Non-binary LDPC codes associated to high order modulations

Ahmed Abdmouleh

THESE / UNIVERSITE DE BRETAGNE-SUD
sous le sceau de l'Université Bretagne Loire

pour obtenir le titre de
DOCTEUR DE L'UNIVERSITE DE BRETAGNE-SUD

Mention : STIC
Ecole doctorale:SICMA

Présentée par :

ABDMOULEH AHMED

Préparée à l'UMR 6285
Université de Bretagne Sud

Lab-STICC

Codes correcteurs d'erreurs NB-LDPC associés aux modulations d'ordre élevé.

Thèse soutenue le 12 septembre 2017

devant le jury composé de :

Jean-François HELARD
Directeur de la recherche – INSA Rennes / *président*
Charly POULLIAT
Professeur des Universités – INP-ENSEEIHT / *rapporteur*
Christophe JEGO
Professeur des Universités – IPB/ENSEIRB-MATMECA / *rapporteur*
Olivier BERDER
Directeur de la recherche – Université de Rennes / *examinateur*
Andrew HACKETT
Directeur Technique – CTO, France Brevets / *invité*
Charbel ABDEL-NOUR
Encadrant
Laura CONDE-CANENCIA
Encadrant
Catherine DOUILLARD
Co-directeur de thèse
Emmanuel BOUTILLON
Directeur de thèse

Table des matières

Table des figures

Liste des tableaux

"*Believe you can and you are halfway there*"

Theodore Roosevelt

ABBREVIATIONS

LDPC Low-Density Parity-Check

NB Non-Binary

NB-LDPC Non-Binary Low-Density Parity-Check

MAP Maximum a-posteriori

SSD Signal Space Diversity

QAM Quadrature Amplitude Modulation

AWGN Additive White Gaussian Noise

GF Galois Field

CN Check Node

VN Variable Node

ML Maximum Likelihood

BP Belief Propagation

LLR Logarithmic Likelihood Ratio

EMS Extended Min-Sum

MS Min-Sum

SNR Signal to-Noise Ratio

CM Coded modulation

BICM Bit Interleaved Coded Modulation

MI Mutual Information

SFN Single-Frequency Networks

DVB-T2 Digital Video Broadcasting Terrestrial, the second generation

CSI Channel State Information

BER Bit Error Rate

SER Symbol Error Rate

FER Frame Error Rate

FEC Forward Error Correction

QPSK Quadrature Phase-Shift keying

DS Distance Spectrum

DEDICATION

To all people who helped me to follow my dreams...

ACKNOWLEDGEMENTS

Finally, after an intensive work on my dissertation, I'm glad to write this note of thanks to the people who helped and supported me during my PhD. This PhD was carried out at the laboratory Lab-STICC (Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance) in Université Bretagne Sud and Telecom Bretagne.

My foremost thanks are dedicated to Emmanuel Boutillon, for his guidance through the work on this thesis, for the continuous support, and his immense knowledge. He supported me in all steps of my thesis research and redaction. I cannot find a better mentor for my PhD study. I would like to thank Catherine Douillard, who has been a tremendous mentor for me. Thank you so much for your patience and continuous support. I would like to thank my supervisor Charbel Abdel-Nour for his advises and interesting discussions that helped me overcome obstacles in my PhD. I would like to thank Laura Conde-Canoncia for her kindness and help during difficult moments, she was my ultimate refuge in times of trouble.

During my PhD I spent good time in Brest, Lorient, Kaiserslautern and Lannion. This allowed me to meet friends that were very nice and helpful, they became like a family for me. We spent unforgettable moments and we had several interesting discussions about meaning of life and the world were we live.

I am forever thankful to my parents. The are the key of my success. They have both scarified a lot to help me achieving my dreams. My brother and sister are such a wonderful gift, thank you for everything you have done for me.

ABSTRACT

Non-binary LDPC codes associated to high-order modulations

Abdmouleh Ahmed

Department Electronique, Telecom - Bretagne

12 Septembre 2017

This thesis is devoted to the analysis of the association of non-binary LDPC codes (NB-LDPC) with high-order modulations. This association aims to improve the spectral efficiency of future wireless communication systems. Our approach tries to take maximum advantage of the straight association between NB-LDPC codes over a Galois Field with modulation constellations of the same cardinality.

We first investigate the optimization of the signal space diversity technique obtained with the Rayleigh channel (with and without erasure) thanks to the rotation of the constellation. To optimize the rotation angle, the mutual information analysis is performed for both coded modulation (CM) and bit-interleaved coded modulation (BICM) schemes. The study shows the advantages of coded modulations over the state-of-the-art BCIM modulations. Using Monte Carlo simulation, we show that the theoretical gains translate into actual gains in practical systems.

In the second part of the thesis, we propose to perform a joint optimization of constellation labeling and parity-check coefficient choice, based on the Euclidian distance instead of the Hamming distance. An optimization method is proposed. Using the optimized matrices, a gain of 0.2 dB in performance is obtained with no additional complexity.

RÉSUMÉ

Non-binary LDPC codes associated to high-order modulations

Abdmouleh Ahmed
Département Electronique, Telecom - Bretagne
12 Septembre 2017

De nos jours, nous vivons dans un monde numérique de plus en plus interconnecté. Les systèmes de communication futurs doivent relever des défis majeurs : assurer l'échange d'un volume de données important, un nombre croissant d'appareils connectés, et plus de données à pourvoir par utilisateur. Cependant, la réponse à ces exigences importantes doit prendre en compte certaines limites de transmission. En 1948, Claude Shannon a montré qu'une transmission connait une certaine limite théorique de transmission appelé capacité du canal, définie comme la quantité maximale d'informations pouvant être envoyées sans erreurs en utilisant un système de communication numérique. Depuis, nous avons vu l'émergence de plusieurs codes correcteurs d'erreurs tels que les codes de Hamming, les codes algébriques, les codes LDPC (Low-Density parity-check) et, plus récemment, les codes turbo et les codes polaires.

Les codes correcteurs d'erreurs se classent en deux grandes catégories : les codes en blocs et les codes convolutionnels. Dans le cas des codes en blocs, le message est envoyé sur plusieurs blocs de données séparés, et l'encodeur traite chaque bloc indépendamment. Par conséquent, l'encodeur doit attendre la réception d'un bloc entier pour démarrer. Dans le cas des codes convolutionnels, le codeur traite le message d'une façon continue et génère séquentiellement les symboles de redondance sans avoir besoin du message complet. La plupart des normes de communication actuelles utilisent une de ces deux catégories de codes correcteurs d'erreur.

Les codes correcteurs d'erreurs à faible densité (LDPC) sont une classe de codes de blocs linéaires. Initialement présentés par Gallager en 1963, les codes LDPC se caractérisent par une matrice de parité qui contient un petit nombre d'éléments non nuls. Malgré leur excellente performance, cette classe de codes a été ignorée pendant trois décennies en raison de sa complexité de décodage qui a dépassé les capacités des systèmes électroniques de l'époque. Mackay et al. ont repris les codes LDPC au milieu des années 1990 et ils ont montré que ces codes permettent d'atteindre des performances proches de la limite de Shannon en utilisant les algorithmes de décodage souples. Au cours des deux dernières décennies, les codes LDPC ont connus un progrès spectaculaire, leur capacité de décodage pour différents modèles de canaux est devenu assez intéressante ce qui a attiré l'intérêt de la communauté scientifique. Les avancements théoriques ont boosté le transfert de ces codes correcteurs d'erreurs au domaine industriel. Maintenant, les codes LDPC jouent un rôle majeur dans la définition de plusieurs normes comme DVB-S2, WI-MAX, DSL, W-LAN. Les performances de décodage des codes LDPC ont atteint des capacités de correction très proches des limites théoriques (seulement 0.0045 dB de la limite de Shannon), ce qui en fait parmi les meilleures codes correcteurs d'erreurs expérimentée jusqu'à présent. Cependant, ces performances proches de la limite de Shannon sont observés pour les codes associés à des blocs de très grande longueur (séquence de 10^6 -bit).

Plus tard, Gallager a étendu la définition des codes LDPC sur les alphabets non binaires pour proposer les codes LDPC non binaires. Ces codes LDPC non binaires, définis sur les corps de Galois de dimensions strictement supérieurs à 2, ont offert une bonne alternative aux codes LDPC binaires en raison de leur capacité de correction supérieure. Les récentes études ont confirmé l'amélioration apportée par ces codes LDPC non binaires par rapport à leurs homologues binaires, en particulier pour les mots de

code de petite et moyenne taille. Le gain apporté par ces codes LDPC non binaires devient encore plus important lorsque les symboles sont envoyés en utilisant des modulations d'ordre élevé. Le nombre de publications croissant liées aux décodeurs LDPC non binaires confirme l'intérêt grandissant de la communauté scientifique pour cette famille de codes. Plusieurs auteurs ont proposé dans la littérature des constructions efficaces des codes LDPC non binaires ainsi que bon nombre d'algorithmes de décodage pour les codes LDPC non binaires. L'algorithme de propagation de croyance est l'un des décodeurs itératifs les plus connus. Cependant, le gain de performance fourni par les codes LDPC non binaires s'accompagne d'une importante complexité de décodage. Pour un code LDPC défini sur le champ Galois GF (q), la complexité du décodage est de l'ordre $\mathcal{O}(q^2)$. Ce fait rend l'utilisation des codes LDPC non binaires un compromis entre l'amélioration de la performance et l'augmentation de la complexité du décodage.

De nos jours, la coexistence de différentes applications radio (téléphonie mobile, réseaux sans fil, radiodiffusion terrestre, communications par satellite, etc.) limite les ressources spectrales. En d'autres termes, les données transmises dans de nombreuse d'applications continuent de croître et le nombre d'utilisateurs augmente constamment, cela sans être couplée par une augmentation des ressources spectrales. Dans ce contexte, les opérateurs et les fabricants du monde numérique visent à maximiser l'efficacité spectrale des systèmes, définis comme le taux de transmission utile par unité de bande occupée. La solution ultime pour contrer le manque de ressources en spectre de fréquence et pour répondre aux besoins de transmissions à débit élevé, est l'utilisation de modulations d'ordre élevé. Les communications radio-mobiles et par satellite ont déjà intégré des modulations à ordre élevé dans leurs schémas de transmission. Au cours des deux dernières décennies, un progrès significatif a bénéficié à la recherche sur des systèmes de transmission ayant une efficacité spectrale élevé. Cela a permis de faire face à la demande industrielle. Le schéma de modulation codé, qui combine les codes correcteurs d'erreur avec les modulations à haut ordre, devient essentiel pour les canaux qui sont limités en bande spectrale.

Les motivations des travaux de cette thèse viennent de deux faits principaux. Tout d'abord, au cours de la dernière décennie, les codes LDPC non binaires ont été bien développés pour les corps de Galois d'ordre $q > 2$. Le deuxième fait est que le besoin croissant de transmissions d'haut débit a conduit à une croissance de l'utilisation des modulations à ordre élevé dans les nouvelles normes de transmission. Par conséquent, l'association de codes LDPC non binaires avec des modulations à ordre élevé mérite d'être étudiée. En fait, lors de l'association d'un code LDPC binaire à une modulation M-are, le démappeur (MAP) crée des probabilités au niveau binaire pour le décodeur. La dépendance entre les bits implique que le démapper génère des probabilités corrélées au niveau binaire. Par conséquent, le décodeur est initialisé avec des messages déjà corrélés par le canal. L'utilisation de démappeur itératif atténue partiellement cet effet, mais augmente la complexité totale du décodeur. À l'inverse, dans le cas NB (code LDPC non binaires avec modulation NB), la dépendance entre les messages est réduite et les probabilités des symboles sont moins corrélées. Si les dimensions du code LDPC non binaires et la modulation coïncident, le décodeur LDPC non binaires sera initialisé avec des messages non corrélés, ce qui entraînera une meilleure performance au niveau des algorithmes de décodage. Par conséquent, les codes LDPC non binaires offrent toujours de meilleures performances pour la modulation d'ordre élevé. Des résultats prometteurs été observés suite à l'association d'un code LDPC défini sur GF (64) avec la modulation en 64-QAM pour transmission dans un canal gaussien. En outre, lorsque la dimension du corps de Galois des codes LDPC non binaires est égale à la dimension de la modulation, la relation directe entre la modulation et les symboles du code LDPC non binaire élimine

le besoin de démapping itératif entre le décodeur et Maximum a Détecteur postérieur (MAP). Par conséquent, l'utilisation de codes LDPC non binaires, réduit la latence chez les récepteurs et offre des gains de codage plus élevés. Lorsque les tailles de constellation augmentent, un gain de codage supplémentaire est offert par les codes LDPC non binaires aux codes LDPC binaire. Par conséquent, plus l'efficacité spectrale augmente, plus la taille des constellations continuent à croître. Par conséquent, ces avantages des codes LDPC non binaires lorsqu'ils sont associés à des modulations à ordre élevé auront une influence majeure dans les normes de transmission de la prochaine génération.

Cette thèse est consacrée à l'association des codes LDPC non binaires aux modulations à d'ordre élevé. A travers les travaux de cette thèse, nous essayons d'atteindre deux objectifs principaux. Tout d'abord, nous nous intéressons à ressortir les avantages du bon ajustement entre les codes LDPC non binaires et les modulations à ordre élevé, surtout lorsqu'ils ont la même dimension (relation direct entre les symboles et les points de la constellation).Deuxièmement, nous proposerons des méthodes novatrices pour améliorer les systèmes existants qui utilisent des codes LDPC non binaires dans un contexte de transmission avec une grande efficacité spectrale.

Cette thèse englobe quatre chapitres dans lesquels nous étudions les résultats et les avantages de l'association des codes LDPC non binaires avec des modulations à ordre élevé. Dans le premier chapitre de la thèse, les codes LDPC non binaires sont introduits. Des notions mathématiques utiles à leur étude sont présentées, ainsi que quelques exemples d'algorithmes de décodage. Enfin, certaines des études de performance existantes sont présentées pour comparer les codes LDPC non binaires à leurs homologues binaires. Dans le deuxième chapitre, nous nous concentrons sur les différents éléments de la communication numérique et les concepts liés aux modulations à ordre élevé. Nous présentons une modélisation des canaux de transmission considérés dans cette thèse, avant de présenter les schémas de modulation codée et les schémas de modulations codée entrelacées au niveau bit. Ensuite, nous mettons en évidence leurs limites de transmission théoriques. Enfin, la diversité en espace et signal appelé en anglais Signal Space Diversity (SSD), est présentée et certaines de ses applications et méthodes d'optimization sont introduites. Dans la troisième partie de cette thèse, nous présentons notre première contribution lors de l'utilisation de la technique SSD dans le contexte d'une transmission à haute efficacité spectrale, la méthode d'optimization de la technique SSD proposé est basée sur la maximisation de l'information mutuelle. Une analyse des limites théoriques de transmission est réalisée pour le canal de Rayleigh et canal de Rayleigh avec effacement. Sur la base d'une maximisation de l'information mutuelle, nous proposons les meilleurs angles de rotation pour la technique SSD. Un impact positif sur la performance théorique est obtenu. Les résultats de la simulation révèlent que cette technique de diversité, la SSD, peut encore être améliorée en comparaison avec les méthodes d'optimization existantes. Dans le quatrième chapitre, nous proposons une nouvelle méthode pour optimizer le schéma de transmission en modulation codé. L'idée principale consiste à effectuer une optimization conjointe des du codage de canal (codes LDPC non binaires) et de la modulation (modulation M-QAM). En fait, la méthode proposée exploite l'avantage d'utiliser un schéma de modulation avec un ordre égal à celui du GF sur lequel les codes LDPC non binaires sont définis. Un gain de performance est obtenu sans ajouter la moindre complexité par rapport aux systèmes existants.

Chapitre 1
Introduction

Nowadays, we live in a world that is becoming increasingly connected, and the upcoming communication systems must meet crucial challenges : a bigger volume of data, more interconnected devices and higher data flow to be consumed by users. However, the answer to these important demands faces certain limitations. In 1948, Claude Shannon had shown that one of these limitations is the channel capacity, defined as the maximum amount of information that can be reliably sent by employing a digital communication system. Since 1948, several error correction codes have been proposed, such as algebraic codes, Hamming codes, Low-Density parity-check (LDPC) codes and more recently, turbo codes and polar codes. Among the listed correction codes two main families can be distinguish : block codes and convolutional codes. For the first code family, the message is separated into blocks of data and the encoder processes these blocks separately. Therefore, the encoder must receive the whole block to start encoding. For the second family code, the encoder processes the message continuously and generates the redundancy symbols without any need to get the full message. Most of the current communication standards call for one of these two families of error correction codes.

LDPC codes are a class of linear block codes, originally presented by Gallager in 1963. LDPC codes are characterized by a sparse Parity Check Matrix (PCM) that contains a small number of nonzero elements. Despite their excellent performance, LDPC codes were ignored till the mid 1990 because of their decoding complexity that is superior to the capacity of electronic systems of that time. When Mackay et al. revisited the LDPC codes in 1996 [1], they showed that these codes offer near Shannon limit performance when decoded by means of probabilistic soft decision decoding algorithms. LDPC codes have known spectacular advances in the last decades. Their capacity approaching performance for a wide range of channel models attracts the interest of the scientific community. Fundamental theoretical advancement encourages the transfer of these correcting codes to the industrial domain. Now LDPC codes play a major role in the definition of several standards like DVB-S2, WI-MAX, DSL, W-LAN. The importance of LDPC coding has still grown by pushing its capacity (only 0.0045 dB from the Shannon limit), which makes them the best experienced error correcting code till now. However these near Shannon's limit performance is obtained

for randomly constructed codes of very large block lengths (10^6-bit sequence).

Later on, Gallager extended the definition of LDPC codes on non-binary alphabets to propose non-binary LDPC (NB-LDPC) codes. These NB-LDPC codes are defined over Galois Fields of order strictly higher than 2. They offered a good alternative to LDPC codes due to their enhanced correction capacity. Recent studies confirmed that NB-LDPC codes give better performance compared to their binary counterparts, especially for small to moderate codewords. Moreover NB-LDPC codes provide additional performance gain when symbols are sent using high-order modulations. The increasing number of publications related to non-binary LDPC decoders confirms the growing interest of scientific community for these codes. Several authors have proposed in the literature effective constructions of NB-LDPC codes, and number of efficient decoding algorithms for NB-LDPC codes, i.e. Belief propagation algorithm, one of the most known iterative decoders. However, the performance gain provided by NB-LDPC codes is accompanied by an important decoding complexity. For an LDPC code defined over the Galois field GF(q), the decoding complexity is of the order $\mathcal{O}(q^2)$. This fact make the use of NB-LDPC codes a tradeoff between performance enhancement and the increase of decoding complexity.

Nowadays, the coexistence of different radio applications (mobile telephony, wireless networks, terrestrial broadcasting, satellite communications, etc.), limits the spectral resources. In addition, the transmitted data in a wide range of applications continues to grow while the number of users is constantly increasing. In this context, operators and manufacturers aim at maximizing the spectral efficiency of the systems, defined as the useful transmission rate per unit of occupied band. The ultimate solution to counter the lack of frequency spectrum resources, and to meet the need of high data rate transmissions, is the use of high order modulations. The radio-mobile and satellite communication channels have already integrated high order modulations in their transmission schemes. In the last two decades, research on systems that use high spectral efficiency transmission has benefited from significant progress, making it possible to cope with the industrial demand. The coded modulation (CM) scheme, which combines error correcting codes with high order modulations, becomes essential for channels that are limited both in power and in spectral band.

The motivation behind this thesis comes from two main facts. First, in the last decade, there has been tremendous interest in NB-LDPC codes defined over high-order Galois fields GF(q), with $q >> 2$. The second fact is that the increasing need of high data rate transmissions has led to a growing need of using high order modulations in the new transmission standards. Therefore a good association of NB-LDPC codes with high order modulations is worth investigating. In fact, when associating a binary LDPC code to an M-ary modulation, the Maximum a-posteriori (MAP) demapper creates probabilities at the binary level for the decoder. The dependency between the bits implies that the demapper generates likelihoods that are already correlated at the binary level. Therefore the decoder is initialized with messages already correlated by the channel. The use of iterative demapping partially mitigates this effect but increases the whole decoder complexity. Conversely,

in the NB case (NB-LDPC code with NB modulation), the dependence between messages is reduced and the symbol likelihoods are less correlated. If the NB-LDPC code is defined in the same GF order as the order of the modulation, the NB-LDPC decoder will be initialized with non-correlated messages, which leads to better performance of the decoding algorithms. Therefore, NB-LDPC codes provide always better performance for high order modulation. Promising results have already been obtained with the association of an LDPC code over GF(64) with 64-QAM for transmission in Gaussian channel. Furthermore, the direct relation between modulation and NB-LDPC codes eliminates the need for iterative-demapping between the decoder and MAP detector. Hence employing NB-LDPC codes, reduces the latency at the receivers and offers higher coding gains. When the constellation sizes increase, additional coding gains are obtained with NB-LDPC. Therefore, as the transmission rates continue to increase, the constellation sizes will continue to grow ; consequently, these benefits of NB-LDPC codes associated with high order modulations will have a major influence in the next generation transmission standards.

This thesis is dedicated to the association of NB-LDPC codes with high order modulations. Through this thesis we try to achieve two main goals. First, we are interested to bring out the advantage of the good fit between NB-LDPC codes and high order modulations, especially when they are of the same order. Second, we will try to propose some innovative methods to ameliorate the existing systems that already use NB-LDPC codes with high spectral efficiency transmission.

This thesis encompasses four distinct chapters, in which we investigate the outcome and advantages of the association of NB-LDPC codes with high order modulations. In the first chapter of the thesis, NB-LDPC codes are introduced. Useful mathematical notions about NB-LDPC codes are presented, as well as the existing decoding algorithms. And some of the existing performance studies are presented to show that NB-LDPC codes are asymptotically better than their binary counterparts. In the second chapter, we focus on the various elements of digital communication and the concepts related to the high order modulations. We present a modelization of the considered transmission channels in this thesis, before presenting the Coded Modulation, and the Bit Interleaved Coded Modulation (BICM) schemes. Then, we highlight some of their theoretical transmission limits. In the third part of this thesis, a diversity technique, called signal space diversity (SSD), is presented and some of its applications and optimization methods are introduced. Then, we present our first contribution when employing the SSD technique in the context of high spectral efficiency transmission, the mutual information based SSD technique optimization. To make such an optimization, an analysis of the theoretical transmission limits is done under both Rayleigh and Rayleigh with erasure channels. Based on Mutual Information maximization, we propose the best rotation angles for the SSD technique, for the BICM that uses a binary error control code, and for the CM that uses a NB-LDPC code of same order of the modulation. A positive impact on the theoretical performance is obtained. Both theory and simulation results shows that the association of CM with SSD improves the performance compared to BICM. For example, with a $\frac{9}{10}$ rate code, SSD with CM brings 1.3 dB of gain, while when

we use the SSD with BICM only 0.3 dB of gain is obtained. In addition, simulation results reveal that the SSD technique can be further ameliorated, when comparing to the state-of-the-art optimization methods. In the fourth chapter, we propose a new method to design an advanced high-spectral efficiency communication for CM transmission scheme. The main idea consists in performing a joint optimization of both channel coding (NB-LDPC codes) and modulation (M-QAM modulation). To be precise, the joint optimization is done on the constellation mapping and the non-null entries of the NB-LDPC code. This optimization is based on the evaluation of the distance spectrum of the Euclidean distances between all possible codewords. In fact, the proposed method exploits the advantage of using a modulation scheme with an order equal to the one of the GF over which the NB-LDPC codes are defined. A gain of performance is obtained free of any additional complexity compared to existing schemes.

Part of the work done during the PhD has been published in [2] it was about the SSD technique optimization ; and in [3] to present the joint NB-LDPC code and mapping optimization which was also protected by a patent in [4].

Chapitre 2
Non-Binary LDPC codes

This chapter presents the background and state-of-the-art information about Non-Binary Low-Density parity-check (NB-LDPC) codes and the principles of their decoding process. In Section 2.1, we introduce the notion of Galois fields necessary for defining NB-LDPC codes, before presenting the NB-LDPC codes in Section 2.2, as an extension of the LDPC codes. Then, decoding algorithms of NB-LDPC codes is the subject of Section 2.3. Finally, we conclude this chapter in Section 2.4 by comparing the performance of LDPC and NB-LDPC codes using state-of-the-art-codes, over additive white Gaussian noise (AWGN) and Rayleigh channels.

2.1 ALGEBRAIC DEFINITION OF GALOIS FIELDS GF(Q)

Classical algebra is known to study the most commonly used sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ built with arithmetic operations such as addition and multiplication. However, modern algebra is characterized by a higher level of abstraction ; the concept of operation is defined as an application that returns a symbol from two or more symbol combination. This allows the scientists to extend the definition of error correction codes to sets other than classical ensembles. In this PhD thesis, we have a special interest non-binary LDPC codes defined on Galois Fields. In order to present a clear definition of Galois field, we first show the basic algebraic structures and their internal composition laws. The content of this section was mainly extracted from [5, 6, 7].

2.1.1 GROUPS

Let G be a set of elements. A binary operation « $*$ » on G is a function that assigns to a couple of elements a and b a unique element $c = a * b$ in G. A binary operation « $*$ » on G is associative if, for any a, b, and c in G, $a * (b * c) = (a * b) * c$

A set G on which a binary operation « $*$ » is defined is called a group if the following conditions are satisfied :

1. The binary operation « $*$ » is associative.
2. G contains an identity element e of G, with $\forall a \in G$, $a * e = e * a = a$.
3. For any element $a \in G$, there exists another element $a^{'} \in G$ such that $a * a^{'} = a^{'} * a = e$; a and $a^{'}$ are inverse to each other.

A group G is called commutative if its operation « $*$ » also satisfies the following condition : for any a and b in G, $a * b = b * a$. Finally, a Group G satisfies the following properties

— The identity element in a group G is unique.

Proof : If e and $e^{'}$ are identity elements $\in G$. Then $e^{'} = e^{'} * e = e$.

— Every element has a unique inverse.

Proof : If $a^{'}$ and $a^{''}$ are inverse to a, then $a^{'} = a^{'} * e = a^{'} * a * a^{''} = e * a^{''} = a^{''}$

2.1.2 FIELDS

Let F be a set of elements defined with two binary operations, addition « $+$ », and multiplication « $*$ ». The set F together with the two binary operations « $+$ » and « $*$ » is a field if the following conditions are satisfied :

1. $(F, +)$ is a commutative group. The identity element 0 of the addition operation is called the zero element of F.
2. $(F - \{0\}, *)$ is a commutative group. The identity element of the multiplication operation 1 is called the unit element of F.
3. Multiplication is distributive over addition ; $\forall\, a, b$ and $c \in F$, $a*(b+c) = a*b+a*c$.

2.1.3 GALOIS FIELDS

A Galois field has a finite order, which is either a prime number or the power of a prime number. A field of order $q = n^p$ GF(n^p) or GF(q) contains q-elements which are denoted as $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$, where α is called the primitive symbol of the field, the powers of which construct all the other elements of the field [8]. A specific type called characteristic-2 fields represent the fields when $n = 2$. All the elements of a characteristic-2 field can be represented in a polynomial format [9].

The primitive polynomial P_p of the field of order 2^p is an irreducible polynomial of degree p that generates all the other polynomials. The set of polynomials defined over $GF_{(2)}[x]$ modulo P_p defines the Galois Field GF(q), with $GF_{(2)}[x]$ is the set of polynomials with coefficient in the set $\{0, 1\}$. Note that for each field GF(q) we can find one or more primitive polynomial P_p of degree p over GF(q) [10].

Table 2.1 lists the primitive polynomials for $p \in \{1, 2, 4, 6, 8\}$. For $p = 1$, the field is a binary field and for $p \geq 2$, it represents a non-binary field. Binary LDPC codes are defined over a Galois field GF(2), with $0, 1$ being the field elements. Hence non-binary LDPC codes

TABLE 2.1 – Primitive polynomials

polynomial degree	Primitive Polynomials
1	$1+x$
2	$1+x+x^2$
4	$1+x+x^4, 1+x^3+x^4$
6	$1+x+x^6$
8	$1+x^2+x^3+x^4+x^8$

are a generalization of binary LDPC codes. Each element of a binary representation of the Galois field is represented by a polynomial with binary coefficients.

Table 2.2 shows the example for $p = 3$ while considering the primitive polynomial $1+x+x^3$. The field consists of 8 elements and each one has a binary representation composed of the binary coefficients of the associated polynomial. With this representation finite field addition and multiplication becomes polynomial addition and multiplication, where the addition is modulo-2 ($\alpha+\alpha=0$). The result of a multiplication is realized by applying a polynomial multiplication followed by a modulo reduction using P_p. Only the remainder of the Euclidean division is kept. In Table 2.2 all the α^j, $j \in \{0\dots6\}$ have their binary representation by applying an Euclidean division by the primitive polynomial. Equation 2.1 presents the example of division of α^4 by the primitive polynomial.

$$\alpha^4 = \alpha * (\alpha^3+\alpha+1) + \alpha^2 + \alpha = \alpha^2 + \alpha \; mod[P_p] \tag{2.1}$$

We can consider GF$_{(2^p)}$[x] modulo P_r as the polynomial representation of GF(2^p). Then GF$_{(2^p)}[x] = GF_{(2)}[x]/P_p[x]$, where $GF_2[x]$ is the polynomial set with coefficient in $\{0,1\}$ and $P_p[x]$ is the representation of P_p in $GF_2[x]$.

TABLE 2.2 – Binary representation of symbols

Element	Binary representation	Polynomial Sum
0	000	0
α^0	100	1
α^1	010	α
α^2	001	α^2
α^3	110	$1+\alpha$
α^4	011	$\alpha+\alpha^2$
α^5	111	$1+\alpha+\alpha^2$
α^6	101	$1+\alpha^2$

2.2 NB-LDPC CODES DEFINED OVER GF(Q)

In this section we start by presenting LDPC codes, and then a generalization of the obtained properties will be done to present NB-LDPC codes as an extension of LDPC codes.

2.2.1 LOW-DENSITY PARITY-CHECK CODES

The invention of Turbo-Codes [11] by Berrou et al. in 1993 made possible having practical error correction codes that approach the Shannon limit [12]. Few years later (1996), an old class of codes was rediscovered [1], which won the interest of the scientific scene and successfully competed the Turbo-Codes. We talk about the Low Density parity-check codes, known as LDPC codes. Yet invented in 1963 by Gallager in his PhD thesis [13] they were ignored because of the technological limits at that time for efficient hardware implementation. In the second half of 1990, the two researchers Mackay and Neal's research [1, 14], Have resurrected the use of LDPC codes. In fact, they showed that LDPC code performance cannot only considerably approach the Shannon limit but also outperform the existent Turbo-Codes for long frame sizes. In the recent studies of error correcting codes, LDPC codes are playing crucial role. They were adopted in the new standards [15][16][17][18], due to their low decoding complexity asymptotic performance approaching the theoretical Shannon limit [19].

LDPC codes are linear block codes [20], that uses a generator matrix for encoding, and a parity-check matrix (PCM) for decoding. In the transmitter side, the generator matrix G encodes a K-length information message U to obtain a codeword C. The transmitted message C is obtained as follows :

$$C = UG \tag{2.2}$$

However, in the receiver part a sparse PCM of dimensions $(M \times N)$ generally denoted by H, represents the LDPC code. This matrix is dedicated to perform the decoding process. The PCM is said sparse, due to the fact that the number of non-null elements is far lower than the number of zero elements in the H matrix. In a PCM H, the number of lines M, represents also the number of parity equations in the PCM, and the number of columns N, represents also the length of the codewords. A codeword consists of K symbols that correspond to the initial information message and $M = N-K$ is the number of redundancy symbols added by the encoder. The H matrix parity-check equations must be respected by the codewords. Thus, a message C of length N is a codeword only if $C \times H^T = 0$, where H^T denotes the transposed matrix of H. Let us consider for example the following the PCM H of size 4×6 :

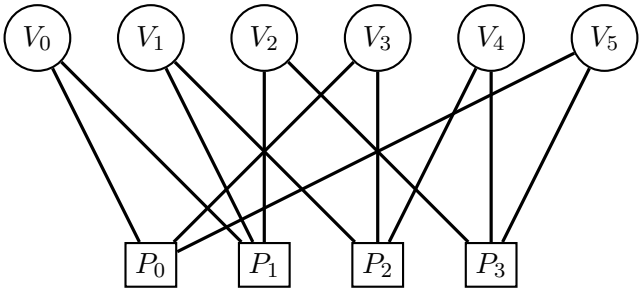

FIGURE 2.1 – Tanner Graph of an LDPC code

$$H = \begin{pmatrix} h_{0,0} & 0 & 0 & h_{0,3} & 0 & h_{0,5} \\ h_{1,0} & h_{1,1} & h_{1,2} & 0 & 0 & 0 \\ 0 & h_{2,1} & 0 & h_{2,3} & h_{2,4} & 0 \\ 0 & 0 & h_{3,2} & 0 & h_{3,4} & h_{3,5} \end{pmatrix} \tag{2.3}$$

Hence a codeword $C = [c_0; c_1; c_2; c_3; c_4; c_5]$ satisfies the following four equations :

$$h_{0,0}c_0 + h_{0,3}c_3 + h_{0,5}c_5 = 0 \tag{2.4}$$
$$h_{1,0}c_0 + h_{1,1}c_1 + h_{1,2}c_2 = 0 \tag{2.5}$$
$$h_{2,1}c_1 + h_{2,3}c_3 + h_{2,4}c_4 = 0 \tag{2.6}$$
$$h_{3,2}c_2 + h_{3,4}c_4 + h_{3,5}c_5 = 0 \tag{2.7}$$

In addition, the PCM of an LDPC code can be represented by a bipartite graph know as Tanner graph [21].Bipartite graph describes the code structure and also helps to perform the decoding algorithms, especially the iterative ones. A bipartite graph is composed of two sets of nodes. Each node is connected only to other nodes of the other set. For LDPC code, the two sets of nodes are the Check Nodes (CNs) and variable nodes (VNs).CN referrers to one row of the PCM and VN referrers to one column or equivalently a symbol of the codeword. Thus, the bipartite graph associated with an LDPC code is represented by a $M \times N$ dimension H parity-check matrix. It represent the relation between M CNs and N VNs. If a CN p_i is connected to a VN v_j, the element of the i^{th} row and j^{th} column of the PCM will be non-null. The matrix of the cited example can be represented by the bipartite graph in Figure 2.1.

