Thesis for the degree of
Doctor in Telecommunication
delivred by

CY Cergy Paris Université

ERROR-CONTROL CODES AND CODED MODULATIONS FOR THE OPTICAL FIBER COMMUNICATION

---

by

GADA REZGUI

ETIS UMR8051, CY Cergy Paris Université / ENSEA / CNRS
6 avenue du Ponceau, 95014 Cergy-Pontoise Cedex, France

Jury:

Pr. Iryna ANDRIYANOVA	CY Cergy Paris Université, ENSEA, CNRS	Thesis supervisor
Pr. Inbar FIJALKOW	CY Cergy Paris Université, ENSEA, CNRS	Thesis director
Pr. Alexandre GRAELL I AMAT	Chalmers University of Technology	Examiner
Pr. Jean-Pierre TILLICH	INRIA Paris	Reviewer
Pr. Joseph BOUTROS	Texas A&M University at Qatar	Reviewer
Pr. Valentin SAVIN	CEA-LETI Grenoble	Examiner
Pr. Charly POULLIAT	INP-ENSEEIHT	Examiner

Thèse de doctorat

pour l'obtention du titre de
docteur en télécommunication
délivré par

CY Cergy Paris Université

CODES CORRECTEURS ET MODULATIONS CODÉES POUR LA COMMUNICATION OPTIQUE

---

par

GADA REZGUI

ETIS UMR8051, CY Cergy Paris Université / ENSEA / CNRS
6 avenue du Ponceau, 95014 Cergy-Pontoise Cedex, France

Devant le jury composé de :

Pr. Iryna ANDRIYANOVA	CY Cergy Paris Université, ENSEA, CNRS	Encadrante
Pr. Alexandre GRAELL I AMAT	Chalmers University of Technology	Examinateur
Pr. Jean-Pierre TILLICH	INRIA Paris	Rapporteur
Pr. Joseph BOUTROS	Texas A&M University at Qatar	Rapporteur
Pr. Valentin SAVIN	CEA-LETI Grenoble	Examinateur
Pr. Charly POULLIAT	INP-ENSEEIHT	Examinateur
Pr. Inbar FIJALKOW	CY Cergy Paris Université, ENSEA, CNRS	Directrice de thèse

To my parents, my brothers, my husband and my son.

Résumé

Les câbles de communication optique transcontinentale constituent un maillon essentiel dans les communications modernes. Ils permettent de faire transiter des volumes importants de données à grande distance, tout en induisant une faible latence de transmission. L'amélioration de leurs performances est un enjeu pour la société d'aujourd'hui, la société numérique et connectée. Les précédentes évolutions de la communication optique ont été majoritairement liées à l'amélioration en termes du traitement du signal, comme par exemple le multiplexage par division de polarisation, qui a pratiquement multiplié par dix le débit de transmission. Le moment est venu de revoir la conception des codes correcteurs et des modulations numériques dans la chaine de communication optique.

L'objectif de cette thèse est d'étudier la conception des codes correcteurs et des modulations codées pour la transmission optique tout en s'appuyant sur le concept des codes en graphes sur $GF(q)$, $q = 2^m$. L'originalité de notre approche par rapport à l'état de l'art se trouve dans le fait qu'on se positionnera sur les tailles des alphabets modérées, notamment $GF(4)$ et $GF(8)$, ce qui nous permettrait, sans grande augmentation de complexité, de s'approcher de la capacité de canal et de réduire la taille de l'entrelaceur entre le démodulateur et le décodeur.

Le travail effectué se résume en trois contributions principales. La première contribution concerne le schéma de Symbol Interleaved Coded Modulation (SICM) basée sur les modulations de type M-QAM: il est démontré que la QAM-SICM avec $q > 2$ se comporte mieux que la Bit Interleaved Coded Modulation (BICM) et que, dans le cas de $q = \sqrt{M}$, la SICM atteint la capacité du canal AWGN. La deuxième contribution concerne les codes LDPC réguliers sur $GF(q)$ utilisés dans le schéma QAM-SICM : pour les rendements de code élevés, les codes LDPC 3-réguliers avec des valeurs modérées de q offrent des meilleurs performances que les autres codes LDPC réguliers, considérés dans le cadre de la transmission optique. Finalement, la troisième contribution réside dans la construction d'une nouvelle famille des codes LDPC doublement généralisées sur $GF(q)$, appelés les codes RPP (Repeatition-Parity-Parity), efficaces pour des rendement de code élevés à la fois en terme du seuil asymptotique et de la distance minimale.

Abstract

Transcontinental optical-fiber communication cables play an essential role in data networking. They enable to transmit huge amount of data at large distances, while respecting low-latency transmission constraints. Their design upgrade is an important challenge, given that the optical networks are the backbone of modern Internet. The main evolution in the optical-fiber transmission in the past has been mainly related to the improvement of the signal-processing part of the communication chain, for example the introduction of the polarization division multiplexing technique has increased the transmission throughput by a factor of ten. Nowadays, it became relevant to reconsider the design of error-control and modulation parts of the optical communication chain.

The main goal of this thesis is to investigate the design of error-control codes and coded modulations for optical communication by using the concept of non-binary graph codes over $GF(q)$, $q = 2^m$. The novelty of the approach with respect to the state of art lies in the fact that we are going to consider the codes over moderate alphabet sizes such as $GF(4)$ and $GF(8)$. This would allow us to approach to the channel capacity and to reduce the size of the interleaver between the demodulator and the decoder, at cost of a reasonable complexity growth.

Our work has lead to three following contributions. The first contribution relates to the scheme of Symbol Interleaved Coded Modulation (SICM) based on M-QAM modulations: it has been demonstrated that the QAM-SICM scheme with $q > 2$ behaves better than the traditional Bit Interleaved Coded Modulation (BICM), and that, in the case of $q = \sqrt{M}$, the SICM scheme achieves the AWGN capacity. The second contribution is focused on regular LDPC codes over $GF(q)$ used within the QAM-SICM scheme: in the context of high-rate codes, 3-regular LDPC codes with moderate values of q offer better Bit-Error Rate (BER) performances than other regular LDPC codes, considered for optical transmission. Finally, the third contribution consists in a design of a new non-binary Doubly-Generalized LDPC (DG-LDPC) code family, called RPP (Repetition-Parity-Parity) codes, showing remarkable performances both in terms of the asymptotic decoding threshold and average minimum, in the interval of high code rates.

Acknowledgement

The realization of this thesis was possible thanks to the help of several people to whom I would like to express my gratitude.

First of all, I would like to thank Iryna ANDRIYANOVA, my thesis supervisor, for having accompanied me throughout this thesis. I would like to thank her for all the knowledge she gave me, her patience and her support. Each point with her was a source of motivation for me.

I also would like to express my gratitude to the following people for their help in the realization of this thesis:

- Inbar FIJALKOW, my thesis director, for all advices she gave me.
- Charly POULLIAT and Cyril MEASSON, our collaborators in the ANR MUSICO project, for all the fruitful discussions we have had.
- All the PhD students with whom I have established links during this thesis, who advised me and helped me when I needed it.
- The reviewers, Joseph BOUTROS and Jean-Pierre TILLICH, for agreeing to review this manuscript.
- My family for their unconditional support and encouragement.

Contents

List of abbreviations

The most frequently used abbreviations in this manuscript are listed below.

Abbreviation	Meaning
LDPC	Low Density Parity Check
DG-LDPC	Doubly-Generalized Low Density Parity Check
RPP	Repetition Parity Parity
NB-LDPC	Non-Binary Low Density Parity Check
AWGN	Additive White Gaussian Noise
BEC	Binary Erasure Channel
BICM	Binary Interleaved Coded Modulation
SICM	Symbol Interleaved Coded Modulation
QAM	Quadrature Amplitude Modulation
PAM	Pulse-Amplitude Modulation
BER	Bit Error Rate
LLR	Log Likelihood Ratio
CN	Check Node
VN	Variable Node
EGL	Ensemble over the General Linear group

List of notations

The most frequently used notations are listed below.

Symbol	Meaning
$\mathcal{C}$	a linear error-correcting code
K	initial message length (in bits), $K \in \mathbb{N}^*$
N	binary codelength of a code $\mathcal{C}$, $N \in \mathbb{N}^*$
q	cardinality of a Galois field
m	number of bits in a symbol in GF(q), in case of $q = 2^m$, $m \in \mathbb{N}^*$
n	symbol codelength of a code, $n = \frac{N}{m}$, $n \in \mathbb{N}^*$
M	cardinality of a QAM modulation, $M \in \mathbb{N}^*$
r	code rate $r = \frac{K}{N}$
η	Gaussian noise $\eta \sim \mathcal{N}(0, \sigma^2)$
σ^2	Gaussian noise variance, $\sigma \in \mathbb{R}_+$
$\mathcal{A}$	modulation constellation, $M = |\mathcal{A}|$
a_i	symbol of the constellation $\mathcal{A}$
b_j	j-th bit of a Grey labeling for a M-QAM symbol
H	parity-check matrix of a code $\mathcal{C}$
(a, d) LDPC	ensemble of regular LDPC codes of VN degree a and CN degree d
(a, d, m) LDPC	ensemble of regular LDPC codes over GF(2^m)
d_{min}	Hamming minimum distance

Introduction

1.1 Background and motivation

Our work is motivated by optical-fiber data transmission applications.

The evolution of the optical communication in the 90s has been marked by such advances as design of Erbium-doped fiber amplifiers (EDFAs) [1] and introduction of wavelength multiplexing (WDM) techniques [2]. In early 2000s, the commercialisation of the WDM allowed to reach transmission throughputs up to 10Gb/s. During the last decade, the deployment of the coherent detection [3] together with digital signal processing methods has contributed a lot to the deployment of transoceanic optical-fiber systems with high spectral efficiency (from 100Gb/s up to 400 Gb/s per wavelength). It is expected that upcoming, next-generation long-haul systems will be flexible and may support even higher data rate depending on the use cases.

The most recent works in optical communication are focused on modulation and error-control coding techniques. In terms of the modulations, classical Quadrature-Amplitude Modulation (QAM) and Pulse-Amplitude Modulation (PAM) schemes are always considered, but in the context of the so called probabilistic shaping [4–18]. As for the error-control coding designs, the design of non-binary algebraic code construction such as short BCH codes [19, 20] have been further replaced by the design of 2-regular non-binary LDPC codes [21, 22] and (binary) spatially-coupled LDPC codes [23–31]. The relevance of using spatially-coupled codes in optics has been studied in [25, 26]. In both papers the authors show that spatially-coupled codes can have good performance, particularly in terms of capacity approaching and low error rates. However, the decoding complexity and the latency induced by their practical implementation (in terms of power consumption and throughput) is barely mentioned. Which in itself can be a limitation in the use of such codes in optics. In [26], the authors point out that this is a open research problem, in the use of spatially-coupled codes in optics.

This manuscript is aligned in a continuation of development of coding and modulation techniques for optics. Our main objective is to suggest a class of efficient and practical coding-modulation schemes for the optical channel. Although in the today's state of the

art a lot of codes and modulations from wireless communications standards have been mapped to the optical transmission, these schemes (almost) never consider practical implementation constraints which makes them completely non-operational under optical transmission constraints on high-throughput, low latency and parallelized implementation. In particular, most coded modulation designs are based on the well-known Binary Interleaved Coded Modulation (BICM) scheme [32], which makes latency constraints difficult to meet in practice. It would be interesting to overcome this issue and to suggest an alternative solution to the BICM.

Designing a joint coded modulation scheme first goes through a judicious choice of separately code and modulation type. Given that the most popular signal constellation in practice is the M-ary QAM lattice used on each polarization for each wavelength, the approach taken in this manuscript will combine a M-QAM modulation and Non-Binary Low Density Parity Check (NB-LDPC) codes. It is to note that, even if high-throughput non-binary codes have been already considered for optics in the past [33], the overall scheme did not exploit the symbol representation of the transmitted data. When considering non-binary codes, one should respond to some fundamental questions in optical communications such as how to achieve capacity by increasing the symbol alphabet, while considering the transmission over a Gaussian communication channel.

In this work, we are therefore focusing on design of NB-LDPC codes over a Gaussian channel with M-ary QAM modulation schemes. NB-LDPC codes have been proposed by Gallager in his PhD thesis in 1963 [34]. In 1998, Davey and MacKay [35] have shown that NB-LDPC codes achieve better performance than binary LDPC codes, over the binary symmetric channel and the binary-input Gaussian channel. The application of NB-LDPC codes to optical communication has been studied in [33, 36, 37]. In the latter work, the authors simply replaced binary LDPC codes by non-binary ones, while only considering BICM models or simple one-to-one mappings of code symbols to modulation ones.

Our tools, used in the manuscript, are density evolution and calculation of average weight enumerators and of the growth rate [38]. When put together, they give a good estimation of the NB-LDPC performance in asymptotic and finite-length region. Our performance region of interest is the region of low Bit Error Rates (BER), ideally $BER < 10^{-12}$. Moreover, the code constructions aimed for use in the optical communications should enjoy high code rates r (around $r \simeq 0.8$). Finally, they should be easy to encode and decode as decoding complexity and latency of optical transceivers is bounded. Thus, the code design framework that is considered is the design of high-rate codes of low encoding/decoding complexity, able to achieve low BERs over a Gaussian channel.

1.2 Structure of this manuscript

Let us give an idea of the structure of the manuscript. Next Chapter 2 describes a state of the art and some notation used in the rest of the document. Chapter 3, considers coded modulation aspects. A motivating example is given there in order to show why it is pertinent to reconsider usual coded modulation designs. Then, the Symbol Interleaved Coded Modulation (SICM) model is presented and compared to the BICM. Chapter 4 studies the performance of high-rate NB-LDPC ensembles with regular degrees, in the context of very low BERs, large codelengths ($N >= 32000$ bits) and high code rates r ($0.8 \leq r \leq 0.9$). The example of regular code ensembles allows to determine more precisely the range of code parameters and alphabet sizes that might be interesting to consider for our goals. Chapter 5 introduces a new code construction, called RPP. The RPP code family is a non-binary code family that outperforms regular LDPC codes in

the interval of high-code rates, both in asymptotic and finite-length regimes. Chapter 6 contains conclusions and further perspectives.

Bibliography

[1]   Emmanuel Desurvire, Jay R Simpson, and PC Becker. "High-gain erbium-doped traveling-wave fiber amplifier". In: *Optics letters* 12.11 (1987), pp. 888–890 (cit. on p. 17).

[2]   WJ Tomlinson. "Wavelength multiplexing in multimode optical fibers". In: *Applied Optics* 16.8 (1977), pp. 2180–2194 (cit. on p. 17).

[3]   Ezra Ip, Alan Pak Tao Lau, Daniel JF Barros, and Joseph M Kahn. "Coherent detection in optical fiber systems". In: *Optics express* 16.2 (2008), pp. 753–791 (cit. on p. 17).

[4]   Fabian Steiner. "Coding for higher-order modulation and probabilistic shaping". PhD thesis. Technische Universität München, 2020 (cit. on p. 17).

[5]   Joseph J Boutros, Fanny Jardel, and Cyril Méasson. "Probabilistic shaping and non-binary codes". In: *2017 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2017, pp. 2308–2312 (cit. on p. 17).

[6]   Fanny Jardel, Tobias A Eriksson, Fred Buchali, Wilfried Idler, Amirhossein Ghazisaeidi, Cyril Measson, and Joseph J Boutros. "Experimental comparison of 64-QAM and combined geometric-probabilistic shaped 64-QAM". In: *2017 European Conference on Optical Communication (ECOC)*. IEEE. 2017, pp. 1–3 (cit. on p. 17).

[7]   Fanny Jardel, Tobias A Eriksson, Cyril Méasson, Amirhossein Ghazisaeidi, Fred Buchali, Wilfried Idler, and Joseph J Boutros. "Exploring and experimenting with shaping designs for next-generation optical communications". In: *Journal of Lightwave Technology* 36.22 (2018), pp. 5298–5308 (cit. on p. 17).

[8]   Fred Buchali, Georg Böcherer, Wilfried Idler, Laurent Schmalen, Patrick Schulte, and Fabian Steiner. "Experimental demonstration of capacity increase and rate-adaptation by probabilistically shaped 64-QAM". In: *2015 European Conference on Optical Communication (ECOC)*. IEEE. 2015, pp. 1–3 (cit. on p. 17).

[9]   Fred Buchali, Fabian Steiner, Georg Böcherer, Laurent Schmalen, Patrick Schulte, and Wilfried Idler. "Rate adaptation and reach increase by probabilistically shaped 64-QAM: An experimental demonstration". In: *Journal of Lightwave Technology* 34.7 (2016), pp. 1599–1609 (cit. on p. 17).

[10] Georg Böcherer, Patrick Schulte, and Fabian Steiner. "Probabilistic shaping and forward error correction for fiber-optic communication systems". In: *Journal of Lightwave Technology* 37.2 (2019), pp. 230–244 (cit. on p. 17).

[11] Georg Böcherer, Fabian Steiner, and Patrick Schulte. "Fast probabilistic shaping implementation for long-haul fiber-optic communication systems". In: *2017 European Conference on Optical Communication (ECOC)*. IEEE. 2017, pp. 1–3 (cit. on p. 17).

[12] Patrick Schulte, Fabian Steiner, and Georg Bocherer. "Four dimensional probabilistic shaping for fiber-optic communication". In: *Signal Processing in Photonic Communications*. Optical Society of America. 2017, SpM2F–5 (cit. on p. 17).

[13] Tobias Fehenberger, Alex Alvarado, Georg Böcherer, and Norbert Hanik. "On probabilistic shaping of quadrature amplitude modulation for the nonlinear fiber channel". In: *Journal of Lightwave Technology* 34.21 (2016), pp. 5063–5073 (cit. on p. 17).

[14] Tobias Fehenberger, Domaniç Lavery, Robert Maher, Alex Alvarado, Polina Bayvel, and Norbert Hanik. "Sensitivity gains by mismatched probabilistic shaping for optical communication systems". In: *IEEE Photonics Technology Letters* 28.7 (2016), pp. 786–789 (cit. on p. 17).

[15] Junho Cho, Laurent Schmalen, and Peter J Winzer. "Normalized generalized mutual information as a forward error correction threshold for probabilistically shaped QAM". In: *2017 European Conference on Optical Communication (ECOC)*. IEEE. 2017, pp. 1–3 (cit. on p. 17).

[16] Amirhossein Ghazisaeidi, Ivan Fernandez de Jauregui Ruiz, Rafael Rios-Muller, Laurent Schmalen, Patrice Tran, Patrick Brindel, Alexis Carbo Meseguer, Qian Hu, Fred Buchali, Gabriel Charlet, et al. "65Tb/s transoceanic transmission using probabilistically-shaped PDM-64QAM". In: *ECOC 2016-Post Deadline Paper; 42nd European Conference on Optical Communication*. VDE. 2016, pp. 1–3 (cit. on p. 17).

[17] Tobias Fehenberger, Helmut Griesser, and Jörg-Peter Elbers. "Mitigating fiber nonlinearities by short-length probabilistic shaping". In: *Optical Fiber Communication Conference*. Optical Society of America. 2020, Th1I–2 (cit. on p. 17).

[18] Fabian Steiner, Patrick Schulte, and Georg Böcherer. "Blind decoding-metric estimation for probabilistic shaping via expectation maximization". In: *2018 European Conference on Optical Communication (ECOC)*. IEEE. 2018, pp. 1–3 (cit. on p. 17).

[19] Alexandre Graell i Amat and Raphaël Le Bidan. "Rate-compatible serially concatenated codes with outer extended BCH codes". In: *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*. IEEE. 2007, pp. 1476–1481 (cit. on p. 17).

[20] Alexandre Graell i Amat, Charbel Abdel Nour, and Catherine Douillard. "Serially concatenated continuous phase modulation with extended BCH codes". In: *2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks*. IEEE. 2007, pp. 1–5 (cit. on p. 17).

[21] Ahmed Abdmouleh, Emmanuel Boutillon, Laura Conde-Canencia, Charbel Abdel Nour, and Catherine Douillard. "A new approach to optimise Non-Binary LDPC codes for coded modulations". In: *2016 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC)*. 2016, pp. 295–299. DOI: 10.1109/ISTC.2016.7593124 (cit. on pp. 17, 57).

[22] Charly Poulliat, Marc Fossorier, and David Declercq. "Design of regular (2, d/sub c/)-LDPC codes over GF (q) using their binary images". In: *IEEE Transactions on Communications* 56.10 (2008), pp. 1626–1635 (cit. on pp. 17, 57, 76).

[23] Sima Naseri. "Error Floor Analysis of Quasi-Cyclic LDPC and Spatially Coupled-LDPC Codes and Construction of Codes with Low Error Floor". PhD thesis. Carleton University, 2021 (cit. on p. 17).

[24] Christian Häger, Alexandre Graell i Amat, Fredrik Brännström, Alex Alvarado, and Erik Agrell. "Terminated and tailbiting spatially coupled codes with optimized bit mappings for spectrally efficient fiber-optical systems". In: *Journal of Lightwave Technology* 33.7 (2015), pp. 1275–1285 (cit. on p. 17).

[25] Laurent Schmalen, Detlef Suikat, Detlef Rösener, Vahid Aref, Andreas Leven, and Stephan ten Brink. "Spatially coupled codes and optical fiber communications: An ideal match?" In: *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE. 2015, pp. 460–464 (cit. on p. 17).

[26] Alexandre Graell i Amat, Christian Häger, Fredrik Brännström, and Erik Agrell. "Spatially-coupled codes for optical communications: state-of-the-art and open problems". In: *2015 Opto-Electronics and Communications Conference (OECC)*. IEEE. 2015, pp. 1–3 (cit. on p. 17).

[27] Laurent Schmalen, Detlef Suikat, Detlef Rösener, and Andreas Leven. "Evaluation of left-terminated spatially coupled LDPC codes for optical communications". In: *2014 The European Conference on Optical Communication (ECOC)*. IEEE. 2014, pp. 1–3 (cit. on p. 17).

[28] Laurent Schmalen, Detlef Suikat, Vahid Aref, and Detlef Roesener. "On the design of capacity-approaching unit-memory spatially coupled LDPC codes for optical communications". In: *ECOC 2016; 42nd European Conference on Optical Communication*. VDE. 2016, pp. 1–3 (cit. on p. 17).

[29] Laurent Schmalen, Stephan ten Brink, and Andreas Leven. "Advances in detection and error correction for coherent optical communications: Regular, irregular, and spatially coupled LDPC code designs". In: *arXiv preprint arXiv:1704.04618* (2017) (cit. on p. 17).

[30] Yohei Koganei, Tomofumi Oyama, Kiichi Sugitani, Hisao Nakashima, and Takeshi Hoshida. "Multilevel coding with spatially coupled repeat-accumulate codes for high-order QAM optical transmission". In: *Journal of Lightwave Technology* 37.2 (2019), pp. 486–492 (cit. on p. 17).

[31] Xiaole Sun and Ivan B Djordjevic. "FPGA implementation of rate-adaptive spatially coupled LDPC codes suitable for optical communications". In: *Optics express* 27.3 (2019), pp. 3422–3428 (cit. on p. 17).

[32] E. Zehavi. "8-PSK trellis codes for a Rayleigh channel". In: *IEEE Transactions on Communications* 40.5 (May 1992), pp. 873–884. ISSN: 0090-6778. DOI: 10.1109/26.141453 (cit. on pp. 18, 48).

[33] Laurent Schmalen, Alex Alvarado, and Rafael Rios-Müller. "Performance prediction of nonbinary forward error correction in optical transmission experiments". In: *Journal of Lightwave Technology* 35.4 (2016), pp. 1015–1027 (cit. on pp. 18, 46, 57).

[34] Robert G. Gallager. *Low-Density Parity-Check Codes*. 1963 (cit. on pp. 18, 29, 30, 35, 57, 58, 61, 62).

[35] M. C. Davey and D. MacKay. "Low-density parity check codes over GF(q)". In: *IEEE Communications Letters* 2.6 (June 1998), pp. 165–167. ISSN: 1089-7798. DOI: 10.1109/4234.681360 (cit. on pp. 18, 32, 57).

[36] Murat Arabaci, Ivan B. Djordjevic, Ross Saunders, and Roberto M. Marcoccia. "Polarization-multiplexed rate-adaptive non-binary-quasi-cyclic-LDPC-coded multilevel modulation with coherent detection for optical transport networks". In: *Opt. Express* 18.3 (Feb. 2010), pp. 1820–1832. DOI: 10.1364/OE.18.001820. URL: http://www.opticsexpress.org/abstract.cfm?URI=oe-18-3-1820 (cit. on pp. 18, 57).

[37] Ivan B Djordjevic and Murat Arabaci. "LDPC-coded orbital angular momentum (OAM) modulation for free-space optical communication". In: *Optics express* 18.24 (2010), pp. 24722–24728 (cit. on pp. 18, 57).

[38] Tom Richardson and Ruediger Urbanke. *Modern coding theory*. Cambridge university press, 2008 (cit. on pp. 18, 26, 29, 32, 34, 81).

State of the art

This chapter introduces all basic notions needed for reading of next chapters. In particular it revises communication chain, channel model and non-binary LDPC codes that will be mentioned through all the document, as well as some fundamental analysis tools for graph-based codes.

2.1 Important notions from the digital communication theory

Let us start with a brief introduction of notions from digital communications.

2.1.1 Communication chain with an AWGN channel

All the results, further introduced in this manuscript, are developed in the framework of the communication scheme depicted in Figure 2.1.
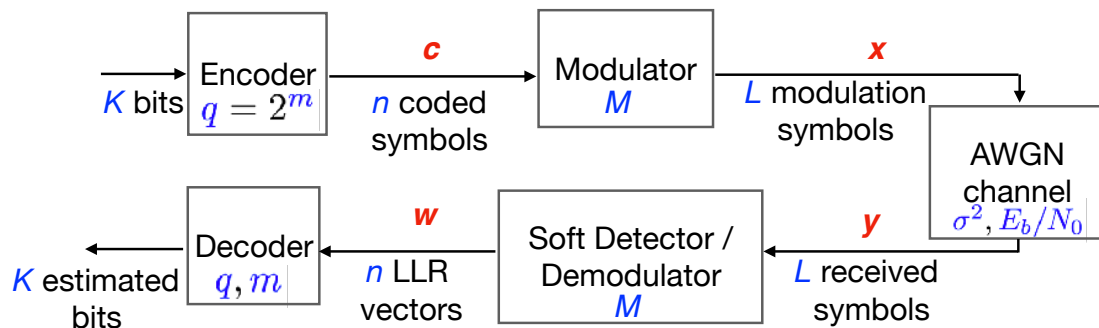

Figure 2.1: AWGN Communication chain.

