



**HAL**  
open science

# Contributions au codage correcteur d'erreurs et aux communications numériques : vers les communications à trames courtes

Frédéric Guilloud

## ► To cite this version:

Frédéric Guilloud. Contributions au codage correcteur d'erreurs et aux communications numériques : vers les communications à trames courtes. Traitement du signal et de l'image [eess.SP]. UBO Brest; IMT Atlantique, 2016. tel-02433823

**HAL Id: tel-02433823**

**<https://imt-atlantique.hal.science/tel-02433823>**

Submitted on 9 Jan 2020

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**Frédéric GUILLOUD**

frederic.guilloud@telecom-bretagne.eu

10 octobre 2016



**Contributions au codage correcteur d'erreurs  
et aux communications numériques :  
vers les communications à trames courtes**

Mémoire présenté en vue d'obtenir

**l'Habilitation à Diriger des Recherches (HDR)**

soutenu le 12 décembre 2016 devant le jury constitué de :

Jean-Claude Belfiore	Professeur, Telecom Paristech	Rapporteur
Antoine Berthet	Professeur, CentraleSupélec	Rapporteur
Jérôme Lacan	Professeur, ISAE	Rapporteur
Jean-Marie Gorce	Professeur, INSA Lyon	Président
Emanuel Radoi	Professeur, UBO	Examineur
Ramesh Pyndiah	Professeur, Telecom Bretagne	Examineur





# Table des matières

<b>Remerciements</b>	<b>1</b>
<b>Organisation du document</b>	<b>3</b>
<b>I Parcours professionnel</b>	<b>5</b>
<b>1 Curriculum vitae</b>	<b>7</b>
1.1 Etat civil . . . . .	7
1.2 Titres universitaires . . . . .	8
1.3 Expérience professionnelle . . . . .	8
<b>2 Activités d’enseignement</b>	<b>11</b>
2.1 Enseignements dispensés (programme Télécom Bretagne) . . . . .	11
2.1.1 Charge en 2015-2016 . . . . .	11
2.1.2 Détails des enseignements les plus significatifs . . . . .	11
2.2 Coordination . . . . .	14
2.3 Implication dans la préparation des nouveaux enseignements (IMT Atlantique) . . . . .	15
<b>II Activités de recherche 2005-2016</b>	<b>17</b>
<b>3 Codage correcteur d’erreurs</b>	<b>21</b>
3.1 Introduction . . . . .	21
3.2 Codes LDPC non-binaires . . . . .	22
3.2.1 Définition . . . . .	22
3.2.2 Décodage et séquençement . . . . .	22
3.2.3 Construction . . . . .	24
3.2.4 Conclusions . . . . .	28
3.3 Codes Reed-Solomon . . . . .	28
3.3.1 Définition et décodage . . . . .	28
3.3.2 Décodage à entrée souple des codes RS . . . . .	30
3.3.3 Génération de vecteurs de tests basée sur les statistiques d’ordre . . . . .	31
3.3.4 Conditions d’optimalité . . . . .	32
3.3.5 Conclusions . . . . .	34
3.4 Réseaux de points . . . . .	34
3.4.1 Définitions . . . . .	35
3.4.2 Comparaison aux constellations QAM . . . . .	37
3.4.3 Réseaux de points et codage correcteur d’erreurs . . . . .	39
3.4.4 Constructions multi-niveaux . . . . .	43
3.4.5 Conclusions . . . . .	49
3.5 Conclusions . . . . .	50

3.6	Bibliographie . . . . .	51
<b>4</b>	<b>Communications sans fils et réduction de consommation</b>	<b>57</b>
4.1	Introduction . . . . .	57
4.2	Réduction de PAPR dans les modulations OFDM . . . . .	58
4.2.1	Etat de l'art . . . . .	58
4.2.2	Technique SLM et critère de sélection . . . . .	62
4.2.3	Technique SLM basée sur le codage correcteur d'erreurs . . . . .	64
4.2.4	Conclusion . . . . .	66
4.3	Modulations CPM pour la télémesure . . . . .	67
4.3.1	Introduction . . . . .	68
4.3.2	Réduction de complexité . . . . .	71
4.3.3	Augmentation de la robustesse . . . . .	73
4.3.4	Accès multiple . . . . .	78
4.4	Conclusion . . . . .	79
4.5	Bibliographie . . . . .	81
<b>III</b>	<b>Perspectives et conclusions</b>	<b>87</b>
<b>5</b>	<b>Perspectives : trames courtes</b>	<b>89</b>
5.1	Contexte . . . . .	89
5.2	Enjeux . . . . .	90
5.3	Mise en forme . . . . .	92
5.3.1	Distribution non uniforme des symboles . . . . .	92
5.3.2	Considérations pratiques . . . . .	95
5.3.3	Propositions de solutions . . . . .	97
5.3.4	Conclusions . . . . .	98
5.4	Accès multiple . . . . .	98
5.4.1	Introduction . . . . .	98
5.4.2	Détection parcimonieuse . . . . .	100
5.4.3	Conclusions . . . . .	103
5.5	Conclusion . . . . .	103
5.6	Bibliographie . . . . .	104
	<b>Conclusions</b>	<b>109</b>
<b>IV</b>	<b>Annexe</b>	<b>113</b>
<b>A</b>	<b>Détails des activités de recherche</b>	<b>115</b>
A.1	Activité contractuelle . . . . .	115
A.2	Encadrement . . . . .	120
A.2.1	Doctorants . . . . .	120
A.2.2	Post-doctorants et ingénieurs de recherche . . . . .	124
A.2.3	Stagiaires . . . . .	124
A.3	Collaborations . . . . .	126
A.4	Publications . . . . .	127
A.4.1	Articles de revues internationales avec comité de lecture . . . . .	128
A.4.2	Conférences avec comité de lecture . . . . .	129
A.4.3	Présentations invitées . . . . .	131
A.4.4	Brevets . . . . .	131
A.4.5	Chapitre de livre . . . . .	131

---

A.4.6	Soumissions en cours . . . . .	131
-------	--------------------------------	-----



# Remerciements

Je tiens à remercier vivement Jean-Marie Gorce pour avoir accepté de présider mon jury de HDR, ainsi que Jean-Claude Belfiore, Antoine Berthet et Jérôme Lacan pour avoir accepté de rapporter mon travail. Un grand merci également à Emanuel Radoi pour sa participation à ce jury et pour toutes les démarches qu'il a assurées pour me permettre de soumettre mon dossier de qualification à temps. Je remercie chaleureusement Ramesh Pyndiah de sa participation à ce jury, et également de m'avoir accueilli au sein du département Signal et Communications de Télécom Bretagne qu'il dirigeait à mon arrivée.

Les contributions rassemblées dans ce manuscrit proviennent en grande partie de travaux réalisés en collaboration avec des doctorants (Andrzej Kabat, Hyunseuk Yoo, Sanae El Hassani, Jia Dong, Malek Messai, Carole Al Beschlawi, Jialong Duan, Yupeng Tai, The Phuong Nguyen), des stagiaires (Amin Zribi, Nizar Trabelsi, Hayet Msilini, Tarek Chehade, Clément Acquitter, Amine Semma, Mohamed Abdelli, Minh On Vu Ngoc, Vinh Hoang Son Le) et des ingénieurs de recherche ou post-doctorants (Mohamed Et Tolba, Haïfa Fares, Vincent Herbert, Malek Messai, Zeina Mheich) que j'ai eu (ou que j'ai encore) l'honneur d'encadrer ou de co-encadrer. Merci à toutes et à tous pour vos efforts et votre enthousiasme !

Je remercie également chaleureusement tous les membres du département Signal et Communication, ainsi que tous les membres de l'équipe COM du Lab-STICC, pour l'excellente ambiance de travail à laquelle ils contribuent. Je remercie tout particulièrement Raphaël Le Bidan, dont j'ai eu le plaisir de partager le bureau pendant une dizaine d'années et qui m'a transmis une partie de sa passion pour le codage correcteur d'erreur, ainsi que Karine Amis dont je partage à présent le bureau : merci pour ta gentillesse et ta rigueur mathématique si stimulante !

Enfin, je remercie mon épouse Raphaëlle qui a relu chacune des phrases de ce manuscrit, en suggérant des modifications qui en ont grandement amélioré la qualité. Merci également pour ton écoute patiente des répétitions de soutenance et pour tes propositions toujours très pertinentes. Je n'aurais pas pu faire tout cela sans ton aide !





# Organisation du document

Ce mémoire d'Habilitation à Diriger des Recherches présente la synthèse de mon travail de recherche et d'encadrement durant les douze dernières années (2004-2016) que j'ai passées à Télécom Bretagne dans le département Signal & Communications dirigé successivement par les professeurs Ramesh Pyndiah puis Samir Saoudi, et simultanément au sein de l'équipe COM du laboratoire Lab-STICC (Lab-STICC/CACS/COM, UMR 6285). Il est organisée en 3 parties et une annexe.

Dans la première partie, je présente mes études et mon parcours professionnel, et je résume mes activités d'enseignement et de recherche.

Dans la deuxième partie, je présente mes deux thématiques de recherche principales : la première rassemble mes contributions dans le domaine du codage correcteur d'erreurs et la seconde rassemble mes contributions dans le domaine de la réduction de la consommation d'énergie liée à l'amplificateur de puissance.

Dans la troisième partie, je présente la thématique de recherche que je souhaite développer dans les années à venir et que j'intitule "les communications sans fil à trames courtes". Cette troisième partie se termine avec la conclusion.

En annexe de ce manuscrit, je présente les détails chiffrés de mes activités de recherche en matière de projets, d'encadrements et de publications.



## **Première partie**

# **Parcours professionnel**



# Chapitre 1

## Curriculum vitae

### 1.1 Etat civil

Frédéric GUILLOUD

Né à Tassin-la-demi-Lune (Rhône) le 18 janvier 1975

Marié, deux enfants

Maître de conférences

IMT Atlantique, Lab-STICC, UBL

Département Signal & Communications

Technopôle Brest-Iroise - CS 83818

29 238 Brest Cedex 3 - France

Qualifié aux fonctions de professeur des universités de la section CNU 63

Numéro de la qualification : 17163303489

Téléphone : 02 29 00 13 56

Télécopie : 02 29 00 10 12

E-mail : frederic.guilloud@imt-atlantique.fr

Page internet : <http://www.imt-atlantique.fr/fr/personne/frederic-guilloud>

<http://perso.telecom-bretagne.eu/fredericguilloud>

Google Scholar :

[https://scholar.google.fr/citations?hl=fr&user=YA\\_vE-4AAAAJ](https://scholar.google.fr/citations?hl=fr&user=YA_vE-4AAAAJ)

## 1.2 Titres universitaires

**2017** : Qualification aux fonctions de professeur des universités de la section CNU 63 (Numéro 17163303489)

**2016** : Habilitation à Diriger des Recherches (HDR) de L'Université de Bretagne Occidentale (UBO) intitulée : “*Contributions au codage correcteur d'erreurs et aux communications numériques : vers les communications à trames courtes*”, soutenue le 12 décembre 2016 devant le jury composé par :

Jean-Claude Belfiore	Rapporteur
Antoine Berthet	Rapporteur
Jérôme Lacan	Rapporteur
Jean-Marie Gorce	Président
Emanuel Radoi	Examineur
Ramesh Pyndiah	Examineur

**2004** : Thèse de doctorat au département COMELEC (Communications et Électronique) de Télécom ParisTech (ex École Nationale Supérieure des Télécommunications de Paris), financée par le projet européen SPRING, sur le thème : “*Architecture générique de décodeurs de codes LDPC*”, soutenue le 02 Juillet 2004 devant le jury composé par :

Michel Jézéquel	Président du jury
Marc Fossorier	Rapporteur
Jean-Didier Legat	Rapporteur
François Barbara	Examineur
David Declercq	Examineur
Emmanuel Boutillon	Directeur de thèse
Jean-Luc Danger	Directeur de thèse

obtenue avec la mention “*Très Honorable*”

**2000** : Diplôme d'études approfondies (DEA) "Systèmes de Transmission Numérique", de Télécom ParisTech / Université Pierre et Marie Curie (Paris 6).

**1999** : Reçu à l'agrégation de Génie Électrique (option A).

**1998** : Admission à l'École Normale Supérieure de Cachan.

**1998** : Diplôme d'ingénieur ENSEA (École Nationale Supérieure de l'Électronique et de ses Applications), option Mesure et Instrumentation.

**1993** : Baccalauréat Série E.

## 1.3 Expérience professionnelle

— **Jan.–Juin 2017** : Séjour d'études au LNT (Institute for Communications Engineering) de l'université technique de Munich (TUM), Allemagne.

- 
- **Depuis Sept. 2004** : Maître de conférences au département Signal & Communications de l'IMT Atlantique.
  - **Oct. 2000–Août 2004** : Doctorant au département COMELEC de Télécom ParisTech dans le cadre du projet européen SPRING :
    - 2000–2001 : Recherche dans le domaine de la télémétrie en association avec l'entreprise Schlumberger.
    - 2001–2004 : Recherche dans le domaine du codage correcteur d'erreur (LDPC) : algorithme sous-optimal de décodage, et implémentation sur FPGA.
  - **Sept. 2000–Août 2003** : Allocataire Moniteur Normalien à l'Université Pierre et Marie Curie (Paris VI), enseignements en Électronique, Théorie de l'Information, Traitement du signal, à des élèves en prépa-CAPES, Licence et DEUST.
  - **Avril–Sept. 2000** : Stage de fin d'étude de DEA à Thalès Communication (ex. Thomson-CSF Communication), Gennevilliers, intitulé : "*Élaboration d'une forme d'onde à haute efficacité spectrale basée sur de l'OFDM filtré*", dans le cadre du projet RNRT THESEE.
  - **Fév.–Juil. 1998** : Stage ingénieur au Laboratoire d'Optique Appliquée, École Polytechnique / ENSTA, Palaiseau, intitulé "*Optimisation graphique de mesures en spectroscopie laser femtoseconde.*"





## Chapitre 2

# Activités d'enseignement

## 2.1 Enseignements dispensés (programme Télécom Bretagne)

### 2.1.1 Charge en 2015-2016

Depuis mon recrutement, j'ai assuré divers enseignements axés principalement sur les probabilités, le codage correcteur d'erreurs et les communications numériques, ainsi qu'une activité régulière de tutorat.

Je suis impliqué auprès des différents profils d'élèves : élèves de formation initiale (FIG), élèves en alternance (FIP), élèves étrangers en *master of science* (MSC). J'interviens également auprès des professionnels à travers les formations continues (FC).

Mon activité d'enseignement est répartie suivant des enseignements de type face à face ou de type apprentissage par projet. Elle comporte également des responsabilités de module ou d'UV ainsi que du tutorat d'élèves. L'apprentissage sous forme de projets tient une place significative dans les enseignements dispensés aux élèves. Cette diversité de modalité de formation augmente leur motivation mais elle permet également de consolider leurs acquis en faisant varier les contextes des problèmes dont ils relèvent. Chacun des semestres de la scolarité des FIG (notés S1 à S5) est concerné par ce type d'apprentissage.

Le tableau 2.1 présente la charge annuelle correspondant aux différentes activités d'enseignement sur l'année scolaire 2015-2016, l'année scolaire 2016-2017 n'étant pas représentative du fait de mon séjour d'étude de 6 mois en Allemagne entre janvier et juin 2017. Les plans de charges détaillés des 3 dernières années scolaires sont disponibles au chapitre ??, page ??.

### 2.1.2 Détails des enseignements les plus significatifs

Dans cette section, je présente plus en détails le contenu des enseignements les plus significatifs en terme de nombre d'heures en face-à-face.

- [UVTC-101B] : Probabilité (24 heures), 1ère année du cycle de formation d'ingénieur généraliste.

Ce module privilégie un apprentissage progressif des notions élémentaires (espace probabilisé, variables et vecteurs aléatoires, lois discrètes et absolument continues, fonction de répartition et densité, moments, conditionnement, indépendance, ...) et des techniques de calcul que l'ingénieur doit maîtriser. Les objectifs pédagogiques sont :

TABLE 2.1 – Charge annuelle des activités d'enseignement sur l'année 2015-2016.

Matière	Niveau	Nombre d'heures
Face à Face		
FIP MGP321 : projet de développement	FIP 3eme année	6
FIP RT323 : codage	FIP 2ème année	21
F4B301A : codage	FIG 3ème année	7,5
MTS 203 : communication numériques	FIG 1ère ou 2ème année	25,5
Mineure Recherche : analogie	FIG 2ème année	7,5
TC101B : probabilités	FIG 1ère année	24
FIP MTS213 : communications numériques	FIP 2ème année	4,5
F1B301A : communications spatiales	FIG 3ème année	6
MTS 423/443 : codage	FIG 1ère ou 2ème année	15
PEPS DEC A : projet découverte	FIG 1ère année	31
ATE 205 : communications numériques	FIG 1ère ou 2ème année	12
MTSE101 : processus stochastiques	Master of science 2ème année	3
Encadrement		
FIP MGP321 : projet de développement	FIP 3eme année	6
F4BP01B : projet de développement	FIG 3ème année	2
TUT FIP : tutorat	FIP 1ère, 2ème et 3ème année	10
Coordination		
UV FIP MGP320 : projet de développement	FIP 3eme année	6,25
UV F4B301 : codage	FIG 3ème année	6,25
FIP RT323 : codage	FIP 2ème année	2,5
MTS 203 : communications numériques	FIG 1ère ou 2ème année	2,5

- Connaître les résultats élémentaires du calcul des probabilités.
- Être capable d'appliquer ces résultats élémentaires à des expériences aléatoires usuelles.
- Être capable de discuter les résultats des calculs et des simulations dérivés des modèles et des expériences aléatoires usuels.
- **[MTS-203 P]** : Communications numériques (25.5 heures), 2ème et 4ème semestre du cycle de formation d'ingénieur généraliste.

Dans ce module, on se propose de définir les éléments de base constituant une chaîne de communication numérique ainsi que l'optimisation des paramètres de réception pour garantir une transmission fiable. Les objectifs pédagogiques sont :

- Acquérir les principes de base de fonctionnement d'une chaîne de communications numériques
- Définir un code en bloc, coder un message à partir d'une matrice génératrice, calculer les paramètres du code, appliquer le décodage par syndrome
- Définir un code convolutif, coder un message à partir des polynômes générateurs, calculer les paramètres, appliquer un décodage de Viterbi ferme
- Définir les paramètres caractéristiques (débit, rapidité de modulation, rendement de codage, énergie symbole,...)
- Comprendre le rôle et calculer les signaux en sortie des dispositifs de réception, exprimer

et appliquer les critères de Nyquist

- **[PEPS DEC A]** Le projet « Découverte » (31 heures), 1ère année du cycle de formation d'ingénieur généraliste.

Ce projet a pour but de former les étudiants au travail en groupe, de poser les bases de présentation orale, de conduire un premier développement intégrant une plateforme matérielle et logicielle fonctionnelle à partir d'un cahier des charges précis. A l'issue du projet, les étudiants seront capables d'expliquer les concepts scientifiques et techniques mis en œuvre dans la réalisation.

Le projet est découpé en trois phases. La phase 1 se déroule en septembre et octobre. Elle permet par des mises en situation courtes et variées d'acquérir rapidement une première expérience du travail en groupe et de présentation orale. Les phases 2 et 3 permettent aux étudiants de participer à une compétition de mini-véhicules pilotés par un smartphone en janvier. La phase 2 se déroule en novembre et décembre. Elle met l'étudiant en situation de travail en petit groupe (typiquement par trois) sur une réalisation soit matérielle de type arduino (<https://www.arduino.cc/>), soit logicielle de type application smartphone.

Je participe régulièrement à la phase 1 (course d'orientation, présentations de type Pecha-Kucha) et à la phase 2 (réalisation matérielle Arduino).

Le projet Découverte repose sur un apprentissage par pédagogie active. L'étudiant est ici acteur de son apprentissage au sein de son groupe. La situation problème est un prétexte à l'acquisition de connaissances et de capacités nouvelles. Le projet Découverte débute la série de projets semestriels visant à vous faire progresser sur un ensemble de compétences nécessaires à la réalisation de projets. Ce type de formation constitue un changement par rapport aux apprentissages de type transmissif des classes préparatoires aux grandes écoles, et vise à vous amener vers plus d'initiative et d'autonomie. Les objectifs pédagogiques sont :

- Construire une plateforme matérielle et logicielle fonctionnelle à partir d'un cahier des charges précis et en réutilisant des briques existantes.
  - Utiliser des outils fondamentaux du développement logiciel
  - Expliquer des concepts scientifiques et techniques mis en œuvre dans la plateforme
  - Appliquer des méthodes de recherche documentaire pour exploiter les ressources nécessaires à la réalisation du projet
  - Réaliser des synthèses de travaux
  - Utiliser un cahier des charges fourni pour développer une solution technique
  - Prendre du recul sur son expérience de travail technique en équipe
  - Reconnaître les mécanismes d'apprentissage au sein d'un groupe
  - Animer un groupe de travail
  - Travailler de manière structurée au sein d'un groupe de travail
  - Appliquer les fondamentaux pour la bonne prise de parole en public avec un support visuel
- **[FIP RT323]** Codage correcteur d'erreurs (21 heures), 3ème année du cycle de formation d'ingénieur en partenariat.

Le codage de canal, appelé aussi codage détecteur et/ou correcteur d'erreurs est une fonction spécifique des transmissions numériques, qui permet d'améliorer la qualité d'une transmission. Cette technique est utilisée dans la quasi-totalité des systèmes de télécommunications

TABLE 2.2 – Responsabilité d'enseignement (2015/2016)

Nom	type	Nombre d'intervenants
FIG MTS 203P (com. num.)	Module	2
FIP RT323 (codage)	Module	2
FIP MGP320 (projet S5)	UV	15-20
FIG F4B301 (codage)	UV	10

et notamment, dans les systèmes de radiocommunications avec les mobiles pour lesquels le milieu de transmission est généralement hostile (présence de trajets multiples par exemple). Dans le cadre de ce module, nous présentons tout d'abord les deux principales familles de codes correcteurs d'erreurs : les codes en blocs et les codes convolutifs. Pour chaque famille, nous décrivons l'encodeur, discutons la réalisation du décodeur optimal, étudions leurs performances sur différents modèles de canaux afin d'identifier ce qui définit un « bon » code, et discutons de leur utilisation dans les normes. Un TP et 3 PC permettent d'approfondir ces notions et d'apprendre à évaluer l'apport du codage correcteur dans une communication numérique. Nous nous penchons ensuite sur les systèmes avec voie de retour entre l'émetteur et le récepteur. Le récepteur peut ainsi demander la retransmission de certains paquets détectés en erreurs. C'est le principe de l'ARQ (automatic repeat request), une technique fréquemment mise en œuvre dans les systèmes radio. Nous abordons ensuite la combinaison de la retransmission avec le codage correcteur (ARQ hybride). Nous terminons avec une présentation des deux principales techniques modernes de codage correcteur d'erreur : les turbo codes et les codes LDPC.

Les objectifs pédagogiques sont :

- Etre capable de caractériser l'apport du codage correcteur d'erreur dans une chaîne de communication numérique
- Etre capable de spécifier un système de codage en fonction d'un cahier des charges (débit utile, taux d'erreur cible, bande, point de fonctionnement)
- Connaître les principales techniques de retransmission Se familiariser avec les techniques modernes de codage correcteur (turbo codes et codes LDPC)
- Comprendre le principe du codage en blocs et du codage convolutif
- Connaître les schémas d'encodage et les décodeurs associés

## 2.2 Coordination

Le tableau 2.2 donne la liste des modules et UV dont j'ai été responsable durant l'année scolaire 2015-2016, associé avec le nombre d'intervenants dans l'enseignement concerné. Je suis également le correspondant Télécom Evolution pour les activités de formation continue du département Signal & Communications.

Depuis la rentrée 2017, je suis responsable également du domaine Science et Ingénierie des Télécom (SIT) qui est spécifique à la formation d'ingénieur en partenariat.

## 2.3 Implication dans la préparation des nouveaux enseignements (IMT Atlantique)

Depuis 2014, je participe également à la réforme des enseignements afin de préparer les enseignements de l'IMT Atlantique Bretagne-Pays de la Loire, issue de la fusion entre Télécom Bretagne et l'école des Mines de Nantes. A ce titre, j'ai contribué à faire évoluer certains enseignements où je suis impliqué :

- **[PEPS DEC A]** participation à la phase 1 et à la phase 2 (robots mobiles pilotés par carte arduino).
- **[UVTC-101B]** Refonte du cours de probabilité pour s'adapter aux nouveaux programmes de classes préparatoires, ajouts de travaux pratiques et augmentation du nombre de séances en effectif réduit (baisse du nombre de cours en amphithéâtre), ajout d'un mini-projet sur le thème du radar à réaliser par groupe sur 4 séances dont l'objectif est d'illustrer l'intérêt des probabilités en s'appuyant sur les notions vues au cours des séances précédentes. Travail en collaboration avec le CAPE des Mines de Nantes (2015).

Je participe également à la conception d'Unités d'Enseignement (UE) du futur tronc commun :

- UE Probabilité / Statistique
- UE Traitement du signal, Analyse et Automatique

ainsi qu'à la conception de la Thématique d'Approfondissement (TAF) intitulée "Ingénierie des systèmes de communications", et plus particulièrement aux :

- UE coeur numéro 2 : Communications Numériques
- UE coeur numéro 3 : Architectures et Ingénierie des systèmes de transmission
- UE élective : Codage de l'information



## **Deuxième partie**

# **Activités de recherche 2005-2016**





# Introduction

Cette partie est consacrée à la présentation de mes activités de recherche menées depuis septembre 2005 au sein du département Signal & Communications de Télécom Bretagne, et simultanément au sein du pôle Communications, Architecture et Circuits (CACS) du laboratoire des Sciences et Techniques de l'Information, Communication et Connaissance (Lab-STICC). Le pôle CACS possède des compétences dans trois grands domaines : communications numériques, conception de systèmes numériques matériels et systèmes logiciels embarqués. Cette triple compétence lui permet à la fois de concevoir des nouveaux algorithmes, d'en proposer des mises en œuvre originales et de développer des outils et des méthodologies de conception de systèmes numériques. Au sein de ce pôle, j'effectue principalement ma recherche dans l'équipe thématique Communications (COM), axée sur les thématiques de recherche suivantes : le codage correcteur d'erreurs et les communications sans fil. Ces thématiques sont développées respectivement dans les chapitres 3 et 4 qui sont écrits de façon à permettre au lecteur de cerner les différentes contributions de mes travaux. Je renvoie le lecteur vers les thèses ou les articles décrivant plus en détails les sujets présentés dans ces chapitres.

Dans le premier chapitre, j'aborde certains aspects du codage correcteur d'erreurs. Je commence à présenter des travaux qui font suite à mon travail de thèse sur l'architecture de décodage des codes de parités à faible densité (codes LDPC, pour *Low Density Parity Check codes*) en abordant des contributions relatives aux codes LDPC non-binaires. Je poursuis par l'étude du décodage souple des codes Reed-Solomon. J'ai voulu ensuite m'intéresser aux pendants du codage correcteur d'erreurs dans l'espace euclidien que sont les réseaux de points et que l'on peut considérer comme des modulations codées particulières.

Dans le deuxième chapitre, je présente les activités que j'ai menées dans le domaine des communications sans fil : la réduction de la consommation d'énergie liée à la consommation de l'amplificateur, en commençant par la réduction de puissance crête dans les modulations multi-porteuses, puis en proposant des solutions apportant une plus grande robustesse aux modulation à phase continue.



## Chapitre 3

# Codage correcteur d'erreurs

### 3.1 Introduction

Lorsque l'on parle de système de transmission numérique, il est souvent fait référence à la *chaîne* de transmission numérique, en considérant tous les traitements subis par l'information à transmettre comme une succession de fonctionnalités élémentaires plus ou moins indépendantes. Dans cette chaîne, le codage correcteur d'erreurs est devenu un élément essentiel depuis sa naissance en 1950 avec le code de Hamming à la suite des travaux de Claude Shannon sur la capacité des canaux de communication, et notamment celle du canal gaussien. De nombreux autres codes ont été publiés au cours des décennies qui ont suivi (codes convolutifs, codes algébriques), améliorant notamment les performances des transmissions spatiales. Avec l'invention en 1993 des turbocodes convolutifs par C. Berrou et al., les premiers décodeurs efficaces de codes concaténés font leur apparition. Ils sont suivis en 1994 par les turbocodes en blocs proposés par R. Pyndiah et al., puis par la redécouverte par D. MacKay et R. Neal des codes à faible densité : les codes LDPC (Low Density Parity Check codes), inventés par Robert Gallager en 1962.

Ce chapitre commence par les codes LDPC non-binaires. Après avoir exposé les notations et les principales définitions concernant les LDPC non-binaires, j'aborde l'algorithme de décodage par propagation de croyance et les analyses de ses séquencements. Je termine par la présentation des résultats de recherche obtenus pendant la collaboration avec Dai Kimura (Fujitsu, Yokohama) portant sur la construction des codes LDPC non-binaires et notamment sur l'optimisation des valeurs non-binaires de la matrice de contrôle de parité.

Je présente ensuite en section 3.3 les contributions relatives au décodage à entrées souples des codes Reed-Solomon (RS). Je m'intéresse notamment aux algorithmes de décodage où un ensemble de bits indépendants parmi les plus fiables est ré-encodé. La performance de tels algorithmes étant fortement conditionnée par les conditions d'optimalité, je présente à la fin de cette section une synthèse de ces conditions.

La section 3.4 est consacrée à l'étude du codage par réseau de points, et notamment à la question de la comparaison de schémas de communications basés sur l'utilisation de codes défini à partir de réseaux de points. Cet objectif passe par une bonne compréhension de l'encodage et du décodage des réseaux de points. J'aborde cet aspect sous une forme générique dans un premier temps, mais qui reste limitée à des réseaux de petites dimensions à cause de la complexité des encodeurs et des décodeurs utilisés. L'augmentation des dimensions, souhaitable pour améliorer les performances du

codage, est rendue possible en utilisant certaines construction de réseaux de points à base de codes correcteurs d'erreurs. Je me focalise alors sur les codes binaires et les constructions multi-niveaux.

## 3.2 Codes LDPC non-binaires

A la suite de mes travaux de thèse entre 2000 et 2004 qui portaient sur le décodage des codes LDPC binaires, j'ai travaillé sur les codes LDPC non-binaires en collaboration avec Daï Kimura, ingénieur de recherche chez Fujitsu-Laboratories, qui a passé une année en 2005 dans le département Signal & Communication [1, 2, 3, 4]. Ce travail s'est poursuivi avec la thèse de Sanae El Hassani effectuée entre 2008 et 2011 chez Orange Labs [5]. Une nouvelle étude sur les codes LDPC non-binaires est en cours pour des codes de petite longueur. Cette étude a été sélectionnée par le centre de recherche de Huawei France suite à leur appel à projet ICT, et permet de financer le post-doc de Zeina Mheich.

### 3.2.1 Définition

Les codes LDPC (low-Density Parity-Check) forment une grande famille de codes correcteurs en bloc. Ils ont été inventés en 1962 par Robert Gallager [6] puis redécouverts par David MacKay et Radford Neal en 1995 [7]. Les codes LDPC ont la propriété d'avoir une matrice de contrôle de parité  $\mathbf{H}$  très creuse, c'est à dire qu'elle contient une très grande proportion de valeurs nulles. On peut définir la matrice de contrôle de parité d'un code LDPC par le fait que la proportion de valeurs non-nulle tende vers 0 lorsque la longueur du code tend vers l'infini.

Dès leur découverte et leur redécouverte, les codes LDPC ont été proposés dans leur version binaire et non-binaire. On peut décrire un code LDPC de longueur  $N$  et de rendement  $R$  par :

$$\mathcal{C}_{\text{LDPC}} = \{ \mathbf{c} \in (\text{GF}(2^m))^N \mid \mathbf{H}\mathbf{c}^t = \mathbf{0} \}$$

où  $\mathbf{H} = \{h_{i,j}\}$  est une matrice creuse de  $N$  colonnes à valeurs dans  $\text{GF}(2^m)$  et de rang

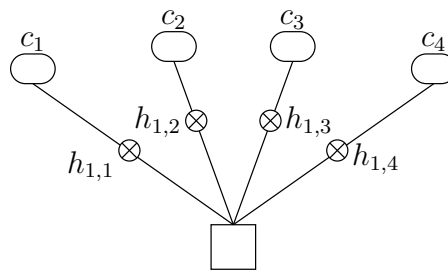
$$\text{rank}(\mathbf{H}) = N(1 - R) = N - K$$

,  $K$  étant la dimension du code. On supposera par la suite les matrices  $\mathbf{H}$  de rang plein et donc ayant  $N - K$  lignes. La définition proposée ici est restreinte aux corps finis de caractéristique 2 à  $2^m$  éléments, notés  $\text{GF}(2^m)$ , même si elle est généralisable à d'autres espaces algébriques comme les anneaux ou même les groupes [8, 9, 10].

### 3.2.2 Décodage et séquençement

#### Décodage des codes LDPC

Le décodage des codes LDPC se fait par des algorithmes itératifs sur le graphe ayant  $N$  nœuds dits nœuds variables représentant les  $N$  symboles d'un mot de code, et reliés à  $N - K$  nœuds dit contrainte ou parité représentant les équations de parité de la matrice  $\mathbf{H}$ . Le terme équation de parité est à prendre au sens large, c'est à dire dans des corps  $\text{GF}(2^m)$ . Il y a une équivalence entre la matrice



$$h_{1,1}c_1 + h_{1,2}c_2 + h_{1,3}c_3 + h_{1,4}c_4 = 0$$

FIGURE 3.1 – Une équation de parité ( $N = 4, K = 3$ ) dans  $\text{GF}(2^m)$  et sa représentation graphique équivalente où un mot de code  $\mathbf{c} = \{c_i\}_{1 \leq i \leq N}$ .

de contrôle de parité et le graphe, chaque connexion entre nœuds correspondant à une valeur non-nulle de la matrice (voir l'illustration dans le cas d'une équation de parité de degré 4 sur la figure 3.1).

Le décodage des codes LDPC par propagation de croyance (BP) n'est optimal (au sens de la maximisation a-posteriori des symboles reçus) que si le graphe du code n'a pas de cycle. Cependant pour des tailles finies, les bons codes ont des cycles [11] et l'algorithme BP n'est plus optimal, mais il reste performant si les cycles sont suffisamment longs.

La complexité de décodage est proportionnelle au nombre de valeurs non-nulles de la matrice de contrôle de parité, ce qui permet d'atteindre une complexité évoluant de manière linéaire avec la longueur du code. La complexité de décodage est donc liée à la complexité élémentaire associée à un nœud variable et à un nœud parité : on parle de mise à jour. Si la mise à jour des variables est simple, celle de la parité est plus compliquée. Elle consiste à trouver toutes les possibilités de vérifier l'équation de parité et d'en déduire la probabilité pour une variable donnée la probabilité de ses valeurs possibles.

Dans le cas binaire, cela se réduit à une équation donnant le logarithme du rapport de vraisemblance (LLR) pour une variable donnée. Un seul LLR suffit à exprimer les probabilités des valeurs possibles d'une variable. Cette équation utilise des fonctions exponentielles ou tangente hyperbolique qui nécessitent une implémentation à base de tables. Les réductions de complexité proposées visent donc à simplifier cette équation. La plus populaire est celle dite du Min-Sum (MS) [12] qui consiste à approximer le résultat du calcul du LLR de sortie par la plus petite valeur des LLR en entrée, ou sa variante dite "*self-correcting*" MS [13].

Dans le cas non-binaire, le nombre de configurations de symboles vérifiant l'équation de parité augmente. De même, plusieurs LLR sont nécessaires pour exprimer la distribution de probabilité d'une variable sur les  $2^m$  symboles possibles. Les algorithmes les plus populaires permettant de réduire la complexité dans le cas non-binaire sont l'EMS [14] et le Min-Max [15].

### Séquencement du décodage

Dans le cas où il n'y a pas de cycles dans le graphe représentant les contraintes de parité d'un code LDPC, le décodage BP est non-seulement optimal et converge vers le résultat de décodage MAP, mais en plus, les mises à jour des nœuds variables et contrainte de parité peuvent se faire dans n'importe

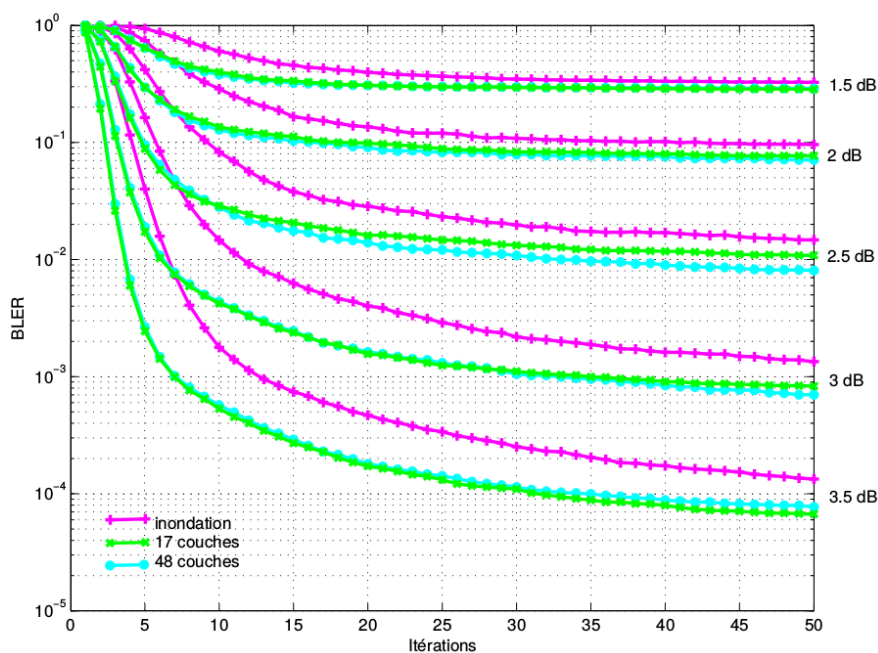


FIGURE 3.2 – Influence du séquençement sur la vitesse de convergence. Cas d'un code LDPC dans GF(16) de longueur 96 symboles et de rendement 0.5. Figure extraite de la thèse de Sanae El Hassani [16]

quel ordre. Cet ordre dans lequel sont faites les mises à jour est appelé séquençement (*scheduling*).

Dans le cas des codes utilisés en pratique, le séquençement peut avoir une influence sur le taux d'erreur et sur sa vitesse de convergence en fonction du nombre d'itérations, comme l'illustre la figure 3.2 pour un code dans GF(16) de longueur  $N = 96$ . Une partie de la thèse de Sanae El Hassani a porté sur l'étude et l'amélioration des techniques de séquençements, en distinguant les techniques statiques et les techniques dynamiques.

Le séquençement originel est dit par inondation (*flooding*) [17] : il consiste en la mise à jour de tous les nœuds variables puis tous les nœuds parité. Pour accélérer la convergence, le séquençement de type *shuffle* a été proposé [18, 19, 20]. Dans le *shuffle* vertical (resp. horizontal), le principe est de mettre à jour séquentiellement les variables (resp. les parités). Après la mise à jour d'un nœud variable (resp. parité), tous les nœuds parité (resp. variable) qui lui sont connectés sont mis à jour puis on met à jour le nœud variable (resp. parité) suivant.

Les séquençements peuvent ensuite être modifiés de manière dynamique, c'est à dire qu'il peut y avoir des modifications apportées lors des mises à jour, selon différents critères. Un classement de ces techniques a été proposé dans la thèse de S. El Hassani [16] et est reporté dans le tableau 3.1. Cependant, l'influence de ces techniques reste faible devant la dispersion de performance des techniques de construction des codes LDPC.

### 3.2.3 Construction

Les turbocodes et les codes LDPC ont cette particularité d'avoir un algorithme de décodage performant décrit sans la connaissance exacte du code considéré. Il s'agit ensuite de construire le code correspondant à des spécifications de longueur, de rendement, mais qui permette un décodage donnant

TABLE 3.1 – Classement des modifications dynamiques que l'on peut apporter au séquençement de décodage des codes LDPC, extrait de [16]

Détection	cycles	iterations	syndrome	fiabilité	stabilité
<b>Action</b>					
calcul des message	[16]		[16]	[22]	[23]
	[21]				
désactivation des noeuds	[25]	[24]		[27]	[28]
		[26]	[27, 29, 24]		
		[16]			
ordre des mises à jour	[16]	[16]		[30, 31]	[29]

les meilleures performances possibles. On est donc dans un processus inverse des codes construits pour leur propriété intrinsèque, et pour lesquels on doit ensuite trouver un décodeur performant à complexité raisonnable (par exemple, les codes algébriques de type BCH ou Reed-Solomon, ou plus récemment les codes polaires).

Comme pour les codes LDPC binaires, la construction des codes LDPC non-binaires peut se faire de manière algébrique ou pas. En revanche, il existe une étape supplémentaire qui consiste à choisir les valeurs non-nulles parmi les  $(2^m - 1)$  valeurs possibles. Le choix des valeurs non-binaires est un degré de liberté supplémentaire qui permet d'améliorer les performances des codes LDPC non-binaires. Il est possible d'améliorer ces performances selon 2 axes :

1. Augmentation de la distance minimale binaire des équations de parité [32]

Une équation de parité non binaire dans  $\text{GF}(2^m)$  de degré  $d_c$ <sup>1</sup> peut être vue comme un code binaire de longueur  $n = md_c$  et de dimension au plus  $k = m(d_c - 1)$ . Si la distance minimale en symboles d'une telle équation de parité est toujours 2, la distance minimale du code binaire correspondant peut parfois être augmentée : cela dépend du degré, de la taille du corps et du choix des coefficients multiplicatifs non-binaires constituant l'équation de parité.

La figure 3.3 illustre sur une simple équation de parité de degré 4 les différences de performances obtenues selon le choix des coefficients non-binaires. Trois choix illustrent les différents cas possibles : une distance binaire minimale de 2, ou une distance binaire minimale de 3 avec 20 ou 43 mots de code à distance minimale.

La table 3.2 donne les plus grandes distances minimales possibles d'une équation de parité en fonction de son degré et de la taille du corps.

2. Élimination de mots de code de poids faibles : cas particulier des codes réguliers  $(2, d_c)$ .

Les codes LDPC non-binaires ont des seuils de convergence d'autant plus bas que la taille de corps est élevée et que leur degré variable diminue [33, 34] vers le degré minimum égal à 2. De plus, à longueur et rendement fixé, un degré 2 permet d'avoir une matrice de contrôle de

1.  $d_c$  est le nombre de symboles impliqués dans l'équation de parité.



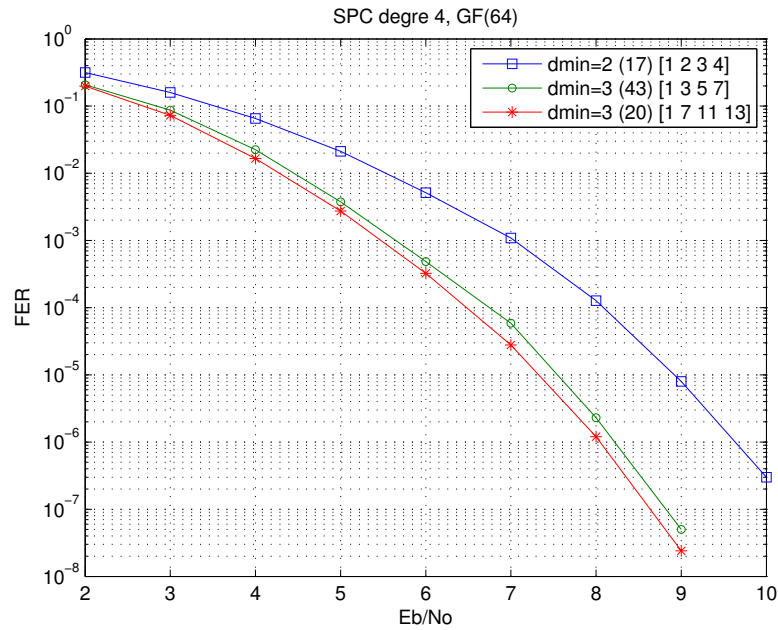


FIGURE 3.3 – Taux d’erreur trame d’une équation de parité de degré 4 dans GF(64) pour différents labels non-binaires.

TABLE 3.2 – Distances minimales binaires maximales obtenues pour certaines combinaisons de coefficients non-binaires d’une équation de parité en fonction de son degré et de la taille du corps considéré, inspirée d’après [32].

$d_c \backslash GF$	3	4	5	6	7	8	9	10	11	12
8	2									
16	4		2							
32	4			2						
64	4				2					
128	4	4		3						
256	4		3							

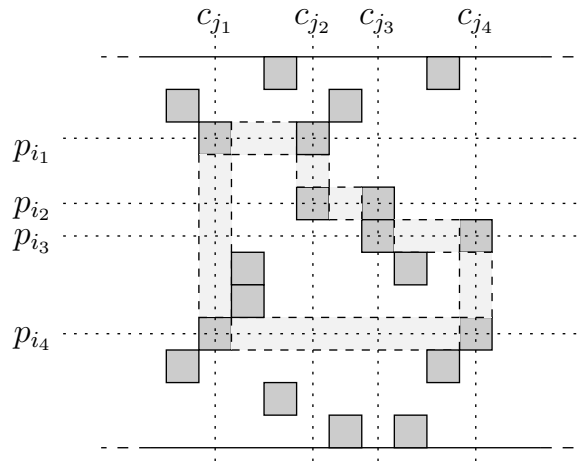


FIGURE 3.4 – Illustration d'un cycle de longueur 8 dans une matrice de contrôle de parité ayant des variables de degré 2.

parité plus creuse et donc ayant des cycles plus longs et des cycles courts moins nombreux. C'est la raison pour laquelle de nombreuses constructions LDPC non-binaires sont proposées avec des codes réguliers  $(2, d_c)$ .