The number of non-null symbols in the i^{th} column of the PCM is denoted by $d_v(i)$, $i \in \{1 \dots N\}$, and the number of non-null symbols in the j^{th} row is denoted $d_c(j)$, $j \in \{1 \dots M\}$. An LDPC code is regular if d_v and d_c are constant (i.e $\forall i, j$ $d_v(i)$=d_v, $d_c(j) = d_c$) respectively, for all the columns and all rows of the matrix, otherwise, the code is said irregular. We can identify the regularity of a PCM using its associated bipartite graph. The

code is regular if d_v and d_c that define the number variable node connections and check node connections, respectively, are constant. In the case of a regular LDPC code, the rate R of the code can be expressed as a function of d_v and d_c as follows :

$$R = \frac{K}{N} = \frac{N - M}{N} \geq 1 - \frac{d_v}{d_c} \tag{2.8}$$

2.2.2 NB-LDPC CODES OVER GF(Q) : AN EXTENSION OF LDPC CODES

LDPC codes with symbols that belong to the binary Galois field ($p = 1$) are said binary, while LDPC codes whose symbols of the codewords that belong to a Galois field of order $p \geq 2$ are said non-binary. In other words, NB-LDPC codes can be considered as an extension of binary LDPC codes. All the definitions and proprieties related to LDPC codes can be applied for NB-LDPC codes. However, the Tanner graph of a PCM NB-LDPC code has to incorporate new family of nodes called permutation nodes that are associated to the null-null entries of the PCM.

The elements of a PCM of a code GF(q)-LDPC belong to a Galois field GF(2^p), with $p \geq 2$, and operation applied on the matrix parity equations are performed using operations defined above for the Galois field GF(q). Figure 2.2 shows the bipartite graph that corresponds to the Equation 2.4. Note that we added the permutation nodes h_{00}, h_{03} and h_{05} that link Check node P_0 to variables nodes V_0, V_3 and V_5, respectively, to generate the parity-check equation P_0 over GF(2^p) $h_{0,0}c_0 + h_{0,3}c_3 + h_{0,5}c_5 = 0$.

Davey and Mackay have shown that NB-LDPC codes offer better performance compared to than their binary counterparts when the code length is small or when using higher order modulation [22]. In this manuscript, we will consider LDPC codes defined on the Galois field GF($q = 2^p$), with $p = 1$ (binary case), and NB-LDPC codes, with $p \geq 2$ (non-binary case).

2.3 ITERATIVE DECODING OF NB-LDPC CODES

Forward error correction is an imperative part of digital communication systems. In general the evaluation of a communication performance is determined by the used channel code (i.e. LDPC and NB-LDPC codes) at the transmitter part, and the decoding algorithm performed at the receiver part. In our dissertation we will consider the LDPC and NB-LDPC codes. We will detail the decoding process of some iterative decoding only for NB-LDPC codes. First, let us define the optimum decoding algorithm which is maximum likelihood decoding.

Let us consider $x = (x_0, \ldots, x_{n-1})$ be a random vector of length equal to n, transmitted over a noisy channel, and $y = (y_0, \ldots, y_{n-1})$ be the received vector. Then, y depends

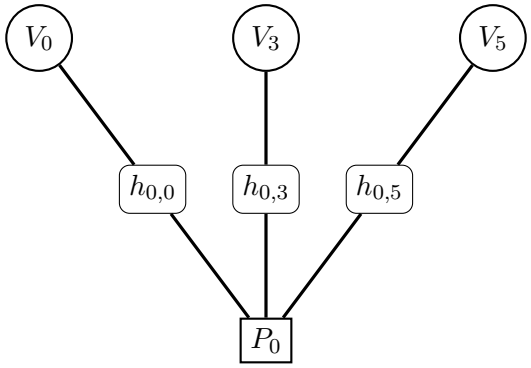

FIGURE 2.2 – Tanner Graph of a NB-LDPC code.

on x via the conditional probability $P_{X|Y}(x|y)$. Given the received vector y, the most likely transmitted codeword $\widehat{x}$ is the one that maximizes the probability $P_{X|Y}(x|y)$. This is commonly known as the maximum likelihood (ML) estimator. The transmitted codeword determination is performed as follows :

$$\widehat{x} = \underset{x \in \mathrm{C}}{\operatorname{argmax}} P_{Y|X}(y|x). \tag{2.9}$$

where C is the set of all possible codewords.

The ML decoder is the optimal decoder in term of codeword error probability. However its complexity grows exponentially with the length of the code. Only very short codewords can be decoded by means of the ML decoder. In practical, ML decoder cannot be chosen ; only iterative decoding algorithms can offer the possibility of decoding the received messages, by using their corresponding bipartite graphs. Iterative decoding has a linear complexity with the code length. The main principle of the iterative decoding algorithm of LDPC codes consists on exchanging messages between variable and check nodes with an iterative manner. This can be performed in two main steps for all types of iterative decoding :

— First, the message passed from a variable node V to a check node P contains the probabilities that V takes for the i^{th} element of GF(q), $i \in \{0, \ldots, q-1\}$. This is performed given the intrinsic probability values received from the channel and the extrinsic probability values received in the preceding iterations from other check nodes.

— Second, the message passed from P to V contains the probabilities that V takes for the q elements in GF(q). This message is concluded from the messages passed to P in the preceding iterations from variable nodes connected to V.

These two-step procedure is repeated n times, then, each variable node is decoded based on all the information obtained from its depth-n subgraph of neighbours.

2.3.1 BELIEF-PROPAGATION ALGORITHM

In the sixties, Gallager proposed a performing iterative decoding algorithm for binary LDPC codes called Belief Propagation (BP) [23] ; it is also called the Sum-Product algorithm (SPA). This decoding algorithm [24] has the closest performance to ML decoding among the existent iterative decoding algorithms. As the name belief propagation suggests, the algorithm is based on the propagation of messages composed of the probabilities of the symbols.

The algorithm used to decode binary LDPC codes can also be generalized to non-binary LDPC codes defined over finite fields by employing internal operations defined for the Galois fields. MacKay et al. generalized the BP algorithm to non-binary LDPC codes defined over finite fields [22].

The BP algorithm consists on updating messages between variable nodes and check nodes with an iterative manner until the decoder converge to valid codeword. In practice, it is easier to set the number of maximum iterations regardless of the convergence of the decoder. To reduce the latency of the decoder is advisable to stop decoding when the decoded mesaage converges to a valid codeword.

If we consider a transmitted codeword $x = (x_0, \ldots, x_{n-1})$, the a-posteriori probability (APP) of a given symbol α_j of a word x_i that belong to the transmitted codeword, and given the received word $y = (y_0, \ldots, y_{n-1})$ is defined as follows :

$$P(x_i = \alpha_j | y) \tag{2.10}$$

BP algorithm can be presented with a flow of messages in the Tanner graph that link variable nodes and check nodes. From now on we consider the following representation VO and VI that represent the messages flowing, out and in, respectively, of the variable node. A comparable notation will be adopted for parity-check nodes messages, PI for input messages PO, for output messages. Thus, $\{VI_{P_i,V}\}_{i=0\ldots d_v-1}$ is the set of messages entering a variable node V of degree d_v and $\{VO_{V,P_i}\}_{i=0\ldots d_v-1}$ is the set of output messages of the same variable node. Similarly, the sets $\{PI_{V_i,P}\}_{i=0\ldots d_c-1}$ and $\{PO_{P,V_i}\}_{i=0\ldots d_c-1}$ are the set of inputs and outputs of the check node P of degree d_c. Figure 2.3 represents the Tanner graph of a 2 parity-checks and denotes the various messages traversing though the graph.

To start performing the BP algorithm we need to compute at first the intrinsic information message that referrers to all variable nodes. This is done by the determination of q probabilities as follows :

$$P_{V_i} = [P_{V_i}[\alpha_0], P_{V_i}[\alpha_1], \ldots, P_{V_i}[\alpha_{q-1}]] \tag{2.11}$$

where, $\{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\} \in$ GF(q) and $P_{V_i}[\alpha_j]$, $j \in \{0, \ldots, q-1\}$ is the likelihood probability of symbol α_j. $P_{V_i}[\alpha_j]$ is calculated in the receiver part, and is defined as follows :

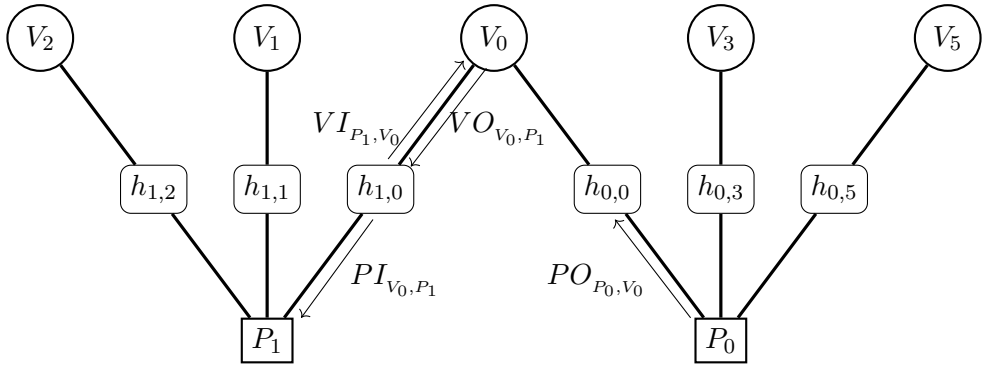

FIGURE 2.3 – Tanner Graph of an LDPC code.

$$P_{V_i}[\alpha_j] = P[y_i|x_i = \alpha_j] \tag{2.12}$$

The Belief Propagation (BP) algorithm can be performed in six distinct steps :

- **Initialization :** Here, all the messages VO are initialized with the likelihood information directly from the channel.

$$VO_{V_i,P} = P_{V_i} \tag{2.13}$$

- **Variable nodes update :** Consider a variable node V of degree d_v with the input messages $\{VI_{P_i,V}\}_{i=0\ldots d_v-1}$. To calculate the output message VO_{V,P_k} on the edge k, $k \in [0 \ldots d_v - 1]$, we consider all the input messages except the input message on the edge k.

$$VO_{V,P_k}[\alpha_j] = \frac{P_V[\alpha_j] \prod_{i=0,i\neq k}^{d_v-1} VI_{P_i,V}[\alpha_j]}{\sum_{l\in[0\ldots q-1]} P_V[\alpha_l] \prod_{i=0,i\neq l}^{d_v-1} VI_{P_i,V}[\alpha_l]} \tag{2.14}$$

- **Variable to parity-check permutation :** As we have a multiplication coefficient $h_{l,i}$ between the variable node V_i and the parity-check P_l in the Tanner graph :

$$PI_{V_i,P_l}[\alpha_j] = VO_{V_i,P_l}[\alpha_j \times h_{l,i}^{-1}] \tag{2.15}$$

Such an operation is equivalent to a permutation function in GF(q).

- **parity-check update :**

$$PO_{P,V_i}[\alpha_j] = \sum_{\left(\sum_{l\in[0\ldots q-1]} \alpha_l\right)=\alpha_j} \prod_{k=0,k\neq i}^{k=d_c-1} PI_{V_k,P}[\alpha_l] \tag{2.16}$$

- **parity-check to variable permutation :** As we have applied a permutation before transmitting the information messages from variable nodes to parity-checks, the reverse operation has to be performed after uploading the messages at the check nodes to transmit them to variable nodes.

$$VI_{V_i,P_l}[\alpha_j] = PO_{V_i,P_l}[\alpha_j \times h_{l,i}] \tag{2.17}$$

- **APP computation and codeword decision :** Finally, the APP of the symbols is computed at the variable nodes using the new probabilities. A decision is then made on each symbol.

$$\widehat{x_i} = \underset{\alpha_j \in GF(q)}{\operatorname{argmax}} \left\{ P_{V_i}[\alpha_j] \prod_{k=0}^{d_v-1} VI_{P_k,V_i}[\alpha_j] \right\}. \tag{2.18}$$

If all $\widehat{x_i}$ symbols verify all the PCM equations ($\widehat{x_i}$ symbols may not form a valid codeword see [25]) when the last iteration of the iterative decoding algorithm is ended, we can stop the decoding process. Otherwise, these steps are iteratively repeated until a valid codeword is obtained or a fixed number of iterations have been completed. Thus, if the maximum number of iterations is completed without decoding a valid codeword, a decoding failure is declared.

The main disadvantage of the BP decoding algorithm is its computational complexity, especially in the check nodes process. The complexity of the BP algorithm for a NB-LDPC code defined over a Galois field GF(q), is of the order $\mathcal{O}(q^2)$. Thus, lower complexity and performing algorithms were proposed. Log-BP, Min-Sum and Extended Min-Sum algorithms are the derivatives of the BP algorithm, that offer a computationally less complex alternatives. We will explain the steps that changes comparing to the BP algorithm in the next two sections.

2.3.2 LOG-BP ALGORITHM

Iterative decoding procedure, based on BP algorithm, guarantees the good performance of NB-LDPC codes. It is well known that the log-BP algorithm is essentially identical to BP algorithm proposed by Gallager [13]. Instead of computing probabilities as in [14], log-BP uses instead the logarithmic likelihood ratio (LLR) to communicate between variable nodes and check nodes.

- **Initialization :** $\forall\, v_i, i \in [1 \dots N]$, the reliability of a symbol α_j, $j \in [1 \dots q-1]$, can be represented by the LLR defined by Equation 2.19 :

$$\mathrm{LLR}(\alpha_j) = \log\left(\frac{P(x_i = \widehat{\alpha}|yi)}{P(x_i = \alpha_j|yi)}\right) \tag{2.19}$$

with

$$\widehat{\alpha} = \operatorname{argmax} \{P(x_i = \alpha), \alpha \in GF(q)\}. \tag{2.20}$$

Replacing the probabilities by LLR values in Equations 2.11, 2.14 and 2.16 makes it possible to convert the multiplication operations into addition operations and to reduce quantization errors. Thus, in the log-BP algorithm, the intrinsic information of a variable node V_i is defined by equation 2.21.

$$P_{V_i} = \left[\log(\frac{P_{V_i}[\widehat{\alpha}]}{P_{V_i}[\alpha_0]}), \log(\frac{P_{V_i}[\widehat{\alpha}]}{P_{V_i}[\alpha_1]}), \ldots \log(\frac{P_{V_i}[\widehat{\alpha}]}{P_{V_i}[\alpha_q - 1]})\right] \tag{2.21}$$

- **Variable node update :** The flow of messages in the bipartite graph contains the LLR values. Log-BP uses the same algorithm as the BP in the different decoding steps with some some modifications on the update equations. To update a variable node output messages we have to perform the following equation 2.29.

$$VO_{V,P_k}[\alpha_j] = P_V[\alpha_j] + \sum_{i=0, i\neq k}^{d_v - 1} VI_{P_i,V}[\alpha_j] \tag{2.22}$$

- **parity-check update :** The update of a Check node P_i is performed with the following equation 2.23 :

$$PO_{P,V_i}[\alpha_j] = \log \sum_{\left(\sum_{l\in[0\ldots q-1]} \alpha_l\right)=\alpha_j} exp\left(\sum_{k\neq l} PI_{V_k,P}[\alpha_l]\right) \tag{2.23}$$

- **APP computation and codeword decision :** Finally the MAP information of the variable nodes associated to $\widehat{x}$ is defined by equation 2.24 :

$$\widehat{x_i} = \underset{\alpha_j \in GF(q)}{\operatorname{argmax}} \left\{ P_{V_i}[\alpha_j] + \sum_{k=0}^{d_v - 1} VI_{P_k,V_i}[\alpha_j] \right\}. \tag{2.24}$$

2.3.3 MIN-SUM AND EXTENTED MIN-SUM ALGORITHM

2.3.3.1 MIN-SUM ALGORITHM

The Min-Sum (MS) algorithm was proposed in [26] to reduce the complexity of the log-BP algorithm using an approximation of equation 2.23. Indeed, in the Min-Sum algorithm, check node P is updated following Equation 2.25.

$$PO_{P,V_i}[\alpha_j] = \min_{\left(\sum_{l\in[0\ldots q-1]} \alpha_l\right)=\alpha_j} \left\{ \sum_{k\neq i} PI_{V_k,P}[\alpha_l] \right\} \tag{2.25}$$

The Min-Sum algorithm therefore simplifies the decoder by removing the mapping tables necessary to implement exponential functions and logarithms and minimizing the number of arithmetic operations.

2.3.3.2 EXTENDED MIN-SUM ALGORITHM

To simplify the Min-Sum decoder, the authors of [26] introduced the Extended Min-Sum (EMS) algorithm in which the messages flowing between the two sides of the bipartite graph are truncated. The main principle of the EMS algorithm is to select the first n_m symbols with the higher LLR values among the q possible symbols at both the check and variable nodes, with $n_m \ll q$. This idea was examined studied in [27].

In order to efficiently process the check nodes, the authors used a recursive implementation called Forward-Backward algorithm [26]. The complexity of the check nodes was then reduced to $\mathcal{O}(n_m log(n_m))$, instead of $\mathcal{O}(q^2)$ in the Min-Sum algorithm. However, the value of n_m should be carefully chosen so that the decoding performance does not suffer from significant degradation. In the case of the log-BP algorithm, the message vector is composed of q unsorted reliability values, thus the value of the symbol associated with each of the reliabilities can be easily derived from its position in the message.

Due to the truncation, the EMS algorithm messages must be sorted and the values of the symbols must be explicitly mentioned. The messages circulating from the variable nodes towards the check nodes and vice versa have the same representation. These messages are sorted in decreasing order of their corresponding LLR, and are limited to size n_m. The remaining $(q - n_m)$ elements of the LLR vector are considered to carry a default LLR value γ, computed by means of an offset O, in order to compensate for the performance degradation. The offset value have to be chosen carefully through a Monte Carlo estimation, in order to minimize the decoding performance of the NB-LDPC code, or by a density evolution minimization like in [26]. The message M carries the n_m most reliable LLR values. In order to keep track of the symbol corresponding to each LLR value, we have to associate an additional vector P, that indicates the set of GF symbols corresponding to the truncated LLR message. M and P can be expressed as :

$$M = [\mathrm{LLR}(j)]_{0 \leq j < n_m} \tag{2.26}$$

$$P = [\alpha_{\theta(j)}]_{0 \leq j < n_m} \tag{2.27}$$

where $\alpha_{\theta(j)}$ is the j^{th} most reliable symbol in the transmitted message M. And γ is defined as follows :

$$\gamma = \mathrm{LLR}(n_m - 1) + O \tag{2.28}$$

where O is a determined by doing Monte-Carlo simulations over different values of O in order to minimize the frame error rate (FER) [26].

- **Variable node update :** Consider the LLR-vector $VI_{P_i,V}$ as the inputs from the check node P_i to a variable node V of degree d_v. Vectors $VI_{P_i,V}$ are sorted in decreasing order, each of size n_m. The output vector VO_{V,P_k} from variable V to check node P_k is calculated as the highest n_m values from the symbol by symbol summation of all the inputs. VO_{V,P_k} is calculated as :

$$VO_{V,P_k}[\alpha_j] = P_V[\alpha_j] + \sum_{i=0,i\neq k}^{d_v-1} VI_{P_i,V}[\alpha_j] \tag{2.29}$$

and γ is the LLR-value corresponding to the symbols non considered in the input message. The n_m symbols with the lowest n_m LLR values sorted in increasing order are kept in the output VO_{V,P_k}. The symbols carrying highest LLR-values are truncated.

- **parity-check update :** To simplify the check node process, the Forward-Backward (FB) algorithm is adapted in the EMS decoding [28]. In fact, the FB algorithm is based on the division of a process into several elementary modules called Elementary Check Nodes (ECN). The outputs of the different ECN are putted together to form the whole process. The FB algorithm divides the CN processing in three layers : forward layer, backward layer and merge layer. Each layer is composed of $(d_c - 2)$ ECNs. The FB algorithm propose a linear structure which can be extended to any degree of check nodes. Given a check node of degree d_c, the number n_{ECN} ECNs needed for the FB algorithm is :

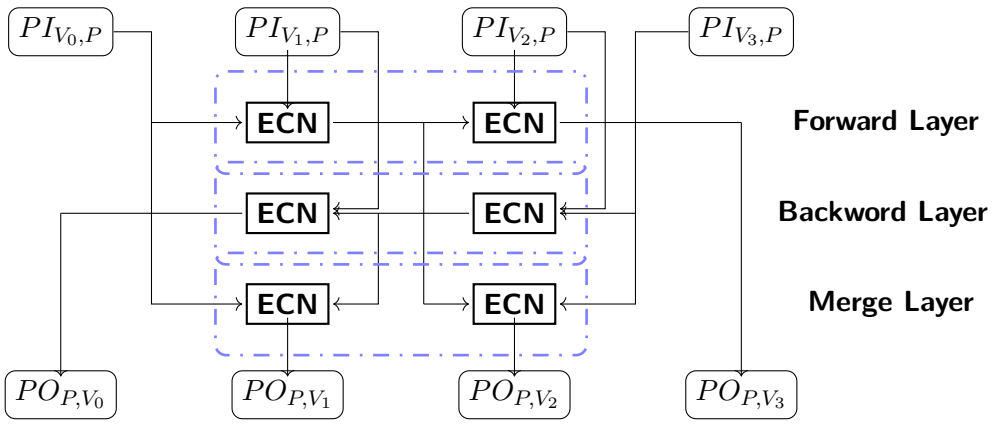

FIGURE 2.4 – The forward/backward CN processor with d_c =4.

$$n_{ECN} = 3(d_c - 2) \tag{2.30}$$

Fig. 2.4 shows the FB algorithm in a check node of degree d_c equal to 4, where, $PI_{V_k,P}$, $k \in \{0 \dots 3\}$ are the inputs and PO_{P,V_k}, $k \in \{0 \dots 3\}$ are the outputs of the check node.

The FB algorithm is based on the ECN process. Here we explain only the ECN update process, a process with two inputs V_1 and V_2 and a single output M LLR-vector only. All the vectors are of size n_m and sorted in decreasing order. P_1, P_2 and P are the vectors carrying the symbol information corresponding to LLR values of each vector respectively. Let $S(P[k])$ be the set of all the possible symbol combinations, (i,j) of $[0, 1, \dots n_m - 1]^2$, that satisfy the parity equation :

$$P_1[i] + P_2[j] + P[k] = 0 \tag{2.31}$$

The output message M is then obtained as :

$$M[k] = \min_{S(P[k])} (V_1[i] + V_2[j]) \tag{2.32}$$

In the previous sections, we presented the algebraic proprieties of the Galois fields, then, we have examined the main characteristics related to the structure of NB-LDPC, before explaining the new concepts that requires an extension of LDPC to NB-LDPC codes. Finally we have detailed the most used decoding algorithms of NB-LDPC codes in the literature. The main purpose of our dissertation is to get out the advantages of NB-LDPC codes when using high order modulations. These advantages will be determined from a comparative point of view with the existent codes especially the LDPC codes. Thus a comparison of NB-LDPC codes with their binary counterparts based on the state-of-the-art is performed in the next section. We will consider high spectral efficiency transmission for both LDPC and NB-LDPC codes. We will present some of the advantages of NB-LDPC codes. Later in Chapters 4.1 and 4 we will develop our contribution to broaden the existing advantages.

2.4 BINARY VS. NON-BINARY LDPC CODES

Binary LDPC codes have been extensively studied in the literature, which helped to adopt them in many communication standards. It has been shown that LDPC codes have asymptotic performance approaching the Shannon limit [1, 14]. Several studies were performed to improve the decoding performance and to simplify their implementation complexity. However, the binary LDPC codes performance decreases for small and medium size codewords. It has been shown in [22] that this loss can be compensated by using NB-LDPC codes with GF(q), where $q >> 2$. For small and medium size codewords, when applying an iterative low complexity algorithm, NB-LDPC decoders have a performance very close to the maximum-likelihood (ML) decoder as compared to binary LDPC decoders [29]. The

use NB-LDPC codes in place of binary LDPC codes will be then more efficient. This improved performance can be explained by different factors, we can enumerate some of most relevant ones. In fact NB-LDPC codes offer better resistance to errors and fit better the high spectral efficiency transmission. Different channel scenarios and transmission techniques confirm such assumption. NB-LDPC codes proved their superiority under AWGN channel [30], in a transmission with burst noise [31] and when using MIMO systems [32].

The NB-LDPC codes have proven their superiority in term of performance compared to their binary counterparts under certain transmission channel conditions and system applications. This was confirmed by a state-of-the-art review of the literature. Here we list some of the reasons why NB-codes offer good error decoding performance when compared to binary LDPC codes. Here we present some comparative ascertainment.

1. Better resistance to errors : The large cardinality codes offer better resistance to burst errors [33]. In fact, combining $\log_2(q)$ bits in a one symbol averages the errors over the received information, which helps the iterative decoding algorithm to converge more rapidly.

2. Good parity-check matrix structure : The bipartite graph associated to NB-LDPC codes offers better properties comparing to the binary ones, in terms of the number of cycles and minimum length cycle called girth. It was proven in [34] that when q becomes large ($q >> 2$), the best performances are obtained for ultrasparse NB-LDPC codes, which are NB-DPC codes with the minimum connectivity on the symbol nodes $d_v = 2$. Hence, the NB-LDPC codes help in avoiding the disturbance of short length cycles and thus improves the performance of the decoding algorithms e.g. BP algorithm. Such properties help to avoid the correlation induced in the messages due to the topological structures.

3. Good performance with high spectral efficiency transmission : NB-LDPC codes have better performance over channels with high spectral efficiency while using high order modulation [30, 35]. For the case of an M-QAM modulated transmission while using binary LDPC codes, the MAP demapper at the receiver side constructs symbol likelihoods which are inter-correlated at the binary level. This means that the decoder is initialized with already correlated messages even in the absence of cycles in the decoding graph. However, if the code is constructed in a non-binary Galois field with order greater than or equal to the modulation order, the decoder is initialized with uncorrelated messages which in turn improve the performance of the BP decoder. This was proved analytically and by means of simulations in [36].

4. Better performance under AWGN channel : In [31] decoding algorithms make NB-LDPC codes near capacity limit particularly at high rates for AWGN channel. The effect of using NB-LDPC codes with AWGN channel was investigated also in [37]. Decoding performances of NB-LDPC codes demonstrated that with sufficiently long codewords, the Shannon capacity of the binary AWGN channel can be approached by simply increasing the field order q of NB-LDPC codes.

5. More resistance to burst noise : Yang et al. showed in [38] that LDPC codes are very effective against noise bursts, however, Morinoni et al. proved in [39] that NB-LDPC

codes outperform their binary counterparts in the presence of burst errors. Performance on AWGN channel demonstrates that NB-LDPC codes offer better performance in presence of long bursts. This is explained by the fact that consecutive bits are grouped together forming symbols in the non-binary field GF(q).

6. Better performance under the MIMO systems : When using NB-LDPC codes with MIMO (Multiple-Input Multiple-Output) transmission schemes, we get better performance as compared to binary LDPC codes [32]. NB-LDPC codes exhibit a better balance between performance and complexity when detection and decoding are performed jointly as compared to when done separately [40].

Nevertheless, improving performance by increasing the order of the Galois field is accompanied by a significant increase in decoding complexity which make the use of codes GF(q)-LDPC a tradeoff between performance enhancement and the increase of decoding complexity.

2.4.1 NB-LDPC VS BINARY LDPC SIMULATION RESULTS

As we have mentioned in the previous section, Non-binary LDPC codes have a superior performance comparing to binary counterparts. This section presents examples of simulation results that encompass the performance of binary and NB-LDPC codes. To make the comparison clear and fair, note that LDPC codes are associated with Gray mapping, the best performing mapping when using binary decoding [41]. In addition, the simulations will consider for both LDPC and NB-LDPC codes the same decoding algorithm, e.g. the BP algorithm.

We will start by presenting some results of comparison by means of BP algorithm. We have chosen the BP decoding because it is the best performing iterative algorithm, hence it is possible to measure the contribution of the code structure. In Fig. 2.5 we present the comparison of the error correcting performance of binary and NB-LDPC codes. The comparison is performed over a binary-input AWGN channel. The considered codes have the same rate (r=$\frac{1}{2}$) and length (N=3000). When the Galois Field cardinality increases, better performance is obtained in both error floor and waterfall regions. In Fig. 2.5, we can notice easily the gain obtained when q evaluate form 2 to 64 and then 256. These results confirm that NB-LDPC codes perform better than their binary counterparts when using binary channel entries e.g. BPSK modulation. Let us confirm this affirmation when using high spectral efficiency transmission.

We now present the performance comparison of NB-LDPC codes for high order modulations (transmission using a 256-QAM modulation). Figure 2.6 represents the FER and BER performance of both binary and NB-LDPC codes. The binary code is optimized for the DVB-T2 standard [15], while the NB-LDPC codes is chosen with the same DVB-T2 standard codeword length [15], $N = 64800$ bits, equivalently $N = 8100$ symbols that belongs to GF(256). For the binary case, the Sum Product decoding algorithm is performed, while the GF(256)-NB-LDPC is decoded by means of the EMS algorithm [42] with n_m equal to

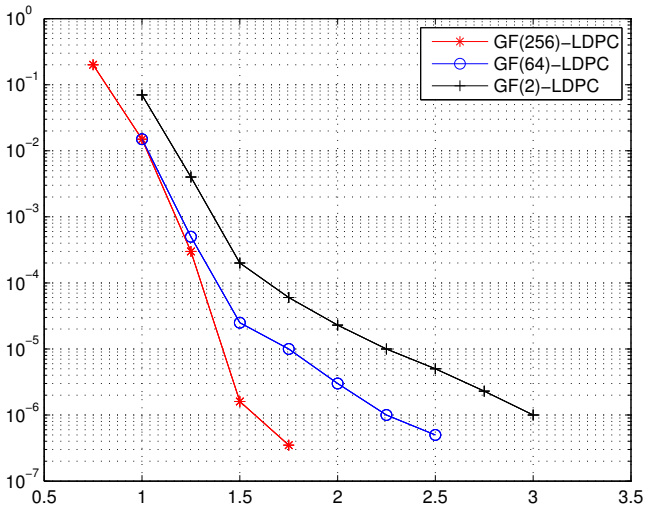

FIGURE 2.5 – Binary vs. NB-LDPC BER decoding over AWGN channel, for rate $= 1/2$, N_b=3000, and BPSK modulation.

30, 40 and 50.

Although EMS is sub-optimal compared to the Sum Product decoding algorithm, we can observe a gain for GF(256)-LDPC codes of almost 1 dB as compared to the binary decoding of the 256-QAM modulation. The gain in performance reaches 1.3 dB for $n_m = 50$. However, the decoder complexity is significantly increased. These simulation results show that using an order of field equal to the order of modulation order increases the gain of performance. When using a high efficiency transmission NB-LDPC codes can be a good alternative when comparing to their binary counterparts. Therefore, NB-LDPC codes are good candidates for future communication systems. However, the high decoding complexity of NB-LDPC codes makes it a trade-off choice.

2.5 CONCLUSION

In this chapter, we began by recalling some basic mathematical notions that were used to generalize the definition of LDPC codes on Galois Fields. Then we discussed the NB-LDPC decoding algorithms by describing in detail the BP, log-BP and EMS algorithms. The Extended-Min-Sum (EMS) algorithm emerged to be a promising candidate. It is a simplification of the binary Min-Sum algorithm. Boutillon et al. proposed methods to enhance performance of the EMS algorithm to lower the value of n_m number [42]. A comparative study between NB-LDPC codes and LDPC codes was finally performed. The presented examples of simulation results prove the given assumptions in the beginning of the chapter.

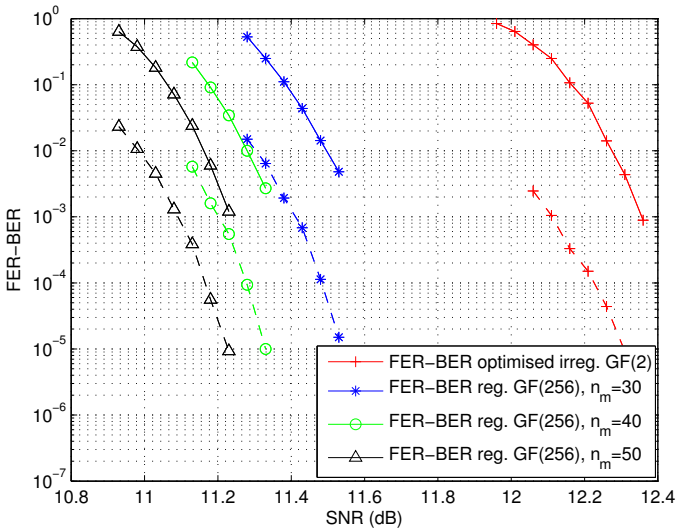

FIGURE 2.6 – Binary vs. NB-LDPC decoding over Rayleigh channel, for rate $= 1/3$, N_b=64800, and 256-QAM modulation.

Some of the high order modulation characteristics, especially for Coded modulation (CM) and Bit Interleaved Coded Modulation (BICM) schemes will be presented the next chapter.

Chapitre 3

Transmissions using high order modulations : Coded Modulation (CM) and Bit-Interleaved Coded Modulation (BICM) schemes

We have presented in the previous chapter the characteristics of LDPC and NB-LDPC codes, before having described some of the used decoding algorithms in the literature. This chapter is devoted to the presentation of the various elements of digital communication, required to this dissertation. In Section 3.1, we first present the considered transmission channel. Then, in Section 3.2, the considered modulations are described in detail. In sections 3.3 and 3.4, CM and BICM will be introduced in term of channel properties and mutual information (MI) metric. Finally, in the Section 3.5 we compute the channel capacity before presenting several capacity and MI curves in section 3.6.

3.1 TRANSMISSION CHANNEL MODELING

This section describes the different types of channels viewed in the context of this thesis. First, we present the model of the AWGN. Second, a detailed description of the fading channel is given in our study. Third, the Rayleigh channel with erasure is introduced to study the channel with destructive interferences caused by single-frequency networks (SFN).

3.1.1 ADDITIVE WHITE GAUSSIAN NOISE CHANNEL

The AWGN channel is the simplest used model to characterize a transmission channel. In this model, the received signal $r(t)$ is the sum of the transmitted signal $s(t)$ and a Gaussian noise $n(t)$:

$$r(t) = s(t) + n(t) \tag{3.1}$$

This channel modeling has a very important theoretical and practical importance. It is indeed a very accurate model for certain types of transmission channels for satellite and space communications. The additive Gaussian noise is modeling either an internal or an external noise. Internal noise sources are generated inside the electronic components of the system device. In general, this is a noise easy to characterize. External noise caused in general by weather and industrial noise, and their modelization is not obvious.

The AWGN is characterized by a centered Gaussian random process and with a bilateral power spectral density equal to $N_0/2$. The noise variance is related to the noise power spectral density N_0 as : $\sigma^2 = N_0/2$ and the probability density function $P_G(x)$ is given by :

$$P_G(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp(\frac{-x^2}{2\sigma^2}) \tag{3.2}$$

Let us consider a transmission system defined by the following parameters : E_s is the average symbol energy, E_b the average energy per information bit and n the number of bits per symbol. We can express E_s as follows :

$$E_s = nRE_b \tag{3.3}$$

where R is the code rate.

