)}(S_1|\boldsymbol{s_2})|
\end{aligned}$$

Q.E.D.

7.

$$\begin{aligned}
P((\tilde{S_1^n}, \tilde{S_2^n}, \tilde{S_3^n}) \in A_\varepsilon^{(n)}) &= \sum_{(\boldsymbol{s_1}, \boldsymbol{s_2}, \boldsymbol{s_3}) \in A_\varepsilon^{(n)}} p(\boldsymbol{s_3}) p(\boldsymbol{s_1}|\boldsymbol{s_3}) p(\boldsymbol{s_2}|\boldsymbol{s_3}) \\
&\doteq 2^{n(H(S_1,S_2,S_3)\pm 2\varepsilon)} 2^{-n(H(S_3)\pm\varepsilon)} 2^{-n(H(S_1|S_3)\pm 2\varepsilon)} 2^{-n(H(S_2|S_3)\pm 2\varepsilon)} \\
&\doteq 2^{-n(I(S_1;S_2|S_3)\pm 7\varepsilon)}
\end{aligned}$$

Q.E.D.

□

## B.2 Multiple-access channel

**Definition B.2.1** (Multiple-access channel)**.** A discrete memoryless multiple-access channel $(\Omega_{X_1} \times ... \times \Omega_{X_m}, p(y|x_1, ..., x_m), \Omega_Y)$ with $m$ transmitters and one receiver consists of:

- $m$ alphabets $\Omega_{X_1}, ..., \Omega_{X_m}$ associated to the $m$ transmitters
- One alphabet $\Omega_Y$ to the receiver
- A probability transition matrix $p(y|x_1, ..., x_m)$

Each user $i \in \{1, ..., m\}$ transmits a message belonging to his message set $W_i \in \{1, ..., M_i\}$

**Definition B.2.2.** An $(M_1, ..., M_m, n)$ code with $M_i$ messages per transmitter $i$ ($M_i = \lceil 2^{nR_i} \rceil$; where $R_i$ is the code rate of user $i$) and $n$ symbols per message consists of:

- $m$ encoding functions:

  - $f_1 : W_1 \to \Omega^n_{X_1}$
  - $\vdots$
  - $f_m : W_m \to \Omega^n_{X_m}$

- $\Omega^n_{X_i}$ represents the codebook of the user $i$.
- A decoding function:
  - $g : \Omega^n_Y \to W_1 \times ... \times W_m$

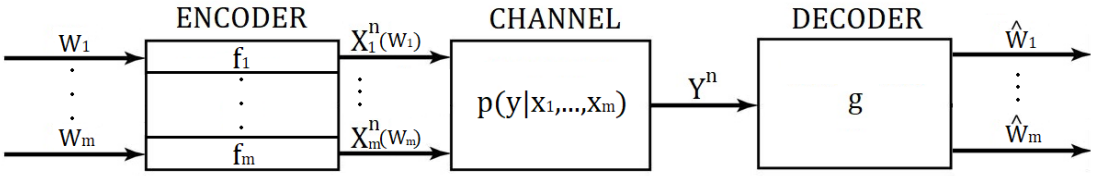



**Figure B.1:** Multiple access communication scheme

Similarly to how we did in Section A.5 we define the average error probability (over codewords). We suppose that each user uniformly chooses a message (from his message set) independently from the other users selected messages. Therefore:

**Definition B.2.3** (Average probability of error for multiple-access channel)**.**

$$\lambda_{AVE} \triangleq \alpha \sum_{\boldsymbol{w}=(w_1,...,w_m)\in W_1\times...\times W_m} P(g(Y^n) \neq \boldsymbol{w} | x^n_1(w_1), ..., x^n_m(w_m) \; sent)$$

where:

$$\alpha \triangleq {}^1\!/\!_{(M_1 \times ... \times M_m)}$$

Differently from how we did in Section A.5.2, where we defined the achievability in respect to the maximal probability of error, we now define the achievability of the set of rates in respect to the average probability of error:

**Definition B.2.4.** The set of rates $(R_1, ..., R_m)$ is said to be achievable for the multiple-access channel if there exists a $((2^{nR_1}, ...,2^{nR_m}), n)$ code such that $\lambda_{AVE} \to 0$ as $n \to \infty$.

