TELECOM PARIS

Thèse

présentée pour obtenir le grade de docteur

de l'Ecole nationale supérieure
des télécommunications

Spécialité : Electronique et Communications

Catherine Lamy

Communications à grande efficacité spectrale sur le canal à évanouissements

soutenue le 18 avril 2000 devant le jury composé de

Hikmet Sari	Président
Jean-Yves Chouinard	Rapporteurs
Emanuele Viterbo	
Alain Glavieux	Examinateurs
Philippe Godlewski	
Lionel Songeon	
Joseph Boutros	Directeur de thèse

Ecole nationale supérieure des télécommunications

PhD thesis

Ecole nationale supérieure des télécommunications
Communications and Electronics department
Digital communications group

Catherine Lamy

High spectral efficiency communications over the Rayleigh fading channel

Defense date: April, 18th 2000

Committee in charge:

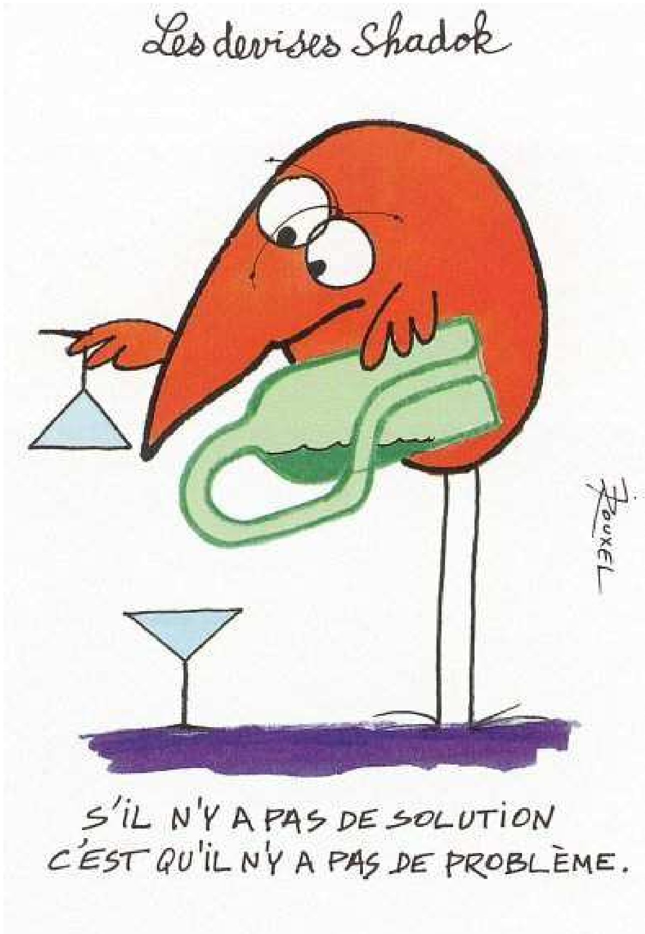
Hikmet Sari	Chairman
Jean-Yves Chouinard	Reporters
Emanuele Viterbo	
Alain Glavieux	Examiners
Philippe Godlewski	
Lionel Songeon	
Joseph Boutros	Advisor

Ecole nationale supérieure des télécommunications

À mes parents,
pour l'éducation et l'exemple qu'ils ont su me donner.

À tous ceux et à toutes celles qui m'ont jour après jour appris le peu que je sais.

"Parce que"
–Barbara



Remerciements

Je tiens à exprimer ici toute ma reconnaissance aux personnes qui m'ont aidée, encouragée, soutenue ou tout simplement supportée tout au long de mon travail de thèse.

Je veux tout d'abord remercier le professeur Hikmet Sari d'*Alcatel Research and Technology* de m'avoir fait l'honneur de présider mon jury de thèse. Toute ma gratitude va également au professeur Jean-Yves Chouinard, de l'université d'Ottawa, pour sa lecture attentive de mon manuscrit, ses remarques constructives et sa grande gentillesse. Mes plus vifs remerciements s'adressent à Emanuele Viterbo, du *Politecnico* de Turin pour son rôle de rapporteur mais aussi pour les différentes discussions que nous avons eues ensemble au sujet des modulations tournées et de l'étude de leurs capacités. Je remercie également messieurs Alain Glavieux, professeur à l'E.N.S.T. de Bretagne et Philippe Godlewski, professeur à E.N.S.T., pour avoir accepté de faire partie de mon jury de thèse et pour leur intérêt pour mon travail.

Je n'oublie évidemment pas Motorola Semi-Conducteurs (Toulouse) et Pascal Mabille en particulier, qui a été l'artisan de cette collaboration entre Motorola et le département Communications et Electronique de l'E.N.S.T. Je remercie ici également Lionel Songeon, pour avoir fait partie de mon jury mais aussi deux personnes dont la gentillesse n'a eu d'égale que leur disponibilité, à savoir Maryline Richard et surtout Pierrette Capelle.

Il ne saurait être question de ne pas parler ici de Joseph Boutros, mon directeur de thèse sans lequel ce travail n'aurait jamais vu le jour. Son dynamisme, son expérience, et son "sens" des communications numériques, sont autant de raisons pour lesquelles son encadrement fut extrêmement profitable. Joseph, je ne saurais trop te remercier pour ton temps, tes conseils et ta confiance.

Je pense pouvoir dire que le temps que j'ai passé au département Communications et Electronique de l'E.N.S.T. fut pour moi une expérience fort enrichissante. Je tiens à remercier le professeur Philippe Gallion pour m'y avoir acceptée, les secrétaires Jany Bats, Laurence Monnot, Marie-Thérèse Perucca et Danielle Childz pour leur aide, Robert Vallet pour ses conseils précieux dans le domaine de l'estimation de canal et tous les autres permanents du département.