The signal-to-noise-ratio (SNR) is the ratio of signal power (P_E) and noise power (P_N), it can be then computed as :

$$SNR = \frac{P_E}{P_N} = \frac{E_s}{N_0} = \frac{n\,R\,E_b}{N_0} = \frac{n\,R\,E_b}{2\,\sigma^2} \tag{3.4}$$

We can then deduce the expression of σ from (3.4) :

$$\sigma = \sqrt{\frac{n\,R\,E_b}{2\,SNR}} \tag{3.5}$$

3.1.2 THE FADING CHANNEL MODEL

Several mobile radio communications systems use transmitting and receiving non-directional antennas to ensure total coverage of a geographic area. Consequently, the transmitted signal propagates in several directions and arrives at the receiver via different paths. Thus the received signal is the result of multiple superposed signals. Due to the multiple paths, interference between the different received signals can be constructive or destructive [43]. This results on a channel characterized by a fading related to multiple paths. Fading related to multiple paths can be classified into large-scale and small-scale fading. The large-scale fading, which can also be characterized as long-term fading, is due

to the attenuation of the received signal power when transmitter and receiver are at great distances. The degradation is caused by the presence of physical objects of considerable size in the wireless signal path. The receiver is said to be shadowed by these obstacles. This type of fading can be modeled through the estimate of a path loss as a function of the distance between the transmitter and the receiver. Small-scale fading events describe changes in the environment between a transmitter and a receiver. They can be caused by the mobility of the transmitter or of the receiver or by the crossing by any physical object of the line of sight path stretching between them. Small-scale fading events include also changes in the amplitude and phase of very short duration (of the order of a half wavelength) due to the time spreading of the signal or signal dispersion and to the Doppler effect [44]. Let us consider B_c the coherence bandwidth of the channel, over which the amplitudes of the different frequency components have the same attenuation, B is the frequency bandwidth of the signal. The channel is not frequency selective if $B \ll B_c$. In this case, all the signal frequency components have the same attenuation [45]. Otherwise, the channel will be a frequency selective channel, characterized by the presence of Inter-Symbol Interference (ISI). The Doppler frequency f_{max} characterizes the maximum Doppler frequency shift of the signals in a mobile environment. Thus, from the frequency domain point of view, fast fading occurs when the signal bandwidth is less than the maximum frequency Doppler shift. This frequency f_{max} is a function of the relative speed between the transmitter and the receiver v, and the wavelength of the transmitted signal λ as follows :

$$f_{max} = \frac{v}{\lambda} \tag{3.6}$$

Any wireless radio signal transmitted over large physical distances is subject to both small as well as large-scale fading types. The large-scale fading affects only the average strength of the received signal, and thus will not be considered in the remaining of our study. To be specific, we will focus our study to non-selective small-scale fading channels and precisely to the Rayleigh fading channels. Such a channel model is a typical channel encountered in many wireless environments. For instance, many systems such as Digital Video Broadcasting, Terrestrial (DVB-T) [46], the Digital Video Broadcasting, Terrestrial, the second generation (DVB-T2) [15], the Wireless Fidelity (IEEE 802.11) (WiFi) [18] and Worldwide Interoperability for Microwave Access (IEEE 802.16) (WiMax) [47], can be modeled as fading channels, since they use the Orthogonal Frequency Division Multiplexing (OFDM) technique that has the capability to transform frequency selective channels into parallel fading channels [48]. The received signal is expressed as :

$$r(t) = \rho(t)s(t) + n(t) \tag{3.7}$$

In this channel model, the received signal $r(t)$ is the sum of the product of transmitted signal $s(t)$ by the Rayleigh attenuation coefficient $\rho(t)$ and Gaussian noise $n(t)$. The envelope of the channel response will therefore be Rayleigh distributed. Calling this random variable ϱ,

it will have a probability density function $P_\varrho(x)$ expressed as :

$$P_\varrho(x) = \frac{x}{\Omega^2} e^{\frac{-x^2}{2\Omega^2}}, \quad x \geq 0. \tag{3.8}$$

Where $\Omega = E[\varrho^2]$ and $E[]$ is the expected value function. In our considered model Ω is equal to 1. The SNR is computed as follows :

$$\begin{aligned} SNR &= E[\varrho^2]\frac{nRE_b}{2\sigma^2} \\ &= \frac{nRE_b}{2\sigma^2}. \end{aligned} \tag{3.9}$$

3.1.3 THE FADING CHANNEL WITH ERASURE MODEL

This channel model has been used to model the destructive interferences caused by SFN in the case of the DVB-T2 standard [49, 15]. In fact, this standard uses the OFDM technique to eliminate Inter-Symbol Interference (ISI) and fading caused by multipath propagation. These characteristics allow a good deployment of SFN networks. Unlike multiple frequency networks (MFN), SFN involves several transmitters broadcasting synchronously the same program at the same frequency. The main advantage of this deployment strategy is the efficient use of bandwidth spectrum. However, the receiver may experience a superposition of two identical delayed signals, which can considerably damage the received signal. In that case, an erasure occurs, and the transmitted signal is unavailable at the receiver side, making it unrecoverable.

This considered channel model is equivalent to a Rayleigh channel model with some erasure events that affect the transmitted signal [50]. In general an interleaver component is inserted between the QAM labeling and the OFDM modulator. Thus, the erasure events can be modeled by a discrete random process $e(t)$ taking value 0 with a probability of P_e and value 1 with a probability $1 - P_e$. For this channel model, the received signal $r(t)$ can be represented as :

$$r(t) = e(t)\rho(t)s(t) + n(t) \tag{3.10}$$

Where $s(t)$ is the transmitted signal, $\rho(t)$ the Rayleigh attenuation coefficient, $n(t)$ the Gaussian noise and $e(t)$ the error event.

Erasure ratios up to 15% have been considered in the context of the DVB-T2. In a fading channel with erasures, the erasure ratio sets a bound on the coding rate R. In fact, with an erasure probability of P_e, reliable coded transmission cannot be done with a coding rate greater than $1 - P_e$, or in other words with a redundancy ratio lower than P_e. This prevents the considered channel system from operating at high coding rates especially when using the SFN. In our considered model, the SNR can be computed as follows :

$$\begin{aligned} SNR &= E[e]E[\rho]\frac{nRE_b}{2\sigma^2} \\ &= (1-P_e)\frac{nRE_b}{2\sigma^2} \end{aligned} \tag{3.11}$$

Throughout out dissertation, we assume a perfect Channel State Information (CSI) at the receiver side. Then, the Rayleigh fading value ρ and erasure e are supposed known. The estimation can be done by means of some specific techniques, like the use of pilot symbols [51]. We can insert pilots into the data flow symbols to deduce the channel fading events during the transmission process. In [15] pilots of pre-defined amplitude and phase are inserted into the signal at regular intervals in both time and frequency directions. They are used by the receiver part to estimate the channel state over the times and the different frequencies.

Now, we are able to characterize three different channel models : the Gaussian, the Rayleigh and the Rayleigh with erasure channels. These channel models will be considered in this dissertation.

3.2 HIGH ORDER MODULATIONS

Recent times have witnessed a tremendous surge in data rate requirements especially in wireless networks [52]. Data traffic within networks worldwide increases exponentially ; different authors gave some mention growth rates up to 50% per year [53]. This increasing in data traffic imposes different challenges for the network operators. In fact, more users of applications and higher data rate applications (Maps, Images, Video . . .), lead to a growing need for wireless capacity. Taking into account that the bandwidth is limited and considered as a very required resource and that higher frequencies are limited by propagation distances, the existing transmission capacity offered by the actual schemes is becoming insufficient. Thus, an increase of transmission limits is becoming very crucial by considering better performing schemes.

The ultimate solution is to develop communications systems that use high order modulation schemes, to provide high spectral efficiencies. Such solution enhances the amount of information transmitted using a given frequency bandwidth, i.e. transmitting more bits per second and per Hertz. Thus, the search for high order modulation formats plays an important role in high spectral transmission standards [15] [54]. By encoding $m = \log_2 M$ data bits on M symbols, the symbol rate is reduced by m compared to the data rate. Higher spectral efficiencies are then obtained via accumulating in one transmitted symbol m information bits.

3.2.1 TRANSMISSION OF MODULATED SIGNAL

In a digital transmission, the modulation is used to send one information among a set of M signals. Each digital transmission system is then associated to a set of M points named constellation $\mathcal{M}$. At reception, we assume a coherent demodulation. The average energy of the constellation $\mathcal{M}$ is defined by :

$$E_m = \sum_{k=0}^{M-1} P_k(x_{I_k}^2 + x_{Q_k}^2) \tag{3.12}$$

where (x_{I_k}, x_{Q_k}) define the k_{th} constellation point coordinates, and P_k is the probability of choosing the k_{th} constellation point coordinates in the transmitter part, $k \in [0 \dots M-1]$. When all the constellation symbols are equiprobable the average energy of the constellation can be expressed as :

$$E_m = \frac{1}{M} \sum_{k=0}^{M-1} x_{I_k}^2 + x_{Q_k}^2 \tag{3.13}$$

3.2.2 BIT AND SYMBOL RATES

In the digital transmission diagram scheme shown in Figure 3.3, the source encoder delivers binary elements (or bits) every T_b seconds. The binary flow rate of the source is defined as $D_b = \frac{1}{T_b}(bit/s)$. The bits are grouped into m-tuples or symbols to be assigned to the modulation signals. If the constellation has M points (i.e. the modulation of order M) : $m = \log_2 M$. The rate of the modulation, denoted by D_s, is defined as the number of symbols transmitted per unit time. It is expressed in Bauds and expressed as :

$$D_s = \frac{1}{T_s} = \frac{D_b}{\log_2 M} = \frac{D_b}{m} \tag{3.14}$$

where $T_s = mT_b$ is the transmission period of a symbol.

The spectral efficiency of a communication system is the number of bits of information transmitted per unit time and per unit of occupied band, or in other words, the throughput transmitted per unit of occupied spectral bandwidth. If we consider a linear M-point modulation for the transmission, the spectral efficiency of uncoded system, denoted by η, is :

$$\eta = \log_2 M(bit/s/Hz) \tag{3.15}$$

If a code of rate R is associated with the modulation, the spectral efficiency of the association is expressed as follows :

$$\eta = R\log_2 M(bit/s/Hz) \tag{3.16}$$

3.2.3 QUADRATURE AMPLITUDE MODULATION (QAM)

The modulation choice plays an important role in a communication system. Our approach aims to choose the most commonly used modulations in the literature. Thus, we will mainly consider amplitude modulation on two quadrature carriers (Quadrature Amplitude Modulation), commonly represented by M-QAM modulation, with M is the modulation order.

One of the easiest ways to implement QAM with hardware is to generate two separate signals with two independent amplitudes x_I and x_Q. Adjusting only the amplitude of any signal can affect the phase and amplitude of the resulting mixed signal. These two separate modulated signals are then added and transmitted to the receiver part. The bit-to-symbol mapping operation affects to each symbol of the constellation point a sequence of bits. This procedure influences the bit error rate (BER). Thus, bit-to-symbol mapping aims to choose the constellation point labels that minimizes the BER for a given symbol error rate (SER). Here we consider the Gray mapping, which is characterized by only one different bit between one constellation point and all of its neighbors. Such mapping minimizes the BER at the receiver part. Consequently, when code and modulation are separate entities, Gray mapping provides the lowest BER of all mapping types.

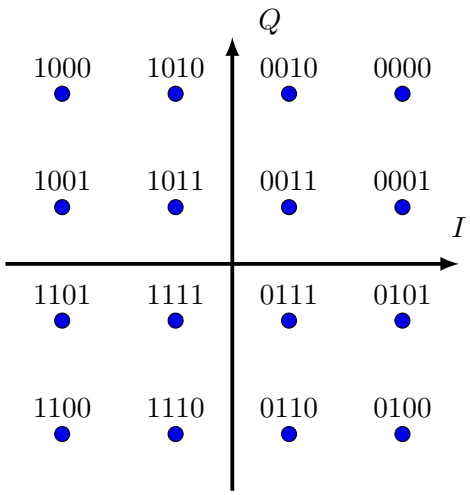

FIGURE 3.1 – 16-QAM modulation with Gray mapping.

The structure of QAM offers M distinct constellation points. Thus, it permits a symbol to contain $m = \log_2(M)$ bits of information. The signal constellation for 16-QAM is shown in Fig.3.1. Studies such as [55] have shown a substantial increase in average data rates when using 64-QAM. Higher data rates allow for example higher quality video calling and other multimedia services. The downside is that 64-QAM is much more sensitive to errors than 16-QAM. Such assumption is explained by the increase of BER with the modulation

order. To get a fixed BER, an increase of the modulation order must be accompanied with an SNR increase (The minimum Euclidean distance decrease with a constant E_s). The QAM modulation is widely used in modems designed for telephone communications [56], in second generation of terrestrial Digital Video Broadcasting [15], wireless networks, and mobile cell phone systems [57][58]. We can enhance the spectral efficiency by using the 256-QAM modulation or even the 4096-QAM one. For example the 256-QAM modulation is widely used for digital cable TV and cable modem [59, 60], while 4096-QAM modulation is used for cable systems [16].

3.3 CODED MODULATION SCHEME

To enhance the transmission robustness, a Forward Error Correction (FEC) is used for controlling errors in data transmission over unreliable or noisy communication channels. There are several ways to associate error correcting codes with the modulation. The most known are the Coded Modulation and the Bit-Interleaved Coded Modulation schemes.

The main principle of coded modulation scheme is to concatenate an error correcting code (NB-LDPC codes for example) and a signal constellation. It makes a group of coded bits mapped into points in the signal constellation in a way that enhances the minimal distance properties of the code. Thus, a codeword can be seen as a vector of signal points. Decoding will be ideally performed by choosing the closest codeword to the received vector in terms of the Euclidean distance in case of a AWGN channel.

3.3.1 SYSTEM MODEL

In coded transmission schemes, the fundamental elements are the channel encoder, modulator, channel, demodulator, and decoder as shown in Fig 3.2. Here we present a transmission over Rayleigh with erasure channel. When P_e, the erasure probability, is equal to 0, the channel is equivalent to the conventional Rayleigh channel.

3.3.2 NB-LDPC CODES ASSOCIATED TO MODULATIONS WITH THE SAME ORDER

In the previous chapter we have introduced the NB-LDPC codes. These codes present a good alternative to their binary counterparts, especially when using high order modulations. Since NB-LDPC codes are defined on high-order fields, it is possible to identify a closer connection between NB-LDPC and high-order modulation schemes. In such a case the GF(q) code, where $q = 2^p$, is associated to an M dimension coded modulation, and we have $M = q$ and $m = p$.

Using LDPC codes with a field order equal to the size of the constellation has a clear advantage compared to binary codes (LDPC codes for example). The encoder/decoder

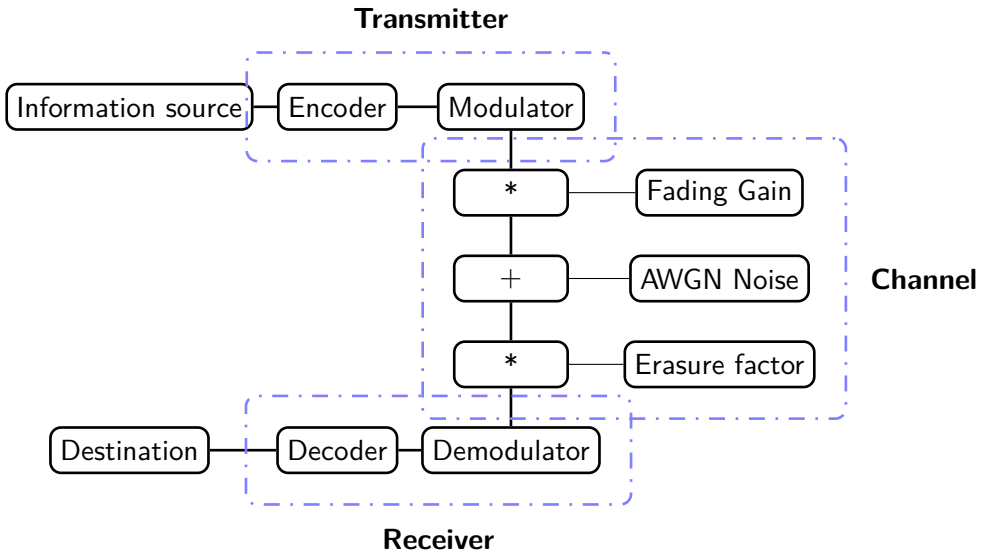

FIGURE 3.2 – Coded Modulation transmission scheme over Rayleigh channel with erasure.

works directly with symbols, thus, there is no loss of performance due to a demapping at the receiver. From a probabilistic decoding point of view, the channel likelihoods are directly processed by the decoder without any information loss, which automatically improves the performance of the decoding algorithms [30]. Conversely, when associating binary LDPC to M-ary modulation, the demapper generates likelihoods that are correlated at the binary level, and thus the decoder is initialized with messages that are already correlated. Standard information theoretical tools [61] show that a significant loss in performance is caused by symbol-to-bit and bit-to-symbol conversions.

Promising results have already been obtained with the association of an LDPC code over GF(64) with 64-QAM for transmission in Gaussian channel [62]. The gain of NB-LDPC codes becomes more important under short to moderate codeword lengths and high spectral efficiency. Promising results have been shown in the DAVINCI project [35]. In this thesis, we will investigate the performance of NB-LDPC codes associated to M-QAM modulations of the same order. The order of the GF(q) q will be equal to the order M of the QAM modulation, $q = M$.

3.3.3 THEORETICAL LIMITS FOR TRANSMISSIONS : MUTUAL INFORMATION COMPUTATION

This section is dedicated to Shannon's theory, which is the basis of the modern communication systems. Shannon developed a mathematical model based on probability theory and statistics to quantify the maximum amount of information that can be transmitted through a communication channel. The information is measured in terms of mutual information. We will present some theoretical tools in order to compute the limits of transmission and the capacity of the considered channels, for both Coded Modulation and Bit Interleaved Coded Modulation schemes.

3.3.3.1 NOTATIONS AND DEFINITIONS

Let us consider the following definitions :

— **X** is a random variable. $\mathbb{X}_n = \{x_0, ...x_{n-1}\}$ is the set of values that **X** can take. where n = $|\mathbb{X}_n|$ is the cardinality of **X**.
— **Y** is a random variable. $\mathbb{Y}_m = \{y_0, ...y_{m-1}\}$ is the set of values that **Y** can take. where m = $|\mathbb{Y}_m|$ is the cardinality of **Y**.

We can define the probability functions :

— $\mathbf{P_X}$ is the probability distribution of **X** given by $\mathbf{P_X}(x) = Pr(\mathbf{X} = x), \forall x \in \mathbb{X}_n$
— $\mathbf{P_Y}$ is the probability distribution of **Y** given by $\mathbf{P_Y}(y) = Pr(\mathbf{Y} = y), \forall y \in \mathbb{Y}_m$
— $\mathbf{P_{X,Y}}$ is the probability distribution of $\mathbf{X} \times \mathbf{Y}$ given by $\mathbf{P_{X,Y}}(x, y) = Pr(\mathbf{X} = x, \mathbf{Y} = y), \forall (x, y) \in \mathbb{X}_n \times \mathbb{Y}_m$
— $\mathbf{P_{X|Y}}$ is the probability distribution of **X** knowing **Y** given by : $\mathbf{P_{X|Y}}(x|y) = Pr(\mathbf{X} = x|\mathbf{Y} = y) = \frac{Pr(\mathbf{X}=x,\mathbf{Y}=y)}{Pr(\mathbf{Y}=y)}$

To simplify the task, the above probability distributions will be simply represented by $p(x)$, $p(y)$, $p(x, y)$, and $p(x|y)$.

3.3.3.2 MUTUAL INFORMATION COMPUTATION : DISCRETE PROBABILITY DISTRIBUTION

Self Information By definition, the amount of self-information contained in a probabilistic event $x \in \mathbf{X}$ depends only on the probability of that event

$$I(x) = \log_2 \frac{1}{p(x)} \tag{3.17}$$

Then, a small the probability event is associated to a larger self-information in the received information.

Entropy The information of the random variable **X**, called commonly **entropy**, is the average information over all the events $x \in \mathbb{X}_n$ and is denoted by $H(\mathbf{X})$ [63].

$$\begin{aligned} H(\mathbf{X}) &= E[I(x)] \\ &= \sum_{x \in \mathbb{X}_n} p(x) I(x) \\ &= \sum_{x \in \mathbb{X}_n} p(x) \log_2 \frac{1}{p(x)} \end{aligned} \tag{3.18}$$

The entropy $H(\mathbf{X})$ reflects of the uncertainty of a the random variable **X**. If $H(\mathbf{X}) = 0$ **X** in then known, while the case of maximum entropy $H(\mathbf{X}) = \log_2(n)$ corresponds to the maximum uncertainty (all the events are equiprobable). The entropy takes a value between 0 and $\log_2(n)$, thus $H(\mathbf{X}) \in [0, \log_2(n)]$.

Conditional Entropy The entropy of **X** conditioned on a particular event y, $y \in \mathbb{Y}_m$ is defined by :

$$H(\mathbf{X}|y) = \sum_{x \in \mathbb{X}_n} p(x|y) \log_2 \frac{1}{p(x|y)} \tag{3.19}$$

The definition of the conditioned entropy, $H(\mathbf{X}|\mathbf{Y})$, is obtained by computing the mean of all the events $y \in \mathbb{Y}_m$. Using of the Bayes' rule we obtain :

$$\begin{aligned} H(\mathbf{X}|\mathbf{Y}) &= \sum_{y \in \mathbb{Y}_m} p(y) H(\mathbf{X}|y) \\ &= \sum_{y \in \mathbb{Y}_m} p(y) \sum_{x \in \mathbb{X}_n} p(x|y) \log_2 \frac{1}{p(x|y)} \\ &= \sum_{y \in \mathbb{Y}_m} \sum_{x \in \mathbb{X}_n} p(x,y) \log_2 \frac{1}{p(x|y)} \end{aligned} \tag{3.20}$$

Mutual Information : The mutual information of **X** and **Y** is defined by :

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}) &= H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}) \\ &= \sum_{y \in \mathbb{Y}_m} \sum_{x \in \mathbb{X}_n} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} \end{aligned} \tag{3.21}$$

The Mutual information computation depends of the considered association code-Modulation. In other words, such metric depends of the entries of the decoding algorithm (Symbols in the case fo CM scheme, and Bits in the case of BICM scheme), and the used modulation. Thus, the Mutual information computation can be detailed for the CM and BICM schemes for the different considered channels in our dissertation.

3.3.3.3 MUTUAL INFORMATION COMPUTATION : APPLICATION TO CM FOR THE CONSIDERED TRANSMISSION CHANNEL MODELS

Let us define **X** and **Y** as the random variables that represent the input and output of the transmission channel. In the case of a wireless transmission, where the transmitter uses a pre-defined constellation, **X** and **Y** will be considered respectively as a discrete event and a continuous one. The mutual information $I(\mathbf{X};\mathbf{Y})$ between **X** and **Y** is given in (3.21) by

$$I(\mathbf{X};\mathbf{Y}) = H(\mathbf{X}) - H(\mathbf{X}|\mathbf{Y}). \tag{3.22}$$

The first term in (3.22) is maximized when all the constellation points have the same uniform probability $1/M$ of being selected (M is the number of the constellation points). In that case,

$$H(\mathbf{X}) = -\sum_{k=1}^{q} P(x_k)\log 2(P(x_k)) = m, \tag{3.23}$$

where $m = \log_2(M)$.

The second term in (3.22) is more complex to compute. We can derive its expression for AWGN, Rayleigh and Rayleigh with erasure channels.

GAUSSIAN CHANNEL

$$H(\mathbf{X}|\mathbf{Y}) = -\int_{y\in\mathbb{C}} p(y)H(\mathbf{X}|y)\mathrm{d}y, \tag{3.24}$$

where $\mathbb{C}$ is the set of complex numbers, and $H(\mathbf{X}/y)$ is defined as

$$H(\mathbf{X}|y) = -\sum_{k=1}^{q} P(x_k|y)\log 2(P(x_k|y)). \tag{3.25}$$

At the receiver side, $P(x_k|y)$, represent the probability that x_k was sent for a given y is defined as :

$$P(x_k|y) = \frac{P(y|x_k)P(x_k)}{\sum_{l=1}^{q} P(y|x_l)P(x_l)} \tag{3.26}$$

with

$$P(y|x_l) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y_I - r_I x_I)^2 + (y_Q - r_Q x_Q)^2}{2\sigma^2}}. \tag{3.27}$$

RAYLEIGH CHANNEL

$$H(\mathbf{X}|\mathbf{Y}) = -\int_{y\in\mathbb{C}} p(y)\left(\int_{\rho\in\mathbb{R}^2} H(\mathbf{X}|y;\rho)p(\rho)\mathrm{d}\rho\right)\mathrm{d}y, \tag{3.28}$$

where $\mathbb{R}$ is the set of real numbers and $p(\rho)$ is-two dimension Rayleigh probability distribution vector. $p(\rho)$ include both $p(\rho_I)$ and $p(\rho_Q)$, the Rayleigh probability distribution related respectively to the In-phase and the Quadrature components.

$$p(\rho) = (p(\rho_I), p(\rho_Q)) \tag{3.29}$$

Finally, $H(\mathbf{X}/y;\rho)$ is defined as :

$$H(\mathbf{X}|y;\rho) = -\sum_{k=1}^{q} P(x_k|y;\rho)\log_2(P(x_k|y;\rho)). \tag{3.30}$$

RAYLEIGH CHANNEL WITH ERASURE

$$H(\mathbf{X}|\mathbf{Y}) = -\int_{y\in\mathbb{C}} p(y)\left(\int_{\rho\in\mathbb{R}^2}\left(\int_{e\in[0\ldots1]^2} H(\mathbf{X}|y;\rho;e)p(e)\mathrm{d}e\right)p(\rho)\mathrm{d}\rho\right)\mathrm{d}y, \tag{3.31}$$

where $p(\rho)$ is the Rayleigh probability distribution and $p(e)$ the erasure probability distribution. With $p(e) = (p(e_I), p(e_Q))$, $p(e_I)$ and $p(e_Q)$ are respectively the erasure probabilities on the In-phase and the Quadrature components. $p(e_I) = 1$ with a probability equal to P_e, and $p(e_I) = 0$ with a probability equal to $1 - P_e$ (P_e being the erasure probability). The same holds for $p(e_Q)$. Finally, $H(\mathbf{X}/y;\rho;e)$ is defined as

$$H(\mathbf{X}|y;\rho;e) = -\sum_{k=1}^{q} P(x_k|y;\rho;e)\log_2(P(x_k|y;\rho;e)). \tag{3.32}$$

3.4 BIT INTERLEAVED CODED MODULATION

Bit-interleaved coded modulation (BICM) was first introduced by Zehavi in [64], and later analyzed from an information theory point of view by Caire and al [65]. It provides a pragmatic approach to coded modulation that can improve the transmission in wireless communications. The key point of the BICM advantage is that a wide range of scenarios can be achieved by separating modulation and demodulation from channel coding and decoding. Thus, they can be chosen to get a simpler and flexible design [65]. BICM is considered the dominant technique for coded modulation in fading channels [66], but it has

a small penalty when compared to the coded CM capacity [67, 65]. BICM schemes have been proposed in the ETSI broadcast standards such as the DVB-T2 standard [15] and IEEE wireless standards such as IEEE 802.11a/g [68] (wireless local area network) and IEEE 802.16 [69] (broadband wireless access).

3.4.1 SYSTEM MODEL

In the BICM scheme, the main blocks are : the channel encoder, bit interleaver, modulator, channel, demodulator, bit de-interleaver, and a decoder. Fig 3.3 shows this breakdown. We present here the Rayleigh with erasure channel, but it also covers the Rayleigh channel when P_e is equal to 0, and the AWGN channel when the channel gain is equal to 1 and P_e is equal to 0.

The BICM receiver demodulates groups of bits, each group mapped to a single data-symbol and transmitted over a memoryless channel. The soft reliability information represented by log-likelihood ratios (LLRs) is then sent to a subsequent binary decoder. In the binary decoder, bits of all the different groups are treated independently (We suppose that a performing bit-interleaver component is used in the transmission scheme).

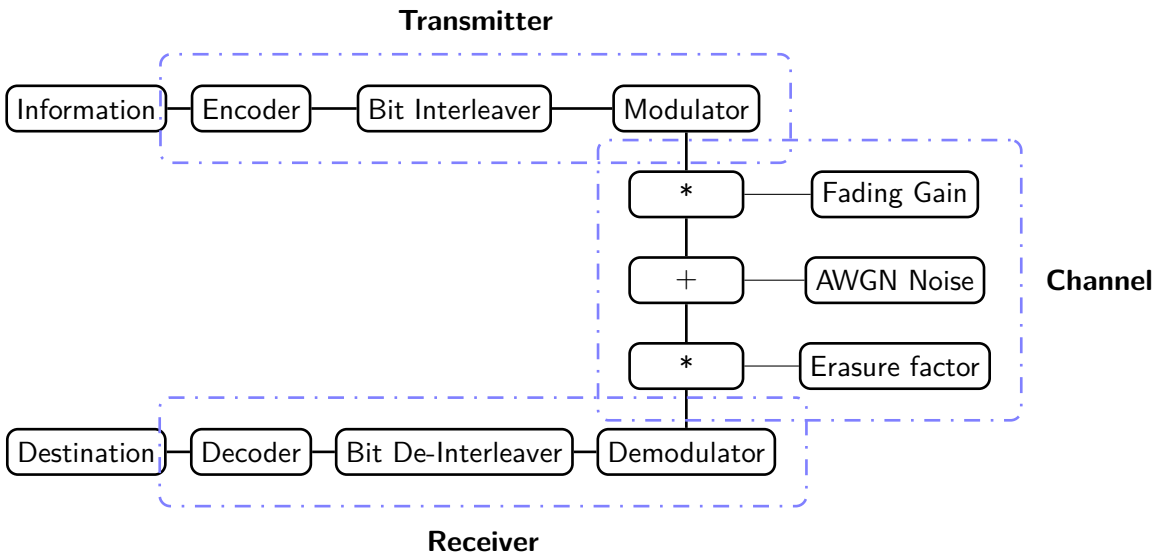

FIGURE 3.3 – Bit Interleaved Coded Modulation transmission scheme

3.4.2 THEORETICAL LIMITS FOR TRANSMISSIONS : MUTUAL INFORMATION COMPUTATION

The information-theoretic properties of the BICM were first introduced and studied in [65] under the assumption of an ideal interleaver which guarantees a completely random process. This assumption provided a rigorous background for the independent bit assumption and allowed the BICM system to be modeled as a set of independent parallel channels with binary inputs. The BICM scheme MI is then defined as the sum of MIs of the parallel channels representing the different bits of the transmitted signal [65, 70].

Let us consider a binary mapping of the constellation $\mathcal{M}$ that associates to each point x_k a binary codeword $(b_{k,1}, \cdots b_{k,m})$. Let X_i^0 be the set of symbols where the i^{th} bit b_i is equal to 0 and X_i^1 the set of symbols where the i^{th} bit b_i is equal to 1. Thus,

$$P(b_i = s|y) = \sum_{x \in X_i^s} P(x|y),\ s = 0, 1. \tag{3.33}$$

Assuming ideal bit interleaving, which makes the considered channel equivalent to m binary channels ([41] eq. 14), the second term of (3.22) can be expressed as

$$H(\mathbf{X}|\mathbf{Y}) = \sum_{i=1}^{m} H(\mathbf{B}_i|\mathbf{Y}) \tag{3.34}$$

where $\mathbf{B}_i$ represents the i^{th} binary channel associated to the i^{th} bit and $H(\mathbf{B}_i|\mathbf{Y})$ can be expressed for Gaussian, Rayleigh and Rayleigh with erasure channels, as follows :

GAUSSIAN CHANNEL

$$H(\mathbf{B}_i|\mathbf{Y}) = -\int_{y \in \mathbb{C}} p(y) H(b_i|y) \mathrm{d}y. \tag{3.35}$$

The entropy $H(b_i|y; r)$ is defined as

$$H(b_i|y; r) = -\sum_{s=0,1} P(b_i = s|y) \log 2P(b_i = s|y). \tag{3.36}$$

RAYLEIGH CHANNEL

$$H(\mathbf{B}_i|\mathbf{Y}) = -\int_{y \in \mathbb{C}} p(y) \left(\int_{\rho \in \mathbb{R}^2} H(b_i|y; \rho) p(\rho) \mathrm{d}\rho \right) \mathrm{d}y. \tag{3.37}$$

The entropy $H(b_i|y; \rho)$ is defined as

$$H(b_i|y;\rho) = -\sum_{s=0,1} P(b_i = s|y;\rho)\log 2P(b_i = s|y;\rho). \tag{3.38}$$

RAYLEIGH CHANNEL WITH ERASURE

$$H(\mathbf{X}|\mathbf{Y}) = -\int_{y\in\mathbb{C}} p(y)\left(\int_{\rho\in\mathbb{R}^2}\left(\int_{e\in[0\ldots1]^2} H(b_i|y;\rho;e)p(e)\mathrm{d}e\right)p(\rho)\mathrm{d}\rho\right)\mathrm{d}y, \tag{3.39}$$

The entropy $H(b_i|y;\rho;e)$ is defined as

$$H(b_i|y;\rho;e) = -\sum_{s=0,1} P(b_i = s|y;\rho;e)\log 2P(b_i = s|y;\rho;e). \tag{3.40}$$

3.5 CHANNEL CAPACITY

Claude Shannon was the pioneer of the information theory field ; he succeeded to characterize the limits of reliable communication on a transmission channel. Before Shannon, the only way to achieve small error probability over a noisy communication channel was to reduce the transmitted data rate. Shannon showed that, by coding the information, one can communicate at any rate strictly lower than the channel capacity with probability error transmission as small as we desire by means of the right correcting codes errors. Reciprocally, if the transmission rate is greater of equal to the channel capacity, then the probability of transmission error has a non-null lower bound. For every discrete memoryless channel, the channel capacity is the maximum information rate expressed in units of information per channel use, which can be achieved with a vetu small error probability, and is defined as follows :

$$C = \max_{P_{(\mathbf{X})}} I(\mathbf{X};\mathbf{Y}) \tag{3.41}$$

where the maximization is taken over all the possiblities of $P_{(\mathbf{X})}$, the distribution of the transmitted constellation.