**Theorem B.2.1** (Multiple-access channel capacity region)**.** *The capacity region (i.e. the closure of the achievable rates sets $(R_1, ..., R_m)$) of a multiple-access channel $(\Omega_{X_1} \times ... \times \Omega_{X_m}, p(y|x_1, ..., x_m), \Omega_Y)$, corresponds to the closure of the convex hull of all $(R_1, ..., R_m)$ satisfying:*

$$R(S) < I(X(S); Y | X(S^c)), \;\; \forall S \subseteq \{1, ..., m\}$$

*Where:*

- $(X_1, ..., X_m) \sim p_1(x_1) \cdot ... \cdot p_m(x_m)$
- $S^c = \{1, ..., m\} \setminus S$
- $R(S) = \sum_{i \in S} R_i$
- $X(S) = \{X_i : i \in S\}$

*In words: given any subset of users, the sum of their rates to be achievable should be less than the information that we gain on their transmitted symbols once the received symbol is revealed, given the transmitted symbols of the other users.*

For $m = 2$ (let's call the two users $A$ and $B$) we get the following achievability constraints:

- $R_A < I(X_A; Y|X_B)$
- $R_B < I(X_B; Y|X_A)$
- $R_A + R_B < I(X_A, X_B; Y)$

*Proof.* We prove the achievability for two users ($A$ and $B$). We extend the assumptions we made for the single user in Section A.5.2 to the two-user scenario:

- Both codebooks of user $A$ and $B$ are randomly generated as $M_j \times n, \;\; j \in \{A, B\}$ matrices where each row is a $n$-symbols codeword drawn according to
  - $p_A(x_A^n) = \prod_{i=1}^n p_A(x_{Ai})$ for user $A$
  - $p_B(x_B^n) = \prod_{i=1}^n p_B(x_{Bi})$ for user $B$
- The resulting codebooks are:
  - $\mathcal{C}_A = \begin{bmatrix} x_{A1}(1) & x_{A2}(1) & \cdots & x_{An}(1) \\ \vdots & \vdots & \ddots & \vdots \\ x_{A1}(M_A) & x_{A2}(M_A) & \cdots & x_{An}(M_A) \end{bmatrix}$
  - $\mathcal{C}_B = \begin{bmatrix} x_{B1}(1) & x_{B2}(1) & \cdots & x_{Bn}(1) \\ \vdots & \vdots & \ddots & \vdots \\ x_{B1}(M_B) & x_{B2}(M_B) & \cdots & x_{Bn}(M_B) \end{bmatrix}$
- Each element of each matrix is *i.i.d.* hence the probability of a particular multiple-access code is given by:
  - $P(\mathcal{C}_A, \mathcal{C}_B) = P(\mathcal{C}_A)P(\mathcal{C}_B) = \prod_{w_A=1}^{M_A} \prod_{w_B=1}^{M_B} \prod_{i=1}^n p_A(x_{Ai}(w_A))p_B(x_{Bi}(w_B))$

1. Sender $A$ picks a message with index $W_A = w_A$, where $P(W_A = w_A) = 1/M_A$, $\forall w_A \in \{1, ..., M_A\}$ and encodes it to $X_A^n(w_A)$ (the $w_A^{th}$ row of $\mathcal{C}_A$)

2. Sender $B$ picks a message with index $W_B = w_B$, where $P(W_B = w_B) = {}^1/_{M_B}$, $\forall w_B \in \{1, ..., M_B\}$ and encodes it to $X_B^n(w_B)$ (the $w_B^{th}$ row of $\mathcal{C}_B$)

3. Codewords $X_A^n(w_A)$ and $X_B^n(w_B)$ are transmitted; the receiver receives $Y^n$ according to $p(y^n|x_A^n(w_A), x_B^n(w_B)) = \prod_{i=1}^n p(y_i|x_{Ai}(w_A), x_{Bi}(w_B))$ and uses a decoding algorithm to guess $(W_A, W_B)$ as $(\hat{W}_A, \hat{W}_B)(Y^n)$