Let us describe the communication chain step by step. For simplicity of explanation,

let us assume the use of binary error-correcting codes. Starting from a message **m** (where **m** is a binary vector of length K, **m** $= (m_1, \ldots, m_K)$, $m_i \in \{0,1\}$), the encoder generates a codeword **c** of symbol code-length n (binary length N) **c** $= (c_1, \ldots, c_n)$, $c_i \in GF(q)$. Code symbols are mapped to modulation symbols: each subpacket of L bits (L is the modulation symbol size in bits, it depends on N and the modulation symbol size M, $L = \frac{N}{\log_2 M}$) is mapped to one modulation symbol. Thus, the modulator outputs a vector **x** $= (x_1, \ldots, x_L)$, defined over the modulation alphabet $\mathcal{A} = (a_1, .., a_M)$ with $a_i \in \mathbb{R}^2$, which implies that $x_i \in \mathcal{A}$. The modulation mapping usually belongs to the class of Gray labeling [39]. The obtained modulation symbols are further sent through the Additive White Gaussian Noise (AWGN) channel. Therefore, if the output vector of the AWGN channel is denoted by **y** $= (y_1, \ldots, y_L)$, each symbol y_i from this vector belongs to $\mathbb{R}^2$ and it is expressed as [40]

$$y_i = x_i + \eta. \tag{2.1}$$

where In the equation above, $\eta \sim \mathcal{N}(0, \sigma^2 I^2)$ is the uncorrelated AWGN noise of zero mean and of variance σ^2, $\sigma \in \mathbb{R}_+$.

Ⓡ Remark 1: The communication scheme, described above, is the one based on M-ary modulation and binary codes. It will further be extended to non-binary coding schemes and will give rise to the SICM model (see Section 3.2).

Ⓡ Remark 2: Note that there exist several channel models to describe the optical channel transmission, like 2x2 MIMO AWGN model [41]. However if the optical system operates in a linear amplification regime its functioning is well approximated by the classical Gaussian model (2.1). Moreover it was argued in [42] that one can transform an efficient coded modulation scheme over the AWGN channel into the one over the AWGN channel with the polarization dependent rate loss.

Ⓡ Remark 3: For simplicity of analysis, some theoretical results of this work will be derived while assuming the transmission over the Binary Erasure Channel (BEC). In the BEC model, bit can either be correctly received, with probability $1-p$, or erased with probability p (Fig. 2.2). In the BEC communication chain, the modulator function is the equality function, thus both modulator and demodulator may be omitted. An important observation to note from [38] is the following: if a family of graph-based codes show good performance over the BEC, it will also have a good performance over the AWGN channel, as these both channel models belong to the same class of discrete memoryless input symmetric channels.
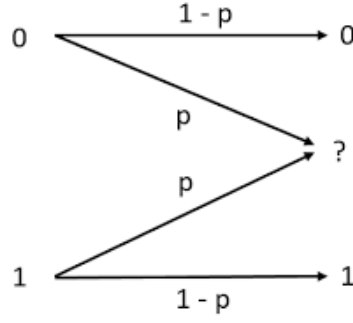
Figure 2.2: BEC model.

2.1.2 Modulation

In this work, we mainly use M-ary ($M \in \mathbb{N}^*$) Quadrature Amplitude Modulation (QAM).
Let us define the QAM in a more formal way.

Definition 2.1.1 — Pulse-Amplitude Modulation (PAM) [40]. Pulse amplitude modulation (PAM) is the transmission of data by varying the amplitude of a series of signal pulses, in a regularly timed sequence.

Definition 2.1.2 — Gray labeling [39]. Gray labeling is an ordering of the binary numeral system such that two successive values differ in only one bit.

Definition 2.1.3 — Quadrature Amplitude Modulation (QAM) [43]. QAM is a signal in which two carriers shifted in phase by 90 degrees (i.e. sine and cosine) are modulated and combined.

The resulting QAM signal consisting of the combination of both carriers contains of both amplitude and phase variations. In view of the fact that both amplitude and phase variations are present it may also be considered as a mixture of amplitude and phase modulation.

It is to note that a M-ary QAM can be seen as a combination of two P-ary PAMs. If a Gray labeling is used for each of the P-PAM modulations, then the obtained M-QAM symbols are also labeled by Grey labeling. The reader is referred to Chapter 3 for an example (Figure 3.1).

2.1.3 Soft detection and demodulation

Once the signal **y** is received at the output of the AWGN channel, there is a Maximum A Posteriori (MAP) detection phase that allows to estimate which modulation symbol has been sent.

Two types of detectors are possible in the optical communication scheme: hard detector and soft detector. For each received symbol y from **y**, a hard detector outputs symbols the most likely modulation symbol $a \in \mathcal{A}$ while soft detectors outputs a vector of probabilities or Log-Likelihood Ratios (LLR), for all possible values of a from $\mathcal{A}$. In what follows, the soft detection strategy will be used. Therefore, we will be using the LLR notation. Let us define it below.

> **Definition 2.1.4 — Log-Likelihood Ratio (LLR) over modulation symbols.** Given
> the modulation alphabet $\mathcal{A} = \{a_1, \ldots, a_M\}$ with $a_1 = 0$ and a received symbol y_i
> $(1 \leq i \leq L)$, the Log-Likelihood Ratio is a vector
>
> $$L(y_i) \triangleq \{L_1(y_i), L_2(y_i), \ldots, L_{M-1}(y_i)\},$$
>
> where
>
> $$L_j(y_i) = \log\left(\frac{P(a_j|y_i)}{P(a_1|y_i)}\right), \tag{2.2}$$
>
> for $2 \leq j \leq M$.

Let us come back to the communication chain in Figure 2.1. Given the received
vector $\mathbf{y} = (y_1, \ldots, y_L)$ and taking into account the definition above, the soft detector
outputs a matrix $\mathbf{v}$ of size $L \times (M-1)$, the (i,j)-th element of it being a LLR estimation
$L_j(y_i)$. Futhermore, the soft demodulator in Figure 2.1 outputs a vector $\mathbf{v'}$ of length N,
$\mathbf{v'} = (v_1', \ldots, v_N')$, where the i-th element v_i' of the vector is a LLR estimate of the i-th
coded bit u_i, defined below.

> **Definition 2.1.5 — Log-Likelihood Ratio (LLR) over coded bits.** Given a codeword
> $\mathbf{u}$ and its associated received vector $\mathbf{y}$, the Log-Likelihood Ratio is a coded bit u_i is
> defined as
>
> $$L(u_i|\mathbf{y}) = \log\left(\frac{P(u_i = 1|\mathbf{y})}{P(u_i = 0|\mathbf{y})}\right), \tag{2.3}$$
>
> for $1 \leq i \leq N$.

Note that there exist a following link between $L_j(y_k)$ and $L(u_i|\mathbf{y})$:

Proposition 2.1.1 Assume a binary codeword $\mathbf{u}$ of length N and a costellation $\mathcal{A} = \{a_1, \ldots, a_M\}$ of modulation symbols. Let $j = \lfloor \frac{i-1}{\log_2 M} \rfloor + 1$ and $k = i - (j-1)\log_2 M$.
Denote by $\mathcal{R}_0$ (resp. $\mathcal{R}_1$) the subset of symbols a_i from $\mathcal{A}$ such that their k-th label bit
equals to 0 (resp. to 1). Then,

$$L(u_i|\mathbf{y}) = \log \frac{\sum_{a_\ell \in \mathcal{R}_1} e^{L_\ell(y_j)}}{\sum_{a_s \in \mathcal{R}_0} e^{L_s(y_j)}}, \quad \text{for } 1 \leq i \leq N. \tag{2.4}$$

Moreover, the following useful result also holds:

Proposition 2.1.2 Given a binary codeword $\mathbf{u}$ of length N and a costellation $\mathcal{A}$ of equiprobable QAM symbols, assume the transmission over an AWGN channel of channel variance
σ^2. Let $\mathbf{y} = (y_1, \ldots, y_L)$ be the received vector, associated to the transmission of u. Then,
the LLR estimate $L(u_i|\mathbf{y})$ for $1 \leq i \leq N$ is computed as

$$\begin{aligned} L(u_i|\mathbf{y}) = \quad & \log\left(\sum_{a_\ell \in \mathcal{R}_1} e^{-\frac{1}{2\sigma^2}\left((Re(y_j)-Re(a_\ell))^2 - (Im(y_j)-Im(a_\ell))^2\right)}\right) \\ & - \log\left(\sum_{a_k \in \mathcal{R}_0} e^{-\frac{1}{2\sigma^2}\left((Re(y_j)-Re(a_k))^2 - (Im(y_j)-Im(a_k))^2\right)}\right), \end{aligned} \tag{2.5}$$

where $j = \lfloor \frac{i-1}{\log_2 M} \rfloor + 1$, $\mathcal{R}_0$ (resp. $\mathcal{R}_1$) is the set of symbols a_i from $\mathcal{A}$ such that their j-th
label bit equals to 0 (resp. to 1). $Re(\cdot)$ and $Im(\cdot)$ denote real and imaginary parts of a
symbol.

2.2 Notions from the coding theory

The decoder operation in Figure 2.1 depends on the type of the error-correcting code used during the transmission. In what follows, let us define some notions from the coding theory. They will further be used in order to define the class of Low-Density Parity-Check (LDPC) codes and their iterative decoding algorithm. Thus, in this work, the decoder in Figure 2.1 is considered to be an iterative decoder, that outputs the estimated message $\mathbf{m}'$ of binary length K given LLR estimates of coded bits in the codeword $\mathbf{u}$.

> **Definition 2.2.1 — Code [38].** A code $\mathcal{C}$ of length n and cardinality F over a field $GF(q) \in \{0, 1, ..., q-1\}$ is a collection of F elements from $\mathbb{F}^n$, i.e.,
>
> $$\mathcal{C}(n, F) = \{x^{[1]}, \ldots, x^{[F]}\}, x^{[F]} \in \mathbb{F}^n, 1 \le f \le F. \tag{2.6}$$

The elements of the code are called codewords. The parameter n is called the block-length of the code. In case when $q = 2^m$, one has $n = \frac{N}{m}$, where N is the binary codelength of the code.

> **Definition 2.2.2 — Linear code.** A code $\mathcal{C}$ is a linear code if a linear combination over GF(q) of any two codewords remains a codeword:
>
> $$\forall x_1, x_2 \in \mathcal{C}, \forall \alpha_1, \alpha_2 \in \mathbb{F}^n : \alpha_1 x_1 + \alpha_2 x_2 \in \mathcal{C} \tag{2.7}$$

A linear code $\mathcal{C}$ can be described by a parity-check matrix.

The focus of our work is a class of codes called Low-Density-Parity-Check (LDPC) codes, introduced by Gallager [34] during his thesis in Massachusetts Institute of Technology in 1963:

> **Definition 2.2.3 — Low-Density-Parity-Check (LDPC) codes [34].** LDPC codes are codes having a sparse parity-check matrix H, when the number of non-zero elements in H per row/column is upper bounded by a constant.

2.2.1 Tanner graph representation of H

A parity check matrix H can also be represented by a bipartite graph, as it has been first pointed out by Tanner [44].

The rows of the parity check matrix correspond to variable nodes (VN) of the Tanner graph, and the columns to the check nodes (CN). Each non-zero element of the matrix corresponds to an edge connecting the i-th variable node with a j-th check node.

■ **Example 2.1** As an example, a parity check matrix is given below on the left, and its associated Tanner graph on the right.

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Tanner Graph

■
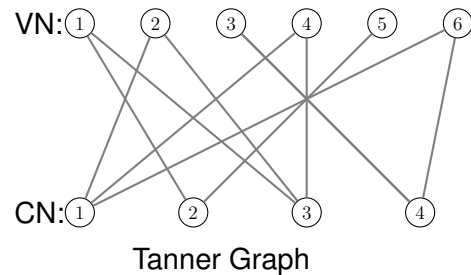
In the q-ary case, the non-zero elements of the matrix are labeled by a mapping f, $f : GF(q) \rightarrow GF(q)$, f is an $m \times m$ invertible matrix ($m = log_2(q)$, $m \in \mathbb{N}^*$), and the zero elements are all zero matrix, for the Ensemble over the General Linear group (EGL). Also, f can be defined as $f(x) = \omega x$, where $\omega \in GF(q) \setminus \{0\}$, for the Ensembles over Finite Field (EGF).

■ **Example 2.2** Here is an example of the Tanner graph representation in the EGF q-ary case.

$$H = \begin{pmatrix} 0 & f_2 & f_1 & 0 \\ f_1 & 0 & f_4 & 0 \\ 0 & 0 & 0 & f_1 \\ f_4 & 0 & f_3 & 0 \\ 0 & f_3 & 0 & 0 \\ f_2 & 0 & 0 & f_4 \end{pmatrix}$$
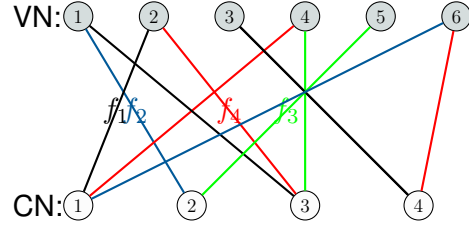

■

Definition 2.2.4 — Regular and irregular code. One says that a code is (a, d) regular if:
   • each column of its parity check matrix H contains exactly a non-zero elements, and
   • each row contains d nonzero elements.
Otherwise the code is said to be irregular.

2.2.2   Decoding for LDPC codes for transmission over the AWGN channel

In order to decode the received message, one need to use a decoding algorithm. An optimal decoding algorithm is the Maximum-Likelihood decoding algorithm defined below by using the notatoin from Figure 2.1.

Definition 2.2.5 — Maximum-Likelihood (ML) [45]. Consider a transmission over a noisy channel. Let **U** be a random vector on its input and let **V'** be a random vector on its output. We assume that **V'** depends on **U** via a conditional probability density function $P_{\mathbf{U}|\mathbf{V'}}(\mathbf{u}|\mathbf{v'})$. Given a received vector $\mathbf{v'} = (v'_0, \ldots, v'_{N-1})$, the most likely transmitted codeword is the one that maximizes $P_{\mathbf{U}|\mathbf{V'}}(\mathbf{u}|\mathbf{v'})$. If the channel is memoryless and each of the codewords are equally likely, then this reduces to the codeword $\mathbf{u} = (u_0, \ldots, u_{N-1})$ which maximizes $P_{\mathbf{V'}|\mathbf{U}}(\mathbf{v'}|\mathbf{u})$. This is known as maximum likelihood (ML) estimate of the transmitted codeword and is written as follows

$$\mathbf{m'} = \hat{\mathbf{u}} = \arg \max_{\mathbf{u} \in C} P_{\mathbf{V'}|\mathbf{U}}(\mathbf{v'}|\mathbf{u}).$$

When the message is encoded using a LDPC code, a suboptimal yet low-complexity **iterative decoding** algorithm is used. Among all possible version of iterative decoding, let us cite message passing decoding [34], sum product decoding [46] or belief propagation (BP) decoding [47]. In what follows, let us assume the use of the LLR-based sum product decoding algorithm, as it is adapted to the decoding while the transmission takes place over the AWGN channel. The sum-product algorithm is detailedly described in Algorithm 1) below.

input : **r** - LLR values of coded symbols, (after demodulation),
$\qquad$ $\mathbf{r} = (r_1, ..., r_N), r_i \in \mathbb{R}$
$\qquad$ G - Tanner graph with VNs and CNs, associated with H
$\qquad$ I_{max} - maximal number of iterations
output : **L** - output LLR vector of coded symbols $\mathbf{L} = (L_1, ..., L_N), L_i \in \mathbb{R}$
$\qquad$ **m**' - hard decisions on coded symbols

```
/* I - the iteration step, I ∈ {0,...,Imax}                    */
```
1 I = 0;
```
/* N - binary codelength                                       */
```
2 **for** *i=1:N* **do**
```
   /* μ - number of nodes at check node side              */
```
3 $\quad$ **for** *j=1:μ* **do**
```
      /* Int - the intrinsic matrix is initialized with channel
         informations                                          */
```
4 $\quad\quad$ $Int_{j,i} = r_i$
5 $\quad$ **end**
6 **end**
7 **while** $I < I_{max}$ **and** $convergence(Int) \neq 1$ **do**
```
   /* Passing LLRs from CNs to VNs                             */
```
8 $\quad$ **for** *j=1:μ* **do**
```
      /* B_j is the set of VN connected to the CN j.         */
```
9 $\quad\quad$ **for** $i \in B_j$ **do**
```
         /* Ext - the extrinsic matrix                       */
         /* the indexes j,i under Int and Ext refers to the edge
            between the CN j and the VN i.                     */
```
10 $\quad\quad\quad$ $Ext_{j,i} = \log\left(\dfrac{1 + \Pi_{i' \in B_j, i' \neq i} \tanh\left(\frac{Int_{j,i'}}{2}\right)}{1 - \Pi_{i' \in B_j, i' \neq i} \tanh\left(\frac{Int_{j,i'}}{2}\right)}\right)$
11 $\quad\quad$ **end**
12 $\quad$ **end**
```
   /* Passing LLRs from VNs to CNs                             */
```
13 $\quad$ **for** *i=1:N* **do**
```
      /* A_i is the set of CN connected to the VN i.          */
```
14 $\quad\quad$ **for** $j \in A_i$ **do**
15 $\quad\quad\quad$ $Int_{j,i} = \sum_{j' \in A_i, j' \neq j} Ext_{j',i} + r_i$;
16 $\quad\quad$ **end**
17 $\quad$ **end**
18 $\quad$ I = I+1;
19 **end**
20 **for** *i=1:N* **do**
```
   /* L is the final LLR, it provides a soft output            */
```
21 $\quad$ $L_i = \sum_{j \in A_i} Ext_{j,i} + r_i$
22 **end**
```
/* Hard decision output                                        */
```
23 **if** $L_i > 0$ **then**
24 $\quad$ $m'_i = 0$
25 **end**
26 **else**
27 $\quad$ $m'_i = 1$
28 **end**

Algorithm 1: Sum product algorithm for decoding a binary LDPC code.

Let us describe some main steps of Algorithm 1. It takes as input a vector **r** which is the vector of LLRs obtained after the demodulation operation. It also serves of the structure of the associated Tanner graph of the code (or equivalently of the structure of H). I_{max} is the parameter that denotes the maximum number of iterations. The algorithm is based on two main operations:

1. Extrinsic message calculation: calculation of LLR messages sent from CNs to VNs, using the single-parity check structure associated to CNs;
2. Intrinsic message calculation: calculation of LLR messages sent from VNs to CNs, using the repetition structure associated to VNs as well as input LLRs values of the algorithm.

Both operations above are repeated alternatively until a maximal number of iteration I_{max} or the algorithm convergence is achieved. At the final step, the algorithm provides a soft LLR decision $L(b_i|\mathbf{y})$ for each bit of in the codeword. Out of the soft decision, a hard decision value for each bit might be obtained as:

$$m'_i = \left\{ \begin{array}{ll} 1, & L(b_i|\mathbf{y} \leq 0 \\ 0, & L(b_i|\mathbf{y} > 0 \end{array} \right. \tag{2.8}$$

> **R** The decoding algorithm above is defined for binary LDPC codes for the simplicity of explanation. Its extension to NB-LDPC codes is given in [35]. We will constantly use it in further sections.

2.2.3 Non binary LDPC ensembles

In this work, a focus is made on the average performance of a code ensemble. The reason for this is that it is much easier to design an efficient LDPC or LDPC-like code ensemble with a concentration property and to pick at random a code from the ensemble [38], than to design an efficient code by itself.

Let us define such a code ensemble for NB-LDPC codes, which will be our codes of interest. NB-LDPC codes were already proposed by Gallager in his PhD thesis. In 1998, Davey and MacKay [35] have shown that NB-LDPC codes achieve superior performance than the binary codes for binary symmetric channel and binary Gaussian channel.

> **Definition 2.2.6 — Regular NB-LDPC ensemble over the general linear group.** An ensemble of (a, d)-regular NB-LDPC codes of binary codelength N is defined over the finite field of cardinality $q = 2^m$ and is further denoted by $\mathcal{C}_{LDPC}(a, d, m, n)$. A code from this ensemble has a Tanner graph representation with $n = \frac{N}{q}$ variable nodes of degree a and a number r of check nodes of degree d. Each edge of the graph is labeled by a bijective linear mapping $f : GF(q) \to GF(q)$. The code ensemble of our consideration is in one-to-one correspondence to the ensemble of Tanner graphs, obtained over all possible invertible matrices and over all possible edge labels.

2.3 Analysis tools for NB-LDPC ensembles

In this section, the analysis tools that are used in this work are presented. Density Evolution (DE) analysis [48] is used in the limit of large codelenghts (asymptotic regime). Moreover, the minimum distance and asymptotic growth rate analysis are our main tools for finite codelengths.

2.3.1 Asymptotic analysis: density evolution

Consider the ensemble $\mathcal{C}_{LDPC}(a, d, m, n)$ in the limit of large codelengths $n \to \infty$ and denote it by $\mathcal{C}_{LDPC}(a, d, m)$. Also, let the average bit error rate after iterative decoding be denoted as $P_b^{\mathcal{C}(a,d,m)}$. The main parameter of $\mathcal{C}_{LDPC}(a, d, m)$ ensemble in the asymptotic regime is an *asymptotic iterative threshold*. The definition of the threshold might differ from one communication model to another. Let us give the most popular definitions for the BEC and the AWGN models.

> **Definition 2.3.1 — Asymptotic threshold over BEC [48].** Consider $\mathcal{C}_{LDPC}(a, d, m)$ over the BEC with erasure probability ε. Then the asymptotic iterative threshold ε^* is the *lowest* value of ε such that $P_b^{\mathcal{C}(a,d,m)} > 0$.

> **Definition 2.3.2 — Asymptotic iterative threshold over the AWGN channel [49, 50].** Consider $\mathcal{C}_{LDPC}(a, d, m)$ over the AWGN with signal-to-noise ratio $\frac{E_b}{N_0}$, in decibels (dB). Then the asymptotic iterative threshold $\left(\frac{E_b}{N_0}\right)^*$ is defined as the *highest* value of $\frac{E_b}{N_0}$ such that $P_b^{\mathcal{C}(a,d,m)} > 0$.

The value of the asymptotic threshold for the $\mathcal{C}_{LDPC}(a, d, m)$ ensemble has been first derived in [48], in case of the BEC, with the help of the so called density evolution approach. Let us detail it below.

> **Definition 2.3.3 — Density evolution over the BEC and ε^* [48].** Assume transmission over the BEC of probability ε. Let E be the probability vector of length $m + 1$ (m is the number of bits in a code symbol of cardinality q, $m = log_2(q)$, $m \in \mathbb{N}^*$) corresponding to channel input messages, the i-th element of which is
>
> $$E(i) \triangleq \binom{m}{i} \varepsilon^i (1 - \varepsilon)^{m-i}, \quad i = 0 \ldots m.$$
>
> Let $x^{(\ell)}$ and $y^{(\ell)}$ be probability vectors of length $m+1$, each of them associated with decoding messages of particular type at decoding iteration ℓ. Then the density evolution is defined by
>
> $$\begin{cases} x^{(\ell)} \triangleq & E \boxdot \left(\boxdot^{c-1} y^{(\ell-1)}\right) \\ y^{(\ell)} \triangleq & \boxtimes^{d-1} x^{(\ell)} \end{cases} \tag{2.9}$$
>
> where $y^{(0)} = (0, \ldots, 0, 1)$ and the upperscript k at $\boxdot^e$ or $\boxtimes^e$ denotes the recursive application of the corresponding operation e times. For two probability vectors a and b of length $m + 1$, the operations $a \boxdot b$ and $a \boxtimes b$ are defined as
>
> $$a \boxdot^k b \triangleq \sum_{i=k}^{m} \sum_{j=k}^{m+k-i} \frac{G_{i,k} G_{m-i,j-k} 2^{(i-k)(j-k)}}{G_{m,j}} \tag{2.10}$$
>
> $$a \boxtimes^k b \triangleq \sum_{i=0}^{k} \sum_{j=k-i}^{k} \frac{G_{m-i,m-k} G_{i,k-j} 2^{(k-i)(k-j)}}{G_{m,m-j}}, \tag{2.11}$$
>
> where $k = 0, ..., m$ and $G_{m,k}$ is the Gaussian binomial coefficient,

$$G_{m,k} = \begin{bmatrix} m \\ k \end{bmatrix} = \begin{cases} 1, & \text{if } k = m \text{ or } k = 0 \\ \Pi_{l=0}^{k-1} \frac{2^m - 2^l}{2^k - 2^l}, & \text{if } 0 < k < m \\ 0, & \text{otherwise} \end{cases} \qquad (2.12)$$

which gives the number of different subspaces of dimension k of GF(2^m).

Finally, given (5.6), the asymptotic decoding threshold of the $\mathcal{C}_{LDPC}(a,d,m)$ ensemble is the lowest value of ε such that $x^{(\infty)}(0) < 1$.

> **R**   Note that DE can also be performed over the AWGN channel by an approximation, obtained with Monte-Carlo density evolution [51–53]. Where Monte-Carlo method is used to simulate an infinite LDPC code in order to investigate the properties of the decoding algorithm.

2.3.2   Finite-length analysis: minimum distance and asymptotic growth rate calculation

Consider a NB-LDPC ensemble of some finite-length n. The bit error probability of a code from the ensemble is usually approximated by the average bit error probability of the ensemble $P_b^{\mathcal{C}_{LDPC}(a,d,m,n)}$, which in its turn, is lower bounded by the bit error probability $P_{b,ML}$ under Maximum-Likelihood (defined on definition 2.2.5) decoding. In the case of the transmission over the AWGN, upper and lower bounds on the ML decoding probability were presented by Sason and Shamai [54], where the authors derive a Gallager-like upper bound on the decoding error probability under ML decoding. These work has been followed by a multitude of results derived under different code/transmission models. For binary LDPC codes, the most recent papers refer to bounds for decoding over the BEC [55] and the BSC [56] Nonbinary regular LDPC codes and AWGN channel are addressed in [57].

It is to note that all the aforementioned bounds heavily depend on the average weight distribution of the considered code ensemble. Let us give some important definitions below and explain what weight properties a NB-LDPC code ensemble should have in order to have good decoding performance and is able to attain very low bit error rates in the optical communication setting. First, let us start with the Hamming distance, defined by Richard Hamming in the fifties.

> **Definition 2.3.4 — Hamming weight (distance) [38].** The Hamming weight (distance) $d(u,v)$ of a pair of vectors (u,v) with the elements in $GF(q)$ is the number of positions in which u differs from v.

> **Definition 2.3.5 — Minimum distance [38].** The minimum distance d_{min} of a code C is defined as
> $$d_{min} = \min\{d(u,v) : u,v \in C, u \neq v\}.$$
> With some abuse of notation one also denotes by d_{min} the average Hamming minimum distance of some code ensemble $\mathcal{C}$.

Given the average minimum Hamming distance of a non-binary LDPC ensemble $\mathcal{C}$, one can lower bound its average ML decoding probability and thus the desired error probability $P_b^{\mathcal{C}_{LDPC}(a,d,m,n)}$. In particular, for erasure channels of erasure probability ε one

can conclude from [55] that

$$P_b^{\mathcal{C}_{LDPC}(a,d,m,n)} \leq O(\varepsilon^{d_{min}}),$$

as well as, for binary-input memoryless symmetric channels [58]

$$P_b^{\mathcal{C}_{LDPC}(a,d,m,n)} \leq O(D^{d_{min}}),$$

where $D = \sum_y \sqrt{P(y|0)P(y|1)}$ is a Bhattacharyya channel parameter. As for the bounds developed in the AWGN case, their expressions can be found in [59] and [60].

Given the bounds above and the fact that, for optical communications, one desires to use code ensembles able to achieve extremely low BERs, a special focus should be given to *asymptotically good* code ensembles, i.e., code ensembles whose minimum distance grows linearly in the codelength n. Note that the estimation of d_{min} properties of NB-LDPC is well studied in the state of the art. For regular NB-LDPC codes with $a > 2$, it is known from [34] that d_{min} grows linearly with n. Moreover, NB-LDPC codes with $a = 2$ have logarithmically growing minimum distance.