3.5.1 GAUSSIAN CHANNEL CAPACITY

Let us consider a Gaussian channel with a signal power P_E, and an additive Gaussian noise power P_N. As shown in Equation 3.21, when calculating the capacity, the expression of the second term of $I(\mathbf{X};\mathbf{Y})$, $H(\mathbf{Y}|\mathbf{X})$, is computed as follows :

$$H(\mathbf{Y}|\mathbf{X}) = H(\mathbf{X}+\mathbf{N}|\mathbf{X}) \overset{(a)}{=} H(\mathbf{N}|\mathbf{X}) \overset{(b)}{=} H(\mathbf{N}) \tag{3.42}$$

In (a) we used the fact that, conditioned on **X**, $\mathbf{X}+\mathbf{N}$ is a known shift of the value of **N** which does not affect the entropy. In (b), it is obvious that **X** and **N** are independent. This means that the information over the channel can be computed as the difference between the received symbol and the noise entropies,

$$I(\mathbf{Y}|\mathbf{X}) = H(\mathbf{Y}) - H(\mathbf{N}) \tag{3.43}$$

N is a noise with a normal distribution : zero mean and variance $N_0 = P_N$, we can get then the expression of $H(\mathbf{N})$

$$H(\mathbf{N}) = \frac{1}{2}\log(2\pi e P_N) \tag{3.44}$$

We also know that for a given mean and variance, the distribution that maximizes the entropy is the Gaussian one (See [71] p. 181). Thus, maximizing $H(\mathbf{Y})$ over all distributions of **X** gives :

$$\max_{F(\mathbf{x})} H(\mathbf{Y}) = \frac{1}{2}\log_2(2\pi e(P_E + P_N)) \tag{3.45}$$

Hence, the information capacity C is given by :

$$\begin{aligned} C &= \max_{F(\mathbf{x})} I(\mathbf{X};\mathbf{Y}) \\ &= \frac{1}{2}\log_2(1+\frac{P_E}{P_N}) \\ &= \frac{1}{2}\log_2(1+SNR) \end{aligned} \tag{3.46}$$

When using a 2-Dimension constellation, the exact value of the capacity C of a discrete Gaussian channel is given by :

$$C = \log_2(1+SNR) bits/s/Hz \tag{3.47}$$

3.5.2 RAYLEIGH CHANNEL CAPACITY

The basic capacity results developed in the case of the Gaussian channel are now applied to analyze the limits of communication over fading channels. Assuming that the transmission has a constant fading event ρ, conditioned on this realization, the obtained channel is equivalent to an AWGN channel with received signal-to-noise ratio $|\rho|^2 SNR$. We can deduce the capacity of the channel as

$$C = \frac{1}{2}\log_2(1 + |\rho|^2 SNR) \tag{3.48}$$

Now we can average over many independent fades of the channel, and a reliable rate of communication of $E[\frac{1}{2}\log_2(1 + |\rho|^2 SNR)]$ can be achieved.

$$C = E[\frac{1}{2}\log_2(1 + |\rho|^2 SNR)] \tag{3.49}$$

When using a 2-dimension constellation, the exact value of the capacity C of the Rayleigh channel is given by

$$C = E[\log_2(1 + |\rho|^2 SNR)] \tag{3.50}$$

For a very large block length N with $N \to \infty$ and a given realization of the fading gains $\{\rho_1, \rho_2, \ldots, \rho_N\}$, the maximum achievable rate through this interleaved channel is

$$C = \frac{1}{N}\sum_{m=1}^{N}\log_2(1 + |\rho_m|^2 SNR) \tag{3.51}$$

3.6 MUTUAL INFORMATION AND CAPACITY CURVES

Based on the theoretical equations of MI and capacity computation developed in the previous chapter, we present here some MI and capacity curves, for both AWGN and Rayleigh channels. The MI is computed based on the Equation 3.22. The first term of the equation can be determined easily by means of the Equation 3.23. The second term of the Equation 3.22 is developed in Equation 3.24 (AWGN channel), and can be computed through a Monte Carlo simulation as detailed in Algorithm 1. Note that the same algorithm can be adapted for the Rayleigh channel by simply modifying the channel equation. In regards to the channel capacity, defined in Equation 3.41 we can get its expression for the considered channels in our dissertation. The curves as a function of the SNR can be easily derived directly from the expressions in Equation 3.47 and Equation 3.51 respectively, for AWGN and Rayleigh channels.

In Figure 3.4 we can observe MI curves of the most used M-QAM modulations : QPSK, 16-QAM, 64-QAM and the 256-QAM modulation when using the AWGN channel model. We plotted besides these MI curves the Shannon limit of the AWGN channel. All curves are presented as a function of the SNR. Figures (Fig. 3.5) and Fig. (3.6) present the MI obtained for the CM and the BICM schemes respectively for AWGN and Rayleigh channels for the 64-QAM modualtion. We observe that the CM curve outperforms the BICM for rates under $\frac{2}{3}$ (or a spectral efficiency smaller than 4 bit/s/Hz), in other terms more information can be transmitted in a case of CM scheme than the BICM one, for the same SNR value.

At this point, we have all the necessary tools to perform MI and channel capacity computation for both BICM and CM schemes. In the next section, we will introduce the signal

Algorithm 1

Initialization step : $H = 0$.
for $k = 1$ **to** N **do**
Randomly select a point x *of the M-QAM constellation*
Generate a sample w *of a complex AWGN of variance* σ^2
The received point y *is equal to* $y = x + w$
Compute $H(\boldsymbol{X}/y)$
for $i = 1$ **to** q, i.e. for each constellation point **do**
$p(y|x_i) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{d(y,x_i)^2}{2\sigma^2}}$
where $d(y, x_i)$ is the Euclidean distance between y and the x_i
end for
for $i = 1$ **to** q **do**
$p_i = P(x_i|y) = \frac{p(y|x_i)}{\sum_{k=1}^{q} p(y|x_i)}$ (x_i are equiprobable)
end for
$H(X/y) = -\sum_{i=1}^{q} p_i \log 2(p_i)$
$H = H + H(X|y)$
end for
$C = \log 2q - \frac{H}{N}$

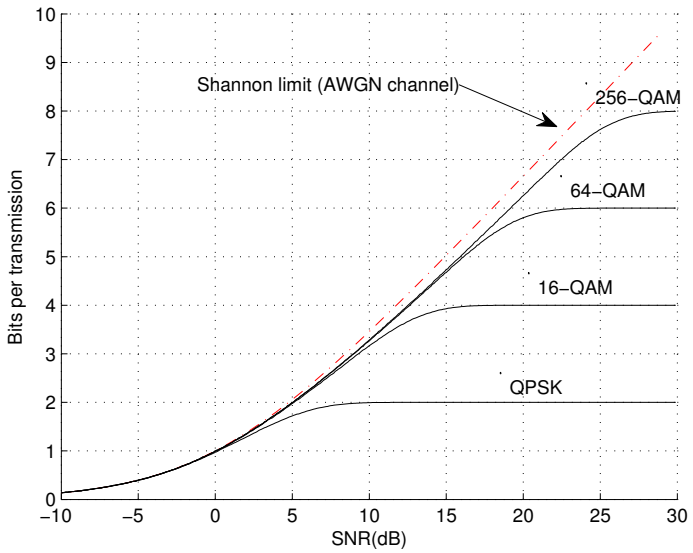

FIGURE 3.4 – MI of M-QAM modulation with Shannon limit for AWGN channel.

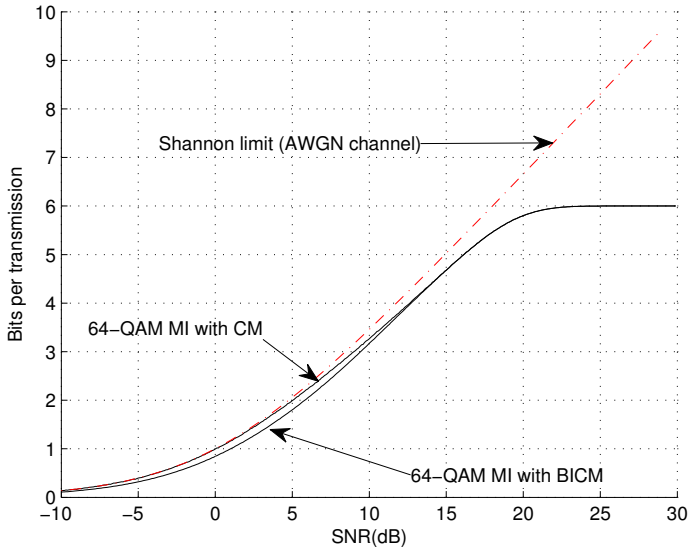

FIGURE 3.5 – 64-QAM MI under CM and BICM schemes.

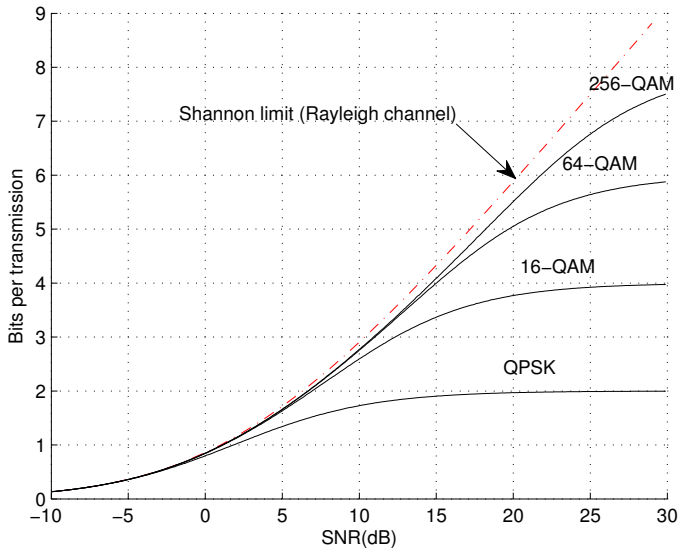

FIGURE 3.6 – MI of M-QAM modulation with Shannon limit for Rayleigh channel.

space diversity technique, its domains of application, and the proposed methods of its optimization.

3.7 CONCLUSION

In this chapter, we began by recalling some elements of the digital communication in a transmission channel. Then the considered modulations in this thesis were particularly advanced. Next, channel properties like MI, and channel capacity of CM and BICM schemes are introduced, and some of the MI curves are presented. The following chapter is dedicated to introduce the first novelty proposed in this dissertation, which is the MI based SSD technique optimization. The proposed method aim to select the rotation angle that maximizes the MI. An in-depth study will be carried out to optimize the SSD for both CM and BICM schemes.

Chapitre 4

Signal Space Diversity optimization based on the analysis of Mutual Information

In new broadcast systems, where fading channels with and without erasures are the most used channel models [54] [15] [17], and where high order signal constellations are being considered for transmission, big fading events and erasures can incur heavy losses in terms of error rate and throughput. These impairments have to be appropriately compensated for to enhance system performance. A solution proposed to mitigate the effect of big fade events and erasures is to combine the SSD with error control code [72] [73] [74], to achieve high data rates over wireless links. Several studies have been carried out to optimize the use of the SSD in the transmission systems. They revealed that SSD represents a promising technique to improve performance of modern communication systems. Recently the DVB-T2 standard [75] witnessed the incorporation of such technique to satisfy the surge in data rate requirements in new broadcast networks.

In this dissertation, we address the problem of optimizing the signal space diversity technique. For this purpose we consider mutual information (MI) which provides an analytical framework for constellation rotation optimization. This kind of optimization was considered in different areas of application. In the proposed formulation, we aim to optimize SSD in terms of MI for the Rayleigh channel with and without erasure. Thus, we will give two analytical characterizations of the MI of these two channels for both CM and BICM schemes, which are shown to characterize a wide range of transmission conditions. The method that we follow consists in first deriving the MI expression of these considered channels for all possible rotation angles. Then, we select the rotation angle that maximizes the MI for considered diversity technique. For both Rayleigh channel and Rayleigh channel with erasure and CM and BICM schemes, we present a detailed analysis of the optimal rotation angles and their performance depending on the signal to noise ratio. We show that the optimal rotated constellations significantly outperform conventional constellations and those proposed in the literature in terms of MI-based theoretical analysis and performance.

In Section 4.1, we introduce the SSD technique, before presenting some examples of its application in Section 4.2. In sections 4.3 and 4.4, some methods of optimization are exposed. Then, motivations behind considering the mutual information metric are derailed in Section 4.5. Theoretical study and an explanation of the proposed optimization method are presented in Section 4.6. Finally, in Section 4.7 we show simulation results to confirm the predicted results announced by the theoretical study.

4.1 SIGNAL SPACE DIVERSITY

Signal Space Diversity (SSD), defines a diversity technique known as coordinate interleaving or modulation diversity. The main idea of the SSD technique is to correlate the In-phase (I) and the Quadrature (Q) components of the conventional QAM signals using a rotation, and then to introduce different fading attenuations to I and Q components by distributing these components on different sub-carriers. SSD was first presented in 1992 [76] and then mentioned again represented in 1996 [77] as a coordinate interleaving scheme for performance improvement over fading channels. In 1998 [78], the same scheme was introduced as an improved PSK scheme for fading channels and was generalized in 1998 [72] as a signal space diversity scheme. In 2003 [79], it was presented as modulation diversity scheme for frequency selective channels. In 2008, this technique was adopted for the first time in a transmission standard (DVB-T2 standard) [15].

In fact, SSD increases the diversity order of the signal set with high order modulations, e.g. QAM constellations [72]. Very high diversity order can be achieved, and this results in an almost Gaussian performance over the fading channel [80]. This modulation diversity is essentially uncoded and enables to add diversity with a limited increase of the transmission system complexity, without any of power nor bandwidth expense. The transmitted bits are grouped into blocks and directly mapped to the constellation points. This means that the coding gain is obtained only with some modulation/demodulation complexity increases. To distinguish from other types of diversity like time, frequency, space and code, here the diversity will be related to modulation. The key point to increase the modulation diversity is to apply a certain rotation to a classical signal constellation that maximizes maximum number of distinct components, with independent attenuation events on the two components. In addition to the fact that SSD does not require bandwidth nor power expansion, such a technique leads to significant performance improvement over conventional radio link communication systems, see DVB-T2 as an example [50, 81].

To apply the SSD technique over wireless communication systems, we have to combine the rotated constellation with independent fading events over the two components of the sent signal constellation. The independence of fading channels can be performed by means of an interleaver in the transmission part and a De-interleaver in the receiver part. Such type of diversity tries to exploit the low probability that deep fades occurrence simultaneously in both I and Q components. Therefore, SSD offers the possibility to lower the probability of error. SSD exploits the orthogonality between the I and Q components to

achieve gain in fading channels with and without erasure. Many techniques have been proposed to achieve the independence of the channels required by diversity : Space diversity, antenna polarization diversity, frequency diversity and Time diversity.

The research community showed interest towards the SSD technique and tried to optimize its application, however certain important questions are not fully answered. Thus, optimizing the SSD technique still has an interesting spectrum of research and developing. Some of these questions include the exact calculation of optimum rotation angles, the effect of different signal constellation mappings, and the influence of the type of transmission channel. In the following section we will explain how the SSD technique can be considered in a transmission channel.

4.1.1 SSD TECHNIQUE DESCRIPTION

In fact, the SSD technique combines a rotated constellation with independent fading events over the two components of the sent signal constellation. First, the rotation can be applied on an M-QAM or M-PSK modulation constellations for example, which is relatively an easy task. Second, since the two components I and Q are orthogonal, a separation of the two component must be done before transmission. A component interleaver based on time diversity is practical method to make both components fade independently. It can be performed by introducing a delay on the Q component. The constellation symbol $X{=}(x_I, x_Q)$ is sent to the receiver via a modulated signal $x^t = (x_I^t, x_Q^t)$, where t represents the time index. Then the quadrature component x_Q^t is delayed by d time slots. Thus, at time t, the transmitted symbol (x_I^t, x_Q^{t-d}) is affected by a multiplicative factor r_t and at time $t + d$, the transmitted symbol (x_I^{t+d}, x_Q^t) is affected by r_{t+d}. At the receiver side, a delay d on the I component allows the received symbol y^t to be reconstructed, with $y_I^t = r_I^t x_I^t + w_I$ and $y_Q^t = r_Q^t x_Q^t + w_Q$, where w_I and w_Q represent the additive noise on the I and Q axes, $r_I^t = r^t$ and $r_Q^t = r^{t+d}$. In [82], the authors propose to make I and Q fade independently by means of a random component interleaver, where an efficient component interleaver for NB-LDPC scheme on Rayleigh channel is presented.

When using the SSD technique, the transmission scheme elements are almost the same as for the CM (Fig. 3.2) and BICM (Fig. 3.3) schemes. We have to add in the transmitter part, a rotation to the modulator component and, a component interleaver, while for the receiver part, a component de-interleaver will be considered. Figure 4.1 shows the block diagram of a transmission system employing the SSD technique, as described above, applied to a CM scheme. This concept is generic to all constellations, and can be extended the BICM scheme by introducing a bit-to-symbol mapper and a bit-to-symbol demapper, respectively, in the transmitter and receiver parts.

Let us consider a constellation $\mathcal{M}$ and a symbol X represented with I component x_I and Q component x_Q. If the transmission of X over the Rayleigh fading channel, is performed as described by Figures 3.2 and 3.3, both the I (x_I) and Q (x_Q) components will

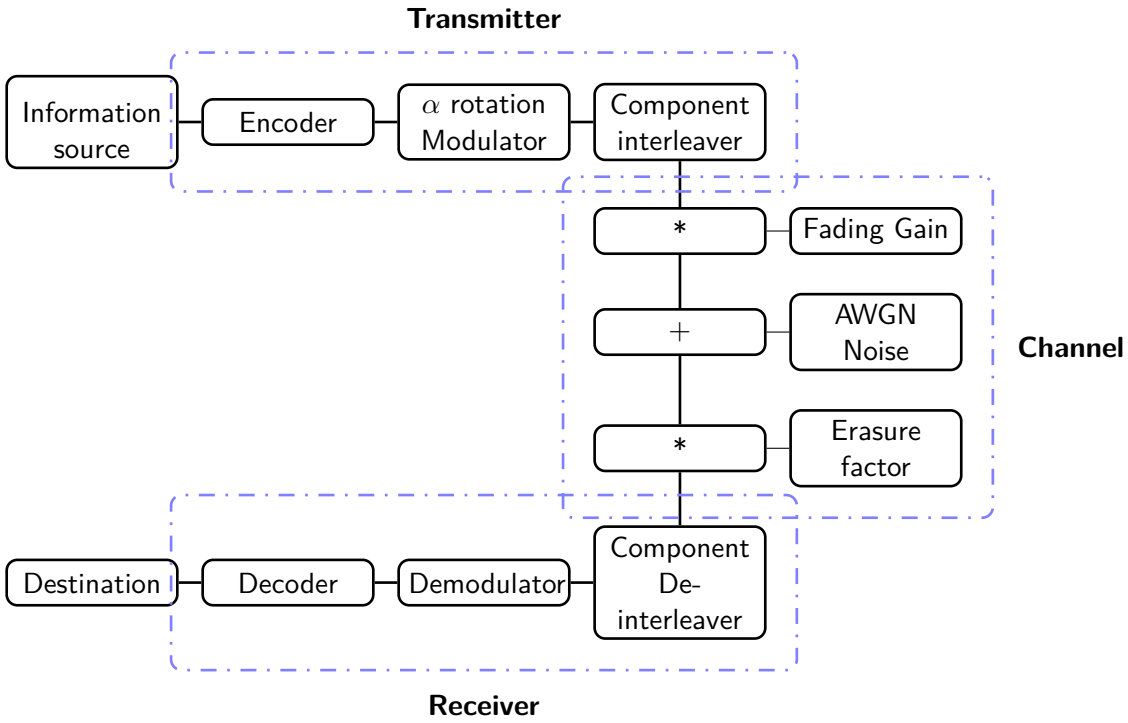

FIGURE 4.1 – Coded Modulation transmission scheme with the SSD technique

fade identically. Let us present a frequent scenario when using the Rayleigh channel, a severe fading event on a 16-QAM modulation, without rotation (Figures 4.2 and 4.3). The reconstructed constellation has points which are very close one to each other. The loss of information on both components is irreversible which increases the decoding error probability. In order to help the demapper to retrieve the transmitted symbol, it is more efficient to send separately x_I and x_Q in two different times or frequency slots, so that the fading coefficient r_I affecting x_I will be independent of the fading coefficient r_Q affecting x_Q. Figures 4.4 and 4.5 show the SSD technique effect when a deep fade event occurs on one component. The rotated constellation increases the minimum distance between the points of the reconstructed constellation. That offers more protection against the effects of noise, given that the two components will keep a minimum of information. Signal demodulation is assumed to be coherent, so that the fading coefficients can be modeled.

In the next section we provide further details on the SSD technique in order to justify the performance gain introduced by this technique in both Rayleigh channel and Rayleigh channel with erasure.

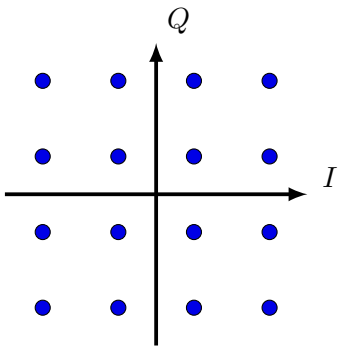

FIGURE 4.2 – 16-QAM modulation (Constellation before transmission)

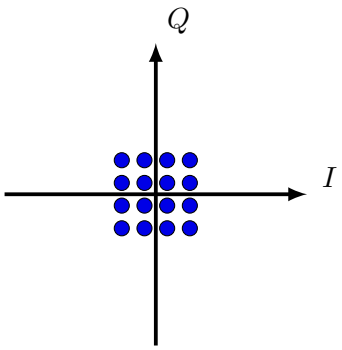

FIGURE 4.3 – 16-QAM modulation with severe fading on Q axis

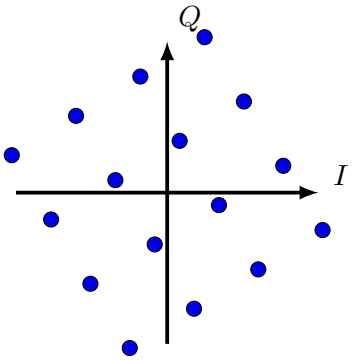

FIGURE 4.4 – Rotated 16-QAM modulation (Constellation before transmission)

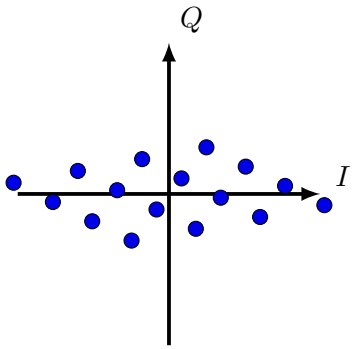

FIGURE 4.5 – Rotated 16-QAM modulation with severe fading on Q axis

4.1.2 INTUITIVE EXPLANATION OF THE SSD TECHNIQUE ADDED VALUE

The advantages of the SSD are revealed when we apply such a technique to the Rayleigh channel with and without erasure. For both channels we can propose an intuitive explanation of reasons behind its good performing [74]. Here, we will propose a geometrical approach to compare the impact of the two scenarios with and without rotation on the minimum Euclidean distance (we assume that I and Q fade independently).

An intuitive explanation for the benefit of the SSD technique under the Rayleigh channel can be given with reference to figures Fig.4.6 and Fig.4.7 that represent respectively the received constellation (QPSK modulation) without and with rotation. In such a system with a component interleaver, the I and Q components may experience different fading events that can be deep or only moderate. Looking on both figures Fig.4.6 and Fig.4.7, the fading applied on the Q component is clearly important. By comparing these two figures, the possible

added value of rotation becomes evident, we can easily notice that the minimum Euclidean distance $d2_{min}$ in Fig.4.7 is superior than that of Fig.4.6 $d1_{min}$, which clearly shows that the symbol distance increased with rotation. Therefore, the rotation can be intuitively judged as an advantage for Rayleigh channel, based on an observation of geometrical properties.

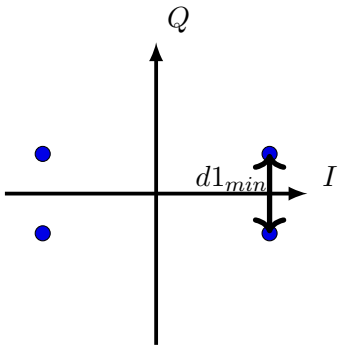

FIGURE 4.6 – QPSK modulation with fading

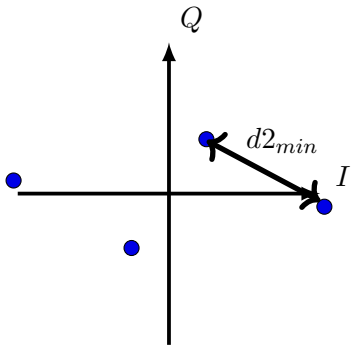

FIGURE 4.7 – Rotated QPSK modulation with severe fading

A theoretical study of of the impact of rotation on the minimum Euclidean distance can be performance. Let us consider the received constellation when using a rotated (rotation angle α) and non-rotated constellation (we suppose that $r_I < r_Q$). If we consider an M-QAM modulation with a minimum Euclidean distance d_{min}, for non-rotated constellation the minimum Euclidean distance of the received constellation is $d1_{min} = r_I d_{min}$. When using a rotated constellation, the minimum Euclidean distance $d2_{min}$ will be the distance between $X_1 = (r_I(cos(\alpha)x_I - sin(\alpha)x_Q), r_Q(sin(\alpha)x_I + cos(\alpha)x_Q))$ and $X_2 = (r_I(cos(\alpha)(x_I + d_{min}) - sin(\alpha)x_Q), r_Q(sin(\alpha)(x_I + d_{min}) + cos(\alpha)x_Q))$, it can be computed as follows :

$$\begin{aligned} d2_{min} &= |X_1 - X_2| \\ &= \sqrt{d_{min}^2((r_I cos(\alpha))^2 + (r_Q sin(\alpha))^2)} \\ &= \sqrt{d_{min}^2((r_I cos(\alpha))^2 + (r_I sin(\alpha))^2) + \zeta}; \zeta > 0 \\ &= \sqrt{d_{min}^2 r_I^2 + \zeta} > d_{min} r_I = d1_{min} \end{aligned} \tag{4.1}$$

Thus, in a theoretical point of view, rotating the constellation will enhance the minimum Euclidean distance of the received constellation.

For Rayleigh channel with erasure, benefit of the SSD technique can be given with reference to figures Fig.4.8 and Fig.4.9 that represent respectively the received constellation (QPSK modulation) without and with rotation. When P_e is low the probability of getting both components erased on the received part is then of the order of the square of P_e, so that in most cases at least one of the two components reaches the receiver part with only a

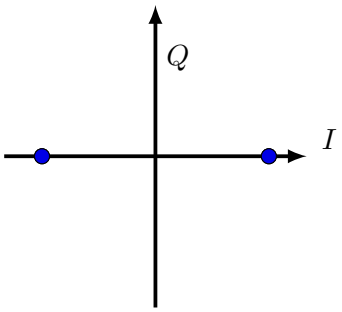

FIGURE 4.8 – QPSK modulation with an erasure on the Q component

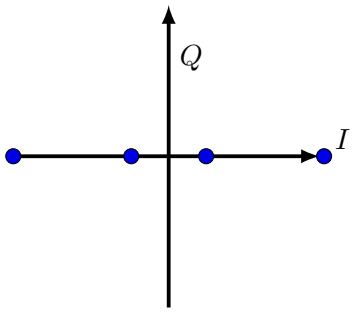

FIGURE 4.9 – Rotated QPSK modulation with an erasure on the Q component

fading event with a known coefficient. We avoid then an irreversible loss of information in the receiver part. Thus the received information will be carried up on a one dimension vector as we can see on the two figures above. By comparing these two figures, the possible added value of rotation becomes clearer. We can observe that, in Fig.4.8, the projections of constellation points having the same I component are superposed. Thus the minimal distance become equal to 0. That induces disruptions on the decoding process. While when adding rotation, the image of the received constellation, shown in Fig.4.9, has dissociated projections on the I axis. We can clearly notice that the symbol minimum distance increases under rotation. Therefore rotation associated with a component interleaver, can be judged to be advantageous under the Rayleigh channel with erasure.

4.2 EXAMPLES OF APPLICATION OF THE SSD

We can find several studies in the state-of-the-art, that tries to get out advantages of the SSD technique application [74] [83] [84]. These applications consider in especially the 2-dimension transmission using the Rayleigh channel model with and without erasure [74] [50] [81], but d-dimension transmission ($d > 2$) were also considered like the multiplicative fading channel and the MIMO (multiple input multiple output) channel.

Two-dimension transmission under the Rayleigh channel model with and without erasure : The two dimension (2-D) transmission over a Rayleigh channel is known to be a common scheme in the communication systems, [85] [86]. The DVB-T2 standard is an example of industrial application that employs the SSD technique over a 2-D channel with QAM modulation. SSD enables important gains compared to conventional QAM modulation under severe channel conditions. Rotation angles for the different QAM constellations were proposed and a corresponding low-complexity detection method, and more than 1-dB gain was observed in high rate transmission [15]. However, the corresponding demodulation complexity remains an optimization issue [87]. An extension was made for the Rayleigh channel with erasure [50], where more than 6 dB gain can be obtained (Erasure probability

of 15%, coding rate $4/5$ and 16-QAM modulation).

Multiplicative Fading Channels : In [83] the authors generalize the application of SSD over multiplicative fading channels, where fading is represented by the product of statistically independent Nakagami-random variables. Based on the pairwise error probability (PEP) expression in [83], it is shown that for large dimensions, the error performance over multiplicative fading channels can be significantly improved by using the SSD technique, without any bandwidth expansion. Such a fading model matches very well with the forest environment, in keyhole propagation, or in a propagation in the presence of diffraction street corners.

MIMO channel : In [84] an efficient wireless transmission scheme with SSD is proposed to improve the MIMO systems reliability in fading channels and to reduce transmission energy. In fact, by introducing the SSD, the proposed scheme optimizes modulation and MIMO, and can enhance the whole transmission performance. Rotation angles for the different QAM modulation signals are proposed for the MIMO scheme in [84]. So, the proposed scheme is more efficient, and promising for future wireless communication systems.

4.3 OPTIMIZATION OF THE SSD ROTATION ANGLE

The SSD is a simple combination of a component interleaver and a rotated constellation, where the rotation angle is the unique determinant parameter. Therefore, the outcome of the SSD technique depends directly on the angle α [81, 50]. An efficient choice of the rotation angle becomes an important task to achieve. Several studies were performed to improve the SSD technique. As the choice of the SSD rotation angle α depends on different factors, different solutions have been considered in the literature. In [72] the choice of α aims to maximize the product distance in order to minimize the pairwise error probability between two different transmitted sequences. Other criteria are considered in [81] like the mean Hamming distance between adjacent constellation symbols in the 2-D constellation and the incidence on the Gray mapping in the projected constellation points after rotation.

A review of the literature related to the choice of the rotation angle is presented.

4.3.1 BER-BASED ROTATION ANGLE SELECTION

Here, the main idea consists in visualizing the effect of the constellation rotation, when using non-binary LDPC codes and a fixed SNR, on the BER performance. Fig. 4.10 shows the BER as a function of various rotation angles for a 16-QAM modulation at $SNR = 12.8$ dB, for Rayleigh channel and under the DVB-T standard conditions [88]. The simulation shows that the best performance is obtained at 22.5° for Gray mapped constellation.

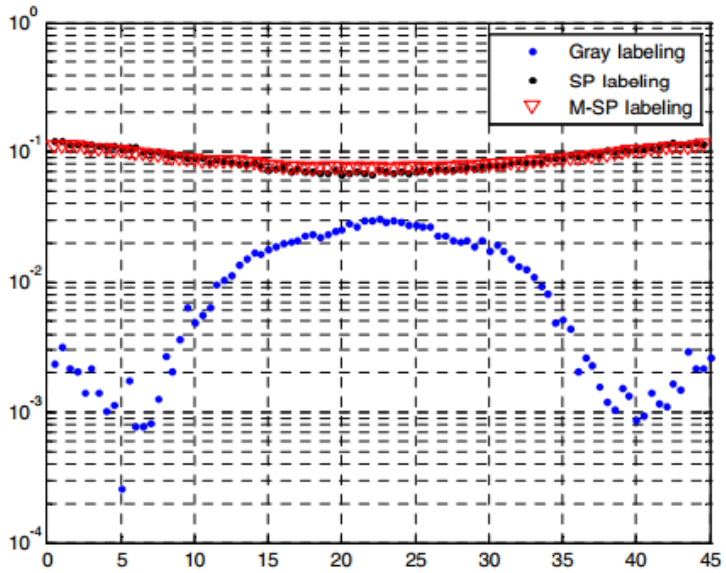

FIGURE 4.10 – BER performance of the proposed solution systems with different labeling over different rotation angles at SNR=12.8 dB, Rayleigh channel.

4.3.2 UNCODED SER UPPER BOUND APPROACH TO PERFORM THE ANGLE SELECTION

In [89], the SSD technique was combined with Alamouti coding [90]. It helped to achieve more diversity gain in fading channels. The main idea to select the best rotation angle relies on the minimization of uncoded SER. In [89], the authors derived the expression of the upper bound of the uncoded SER over Rayleigh fading channels. To perform such a computation, the authors have used the Gaussian distribution formula after the application of the Alamouti decoding. A numerical evaluation was performed for different M-QAM modulations, to compute the Upper bound of SER for different rotation angles. Such a numerical evaluation with a low computational complexity offers the possibility to test different channel conditions. Figure 4.11 shows the SER for 16-QAM combined with SSD as a function of the rotation angle for given values of SNR. For the 16-QAM modulation, by increasing the number of receive antennas, the optimal angle at which the SER is minimum is located approximately between $35°$ and $45°$.

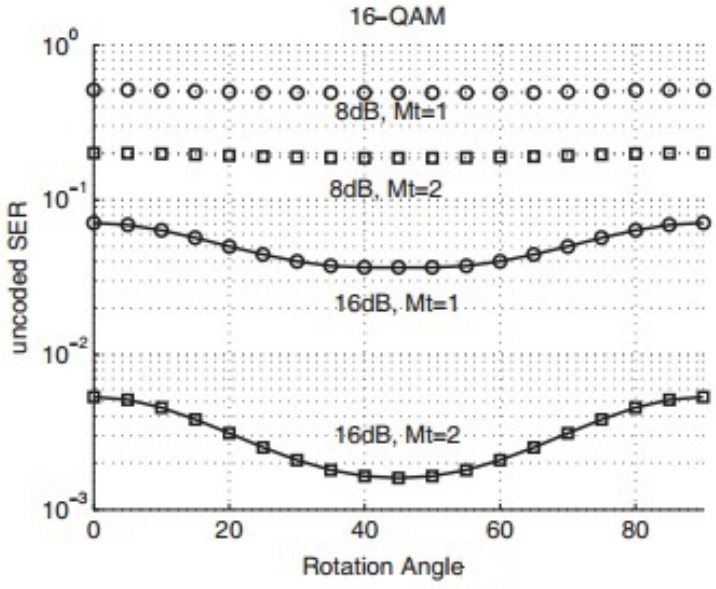

FIGURE 4.11 – SER for 16-QAM as a function of rotation angle α for different values of SNR and M_t.