Je tiens aussi et surtout à remercier mes compagnons de voyage, collègues et camarades de l'E.N.S.T. avec lesquels j'ai partagé des moments inoubliables entre bouilloire, présentations et discussions scientifiques ou plus personnelles animées : Loïc Brunel et son genou, Olivier “Gadget” Pothier, Céline “de souche” Durand, Sandrine “Step” Vialle et sa théière, Christophe Brutel et les bières du vendredi, Hadi Sawaya bien qu'à distance, Francesc Boixadera et Sabine “blonde cendrée” Leveiller, mes compagnons en Josephie, mais également Cédric Ware, dont dire qu'il est notre sys-admin astronome serait tellement restrictif, Amal Abou Hassan, terroriste du tetris, Bahram Zahir-Azami et les chevaux, Stefan Lauffenburger, l'homme à femmes venu du pays du chocolat, Mohamed Ratni, Daniela Boggio, Mohamad Aoudé, Christophe “Rabiche” Gosset, Ammar Chkeif, Nicolas Ibrahim... et tous les autres.

Merci enfin à celui qui a été là pour moi tout au long de cette aventure, tour à tour, camarade, ami, “secrétaire” et tant d'autres choses : merci à toi, FX, merci de toi, comme disait une chanteuse célèbre.

"Finishing a book is just like you took a child out in the yard and shot it."
(Terminer un livre revient à emmener un enfant dans le jardin et l'abattre).
–Truman Capote

Paris, le 26 avril 2000

Résumé

Du fait de l'explosion actuelle des télécommunications, les opérateurs sont victimes d'une crise de croissance les obligeant à installer toujours plus de relais, à découper les cellules (zone de couverture d'un relais) en micro-cellules dans les grandes villes, afin de faire face à la demande toujours grandissante de communications. Les concepteurs des nouveaux réseaux de transmission sont donc constamment à la recherche d'une utilisation plus efficace des ressources disponibles.

Une solution est l'utilisation de modulations à haute efficacité spectrale, c'est-à-dire pour lesquelles chaque symbole émis contient un grand nombre de bits d'information. Par ailleurs, il est indispensable d'adapter l'émission aux caractéristiques du canal radio-mobile. En effet, contrairement au canal gaussien, la transmission sur canal radio-mobile est atténuée sévèrement du fait des évanouissements liés aux obstacles et à la propagation multi-trajets. Lorsque l'atténuation est trop forte, il est impossible de déterminer en réception le signal qui a été émis à moins qu'une réplique moins atténuée du signal ne soit également disponible. L'existence de telles répliques correspond à l'utilisation d'une technique dite de diversité.

Deux types de diversité sont traités dans ce mémoire de thèse, qui permettent de combattre les évanouissements tout en assurant une transmission à haute efficacité spectrale. Tout d'abord, nous considérons la diversité de modulation, créée par l'utilisation de réseaux de points tournés. Ensuite nous envisageons l'emploi d'une diversité d'antennes en réception, combinée avec des antennes multiples en émission afin de garantir une forte efficacité spectrale.

Abstract

One of the effects of the explosion in the field of telecommunications that we are experiencing at the moment is that the operators are, at every instant, victims of a growth crisis which forces them to install more relays, to cut the cells (covering the zones of a relay) into micro-cells in urban areas, in order to meet the growing demand in communications. The architects of the new transmission networks are therefore constantly in search of available resources.

A solution is the utilisation of modulations with high spectral efficiency, that is to say, for which each symbol emitted contains a large number of bits of information. What is more, it is necessary to adapt the emission to the characteristics of the mobile channel. In fact, unlike the Gaussian channel, the transmission on a mobile channel is severely attenuated by the phenomenon of fading linked to obstacles and the multi-trajectory propagation. When the attenuation is too strong, it is impossible to determine at reception the signal which has been emitted unless a less attenuated replica of the signal is equally available. The existence of such replicas corresponds to the utilisation of a technique called diversity.

This thesis treats of two types of diversity which enable you to combat the phenomenon of fading while at the same time ensuring high efficiency spectral transmission. The first type encountered corresponds to the diversity of modulation, with utilisation of rotated lattices and the second corresponds to a multiple antennas diversity in emission in order to guarantee high spectral efficiency.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

Pour des raisons de lisibilité, la signification d'une abréviation ou d'un acronyme n'est souvent rappelée qu'à sa première apparition dans le texte d'un chapitre. Par ailleurs, puisque nous utilisons toujours l'abréviation la plus usuelle, il est fréquent que ce soit le terme anglais qui soit employé, auquel cas nous présentons une traduction.

APP	*A Posteriori* Probability	Probabilité *a posteriori*
AWGN	Additive White Gaussian Noise	Bruit additif blanc gaussien
BPSK	Binary Phase Shift Keying	Modulation de phase binaire
BICM	Bit Interleaved Coded Modulation	Modulation codée avec entrelacement de bits
CSI	Channel State Information	État du canal
DFE	Decision Feedback Equalizer	Égaliseur à retour de décision
EM	Expectation-Maximization	
fcc	face centered cubic (lattice)	(Réseau) cubique à faces centrées
FFT	Fast Fourier Transform	Transformée de Fourier rapide
FHT	Fast Hadamard Transform	Transformée de Hadamard rapide
FRT	Fast Rotation Transform	Transformée de Rotation rapide
GSM	Global System for Mobile communications	Système global pour les télécommunications mobiles
IES	Intersymbol Interference	Interférence entre symboles
LLR	Log-Likelihood Ratio	Logarithme du rapport des vraisemblances
MAQ	Quadrature Amplitude Modulation	Modulation d'amplitude en quadrature
MIMO	Multiple-Input Multiple-Output	Entrées multiples sorties multiples
ML	Maximum Likelihood	Maximum de vraisemblance
MSE	Mean Square Error	Erreur quadratique moyenne
MMSE	Minimum Mean Square Error	Erreur quadratique moyenne minimale
NRNSC	Non-Recursive Non-Systematic Convolutional code	Code convolutif non-récursif non-systématique
PAM	Pulse Amplitude Modulation	Modulation d'impulsion en phase
pdf	Probability Density Function	Densité de probabilité
P_{eb}	Bit Error Rate	Probabilité d'erreur par bit
QPSK	Quaternary Phase Shift Keying	Modulation de phase quaternaire
RSC	Recursive Systematic Convolutional code	Code convolutif récursif systématique
Rx	Receiving (antenna)	(Antenne de) réception

SNR	Signal-to-Noise Ratio	Rapport signal à bruit
SISO	Soft-Input Soft-Output (decoder)	(Décodeur) à entrées souples et sorties souples
TCM	Trellis Coded Modulation	Modulation codée en treillis
Tx	Transmitting (antenna)	(Antenne d')émission
ZF	Zero Forcing	Forçage à zéro

Liste des notations

Nous avons regroupé ci-dessous les principales notations employées dans les différents chapitres du document. Dans la mesure du possible, nous avons tenté de conserver les mêmes notations d'un chapitre à l'autre. Nous présentons tout d'abord une liste générale puis des listes relatives aux différents chapitres. On notera que seules les notations qui diffèrent de celles précédemment définies seront données dans ces listes. Enfin, certaines notations, apparaissant uniquement de manière ponctuelle, ont été omises.