Dans ce cas, un cycle correspond à une sous-matrice de la matrice de contrôle. Une illustration est proposée sur la figure 3.4 pour un cycle de longueur 8. Les entrées non-nulles  $h_{i,j}$  de la matrice de contrôle de parité sont représentées par des petits carrés gris, le cycle est mis en évidence ainsi que les variables  $c_j$  et les parités  $p_i$  impliquées dans ce cycle. Si on prend un vecteur  $\mathbf{c}$  de longueur  $N$  de sorte que  $c_j = 0$  pour tout  $j \notin \{j_1, j_2, j_3, j_4\}$ , ce vecteur sera considéré comme un mot de code si  $\mathbf{H}\mathbf{c}' = \mathbf{0}$ , et donc la distance minimale en symbole serait au plus 4. Pour éviter ce cas de figure, il faut assurer que

$$\begin{aligned} & \forall \mathbf{c} \{c_i = 0 \forall i \notin \{j_1, j_2, j_3, j_4\}\}, \mathbf{H}\mathbf{c}' \neq \mathbf{0} \\ \Leftrightarrow & \begin{pmatrix} h_{i_1, j_1} & h_{i_1, j_2} & h_{i_1, j_3} & h_{i_1, j_4} \\ h_{i_2, j_1} & h_{i_2, j_2} & h_{i_2, j_3} & h_{i_2, j_4} \\ h_{i_3, j_1} & h_{i_3, j_2} & h_{i_3, j_3} & h_{i_3, j_4} \\ h_{i_4, j_1} & h_{i_4, j_2} & h_{i_4, j_3} & h_{i_4, j_4} \end{pmatrix} \times \begin{pmatrix} c_{j_1} \\ c_{j_2} \\ c_{j_3} \\ c_{j_4} \end{pmatrix} \neq \mathbf{0} \\ \Leftrightarrow & \det \begin{vmatrix} h_{i_1, j_1} & h_{i_1, j_2} & h_{i_1, j_3} & h_{i_1, j_4} \\ h_{i_2, j_1} & h_{i_2, j_2} & h_{i_2, j_3} & h_{i_2, j_4} \\ h_{i_3, j_1} & h_{i_3, j_2} & h_{i_3, j_3} & h_{i_3, j_4} \\ h_{i_4, j_1} & h_{i_4, j_2} & h_{i_4, j_3} & h_{i_4, j_4} \end{vmatrix} \neq 0 \end{aligned}$$

On peut donc éviter la présence de mots de code de poids  $L$  en assurant que le choix des valeurs non-binaires garantisse que les matrices construites avec les valeurs non-binaires des entrées de  $\mathbf{H}$  associées aux cycles de longueurs  $2L$  soient de rang plein. Nous avons publié cette contribution dans [3], et elle apparaît également de manière indépendante dans [35].

L'élimination de mots de code de poids faibles par le choix de valeurs non-binaires a été généralisée aux *stopping set* dans [36].

### 3.2.4 Conclusions

Je poursuis actuellement cette thématique sur les codes LDPC non-binaires à travers un contrat d'études avec le centre de recherche France de Huawei, suite à un appel à projet lancé en 2014. Ce contrat a permis l'embauche de Zeina Mheich en post-doctorat. Cette étude porte sur l'étude des codes de longueurs courtes (typiquement moins de 512 bits codés). Les codes LDPC non-binaires semblent en effet prometteurs pour des petites longueurs : la complexité reste raisonnable et les performances sont améliorées par rapport à leur équivalent binaire.

## 3.3 Codes Reed-Solomon

L'arrivée des codes concaténés a généré beaucoup de nouvelles activités de recherche et de développement dans le domaine du codage correcteur. Cependant, il ne faut pas oublier que les codes algébriques inventés par Irving S. Reed et Gustave Solomon (codes RS) en 1960 [37] ont été et sont encore présents dans la majorité des systèmes de communication ou de stockage numérique, seuls ou en concaténation avec des codes convolutifs. Les codes RS sont des codes très puissants<sup>2</sup>, ce qui rend leur décodage difficile. Un algorithme de décodage algébrique efficace a été proposé par Elwyn Berlekamp et James Massey en 1969, mais aucun décodage pondéré de complexité raisonnable n'est pour l'instant disponible.

Dans cette optique, la thèse d'Andrzej Kabat (2006-2009) [38, 39] s'est focalisée sur le décodage pondéré des codes RS de grande longueur dans le contexte du contrat de recherche externe pour France Telecom [40]. J'ai également étudié ce type de décodage pour les récepteurs ADSL dans le cadre du contrat Distrimages (2005-2008). Enfin, j'ai proposé d'utiliser un code RS pour le lien radio de télémessure des compteurs de gaz (contrat GrDF en 2011) en raison de leur faible complexité d'encodage et de décodage algébrique.

### 3.3.1 Définition et décodage

#### Définition

Les codes RS sont des codes en blocs linéaires cycliques définis sur un corps de Galois  $GF(Q = q^m)$ . Cependant, nous ne considérerons dans la suite que les corps de caractéristique  $q = 2$ . Ainsi, les symboles utilisés seront choisis parmi les  $2^m$  symboles de  $GF(Q)$ , chacun d'eux étant représentable sur  $m$  bits.

Un code RS de longueur  $N$  et de dimension  $K$  (noté  $RS(N, K)$ ) est défini dans un corps par les  $N - K$  racines de son polynôme générateur  $g(x)$  qui sont de la forme  $\alpha^b, \dots, \alpha^{b+N-K-1}$  où  $\alpha$  est un élément primitif de  $GF(Q)$  et  $b$  est un entier positif ou nul qu'il est possible de choisir judicieusement pour améliorer la distance minimale binaire du code [41]. Dans la suite de cette section je me focaliserai sur le code  $RS(255, 239)$  pour illustrer mes propos.

#### Décodage ferme

Dans le cadre d'un décodage ferme (HDD), les codes RS permettent de retrouver au plus  $(N - K)$  symboles effacés, ou de corriger  $\lfloor \frac{N-K}{2} \rfloor$  symboles faux (où  $\lfloor x \rfloor$  désigne l'arrondi par valeur

2. Ils offrent le meilleur rendement pour une distance minimale (symboles) données

inférieure de  $x$ ). Il existe plusieurs algorithmes algébriques de décodage ferme des codes RS : ils sont dits "à distance bornée" (BDD). Les algorithmes BDD permettent de corriger au maximum  $t$  erreurs, ( $t \leq \lfloor \frac{N-K}{2} \rfloor$ ). Si le mot reçu est éloigné de plus de  $t$  symboles des mots du codes, le décodeur BDD déclare un échec de décodage. Ainsi, on peut exprimer une borne sur les performances de taux d'erreur par mot transmis en énumérant la liste des motifs d'erreurs ayant au plus  $t$  symboles faux parmi les  $N$  symboles du mots reçu :

$$\text{WER}_{\text{HDD-BDD}} = 1 - \sum_{i=0}^t \binom{N}{i} p_s^i (1 - p_s)^{N-i}$$

où  $p_s$  est la probabilité qu'un symbole soit faux. Dans le cas d'une modulation binaire (BPSK) sur un canal à bruit additif blanc gaussien (AWGN), on a  $p_s = 1 - (1 - p)^m$ ,  $p$  étant la probabilité d'erreur binaire donnée par  $p = \frac{1}{2} \text{erfc} \left( \sqrt{R \frac{E_b}{N_0}} \right)$ .

Les algorithmes de décodage algébrique sont composés des 4 étapes suivantes :

1. Calcul du syndrome
2. Calcul de la position des erreurs en cherchant tout d'abord les coefficients du polynôme localisateur d'erreurs (algorithme de Peterson-Gorenstein-Zierler [42], algorithmes itératifs de Berlekamp-Massey [43, 44] ou d'Euclide étendu [45], puis en cherchant ses racines (recherche dite "de Chien" [46] mais qui se fait maintenant en parcourant exhaustivement les éléments du corps utilisé). La position des erreurs est alors donnée par le logarithme base  $\alpha^3$  des inverses des racines obtenues.
3. Calcul de la valeur des erreurs en cherchant les coefficients du polynôme évaluateur d'erreurs donné par l'équation clef [44]<sup>4</sup>, puis en calculant les valeurs des erreurs par la formule de Forney [47].
4. Génération du résultat du décodage, en vérifiant qu'il s'agit bien d'un mot de code.

Le décodage algébrique peut aboutir à un échec de décodage (étapes 2 ou 4), auquel cas aucun mot de code n'est fourni par le décodeur.

### Potentiel du décodage à entrée pondérée

Pour minimiser la probabilité d'erreur par mot, le décodeur doit tenir compte de l'alphabet de modulation en maximisant la vraisemblance (ML) des mots reçus  $\mathbf{r}$  sur tous les mots de code modulés possibles. Si l'on note  $\mathcal{S}$  l'ensemble des séquences codées modulées possibles, alors le décodage ML s'écrit :

$$\hat{s} = \arg \max_{s^i \in \mathcal{S}} \Pr(\mathbf{r} | s^i)$$

Si l'on considère le canal AWGN, ce décodage ML revient à minimiser la distance euclidienne entre  $\mathbf{r}$  et les séquences modulées codées  $s^i$  : les performances seront limitées par la distance euclidienne minimale, et plus généralement par la distribution (ou spectre) des distances des séquences modulées codées. Dans l'hypothèse d'une modulation binaire BPSK, la relation linéaire qui existe entre la

3. C'est simplement l'exposant  $i$  permettant d'écrire le nombre sous la forme  $\alpha^i$ .

4. Le polynôme évaluateur d'erreurs est égale au produit du polynôme localisateur d'erreur par le polynôme syndrome, modulo  $x^{2t}$ .

distance euclidienne et la distance de Hamming permet de considérer le spectre des distances binaires du code pour l'évaluation du taux d'erreur.

Une borne supérieure sur la probabilité d'erreur par mot peut être obtenue par la borne de l'union [48] exprimée comme :

$$\text{WER}_{\text{ML-SDD}} \leq \sum_{w=D}^{mN} \frac{B_w}{2} \operatorname{erfc} \left( \sqrt{Rw \frac{E_b}{N_0}} \right) \quad (3.1)$$

et qui nécessite la connaissance du spectre de distances binaires du code dans le cas d'une transmission en modulation binaire sur canal AWGN ( $B_w$  est le nombre de mots de code de poids binaire  $w$ ). Le spectre de distances binaires n'est pas connu en général pour les codes RS, et en particulier pour le code RS(255, 239). En revanche, le spectre de distances symboles est connu [48] et donné par :

$$A(x) = \sum_{w=0}^N A_w x^w$$

où

$$A_w = \begin{cases} (Q-1) \binom{N}{w} \sum_{i=0}^{w-D} (-1)^i \binom{w-1}{1} Q^{w-D-i} & , w \geq D \\ 1 & , w = 0 \\ 0 & , 0 < w < D \end{cases}$$

est le nombre de mots de code de poids  $w$  (en symboles) et où  $D = N - K + 1$  est la distance minimale en symboles du code RS( $N, K$ ). A partir du spectre de distances symboles, on peut donner une expression du spectre de distance binaire moyen en supposant que la distribution de 1 et 0 d'un symbole non-binaire représenté sur  $m$  bits suit une distribution binomiale, on peut obtenir une expression moyenne du spectre de distances binaires d'un code RS [49] :

$$B(x) = \sum_{w=0}^m N B_w x^w$$

avec

$$B_w = \frac{A_i}{N^i} \sum_{j=0}^i (-1)^{i-j} \binom{i}{j} \binom{jm}{w}$$

La borne de l'union pour le code RS(255,239) est évaluée sur la figure 3.5 et comparée aux performances du décodage ferme à distance bornée. On peut constater qu'environ 2dB peuvent être gagnés par un changement de décodeur.

### 3.3.2 Décodage à entrée souple des codes RS

On peut regrouper les nombreux résultats publiés à propos du décodage souple des codes RS dans 3 grandes catégories [50, 40] :

1. les décodeurs utilisant les propriétés algébriques des codes RS,
2. les décodeurs à propagation de croyance,
3. les décodeurs à liste de candidats.

Pour des codes de grandes longueurs telles que celles considérées dans cette section (le code

RS(255,239) a une longueur de 2040 bits), seules les catégories 2 et 3 conservent une complexité raisonnable, c'est à dire permettant de simuler des taux d'erreur usuels.

Les décodeurs à propagation de croyance modifient la structure de la matrice de contrôle de parité du code RS afin que l'algorithme de propagation de croyance (BP) puisse donner des performances satisfaisantes. La modification peut par exemple consister à rajouter des équations de parité redondantes (BK) [51], ou à les transformer de sorte que les bits les moins fiables soient impliqués dans le moins de parités possibles (ABP) [52].

Les décodeurs à liste génèrent une liste de plusieurs mots de code en espérant obtenir le mot de code ML. La décision du décodage correspond au mot de code de la liste le plus proche du mot reçu (au sens de la distance euclidienne). Plus la liste générée est grande, plus les chances de l'obtenir augmentent, et en tous les cas meilleur est le décodage. Pour générer une telle liste, on peut par exemple utiliser la technique de Chase [53] qui consiste à modifier successivement un ou plusieurs bits reçus puis à effectuer un décodage algébrique. Il est judicieux de changer en priorité les bits les moins fiables, en commençant par changer un seul bit à la fois, puis 2, 3, etc ... selon la longueur de la liste souhaitée. Une autre technique de génération de liste consiste à ré-encoder les  $K$  symboles indépendants (ou les  $mK$  bits indépendants) les plus fiables, également en changeant 1 ou plusieurs symboles (ou bits) parmi eux selon la taille souhaitée de la liste. De nombreuses variantes sur ce thème ont été proposées, et nous pouvons citer la plus ancienne (Dorsch) [54] et l'une des plus populaire (OSD) [55].

Notons qu'à part l'algorithme de Chase pour lequel il faut disposer d'un décodeur algébrique, les autres versions des décodeurs des catégories 2 et 3 sont universelles en ce sens qu'elles peuvent décoder un code linéaire quelconque dont seule une matrice génératrice ou une matrice de parité serait connue.

Dans la thèse d'Andrzej Kabat [50], nous nous sommes intéressés aux décodeurs à liste en étudiant les 2 étapes clefs qui les constituent :

- la stratégie de modification des bits : c'est cette stratégie qui va définir les différents mots de code qui seront générés, ainsi que l'ordre dans lequel ils seront générés. La génération de ces mots de code étant faite en commutant certains bits de la séquence reçue, on parle alors de vecteurs de test, qui contiennent des 0 aux positions des bits à ne pas changer, et des 1 aux positions des bits à changer. Le premier vecteur de test est bien sûr le vecteur tout à zéro.
- le choix du critère d'arrêt : il est recommandé de ne pas parcourir la liste entière des mots de code à générer selon la stratégie définie précédemment afin de réduire le temps de décodage moyen.

### 3.3.3 Génération de vecteurs de tests basée sur les statistiques d'ordre

Nous nous plaçons dans le cas du décodage par ré-encodages successifs des bits indépendants les plus fiables. Dans l'algorithme OSD binaire d'ordre 1 par exemple, les vecteurs de test suivant le vecteur tout à zéro sont tous les vecteurs binaires de taille  $mK$  (il y a  $mK$  bits indépendants dans un code RS de dimension  $K$ ) et de poids de Hamming unitaire. Cette liste est cependant ordonnée : le premier vecteur de test non nul est donc le vecteur de poids de Hamming 1 ayant l'élément non nul à la position du bit reçu le moins fiable. Cela permet d'accélérer le décodage si des critères d'arrêt sont mis en place car la probabilité qu'un bit peu fiable soit faux est plus grande que la probabilité qu'un

bit fiable soit faux.

Lorsque l'on souhaite augmenter les performances de l'OSD, on peut passer à l'OSD d'ordre 2. Dans ce cas, après avoir examiné tous les vecteurs de test de poids 1, on examine tous les vecteurs de test de poids 2. Pour le code RS(255,239), le nombre de vecteurs de test de poids 1 est de  $239 * 8 = 1912$  et celui des vecteurs de test de poids 2 est de  $\binom{239 \times 8}{2} \simeq 1.8 \times 10^6$ . Devant un tel nombre de vecteurs de test à générer, il est nécessaire d'utiliser des algorithmes efficaces pour les générer : citons par exemple [55] et [56] qui offrent les mêmes performances en termes de taux d'erreur, mais dont la complexité moyenne en termes de nombre de vecteurs de test générés est différente (la comparaison étant faite avec les mêmes critères d'arrêt).

La génération des vecteurs de test dans l'OSD est dite pré-définie : elle reste identique quel que soit le vecteur reçu, dont les bits ont été préalablement classés par ordre de fiabilité (elle ne dépend pas des valeurs souples reçues). Mais il est légitime de se poser la question : ne serait-il pas judicieux de tester 2 bits très peu fiables avant d'en tester un seul très fiable ? Autrement dit, il est possible que la probabilité que 2 bits peu fiables soient faux tous les 2 soit plus élevée que la probabilité qu'un seul bit très fiable soit faux : cela dépend des valeurs reçues. Les auteurs de [54, 57] proposent ainsi de créer les vecteurs de test selon une métrique croissante appelée poids elliptique qui dépend des valeurs souples reçues. Les performances sont meilleures que celles de l'OSD pour une même taille de liste mais le problème majeur est alors la complexité issue de l'absence de liste prédéfinie.

Dans la thèse d'Andrzej Kabat [50], nous avons proposé d'allier la simplicité d'une liste prédéfinie avec les performances des listes basées sur la fiabilité en utilisant les statistiques des valeurs souples reçues pour un SNR donné (algorithme ALMRT). Dans le cas des codes RS de grandes longueurs, les fiabilités reçues et classées par ordre croissant sont très proches de leurs statistiques. Ainsi, les performances de liste non-prédéfinie sont conservées, avec une complexité de l'ordre de celle des algorithmes avec liste prédéfinie. Les performances obtenues sont illustrées sur la figure 3.5, où l'on peut retenir que les performances de l'ALMRT sont meilleures que celles de l'OSD d'ordre 2 avec un nombre comparable de vecteurs de test.

### 3.3.4 Conditions d'optimalité

Des critères d'arrêt doivent être appliqués pour accélérer le décodage par liste de candidats. Ces critères sont basés sur des conditions nécessaires ou suffisantes, dites conditions d'optimalité :

- Condition nécessaire : ce sont le ou les critères que doivent respecter les vecteurs de test eu égard au mot reçu pour avoir une chance de conduire à un mot de code candidat intéressant. Si cette condition n'est pas respectée, cela permet de passer aux vecteur de test suivants sans avoir besoin de générer le mot de code candidat correspondant.
- Condition suffisante : ce sont le ou les critères que doit respecter le mot de code optimal (ML). Lorsque la condition suffisante est satisfaite, l'algorithme de décodage doit bien entendu s'arrêter et déclarer comme résultat le mot de code concerné.

Ces conditions nécessaires et suffisantes sont par essence déterministes. Cependant, elles ont été complétées par d'autres conditions probabilistes pour lesquelles on a conservé par abus de langage les noms de conditions nécessaires et suffisantes. Ces conditions probabilistes rendent plus flexibles le compromis performance / complexité grâce aux seuils qu'elles introduisent, au prix d'une certaine sous-optimalité. Le tableau 3.3 permet de classer les critères principaux issus de la littérature.

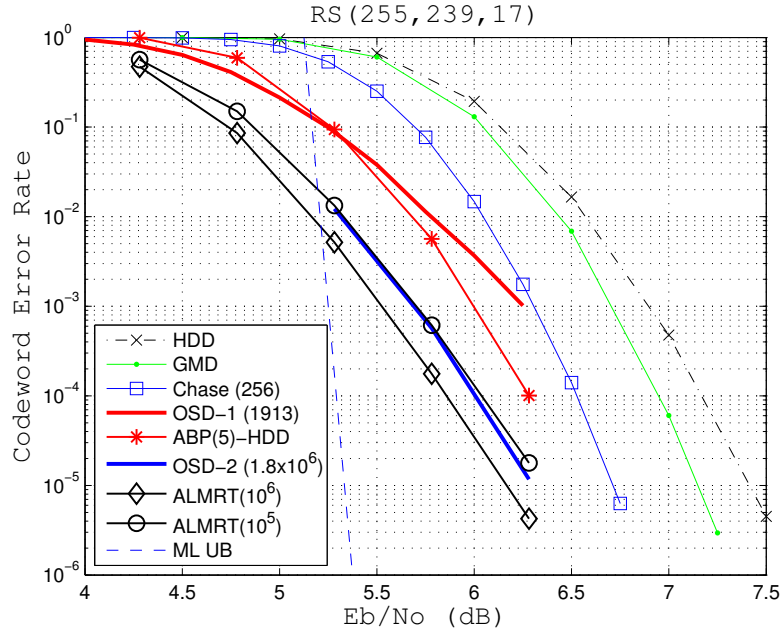


FIGURE 3.5 – Comparaison des performances de l’algorithme ALMRT par rapport aux algorithmes de l’état de l’art pour le décodage d’un code RS(255,239). Le nombre de vecteurs de test pour les décodeurs à liste de candidats est inscrit entre parenthèses dans la légende. (extrait de [50])

TABLE 3.3 – Classement des conditions nécessaires (CN) et suffisantes (CS) selon leur nature déterministe ou probabiliste

	Déterministe	Probabiliste
CN	Ressource Test [55]	Upper Bound on the test vector correlation discrepancy [58]
CS	Acceptance criterion [59]	<ul style="list-style-type: none"> <li>• Upper bound on the number of errors in the set of less reliable parity bits [60]</li> <li>• Lower bound on the cross correlation [61]</li> </ul>



Nous avons proposé dans la thèse d'Andrzej Kabat [50] des améliorations sur les CN (déterministes et probabilistes) en permettant l'arrêt durant la génération d'un mot de code candidat en prenant en compte les bits de parité (alors que les CN de l'état de l'art sont limitées aux vecteurs de test, donc aux bits d'information). Nous avons également proposé une méthode de calcul de seuil pour la CS probabiliste.

### 3.3.5 Conclusions

Les codes Reed-Solomon de grandes longueurs sont un véritable défi pour la conception de décodeurs qui pourront offrir tout le potentiel de correction que recèlent ces codes. Les travaux menés durant la première partie de la thèse d'Andrzej Kabat ont permis d'améliorer très sensiblement les performances de décodage à entrée souple des codes RS de grandes longueurs. Si les codes Reed-Solomon ont été proposés il y a maintenant plus de 50 ans, leur utilisation est toujours d'actualité et le problème de leur décodage optimal toujours ouvert. Avec l'émergence des communications entre machines nécessitant des codes performants et simple d'encodage, ils peuvent constituer une solution pertinente à la protection de l'information pour des paquets de longueurs moyennes.

C'est dans cet esprit que j'ai pu recommander ces codes en normalisation européenne pour les systèmes communications numériques associés aux compteurs intelligents pour les réseaux de transport de fluides (eau, gaz, etc ...) ou d'énergie (CEN / TC 294 / WG5). Cette recommandation est soutenue par GrDF en lien avec leur projet de déploiement de compteurs de gaz sans fil.

## 3.4 Réseaux de points

Les codes correcteurs d'erreur linéaires permettent une dépendance entre les bits ou les symboles codés. Cette dépendance est principalement décrite dans des corps finis de caractéristique 2 (binaires ou non-binaires). Ainsi, lorsque les bits codés sont associés à des symboles de la constellation (symboles de modulation), la dépendance entre les bits codés entraîne une dépendance entre les symboles de modulation. Mais cette dépendance n'est pas explicite sauf dans certains cas particuliers (modulation BPSK par exemple), et les propriétés topologiques des corps finis utilisés pour le codage correcteur d'erreurs ne sont plus utilisables dans le domaine des symboles de modulation.

Il existe dans le domaine des symboles de modulation des structures algébriques qui permettent d'introduire des relations de dépendance entre les symboles de modulation : les réseaux de points (lattices). Il s'agit de groupes discrets de  $\mathbb{R}^n$ , qui apportent les propriétés de linéarité et une loi de composition interne (addition). Ces réseaux de points permettent d'atteindre la capacité du canal gaussien lorsque la dimension  $n$  tend vers l'infini. Ainsi, ils constituent le pendant des codes correcteurs d'erreur dans l'espace des signaux, avec cependant une structure algébrique moins riche. De nombreux résultats asymptotiques mettent en avant l'intérêt des réseaux de points pour les communications numériques. Cependant, les algorithmes d'encodage et de décodage font l'objet de moins d'études que ceux concernant leurs performances asymptotiques et les comparaisons aux techniques de transmissions usuelles sont rares. Il est donc difficile de savoir si le codage par réseau de points peut offrir une solution intéressante en pratique pour les systèmes de communication numérique.

C'est donc avec cet objectif que j'ai commencé à travailler sur ce thème, avec tout d'abord le stage de Clément Acquitter (2012) puis avec le contrat METIS qui a permis de financer la thèse de

Carole Al Beschlawi (2012-2015) et le post-doc de Vincent Herbert (2013-2014).

### 3.4.1 Définitions

Si les réseaux de points sont le pendant des codes correcteurs d'erreurs (FEC) dans l'espace des signaux, la comparaison s'arrête rapidement car un réseau de points contient un nombre infini de points, contrairement aux FEC. Il faut donc définir un réseau de points, puis un code défini sur un tel réseau.

**Un réseau de point (lattice)**  $\Lambda$  de dimension  $n$  est un groupe discret dans un espace euclidien réel  $\mathbb{R}^n$ . On peut le définir comme l'ensemble des points de  $\mathbb{R}^n$  qui peuvent être décomposés en une somme de  $n$  vecteurs indépendants de  $\mathbb{R}^n$  pondérés par des coefficients **entiers**. Si on note  $\mathbf{g}_1, \dots, \mathbf{g}_n$  un ensemble de  $n$  vecteurs indépendants de  $\mathbb{R}^n$ , alors tous les points  $\mathbf{x} = \sum_{i=1}^n b_i \mathbf{g}_i$  où  $b_i \in \mathbb{Z}$ , appartiennent à un même réseau de points. On définit une matrice génératrice d'un réseau de point comme la matrice constituée par la concaténation (en colonne par exemple) de l'ensemble des  $n$  vecteurs indépendants  $\mathbf{g}_i$  :  $\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_n]$ .

**Exemple : le réseau D4** ( $n = 4$ ) qui contient tous les points de  $\mathbb{R}^4$  dont les coordonnées sont entières et font une somme paire. Une matrice génératrice est donnée par :

$$G_{D4} = \begin{bmatrix} 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

**Un code  $\Lambda_{\mathcal{B}}$  issu d'un réseau de points  $\Lambda$  (Lattice Code) :** pour définir un tel code, on commence par décaler le réseau de points  $\Lambda$  d'un vecteur  $\mathbf{a} \in \mathbb{R}^n$ , puis on choisit une région convexe  $\mathcal{B}$  de  $\mathbb{R}^n$  appelée région de mise en forme (*shaping*). L'ensemble des mots du code est l'ensemble des points du réseau qui sont inclus dans la région  $\mathcal{B}$ . On notera donc :

$$\Lambda_{\mathcal{B}} = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} \in ((\Lambda + \mathbf{a}) \cap \mathcal{B}), \mathbf{a} \in \mathbb{R}^n\}$$

**Exemple trivial : constellation QAM-16.** En partant du réseau de points à coordonnées entières dans  $\mathbb{R}^2$ , noté  $\mathbb{Z}^2$ , dont une matrice génératrice est la matrice identité de taille 2, on choisit un décalage  $\mathbf{a} = [0.5, 0.5]$  et une région de mise en forme carrée décrite par le produit cartésien  $[-2, 2] \times [-2, 2]$ , on obtient ainsi les 16 symboles d'une modulation QAM comme illustrée sur la figure 3.6.

La performance d'un code issu d'un réseau de points va dépendre de 2 facteurs [62] :

- le réseau de points : selon le réseau de points choisi, le gain de codage apporté sera plus ou moins important. Par exemple, le réseau de points des entières n'apporte pas de gain de codage.
- la région de mise en forme : selon la forme de cette région, le gain de codage sera complété par un gain de mise en forme (*shaping gain*).

Si le code contient un très grand nombre de points, la propriété du code provient essentiellement de celle du réseau de points : l'influence de la région de mise en forme devient négligeable. On peut donc étudier les performances de réseaux de différentes dimensions sans se préoccuper de la région

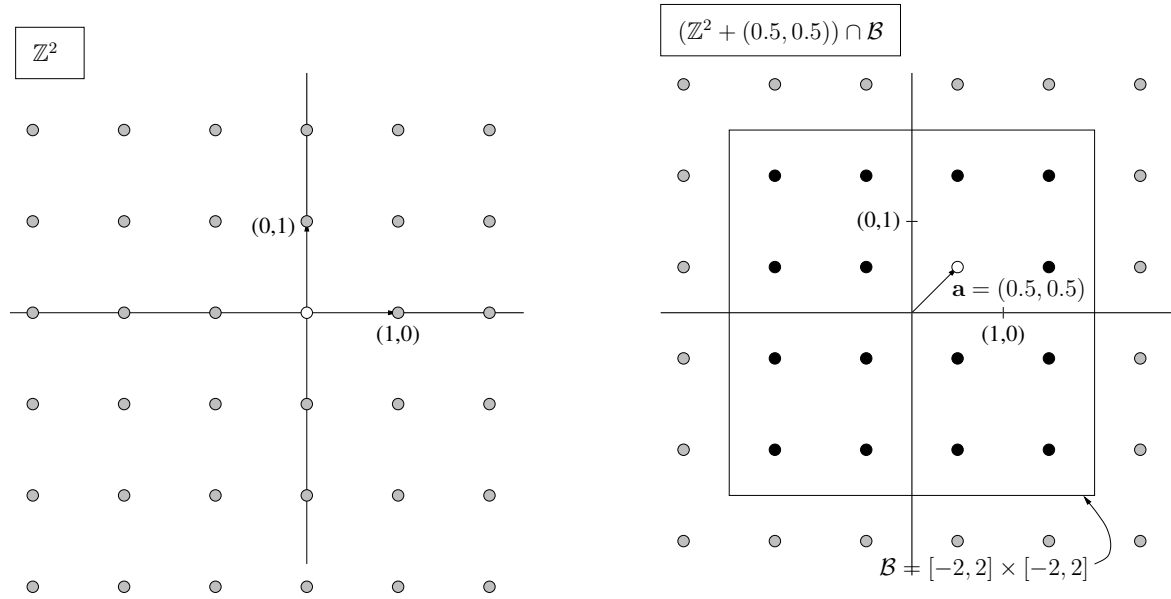


FIGURE 3.6 – La modulation QAM est un code basé sur le réseau de points des entiers en dimension 2.

de mise en forme. Le nombre de points est alors infini mais on peut définir le rapport entre le volume fondamental du réseau et le volume d'une hypersphère de bruit de rayon égal à  $n\sigma^2$  ( $\sigma^2$  est la variance du bruit gaussien sur chaque dimension). Ce rapport est noté VNR (Volume to Noise Ratio) et vaut :

$$\text{VNR} = \frac{V(\Lambda)^{\frac{2}{n}}}{2\pi e\sigma^2},$$

où  $V(\Lambda)$  est le volume fondamental d'un réseau : c'est un élément invariant du réseau (il ne dépend pas du choix de la matrice génératrice) défini comme la racine carrée du déterminant du produit de la matrice génératrice par sa version transposée :  $V(\Lambda) = |G^T G|^{1/2}$ .

Le gain de codage que peut apporter un réseau de points est lié à la densité de points de ce réseau. Trouver des réseaux de points denses dans un espace euclidien à  $n$  dimensions correspond au problème mathématique de l'empilement régulier de sphères [63] et n'est résolu que pour les plus petites dimensions. La figure 3.7 présente une estimation du taux d'erreur obtenu avec différents réseaux de points en différentes dimensions en fonction du VNR. Afin de comparer des taux d'erreur de symboles ayant des dimensions variables, on compare le taux d'erreur par symbole divisé par la moitié de la dimension, ce qui est équivalent à un symbole à 2 dimensions. On constate que les performances des réseaux d'entiers sont identiques quelle que soit leur dimension, et sont les moins bonnes. Pour  $n = 8$  dimensions, le réseau E8 offre une meilleure performance que le réseau D8 (qui est l'analogue du réseau D4 en 8 dimensions) : en effet, le réseau E8 est le plus dense en 8 dimensions (densité de 0.2536 contre 0.1268 pour D8). En dimension 16, le réseau BW16 est le plus dense connu (densité de 0.0147 contre  $4.6 \times 10^{-4}$  pour D16). L'augmentation de la dimension associée avec de bons réseaux de points permet d'améliorer les performances en terme de taux d'erreur (gain de codage). Cette conclusion est à nuancer car le taux d'erreur va également être influencé par le nombre de plus proches voisins d'un point du réseau (*kissing number*) qui doit être le plus faible possible à densité fixée.

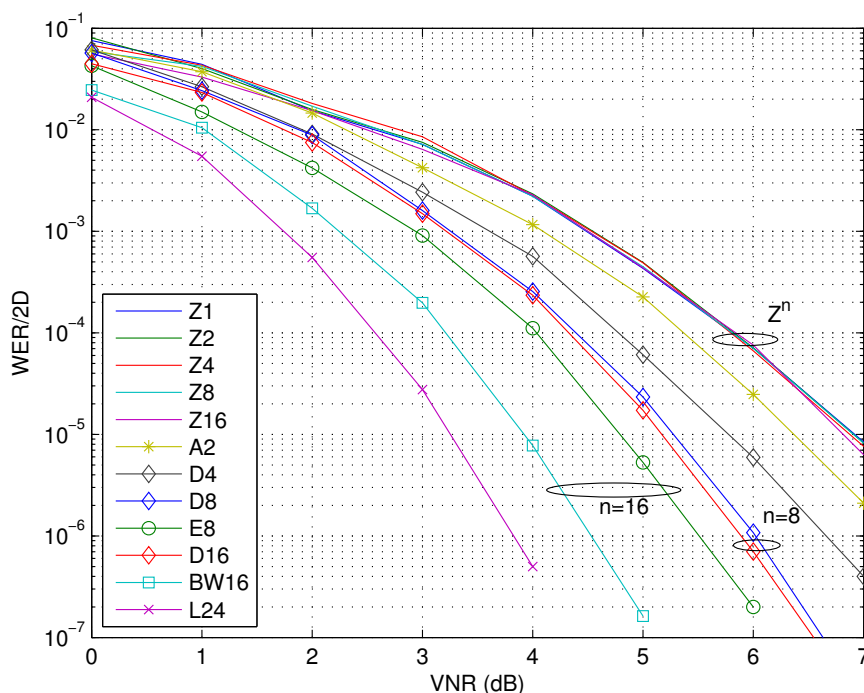


FIGURE 3.7 – Le taux d’erreur par symbole du réseau de point divisé par la moitié de la dimension en fonction du rapport entre le volume fondamental normalisé du réseau et la variance du bruit par dimension, pour différents réseaux connus de petites dimensions.

### 3.4.2 Comparaison aux constellations QAM

Lorsque l’on veut utiliser un code basé sur un réseau de points donné, il faut choisir une région de mise en forme de taille suffisante pour l’efficacité spectrale visée. Mais cette région de mise en forme n’est pas forcément explicite : une solution simpliste pour transmettre de l’information à l’aide d’un code défini sur un réseau de points consiste à utiliser la matrice génératrice multipliée par les symboles (entiers) d’information à transmettre. L’efficacité spectrale dépendra alors du nombre de valeurs possibles d’entiers utilisés à l’encodage. Notons  $L$  le nombre d’entiers différents et supposons pour simplifier que  $L = 2^l$ ,  $l \in \mathbb{Z}$ . L’efficacité spectrale sera de  $\eta = \log 2(L) = l$  bits par dimension et le cardinal du code sera de  $L^n$  mots. Sur la figure 3.8, le taux d’erreur d’une QAM non codée est comparé à celle de même efficacité spectrale utilisant le réseau E8 sans prendre de précaution particulière quant à la région de mise en forme (*E8 no shaping*) : l’encodage est fait par multiplication de la matrice génératrice de E8 avec un vecteur de 8 entiers  $\mathbf{b} = \{b_i\}$  où  $b_i \in [-L/2, L/2 - 1]$ . Le mot obtenu  $\mathbf{x} = \mathbf{G}\mathbf{b}$  est transmis dans un canal additif blanc gaussien (AWGN) et le vecteur reçu  $\mathbf{y} = \mathbf{x} + \mathbf{w}$  ( $\mathbf{w}$  est un vecteur de  $n = 8$  échantillons aléatoires suivant une loi gaussienne de variance  $\sigma^2$ ) est décodé par un algorithme de décodage par sphère afin de rechercher le point du réseau le plus proche de  $\mathbf{y}$ . On constate que les performances de E8 sont nettement dégradées par rapport à la QAM, contrairement aux résultats obtenus sur la figure 3.7 où le gain du réseau E8 par rapport au réseau d’entier était très net. Ceci est expliqué par l’influence de la région de mise en forme qui est tellement mauvaise que le gain de mise en forme est négatif.

Afin d’améliorer ce schéma de transmission, il faut donc mettre en œuvre une procédure per-

mettant de n'envoyer que les  $L^n$  points les plus proches de 0, autrement dit permettant de minimiser l'énergie moyenne par symbole transmis. Cette opération porte le nom de "*shaping*" (mise en forme)<sup>5</sup>.

La région de mise en forme idéale est la sphère (hypersphère en dimension quelconque). Mais lister l'ensemble des points situés dans une hypersphère de rayon donné est trop complexe. Une mise en forme de type hypercube peut être appliquée, ou une mise en forme appelée "*nested shaping*" que l'on pourrait traduire par emboîtement : cette dernière est une bonne approximation de l'hypersphère car elle utilise comme région de mise en forme la région de Voronoï d'un réseau de points inclus dans le réseau de points du code. Dans ces 2 cas, le principe est le suivant. Au lieu d'envoyer l'entier  $b_i$ , un algorithme va chercher un entier  $k_i$  tel que l'entier  $b'_i = b_i + k_i L$  soit envoyé à sa place. Le récepteur retrouve facilement l'entier  $b_i$  à l'aide d'une opération modulo  $L$ . Dans le cas d'une mise en forme de type hypercube, l'optimisation des  $b_i$  se fait de manière indépendante sur chaque dimension. En ce qui concerne celle de type emboîtement, l'optimisation se fait conjointement sur toutes les dimensions à l'aide d'un décodage par sphère. Cette dernière est plus complexe mais plus performante. Les performances d'une mise en forme par emboîtement dans le cas du réseau E8 sont illustrées sur la figure 3.8 (courbes "*E8 nested shaping*"). On voit alors que les gains promis par rapport à la modulation QAM apparaissent, notamment pour les efficacités spectrales élevées. Cependant, pour les courbes à 1 bit/dim, cela reste encore moins bon que la QAM : la région de mise en forme n'est pas très performante pour une aussi faible efficacité spectrale (il n'y a qu'un rapport 2 entre les rayons de la région fondamentale du réseau du code et celle du réseau de mise en forme). Dans ce cas particulier, l'énumération des points du réseaux les plus proches de l'origine peut se faire et en sélectionnant ceux de la première "coquille" (*shell*), c'est à dire tous les mots ayant 6 composantes nulles et les 2 autres d'amplitude unité, de signes quelconques, on obtient 240 points, qui avec l'origine permettent d'atteindre un efficacité spectrale proche de l'unité par dimension. Les écarts ainsi obtenus montrent alors bien la sous-optimalité de la mise en forme par emboîtement pour une petite efficacité spectrale.

L'influence de la région de mise en forme est importante dans le cas des transmissions sur canal AWGN, mais les techniques employées pour améliorer les performances par rapport aux constellations QAM non-codées utilisent des algorithmes de décodage par sphère. Ces algorithmes sont envisageables pour de petites dimensions. Dans ce cas, les performances se révèlent excellentes, car :

1. la région de mise en forme est proche de l'optimale ;
2. le décodage utilisé mettant en œuvre un algorithme de décodage par sphère est également proche de l'optimal, et il est rendu possible par la nature linéaire du réseau de points. Cela reviendrait à décoder conjointement le codage correcteur d'erreurs et la modulation dans un schéma de type BICM.

Ainsi, pour des petites dimensions, c'est à dire pour des petites tailles de trame, ces réseaux de points peuvent avoir un intérêt par rapport à des schémas classiques de type BICM (Bit Interleaved Coded Modulation). Pour des tailles plus importantes, il faut abandonner la matrice génératrice et s'intéresser aux constructions des réseaux de points à l'aide des codes correcteurs, puis envisager des encodages de type modulation codée.

---

5. Il ne faut pas confondre cette mise en forme avec d'autres : nous considérons ici des points positionnés régulièrement dans l'espace et envoyés de manière équiprobable ; la mise en forme consiste à choisir les  $\eta^n$  points les plus proches de l'origine. En ce qui concerne les constellations de cardinal fini, la mise en forme consiste soit à modifier la distribution de probabilité de transmettre les symboles, soit la disposition géométrique des ces symboles

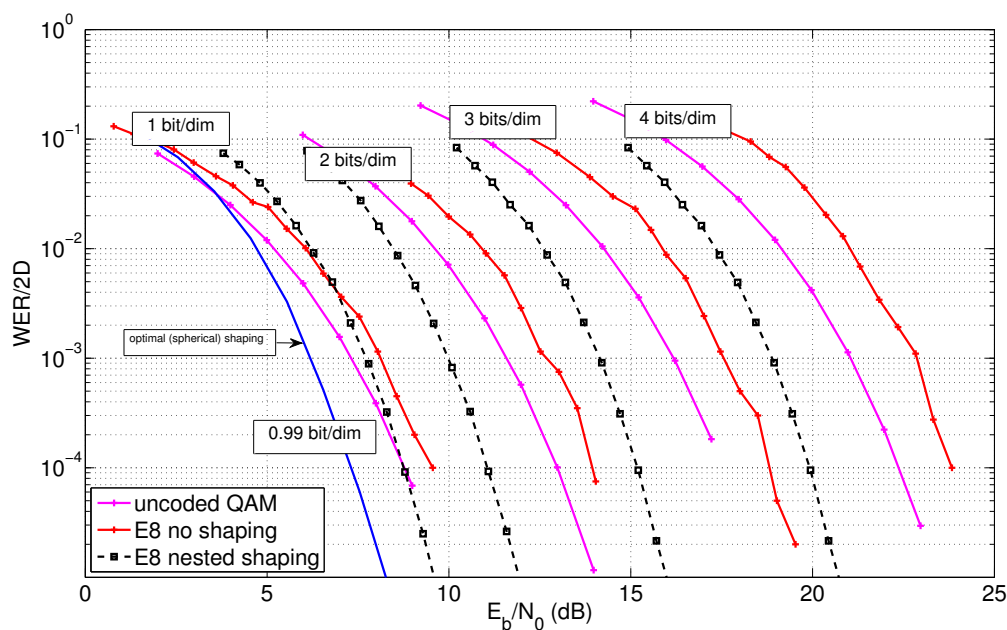


FIGURE 3.8 – Taux d’erreur (par 2 dimensions) d’une constellation QAM comparée à l’utilisation du réseau E8 pour différentes efficacités spectrales.

### 3.4.3 Réseaux de points et codage correcteur d’erreurs

Dans cette section, je souhaite expliquer que derrière certains réseaux de points se cachent des codes correcteurs d’erreurs. Je ne souhaite pas être exhaustif sur ce sujet et je renvoie le lecteur vers l’ouvrage de référence de Conway et Sloane [63] pour une approche plus exhaustive et approfondie de cette question. Mon objectif est seulement d’expliquer que de cette association entre réseaux de points et codage correcteur d’erreurs peuvent découler un encodage et un décodage de type modulation codée. Notons que ce n’est pas le cas de tous les réseaux de points, et qu’inversement toute modulation codée ne constitue pas forcément des symboles appartenant à un réseau de points.

#### Construction A

Il s’agit d’une des principales familles de construction de réseaux de points. Elle a été proposée à l’origine à partir de codes linéaires binaires, puis elle a été étendue à d’autres codes linéaires mais l’objectif n’étant pas d’être mathématiquement exhaustif, on se limitera ici aux codes linéaires binaires. Un réseau de points peut donc être obtenu à partir d’un code linéaire binaire de longueur  $n$  et de dimension  $k$  noté  $\mathcal{C}(n, k)$  en associant ses mots de code dans  $\mathbb{F}_2^n$  (l’ensemble des vecteurs binaires de longueur  $n$ ) à des vecteurs binaires dans  $\mathbb{R}^n$  selon la correspondance triviale  $0 \mapsto 0$  et  $1 \mapsto 1$  (on omettra par la suite de noter cette correspondance). Ensuite, on ajoute au vecteur ainsi obtenu et constitué uniquement de 0 et de 1 un vecteur d’entiers pairs quelconques pour obtenir un point quelconque du réseau. On écrira ainsi avec un certain abus le réseau de point  $\Lambda$  obtenu par construction A à partir du code linéaire binaire  $\mathcal{C}(n, k)$  par :

$$\Lambda = \mathcal{C}(n, k) + 2\mathbb{Z}^n \quad (3.2)$$

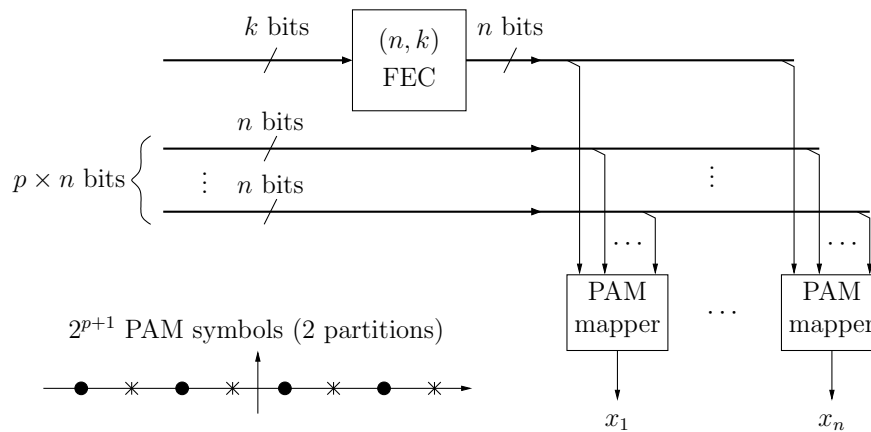


FIGURE 3.9 – Illustration de l’encodage de type modulation codée d’un réseau de points issu d’une construction de type A à partir d’un code linéaire binaire  $(n, k)$ .

Si l’on applique une opération modulo 2 à un tel réseau, on obtient donc le code sous-jacent. Ainsi, les réseaux  $D_n$  peuvent être obtenus par construction A avec le code binaire de parité  $(n, n - 1)$ , le réseau E8 avec le code de Hamming étendu  $(8, 4)$ .