4.4 SSD WITH BICM SCHEME : THE DVB-T2 STANDARD AS AN EXAMPLE OF APPLICATION

4.4.1 THE DVB-T2 STANDARD

DVB-T2 is the second Generation Digital Terrestrial Television Broadcasting standard. It is one of the best performing Digital Terrestrial Transmission systems [91]. In fact, this standard offers high efficiency and robustness for terrestrial broadcasting [75]. It includes all the parameters of the first standard DVB-T, but the overheads are significantly reduced, making the new system perform closer to the Shannon limit [75]. DVB-T2 adopted new parameters that enhance the system performance. The key point is the introduction of the SSD technique.

4.4.2 ROTATION ANGLE CHOICE PARAMETERS FOR THE DVB-T2 STANDARD

Long before the DVB-T2 standardization work, the first studies aimed to maximize the minimum product distance [72] minimizing the Pairwise error probability (PEP) between two different transmitted sequences. This criterion was derived for fading channel and QAM modulations, the best rotation angle found is $31.7°$. Unfortunately, this criterion can be

considered just for the asymptotical performance, that is for high SNR values. In practice, actual operating SNRs are not in the high SNR regions, especially when we use performing FEC coding and low rate codes are considered. Therefore, it is obvious that the product distance criterion is insufficient for the SNR region of interest in DVB-T2 and other criteria are needed to determine the optimal rotation angle [50]. Moreover, constellation signals with erasure, the distances between the constellation points have to be measured on the projection axis I or Q. Thus, a new criterion based on a one-dimensional (1-D) distance is introduced. To resume, a well-chosen angle should tries to combine the advantages of the angles designed for both fading and erasure channels. The choice of the rotation angle has to deal with the different criterion that ameliorates transmission over fading channels with and without erasure events. In order to satisfy this goal, the following design criteria have to be considered :

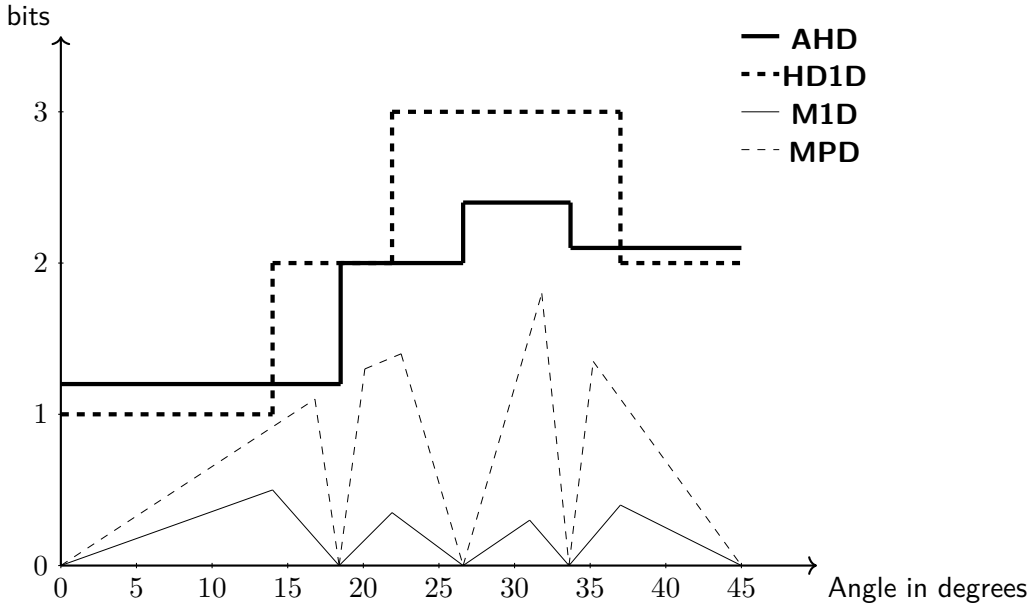

FIGURE 4.12 – DVB-T2 standard rotation angle choice parameters : 16-QAM modulation

The minimum product distance (MPD) : This 2-D distance has to be maximized in order to minimize the asymptotical BER at the output of the demapper over fading channels without erasures.

The average Hamming distance (AHD) between any two adjacent constellation symbols : This is related to the Hamming distance obtained using a certain mapping. This criterion is important especially in the presence of erasures. In fact, when one of the two components is erased, the received constellation (which is a 1-D constellation) may lose its Gray mapping. The rotation angle impacts the Hamming distance between adja-

Constellation	Rotation Angle α value (degree)
QPSK	29.0
16-QAM	16.8
64-QAM	8.6
256-QAM	3.6

TABLE 4.1 – Values of the rotation angles in the DVB-T2 standard

cent projected points varies. When the demapper is in error, the wrong symbol is chosen and respectively its projection. Since the mapping is different from a Gray mapping, the large average number of binary errors will increase.

The minimum 1-D Distance (M1D) : In order to minimize the asymptotical BER at the output of the demapper in the presence of erasures, 1-D minimum distance must be maximized.

The Hamming distance between any two adjacent constellation symbols on the projected 1-Dimension axes (HD1D) : For high SNR regions the minimum distance the 1-D dominates error events, the constellation have to be chosen to improve the BER at the output of the demapper in this region of interest.

All these criteria were considered to choose the most suitable rotation angle for the DVB-T2 standard for fading channels with and without erasures. Unfortunately, these criteria are in conflict, each one leads to different values of the angle. Thus, a compromise is inevitable. Figure 4.12 shows a graphical representation of the distance measures as a function of the rotation angle in the case of 16-QAM. The results span only up to 45° due to symmetry. In the DVB-T2 standard, [15] the angle 16.8° is selected to be a good compromise angle. The angle values adopted in the DVB-T2 standard [15] represent a compromise between the listed criteria. They are given in Table-4.1 for different modulation orders.

4.5 MUTUAL INFORMATION : METRIC FOR PERFORMANCE ENHANCEMENT

In our dissertation, we propose a MI-based optimization of the SSD technique. Theoretically, MI is known to quantify the amount of information obtained in a communication system, which represents a fundamental notion in information theory. From a practical point of view, MI was considered as a very efficient metric, and it was a good indicator to target better performance in different areas of application [92] [93]. Different studies have been performed to optimize MI of several transmission channel models, specifically in the context of wireless transmissions.

This MI is an interesting performance metric for systems that employ codes with hard decision decoding, like Reed Solomon codes [92]. MI is also relevant for soft-decoding. It gives an upper bound on the achievable rate for any decoder [94], and is particularly

relevant for symbol-based decoders as in trellis-coded modulation or LDPC-based non-binary coded schemes, as well as for systems that employ binary capacity-achieving codes like multilevel codes [95]. By properly designing non-binary codes to match the optimized constellations, or by means of binary multilevel codes, the MI of the constellation can be approached.

The design of shaped constellations that optimize the overall of the transmission system via MI maximization was rigorously addressed in [96]. MI was the key point to perform the best shaping technique. An important gain was achieved over conventional PSK and QAM constellations by properly designing constellations for different SNRs over the Gaussian channel. In [97] and [93], the problem of designing constellations that maximize the MI of a memoryless phase noise channel was addressed. The proposed method leads to a new system that outperforms the existing one that uses conventional constellations.

Current fiber optic communications systems adopted the BICM channel coding scheme. In [98] a comparison between the most used 8-dimension constellations in the optical systems was done to choose the best alternative in order to maximize performance for different spectral efficiency. The optimization procedure was based on the BICM MI metric. The results show that circular 8-QAM offers the best constellation for high coding rates.

The constellation and its labeling are jointly optimized over systems that employ BICM in [99]. Maximizing the MI of the constellation under a given power constraint enhances the performance compared to the conventional QAM and PSK constellations, showing considerable gains for the AWGN channel model [99]. In [100], the joint signal-labeling optimization scheme for constellation design that maximize the MI under the peak power constraint is done for transmission over nonlinear satellite channels.

The listed examples motivate the use of the MI metric. Then, we will consider it in our quest towards an effective determination of the parameters of the SSD technique. Since rotation angle is the only parameter that we can play with in the SSD technique, our optimization will be concentrated on the rotation angle determination.

4.6 ROTATION ANGLE OPTIMIZATION VIA MI MAXIMIZATION

In sections 3.4 and 3.3 we have developed tools for MI computation, in both CM and BICM schemes. The proposed MI-based optimization method of the SSD technique will be performed in four steps. First, we plot curves that present the MI as a function of the rotation angle for different M-QAM modulation and for a fixed SNR. This offers the possibility to detect the optimal rotation angles for a given SNR range. This operation can be applied for different channels via Monte Carlo simulation. In the context of this work, we have concentrated our work on the Rayleigh without and with erasure channels. In the second step, we determine the best rotation angle for each value for the studied SNRs. Thus, we can easily plot a curve that presents the best rotation angle as a function of the SNR. This can be done by selecting the angles that maximize the MI using the results of the curves

developed in the first step. The third step consists in presenting the advantage, in term of spectral efficiency gain, obtained by the best performing rotation angles. Such gains are plotted to highlight the additional income on MI when applying the SSD with the best rotation angles. Finally, in the fourth step, depending on the chosen rotation angle that best suites the considered SNR region, we can plot the curve of the MI as a function of the SNR. A comparison of the potential gains of decoding performance can be deduced, and a better SSD application can be expected. This process, presented in a detailed successive steps, aim to present an effective way to prove the interest of using SSD technique, and to show that its application with CM scheme has a superior performance when comparing to BICM.

4.6.1 MUTUAL INFORMATION AS A FUNCTION OF THE ROTATION ANGLE

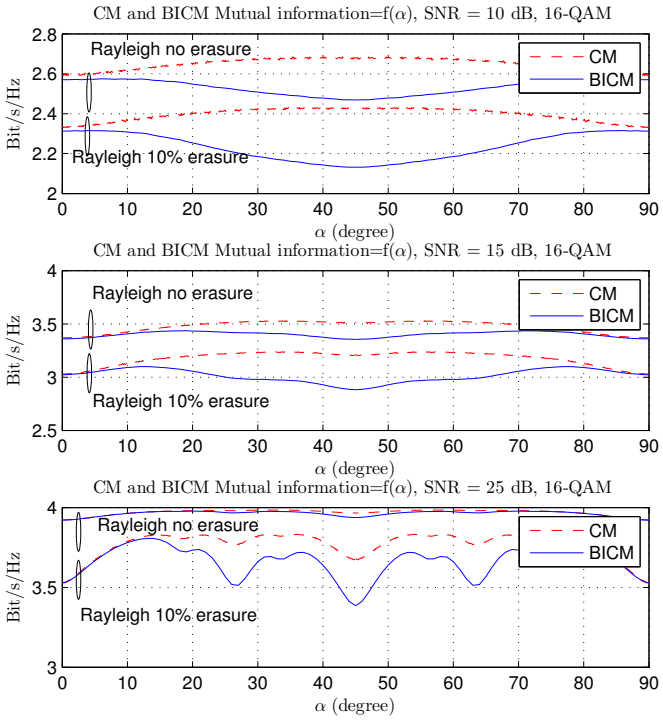

FIGURE 4.13 – Mutual information as a function of the rotation angle α for CM and BICM. $SNR = 10$, 15 and 25 dB. Rayleigh fading channel and 16-QAM modulation.

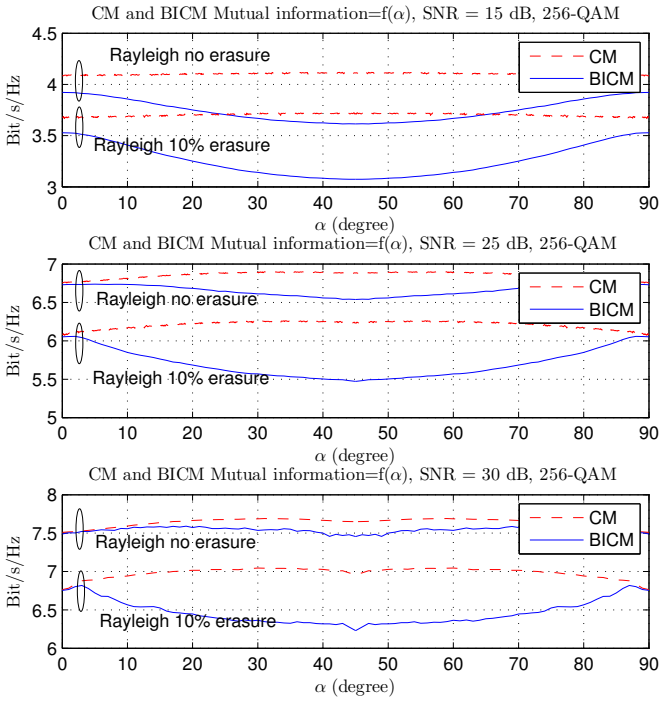

FIGURE 4.14 – Mutual information as a function of the rotation angle α for CM and BICM schemes. $SNR = 15$, 25 and 30 dB. Rayleigh fading channel and 256-QAM modulation.

Our goal is to clarify the influence of the rotation angle of the SSD technique, on the MI metric. Thus, we can simply present the MI curves as a function of the SSD rotation angle for both CM and BICM schemes (i.e the SNR value is then fixed). Fig.4.13 and Fig.4.14 show the MI curves as a function of the SSD rotation angle respectively for 16-QAM and 256-QAM modulations. Fig.4.15 and Fig.4.16 represent similar curves for the 64-QAM modulation with a focus on the erasure ratio. We define $MI^{CM}_{SNR}(\alpha)$ and $MI^{BICM}_{SNR}(\alpha)$ as the functions that return the MI value when using α as a rotation angle respectively for CM and BICM, for a fixed SNR value. These functions $MI^{CM}_{SNR}(\alpha)$ and $MI^{BICM}_{SNR}(\alpha)$ can be expressed as :

$$MI^{CM}_{SNR}(\alpha) = I_{CM}(\mathbf{X};\mathbf{Y};\alpha) \tag{4.2}$$

$$MI^{BICM}_{SNR}(\alpha) = I_{BICM}(\mathbf{X};\mathbf{Y};\alpha) \tag{4.3}$$

where $I_{CM}(\mathbf{X};\mathbf{Y};\alpha)$ and $I_{BICM}(\mathbf{X};\mathbf{Y};\alpha)$ are the MI values of a channel scheme that

apply the SSD with a rotation angle equal to α, respectively for CM and BICM schemes. We can derive their expression from the MI expression $I(\mathbf{X};\mathbf{Y})$ developed in section 3.3.3.3 for the CM scheme, and in section 3.4.2 for the BICM scheme. The only change we have to make in the MI computation is in the equation (Eq. 3.27) where $P(y|x_l)$ can be expressed as :

$$P(y|x_l) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y_I^r - r_I x_I^r)^2 + (y_Q^r - r_Q x_Q^r)^2}{2\sigma^2}}. \tag{4.4}$$

with (x_I^r, x_Q^r) the coordinates of the transmitted constellation point after the rotation applied on the point with (x_I, x_Q) as coordinates. The coordinates (y_I^r, y_Q^r) are the image of (y_I, y_Q) knowing the rotation angle and the fading events r_I and r_Q applied respectively on the I and Q components. We can derive their expression as follows :

$$\begin{pmatrix} x_I^r \\ x_Q^r \end{pmatrix} = \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix} \begin{pmatrix} x_I \\ x_Q \end{pmatrix} \tag{4.5}$$

$$\begin{pmatrix} y_I^r \\ y_Q^r \end{pmatrix} = \begin{pmatrix} r_I & r_Q \end{pmatrix} \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix} \begin{pmatrix} y_I \\ y_Q \end{pmatrix} \tag{4.6}$$

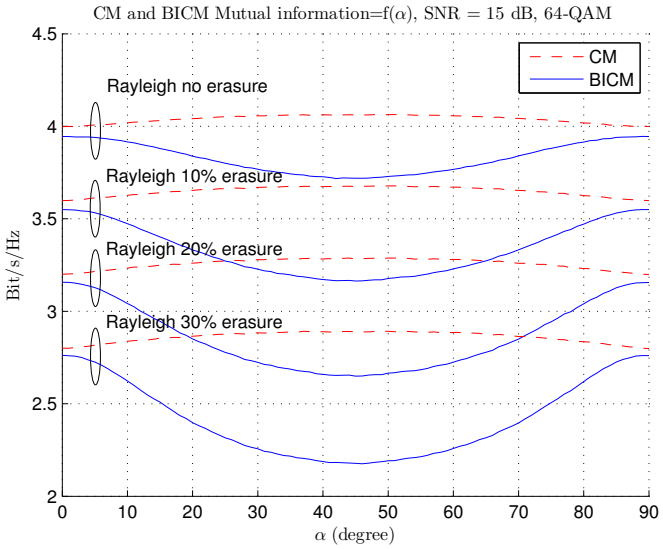

FIGURE 4.15 – Mutual information as a function of the rotation angle α for CM and BICM. Rayleigh channel and Rayleigh channel with erasure ($P_e \in \{0.1, 0.2, 0.3\}$). $SNR = 15$ dB and 64-QAM modulation.

Fig. 4.13 considers a 16-QAM with SNR values of 10, 15 and 25 dB. Fig. 4.14 considers a 256-QAM with the same values of SNR. Both figures show results for the Rayleigh

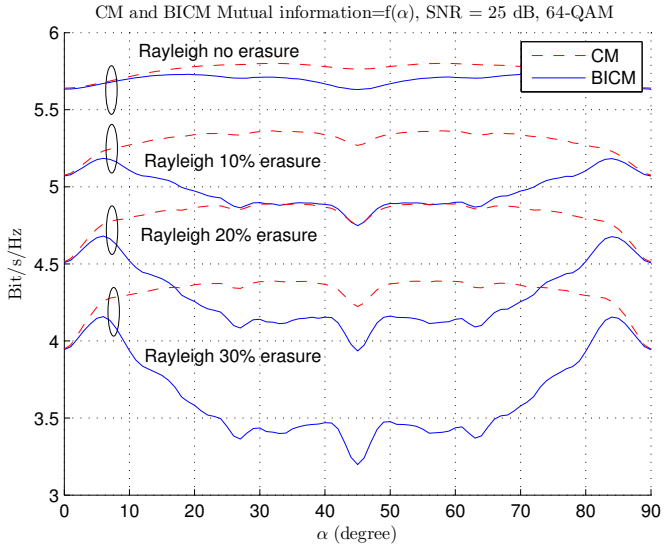

FIGURE 4.16 – Mutual information as a function of the rotation angle α for CM and BICM. Rayleigh channel and Rayleigh channel with erasure ($P_e \in \{0.1, 0.2, 0.3\}$). $SNR = 25$ dB and 64-QAM modulation.

fading channel with erasures ($P_e = 0.1$) and without erasure. In order to perform performance comparison between the CM and BCIM schemes, we present the MI curves of both schemes in one figure to make the comparison clearer. Note that, for the BICM scheme, the Gray mapping of DVB-T2 [15] is used. Gray mapping maximizes performance over the BICM scheme if no iterative decoding is used. Therefore, the comparison with the CM scheme is fair.

From these curves we can derive several conclusions. First, the rotation angle α that maximizes the MI depends on the used SNR, for both CM and BICM schemes. Second, rotation always provides gain for the CM scheme while for the BICM rate loss may appear for the same rotation angle. Third, for all rotation angles, the CM scheme presents higher MI than the BICM. The CM curve is always above the BICM one. We can deduce the following properties :

1. $\forall \alpha, MI^{CM}_{SNR}(\alpha) \geq MI^{CM}_{SNR}(0)$
2. $\exists \alpha, MI^{BICM}_{SNR}(\alpha) < MI^{BICM}_{SNR}(0)$
3. $\forall \alpha, MI^{CM}_{SNR}(\alpha) \geq MI^{BICM}_{SNR}(\alpha)$

These properties show that the SSD technique is always beneficial for the CM modulation scheme. In addition, CM outperforms BICM for almost all spectral efficiencies. We can notice also that for fixed channel conditions, the rotation angle that maximizes the MI varies

with the SNR (See Fig. 4.13). An analysis of the dependence between MI and SNR is then required.

To clarify the impact of the erasure factor on the MI when varying the rotation angle, we plot Fig. 4.15 and Fig. 4.16. They present a 64-QAM modulation, with SNR value of 15 and 25 dB, respectively. We present the impact of the SSD technique on Rayleigh channel with erasure when using different values of P_e. For these two figures we show curves of MI as a function of the rotation angle α for CM and BICM schemes, for Rayleigh fading channel with erasures ($P_e = 0.1$, $P_e = 0.2$, $P_e = 0.3$) and without erasure. CM and BICM schemes are considered. Then, a comparison between CM and BICM schemes can also be performed.

From curves in Fig. 4.15 and Fig. 4.16, we can observe that the increase in MI is higher in the Rayleigh with erasure channel. MI gain increases with P_e. Thus, the SSD can potentially provide more gain in the erasure channel. This conclusion is explained by the increase of diversity when we apply the SSD technique. If one of the two components vanishes the second one can provide information about the received signal. In other terms, each one of the two components encompasses information about the initial two components before the rotation, which make it possible to recover the whole information in the receiver part. We compare the CM and BICM and observe that when P_e increases, CM benefits more from the SSD technique. In fact the increase of spectral efficiency is more significant when comparing to the BICM scheme. We can deduce the following properties :

1. $P_e \nearrow \Rightarrow MI^{CM}_{SNR}(\alpha) - MI^{CM}_{SNR}(0) \nearrow$
2. $\forall P_e, \forall \alpha, MI^{CM}_{SNR}(\alpha) \geq MI^{BICM}_{SNR}(\alpha)$

An analysis of the MI value as a function of the rotation angle is performed, the next step aim to evaluate the dependence between the SNR and the best rotation angle that the SSD offers.

4.6.2 BEST ROTATION ANGLE AS A FUNCTION OF THE SNR

Our optimization approach rationalizes the one proposed in [81], which implies a complex trade-off with several contradictory criteria. In our case, the MI is the only criterion to choose the rotation angle. Selecting the most performing rotation angle via MI maximization enhance the system performance with the SSD technique. We have shown in the previous section that for a fixed channel conditions, the best rotation angles varies with the SNR. Thus, we try to find out a relation between the SSD best rotation angle and the channel SNR values. For example, from the curves presented in Fig.4.13 and Fig.4.14, we can easily select the rotation angles that maximizes the MI for all tested SNRs belonging to the sets $\{10, 15, 25\}$ and $\{15, 25, 30\}$, respectively. We can generalize the procedure for other SNR values, thus, for each SNR, the optimal rotation angle $\alpha^{CM}_{opt}(SNR)$ for the CM scheme and $\alpha^{BICM}_{opt}(SNR)$ for the BICM scheme can be expressed as follows :

$$\alpha^{CM}_{opt}(SNR) = \underset{\alpha \in [0-90]}{\operatorname{argmax}} \{MI^{CM}_{SNR}(\alpha)\}. \tag{4.7}$$

$$\alpha_{opt}^{BICM}(SNR) = \underset{\alpha\in[0-90]}{\operatorname{argmax}}\{MI_{SNR}^{BICM}(\alpha)\}. \tag{4.8}$$

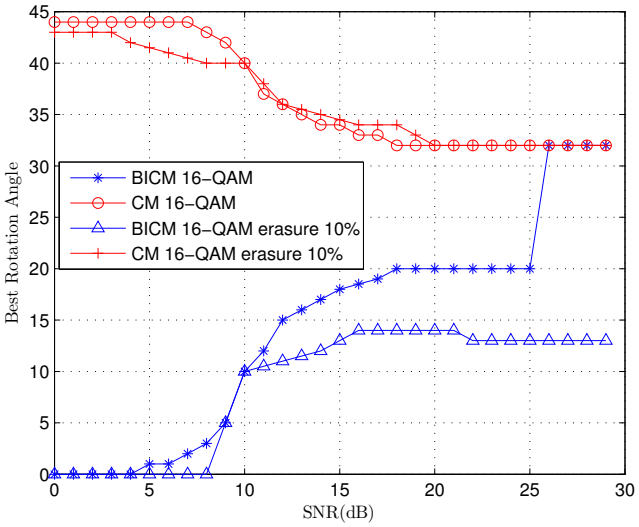

FIGURE 4.17 – Rotation angle that maximizes mutual information, as a function of the SNR, for the Rayleigh channel and Rayleigh channel with 10% erasures. 16-QAM modulation.

We can evaluate the result of equations Eq. 4.7 and Eq. 4.8 via Monte Carlo simulations for SNR values varying from 0 to 30 dB with a step of 1 dB. For each SNR, we determine $\alpha_{opt}^{CM}(SNR)$ and $\alpha_{opt}^{BICM}(SNR)$ values. The resulting plot that present the angles maximizing the MI for each SNR value for 16-QAM and 256-QAM modulations is given in Fig. 4.17 and Fig. 4.18 under Rayleigh without and with erasure ($P_e = 0.1$) channels, respectively.

As in [50], for the BICM scheme with a 16-QAM modulation, the optimal angle value for high SNRs (i.e. greater than 25 dB) is $\alpha_{opt}^{BICM} \approx 31.7°$. However for practical operating SNR values (between 18 dB and 25 dB), $\alpha_{opt}^{BICM} \approx 20°$. If this angle value is considered for lower SNRs, a rate loss of about 0.03 bit/s/Hz would be introduced at SNR = 10 dB with respect to the optimal angle $\alpha_{opt}^{BICM}(10\text{dB}) \approx 10°$ (Fig. 4.13). For CM, the optimal angle value for high SNRs is also $\alpha_{opt}^{CM} = 31.7°$. However, considering this angle also for lower SNRs barely affects performance (unlike for BICM) : at 10 dB, using $\alpha_{opt}^{CM} = 31.7°$ instead of the optimal angle $\alpha_{opt}^{CM}(10dB) = 40°$ introduces only a rate loss of 0.004 bit/s/Hz for the 16-QAM (Fig. 4.13) and 0.003 bit/s/Hz for the 256-QAM (Fig. 4.14). In other words, the choice of the same rotation angle for all SNRs, introduces negligible rate loss for the CM scheme and a some tenths of bit/s/Hz rate loss for BICM. This fact was already observed

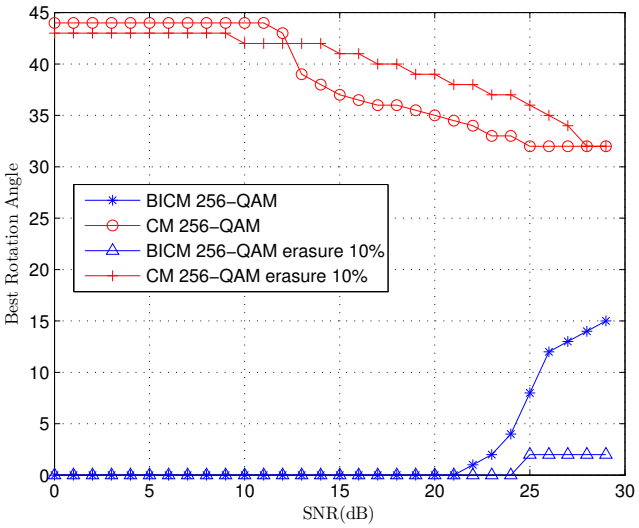

FIGURE 4.18 – Rotation angle that maximizes mutual information, as a function of the SNR, for the Rayleigh channel and Rayleigh channel with 10% erasures. 256-QAM modulation.

in Fig. 4.13 and Fig. 4.14, where the MI in the CM scheme is much less sensitive (about a factor of 10) to the angle variation than in BICM.

In order to clear up the effect of the choice of the SSD rotation angle on CM and BICM schemes for a fixed SNR, we present MI variations between rotation angles $0°$ and α_{opt} in tables Tab. 4.2 and Tab. 4.3 for 16-QAM and 256-QAM modulations. We consider an SNR value of 10 dB for the 16-QAM modulation and 25 dB for the 256-QAM modulation, respectively. From the two tables we compare the gap Δ between MI_0 ($\alpha = 0°$) and MI_{opt} ($\alpha = \alpha_{opt}$). The results show an advantage for CM of 0.06 dB in Tab. 4.2 and of 0.12 dB in Tab. 4.3. That confirms the superiority of the MI performance that brings SSD to CM, comparing to their binary counterparts BICM.

	MI_0	α_{opt}	MI_{opt}	Δ
CM	2.60	40°	2.68	0.08
BICM	2.58	10°	2.60	0.02
Δ	0.02		0.08	0.06

TABLE 4.2 – Mutual information for CM and BICM. $SNR = 10$ dB. Rayleigh fading channel and 16-QAM.

In Fig. 4.19, the angles that maximize the MI for each SNR value ($SNR \in [0 \ldots 30]$ dB), are presented with different erasure factors for the 64-QAM modulation. We aim to find out

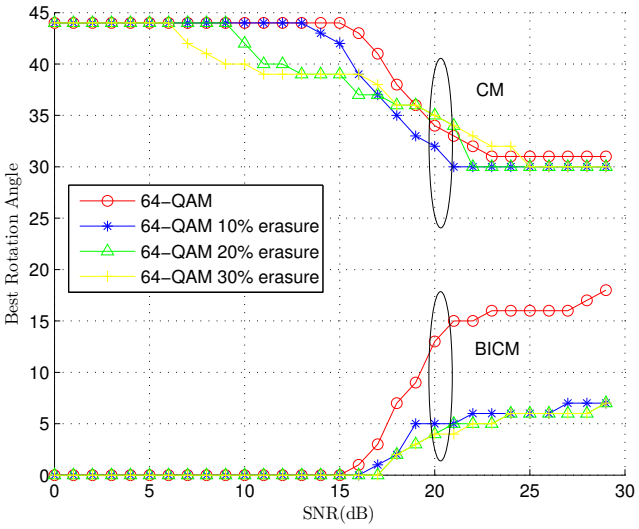

FIGURE 4.19 – Rotation angle that maximizes mutual information, as a function of the SNR, for the Rayleigh channel and Rayleigh channel with 10%, 20% and 30% erasures. 64-QAM modulation.

	MI_0	α_{opt}	MI_{opt}	Δ
CM	6.75	31°	6.88	0.13
BICM	6.75	8°	6.76	0.01
Δ	0		0.12	0.12

TABLE 4.3 – Mutual information for CM and BICM in bit/s/Hz. $SNR = 25$ dB. Rayleigh fading channel and 256-QAM.

the effect of the SSD technique depending of the erasure probability value. Here we show curves for Rayleigh channel and Rayleigh channel with an erasure probability P_e, with $P_e \in \{0.1, 0.2, 0.3\}$. From Fig. 4.19, we can see that the best rotation angles for CM barely varies when P_e increases. α_{opt}^{CM} remains almost constant for Rayleigh channel with and without erasure, while for BICM the value of α_{opt}^{BICM} differs when using different erasure factors (see Fig. 4.19) in the transmission channel. The same conclusion can be derived with reference to Fig. 4.17 and Fig. 4.18.

From a practical point of view, for the broadcasting applications where each receiver experiments a different level of SNR and erasure, the choice of the rotation angle is always a trade-off for BICM. This is not the case with the CM scheme, where the rotation angle offers good performance for different channel properties. This fact confirms that SSD fits better with the CM scheme, in terms of performance and rotation angle choice flexibility.

As a summary, in this section we derived the best rotation angle for SSD and different channel parameters. We performed a performance analysis, and a comparative procedure between CM and BICM schemes. Next section discusses with more details the gain obtained with SSD.

4.6.3 MUTUAL INFORMATION GAIN PROVIDED BY THE BEST ROTATION ANGLES

The SSD technique is applied to enhance the spectral efficiency of the transmission channel. After presenting the best rotation angle as a function of the SNR, here we will evaluate the MI gain they offer as a function of the SNR, for different M-QAM modulations, M $\in \{16, 64, 256\}$. This expression can be deduced for both CM ($MI^{CM}_{gain}(SNR)$) and BICM schemes ($MI^{BICM}_{gain}(SNR)$) as follows :

$$MI^{CM}_{gain}(SNR) = MI^{CM}_{SNR}(\alpha_{opt}) - MI^{CM}_{SNR}(0) \tag{4.9}$$

$$MI^{BICM}_{gain}(SNR) = MI^{BICM}_{SNR}(\alpha_{opt}) - MI^{BICM}_{SNR}(0) \tag{4.10}$$

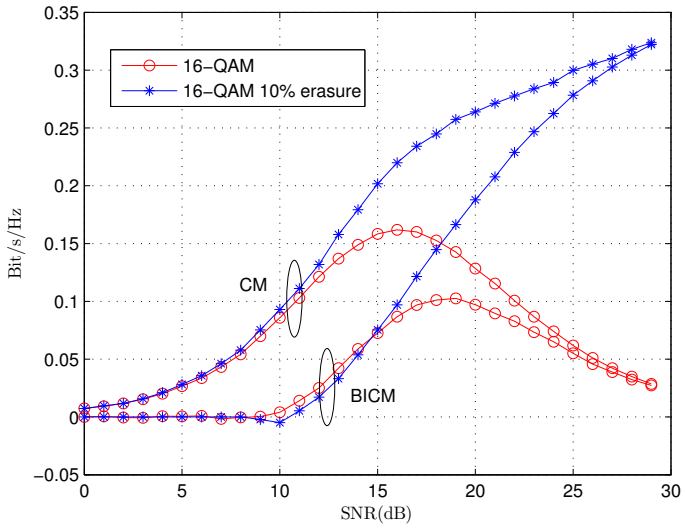

FIGURE 4.20 – Maximum MI gain with SSD, as a function of the SNR, for the Rayleigh channel and Rayleigh channel with 10% erasures. 16-QAM modulation.

Fig. 4.20 and Fig. 4.21 plot the rate gain with SSD when using the optimal rotation angles α^{CM}_{opt} and α^{BICM}_{opt}, with 16-QAM and 256-QAM modulations, respectively. They can be easily deduced from the curves presented in Fig. 4.17 and Fig. 4.18, using the equations

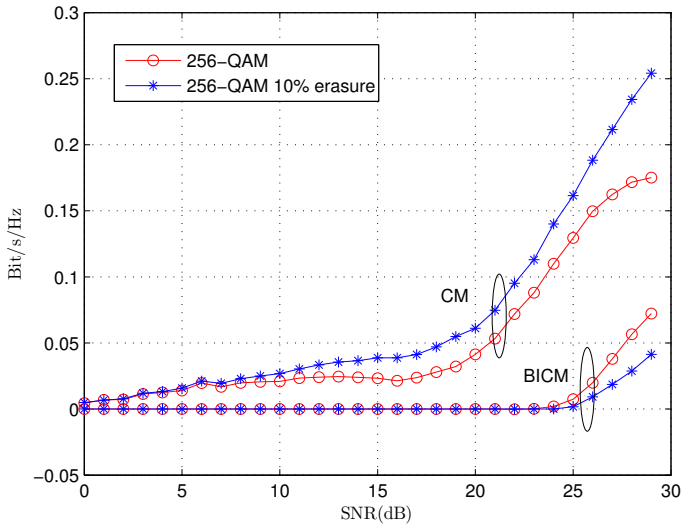

FIGURE 4.21 – Maximum MI gain with SSD, as a function of the SNR, for the Rayleigh channel and Rayleigh channel with 10% erasures. 256-QAM modulation.