Notations générales

$\Re(z)$	partie réelle du nombre complexe z
$\Im(z)$	partie imaginaire du nombre complexe z
$\odot$	produit composante par composante
$C_n^k = \binom{n}{k}$	opérateur combinaison : nombre de manières de choisir k valeurs parmi n
$d_E(\mathbf{u}_1, \mathbf{u}_2)$	distance euclidienne entre les deux points (les deux vecteurs) $\mathbf{u}_1$ et $\mathbf{u}_2$
$d_H(\mathbf{u}_1, \mathbf{u}_2)$	distance de Hamming entre les deux points (les deux vecteurs) $\mathbf{u}_1$ et $\mathbf{u}_2$
$\mathbf{D}(\mathbf{u})$	la matrice diagonale $n \times n$ ayant sur sa diagonale principale les composantes $u_1, \cdots, u_n$ du vecteur $\mathbf{u}$
$E[u]$	espérance mathématique de la variable u
$\mathbf{u}^t$	transposé de u (nombre, vecteur ou matrice)
$\mathbf{u}^*$	conjugué de u (nombre, vecteur ou matrice)
$\mathbf{u}^h$	transconjugué de u (nombre, vecteur ou matrice)
I_n	matrice identité en dimension n
$Q(x) = \frac{1}{2}\mathrm{erfc}\left(\frac{x}{\sqrt{2}}\right)$	fonction erreur

Les réseaux de points

$n = 2^m$	dimension de l'espace euclidien
p	rang d'un réseau Λ (très vite, on a : $p = n$)
Λ	un réseau de points
$\mathbf{0} = (0, \cdots, 0)$	point origine dans un espace de dimension n
M	matrice génératrice d'un réseau Λ
$G_\Lambda = (\varsigma_{ij})$	matrice de Gram d'un réseau Λ

d_{Emin}	distance euclidienne minimale d'un réseau Λ
$det(\Lambda)$	volume fondamental d'un réseau Λ
$\mathcal{V}(\mathbf{u})$	cellule de Voronoï d'un point $\mathbf{u}$ d'un réseau Λ
ρ	rayon d'empilement d'un réseau Λ
Δ	densité d'un réseau Λ
δ	densité centrée d'un réseau Λ
V_n	volume d'une sphère de rayon unité en dimension n
$\tau(\Lambda)$	coefficient d'erreur d'un réseau Λ
$\gamma(\Lambda)$	gain fondamental d'un réseau Λ
$\mathcal{C}$	constellation tirée d'un réseau Λ
$\gamma(\mathcal{C})$	gain total d'une constellation $\mathcal{C}$
η	efficacité spectrale par deux dimensions
L	diversité d'un réseau Λ ou, de manière équivalente, d'une constellation $\mathcal{C}$
$m(\mathbf{y}\|\mathbf{x})$	métrique à maximum de vraisemblance sur canal AWGN
$\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)^t$	vecteur des évanouissements sur le canal de Rayleigh
$m(\mathbf{y}\|\mathbf{x}, \boldsymbol{\alpha})$	métrique à maximum de vraisemblance sur canal de Rayleigh
C	rayon de la sphère utilisée dans l'algorithme de décodage par sphères
$C_0, \cdots C_a$	codes convolutifs utilisés pour construire des réseaux de points
$RM(r, m)$	code de Reed-Müller d'ordre r et de longueur m
BW_n	réseau de Barnes-Wall en dimension n
W	matrice aller de l'égaliseur à retour de décision (filtre transverse)
$G = (g_{ij})$	matrice retour de l'égaliseur à retour de décision (filtre de retour)
$\mathbf{z}$	vecteur entier en entrée du réseau de points
$\hat{\mathbf{z}}$	vecteur estimé en sortie du détecteur à seuil du DFE
$\tilde{\mathbf{z}}$	version souple du vecteur estimé $\hat{\mathbf{z}}$
$\mathbf{x}$	point du réseau Λ : vecteur en entrée du canal
$\mathbf{y}$	vecteur en sortie du canal
$\mathbf{b}$	bruit additif blanc gaussien sur le canal considéré
N_0	densité spectrale de puissance du bruit blanc gaussien en bande de base
$\boldsymbol{\lambda} = (\lambda_i)$	vecteur des multiplicateurs de Lagrange
E_b/N_0	Rapport signal à bruit par bit d'information

Les rotations et MAQ multidimensionnelles

$R = (r_{ij})$	matrice de rotation
$\mathcal{I}_1, \cdots, \mathcal{I}_M$	contellation PAM de taille M
$\mathbf{z} = (z_i)^t$	vecteur d'entiers appartenant à une constellation MAQ multidimensionnelle
$\mathbf{x}$	point appartenant à la constellation MAQ tournée : vecteur en entrée du canal
$G(i, j, \xi)$	matrice de Given correspondant à la rotation d'angle ξ dans le plan $(\mathbf{0}u_i, \mathbf{0}u_j)$
$\hat{I}$	réflexion ou composée de réflexions
$\mathbb{Z}_{n,L}$	version tournée du réseau cubique $\mathbb{Z}^n$ en dimension n de diversité L
$\mu_\beta(x)$	polynôme minimal de β
J	Idéal premier
$T_k(x)$	$k^{ème}$ polynôme de Tchebicheff du premier ordre

H_n	matrice de Hadamard en dimension n
$L[l]$	nombre de vecteurs de diversité l
$D[d^2]$	nombre de vecteurs d'énergie d^2
c_j	bit codé
$Ext(c_j)$	information extrinsèque sur le bit codé c_j
$\pi(c_j)$	probabilité *a priori* du bit codé c_j
$APP(c_j)$	probabilité *a posteriori* du bit codé c_j
$obs(c_j)$	observation sur le bit codé c_j