We now compute the average error probability over codebooks and codewords (transmitted messages):

$$E_{[W_A,W_B,\mathcal{C}_A,\mathcal{C}_B]}(e) \triangleq \sum_{\mathcal{C}_A,\mathcal{C}_B,w_A,w_B} P(\mathcal{C}_A,\mathcal{C}_B,W_A{=}w_A,W_B{=}w_B)P((\hat{W}_A,\hat{W}_B)(Y^n){\neq}(w_A,w_B)|\mathcal{C}_A,\mathcal{C}_B,w_A,w_B)$$

Since $W_A, W_B, \mathcal{C}_A, \mathcal{C}_B$ are independent, we get:

$$E_{[W_A,W_B,\mathcal{C}_A,\mathcal{C}_B]}(e) = \sum_{\mathcal{C}_A,\mathcal{C}_B} P(\mathcal{C}_A,\mathcal{C}_B) \frac{1}{M_A \times M_B} \sum_{w_A,w_B} P((\hat{W}_A,\hat{W}_B)(Y^n){\neq}(w_A,w_B)|\mathcal{C}_A,\mathcal{C}_B,w_A,w_B)$$

By the symmetry of the codebooks construction, the average error probability does not depend on the particular transmitted messages $W_A$ and $W_B$; in other words, as long as the codebooks are not revealed, the probability of error is the same for any selected messages (for any transmitted codewords); hence, for simplicity and without loss of generality, we suppose that the messages $W_A = 1, W_B = 1$ are selected:

$$\sum_{w_A,w_B} P((\hat{W}_A, \hat{W}_B)(Y^n) \neq (w_A, w_B)|...) = (M_A \times M_B)P((\hat{W}_A, \hat{W}_B)(Y^n) \neq (1{,}1)|...)$$

$$\implies E_{[W_A,W_B,\mathcal{C}_A,\mathcal{C}_B]}(e) = \sum_{\mathcal{C}_A,\mathcal{C}_B} P(\mathcal{C}_A, \mathcal{C}_B)P((\hat{W}_A, \hat{W}_B)(Y^n) \neq (1{,}1)|\mathcal{C}_A, \mathcal{C}_B, 1{,}1)$$

We consider the jointly typical decoding algorithm:

- The receiver guess $(\hat{W_A}, \hat{W_B})$ iff $(X_A^n(\hat{W_A}), X_B^n(\hat{W_B}), Y^n) \in A_\varepsilon^{(n)}$ and there is no other pair of indexes $(W_A', W_B') \neq (\hat{W_A}, \hat{W_B}) : (X_A^n(W_A'), X_B^n(W_B'), Y^n) \in A_\varepsilon^{(n)}$.

We consequently have a decoding error if one or more of the following events occur:

- $\mathcal{E}_{11}^c \equiv$ "$(X_A^n(1), X_B^n(1), Y^n) \notin A_\varepsilon^{(n)}$"
- $\boldsymbol{\mathcal{E}_{i1}} = \{\bigcup_{i=2}^{M_A} \mathcal{E}_{i1}\}$, $\mathcal{E}_{i1} \equiv$ "$(X_A^n(i), X_B^n(1), Y^n) \in A_\varepsilon^{(n)}$"
- $\boldsymbol{\mathcal{E}_{1j}} = \{\bigcup_{j=2}^{M_B} \mathcal{E}_{1j}\}$, $\mathcal{E}_{1j} \equiv$ "$(X_A^n(1), X_B^n(j), Y^n) \in A_\varepsilon^{(n)}$"
- $\boldsymbol{\mathcal{E}_{ij}} = \{\bigcup_{(i\neq1,j\neq1)} \mathcal{E}_{ij}\}$, $\mathcal{E}_{ij} \equiv$ "$(X_A^n(i), X_B^n(j), Y^n) \in A_\varepsilon^{(n)}$"

Where for simplicity we use $i, j$ instead of $w_A, w_B$ respectively.