(R) The weight distribution of a NB-LDPC can be defined symbolwise as above and in [61], or bitwise, see [62] for instance. As both symbol Hamming minimum distance and binary Hamming minimum distance of an ensemble have the same growth with respect to the codelength n, the two approaches are equivalent for our purposes. In what follows, the symbol minimum distance is considered.

In order to estimate whether the d_{min} growth is linear, a possible approach is to use the *asymptotic growth rate* of the $\mathcal{C}(a, d, m)$ ensemble [61, 63]. Let us define it here for further use.

Definition 2.3.6 — Asymptotic growth rate. The growth rate of the $\mathcal{C}_{LDPC}(a, d, m, n)$ ensemble is defined as

$$G_m(\omega) \triangleq \lim_{n \to \infty} \frac{1}{n} \log A_{\lfloor n\omega \rfloor}, \quad 0 < \omega < 1,$$

where $\bar{A}_t$ is the average number of codewords of Hamming weight t in the ensemble, $0 \leq t \leq n$.

Bibliography

[39] Gray Frank. *Pulse code communication*. US Patent 2,632,058. 1953 (cit. on pp. 26, 27).

[40] Amos Lapidoth. *A foundation in digital communication*. Cambridge University Press, 2017 (cit. on pp. 26, 27).

[41] Arnaud Dumenil, Elie Awwad, and Cyril Measson. "Rate optimization using SO (4) transforms for PDL mitigation". In: *45th European Conference on Optical Communication (ECOC 2019)*. IET. 2019, pp. 1–4 (cit. on p. 26).

[42] Arnaud Dumenil, Elie Awwad, and Cyril Méasson. "Polarization dependent loss: Fundamental limits and how to approach them". In: *Signal Processing in Photonic Communications*. Optical Society of America. 2017, SpM4F–1 (cit. on p. 26).

[43] C Campopiano and B Glazer. "A coherent digital amplitude and phase modulation scheme". In: *IRE Transactions on Communications Systems* 10.1 (1962), pp. 90–95 (cit. on p. 27).

[44] R. Tanner. "A recursive approach to low complexity codes". In: *IEEE Transactions on Information Theory* 27.5 (Sept. 1981), pp. 533–547. ISSN: 0018-9448. DOI: 10.1109/TIT.1981.1056404 (cit. on p. 29).

[45] Iryna Andriyanova. "Analysis and design of a certain family of graphbased codes: TLDPC codes". PhD thesis. PhD thesis, National Superior School of Telecommunications, Paris, France, 2006 (cit. on pp. 30, 81).

[46] Frank R Kschischang, Brendan J Frey, and H-A Loeliger. "Factor graphs and the sum-product algorithm". In: *IEEE Transactions on information theory* 47.2 (2001), pp. 498–519 (cit. on p. 30).

[47] Robert J. McEliece, David J. C. MacKay, and Jung-Fu Cheng. "Turbo decoding as an instance of Pearl's" belief propagation" algorithm". In: *IEEE Journal on selected areas in communications* 16.2 (1998), pp. 140–152 (cit. on p. 30).

[48] Vishwambhar Rathi and Rüdiger L. Urbanke. "Density Evolution, Thresholds and the Stability Condition for Non-binary LDPC Codes". In: *CoRR* abs/cs/0511100 (2005). arXiv: cs/0511100. URL: http://arxiv.org/abs/cs/0511100 (cit. on pp. 32, 33, 57).

[49] G. Li, I. J. Fair, and W. A. Krzymien. "Density Evolution for Nonbinary LDPC Codes Under Gaussian Approximation". In: *IEEE Transactions on Information Theory* 55.3 (2009), pp. 997–1015 (cit. on p. 33).

[50] A. Bennatan and D. Burshtein. "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels". In: *IEEE Transactions on Information Theory* 52.2 (Feb. 2006), pp. 549–583. ISSN: 0018-9448. DOI: 10.1109/TIT.2005.862080 (cit. on p. 33).

[51] M.C. Davey. "Error-correction using Low-Density Parity-Check Codes". PhD thesis. University of Cambridge, 1999 (cit. on pp. 34, 61).

[52] M. Gorgoglione, V. Savin, and D. Declercq. "Optimized puncturing distributions for irregular non-binary LDPC codes". In: *IEEE International Symposium on Information Theory and Applications (ISITA)*. Taichung, Taiwan, Oct. 2010 (cit. on pp. 34, 61).

[53] Matthew C Davey and David JC MacKay. "Monte Carlo simulations of infinite low density parity check codes over GF (q)". In: *Proc. of Int. Workshop on Optimal Codes and related Topics*. Citeseer. 1998, pp. 9–15 (cit. on pp. 34, 61).

[54] E. Hof, I. Sason, and S. Shamai. "Performance Bounds for Nonbinary Linear Block Codes Over Memoryless Symmetric Channels". In: *IEEE Transactions on Information Theory* 55.3 (2009), pp. 977–996 (cit. on p. 34).

[55] Irina E. Bocharova, Boris D. Kudryashov, Vitaly Skachek, Eirik Rosnes, and Øyvind Ytrehus. "LDPC Codes Over the BEC: Bounds and Decoding Algorithms". In: *IEEE Transactions on Communications* 67.3 (2019), pp. 1754–1769. DOI: 10.1109/TCOMM.2018.2879107 (cit. on pp. 34, 35).

[56] Pavel Rybin, Kirill Andreev, and Victor Zyablov. "On the Error Exponents of LDPC Codes Approaching Capacity Under a Low-Complexity Decoding Algorithm". In: *Entropy* 23.2 (2021), p. 253 (cit. on p. 34).

[57] Irina E. Bocharova, Boris D. Kudryashov, and Vitaly Skachek. "Performance of ML decoding for ensembles of binary and nonbinary regular LDPC codes of finite lengths". In: *2017 IEEE International Symposium on Information Theory (ISIT)*. 2017, pp. 794–798. DOI: 10.1109/ISIT.2017.8006637 (cit. on p. 34).

[58] G. Miller and D. Burshtein. "Bounds on the maximum-likelihood decoding error probability of low-density parity-check codes". In: *IEEE Transactions on Information Theory* 47.7 (2001), pp. 2696–2710 (cit. on p. 35).

[59] Eran Hof, Igal Sason, and Shlomo Shamai. "Performance bounds for nonbinary linear block codes over memoryless symmetric channels". In: *IEEE transactions on information theory* 55.3 (2009), pp. 977–996 (cit. on p. 35).

[60] Irina E Bocharova, Boris D Kudryashov, and Vitaly Skachek. "Performance of ML decoding for ensembles of binary and nonbinary regular LDPC codes of finite lengths". In: *2017 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2017, pp. 794–798 (cit. on p. 35).

[61] Kenta Kasai, Charly Poulliat, David Declercq, Tomoharu Shibuya, and Kohichi Sakaniwa. "Weight Distribution of Non-binary LDPC Codes". In: Jan. 2009, pp. 1–6. DOI: 10.1109/ISITA.2008.4895508 (cit. on pp. 35, 57).

[62] Iryna Andriyanova, Vishwambhar Rathi, and Jean-Pierre Tillich. "Binary weight distribution of non-binary LDPC codes". In: *IEEE International Symposium on Information Theory : ISIT 2009*. Seoul, South Korea, July 2009, pp. 65–69. DOI: 10.1109/ISIT.2009.5205662. URL: https://hal.archives-ouvertes.fr/hal-00524696 (cit. on pp. 35, 57).

[63] Changyan Di, T.J. Richardson, and R.L. Urbanke. "Weight Distribution of Low-Density Parity-Check Codes". Undetermined. In: *IEEE Transactions on Information Theory* 52.11 (2006), pp. 4839–4855. DOI: 10.1109/TIT.2006.883541 (cit. on p. 35).

Symbol Interleaved Coded Modulation (SICM)

In the previous chapter, a QAM-based communication chain with binary encoding/decoding has been introduced for transmission over the AWGN channel. Moreover, a class of NB-LDPC codes has been defined.

In this chapter, let us focus on a communication chain based both on a channel code over $GF(q)$ and M-QAM modulation scheme, while the transmission is still assumed to take place over the AWGN channel. Such a setup motivates us to investigate us two following questions:

- what is the best value of q with respect to M;
- for fixed q and M, what matching between q-ary coded symbols and M-ary modulation symbols would give the lowest error probability after decoding.

Note that, even though there exist a number of numerical results for such a matching in the optics community, it seems that there is no explicit result on this subject.

The chapter starts with a motivating numerical example that illustrates the relevance of considering different mapping of coded symbols to modulation symbols. Inspired by the example, a *Symbol Interleaved Coded Modulation (SICM)* scheme is further defined, and its performance is studied.

3.1 Our motivating example: $M = 16$ and $q = 2; 4; 16$

Let us consider a particular example of the 16-QAM modulation and of a regular NB-LDPC code over $GF(q)$.

3.1.1 Bit-level LLRs after demodulation

Our first observation is on bit-level LLR estimations after the demodulation process. We are going to show on an example of 16-QAM that some bits are more reliably estimated than the other.

Proposition 3.1.1 Let the 16-QAM modulation be seen as the Kronecker product of two

4-PAM modulations, each using a Gray labeling . Therefore, a label (b_0, b_1, b_2, b_3) of each QAM symbol is a concatenation of labels (b_0, b_1) and (b_2, b_3) of two respective 4-PAM symbols. Let Δ be the half of the distance between two closest QAM symbols and let modulation symbols be equiprobable.

Let y be the received value, when a 16-QAM symbol has been sent though an AWGN channel of variance σ^2. Then the LLRs of label bits b_0 and b_1 are approximated as follows:

$$L(b_0|y) \approx \begin{cases} \frac{-2\Delta Re(y) - 4\Delta^2}{\sigma^2} & \text{if } Re(y) < 0 \\ \frac{2\Delta Re(y) - 4\Delta^2}{\sigma^2} & \text{otherwise.} \end{cases} \tag{3.1}$$

$$L(b_1|y) \approx \begin{cases} \frac{-4\Delta Re(y) - 4\Delta^2}{\sigma^2} & \text{if } Re(y) < -2\Delta \\ \frac{-2\Delta Re(y)}{\sigma^2} & \text{if } -2\Delta \leq Re(y) < 2\Delta \\ \frac{-4\Delta Re(y) + 4\Delta^2}{\sigma^2} & \text{otherwise.} \end{cases} \tag{3.2}$$

Moreover, the LLRs $L(b_2|y)$ and $L(b_3|y)$ for label bits b_2 and b_3 are expressed by (3.1)-(3.2), if one replaces $Re(y)$ with $Im(y)$.

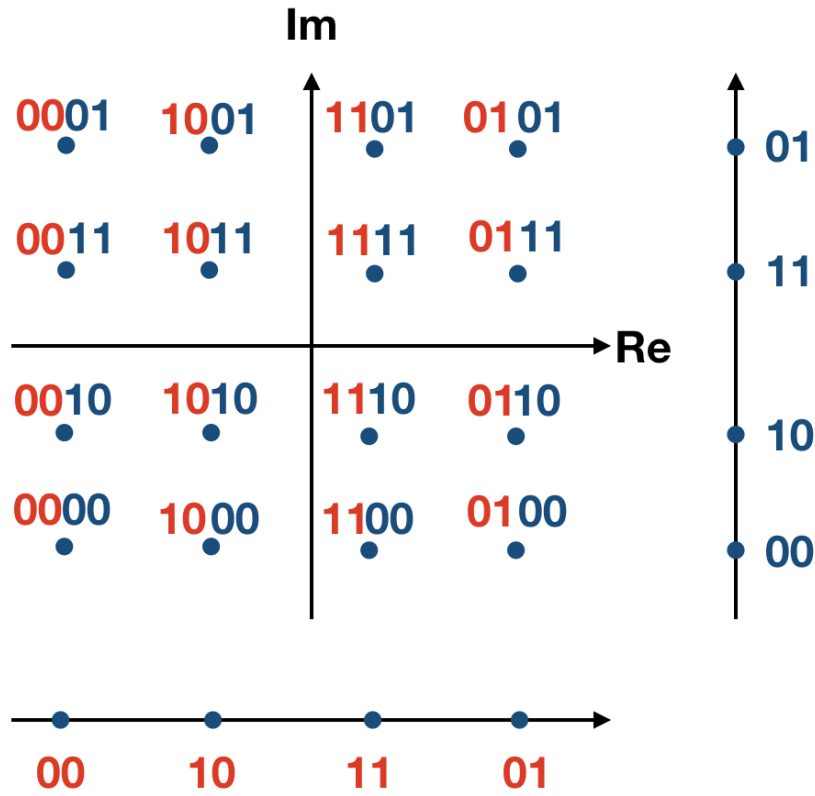Figure 3.1: Construction of 16-QAM modulation from two 4-PAMs (red one and blue one).

Proof. An illustration to the setup of the lemma is given in Figure 3.1). It depicts two 4-PAM modulations (vertical axis with blue points and horizontal axis with red points), and the resulting 16-QAM modulation. Note that, as 4-PAMs use Gray labeling, the symbols of the 16-QAM have a Gray labeling as well.

Consider the k-th bit in the Gray label of a 16-QAM symbol. Denote by $\mathcal{R}_0^k$ and $\mathcal{R}_1^k$ two subsets of $\mathcal{A}$ such that their k-th label bit equals to 0 and 1 respectively. Using Definition 2.1.5) and that $P(b_k = b|y) = \sum_{a_j \in \mathcal{R}_b^k} P(a_j|y)$,

$$
L(b_k|y) = \log\left(\frac{\sum_{a_j \in \mathcal{R}_1^k} P(a_j|y)}{\sum_{a_j \in \mathcal{R}_0^k} P(a_j|y)}\right) \tag{3.3}
$$

$$
= \log\left(\frac{\sum_{a_j \in \mathcal{R}_1^k} P(y|a_j)}{\sum_{a_j \in \mathcal{R}_0^k} P(y|a_j)}\right), \tag{3.4}
$$

where at the last step it was used that the modulation symbols are equiprobable. Given that $y = x + n$ where $x = a_i$ and $n \sim \mathcal{N}(0, \sigma^2 I^2)$ is the AWGN noise sample, one has that $y \sim \mathcal{N}(a_i, \sigma^2 I)$. Therefore

$$
L(b_k|y) = \log\left(\sum_{a_\ell \in \mathcal{R}_1^k} e^{\frac{-(Re(y)-Re(a_\ell))^2}{2\sigma^2} - \frac{(Im(y)-Im(a_\ell))^2}{2\sigma^2}}\right)
$$
$$
- \log\left(\sum_{a_{\ell'} \in \mathcal{R}_0^k} e^{\frac{-(Re(y)-Re(a_{\ell'}))^2}{2\sigma^2} - \frac{(Im(y)-Im(a_{\ell'}))^2}{2\sigma^2}}\right), \tag{3.5}
$$

and one obtains an expression similar to the one in Proposition 2.1.2. With the use of the max-log approximation [64] $\log\left(\sum_j e^{a_j}\right) \approx \max_j(a_j)$, one obtains that

$$
L(b_k|y) \approx \frac{1}{2\sigma^2}\Big[\min_{a_j \in \mathcal{R}_1^k}\big((Re(y) - Re(a_j))^2 + (Im(y) - Im(a_j))^2\big)
$$
$$
- \min_{a_j \in \mathcal{R}_0^k}\big((Re(y) - Re(a_j))^2 + (Im(y) - Im(a_j))^2\big)\Big] \tag{3.6}
$$

Let us consider two first bits labels b_0 and b_1 (red labels in Figure 3.1). They are provided by the first $4 - PAM$ and play their role in the real part of $16 - QAM$ symbols. Therefore, it is sufficient to consider exclusively $Re(y)$. Given 4-PAM labeling as shown in Figure 3.2 and the k-th bit label ($k = 0; 1$), denote by $\bar{a}_0^k(y)$ (resp. $\bar{a}_1^k(y)$) the 4-PAM symbol, closest to $Re(y)$ and which k bit label equals to 0 (resp. 1). Then, for $k = 0; 1$ one has that

$$
L(b_k|y) \approx \frac{1}{2\sigma^2}\Big[(Re(y) - \bar{a}_1^k(y))^2 - (Re(y) - \bar{a}_0^k(y))^2\Big], \tag{3.7}
$$

$$
= \frac{1}{2\sigma^2}\Big[2Re(y)(\bar{a}_0^k(y) - \bar{a}_1^k(y)) + (\bar{a}_1^k(y))^2 - (\bar{a}_0^k(y))^2\Big]. \tag{3.8}
$$

Similarly to [65] where the bit-level LLR calculation has been done for PAM modulations, let us split 4-PAM bit labels into two parts: the Least Significant Bits (LSB) part and the Most Significant Bits (MSB) part, and to consider them separately. See Figure 3.2 for illustration if the LSB/MSB splitting.

1. *LSB case:*
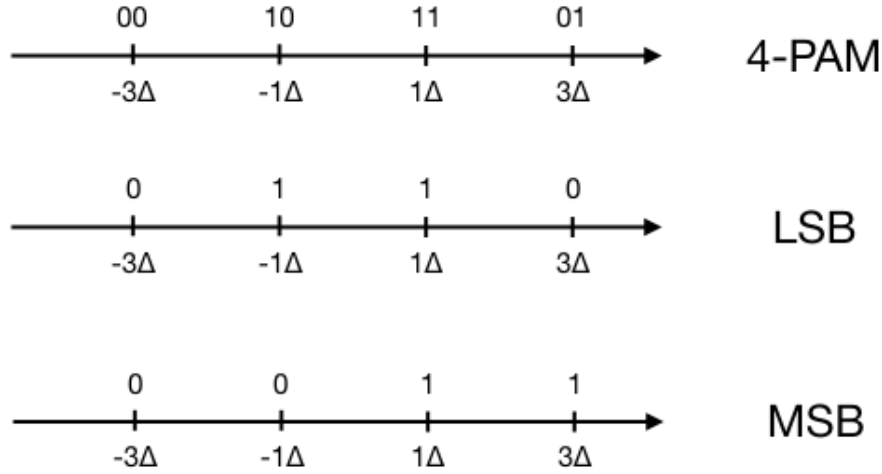   Let us distinguish $Re(y) \geq 0$ and $Re(y) < 0$.

Figure 3.2: Dividing a 4-PAM bit label into LSB ans MSB parts.

a) For $Re(y) < 0$, $\bar{a}_0^0(y) = -3\Delta$ and $\bar{a}_1^0(y) = \Delta$, thus

$$
\begin{aligned}
L(b_0|y) &= \frac{1}{2\sigma^2}\left[2Re(y)(-3\Delta + \Delta) + (-\Delta)^2 - (-3\Delta)^2\right], \\
&= \frac{-2\Delta Re(y) - 4\Delta^2}{\sigma^2}
\end{aligned}
$$

b) For $Re(y) \geq 0$, as $\bar{a}_0^0(y) = 3\Delta$ and $\bar{a}_1^1(y) = \Delta$,

$$
\begin{aligned}
L(b_0|y) &= \frac{1}{2\sigma^2}\left[2Re(y)(3\Delta - \Delta) + (\Delta)^2 - (3\Delta)^2\right], \\
&= \frac{2\Delta Re(y) - 4\Delta^2}{\sigma^2}
\end{aligned}
$$

By putting the cases a) and b) together, one obtains (3.1).

2. *MSB case:* Let us distinguish $Re(y) < -2\Delta$, $-2\Delta \leq Re(y) < 2\Delta$, and $Re(y) \geq 2\Delta$:

a) For $Re(y) < -2\Delta$, $\bar{a}_0^1(y) = -3\Delta$ and $\bar{a}_1^1(y) = 1\Delta$

$$
\begin{aligned}
L(b_1|y) &\approx \frac{1}{2\sigma^2}\left[2Re(y)(-3\Delta - \Delta) + (\Delta)^2 - (-3\Delta)^2\right], \\
&= \frac{-4\Delta Re(y) - 4\Delta^2}{\sigma^2}
\end{aligned}
$$

b) For $-2\Delta \leq Re(y) < 2\Delta$, we have $\bar{a}_0^1(y) = -\Delta$ and $\bar{a}_1^1(y) = \Delta$, and thus

$$
\begin{aligned}
L(b_1|y) &= \frac{1}{2\sigma^2}\left[2Re(y)(-\Delta - \Delta) + (\Delta)^2 - (-\Delta)^2\right], \\
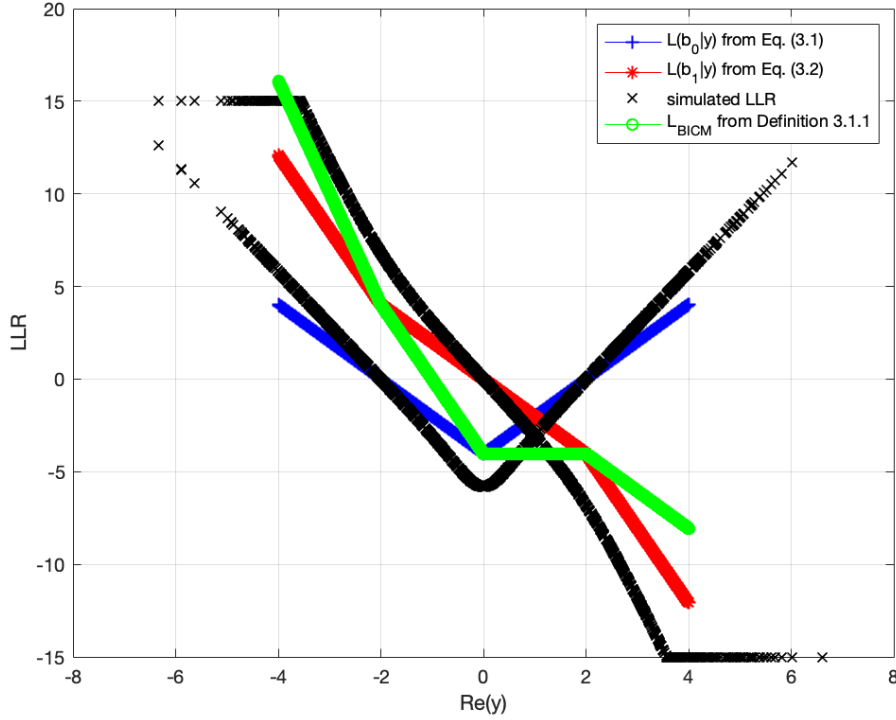&= \frac{-2\Delta Re(y)}{\sigma^2}
\end{aligned}
$$

Figure 3.3: Comparison of results of Lemma 3.1.1 with numerical simulations.

c) For $Re(y) \geq 2\Delta$, $\bar{a}_0^1(y) = -\Delta$ and $\bar{a}_1^1(y) = 3\Delta$

$$
\begin{aligned}
L(b_1|y) &= \frac{1}{2\sigma^2}\left[2Re(y)(-\Delta - 3\Delta) + (3\Delta)^2 - (-\Delta)^2\right], \\
&= \frac{-4\Delta Re(y) + 4\Delta^2}{\sigma^2}
\end{aligned}
$$

By putting together the cases a), b) and c) above, one obtains (3.2). The calculation for b_2 and b_3 is similar. ∎

Using Lemma 3.1.1 above, one can compare approximated bit LLR values in the case of LSB and MSB. Figure 3.3 compares $L(b_0|y)$ (blue curve) and $L(b_1|y)$ (red curve) approximations for different values of $Re(y)$, as well as their exact LLR values (two black curves). One can see that the red and blue approximations capture pretty well the behaviour of exact LLRs. Also, note that $L(b_0|y)$ and $L(b_1|y)$ behave differently with $Re(y)$. This is the point which further be used in the chapter. Moreover, let us define the average LLR value as follows:

Definition 3.1.1 Given $L(b_0|\mathbf{y})$ and $L(b_1|\mathbf{y})$, let the average LLR expression L_{BICM} be defined as

$$
L_{BICM}(y) = \frac{1}{2}[L(b_0|y) + L(b_1|y)].
$$

L_{BICM} is represented by the green curve on Figure 3.3.

3.1.2   Numerical results with q-ary LDPC codes for $q = 2; 4; 16$ and 16-QAM

Given the observation on the difference of LLR estimations from the previous section, one expects to have a different decoding performance for different values of q and different ways of grouping bit labels into the symbols of the code (i.e. different coded modulation schemes).

The difference indeed has place. Let us illustrate it on a numerical example of a regular $(3, 6)$ LDPC code over $GF(q)$ of binary codelength $N = 1000$ bits. As $M = 16$ in our particular example, let us consider the following cases:

- **Case** $q = 2$**:** a coded LDPC symbol corresponds to a bit label in the 16-QAM.The average bit LLR behaviour is given by the green curve in Figure 3.3.
- **Case** $q = 4$**:** a coded LDPC symbol corresponds to two bit labels in the 16-QAM. Two choices to form a coded symbols are possible :
  - (a) a LDPC symbol consists of two bits chosen uniformly at random among all possible bit labels. Such a mapping will further be defined as a *Bit-Interleaved Coded Modulation (BICM)*. Not that its average bit LLR behaviour is given by the green curve in Figure 3.3;
  - (b) a LDPC symbol consists of two bits that correspond either to the first half either to the second half of the 16-QAM symbol label. Such a mapping will further be defined as a *Symbol-Interleaved Coded Modulation (SICM)*. In this case, the LDPC symbols are partitioned by type : MSB or LSB.
- **Case** $q = 16$**:** a coded LDPC symbol corresponds to four bit labels in the 16-QAM. Let us again consider two possibilities to form a coded symbol :
  - (a) in a BICM way, when a LDPC symbol consists of four bits chosen uniformly at random among all possible bit labels;
  - (b) in a SICM way, where one 16-QAM symbol is mapped to one 16-ary LDPC symbol.

Figure 3.4 illustrates the BER performance versus signal-to-noise ration $\frac{E_b}{N_0}$ in dB for all the five options presented above. Moreover, it also contains the sixth curve (blue with triangle marks) from the state of the art, for a particular case presented by Schmalen *et al.* [33], where q-ary code symbols are converted to bits before modulation, we found that it was sub-optimal compared to SICM.

By comparing the BER performances in Figure 3.4, we conclude that:

- the decoding performance for $q = 4$ outperforms $q = 2$ and $q = 16$ cases;
- for a fixed value of q, the mapping of modulation symbols to coded symbols matters. For both $q = 4$ and $q = 16$ the SICM way of mapping outperforms the BICM way of mapping;
- the best BER performance in our example is given by the $q = 4$ with SICM, and this for any value of $\frac{E_b}{N_0}$. This coded modulation scheme outperforms the one with BICM by 0.25 dB at $BER = 10^{-4}$.

In order to explain the obtained results, let us define the SICM scheme in a more formal way and to study its performance. This is the main topic of the following section.