Modulations pour les antennes multiples

n_t	nombre d'antennes en émission
n_r	nombre d'antennes en réception
canal (n_t, n_r)	canal avec n_t antennes d'émission et n_r antennes de réception
E_s	énergie moyenne d'un symbole
$P(U \to V)$	probabilité d'erreur par paire : probabilité de décoder V lorsque U a été effectivement émis en faisant abstraction des autres mots du code
$H = (h_{ij})$	matrice des évanouissements sur le canal MIMO
M	taille de la constellation à laquelle appartiennent les symboles émis
$m = \log_2 M$	nombre de bits codés par symbole émis
N_c	nombre de bits codés par trame émise
N	taille de la trame émise (en nombre de symboles)
$\mathbf{u}$	vecteur de bits d'information
$\mathbf{c}$	vecteur de bits codés
$\mathbf{x}$	vecteur des symboles émis
$\mathbf{y}$	vecteur des symboles reçus
N_p	nombre de symboles pilotes ajoutés à la trame de taille N
$\hat{H}$	estimation de H
$\hat{N}_0$	estimation de N_0
$\Theta = (N_0, H)$	paramètres du canal

Étude de la capacité

$\mathcal{H}(X)$	entropie de X
$p(\mathbf{x})$	densité de probabilité de X (de réalisation $\mathbf{x}$)
$\mathcal{H}(X, Y)$	entropie conjointe des variables X et Y
$\mathcal{H}(X\|Y)$	entropie conditionnelle de X étant donné Y
$I(X; Y)$	information mutuelle entre X et Y
χ	constellation à laquelle appartiennent les entrées du canal
R_D	débit binaire de transmission sur le canal
C	capacité en bits d'information par symbole
$C_{\|H}$	capacité sachant la réalisation de l'évanouissement H

$d_{P,min}^{(\ell)}$	ditance produit-ℓ minimale
H_n	matrice de type Hadamard en dimension n
$\delta(\cdot)$	impulsion de Dirac
$M = 2^m$	taille de la constellation tournée dont on calcule la capacité
C_{dim}	capacité en bits d'information par dimension
E_c/N_0	Rapport signal à bruit par bit codé

Introduction

Nous vivons dans l'ère des télécommunications. Les téléphones mobiles, les messages électroniques, le multimédia font désormais partie de notre quotidien. À titre indicatif, près d'un tiers de la population française dispose d'un téléphone portable (janvier 2000). Alors que ce phénomène avait commencé presque uniquement chez les hommes d'affaires et autres médecins, on trouve à présent des utilisateurs de portables dans toutes les couches de la population : enfants, cadres, techniciens, employés voire retraités. Les prix des communications ont d'ailleurs, grâce à des formules d'abonnement en tous genres, baissé de telle façon que le volume global des communications a pu s'accroître considérablement. Parallèlement, le goût du "sans fil" s'étant développé, son caractère pratique et la plus grande facilité de la maintenance jouant en sa faveur, il se pourrait qu'à plus ou moins court terme les téléphones domestiques soient remplacés par des appareils sans fils (voir figure 1). Ainsi, arrive le moment où, avec le même numéro, on pourra partir traverser le Sahara à dos de chameau et pourtant avoir la certitude de pouvoir appeler, envoyer un message ou être contacté à tout moment.

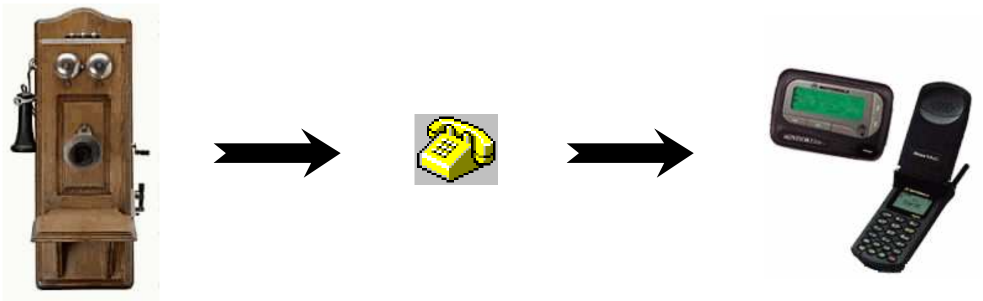


Fig. 1: L'évolution des téléphones au cours du temps.

Un des effets de cette explosion des télécommunications est que les opérateurs sont presque à tout moment victimes d'une crise de croissance qui les oblige à installer toujours plus de relais, à découper les cellules (zone de couverture d'un relais) en micro-cellules dans les grandes villes, afin de faire face à la demande toujours grandissante de communications. Les concepteurs des nouveaux réseaux de transmission sont donc constamment à la recherche d'une utilisation toujours plus efficace des ressources disponibles. Une des solutions est l'utilisation de modulations *à haute efficacité spectrale*, c'est-à-dire pour lesquelles chaque symbole émis contient un grand nombre de bits d'information. Par ailleurs, il est

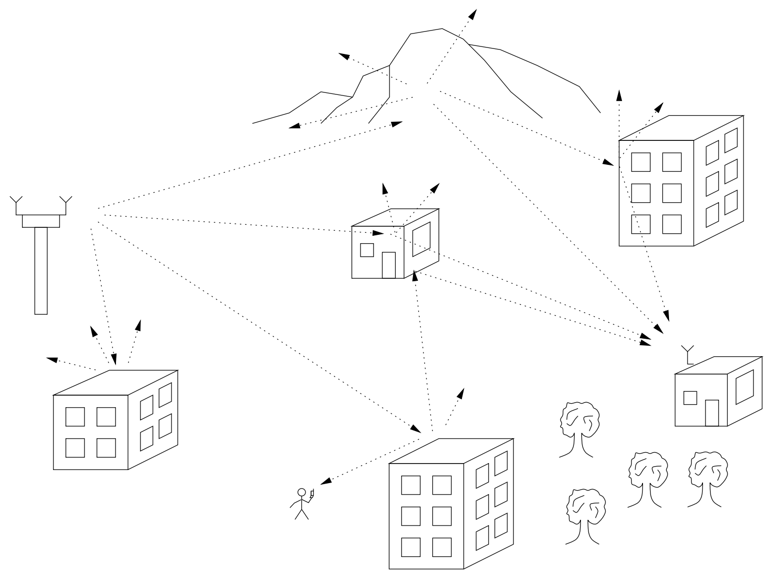


FIG. 2: Exemple d'un canal sans fil avec évanouissements

indispensable d'adapter l'émission aux caractéristiques du canal radio-mobile, présenté en figure 2. En effet, contrairement au canal gaussien, la transmission sur canal radio-mobile est atténuée sévèrement du fait des interférences ou *évanouissements* liés aux obstacles et à la propagation multi-trajets. Lorsque l'atténuation est trop forte, il est impossible de déterminer en réception le signal qui a été émis à moins qu'une réplique moins atténuée du signal ne soit également disponible. L'existence de telles répliques correspond à l'utilisation d'une technique dite de *diversité*.