A partir de cette construction, on peut mettre en œuvre un schéma de modulation codée faisant intervenir le codeur du code sous-jacent et une constellation de symboles. Ce type d’encodage ne fait pas apparaître les coordonnées entières générant un symbole du réseau de points à partir de sa matrice génératrice. La figure 3.9 illustre l’encodage d’un point du réseau  $\mathbf{x} = [x_1, \dots, x_n]$  associé à une modulation d’amplitude (PAM) à  $2^{p+1}$  symboles, où  $p$  est un entier positif ou nul permettant de faire varier l’efficacité spectrale donnée par  $\eta = (p + k)/n$  bits/dimension. Le symbole de la constellation est choisi pour chacune des dimensions  $i$  à l’aide du  $i$ -ème bit codé (la constellation est partitionnée en 2 sous-constellations) et les  $p$  bits non codés restants permettent de choisir le symbole PAM au sein de la sous-constellation.

L’intérêt d’une telle construction est donc de faire apparaître un encodage simple quelle que soit la dimension  $n$  du réseau. Cependant, si l’on souhaite augmenter la dimension  $n$  pour obtenir un réseau de grande dimension, ses performances en termes de taux d’erreur resteront limitées. En effet, le gain de codage est donné par le rapport entre le volume fondamental est la distance euclidienne minimale du réseau :

$$\gamma_c = \frac{d_{\min}^2}{V(\Lambda)^{2/n}}.$$

Or en construction A, on peut toujours obtenir un point du réseau avec le mot de code tout-à-zéro auquel on ajoute un vecteur d’entiers nuls sauf en une seule coordonnée qui vaut 2 ; on obtient ainsi un mot de distance euclidienne égale à  $\sqrt{2}$  par rapport à l’origine, qui est indépendante de la dimension. On voit donc que l’augmentation des performances du réseau de points par augmentation de sa dimension n’est pas valable en conservant une construction de type A. Il faut donc envisager d’autres types de construction.

## Décodage

Le décodage des points d’un réseau de points envoyés dans un canal gaussien peut se faire également en utilisant la structure du code sous-jacent comme dans le cas des modulations codées. No-

tamment, en observant l'équation 3.2 décrivant un réseau obtenu par construction A, on constate que les composantes du vecteurs sont toutes entières<sup>6</sup>, la parité de ces entiers étant dictée par les bits du mot de code.

Pour décoder le vecteur reçu  $\mathbf{y} = \mathbf{x} + \mathbf{w}$ , où  $\mathbf{w}$  est un vecteur de  $n$  échantillons de bruit issus d'une loi gaussienne de variance  $\sigma^2$ , une première solution naïve serait de prendre l'arrondi à l'entier le plus proche : mais l'arrondi n'est optimal que pour le réseau des entiers, pas pour les autres réseaux où les composantes ne sont plus indépendantes du fait du mot de code sous-jacent. On peut alors simplement prendre le modulo-2 des entiers obtenus après l'arrondi pour vérifier si le mot binaire est un mot du code. Si ce n'est pas le cas, on peut procéder au décodage binaire à décision ferme du code. Le mot de code décodé indique par comparaison avec le mot binaire à décoder les bits qui ont changé. Les bits qui sont devenus nuls indiquent que l'arrondi doit être fait vers l'entier pair le plus proche, et les bits qui sont devenus 1 indiquent que l'arrondi doit être fait vers l'entier impair le plus proche et enfin les bits qui n'ont pas changé indiquent que l'arrondi doit être conservé. Cependant cette technique est limitée par le pouvoir de correction en décodage ferme du code.

Pour réaliser le décodage pondéré du code, on doit calculer les fiabilités des éléments binaires obtenus après l'opération modulo-2. On calcule donc l'opération modulo-2 sur le vecteur reçu  $\mathbf{z} = \mathbf{y} \bmod 2 = (\mathbf{x} + \mathbf{w}) \bmod 2 = (\mathbf{x} \bmod 2 + \mathbf{w} \bmod 2) \bmod 2$ . La fiabilité du  $i$ -ème bit observé est donnée par le logarithme du rapport de vraisemblance (LLR) et définie par :

$$\text{LLR}_i = \ln \left( \frac{\Pr(y_i | c_i = 1)}{\Pr(y_i | c_i = 0)} \right)$$

Du fait de l'opération modulo-2, le bruit gaussien est "replié" c'est à dire que la densité de  $w_i \bmod 2$  est donnée par  $f_{w_i \bmod 2}(w_i) = \sum_{k \in \mathbb{Z}} \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{|w_i - 2k|^2}{2\sigma^2}\right)$ . Le LLR devient :

$$\text{LLR}_i = \ln \left( \frac{\sum_{c \in 2\mathbb{Z}} \exp\left(-\frac{|y_j - c + 1|^2}{2\sigma^2}\right)}{\sum_{c \in 2\mathbb{Z}} \exp\left(-\frac{|y_j - c|^2}{2\sigma^2}\right)} \right)$$

Les performances du décodeur de type modulation codée avec un décodage pondéré sont quasi-ML et identiques au décodeur par sphère comme l'illustre la comparaison faite sur la figure 3.10. On remarque également la perte obtenue avec un décodage ferme. Le schéma de construction A vu comme une modulation codée est donc particulièrement intéressant puisqu'il simplifie l'encodage et le décodage, si le décodage ML pondéré du code correcteur d'erreurs est de complexité raisonnable. Remarquons en revanche que les efficacités spectrales disponibles sont nécessairement de la forme  $p + 0.5$  bits par dimension, pour  $p$  entier, ce qui est moins souple que celui par matrice génératrice qui vaut  $\log_2(K)$  pour  $K$  entier positif.

Le calcul de ce LLR n'est pas très commode pour une implémentation mais un calcul approché classique consiste à prendre la distance entre l'échantillon  $z_i$  et le seuil de décision (0.5 ou 1.5 pour

6. En construction A, un facteur multiplicatif peut toujours être appliqué pour revenir à des composantes entières si ce n'est pas le cas



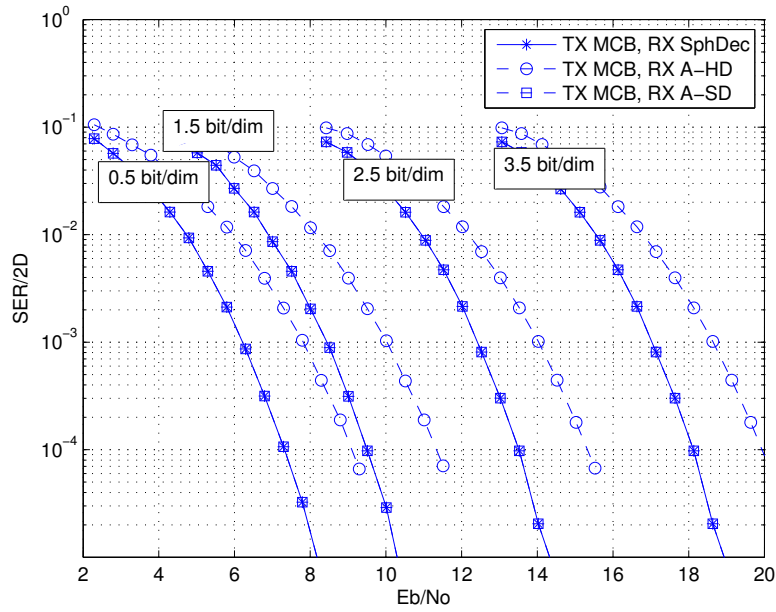


FIGURE 3.10 – Comparaison du décodage par sphère (RX SphDec) et du décodage de type modulation codée selon un décodage ML ferme (RX A-HD) ou ML pondéré (RX A-SD) du code sous-jacent du réseau E8 (code de Hamming étendu (8, 4, 4))

l'opération modulo-2) et à affecter le bon signe :

$$\text{LLR}_i (\text{distance}) = \min(|z_i - 0.5|, |z_i - 1.5|) \times (2([z_i] \bmod 2) - 1)$$

où  $[z_i]$  désigne l'arrondi de  $z_i$ . Cependant cette approximation reste relativement grossière. Je propose donc ci-après une approximation plus fine tout en restant peu complexe à calculer, et qui utilise l'approximation d'une densité gaussienne repliée par une distribution dite de Von Mises (ou encore appelée circulaire normale, ou encore de Tikhonov). La distribution de Von Mises est définie par :

$$f(\theta, \eta, \kappa) = \frac{\exp(\kappa \cos(\theta - \eta))}{2\pi I_0(\kappa)}$$

où  $\theta \in [0, 2\pi]$ ,  $\eta$  est la direction moyenne (ou angle moyen),  $\kappa \geq 0$  est appelé le paramètre de concentration et  $I_n(\kappa)$  est la fonction de Bessel modifiée de première espèce à l'ordre  $n$ . L'approximation d'une loi gaussienne repliée par une loi de Von Mises a été proposée dans [64] en posant la moyenne égale à  $\eta$  et la variance égale à  $-2 \ln(Q(\kappa))$  où  $Q(\kappa) = \frac{I_1(\kappa)}{I_0(\kappa)}$ . On en déduit une approximation de LLR par [65] :

$$\text{LLR}_i (\text{Von Mises}) = \kappa(\cos(\pi z_i - \pi) - \cos(\pi z_i))$$

où  $\kappa = Q^{-1}(\exp(-\sigma^2 \pi^2 / 2))$  peut être calculé hors-ligne par tabulation de la fonction  $Q^{-1}$ . La figure 3.11 illustre pour 2 variances différentes de bruit les allures des densités gaussiennes, gaussiennes repliées, leurs approximations par la densité de Von Mises et enfin les différents LLR obtenus (sans approximation, avec approximation de distance ou de Von Mises).

Le gain de performance obtenu en utilisant l'approximation du LLR proposée par rapport à celle utilisant la distance est illustré sur la figure 3.12 avec une construction A utilisant un code LDPC

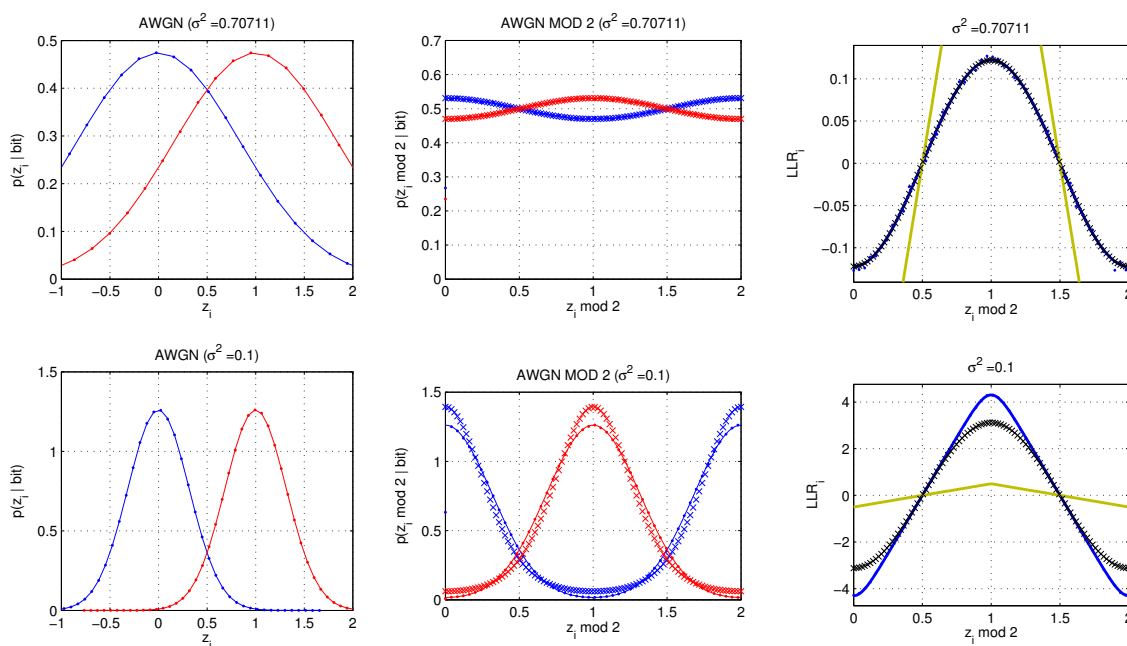


FIGURE 3.11 – Illustration pour 2 variances des densités gaussiennes (à gauche) des échantillons reçus pour une transmission d’un 1 (rouge) ou d’un 0 binaire (bleu), des densités gaussiennes repliées par le modulo-2 (au centre) et enfin à droite des LLR obtenus par simulation (points bleus), du LLR théorique sans approximation (courbe bleue), du LLR approximé selon la distance (courbe en vert) et selon Von Mises (croix noires)

(128,64). Les performances sont également comparées à la courbe du génie, c’est à dire à la performance obtenue lorsque le mot de code LDPC transmis est connu du récepteur.

### 3.4.4 Constructions multi-niveaux

L’augmentation de la dimension des réseaux de points pour améliorer le taux d’erreur doit se faire avec des techniques d’encodage et de décodage moins complexes qu’un décodage par sphère par exemple dont la complexité augmente exponentiellement avec la dimension. La construction A vue dans la section précédente est intéressante puisqu’elle permet de mettre en évidence un codage correcteur d’erreurs linéaire que l’on peut exploiter dans l’encodage et le décodage. Pour augmenter la distance euclidienne minimale avec la dimension du réseau, il faut cependant augmenter l’alphabet du code utilisé (codes  $q$ -aires avec  $q$  premier par exemple). Cela complique donc l’encodage et le décodage. Afin de conserver l’utilisation de code linéaires binaires, une construction appelée construction D permet d’améliorer le gain de codage des réseaux de points quand la dimension augmente. Cette construction généralise la construction A à plusieurs réseaux de points imbriqués, et utilise des codes correcteurs d’erreurs également imbriqués ; c’est aussi une forme de modulation codée utilisant plusieurs codes correcteurs d’erreurs : la modulation codée multi-niveaux [66] pour laquelle de nombreuses contributions ont été proposées (voir par exemple [67] pour une synthèse des concepts théoriques et des règles de conception).

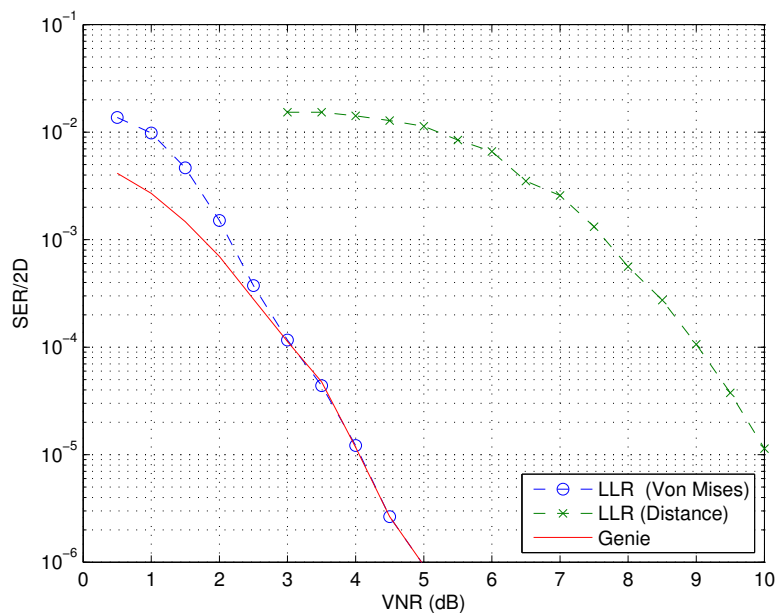


FIGURE 3.12 – Illustration du décodage d'un réseau de points ayant un code LDPC binaire sous-jacent (construction A) : le code LDPC est décodé de manière itérative en utilisant des LLR obtenus soit par l'approximation de type Distance, soit par l'approximation de type Von Mises.

### Construction D à une dimension

En utilisant la notation proposée dans [62] qui généralise l'expression 3.2 de la construction A, un réseau de points  $\Lambda$  peut être obtenu à partir d'une famille de  $a$  codes linéaires binaires imbriqués notés  $\{\mathcal{C}_i(n, k_i)\}$ ,  $1 \leq i \leq a$ , tels que  $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \dots \subseteq \mathcal{C}_a$ , par :

$$\Lambda = \mathcal{C}_1 + 2\mathcal{C}_2 + \dots + 2^{a-1}\mathcal{C}_a + 2^a\mathbb{Z}^n$$

On parle ici de construction D à une dimension car chaque composante d'un mot de code pondère une seule coordonnée du réseau. Les exemples les plus connus de constructions D sont le réseau de Leech à 24 dimensions obtenu avec  $a = 2$  codes (le code de Golay (24, 12, 8) et le code de parité (24, 23, 2)) et la famille des réseaux de Barnes-Wall de dimension  $n$ , notés  $\text{BW}(n)$ , qui sont obtenus à partir de familles de codes Reed-Muller ; en notant par  $\text{RM}(r, m)$  le code de Reed-Muller d'ordre  $r$  et de longueur  $2^m$ , on obtient par exemple le réseau réel avec  $m$  impair<sup>7</sup> par :

$$\text{BW}(2^m) = \sum_{\substack{1 \leq r' \leq m-1 \\ (m-1-r') \text{ impair}}} \text{RM}(r', m) 2^{\frac{r'-1}{2}} + 2^{(m-1)/2} \mathbb{Z}^{2^m}$$

7. Si  $m$  est pair, la même formule s'applique en changeant la parité de  $(m - r')$  sous le signe somme, ainsi que le coefficient multiplicatif du réseau d'entier par  $2^{\frac{m+1}{2}}$ .

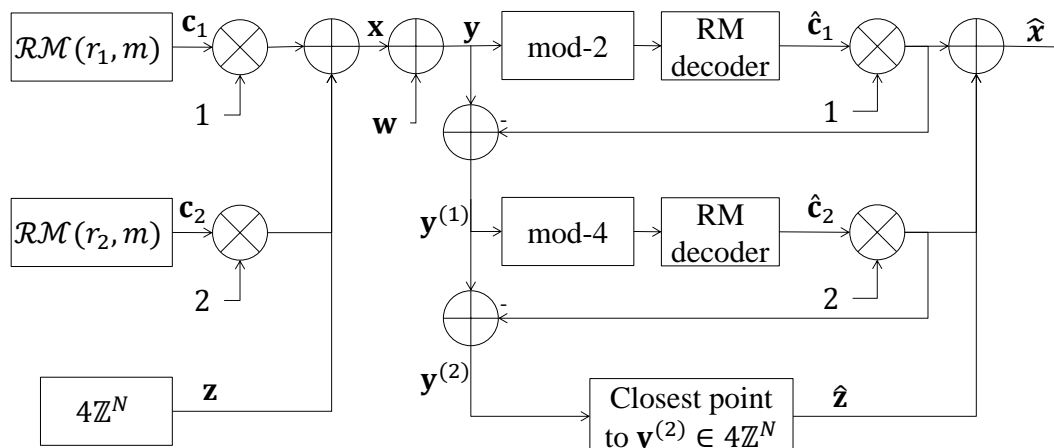


FIGURE 3.13 – Encodage et décodage multi-niveaux pour une construction D à une dimension et un réseau impliquant 2 codes de Reed-Muller, comme par exemple BW(16) ou BW(32) (extrait de [68]).

Ainsi par exemple :

$$\text{BW}(16) = \text{RM}(1, 4) + 2\text{RM}(3, 4) + 4\mathbb{Z}^{16}$$

$$\text{BW}(32) = \text{RM}(1, 5) + 2\text{RM}(3, 5) + 4\mathbb{Z}^{32}$$

$$\text{BW}(64) = \text{RM}(1, 6) + 2\text{RM}(3, 6) + 4\text{RM}(5, 6) + 8\mathbb{Z}^{64}$$

Le principe de l'encodage généralise celui de la construction A en s'inspirant directement des relations précédentes explicitant la construction. La figure 3.13 présente l'exemple d'un schéma d'encodage avec 2 niveaux de codes Reed-Muller. Le résultat de l'encodage est le vecteur  $\mathbf{x}$  dont les composantes entières ne sont pas associées à un schéma de modulation de type PAM par souci de simplification. Après transmission dans un canal AWGN (représenté par l'addition du vecteur d'échantillons de bruit  $\mathbf{w}$ ), le vecteur reçu  $\mathbf{y}$  est décodé par un décodeur multi-niveaux. Le principe consiste à filtrer toutes les composantes du mot reçu sauf une par l'opération "modulo" puis à décoder le code impliqué dans la composante restante. Le résultat de ce décodage est ensuite soustrait au mot reçu, puis on ré-itére ce processus avec la composante suivante.

### Construction D et partitions à $N$ dimensions

**Un partitionnement de réseau de point**  $\Lambda$  à l'aide d'un sous-réseau  $\Lambda'$  correspond à l'ensemble des décalages que l'on doit ajouter à  $\Lambda'$ , qui une fois réunis permettent de retrouver  $\Lambda$ . Par exemple, la réunion des décalages par les entiers  $\{0, 1, 2, 3\}$  du réseau des entiers multiples de 4 ( $\Lambda' = 4\mathbb{Z}$ ) permet de retrouver le réseau des entiers ( $\Lambda = \mathbb{Z}$ ). Comme  $4\mathbb{Z}$  est un sous-réseau de  $\mathbb{Z}$ , on écrira que  $\mathbb{Z}/(4\mathbb{Z})$  est un partitionnement de réseaux. Bien sur, dans l'exemple précédent, le 0 peut-être remplacé par n'importe quel entier multiple de 4, le 1 par n'importe quel entier multiplié de 4 plus 1, etc ... On peut donc en fait définir 4 classes (*cosets*) de décalage ( $4k, 4k + 1, 4k + 2$  et  $4k + 3$ , où

$k \in \mathbb{Z}$ ) pour retrouver le réseau des entiers à partir de  $4\mathbb{Z}$ ; mathématiquement, ces 4 classes forment un groupe quotient noté  $\mathbb{Z}/(4\mathbb{Z})$ . Comme ce groupe quotient est isomorphe à l'ensemble  $\{0, 1, 2, 3\}$  par l'opération modulo-4, un abus de notation usuel abouti à écrire que  $\mathbb{Z}/(4\mathbb{Z}) = \{0, 1, 2, 3\}$  avec l'addition modulo-4. Les entiers  $\{0, 1, 2, 3\}$  sont appelés les représentants de chacune des 4 classes (*coset representative*). Le nombre de classes (et donc de représentants) est appelé ordre de la partition et noté comme le cardinal du groupe quotient  $|\Lambda/\Lambda'|$ . Nous nous intéresserons par la suite aux partitionnements d'ordre 2 : c'est à dire qu'il n'y aura que 2 classes, soit autant que de symboles binaires dans l'alphabet des codes correcteurs linéaires binaires que nous souhaitons mettre en œuvre.

**Une chaîne de partitionnement** est un partitionnement d'un réseau de points  $\Lambda_1$  par un sous-réseau  $\Lambda_2$ , lui-même partitionné par un sous-réseau  $\Lambda_3$  de  $\Lambda_2$  etc ... Cette chaîne de partitionnement se note  $\Lambda_1/\Lambda_2/\dots/\Lambda_{a+1}$ . Dans le codage multi-niveaux à une dimension, on a utilisé la chaîne de partitionnement  $\mathbb{Z}/2\mathbb{Z}/\dots/2^{a+1}\mathbb{Z}$  où chaque niveau de partitionnement est associé à un code correcteur d'erreurs. Chaque symbole du  $i$ -ème code correcteur d'erreurs permet de choisir l'une des 2 classes de  $2^{i-1}\mathbb{Z}/2^i\mathbb{Z}$  dont les représentants sont  $\{0, 2^{i-1}\}$ . (Rappelons que l'on ne s'intéresse qu'aux chaînes de partitionnement binaires.)

**Partitionnement en dimension  $N$**  : les exemples précédents se sont intéressés au partitionnement du réseau d'entiers, c'est à dire au partitionnement d'un réseau à une dimension. En associant ce partitionnement à des codes correcteurs d'erreurs de longueur  $n$ , on a pu obtenir des réseaux de points de dimension  $1 \times n = n$ . Mais il est possible de partitionner un réseau de dimension plus grande. Par exemple, le réseau des points de l'espace à 2 dimensions dont les coordonnées sont entières,  $\mathbb{Z}^2$ , peut se partitionner selon la chaîne :  $\mathbb{Z}^2/R\mathbb{Z}^2/2\mathbb{Z}^2/2R\mathbb{Z}^2/\dots/2^{a+1}\mathbb{Z}^2/2^{a+1}R\mathbb{Z}^2$ , où  $R = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  est une matrice de rotation. Pour  $a = 4$ , les représentants des classes seront les couples de points  $\{(0, 0), (1, 0)\}$  pour le partitionnement  $\mathbb{Z}^2/R\mathbb{Z}^2$ ,  $\{(0, 0), (1, 1)\}$  pour le partitionnement  $R\mathbb{Z}^2/2\mathbb{Z}^2$ ,  $\{(0, 0), (2, 0)\}$  pour le partitionnement  $2\mathbb{Z}^2/2R\mathbb{Z}^2$  et  $\{(0, 0), (2, 2)\}$  pour le partitionnement  $2R\mathbb{Z}^2/4\mathbb{Z}^2$ . Dans ce cas, un réseau de points de dimension  $n$  pourrait être obtenu avec des codes binaires imbriqués de longueur  $n/2$ ; par exemple avec  $a = 4$  codes, on écrira :

$$\Lambda = (1, 0)\mathcal{C}_1 + (1, 1)\mathcal{C}_2 + (2, 0)\mathcal{C}_3 + (2, 2)\mathcal{C}_4 + (4\mathbb{Z}^2)^{n/2}.$$

On peut également partitionner le réseau de points à coordonnées entières en 4 dimensions  $\mathbb{Z}^4$  selon la chaîne :  $\mathbb{Z}^4/D_4/R\mathbb{Z}^4/RD_4/2\mathbb{Z}^4/2D_4/2R\mathbb{Z}^4/\dots$ , où  $D_4$  est le réseau  $D_n$  à 4 dimensions (voir le paragraphe sur la construction A à la section 3.4.3) et où

$$R = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

est une matrice de rotation multipliée par  $\sqrt{2}$ . Avec l'augmentation des dimensions, la recherche des représentants des classes du partitionnement est plus difficile [68]. On obtient par exemple les couples de points  $\{(0, 0, 0, 0), (1, 0, 0, 0)\}$  pour le partitionnement  $\mathbb{Z}^4/D_4$ ,  $\{(0, 0, 0, 0), (1, 0, 1, 0)\}$

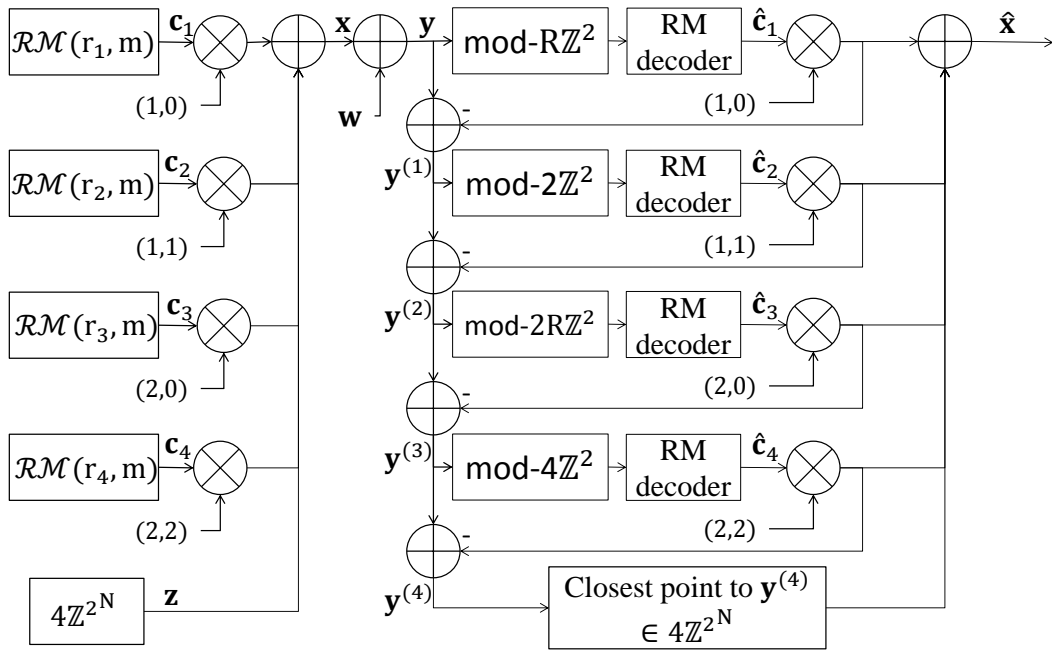


FIGURE 3.14 – Encodage et décodage multi-niveaux pour une construction D à 2 dimensions et un réseau impliquant 4 codes de Reed-Muller (extrait de [68])

pour le partitionnement  $D_4/RZ^4$ ,  $\{(0, 0, 0, 0), (1, 1, 0, 0)\}$  pour le partitionnement  $RZ^4/RD_4$  et  $\{(0, 0, 0, 0), (1, 1, 1, 1)\}$  pour le partitionnement  $RD_4/2Z^4$ . Dans ce cas, un réseau de points de dimension  $n$  pourrait être obtenu avec des codes binaires imbriqués de longueur  $n/4$ .

### Performances sur canaux gaussiens

Avec une construction multi-niveaux basée sur une partition à  $N$  dimensions, le décodage multi-niveaux reste analogue au décodage multi-niveaux basé sur une partition à 1 dimension. La seule différence est l'opération modulo au récepteur qui doit se faire non-pas modulo un entier mais modulo le réseau partitionnant à l'aide d'un algorithme de décodage par sphère, de façon générale, ou en appliquant un opérateur modulo sur chaque coordonnée pour les réseaux d'entiers. La figure 3.14 illustre le schéma de transmission dans le cas à  $N = 2$  dimensions. Les résultats de décodage en fonction du VNR sont présentés sur la figure 3.15 pour des réseaux de points en dimensions  $n = 1024$  et  $n = 4096$ . Ces réseaux ont été obtenus à partir d'une construction D multi-niveaux utilisant des codes de Reed-Muller, associés à des chaînes de partitionnement du réseau des entiers à 1, 2 et 4 dimensions. Le nombre de niveaux utilisé a été optimisé en fonction des courbes de capacité de chaque niveau [67]. La comparaison avec les réseaux Barnes-Wall qui sont construits avec un nombre plus grand de niveaux montre le gain apporté par l'utilisation du critère de capacité dans la construction des codes multi-niveaux. Cependant, l'augmentation de la dimension 1024 à la dimension 4096 n'apporte pas d'amélioration de performance : le décodage sous-optimal des codes de Reed-Muller et la propagation des erreurs entre les niveaux est sans doute l'explication de ce phénomène. Nous avons cependant préféré choisir de poursuivre l'étude par les canaux à évanouissements pour qui les réseaux de points associés aux canaux à relais ou aux canaux à accès multiples sont les plus promet-

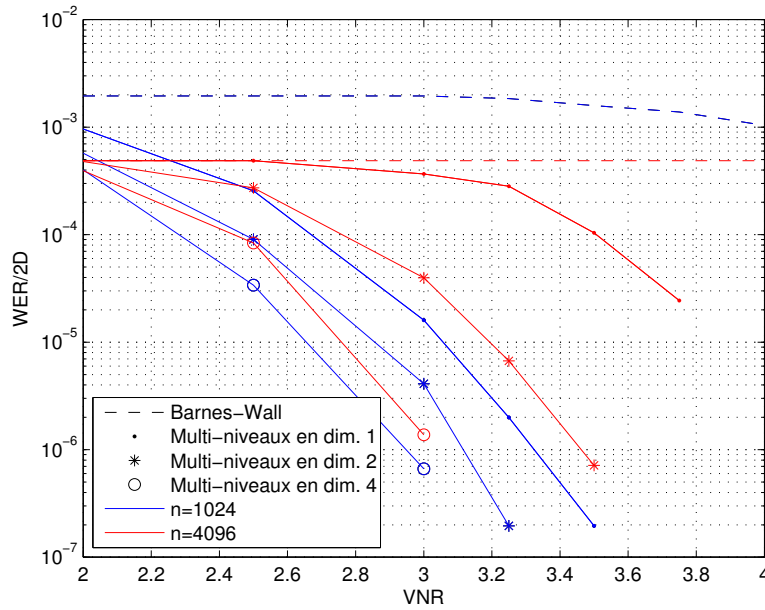


FIGURE 3.15 – Performances de réseaux de points de dimensions 1024 ou 4096, obtenus par construction multi-niveaux (construction D) associant des codes Reed-Muller à une chaîne de partitionnement des réseaux d'entiers à 1, 2 et 4 dimensions.

teurs [69, 70, 71, 72, 73, 74].

### Performance sur canaux à évanouissements

La difficulté à construire de bons réseaux de points pour les canaux gaussiens réside dans la difficulté à trouver des réseaux denses en dimension élevée (le problème est résolu pour la plupart des petites dimensions). En revanche, sur les canaux à évanouissements, la densité du réseau n'est pas un critère de bonne performance. La probabilité de décider un symbole  $\mathbf{x}_j$  alors que le symbole  $\mathbf{x}_i$  a été envoyé (probabilité d'erreur par paire) est bornée par :

$$\Pr(\mathbf{x}_i \rightarrow \mathbf{x}_j) \leq \frac{\left(\frac{8\sigma}{\mathbb{E}(|\mathbf{x}_i|^2)}\right)^{l_{i,j}}}{d_p^2(\mathbf{x}_i, \mathbf{x}_j)},$$

où  $d_p(\mathbf{x}_i, \mathbf{x}_j) = \prod_{\substack{k \leq n \\ x_{i,k} \neq x_{j,k}}} |x_{i,k} - x_{j,k}|$  est la distance produit qui se calcule sur les  $l_{i,j} \leq n$  composantes

des vecteurs  $\mathbf{x}_i$  et  $\mathbf{x}_j$  qui sont différentes. Asymptotiquement, la probabilité d'erreur est dominée par la plus petite valeur de  $l_{i,j}$ , notée  $L = \min(l_{i,j})$ , qui est donc le plus petit nombre de composantes différentes entre n'importe quels points  $\mathbf{x}_i$  et  $\mathbf{x}_j$  et que l'on appelle la diversité. Réduire le taux d'erreur implique donc de maximiser la diversité  $L$  et de minimiser la distance produit minimum. La théorie algébrique des nombres apporte un formalisme de construction de corps totalement réels pouvant garantir une diversité maximale égale à la dimension du réseau  $L = n$ , incluant les réseaux de points idéaux (*ideal lattices*) pour qui il est possible de relier la distance produit minimale avec des paramètres du réseau [75].

Dans la thèse de Carole Al Beschlawi et avec la collaboration de Jean-Claude Belfiore [68, 76],

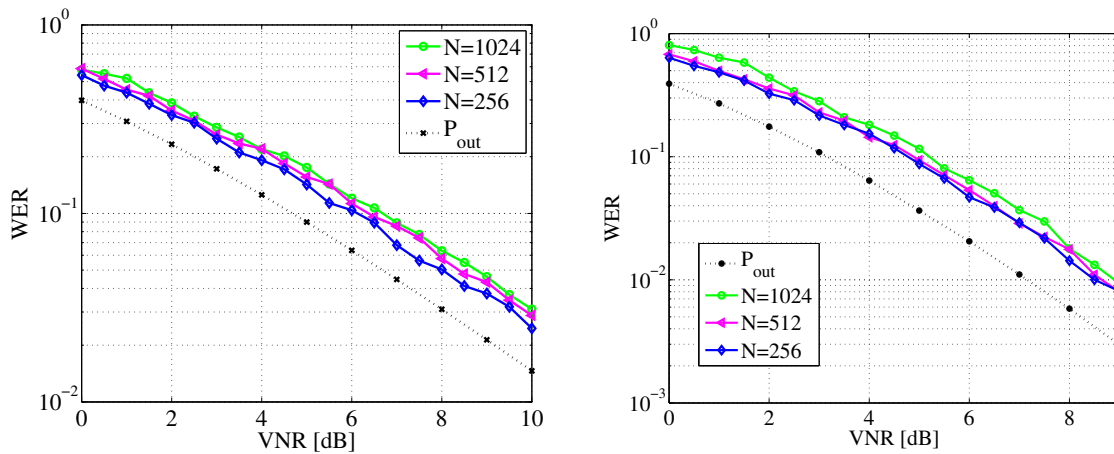


FIGURE 3.16 – Performances sur le canal à évanouissements par bloc des constructions multi-niveaux à partir de réseaux à 2 et 4 dimensions, extraites de [68], et comparaison à la probabilité de coupure  $P_{\text{out}}$ .  $N$  représente la dimension du réseau obtenu.

nous avons proposé des constructions multi-niveaux pour le canal à évanouissements par bloc en partant d'un partitionnement de réseaux à 2 et 4 dimensions. Le résultat obtenu est comme celui du cas gaussien, mais avec une matrice de rotation  $\mathbf{O}_2$  en plus, soit par exemple pour 2 dimensions :  $\mathbf{O}_2\mathbb{Z}^2 / \mathbf{O}_2R\mathbb{Z}^2 / \mathbf{O}_22\mathbb{Z}^2 / \mathbf{O}_22R\mathbb{Z}^2 / \mathbf{O}_24\mathbb{Z}^2$ , avec :

$$\mathbf{O}_2 = \begin{pmatrix} \sqrt{2 + \sqrt{2}} & \sqrt{2 + \sqrt{2}}(\sqrt{2} - 1) \\ \sqrt{2 - \sqrt{2}} & -\sqrt{2 - \sqrt{2}}(\sqrt{2} + 1) \end{pmatrix}.$$

Les représentants des classes sont obtenus en multipliant ceux du cas gaussien par la matrice de rotation ad hoc.

Les résultats de simulations obtenus pour des constructions multi-niveaux en partitionnant un réseau à 2 et 4 dimensions sont présentés sur la figure 3.16 pour différentes dimensions de réseaux. On constate que la perte par rapport à la probabilité de coupure reste pratiquement constante lorsque la dimension augmente, contrairement à des réseaux construits sans respecter la règle de la capacité [68].

### 3.4.5 Conclusions

Les réseaux de points pour les communications numériques constituent une structure algébrique de codage permettant i) d'atteindre la capacité de canal gaussien (la seule connue à ce jour), ii) d'améliorer les débits sur les réseaux sans-fil à relais par la technique de relayage de type calcul et envoi (*compute-and-forward*). L'objectif que je me suis fixé en ce qui concerne les réseaux de points est de comprendre si cette structure de codage n'a d'intérêt que théorique, et/ou asymptotique, ou si certaines d'entre elles peuvent se révéler compétitives dans un schéma pratique de communications sans fil par rapport aux schémas classiques associant codage correcteur d'erreurs, entrelacements et constellations usuelles.

Apporter une réponse à cette question nécessite un investissement important en temps et en ressources. Je compte à présent poursuivre cette thématique en étudiant des implémentations de codage



et de décodage des réseaux multi-niveaux que nous avons étudiés sur des canaux à accès multiples à relais. Il est indéniable que l'intrication des communications numériques et du codage correcteur d'erreurs font de l'étude des réseaux de points un sujet passionnant.

### 3.5 Conclusions

Ce chapitre a pour objectif de présenter la synthèse de mes activités dans le domaine de codage correcteur d'erreurs et des contributions que j'ai apportées au domaine à travers l'encadrement de stagiaires, doctorants, post-doctorants et le financement des projets auxquels j'ai participé. J'ai voulu présenter, à travers les codes LDPC, les codes Reed-Solomon et les codes basés sur les réseaux de points, toute la diversité que peut embrasser cette thématique qui, presque 25 ans après la découverte des turbocodes, reste scientifiquement riche et passionnante de questions et de problèmes.

Cette conclusion me permet d'aborder un point que je n'ai pas souhaité développer dans ce chapitre mais qui a été également présent dans mes activités de recherches : le codage correcteur d'erreurs appliqué à la couche application, qui du point de vue théorie de l'information équivaut au canal à effacement. En effet, avec l'augmentation du nombre de communications sur des ressources limitées, les voix de retour permettant l'acquiescement de la réception des paquets de données peuvent être rapidement saturées, ou même inexistantes en mode diffusion (*broadcast*). Ainsi, le codage correcteur d'erreurs peut permettre de récupérer un ou plusieurs paquets perdus, à partir des paquets reçus, sans avoir à en faire la demande avec une voix de retour. Il s'agit d'un modèle de canal à effacement, pour lequel les codes Reed-Solomon offriraient le meilleur rendement pour corriger un nombre donné de symboles effacés. Cependant, ces codes sont construits sur des corps finis dont la cardinalité augmente exponentiellement avec la taille (en bits) des symboles. Si les symboles étaient les paquets transmis, la taille du corps serait trop grande pour être implémentée. Ainsi, ce sont des codes à base de parités binaires qui sont employés.

Un exemple simple est le code appelé "COP#3", qui est utilisé pour la diffusion de flux MPEG. Il s'agit d'un code produit ayant des codes de parité comme codes constituants sur les lignes et les colonnes. Dans le projet Distrimage (2005-2008), j'ai travaillé sur le décodage de ce code dans un schéma itératif avec le décodage du code RS utilisé dans la couche physique.

De nouveaux types de codes de parité inspirés des codes LDPC sont apparus en 2002 pour cette couche applicative : les codes fontaines (*fountain codes*). Dans ce contexte, j'ai étudié les codes Raptor (seuls codes fontaines standardisés pour l'instant) dans le cadre d'une étude pour le compte du CNES et de la société Turboconcept (2006), puis dans le cadre d'une collaboration avec la société EMC Norway et l'encadrement d'Amine Semma (2014). J'ai également eu l'occasion de travailler sur le projet ForWin (2008) où nous avons associé le codage de type fontaine aux réseaux tolérants aux délais (DTN). Depuis octobre 2015 et jusqu'en novembre 2016 avec le co-encadrement de Yupeng Tai, doctorant à la Chinese Academy of Science, en visite dans notre département pendant un an et financé par le Chinese Scholarship Council, nous étudions l'utilisation des codes LT et des codes spinaux (*spinal codes*) dans les canaux acoustiques sous-marins. Ces canaux sont difficiles et nous souhaitons mettre en évidence l'intérêt de travailler avec des trames courtes en utilisant ces nouveaux type de codes.

### 3.6 Bibliographie

- [1] Dai Kimura, Ramesh Pyndiah, and Frédéric Guilloud. Multiple-Input-Multiple-Output Transmission Using Non-Binary LDPC Coding, 2006.
- [2] Dai Kimura, Ramesh Pyndiah, and Frédéric Guilloud. Construction of Parity Check Matrices for Non-Binary LDPC Codes, 2006.
- [3] Dai Kimura, Ramesh Pyndiah, and Frédéric Guilloud. Construction of parity-check matrices for non-binary LDPC codes. In *4th international symposium on turbo codes and related topics, Munich, Allemagne, April 3-7, 2006*.
- [4] Dai Kimura, Frédéric Guilloud, and Ramesh Pyndiah. Application of non-binary LDPC codes for small packet transmission in vehicle communications. In *5th International Conference on ITS telecommunications, Brest, France, pages 109 – 112, June 27-29, 2005*.
- [5] Sanae El Hassani, Frédéric Guilloud, Ramesh Pyndiah, Pierre Penard, and Marie-Hélène Hamon. New Optimizations for Layered Non-Binary LDPC Codes Decoding. *International Journal of Applied Research on Information Technology and Computing*, 3(1), May 2012.
- [6] R.G. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8:21–28, Jan. 1962.
- [7] D.J.C MacKay and R.M. Neal. Good codes based on very sparse matrices. In *5th IMA Conference on Cryptography and Coding, Berlin, Germany, 1995*. Springer.
- [8] D. Sridhara and T. E. Fuja. Low density parity check codes over groups and rings. In *Information Theory Workshop, 2002. Proceedings of the 2002 IEEE*, pages 163–166, Oct 2002.
- [9] A. Goupil, M. Colas, G. Gelle, and D. Declercq. On belief propagation decoding of ldpc codes over groups. In *Turbo Codes Related Topics ; 6th International ITG-Conference on Source and Channel Coding (TURBOCODING), 2006 4th International Symposium on*, pages 1–4, April 2006.
- [10] A. Goupil, M. Colas, G. Gelle, and D. Declercq. Fft-based bp decoding of general ldpc codes over abelian groups. *IEEE Transactions on Communications*, 55(4):644–649, April 2007.
- [11] Tuvi Etzion, Ari Trachtenberg, and Alexander Vardy. Which codes have cycle-free tanner graphs ?. *IEEE Transactions on Information Theory*, 45, Sept. 1999.
- [12] M.P.C. Fossorier, M. Mihaljević, and I. Imai. Reduced complexity iterative decoding of low-density parity-check codes based on belief propagation. *Transactions on Communications*, 47:673–680, May 1999.
- [13] V. Savin. Self-corrected min-sum decoding of ldpc codes. In *2008 IEEE International Symposium on Information Theory*, pages 146–150, July 2008.
- [14] D. Declercq and M. Fossorier. Extended minsum algorithm for decoding ldpc codes over  $gf(q)$ . In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 464–468, Sept. 2005.
- [15] V. Savin. Min-max decoding for non binary ldpc codes. In *2008 IEEE International Symposium on Information Theory*, pages 960–964, July 2008.