3.2   Symbol Interleaved Coded Modulation (SICM)

This section is devoted to the definition and asymptotic performance analysis of the so called Symbol Interleaved Coded Modulation .
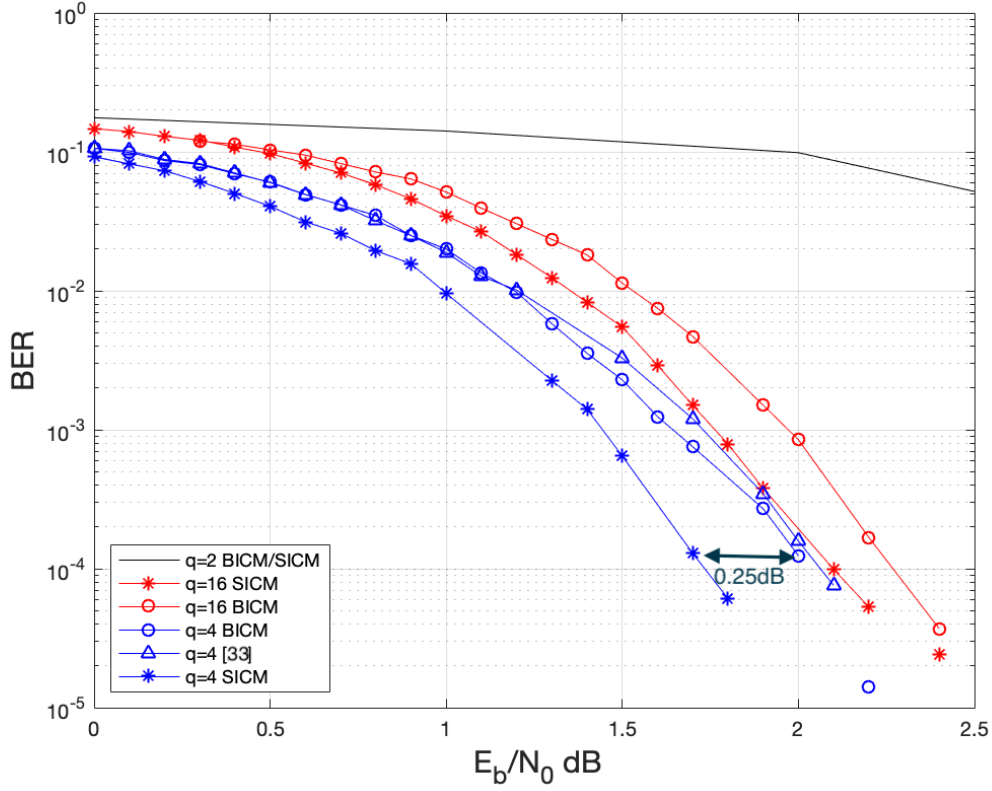
3.2.1   Definition of SICM

Figure 3.4: BER performance of a q-ary (3,6) LDPC code of binary codelength $N = 1000$ with various coded modulation schemes, assuming the transmission with 16-QAM and over AWGN channel.

Definition 3.2.1 The SICM scheme (see Figure 3.5) is given by the serial concatenation of an error-control code over $GF(q)$, and of a QAM of order M, separated by a symbol interleaver that maps one or several code symbols into a modulation symbol.
   SICM operations are described as follows.
   - *Channel encoding.* Information symbols are first encoded into a codeword $\mathbf{c} = [\mathbf{c_1}, \cdots, \mathbf{c_n}] \in GF(q)^n$, of binary codelength $N = mn$ bits, $m = \log_2(q)$.
   - *Interleaving.* The coded symbols are then interleaved using the symbol interleaver. After interleaving and grouping the interleaved coded symbols into groups of l symbols over $GF(q)$ ($l = (\log_2 M)/q$), one obtains $\underline{\mathbf{C}}[k] = [\underline{\mathbf{c}}_1[k], \underline{\mathbf{c}}_2[k], \cdots, \underline{\mathbf{c}}_l[k]]$ – a sequence of nonbinary l-tuples for $1 \leq k \leq N_s$ and $N_s = n/l$. From all the said above, it follows that symbol interleaver is a bijective map given by

$$\text{Symbol interleaver}: [1, \cdots, n] \mapsto [1, \cdots N_s] \times [1, \cdots l]$$
$$k' \qquad (k'', i) \qquad\qquad (3.9)$$

where $\mathbf{c}_{k'} \in GF(q)$ is the k'-th coded symbol and $\underline{\mathbf{c}}_i[k'']$ is the i-th component of the l-tuple $\underline{\mathbf{C}}[k'']$. For the ease of exposition, the time index will be omitted in the following when the context is clear enough.
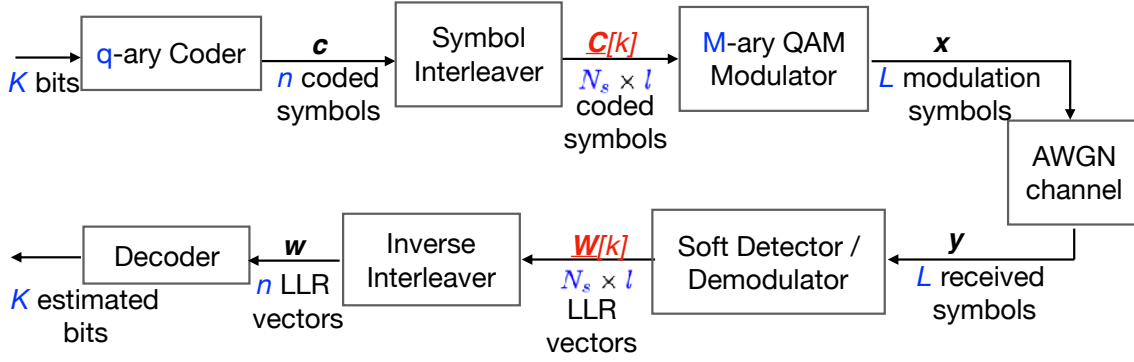
Figure 3.5: SICM model with a q-ary error-control code and M-QAM modulation.
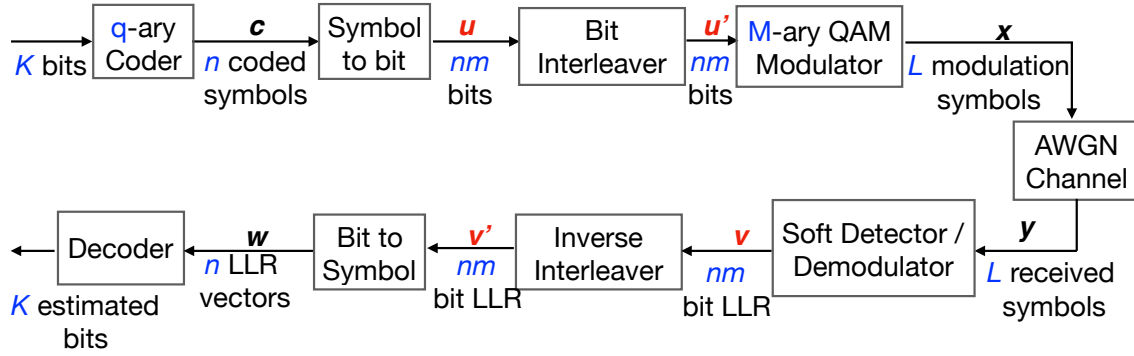
Figure 3.6: Extended BICM model with a q-ary error-control code and M-QAM modulation.

- *Modulation.* A QAM symbol $\mathbf{x}[k] \in \mathcal{A}$ is then selected based on the value of the symbol labeling $\underline{\mathbf{C}}$.
- *Receiver side.* After having observed $\mathbf{y}$, the transmitted symbols are detected by a soft symbol maximum a posteriori (MAP) demapper, and inverse interleaving and decoding operations are then performed.

Note that the defined SICM model is an extension of the classical communication chain presented in Section 2.1.1. To the best of our knowledge, the SICM scheme has not been yet studied (although the notion of symbol interleaving is not new and first papers on it refer to 1988 [66], most of symbol interleaving schemes from the state of the art address the interleaving for OFDM and MIMO transmission protocols). In case of $q = 2$, the SICM is equivalent to the classical Bit-Interleaved Coded Modulation (BICM) scheme with binary codes, considered in [32, 67, 68]. Note that such a BICM is widely used under various wireless and optical communication scenarios and is very well investigated, see for instance [69] for the optical-fiber application. The interested in BICM is referred to [70] for further details.

While considering non-binary channel codes over $GF(q)$, there might be interesting to extend the BICM definition to this case. In fact, the extension has been already presented in an implicit way in [71], let us simply reformulate it in the following way:

> **Definition 3.2.2** The extended BICM scheme, depicted in Figure 3.6, is given by the serial concatenation of an error-control code over $GF(q)$, and of a QAM of order M, separated by a bit interleaver that interleaves bits in the code symbols and maps them into into a M-ary modulation symbol.

Note that the BICM cases considered in Section 3.1.2 fall into the framework of Definition 3.2.2.

3.2.2 Asymptotic performance of the SICM scheme parametrized by q and M

Let us compare the asymptotic performance of SICM and (extended) BICM schemes. Our reference measure will be the *coded modulation (CM) capacity*:

> **Definition 3.2.3** For independent and identically and uniformly distributed constrained inputs, the coded modulation (CM) capacity C_{CM} is defined as $C_{CM} = I(X;Y)$. Moreover, in our setting (i.e., M-ary modulation of alphabet $\mathcal{A}$ and q-ary channel code with $q = 2^m$, while the transmission takes place over the AWGN channel) it expressed as
>
> $$C_{CM} = m - \mathbb{E}_{\mathbf{x},\mathbf{y}}\left[\log_2 \frac{\sum_{\mathbf{a} \in \mathcal{A}^{N_s}} p(\mathbf{y}|\mathbf{a})}{p(\mathbf{y}|\mathbf{x})}\right]. \tag{3.10}$$

By the chain rule applied to the binary labeling with $l = \log_2 M$ bits, the coded modulation capacity (3.10) can be rewritten for as follows

$$
\begin{aligned}
C_{CM} &= I(c_1, \ldots, c_l; Y) \\
&= I(c_1; Y) + \sum_{k=2}^{l} I(c_k; Y|c_1, \ldots, c_{l-1})
\end{aligned}
\tag{3.11}
$$

where $[c_1, \cdots, c_l]$ is the binary l-tuple associated to the labeling of a M-ary symbol $x \in \mathcal{A}$. From (3.11) it follows that the optimal coded modulation scheme can be seen as the transmission scheme with l binary channels.

Let us also define SICM and BICM capacities:

> **Definition 3.2.4** Assuming independent decoding of l symbol channels under the SICM setting from Definition 3.2.1. Then the SICM capacity $\mathbf{C}_{SICM}$ is defined as
>
> $$\mathbf{C}_{SICM} = \sum_{k=1}^{l} \mathbf{C}_{\underline{c}_k},$$
>
> where $\mathbf{C}_{\underline{c}_k} = I(Y; \underline{c}_k)$ is the capacity of the equivalent symbol-channel associated to the label index $\underline{c}_k$.

> **Definition 3.2.5** The BICM capacity is given by
>
> $$C_{bicm} = \sum_{k=1}^{\log_2 M} I(c_i; Y).$$

It is to note that in general $C_{bicm} \leq C_{cm}$, due to the gap between $\sum_{k=1}^{l} I(c_i; Y)$ and $I(c_1, \ldots, c_l; Y)$ in (3.11).

One could expect that, similarly to the BICM case, $C_{SICM} \leq C_{CM}$. Moreover, in the state of the art, it is often argued that nonbinary coding schemes matching to the order of the QAM constellation (i.e., $M = q$) are the best choice in order to fill the gap between
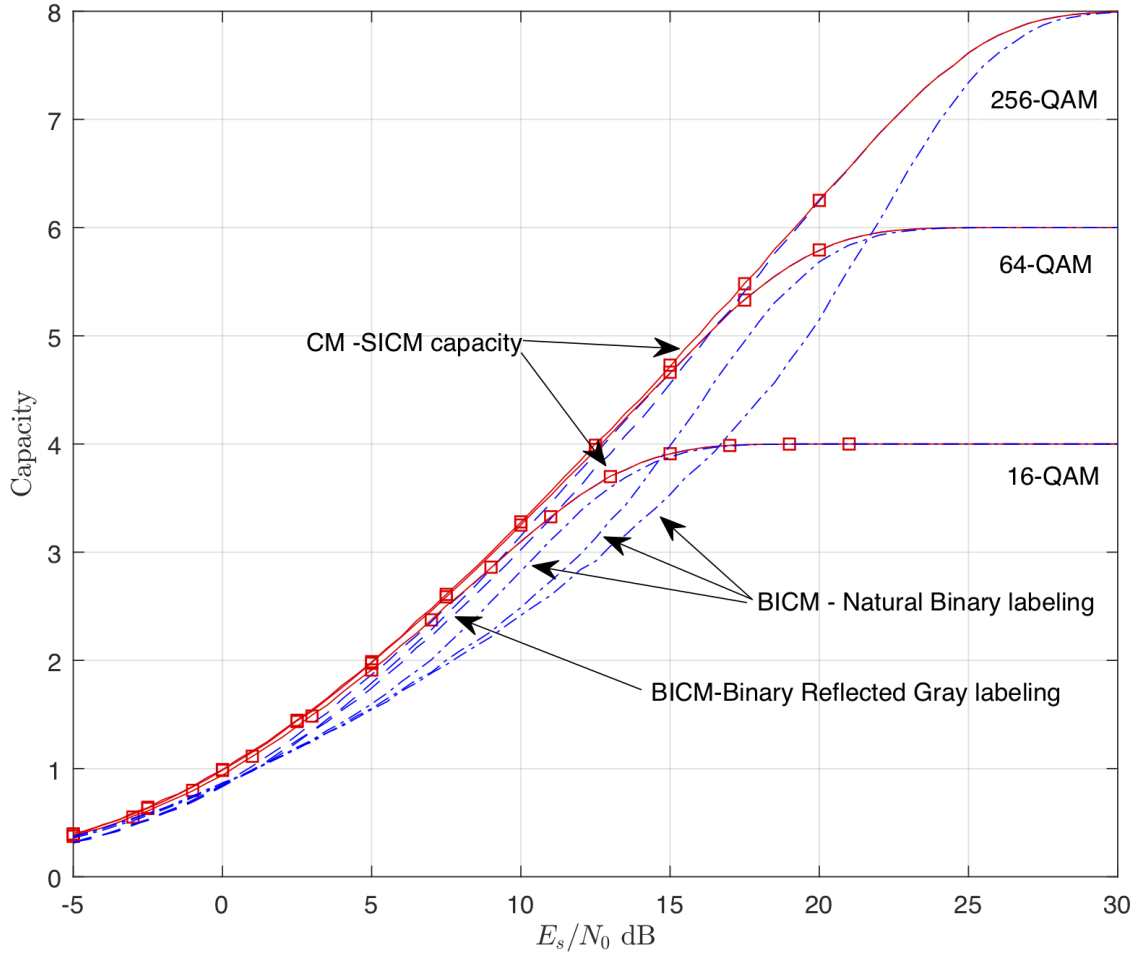
Figure 3.7: CM, SICM and BICM capacities for q^2-PAM for $q^2 \in \{16, 64, 256\}$ with Natural binary and Binary Reflected Gray mappings (thus here $q = \sqrt{M}$).

$\mathbf{C}_{BICM}$ and $\mathbf{C}_{CM}$. However we have the following interesting result regarding the SICM capacity:

> **Theorem 3.2.1** Consider transmission over the AWGN channel using a SICM scheme with M-ary QAM modulation and a q-ary channel code, such that:
> * the QAM modulation is designed as a direct product of two PAMs, and
> * q divides M.
> Then, if $q = \sqrt{M}$, $\mathbf{C}_{SICM} = \mathbf{C}_{CM}$. Otherwise, for $q < \sqrt{M}$, $\mathbf{C}_{SICM} \leq \mathbf{C}_{CM}$.

Proof. Let $\underline{C} = [\underline{\mathbf{c}}_1, \underline{\mathbf{c}}_2]$ be the resulting nonbinary partitioning of the QAM symbol labeling into two PAM labeling parts as illustrated in Figure 3.1. Let us denote by $\mathbf{C}_{\underline{\mathbf{c}}_k} = I(Y, \underline{\mathbf{c}}_k)$ the equivalent nonbinary channel associated to the non-binary label $\underline{\mathbf{c}}_k$. The SICM capacity is then given by

$$\mathbf{C}_{sicm} = \mathbf{C}_{\underline{\mathbf{c}}_1} + \mathbf{C}_{\underline{\mathbf{c}}_2}. \tag{3.12}$$

Figure 3.8: CM, SICM and BICM capacities for 64-QAM and channel codes over GF(4) (thus here $Q < \sqrt{M}$).

Now, note that

$$
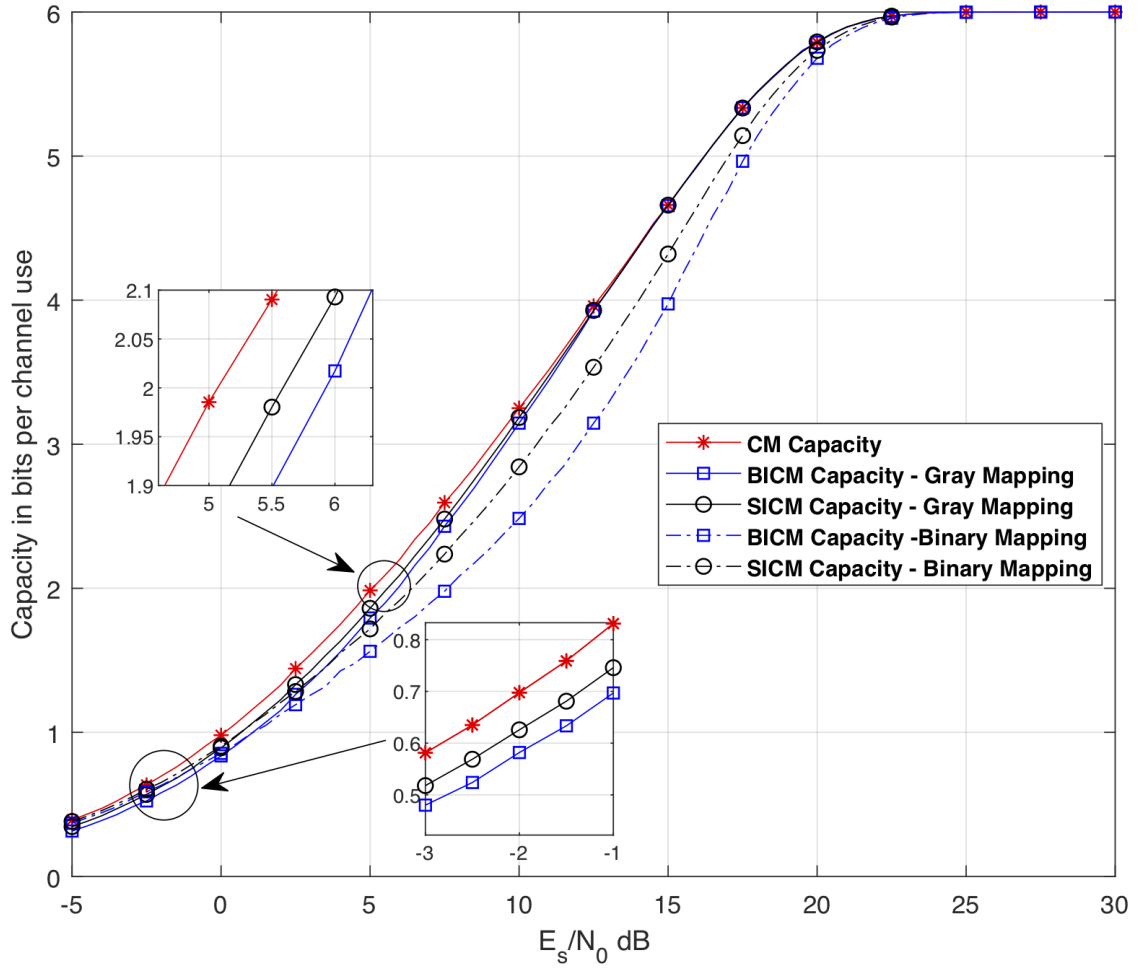\begin{aligned}
\mathbf{C}_{CM} &= I(y; \underline{\mathbf{c}}_1) + I(y; \underline{\mathbf{c}}_2 | \underline{\mathbf{c}}_1) \\
&= I(y; \underline{\mathbf{c}}_1) + I(y; \underline{\mathbf{c}}_2) = \mathbf{C}_{SICM},
\end{aligned}
\tag{3.13}
$$

where that the second equality is due to the orthogonal nonbinary signaling of 2 PAMs. Also note that $\mathbf{C}_{b_0} = \mathbf{C}_{b_1}$ by symmetry.

In general, $I(\underline{\mathbf{c}}_2; Y | \underline{\mathbf{c}}_1) \geq I(\underline{\mathbf{c}}_2; Y)$. One can use this statement to prove $\mathbf{C}_{SICM} \leq \mathbf{C}_{CM}$, for $q < \sqrt{M}$. ∎

The theorem above suggests that, using M-ary coding schemes with M-QAM modulations is an unnecessarily complex solution. Figure 3.7 illustrates numerical estimations of capacities of q^2-QAM modulations for different values of q, when natural binary and binary reflected Gray mappings are used. As predicted, $\mathbf{C}_{SICM}$ is naturally equal to $\mathbf{C}_{CM}$ for all considered values of q. The BICM capacity is also reported, thus showing the impact of the binary labeling of the constellation symbols. Remind that there is no influence when non-binary mapping is used for q^2-QAM modulations.
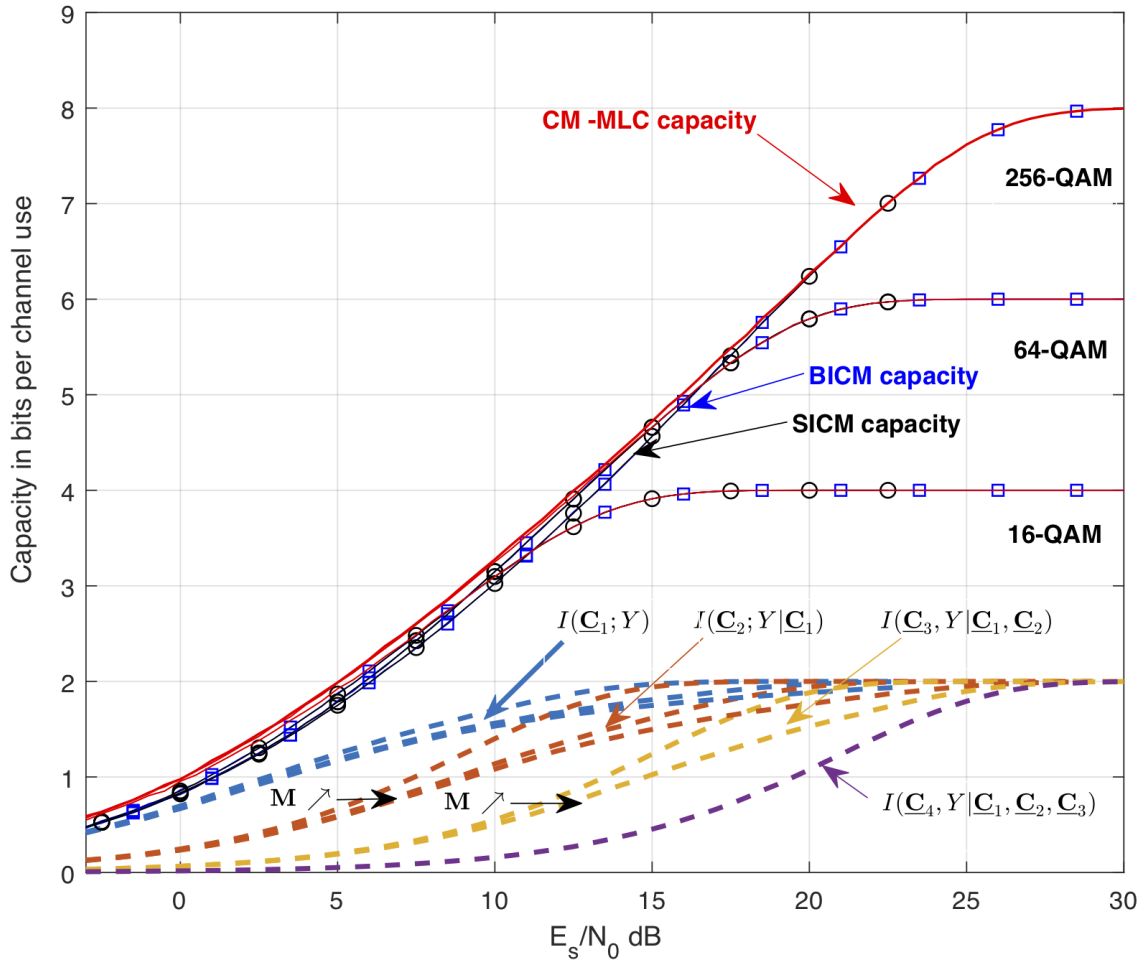
Figure 3.9: CM, SICM and BICM capacities for a $16/64/256$-QAM constellation build by superposition.

Theorem 3.2.1 states that the SICM scheme is no longer optimal if $q < \sqrt{M}$ and some performance loss is expected. For an example, Figure 3.8 shows the SICM capacity for $M = 64$ and $q = 4 < \sqrt{M}$. One observes that SICM outperforms BICM at low capacity rates; the gain up to 0.5 dB can be obtained for the Gray mapping, and even more for the natural binary mapping. The same result has also been observed for 256-QAM.

(R) Note that it is also possible to design SICM schemes by the so called *superposition* [72, 73], also referred sometimes to as hierarchical modulations. In dshort, this type of QAM constellations is generated based on the linear superposition in the signal spaces of 4-QAM modulations (so called superposition layers), following some specific rules when adding a layer to another the final labeling is a Gray labeling [72, 73]. It can be shown that the SICM schemes with QAM modulations build by superposition are performing the same when as the BICM scheme for the same value of q. Indeed, it can be shown that, when Binary Reflected Gray mapping is used, bit channels in the twi cases are equivalent up to a permutation of the bit labeling. To illustrate this point, Figure 3.9 compares CM, SICM and BICM capacities for various modulation orders, for channel codes over GF(4) and based on the

modulations defined in the LTE standard [74]. These modulations are Gray QAM modulations and can be interpreted as superposed QAM modulations. Rates of respective layers for the optimal CM scheme are also given in the figure. One can see the SICM behaves similarly to the BICM.

3.3 Conclusion

In this chapter, the following points have been discussed:

- $q = \sqrt{M}$: SICM capacity = CM capacity, if one uses the Gray labeling obtained from a direct product of 2 q-ary PAM modulations.
- $q < \sqrt{M}$: BICM capacity $\leq$ SICM capacity $\leq$ CM capacity. Moreover, in case of q-ary codes with $q < M$, it is only possible to achieve the capacity by using a multi-level coding which would give rise from (3.11). The design by superposition behaves worse than the design by direct product of PAMs.
- Although the SICM scheme for $2 < q < \sqrt{M}$ is bounded away from the CM capacity, it still outperforms the extended BICM scheme at low and moderate values of SNR.

Bibliography

[64] A.J. Viterbi. "Viterbi, A.J.: An Intuitive Justification and a Simplified Implementation of the MAP Decoder for Convolutional Codes. IEEE Journal on Select Areas in Communications 16(2), 260-264". In: *Selected Areas in Communications, IEEE Journal on* 16 (Mar. 1998), pp. 260–264. DOI: 10.1109/49.661114 (cit. on p. 43).