Parmi les différentes techniques les plus classiques de diversité, on peut définir trois grandes familles, à savoir les diversités "physiques", i.e. liées à la propagation, les diversités d'antennes et la diversité de modulation. Par exemple, on trouve :

• **la diversité en fréquence** ("frequency diversity") : il s'agit de recevoir sur n fréquences différentes des versions décorrélées d'un même signal. Il est alors nécessaire de disposer de fréquences différentes séparées d'au moins la bande de cohérence du canal.

• **la diversité en temps** ("time diversity") : il s'agit de recevoir en n instants différents des versions décorrélées d'un même signal. Il est alors nécessaire de pouvoir séparer les instants de réception d'au moins le temps de cohérence du canal.

Ces deux premières techniques sont fort coûteuses en terme d'efficacité spectrale, puisqu'elles supposent que l'on répète le même signal à des instants ou sur des fréquences différentes. Elles furent surtout utilisées dans le domaine des communications analogiques.

• **la diversité de trajet** ("path diversity") : en raison des conditions de propagation, elle est due aux réflexions, réfractions et éléments dispersifs sur le canal.

• **la diversité d'antennes en réception** ("space diversity in reception") : elle suppose que les n antennes sont séparées d'au moins une demi-longueur d'onde. La diversité maximale possible est alors égale à n. En pratique, plus il y a d'éléments dispersifs à proximité des antennes, plus les décorrélations sont importantes. L'inconvénient est que cette technique n'est pas applicable aux communications par satellites (les angles d'arrivées des différentes antennes sont les mêmes) et peu aux mobiles (2 à 3 antennes semblent un grand maximum).

• **la diversité d'antennes en émission** ("space diversity in emission") : la méthode la plus simple consiste pour l'émetteur à émettre le même signal sur plusieurs antennes, supposées suffisamment séparées. En réception on a alors de la diversité temporelle. Une autre méthode consiste à remplacer la répétition des symboles en émission par un code correcteur d'erreurs de rendement plus élevé. On gagne alors en puissance et en efficacité spectrale en raison de l'augmentation du rendement.

• **la diversité de modulation** (modulation diversity) : due au type de modulation, elle correspond au nombre minimal de composantes dont deux symboles de la constellation utilisée diffèrent.

Les systèmes pratiques combinent souvent plusieurs types de diversité pour en tirer différents avantages et de manière générale une meilleure efficacité spectrale à un moindre coût. Ainsi le système GSM regroupe-t-il :

- de la diversité temporelle (codage suivi d'un entrelaceur)
- de la diversité en fréquence (sauts de fréquence)
- de la diversité d'antennes en réception (sur la voie montante)
- de la diversité de trajet (présence d'un égaliseur pour utiliser cette diversité liée à la propagation).

Ce mémoire de thèse traite de deux types de diversité permettant de combattre les évanouissements tout en assurant une transmission à haute efficacité spectrale. Le premier type abordé correspond à la diversité de modulation, avec utilisation de réseaux de points tournés et le second correspond à une diversité d'antennes en réception, avec utilisation d'antennes multiples en émission afin de garantir une forte efficacité spectrale.

Organisation de la thèse

Ce document est divisé en quatre chapitres et quatre annexes. Certains développements analytiques ont ainsi été placés en annexe afin de simplifier au maximum les idées exposées dans le corps du document. On trouvera également une liste des différentes matrices de rotation utilisées dans ce mémoire pour des dimensions inférieures ou égales à 8.

Le chapitre 1 de ce document débute par une introduction aux réseaux de points. Les paramètres principaux d'un réseau sont décrits, ainsi que ses performances sur le canal à bruit additif blanc gaussien (AWGN) et sur le canal de Rayleigh non sélectif à évanouissements indépendants. Nous rappelons ensuite l'algorithme de décodage par sphères permettant de décoder tout réseau en dimension inférieure ou égale à 32 (limite pratique due à la complexité de l'algorithme). Nous donnons également les constructions A, B et D d'un réseau à partir de codes correcteurs d'erreurs et appliquons cette dernière construction au cas des réseaux de Barnes-Wall. Nous proposons enfin un nouveau décodeur de réseaux en grandes dimensions sur le canal AWGN reposant sur le critère de minimisation de l'erreur quadratique moyenne MMSE.

Dans le chapitre 2 nous passons en revue différents types de rotations adaptées au canal de Rayleigh non sélectif. Nous présentons également de nouvelles rotations : une adaptation en grande dimension des rotations algébriques avec la transformée de rotation rapide (FRT) et de nouvelles méthodes de construction comme l'utilisation de polynômes de Tchebicheff ou l'utilisation de matrices aléatoires. La distribution de diversité de certaines de ces rotations est alors calculée analytiquement. Trois différents modes de décodage pour une constellation tournée sont ensuite étudiées : après avoir considéré les performances et la robustesse du décodage par sphères, nous proposons une adaptation de notre décodeur reposant sur le critère MMSE au cas des réseaux tournés et enfin exposons un nouvel algorithme de décodage itératif reposant sur le calcul des probabilités *a posteriori* (APP) des bits codés.

Nous proposons au chapitre 3 une nouvelle méthode de décodage pour les systèmes à antennes multiples sur canal de Rayleigh ou canal de Rayleigh par blocs. Nous employons pour cela un décodage itératif à entrées et sorties souples, dans lequel nous avons intégré une estimation itérative des paramètres du canal grâce à l'algorithme EM. Choisissant d'émettre des symboles différents sur chacune des antennes d'émission, on atteint ainsi de fortes efficacités spectrales.