The average probability of error becomes:

$$E_{[W_A,W_B,\mathcal{C}_A,\mathcal{C}_B]}(e) = \sum_{\mathcal{C}_A,\mathcal{C}_B} P(\mathcal{C}_A,\mathcal{C}_B)P(\mathcal{E}_{11}^c \cup \boldsymbol{\mathcal{E}_{i1}} \cup \boldsymbol{\mathcal{E}_{1j}} \cup \boldsymbol{\mathcal{E}_{ij}}|\mathcal{C}_\mathcal{A},\mathcal{C}_\mathcal{B},1,1)$$

From the union bound inequality we get:

$$P(\mathcal{E}_{11}^c \cup \boldsymbol{\mathcal{E}_{i1}} \cup \boldsymbol{\mathcal{E}_{1j}} \cup \boldsymbol{\mathcal{E}_{ij}}|...) \leq P(\mathcal{E}_{11}^c|...) + \sum_{i=2}^{M_A} P(\mathcal{E}_{i1}|...) + \sum_{j=2}^{M_B} P(\mathcal{E}_{1j}|...) + \sum_{i\neq 1, j\neq 1} P(\mathcal{E}_{ij}|...)$$

In what follows we will apply the properties of the joint typical sequences listed in Section B.1.

We start to consider: $P(\mathcal{E}_{11}^c|...) = P((X_A^n(1), X_B^n(1), Y^n) \notin A_\varepsilon^{(n)}|\mathcal{C}_A,\mathcal{C}_B,1,1)$

Since $p(y^n|x_A^n(1), x_B^n(1)) = \prod_{i=1}^n p(y_i|x_{Ai}(1), x_{Bi}(1))$, we have that:

$$\begin{aligned} p(y^n, x_A^n(1), x_B^n(1)) &= p(x_A^n(1), x_B^n(1))p(y^n|x_A^n(1), x_B^n(1)) \\ &= \prod_{i=1}^n p(x_{Ai}(1), x_{Bi}(1))p(y_i|x_{Ai}(1), x_{Bi}(1)) \\ &= \prod_{i=1}^n p(x_{Ai}(1), x_{Bi}(1), y_i) \end{aligned}$$

This last observation allows us to state that (from the $1^{st}$ property of jointly typical sequences presented in Section B.1) sequences $X_A^n(1)$,$X_B^n(1)$ and $Y^n$ are jointly typical with probability close to 1, independently from the particular random codebooks $\mathcal{C}_A, \mathcal{C}_B$ provided that $n$ is sufficiently large; therefore we have:

$$P(\mathcal{E}_{11}^c|\mathcal{C}_A,\mathcal{C}_B,1,1) \leq \varepsilon, \ \ \forall \mathcal{C}_A, \mathcal{C}_\mathcal{B}$$

Now let's consider: $P(\mathcal{E}_{i1}|...) = P((X_A^n(i), X_B^n(1), Y^n) \in A_\varepsilon^{(n)}|\mathcal{C}_A,\mathcal{C}_B,1,1)$

We note that $X_A^n(i)$, $i \neq 1$ and $X_A^n(1)$ are independent, so are $X_A^n(i)$ and $Y^n$; therefore we have:

$$\begin{aligned} &P((X_A^n(i), X_B^n(1), Y^n) \in A_\varepsilon^{(n)}|\mathcal{C}_A,\mathcal{C}_B,1,1) \\ &= \sum_{(x_A^n(i), x_B^n(1), y^n) \in A_\varepsilon^n} p(x_A^n(i), x_B^n(1), y^n|\mathcal{C}_A,\mathcal{C}_B,1,1) \\ &= \sum_{(x_A^n, x_B^n, y^n) \in A_\varepsilon^n} p_A(x_A^n)p(x_B^n, y^n) \leq 2^{n(H(X_A,X_B,Y)+2\varepsilon)}2^{-n(H(X_A)-\varepsilon)}2^{-n(H(X_B,Y)-\varepsilon)} \\ &= 2^{-n(I(X_A;X_B,Y)-4\varepsilon)} = 2^{-n(I(X_A;X_B)+I(X_A;Y|X_B)-4\varepsilon)} \\ &= 2^{-n(I(X_A;Y|X_B)-4\varepsilon)} \end{aligned}$$

After repeating the same procedure for $P(\mathcal{E}_{1j}|...)$, we obtain the following inequalities:

- $P(\mathcal{E}_{i1}|\mathcal{C}_A,\mathcal{C}_B,1,1) \leq 2^{-n(I(X_A;Y|X_B)-4\varepsilon)},\ \ \forall i \neq 1, \forall \mathcal{C}_A,\mathcal{C}_B$
- $P(\mathcal{E}_{1j}|\mathcal{C}_A,\mathcal{C}_B,1,1) \leq 2^{-n(I(X_B;Y|X_A)-4\varepsilon)},\ \ \forall j \neq 1, \forall \mathcal{C}_A,\mathcal{C}_B$

Finally:

$$
\begin{aligned}
P(\mathcal{E}_{ij}|...) &= P((X_A^n(i), X_B^n(j), Y^n) \in A_\varepsilon^{(n)}|\mathcal{C}_A,\mathcal{C}_B,1,1) \\
= \sum_{(x_A^n(i),x_B^n(j),y^n)\in A_\varepsilon^n} p(x_A^n(i), x_B^n(j), y^n|\mathcal{C}_A,\mathcal{C}_B,1,1) &= \sum_{(x_A^n,x_B^n,y^n)\in A_\varepsilon^n} p(x_A^n)p(x_B^n)p(y^n) \\
&\leq 2^{n(H(X_A,X_B,Y)+2\varepsilon)}2^{-n(H(X_A)-\varepsilon)}2^{-n(H(X_B)-\varepsilon)}2^{-n(H(Y)-\varepsilon)} \\
&= 2^{n(H(X_A,X_B,Y)+2\varepsilon)}2^{-n(H(X_A)-\varepsilon)}2^{-n(H(X_B|X_A)-\varepsilon)}2^{-n(H(Y)-\varepsilon)} \\
&= 2^{-n(H(X_A,X_B)+H(Y)-H(X_A,X_B,Y)-5\varepsilon)} \\
&= 2^{-n(I(X_A,X_B;Y)-5\varepsilon)}
\end{aligned}
$$

Where we exploit the independency between $X_A$ and $X_B$ so that $H(X_B) = H(X_B|X_A) \rightarrow H(X_B|X_A) + H(X_A) = H(X_A, X_B)$. We put everything together and we get:

$$
\begin{aligned}
E_{[W_A,W_B,\mathcal{C}_A,\mathcal{C}_B]}(e) \leq \varepsilon &+ (M_A-1)2^{-n(I(X_A;Y|X_B)-4\varepsilon)} + (M_B-1)2^{-n(I(X_B;Y|X_A)-4\varepsilon)} \\
&+(M_A-1)(M_B-1)2^{-n(I(X_A,X_B;Y)-5\varepsilon)} \xrightarrow{n\to\infty} 2^{n(R_A-[I(X_A;Y|X_B)-4\varepsilon)]} \\
&+2^{n(R_B-[I(X_B;Y|X_A)-4\varepsilon)]} + 2^{n([R_A+R_B]-[I(X_A,X_B;Y))-5\varepsilon)]} \\
&\xrightarrow{IF\ \ R_A<I(X_A;Y|X_B),\ R_B<I(X_B;Y|X_A),\ R_A+R_B<I(X_A,X_B;Y)} 0
\end{aligned}
$$

Hence the average error probability over codebooks and codewords tends to zero if the rates constraints are satisfied; therefore, in these conditions, there exists at least a good codebooks pair $(C_A^*, C_B^*)$ such that the average error probability over codewords (defined in $Def^n$ B.2.3) tends to zero for that codebooks; this proves the achievability for the multiple-access channel. □

## B.3 Broadcast channel

**Definition B.3.1** (Broadcast channel)**.** A discrete memoryless broadcast channel $(\Omega_X, p(y_1, ..., y_m|x), \Omega_{Y_1} \times ... \times \Omega_{Y_m})$ with one transmitter and $m$ receivers consists of:

- $m$ alphabets $\Omega_{Y_1}, ..., \Omega_{Y_m}$ associated to the $m$ receivers
- One alphabet $\Omega_X$ to the transmitter
- A probability transition matrix $p(y_1, ..., y_m|x)$

The transmitter transmits a message $W_i \in \{1, ..., M_i\}$ to each user $i \in \{1, ..., m\}$.