- [16] S. El Hassani. *Optimisation du décodage des codes LDPC non-binaires pour leur implémentation*. PhD thesis, SC - Dépt. Signal et Communications (Institut Mines-Télécom-Télécom Bretagne-UEB), UR1 - Université de Rennes 1, UEB - Université Européenne de Bretagne (UEB), 2011.
- [17] F.R. Kschischang and B.J. Frey. Iterative decoding of compound codes by probability propagation in graphical models. *Journal on Selected Areas in Communications*, 16:219–230, 1998.
- [18] E. Yeo, B. Nikolić, and V. Anantharam. High throughput low-density parity-check decoder architectures. In *IEEE Globecom, San Antonio*, Nov. 25-29, 2001.
- [19] Juntan Zhang and M. Fossorier. Shuffled belief propagation decoding. In *Signals, Systems and Computers, 2002. Conference Record of the Thirty-Sixth Asilomar Conference on*, 3-6 Nov. 2002.
- [20] M.M. Mansour and N.R. Shanbhag. Turbo decoder architectures for low-density parity-check codes. In *Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, Nov 17 - 21, 2002.
- [21] O. S. Chauhan, T. K. Moon, and J. H. Gunther. Accelerating the convergence of message passing on loopy graphs using eigenmessages. In *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Seventh Asilomar Conference on*, volume 1, pages 79–83 Vol.1, Nov 2003.
- [22] S. Planjery, D. Divsalar, K. Andrewsand, S. Dolinar, and J. Hamkins. Trapping sets and ldpc decoder performance. *CCSDS Fall Meeting*, Berlin, Oct. 2008.
- [23] E. Alghonaim, A. El-Maleh, and M. A. Landolsi. New technique for improving performance of ldpc codes in the presence of trapping sets. *EURASIP Journal on Wireless Communications and Networking*, 2008.
- [24] R. Aoyama and Y. Kaji. Improvement of the forced-convergence decoding for ldpc codes. In *Information Theory and Its Applications, 2008. ISITA 2008. International Symposium on*, pages 1–6, Dec 2008.
- [25] Yongyi Mao and A. H. Banihashemi. Decoding low-density parity-check codes with probabilistic scheduling. *IEEE Communications Letters*, 5(10):414–416, Oct 2001.
- [26] D. Levin, E. Sharon, and S. Li. Lazy scheduling for ldpc decoding. *IEEE Communications Letters*, 11(1):70–72, Jan 2007.
- [27] E. Zimmermann, W. Rave, and G. Fettweis. Forced convergence decoding of ldpc codes - exit chart analysis and combination with node complexity reduction techniques. In *Wireless Conference 2005 - Next Generation Wireless and Mobile Communications and Services (European Wireless), 11th European*, pages 1–8, April 2005.
- [28] G. Elidan, I. McGraw, and D. Koller. Residual Belief Propagation : Informed Scheduling for Asynchronous Message Passing. In *22nd Conference on Uncertainty in Artificial Intelligence (UAI2006)*, 2006.
- [29] V. Savin. Iterative ldpc decoding using neighborhood reliabilities. In *2007 IEEE International Symposium on Information Theory*, pages 221–225, June 2007.
- [30] A. I. V. Casado, M. Griot, and R. D. Wesel. Improving ldpc decoders via informed dynamic scheduling. In *Information Theory Workshop, 2007. ITW '07. IEEE*, pages 208–213, Sept 2007.

- [31] J. H. Kim, M. Y. Nam, H. Y. Song, and K. M. Lee. Variable-to-check residual belief propagation for informed dynamic scheduling of ldpc codes. In *Information Theory and Its Applications, 2008. ISITA 2008. International Symposium on*, pages 1–4, Dec 2008.
- [32] 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*, 56(10):1626–1635, October 2008.
- [33] X. Y. Hu and E. Eleftheriou. Binary representation of cycle tanner-graph  $gf(2b)$  codes. In *Communications, 2004 IEEE International Conference on*, volume 1, pages 528–532 Vol.1, June 2004.
- [34] G. Li, I. J. Fair, and W. A. Krzymien. Density evolution for nonbinary ldpc codes under gaussian approximation. *IEEE Transactions on Information Theory*, 55(3):997–1015, March 2009.
- [35] C. Poulliat, C. Poulliat, M. Fossorier, and D. Declercq. Using binary images of non binary ldpc codes to improve overall performance. In *Turbo Codes Related Topics ; 6th International ITG-Conference on Source and Channel Coding (TURBOCODING), 2006 4th International Symposium on*, pages 1–6, April 2006.
- [36] S. V. S. Ranganathan, D. Divsalar, K. Vakilinia, and R. D. Wesel. Design of high-rate irregular non-binary ldpc codes using algorithmic stopping-set cancellation. In *2014 IEEE International Symposium on Information Theory*, pages 711–715, June 2014.
- [37] G. Solomon I. S. Reed. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.
- [38] Andrzej Michal Kabat, Frédéric Guilloud, and Ramesh Pyndiah. New approach to order statistics decoding of long linear block codes. In *GLOBECOM'07 : 50th annual IEEE Global telecommunications conference, November 26-30, Washington, USA, 2007*.
- [39] Andrzej Michal Kabat, Frédéric Guilloud, and Ramesh Pyndiah. On the sensibility of the arranged list of the most a priori likely tests algorithm. In *MILCOM'07 : Military communications conference, October 29-31, Orlando, Florida, USA, 2007*.
- [40] Raphaël Le Bidan, Andrzej Kabat, Samar Changuel, Frédéric Guilloud, and Ramesh Pyndiah. Décodage à entrée et sortie pondérée des codes de reed-solomon et ses applications. CRE France Telecom R& D 3ZCIF406, ENST-Bretagne, November 2007.
- [41] R. Le Bidan, R. Pyndiah, and P. Adde. Some results on the binary minimum distance of reed-solomon codes and block turbo codes. In *2007 IEEE International Conference on Communications*, pages 990–994, June 2007.
- [42] D. Gorenstein and N. Zierler. A class of cyclic linear error-correcting codes in  $p^m$  symbols. *Journal of the Society for Industrial and Applied Mathematics*, 9:207–214, June 1961.
- [43] J. Massey. Shift-register synthesis and bch decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, Jan 1969.
- [44] E.R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill series in systems science. Aegean Park Press, 1984.
- [45] Yasuo Sugiyama, Masao Kasahara, Shigeichi Hirasawa, and Toshihiko Namekawa. A Method for Solving Key Equation for Decoding Goppa Codes. *Information and Control*, 27(1):87–99, 1975.

- [46] R. Chien. Cyclic decoding procedures for bose- chaudhuri-hocquenghem codes. *IEEE Transactions on Information Theory*, 10(4):357–363, Oct 1964.
- [47] G. Forney. On decoding bch codes. *IEEE Transactions on Information Theory*, 11(4):549–557, Oct 1965.
- [48] Daniel J. Costello Shu Lin. *Error Control Coding (2nd Edition)*. Prentice Hall, 2 edition, 2004.
- [49] M. El-Khamy and R. McEliece. Bounds on the average binary minimum distance and the maximum likelihood performance of Reed–Solomon codes. In *42nd Annual Allerton Conference*, pages 290–299, October 2004.
- [50] Andrzej Kabat. *Contributions au codage correcteur d’erreurs : décodage pondéré des codes de Reed-Solomon et codage distribué pour les communications coopératives sans fil*. PhD thesis, Telecom Bretagne, 2009.
- [51] J. Bellorado, A. Kavcic, and Li Ping. Soft-input, iterative, reed-solomon decoding using redundant parity-check equations. In *Information Theory Workshop, 2007. ITW ’07. IEEE*, pages 138–143, Sept 2007.
- [52] Jing Jiang and K. R. Narayanan. Iterative soft decoding of reed-solomon codes. *IEEE Communications Letters*, 8(4):244–246, April 2004.
- [53] D. Chase. Class of algorithms for decoding block codes with channel measurement information. *IEEE Transactions on Information Theory*, 18(1):170–182, Jan 1972.
- [54] B. Dorsch. A decoding algorithm for binary block codes and  $j$ -ary output channels (corresp.). *IEEE Transactions on Information Theory*, 20(3):391–394, May 1974.
- [55] M. P. C. Fossorier and Shu Lin. Soft-decision decoding of linear block codes based on ordered statistics. *IEEE Transactions on Information Theory*, 41(5):1379–1396, Sep 1995.
- [56] D. Gazelle and J. Snyders. Reliability-based code-search algorithms for maximum-likelihood decoding of block codes. *IEEE Transactions on Information Theory*, 43(1):239–249, Jan 1997.
- [57] Antoine Valembois and Marc Fossorier. A comparison between "most-reliable-basis reprocessing" strategies. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E85-A(7):1727–1741, July 2002.
- [58] Y. Wu and C. N. Hadjicostis. Soft-decision decoding using ordered recordings on the most reliable basis. *IEEE Transactions on Information Theory*, 53(2):829–836, Feb 2007.
- [59] D. J. Taipale and M. B. Pursley. An improvement to generalized-minimum-distance decoding. *IEEE Transactions on Information Theory*, 37(1):167–172, Jan 1991.
- [60] W. Jin and M. Fossorier. Probabilistic sufficient conditions on optimality for reliability based decoding of linear block codes. In *2006 IEEE International Symposium on Information Theory*, pages 2235–2239, July 2006.
- [61] R. Kerr and J. Lodge. Near ml performance for linear block codes using an iterative vector siso decoder. In *Turbo Codes Related Topics; 6th International ITG-Conference on Source and Channel Coding (TURBOCODING), 2006 4th International Symposium on*, pages 1–6, April 2006.
- [62] G. D. Forney, M. D. Trott, and Sae-Young Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *IEEE Transactions on Information Theory*, 46(3):820–850, May 2000.

- [63] John Conway and Neil J. A. Sloane. *Sphere Packings, Lattices and Groups*. Springer New York, 2010.
- [64] N. I. Fisher. Problem with the current definition of the standard deviation of wind direction. *Journal of Climate and Applied Meteorology*, 26:1522–1529, 1987.
- [65] Carole Al Bechlawi and Frédéric Guilloud. Efficient LLR Estimation for Multistage Decoding . *Electronics letters*, 51(14):1076 – 1078, July 2015.
- [66] H. Imai and S. Hirakawa. A new multilevel coding method using error-correcting codes. *IEEE Transactions on Information Theory*, 23(3):371–377, May 1977.
- [67] U. Wachsmann, R. F. H. Fischer, and J. B. Huber. Multilevel codes : theoretical concepts and practical design rules. *IEEE Transactions on Information Theory*, 45(5):1361–1391, Jul 1999.
- [68] Carole Al Beschlawi. *On Lattice Coding for Point-to-Point Communications over AWGN and Fading Channels : Design and Implementation*. PhD thesis, Telecom Bretagne, 2016.
- [69] Yiwei Song and N. Devroye. Lattice codes for the Gaussian relay channel : Decode-and-forward and compress-and-forward. *IEEE Transactions on Information Theory*, 59(8):4927–4948, Aug 2013.
- [70] Chen Feng, D. Silva, and F.R. Kschischang. Design criteria for lattice network coding. In *45th Annual Conference on Information Sciences and Systems (CISS)*, March 2011.
- [71] B. Nazer and M. Gastpar. Compute-and-forward : Harnessing interference through structured codes. *IEEE Transactions on Information Theory*, 57(10):6463–6486, Oct 2011.
- [72] Chung-Pi Lee, Shih-Chun Lin, Hsuan-Jung Su, and H.V. Poor. Multiuser lattice coding for the multiple-access relay channel. *IEEE Transactions on Wireless Communications*, 13(7):3539–3555, July 2014.
- [73] J.-C. Belfiore and F. Oggier. Lattice code design for the Rayleigh fading wiretap channel. In *IEEE International Conference on Communications Workshops (ICC)*, June 2011.
- [74] C. Feng, D. Silva, and F. R. Kschischang. An algebraic approach to physical-layer network coding. *IEEE Transactions on Information Theory*, 59(11):7576–7596, Nov 2013.
- [75] F. Oggier and E. Viterbo. *Algebraic Number Theory and Code Design for Rayleigh Fading Channels*. Foundations and trends in communications and information theory. Now, 2004.
- [76] Carole Al Besclawi, Jean-Claude Belfiore, and Frédéric Guilloud. Reed-muller lattice coding for the rayleigh block fading channel. In *IEEE Wireless Communications and Networking Conference, WCNC 2016*, April 2016.



## Chapitre 4

# Communications sans fils et réduction de consommation

### 4.1 Introduction

Le gain de codage apporté par le codage correcteur d'erreurs permet de travailler à des rapports signaux-à-bruit plus faibles. La possibilité de travailler à des rapports signaux à bruits plus faibles peut être mise à profit de deux manières : soit pour augmenter la bande passante du signal transmis, et donc le débit, soit pour réduire la puissance de l'émetteur et ainsi économiser de l'énergie de transmission (diffusion), augmenter la durée d'utilisation d'une batterie avant son rechargement (téléphone portable) ou permettre à un système autonome en énergie et avec une maintenance limitée d'avoir la plus longue durée de vie possible (réseaux de capteurs, compteurs intelligents de fluides).

Cependant, d'autres leviers existent pour réduire la consommation d'énergie. Notamment, le traitement numérique au niveau de la bande de base, et la puissance liée à la transmission radio [17]. En ce qui concerne la transmission radio, la conception de l'amplificateur de puissance joue un rôle important dans la consommation de la partie radio : en effet, cette consommation est constituée d'une part de la puissance du signal transmis, mais également de la puissance consommée par l'amplificateur de puissance. Cette puissance dépend de la technologie de l'amplificateur (classe A/B, classe C etc ...) et de sa tension d'alimentation. Or la conception de l'amplificateur de puissance va directement dépendre de la dynamique du signal que l'on souhaite émettre.

La figure 4.1 illustre comment la dynamique d'un signal à amplifier influence la puissance consommée par un amplificateur. La figure montre dans 2 cas différents (petite et grande dynamique) la caractéristique reliant la puissance instantanée de sortie à la puissance instantanée d'entrée (homogène à l'amplitude du signal au carré). Si le signal à amplifier est distordu par une caractéristique non linéaire de l'amplificateur, le taux d'erreur de la transmission risque de se dégrader. On doit donc faire en sorte que toute la dynamique du signal à amplifier soit dans la partie linéaire de la caractéristique de l'amplificateur, c'est à dire loin de la puissance maximum que peut délivrer l'amplificateur, et donc loin de sa puissance d'alimentation. Si la dynamique du signal augmente, il faut agrandir la partie linéaire de l'amplificateur, et donc augmenter sa puissance d'alimentation, et donc sa consommation. La dynamique des signaux est habituellement quantifiée par le rapport entre la puissance max et la puissance moyenne du signal considéré (PAPR pour Peak-to-Average Power Ratio) et se mesure en



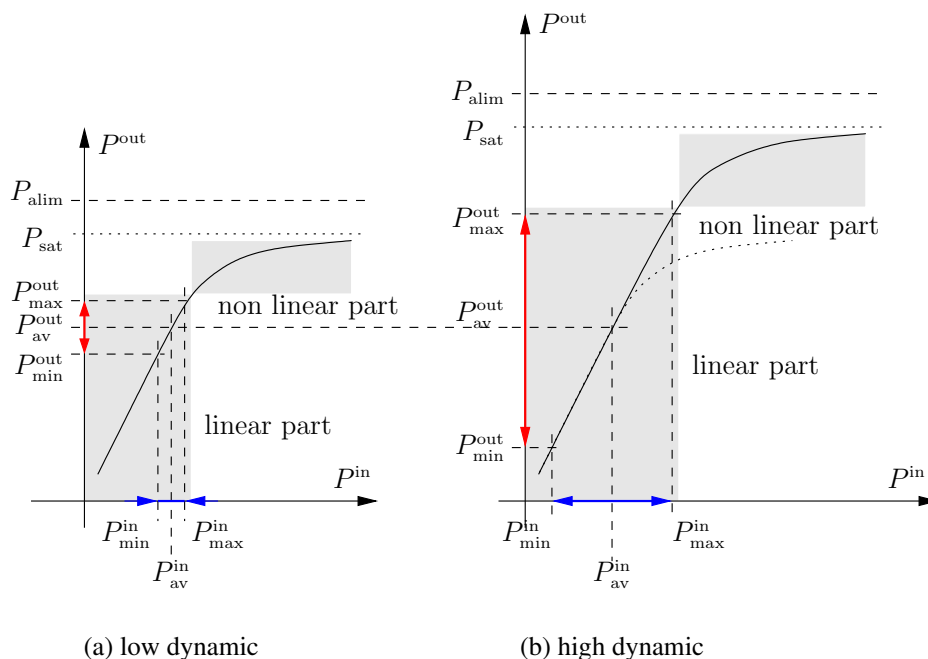


FIGURE 4.1 – La consommation d’un amplificateur dépend de sa tension d’alimentation, qui elle-même dépend de la dynamique du signal d’entrée ((a) faible ou (b) forte) pour une même puissance moyenne de sortie et un même gain.

échelle logarithmique :

$$\text{PAPR} = 10 \log_{10} \frac{P^{\max}}{P^{\text{av.}}}$$

Dans ce chapitre, je propose de décrire deux techniques permettant de réduire la consommation d’énergie au niveau de l’amplificateur. La première concerne les signaux de modulations multiporteuses orthogonales (OFDM) qui présente la caractéristique d’avoir une très grande dynamique. Dans la thèse de Hyunseuk Yoo [54] que j’ai co-encadrée entre 2008 et 2011, nous avons travaillé sur des techniques de réduction du rapport entre la puissance maximale et la puissance moyenne (PAPR) des signaux OFDM. La synthèse de ces travaux est présentée en section 4.2.

La famille de modulations présentant le PAPR le plus faible est celle des modulations dites à enveloppe constante dont font partie les modulations à phase continue. Dans la section 4.3, je présente les travaux que j’ai menés dans cette thématique inspirée par les applications de télémétrie, à travers la thèse de Malek Messai [29] dirigée par Karine Amis et soutenue en novembre 2015.

## 4.2 Réduction de PAPR dans les modulations OFDM

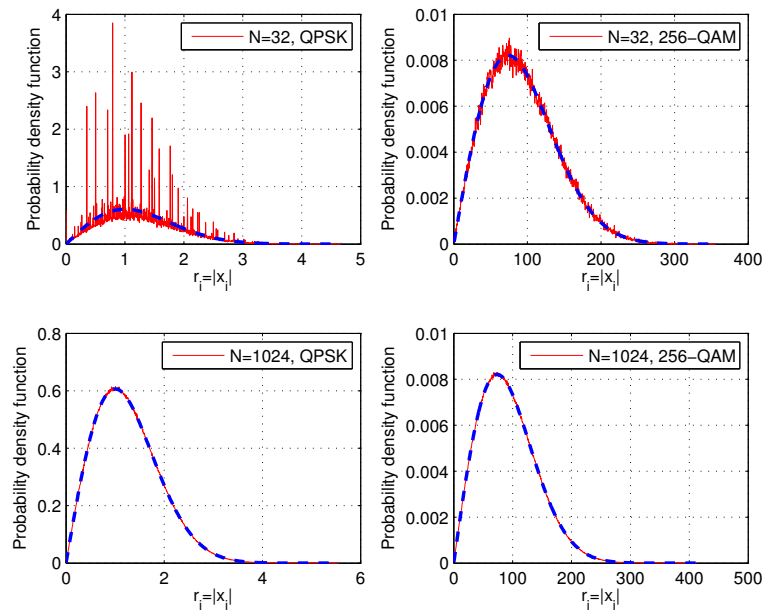
### 4.2.1 Etat de l’art

#### Définitions

Les modulations OFDM permettent de transmettre l’information sur des sous-bandes fréquentielles suffisamment étroite devant la bande de cohérence du canal (multiplexage fréquentiel) permettant la simplification de l’égalisation. De plus, les sous-bandes sont superposées deux-à-deux permettant une utilisation efficace de la bande fréquentielle disponible (bonne efficacité spectrale).



FIGURE 4.2 – Schéma de transmission et de réception de base pour la modulation OFDM

FIGURE 4.3 – Histogramme des amplitudes des échantillons dans le domaine temporel pour 32 ou 1024 sous-porteuses, et pour une QPSK et une QAM-256. Lorsque le nombre de sous-porteuses est suffisamment important, l'approximation gaussienne des échantillons  $x_i$  en sortie de IFFT est valable, d'autant plus si le nombre de symboles dans la constellation est élevé.

Le modèle de transmission et de réception utilisé est illustré sur la figure 4.2 :  $K_d$  éléments binaires d'information constituant le vecteur  $\mathbf{d}$  sont encodées par un codage correcteur d'erreurs en le mot de code  $\mathbf{c}$  de longueur  $N_{cw}$  puis les bits codés sont associés aux symboles de modulation pour former le vecteur de  $N$  symboles  $\mathbf{X}$ , chaque symbole étant associé à une sous-porteuse. Le vecteur d'échantillons dans le domaine temporel  $\mathbf{x}$  est obtenu par transformée de Fourier inverse (IFFT) de taille  $N$ . La suite des opérations est constituée de l'ajout du préfixe cyclique (CP) puis de la conversion numérique-analogique (CNA) et enfin des fonctions radio-fréquences (RF).

La grande dynamique des amplitudes des composantes de  $\mathbf{x}$  est due à la transformée de Fourier inverse qui tend à blanchir les échantillons en sortie lorsque le nombre de sous-porteuses  $N$  augmente (théorème central limite), donnant ainsi une distribution de type Rayleigh aux amplitudes des composantes de  $\mathbf{x}$  pour  $N$  grand ou pour une taille de constellation grande, comme l'illustre la figure 4.3.

Plutôt que sa densité de probabilité, le PAPR est souvent caractérisé par sa fonction de répartition réciproque (CCDF), c'est à dire la probabilité qu'il dépasse un certain seuil. On note  $\lambda$  le PAPR du

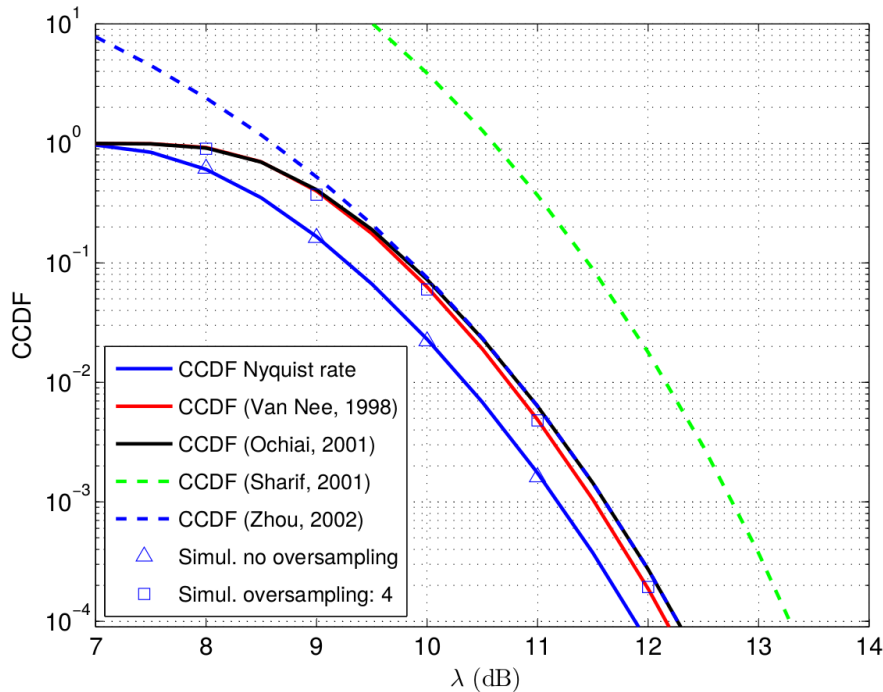


FIGURE 4.4 – Comparaison de l'approximation au temps symbole de la fonction de répartition réciproque du PAPR par rapport à d'autres modèles à temps continu ou sur-échantillonné : [60] Van Nee, 1998, [40] Ochiai, 2001, [45] Sharif, 2001, [58] Zhou, 2002. (extrait de [54])

signal OFDM discrétisé au temps symbole, et on le définit par :

$$\lambda = \frac{\max_{m \in [1, N]} |x_m|^2}{\frac{1}{N} \sum_{m=1}^N |x_m|^2}$$

En pratique cependant, le PAPR est lié au signal continu obtenu après conversion numérique analogique et l'expression précédente n'est qu'une approximation. De nombreux travaux ont modélisé la CCDF du signal OFDM continu, ou sur-échantillonné comme l'illustre la figure 4.4. On constate que la CCDF du signal échantillonné au temps symbole est une borne inférieure sur la CCDF, et donc une borne supérieure sur les performances. Dans la suite de ce travail, le sur-échantillonnage ne sera pas pris en compte.

Le PAPR se dégrade lorsque le nombre de sous-porteuses augmente, comme le montre la figure 4.5 où l'on observe pour différentes valeurs de CCDF le seuil en dB nécessaire en fonction du logarithme base 2 du nombre de sous-porteuses. Ainsi, pour 1024 sous-porteuses, il y aura une chance sur 10 (CCDF =  $10^{-1}$ ) d'être en dessous d'un PAPR de 9.6 dB, et cela augmente à une chance sur 10 d'être en dessous de 10.2 dB pour 4096 porteuses. Bien entendu, plus la probabilité est faible d'être en dessous d'un certain seuil, moins il y a de risques de distordre le signal ; plus ce même seuil est faible, plus on peut se permettre de diminuer la plage linéaire de l'amplificateur.

### Techniques classiques de réduction de PAPR

Il existe plusieurs techniques permettant de réduire le PAPR d'un signal OFDM portant une information numérique [19, 26, 54]. On peut distinguer tout d'abord le simple seuillage (clipping), qui va écrêter le signal à une amplitude maximale mais également distordre l'information. Il existe

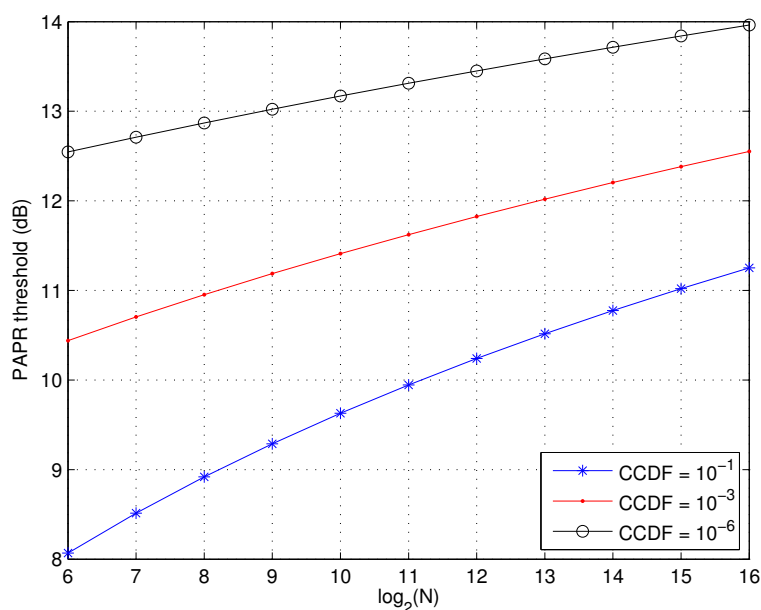


FIGURE 4.5 – Dégradation du PAPR avec l’augmentation du nombre de sous-porteuses.

TABLE 4.1 – Comparaison des techniques de réduction de PAPR

Distorsion	Augmentation de puissance	Diminution de débit
Clipping [41]	Tone Injection (TI) [52, 14], Active Constellation Extension (ACE) [53]	Coding [22], Tone Reservation (TR) [51, 18], Partial Transmit Sequence (PTS) [37], Selected Mapping (SLM) [11], Interleaving [21]

également d’autres techniques qui ne distordent pas le signal et qui parviennent à réduire le PAPR en utilisant un degré de liberté sur le signal au détriment du débit d’information ou de la puissance moyenne. Le tableau 4.1 présente un synthèse des techniques les plus populaires de l’état de l’art associée à leurs principales caractéristiques (distorsion, augmentation de puissance, perte en débit). Pour chacune des ces techniques, une ou deux références bibliographiques ont été choisies parmi la multitude des références possibles. Les deux techniques liées à l’augmentation de la puissance de transmission (ou à la diminution du  $E_b/N_0$ ) reposent sur le principe d’augmenter l’alphabet de symboles : à un symbole de la constellation d’origine correspond un ensemble de symboles plus éloignés dont le décodage dans l’alphabet d’origine est sans ambiguïté. Le choix des symboles transmis est celui qui minimise le PAPR. Pour les techniques basées sur la diminution du débit utile, le principe consiste à diminuer le nombre de bits d’informations à transmettre tout en conservant le même nombre de bits transmis. Les bits d’informations sont alors complétés par des bits choisis afin de minimiser le PAPR. La dernière catégorie est celle des techniques dites à plusieurs candidats : on génère au niveau de l’émetteur plusieurs symboles OFDM contenant la même information binaires mais modifiés par un traitement qui ne change pas sa puissance (par exemple un déphasage, ou un entrelacement). Le symbole OFDM transmis est le candidat ayant le plus faible PAPR. Pour retrouver l’information utile au niveau du récepteur, une information supplémentaire doit être envoyée au récepteur pour faire le traitement inverse sur le symbole OFDM reçu, auquel cas le débit binaire est modifié malgré tout, sinon on utilise un algorithme de réception aveugle.

La comparaison des principale techniques (TR, ACE et SLM) est présentée sur la figure 4.6, reproduite d'après [54], où les paramètres du standard DVB-T2 [1] ont été utilisés. On constate que la technique ACE n'apporte pas le meilleur gain en terme de PAPR, contrairement à la technique TR, qui en revanche a une perte d'efficacité spectrale importante car 5 sous-porteuses sur les 32 lui sont dédiées. La technique SLM nécessite seulement 8 candidats pour une baisse de PAPR équivalente et une perte en efficacité spectrale négligeable (3 bits sur les 128 disponibles). La comparaison en terme de taux d'erreur binaire est également en faveur de la technique SLM pour laquelle on n'observe presque pas de saturation dès 4 candidats. Le phénomène de saturation est observé car le PAPR est limité à 4 dB pour tous les schémas comparés. La distorsion est d'autant plus faible que le PAPR aura été réduit, conduisant à un plancher d'erreurs d'autant plus bas.

Nous avons donc choisi le principe de technique de réduction de PAPR de type SLM. Dans la suite de cette partie, je vais exposer les principaux résultats de nos travaux de recherche où nous avons associé une technique SLM innovante avec un seuillage souple du signal transmis, après avoir évoqué les travaux préliminaires relatifs aux critères de sélection du symbole OFDM candidat.

#### 4.2.2 Technique SLM et critère de sélection

L'augmentation du nombre de candidats générés avec la technique SLM permet d'améliorer le PAPR comme l'illustre la figure 4.7. Le critère usuel pour choisir le candidat est celui du PAPR minimum que l'on appellera par la suite "Critère A". Comme les candidats ont tous la même puissance moyenne, le candidat sélectionné est celui ayant l'amplitude maximum la plus faible.

Pour analyser les performances de ce critère en terme de réduction de PAPR mais également en terme de taux d'erreur lorsqu'un seuillage souple est effectué avant la transmission, les auteurs de [41] ont proposé de définir le rapport entre la puissance du signal et la puissance du bruit plus distorsion apportée par le seuillage (SNDR). L'estimation de ce SNDR fait intervenir la densité de probabilité des amplitudes des échantillons du symbole OFDM avant seuillage noté  $f_r(r)$  supposés indépendants et identiquement distribués (i.i.d.) selon une loi de Rayleigh :  $f_r(r) = 2r \exp(-r^2)$ . Avec la technique SLM, la distribution de probabilité des échantillons du symbole OFDM transmis change car celui ayant la plus faible amplitude max est systématiquement choisi.

A l'aide des statistiques d'ordre, nous pouvons calculer la densité de l'amplitude max :

$$f_{\max(r)}(r) = N f_r(r) (1 - \exp(-r^2))^{N-1}$$

ainsi que celle de la plus petite parmi les  $n$  amplitudes max des  $n$  symboles OFDM candidats :

$$f_{\min(\max(r))}(r) = 2nNr(S(r)^{N-1} - S(r)^N)(1 - S(r)^N)^{n-1}$$

où  $S(r) = 1 - \exp(-r^2)$ . Il ne reste alors qu'à trouver la densité des amplitudes du symbole OFDM choisi dont l'amplitude max suit la loi  $f_{\min(\max(r))}$  [55] :

$$f_{r_{i_0}}(r) = n f_r(r) (1 - (1 - S(r)^N)^n)^{1/N-1} S(r)^{N-1} (1 - S(r)^N)^{n-1}$$

où l'on a noté  $i_0 = \arg \min_{1 \leq i \leq n} (\max_{1 \leq j \leq N} (r_{i,j}))$ ,  $r_{i,j}$  étant la  $j$ -ième amplitude du  $i$ -ème symbole OFDM candidat.

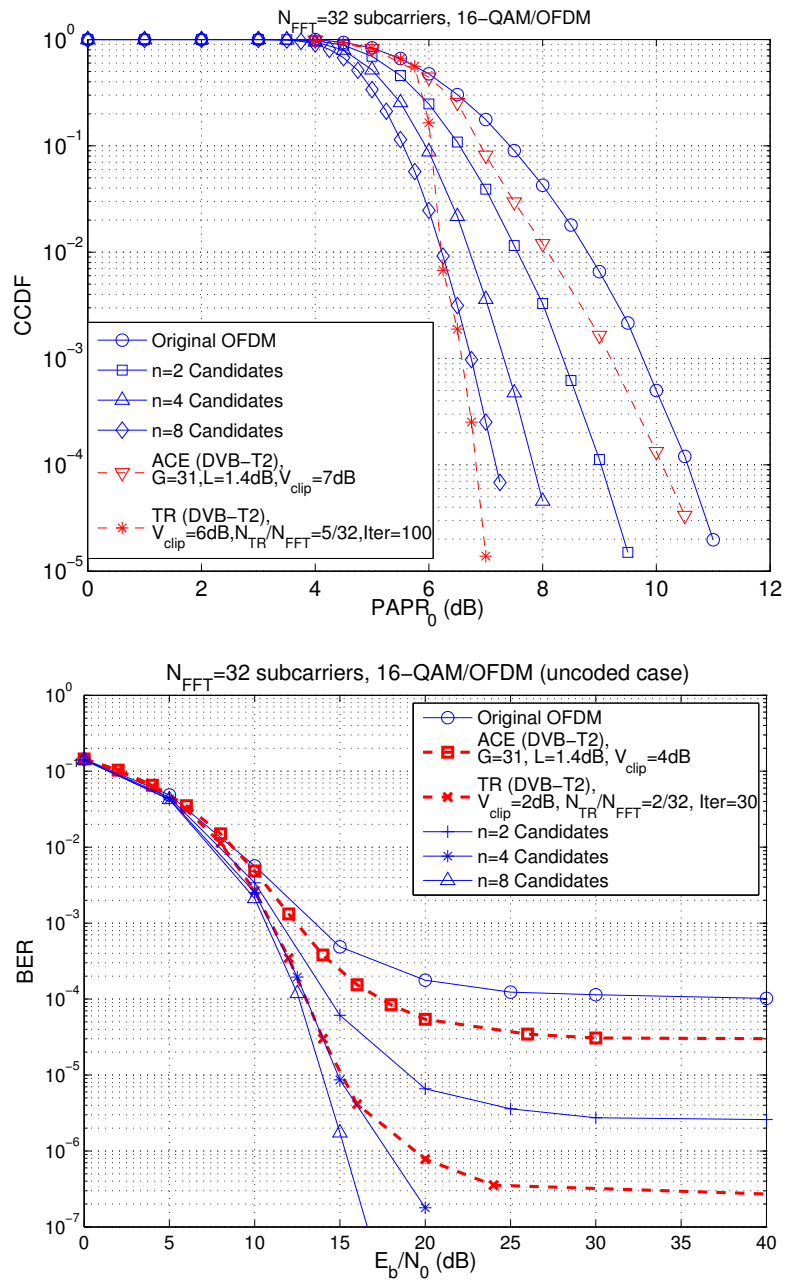


FIGURE 4.6 – CCDF et taux d’erreur binaires en modulation OFDM pour  $N = 32$  porteuses, constellation 16–QAM, utilisant des techniques de réduction de PAPR de type ACE et TR telles que préconisées dans DVB-T2, et SLM. (Extrait de [54])

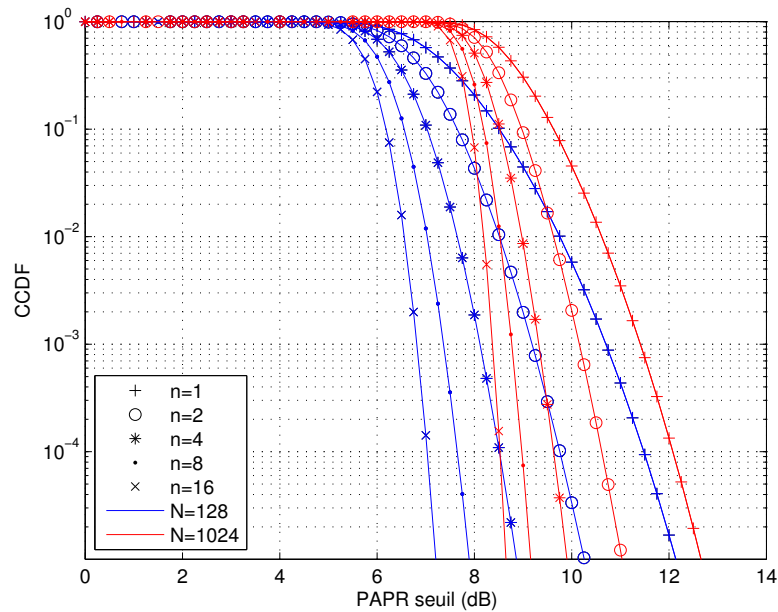


FIGURE 4.7 – Amélioration du PAPR avec la technique SLM à  $n$  candidats pour  $N = 128$  et  $N = 1024$  sous-porteuses.

Nous avons défini un autre critère de sélection d'un symbole OFDM parmi l'ensemble des  $n$  symboles candidats, que nous noterons "Critère B" : celui minimisant la puissance de distorsion après le seuillage. Comme le seuillage est fait volontairement, nous pouvons calculer et comparer les puissances des signaux obtenus par différence entre le signal candidat et le signal candidat seuillé. Dans ce cas, c'est la densité de probabilité du bruit de distorsion, dont dépend également le SNDR, qui va changer. Un calcul publié dans [55] également basé sur les statistiques d'ordre nous a permis de déterminer cette densité et donc de calculer également les performances théoriques du "Critère B".

La possibilité de calculer le SNDR permet de déterminer les probabilités d'erreurs théorique par symbole. Elles sont comparées à celles obtenues par simulation sur la figure 4.8 dans le cas de modulations OFDM non-codées 16-QAM pour  $N = 1024$  sous-porteuses, le seuillage étant fait à un PAPR de 3 dB, sur des canaux gaussiens et de Rayleigh, pour  $n = 4$  candidats. La comparaison entre les critères A et B donne l'avantage au "Critère B" en ce sens qu'il améliore le plancher d'erreurs dû au seuillage, ce qui est cohérent avec la minimisation de la distorsion.

### 4.2.3 Technique SLM basée sur le codage correcteur d'erreurs

L'étude précédente portait sur les performances de réduction de PAPR par l'utilisation de  $n$  candidats. On a fait l'hypothèse que ces candidats étaient identiquement distribués pour établir les performances théoriques de ce schéma. Je présente maintenant une technique pratique de génération de candidats basée sur le codage correcteur d'erreurs et qui permet de transmettre de manière protégée l'information liée au choix du candidat simultanément avec l'information utile. Cette technique est basée sur l'utilisation de masques binaires. Le principe consiste à sacrifier  $L_I$  bits parmi les  $K_d$  bits d'information : ils seront dédiés à l'indexation de  $n \leq 2^{L_I}$  masques binaires. Les  $L_D = K_d - L_I$  bits restant demeurent des bits d'information. Ces masques binaires sont connus de l'émetteur et du

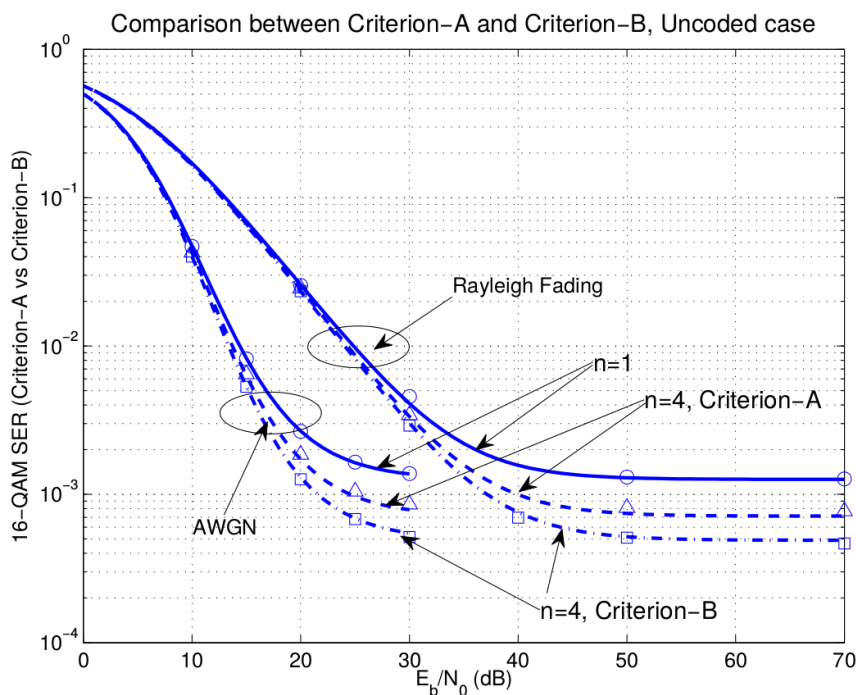


FIGURE 4.8 – Probabilité d’erreur symbole d’une modulation OFDM 16–QAM non-codée de  $N = 1024$  sous-porteuses, sur un canal gaussien et un canal de Rayleigh, permettant la comparaison des performances des critères A et B avec  $n = 4$  candidats. Les lignes correspondent aux estimations théoriques et les marques correspondent aux estimations faites par simulation de Monte-Carlo. (Extrait de [54])

récepteur. Les masques binaires sont tous construits avec des données binaires aléatoires sauf un : le masque "nul" qui ne contient que des 0. Les index doivent eux être tous différents. Le vecteur de données contient quant à lui  $L_I$  bits d’index nuls puis  $L_D$  bits d’information à transmettre.

L’encodage par le code correcteur d’erreurs se fait sur la somme du vecteur de données et d’un masque binaire. La dimension du code reste donc  $K_d$ . La linéarité du code permet d’encoder séparément les masques binaires et d’additionner ensuite le masque codé au mot de code correspondant aux données à transmettre. On peut ainsi générer  $n \leq 2^{L_I}$  symboles OFDM candidats et sélectionner, selon l’un des 2 critères vus en section 4.2.2, celui à transmettre. A la réception, on procède au décodage de la somme des 2 mots de codes. En l’absence d’erreur, les bits d’index permettent de connaître le masque utilisé et ainsi de retrouver les données binaires utiles. Cette technique a été publiée dans [56] et la figure 4.9 illustre quelques performances sur le canal gaussien pour  $L_I = 1$  bit d’index et  $n = 2$  candidats pour des masques binaires choisis aléatoirement (notés RDM). Ces performances sont également comparées aux performances obtenues sans faire d’erreur sur l’index binaire : elles sont inchangées en ce qui concerne la probabilité d’erreur par mot. Cela indique que les erreurs éventuelles sur les bits d’index ne sont pas pénalisantes car la probabilité d’avoir seulement les bits d’index faux est très faible.

L’inconvénient principale de cette technique SLM est la nécessité d’utiliser  $n$  fois la transformée de Fourier inverse pour générer les  $n$  candidats, ce qui peut limiter les possibilités d’implémentation. Dans [57], nous avons proposé de réduire cette complexité en diminuant le nombre d’IFFT par rapport au nombre de candidats en générant de nouveaux symboles OFDM candidats par combinaisons



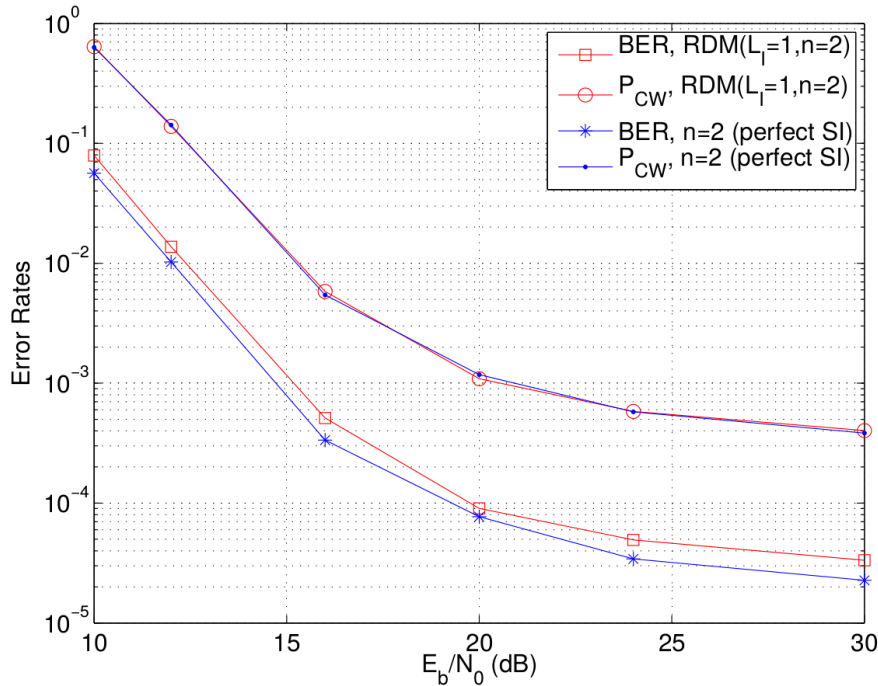


FIGURE 4.9 – Taux d’erreur par bit (BER) et par mot de code ( $P_{CW}$ ) obtenu dans le cas  $n = 2$  candidats et 1 bits d’index sur canal gaussien pour le critère A, permettant de comparer l’influence d’erreurs au niveau des bits d’index. La modulation OFDM possède 128 sous-porteuses en 64-QAM codée par un code LDPC de rendement 1/2 et de longueur  $N_{cw} = 768$  bits. Le seuillage est effectué à un PAPR de 3 dB. (Extrait de [54])

linéaires d’autres symboles candidats. Le principe repose sur la division des données du masque en  $Q$  blocs, avec un seul bloc non-nul à la fois qui permet de générer  $n$  candidats, soit un nombre total de  $n^Q$  candidats mais avec seulement  $nQ$  IFFT. La figure 4.10 compare cette solution avec la technique SLM théorique classique à 8, 16 et 64 candidats. On constate qu’à nombre de IFFT identique, la solution proposée permet d’améliorer la réduction du PAPR : par exemple pour 8 IFFT avec la solution proposée (FDM( $n = 4, Q = 2$ )), on atteint presque la performance de la solution SLM avec 16 IFFT (SLM( $n = 16$ )).

#### 4.2.4 Conclusion

La réduction du PAPR est l’une des limitations à l’utilisation des modulations OFDM. Le standard de diffusion numérique terrestre DVB-T2 est le premier à proposer une technique de réduction de PAPR, montrant par la même occasion que la surconsommation induite par le PAPR n’affecte pas seulement les émetteurs disposant de ressources énergétiques limitées (satellites, téléphone mobile, tablettes, etc ...) mais également les émetteurs de forte puissance alimentés par le réseau de distribution électrique.