Eq. 4.9 and Eq. 4.10, respectively. These are results developed for the Rayleigh fading channel with erasures ($P_e = 0.1$) and without erasures.

From these curves we can draw several conclusions. First, the gain that SSD offers to CM is always greater than that of BICM. Second, for certain SNR values MI^{CM}_{gain} has 0.1 more rate that MI^{BICM}_{gain} (e.g. for $SNR \in [10 \dots 15]$, with 16-QAM and Rayleigh channel and Rayleigh channel with erasure $P_e = 0.1$). Third, the gain converge to a strictly positive value with Rayleigh with erasure channel. We can deduce the following properties for the Rayleigh channel :

1. $\forall SNR, MI^{CM}_{gain}(SNR) \geq MI^{BICM}_{gain}(SNR)$
2. $\forall SNR \in [10 \dots 15], MI^{CM}_{gain}(SNR) - MI^{BICM}_{gain}(SNR) \approx 0.1$ with 16-QAM
3. $SNR \to \infty, MI^{CM}_{gain}(SNR) \to 0$
4. $SNR \to \infty, MI^{BICM}_{gain}(SNR) \to 0$

For Rayleigh channel with a non-zero P_e erasure probability we can conclude in addition the following properties for any M-QAM modulation :

1. $SNR \to \infty, MI^{CM}_{gain}(SNR) \to log_2(M) * (P_e - P_e^2)$
2. $SNR \to \infty, MI^{BICM}_{gain}(SNR) \to log_2(M) * (P_e - P_e^2)$

The last two properties can be demonstrated as follows : when considering a transmission with erasure probability P_e without SSD application, P_e of the transmitted information

will be lost through the considered transmission system. But, when using SSD, the probability that the whole information is lost (I and Q are erased), will be equal to P_e^2. Thus when using and M-QAM modulation the maximum MI increases by $log_2(M) * (P_e - P_e^2)$, for both CM and BICM schemes.

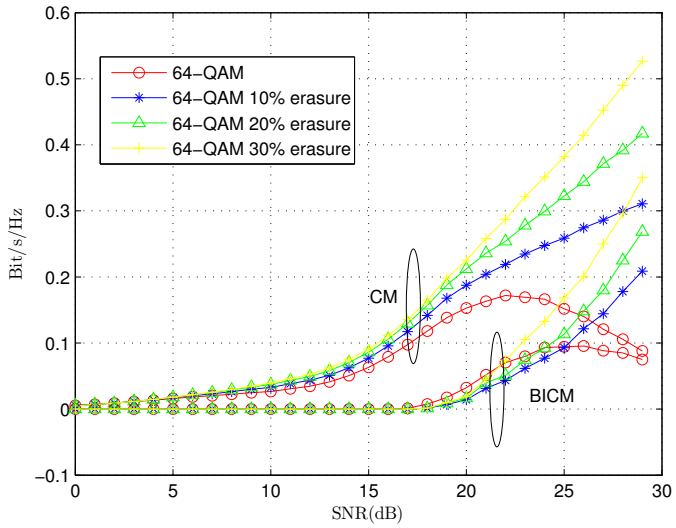

FIGURE 4.22 – Maximum MI gain with SSD, as a function of the SNR, for the Rayleigh channel and Rayleigh channel with 10%, 20% and 30%, erasures. 256-QAM modulation.

In Fig. 4.22, we present the MI gain of the SSD when using optimal rotation angles α_{opt}^{CM} and α_{opt}^{BICM} for the 64-QAM modulation (See Fig. 4.19). The results are presented over Rayleigh channel and Rayleigh channel with erasure, for different P_e values, $P_e \in [0.1, 0.2, 0.3]$, and SNRs $\in [0 \dots 30]$ dB. From (Fig. 4.22), we can notice that the gain of spectral efficiency increases with P_e. For $SNR = 25$ dB, $MI_{gain}^{CM} = 0.25$ for $P_e = 0.1$, while $MI_{gain}^{CM} = 0.38$ for $P_e = 0.3$, . Unlike BICM, CM takes always advantage of SSD and offers positive MI gain for practical SNRs, $SNR \in [10 \dots 20]$ for all different erasure probabilities P_e. In the next section, as a complement to this analysis, we analyze the curves representing the MI as a function of the SNR.

4.6.4 MUTUAL INFORMATION AS A FUNCTION OF THE SNR

Let us now consider the curves that present the relation between MI and SNR for the CM and BICM schemes. In fact, to get such curves we have to choose at the beginning a fixed rotation angle. We will consider the most appropriate rotation angle for the CM scheme which is $\alpha_o = 31.7$, this angle choice is a good compromise for high and low SNRs. For the

BICM scheme, the angle values will be those adopted in the DVB-T2 standard [15] reported in Tab. 4.1.

Using the MI equation developed in section 3.3.3.3, and by considering the equation developed in section 4.6.1, we plotted curves in Fig 4.23. We have considered the 16-QAM with rotation angles $\alpha_o = 31.7$ for CM and $\alpha_o = 16.8$ for BICM. The MI curves are presented for the Rayleigh channel with no erasure and with erasure ($P_e = 0.1$).

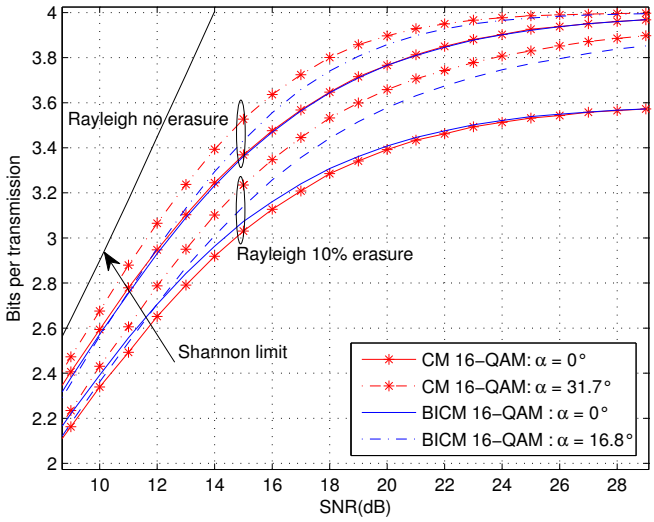

FIGURE 4.23 – CM and BICM mutual information curves for a 16-QAM modulation over fast flat fading Rayleigh channel (without erasures and with 10% erasures)

The same curves are presented for the 256-QAM modulation in Fig. 4.24. The chosen rotation angles are $\alpha_o = 31.7$ for the CM and $\alpha = 3.6$ for the BICM (see Tab. 4.1). With the BICM scheme, the SSD barely changes the MI performance and does not offer any significant advantage. However, for the CM scheme, a SNR gain greater than 1 dB can be observed for spectral efficiencies larger than 7 bit/Hz/s.

From these curves again, we observe that the CM with SSD outperforms the non-rotated scheme for all SNRs. This does not occur for BICM : at low SNR (up to approximately 12 dB for the 16-QAM), the rotation causes a MI loss compared to non-rotated BICM. This can also be observed in Figures 4.13 and 4.14, where the MI curve decreases with rotation. Therefore, the gains displayed by the rotated CM are more significant than for BICM. Over the erasure Rayleigh channel ($p_e = 0.1$), the gain introduced with the SSD is more significant than the one for the no-erasure case, for both 16- and 256-QAM and especially for high SNR values.

These theoretical studies are performed in order to optimize MI with SSD technique. We proposed MI as a parameterto optimize the SSD technique application. To validate the

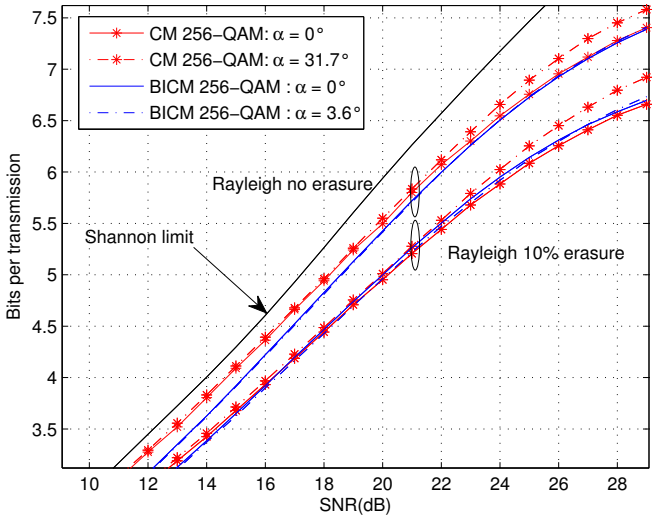

FIGURE 4.24 – CM and BICM mutual information curves for a 256-QAM modulation over fast flat fading Rayleigh channel (without erasures and with 10% erasures)

previous analysis and to show its impact, we have carried out error rate simulations. The corresponding simulation results are presented in the next section.

4.7 SIMULATION RESULTS AND PERFORMANCE COMPARISON

To verify the theoretical results, we ran Monte-Carlo simulations for the different scenarios discussed in the previous sections. Our simulation results are shown in Fig. 4.25 and Fig. 4.26. We have simulated for the 256-QAM modulation and two coding rates, $\frac{3}{4}$ and $\frac{9}{10}$.

The considered BICM scheme is the one of the DVB-T2 standard, i.e., rotation angle of $3.6°$, a specific interleaver pattern and an $N = 64800$ binary irregular LDPC code. For the CM, two specific Non-Binary LDPC codes were designed for rates 3/4 and 9/10. The length of these codes is 64800 bits or 8100 symbols defined over GF(256). These NB-LDPC codes are available at [101]. The decoding algorithm of the NB-LDPC codes is the Extended Min-Sum (EMS) algorithm [26]. For the BICM, the LDPC decoder implements the Sum-Product algorithm followed by a BCH decoder as in [15]. We have used a maximum number of iterations equal to 50, same frame length and same channel conditions for both cases. Each point of the simulation curves represents the transmission of data until 100 erroneous frames have been encountered. For the EMS decoding, we have performed simulations with $n_m = 50$, i.e. length of the exchanged messages between check and variable nodes [26].

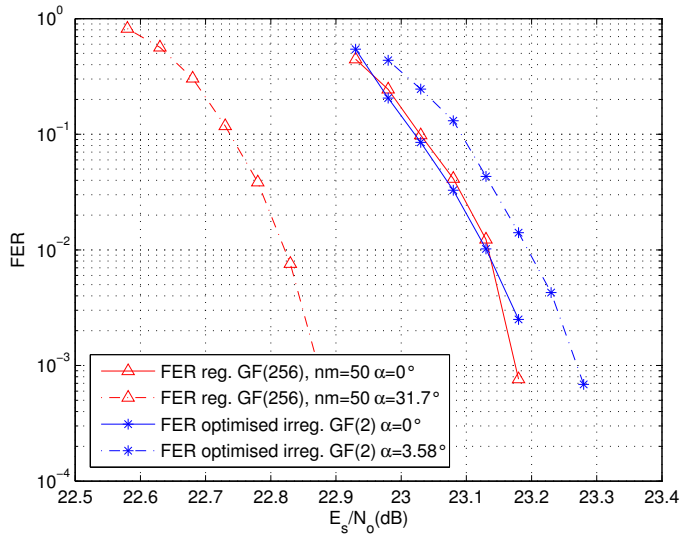

FIGURE 4.25 – FER simulation for 3/4-rate BICM-GF(2) and CM-GF(256) schemes over the fast flat Rayleigh fading channel, with and without Rotated Constellation

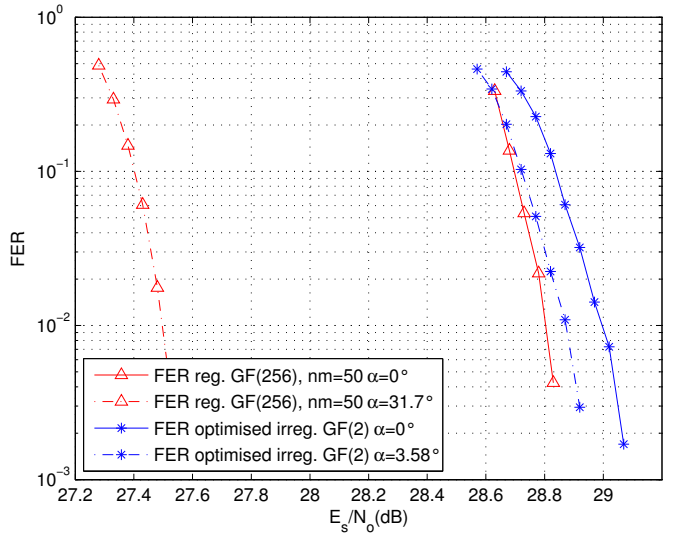

FIGURE 4.26 – FER simulation for 9/10-rate BICM-GF(2) and CM-GF(256) schemes over the fast flat Rayleigh fading channel, with and without Rotated Constellation

Fig. 4.25 presents results for a code rate of 3/4. As already observed in Fig. 4.14, the SSD technique introduces performance loss in the BICM scheme for spectral efficiencies

lower than 7 bit/Hz/s. However, as announced by the theoretical study, a gain of about 0.3 dB is provided by the SSD technique for CM. For higher spectral efficiencies (9/10-rate in Fig. 4.26), SSD introduces gain for both the BICM and CM schemes (see the right upper zone of Fig. 4.24). This gain is more significant with the CM scheme (1.3 dB at FER = 10^{-2} compared to about 0.15 dB for BICM). Note that these performance results are consistent with the analysis of Fig. 4.14.

4.8 CONCLUSION

This chapter investigates the application of the SSD technique to high spectral efficiency communications in the context of next generation broadcasting systems. The issues of combining SSD with CM and BICM schemes is considered under Rayleigh channels with and without erasures. At the beginning, we have described the principle of the SSD technique, and introduced some of its state-of-the-art optimizations. Then, we proposed a new criterion to determine the optimal rotation angle for the SSD technique based on the MI metric. The rotation angle is the one that maximizes the MI for practical SNR values. For both CM and BICM schemes, with Gray labeled square M-QAM modulations, M $\in \{16, 64, 256\}$, several interesting properties are obtained, based on which the optimization work is presented. We have found that absolute optimal rotation angle does not exist, and that its value varies with the SNR. For the CM scheme, we can conclude that a constellation rotation has always a positive effect on the MI metric, which is not the case for BICM scheme where MI degradation can be seen for some SNR or α values. An evaluation of the best rotation angle was then performed, and a study the obtained gain is detailed to facilitate our analysis of the SSD technique. We showed that non-binary CM are more robust than BICM and take better advantage of the SSD technique. Severe fading and erasure events in the transmission channels can be mitigated by applying the SSD technique to CM and BICM schemes. This allows for optimized performance in fading channels with and without erasure. The solutions that we proposed can lead to significant performance gains for next generation broadcasting systems. Simulation results presented performance gain that reaches 1.3 dB for CM scheme compared to BICM systems with DVB-T2 LDPC codes, with a code rate of $\frac{1}{3}$ and a BER of 10^5.

Chapitre 5

Joint modulation and coding optimization with NB-LDPC codes

The joint optimization of binary error code and binary mapping of the constellation points is an efficient method to improve the overall performance of a communication system. For example in the eighties, Ungerboeck proposed in [102] the trellis coded modulation, while since the early 2000s, the problem of optimizing the BICM scheme for LDPC codes [103] studied the dependence between the binary LDPC code matrix and the different levels of error protection provided bits in one symbol. To the best of our knowlege, nothing so far has been done about joint optimization of non-binary code and mapping on constellation points.

This chapter constitute a first attempts to construct an efficient CM scheme in the context of high spectral efficiency transmission. In this context, we propose to perform a joint optimization of both channel coding and modulation, when using the CM scheme. In fact, the dependence between the code symbols and the constellation points leads to rethink about their relation and its impact on the decoding results. Intuitively, we can say that the joint optimization of channel coding and modulation can bring additional improvement on the decoding performance. Here we will focus on a case of application involving the association of NB-LDPC codes over GF(q) with the QAM modulations of the same cardinality q, (e.g. GF(64) and 64-QAM modulation). We will restrict our optimization method to the joint labeling of the constellation point, with the choice of the coefficients of one parity-check equation. In other words, we will generalize the method proposed by Poulliat et al. [25] that uses the minimum Hamming distance and the multiplicity of a binary code associated to one parity-check equation coefficients. The former method is efficient for BPSK modulation where the Hamming distance is proportional to the Euclidean one. This is not the case for the QAM modulation, thus the Euclidiean distance has to be reconsidered in the CM scheme design criteria.

In Section 5.1, we will review the construction of a non-binary PCM. We will present the key steps to build a NB-LDPC PCM. In general, NB-LDPC PCM construction is realized in two distinct steps : non-null positions selection and the coefficients choice. In Section

5.2 we will introduce our motivation behind the proposed method. A study of the Euclidean distance and a comparison with the Hamming distance over CM will be presented respectively in Section. 5.3 and Section. 5.4. Then, a distance spectrum evaluation for NB codes will presented in 5.5. The incidence of Gray mapping choice on Euclidean distance and distance spectrum will be studied in Section. 5.6. In Section 5.7 the joint optimization of mapping and NB-LDPC matrix coefficient will be explained. We will present the choice of coefficient and modulation mapping that optimizes the NB-LDPC codes with high order modulations decoding performance. Finally simulation results will be presented in Section. 5.8

5.1 NB-LDPC CODES CONSTRUCTION

The coding theory domain is mainly characterized by the development of powerful binary error-correcting codes that can be iteratively decoded. Gallager proposed the LDPC codes with arbitrary alphabet size [13]. Since their rediscovery in [1], LDPC codes are one of the most performing coding techniques for error control in communication and data storage systems. They offer capacity-approaching performance [104] and practically implementable decoding algorithms. Several research efforts focused on how to design, analysis, and decode of these LDPC codes. However, the research efforts devoted to NB-LDPC codes are far less than those already achieved to their binary counterpart. This lack of enthusiasm in NB-LDPC codes is due to their decoding complexity which makes them difficult to be implemented on hardware. Based on the experimental results presented by Davey and MacKay in [22] on LDPC codes built on finite Galois fields, recent works focused on the analysis and design of NB-LDPC codes on both binary, e.g. BPSK modulation, and non-binary channels, e.g. M-QAM modulation.

There exist several propositions of NB-LDPC construction in the literature. Constructions of NB-LDPC codes have been proposed through the design of the PCM with prescribed properties. The design aim to satisfy various criteria like the near-capacity performance, and efficient encoding and decoding. But, the PCM construction was always dealing with contradictory parameters. The PCM with high column weight offers a better evaluation of the circulating messages between nodes, while, lower row weights of H decreases the computation complexity in check-node processing. This trade-off was an important issue for PCM construction. It was proven in [34, 25] that when q becomes large ($q >> 2$), the best performances are obtained for ultra sparse NB-LDPC codes, which are NB-DPC codes with the minimum connectivity on the variable nodes $d_v = 2$.

Several methods have been developed to assess the asymptotic performance of NB-LDPC codes. Bennatan and Burshtein studied error correcting performance of NB-LDPC codes by applying the ML decoding and the BP algorithm [105] and by including the development of extrinsic information transfer charts for arbitrary channels [106]. Analysis via the Gaussian approximation was discussed in [107]. The study of the density evolution of NB-LDPC codes was performed for the erasure channel in [108].

The construction of the PCM of NB-LDPC codes can be performed in two steps that are generally solved in a sequential manner. First, the positions of the non-null entries of the PCM are optimized in order to improve the error floor region [71]. The main idea is to have good girth properties to minimize the impact of cycles when using the BP algorithm on the associated Tanner graph. This can be efficiently achieved using algorithms like the progressive edge growth (PEG) algorithm [109], or using Quasi-cyclic matrix as in [110], where efficiently encodable quasi-cyclic NB-LDPC (QC-NB-LDPC) codes were proposed. In the second step, the PCM non-null entries must be carefully chosen to optimize the rows of the PCM, and then, the whole PCM structure properties to lower the waterfall. They can be selected either randomly from a uniform distribution among non-null elements of GF(q) [109] or carefully to meet some design criteria, as done in [25]. In [111] the proposed method for NB-LDPC code construction is based on the selection on nearly optimum non-null entries in the PCM for codes of column weight d_v equal to 2. Once non-null coefficients are chosen to optimize one row in the PCM, they have to be meticulously positioned in the whole PCM to guarantee good cycle properties in the PCM [25] in order to improve the waterfall region and to lower the error floor. Another construction method was proposed in [9] that consist on designing regular NB-LDPC codes over GF(q) via their binary image. Thus, both non-null positions and non-null entries will be determined simultaneously. Poulliat et al. proved in [9] that good waterfall and error floor properties can be obtained.

5.1.1 NON-NULL POSITIONS CHOICE IN THE PCM

The first step of a NB-LDPC construction consists in selecting of the non-null positions entries on the PCM. They must be meticulously chosen because they lead to the structure of the Tanner graph and its topological properties, such as the number of cycles in the Tanner graph associated with the code. It was shown in [25] that short cycles in the Tanner graph result in non-codeword errors. The fundamental issue when we select the non-null positions is the presence of cycles that affects negatively the NB-LDPC codes performance. In other words, when using an iterative decoding algorithm with a message passing type algorithm, cycles lead to self-confirmation of exchanged messages. Short cycles may lead to have certain non-codewords that compete with the transmitted codeword to be the output of the decoder, which degrade the decoder performance. As cycles impact the decoding error performance, the positions of the non-null entries of the parity-check matrix need to be carefully chosen to maximize the minimum size of a cycle in the graph i.e. the girth of the code, and to minimize the multiplicity of cycles of minimum sizes of cycles. The goal is to have a small number of short cycles.

In practice, it is not affordable to avoid cycles in the Tanner graph, but it is possible to construct the PCM with girths as large as possible, so that the correlation of messages can be minimized. To fulfill such an objective, we can find several construction techniques in the literature that claim different advantages. Based on the methods of construction, LDPC codes can be classified into two main categories, random or random-like codes and

structured codes. Among these non-null positions selection techniques, we can recall some of the most used algorithms :

Quasi-cyclic NB-LDPC construction : NB-LDPC can be efficiently constructed using a Quasi-Cyclic structure on the parity-check matrix. The resulting codes are the so-called Quasi Cyclic NB-LDPC (QC-NB-LDPC) codes, considered as an extension of the Protograph LDPC codes [112]. QC-NB-LDPC codes [113] are defined by an $m \times n$ incidence matrix, known as a protomatrix, with non-negative integer entries a_{ij} that correspond to a_{ij} parallel edges in the graph. An $rm \times rn$ matrix is obtained by replacing each non-null entry a_{ij} by an a_{ij}-shift applied on the identity matrix (circulant matrix) of size r and the zero entry by an $r \times r$ zero matrix. The design and optimization of QC-LDPC codes are of great interest to code designers since they offer not only performing decoding results but also an implementation friendly structure. They can be encoded with low complexity by means of simple shift registers with linearly complexity [114] and can be efficiently decoded [38, 113]. We can find several high-performance QC-NB-LDPC codes construction propositions [110, 38], and some recent constructions include [115, 116]. However, QC-NB-LDPC codes have limitations ; some cycles in the protograph matrix cannot be suppressed during the extension phase, which give an upper minimum Hamming distance associated to each protograph matrix. These results are obtained independently of the size of the circulant matrix entries [117] ; therefore, an increase in the circulant size matrix does not provide an increase in minimum distance beyond a certain limit.

Selecting the non-null positions in the PCM is a determinant step in the construction of NB-LDPC codes. In our dissertation, we will consider the QC-NB-LDPC codes with the minimum connectivity on the symbol nodes, $d_v = 2$. We have made this choice of d_v due to its performing performance and low complexity implementation [25]. The edge label choice represents another degree of freedom in the design of NB-LDPC code. It will be a matter of study in the following sections.

5.1.2 NB COEFFICIENTS CHOICE IN THE PCM

The second step of a NB-LDPC code construction, consist in the determination of non-null entries values of one rows for the PCM, regardless of the structure of the Tanner graph associated with it. In other words, the problem of the selection and the matching of the PCM non-null entries is done assuming that the positions of non-null entries in the PCM associated with the NB-LDPC code have been already optimized. Different methods were proposed in the state-of-the-art to select the non-null entries of one in a PCM. In [118] the values of the non-null entries of the PCM are selected randomly from a uniform distribution among non-null elements of GF (q). Davey et al. [22] proposed an optimization method to choose the non-null entries based on the density evolution determination, which is computationally expensive for high order field. In [25], authors optimized the choice of the non-null entries based on the binary image representation of the PCM by improving the minimum Hamming distance of the binary image of the code per row.

Efficient choice of non-null entries makes more reliable the exchanged messages along the Tanner graph edges. It was proven that optimized row of coefficients to generate the PCM ameliorate performance compared to code with randomly selected coefficients especially for Galois fields GF(q) with $q >> 2$. In fact, a row optimization, through non-null entries selection, improves the waterfall region of the decoding performance curves [71]. To lower the error floor region, coefficients that belongs to the short length cycles and stopping sets must be carefully chosen to avoid low weight code word associated, and then to improve the minimum distance of the codes [9].

Choosing the non-null entries in the PCM was a subject of research developed specially for binary transmission, thus the proposed optimizations were sufficient to make this step fulfilled with optimal non-null values. However, when using high spectral efficiency transmissions, these optimizations may not be enough to make the choice of non-null entries optimal. In the chapter, the choice of the non-null entries will take into account the use of high order modulations, (i.e. M-QAM modulation), in the transmission scheme.

5.2 NB-LDPC CODES AND MODULATION JOINT OPTIMIZATION : MOTIVATION FACTS

In a case of non-binary transmission, were the code and modulation order matches, the N codeword symbols are associated directly to a sequence of N points from the constellation. Thus, the symbols can be represented as points in the Euclidean space. The resulting modulated codeword vector can be seen as a vector of signal points. The distance between any two modulated codeword vectors can be determined from the Euclidean distance between the signal points representing each vector in the Euclidean space. The digital signal uses a modulation mapping (Gray mapping as an example) which associates to each symbol a sequence of binary signals. Codeword vectors are mapped onto points in the signal constellation in a way that enhances the distance properties of the error correcting code.

Binary modulation systems with NB-LDPC codes are optimized for Hamming distance [25]. Soft decision decoding of NB-LDPC codes have been well established for power-efficient transmission at spectral efficiency of 2 bit/sec/Hz. In fact, for binary modulations, e.g. BPSK or QPSK (with Gray mapping) modulations, the Hamming distance of the error correcting code is equivalent to the Euclidean distance of the modulated codeword vectors. Then, the values and the positions of the non-null entries of the PCM can be optimized in a way that maximizes the Hamming distance of the code [25]. For non-binary modulations, the Euclidean distance of modulated codeword vectors is not equivalent to the Hamming distance of the error correcting code. In addition, the Euclidean distance properties depend on the modulation mapping used to map the codeword vectors onto signal points. As a result, the construction of PCM of NB-LDPC codes for coded modulations in order to maximize the Hamming distance is sub-optimal. This relation between the mapping and the Euclidean distance for coded modulation is a relevant factor and offers an interesting possibility to propose better CM scheme. There is accordingly a need for constructing effi-

cient non-binary coded modulations involving error correcting codes that are optimized for the Euclidean distance rather than for the Hamming distance and are jointly optimized with the modulation mapping.

The main reason behind the development of such an optimization method is the fact that the Euclidean distance properties of the codes depend on the modulation used in the transmission scheme. This dependence is especially revealed when we consider high order modulation. If the Galois Field symbols are affected directly to the constellation points, any permutation of the constellation point's positions will impact the Euclidean distance values between symbols, and consequently will impact also the Euclidean distance between codewords. Thus, a good optimization of should be aware of the modulation and channel coding to enhance the whole transmission systems properties and then the CM performance. For high spectral efficiency transmission, the problem of the adaptation of the non-null entries of the PCM to a high order modulation was ignored in the literature, for NB-LDPC codes or any other non-binary code.

Two parameters of the CM scheme will be jointly optimized for a better decoding performance. The first parameter is the non-null entries of one row in the PCM, and the second one is the mapping of the modulation. These two parameters need to be meticulously optimized together. Two main metrics will be our references in the proposed method optimization which are the minimum Euclidean distance and the spectrum of the Euclidean distances between codewords. Before proceeding such an optimization method, some tools needs to be developed to facilitate the Euclidean distance computation, and the code spectrum evaluation.

5.3 EUCLIDEAN DISTANCE EVALUATION

To perform an Euclidean distance evaluation between two vectors we need to clarify some notions. Let us consider two vectors $x = (x_0, x_1 \dots x_{n-1})$ and $y = (y_0, y_1 \dots y_{n-1})$ of $\mathbb{R}^n$. Their Euclidean distance $D(x, y)$ can be computed as follows :

$$D(x,y) = \sqrt{\sum_{i=0}^{n-1} (x_i - y_i)^2}. \tag{5.1}$$

Assuming that each symbol x in GF(q) is associated with an element of the q-ary constellation $\mathcal{M}$, we can define the mapping function π as follows :

$$\begin{aligned} \pi : \mathrm{GF}(q) &\rightarrow \mathbb{R}^2 \\ x &\rightarrow (\pi_I(x), \pi_Q(x)) \end{aligned} \tag{5.2}$$

Where $\pi_I(x)$ and $\pi_Q(x)$ represent the In-phase and the Quadrature amplitudes of the modulated signal associated to x, respectively. The squared Euclidean distance $D^2_\pi(x, y)$

between two elements x and y in GF(q) is the squared Euclidean distance between $\pi(x)$ and $\pi(y)$ in $\mathbb{R}^2$, and it is computed as follows :

$$D_\pi^2(x,y) = |\pi_I(x) - \pi_I(y)|^2 + |\pi_Q(x) - \pi_Q(y)|^2. \tag{5.3}$$

As we can notice $D_\pi(x,y)$ is expressed using the mapping function π, thus, dependence between the Euclidean distance and the π function exits. In other words, the change of the constellation mapping, may leads to have different Euclidean distances between two distinct symbols in GF(q). The Euclidean distance between two codewords of length N, $\mathbf{x} = \{x_k\}_{k=1\dots N}$ and $\mathbf{y} = \{y_k\}_{y=1\dots N}$, depend then of the mapping function π and can be expressed as follows :

$$D_\pi^2(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{N} D_\pi^2(x_k, y_k). \tag{5.4}$$

To enhance the decoding performance, the minimum Euclidean distance d_{min}^{Euc} between codewords should be as high as possible. The d_{min}^{Euc} value can be determined as follows :

$$d_{min}^{Euc} = \underset{\mathbf{x},\mathbf{y}\in \mathrm{C};\mathbf{x}\neq\mathbf{y}}{\operatorname{argmin}} D_\pi^2(\mathbf{x},\mathbf{y}). \tag{5.5}$$

where C is the set of all possible codewords.

The problem of the minimum Euclidean distance determination occurs when we realize that enumerating all the codewords is a task too complex to achieve, especially for long length codes (For codewods of length N and rate $\frac{K}{N}$ we need to test all distances between 2^K codewords). To maintain a reasonable optimization set, our approach will reduce the determination of the minimum Euclidean distance to the level of one parity-check equation. The proposed approach consists in optimizing the coefficients of one row of the matrix as in [71, 25], with the novelty of including the mapping in the optimization parameters. A single parity-check equation of the code expressed as :

$$\sum_{k=1}^{d_c} h_k x_k = 0, \tag{5.6}$$

where $h_k \in$ GF(q), $k = 1 \dots d_c$, are the non-null entries and $x_k \in$ GF(q), $k = 1 \dots d_c$ are the d_c variables of the parity-check equation. Note that this equation defines a code over GF$(q)^{d_c}$.

Let us denote by $\mathcal{C}$ the set of d_c-uple $\mathbf{x} = \{x_k\}_{k=1\dots d_c}$ in GF$(q)^{d_c}$ that verify (5.6). It is important to notice that from now on, our study will focus exclusively on codewords that belong to $\mathcal{C}$, the set of codewords defined by specific d_c non-null entries, and mapping π. The definition of the squared Euclidean distance between two codewords $(\mathbf{x},\mathbf{y}) \in \mathcal{C}^2$ that verify a parity-check equation and when using the mapping π is computed as follows :

$$D_\pi^2(\mathbf{x},\mathbf{y}) = \sum_{k=1}^{d_c} D_\pi^2(x_k, y_k). \tag{5.7}$$

Now we have the possibility to evaluate the Euclidean distance between any two codewords that belong to a set $\mathcal{C}$, for a given non-null entries, and for a mapping π. In the next section, we intend to show that the Euclidean distance is a more appropriate metric that the Hamming distance for the design of coded modulation schemes

5.4 EUCLIDEAN DISTANCE VS HAMMING DISTANCE IN CODED MODULATION

A Galois Field GF(q), with $q = 2^p$, is defined by the set of polynomials over $\mathbb{Z}/2\mathbb{Z}[\alpha]$ $\mod P[\alpha]$, with $P[\alpha]$ is an irreducible polynomial of degree p. All elements of GF(q) can be represented by a binary vector of size p as $x = (x_0, x_1, \dots x_{p-1})_2$, with $x = x_0\alpha^0 + x_1\alpha^1 \dots + x_{p-1}\alpha^{p-1}$. A non-null elements x of GF(q) can also be represented as $x = \alpha^\mu$, $\mu = 0 \dots q-2$.

When using a binary BPSK modulation, the binary representation $(x_0, x_1 \dots x_{r-1})$ of $x \in$ GF(q) is used to modulate r BPSK symbol, with $x_i \in \{0,1\}$. For each bit x_i we associate the modulated value $s_i(x)$, with $s_i(x) = (1-2x_i)$, $i \in \{0 \dots r-1\}$. The Hamming distance and the Euclidean distance between two symbols x and y of GF$(q)^2$ $d_H(x,y)$ and $D(x,y)$ are defined as follows :

$$d_H(x,y) = \sum_{i=0}^{r-1} x_i \oplus y_i. \tag{5.8}$$

$$D(x,y) = \sqrt{\sum_{i=0}^{r-1} (s_i(x) - s_i(y))^2} = 2\sqrt{d_H(x,y)}. \tag{5.9}$$

Here, we can easily notice that there exists a direct relation between the Euclidean distance $D(x,y)$ and the Hamming distance $d_H(x,y)$ of any two symbols $(x, y) \in$ GF$(q)^2$. By extension, $D(\mathbf{x},\mathbf{y})$ and $d_H(\mathbf{x},\mathbf{y})$ have also a direct relation for any two codewords $(\mathbf{x}, \mathbf{y}) \in \mathcal{C}^2$. Thus, the Euclidean distance and Hamming distance change with the same manner. This means that the coefficients h_k, $k = 1 \dots d_c$ in (5.6) should be chosen so as to optimize the Hamming distance of the code. This approach was proposed in [25]. For GF(64), $d_c = 4$, and $P[\alpha] = \alpha^6 + \alpha + 1$, the best coefficients found are $\{h_k\}_{k=1\dots4} = \{\alpha^0, \alpha^9, \alpha^{22}, \alpha^{37}\}$. With these optimal coefficients, the minimum Hamming distance between two codewords is 3 and there are exactly 20 codewords at a distance 3 of the all-zero codeword (see [25]).