[65] M. Benjillali, L. Szczecinski, and S. Aissa. "Probability Density Functions of Logarithmic Likelihood Ratios in Rectangular QAM". In: *23rd Biennial Symposium on Communications, 2006*. May 2006, pp. 283–286. DOI: 10.1109/BSC.2006.1644623 (cit. on p. 43).

[66] W. Rafferty and D. Divsalar. "Modulation and coding for land mobile satellite channels". In: *IEEE International Conference on Communications, - Spanning the Universe.* 1988, 1105–1111 vol.2. DOI: 10.1109/ICC.1988.13726 (cit. on p. 48).

[67] Giuseppe Caire, Giorgio Taricco, and Ezio Biglieri. "Bit-Interleaved Coded Modulation". In: *IEEE Trans. Information Theory* 44 (1998), pp. 927–946 (cit. on p. 48).

[68] Albert Guillén i Fàbregas, Alfonso Martinez, and Giuseppe Caire. "Bit-Interleaved Coded Modulation". In: *Foundations and Trends® in Communications and Information Theory* 5.1–2 (2008), pp. 1–153. ISSN: 1567-2190. DOI: 10.1561/0100000019. URL: http://dx.doi.org/10.1561/0100000019 (cit. on p. 48).

[69] Ivan B. Djordjevic, Milorad Cvijetic, Lei Xu, and Ting Wang. "Proposal for Beyond 100-Gb/s Optical Transmission Based on Bit-Interleaved LDPC-Coded Modulation". In: *IEEE Photonics Technology Letters* 19.12 (2007), pp. 874–876. DOI: 10.1109/LPT.2007.897520 (cit. on p. 48).

[70] Albert Guillen i Fàbregas, Alfonso Martinez, and Giuseppe Caire. 2008 (cit. on p. 48).

[71] Laurent Schmalen, Alex Alvarado, and Rafael Rios-Müller. "Performance Prediction of Nonbinary Forward Error Correction in Optical Transmission Experiments". In: *Journal of Lightwave Technology* 35.4 (2017), pp. 1015–1027. DOI: 10.1109/JLT.2016.2609932 (cit. on p. 48).

[72] P. K. Vitthaladevuni and M. S. Alouini. "A recursive algorithm for the exact BER computation of generalized hierarchical QAM constellations". In: *IEEE Transactions on Information Theory* 49.1 (Jan. 2003), pp. 297–307. ISSN: 1557-9654. DOI: 10.1109/TIT.2002.806159 (cit. on p. 52).

[73] Q. Li, J. Zhang, L. Bai, and J. Choi. "Performance Analysis and System Design for Hierarchical Modulated BICM-ID". In: *IEEE Transactions on Wireless Communications* 13.6 (June 2014), pp. 3056–3069. ISSN: 1558-2248. DOI: 10.1109/TWC.2014.042814.130912 (cit. on p. 52).

[74] *3GPP TS 36.211, "Physical Channels and Modulation." Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA).* Technical Specification (TS). 3rd Generation Partnership Project (3GPP) (cit. on p. 53).

[75] A. Bennatan and D. Burshtein. "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels". In: *IEEE Transactions on Information Theory* 52.2 (Feb. 2006), pp. 549–583. ISSN: 0018-9448. DOI: 10.1109/TIT.2005.862080 (cit. on p. 90).

On high-rate regular NB-LDPC codes

In the previous chapter we have seen that q-ary error-control codes are a part of the SICM scheme that might help to obtain a better decoding performance in QAM-based transmissions over the AWGN channel.

This chapter will be therefore focused of the most known family of NB-LDPC codes over $GF(q)$ – regular NB-LDPC codes from the $C_{LDPC}(a, d, m, n)$ ensemble, defined in Chapter 2. The decoding performance of the codes will be considered in the context of optical transmission, i.e. assuming high code rates r, $0.8 \leq r \leq 0.9$. It is to note that this operational point did not receive much attention in the state of the art yet, and thus needs to be investigated.

4.1 State of the art: NB-LDPC codes and optical communications

Regular NB-LDPC codes have been first proposed by Gallager in his PhD thesis [34]. Later, Davey and MacKay [35] have shown that NB-LDPC codes achieve better decoding performance compared to binary codes, over the binary symmetric and the binary-input AWGN channels. Asymptotic and finite-length of regular NB-LDPC codes has been studied in many research works, i.e., in [22, 48, 61, 62, 76, 77]. It is however to note that the main accent in the design of NB-LDPC codes is mostly made on 2-regular NB-LDPC codes [21, 22, 62, 78], as they show the best improvement in the asymptotic iterative threshold $\left(\frac{E_b}{N_0}\right)^*$ with respect to the alphabet size q (up to $q = 64$). It is also important to note that 2-regular NB-LDPC codes have a logarithmic minimum distance, thus they might be unable to achieve very low BERs; this point will be illustrated later on in this chapter. To the best of our knowledge, 2-regular NB-LDPC codes can only achieve $BER = 10^{-10}$, and this with a significant alphabet size q, which implies an important decoding complexity. Other works on NB-LDPC codes [33, 36, 37, 79–83] can also be mentioned, such as works of Djordjevic *et al.* [36, 84, 85] on non-binary codes for optical communication. The most of the works address the complexity issue of decoding of non-binary codes. For instance, a Min-Max decoding has been suggested in [86], while the

authors in [87] proposed a version of a Gallager-B decoding algorithm based on symbol representation of message passing algorithm from [34]. Another version of message-passing, the so called binary message passing algorithm from [88] has been suggested for decoding of non-binary codes used for optical channel transmissions.

Given all the said above, regular NB-LDPC codes did not seem to be so good candidates for optical-fiber transmissions because of their poor asymptotic/d_{min} properties and higher decoding complexity, and the most of the optical community has recently turned into the design of so called Spatially-Coupled LDPC (SC-LDPC) codes [89, 90]. SC-LDPC codes offer good performance at large codelengths and a regular code structure, which is highly appreciated in the optics community because of implementation reasons. Their decoder complexity and latency are however a big issue (a SC-LDPC decoder of window size W runs over a graph with WN bit nodes in order to decode N bits).

In this chapter, let us reconsider regular NB-LDPC codes in the setting of high code rates r ($0.8 \leq r \leq 0.9$) and to see if there are still some regular NB-LDPC codes that might be interesting in our setting.

4.2 Performance analysis of high-rate NB-LDPC Codes

In order to an efficient high-rate coded modulation scheme, one needs to choose a code ensemble having both *good asymptotic performance* (to guarantee that the BER after decoding improves even for high levels of channel noise) and *good typical minimum distance* (to guarantee that the error probability after decoding does not experience the "error-floor" effect and therefore achieves very low BER values). In what follows, one studies which codes within the $\mathcal{C}_{LDPC}(a, d, m, n)$ ensemble, defined in Section 2.2.3, are the most suited from asymptotic and minimum distance considerations.

4.2.1 Asymptotic analysis of NB-LDPC codes over the BEC

First, let us assume the transmission over the BEC with erasure probability ε, and let us directly apply the density evolution, explained in Section 2.3.1, to the $\mathcal{C}_{LDPC}(a, d, m, n)$ ensemble, and observe the asymptotic threshold behaviour with respect to the code rate r.

As a result of the density evolution, Figure 4.1 compares thresholds ε^* (Definition 2.3.1) of three ensembles, $\mathcal{C}_{LDPC}(2, d, m)$ (top picture), $\mathcal{C}_{LDPC}(3, d, m)$ (middle picture) and $\mathcal{C}_{LDPC}(4, d, m)$ (bottom picture), plotted for different values of d (and thus of r as $r = 1 - \frac{a}{d}$) and q (here $q \in \{2, 4, 8, 16, 64\}$). Moreover, Figure 4.2 plots threshold values of the same NB-LDPC ensembles, but per alphabet size q ($q = 2; 4; 16$). One observes that:

1) In the region of medium code rates $0.3 \leq r \leq 0.6$, the threshold of 2-regular NB-LDPC codes improves a lot with q, while the threshold of 3- and 4-regular NB-LDPC codes strictly worsens with q.

2) In the region of high code rates ($r > 0.75$), the threshold behavior of 3- and 4-regular codes is similar to what have been observed for lower rates but the change in thresholds for different values of q is much smaller. Indeed, at $r = 0.8$ the difference of thresholds of 3-regular codes for $q = 2$ and $q = 4$ is only 0.001, which is negligeable.

The second observation is critical for the high-rate code design: it shows that 3- and 4-regular NB-LDPC codes with moderate values of q do not loose much in ε^*. Figure 4.2 supports even more 3-regular NB-LDPCs: one can see that their thresholds ε^* are comparable to the threshold of 2-regular NB-LDPC codes up to $q = 16$.

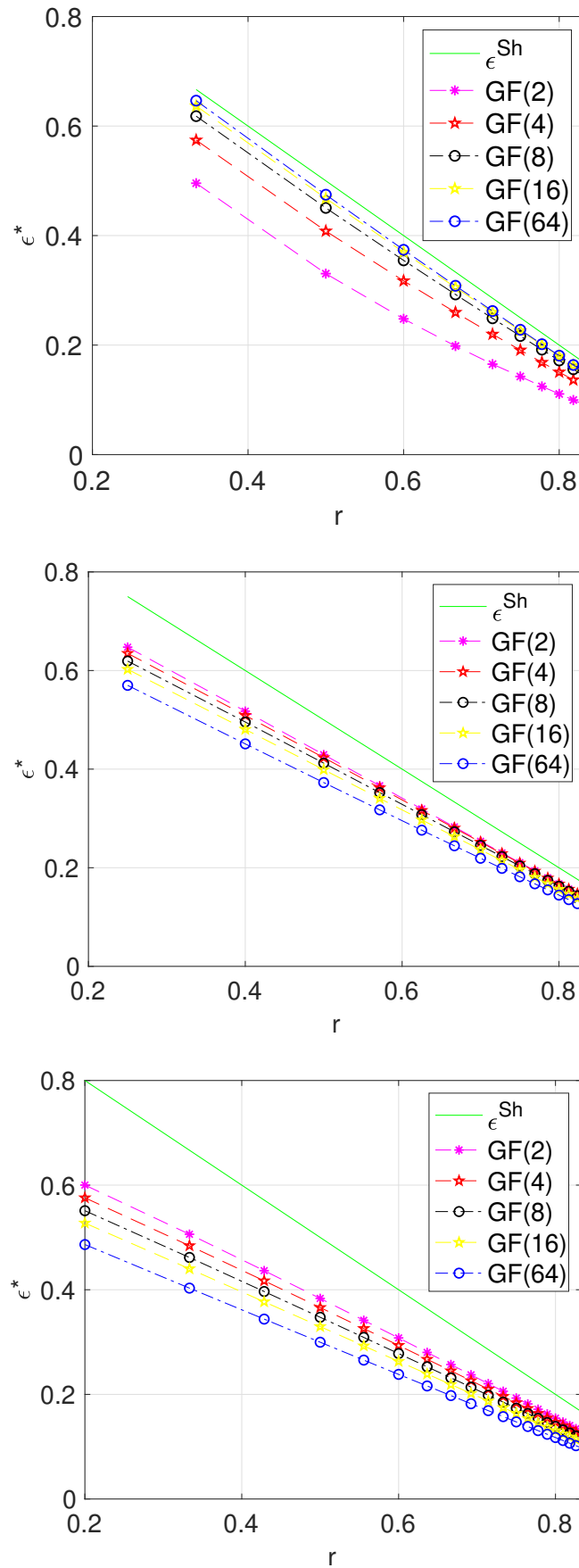Figure 4.1: ε^* vs. r for $(2,d)$ (top picture), $(3,d)$ (middle picture) and $(4,d)$ (bottom picture) NB-LDPC codes. $d = \frac{a}{1-r}$ and ϵ^{Sh} is the Shannon capacity.
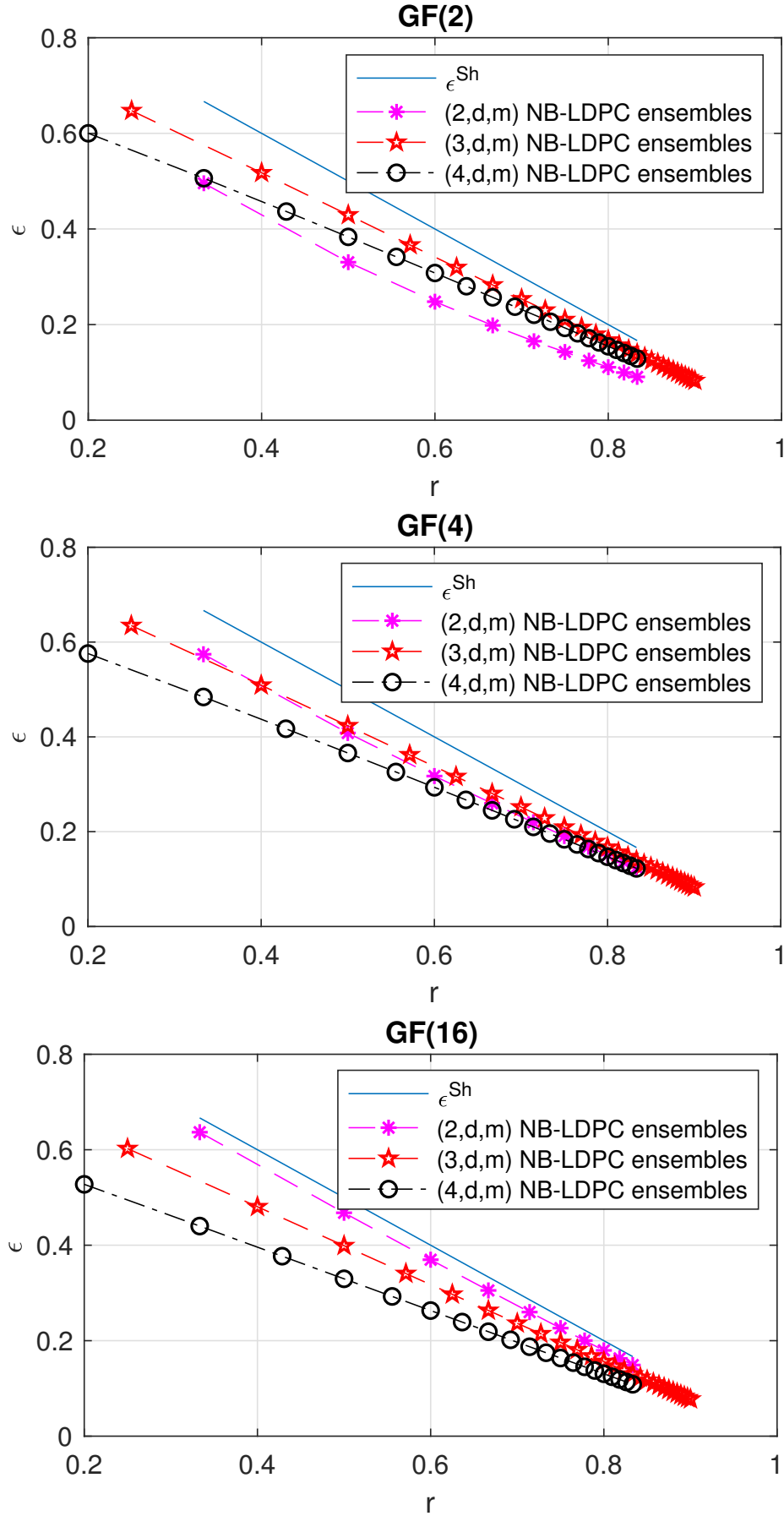
Figure 4.2: The threshold ε^* vs. the code rate r for $(2, d, m)$, $(3, d, m)$ and $(4, d, m)$ NB-LDPC ensembles over the BEC, $d = \frac{a}{1-r}$ for $q = 2; 4; 16$.
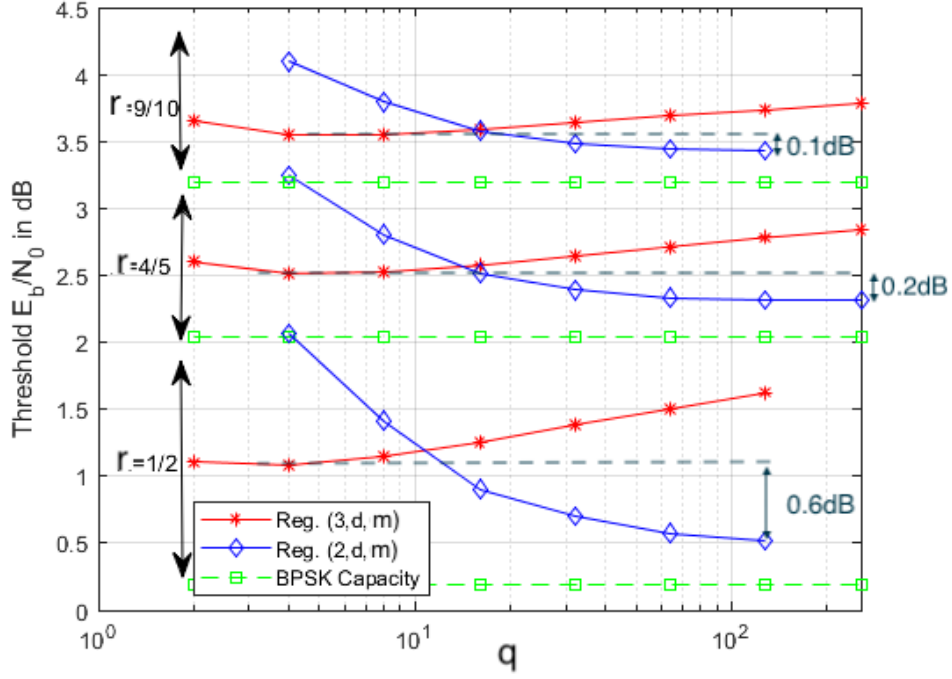
Figure 4.3: Thresholds of $\mathcal{C}_{LDPC}(2, d, m)$ and $\mathcal{C}_{LDPC}(3, d, m)$ over the binary input AWGN channel, $d = \frac{a}{1-r}$, $m = \log_2(q)$, for rates $r = 1/2; 4/5; 9/10$ (from bottom to top).

A similar result can also be reported over the binary-input AWGN channel with the BPSK signaling. Figure 4.3 shows the approximation of the AWGN thresholds for different rates $r \in \{1/2, 4/5, 9/10\}$ and $2 \leq q \leq 256$, obtained with Monte-Carlo density evolution [51–53]. For any rates of Figure 4.3, an intersection point seem to operate between $q = 8$ and $q = 16$. Before this point, 3-regular NB-LDPC codes outperform and after this point it is 2-regular NB-LDPC codes. Note that in the high-rate regime, there is no a strict monotonic degradation of the threshold w.r.t. q for 3-regular NB-LDPC codes, as it was the case over the BEC. For $q = 4$ and $q = 8$, one has even (slightly) better thresholds of $\mathcal{C}(3, d, m)$ in comparison with $q = 2$. Note that, for $q = 4$ and $q = 8$, the asymptotic threshold of 3-regular NB-LDPC codes outperforms the one of 2-regular NB-LDPC codes. In fact, one needs to take $q \geq 32$ in order to ensure that 2-regular codes perform sufficiently well. We can also observe that the higher the code rate r is, the more the gap between the lowest thresholds of 2- and 3-regular LDPC codes become smaller (e.g. gap of 0.6dB at rate $r = 0.5$, while a gap of 0.1dB at $r = \frac{9}{10}$).

4.2.2 Finite-length analysis of NB-LDPC codes using minimum distance approach

By using tools from Section 2.3.2 let us present some results for high-rate NB-LDPC codes.

For 2-regular NB-LDPC codes, the typical Hamming distance is upper bounded [34] by

$$d_{\mathsf{min}} \leq 2 + 2\log_{d-1} \frac{n}{2q} \tag{4.1}$$
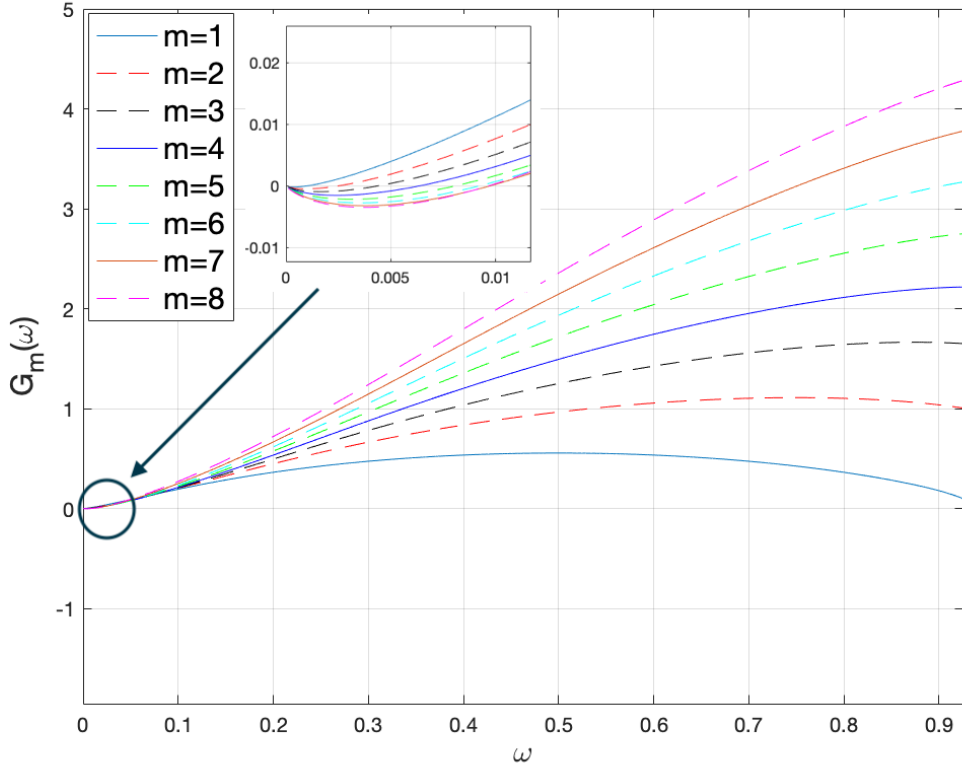
Figure 4.4: Growth rate $G_m(\omega)$ of the $(3,15,m)$ NB-LDPC ensemble.

which in fact means that d_{min} of 2-regular codes is logarithmic in the codelength n. This gives rise to poor values of d_{min}, as illustrated in Table 4.1 for $\mathcal{C}(2,d,m,n)$. For $\mathcal{C}(a,d,m,n)$ with $a>2$, it is known [34] that d_{min} grows linearly with n. One can observe from Table 4.1 that d_{min} of 3- and 4-regular ensembles grows fast with q (up to the value of q around 16 when the number $n=\frac{N}{m}$ of variable nodes in the associated Tanner graph of the code becomes too restrictive). Table 4.1, i.e. the estimation of d_{min}, is obtained using (4.1) when $a=2$. For $a>2$, $d_{\mathsf{min}} \approx \gamma n$, where γ is the value obtained when $G_m(\omega) = 0$. For instance, $\gamma = 0.0064$ for $(3,15)$ LDPC codes over $\mathrm{GF}(16)$. Equation (4.1), together with Table 4.1 and lower bounds on the ML decoding error probability from Chapter 2, strongly suggest that 2-regular NB-LDPC codes are not good candidates for high-rate code applications requiring low BERs after decoding.

(a,d) \ q	2	4	8	16	32	64
(2,10)	10	10	9	9	9	9
(3,15)	32	40	46	51	51	49
(4,20)	80	90	83	82	80	71

Table 4.1: Estimation of d_{min} as a function of q for $r = 0.8$ and fixed binary code-length $N = 32000$.
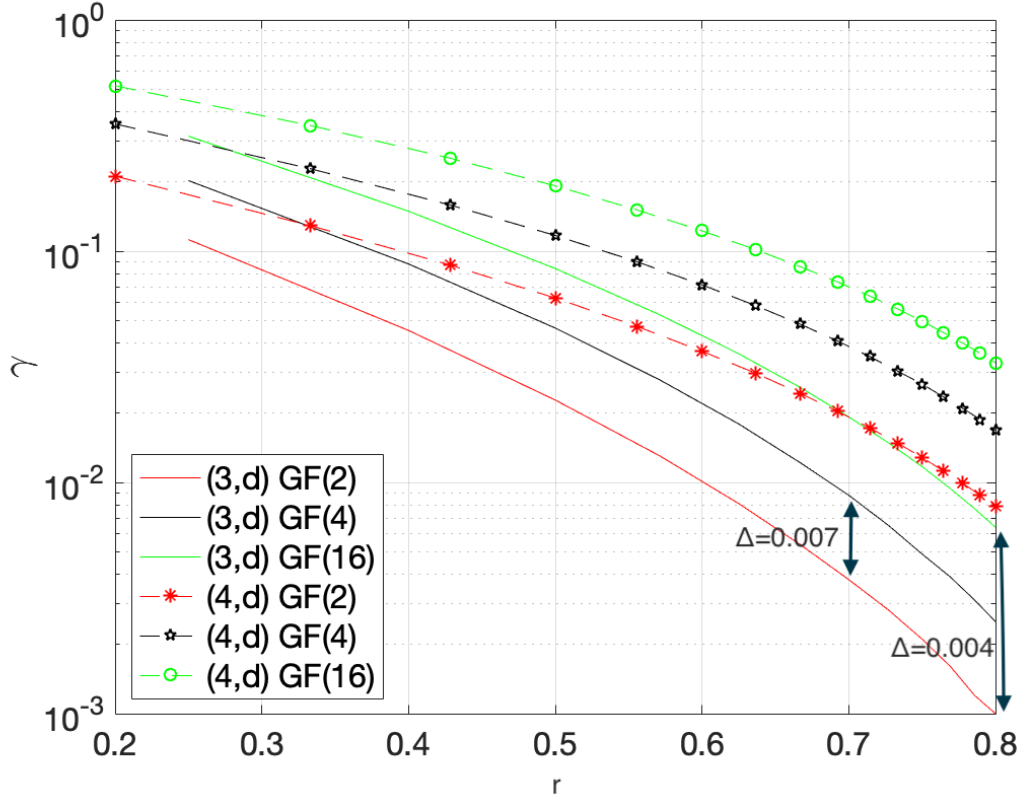
Figure 4.5: Minimum distance for (a, d) LDPC codes over GF(q), $q = \{2, 4, 16\}$ and $d = \frac{a}{1-r}$.

Let us investigate how fast d_{min} grows for NB-LDPC codes. Figure 4.4 illustrates a known result of the asymptotic growth rate $G_m(\omega)$, mentioned in [91]. Denote by γ_m the smallest positive value of ω such that $G_m(\omega) = 0$. Then $d_{min} \approx \gamma_m n$. Figure 4.4 therefore shows that d_{min} quickly grows with q; this trend remains true for all values of $a > 2$ and all values of d.

However, in the region of high code rates, γ_m is not as large. This is illustrated in Figure 4.5. Figure 4.5 shows the behaviour of γ_m with respect to the code rate r, for degrees $a = 3; 4$ and alphabet sizes $q = 2; 4; 16$. Given a and r, the degree d is fixed as $d = \frac{a}{1-r}$. Figure 4.5 shows that γ_m (and thus d_{min}) significantly decreases with r. Therefore, if one is looking to achieve very low BERs such as $BER = 10^{-15}$, one should pay a particular attention to chosen parameters a and q. Note however that increasing a has an impact in a much higher decoding complexity (at high code rates, d also quickly increases with a). Fortunately, it is possible to improve γ_m by increasing q. For instance, for $(3, d)$ regular NB-LDPC codes one can gain $\Delta\gamma_m = 0.007$ at $r = 0.7$, when passing from $q = 2$ to $q = 4$, or $\Delta\gamma_m = 0.0007$ at $r = 0.7$, when passing from $q = 2$ to $q = 16$.