**Definition B.3.2.** An $(M_1, ..., M_m, n)$ code with $M_i$ messages per receiver $i$ ($M_i = \lceil 2^{nR_i} \rceil$; where $R_i$ is the code rate of user $i$) and $n$ symbols per message consists of:

- one encoding function:
  - $f : (W_1, ..., W_m) \to \Omega_X^n$
- m decoding functions:
  - $g_1 : \Omega_{Y_1}^n \to W_1$
    $\vdots$
  - $g_m : \Omega_{Y_m}^n \to W_m$

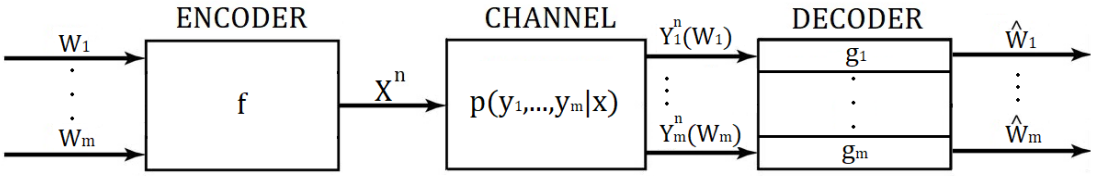



**Figure B.2:** Broadcast communication scheme

**Definition B.3.3.** Assuming $(W_1, ..., W_m)$ uniformly distributed over $M_1 \times ... \times M_m$, the average probability of error can be defined as:

$$\lambda_{AVE} \triangleq P(g_1(Y_1^n) \neq W_1 \cup ... \cup g_m(Y_m^n) \neq W_m)$$

**Definition B.3.4.** The set of rates $(R_1, ..., R_m)$ is said to be achievable for the broadcast channel if there exists a $((2^{nR_1}, ..., 2^{nR_m}), n)$ code such that $\lambda_{AVE} \to 0$ as $n \to \infty$.

Unlike the multiple-access channel, for the broadcast channel, there is no comprehensive theory capable of defining its capacity. However, there are specific cases in which it is possible to define it. One of these is the so-called degraded broadcast channel, where we can a priori identify the receivers with a "good" channel and those with a "bad" channel [21].

As in the multiple-access channel, it is possible to derive such capacity using the notions of random codebook and jointly typical decoding. However, we avoid presenting the proof in this thesis, furthermore in [22], it has been demonstrated that there is a strong duality between the capacity region of the multiple-access channel and the one of the Gaussian broadcast channel, which is our primary focus.

Specifically, given two channels, one being a multiple-access and the other being its dual broadcast (with the same gains and noise power), if we know the capacity of one, it is possible to deduce the capacity of the other.

# Bibliography


[1] M. Latva-aho. «Radio Access Networking Challenges Towards 2030». In: *Proc. 1st International Telecommunication Union Workshop on Network 2030*. Oct. 2018. URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201810/Documents/Matt_Latva-aho_Presentation.pdf (cit. on p. 2).

[2] Zhiguo Ding, Xianfu Lei, George K. Karagiannidis, Robert Schober, Jinhong Yuan, and Vijay K. Bhargava. «A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and Future Trends». In: *IEEE Journal on Selected Areas in Communications* 35.10 (2017), pp. 2181–2195. DOI: 10.1109/JSAC.2017.2725519 (cit. on p. 5).

[3] Jinho Choi. *Massive Connectivity: Non-Orthogonal Multiple Access to High Performance Random Access*. John Wiley & Sons, Ltd, 2022. ISBN: 9781119772804 (cit. on p. 5).

[4] European Telecommunications Standards Institute (ETSI). *"Universal Mobile Telecommunications System (UMTS): Multiplexing and Channel Coding (FDD)," 3 GPP TS 125.212 Version 3.4.0 (23 September, 2000): 14–20* (cit. on p. 10).

[5] Verdu S. *Multiuser Detection*. Cambridge, UK:Cambridge University Press, 1998 (cit. on p. 11).

[6] Matthew C. Valenti and Jian Sun. «Chapter 12 - Turbo Codes». In: *Handbook of RF and Wireless Technologies*. Ed. by Farid Dowla. Burlington: Newnes, 2004, pp. 375–399. ISBN: 978-0-7506-7695-3. DOI: https://doi.org/10.1016/B978-075067695-3/50014-8. URL: https://www.sciencedirect.com/science/article/pii/B9780750676953500148 (cit. on p. 15).