Dans ce contexte, nous avons travaillé à améliorer les techniques de réduction de PAPR basées sur la sélection d’un symbole OFDM parmi une liste de symboles candidats. L’originalité de ce travail réside dans la volonté de proposer un calcul théorique des performances et de le confronter aux résultats de simulation.

Les perspectives d’évolution des systèmes de téléphonie mobile (5G) font apparaître de nouvelles

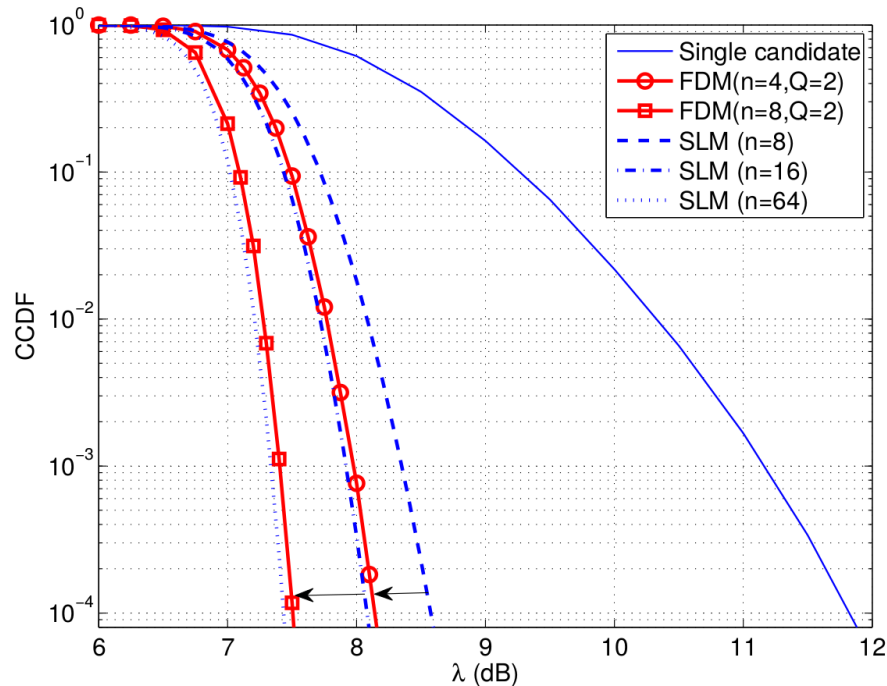


FIGURE 4.10 – Comparaison des CCDF avec la technique SLM et avec la technique proposée permettant de réduire le nombre de IFFT. (Extrait de [54])

formes d'ondes multi-porteuses non-orthogonales incluant la présence de filtrage. On les retrouve sous différentes dénominations, selon que le filtrage n'est pas circulaire (FBMC/OQAM, UFMC) ou circulaire (C-FBMC, GFDM). La présence de filtrage rend les symboles dépendants et les techniques classiques de réduction de PAPR travaillant au niveau symbole sont donc à adapter. Avec Younes Jabrane, professeur à l'université Cadi Ayyad au Maroc, nous souhaitons poursuivre ce travail grâce au financement collaboratif PHC Toubkal (montage prévu au printemps 2017).

### 4.3 Modulations CPM pour la télémesure

Les perspectives d'évolution des communications numériques qui accompagnent la construction de la 5G évoquent notamment l'explosion des communications dites entre machines. Cette expression traduit en fait des communications ayant une autre finalité qu'un échange d'informations impliquant une ou plusieurs personnes, comme par exemple dans des applications de surveillance ou de contrôle à distance dans divers domaines tels que l'environnement (anticiper les éruptions volcaniques par exemple), la santé (pour le suivi d'un patient) ou de l'industrie (réseaux de capteurs, compteurs intelligents pour le gaz, l'eau ou l'électricité). Dans ce type de transmission, l'énergie consommée par l'émetteur peut être très limitée (autonomie complète, sans possibilité de changer la pile). Dans ces conditions, le PAPR doit être réduit le plus possible. L'utilisation des modulations à enveloppe constante (et parmi elles les modulations à phase continue) permet d'obtenir un PAPR de 0 dB. J'ai commencé à travailler sur ce thème dans le cadre d'un contrat avec GrDF pour la télé-relève automatique des compteurs de gaz, puis que dans le cadre du contrat SATAIS pour le compte de CLS et du CNES. Ces travaux ont donné naissance au sujet de la thèse de Malek Messai (2012-2015) [29] dans laquelle de nouveaux schémas robustes basés sur la modulation CPM ont été proposés pour l'émission

et la réception. Malek Messai poursuit ce travail avec un post-doc financé partiellement par le projet H2020 Fantastic-5G pour étudier l'accès multiple non-orthogonal de tels schémas de transmission.

### 4.3.1 Introduction

#### Notations

Les modulations à enveloppe constante ont une puissance maximum égale à la puissance moyenne : l'amplitude du signal en bande de base reste constante en fonction du temps (exemple : modulation de fréquence (FM), modulation à déplacement de fréquence (FSK) ou de phase (GMSK)). Pour ces modulations, la densité spectrale de puissance peut présenter un support assez large, notamment si des discontinuités de phase sont présentes comme pour la FSK par exemple. Pour améliorer l'efficacité spectrale, on peut rendre la phase continue par filtrage : ce sont les modulations à phase continue (CPM), dont le signal en bande de base s'exprime en fonction du temps  $t$  par :

$$s(t, h, \mathbf{a}) = \sqrt{\frac{E_s}{T}} \exp(j\phi(t, h, \mathbf{a}))$$

où  $E_s$  est l'énergie moyenne d'un symbole,  $T$  est la durée d'un symbole,  $h$  est l'indice de modulation et  $\mathbf{a}$  est le vecteur de symboles  $a_i$  portant l'information et choisis dans un alphabet  $M$ -aire  $\{\pm 1, \pm 3, \dots, \pm(M-1)\}$ ,  $\phi(t, h, \mathbf{a})$  est la phase du signal donnée par :

$$\phi(t, h, \mathbf{a}) = 2\pi h \sum_{i=0}^{+\infty} a_i q(t - iT).$$

La phase du signal est en fait une modulation linéaire de symboles au rythme  $1/T$  et utilisant la forme d'onde  $q(t)$ . Dans le contexte des CPM,  $q(t)$  est appelée la réponse en phase, et est définie à partir du pulse fréquentiel  $g(t)$  par :

$$q(t) = \int_{-\infty}^t g(\tau) d\tau.$$

Le pulse fréquentiel doit répondre à certaines propriétés : il doit avoir un support borné  $[0, LT]$ , être une fonction symétrique autour de  $LT/2$  ( $g(t) = g(LT - t)$ ), et être normalisé ( $\int_0^{LT} g(\tau) d\tau = q(LT) = 1/2$ ).

Les modulations CPM ne sont pas linéaires et ont un support fréquentiel infini. Nous supposons que  $N_s$  échantillons par symbole sont obtenus après conversion analogique-numériques et que  $N_s$  est assez grand ( $N_s = 10$  en pratique) pour que les échantillons obtenus procurent une statistique suffisante (exhaustive) du signal reçu [35].

La phase évoluant de manière continue en fonction du temps, il est pratique de la décomposer sur le  $n$ -ième intervalle de temps ( $t \in [nT, (n+1)T]$ ) de la façon suivante :

$$\phi(t, h, \mathbf{a}) = \underbrace{\pi h \sum_{i=0}^{n-L} a_i}_{\phi_{h,n}} + \underbrace{2\pi h \sum_{i=n-L+1}^n a_i q(t - iT)}_{\phi_{h,n}(t)}$$

c'est à dire comme étant la somme d'une phase dépendant uniquement des  $n - L$  symboles précédents et de l'indice de modulation d'une part, et d'autre part d'une phase fonction du temps, des  $L - 1$  derniers symboles transmis et de l'indice de modulation.  $\phi_{h,n}$  est l'état de phase : pour un indice de modulation rationnel ( $h = r/p$ ,  $r$  et  $p$  premiers entre eux), la phase  $\phi_{h,n}$  (modulo  $-2\pi$ ) ne peut prendre que  $p$  valeurs différentes.

### Décodage optimal des modulations CPM

Le décodage optimal des modulations CPM dans un canal gaussien où l'on note le signal reçu  $r(t) = s(t, h, \mathbf{a}) + n(t)$ ,  $n(t)$  étant la réalisation d'un processus gaussien complexe centré, stationnaire au sens large et indépendant de  $s(t, h, \mathbf{a})$ , dont la densité spectrale bilatérale de puissance vaut  $2N_0$ , correspond à la recherche de la séquence de symboles  $\hat{\mathbf{a}}$  minimisant la distance euclidienne avec le signal reçu :

$$\hat{\mathbf{a}} = \arg \min_{\tilde{\mathbf{a}}} \|r(t) - s(t, h, \tilde{\mathbf{a}})\|^2 = \arg \max_{\tilde{\mathbf{a}}} \underbrace{\Re \left\{ \int r(t) s^*(t, h, \tilde{\mathbf{a}}) dt \right\}}_{\Omega(\tilde{\mathbf{a}})}.$$

La dernière équation, où  $s^*$  signifie complexe conjugué de  $s$ , vient du fait que l'enveloppe étant constante, il ne reste plus qu'à maximiser la corrélation entre les 2 termes. Pour des longueurs raisonnables de séquences de symboles, il y a trop de métriques  $\Omega(\tilde{\mathbf{a}})$  à calculer. On définit alors l'accumulation de métriques suivante :

$$\Omega_n(\tilde{\mathbf{a}}) = \Omega_{n-1}(\tilde{\mathbf{a}}) + \Omega^{(n)}(\tilde{\mathbf{a}})$$

avec :

$$\begin{aligned} \Omega_n(\tilde{\mathbf{a}}) &= \Re \left\{ \int_{-\infty}^{nT} r(t) s^*(t, h, \tilde{\mathbf{a}}) dt \right\} \\ \Omega^{(n)}(\tilde{\mathbf{a}}) &= \Re \left\{ \int_{(n-1)T}^{nT} r(t) s^*(t, h, \tilde{\mathbf{a}}) dt \right\} \end{aligned}$$





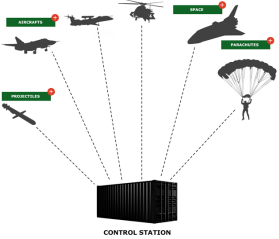


Ainsi, le décodage optimal sur canal gaussien peut être fait récursivement par un algorithme de Viterbi où les métriques de branche sont les  $\Omega^{(n)}(\tilde{\mathbf{a}})$ . Si l'indice de modulation est un rationnel, le treillis sur lequel effectuer cet algorithme possède un nombre fini d'états égal à  $pM^{L-1}$ , et  $pM^L$  métriques de branche à calculer par intervalle de temps symbole. Si l'indice de modulation est irrationnel, le nombre d'états du treillis est infini.

### Utilisation des modulations CPM en pratique

Les modulations MSK (*Minimum Shift Keying*) et GMSK (*Gaussian MSK*) sont des instances particulières de CPM, pour lesquelles  $h = 1/2$  et le pulse fréquentiel  $g(t)$  est respectivement un rectangle de durée  $L = 1$  temps symbole, et un pulse gaussien ayant comme paramètre la largeur du pulse à -3dB (appelé parfois produit BT,  $\beta$  ou produit gain-bande).

Les modulations CPM au sens large ont été largement étudiées depuis leur formalisation par Tor Aulin et Carl-Erik Sundberg en 1979 [9, 8, 7]. Devant les efficacités spectrales réduites qu'elles offraient par rapport aux modulations QAM linéaires et devant la complexité importante liée au dé-

TABLE 4.2 – Liste de quelques standards implémentant une modulation CPM

Nom du standard	indice de modulation	alphabet	pulse fréquentiel
	$0.35 < h < 0.7^1$	$M = 2$	gaussien (GFSK) avec $BT = 0.5$
	$h = 0.5$	$M = 2$	gaussien (GMSK) avec $BT = 0.3$
 (basic rate)	$0.28 < h < 0.35$ [3]	$M = 2$	gaussien (GFSK) avec $BT = 0.5$
	$h \in \{\frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{2}{7}\}$ [4] <sup>2</sup>	$M = 4$	$(1 - \alpha)$ Rectangle + $\alpha$ (cosinus sur-élevé), $L = 2$
	multi- $h$ $(\frac{4}{16}, \frac{5}{16})$ (ARTM <sup>3</sup> ) ou $h = \frac{1}{2}$ (SOQPSK-TG <sup>4</sup> )	$M = 4$ (ARTM) ou $M = 3$ pré-codé (SOQPSK-TG)	Racine de cosinus sur-élevé ( $L = 3$ ) (ARTM)
	$h = \frac{1}{2}, 1$ ou $\frac{1}{3}$	$M = 2$ ou $4$	gaussien (GFSK) avec $BT = 0.5$ [5]
	$h \simeq \frac{1}{2}$	$M = 2$	gaussien (GFSK) avec $BT \simeq 0.4$ [6]

codage optimal, l'augmentation incessante des débits n'a pas incité à les choisir dans les standards de communications numériques, à l'exception notoire de la 2G qui implémente une GMSK. Cependant, récemment, l'arrivée de nouveaux besoins de communications numériques caractérisés par une faible consommation et des débits peu importants constitue un contexte favorisant le choix de modulations CPM. La table 4.2 rassemble quelques standards récents ou toujours en vigueur utilisant un ou plusieurs format de CPM. On constate que ces standards se regroupent dans 2 industries séparées : celle des télécoms proprement dite et celle d'autres industries où la mesure à distance joue un rôle important.

### Limitation des CPM

Dans cette liste d'applications (tableau 4.2) on constate que l'indice de modulation n'est pas toujours spécifié (intervalles de valeurs possibles comme pour le Bluetooth par exemple) ou bien est spécifié avec une certaine tolérance (comme pour le système d'identification automatique de navires (AIS) par exemple). Comme le récepteur idéal est construit sur un treillis dont le nombre d'états est basé sur l'écriture rationnelle de l'indice de modulation, la conception d'un récepteur optimal pour ces cas de figures devient impossible. Lorsque plusieurs indices sont spécifiés, une solution consisterait à prendre le dénominateur commun à tous les indices de modulations, mais cela conduirait à une

**complexité** trop importante.

Si le récepteur, pour simplifier sa complexité, est construit avec un treillis supposant une certaine valeur d'indice de modulation, mais que l'émetteur n'utilise pas exactement le même (défaut à l'émetteur, ou intervalle de valeurs possibles), le récepteur finit par se déphaser complètement du signal reçu et le taux d'erreur est catastrophique. Pour simplifier la complexité et apporter de la **robustesse** au système en cas de décalage entre l'indice de modulation de l'émetteur et celui considéré pour concevoir le récepteur, le décodage non-cohérent s'avère être une bonne solution, si le bilan de liaison le permet. Ce n'est pas envisageable si l'énergie consommée à l'émetteur est un critère de conception prioritaire.

On constate que la réduction du coût des émetteurs (consommation d'énergie, complexité) va de paire avec la présence d'un déploiement à grande échelle de ces émetteurs. Il faut donc envisager la **gestion multi-utilisateurs** en limitant le plus possible la surcharge de signalisation.

Ces 3 problématiques sont développées dans les 3 sections suivantes.

### 4.3.2 Réduction de complexité

#### Etat de l'art

La réduction de complexité des détecteurs cohérents de séquences CPM au sens du maximum de vraisemblance peut suivre différentes approches mais revient généralement à diminuer le nombre d'états dans le treillis ou/et à diminuer le nombre de signaux distincts avec lesquels effectuer l'opération de filtrage adapté (qui n'est plus adapté de par cette simplification). On peut citer notamment [47] où tous les états ne sont pas nécessairement parcourus, ou bien [48] où l'égalisation est faite sur un treillis plus petit (en nombre d'états). Svensson et Aulin [49] ont quant à eux proposé un détecteur non-adapté (*mismatched detector*) qui consiste à modifier le pulse fréquentiel afin de raccourcir son support temporel ( $L$ ) qui intervient à la fois dans le nombre d'états et dans le nombre de filtres adaptés. Une autre stratégie permettant de réduire le nombre de filtres consiste à projeter la signal CPM dans une base de signaux et à ne conserver que les composantes les plus significative, comme dans [20] avec une base orthonormale obtenue par l'algorithme de Gram-Schmidt, dans [16, 46] avec des fonctions d'échantillonnage et des fonctions de Walsh dans [50] ou sinusoïdales dans [20].

Finalement, une représentation du signal CPM sous la forme d'une combinaison linéaire de signaux de modulations linéaires d'amplitude, pondérés par des pseudo-symboles, a été proposée par Laurent en 1986 [25]. Cette décomposition est très souvent utilisée dans la littérature car même si la décomposition est une somme infinie, une excellente approximation peut être obtenue avec le ou les premiers termes de cette somme. Basé sur les premiers termes de cette décomposition ainsi que sur un sous-ensemble des pseudo-symboles, un détecteur à complexité réduite a été proposé dans [23] réduisant à la fois le nombre d'états et de filtres. La décomposition de Laurent a été étendue au cas non-binaire dans [28], le détecteur correspondant par [15] et par [43] dans le cas d'une CPM  $M$ -aire multi- $h$  (dans ce cas, un ensemble d'indices de modulation est choisi et ils sont utilisés successivement à chaque nouveau symbole à transmettre).

Toutes les méthodes de réduction de complexité précédentes utilisent l'indice de modulation du signal émis pour concevoir le récepteur, et le supposent rationnel.

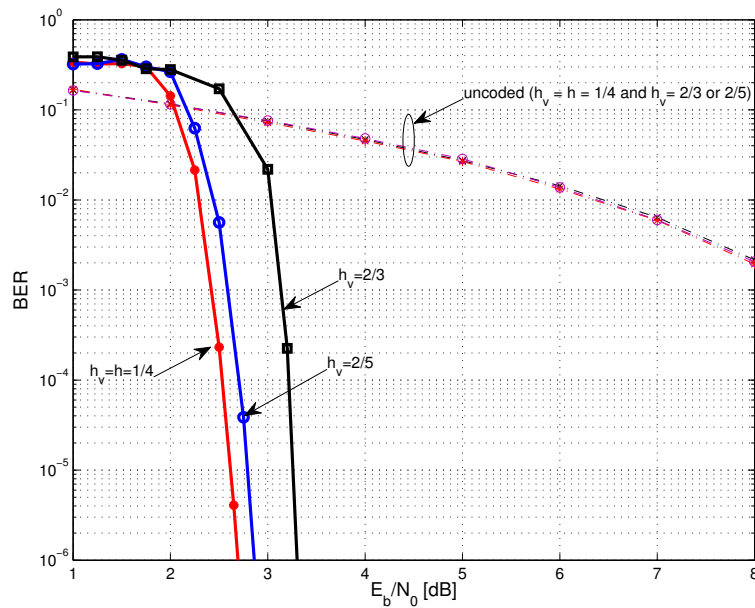


FIGURE 4.11 – taux d’erreur binaire obtenu avec une CPM quaternaire ( $M = 4$ ),  $L = 2$  (pulse de type cosinus sur-élevé) et  $h = 1/4$  non-codée, ou codée avec un code convolutif  $(7, 5)$  et un entrelaceur de longueur 4096, pour des décodeurs ayant différentes valeurs d’indice virtuel  $h_v$ . (Extrait de [30])

### Détecteur à nombre d’états réduit [29]

Dans le thèse de Malek Messai, nous avons proposé de décomposer l’indice de modulation selon  $h = h_v + \Delta_h$ , où  $h_v = \frac{l_v}{p_v}$  doit être rationnel, sans que  $h$  le soit obligatoirement. Nous construisons alors un treillis ayant un nombre d’états imposé par  $p_v$ . Nous offrons donc un degré de liberté dans le choix de  $h_v$ , que l’on peut utiliser par exemple pour réduire le nombre d’états dans le treillis utilisé au décodage. Moyennant une modification minimale des métriques de nœuds et de branches, nous n’observons aucune perte de taux d’erreur par rapport au décodage sur le treillis basé sur l’indice de modulation original pour certaines valeur de  $h_v$  comme on peut l’observer sur la figure 4.11 dans le cas non-codé d’une CPM quaternaire ayant un pulse en cosinus sur-élevé et d’indice de modulation  $h = 1/4$  : les courbes avec  $h_v = 2/5$  et  $2/3$  sont superposées à la courbe obtenue avec l’algorithme de base correspondant à  $h_v = h = 1/4$ . On constate cependant que ce qui est vrai en non-codé ne l’est pas forcément en codé puisque la courbe pour  $h_v = 2/3$  est nettement en retrait. Les taux d’erreur obtenus pour la même forme d’onde que celle de la figure 4.11 mais avec un indice de modulation plus élevé  $h = 2/5$  sont présentés sur la figure 4.12. On constate dans que pour  $h_v = 2/3$ , même le cas non-codé n’est pas aussi performant que l’optimal  $h_v = h = 2/5$ , et que cela se répercute dans le cas codé.

### Optimisation du détecteur à nombre d’états réduit [30]

Les résultats illustrés sur les figures 4.11 et 4.12 indiquent que certains choix de  $h_v$  ne sont pas judicieux en termes de taux d’erreur, et que la réduction de complexité (dénominateur de  $h_v$ ) ne doit pas être le seul critère à prendre en compte pour le choix de  $h_v$ . Nous avons donc étudié l’évolution de la borne supérieure de la distance minimale associée au treillis à nombre d’états réduit [7, 30] pour

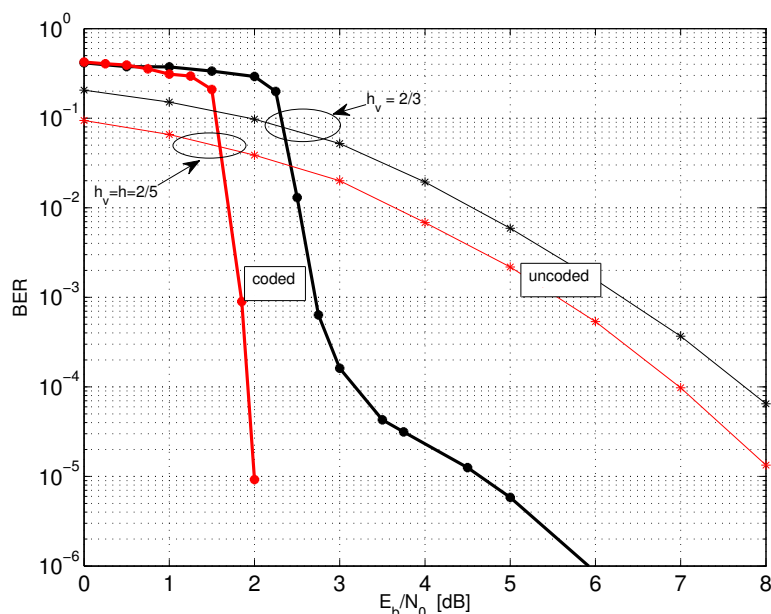


FIGURE 4.12 – taux d’erreur binaire obtenu avec une CPM quaternaire ( $M = 4$ ),  $L = 2$  (pulse de type cosinus sur-élevé) et  $h = 2/5$  non-codée, ou codée avec un code convolutif  $(7, 5)$  et un entrelaceur de longueur 4096, pour des décodeurs ayant différentes valeurs d’indice virtuel  $h_v$ . (Extrait de [30])

certaines familles de  $h_v$  en fonction de  $h$ , afin d’éliminer les valeurs de  $h_v$  qui pourraient exhiber un taux d’erreur dégradé dans le cas non-codé. Cette borne supérieure est tracée sur la figure 4.13 pour une modulation CPM quaternaire ( $M = 4$ ),  $L = 2$  (pulse de type cosinus sur-élevé) selon différentes familles de valeurs de  $h_v$ . On constate que si  $h_v = k/2$ , où  $k$  est un entier premier avec 2, la borne chute par rapport à la borne la plus haute pour certaines plages de valeurs de  $h$  (par exemple entre 0.4 et 0.65 environ, ou bien au-delà de 0.85). Autrement dit, si par exemple le transmetteur a un indice de modulation  $h = 0.9$ , il vaudra mieux éviter de prendre  $h_v = 1/2$  pour ne pas dégrader le taux d’erreur binaire par rapport au détecteur ayant  $h_v = h = 0.9$ . Le calcul portant sur une borne supérieure de la distance minimale, nous avons validé la pertinence de cette borne en reportant des estimations de la distance minimale obtenues par l’approximation de la probabilité d’erreur binaire  $P_b \sim Q(\sqrt{\frac{E_b}{N_0} d_{\min}^2})^5$ , pour  $h_v = 2/3$  (marques triangulaires) et  $h_v = 2/5$  (marques carrées).

Pour prendre en compte ensuite le comportement en décodage itératif dans le cas où la CPM est codée, une analyse à base de diagramme EXIT [59] permet à nouveau de ne pas considérer certaines valeurs de  $h_v$ , comme dans le cas par exemple de la figure 4.11 pour laquelle l’analyse de la distance minimale ne peut pas permettre d’écarter  $h_v = 2/3$  mais qui pourtant dégrade les performances dans le cas d’un décodage itératif, comme l’illustre le diagramme EXIT de la figure 4.14, où l’on visualise nettement le décalage de seuil de convergence entre les différentes valeurs de  $h_v$ .

### 4.3.3 Augmentation de la robustesse

La connaissance parfaite de l’indice de modulation (supposée dans la section précédente) n’est pas toujours applicable. Dans le cas d’une transmission avec indice de modulation fixé, l’indice de

5.  $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp -\frac{u^2}{2} du$



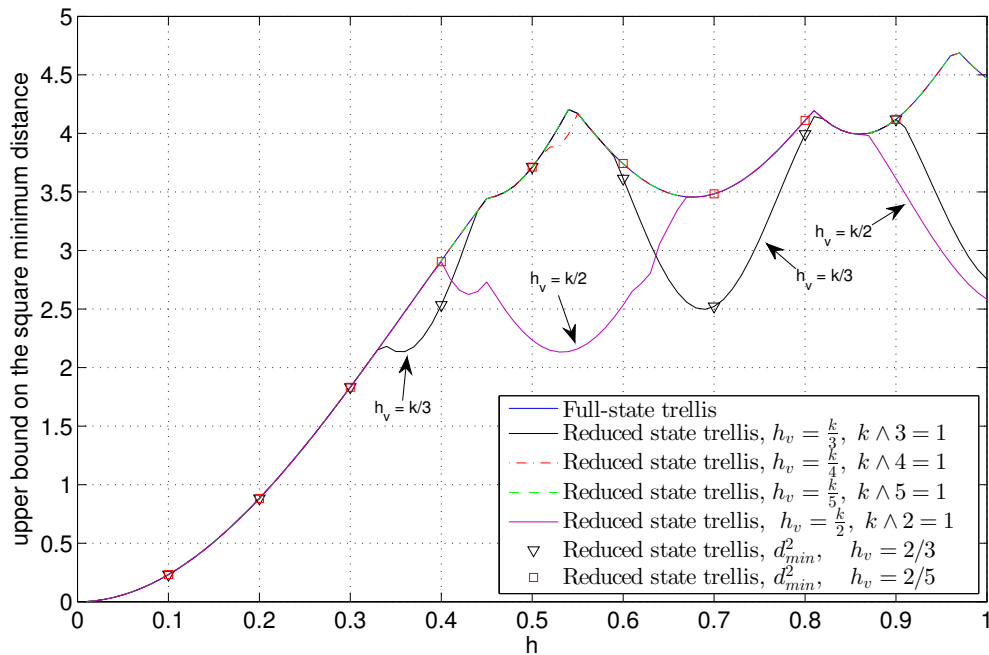


FIGURE 4.13 – Borne supérieure de la distance minimale en fonction de l'indice de modulation  $h$  d'une CPM quaternaire ( $M = 4$ ),  $L = 2$  (pulse de type cosinus sur-élevé) pour un trellis à nombre réduit d'états correspondant à différentes familles de valeurs de  $h_v$ . La notation  $h_v = k/3$ ,  $k \wedge 3 = 1$  par exemple signifie toutes les valeurs qui s'écrivent  $k/3$  où  $k$  est un entier premier avec 3. (Extrait de [30])

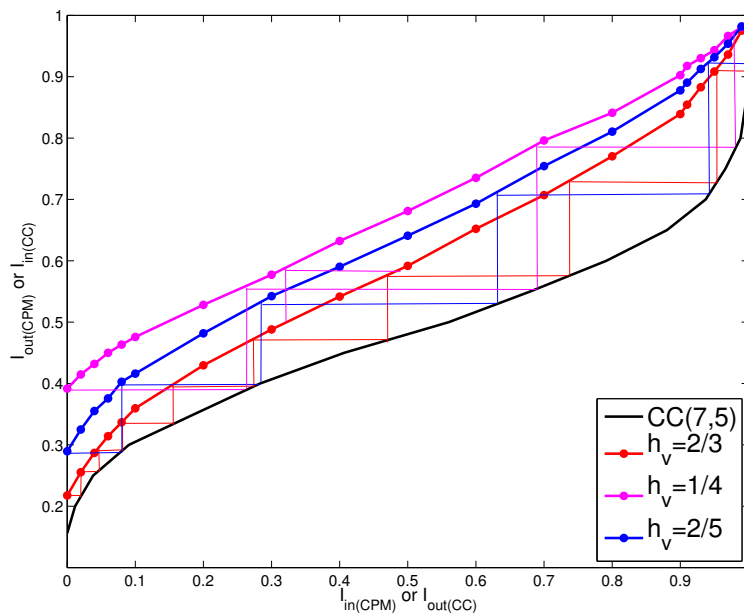


FIGURE 4.14 – Diagramme EXIT pour un décodage itératif entre un détecteur de signal CPM quaternaire ( $M = 4$ ),  $L = 2$  (pulse de type cosinus sur-élevé) et  $h = 1/4$  basé sur un nombre d'états réduit pour  $h_v = 2/3$  et  $h_v = 2/5$  et pour le détecteur classique  $h_v = h = 1/4$ , et un décodeur de code convolutif (7, 5) pour un SNR de  $E_b/N_0 = 1.5\text{dB}$  (Extrait de [30])

modulation réel peut être un peu différent, comme par exemple lorsqu'un émetteur CPM est réalisé à l'aide d'un oscillateur commandé en tension (VCO) dans le but de réduire son coût de fabrication. Dans ce cas, l'indice de modulation est déterminé par le gain du VCO. Avec une réalisation bas-coût, ce gain peut s'écarter de sa valeur nominale pour plusieurs raisons : dispersion de fabrication, vieillissement, influence de la température ou de l'humidité etc ... Sur les émetteurs de signaux AIS, dont l'indice de modulation nominal est  $h = 0.5$ , on peut constater jusqu'à 10% d'écart sur les indices de modulation observés [13]. Dans d'autres cas, ce n'est pas la qualité du matériel d'émission qui perturbe l'indice de modulation, mais le standard qui ne fixe pas de valeur précise d'indice de modulation (comme pour le DECT ou le Bluetooth, c.f. tableau 4.2).

Dans tous ces cas, l'indice réel de modulation du signal émis est la valeur nominale plus un écart  $h = h_v + \Delta_h$ . On retrouve alors la décomposition de la section précédente mais dans ce cas,  $\Delta_h$  est inconnu. Si on parvient à l'estimer parfaitement, les résultats précédents s'appliquent. Cependant cette estimation n'est pas toujours possible (absence de symboles pilotes) ou bien imparfaite. Dans ce cas, même une très faible valeur de  $\Delta_h$  suffit à dégrader considérablement les performances.

Nous avons donc cherché à rendre plus robuste le système de communication basé sur l'hypothèse que l'écart entre l'indice de modulation nominal et l'indice de modulation réel est inconnu. Nous avons travaillé au niveau de l'émetteur et du récepteur pour des modulations CPM binaires. L'indice de modulation nominal est utilisé pour réaliser le treillis du récepteur.

### Robustesse à l'émetteur [31]

Lorsque l'indice de modulation réellement utilisé lors de la transmission est différent de sa valeur nominale, le taux d'erreur se dégrade car la différence entre ces 2 indices introduit une erreur de phase qui va s'accumuler au fur et à mesure de la transmission des symboles. Pour essayer de limiter cet effet, nous avons conçu un précodeur dont le rôle est de borner l'accumulation d'erreur de phase en évitant que le signe des symboles successivement transmis conduisent à une accumulation de phase trop importante qui conduirait à mettre en échec le détecteur. Nous avons utilisé un précodeur dont les symboles en entrée sont binaires et dont les symboles en sortie sont ternaires. La modulation utilisée ensuite est donc une modulation CPM ternaire. La première idée consiste à proposer un précodeur de type AMI (Alternate Mark Inversion) comme illustré sur la figure 4.15 qui permet d'avoir simplement une somme courante de symboles quasi-nulle (dans tous les cas n'excédant pas la valeur absolue d'un seul symbole). Sur la figure 4.15-(a), on représente l'évolution des états du précodeur AMI par la phase des pseudo-symboles de la décomposition de Laurent. L'inconvénient de ce type de modulation est qu'il fait apparaître des raies spectrales aux fréquences multiples du débit de symboles. Afin de supprimer ces raies spectrales dans la densité spectrale de puissance du signal émis, nous avons proposé un précodeur avec plus d'états que le précodeur AMI afin de fournir des salves de  $p$  symboles de même signe (voir figure 4.15-(b) représentant les états du précodeur pour  $p = 4$ ).

Les performances de ces 2 précodeurs sont illustrées sur la figure 4.16 dans le cas d'une modulation GFSK binaire. Le schéma de base consiste à émettre un indice de modulation nominal  $h = 1/3$  et le récepteur est construit à partir de la décomposition de Laurent en gardant les 2 premiers signaux et d'un détecteur de Viterbi. La décomposition est basée sur l'indice de modulation nominal  $h = 1/3$ . Lorsque l'indice de modulation est changé, sans utiliser de précodeur, le récepteur ne fonctionne plus même à fort SNR. En revanche, l'utilisation des précodeurs permet de conserver de bonnes perfor-

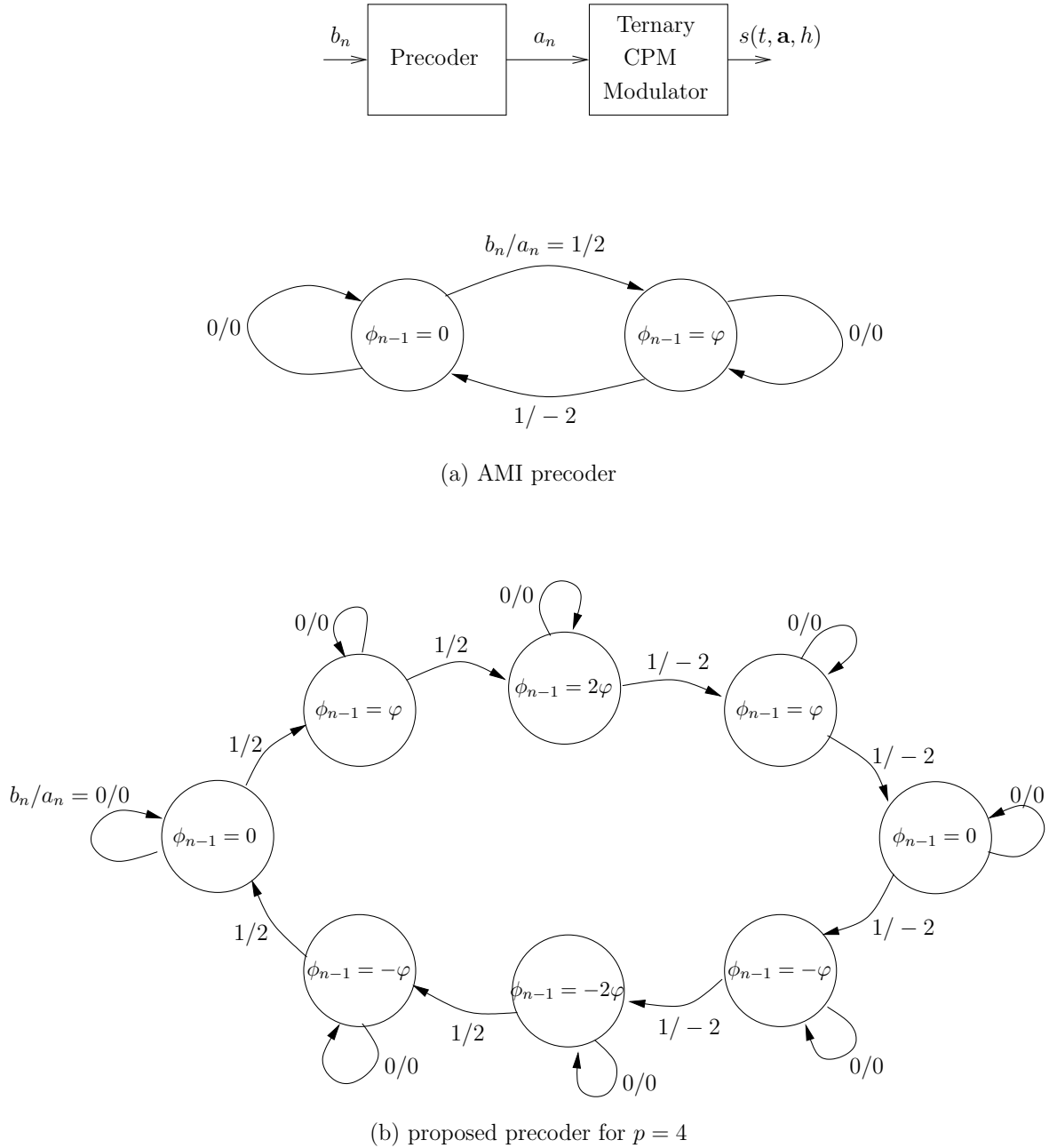


FIGURE 4.15 – Précodeur AMI et précodeur proposé pour supprimer les raies spectrales dans le cas où  $p = 4$  (extrait de [31])

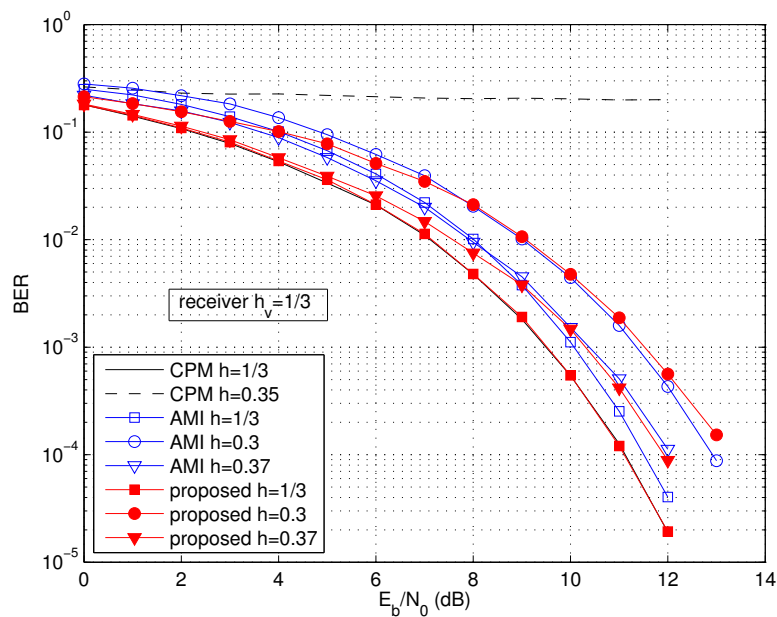


FIGURE 4.16 – Influence du précodage ternaire sur le taux d'erreur binaire d'une CPM de type GFSK binaire ( $L = 2$ ,  $BT = 0.5$ ) obtenu avec  $h_v = 1/3$ , lorsque l'indice de modulation de l'émetteur peut varier (extrait de [31])

mances lorsque l'indice de modulation de l'émetteur s'écarte de sa valeur nominale. La comparaison des performances entre les 2 précodeurs illustre l'intérêt de supprimer les raies spectrales si elles ne sont pas exploitées par d'autres éléments de la chaîne de réception.

### Robustesse au récepteur [32]

Il n'est pas toujours possible de modifier l'émetteur par un précodeur comme proposé précédemment. Dans ce cas, les traitements assurant une certaine robustesse de la réception vis-à-vis d'un décalage inconnu d'indice de modulation doivent être appliqués au récepteur. Les travaux de Barbieri et Colavolpe [10] utilisent la décomposition de Laurent (seul le premier terme est conservé) pour détecter la modulation CPM binaire dans le cas où elle est perturbée par un bruit de phase. Dans notre cas, le principe est d'utiliser le formalisme des *factor graphs* afin de détecter les symboles de la CPM connaissant la densité de probabilité de l'indice de modulation. Selon les cas d'utilisation, cette distribution peut être choisie comme uniforme (par exemple pour le Bluetooth) ou gaussienne (par exemple pour les signaux AIS).

Les performances obtenues sont illustrées sur la figure 4.17 dans le cas du Bluetooth (Basic Rate) pour un indice de modulation  $h = 0.28$ , pour différentes valeurs de l'indice  $h_v$  et différents écarts types de bruit de phase. Les performances sont également comparées à un algorithme non-cohérent dédié au Bluetooth [24] nécessitant l'estimation de l'indice de modulation sur une période de  $N_e = 50$  symboles.

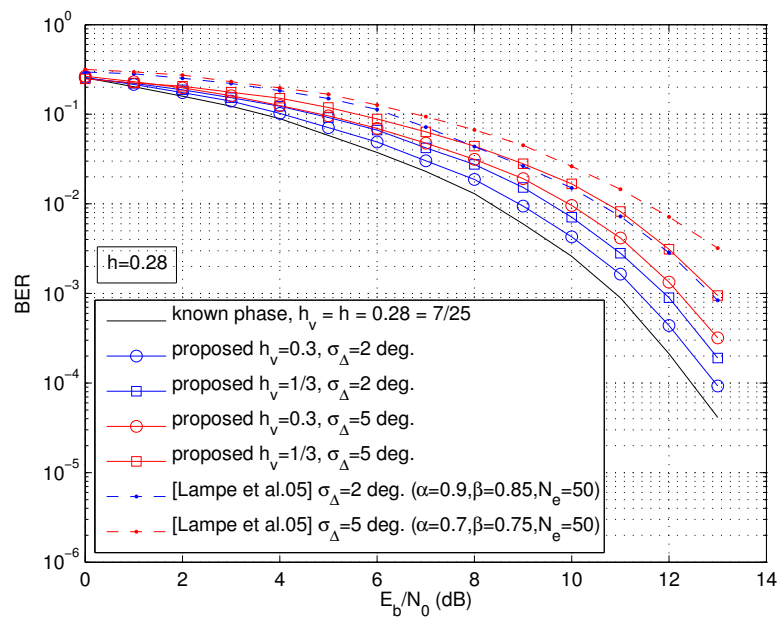


FIGURE 4.17 – Comparaison des taux d’erreur obtenus dans le cas du Bluetooth et en présence de bruit de phase pour un indice de modulation  $h = 0.28$ . L’algorithme non-cohérent est celui proposé par [24] avec une période d’estimation de  $h$  de  $N_e = 50$  symboles. (extrait de [31])

#### 4.3.4 Accès multiple [29, 33, 34]

Le déploiement d’un grand nombre d’émetteurs est rendu possible par la réduction du coût unitaire aidée par la mise en œuvre d’une modulation CPM. La présence de multiples émetteurs doit donc s’accompagner d’une stratégie multi-utilisateurs d’accès au canal. Une stratégie orthogonale classique d’accès multiple de type TDMA nécessite de la signalisation et de la synchronisation qui ne sont pas forcément compatibles avec la réduction de coût d’un tel déploiement ; le CDMA nécessiterait également un trop grand nombre de codes ; le FDMA pose le problème de l’orthogonalité entre les signaux CPM, ou celui de la perte en efficacité spectrale liée au fait que le spectre fréquentiel d’une CPM n’est pas borné (il faudrait un espacement fréquentiel trop grand devant le débit symbole pour que l’interférence entre utilisateurs soit négligeable).

Des schémas CPM multi-utilisateurs ont cependant déjà été proposés dans la littérature. Dans [38], les auteurs ont réduit la complexité d’un détecteur maximum a-posteriori (MAP) multi-utilisateurs de signaux GMSK transmis sur la même fréquence radio mais avec des écarts temporels variant entre 0 et  $T$  (période symbole), en utilisant la décomposition de Laurent qui est particulièrement adaptée à la GMSK. Dans [36], un écart fréquentiel est introduit entre les utilisateurs utilisant une modulation CPM concaténée en série avec un code correcteur d’erreurs. L’utilisation d’un décodage itératif permet d’augmenter l’efficacité spectrale par utilisateur par rapport au schéma mono-utilisateur. En plus de l’écart fréquentiel, un déphasage est également introduit dans [42] et [12] mais seulement pour  $h = 1/2$ ,  $L = 1$  et une réception cohérente et un faible nombre d’utilisateurs. Dans [27], un système multi-utilisateurs basé sur l’étalement de spectre est proposé en association avec une modulation CPM multi- $h$  ; la séquence d’indices de modulation est choisie suffisamment longue par rapport au nombre d’utilisateurs, chacun d’entre eux ayant sa propre séquence. Enfin, un schéma de

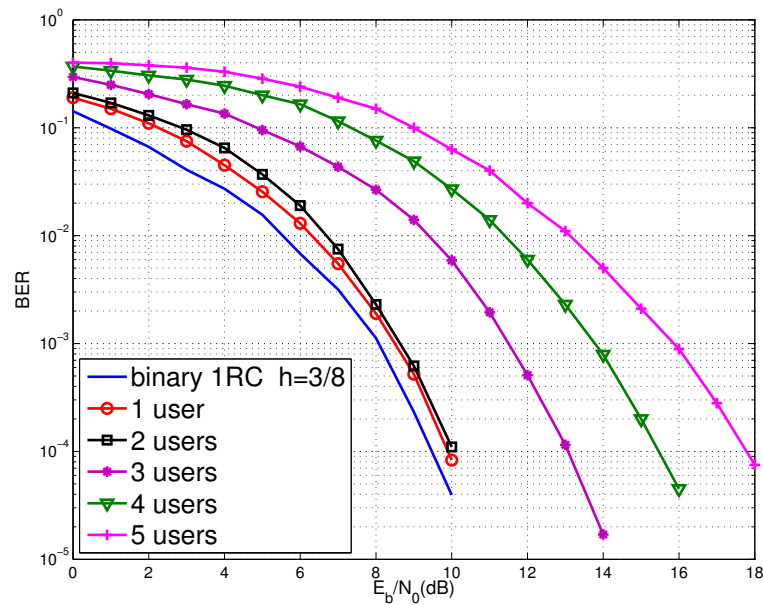


FIGURE 4.18 – Taux d’erreur binaire obtenu pour  $K = 1$  à  $K = 5$  utilisateurs pour un indice de modulation  $h = 3/8 \pm 0.05$  avec une modulation CPM  $L = 1$  et un pulse fréquentiel de type cosinus sur-élevé. Chaque utilisateur utilise un codage AMI ternaire et un déphasage multiple de  $\frac{3\pi}{4K}$  (extraite de [29])

détection à complexité réduite pour l’accès multiple à répartition fréquentielle a été proposé dans [44] : la détection est basée sur la représentation en *factor graphs* et l’implémentation de l’algorithme somme-produit pour des modulations CPM concaténées en série avec un codage convolutif.