4.3   Simulation results

Let us present some performance results for NB-LDPC, over the AWGN transmission channel with M-QAM scheme. Given the fact that the SICM always behaves at least as

good as the BICM, all our numerical results have been obtained in the SICM setup.

Let us fix the code rate $r = 0.8$ and the binary codelength $N = 32000$. Figure 4.6 shows the BER of NB-LDPC codes in two cases $M = 16$ (on the left) and $M = 64$ (on the right). Two values of a has been considered: $a = 2$ and $a = 3$. Here it is to note that 4-regular codes do not have such a good asymptotic threshold as 2- and 3-regular codes, so they have been eliminated. Moreover, 4-regular codes are more complex to encode, which is a big drawback in optical communications. Therefore, Figure 4.6 presents the BER performance of $(2, 10)$ and $(3, 15)$ NB-LDPC codes. One can observe that $(3, 15)$ NB-LDPC codes outperform $(2, 10)$ NB-LDPC codes, and thus even when short cycles from Tanner graphs of 2-regular codes have been removed by the Progressive-Edge Growth (PEG) algorithm [92]. For $M = 16$, even the most efficient $(2, 10)$ NB-LDPC codes (over $GF(16)$) have an error-floor at $BER \approx 5 \cdot 10^{-5}$ due to their logarithmic d_{min}. As another reference curve for $M = 16$, the BER of a binary SC-LDPC code of codelength N has been also presented. Its code parameters have been chosen to take into account the termination rate loss and to obtain the code rate $r = 0.8001$ (we chose $a = 3$, $d = 16$, $L = 16$ and $w = 1$ with one-side coupling). One can observe that this curve have good performance but not better than others curves, less complex to encode.

For $M = 16$, a $(3, 15)$ NB-LDPC code over $GF(4)$ behaves the best BER performance. It has a worse threshold than a $(2, 10)$ NB-LDPC with $q = 16$, but a better slope of the BER curve and the absence of the error-floor due to its better minimum distance properties.

4.4 Discussion

The asymptotic threshold of a NB-LDPC ensemble is a measure of how close one can get to the Shannon limit, under sufficiently large codelengths. Moreover, a sufficiently good typical d_{min} is a necessary condition for a code from the ensemble to be able to attain low values of BER. Note that 2-regular codes have poor values of d_{min}. This implies that, in order to achieve low BER, a large value of q together with a tedious optimisation of edge labels is needed. One observe that 3-regular NB-LDPC codes present a very good performance tradeoff in terms of $\left(\frac{E_b}{N_0}\right)^*$ and d_{min}, if one considers moderate values of q, $4 \leq q \leq 16$. Thanks to relatively high values of d_{min}, there is no need to increase q too much. Moreover, optimisation of edge labeling is neither really necessary.

Here is a recap table for this chapter:

	threshold	d_{min}	encoding/decoding complexity
NB-LDPC:			
$(2, d)$	good	very bad	good
$(3, d)$	good	medium	medium
$(4, d)$	medium	good	bad

As a conclusion, choosing $(3, d)$ LDPC codes with medium values of q seems to be a good choice for high-throughput optical communications.
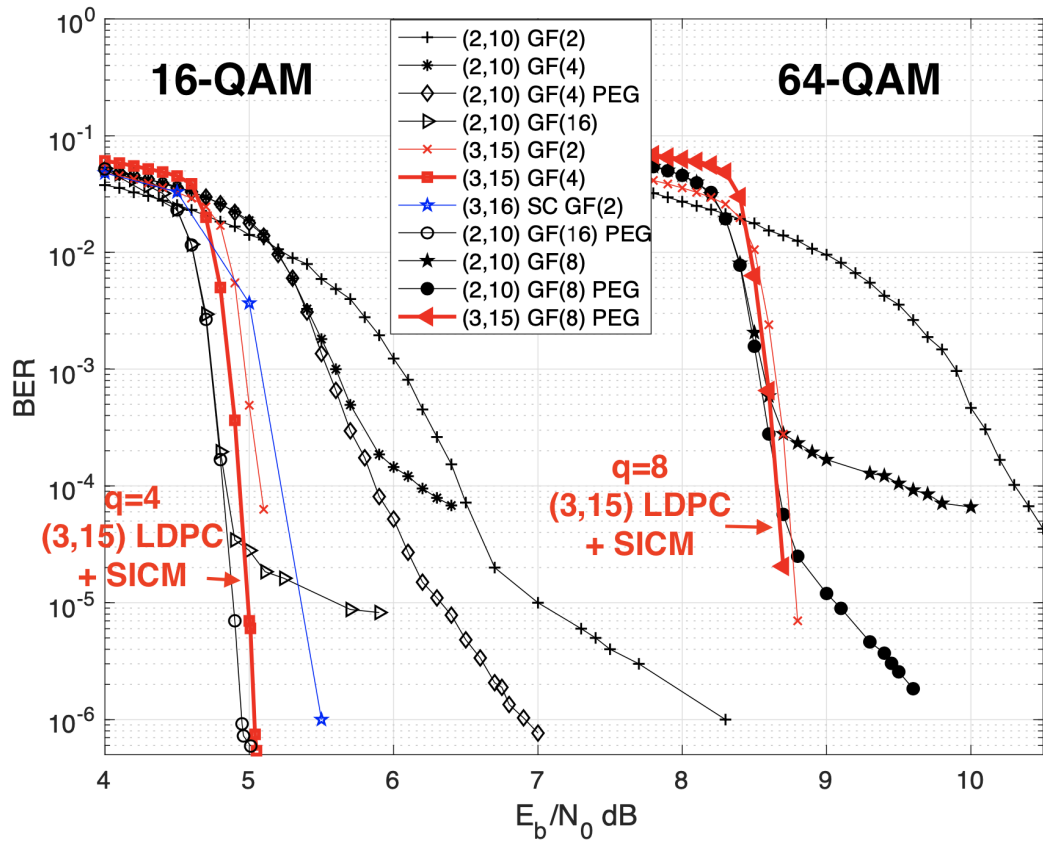
Figure 4.6: Bit error-rate performance of M-QAM SICM schemes based on $(2, 10)$ and $(3, 15)$ NB-LDPC codes of $r = 0.8$ and $N = 32000$ for $M = 16; 64$ and $q \in \{2, 4, 8, 16\}$. Compared to state-of-the-art blue curve: spatially-coupled code.

Bibliography

[76] Iryna Andriyanova and Kenta Kasai. "Finite-length scaling of non-binary (c, d) LDPC codes for the BEC". In: *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA*. 2010, pp. 714–718. DOI: `10.1109/ISIT.2010.5513596`. URL: `https://doi.org/10.1109/ISIT.2010.5513596` (cit. on p. 57).

[77] Irina E Bocharova, Boris D Kudryashov, Vitaly Skachek, and Yauhen Yakimenka. "Average spectra for ensembles of LDPC codes and applications". In: *2017 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2017, pp. 361–365 (cit. on p. 57).

[78] L. Dolecek, D. Divsalar, Y. Sun, and B. Amiri. "Non-Binary Protograph-Based LDPC Codes: Enumerators, Analysis, and Designs". In: *IEEE Transactions on Information Theory* 60.7 (July 2014), pp. 3913–3941. DOI: `10.1109/TIT.2014.2316215` (cit. on p. 57).

[79] G. Liga, A. Alvarado, E. Agrell, and P. Bayvel. "Information Rates of Next-Generation Long-Haul Optical Fiber Systems Using Coded Modulation". In: *Journal of Lightwave Technology* 35.1 (Jan. 2017), pp. 113–123. ISSN: 0733-8724. DOI: `10.1109/JLT.2016.2603419` (cit. on p. 57).

[80] Christian Häger, Alexandre Graell i Amat, Fredrik Brännström, Alex Alvarado, and Erik Agrell. "Terminated and Tailbiting Spatially Coupled Codes With Optimized Bit Mappings for Spectrally Efficient Fiber-Optical Systems". In: *J. Lightwave Technol.* 33.7 (Apr. 2015), pp. 1275–1285. URL: `http://jlt.osa.org/abstract.cfm?URI=jlt-33-7-1275` (cit. on p. 57).

[81] David Declercq, Maggy Colas, and Guillaume Gelle. "Regular GF (2^q)-LDPC Modulations for higher order QAM-AWGN channels". In: 2004 (cit. on p. 57).

[82] A. Abdmouleh. *Non-binary LDPC codes associated to high order modulations*. PhD thesis, University of Bretagne Sud, 2017 (cit. on p. 57).

[83]   S. Kruglik, V. Potapova, and A. Frolov. "On Performance of Multilevel Coding Schemes Based on Non-Binary LDPC Codes". In: *European Wireless 2018; 24th European Wireless Conference*. May 2018, pp. 1–4 (cit. on p. 57).

[84]   Ivan B Djordjevic and Bane Vasic. "Nonbinary LDPC codes for optical communication systems". In: *IEEE Photonics Technology Letters* 17.10 (2005), pp. 2224–2226 (cit. on p. 57).

[85]   Murat Arabaci, Ivan B Djordjevic, Ross Saunders, and Roberto M Marcoccia. "High-rate nonbinary regular quasi-cyclic LDPC codes for optical communications". In: *Journal of Lightwave Technology* 27.23 (2009), pp. 5261–5267 (cit. on p. 57).

[86]   Valentin Savin. "Min-Max decoding for non binary LDPC codes". In: *2008 IEEE International Symposium on Information Theory*. IEEE. 2008, pp. 960–964 (cit. on p. 57).

[87]   Francisco Lázaro, Alexandre Graell i Amat, Gianluigi Liva, and Balázs Matuz. "Symbol Message Passing Decoding of Nonbinary Low-Density Parity-Check Codes". In: *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE. 2019, pp. 1–5 (cit. on p. 58).

[88]   Gottfried Lechner, Troels Pedersen, and Gerhard Kramer. "Analysis and design of binary message passing decoders". In: *IEEE transactions on communications* 60.3 (2011), pp. 601–607 (cit. on p. 58).

[89]   A Jimenez Felstrom and Kamil Sh Zigangirov. "Time-varying periodic convolutional codes with low-density parity-check matrix". In: *IEEE Transactions on Information Theory* 45.6 (1999), pp. 2181–2191 (cit. on p. 58).

[90]   Shrinivas Kudekar, Thomas J. Richardson, and Rüdiger L. Urbanke. "Threshold Saturation via Spatial Coupling: Why Convolutional LDPC Ensembles Perform So Well over the BEC". In: *IEEE Transactions on Information Theory* 57.2 (2011), pp. 803–834. DOI: 10.1109/TIT.2010.2095072 (cit. on p. 58).

[91]   Shengtian Yang, Thomas Honold, Yan Chen, Zhaoyang Zhang, and Peiliang Qiu. "Weight Distributions of Regular Low-Density Parity-Check Codes Over Finite Fields". In: *IEEE Transactions on Information Theory* 57 (Nov. 2011). DOI: 10.1109/TIT.2011.2162642 (cit. on p. 63).

[92]   Xiao-Yu Hu, E. Eleftheriou, and D. M. Arnold. "Regular and irregular progressive edge-growth tanner graphs". In: *IEEE Transactions on Information Theory* 51.1 (2005), pp. 386–398 (cit. on p. 64).

[93]   Vishwambhar Rathi and Ruediger Urbanke. "Density evolution, thresholds and the stability condition for non-binary LDPC codes". In: *IEE Proceedings-Communications* 152.6 (2005), pp. 1069–1074 (cit. on pp. 71–73).

NB-LDPC family for high code rates: RPP codes

In the previous chapter, a choice of the most suitable code parameters for the optical-fiber transmission has been made, for a family of high-rate NB-LDPC codes. It has been shown that $(3, d)$ NB-LDPC codes over $GF(4)$ seem to be the best choice, if one is restricted to a regular code construction. Unfortunately, because of implementation constraints of optical systems, it is not desirable to make an extension to irregular codes : the code construction is recommended to be regular or quasi-regular.

This chapter descries our extension of NB-LDPC codes to doubly-generalized NB-LDPC codes: the so called *Repetition-Parity-Parity (RPP)* code family. It which would keep the decoding complexity similar to the usual LDPC construction, but would behave better in comparison with LDPC counterparts at high code rates. In order to enlarge our search space, we allow ourselves the use of extended alphabets, but of moderate alphabet size.

5.1 State of the art: doubly-generalized LDPC codes

In the classical LDPC code design, the Tanner graph is composed of variable nodes (VN) that correspond to repetition codes, and of check nodes (CN) that correspond to single parity-check codes. As for Generalised LDPC (GLDPC) codes [94, 95], their CN may correspond to other component codes, which are not necessarily parity codes. Finally, Doubly Generalised LDPC (DG-LDPC) codes [96], or Tanner codes [97], can not only have various types of CN, but they are also allowed to have different component codes at the VN side. Note that the asymptotic iterative analysis of DG-LDPC codes have been performed for the Binary Erasure Channel (BEC) [98, 99], as well as over the Gaussian channel [100, 101]. The asymptotic growth rate analysis has been done in [102].

It is interesting to notice that the most used component codes in GLDPC and DG-LDPC constructions (excepting repetition and parity-check codes) are Hamming and BCH codes [103]: they are relatively easy to decode and they enjoy good minimum distance properties. In general, however, DG-LDPC codes are less known that classical LDPC
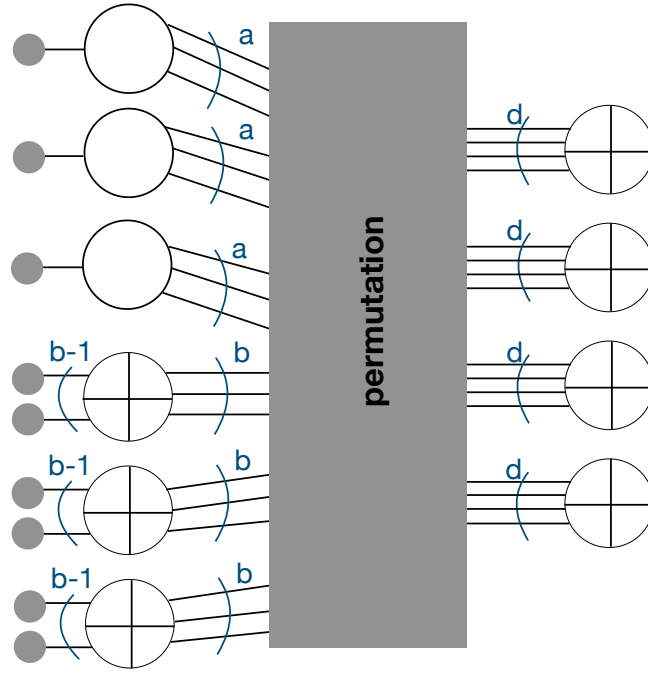
Figure 5.1: Structure of a (a, b, d, α, m) RPP code. Its Tanner graph contains a fraction α of VN of type A and a fraction $1 - \alpha$ of VN of type B. $\bigcirc$ are repetition component codes, $\oplus$ – single-parity check codes, and $\bullet$ – coded symbol nodes.

codes, as they are more difficult to handle and more complex to decode.

5.2   **Repetition-Parity-Parity** (a, b, d, α, m, n) **construction**

Let us introduce a new code family which is a particular case of DG-LDPC codes and that is called repetition-Parity-Parity (RPP):

Definition 5.2.1 A RPP code is parametrized by (a, b, d, α, m, n). It is a DG-LDPC code of symbol codelength n defined over $GF(2^m)$, with the following structure of its Tanner graph presented in Figure 5.1:
- a fraction α of its variable nodes (VN) is said to be of type A. These VNs correspond to repetition codes over $GF(2^m)$ and of codelength $a > 2$;
- a fraction $(1 - \alpha)$ of its variable nodes (VN) is said to be of type B. These VNs correspond to single parity-check codes over $GF(2^m)$, of codelength $b > 2$ and of dimension $b - 1$;
- nodes representing coded symbols over $GF(2^m)$ are connected both to VN nodes of type A and B: each A-type VN node is connected to exactly one symbol node, and each VN node of type B is connected to $b - 1$ symbol nodes;
- all its check nodes (CN) correspond to single parity-check codes over $GF(2^m)$, of codelength d;
- each edge connecting a variable and a check node is labelled by $f : GF(2^m) \to GF(2^m)$.

An ensemble of (a, b, d, α, m, n) DG-LDPC codes is defined over all possible edge permutations and edge labels.

One assumes $0 \leq \alpha \leq 1$, $a < d$, $b < d$ and $a, b, d \in \mathbb{N}$.

A binary codelength of the code is, as before, $N = mn$. Moreover, let a RPP code have n_A variable nodes of type A and n_B variable nodes of type B. Then, by construction, n_A and n_B satisfy the following:

$$\begin{cases} n_A + (b-1)n_B = n \\ n_A = \alpha(n_A + n_B) \end{cases} \implies \begin{cases} n_A = \frac{\alpha n}{(b-1)(1-\alpha)+\alpha} \\ n_B = \frac{(1-\alpha)n}{(b-1)(1-\alpha)+\alpha} \end{cases} \tag{5.1}$$

The total number of edges n_e in the Tanner graph can be computed as

$$\begin{aligned} n_e &= an_A + bn_B \\ &= \frac{\alpha a + b(1-\alpha)}{(b-1)(1-\alpha)+\alpha}n \end{aligned} \tag{5.2}$$

R If $\alpha = 1$, the RPP ensemble corresponds to the (a, d)-regular NB-LDPC ensemble over $GF(2^m)$.

The iterative decoding algorithm of RPP codes is performed over the Tanner graph in Fig. 5.1 by using a usual decoding scheduling for DG-LDPC codes, including 1) update of messages at the VN side; 2) update of messages at the CN side. This decoding algorithm is a slight extension of the sum-product algorithm presented in Section 2.2.

Lemma 5.2.1 The design code rate r of the (a, b, d, α, m, n) RPP ensemble is

$$r \geq 1 - \frac{1}{d} \cdot \frac{ab}{\alpha b + a(1-\alpha)(b-1)}. \tag{5.3}$$

Proof. For a Tanner code with the average rate of variable nodes (resp. check nodes) equal to R_{VN} (resp. to R_{CN}), the design rate is [97]

$$r \geq 1 - \frac{1 - R_{CN}}{R_{VN}}.$$

In the case of a (a, b, d, α, m, n) RPP code, one has

$$R_{CN} = \frac{d-1}{d} \tag{5.4}$$

$$R_{VN} = \frac{\alpha}{a} + (1-\alpha)\frac{b-1}{b}. \tag{5.5}$$

∎

5.3 Asymptotic analysis over the BEC

Assuming the transmission over the binary erasure channel and applying the similar approach as in [93], we derive the following density evolution (DE) equations for the (a, b, d, α, m, n) RPP ensemble. Remind that the DE equations are given in terms of probability mass functions. In the particular case of the BEC, they are probability vectors of length $m + 1$. Also, remind that the DE operations are defined with the help of two elementary operations $\boxdot$ and $\boxtimes$, that represent correspondingly the convolution at the repetition nodes and the special convolution at the single parity-check nodes for two input vectors. The reader is referred to equations (2.10) and (2.11) or [93] for more details.
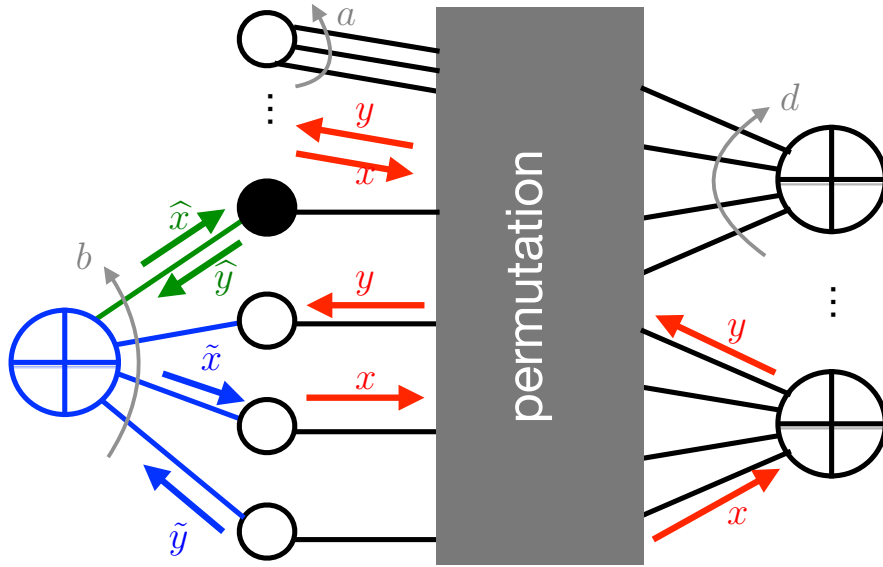
Figure 5.2: Probability vectors x, y, $\tilde{x}$, $\tilde{y}$, $\widehat{x}$ and $\widehat{y}$, associated with different decoding messages over the Tanner graph.

Theorem 5.3.1 Assume transmission over the BEC of probability ε. Let E be the probability vector of length $m+1$ corresponding to channel input messages, the i-th element of which is

$$E(i) = \binom{m}{i} \varepsilon^i (1-\varepsilon)^{m-i}, \quad i = 0 \dots m.$$

Let $x^{(\ell)}$, $y^{(\ell)}$, $\tilde{x}^{(\ell)}$, $\tilde{y}^{(\ell)}$, $\widehat{x}^{(\ell)}$ and $\widehat{y}^{(\ell)}$ be probability vectors of length $m+1$, each of them associated with decoding messages of particular type at decoding iteration ℓ, as is it shown in Figure 5.2 and described in [93]. Then,

$$\begin{cases}
\tilde{y}^{(\ell)} = & E \boxdot y^{(\ell-1)} \\
\widehat{y}^{(\ell)} = & y^{(\ell-1)} \\
\tilde{x}^{(\ell)} = & \widehat{y}^{(\ell)} \boxtimes \left(\boxtimes^{b-2} \tilde{y}^{(\ell)} \right) \\
\widehat{x}^{(\ell)} = & \boxtimes^{b-1} \tilde{y}^{(\ell)} \\
x^{(\ell)} = & \gamma \left(E \boxdot \left(\boxdot^{a-1} y^{(\ell-1)} \right) \right) + \frac{1-\gamma}{b} \left(\widehat{x}^{(\ell)} + (b-1)(E \boxdot \tilde{x}^{(\ell)}) \right) \\
y^{(\ell)} = & \boxtimes^{d-1} x^{(\ell)}
\end{cases} \tag{5.6}$$

where $y^{(0)} = (0, \dots, 0, 1)$ and

$$\gamma = \frac{\alpha a}{\alpha a + (1-\alpha)b}. \tag{5.7}$$

Proof. Let us start with a particular case of binary RPP codes below. If one assumes the binary RPP ensemble characterized by $(a, b, d, \alpha, 1)$, then $x^{(\ell)}$, $y^{(\ell)}$, $\tilde{x}^{(\ell)}$, $\tilde{y}^{(\ell)}$, $\widehat{x}^{(\ell)}$ and $\widehat{y}^{(\ell)}$ are erasure probabilities, associated with decoding messages of particular type at decoding iteration ℓ. Before the start of decoding ($\ell = 0$), $y^{(0)} = 1$. Then, by following the flow of the decoding messages exchange in Figure 5.2, we obtain the following equations for a decoding iteration $\ell > 0$:

$$
\begin{aligned}
\tilde{y}^{(\ell)} &= \varepsilon y^{(\ell-1)} \\
\widehat{y}^{(\ell)} &= y^{(\ell-1)} \\
\tilde{x}^{(\ell)} &= 1 - (1 - \widehat{y}^{(\ell)})\left(1 - \tilde{y}^{(\ell)}\right)^{b-2} \\
\widehat{x}^{(\ell)} &= 1 - (1 - \tilde{y}^{(\ell)})^{b-1} \\
x^{(\ell)} &= \gamma\varepsilon\left(y^{(\ell-1)}\right)^{a-1} + \frac{1-\gamma}{b}\left(\widehat{x}^{(\ell)} + (b-1)(\varepsilon\tilde{x}^{(\ell)})\right) \\
y^{(\ell)} &= 1 - (1 - x^{(\ell)})^{d-1}
\end{aligned}
$$

where γ is the fraction of edges between VNs and CNs, connected to VN of type A, it is given by (5.7).

The extension to a general case of $m \geq 1$ is straightforward, when using the approach described in [93]. ∎

Definition 5.3.1 The asymptotic iterative threshold ε^* of the RPP ensemble (a, b, d, α, m, n) is the smallest value of $\varepsilon \in (0, 1)$ so that (5.6) has a solution in the limit of decoding iterations $\ell \to \infty$.

For the observation how ε^* depends on the RPP code parameters, the reader is referred to the subsection below.

5.3.1 Numerical DE results

This section presents examples of ε^*, obtained for (a, b, d, α, m, n) ensembles.

Let $a = 3$ and $b = 3$. Note that in this case, for a fixed code rate r, the value of d is fixed and computed as

$$
d = \frac{ab}{\alpha b + a(1-\alpha)(b-1)} \cdot \frac{1}{1-r} = \frac{3}{(2-\alpha)(1-r)}.
$$

Tables 5.1 and 5.2 show values of ε^* for RPP ensembles of rates $r = 0.5$ and $r = 0.8$ respectively, for various values of α and alphabet sizes m. For each value of m, the best value of ε^* is underlined in bold. Figure 5.3 contains all our obtained results, for $r = 0.5;\ 0.6;\ 0.7;\ 0.8$. Dashed lines in Figure 5.3 represent BEC capacity limits $\varepsilon^{Sh} = 1-r$ for each of the considered code rates. It is also to note that the case of $\alpha = 1$ corresponds to the case of $(3, d)$ NB-LDPC ensemble over $GF(2^m)$.

Both Tables 5.1 and 5.2 and Figure 5.3 allow us to observe the following:

- ε^* improves with the decrease of α up to some optimal value (depicted by star in Figure 5.3), and then it starts to degrade.

  For example, the ensemble $(3, 3, 5.0.8, 1)$ has a better threshold than the ensemble $(3, 3, 6, 1, 1)$ (which is the binary $(3, 6)$-regular LDPC ensemble). This can be explained by the fact that, by fixing $\alpha < 1$, one reduces the degree of CN, and this has a positive effect on ε^*.

- The threshold improvement becomes even more significant with the code rate r. This is related to the fact that degrees of CN at high code rates are large, and to reduce them with a help of α is beneficial.

- The improvement of ε^* is finally more substantial for larger values of m. The phenomena can be explained with the help of EXIT charts [104]: the shaping of VN and CN EXIT curves is becomes more and more different with m, which acts in a

α (d) \ m	1	2	3	4	6
0.5 $(d = 4)$	0.4113	0.4541	**0.4684**	**0.4714**	**0.4645**
0.8 $(d = 5)$	**0.4502**	**0.4543**	0.4496	0.4406	0.4196
1 $(d = 6)$	0.4294	0.4234	0.4121	0.3988	0.3728

Table 5.1: ε^* for $(3, 3, d, \alpha, m)$ codes of rate $r = 0.5$ for $\alpha = 0.5;\ 0.8;\ 1$ and $m = 1; 2; 3; 4; 6$.