Le chapitre 4 traite de différents calculs de capacité. Nous y rappellons tout d'abord la capacité et la probabilité de coupure (*outage probability*) des canaux à entrées et sorties multiples considérés au chapitre 3. Nous présentons ensuite une étude sur la capacité des canaux de Rayleigh non sélectifs à évanouissements indépendants ayant pour entrée une modulation tournée, et mettons en évidence le phénomène de "gaussianisation" que ces rotations engendrent.

Finalement, les conclusions des différentes idées présentées dans ce document sont données dans un chapitre final, ainsi que quelques perspectives de recherches ultérieures sur le sujet.

On notera les conditions générales dans lesquelles ces travaux ont été menés : nous supposons que la démodulation est cohérente tout au long de notre étude et que le canal à évanouissements est un canal de Rayleigh non sélectif à évanouissements indépendants ou par blocs. La modulation est soit une modulation de phase binaire (BPSK) soit une modulation d'amplitude en quadrature (MAQ).

Chapitre 1

Les réseaux de points *

Prenez un cercle, caressez-le, il deviendra vicieux !
Eugène Ionesco, *La cantatrice chauve*

1.1 Introduction

Un réseau de points (*lattice*) est constitué de centres de sphères empilées possédant une structure de groupe [27]. Utilisés en mathématiques pour les travaux sur les corps finis, les groupes et les formes quadratiques, mais aussi en chimie, où les cristallographes les emploient afin de modéliser le comportement de certains composés chimiques, ils servent également en communications numériques à construire des modulations tant sur le canal à bruit additif blanc gaussien (ou canal AWGN) que sur les canaux à évanouissements (Rice, Rayleigh).

En effet, en utilisant des empilements très denses, il est possible de construire des modulations de grande taille à énergie minimale, permettant ainsi d'effectuer des transmissions à haut débit binaire. Les constellations multidimensionnelles ainsi extraites des réseaux de points connaissent depuis l'apparition des modulations codées au début des années 1980 un grand succès dans le monde des transmissions sur le canal AWGN. Elles ont également été exploitées pour des applications filaires (tels le réseau de Gosset E_8 ou le réseau Leech Λ_{24} avec lesquels ont été construits des modems [46]). Plus récemment, avec le développement des transmissions radiomobiles pour lesquelles les réseaux performants sur le canal AWGN se sont révélés décevants, on a pu voir l'utilité des réseaux de points à grande diversité, qui permettent de récupérer l'information perdue au cours de la transmission en tirant partie de la redondance liant les composantes d'un point d'un tel réseau.

Après un rappel des définitions et résultats élémentaires sur les réseaux de points au

*Certaines parties de ce chapitre ont été publiées dans les journaux *Annales des télécommunications* [82] et *IEEE Transactions on Information Theory* [84].

paragraphe 1.2, et du fonctionnement du décodage des réseaux de points grâce à l'algorithme de décodage par sphères (*Sphere Decoder*) au paragraphe 1.3, nous décrirons au paragraphe 1.4 les méthodes de construction les plus classiques des réseaux de points à partir de codes correcteurs d'erreur, et introduirons les réseaux de Barnes-Wall. Le paragraphe 1.5 présentera alors le décodeur DFE de réseaux en grande dimension que nous avons réalisé, ainsi que des résultats de simulation. Finalement nous tirerons quelques conclusions au paragraphe 1.6.

1.2 Définition et présentation des réseaux de points

Un problème fort ancien auxquel les mathématiciens ont été confrontés est celui de déterminer une méthode permettant d'entasser le plus grand nombre de sphères dans un espace donné. La solution, qui serait triviale si il s'agissait de cubes, fut formalisée par Kepler en 1609 avec sa célèbre conjecture, mais ne fut finalement prouvée que tout récemment par Hales [41][57] : il faut, lorsque l'espace est très grand, ranger les boules en couches planes pavées par un motif de triangles équilatéraux pour obtenir l'empilement le plus dense qui soit en dimension 3. Dans ce rangement, les centres des sphères constituent un groupe algébrique, appelé réseau cubique à faces centrées (*fcc*) (ou réseau de Kepler, présenté en figure 1.1). Le volume occupé par les sphères représente alors $\pi/\sqrt{18} \approx 74.048\%$ de l'espace total.

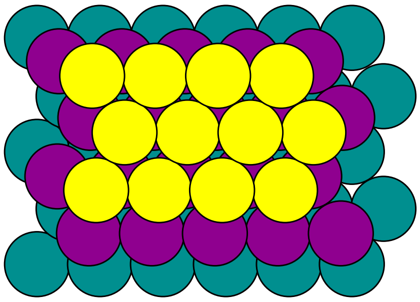


Fig. 1.1: Empilement cubique à faces centrées (vu de dessus).

Ce problème de recherche des empilements de sphères optimaux se généralise aisément en dimension supérieure à 3, sans qu'il en soit hélàs de même pour la démonstration. Nous allons donc nous intéresser aux réseaux de points de dimension n, n entier naturel.

Les notations suivantes seront utilisées : $\mathbb{N}$ est l'ensemble des entiers naturels, $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{R}$ l'ensemble des réels, et $\mathbb{R}^n$ l'espace euclidien réel de dimension n muni de sa distance. $\mathbf{x} = (x_1, \ldots, x_n)^t$ est un vecteur (ou point) de $\mathbb{R}^n$ si ses composantes x_i sont toutes des éléments de $\mathbb{R}$. La notation $(\cdot)^t$, utilisé sur un vecteur ou une matrice indique la transposition. Pour tout réel $a \in \mathbb{R}$, $a\mathbf{x}$ est le vecteur de composantes (ax_i). La norme euclidienne d'un vecteur $\mathbf{x}$ est notée $\|\mathbf{x}\|$. Une sphère dans $\mathbb{R}^n$, de rayon ρ et

de centre $u = (u_1, \ldots, u_n)$, est l'ensemble des points $\mathbf{x}$ vérifiant
$||\mathbf{x} - \mathbf{u}||^2 = (x_1 - u_1)^2 + (x_2 - u_2)^2 + \cdots + (x_n - u_n)^2 = \rho^2$.