Nous avons proposé 2 techniques pour résoudre le problème de l’accès multiple dans le cas où les émetteurs à bas coût ont un indice de modulation inconnu (mais dont on connaît cependant la densité de probabilité) : soit du côté de l’émetteur pour lequel nous avons proposé un codage AMI ternaire associé avec des déphasages différents selon l’utilisateur (voir figure 4.18), soit du côté récepteur où nous avons adapté les travaux de [44] pour prendre en compte la méconnaissance de l’indice de modulation (voir figure 4.19).

## 4.4 Conclusion

L’enveloppe constante des modulations à phase continue (CPM) permet de les mettre en œuvre dans des émetteurs dont la consommation énergétique est un critère de conception important. Utilisées dans des émetteurs implémentés avec un amplificateur de classe C, le rendement énergétique peut être excellent. Les coûts de production des émetteurs peuvent être encore plus bas avec des modulateurs CPM de type oscillateurs commandés en tension (VCO). Mais dans ce cas, l’indice de modulation qui correspond au gain du VCO n’est pas fixé avec précision rendant la réception cohérente de ce type de format hasardeux.

Pendant la thèse de Malek Messai, nous avons proposé différentes solutions permettant de rendre les systèmes à base de CPM plus robustes aux écarts d’indice de modulation, soit par une modification de l’émetteur (précodage), soit par l’implémentation d’un détecteur robuste. La complexité de ces

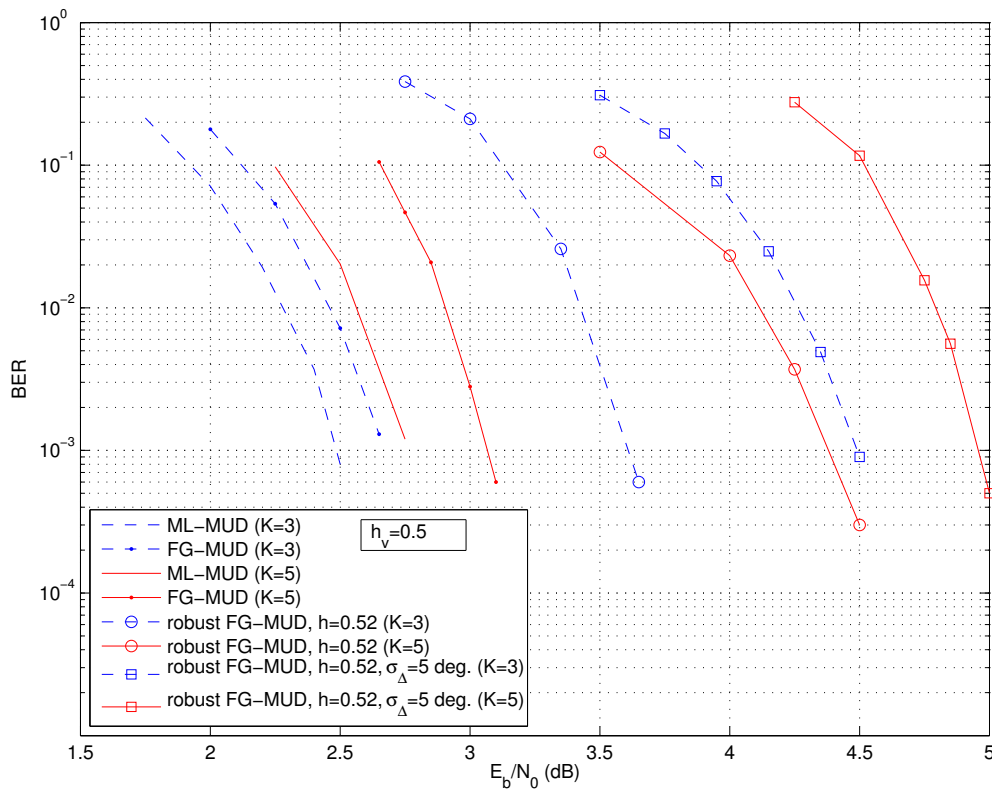


FIGURE 4.19 – Taux d’erreur binaire obtenu pour  $K = 3$  et  $K = 5$  utilisateurs (courbes bleues pointillées et rouges continues respectivement) utilisant une modulation MSK et un treillis basé sur  $h_v = 1/2$  dans un schéma à multiplexage fréquentiel où l’espacement fréquentiel normalisé est de 0.5. Les courbes sans marque sont celle obtenues avec un décodeur multi-utilisateurs optimal ; celles avec des points sont obtenues avec le décodeur de type *factor graph* avec  $h = 0.5$  ; celles avec les cercles sont obtenues quand  $h = 0.53$  avec le détecteur robuste ; enfin celles avec les carrés sont obtenues avec  $h = 0.53$  en présence de bruit de phase (extrait de [33])

récepteurs reste raisonnable et permet d'observer des performances très proches du récepteur optimal.

Nous avons ensuite étendu ces résultats au canal à accès multiples, tout en conservant la robustesse vis à vis de l'indice de modulation. Si les simulations présentent de bons résultats pour quelques utilisateurs (moins de 10), la complexité risque d'être trop importante si l'on considère plusieurs milliers d'utilisateurs. C'est pourtant cet ordre de grandeur qu'il faut viser pour les systèmes de types réseaux de capteurs, ou plus généralement pour l'internet des objets (IoT). C'est la raison pour laquelle je participe à l'encadrement du post-doc de Malek Messai portant sur l'utilisation des techniques de traitement du signal parcimonieux (*compressed sensing*) dans la détection multi-utilisateurs.

## 4.5 Bibliographie

- [1] ETSI/DVB. *Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system*, etsi en 302 755 v1.3.1 edition, 2011. [http://www.etsi.org/deliver/etsi\\_en/302700\\_302799/302755/01\\_03\\_01\\_40/en\\_302755v010301o.pdf](http://www.etsi.org/deliver/etsi_en/302700_302799/302755/01_03_01_40/en_302755v010301o.pdf).
- [2] ETSI. *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2 : Physical Layer (PHL)*, etsi en 300 175-2 v2.4.0 edition, 2011. [http://www.etsi.org/deliver/etsi\\_en/300100\\_300199/30017502/02.04.00\\_40/en\\_30017502v020400o.pdf](http://www.etsi.org/deliver/etsi_en/300100_300199/30017502/02.04.00_40/en_30017502v020400o.pdf).
- [3] Bluetooth Special Interest Group. *Bluetooth Core Specification 4.2*, 2015. <https://www.bluetooth.com/specifications/adopted-specifications>.
- [4] ETSI/DVB. *Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2 : Lower Layers for Satellite standard*, etsi en 301 545-2 v1.2.1 edition, 2014. [http://www.etsi.org/deliver/etsi\\_en/301500\\_301599/30154502/01.02.01\\_60/en\\_30154502v010201p.pdf](http://www.etsi.org/deliver/etsi_en/301500_301599/30154502/01.02.01_60/en_30154502v010201p.pdf).
- [5] AFNOR. *Communication systems for meters and remote reading of meters, Part 4 : Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)*, nf en 13757-4 edition, 2013. <https://www.boutique.afnor.org/norme/nf-en-13757-4/systemes-de-communication-et-de-telereleve-des-compteurs-partie-4-echange-article/778882/fa171157>.
- [6] ITU. *Technical characteristics for an automatic identification system using time-division multiple access in the VHF maritime mobile band*, itu-r m.1371-4 edition, 2010. <http://www.itu.int/rec/R-REC-M.1371-4-201004-S/en>.
- [7] J.B. Anderson, T. Aulin, and C.E. Sundberg. *Digital Phase Modulation*. Applications of Communications Theory. Springer US, 1986.
- [8] T. Aulin, N. Rydbeck, and C. E. Sundberg. Continuous phase modulation - part ii : Partial response signaling. *IEEE Transactions on Communications*, 29(3):210–225, March 1981.
- [9] T. Aulin and C. Sundberg. Continuous phase modulation - part i : Full response signaling. *IEEE Transactions on Communications*, 29(3):196–209, March 1981.



- [10] A. Barbieri and G. Colavolpe. Simplified soft-output detection of CPM signals over coherent and phase noise channels. *IEEE Trans. Wireless Commun.*, 6(7):2486–2496, July 2007.
- [11] R. W. Bauml, R. F. H. Fischer, and J. B. Huber. Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping. *Electronics Letters*, 32(22):2056–2057, Oct 1996.
- [12] L. Bing, T. Aulin, and B. Bai. Spectrally-efficient fdma-cpm systems. In *2014 IEEE International Conference on Communications (ICC)*, pages 5215–5220, June 2014.
- [13] D. Bonacci, R. Prévost, J.-P. Millerioux, J. LeMaitre, M. Coulon, and J.-Y. Tournet. Advanced concepts for satellite reception of ais messages. In *Toulouse Space Show 2012*. June 2012.
- [14] J. C. Chen and C. K. Wen. Papr reduction of ofdm signals using cross-entropy-based tone injection schemes. *IEEE Signal Processing Letters*, 17(8):727–730, Aug 2010.
- [15] G. Colavolpe and R. Raheli. Non-coherent sequence detection of m-ary psk. In *Communications, 1997. ICC '97 Montreal, Towards the Knowledge Millennium. 1997 IEEE International Conference on*, volume 1, pages 21–25 vol.1, Jun 1997.
- [16] M.H.M. Costa. A practical demodulator for continuous phase modulation. In *Information Theory, 1994. Proceedings., 1994 IEEE International Symposium on*, pages 88–89, 1994.
- [17] Haïfa Farès, Raphaël Le Bidan, and Frédéric Guilloud. Techniques d'optimisation de la transmission au niveau de la couche phy. Technical report, Telecom Bretagne, Sept. 2014. Livrable 2.2a du projet GREENCOM.
- [18] Désiré Guel. *Etude de nouvelles techniques de réduction du facteur de crête à compatibilité descendante pour les systèmes multi-porteuses*. PhD thesis, Université de Rennes 1, 2009.
- [19] Seung Hee Han and Jae Hong Lee. An overview of peak-to-average power ratio reduction techniques for multicarrier transmission. *IEEE Wireless Communications*, 12(2):56–65, April 2005.
- [20] J. Huber and W. Liu. An alternative approach to reduced-complexity CPM-receivers. *IEEE J. Select. Areas Commun.*, 7:1437–1449, December 1989.
- [21] A. D. S. Jayalath and C. Tellambura. Reducing the peak-to-average power ratio of orthogonal frequency division multiplexing signal through bit or symbol interleaving. *Electronics Letters*, 36(13):1161–1163, Jun 2000.
- [22] A. E. Jones, T. A. Wilkinson, and S. K. Barton. Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes. *Electronics Letters*, 30(25):2098–2099, Dec 1994.
- [23] G. K. Kaleh. Simple coherent receivers for partial response continuous phase modulation. *IEEE J. Select. Areas Commun.*, 7:1427–1436, December 1989.
- [24] L. Lampe, R. Schober, and M. Jain. Noncoherent sequence detection receiver for bluetooth systems. *IEEE Journal on Selected Areas in Communications*, 23(9):1718–1727, Sept 2005.
- [25] P. A. Laurent. Exact and approximate construction of digital phase modulations by superposition of amplitude modulated pulses (AMP). *IEEE Trans. Commun.*, 34:150–160, February 1986.
- [26] Yves Louët and Jacques Palicot. A classification of methods for efficient power amplification of signals. *annals of telecommunications - annales des télécommunications*, 63(7):351–368, 2008.

- [27] N. Mazzali, G. Colavolpe, and S. Buzzi. Cpm-based spread spectrum systems for multi-user communications. *IEEE Transactions on Wireless Communications*, 12(1):358–367, January 2013.
- [28] U. Mengali and M. Morelli. Decomposition of  $M$ -ary CPM signals into PAM waveforms. *IEEE Trans. Inform. Theory*, 41:1265–1275, September 1995.
- [29] Malek Messai. *Application des signaux CPM pour la collecte de données à grande échelle provenant d'émetteurs faible coût*. PhD thesis, Telecom Bretagne, Nov. 2015.
- [30] Malek Messai, Karine Amis, and Frédéric Guilloud. On the Optimization of a PSP-based CPM Detection. *IEEE transactions on wireless communications*, 2016. in press ; published online 09 Nov 2015.
- [31] Malek Messai, Giulio Colavolpe, Karine Amis, and Frédéric Guilloud. Binary continuous phase modulations robust to a modulation index mismatch. *IEEE Transactions on Communications*, 63(11):4267–4275, Nov 2015.
- [32] Malek Messai, Colavolpe Giulio, Karine Amis, and Frédéric Guilloud. Robust Detection of Binary CPMs With Unknown Modulation Index. *IEEE communications letters*, 19(3):339 – 342, March 2015.
- [33] Malek Messai, Frédéric Guilloud, and Karine Amis. Robust Multiuser Binary CPM Detection with Unknown modulation index. In *EUSIPCO 2015 : 23rd European Signal Processing Conference*, 2015.
- [34] Malek Messai, Frédéric Guilloud, and Karine Amis. Détection Multi-utilisateurs Robuste pour un système Bluetooth. In *GRETSI 2015 : 25ème colloque du Groupement de Recherche en Traitement du Signal et des Images*, 2015.
- [35] H. Meyr, M. Oerder, and A. Polydoros. On sampling rate, analog prefiltering, and sufficient statistics for digital receivers. *IEEE Transactions on Communications*, 42(12):3208–3214, Dec 1994.
- [36] P. Moqvist and T. M. Aulin. Serially concatenated continuous phase modulation with iterative decoding. *IEEE Trans. Commun.*, 49:1901–1915, November 2001.
- [37] S. H. Muller and J. B. Huber. Ofdm with reduced peak-to-average power ratio by optimum combination of partial transmit sequences. *Electronics Letters*, 33(5):368–369, Feb 1997.
- [38] P. A. Murphy, M. Golanbari, G. E. Ford, and M. J. Ready. Optimum and reduced complexity multiuser detectors for asynchronous cpm signaling. *IEEE Transactions on Wireless Communications*, 5(8):1959–1965, Aug 2006.
- [39] T. Nelson and M. Rice. A unified perspective on artm tier i waveforms - part i : common representations. In *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pages 897–903 Vol. 2, Oct 2005.
- [40] H. Ochiai and H. Imai. On the distribution of the peak-to-average power ratio in ofdm signals. *IEEE Transactions on Communications*, 49(2):282–289, Feb 2001.
- [41] H. Ochiai and H. Imai. Performance analysis of deliberately clipped ofdm signals. *IEEE Transactions on Communications*, 50(1):89–101, Jan 2002.

- [42] A. Perotti, S. Benedetto, and P. Remlein. Spectrally efficient multiuser continuous-phase modulation systems. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–5, May 2010.
- [43] E. Perrins and M. Rice. Optimal and reduced complexity receivers for m-ary multi-h cpm. In *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, volume 2, pages 1165–1170 Vol.2, March 2004.
- [44] A. Piemontese and G. Colavolpe. A novel graph-based suboptimal multiuser detector for fdm-cpm transmissions. *IEEE Transactions on Wireless Communications*, 9(9):2812–2819, September 2010.
- [45] M. Sharif and B. H. Khalaj. Peak to mean envelope power ratio of oversampled ofdm signals : an analytical approach. In *Communications, 2001. ICC 2001. IEEE International Conference on*, volume 5, pages 1476–1480 vol.5, 2001.
- [46] S.J. Simmons. Simplified coherent detection of CPM. *IEEE Trans. Commun.*, 43(234):726–728, 1995.
- [47] S.J. Simmons and P.H. Wittke. Low complexity decoders for constant envelope digital modulations. *IEEE Trans. Commun.*, 30:1273–1280, December 1983.
- [48] A. Svensson. Reduced state sequence detection of partial response continuous phase modulation. *Communications, Speech and Vision, IEE Proceedings I*, 138(4):256–268, 1991.
- [49] A. Svensson, Carl-Erik Sundberg, and Tor Aulin. A class of reduced-complexity Viterbi detectors for partial response continuous phase modulation. *IEEE Trans. Commun.*, 32(10):1079–1087, 1984.
- [50] W. Tang and E. Shwedyk. A quasi-optimum receiver for continuous phase modulation. *IEEE Trans. Commun.*, 48(7):1087–1090, 2000.
- [51] J. Tellado and J. M. Cioffi. Efficient algorithms for reducing par in multicarrier systems. In *Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on*, pages 191–, Aug 1998.
- [52] Jose Tellado. *Multicarrier Modulation with Low PAR : Applications to DSL and Wireless*. Kluwer Academic Publishers, Norwell, MA, USA, 2000.
- [53] Zhixing Yang, Haidong Fang, and Changyong Pan. Ace with frame interleaving scheme to reduce peak-to-average power ratio in ofdm systems. *IEEE Transactions on Broadcasting*, 51(4):571–575, Dec 2005.
- [54] Hyunseuk Yoo. *PAPR Reduction in coded-OFDM systems by using multiple candidates and deliberate clipping*. PhD thesis, Telecom Bretagne, Nov. 2011.
- [55] Hyunseuk Yoo, Frédéric Guilloud, and Ramesh Pyndiah. Amplitude PDF analysis of OFDM signal using probabilistic PAPR reduction method. *EURASIP journal on wireless communications and networking*, 2011, 2011.
- [56] Hyunseuk Yoo, Frédéric Guilloud, and Ramesh Pyndiah. PAPR reduction for LDPC coded OFDM systems using binary masks and optimal LLR estimation. *Signal processing*, 91:2606 – 2614, November 2011.

- 
- [57] Hyunseuk Yoo, Frédéric Guilloud, and Ramesh Pyndiah. OFDM-PAPR reduction using coded frequency division binary mask. In *EW 2011 : European Wireless*, 2011.
- [58] Xuefu Zhou and J. J. Caffery. A new distribution bound and reduction scheme for ofdm papr. In *Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on*, volume 1, pages 158–162 vol.1, Oct 2002.
- [59] S. ten Brink. Convergence behavior of iteratively decoded parallel concatenated codes. *IEEE Trans. Commun.*, 49(10):1727–1737, October 2001.
- [60] R. van Nee and A. de Wild. Reducing the peak-to-average power ratio of ofdm. In *Vehicular Technology Conference, 1998. VTC 98. 48th IEEE*, volume 3, pages 2072–2076 vol.3, May 1998.



## **Troisième partie**

# **Perspectives et conclusions**



## Chapitre 5

# Perspectives de recherche : les communications numériques sans fil à trames courtes

### 5.1 Contexte

Les communications entre machines constituent l'un des nouveaux enjeux de la conception de la future norme de communications mobiles de cinquième génération (5G). Ce terme de communication entre machines souligne un nouveau mode de communications qui ne serait pas centré sur la personne mais sur des échanges d'information entre différents objets connectés (internet des objets) [7, 15]. Ces objets connectés peuvent être aussi bien liés à la santé pour le grand public, en transmettant à un téléphone portable par exemple le rythme cardiaque d'un jogger pendant son entraînement, ou en envoyant un signal d'alarme en cas de chute d'une personne dépendante, transmis de son bracelet électronique vers un centre de surveillance. Mais ils peuvent être également présents dans des milieux moins grand public comme par exemple la télé-relève des compteurs d'eau et de gaz, ou bien comme système de mesure dans une industrie permettant un contrôle et une régulation automatique de la production. Les prévisions d'augmentation de ce type de communications n'hésitent pas à avancer des chiffres parfois exagérés mais il ne fait aucun doute que le potentiel des applications est très important.

De nombreux acteurs technologiques se sont déjà positionnés sur les réseaux de communications qui permettront de favoriser l'émergence de ces nouveaux usages comme Sigfox, LoRa et NB-IOT [7]. On peut citer également GrDF avec le démarrage prochain du déploiement de 11 millions de compteurs "Gazpar" [14] transmettant l'index de consommation par voie radio vers des concentrateurs. Ces types de communication sont caractérisés par des transmissions à bas débit car le volume d'informations échangées est faible. Ce petit volume de données doit cependant être transmis sans augmenter significativement la latence, ce qui rend impossible la concaténation de plusieurs messages à transmettre pour envoyer en une seule fois une grande quantité d'information. On se retrouve donc avec le besoin de transmettre régulièrement de petites quantités d'information, ce qui conduit à transmettre de petites trames sur le canal radio. La fréquence de ces trames pour un même utiliza-



teur<sup>1</sup> peut être variable selon l'application. Une autre raison expliquant l'utilisation de trames courtes vient du besoin de devoir communiquer avec un grand nombre d'utilisateurs. Dans ce cas, réduire la durée et le débit d'une trame permet d'éviter les collisions entre utilisateurs. Dans certaines communications entre machines, où la latence est un paramètre important, la réduction de la taille de la trame permet d'augmenter la réactivité des processus dépendants de l'échange de ces informations. Alliées à une grande fiabilité, ces communications sont souvent présentes dans les systèmes où la sécurité des personnes ou des machines est en jeu (communications entre véhicules et l'extérieur (V2X communications), détection nécessitant un arrêt d'urgence, etc ...).

## 5.2 Enjeux

Lorsque l'information est transmise par trames courtes, les conséquences sur la couche physique ne sont pas négligeables. La première porte sur codage correcteur d'erreurs. En effet, si la taille de la trame est réduite, à débit symboles constant, le nombre de bits codés (la longueur du code) est également réduit. Or les performances d'un code correcteur d'erreurs sont fortement contraintes par sa longueur. Ce phénomène est illustré sur la figure 5.1 où est représentée la perte en rapport signal-sur-bruit que l'on doit accepter lorsqu'on limite la longueur de code de canal. Cette perte est la différence entre le SNR nécessaire pour atteindre un taux d'erreur trame fixé (à  $10^{-6}$  pour les courbes en bleu, et à  $10^{-2}$  pour celles en rouge) à débit fixé (entre 0.5 et 2.5 bits par dimension réelle), et le SNR nécessaire pour atteindre la capacité du canal gaussien (impliquant l'utilisation de codes gaussiens de longueur infinie). L'estimation de cette perte est réalisée grâce à la borne inférieure du taux d'erreur en longueur finie proposée par [22] et évaluée numériquement selon [9, 10]. Pour cette figure, on fait l'hypothèse du codage sans restriction sur l'alphabet de modulation et avec une contrainte de puissance moyenne par mot de code constante. On constate que la perte augmente exponentiellement avec la décroissance de la longueur. Bien entendu, elle est d'autant plus importante que le taux d'erreur trame est faible. On remarque également que plus la capacité augmente (à fort SNR) plus l'écart à la capacité devient indépendant de cette capacité (typiquement pour une capacité  $> 2$  bits/dimension sur la courbe). Je propose par la suite de considérer que les trames de petites longueurs contiennent moins de 500 bits. Cet ordre de grandeur permet de fixer les idées et n'a pas d'autre objectif. Notamment, selon le contexte, la longueur d'une petite trame pourrait être également exprimée en nombre de symboles transmis sur le canal, et pas en nombre de bits codés.

Si dans le régime des grandes longueurs, les codes LDPC et Turbocodes binaires sont incontournables, de nombreuses autres possibilités existent pour les codes de petites tailles : codes algébriques, codes concaténés, codes binaires ou non-binaires, codes polaires. Mais leur conception dépend également des spécifications de la chaîne de communication dans laquelle ils seront intégrés : présence ou non d'une voie de retour (impliquant des codes compatibles en rendement, la détection et la correction d'erreurs), type de canal (canal mobile ou quasi-statique), complexité du décodage. Ces spécifications entraînent des stratégies de codage différentes.

Outre le codage correcteur d'erreur, il faut étudier la conception de l'ensemble des éléments de la chaîne. Par exemple, pour s'adapter au rapport signal sur bruit du canal, les schémas classiques consistent à changer le rendement du codage et la taille de la constellation. Un nouveau principe basé

1. Je me permet de parler d'utilisateur, même si il s'agit d'une machine : c'est l'aspect utilisation de la ressource radio qui est concernée.

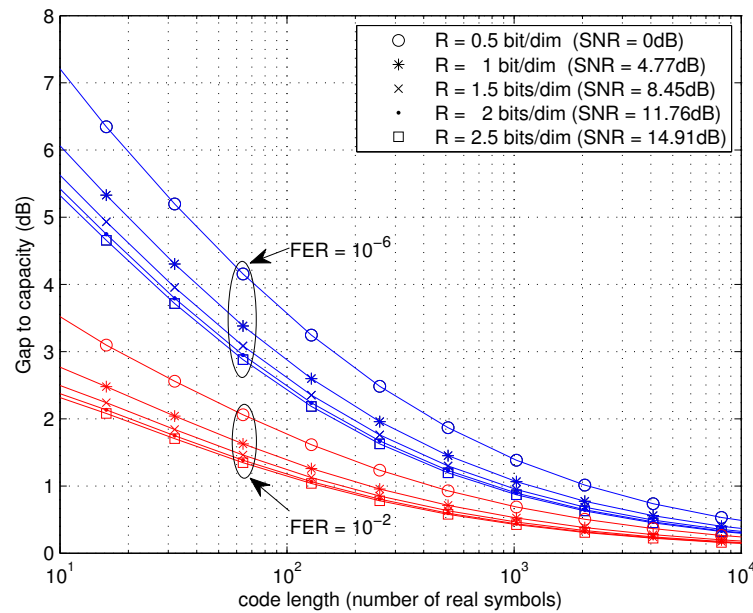


FIGURE 5.1 – Influence de la longueur du code sur les performances de la transmission [9, 10]. Le code source permettant cette évaluation numérique est disponible sur <http://dgt.dei.unipd.it/media/download/427/>.

sur la mise en forme (*shaping*) des symboles de modulation a été proposé par Georg Böcherer et al. [2]. Ce schéma permet de modifier l'efficacité spectrale en conservant un seul schéma de codage correcteur et de modulation. Il a été proposé dans le cadre de la diffusion par satellite mais je souhaite étudier ce principe dans le cadre des trames courtes, notamment lors de mon prochain séjour sabbatique au LNT de la Technische Universität de Munich. La mise en forme peut également apporter un complément de gain de rapport signal-sur-bruit. Ce point sera développé en section 5.3

On associe souvent la communication entre machines avec les problèmes de consommation énergétique dans le sens où l'on souhaite la réduire le plus possible. En effet, quand des communications sans fil sont déployées pour transmettre une faible quantité de données, il y a souvent i) absence d'énergie disponible via un réseau de distribution et ii) impossibilité de maintenance pour changer les batteries d'alimentation (pour des raisons techniques et/ou économiques). De ce fait, comme je l'ai décrit dans la section 4.3, la modulation à phase continue est un choix pertinent car il permet d'obtenir une excellente efficacité énergétique. Le travail de thèse de Malek Messai se poursuit par l'étude du problème de l'accès multiple : l'enjeu est d'avoir le plus de transmissions possibles de petites trames vers un même concentrateur. Les collisions éventuelles entre les transmissions issues de différents émetteurs sont à résoudre avec le moins de complexité possible. L'hypothèse de transmission sporadique liée à la petite taille des trames permet de réduire la complexité en mettant en œuvre les techniques de traitement du signal parcimonieux. Ce point sera développé en section 5.4.

Pour terminer la présentation de ces enjeux des communications à trames courtes, il faut évoquer l'en-tête (ou le préambule) de la trame envoyée qui n'est pas constitué de bits d'information mais de symboles connus (symboles pilotes) ou de symboles liés à l'information de signalisation. On peut également mettre dans la même problématique les éventuels bits constituant le post-ambule pouvant contenir des bits de CRC et des symboles indiquant la fin de trame. La taille de ces informations

annexes n'est pas liée à la taille de la trame et occasionne une réduction de l'efficacité spectrale qui n'est plus négligeable si la trame est trop petite. Pour ne pas réduire l'efficacité spectrale de la transmission, il faut soit éliminer l'en-tête, soit le réduire le plus possible, et résoudre d'une autre manière les problèmes qui en découleront : la synchronisation, l'estimation du canal (et les conséquences sur l'adaptation du lien —puissance, choix du codage et de la modulation— ou de l'égalisation), la gestion de l'accès multiple, la détection d'erreurs (CRC) et stratégie de retransmission (HARQ), etc...

Ces communications à trames courtes peuvent donc faire l'objet d'un grand nombre de sujets d'étude. Je propose dans ce chapitre d'approfondir deux d'entre eux : la mise en forme (*shaping*), puis l'accès multiple avec les modulations à phase continue (CPM).

## 5.3 Mise en forme

### 5.3.1 Distribution non uniforme des symboles

#### Distribution optimale

Lorsque l'on calcule la quantité maximale d'information mutuelle entre l'entrée et la sortie d'un canal à bruit additif blanc gaussien si l'entrée est contrainte par une constellation de taille finie  $M$ , on constate d'une part que cette information mutuelle est bornée par  $\log_2(M)$  bits par symbole, mais qu'en plus, pour des valeurs beaucoup plus faibles que cette borne, il y a un écart d'environ 1.53 dB ( $10 \log_{10}(\frac{\pi e}{6})$ ) avec la capacité du canal gaussien. Ce phénomène est illustré sur la figure 5.2 pour laquelle j'ai choisi le modèle de canal discrétisé au temps symbole avec  $R_n = X_n + Z_n$  où  $R_n$  est la sortie du canal,  $X_n$  est le symbole transmis appartenant à une constellation de symboles réels de type PAM (*Pulse Amplitude Modulation*) et  $Z_n$  est une variable aléatoire de distribution gaussienne centrée de variance  $N$ . On définit également l'énergie moyenne d'un symbole transmis par  $E_s = \mathbb{E}(X_n^2)$ . Il a été montré qu'une partie de cet écart pouvait être récupéré en jouant sur la distribution des symboles : distribution de probabilité et/ou distribution géométrique des symboles dans l'espace [13, 16]. Le gain ainsi apporté est appelé gain de mise en forme (*shaping gain*), et il est complémentaire du gain de codage. Il peut donc apporter un gain de performance intéressant si le gain de codage est limité par la taille du code.

Dans la suite de cette partie, je conserve la constellation de symboles PAM par souci de simplification mais l'extension aux symboles QAM complexes est immédiate. La constellation PAM à  $M$  symboles notée  $A_M$  sera définie à l'aide de la distance entre 2 symboles notée  $\Delta = 2$  et on aura  $A_M = \{a_i = -(M-1) + \Delta i, 0 \leq i \leq M-1\}$ . Si on suppose que les symboles sont émis de manière équiprobable, la valeur maximale de l'information mutuelle est simplement donnée par l'entropie des symboles émis :  $H(X) = -\sum_{i=0}^{M-1} p_i \log_2(p_i) = \log_2(M) \Leftrightarrow p_i = \frac{1}{M}$  où  $p_i = \Pr(X = a_i)$ , et l'énergie moyenne par symbole s'écrit  $E_s = \mathbb{E}(X_n^2) = \sum_{i=0}^{M-1} p_i |a_i|^2 = \frac{M^2-1}{3}$  dans le cas d'une distribution uniforme.

Dans l'hypothèse où les symboles ne sont pas associés à une probabilité uniforme, l'entropie va diminuer, et l'information mutuelle également. Cependant, si on augmente également la taille de la constellation, il est possible de retrouver la même quantité d'information par symbole qu'avec la constellation plus petite et une distribution équiprobable. Le problème est alors d'optimiser la distribution de probabilité  $\mathbf{p} = \{p_i\}_{0 \leq i \leq M-1}$  d'une constellation  $A_M$  afin d'atteindre une entropie

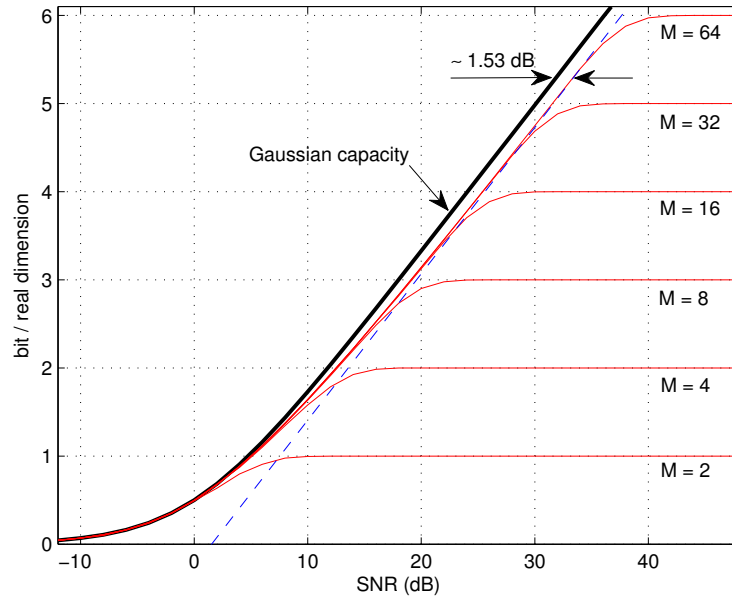


FIGURE 5.2 – Illustration de l'écart entre les capacités contraintes par la constellation (ici pour des constellation réelles de symboles PAM) et la capacité du canal gaussien lorsque les symboles de la constellation ont une distribution de probabilité uniforme. (Inspirée de [12].)

$H_0$  donnée en minimisant l'énergie moyenne par symbole. Ce problème d'optimisation s'écrit :

$$\begin{aligned} \tilde{\mathbf{p}} &= \arg \min_{\mathbf{p}} E_s(\mathbf{p}) \\ \text{s.t.} & \begin{cases} H(\mathbf{p}) = H_0 \\ \sum_{i=0}^{M-1} p_i = 1 \end{cases} \end{aligned}$$

et peut se résoudre à l'aide du lagrangien [11]

$$J(\mathbf{p}) = \sum_{i=0}^{M-1} p_i |a_i|^2 + \lambda_1 \left( - \sum_{i=0}^{M-1} p_i \log_2(p_i) - H_0 \right) + \lambda_2 \left( \sum_{i=0}^{M-1} p_i - 1 \right)$$

où  $\lambda_1$  et  $\lambda_2$  sont les multiplicateurs de Lagrange. La dérivation du lagrangien par rapport aux probabilités  $p_i$  fournit  $M$  équations :

$$\left( \frac{\partial J(\mathbf{p})}{\partial p_i} \right)_{\mathbf{p}=\tilde{\mathbf{p}}} = 0 \Leftrightarrow |a_i|^2 - \frac{\lambda_1}{\ln(2)} (\ln(\tilde{p}_i) + 1) + \lambda_2 = 0, \quad 0 \leq i \leq M-1$$

La densité optimale  $\tilde{\mathbf{p}}$  ainsi obtenue est une densité gaussienne échantillonnée aux position des symboles de la constellation  $A_M$ , de la forme  $\tilde{p}_i = \alpha \exp(-s|a_i|^2)$  où  $(\alpha, s) = \left( \exp\left(-1 + \frac{\lambda_2}{\lambda_1} \ln(2)\right), -\frac{\ln(2)}{\lambda_1} \right)$ . On dispose ainsi de  $M+2$  équations (les  $M$  dérivées nulles du lagrangien, la condition de normalisation, et l'entropie ciblée) permettant de trouver les  $p_i$  ainsi que les valeurs de  $\alpha$  et de  $s^2$ . J'illustre sur la figure 5.3 quelques exemples de distributions pour une constellation à  $M=16$  symboles PAM permettant d'atteindre des valeurs de  $H_0 = 2, 3$  ou 4 bits/dimension (figure de gauche) et

2. On trouve simplement  $\alpha = \frac{1}{\sum_{i=0}^{M-1} \exp(-s|a_i|^2)}$  mais la valeur de  $s$  se résout numériquement.

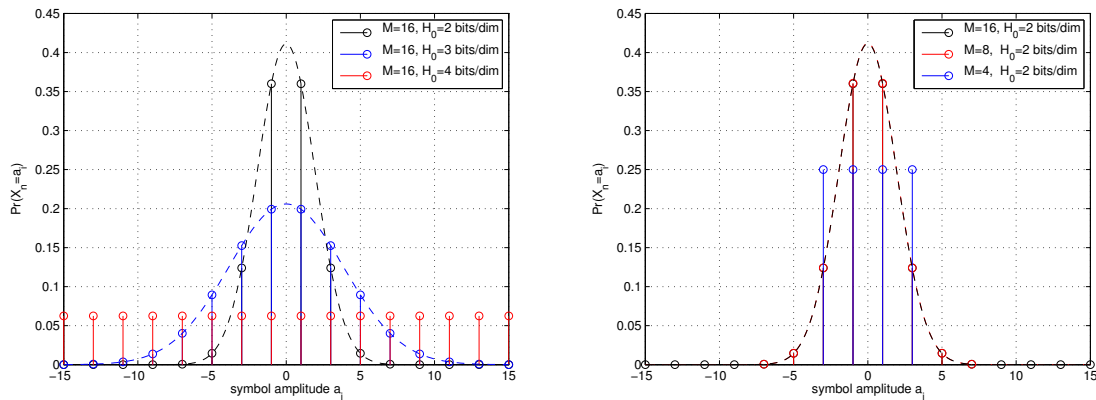


FIGURE 5.3 – Densités de probabilité uniformes ou non-uniformes permettant soit de changer le nombre maximal de bits par symbole  $H_0$  en conservant une taille de constellation  $M$  constante, soit de conserver le même  $H_0$  avec différentes tailles de constellations  $M$ .

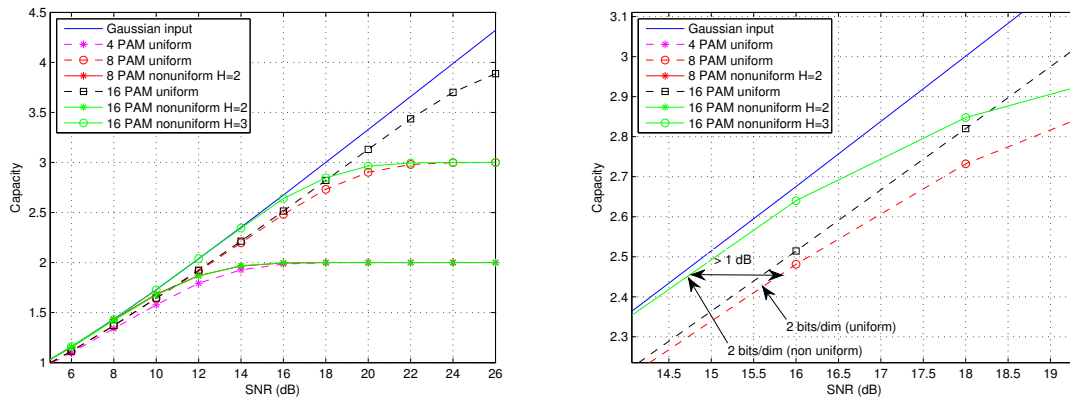


FIGURE 5.4 – Comparaison des capacités des modulation PAM avec distributions uniformes ou non-uniformes, et zoom (à droite) sur la zone mettant en évidence l'intérêt de la distribution non-uniforme.

quelques exemples de constellations à  $M = 4, 8$  ou  $16$  symboles PAM permettant d'atteindre  $H_0 = 2$  bits/dimension (figure de droite).

### Influence sur les performances

L'information mutuelle d'une modulation à constellation finie dans un canal AWGN dépend de la position et de la distribution de probabilité des symboles. Lorsque la distribution de probabilité change, cette information mutuelle est changée comme l'illustre la figure 5.4. On constate que pour atteindre une efficacité spectrale donnée, l'information mutuelle obtenue avec une modulation à grand nombre d'états conjointement avec une distribution de probabilité non uniforme sur les symboles permet de se rapprocher de la capacité gaussienne et offre dans cet exemple une amélioration d'environ 1 dB de l'information mutuelle obtenue avec une distribution uniforme. Cette amélioration est également visible sur les courbes de taux d'erreur symbole présentées sur la figure 5.5.

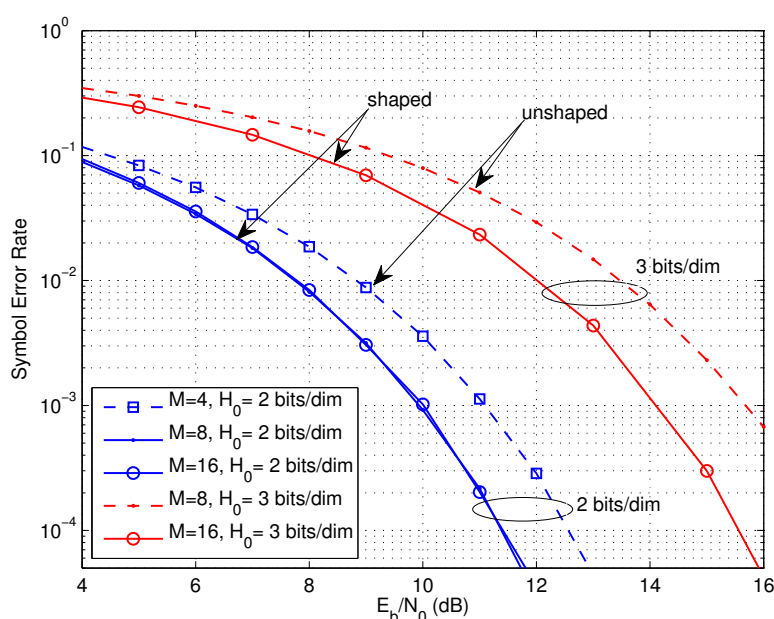


FIGURE 5.5 – Borne supérieure des taux d’erreurs symboles des modulations PAM à  $M$  symboles non codées, pour différentes efficacités spectrales obtenues avec ou sans mise en forme (extrait de [21]).

### 5.3.2 Considérations pratiques

Les éléments binaires à transmettre étant uniformément distribués, il faut pouvoir effectuer un traitement qui, à partir de ce flux binaire va générer un flux de symboles dont la distribution de symboles suit la loi  $\tilde{\mathbf{p}}$  obtenue en section 5.3.1. Ce traitement est analogue au décodage de source entropique qui fait correspondre des séquences binaires équiprobables à des séquences de symboles non-équiprobables. C’est la raison pour laquelle le codage de Huffman a été proposé notamment dans [16, 30, 3] afin de réaliser pratiquement cette mise en forme dénommée *Huffman Shaping*. Je présente par la suite l’utilisation de l’algorithme de Huffman afin d’illustrer la sous-optimalité introduite par cette mise en forme. En effet, si on part de la distribution optimale  $\tilde{\mathbf{p}}$  qui permet de satisfaire aux contraintes d’énergie moyenne par symbole et d’entropie, l’utilisation d’un codage de Huffman va entraîner une modification des probabilités symbole obtenues par le biais de ce codage et va ainsi modifier l’énergie symbole moyenne et l’entropie. Le tableau 5.1 donne un exemple de codage associé au cas  $M = 8$  et  $H_0 = 2$  bits/dim dans lequel on constate que les probabilités obtenues  $\hat{\mathbf{p}}$  sont différentes de celles souhaitées  $\tilde{\mathbf{p}}$ . Cela conduit à une entropie de  $H(\hat{\mathbf{p}}) = 1.92$  bits/dim au lieu de 2 bits/dim. Cet écart peut pénaliser le gain espéré en taux d’erreurs symbole comme l’illustre la figure 5.6 pour 2 bits/dim : le gain par rapport à la version non-mise en forme est plus faible que celui obtenu avec la distribution optimale car les probabilités sont difficiles à coder fidèlement avec le codage de Huffman lorsque la distribution s’éloigne d’une distribution dyadique. Pour 3 bits/dim, on constate que le code de Huffman n’entraîne qu’une très faible perte par rapport à la distribution optimale.

Le second problème du codage de Huffman pour la mise en forme est la longueur variable des éléments du code. Leur transmission dans un canal bruité entraîne des erreurs de synchronisation et rend la transmission à bas rapport signal sur bruit impossible.

TABLE 5.1 – Exemple de distribution de probabilités obtenus pour  $M = 8$  et  $H_0 = 2$  bits/dim et influence de l'utilisation d'un code de Huffman sur cette distribution.

$a_i$	$\tilde{p}$	code binaire	$\hat{p}$
-7	0.0006	0000001	$2^{-7}$
-5	0.0147	00001	$2^{-5}$
-3	0.1241	001	$2^{-3}$
-1	0.3607	1	$2^{-1}$
1	0.3607	01	$2^{-2}$
3	0.1241	0001	$2^{-4}$
5	0.0147	000001	$2^{-6}$
7	0.0006	0000000	$2^{-7}$

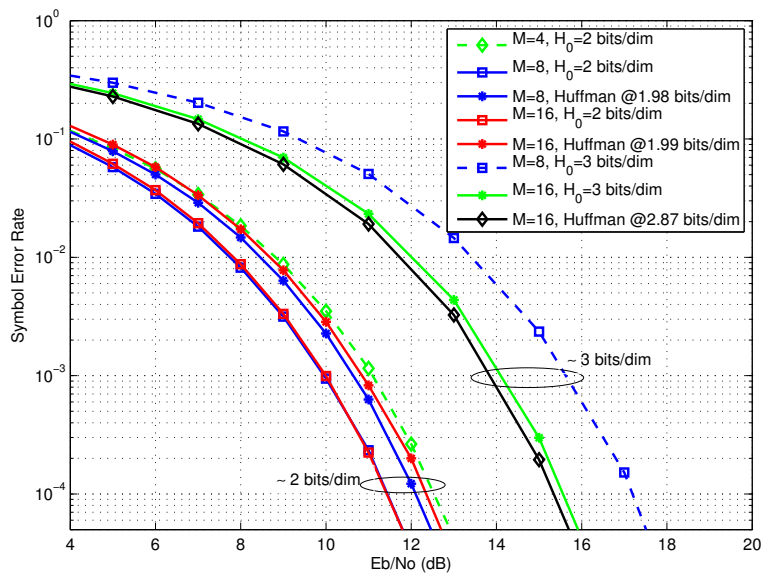


FIGURE 5.6 – Influence de l'utilisation du codage de Huffman sur la borne supérieure des taux d'erreurs symboles des modulations PAM à  $M$  symboles non codées pour différentes efficacités spectrales (extrait de [21]).