α (d) \ m	1	2	3	4	6	8
0.1250 $(d = 8)$	0.1154	0.1545	0.1731	0.1796	**0.1798**	**0.1756**
0.3333 $(d = 9)$	0.1314	0.1659	0.1781	**0.1811**	0.1777	0.1718
0.5000 $(d = 10)$	0.1524	0.1736	**0.1800**	0.1799	0.1736	0.1663
0.6364 $(d = 11)$	0.1644	**0.1766**	0.1789	0.1767	0.1682	0.16
0.7500 $(d = 12)$	0.1693	0.1763	0.1759	0.1722	0.1622	0.1535
0.8462 $(d = 13)$	**0.1705**	0.1742	0.1719	0.1671	0.1562	0.147
0.9286 $(d = 14)$	0.1696	0.1709	0.1673	0.1617	0.1502	0.1409
1 $(d = 15)$	0.1675	0.1670	0.1625	0.1564	0.1445	0.1351

Table 5.2: ε^* for $(3, 3, d, \alpha, m)$ for fixed code rate $r = 0.8$.

negative way to the value of ε^*. To have $\alpha < 1$ allows to obtain the shape of the VN EXIT curve, more similar to the shaping of the CN EXIT curve.

α \ m	1	2	4	6
1	1	1	1.2	1.5
0.8	**0.9**	**0.75**	0.8	N/A
0.5	1.6	N/A	**0.5**	**0.5**

Table 5.3: $\frac{E_b}{N_0}^*$ in dB for $(3, 3, d, \alpha, m)$ RPP codes overs the AWGN channel, $\alpha = 0.5; 0.8; 1$ and $m = 1; 2; 4; 6$, given a fixed code rate $r = 0.5$.
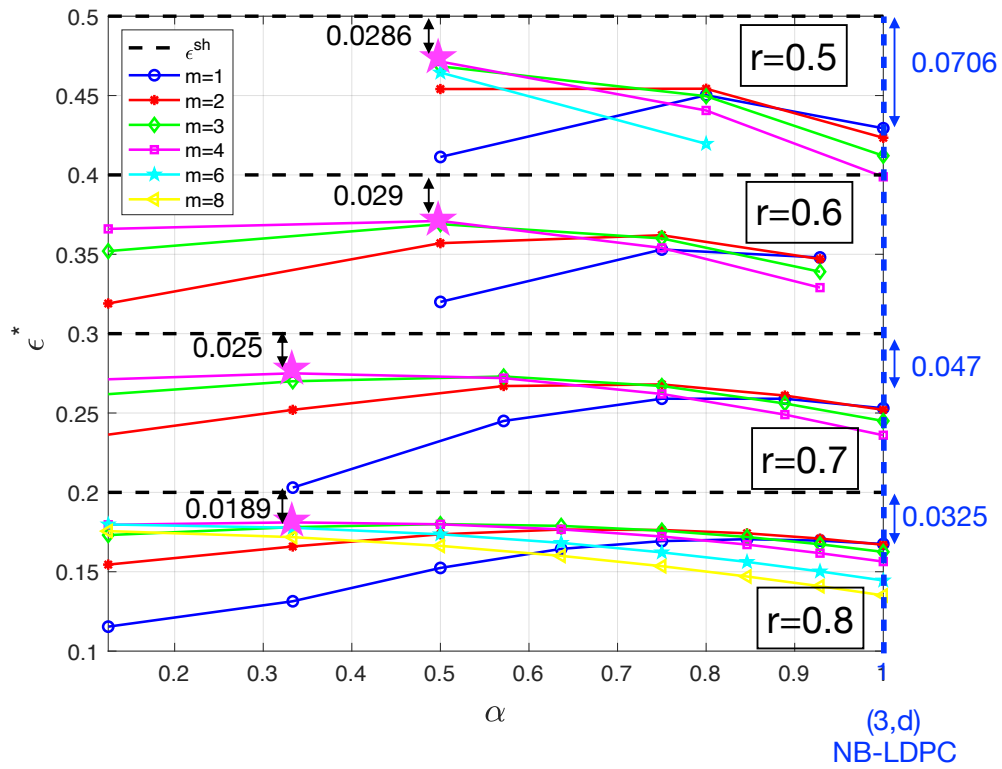
Figure 5.3: Thresholds of $(3, 3, d, \alpha, m)$ RPP codes vs. α, for various values of m and for code rates $r = 0.5; 0.6; 0.7; 0.8$.
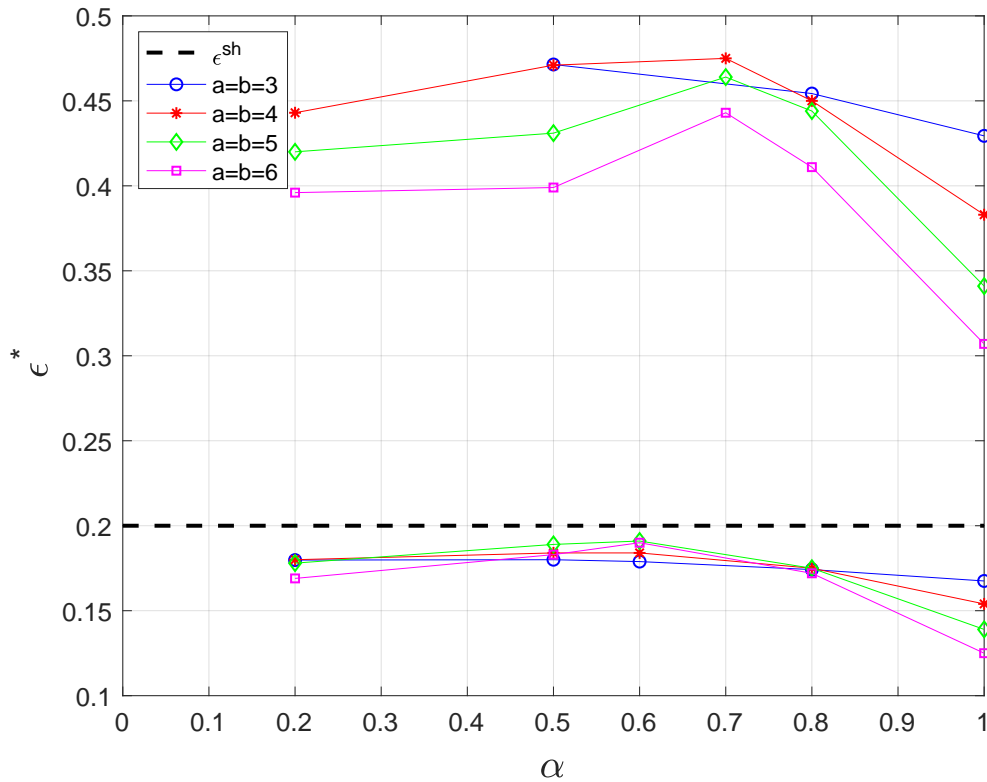

Figure 5.4: Thresholds of RPP codes vs. α, for various values of a, b and m and for code rates $r = 0.5; 0.8$.

Some results for the Gaussian channel are also available. Table 5.3 shows simulated thresholds $\frac{E_b}{N_0}^*$ (dB) over the AWGN channel for $r = 0.5$. One observes a similar behaviour to BEC: the best AWGN threshold are obtained for $\alpha = 0.5$ and large values of m, and the best threshold for $\alpha = 0.8$ is achieved when $m = 2$, exactly like on the BEC case.

Finally, let us see the impact of values of a and b on ε^*. Figure 5.4 depicts the asymptotic thresholds of RPP ensembles of code rates 0.5 and 0.8 with respect to α, in the case of $a = b$. Note that here, for each value of $alpha$, one plots the best threshold value, simulated over $1 \leq m \leq 6$. (The reader is referred to Appendix 6.2for more detailed results for $a = 4; 5; 6$.) One considers 4 numeric values of a: $a = 3; 4; 5; 6$. One observes that, at high code rates, there might be beneficial to consider $a = 4$ and $a = 5$, in contrast to the case of $r = 0.5$ when $a = 3$ is the most interesting parameter value.

5.4 Finite-length analysis

In the previous section it has been shown that having a non-zero number of VN nodes of type B (and thus decreasing α) in the RPP structure is beneficial for the asymptotic iterative threshold for basically all values of m. This section studies how this operation impacts on the typical d_{min} of the RPP ensemble. Remind that the initial goal of our work is to design efficient high-rate channel codes that would be able to attain very low BERs, and one needs to have a linear minimum distance for this.

Our study on d_{min} contains two parts. Firstly, a necessary condition on linear minimum distance is formulated in Section 5.4.1. Secondly, the average weight distribution and the asymptotic growth rate of the (a, b, d, α, m) RPP ensemble are computed in Sections 5.4.2 and 5.4.2.

5.4.1 Necessary condition on linear minimum distance

Our first result on d_{min} properties of the RPP ensemble can be stated as following:

> **Lemma 5.4.1** Let $m = 1$, consider a code chosen at random from the $(a, b, d, \alpha, 1, n)$ RPP ensemble. Let $a > 2$. Then, if the parameters b, d and α are chosen so that $\alpha < \alpha_0$ then d_{min} of the code grows sublinearly in the codelength n,
>
> $$\alpha_0 = \frac{(b-1)d - b}{(b-1)(a+d) - b}. \tag{5.8}$$

One can extend to $m > 1$ using [22]. A cycle of length L in the subgraph implies a valid RPP codeword of weight $\frac{L}{2}$ under some condition on the edge labels. Thus, in general, $\alpha_0 \geq \alpha_m$.

Proof. The proof follows the approach presented in Section II in [105].

Assume a code from the considered RPP ensemble and construct its associated graph of codewords of weight 2 G as it is defined in [105]. Following the definition of G in [105] and taking into account that $a > 2$, the set of nodes of G in our case is the union of nodes of degree b (variable nodes of type B) and of nodes of degree d (check nodes). Moreover, the set of edges of G contains all the edges in associated Tanner graph of the code that connect nodes of degree b with nodes of degree d. Therefore the graph G contains n_B nodes of degree b, $\frac{n_e}{d}$ nodes of degree *at most* d, and it has exactly bn_B edges. Remind that n_B and n_e are given by (5.1) and (5.2) respectively.

Moreover, it has been shown in [105] that, if the graph G contains cycles, then the length of the smallest cycle is proportional to d_{min}. In the particular case of the RPP ensemble, there will be always at least one cycle in G of sublinear codelength when $n_B(b-1) > \frac{n_e}{d}$. Therefore, one deduces that a code from the (a, b, d, α, m, n) ensemble has a sublinear minimum distance if

$$(1-\alpha)(b-1)d > \alpha a(b-1) + (1-\alpha)b,$$

which can be rewritten as in (5.8).   ∎

This result implies the following necessary condition on linear d_{min}:

Corollary 5.4.2 For a RPP ensemble for some fixed parameters a, b and d, one should satisfy the following conditions in order to possibly have a linear d_{min}: (1) the degree a should be larger than 2, and α should satisfy $\alpha > \alpha_0$.

∎ **Example 5.1** For an example, for $a = b = 3$, $m = 1$, one has $\alpha_0 = \frac{2d-3}{2d+3}$. Thus, all code ensembles from Table 5.1 satisfy the necessary condition on d_{min}. As for the ensembles mentioned in Table 5.2, only those with $\alpha \geq 0.8462$ satisfy the necessary condition.   ∎

5.4.2 Sufficient condition on linear minimum distance
Let us develop a sufficient condition on d_{min} of RPP ensembles.

Average weight distribution calculation
The following result holds for the average weight distribution of our code construction:

Theorem 5.4.3 Consider the (a, b, d, α, m, n) RPP ensemble of design rate r. Let $b \geq 2$ and let the respective number of edges in the Tanner graph be equal to n_e. Then, the average number of codewords of Hamming weight $m\omega$ in C is given by:

$$\mathbb{E}[N(C, n\omega)] = \sum_{\tau n=0}^{\omega n} \binom{\alpha n}{\tau n}\binom{(1-\alpha)n}{(\omega-\tau)n}\binom{n_e}{S} \tag{5.9}$$

$$\cdot \frac{\mathsf{coeff}(p_m(y)^{n_e/d}, y^S)}{|GL_2^m|^S} \cdot (2^m-1)^{n\omega}, \tag{5.10}$$

where

$$p_m(y) \triangleq \frac{1}{2^m}\left[(1+|GL_2^m|y)^d + \left(1 - \frac{|GL_2^m|y}{2^m-1}\right)^d (2^m-1)\right] \tag{5.11}$$

and

$$S = \begin{cases} na\omega, & \text{if } \tau n = \omega n \\ a\tau n + L \cdot A(\omega - \tau) & \text{if } 0 \leq \tau n < \omega n \end{cases}, \tag{5.12}$$

while $L \triangleq n_B(b-1)$ and

$$A(\gamma) = (2^m - 2) \left(1 - \prod_{i=0}^{b-2} \frac{L - \gamma n - i}{L - i} \right)$$
$$+ (b-1)(2^m - 1) \left(\frac{\gamma n}{L} + \frac{\gamma n}{L - b - \gamma n} \prod_{i=0}^{b-2} \frac{L - \gamma n - i}{L - i} \right) \quad (5.13)$$

The proof of Theorem 5.4.3 is very similar to the one for non-binary LDPC codes in [106], except the intermediate part related to the calculation of the Hamming weight for VNs of type B. Let us proceed as following: 1) we define an input-output weight enumerator polynomial $q(x, z)$ and prove a simple yet useful result on $q(x, z)$ for a single parity-check codes; 2) we derive an expression for a certain parameter v that will be further used in the proof of Theorem 5.4.3; 3) we prove Theorem 5.4.3.

Let us start with the definition of an input-output weight enumerator.

Definition 5.4.1 Given a linear block code C of codelength n and of dimension k, with a $k \times n$ generator matrix G, its input-output weight enumerator (IOWE) is a polynomial $q(x, z)$ s.t.

$$q(x, z) \triangleq \sum_{i=0}^{k} \sum_{j=0}^{n} A_{i,j} x^i z^i,$$

where $A_{i,j} = A_{i,j}(G)$ is the number of codewords in C that have Hamming weight j and for which the Hamming weight of input vectors is i.

We are interested in the IOWE of a single-parity check code over $GF(2^m)$. Even though the weight enumerator of a single parity-check code is well-know from the state of the art, we were not able to find its formulation in the IOWE form. Therefore, let us formulate and prove the following useful lemma:

Lemma 5.4.4 For a single-parity check code of codelength b, defined over $GF(q)$ with $q \geq 2$,

$$q(x, z) = \frac{1}{q - 1} \Big((1 + z(q - 2))[1 + xz]^{b-1}$$
$$+ (z - 1)[(b - 1)xz - (q - 2)] \Big) \quad (5.14)$$

Proof. By enumeration,

$$q(x, z) = 1 + \binom{b - 1}{1} xz^2 + \frac{1 + (q - 2)z}{q - 1} \sum_{k=2}^{b-1} \binom{b - 1}{k} x^k z^k$$

Here we have used the fact that, for a non-zero input vector from $(GF^*(2^m))^{b-1}$, its parity equals to zero with probability $\frac{1}{q-1}$ and it is non-zero otherwise. Finally, by using the binomial formula, one obtains (5.14) ∎

Let us continue with the following lemma related to the output Hamming weight of n_B distinct single-parity check codes over $GF(q)$:

Lemma 5.4.5 Assume n_B distinct single parity-check codes over $GF(q)$, of codelength

b each, for $b \geq 2$. Let an input word of length $L = (b-1)n_B$ and of Hamming weight γn is encoded by means of these n_B codes. Then the resulting output codeword has the average Hamming weight v,

$$v = \begin{cases} 0, & \text{if } \gamma n = 0, \\ L \cdot A(\gamma) & \text{if } \gamma n > 0 \end{cases}$$

and $A(\gamma)$ is given by (5.13).

Proof. Let us prove Lemma 5.4.5.

The IOWE for n_B parity check codes over $GF(q)$ equals to $q(x,z)^{n_B}$, where $q(x,z)$ is the one from Lemma 5.4.4. Let us define the following important quantity:

$$q_\gamma(z) \triangleq \text{coeff}\left(q(x,z)^{n_B}, x^{n\gamma}\right) \tag{5.15}$$

Then the average Hamming weight v at the ouput of n_B parity codes, given that their input Hamming weight is $n\gamma$, is computed as follows

$$v = \left(\frac{q'_\gamma(z)}{q_\gamma(z)}\right)\bigg|_{z=1} \tag{5.16}$$

Note that, if $\gamma n = 0$, $v = 0$.

Now let $\gamma n > 0$. We have

$$q_\gamma(z)|_{z=1} = \text{coeff}\left(q(x,z)^{n_B}, x^{\gamma n}\right)|_{z=1} \tag{5.17}$$

$$= \text{coeff}\left((1+x)^L, x^{\gamma n}\right) \tag{5.18}$$

$$= \binom{L}{\gamma n}. \tag{5.19}$$

and

$$q'_\gamma(z)|_{z=1} = \left(\frac{d}{dz}\text{coeff}\left(q(x,z)^{n_B}, x^{\gamma n}\right)\right)\bigg|_{z=1} \tag{5.20}$$

$$= \text{coeff}\left(\left(\frac{d}{dz}q(x,z)^{n_B}\right)\bigg|_{z=1}, x^{\gamma n}\right) \tag{5.21}$$

$$= L \cdot \text{coeff}\left(r(x) \cdot (1+x)^{L-b+1}, x^{\gamma n}\right), \tag{5.22}$$

where

$$r(x) = (q-2)[(1+x)^{b-1} - 1] + (b-1)x[(q-1)(1+x)^{b-2} + 1] \tag{5.23}$$

Thus,

$$q'_\gamma(z)|_{z=1} = L\left((q-2)\binom{L}{\gamma n} + (b-1)(q-1)\binom{L-1}{\gamma n - 1}\right.$$
$$\left. -(q-2)\binom{L-b+1}{\gamma n} + (b-1)(q-1)\binom{L-b+1}{\gamma n - 1}\right) \tag{5.24}$$

and

$$v = L\left((q-2)\left(1 - \prod_{i=0}^{b-2}\frac{L - \gamma n - i}{L - i}\right) + (b-1)(q-1)\left(\frac{\gamma n}{L} + \frac{\gamma n}{L - b - \gamma n}\prod_{i=0}^{b-2}\frac{L - \gamma n - i}{L - i}\right)\right)$$

(5.25)

This completes the proof of Lemma 5.4.5.

∎

Now we are ready to prove Theorem 5.4.3.

Proof. Pick at random a code C from given ensemble. The number of its codewords of Hamming weight $n\omega$ is given by

$$N(C, n\omega) = \sum_{u \in W} \mathbb{1}_u(C),$$

(5.26)

where W is the set of all the words of length n and of Hamming weight $n\omega$ over $GF(2^m)$. and $\mathbb{1}_u(G)$ is the indicator function ($\mathbb{1}_u(G) = 1$ if u is a codeword of C). Then the expectation is

$$\mathbb{E}_C[N(C, n\omega)] = \sum_{u \in W} \mathbb{E}[\mathbb{1}_u(C)].$$

(5.27)

Because of the symmetry in the permutation of edges and due to uniform probability of all the possible edge labels on every edge, $\mathbb{1}_u(G)$ is independent of the word u and depends only on its weight and on the partition non-zero symbols u between connections to variable nodes of type A and B. Let τn non-zero symbols of u have been allocated to coded symbols, connected with variable nodes of type A, and the rest - to coded symbols connected with variable nodes of type B. Note that, by construction, $\tau \leq \omega \leq \alpha$. Then,

$$\mathbb{E}[N(C, n\omega)] = (2^m - 1)^{n\omega}\sum_{\tau=0}^{\omega}\binom{\alpha n}{\tau n}\binom{(1-\alpha)n}{(\omega-\tau)n}\mathbb{E}(\mathbb{1}_u(G)|\tau),$$

(5.28)

where $\mathbb{E}(\mathbb{1}_u(G)|\tau)$ is the expectation that a codeword of codelength n with τn non-zero symbols of type A and $(\omega - \tau)n$ symbols of type B is a codeword of randomly chosen code from the considered ensemble. We have

$$\mathbb{E}(\mathbb{1}_w(G)|\tau) = \frac{\text{number of graphs for which } u \text{ is a codeword}}{\text{total number of graphs}}$$

(5.29)

The total number of graphs is given by $n_e!|GL_2^m|^{n_e}$. Let us now compute the number of graphs for which the word u of weight ωa and with τn symbols of type A is a codeword.

The number of edges in the Tanner graph, carrying non-zero symbols, is

$$S = v + a\tau n,$$

(5.30)

where v is given by Lemma 5.4.5. Thus, the total number of graph for which u is a codeword is

$$(n_e - S)!S!|GL_2^m|^{n_e - S}\text{coeff}(p_m(y)^{n_{CN}}, y^S),$$

(5.31)

where n_{CN} is the number of check nodes of degree d in the graph,

$$n_{CN} = \frac{n_e}{d}.$$

The factorial terms correspond to permuting the edges carrying zero value and non-zero value. The term $|GL_2^m|^{n_e - S}$ takes care of the fact that we can put any edge label on the edges carrying the value zero. The polynomial $p_m(y)$ is given as in [45]: first we define the quantity F_d,

$$F_d = |\{(M_1, \ldots, M_d) : \sum_{i=1}^{d} M_i x_i = 0, M_i \in GL_2^m, x_i \in GF_2^m\}|;$$

then

$$p_m(y) = 1 + \sum_{i=1}^{d} \binom{d}{i} F_i y^i = \text{(5.11)}$$

In Summary,

$$\mathbb{E}(\mathbb{1}_w(G)|\tau) = \binom{n_e}{S} \frac{\text{coeff}(p_m(y)^{n_{CN}}, y^S)}{|GL_2^m|^S} \tag{5.32}$$

Substituting (5.32) in the expression for $E(N(C, n\omega))$ gives the desired result.
    This completes the proof of Theorem 5.4.3.   ∎

Asymptotic growth rate analysis
Following Theorem 5.4.3, let us derive the growth rate $G_m(\omega)$ of the RPP ensemble.
    Before to start our calculation, we remind the Hayman method from [38] for approximating the term $\text{coeff}(f(x)^n, x^{\theta n})$ when $n \to \infty$, for $f(x)$ being a finite degree polynomial (satisfying some technical conditions). In particular, we are interested in the well-known result for the function $p_m(y)$, defined in chapter D of [38]:

Lemma 5.4.6 [38] Consider the function $p_m(y)$ from (5.11) and two small positive variables η and θ, i.e. $0 \le \eta, \theta \le 1$. Define

$$p_1(y) = \frac{\eta y}{p_m(y)} \frac{dp_m(y)}{dy} \text{ and } p_2(y) = y \frac{dp_1(y)}{dy}.$$

Then, for $n \to \infty$,

$$\text{coeff}\left(p_m(y)^{\eta n}, y^{\theta n}\right) = \frac{p_m(y_0)^{\eta n}}{y_0^{\theta n} \sqrt{2\pi n p_2(y_0)}}(1 + o(1)),$$

where the term $o(1)$ converges to 0 and y_0 is the unique positive solution of $p_1(y) = \theta$.

Corollary 5.4.7 [38] One has that

$$\log \text{coeff}\left(p_m(y)^{\eta n}, y^{\theta n}\right) = \eta n \log p_m(y_0) - \theta n \log y_0 + o(n),$$

where y_0 is the unique positive solution of

$$\frac{(1 + |GL_2^m|y)^{d-1} - \left(1 - \frac{|GL_2^m|y}{2^m - 1}\right)^{d-1}}{(1 + |GL_2^m|y)^d + \left(1 - \frac{|GL_2^m|y}{2^m - 1}\right)^d (2^m - 1)} = \frac{\theta}{\eta d |GL_2^m|y}. \tag{5.33}$$

The definition of $G_m(\omega)$ has been given in Section 4.2.2. Let us state and prove the following result for the RPP ensemble.

Theorem 5.4.8 Assume an RPP ensemble of parameters (a, b, d, α, m). Define

$$K_0 = \frac{n_e}{n} = \frac{\alpha a + b(1 - \alpha)}{(b - 1)(1 - \alpha) + \alpha} \tag{5.34}$$

and

$$K_1 = \frac{L}{n} = \frac{(b - 1)(1 - \alpha)}{(b - 1)(1 - \alpha) + \alpha} \tag{5.35}$$

Then the asymptotic growth rate $G_m(\omega)$ is given by

$$G_m(\omega) = \omega \log(2^m - 1) + \alpha h\left(\frac{\tau_0}{\alpha}\right) + (1 - \alpha)h\left(\frac{\omega - \tau_0}{1 - \alpha}\right) + \frac{K_0}{d} \log(p_m(y_0))$$

$$+ K_0 h\left(\frac{\theta_m(\tau_0)}{K_0}\right) - \theta_m(\tau_0) \log y_0 - \theta_m(\tau_0) \log |GL_2^m|, \tag{5.36}$$

where $h(x)$ is the entropy function,

$$h(x) = -x \log x - (1 - x) \log(1 - x),$$

and,

$$\theta_m(\tau) = a\tau + K_1(2^m - 2)\left(1 - (1 - K_1(\omega - \tau))^{b-1}\right)$$

$$+ K_1(b - 1)(2^m - 1)\left(K_1(\omega - \tau) + \frac{K_1(\omega - \tau)}{1 - K_1(\omega - \tau)}\left(1 - (1 - K_1(\omega - \tau))^{b-1}\right)\right), \tag{5.37}$$

while τ_0 and y_0 are the unique solutions of (5.38) and (5.33) respectively,

$$\log \frac{\alpha - \tau}{\tau} - \log \frac{1 - \alpha - \omega + \tau}{\omega - \tau} + \frac{\partial \theta}{\partial \tau}\left(\log \frac{K_0 - \theta}{\theta} - \log y_0 |GL_2^m|\right) = 0, \tag{5.38}$$

Proof. Let us denote the summation term of Equation (5.10) corresponding to index τn by $T_{\tau n}$, i.e.

$$T_{\tau n} = \binom{\alpha n}{\tau n}\binom{(1 - \alpha)n}{(\omega - \tau)n}\binom{n_e}{S}\frac{\text{coeff}(p_m(y)^{n_e/d}, y^S)}{|GL_2^m|^S} \cdot (2^m - 1)^{n\omega}.$$

Then the growth rate

$$G_m(\omega) = \max\left(\lim_{n\to\infty}\frac{\log T_0}{n}, \lim_{n\to\infty}\frac{\log T_{\omega n}}{n}, \sup_{\tau\in(0,\omega)}\beta(\omega,\tau)\right), \tag{5.39}$$

where

$$\beta(\omega,\tau) = \lim_{n\to\infty}\frac{\log T_{\tau n}}{n}. \tag{5.40}$$

Using the asymptotic approximation of the binomial coefficient $\log\binom{u}{v} = u\cdot h\left(\frac{v}{u}\right)$[1] and the Hayman approximation mentioned above, one obtains that

$$\begin{aligned}
\beta(\omega,\tau) = \lim_{n\to\infty}\frac{1}{n}&\left\{n\omega\log(2^m-1) + n\cdot h\left(\frac{\tau}{\alpha}\right) + n\cdot h\left(\frac{\omega-\tau}{1-\alpha}\right) + \log\binom{n_e}{S}\right.\\
&\left.+ \log\mathsf{coeff}(p_m(y)^{n_e/d}, y^S) - S\log|GL_2^m|\right\} \tag{5.41}\\
= \omega\log&(2^m-1) + \alpha h\left(\frac{\tau}{\alpha}\right) + (1-\alpha)h\left(\frac{\omega-\tau}{1-\alpha}\right)\\
+ K_0 h&\left(\frac{\theta_m(\tau)}{K_0}\right) + \frac{K_0}{d}\log(p_m(y_0)) - \theta_m(\tau)\log y_0 - \theta_m(\tau)\log|GL_2^m|, \tag{5.42}
\end{aligned}$$

where y_0 satisfies (5.33) and

$$\theta \triangleq \lim_{n\to\infty}\frac{S}{n}.$$

Remind that S is given by (5.12). As

$$\begin{aligned}
A_\infty(\gamma) \triangleq \lim_{n\to\infty}&A(\gamma)\\
=(2^m-2)&\left(1-(1-K_1\gamma)^{b-1}\right) + (b-1)(2^m-1)\left(K_1\gamma + \frac{K_1\gamma}{1-K_1\gamma}\left(1-(1-K_1\gamma)^{b-1}\right)\right),
\end{aligned}$$

and $\tau < \omega$, one obtains that

$$\theta = \theta_m(\tau) = a\tau + K_1 A_\infty(\omega-\tau), \tag{5.43}$$

which results in (5.37).