1.2.1 Paramètres fondamentaux

Nous allons commencer par définir les différents paramètres principaux d'un réseau de points, afin de pouvoir d'une part comprendre ce dont il s'agit, ce que ces réseaux représentent et comment les caractériser. Donnons tout d'abord la définition exacte d'un réseau de points :

Définition 1.2.1 *(réseau de points)*
Un **réseau de points** *est un sous-groupe discret de rang p, $p \leq n$ de $\mathbb{R}^n$.*

Topologiquement, un réseau de points est donc également l'ensemble des vecteurs

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_p\mathbf{v}_p \quad a_1, \ldots, a_p \in \mathbb{Z}$$

engendré par la famille de p vecteurs indépendants $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_p$ de $\mathbb{R}^n$. C'est ce que l'on appelle encore un ***$\mathbb{Z}$-module*** engendré par les p vecteurs $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_p$.

Le réseau, que nous nommerons Λ sauf indication contraire, peut être vu comme le groupe additif formé par les centres des boules de l'empilement. Par définition d'un groupe additif, le point $\mathbf{0}$ appartient à Λ, et de plus la topologie d'un groupe est invariante par toute translation d'un de ses éléments donc il nous suffira toujours d'étudier ce qui se passe autour de l'origine $\mathbf{0}$ pour connaître le comportement autour de tout point de Λ.

Définition 1.2.2 *(base du réseau)*
La famille des p vecteurs $\mathbf{v}_1, \ldots, \mathbf{v}_p$ constitue une **base du réseau** *et p est la* **dimension** *ou le* **rang** *de Λ.*

Définition 1.2.3 *(sous-réseau)*
Un **sous-réseau** *de Λ est un sous-groupe de $\mathbb{R}^n$ inclu dans Λ.*
Un réseau est dit **entier** *s'il est sous-réseau de $\mathbb{Z}^n$.*

Définition 1.2.4 *(constellation)*
Une **constellation** *$\mathcal{C}$ extraite d'un réseau de points Λ est un sous-ensemble fini du réseau Λ.*

Définition 1.2.5 *(matrice génératrice)*
Les vecteurs $\mathbf{v}_1, \ldots, \mathbf{v}_p$ de la base du réseau de points forment les colonnes d'une matrice appelée **matrice génératrice** *du réseau.*

Écrivons $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$ pour $i = 1, \ldots, p$. La matrice génératrice M est alors la matrice $n \times p$ définie par

$$M = (\mathbf{v}_1, \ldots, \mathbf{v}_p) = \begin{pmatrix} v_{11} & \cdots & v_{p1} \\ \vdots & & \vdots \\ v_{1n} & \cdots & v_{pn} \end{pmatrix} . \tag{1.1}$$

Un point $\mathbf{x} = (x_1, x_2, \ldots, x_n)^t$ du réseau peut donc être écrit comme $\mathbf{x} = M\mathbf{z}$ où $\mathbf{z} = (z_1, z_2, \ldots, z_p)^t$ est un vecteur de $\mathbb{Z}^p$. Le réseau Λ peut alors être vu comme le résultat d'une transformation linéaire définie par la matrice M appliquée au réseau cubique $\mathbb{Z}^p$.

Définition 1.2.6 *(matrice de Gram)*
La **matrice de Gram** G_Λ *du réseau est la matrice définie par*

$$G_\Lambda = M^t M \tag{1.2}$$

où M est la matrice génératrice du réseau.

Les éléments $\varsigma_{ij}, i, j = 1, \ldots, p$ de la matrice de Gram d'un réseau sont les produits scalaires des paires de vecteurs de la base du réseau, à savoir $\varsigma_{ij} = \mathbf{v}_i.\mathbf{v}_j = \sum_{k=1}^{n} v_{ik} v_{jk}$. La matrice G_Λ est définie positive et symétrique, ses éléments diagonaux étant égaux aux normes au carré des vecteurs de la base.

Définition 1.2.7 *(parallélotope fondamental, volume fondamental)*
La région de l'espace $P = \{\mathbf{x} \in \mathbb{R}^n \ / \ \mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_p\mathbf{v}_p \ , \ 0 \leq a_i < 1\}$ est le **parallélotope fondamental** *du réseau. Son* **volume fondamental** *est le volume du parallélotope fondamental, noté $vol(\Lambda)$.*

Si le parallélotope fondamental d'un réseau n'est pas unique puisqu'il dépend du choix de la base du réseau, le volume fondamental est lui indépendant du choix de la base engendrant Λ. Dans le cas où $p = n$, le volume fondamental est encore égal à la valeur absolue du déterminant de la matrice génératrice $|det(M)|$, que l'on note souvent, par abus de langage, $det(\Lambda)$.

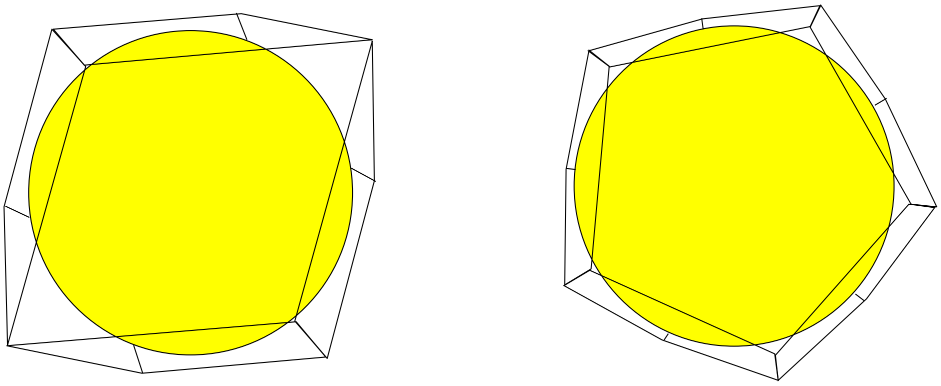
Définition 1.2.8 *(cellule de Voronoï)*
La région de l'espace associée à un point $\mathbf{u}$ *d'un réseau Λ définie par*

$$\mathcal{V}(\mathbf{u}) = \{\mathbf{x} \in \mathbb{R}^n \ / \ ||\mathbf{x} - \mathbf{u}|| \leq ||\mathbf{x} - \mathbf{y}|| \ , \ \mathbf{y} \in \Lambda\} \tag{1.3}$$

est appelée **cellule** *(ou région)* **de Voronoï**[1] *de* $\mathbf{u}$.