When using an M-ary modulation, there is no longer any direct connection between Hamming distance and Euclidean distance, except if a Gray mapping (for q-QAM modulation) or Gray-like mapping (for q-APSK modulation) is used. Let us consider, for example,

the 64-QAM modulation with the Gray mapping π_0 defined in the DVB-T2 standard [15] presented in Fig. 5.1. A symbol $x = (x_0, x_1, \ldots, x_5)_2$ is associated with $\pi_0(x) = (\pi_{0I}(x), \pi_{0Q}(x))$, where $\pi_{0I}(x) = G(x_0+2x_2+4x_4)$ and $\pi_{0Q}(x) = G(x_1+2x_3+4x_5)$, with $\{G(i)\}_{i=0\ldots7} = \{+7, -7, +1, -1, +5, -5, +3, -3\}$. For example, $x = (100101)_2$ is assigned to $\pi_0(x) = (G(1 + 2 \times 0 + 4 \times 0), G(0 + 2 \times 1 + 4 \times 1)) = (G(1), G(6)) = (-7, 3)$. If we consider x, y and $z \in$ GF$(q)^2$, the symbols associated to the bit sequences $(000000)_2$, $(000001)_2$ and $(100000)_2$ respectively, while using the Gray mapping π_0 presented in Fig. 5.1, we can observe that $d_H(x, y) = d_H(x, z) = 1$, while $D_{\pi_0}(x, y) = 2$ and $D_{\pi_0}(x, z) = 14$. Nevertheless, using Gray mapping ties Hamming distance and Euclidean distance according to a set of properties defined bellow.

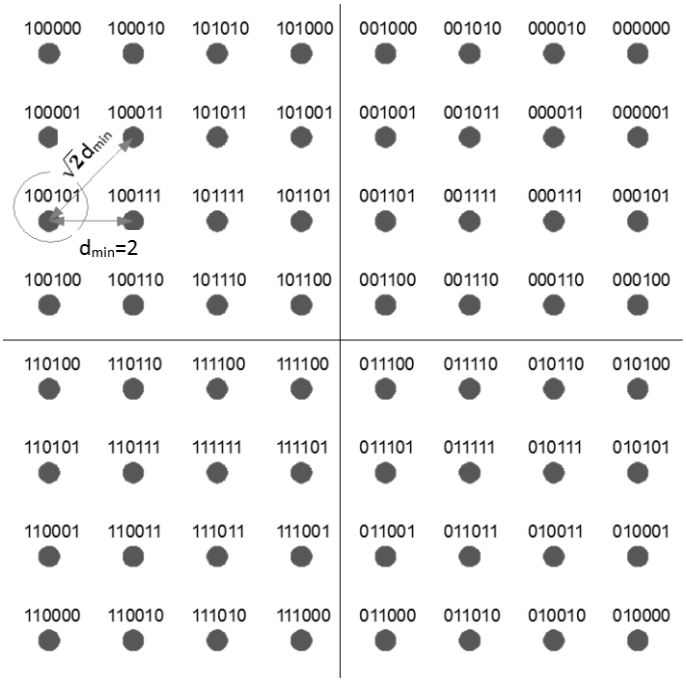

FIGURE 5.1 – Mapping π_0 : Gray Mapping of the DVB-T2 standard for 64-QAM modulation

Let us consider in general an M-QAM modulation associated to a Gray-mapped constellation with a $d_{min} = 2$, where d_{min} is the minimum distance between two distinct points of the constellation. The following properties can be verified for both Euclidean distance and Hamming distance for all couple of symbols $(x, y) \in$ GF$(q)^2$ for any mapping π : :

— Property 1 (**P1**) : $D_\pi(x, y) = d_{min} \Rightarrow d_H(x, y) = 1$, for example $x = (100101)_2$ and $y = (100111)_2$ in mapping $\pi_0(Fig.5.1)Property2$(**P2**) :D$\pi(x, y) = 2\sqrt{2} \Rightarrow d_H(x, y) = 2$ (corresponding to two points in opposite positions in a square of side d_{min}). For example, $x = (100101)_2$ and $y = (100011)_2$ in Fig. 5.1.

— Property 3 (**P3**) : $d_H(x,y) = 2 \Rightarrow D\pi(x,y) \geq 2\sqrt{2}$
— Property 4 (**P4**) : $d_H(x,y) \geq 3 \Rightarrow D\pi(x,y) \geq 4$.

From these properties, we can infer that for any mapping π :

— $\forall$(x,y)$\in \mathcal{C}^2$, $d_H(\mathbf{x},\mathbf{y}) \geq 3 \Rightarrow D_\pi(\mathbf{x},\mathbf{y}) \geq 2\sqrt{3}$,

Proof : Three possibilities occurs.

1. If $\mathbf{x}$ and $\mathbf{y}$ differ at least of three distinct symbols, $\exists$ i, j and, k ; $x_i \neq y_i$, $x_j \neq y_j$ and, $x_k \neq y_k \Rightarrow D_\pi(\mathbf{x},\mathbf{y})^2 \geq D_\pi(x_i,y_i)^2 + D_\pi(x_j,y_j)^2 + D_\pi(x_k,y_k)^2$, see Eq. 5.7. Then $D_\pi(\mathbf{x},\mathbf{y})^2 \geq 3d_{min}^2 = 12$.
2. If $\mathbf{x}$ and $\mathbf{y}$ differ by two positions in a symbol ($\exists i, D_H(x_i,y_i) = 2$) and at least one position in another symbol ($\exists j, D_H(x_j,y_j) = 1$), with $i,j \in \{0 \dots d_c - 1\}$ than (**P1**) and (**P3**) proves the inequality. $D_\pi(\mathbf{x},\mathbf{y})^2 \geq D_\pi(x_i,y_i)^2 + D_\pi(x_j,y_j)^2 \geq 2\sqrt{2}^2 + 2^2 \geq 2\sqrt{3}^2$.
3. If $\mathbf{x}$ and $\mathbf{y}$ differs of 3 bits in one GF(q) symbol, than (**P4**) proves the proposed inequality.

To summarize, using a M-QAM Gray-mapped constellation and a parity-check equation that guarantee a minimum Hamming distance of three yields a code with a minimum Euclidean distance of $2\sqrt{3}$.

Here we have seen that the Euclidean distance is equivalent to the Hamming distance when using binary modulation metric, but this is not the case when using high order modulations e. i. M-QAM modulation (M > 4). Thus, when using high order modulations Hamming distance becomes a sub-optimal metric to choose the non-null coefficient entries of the PCM. It is obvious that the minimum Euclidean distance is important to determine to optimize the code algebraic properties, but the multiplicity of the Euclidean distances called distance spectrum is also an important indicator in our optimization approach. The next step consists in the evaluation of the distance spectrum of a code $\mathcal{C}$. Such an operation aims to compute the occurrence of each Euclidean distance between all the couple of codewords of $\mathcal{C}$ defined by non-null entries and mapping π.

5.5 DISTANCE SPECTRUM EVALUATION

In this section we propose a definition of the distance spectrum (DS) function. We explain the reasons for the DS evaluation task simplification by considering only the first terms of the DS. Finally, a simple algorithm is proposed to evaluate the first terms of the DS for M-QAM modulations.

5.5.1 DEFINITION OF DISTANCE SPECTRUM

The DS of a code $\mathcal{C}$, defined by d_c non-null entries, and a mapping π, presents the enumeration of all the possible distances between two couple of codewords and the number

of distinct couples at each of those distances. For every distance $d \in \mathbb{R}$, the DS function $S_{\pi,\mathcal{C}}(d)$ return the number of couple of codewords with an Euclidean distance equal to d. More formally :

$$\begin{aligned} S_{\pi,\mathcal{C}} : \mathbb{R} &\rightarrow \mathbb{N} \\ d &\rightarrow S_{\pi,\mathcal{C}}(d) = |\{(\mathbf{x},\mathbf{y}) \in \mathcal{C}^2 / D_\pi^2(\mathbf{x},\mathbf{y}) = d^2\}|. \end{aligned} \tag{5.10}$$

where $|.|$ represents the cardinality of a set. $S_{\pi,\mathcal{C}}$ verify the following equations :

$$\begin{aligned} &\int_0^\infty S_{\pi,\mathcal{C}}(\gamma) d\gamma = \binom{2}{|\mathcal{C}|} = \frac{|\mathcal{C}|!}{|\mathcal{C}|-2)!2!} \\ &S_{\pi,\mathcal{C}}(0) = q \end{aligned} \tag{5.11}$$

The exact evaluation of the DS of a code $\mathcal{C}$ associated to a mapping π is a computationally intensive task. For a check node of degree d_c, the first $d_c - 1$ symbol inputs can be set arbitrarily to any value of GF(q), while the last symbol is determined by the equation 5.6, thus $|\mathcal{C}| = q^{d_c-1}$. The evaluation of all possible couples of codewords that belong to $\mathcal{C}$ has a complexity computed as follows :

$$\binom{2}{|\mathcal{C}|} = \frac{|\mathcal{C}|!}{|\mathcal{C}|-2)!2!} \tag{5.12}$$

Thus, the straight evaluation of the distance spectrum has a complexity that increases exponentially when d_c increases. For instance, for values of $q = 64$ and $d_c = 4$, more than 3.4×10^{10} Euclidean distances have to be evaluated, and when $q = 64$ and $d_c = 6$, the number of couple becomes 5.8×10^{18}, which is computationally impossible to be evaluated. A simplification of the DS evaluation task becomes crucial. Knowing that the lowest Euclidean distances are determinant to evaluate the decoding PCM performance, only the first terms of the DS need to be evaluated.

5.5.2 UNION BOUND DERIVATION

The main purpose behind the determination of the DS is to choose the best code (d_c entries) and mapping π that ameliorate the algebraic properties of one parity-check equation. This allows to get better FER performance if we consider only the codewords in $\mathcal{C}$ and consequently better decoding performance of the whole PCM. In fact, for $\mathbf{x}$ and $\mathbf{y} \in \mathcal{C}$, we have the possibility to evaluate the probability $P(\mathbf{x} \rightarrow \mathbf{y})$ of transmitting $\mathbf{x}$ and decoding $\mathbf{y} \neq \mathbf{x}$ when using a Maximum Likelihood (ML) decoder. If the d_c symbols of an element $\mathbf{x} \in \mathcal{C}$ are transmitted through an AWGN channel, the received message is thus $\mathbf{r} = \pi(\mathbf{x}) + \mathbf{w}$, where $\mathbf{w}$ is a complex vector of size $2d_c$, with each coordinate being the

realization of a complex Gaussian noise of variance $\sigma^2 = N_0/2$, where N_0 is the power spectral density of the AWGN. For a given SNR the pairwise error probability $P(\mathbf{x} \to \mathbf{y})$ can be expressed as :

$$P(\mathbf{x} \to \mathbf{y}) = \text{Prob}(||\mathbf{r} - \pi(\mathbf{x})||^2 > ||\mathbf{r} - \pi(\mathbf{y})||^2). \tag{5.13}$$

Since we consider the AWGN channel, this probability can be expressed as

$$P(\mathbf{x} \to \mathbf{y}) = Q\left(\frac{D_\pi(\mathbf{x}, \mathbf{y})}{2\sigma}\right), \tag{5.14}$$

where $Q(u)$ is the Q-function defined as :

$$Q(u) = \frac{1}{\sqrt{2\pi}} \int_u^{+\infty} e^{\frac{-t^2}{2}} dt. \tag{5.15}$$

The probability of error on a received codeword $P_e(\sigma)$ can be upper bounded (union bound inequality) by $U_b(\sigma) : P_e(\sigma) \leq U_b(\sigma)$, with

$$U_b(\sigma) = \frac{1}{|\mathcal{C}|} \sum_{\mathbf{x} \in \mathcal{C}} \sum_{\mathbf{y} \in \mathcal{C}/\mathbf{x}} P(\mathbf{x} \to \mathbf{y}) = \frac{1}{|\mathcal{C}|} \int_d S_{\pi,\mathcal{C}}(\gamma) Q(\frac{\gamma}{2\sigma}) d\gamma, \tag{5.16}$$

Fortunately, the Q function decreases very rapidly and only the first terms in the DS are useful to accurately estimate the union bound for high SNRs. For high SNRs, equation (5.16) can be approximated by only using the first (dominating) terms in the union bound which concern the codewords at minimum distances. Then, it will be more accurate to estimate only the first terms of DS. Next section explains a simplification of such task.

5.5.3 PROPOSED METHOD TO EVALUATE THE FIRST TERMS OF THE DS

To evaluate the first terms of the DS, we will consider the following approach : we define d_u as the maximum value of the Euclidean distance for which the DS should be exactly evaluated, in others terms, if $d \leq d_u$, then $S_{\pi,\mathcal{C}}(d)$ should be exactly evaluated. Since two distinct codewords $\mathbf{x}$ and $\mathbf{y}$ of $\mathcal{C}$ satisfy (5.6), then $\mathbf{x}$ and $\mathbf{y}$ differ at least by two distinct symbols among the possible d_c symbols. We can infer there exists i and j with $i \neq j$ where $x_i \neq y_i$ and $x_j \neq y_j$ that verify $D_\pi(x_i, y_i) + D_\pi(x_j, y_j) \leq D_\pi(\mathbf{x}, \mathbf{y}) \leq d_u$, we can deduce that $D_\pi(x_i, y_i) \leq d_u - D_\pi(x_j, y_j) \leq d_u - d_{min}$ ($D_\pi(x_j, y_j) \geq d_{min}$). For each constellation point $\pi(x) \in \mathcal{M}$, we can define its near neighborhood symbols as the set $V(x)$ expressed by :

$$V(x) = \{y \in \text{GF}(q) / D_\pi(x, y)^2 \leq d_u^2 - d_{min}^2\}. \tag{5.17}$$

From this property, we deduce that having $D_\pi(\mathbf{x}, \mathbf{y})^2 \leq d_u^2$ implies that $y_k \in V(x_k)$ for $k = 1 \dots d_c$. Thus, for a given codeword $\mathbf{x}$, estimating the codewords $\mathbf{y} \in \mathcal{C}$ such

that $D_\pi(\mathbf{x}, \mathbf{y}) \leq d_u$ requires a maximum of v^{d_c-1} distance evaluations, where v is the maximum cardinality of $V(x)$ that can be expressed as follows :

$$v = \max\{|V(x)|, x \in \text{GF}(q)\}. \tag{5.18}$$

The application on an M-QAM modulation can efficiently determine the set $V(x)\ \forall x \in$ GF(q). For any value of d_u with a minimum distance d_{min}, $V(x)$ should contain all points of the constellation at a distance smaller than or equal to $\sqrt{d_u^2 - d_{min}^2}$, $V(x) = \{y \in \text{GF}(q)\}$ such that $|\pi_I(x) - \pi_I(y)| \leq F(\sqrt{d_u^2 - d_{min}^2})$ and $|\pi_Q(x) - \pi_Q(y)| \leq F(\sqrt{d_u^2 - d_{min}^2})$. $F(\alpha)$ is the floor function that returns the greatest integer less than or equal to α.

For the example previously introduced with $q = 64$, $d_c = 4$, and a 64-QAM constellation, let us set $d_u = 4$. The minimum distance in the 64-QAM constellation is $d_{min} = 2$. Therefore, the neighborhood of x, $V(x)$ contains constellation points that have an Euclidean distance inferior to $\sqrt{d_u^2 - d_{min}^2} = 2\sqrt{3}$ from x. Since $2\sqrt{2} < \sqrt{12} < 4$, $V(x) = \{y \in \text{GF}(64)\}$ such that $|\pi_I(x) - \pi_I(y)| \leq 2$ and $|\pi_Q(x) - \pi_Q(y)| \leq 2$. In that case, $|V(x)| \leq 9$, $x \in \text{GF}(64)$ and hence $v = 9$. Enumerating the set of points $\mathbf{y}$ of $\mathcal{C}$ at a distance smaller than or equal to $d_u = 4$ from a given point $\mathbf{x}$ of $\mathcal{C}$ requires a maximum number of distance computations equal to $v^{d_c-1} = 9^3 = 729$. Then, the exact evaluation of the first terms of the DS is bounded by $64^3 \times 9^3 \cong 1.91 \times 10^8$, which is computationally more tractable.

Since the computation of the first terms of the DS is affordable, we will try to put in clearer the dependence between the Euclidean distance as well as the DS and the mapping for fixed non-null entries.

5.6 INCIDENCE OF GRAY MAPPING CHOICE ON EUCLIDEAN DISTANCE AND DISTANCE SPECTRUM

In this section, we show that the choice of the Gray mapping impacts directly the spectrum of the code. In other words, among the set of all possible Gray mapping, the one that leads to the best distance property should be used. Our objective here is to clear up the incidence of using other mappings than those used by default in the standards [15, 17, 16]. We will concentrate our effort on the set of M-QAM modulations with Gray mapping. Indeed, such schemes provide a signal constellation in which signal points have adjacent signal points that differ in only one bit, which provides interesting properties of symmetry and predictable repartition of Euclidean distances between the constellation points.

Let π_0 be a given Gray mapping on a QAM modulation, i.e. $\forall\ x, y\ D_{\pi_0}(x, y) = d_{min} \Rightarrow d_H(x, y) = 1$. In other words, if two neighbor points are associated to a GF value, they will have a binary representation that differs only in one position. In fact, applying a permutation on the binary representation of π_0 leads also to a Gray-mapped constellation with a different structure. More formally, when using an M-QAM modulation with M=2^p, we can define the

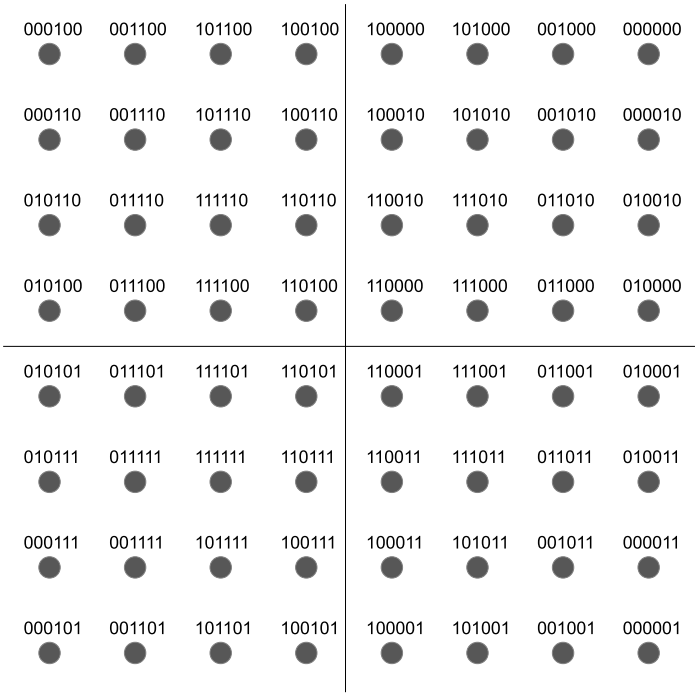

FIGURE 5.2 – Mapping π_1

mapping π_σ associated to the permutation function σ in the set $\{0, 1, \ldots, p-1\}$. π_σ can be defined as $\pi_\sigma(x) = \pi_0(\Sigma(x))$, with Σ is a symbol permutation function deduced using σ as follows :

$$\begin{aligned} \Sigma : \mathrm{GF}(q) &\rightarrow \mathrm{GF}(q) \\ x = (x_0, x_1, \ldots x_{p-1}) &\rightarrow \Sigma(x) = (x_{\sigma(0)}, x_{\sigma(1)}, \ldots x_{\sigma(p-1)}) \end{aligned} \tag{5.19}$$

The M-QAM constellation representation, of a symbol $x = (x_0, x_1, \ldots, x_{p-1})_2$, of the resultant Gray mapping with p an even number can define $\pi(x) = (\pi_I(x), \pi_Q(x))$ as follows :

$$\pi_I(x) = \sum_{k=0}^{\frac{k}{2}} 2^{2\times k} x_{2\times k} \tag{5.20}$$

$$\pi_Q(x) = \sum_{k=0}^{\frac{k}{2}} 2^{2\times k+1} x_{2\times k+1} \tag{5.21}$$

Note that a permutation of the binary representation does not affect the Hamming distance of the binary representation, i.e., $\forall (x, y) \in \mathrm{GF}(64), d_H(x, y) = d_H(\sigma(x), \sigma(y))$ but

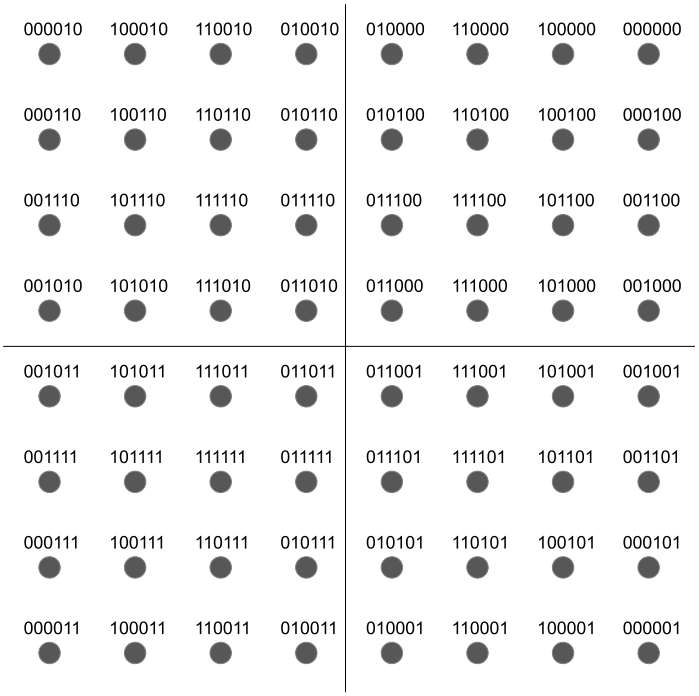

FIGURE 5.3 – Mapping π_2

may affect the Euclidean distance after mapping, and this eventually modifies the DS of the coded modulation.

Let us take the example of the Gray-mapped 64-QAM modulation. We can reconsider the mapping π_0 already defined, and π_σ a new Gray mapping where σ is a permutation in the set $\{0, 1, \ldots, 5\}$ as $\pi_\sigma = \pi_0(\Sigma(x))$, with

$$\begin{aligned} \Sigma : \mathrm{GF}(64) &\rightarrow \mathrm{GF}(64) \\ x = (x_0, x_1, \ldots x_5) &\rightarrow \Sigma(x) = (x_{\sigma(0)}, x_{\sigma(1)}, \ldots x_{\sigma(5)}). \end{aligned} \tag{5.22}$$

Mappings in Fig. 5.2 and 5.3 can then be obtained from mapping π_0 (Fig. 5.1) respectively by applying permutations σ_1 and σ_2 associated to permutations Σ_1 and Σ_2 on the mapping π_0, with $\Sigma_1(x) = (x_3, x_0, x_2, x_1, x_5, x_4)$ and $\Sigma_2(x) = (x_4, x_2, x_1, x_0, x_5, x_3)$. We can easily notice that the Euclidean distance between two distinct symbols x and y varies depending of the used mapping. For instance, if $x^{'}$ and $y^{'}$ are two symbols that represent respectively the bit sequences (000000) and (000001), the Euclidean distance in mapping π_0 (Fig. 5.1), $D_{\pi_0}(x^{'}, y^{'}) = d_{min}$ becomes $D_{\pi_1}(x^{'}, y^{'}) = 7 \times d_{min}$ with mapping π_1 (Fig. 5.2), and $D_{\pi_2}(x^{'}, y^{'}) = 7 \times d_{min}$ with mapping π_2 (Fig. 5.3).

Therefore we have shown that changing the mapping can impact the Euclidean distance between two distinct symbols x and y, and thus an impact on the DS of a couple of code

$\mathcal{C}$ and mapping π is inevitable. In the next section, we propose a joint optimization of the mapping and the NB-LDPC code at the parity-check equation level. Then we generalize it to the whole PCM.

5.7 JOINT OPTIMIZATION OF MAPPING AND NB-LDPC MATRIX COEFFICIENTS

In this section, we propose to jointly optimize both modulation and PCM of NB-LDPC code. We aim to find out the best couple mapping π and d_c non-null entries that defines a $(\mathcal{C}, \pi) \in \mathbf{C}$ in order to minimize error rate, where $\mathbf{C}$ is the set of all possible codes $(\mathcal{C}, \pi)$ defined by a combination of a mapping and non-null coefficients as entries. To fulfill this objective, we start by performing an exhaustive search among all the possible codes $(\mathcal{C}, \pi)$ among $\mathbf{C}$ that optimizes the DS, or in practice, that minimizes the first terms in $S_{\pi,\mathcal{C}}(d)$, for $d < d_u$, with d_u the highest value that guarantees a minimum values of $S_{\pi,\mathcal{C}}(d)$ for $d < d_u$. The optimal code $(\mathcal{C}, \pi)^{opt}$ is thus selected as

$$(\mathcal{C}, \pi)^{opt} = \min_{(\mathcal{C},\pi)\in\mathbf{C}} \{\max_{d_u \in \mathbb{R}} S_{\pi,\mathcal{C}}(d); \forall d < d_u\} \tag{5.23}$$

In practice, the d_u value is incremented till we find out that $S_{\pi,\mathcal{C}}(d)$ cannot be minimized for all values of d lower than d_u. As we have seen in Eq. 5.16, the first values of the DS are always the most predominant values, therefore, there is no need to have a very important d_u value. For the d_c non-null entries, we have q^{d_c-1} possibilities of combinations of d_c-tuples (the first non-null entry is set to α_1). For the possible Gray mappings, we can deduce from one Gray-mapped constellation, a number of $p!$ possible mappings via an exhaustive research. We can use the symmetries in the M-QAM mapping to reduce the number of Gray mappings to be tested. The first symmetry can be modeled by a rotation around the origin. In figures Fig. 5.4, Fig. 5.5, Fig. 5.6 and 5.7 (4-QAM modulation), the represented constellations are associated to the mappings π'_0, π'_1, π'_2 and π'_3, respectively. The mappings π'_1, π'_2 and π'_3 and the result of a rotation applied on the mapping π'_0, using the angles $90°$, $180°$ and $270°$, respectively. Such transformation do not change the Euclidean distances between symbols, thus it is enough to test one of these mapping. The other mappings will have exactly the same results in term of Euclidean distance and DS. Knowing this property we can reduce the number of the tested Gray-mapped constellation to $\frac{n!}{4}$. We can easily generalize the explained property to all M-QAM modulations.

Another property of the M-QAM modulations can be used to lower the number of tested mappings. It consists on considering the diagonal symmetry. In figure Fig. 5.8 and 5.8 we can notice that we used the mapping π'_0 and the mapping π'_5 the image of π'_0 using a diagonal symmetry. Both constellations have same Euclidean distance and DS values. The number of tested mapping can be divided again by 2 to reach a total number of tested Gray-mapped constellation of $\frac{n!}{8}$.

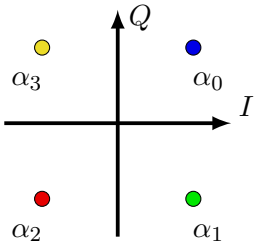

FIGURE 5.4 – Mapping π'_0

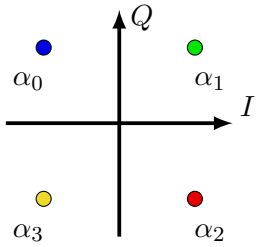

FIGURE 5.5 – Mapping π'_1

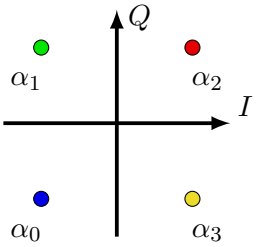

FIGURE 5.6 – Mapping π'_2

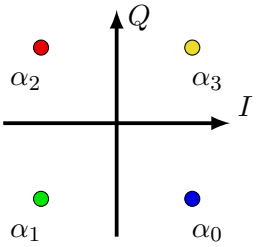

FIGURE 5.7 – Mapping π'_3

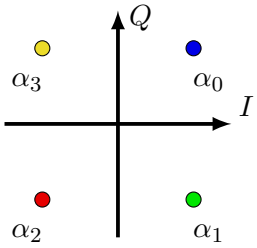

FIGURE 5.8 – Mapping π'_0

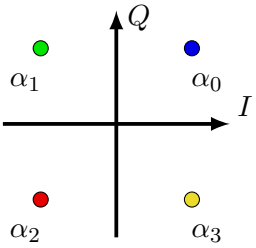

FIGURE 5.9 – Mapping π'_5

If we consider again the example for the 64-QAM, the number of the tested Gray-mapped constellations will be $\frac{6!}{8} = 90$. For $d_c = 4$, the exhaustive search for each mapping should minimize the $S_{\pi,\mathcal{C}}(2\sqrt{3})$ then $S_{\pi,\mathcal{C}}(4)$ in the DS, since these two terms are considered as dominating terms for the high SNR regime performance of the coded modulation. We can use the proposed approximation developed in the previous section to perform the research. Such operation will be done only once, and then the results can be investigated for all PCM with $d_c = 4$ and $q = 64$.

Table 5.1 presents three different coded modulations $(\mathcal{C}, \pi)_i, i = 0, 1, 2$, each one defined by a mapping $\pi_i, i = 0, 1, 2$ as described in Fig. 5.1, Fig. 5.2, and Fig. 5.3 and a set of $d_c = 4$ coefficients $h_k \in$ GF(q), $k = 1 \dots d_c$. These codes have been chosen as follows : $(\mathcal{C}, \pi)_0$ uses the DVB-T2 Gray mapping π_0 [15] (See Fig. 5.1) and coefficients $(\alpha^0, \alpha^9, \alpha^{22}, \alpha^{37})$ as proposed in [25] ; $(\mathcal{C}, \pi)_1$ uses the same coefficients as $(\mathcal{C}, \pi)_0$ and mapping π_1 (Gray mapping that maximizes $S_{\pi,\mathcal{C}}(2\sqrt{3})$ in DS). Note that this corresponds to the worst case, or equivalently the mapping that should show the worst performance for the coded modulation when using the coefficients $(\alpha^0, \alpha^9, \alpha^{22}, \alpha^{37})$, and it is only discussed for comparison purposes. Finally, $(\mathcal{C}, \pi)_2$ is the new proposed combination of mapping and coefficients, i.e. mapping π_2 in Fig. 5.3 with coefficients $(\alpha^0, \alpha^8, \alpha^{16}, \alpha^{42})$. It is obtained after an exhaustive search which consists in calculating the two first terms of DS for a large number of possible mapping/coefficients combinations. Note that $(\mathcal{C}, \pi)_2$ significantly

reduces $S_{\pi,\mathcal{C}}(2\sqrt{3})$. A reduction around 25% compared to the optimized NB-LDPC code in [25] $(\mathcal{C},\pi)_0$ and around 58% compared to $(\mathcal{C},\pi)_1$. This reduction has theoretically a positive impact on the NB-LDPC coded modulation performance. It has to be confirmed through simulations. To summarize, we have considered three codes, the first one $(\mathcal{C},\pi)_0$ uses the PCM entries that are proposed by the state-of-the-art (maximization of the Hamming distance), with the Gray mapping proposed for the DVB-T2 standard [15], the second code $(\mathcal{C},\pi)_1$ consider the same non-null entries but with the worst Gray-mapped constellation, and finally we find the code $(\mathcal{C},\pi)_3$, that represents the best found combination of non-null entries and Gray-mapped constellation.

TABLE 5.1 – First terms of DS for coded modulations $(\mathcal{C},\pi)_0$, $(\mathcal{C},\pi)_1$ and $(\mathcal{C},\pi)_2$

Code	Mapping σ	Coeff.	$S_{\pi,\mathcal{C}}(2\sqrt{3})$		$S_{\pi,\mathcal{C}}(4)$	
$(\mathcal{C},\pi)_0$	$\{5,4,3,2,1,0\}$	$\alpha^{\{0,9,22,37\}}$	516,096		3,868,672	
$(\mathcal{C},\pi)_1$	$\{3,0,2,1,5,4\}$	$\alpha^{\{0,9,22,37\}}$	909,312	+76%	2,910,208	-24%
$(\mathcal{C},\pi)_2$	$\{4,2,1,0,5,3\}$	$\alpha^{\{0,8,16,42\}}$	385,024	-25%	3,499,008	-10%

5.8 SIMULATION RESULTS AND INTERPRETATIONS

In this section we analyse the incidence of the considered codes $(\mathcal{C},\pi)_0$, $(\mathcal{C},\pi)_1$ and $(\mathcal{C},\pi)_2$ on the decoding performance. At the beginning, we consider the decoding performance of one parity-check equation, before extending the performance evaluation results on the whole PCM in order to verify the predicted incidence of choosing better association of NB-LDPC code and mapping. Note that, when better decoding performance is obtained, it comes for free, without any additional complexity.

5.8.1 DECODING PERFORMANCE OF THE ELEMENTARY CHECK NODE

Here we consider the performance of a single parity-check code equation of size $d_c = 4$ in GF(64) associated to a 64-QAM modulation for coded modulations $(\mathcal{C},\pi)_0$, $(\mathcal{C},\pi)_1$ and $(\mathcal{C},\pi)_2$. We aim to find out the repercussion of improving the DS of the code on decoding performance of only one parity-check equation. To clarify the relation between the union bound metric and the FER of the decoded single parity-check equation, Fig. 5.10 presents curves that correspond to the union bound calculation with $S_{\pi,\mathcal{C}}(2\sqrt{3})$ and $S_{\pi,\mathcal{C}}(2\sqrt{4})$, i.e. the first two terms in DS, as well as ML decoding performance curves expressed in FER, i.e. Monte-Carlo simulations with a stopping criterion of 100 frame errors. We have chosen the ML decoding due to the fact that it is the optimal decoding algorithm, and thus the best representative in term of performance.