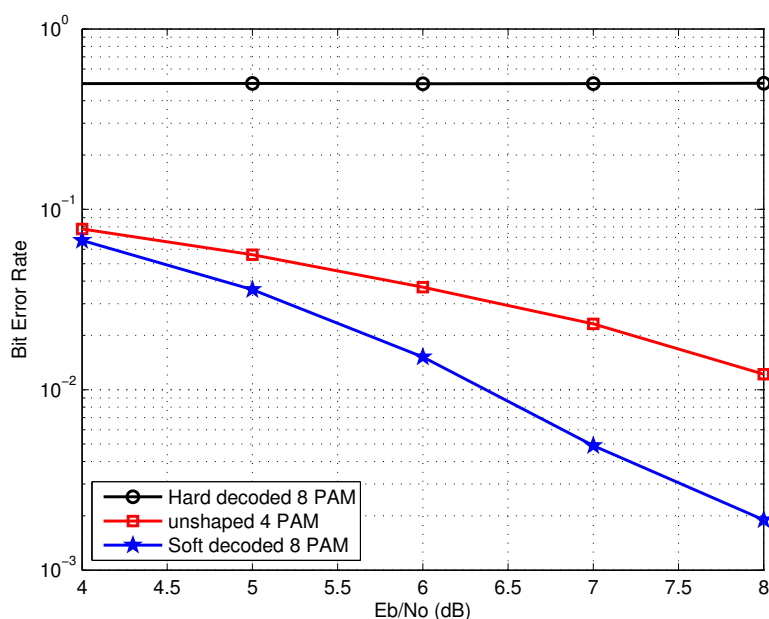


FIGURE 5.7 – Taux d’erreur binaire obtenu après décodage de la mise en forme probabiliste (ferme ou pondéré) et comparaison avec la modulation sans mise en forme (extrait de [21]).

### 5.3.3 Propositions de solutions

Pour résoudre le problème de la longueur variable des codes, il est possible de s’inspirer des codes à longueurs fixes proposés par Böcherer et al. [27] que je vais étudier durant mon séjour sabbatique au LNT de la TU de Munich.

Il est également possible de s’inspirer du schéma de décodage source-canal conjoint proposé dans [34] où les longueurs variables du codage de source sont transmises comme information supplémentaire dans le message envoyé. C’est ce que j’ai proposé de faire durant le stage de fin d’études de Minh On Vu Ngoc [21] en fixant un nombre  $L$  de symboles PAM à transmettre. Du fait du codage entropique utilisé, la  $n$ -ième transmission de  $L$  symboles correspond à une longueur  $l_n$  binaire. On fait alors l’hypothèse que la longueur  $l_n$  binaire est transmise de manière fiable par un autre canal. Un décodage pondéré en liste peut alors être implémenté en ne retenant que la séquence binaire la plus probable parmi toutes les séquences de  $L$  symboles encodées en  $l_n$  bits. Les performances obtenues sont illustrées sur la figure 5.7 où est représenté le taux d’erreur binaire d’une transmission faite avec  $H_0 = 2$  bits/dim en utilisant soit une PAM  $M = 4$  sans mise en forme (courbe rouge, marque carrée), soit une PAM  $M = 8$  avec mise en forme par l’algorithme de Huffman. Dans ce dernier cas, on procède soit au décodage à décision ferme (courbe noire, marque circulaire), soit au décodage à décision pondérée (courbe bleue, marque étoilée). Ces performances indiquent clairement que le schéma de mise en forme de type Huffman ne doit pas être utilisé sans décodage pondéré et que dans ce cas, le gain de décodage apporté vient compléter le gain de mise en forme.

Dans le cas d’une transmission codée, le décodage pondéré de la mise en forme probabiliste permet d’itérer le processus et d’améliorer les performances, comme on peut l’observer sur la figure 5.8. Dans cet exemple, un code convolutif (13, 15) et un entrelaceur de 8192 bits sont utilisés, offrant la possibilité d’un décodage itératif entre le code et la mise en forme. On constate que les performances



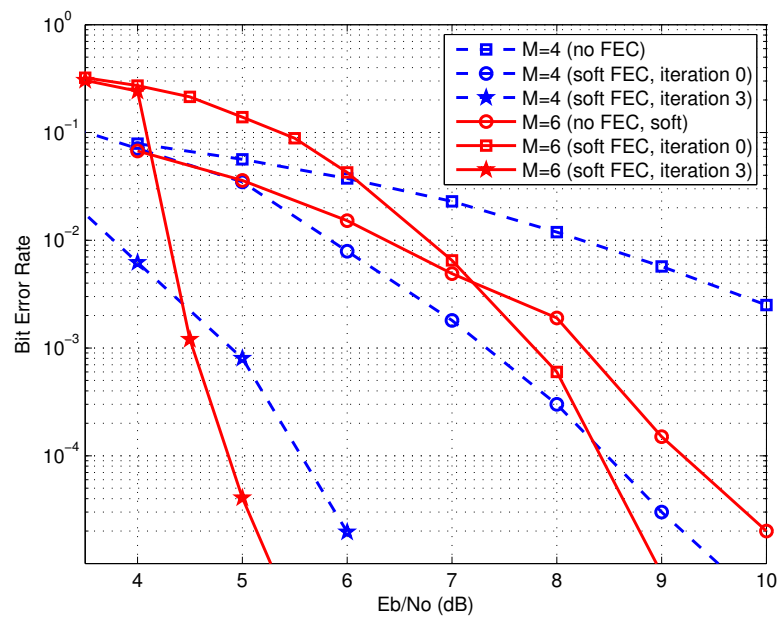


FIGURE 5.8 – Taux d’erreur binaire obtenu après décodage pondéré de la mise en forme probabiliste et comparaison avec la modulation sans mise en forme dans le cas d’une transmission codée par un code convolutif (13, 15) et un entrelaceur de 8192 bits (extrait de [21]).

se croisent à l’avantage de la mise en forme probabiliste pour un taux d’erreur inférieur à  $3 \cdot 10^{-3}$ .

### 5.3.4 Conclusions

Si le gain de mise en forme (*shaping gain*) semble être une solution intéressante pour améliorer les performances de transmission des trames courtes limitées par la taille du code, sa mise en œuvre par l’intermédiaire du codage entropique de Huffman souffre de quelques pondérations sur les gains espérés. Des améliorations de performance acceptables peuvent être obtenues au prix d’une complexité de décodage importante qui limite la taille de la constellation utilisée et la taille des trames.

Il sera donc particulièrement pertinent d’étudier et de comparer la transposition aux trames courtes de la solution à base de codes à longueur fixe que je vais pouvoir approfondir dans le cadre de mon prochain séjour sabbatique au LNT à la TU de Munich durant le premier semestre 2017.

## 5.4 Accès multiple

### 5.4.1 Introduction

Transmettre des trames de petite longueur permet à un grand nombre d’utilisateurs de partager un même canal radio, avec par exemple un accès multiple par division temporelle. Mais la gestion d’un partage d’accès orthogonal (sans collision) pour un très grand nombre d’utilisateurs peut nécessiter une quantité d’information de signalisation trop grande devant la quantité d’information utile. Afin d’éviter cela, on peut choisir un mode d’accès non contrôlé dit "aléatoire", dont l’invention à l’Université de Hawaï par l’équipe de Norman Abramson entre 1968 et 1971 sous le nom d’ALOHA a marqué l’histoire des télécommunications, en lançant les bases du futur réseau Ethernet : le principe

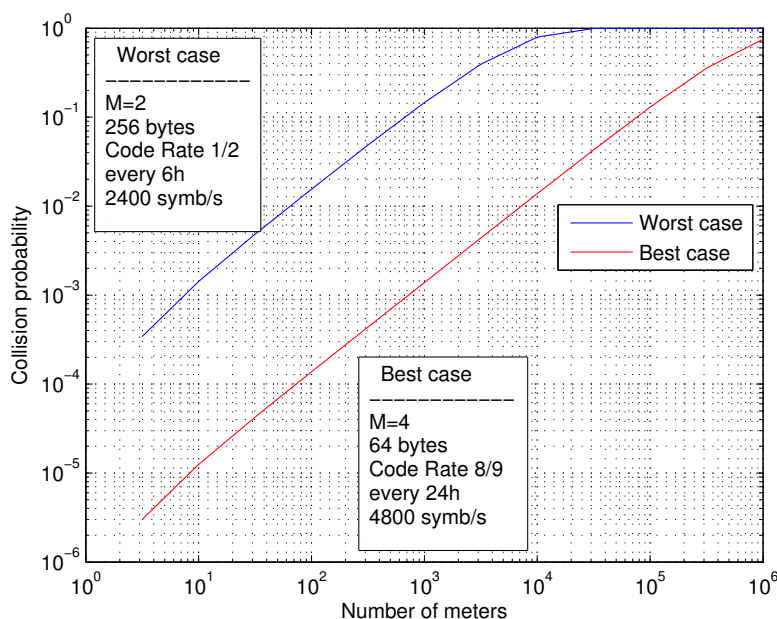


FIGURE 5.9 – Probabilité de collision entre au moins 2 paquets en fonction du nombre d'utilisateurs. Application numérique faite avec les données GrDF.

est un accès aléatoire au canal couplé à un système d'échanges d'accusés de réception permettant la retransmission de l'information non-reçue (à cause d'un conflit d'accès au canal par exemple).

Pour fixer les ordres de grandeur des durées de trames et du nombre d'utilisateurs potentiels, prenons l'exemple de la transmission des index des compteurs de gaz vers les concentrateurs que GrDF va déployer dans les années à venir. Différents paramètres de transmissions ont été envisagés faisant ainsi varier la durée d'une trame notée  $\Delta$  (modulation BPSK ou QPSK, codage correcteur d'erreur de rendement 1/2 ou 8/9, 64 ou 256 octets d'informations, débits de symboles de 2.4 ou 4.8 kbauds, période de transmission  $T_x$  de 6h ou de 24h). La période de retransmission permet de définir le rapport cyclique  $\nu = \frac{\Delta}{T_x}$ . En notant  $K$  le nombre d'utilisateurs (ici les compteurs), et en supposant que les transmissions sont indépendantes et identiquement distribuées, la probabilité de collision entre au moins 2 transmissions est donnée par  $\Pr(\text{collision}) = 1 - (1 - \nu)^{2(K-1)}$  et est représentée sur la figure 5.9 pour le plus petit et le plus grand rapport cyclique. Selon GrDF, il y aura entre  $10^3$  et  $10^4$  compteurs par concentrateur, soit des probabilités de collision pouvant être relativement importantes. Pour retrouver l'information perdue par collision, on peut penser à un système d'acquiescements-retransmissions, mais il risquerait de limiter la capacité du système par la voie descendante.

L'autre solution consiste à essayer de traiter l'interférence de ces collisions au niveau du récepteur afin de retrouver les informations envoyées par tous les utilisateurs en collision. Le nombre d'utilisateurs actifs simultanément reste relativement faible. En effet, si on suppose une transmission synchrone des trames, le nombre d'émissions simultanées suit une loi binomiale d'espérance  $K\nu$  soit en moyenne moins de 5 utilisateurs actifs simultanément dans le cas de GrDF. Cela signifie que le nombre d'utilisateurs actifs (ceux qui transmettent) est très faible devant le nombre total d'utilisateurs : le signal défini par l'ensemble des signaux émis par tous les utilisateurs (les actifs et les silencieux) est un signal parcimonieux (le signal tout-à-zéro représente l'absence de transmission

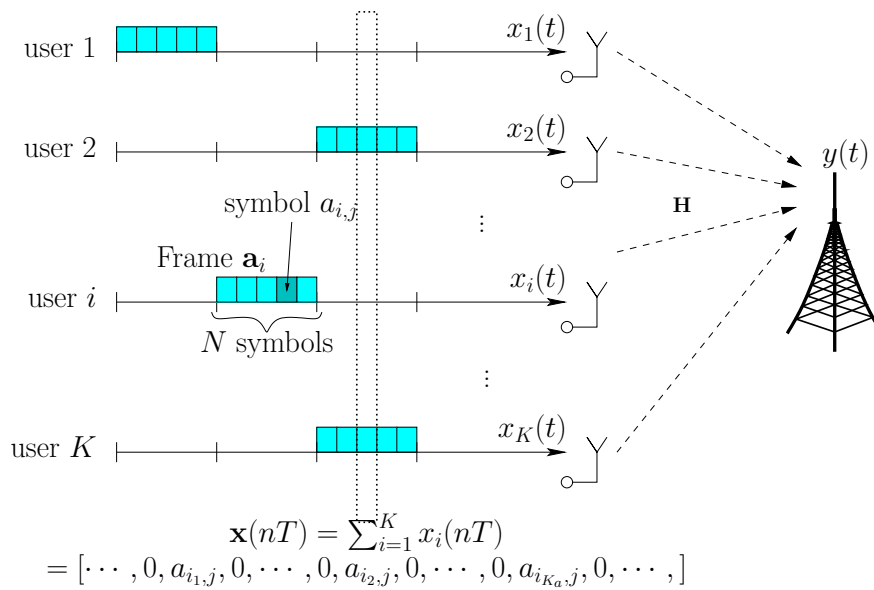


FIGURE 5.10 – Communications sporadiques vers un concentrateur.

pour les utilisateurs silencieux).

Retrouver les informations transmises même en présence de collisions est possible en utilisant les techniques de résolution des problèmes inverses exploitant le caractère parcimonieux des signaux. Dans la suite de cette partie, j'expose l'état de l'art de ce type de techniques utilisées dans le cas des modulations linéaires, puis je dresse les principaux enjeux à relever lorsque l'on souhaite les mettre en œuvre avec des modulations CPM.

## 5.4.2 Détection parcimonieuse

Pour la suite de cette discussion, je suppose que les trames transmises sont synchrones (*slotted ALOHA*) afin de simplifier l'étude et les notations. Les notations liées aux trames transmises par les  $K$  utilisateurs sont représentées sur la figure 5.10; les trames émises par l'utilisateur  $i$  sont notée  $\mathbf{a}_i$ . Le  $j$ -ème symbole de la  $i$ -ème trame est noté  $a_{i,j}$ . Le signal reçu  $y(t)$  est la somme des signaux émis  $x_i(t)$  et du bruit additif blanc gaussien  $\mathbf{n}(t)$ . La somme des signaux émis peut être pondérée par des coefficients de canal dans le cas des canaux à évanouissements.

### Etat de l'art

Dans le cas des modulations linéaires, un filtre de mise en forme est utilisé à l'émetteur et son filtre adapté est utilisé au récepteur, l'ensemble vérifiant le critère de Nyquist. Cela permet d'écrire les signaux échantillonnés au temps symbole  $T$ . Ainsi au temps symbole  $t = nT$ , on a  $\tilde{y}_n = \mathbf{h}_n \mathbf{x}_n + b_n$ . Dans cette expression, la notation  $\tilde{y}$  signifie le résultat du filtrage de  $y$  par le filtre adapté. De plus, la  $i$ -ème composante du vecteur  $\mathbf{x}_n$  correspond au symbole émis par l'utilisateur  $i$  ou à un zéro si l'utilisateur est silencieux. Ce vecteur a donc  $K_a$  composantes non-nulles parmi ses  $K$  éléments ( $K_a$  est le nombre d'utilisateurs actifs). Le vecteur  $\mathbf{h}_n$  contient les affaiblissements du canal. Pour un canal AWGN, on aurait  $h_n(i) = 1, 1 \leq i \leq K$ .

Retrouver le vecteur  $\mathbf{x}_n$  à partir de l'observation  $\tilde{y}_n$  est un problème sous-déterminé ayant une infinité de solutions. Il est possible d'augmenter la dimension de  $\tilde{y}_n$  en introduisant de la diversité :

code d'étalement, diversité d'antennes par exemple. Dans la suite de cette partie, nous allons faire l'hypothèse que des codes d'étalement d'un facteur  $N_s$  sont utilisés (en poursuivant l'application des compteurs de gaz, la fréquence porteuse est trop faible pour envisager une diversité d'antennes avec un encombrement réduit). Il ne s'agit pas de construire un schéma de type CDMA (accès multiple par division par codes), mais juste d'étaler chaque symbole transmis afin d'augmenter la dimension de l'observation qui devient  $N_s$  (pas besoin de séquences orthogonales par exemple). Le facteur d'étalement  $N_s$  reste cependant très inférieur au nombre d'utilisateurs  $K$  et le problème demeure sous-déterminé. Cependant, l'a-priori que le vecteur  $\mathbf{x}_n$  est creux peut être incorporé dans les algorithmes des problèmes inverses et on peut ainsi obtenir des solutions parcimonieuses. Il faut par exemple  $\mathcal{O}(K_a \log(K/K_a))$  dimensions sur  $\check{\mathbf{y}}_n$  pour trouver  $\mathbf{x}_n$  avec l'algorithme *Orthogonal Matching Pursuit* (OMP) [29].

Sur les bases du travail d'échantillonnage compressé et de la reconstruction associée [5, 6], la détection multi-utilisateurs (MUD) basée sur la notion d'échantillonnage compressé (CS) a été proposée dans [33]. On y recherche deux types d'information : la position des émetteurs actifs (détection du support) et la valeurs des symboles transmis (détection des données). Plusieurs algorithmes ont été proposés pour résoudre ce problème au niveau symbole. Dans [33], la détection conjointe du support et des données est faite en utilisant différents critères (*Minimum Mean Square Error –MMSE–*, *Least Squares –LS–*, *Least Absolute Shrinkage and Selection Operator –LASSO–*). Dans [20] et [4], la détection du support (détection d'énergie) est suivie d'une détection des données par un critère LS. Dans [25], les algorithmes de détection sont basés sur l'OMP et l'OLS (*Orthogonal Least Squares*).

### Application aux modulations CPM

L'application des techniques d'échantillonnage compressé pour la détection multi-utilisateur (CS-MUD) n'est pas applicable directement aux modulations CPM car ces modulations sont non-linéaires. En effet, il est nécessaire d'effectuer un filtrage avec différents filtres adaptés (décomposition de Rimoldi [23] par exemple) pour pouvoir déterminer le symbole reçu à chaque temps symbole.

Cependant, en passant par la décomposition de Laurent [18] et en ne conservant que la forme d'onde de plus grande énergie notée  $C_0(t)$ , on obtient l'expression approchée du signal CPM suivante :  $x_i(t) = \sum_n \alpha_{0,n} C_0(t - nT)$ , où  $\alpha_{0,n}$  sont appelés les pseudo-symboles appartenant à un ensemble de  $p$  symboles<sup>3</sup> différents des symboles d'origine. Cette approximation a la forme d'une modulation linéaire. La forme d'onde  $C_0(t)$  a cependant un support de durée  $2T$  et ne vérifie pas le critère de Nyquist. De ce fait, le signal échantillonné après filtrage adapté est de la forme :  $\check{y}_n = \alpha_{0,n-1} p^{(-1)} + \alpha_{0,n} p^{(0)} + \alpha_{0,n+1} p^{(1)}$ , où  $p^{(i)}$  est la convolution entre  $C_0(t)$  et son filtre adapté  $C_0(-t)$ , échantillonnée au temps  $t = iT$ . Cette interférence entre symboles est introduite dans la matrice de mélange  $\mathbf{A}$ <sup>4</sup> et le problème

$$\arg \min |\check{\mathbf{y}}_{\mathbf{b}} - \mathbf{A}\mathbf{x}_{\mathbf{b}}|^2, \quad (5.1)$$

ne peut plus être traité au niveau symbole mais par bloc (par trame transmise). Le vecteur d'observation  $\mathbf{y}_{\mathbf{b}}$  contient  $N_s N$  échantillons correspondant au nombre d'échantillons par bloc. Le vecteur  $\mathbf{x}_{\mathbf{b}}$  résulte de la concaténation des  $K$  trames transmises ou pas (celles de chaque utilisateur), conte-

3.  $p$  étant le numérateur de l'indice de modulation de la CPM  $h = k/p$

4.  $\mathbf{A}$  contient à la fois le canal de transmission, l'interférence entre les pseudo-symboles et leur linéarisation

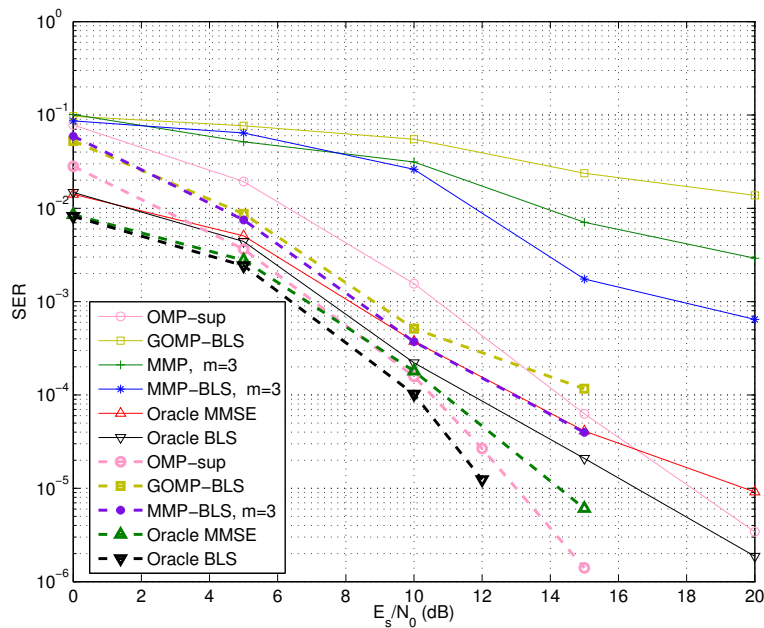


FIGURE 5.11 – Taux d’erreur symbole obtenus avec  $K = 80$  utilisateurs, des trames de  $N = 30$  symboles, un facteur d’étalement  $N_s = 25$  et une probabilité d’activation  $p_a = 5\%$  (donc  $K_a = 4$  utilisateurs actifs) pour une modulation CPM avec  $h = 1/2$  et un pulse fréquentiel rectangulaire d’une durée  $L = 1$  période symbole, appelée MSK (courbes en trait continu). Comparaison dans les mêmes conditions avec la modulation BPSK (courbes en traits pointillés). Extrait de [19]

nant chacune  $N_s N$  échantillons nuls si l’utilisateur n’est pas actif, et non-nuls sinon. Ce vecteur contient donc  $K_a N_s N$  éléments non-nuls répartis dans  $K_a$  blocs non nuls. On parle de parcimonie par bloc [8, 28]. Les algorithmes utilisés pour résoudre le problème 5.1 sont les adaptations à la parcimonie par bloc de ceux utilisés pour la parcimonie par composante. On trouve ainsi par exemple l’algorithme Model-CoSaMP [1], l’algorithme Group-OMP (GOMP) proposé par [8, 4, 24], ou bien l’algorithme Group-LASSO [32] et l’algorithme Group Basis Pursuit [31], et enfin un algorithme où les normes  $\ell_2$  et  $\ell_1$  sont combinées [28]. Cependant, seuls le GOMP dans [4, 24] et l’algorithme OLS par bloc dans [26] ont été appliqués au contexte des communications sporadiques dans des canaux multi-trajets.

La figure 5.11 représente l’estimation de la probabilité d’erreur par symbole obtenus avec de tels algorithmes de traitement par bloc, ou bien des versions améliorées, obtenues avec  $K = 80$  utilisateurs,  $N = 30$  symboles par trames avec un facteur d’étalement  $N_s = 25$  et une probabilité d’activation  $p_a = 5\%$  (donc  $K_a = 4$  utilisateurs actifs) pour une modulation MSK (une CPM avec  $h = 1/2$  et un pulse fréquentiel rectangulaire d’une durée  $L = 1$  période symbole). Différents algorithmes sont utilisés pour résoudre le problème de la détection des utilisateurs actifs et des données transmises, et sont comparés aux courbes génie (*oracles*) qui ont la connaissance parfaite des utilisateurs actifs, mais pas des données transmises [19]. Notamment, les algorithmes OMP / GOMP et MMP [17] (où  $m$  désigne la taille maximale de la liste de candidats) sont utilisés avec une modification permettant d’inclure la connaissance a-priori de l’alphabet des symboles envoyés en utilisant le critère appelé *Bounded Least Square* (BLS). Ces courbes montrent tout d’abord que pour les 2 types de modulation, il est possible d’atteindre des performances entre les deux oracles considérés : l’oracle MMSE (qui

n'a pas la connaissance a-priori de l'alphabet des symboles pour retrouver les données, et qui utilise un critère *minimum mean square error* (MMSE) puis un seuillage pour les estimer) et l'oracle BLS.

### 5.4.3 Conclusions

L'approche de la détection multi-utilisateurs par les outils de traitement de signal parcimonieux offre une possibilité intéressante d'accès multiple non-orthogonal autorisant une augmentation du nombre d'utilisateurs par rapport à un accès orthogonal. Comme cette approche nécessite l'utilisation de modulations linéaires, il n'est pas immédiat de l'appliquer à des modulations non-linéaires telles que les modulations à phase continue dont l'enveloppe constante constitue pourtant un sérieux avantage pour des applications où l'on souhaite déployer des transmetteurs à bas-coût et à très faible consommation. Dans cette partie, j'ai présenté quelques tentatives sur lesquelles nous travaillons actuellement avec Malek Messai, partiellement financées par le projet Fantastic-5G. A partir de la linéarisation de Laurent, le signal CPM peut être exprimé sous la forme d'une modulation linéaire, dont la forme d'onde ne respecte pas le critère de Nyquist, et dont les symboles (appelés pseudo-symboles) sont dépendants. Le traitement parcimonieux par bloc permet de résoudre le problème de la corrélation et de l'interférence entre les symboles, mais doit être associé à une expression judicieuse des pseudo-symboles. Enfin, les algorithmes de traitement parcimonieux de l'état de l'art doivent être améliorés afin d'offrir des taux d'erreur symboles acceptables en prenant en compte par exemple l'information a-priori de la constellation des pseudo-symboles. Tous ces efforts permettent d'obtenir des taux d'erreurs symboles très corrects par rapport à l'état de l'art.

Cependant, les problèmes à résoudre sont encore nombreux : la mise à l'échelle est quasiment impossible sur des algorithmes comme la famille des Group-LASSO, et délicate sur des algorithmes de type GOMP. Seuls les algorithmes à détection de supports basés sur l'OMP peuvent le permettre. L'utilisation de codes d'étalement à l'émetteur n'est pas non plus très réaliste car de nombreuses applications existantes n'en sont pas pourvu. Enfin, l'estimation du canal de transmission est sans doute le point le plus difficile à résoudre pour les applications avec émetteurs mobiles (incompatible avec l'aspect sporadique des transmissions, pas forcément de voie retour). Pour des applications avec émetteurs fixes, le modèle de propagation à évanouissements rapides n'est plus adapté et dans ce cas, la condition de rang plein sur la sous-matrice associée aux utilisateurs actifs n'est plus vérifiée.

Je souhaite poursuivre ce travail après la fin du post-doc de Malek Messai par le démarrage d'une collaboration entre notre équipe et Tarik Benaddi, maître de conférences à Télécom Bretagne, qui vient d'intégrer l'équipe COM du Lab-STICC par la soumission d'un projet aux appels à idée "Recherche et Technologie" CNES puis auprès de l'ANR.

## 5.5 Conclusion

Mes perspectives de recherche s'inscrivent dans la continuité de mes travaux menés jusqu'à ce jour, concentrés autour d'une expertise sur le codage correcteur d'erreur d'une part, et d'autre part sur la conception orientée système des chaînes de communication. Je souhaite plus particulièrement développer ma recherche sur le thème des communications numériques à trames courtes. Cette contrainte apporte un grand nombre de défis de conception au niveau de la couche physique, notamment en ce qui concerne le codage correcteur d'erreurs, la synchronisation, l'égalisation, les mécanismes de

détection d'erreurs et de retransmissions, la réduction de la taille de l'en-tête de la trame et ses conséquences au niveau de la couche d'accès et notamment de la gestion de l'accès multiple. Dans ce chapitre, j'ai illustré deux défis plus en détails.

J'ai tout d'abord présenté une technique de mise en forme des symboles de transmission afin de compléter le gain de codage limité par la taille du code par un gain dit de mise en forme. Cette technique utilise les principes du codage de source pour modifier la distribution de probabilité des symboles envoyés. J'ai utilisé le codage de source entropique qui offre de bonnes performances de rendement mais dont la longueur variable est pénalisante en cas d'erreur de transmission. Une autre technique proposée par Böcherer et al. [2], permettant d'une part un codage à longueur fixe et d'autre part de laisser le codage correcteur d'erreur un position interne par rapport à la mise en forme, offre de très bonnes performances pour des longueurs importantes de codes. Lors de mon séjour d'études au LNT de la Technische Universität de Munich, je vais étudier ce schéma dans le cas des longueurs plus courtes. Avec la thèse d'Alex The Phuong Nguyen, qui va commencer début novembre 2016 et que je vais co-encadrer avec Raphaël Le Bidan, nous allons poursuivre ce travail sur le codage correcteur d'erreurs commencé avec le contrat de recherche Huawei sur les codes courts LDPC non-binaires, puis nous étudierons l'association codage-décodage-détection d'erreurs dans les mécanismes de retransmission hybrides (HARQ); la troisième partie sera consacrée aux canaux à évanouissements.

Le deuxième point que j'ai souhaité développé plus en détail concerne la gestion de l'accès multiple dans le cas où les trames courtes sont utilisées lors de transmissions sporadiques par un grand nombre d'émetteurs. Les outils du traitement du signal parcimonieux permettent de résoudre les problèmes d'interférences entre utilisateurs dans le cas où les modulations sont linéaires. Dans le cas des modulations à phase continue (CPM) qui sont des modulations non-linéaires, le problème est plus délicat. Si la linéarisation de la modulation CPM permet de traiter le problème avec de la parcimonie par bloc, c'est au prix de nombreuses hypothèses qu'il faudra lever : en cas de mobilité, une technique d'estimation du canal doit être proposée; en cas d'absence de mobilité, le traitement parcimonieux sera beaucoup moins performant en raison de la dépendance de la matrice du canal des utilisateurs actifs. Dans ces deux cas, il faut trouver une solution si l'on souhaite appliquer ces traitements dans les applications naissantes des communications entre machines.

Les communications à trames courtes constituent à mon sens un thème de recherche à fort potentiel académique et industriel, pour toutes les remises en cause apportées aux méthodes actuelles de conception de la couche physique. Ce nouveau paradigme de conception doit pouvoir s'accompagner de nouveaux outils théoriques qui manquent actuellement pour les communications à trames courtes, à l'exception des performances du codage à dimension finie de Polyanskiy, Poor et Verdu [22]. Il faudra donc mener conjointement des travaux de recherche liés aux schémas d'émission-réception, sans perdre de vue l'aspect système, et des travaux d'analyse théorique et de recherche d'outils d'aide à la conception : cette dimension reste la plus ambitieuse mais au cœur des préoccupations de l'enseignant-chercheur en communications numériques.

## 5.6 Bibliographie

- [1] R.G. Baraniuk, V. Cevher, M.F. Duarte, and C. Hegde. Model-based compressive sensing. *IEEE Transactions on Information Theory*, 56(4):1982–2001, April 2010.

- [2] G. Böcherer, F. Steiner, and P. Schulte. Bandwidth efficient and rate-matched low-density parity-check coded modulation. *IEEE Transactions on Communications*, 63(12):4651–4665, Dec 2015.
- [3] Georg Böcherer. *Capacity-Achieving Probabilistic Shaping for Noisy and Noiseless Channels*. PhD thesis, Fakultät für Elektrotechnik und Informationstechnik der Rheinisch-Westfälischen Technischen Hochschule Aachen, february 2012. available on <http://www.georg-boecherer.de/capacityAchievingShaping.pdf>.
- [4] C. Bockelmann, H. Schepker, and A. Dekorsy. Compressive sensing based multi-user detection for machine-to-machine communication. *Transactions on Emerging Telecommunications Technologies : Special Issue on Machine-to-Machine : An emerging communication paradigm*, 24(4):389–400, June 2013.
- [5] E.J. Candes and T. Tao. Near-optimal signal recovery from random projections : Universal encoding strategies?. *IEEE Transactions on Information Theory*, 52(12):5406–5425, December 2006.
- [6] Emmanuel J. Candes, Justin K. Romberg, and Terence Tao. Stable signal recovery from incomplete and inaccurate measurements. *Communications on Pure and Applied Mathematics*, 59(8):1207–1223, 2006.
- [7] Sophy Caulier and Didier Généau. Les réseaux pour objets connectés : la nouvelle guerre de l’internet. *Le Monde Economie*, 28 Août 2016. consultable en ligne sur [http://www.lemonde.fr/economie/article/2016/08/28/la-nouvelle-guerre-de-l-internet\\_4988974\\_3234.html](http://www.lemonde.fr/economie/article/2016/08/28/la-nouvelle-guerre-de-l-internet_4988974_3234.html).
- [8] Y.C. Eldar, P. Kuppinger, and H. Bolcskei. Block-sparse signals : Uncertainty relations and efficient recovery. *IEEE Transactions on Signal Processing*, 58(6), June 2010.
- [9] T. Erseghe. On the evaluation of the polyanskiy-poor-verdú converse bound for finite block-length coding in awgn. *IEEE Transactions on Information Theory*, 61(12):6578–6590, Dec 2015.
- [10] Tomaso Erseghe. Coding in the finite-blocklength regime : Bounds based on laplace integrals and their asymptotic approximations. *CoRR*, abs/1511.04629, 2015.
- [11] R.F.H. Fischer. *Precoding and Signal Shaping for Digital Transmission*. Wiley, 2005.
- [12] G. D. Forney and G. Ungerboeck. Modulation and coding for linear gaussian channels. *IEEE Transactions on Information Theory*, 44(6):2384–2415, Oct 1998.
- [13] G. D. Forney and L. F. Wei. Multidimensional constellations. i. introduction, figures of merit, and generalized cross constellations. *IEEE Journal on Selected Areas in Communications*, 7(6):877–892, Aug 1989.
- [14] GrDF. Gazpar : le compteur communicant. <http://www.grdf.fr/dossiers/gazpar-le-compteur-communicant>. consulté le 19 septembre 2016.
- [15] Martin Koppe. Les défis de l’internet des objets. *CNRS Le Journal*, 27 sept. 2016. consultable en ligne sur <https://lejournal.cnrs.fr/articles/les-defis-de-linternet-des-objets>.



- [16] F. R. Kschischang and S. Pasupathy. Optimal nonuniform signaling for gaussian channels. *IEEE Transactions on Information Theory*, 39(3):913–929, May 1993.
- [17] S. Kwon, J. Wang, and B. Shim. Multipath matching pursuit. *IEEE Transactions on Information Theory*, 60(5):2986–3001, May 2014.
- [18] P. A. Laurent. Exact and approximate construction of digital phase modulations by superposition of amplitude modulated pulses (AMP). *IEEE Trans. Commun.*, 34:150–160, February 1986.
- [19] Malek Messai, Frédéric Guilloud, Karine Amis, and Abdeldjalil Aïssa El Bey. Reconstruction of a finite alphabet block-sparse signal via support detection. under preparation for submission to IEEE Transaction on Communications, Dec. 2017.
- [20] F. Monsees, C. Bockelmann, D. Wubben, and A. Dekorsy. Sparsity aware multiuser detection for machine to machine communication. In *Globecom Workshops (GC Wkshps), 2012 IEEE*, pages 1706–1711, December 2012.
- [21] Minh On Vu Ngoc. Probabilistic huffman shaping for pam modulations. Technical report, Telecom Bretagne, 2015.
- [22] Y. Polyanskiy, H. V. Poor, and S. Verdú. Channel coding rate in the finite blocklength regime. *IEEE Transactions on Information Theory*, 56(5):2307–2359, May 2010.
- [23] B. E. Rimoldi. A decomposition approach to CPM. *IEEE Trans. Inform. Theory*, 34:260–270, March 1988.
- [24] H.F. Schepker, C. Bockelmann, and A. Dekorsy. Efficient detectors for joint compressed sensing detection and channel decoding. *Communications, IEEE Transactions on*, 63(6):2249–2260, June 2015.
- [25] H.F. Schepker and A. Dekorsy. Sparse multi-user detection for cdma transmission using greedy algorithms. In *Wireless Communication Systems (ISWCS), 2011 8th International Symposium on*, pages 291–295, November 2011.
- [26] H.F. Schepker and A. Dekorsy. Compressive sensing multi-user detection with block-wise orthogonal least squares. In *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*, pages 1–5, May 2012.
- [27] P. Schulte and G. Böcherer. Constant composition distribution matching. *IEEE Transactions on Information Theory*, 62(1):430–434, Jan 2016.
- [28] M. Stojnic, F. Parvaresh, and B. Hassibi. On the reconstruction of block-sparse signals with an optimal number of measurements. *IEEE Transactions on Signal Processing*, 57(8):3075–3085, August 2009.
- [29] J. A. Tropp and A. C. Gilbert. Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Transactions on Information Theory*, 53(12):4655–4666, December 2007.
- [30] G. Ungerboeck. *Huffman Shaping*. pages 299–313. Springer US, Boston, MA, 2002.
- [31] Ewout van den Berg and Michael P. Friedlander. Probing the pareto frontier for basis pursuit solutions, 2008.
- [32] Ming Yuan and Yi Lin. Model selection and estimation in regression with grouped variables. *JOURNAL OF THE ROYAL STATISTICAL SOCIETY, SERIES B*, 68:49–67, 2006.

- 
- [33] Hao Zhu and G.B. Giannakis. Exploiting sparse user activity in multiuser detection. *IEEE Transactions on Communication*, 59(2):454–465, February 2011.
- [34] Amin Zribi, Ramesh Pyndiah, Sonia Zaibi, Ammar Bouallegue, and Frédéric Guilloud. Low-Complexity Soft Decoding of Huffman Codes and Iterative Joint Source Channel Decoding. *IEEE transactions on communications*, 60(6):1669 – 1680, June 2012.



## Conclusions

Le codage correcteur d'erreurs permet de transmettre à des rapports entre puissance du signal et puissance de bruit plus faibles. Ainsi, il est possible d'augmenter les débits transmis (c'est alors la puissance de bruit qui augmente) ou de baisser la puissance du signal émis pour diminuer la consommation énergétique des émetteurs. Le codage correcteur d'erreurs a connu des avancées majeures depuis l'invention des turbocodes par C. Berrou, A. Glavieux et P. Thitimajshima en 1993, des turbocodes en blocs par R. Pyndiah et al. en 1994, puis la redécouverte des codes de parité à faible densité (LDPC) de R. Gallager (1963) par D. MacKay et R. Neal en 1995. Ces découvertes ont non seulement insufflé en effort de recherche considérable dans le domaine du codage correcteur d'erreurs, mais leurs implémentations dans les standards de télécommunications sans fil ont également permis d'augmenter considérablement les débits offerts aux clients des opérateurs et ont ouvert la voie de la révolution numérique que notre société vit actuellement.

Ces améliorations de performances ont été obtenues par l'augmentation de la longueur des codes. Cependant, les études des scénarios envisagés pour la cinquième génération de téléphonie mobile mettent en évidence de nouvelles applications relatives à l'internet des objets, aux réseaux de capteurs sans fil ou aux communications entre machines. Dans ces applications, on a souvent besoin de transmettre des trames de courte durée, contenant un faible nombre de bits codés. Il faut donc améliorer les performances de la transmission par d'autres moyens que celui de l'augmentation de la longueur du code. Ce constat a donné naissance à la thématique de recherche que je souhaite développer dans les années à venir et que j'ai intitulée :

### *Communications numériques à trames courtes*

L'amélioration des performances des systèmes de transmissions à trames courtes passe par une reconsidération de tous les traitements effectués au niveau de la couche physique et de leurs interactions avec la couche d'accès, comme synthétisé sur la figure 5.12. De façon directe, la réduction de la longueur du code impose une limite sur la capacité de correction. Pour compenser cela, on peut agir au niveau du code directement et aller chercher les meilleures performances que l'on puisse obtenir pour une longueur donnée, ce qu'on est encore loin d'atteindre avec les codes binaires usuels. Les codes LDPC non-binaires permettent par exemple de se rapprocher des performances optimales à longueur fixée, sans aboutir à une complexité de décodage insurmontable étant donnée la taille réduite du code. D'autres codes tels que les turbocodes ou les codes polaires (associés à un CRC) peuvent également offrir des solutions pertinentes. Ces solutions peuvent également être complétées par une mise en forme probabiliste des symboles envoyés afin de profiter d'un gain de mise en forme cumulable avec le gain de codage.

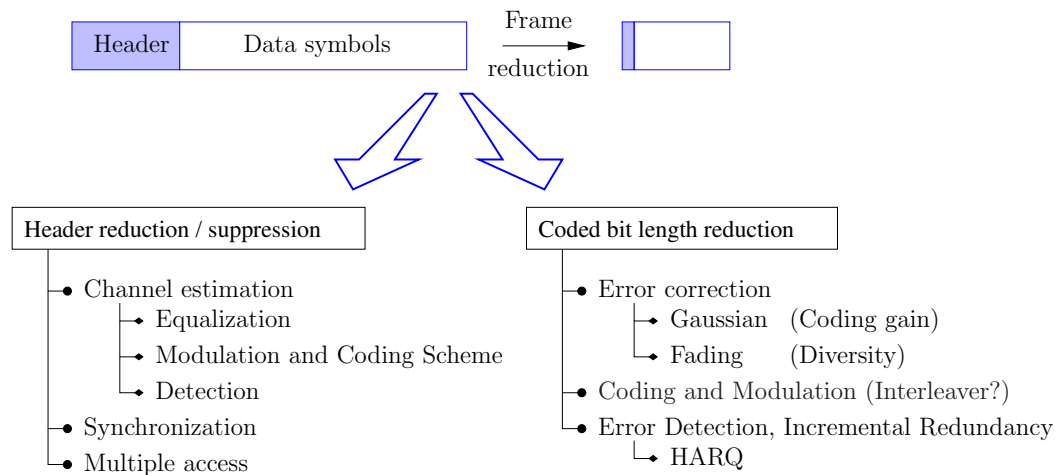


FIGURE 5.12 – Les conséquences de la réduction de la taille des trames

Mais l'utilisation de nouveaux codes correcteurs d'erreurs n'est pas le seul levier. L'association du codage et de la modulation est également remise en question : le schéma pragmatique de type BICM (*Bit Interleaved Coded Modulation*) risque de ne plus être intéressant. Avec des longueurs codées égales à la taille de la trame, l'entrelacement n'a plus beaucoup de sens. Un retour vers des schémas de type modulation codée pourrait être pertinent pour des canaux gaussiens. Sur des canaux à évanouissements, l'augmentation de la diversité sera également limitée par la taille du code. Des solutions à base de réseaux de points pourraient permettre d'obtenir des diversités importantes.

L'ajout d'un code externe détecteur d'erreurs de type CRC (*Cyclic Redundancy Check*) réduit encore plus la longueur du code correcteur d'erreurs à taille de trame fixée. Une solution envisageable pourrait être la fusion du codage correcteur et détecteur d'erreurs avec des enjeux en termes de construction du code et d'algorithmes de détection / décodage. Enfin, la compatibilité en rendement sur des codes de petites longueurs (poinçonnage, extension) reste également ouvert pour mettre en oeuvre des communications avec voie de retour, acquittement et retransmission de type HARQ (*Hybrid Automatic Repeat reQuest*).

La trame est également constituée d'un préambule (en-tête) et parfois d'un post-ambule. L'en-tête comporte notamment des symboles connus permettant de synchroniser, d'estimer le canal, ou des symboles de données portant sur la description de la modulation et du codage utilisé (MCS) ou bien de gérer les accès multiples aux ressources radio communes à plusieurs utilisateurs. Si la même taille d'en-tête est conservée pour des trames plus courtes, l'efficacité spectrale risque d'être fortement affectée. Il faut donc réfléchir à la façon de répondre alternativement aux fonctions portées par l'en-tête. Notamment, une alternative au changement de MCS pour faire varier l'efficacité spectrale pourrait consister à adopter également une mise en forme probabiliste afin de limiter le nombre de paramètres flexibles et la complexité de l'émetteur. De plus, l'accès multiple peut être par exemple résolu au niveau du récepteur où un détecteur multi-utilisateur basé sur l'échantillonnage parcimonieux est utilisé comme par exemple dans les transmissions sporadiques. Cependant, dans ce cas il faut résoudre le problème de l'estimation de canal qui reste un point bloquant dans de nombreuses évolutions proposées dans la 5G.