In order to find $\sup_\tau \beta(\omega,\tau)$, it is needed to find

$$\frac{\partial\beta(\omega,\tau)}{\partial\tau} = \log\frac{\alpha-\tau}{\tau} - \log\frac{1-\alpha-\omega+\tau}{\omega-\tau} + \frac{\partial\theta}{\partial\tau}\left(\log\frac{K_0-\theta}{\theta} - \log y_0|GL_2^m|\right)$$

and we determine τ_0 so that

$$\left.\frac{\partial\beta(\omega,\tau)}{\partial\tau}\right|_{\tau=\tau_0} = 0.$$

∎

---

[1] Remind that $h(\cdot)$ is the entropy function

Corollary 5.4.9 For a (a, b, d, α, n) RPP ensemble, the sufficient condition on linear d_{min} is given by the behaviour of the asymptotic growth rate $G_m(\omega)$ from Theorem 5.4.8 for $\omega \to 0_+$: if $G_m(\omega)$ is negative for small positive values of ω, the corresponding RPP ensemble has a linear minimum distance.

■ **Example 5.2** It is verified that the RPP ensembles with $a = b = 3$ from Tables 5.1 and 5.2, satisfying the necessary condition on d_{min}, also satisfy the sufficient condition.   ■

5.5   Simulation results

Let us present some numerical results, illustrating the performance of RPP codes.

Fig. 5.5 shows the BER performance of $(3, 3, d, \alpha, m)$ RPP codes of fixed rate $r = 0.5$ and of binary codelength $N = 36000$ bits. The following values of d have been tested: $d = 4; 5; 6$, this corresponds to the following values of α: $\alpha = 0.5; 0.8; 1$. As for the alphabet sizes, we chose $m = 1; 2; 4; 6$. As expected from Table 5.1, the codes with $\alpha = 0.5$ and $m = 2$ have the best threshold performance among plotted curves. Note that they also present a steep waterfall region. Similar behaviour is also observed for the AWGN channel 5.7, where $\alpha = 0.5$ and $m \in \{4, 6\}$ have the best threshold performance. Remind that $\alpha = 1$ represents the classical NB-LDPC codes case. One observes the improvement of $\Delta\varepsilon = 0.02$ between the best NB-LDPC code and the best RPP code of rate 0.5.

For code rate $r = 0.8$, among the BER curves of codes of binary codelength of 36000 bits with $a = 3$, $b = 3$, $\alpha = 0.8462; 0.9284; 1$ and $m = 1; 2; 4$, the best performance, among the plotted curve, is observed for $\alpha = 0.8462$ and $m = 2$. This also coincides with the results shown in Table 5.2.

5.6   Conclusion

This chapter introduced a new class of (a, b, d, α, m, n) Repetition-Parity-Parity (RPP) codes, having a fraction $(1 - \alpha)$ of single parity-check nodes at the variable nodes side. We argue that, if the fraction of the parity-check nodes is not too large, it is beneficial for the asymptotic iterative threshold of the ensemble, and it does not change the behaviour of d_{min} of the ensemble.

In the work, DE equations for the (a, b, d, α, m) ensemble have been derived; the DE results are coherent with simulated BER curves. Moreover, both necessary and sufficient conditions on linear minimum distance have been formulated.

In overall, (a, b, d, α, m) codes seem to be good candidates for medium- and high-rate applications, and a further investigation on this code ensemble should be continued.

Figure 5.5: BER vs. ε for $(3, 3, d, \alpha, m)$ code of rate $r = 0.5$ and of binary code-length 36000, with $\alpha = 0.5; 0.8; 1$ and $m = 1, 2, 4, 6$.

Figure 5.6: BER vs. ε for $(3, 3, d, \alpha, m)$ code of rate $r = 0.8$ and of binary code-length 36000, with $\alpha = 0.8462; 0.9286; 1$ and $m = 1, 2, 4$.
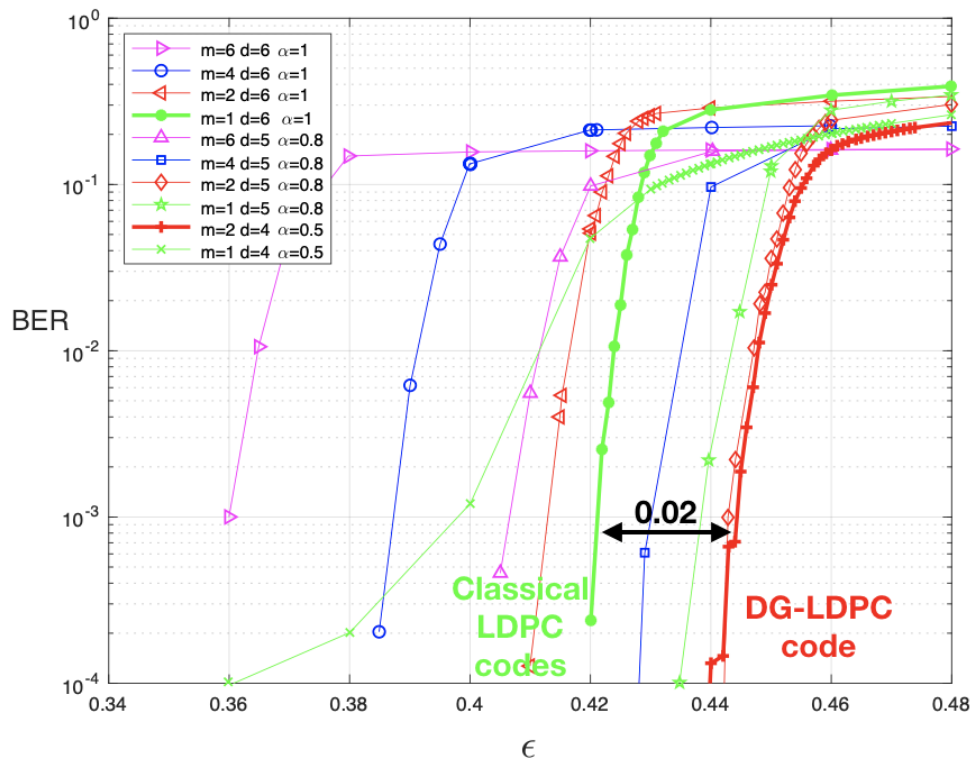

Figure 5.7: BER vs. $\frac{E_b}{n_0}$ for $(3, 3, d, \alpha, m)$ code of rate $r = 0.5$ and of binary code-length 36000, with $\alpha = 0.5; 0.8; 1$ and $m = 1, 2, 4, 6$.

Bibliography
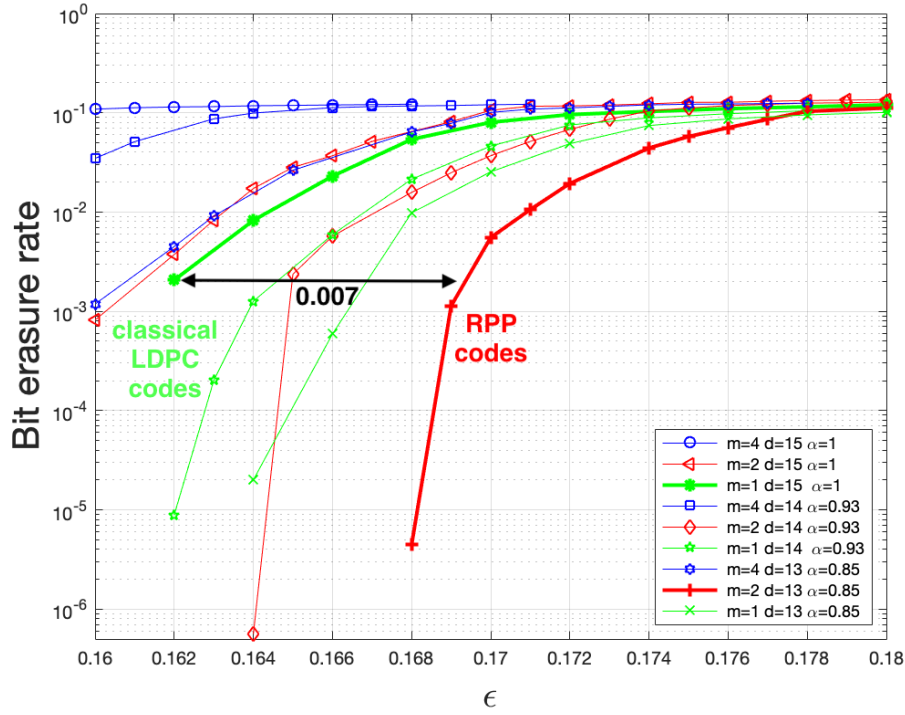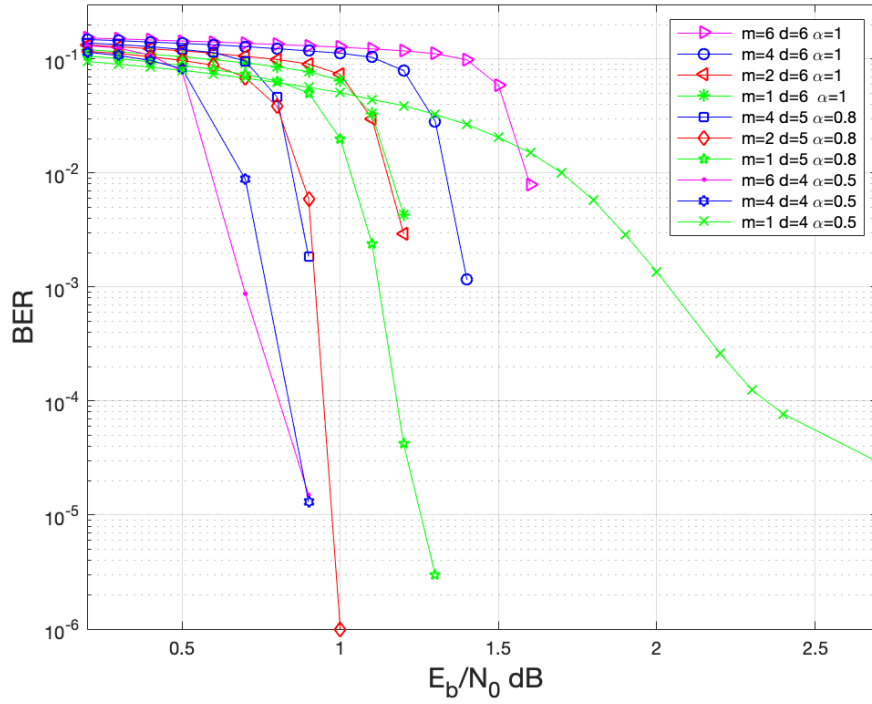
[94]   J Boutros, O Pothier, and G Zemor. "Generalized low density (Tanner) codes". In: *1999 IEEE International Conference on Communications (Cat. No. 99CH36311)*. Vol. 1. IEEE. 1999, pp. 441–445 (cit. on p. 69).

[95]   Roxana Smarandache and Pascal O Vontobel. "Quasi-cyclic LDPC codes: Influence of proto-and Tanner-graph structure on minimum Hamming distance upper bounds". In: *IEEE Transactions on Information Theory* 58.2 (2012), pp. 585–607 (cit. on p. 69).

[96]   Y. Wang and M. Fossorier. "Doubly Generalized LDPC Codes". In: *2006 IEEE International Symposium on Information Theory*. 2006, pp. 669–673 (cit. on p. 69).

[97]   R Tanner. "A recursive approach to low complexity codes". In: *IEEE Transactions on information theory* 27.5 (1981), pp. 533–547 (cit. on pp. 69, 71).

[98]   Enrico Paolini, Marc PC Fossorier, and Marco Chiani. "Generalized and doubly generalized LDPC codes with random component codes for the binary erasure channel". In: *IEEE Transactions on Information Theory* 56.4 (2010), pp. 1651–1672 (cit. on p. 69).

[99]   Enrico Paolini, Marc PC Fossorier, and Marco Chiani. "Doubly-generalized LDPC codes: Stability bound over the BEC". In: *IEEE transactions on information theory* 55.3 (2009), pp. 1027–1046 (cit. on p. 69).

[100]   Y. Wang and M. Fossorier. "Doubly Generalized LDPC Codes over the AWGN Channel". In: *IEEE Transactions on Communications* 57.5 (2009), pp. 1312–1319 (cit. on p. 69).

[101]   Arti D Yardi, Iryna Andriyanova, and Charly Poulliat. "EBP-GEXIT charts over the binary-input AWGN channel for generalized and doubly-generalized LDPC codes". In: *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2018, pp. 496–500 (cit. on p. 69).

[102]   Mark F Flanagan, Enrico Paolini, Marco Chiani, and Marc PC Fossorier. "On the growth rate of the weight distribution of irregular doubly generalized LDPC codes". In: *IEEE transactions on information theory* 57.6 (2011), pp. 3721–3737 (cit. on p. 69).

[103]   Sherif Elsanadily, Ashraf Mahran, and Osama Elghandour. "Improving the Decoding Performance of High-Rate GLDPC Codes in Low Error-Rate Applications". In: *2018 13th International Conference on Computer Engineering and Systems (IC-CES)*. IEEE. 2018, pp. 375–378 (cit. on p. 69).

[93]   Vishwambhar Rathi and Ruediger Urbanke. "Density evolution, thresholds and the stability condition for non-binary LDPC codes". In: *IEE Proceedings-Communications* 152.6 (2005), pp. 1069–1074 (cit. on pp. 71–73).

[104]   Amir Bennatan and David Burshtein. "Design and analysis of nonbinary LDPC codes for arbitrary discrete-memoryless channels". In: *IEEE Transactions on Information Theory* 52.2 (2006), pp. 549–583 (cit. on p. 73).

[105]   Iryna Andriyanova and Jean-Pierre Tillich. "Designing a good low-rate sparse-graph code". In: *IEEE transactions on communications* 60.11 (2012), pp. 3181–3190 (cit. on pp. 76, 77).

[106]   Iryna Andriyanova, Vishwambhar Rathi, and Jean-Pierre Tillich. "Binary weight distribution of non-binary LDPC codes". In: *2009 IEEE International Symposium on Information Theory*. IEEE. 2009, pp. 65–69 (cit. on p. 78).

Conclusions and perspectives

6.1 Conclusions

This work is focused on the design of new high-rate channel coding and coded modulation schemes of communication scheme over the AWGN channel, assuming a M-QAM scheme. Although this transmission model does not take into account polarisation and non-linearities effects in the optical fiber, it is still the most considered model in optical communications.

The first part of the thesis was devoted to the coded modulation aspect. In particular, the SICM model has been investigated, in case of a M-ary QAM modulation and q-ary sparse-graph codes. It has been shown that the AWGN capacity is attained with SICM when $q = \sqrt{M}$, and it is bounded from the capacity for $q < \sqrt{M}$. In the latter case the SICM capacity is still better than BICM capacity. In particular, at lower SNR values, the SICM capacity for $q = 4$ is bounded away by 0.5 dB from the AWGN capacity, while the BICM capacity is 1 dB away. Therefore, even by taking very moderate values of q one might regain a half of the gap induced by the BICM. Moreover, the SICM modulation scheme allows to reduce the interleaver size by the factor of $\log_2 q$, which is interesting for high-throughput implementation of next-generation optical communication systems. From another hand, the use of SICM comes with a higher decoder complexity (by the factor of $\log_2 q$) as the iterative decoder is implemented over $GF(q)$. Finally, our obtained results show that, among all possible mappings (and Gray mappings) of SICM modulation symbols, there exist a subset of Gray mappings that induce a higher SICM capacity.

From the point of view of error-correcting coding, we have shown that the asymptotic threshold for 3-regular LDPC codes over moderate values of q does not change significantly at high code rates r ($r = 0.75 \ldots 0.9$) and they can compete with 2-regular LDPC designs over larger alphabets, suggested in the state of the art. As 3-regular codes also have a better minimum distance, than 2-regular codes, they also outperform the code at low bit error rates (always at high code rates).

In addition to the results obtained for regular non-binary LDPC codes of high code rate, we also designed a new family of (non-binary) RPP codes which have remarkably

good asymptotic thresholds and enjoy, under some conditions, a linear minimum distance property. Both necessary and sufficient conditions on the linear minimum distance of a q-ary RPP ensemble have been derived. Our numerical results show that the new RPP code family is a good candidate for use at high code rates and that q-ary RPP codes outperform regular q-ary LDPC codes studied in Chapter 4.

6.2 Perspectives

High-rate, non-binary sparse-graph code designs have not been much studied until now, although they might be a key for next-generation ultra-high throughput optical communications. In order to continue the investigation on the feasibility of non-binary LDPC-like codes for optics, the following topics could further be studied:

1. *Further investigations on the SICM*
   - **Low-complexity detector design:** The soft detection of q-ary coded symbols is of high relevance if one intends to implement the SICM scheme.
   - An investigation on **Grey labelings** is needed in order to be able to reduce the gap to the channel capacity
   - **Extension to the MIMO AWGN channel model** would be of particular interest in order to capture the effect of polarisation-dependant loss (PDL) of the optical-fiber channel.
   - **Extension to other techniques considered in the optics community** such as probabilistic shaping, would be interesting to consider.

2. *Further investigations on high-rate non-binary RPP codes*
   For the the new code family presented in this work, the following topics could be addressed:
   - **Irregular design of RPP codes:** Only regular RPP constructions have been considered in our work, mainly for the reason of their more efficient hardware implementation (which is important for optical transceiver design). However, it would be interesting to extend the RPP construction to the irregular case and to see whether it is capacity-approaching.
   - **Asymptotic analysis over the AWGN channel:** For the sake of simplicity, the asymptotic analysis of the RPP ensemble has been performed over the BEC. Only several AWGN thresholds have been obtained by simulation. One could extend the existing EXIT chart design for discrete-memoryless symmetric channel from [75] to RPP codes.
   - **Complexity analysis, hardware implementation and feasibility of linear-time encoding:** It would be interesting to study more intensively the decoding convergence of RPP codes, as well as to try other iterative decoding algorithms of lower implementation cost (e.g., Min-Sum). It would also be interesting to determine the conditions, under which there exists a low-complexity encoding algorithm. such as max log max, min sum, etc. To see if one can have lower implementation costs.
   - **Imposing a structure on the RPP bipartite graph:** In this work, our RPP code ensembles are random code ensembles. For more efficiency, in particular in terms of the average minimum distance and/or low-complexity encoding, it would be interesting to design ensembles with a structured bipartite graph, like protographs for instance.

Additional DE results for Chapter 5

This appendix presents the obtained values of ε^* for RPP ensembles with $a, b \in \{4; 5; 6\}$ and for code rates $r \in \{0.5; 0.8\}$.

Moreover, one observes that the closest threshold to the Shannon one, among all rate $r = 0.5$ tables, is obtained for $a = b = 4$ ($\epsilon^* = 0.475, \alpha = 0.7, m = 2$ on table 1) and for $a = b = 5$ at rate $r = 0.8$ ($\epsilon^* = 0.191, \alpha = 0.57, m = 3$ on table 4), the gap to the Shannon threshold is 0.009.

Two major trends can be noticed:

- The best values of ε^* are obtained $2 \leq m \leq 4$.
- The best thresholds ε^* are observed for medium values of α, $\frac{1}{3} \leq \alpha \leq 0.77$.

It is to note that, for all tables, thresholds that do not satisfy the necessary condition on linear minimum distance (sec. 5.4.1) have been gray-shaded.

$\alpha\ (d)$ \ m	1	2	3	4
0.7 $(d = 5)$	0.396	**0.475**	**0.47**	0.459
0.83333 $(d = 6)$	**0.45**	0.438	0.423	0.407
0.92857 $(d = 7)$	0.415	0.399	0.382	0.364
1 $(d = 8)$	0.383	0.366	0.347	0.329

Table 1: Asymptotic thresholds ε^* of $(4, 4, d, \alpha, m)$ for various parameters α and m for given $r = 0.5$.

$\alpha\,(d)$ \ m	1	2	3	4
0.0714 $(d=7)$	0.107	0.146	0.167	0.176
0.25 $(d=8)$	0.113	0.154	0.174	0.18
0.38889 $(d=9)$	0.121	0.163	0.18	0.183
0.5 $(d=10)$	0.13	0.174	0.184	**0.183**
0.59091 $(d=11)$	0.142	0.183	**0.184**	0.18
0.66667 $(d=12)$	0.156	**0.183**	0.18	0.175
0.73077 $(d=13)$	0.175	0.18	0.175	0.169
0.78571 $(d=14)$	**0.178**	0.176	0.169	0.162
0.83333 $(d=15)$	0.175	0.171	0.164	0.156
0.875 $(d=16)$	0.171	0.166	0.158	0.15
0.91176 $(d=17)$	0.167	0.161	0.153	0.145
0.94444 $(d=18)$	0.162	0.156	0.148	0.14
0.97368 $(d=19)$	0.158	0.151	0.143	0.135
1 $(d=20)$	0.154	0.147	0.138	0.13

Table 2: Asymptotic thresholds ε^* of $(4, 4, d, \alpha, m)$ for various parameters α and m for given $r = 0.8$. $\alpha = 1$ corresponds to the $(4, 20)$ LDPC ensemble. Thresholds that do have a linear d_{min} for $m = 1$ have been gray-shaded.

$\alpha\,(d)$ \ m	1	2	3	4
0.77778 $(d=6)$	0.363	**0.441**	**0.444**	0.425
0.85714 $(d=7)$	**0.436**	0.416	0.396	0.376
0.91667 $(d=8)$	0.399	0.378	0.357	0.337
0.96296 $(d=9)$	0.368	0.346	0.325	0.306
1 $(d=10)$	0.341	0.319	0.299	0.28

Table 3: Asymptotic thresholds ε^* of $(5, 5, d, \alpha, m)$ for various parameters α and m for given $r = 0.5$.

m $\alpha\,(d)$	1	2	3	4
$0.14286(d=7)$	0.104	0.143	0.164	0.173
$0.29167(d=8)$	0.108	0.147	0.169	0.178
$0.40741(d=9)$	0.112	0.153	0.175	0.184
$0.5(d=10)$	0.117	0.159	0.182	**0.189**
$0.57576(d=11)$	0.123	0.167	**0.191**	0.187
$0.63889(d=12)$	0.131	0.176	0.188	0.181
$0.69231(d=13)$	0.139	**0.187**	0.182	0.174
$0.7381(d=14)$	0.149	0.183	0.175	0.167
$0.77778(d=15)$	0.161	0.177	0.169	0.16
$0.8125(d=16)$	**0.175**	0.172	0.163	0.154
$0.84314(d=17)$	0.174	0.166	0.157	0.148
$0.87037(d=18)$	0.169	0.16	0.151	0.142
$0.89474(d=19)$	0.164	0.155	0.146	0.137
$0.91667(d=20)$	0.16	0.15	0.14	0.132
$0.93651(d=21)$	0.155	0.145	0.136	0.127
$0.95455(d=22)$	0.151	0.141	0.131	0.123
$0.97101(d=23)$	0.146	0.137	0.127	0.119
$0.98611(d=24)$	0.143	0.133	0.123	0.115
$1(d=25)$	0.139	0.129	0.12	0.111

Table 4: Asymptotic thresholds ε^* of $(5,5,d,\alpha,m)$ for various parameters α and m for given $r=0.8$. Thresholds that do not have a linear d_{min} have been gray-shaded.

$\alpha\ (d)$ $\diagdown$ m	1	2	3	4
$0.17857(d=7)$	0.101	0.138	0.159	0.169
$0.3125(d=8)$	0.103	0.141	0.163	0.173
$0.41667(d=9)$	0.105	0.144	0.167	0.178
$0.5(d=10)$	0.109	0.148	0.172	0.183
$0.56818(d=11)$	0.113	0.153	0.178	0.189
$0.625(d=12)$	0.117	0.159	0.184	**0.19**
$0.67308(d=13)$	0.122	0.166	**0.19**	0.181
$0.71429(d=14)$	0.128	0.173	0.183	0.173
$0.75(d=15)$	0.134	**0.181**	0.175	0.166
$0.78125(d=16)$	0.142	0.179	0.168	0.158
$0.80882(d=17)$	0.15	0.172	0.161	0.152
$0.83333(d=18)$	0.16	0.166	0.155	0.145
$0.85526(d=19)$	**0.171**	0.16	0.149	0.14
$0.875(d=20)$	0.166	0.155	0.144	0.134
$0.89286(d=21)$	0.161	0.15	0.139	0.129
$0.90909(d=22)$	0.156	0.145	0.134	0.125
$0.92391(d=23)$	0.151	0.14	0.13	0.12
$0.9375(d=24)$	0.147	0.136	0.126	0.116
$0.95(d=25)$	0.143	0.132	0.122	0.113
$0.96154(d=26)$	0.139	0.128	0.118	0.109
$0.97222(d=27)$	0.135	0.125	0.115	0.106
$0.98214(d=28)$	0.132	0.121	0.111	0.103
$0.99138(d=29)$	0.129	0.118	0.108	0.1
$1(d=30)$	0.125	0.115	0.105	0.097

Table 5: Asymptotic thresholds ε^* of $(6, 6, d, \alpha, m)$ for various parameters α and m for given $r = 0.8$. Thresholds that do not have a linear d_{min} have been gray-shaded.

$\alpha\ (d)$ $\diagdown$ m	1	2	3	4
$0.82143(d=7)$	0.334	**0.411**	0.411	0.389
$0.875(d=8)$	**0.386**	0.392	0.369	0.347
$0.91667(d=9)$	0.382	0.358	0.335	0.314
$0.95(d=10)$	0.353	0.329	0.306	0.286
$0.97727(d=11)$	0.328	0.305	0.283	0.263
$1(d=12)$	0.307	0.284	0.262	0.244

Table 6: Asymptotic thresholds ε^* of $(6, 6, d, \alpha, m)$ for various parameters α and m for given $r = 0.5$.