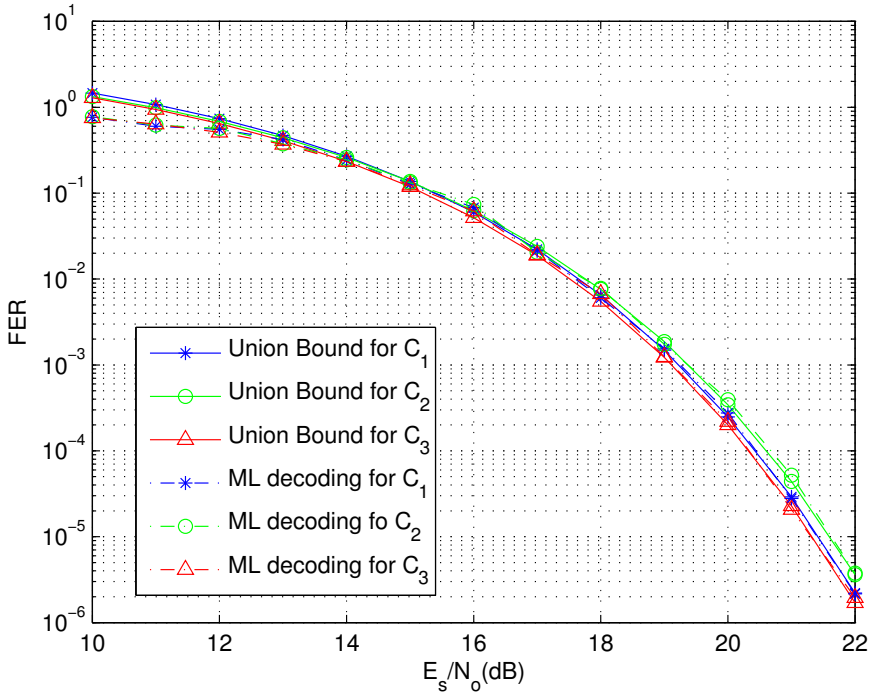

FIGURE 5.10 – Union bound and FER performance for the single parity-check coded modulations $(\mathcal{C}, \pi)_0$, $(\mathcal{C}, \pi)_1$ and $(\mathcal{C}, \pi)_2$.

From Fig. 5.10 we can first notice that the union bound is an accurate approximation for SNR values greater than 16 dB (FER and union bound curves become superposed). A zoom on the low FER region shows that code $(\mathcal{C}, \pi)_2$ offers better performance comparing to $(\mathcal{C}, \pi)_0$. The same conclusion can be derived when comparing performance of $(\mathcal{C}, \pi)_0$ with $(\mathcal{C}, \pi)_1$. Such results of FER and union bound matches with the DS values indicators. We have now to confirm these preliminary results by applying the technique to a NB-LDPC PCM to assess the effectiveness of our approach.

5.8.2 DECODING PERFORMANCE OF THE NB-LDPC JOINT OPTIMIZATION BASED CONSTRUCTED MATRIX

Here we show the incidence of the proposed mapping and non-null entries on a coded modulation scheme with NB-LDPC codes. Let us consider an example of application on a PCM, with a GF(64)-LDPC code of length $N = 48$ symbols, with $d_v = 2$, $d_c = 4$ (coding rate 1/2). In fact, the mapping choice can be easily introduce in the transmission scheme by changing the constellation mapping with reference to figures (Fig. 5.1, Fig. 5.2, and Fig.

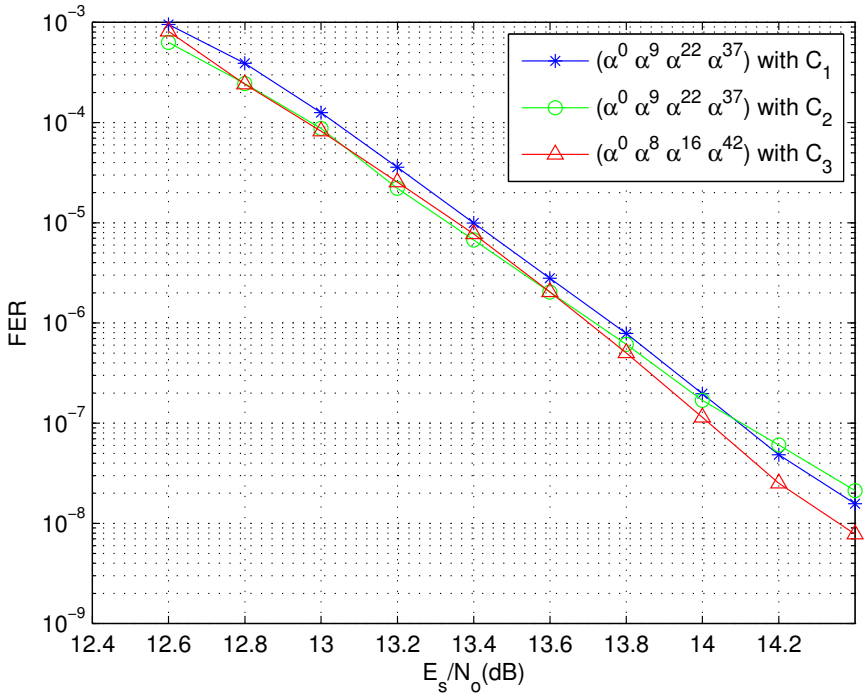

FIGURE 5.11 – EMS decoding performance of a $N = 48$ GF(64)-LDPC code with coded modulations $(\mathcal{C}, \pi)_0$, $(\mathcal{C}, \pi)_1$ and $(\mathcal{C}, \pi)_2$, for a maximum of 100 erroneous frames

5.3), while the non-null entries must be carefully assigned to the non-null positions at each row in the matrix, i.e. for a single check node. To simplify task we will use protograph-based quasi-cyclic LDPC codes [115, 116]. Then, based on [25], we can perform a cycle cancellation and optimize the topological stopping set mitigation of the used the coefficient values presented in Table 5.1.

For the decoding algorithm, we consider the L-Bubble EMS decoding algorithm [42] [119] with a number of significant values $n_m = 25$ and 20 decoding iterations. The de-mapping step follows the principle described in [120] for simplified intrinsic Log-Likelihood Ratio generation. Simulation results show the effectiveness of the proposed optimization approach. Fig. 5.10 shows that $(\mathcal{C}, \pi)_2$ outperforms $(\mathcal{C}, \pi)_0$ and $(\mathcal{C}, \pi)_1$, especially in the high SNR regime region. To be specific, a gain of 0.2 dB (0.15 dB) at a FER = 2×10^{-8} with respect to $(\mathcal{C}, \pi)_1$ ($(\mathcal{C}, \pi)_2$) is achieved with the proposed solution. Note that this performance gain does not entail any additional complexity at the transmitter nor at the receiver compared to existing schemes, as the enhancement comes from the matrix construction and the Gray mapping choice. Also note that even if the proposed approach is based on an exhaustive search to optimize the DS properties of the coded modulation, this step is

performed only once during the code design.

5.9 CONCLUSION

In this chapter we have considered the design of advanced high-spectral efficiency communications with good error-decoding performance. We focused on high-order NB-LDPC coded modulations where the order of the Galois Field and modulation order match. We have proposed to jointly optimize the parity-check equation of a NB-LDPC code and the mapping of the GF(q) symbol in a q-ary constellation. We show an example of rate one half NB-LDPC over GF(64) associated with a 64-QAM performance improvement. We based the NB-LDPC matrix optimization on the analysis of a single check node to find the best GF(q) values for the d_c coefficients for a given modulation mapping. To show the good agreement between the theoretical analysis and practical implementation, we presented and compared the union bound with the ML decoding curves of one parity-check equation. Finally, simulation results of NB-LDPC coded modulation, designed with the proposed method, outperforms the state-of-the-art. The work can be extended to other types of q-ary constellations, likes q-APSK (Asymmetrical Phase Shift Keying) for example, other q Galois Fields, and other code rates.

Chapitre 6
Conclusions and Perspectives

6.1 Conclusions

In the last years, the requirements of modern communication systems have significantly increased, especially in terms of data rate and transmission reliability. New transmission designs that provide high spectral efficiency and good error correcting codes become essential to solve the problem of limited resources. In this context, this thesis explores the high order modulation transmissions that use NB-LDPC codes. More specifically, it is devoted to study the association of highly efficient error-correcting codes, the NB-LDPC codes, with high order modulations. This type of association aims to design systems that are robust to noise and efficient from the point of view of the occupied spectrum.

In our dissertation, we started our work with a detailed study of the state-of-the-art of NB-LDPC codes. We began by recalling some basic mathematical notions that were used to generalize the definition of binary LDPC codes on Galois Fields. Then we directed our interest to the various decoders proposed for NB-LDPC codes. We focused on the EMS algorithm which is a generalization of the Min-Sum decoding algorithm. A performance comparison between Binary and NB-LDPC codes was then presented in order to verify the advantages of NB-LDPC codes. We then presented various elements of digital communication that are useful for our dissertation. We first presented some basic information concerning digital communications, in particular on digital carrier wave transmissions and transmission channel models. Then, we advanced some characteristics of the various high order modulations used in the study (M-QAM,M-PSK). Channel properties like Mutual Information, and channel capacity of Coded Modulation and Bit-Interleaved Coded Modulation schemes were introduced. Using a simplified algorithm allows to display some capacity and Mutual Information curves of the considered channels. Finally, we described the principle of the Signal Space Diversity technique, and introduced some of the state-of-the-art optimizations.

After introducing some state-of-the-art advancements that are related to our dissertation, two main problematics are examined. The first one is related to the optimization of the Signal Space Diversity technique. The second topic considers the CM scheme optimization,

where the NB-LDPC code and the modulation order matches.

The first contribution focuses on the SSD technique optimization in the context of high spectral efficiency communications, under the Rayleigh channel with and without erasure. The proposed optimization method was based on mutual information maximization, and can be applied on any transmission using high-order modulation, i.e. M-QAM and A-PSK modulations. The obtained results for optimal SSD rotation angles, when using CM and BICM schemes, and for different examples of M-QAM modulations, revealed two main interesting results. The first ascertainment shows that there is not an absolute optimal rotation angle for all SNRs. In other terms, the optimal rotation angle value depends on the SNR in the considered transmission channel. For CM there exists a rotation angle close to optimal angle associated to all SNRs, which is not the case for BICM. The second main ascertainment showed that the association of NB-LDPC codes with M-QAM modulations (CM scheme) is more robust than the association of binary LDPC codes with M-QAM modulations (BICM scheme). In a theoretical point of view, the gain in terms of mutual information obtained when using CM is always superior to that with BICM. In practice, simulation results confirm that SSD technique introduces more significant gains in the CM scheme than in the BICM one. Such contribution is important for the next generation broadcasting systems, and can benefit to NB-LDPC codes to be a good alternative to the existing binary decoding codes in the current transmission systems.

The second contribution in this thesis concerns a new method to design an advanced high-spectral efficiency communication CM scheme. The main idea behind the new proposed method is to jointly optimize the NB-LDPC code and the M-QAM modulation, the advantage of using the same order for both (q=M). Such method is different to what is done subsequently, where the NB-LDPC codes and modulation are optimized in a disjoint way. The key motivation behind the proposed optimization method was the difference of values between Euclidean distance and Hamming distance in a case of non-binary modulation transmission ($M >> 2$). That implies that changing the modulation can impact the Euclidean distance between two codewords. The optimization method is concentrated on one single parity-check equation, and proposes the mapping and the d_c coefficients in GF(q) that maximize the Euclidean distance between codewords, and minimize the distance spectrum of the Euclidean distances, especially the lowest ones. We studied an example of application : a one half rate NB-LDPC code over GF(64) associated with a 64-QAM modulation. Through an exhaustive research we proposed to compare three different codes associated to distinct couples of mapping π and d_c non-null entries. The proposed codes aim to get out the influence of the joint choice of mapping and non-null entries. The first code uses the DVB-T2 Gray mapping and coefficients as proposed in the state-of-the-art, while the second one uses the same coefficients but with the worst mapping case. The third one is the result of the exhaustive research of the optimal combination of mapping and coefficients. To clear up the interest of the proposed idea, and to show the good agreement with the theoretical analysis and simulation are performed with the three considered codes. The results proved that a gain of 0.2 dB can be reached when using the optimal mapping

and NB-LDPC codes. It is important to mention that the gain is obtained without any additional complexity compared to existing schemes. We only have to modify the encoding matrix construction and modulation labeling, after performing only once, an exhaustive search of the best labeling and NB-LDPC code for the transmission CM scheme.

Additional work has been performed during this PhD thesis that has not been addressed in this manuscript. I participated in a work that aims to construct protograph based QC-NB-LDPC codes matrix. This work was done to introduce the proposed non-null coefficient in our joint parity-check matrix (PCM) and modulation optimization. In fact, the prototype matrix uses integer values that correspond to the right-rotations of the identity matrices that form the PCM structure. The determination of those integer values is a difficult problem. Based on an exhaustive examination of a simple prototype matrix, we propose a method that reduces the search space by defining topological classes of identical matrices through line and/or column permutations, and by satisfying the programmed constraints to list the exhaustive set of solutions for a given girth and a given expansion factor.

6.2 PERSPECTIVES

Concerning the SSD technique proposed optimization, the mutual information based optimization can be extended to other types of q-ary constellations like the q-APSK modulations, other Galois Fields orders, and other code rates. SSD can also be applied on high dimension transmission i.e. 4-dimension transmission. By considering the mutual information metric, we can find the most performing rotation angles for different SNR values. Then we can provide a detailed study of the SSD impact on a high dimension transmission in the context of the Rayleigh channel with and without erasure.

We can find out different perspectives of development of the joint optimization method of NB-LDPC codes and modulation. First, the proposed joint optimization can be treated for transmission with different rates and codeword lengths. Second, a generalization for other types of constellation is required. In spite of the fact that the M-QAM modulation has good characteristics in terms of regularity of distances between constellation points, other constellations i.e. PSK constellation can be a subject of study. Third, other non-binary codes can be considered in the proposed optimization method. In fact, NB-LDPC codes are the correcting codes considered in this thesis, but the proposed optimization method can be generalized to any non-binary code, e.g. non-binary turbo codes. Relationship between non-binary codes and modulation can be studied in terms of Euclidean distance of the codewords in order to enhance the performance results.

Finally, another perspective of development in the same context concerns the construction of PCM with d_v equal to 2. In fact, the couple of coefficients associated to each variable can impact the decoding performance, especially in the waterfall zone. To verify such assumption, some promising preliminary decoding curves are already obtained for very short PCM, which may lead to interesting results. This is done in the context of joint optimization of non-binary codes and modulation, and can offer an interesting development field in

future studies.

Bibliographie

[1] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *IEEE electronics letters*, Aug 1996.

[2] A. Abdmouleh, E. Boutillon, L. Conde-Canencia, C. A. Nour, and C. Douillard, "On signal space diversity for non binary coded modulation schemes," *IEEE International Conference on Telecommunications (ICT)*, May 2016.

[3] ——, "A new approach to optimise Non-Binary LDPC codes for coded modulations," *IEEE International Symposium on turbo Codes and Iterative Information Processing (ISTC)*, pp. 295–299, Sep 2016.

[4] E. Boutillon and A. Abdmouleh, "Methods and devices for generating optimized coded modulations," *N Demande : EP16306110.4, Déposant : UNIVERSITE DE BRETAGNE SUD*, Sep 2016.

[5] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge : Cambridge University Press, 2008.

[6] J.-P. Deschamps and G. D. Sutter, *Hardware implementation of finite field arithmetic*. New York : McGraw-Hill, 2009.

[7] J. M. Howie, *Fields and Galois Theory*. London : Springer Undergraduate Mathematics Series, 2007.

[8] A. Chamas, "Les codes LDPC non-binaire du nouvelle generation." Ph.D. dissertation, Université de Cergy-Pontoise, Dec. 2010, direction : D. Declercq, V. Heinrich.

[9] C. Poulliat, M. Fossorier, and D. Declercq, "Design of non binary LDPC codes using their binary image : algebraic properties," *IEEE International Symposium on Information Theory*, pp. 93–97, July 2006.

[10] S. Scholl, "GF Matrix Elements." [Online]. Available : http ://www.uni-kl.de/en/channel-codes/channel-codes-database/non-binary-ldpc/

[11] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding : Turbo-codes," *In Communications, 1993. ICC '93 Geneva. Technical Program, Conference Record, IEEE International Conference on,*, vol. 2, pp. 1064–1070, 1993.

[12] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, pp. 379–423 and 623–656, 1948.

[13] R. G. Gallager, *Low-density parity-check codes*. MIT, Cambridge, Mass : PhD thesis, 1963.

[14] D. J. C. MacKay, “Good error-correcting codes based on very sparse matrices,” *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, Aug 1999.

[15] “Digital Video Broadcasting (DVB) ; frame structure, channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2),” in *ETSI EN 302 755*, 2010-10.

[16] “Digital Video Broadcasting (DVB) ; Modulation Interface (C2-MI) for a second generation digital transmission system for cable systems (DVB-C2),” in *ETSI TS 103 287*, 2000.

[17] “Digital Video Broadcasting (DVB) ; Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2),” in *ETSI EN 302 307*, 2009.

[18] IEEE STANDARDS ASSOCIATION, *IEEE Standard for Air Interface for Broadband Wireless Access Systems*. 3 Park Avenue, New York, NY 10016-5997 USA : IEEE Computer Society, 2012.

[19] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, “Design of capacity approaching irregular low density parity check codes,” *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, 2001.

[20] J. Moreira, *Essentials of error-control coding*. West Sussex, England : John Wiley Sons, 2006.

[21] R. Tanner, “A recursive approach to low complexity codes,” *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[22] M. Davey and D. MacKay, “Low-density parity check codes over GF(q),” *IEEE Communications Letters*, vol. 2, no. 6, p. 165–167, 1998.

[23] R. G. Gallager, “Low density parity check codes,” *IEEE transaction on Information theory*, vol. IT-8, p. 21–28, Jan 1962.

[24] N. Wiberg, *Codes and decoding on general graphs*. Likoping University sweden : PhD thesis, 1996.

[25] C. Poulliat, M. Fossorier, and D. Declercq, “Design of regular $(2, d_c)$-LDPC codes over GF(q) using their binary images,” *IEEE Transactions on Communications*, vol. 56, pp. 1626–1635, Oct 2008.

[26] D. Declercq and M. Fossorier, “Decoding algorithms for non-binary LDPC codes over GF(q),” *IEEE Transactions on Communications*, vol. 55, no. 4, pp. 633–643, 2007.

[27] A. Voicila, D. Declercq, F. Verdier, M. Fossorier, and P. Urard, "Low complexity decoding algorithm for non-binary LDPC codes in high order fields," *IEEE Transactions on Communications*, vol. 58, no. 5, pp. 1–11, May 2010.

[28] H. Wymeersch, H. Steendam, and M. Moeneclaey, "Log-domain decoding of LDPC codes over GF(q)," *Communications, 2004 IEEE International Conference on*, vol. 2, pp. 772–776, Jun 2004.

[29] A. Voicila, "Décodage simplifie des codes LDPC non-binaires." Ph.D. dissertation, Universite de Cergy-Pontoise, sept. 2007, direction : D. Declercq, F. Verdier.

[30] D. Declercq, M. Colas, and G. Gelle, "Regular GF(2^q)-LDPC coded modulations for higher order QAM-AWGN channel," *Proc. ISITA. Parma, Italy*, Oct 2004.

[31] L. Ma, L. Wang, and J. Zhang, "Performance advantage of non-binary LDPC codes at high code rate under AWGN channel," *Communication Technology, 2006. ICCT '06. International Conference on*, Nov 2006.

[32] X. Jiand, Y. Yan, X. Xia, and M. H. Lee, "Application of non-binary LDPC codes based on euclidean geometries to MIMO systems," *Proceedings of Intern. conference on wireless comm. and Signal processing*, pp. 1–5, Nov 2009.

[33] H. Song and J. Cruz, "Reduced-complexity decoding of q-ary LDPC codes for magnetic recording," *IEEE Transactions on Magnetics*, vol. 39, no. 2, p. 1081–1087, 2003.

[34] X. Hu and E. Eleftheriou, "Binary representation of cycle tannergraph GF(2^q) codes," *IEEE International Conference on Communications*, Jun 2004.

[35] S. Pfletschinger, A. Mourad, E. Lopez, D. Declercq, and G. Bacci, "Performance evaluation of non-binary LDPC codes on wireless channels," *In Proceedings of ICT Mobile summit*, Jun 2009.

[36] M. Arabaci and I. B. Djordjevic, "Binary and nonbinary LDPC-coded modulations for generalized fading channels," *Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), 2011 10th International Conference on*, Oct 2011.

[37] G. Li, I. J. Fair, and W. Krzymien, "Density evolution for nonbinary LDPC codes under Gaussian approximation," *IEEE Transactions on Information Theory*, vol. 55, no. 3, pp. 997–1015, Mar 2009.

[38] M. Yang and W. Ryan, "Performance of Quasi-Cyclic LDPC codes in noise bursts on the EPR4 channel," *Proceedings of IEEE GLOBECOM*, pp. 2961–2965, Nov 2001.

[39] A. Morinoni, P. Savazzi, and S. Valle, "Efficient design of non-binary LDPC codes for magnetic recording channels, robust to error bursts," $5^{th} International Symposium on Turbo Codes and Related Topics, pp. 288 - 293, Sept 2008.$

[40] T. Chehade, L. Collin, P. Rostaing, O. Bazzi, and E. Radoi, “Adaptive minimum-distance based precoder for NB-LDPC coded MIMO transmission,” *IEEE Global Communications Conference (GLOBECOM)*, Dec 2015.

[41] G. Caire, G. Taricco, and E. Biglieri, “Bit-interleaved coded modulation,” *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 927–946, May 1998.

[42] E. Boutillon, L. Conde-Canencia, and A. Al-Ghouwayel, “Design of a GF(64)-LDPC decoder based on the EMS algorithm,” *IEEE Transactions on Circuits and Systems-I : Regular Papers*, vol. 60, no. 10, Oct. 2013.

[43] B. Sklar, “Rayleigh fading channels in mobile digital communication systems .i. characterization,” *IEEE Communications Magazine*, vol. 35, no. 4, pp. 90–100, July 1997.

[44] J. D. Parsons, *The mobile radio propagation channel*. New York, USA : John Wiley sons, 1992.

[45] S. Benedetto and E. Biglieri, *Principles of digital transmission with wireless applications*. norwell, MA, USA : Kluwer Academic Publishers, 1999.

[46] European Standard (Telecommunications series), “Digital Video Broadcasting (DVB) ; Framing structure, channel coding and modulation for digital terrestrial television,” in *ETSI EN 300 744*, 2009-01.

[47] IEEE STANDARDS ASSOCIATION, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 3 Park Avenue, New York, NY 10016-5997 USA : IEEE Computer Society, 2012.

[48] L. Cimini, “Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing,” *IEEE Transactions on Communications*, vol. 33, no. 7, pp. 665–675, Jul 1985.

[49] M. Mendicute, I. Sobrón, L. Martínez, and P. Ochandiano, *DVB-T2 : New Signal Processing Algorithms for a Challenging Digital Video Broadcasting Standard*. University of Mondragon, spain : Floriano De Rango, 2010.

[50] C. Abdel Nour and C. Douillard, “Improving BICM performance of QAM constellations for broadcasting applications,” *IEEE International Symposium on Turbo Codes and Related Topics*, pp. 55–60, Sept 2008.

[51] J. K. Cavers, “An analysis of pilot symbol assisted modulation for Rayleigh fading channels,” *IEEE Transactions on Vehicular Technology*, p. 686–693, Nov 1991.

[52] E. Boch, “High-capacity ethernet backhaul radio systems for advanced mobile data networks,” *IEEE Microwave Magazine*, vol. 10, no. 5, pp. 108–114, Aug 2009.

[53] S. Scholl, “Global mobile data traffic, 2015 to 2020.” [Online]. Available : http ://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[54] "Digital Video Broadcasting (DVB), Next Generation broadcasting system to handheld, physical layer specification (DVB-NGH)," in *DVB Document A160*, 2012.

[55] A. T. Le and K. Araki, "A group of modulation schemes for adaptive modulation," *IEEE International Conference on Communication Systems (ICCS)*, pp. 864–869, Nov 2008.

[56] D. A. Bryan, "QAM for terrestrial and cable transmission," *IEEE Transactions on Consumer Electronics*, vol. 41, pp. 383–391, Aug 1995.

[57] "Universal Mobile Telecommunications System (UMTS) ; High Speed Downlink Packet Access (HSDPA) ; Overall description ; Stage 2 (3GPP TS 25.308 version 10.6.0 Release 10)," in *ETSI TS 125 308*, 2012.

[58] "LTE ; Evolved Universal Terrestrial Radio Access (E-UTRA) ; User Equipment (UE) radio transmission and reception (3GPP TS 36.101 version 12.5.0 Release 12) ," in *ETSI TS 136 101*, 2014.

[59] "Data-over-cable Service Interface Specifications Radio Frequency Interface Specification," in *ETSI ES 201 488*, 2000.

[60] "Integrated Broadband Cable Telecommunication Networks (CABLE) ; cable equipment operations within its frequency band," in *ETSI TS 102 866*, 2014.

[61] T. Cover and J. Thomas, *Elements of Information Theory*. New York Wiley, 1991.

[62] E. Boutillon, Y. Eustache, P. Bomel, A. Haroune, and L. Conde-Canencia, "Performance measurement of davinci code by emulation," *INFSCO-ICT-216203 DA VINCI D6.2.3 v1.0*, p. 1–47, July 2011.

[63] R. M. Gray, *Entropy and Information Theory*. Springer-Verlag New York : Information Systems Laboratory Electrical Engineering Department Stanford University, 2013.

[64] E. Zehavi, "8-PSK trellis codes for a Rayleigh channel," *IEEE Transactions on Communications*, vol. 40, no. 3, p. 873–884, May 1992.

[65] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 927–946, May 1998.

[66] A. Goldsmith, *Wireless Communications*. New York, NY : Cambridge University Press, 2005.

[67] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Transactions on Information Theory*, vol. 28, no. 1, pp. 55–67, Jan 1982.

[68] IEEE 802, *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications : High-speed physical layer in the 5GHz band*. Tech. Rep : 802.11a-1999(R2003), 2009.

[69] I. Koffman and V. Roman, "Broadband wireless access solutions based on OFDM access in IEEE 802.16," *IEEE Communications Magazine*, vol. 40, no. 4, pp. 96–103, Apr 2002.

[70] J. Jalden, P. Fertl, and G. Matz, "On the generalized Mutual Information of BICM systems with approximate demodulation," *Information Theory (ITW 2010, Cairo), 2010 IEEE Information Theory Workshop on*, Jan 2010.

[71] D. MacKay, *Information Theory, Inference, and Learning Algorithms*. Cambridge University, UK : Cambridge University Press, 2003.

[72] J. Boutros and E. Viterbo, "Signal space diversity : A power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE TRANSACTIONS ON INFORMATION THEORY*, vol. 44, no. 4, pp. 1453–1467, July 1998.

[73] N. H. Tran, H. H. Nguyen, and T. Le-Ngoc, "Application of signal space diversity over multiplicative fading channels," *IEEE Signal Processing Letters*, vol. 16, no. 3, pp. 204–207, mar 2009.

[74] J. Yang, K. Wan, B. Geller, C. Abdel Nour, O. Rioul, and C. Douillard, "A low-complexity 2d signal space diversity solution for future broadcasting systems," *IEEE International Conference on Communications (ICC)*, pp. 2762–2767, Jun 2015.

[75] "DVB fact sheet. DVB-T2, 2^{nd} generation terrestrial," 2010-08.

[76] K. Boulle and J. C. Belfiore, "Modulation schemes designed for the Rayleigh fading channel," *presented at CISS 92, Princeton, NJ*, mar 1992.

[77] G. Taricco and E. Viterbo, "Performance of component interleaved signal sets for fading channels," *Electronics Letters*, vol. 32, no. 13, p. 1170–1172, April 1996.

[78] S. B. Slimane, "An improved PSK scheme for fading channels," *IEEE Transactions on Vehicular Technology*, vol. 47, no. 2, p. 703–710, May 1998.

[79] R. Schober, L. H.-J. Lampe, W. H. Gerstacker, and S. Pasupathy, "Modulation diversity for frequency-selective channels," *IEEE Transactions on Information Theory*, no. 9, p. 2268–2276, Sept 2003.

[80] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 502–518, mar 1996.

[81] C. Abdel Nour and C. Douillard, "Rotated QAM Constellations to improve BICM performance for DVB-T2," *IEEE International Symposium on Spread Spectrum Techniques and Applications*, pp. 354–359, Aug 2008.

[82] Z. Wu, Y. Shi, X. Chen, and Y. Zhu, "An efficient component-interleaved non-binary low density parity check code scheme on Rayleigh fading channels," *Communications and Networking (BlackSeaCom), 2014 IEEE International Black Sea Conference on*, May 2014.

[83] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "N*Nakagami : A novel stochastic model for cascaded fading channels," *IEEE Transactions on Communications*, vol. 55, no. 8, pp. 1453–1468, Aug 2007.

[84] Z. Wu and X. Gao, "An efficient MIMO scheme with signal space diversity for future mobile communications," *EURASIP Journal on Wireless Communications and Networking*, mar 2015.

[85] B. Sklar, "Rayleigh fading channels in mobile digital communication systems .i. characterization," *IEEE Communications Magazine*, vol. 35, no. 7, pp. 90 – 100, Jul 1997.

[86] ——, "Rayleigh fading channels in mobile digital communication systems part ii : Mitigation," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 148–155, Sept 1997.

[87] M. Li, C. Abdel Nour, C. Jégo, and C. Douillard, "Design of rotated QAM mapper/demapper for the DVB-T2 standard," *SiPS, Finland*, pp. 18–23, Oct 2009.

[88] W. Zhou and L. Zou, "Optimized rotations and labeling for non-binary LDPC coded modulation with signal space diversity," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, May 2009.

[89] S. Jeony, J. Lee, I. Kyung, and M.-S. Kim, "Component-interleaved Alamouti coding with rotated constellations for signal space diversity," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Mar 2010.

[90] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 8, pp. 1451–1458, Oct 1998.

[91] L. Polak and T. Kratochvil, "Performance of the rotated constellation in DVB-T2," *The Seventh International Conference on Digital Telecommunications ICDT*, pp. 84–87, 2012.

[92] S. Lin and D. J. Costello, *Error Control Coding*, Englewood Cliffs, NJ : Prentice-Hall, 2004.

[93] R. Krishnan, A. Graell i Amat, T. Eriksson, and G. Colavolpe, "Constellation optimization in the presence of strong phase noise," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5056–5066, Dec 2013.

[94] M. F. Barsoum, C. Jones, and M. Fitz, "Constellation design via capacity maximization," *IEEE International Symposium on Information Theory*, Jun 2007.

[95] U. Wachsmann, R. Fischer, and J. B. Huber, "Multilevel codes : theoretical concepts and practical design rules," *IEEE Transactions on Information Theory*, vol. 45, no. 5, p. 1361–1391, Jul 1999.

[96] J. Zoellner and N. Loghin, "Optimization of high-order non-uniform QAM constellations," *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting*, Jun 2013.

[97] B. Zhang and K. Kiasaleh, "Partially-coherent receivers architectures for QAM communications in the presence of non-constant phase estimation error," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 568–573, Feb 2009.

[98] R. Rios-Müller, J. Renaudier, L. Schmalen, and G. Charlet, “Joint coding rate and modulation format optimization for 8-QAM constellations using BICM Mutual Information,” *Optical Fiber Communications Conference and Exhibition (OFC)*, March 2015.

[99] F. Kayhan and G. Montorsi, “Constellation design for channels affected by phase noise,” *IEEE International Conference on Communications (ICC)*, pp. 3154–3158, Jun 2013.

[100] ——, “Joint signal-labeling optimization for pragmatic capacity under peak-power constraint,” *IEEE Global Telecommunications Conference*, Dec 2010.

[101] C. Marchand and E. Boutillon. (2015, Jul.) Lab-STICC website on Non-Binary LDPC. [Online]. Available : http ://www-labsticc.univ-ubs.fr/nb_ldpc/

[102] G. Ungerboeck, “Trellis-coded modulation with redundant signal sets part i : Introduction.” *IEEE Communications Magazine*, vol. 25, no. 2, pp. 5–11, 1987.

[103] G. Richter, A. Hof, and M. Bossert, “On the mapping of low-density parity-check codes for bit-interleaved coded modulation,” *IEEE International Symposium on Information Theory*, p. 2146–2150, Jun 2007.

[104] S.-Y. Chung, G. Forney, T. Richardson, and R. Urbanke, “On the design of low-density parity-check codes within 0.0045 db of the Shannon limit,” *IEEE Communications Letters*, vol. 5, no. 2, p. 58–60, July 2001.

[105] A. Bennatan and D. Burshtein, “On the application of LDPC codes to arbitrary discrete-memoryless channels,” *IEEE Transactions on Information Theory*, vol. 50, no. 3, pp. 417–438, Mar 2004.

[106] ——, “Design and analysis of non-binary LDPC codes for arbitrary discrete memoryless channels,” *IEEE Transactions on Information Theory*, vol. 52, pp. 549–583, Feb 2009.

[107] G. Li, I. J. Fair, and W. Krzymien, “Analysis of non-binary LDPC codes using Gaussian approximation,” *IEEE International Symp. on Inf. Theory, Yokohama, Japan*, July 2003.

[108] V. Rathi and R. Urbanke, “Density evolution, thresholds and the stability condition for non-binary LDPC codes,” *IEEE Proceedings*, vol. 152, no. 6, pp. 1069–1074, Dec 2005.

[109] D. MacKay. (2003, Aug) Optimizing sparse graph codes over GF(q).

[110] L. Zeng, L. Lan, Y. Y. Tai, S. Song, S. Lin, and K. Abdel-Ghaffar, “Constructions of non-binary Quasi-Cyclic LDPC codes : A finite field approach,” *Transactions Papers*, apr 2008.

[111] D. Kimura, F. Guilloud, and R. Pyndiah, “Construction of parity-check matrices for non-binary LDPC codes,” *4th International Symposium on Turbo Codes and Related Topics*, apr 2006.

[112] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," *Interplanetary Network Progress Report*, vol. 154, pp. 1–7, Aug 2003.

[113] R. Smarandache, D. G. Mitchell, and D. J. Costello, "Partially Quasi-Cyclic Protograph-based LDPC codes," *Communications (ICC), 2011 IEEE International Conference on*, Jun 2011.

[114] X. Zhang and Y. Tai, "Low-complexity transformed encoder architectures for Quasi-Cyclic non-binary LDPC codes over subfields," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1–10, Dec 2016.

[115] B. Amiri, J. A. F. Castro, and L. Dolecek, "Design of non-binary Quasi-Cyclic LDPC codes by absorbing set removal," *Information Theory Workshop (ITW), 2014 IEEE*, Dec 2014.

[116] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "A matrix-theoretic approach to the construction of non-binary Quasi-Cyclic LDPC codes," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1057–1068, Feb 2015.

[117] R. Smarandache and P. O. Vontobe, "Quasi-Cyclic ldpc codes : Influence of proto- and Tanner-graph structure on minimum Hamming distance Upper Bounds," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 585–607, Feb 2012.

[118] X. Hu, E. Eleftheriou, and D. Arnold, "Regular and irregular Progressive Edge-Growth Tanner graphs," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, Jan 2005.

[119] E. Boutillon and L. Conde-Canencia, "Simplified check node processing in non-binary LDPC decoders," in *6th International Symposium on Turbo Codes Iterative Information Processing*, Sept 2010, pp. 201–205.

[120] L. Conde-Canencia and E. Boutillon, "Application of bubble-check algorithm to non-binary LLR computation in QAM coded schemes," *Electronics Letters*, vol. 50, no. 25, pp. 1937–1938, 2014.