[7] Jiaxiang Li, Qingchun Chen, Suyue Gao, Zheng Ma, and Pingzhi Fan. «The optimal puncturing pattern design for rate-compatible punctured Turbo codes». In: *2009 International Conference on Wireless Communications & Signal Processing*. 2009, pp. 1–5. DOI: 10.1109/WCSP.2009.5371462 (cit. on p. 18).

[8] J. Hagenauer. «Rate-compatible punctured convolutional codes (RCPC codes) and their applications». In: *IEEE Transactions on Communications* 36.4 (1988), pp. 389–400. DOI: 10.1109/26.2763 (cit. on p. 18).

[9] S.S. Pietrobon. «Rate compatible turbo codes». English. In: *Electronics Letters* 31 (7 Mar. 1995), 535–536(1). ISSN: 0013-5194. URL: https://digital-library.theiet.org/content/journals/10.1049/el_19950406 (cit. on p. 18).

[10] F. Babich, G. Montorsi, and F. Vatta. «Some notes on rate-compatible punctured turbo codes (RCPTC) design». In: *IEEE Transactions on Communications* 52.5 (2004), pp. 681–684. DOI: 10.1109/TCOMM.2004.826237 (cit. on p. 18).

[11] Jinho Choi. «Power Allocation for Max-Sum Rate and Max-Min Rate Proportional Fairness in NOMA». In: *IEEE Communications Letters* 20.10 (2016), pp. 2055–2058. DOI: 10.1109/LCOMM.2016.2596760 (cit. on p. 21).

[12] Giorgio Taricco. «Fair Power Allocation Policies for Power-Domain Non-Orthogonal Multiple Access Transmission With Complete or Limited Successive Interference Cancellation». In: *IEEE Access* 11 (2023), pp. 46793–46803. DOI: 10.1109/ACCESS.2023.3274470 (cit. on p. 21).

[13] David Tse and Pramod Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005. DOI: 10.1017/CBO9780511807213 (cit. on p. 42).

[14] Andrea Goldsmith. «Multiuser Systems». In: *Wireless Communications*. Cambridge University Press, 2005, pp. 452–504. DOI: 10.1017/CBO9780511841224.015 (cit. on p. 42).

[15] B. Sklar. «Rayleigh fading channels in mobile digital communication systems .I. Characterization». In: *IEEE Communications Magazine* 35.7 (1997), pp. 90–100. DOI: 10.1109/35.601747 (cit. on p. 42).

[16] John G Proakis. *Digital communications*. McGraw-Hill, Higher Education, 2008 (cit. on p. 44).

[17] He Chenguang, Zhang Kaiyu, and Wei Shouming. «Analysis of the Channel Capacity With Shadowing Fading in VANET». In: *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. 2018, pp. 577–581. DOI: 10.1109/IWCMC.2018.8450349 (cit. on p. 44).

[18] A.J. Goldsmith and L.J. Greenstein. «A measurement-based model for predicting coverage areas of urban microcells». In: *IEEE Journal on Selected Areas in Communications* 11.7 (1993), pp. 1013–1023. DOI: 10.1109/49.233214 (cit. on p. 44).

[19] C. E. Shannon. «A mathematical theory of communication». In: *The Bell System Technical Journal* 27.3 (1948), pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x (cit. on p. 48).

[20] Joy A. Thomas Thomas M. Cover. *Elements of information theory*. Second edition. John Wiley & Sons, Inc., 2006 (cit. on p. 48).

[21] Erik Stauffer, Andy Wang, and Nihar Jindal. «Deep Learning for the Degraded Broadcast Channel». In: *2019 53rd Asilomar Conference on Signals, Systems, and Computers*. 2019, pp. 1760–1763. DOI: 10.1109/IEEECONF44664.2019.9048974 (cit. on p. 78).

[22] N. Jindal, S. Vishwanath, and A. Goldsmith. «On the duality of Gaussian multiple-access and broadcast channels». In: *IEEE Transactions on Information Theory* 50.5 (2004), pp. 768–783. DOI: 10.1109/TIT.2004.826646 (cit. on p. 78).