Pour cette thématique de recherche que je souhaite développer, les actions à court terme confirmées ou à déposer sont résumées dans la figure 5.13. En rouge sont représentées celles liées aux

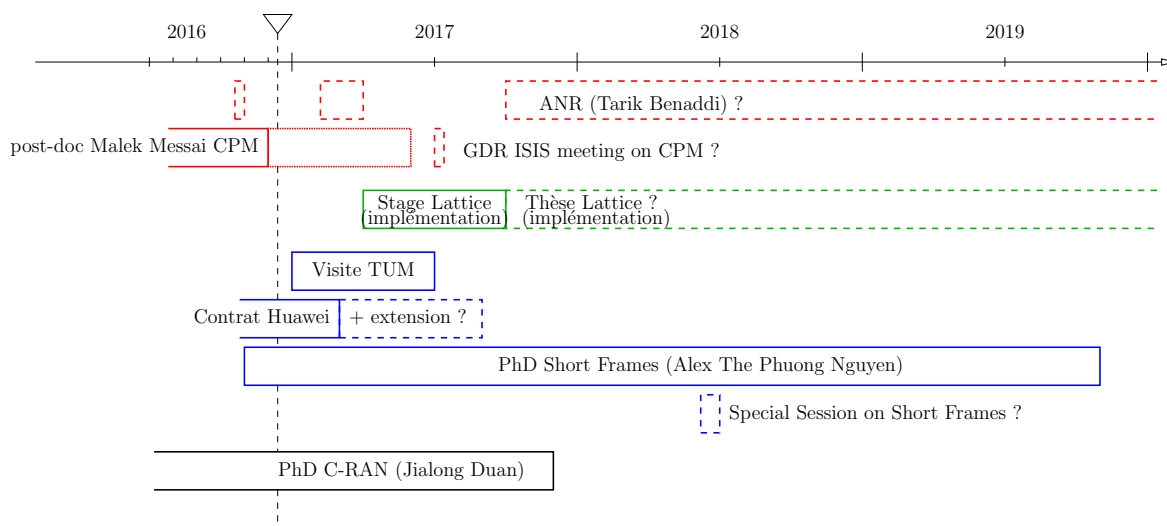


FIGURE 5.13 – Actions confirmées (en trait continu) ou envisagées (en traits pointillés) à court terme sur la thématique des modulation à phase continue (rouge) ou des trames courtes (bleu).

modulations à phase continue (CPM) et en bleu sont représentées celles liées aux communications à trame courte. En trait continu, je représente les actions confirmées et en traits pointillés, je représente les actions à concrétiser. J'ai également fait apparaître le co-encadrement de la thèse de Jialong Duan, dirigée par Xavier Lagrange au département RSM, portant sur le CRAN (*Cloud Radio Access Network*), et qui, sans être au cœur de mes perspectives, constitue un volet supplémentaire de mon activité de recherche. Concernant la thématique CPM, je vais soutenir Tarik Benaddi, enseignant-chercheur à Télécom Bretagne impliquée dans notre équipe de recherche (équipe LABSTICC/CACS/COM), à déposer une demande de financement ANR jeune chercheur sur la thématique des détection CPM utilisant l'échantillonnage compressé, afin de financer une thèse qui pourrait démarrer en octobre 2017. Tarik Benaddi a soutenu ses travaux de thèse récemment sur la CPM dans un contexte de mesure et de surveillance spatiale pour le compte du CNES : cela permettra de soutenir l'effort de recherche que nous avons initié au sein de l'équipe dans ce contexte. Je souhaiterais également construire une rencontre autour de la modulation CPM dans le cadre des journées du GDR ISIS, probablement au début du mois de juillet 2017. Cette journée permettrait de faire le point sur les applications émergentes de la modulation CPM (accès radio des applications de l'internet des objets) et de réunir les principaux contributeurs de France et éventuellement d'Europe. Enfin, les résultats du travail de Malek Messai vont être présentés au sein du projet Fantastic-5G avant sa clôture prévue en Juin 2017.

Concernant la thématique des trames courtes, la thèse d'Alex The Phuong Nguyen va démarrer le 2 novembre 2016, financée par PRACOM<sup>5</sup> (Pôle de Recherche Avancée en Communications). Mon séjour sabbatique à la Technische Universität de Munich (TUM), au sein du laboratoire LNT dirigé par le professeur Gerhard Kramer, s'inscrit également dans cette thématique. J'ai prévu d'y étudier plus particulièrement les techniques de mise en forme probabiliste. Enfin, nous espérons pouvoir étendre notre contrat de recherche bilatéral avec Huawei FRC (France Research Center) portant sur le codage correcteur à longueur courte. Je pense qu'il sera pertinent d'organiser un workshop sur les communications à trames courtes au milieu de l'année 2018 afin de promouvoir le travail de

5. <http://recherche.telecom-bretagne.eu/pracom/>

thèse d'Alex The Phuong Nguyen et de susciter l'intérêt de la communauté scientifique sur cette thématique.

Ces 2 thématiques n'étant pas exclusives, il faudra sans aucun doute envisager la pertinence des modulations CPM dans l'étude des transmissions à trames courtes. Il sera également indispensable de travailler sur les outils théoriques permettant d'apporter des règles de conception et d'étude de performance. Cela constitue un enjeu important car ce sont souvent des considérations asymptotiques qui ont permis d'établir les principaux résultats de la théorie de l'information.

## **Quatrième partie**

### **Annexe**





## Annexe A

# Détails des activités de recherche

### A.1 Activité contractuelle

Dans cette section sont listés les contrats de recherche auxquels j'ai pu participé durant les 10 dernières années. Les allocations de thèse n'apparaissent pas dans cette liste. Pour chacun de ces projets, j'indique les budgets selon la règle suivante :

budget que j'ai perçu	budget perçu par Télécom Bretagne	budget total du projet
-----------------------	-----------------------------------	------------------------

— **Turboconcept (sous-traitance pour le CNES) : Raptor**

- Titre : Protection des fichiers et codes Raptor
- Date : sept. 2006 - dec. 2006
- Implication : Correspondant Télécom Bretagne
- Budget : 

20 k€	20 k€	20 k€
-------	-------	-------
- Partenaire : CNES, Turboconcept
- Description / contributions : Bibliographie sur les codes Raptor et leur alternative proposée par l'INRIA, et développement d'un simulateur pour l'évaluation et la comparaison des performances des deux familles de codes quant à la protection des transmissions sur un canal à effacement.

— **CRE France Télécom**

- Titre : Etude du décodage à entrées et sorties pondérées des codes Reed-Solomon et applications
- Date : Juillet 2004 - Juillet 2007
- Implication : Participant
- Budget : 

0 k€	165 k€	165 k€
------	--------	--------
- Description : L'objectif de ce projet était de proposer et d'évaluer de nouveaux schémas de codage de canal utilisant les codes de Reed-Solomon, et notamment leur décodage à entrée souple.
- Contribution : Rédaction de la proposition, décodage souple des codes Reed-Solomon de grande longueur basé sur la génération a-priori de vecteurs de tests utilisés dans l'algorithme Chase-Pyndiah.

— **ESA : BSDT**

- Titre : Study of enhanced digital transmission techniques for broadband satellite digital transmissions
- Date : dec. 2005 - fev. 2008
- Implication : Participant
- Budget : 

15 k€	83 k€	400 k€
-------	-------	--------
- Partenaires : NEWTEC (Belgique), Université de Parme (Italie), Université de Bologne (Italie)
- Description : Le but de ce projet était de proposer et comparer des solutions alternatives aux standards DVB-S2 et DVB-RCS, basées sur des modulations à phase continue (CPM).
- Contribution : participation à la rédaction de la proposition, étude de la concaténation LDPC et modulation CPM.

— **FUI : DISTRIMAGES**

- Titre : Conception et développement d'une plate-forme prototype de distribution de contenus audiovisuels et interactifs
- Date : dec. 2005 - fev. 2008
- Implication : Participant
- Budget : 

75.5 k€	75.5 k€	10000 k€
---------	---------	----------
- Partenaires : Thomson, France Télécom, Grass Valley, TDF, Enensys Technologies, Niji, QoSmetrics et Sacet.
- Description : Ce projet avait pour objectif la conception et le développement d'une plate-forme prototype de distribution de contenus audiovisuels interactifs et d'un démonstrateur à des fins de préparation de recommandations et de spécifications en partant de la phase 1 du standard DVB IP (ETSI TS 102.034 v1.1.1) puis en étudiant l'évolution de ce standard (phase 2) en augmentant le nombre de services offerts.
- Contribution : Décodage itératif (erreurs / effacements) entre le codage canal (Reed-Solomon) et le codage dit COP#3 (code of practice number 3) consistant en une concaténation lignes-colonnes de codes de parités sur les paquets effacés. Ce travail a nécessité la modélisation de l'entrelacement entre la couche physique et la couche applicative.

— **GET incitatif : ForWin**

- Titre : Fountain Code-based Reliable Transport in Wireless Networks
- Date : janv. 2008 - déc. 2008
- Implication : Participant
- Budget : 

16 k€	16 k€	34 k€
-------	-------	-------
- Partenaires : Télécom Sud-Paris, INRIA
- Description / Contribution : La performance des transferts de données sur réseaux TCP, FTP, subit une dégradation importante dans les réseaux sans fil et ce pour plusieurs raisons. Par exemple, dans les réseaux sans fil basés sur la norme IEEE802.11, la dégradation provient du fait que les liens sont semi-duplex : les paquets de TCP allant dans un sens entrent en collision avec les acquittements allant dans l'autre sens. Cette collision est encore plus élevée quand le trafic est bi-directionnel. Dans les réseaux 3G, l'asymétrie entre les liens HSDPA montants et descendants peut potentiellement limiter les performances

de bout-en-bout de TCP à cause des acquittements transportés par le lien montant. La solution ? Supprimer les acquittements et utiliser le codage pour un transport fiable en boucle ouverte, ce que peuvent fournir par exemple les codes fontaines. L'objectif de ce projet fut de définir, optimiser et implémenter un nouveau protocole de transport fiable en boucle ouverte basé sur les codes fontaines.

— **CNES : PHY4HD**

— Titre : Etude métier méthode d'accès Half-duplex

— Date : sept. 2009 - fev. 2010

— Implication : Responsable

— Budget : 

31.6 k€	31.6 k€	31.6 k€
---------	---------	---------

— Description : Le contexte de ce projet était celui des communication satellitaires mobiles, pour lesquelles le coût du terminal peut être réduit en supprimant le duplexeur. L'accès à la ressource (couche MAC) est alors plus complexe : l'enjeu est de faire passer des télécommunications « full-duplex » dans un mode « half-duplex ». Autrement dit, dans le cadre d'une télécommunication asymétrique, faut-il sacrifier la capacité du segment satellite - terminal et ne perdre aucune donnée ou bien faut-il maintenir la transmission descendante de données pendant la communication montante, quitte à perdre des données transmises ? Ou bien un compromis existe-t-il (codage / entrelacement) ?

— Contribution : elle a porté sur 2 axes. Le premier concernait l'étude de l'entrelacement et du codage pour lutter contre les perturbations induites par les commutations entre les modes transmission et réception. Le deuxième axe concernait l'étude d'algorithmes de synchronisation rapide nécessaire après des évanouissements forts du signal reçu.

— **GrDF : AMR GrDF**

— Titre : Télé-relevage de compteur de Gaz automatique (Automatic Meter Reading)

— Date : mars 2011 - aout 2011

— Implication : Responsable

— Budget : 

13 k€	13 k€	13 k€
-------	-------	-------

— Description / Contribution : Le contexte de cette étude a été la phase initiale du projet de déploiement des compteurs de gaz intelligents chez GrDF. Elle a porté plus précisément sur 2 points : la mise en évidence de l'intérêt du codage correcteur d'erreur pour la transmission sans fil du compteur vers le concentrateur et l'étude théorique des probabilités de collision des trames envoyées en fonction de leur durée, du nombre de compteurs, sous l'hypothèse d'un accès aléatoire au média (couche MAC de type ALOHA).

— **CLS (sous-traitance pour le CNES) : SATAIS**

— Titre : Étude d'un algorithme de réception des messages AIS à l'aide de modèles prédictifs

— Date : fév. 2012 - mars 2013

— Implication : Responsable

— Budget : 

85.3 k€	85.3 k€	85.3 k€
---------	---------	---------

— Partenaire : CNES, CLS (Toulouse)

— Description : Les signaux AIS échangés entre les bateaux permettent d'obtenir des informations relatives à leur identité, leur vitesse, leur cap, leur destination etc ... Pour collecter ces informations, des stations terrestres sont réparties sur le littoral mais elles ne peuvent

collecter les informations des bateaux qui sont au milieu des océans. De petits satellites défilant en orbite basse sont alors utilisés pour intercepter ces signaux. Le problème est que le rapport signal à bruit est très faible, et que la vitesse de défilement du satellite crée un fort Doppler.

- Contributions : Développement d’algorithmes de réceptions cohérentes des signaux CPM et utilisation d’informations a-priori pour améliorer la détection de messages AIS. Application aux signaux réels.
- **EMC Norway : Contrat d’étude**
  - Titre : Proposition et intégration de codes fontaines pour les communications satellitaires DVB
  - Date : fev. 2014 - janv. 2015
  - Implication : participant
  - Budget : 

12.5 k€	30 k€	30 k€
---------	-------	-------
  - Description : Le standard DVB-H propose l’utilisation de codes Raptor pour la diffusion de contenu. Cette étude a porté sur l’état de l’art des codes fontaines, et la proposition de nouveaux schémas de codage adaptés à l’effacement, pour des paquets de grande taille, ainsi que leur implémentation sur FPGA.
  - Contribution : encadrement d’Amine Semma sur les parties codes fontaines / Raptor, et pour sa proposition de codage par effacement inspirée par les codes Reed-Solomon.
- **FUI : GreenCom**
  - Titre : Gestion Raisonnée et Efficace en Energie des noeuds de communication pour la maison Multimedia
  - Date : avril 2013 - avril 2016
  - Implication : participant
  - Budget : 

68.5 k€	581.8 k€	1700 k€
---------	----------	---------
  - Partenaires : Orange, Technicolor Niji, Turboconcept, Siradel, Idil, Satimo
  - Description : L’objectif de ce projet est l’amélioration de l’efficacité énergétique des technologies de connectivité du Réseau Local Domestique, d’une part en minimisant la consommation active des technologies WiFi, PLC, Optique, et d’autre part en étudiant l’exposition des usagers aux ondes électromagnétiques puis en minimisant les rayonnements.
  - Contribution : Etude qualitative de l’impact de la prise en compte d’une puissance circuit sur le rendement maximal d’un système de transmission pour une consommation totale de puissance contrainte, ainsi que sur le problème de réduction de la puissance totale pour une performance cible donnée.
- **Projet européen 7eme PCRD : METIS**
  - Titre : Mobile communications Enablers for Twenty-twenty (2020) Information Society
  - Date : novembre 2012 - avril 2015
  - Implication : Correspondant Télécom Bretagne
  - Budget : 

251.5 k€	578.1 k€	16000 k€
----------	----------	----------
  - Partenaires : Ericsson (Suède), Aalborg University (Danemark), Aalto-University (Finlande), Alcatel Lucent (Allemagne), BMW Forschung und Technik GmbH (Allemagne),

Chalmers Tekniska Hoegskola AB (Suède), Deutsche Telekom (Allemagne), DOCOMO Euro-Labs (Allemagne), NTT Docomo (Japon), Anite (Finlande), France Télécom SA (France), Fraunhofer Institut (Allemagne), Huawei (Allemagne), KTH (Suède), National and Kapodistrian University of Athens (Grèce), NOKIA (Finlande), Nokia Solutions & Networks (Finlande, Allemagne & Pologne), Oulun Yliopisto (Finlande), Poznan University of Technology (Pologne), Rheinisch-Westfaelische Technische Hochschule Aachen (Allemagne), Telecom Italia S.p.A (Italie), Telefonica SA (Espagne), Universitaet Bremen (Allemagne), Technische Universitaet Kaiserslautern (Allemagne), Universidad Politecnica de Valencia (Espagne)

- Description : le projet METIS a été co-financé par la communauté européenne en tant que projet intégré du 7ème PCRD. Il a permis de conduire à un consensus européen sur les questions liées au développement du futur réseau de communications mobiles, et ainsi de baliser le chemin jusqu'à une future standardisation de la 5G.
- Contribution : correspondant et coordonnateur du projet pour Télécom Bretagne. Etude de méthodes d'estimation de taux d'erreurs rapide, étude et mise oeuvre de schémas de codage à base de réseaux de points (*Lattice codes*).

— **Projet européen H2020 : FANTASTIC-5G**

- Titre : Flexible Air iNTERfAce for Scalable service delivery wiThIn wIreless Communication networks of the 5th Generation
- Date : juillet 2015 - juin 2017
- Implication : participant
- Budget : 

25 k€	480 k€	8000 k€
-------	--------	---------
- Partenaires : Aalborg University (Danemark), Alcatel-Lucent AG (Allemagne), CEA-LETI (France), CTTC (Espagne), Fraunhofer HHI (Allemagne), Huawei ERC (Allemagne), Intel Deutschland GmbH (Allemagne), Nokia Solution and Networks (Allemagne, Finlande, Danemark), Orange SA (France), Politecnico di Bari (Italie), Samsung Electronics UK (Grande Bretagne), Sequans Communications (France), Telecom Italia S.p.A. (Italie), University of Bremen (Allemagne), WINGS ICT Solutions (Grèce),
- Description : L'objectif de ce projet est de poursuivre le développement d'une interface air multi-service dessinée dans le projet METIS, pour les fréquences inférieures à 6 GHz.
- Contribution : Nous allons nous intéresser dans ce projet à l'adaptation des modulations à phase continue aux schémas des communications sporadiques entre un grand nombre de machines.

— **Huawei : LowLat**

- Titre : Short-length error-correcting codes for low-latency / high-reliability communications
- Date : fév. 2016 - fév. 2017
- Implication : Responsable
- Budget : 

150 k€	150 k€	150 k€
--------	--------	--------
- Description : L'utilisation de trames courtes est de plus en plus envisagée pour les usages émergents des communications sans fil, comme les communications entre machines (Machine Type Communications), ou comme les communications dans des canaux fortement

variables dans le temps (ondes millimétriques). Il s'agit dans ce projet de développer de nouveaux schémas de codage / décodage de codes correcteurs d'erreur pour des longueurs limitées à quelques centaines de bits : à ces longueurs, les règles usuelles de conception ne sont plus toutes valables.

## A.2 Encadrement

### A.2.1 Doctorants

#### 1- Andrzej Michal KABAT

Titre : *contribution au codage correcteur d'erreur : décodage pondéré des codes Reed-Solomon et codage distribué pour les communications coopératives sans fil*

Financement : projet Distrimages, fonds propres

Date de soutenance : 23 octobre 2009

Situation actuelle : Ingénieur de recherche LS Telecom

Encadrement : Frédéric Guilloud et R. Pyndiah (Directeur de thèse)

Taux d'encadrement : 50%

Jury :

Emmanuel Boutillon	Président du jury
Muriel Médard	Rapporteur
Jean-Claude Belfiore	Rapporteur
Marie-Hélène Hamon	Examineur
Ramesh Pyndiah	Directeur de Thèse
Frédéric Guilloud	Encadrant
Raphaël Le Bidan	Invité

#### 2- Hyunseuk YOO

Titre : *PAPR reduction in coded-OFDM systems by using multiple candidates and deliberate clipping*

Financement : Fonds propres

Date de soutenance : 3 novembre 2011

Situation actuelle : Ingénieur de recherche Samsung (Corée)

Encadrement : Frédéric Guilloud et R. Pyndiah (Directeur de thèse)

Taux d'encadrement : 75%

Jury :

Jean-Philippe Diguët	Président du jury
Charly Poulliat	Rapporteur
Yves Louët	Rapporteur
Stéphane Azou	Examineur
Ramesh Pyndiah	Directeur de Thèse
Frédéric Guilloud	Encadrant

**3- Sanae EL HASSANI**

Titre : *Optimisation du décodage des codes LDPC non-binaires pour leur implémentation*

Financement : CIFFRE Orange

Date de soutenance : 5 juillet 2011

Situation actuelle : Assistant professeur, ENSA (El Jadida, Maroc)

Encadrement : Pierre Pénard, Marie-Hélène Hamon, Frédéric Guilloud et R. Pyndiah (Directeur de thèse)

Taux d'encadrement : 25%

Jury :

Marie-Laure Boucheret	Président du jury
Jean-Pierre Cances	Rapporteur
Yves Louet	Rapporteur
Marie-Hélène Hamon	Encadrant
Pierre Pénard	Encadrant
Ramesh Pyndiah	Directeur de Thèse
Frédéric Guilloud	Encadrant

**4- Jia DONG**

Titre : *Fast Estimation of Bit Error Rate of any Digital Communication System*

Financement : PRACOM, Région Bretagne

Date de soutenance : 15 avril 2014

Encadrement : Frédéric Guilloud et Samir Saoudi (Directeur de thèse)

Taux d'encadrement : 33%

Jury :

Charles TATKEU	Président du jury
Ghais EL ZEIN	Rapporteur
Jean-Pierre CANCES	Rapporteur
Samir SAOUDI	Directeur de thèse
Frédéric GUILLOUD	encadrant

**5- Malek MESSAI**

Titre : *Application des signaux CPM pour la collecte de données à grande échelle provenant d'émetteurs faible coût*

Financement : Région Bretagne, Fonds propres

Date de soutenance : 20 novembre 2015

Situation actuelle : Post-Doctorant, Télécom Bretagne

Encadrement : Frédéric Guilloud et Karine Amis (Directrice de thèse)

Taux d'encadrement : 50%

Jury :



Gilles Burel	Président du jury
Merouane Debbah	Rapporteur
Philippe Ciblat	Rapporteur
Giulio Colavolpe	Examineur
Jérôme Lebrun	Examineur
Karine Amis	Directrice de thèse
Frédéric GUILLOUD	encadrant
Alain Dominique Thomas	Invité

#### 6- Carole AL BESCHLAWI

Titre : *On lattice coding for point-to-point communications over AWGN and fading channels : design and implementation*

Financement : Projet METIS

Date de soutenance : 15 janvier 2016

Situation actuelle : Post-Doctorant, Orange Labs (Rennes)

Encadrement : Frédéric Guilloud et Ramesh Pyndiah (Directeur de thèse)

Taux d'encadrement : 100%

Jury :

Emmanuel Boutillon	Président du jury
Charly Poulliat	Rapporteur
Jean-Francois Héliard	Rapporteur
Jean-Claude Belfiore	Examineur
Ramesh Pyndiah	Directeur de thèse
Frédéric GUILLOUD	encadrant

#### 7- Jialong DUAN

Titre : *Evolution of the cloud-RAN architecture*

Financement : PRACOM, Région Bretagne

Date de soutenance prévue : automne 2017

Encadrement : Frédéric Guilloud et Xavier Lagrange (Directeur de thèse)

Taux d'encadrement : 33%

#### 8- Yupeng TAI

Titre : *Codes LT pour les transmissions acoustiques sous-marines*

Financement : CSC Chinese scholarship

Date de soutenance prévue : automne 2017

Encadrement : Frédéric Guilloud, Christophe Laot et Raphaël Le Bidan

Taux d'encadrement : 50% entre Nov. 2015 et Oct. 2016

#### 9- Alex The Phuong NGUYEN

Titre : *Communications sans-fils de paquets très courts : nouveaux défis pour la couche physique*

Financement : PRACOM

Date de soutenance prévue : automne 2019

Encadrement : Frédéric Guilloud (Directeur de thèse), Raphaël Le Bidan

Taux d'encadrement : 50%

**10- Mohamed YAOUMI**

Titre : *Rethinking LDPC codes and decoders to minimize decoding energy*

Financement : Projet ANR EF-FECTive (Elsa Dupraz)

Date de soutenance prévue : automne 2020

Encadrement : Frédéric Guilloud (Directeur de thèse), Raphaël Le Bidan

Taux d'encadrement : 33%

## A.2.2 Post-doctorants et ingénieurs de recherche

### 1- Mohamed ET TOLBA

Titre : *Algorithmes de synchronisations optimaux*

Financement : Contrat CNES PHY4HD

Duré : 5 mois à partir de octobre 2009

Encadrement : Frédéric Guilloud

Taux d'encadrement : 100%

### 2- Haïfa FARES

Titre : *Etude qualitative de l'impact de la prise en compte d'une puissance circuit sur le rendement maximal d'un système de transmission pour une consommation totale de puissance contrainte, ainsi que sur le problème de réduction de la puissance totale pour une performance cible donnée.*

Financement : projet GREENCOM

Duré : 12 mois à partir de septembre 2013

Encadrement : Frédéric Guilloud, Raphaël Le Bidan

Taux d'encadrement : 50%

### 3- Vincent HERBERT

Titre : *Mise en oeuvre de réseaux de points pour coder et moduler l'information*

Financement : projet METIS

Duré : 18 mois à partir de septembre 2013

Encadrement : Frédéric Guilloud, Eric Rannou (UBO)

Taux d'encadrement : 100%

### 4- Malek MESSAI

Titre : *Parcimonie et Modulations CPM pour les communications massives entre machines*

Financement : projet FANTASTIC-5G, Fonds propres

Duré : 12 mois à partir de décembre 2015

Encadrement : Frédéric Guilloud, Karine Amis

Taux d'encadrement : 50%

### 5- Zeina MHEICH

Titre : *Short-length error-correcting codes for low-latency / high-reliability communications*

Financement : projet LowLat

Duré : 12 mois à partir de mars 2016

Encadrement : Frédéric Guilloud, Raphaël Le Bidan, Elsa Dupraz

Taux d'encadrement : 33%

## A.2.3 Stagiaires

### 1- Amin ZRIBI

Titre : *Etude de l'influence des cycles sur le décodage des codes LDPC*

Niveau : Master 2 ENIT Tunis

Période : Mars.-Juin 2005

Encadrement : Frédéric Guilloud

Taux d'encadrement : 100%

## 2- Yunseuk YOO

Titre : *Coded OFDM System for Reduction of the Peak-to-Average Power Ration*

Niveau : Master 2, Telecommunications (Chonbuk National University, Corée)

Période : Mars.-Juillet. 2008

Encadrement : Frédéric Guilloud et Ramesh Pyndiah

Taux d'encadrement : 50%

## 3- Nizar TRABELSI

Titre : *Etude des codes Raptor pour la diffusion multimédia 3G et TNT*

Niveau : PFE INSAT Tunis

Période : Sept.-Déc. 2008

Encadrement : Frédéric Guilloud et Alex Graell i Amat

Taux d'encadrement : 50%

## 4- Hayet MSILINI

Titre : *Performance des réseaux de points su canal AWGN*

Niveau : PFE Supcom Tunis

Période : Mai.-Oct. 2011

Encadrement : Frédéric Guilloud

Taux d'encadrement : 100%

## 5- Tarek CHEHADE

Titre : *Démodulation robuste de signaux GFSK*

Niveau : PFE Université Libanaise / Master 2 Université de Bretagne Occidentale

Période : Mars-Juillet 2012

Encadrement : Karine Amis et Frédéric Guilloud

Taux d'encadrement : 50%

## 6- Clément ACQUITTER

Titre : *Décodage correcteur d'erreur et réseaux de points*

Niveau : Master 2 Université de Bretagne Occidentale

Période : Mars-Juillet 2012

Encadrement : Frédéric Guilloud et Eric Rannou

Taux d'encadrement : 50%

## 7- Amine SEMMA

Titre : *Proposition et intégration de codes fontaines pour les communications satellitaires DVB*

Niveau : Master 2 Université de Bretagne Occidentale

Période : Fév.-Juillet 2014

Encadrement : Frédéric Guilloud, Mathieu Arzel, Charlotte Langlais

Taux d'encadrement : 33%

## 8- Mohamed ABDELLI

Titre : *codage correcteur d'erreur pour les communications machine to machine*

Niveau : PFE Supcom Tunis  
Période : Mars.-Juillet 2015  
Encadrement : Frédéric Guilloud et Raphaël Le Bidan  
Taux d'encadrement : 50%

#### 9- Minh ON VU NGOC

Titre : *Probabilistic Huffman Shaping for PAM modulations*  
Niveau : PFE Ho Chi Minh City University of Technology  
Période : Mars.-Sept. 2015  
Encadrement : Frédéric Guilloud  
Taux d'encadrement : 100%

#### 10- Vinh Hoang Son LE

Titre : *Codage polaire de faibles longueurs*  
Niveau : PFE Ho Chi Minh City University of Technology  
Période : Avril.-Sept. 2016  
Encadrement : Frédéric Guilloud et Raphaël Le Bidan  
Taux d'encadrement : 50%

#### 11- Vinh Hoang Son LE

Titre : *Décodage pondéré et implémentation de codes Reed-Muller*  
Niveau : Master 2 en systèmes embarqués et traitement de l'information (SETI), Université Paris Saclay ORSAY  
Période : Avril.-Sept. 2017  
Encadrement : Frédéric Guilloud et Amer Baghdadi  
Taux d'encadrement : 50%

### A.3 Collaborations

#### Coopération avec Fujitsu Laboratories (Japon)

Daï Kimura a passé une année (2004-2005) au département Signal et Communications. Nous avons travaillé ensemble sur les codes LDPC non-binaires [B3,B2,C2,C1].

#### Coopération avec Chonbuk National University (Corée)

Échanges entre les 2 équipes (accueil d'une délégation coréenne, séjour de dix jours d'un doctorant (Andrzej Kabat) dans le cadre du programme d'échange STAR (2006).

#### Coopération avec Université de Bejaia (Algérie)

Entre 2006 et 2010, Mohamed Azni est venu chaque année passer environ 1 mois dans le cadre de son travail de recherche. Nous avons travaillé ensemble sur le codage conjoint source-canal appliqué à la transmission vidéo H.264 [J4].

#### Coopération avec Université Polytechnique de Bobo-Dioulasso (Burkina-Fasso)

Pasteur Poda est chercheur associé au département Signal & Communications de Télécom Bretagne. Lors de ses séjours au département, nous avons collaboré sur les estimations rapides de taux d'erreurs binaires [U2].

#### Coopération avec ENSA de Marrakech, Université Cadi Ayyad (Maroc)

Younes Jabrane est venu passer quelques séjours au département Signal & Communications en

2013, 2014 et 2015. J'ai monté des dossiers de financements Hubert Curien avec Dr Younes Jabrane en 2014 et 2015 sur la réduction de PAPR pour la 5G. Je vais faire une présentation invitée lors de la conférence ACOSIS (<http://www.acosis.org>) qu'ils organisent du 17 au 19 octobre 2016.

#### **Coopération avec ISET-COM, Tunisie)**

Amin Zribi est également chercheur associé au département Signal & Communications. A ce titre, il rend visite au département régulièrement. Nous avons pu ainsi travailler sur des techniques de décodages source-canal conjoint [J8].

#### **Coopération avec le laboratoire SPADICC de l'Université de Parme (Italie)**

Malek Messai est allé faire un séjour d'études de 4 mois à la fin de l'année 2014 chez le professeur Giulio Colavolpe, pour poursuivre ses recherches sur l'utilisation des modulations à phase continue dans le contexte des réseaux de capteurs [J14,J12,J10].

#### **Coopération avec le laboratoire COMELEC de Telecom Paristech (France)**

Carole Al Bechlawi est allée faire un séjour d'études de 1 mois en avril 2015 chez le professeur Jean-Claude Belfiore, pour travailler sur la construction de réseaux de points algébriques imbriqués basés sur les codes Reed-Muller [C17].

#### **Coopération avec Institution of Acoustics, Chinese Academy of Sciences (Chine)**

Suite à une demande de financement auprès du Chinese Scholarship Council, nous accueillons entre novembre 2015 et novembre 2016 le doctorant Yupeng Tai pour un travail sur l'égalisation et le codage fontaine pour les communications acoustiques sous-marines.

#### **Coopération avec le laboratoire LNT de la Technische Universität München, TUM (Allemagne)**

Une demande de partenariat Hubert Curien a été faite en 2015 avec Dr. Georg Böcherer pour travailler sur de nouveaux schémas de mise en forme (*shaping*) des modulations numériques dans le cas des trames courtes. Je vais à présent effectuer un séjour sabbatique de 6 mois entre janvier et juin 2017 dans ce laboratoire dirigé par le professeur Gerhard Kramer.

## **A.4 Publications**

Analyse du facteur d'impact (source : Google Scholar, sept. 2016) :

- Nombre de publications : 36
- H index : 9
- Nombre de citation : 423

#### A.4.1 Articles de revues internationales avec comité de lecture

- [J15] Malek Messai, Abdeldjalil Aïssa-El-Bey, Karine Amis, and **Frédéric Guilloud**. Improved sparse multiuser detection based on modulation-alphabets exploitation. *Digital Signal Processing*, 71(Supplement C):27 – 35, 2017.
- [J14] Malek Messai, Amina Piemontese, Giulio Colavolpe, **Frédéric Guilloud**, and Karine Amis. Binary CPMs with Improved Spectral Efficiency. *IEEE communications letters*, 20(1):85–88, Jan 2016.
- [J13] Malek Messai, Karine Amis, and **Frédéric Guilloud**. On the Optimization of a PSP-based CPM Detection. *IEEE transactions on wireless communications*, 2016. in press; published online 09 Nov 2015.
- [J12] Malek Messai, Colavolpe Giulio, Karine Amis, and **Frédéric Guilloud**. Robust Detection of Binary CPMs With Unknown Modulation Index. *IEEE communications letters*, 19(3):339 – 342, March 2015.
- [J11] Carole Al Bechlawi and **Frédéric Guilloud**. Efficient LLR Estimation for Multistage Decoding. *Electronics letters*, 51(14):1076 – 1078, July 2015.
- [J10] Malek Messai, Giulio Colavolpe, Karine Amis, and **Frédéric Guilloud**. Binary continuous phase modulations robust to a modulation index mismatch. *IEEE Transactions on Communications*, 63(11):4267–4275, Nov 2015.
- [J9] Sanae El Hassani, **Frédéric Guilloud**, Ramesh Pyndiah, Pierre Penard, and Marie-Hélène Hamon. New Optimizations for Layered Non-Binary LDPC Codes Decoding. *International Journal of Applied Research on Information Technology and Computing*, 3(1), May 2012.
- [J8] Amin Zribi, Ramesh Pyndiah, Sonia Zaibi, Ammar Bouallegue, and **Frédéric Guilloud**. Low-Complexity Soft Decoding of Huffman Codes and Iterative Joint Source Channel Decoding. *IEEE transactions on communications*, 60(6):1669 – 1680, June 2012.
- [J7] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. Probability Distribution Analysis of M-QAM Modulated OFDM Symbol and Reconstruction of Distorted Data. *EURASIP journal on advances in signal processing*, october 2011.
- [J6] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. PAPR reduction for LDPC coded OFDM systems using binary masks and optimal LLR estimation. *Signal processing*, 91:2606 – 2614, November 2011.
- [J5] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. Amplitude PDF analysis of OFDM signal using probabilistic PAPR reduction method. *EURASIP journal on wireless communications and networking*, 2011, 2011.
- [J4] Mohamed Azni, Ramesh Pyndiah, Karim Mokrani, and **Frédéric Guilloud**. Joint source and channel coding for real time H.264 coded video transmission using mobile hand-held devices. *IETE journal of research*, 55(4):154 – 161, July 2009.
- [J3] **Frédéric Guilloud**, Emmanuel Boutillon, Jacky Tousch, and Jean-Luc Danger. Generic description and synthesis of LDPC decoders. *IEEE transactions on communications*, 55(11):2084 – 2091, November 2007.

- [J2] Abdeslem Hallou, **Frédéric Guilloud**, and Yann Gauduel. Real-time probing of solvent caging effects during ir electron transfers in solution. *Journal of Molecular Liquids*, 96 – 97:265 – 274, 2002.
- [J1] Yann Gauduel, Hélène Gelabert, and **Frédéric Guilloud**. Real-time probing of a three-electron bonded radical : Ultrafast one-electron reduction of a disulfide biomolecule. *Journal of the American Chemical Society*, 122(21):5082 – 5091, 2000.

#### A.4.2 Conférences avec comité de lecture

- [C24] Jialong Duan, Xavier Lagrange, and **Frédéric Guilloud**. Analysis of different user grouping algorithms in a C-RAN downlink system. In *ICC 2017, International Conference on Communications*, May 2017.
- [C23] Yupeng Tai, **F. Guilloud**, C. Laot, R. Le Bidan, and Haibin Wang. Joint equalization and decoding scheme using modified spinal codes for underwater communications. In *OCEANS 16*, Sept. 2016.
- [C22] Pasteur Poda, Samir Saoudi, Thierry Chonavel, **Frédéric Guilloud**, and Théodore Tapsoba. Kernel-based performance evaluation of coded QAM systems. In *13th African Symposium on Research in Computer Science and Applied Mathematics, CARI 2016*, October 2016.
- [C21] P. Poda, T Tapsoba, S. Saoudi, T. Chonavel, and **F. Guilloud**. A kernel-based soft ber estimator for coded qam transmission systems. In *8th International Symposium on Signal, Image, Video and Communications (ISIVC)*, November 2016.
- [C20] Jialong Duan, Xavier Lagrange, and **Frédéric Guilloud**. Maximum throughput in a c-ran cluster with limited fronthaul capacity. In *International Symposium on Wireless Personal Multimedia Communications, WPMC 2016*, Nov. 2016.
- [C19] Jialong Duan, Xavier Lagrange, and **Frédéric Guilloud**. Performance Analysis of Several Functional Splits in C-RAN. In *VTC Spring 2016*, May 2016.
- [C18] Carole Al Besclawi, Jean-Claude Belfiore, and **Frédéric Guilloud**. Reed-muller lattice coding for the rayleigh block fading channel. In *IEEE Wireless Communications and Networking Conference, WCNC 2016*, April 2016.
- [C17] Carole Al Bechlawi and **Frédéric Guilloud**. Frame Length Reduction for Massive-Machine Communications. In *VTC Spring 2015 : IEEE 81st Vehicular Technology Conference*, pages 1 – 5, 2015.
- [C16] Carole Al Bechlawi and **Frédéric Guilloud**. Approximation du LLR pour un Décodage Multi-niveaux de Réseaux de Points Imbriqués. In *GRETSI 2015 : 25ème colloque du Groupement de Recherche en Traitement du Signal et des Images*, 2015.
- [C15] Malek Messai, **Frédéric Guilloud**, and Karine Amis. Détection Multi-utilisateurs Robuste pour un système Bluetooth. In *GRETSI 2015 : 25ème colloque du Groupement de Recherche en Traitement du Signal et des Images*, 2015.
- [C14] Malek Messai, **Frédéric Guilloud**, and Karine Amis. Robust Multiuser Binary CPM Detection with Unknown modulation index. In *EUSIPCO 2015 : 23rd European Signal Processing Conference*, 2015.



- [C13] Malek Messai, Karine Amis, and **Frédéric Guilloud**. A Low Complexity Iterative Soft Detection for Bit Interleaved Coded CPM. In IEEE, editor, *ISTC 2014 : proceedings of the 8th International Symposium on Turbo Codes and Iterative Information Processing*, pages 12 – 16, 2014.
- [C12] Malek Messai, **Frédéric Guilloud**, and Karine Amis. A Low Complexity Coherent CPM Receiver with Modulation Index Estimation. In *EUSIPCO 2014 : 22nd European Signal Processing Conference*, pages 979 – 983, 2014.
- [C11] Tarek Chehade, Karine Amis, and **Frédéric Guilloud**. Récepteur de signaux GFSK de faible complexité robuste aux variations de l'indice de modulation. In *GRETSI 2013 : 24ème Colloque du Groupement de recherche en traitement du signal et des images*, 2013.
- [C10] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. Phase uncertainty algorithm on radix-2 for reducing the PAPR of multiple candidate OFDM system. In *14th International Symposium on Wireless Personal Multimedia Communications*, 2011.
- [C9] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. Low complexity SLM technique with an interleaver- butterfly ensemble for PAPR reduction of power limited OFDM system. In *IEEE Spring VTC 2011 : 73rd Vehicular Technology Conference*, 2011.
- [C8] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. OFDM-PAPR reduction using coded frequency division binary mask. In *EW 2011 : European Wireless*, 2011.
- [C7] Ramesh Pyndiah, **Frédéric Guilloud**, and Karine Amis. Multiple source cooperative coding using turbo product codes with a noisy relay. In *6th International Symposium on Turbo Codes & Iterative Information Processing*, 2010.
- [C6] Hyunseuk Yoo, **Frédéric Guilloud**, and Ramesh Pyndiah. Low complexity partial selected mapping for PAPR reduction of OFDM system. In Mark Benthum, editor, *IEEE SCVT 2010 : 7th Annual Symposium on Communications and Vehicular Technology*, 2010.
- [C5] Andrzej Michal Kabat, **Frédéric Guilloud**, and Ramesh Pyndiah. On the sensibility of the arranged list of the most a priori likely tests algorithm. In *MILCOM'07 : Military communications conference, October 29-31, Orlando, Florida, USA*, 2007.
- [C4] Andrzej Michal Kabat, **Frédéric Guilloud**, and Ramesh Pyndiah. New approach to order statistics decoding of long linear block codes. In *GLOBECOM'07 : 50th annual IEEE Global telecommunications conference, November 26-30, Washington, USA*, 2007.
- [C3] Dai Kimura, Ramesh Pyndiah, and **Frédéric Guilloud**. Construction of parity-check matrices for non-binary LDPC codes. In *4th international symposium on turbo codes and related topics, Munich, Allemagne, April 3-7, 2006*.
- [C2] Dai Kimura, **Frédéric Guilloud**, and Ramesh Pyndiah. Application of non-binary LDPC codes for small packet transmission in vehicle communications. In *5th International Conference on ITS telecommunications, Brest, France*, pages 109 – 112, June 27-29, 2005.
- [C1] **Frédéric Guilloud**, Emmanuel Boutillon, and Jean-Luc Danger. Bit error rate calculation for a multiband non-coherent on-off keying demodulation. In *Communications, 2002. ICC 2002. IEEE International Conference on*, volume 1, pages 202–206, 2002.

### A.4.3 Présentations invitées

- [I3] Carole Al Bechlawi and **Frédéric Guilloud**. How lattice codes compare to conventional fec/modulation schemes?. In *18th Joint Workshop on Communications and Coding (JWCC)*. March 2017.
- [I2] **Frédéric Guilloud**. Continuous phase modulation : a "new" waveform for 5g massive machine-type communications. In *International Conference on Advanced Communication Systems and Information Security (ACOSIS'16)*. Oct. 2016.
- [I1] **Frédéric Guilloud** and Emmanuel Boutillon. Generic LDPC implementation. In *2005 IEEE Communication Theory Workshop (CTW 2005)*. June 2005.

### A.4.4 Brevets

- [B5] Karine Amis, **Frédéric Guilloud**, and Malek Messai. Procédé de démodulation et démodulateur d'un signal modulé à phase continue, et programme d'ordinateur correspondant, 2014.
- [B4] Ramesh Pyndiah, Andrzej Michal Kabat, Karine Amis, and **Frédéric Guilloud**. Method for transmitting a digital signal between at least two transmitters and at least one receiver, using at least one relay, and corresponding program product and relay device, 2009.
- [B3] Dai Kimura, Ramesh Pyndiah, and **Frédéric Guilloud**. Multiple-Input-Multiple-Output Transmission Using Non-Binary LDPC Coding, 2006.
- [B2] Dai Kimura, Ramesh Pyndiah, and **Frédéric Guilloud**. Construction of Parity Check Matrices for Non-Binary LDPC Codes, 2006.
- [B1] Emmanuel Boutillon, **Frédéric Guilloud**, and Jacky Tusch. Ldpc decoder, corresponding method, system and computer program, 2003.

### A.4.5 Chapitre de livre

- [CH1] **Frédéric Guilloud** and Emmanuel Boutillon. *Codes and Turbo Codes*, , chapter 9, (LDPC codes). Springer-Verlag, Paris, 2010. Ouvrage collectif sous la direction de Claude Berrou.

### A.4.6 Soumissions en cours

- [U4] The Phuong Nguyen, **Frédéric Guilloud**, and Raphaël Le Bidan. State of the art in short packet communications : physical layer comparison for block fading channels. submitted to IEEE Wireless Communications and Networking Conference, WCNC 2018, Sept. 2017.
- [U3] Malek Messai, **Frédéric Guilloud**, Karine Amis, and Abdeldjalil Aïssa El Bey. Reconstruction of a finite alphabet block-sparse signal via support detection. under preparation for submission to IEEE Transaction on Communications, Dec. 2017.
- [U2] Jialong Duan, Xavier Lagrange, and **Frédéric Guilloud**. Hybrid joint transmission in a c-ran downlink system with limited fronthaul capacity. submitted to IEEE Transaction on Wireless Communications, july 2017.
- [U1] Malek Messai, Abdeldjalil Aïssa El Bey, Karine Amis, and **Frédéric Guilloud**. Iteratively re-weighted two-stage lasso for sparse recovery under finite-alphabet constraints. submitted to Elsevier Signal Processing (fast communication), November 2017.



# Résumé

Ce mémoire d'Habilitation à Diriger des Recherches présente une synthèse de mes activités de recherches menées au sein du département Signal & Communications de Télécom Bretagne et du laboratoire Lab-STICC (UMR 6285) depuis 2005.

Dans une première partie, je présente certaines contributions relatives au codage correcteur d'erreurs. Je commence par les codes de parité à faible densité (LDPC) non-binaires, en me focalisant d'une part sur le séquençement du décodage par propagation de croyance, et d'autre part sur la construction de matrices de contrôle de parité non binaires. Je poursuis par l'étude du décodage pondéré des codes Reed-Solomon, pour lesquels je présente une technique basée sur les statistiques d'ordre permettant d'effectuer le décodage pondéré de codes longs à hauts rendements. Enfin, je présente une technique de codage dans l'espace des signaux basée sur les réseaux de points, avec pour objectif de comparer ce type de codage avec les techniques usuelles de codage et de modulation. Notamment, j'expose les techniques d'encodage et de décodage pour des petites dimensions et les problèmes de mise en forme associés à ces techniques, puis des schémas de type modulation codée permettant de mettre en œuvre ces réseaux de points pour des dimensions plus élevées.

Dans une deuxième partie, je présente deux contributions permettant de réduire la consommation d'énergie des émetteurs en limitant la dynamique des signaux à amplifier. La première contribution considère la réduction du rapport entre la puissance crête et la puissance moyenne (PAPR) des modulations multi-porteuses orthogonales (OFDM). Parmi les familles de techniques permettant une réduction du PAPR, nous avons choisi celle basée sur la génération de plusieurs symboles candidats portant la même information, combinée avec une saturation du signal lorsque le PAPR dépasse une valeur seuil. La seconde contribution concerne les modulations à phase continue (CPM) qui sont une famille de modulations à enveloppe constante et qui ont par conséquent un PAPR nul. En revanche ces modulations sont plus complexes à détecter que les modulation linéaires, et elles sont également très sensibles à des incertitudes sur les paramètres définissant le signal émis (particulièrement l'indice de modulation). J'expose plusieurs solutions permettant de résoudre ces défauts, ainsi que deux solutions pour envisager les communications multi-utilisateurs.

La troisième partie est consacrée à mes perspectives de recherches regroupées sous le thème "communications numériques sans fil à trames courtes" que l'on retrouve dans le contexte des communications entre machines ou dans le domaine des réseaux de capteurs. L'importance de ces contextes a été mise en évidence notamment dans le projet METIS lors de l'étude des différents scénarios de la future 5G et de l'internet des objets. Après la description du contexte des communications numériques à base de trames courtes, j'expose les défis qu'elles représentent au niveau de la conception de la couche physique et de la couche d'accès radio. En effet, toutes les fonctions de ces couches sont impactées par la faible longueur de la trame, remettant ainsi en cause le tandem classique codage-entrelacement-modulation (BICM) ou l'utilisation des entêtes de trame pour la synchronisation et l'estimation du canal : un nouveau paradigme de conception de la couche physique doit être proposé.