Les cellules de Voronoï d'un réseau pavent donc l'espace euclidien entièrement, remplissant l'espace compris entre les sphères de l'empilement. En figure 1.2-a est présenté en exemple

[1] Elle est également parfois nommée cellule de Dirichlet.



(a) : cellule de Voronoï d'une sphère dans l'empilement fcc.

(b) : dodécaèdre régulier recouvrant une sphère.

FIG. 1.2: Exemple de cellule de Voronoï en dimension 3.

la cellule de Voronoï du réseau à faces cubiques centrées, qui comporte 12 faces. À titre de comparaison, on a représenté en figure 1.2-b le dodécaèdre régulier recouvrant la sphère.

Le réseau étant un groupe additif, on a la propriété de translation des cellules de Voronoï $\mathcal{V}(\mathbf{0})+\mathbf{u} = \mathcal{V}(\mathbf{u})$. Ainsi, toutes les cellules ont-elles le même volume puisqu'elles sont égales (à une translation près) à la cellule de Voronoï de l'origine $\mathcal{V}(\mathbf{0})$. D'après la structure du réseau, le volume d'une cellule de Voronoï est égal au volume fondamental, $vol(\mathcal{V}(\mathbf{0})) = vol(\Lambda)$. De plus, le réseau étant géométriquement uniforme [32], chaque cellule de Voronoï est strictement identique aux autres, donc on parlera de "la cellule de Voronoï" du réseau Λ.

Par la suite, nous ne considérerons que des réseaux engendrés par $p = n$ vecteurs. La figure 1.3 présente un exemple de réseau en dimension 2, à savoir le réseau hexagonal A_2 ainsi que ses différents paramètres élémentaires. Continuons en introduisant des paramètres qui nous permettront de caractériser les performances de nos réseaux de points.

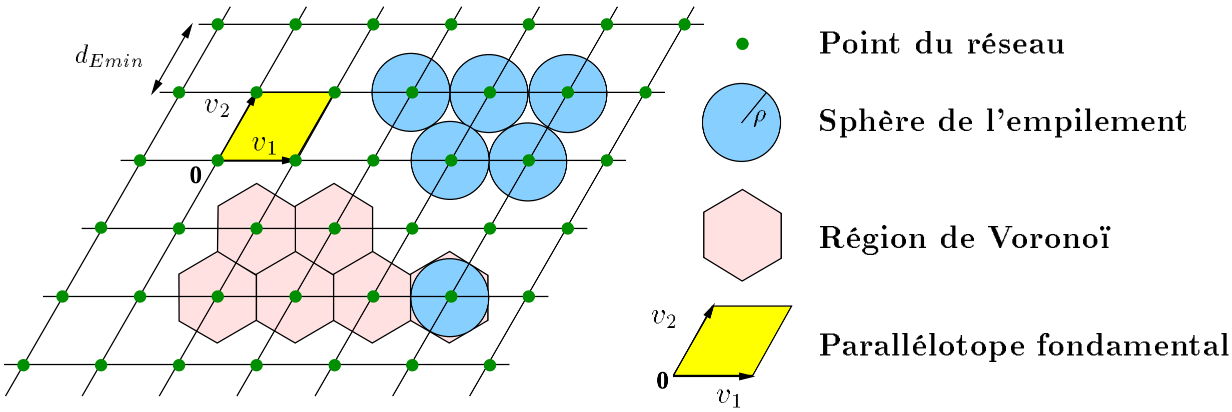


FIG. 1.3: Le réseau hexagonal A_2.

Définition 1.2.9 *(rayon d'empilement, rayon de recouvrement)*
Le **rayon d'empilement** ρ *(resp.* **rayon de recouvrement** R*) d'un réseau* Λ *est le rayon de la plus grande (resp. la plus petite) sphère inscrite (resp. circonscrite) à la région de Voronoï.*

Les sphères de l'empilement ont toutes le même rayon ρ. La distance minimale d_{Emin} entre les points du réseau est alors donnée par :

$$d_{Emin} = 2\rho \ . \tag{1.4}$$

Définition 1.2.10 *(densité d'un réseau)*
La densité de remplissage d'un réseau, ou **densité** Δ *est donnée par le rapport du volume de la sphère de rayon* ρ *sur le volume fondamental*

$$\Delta = \frac{volume\ d'une\ sphère}{volume\ fondamental} = \frac{V_n \times \rho^n}{det(\Lambda)} \ . \tag{1.5}$$

On définit également la **densité centrée** δ*, souvent plus facile à exprimer que la densité du réseau*

$$\delta = \frac{\Delta}{V_n} = \frac{\rho^n}{det(\Lambda)} \tag{1.6}$$

où V_n est le volume d'une sphère de dimension n et de rayon unité, donné par la formule

$$V_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)} = \begin{cases} \frac{\pi^{n/2}}{(n/2)!} & n\ pair \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!} & n\ impair \end{cases} \ . \tag{1.7}$$

Définition 1.2.11 *(coefficient d'erreurs)*
Le **coefficient d'erreur** $\tau(\Lambda)$ *(kissing number) d'un réseau* Λ *est le nombre de sphères tangentes à une sphère donnée.*

La valeur de $\tau(\Lambda)$ ne dépend pas de la sphère considérée en raison de la propriété de translation du réseau.

Définition 1.2.12 *(série theta)*
La **série theta** $\Theta_\Lambda(z)$ *d'un réseau* Λ *est définie*

$$\Theta_\Lambda(z) = \sum_{\mathbf{x} \in \Lambda} q^{\|\mathbf{x}\|^2} = \sum_{u=0}^{+\infty} N_u q^u \tag{1.8}$$

où $q = e^{j\pi z}$, $j = \sqrt{-1} \in \mathbb{C}$, $u \in \mathbb{R}^+$.

La série theta d'un réseau est une série de variable q, dont les coefficients N_u représentent le nombre de points d'un réseau à distance euclidienne u de l'origine.

1.2.2 Performances des réseaux de points sur le canal à bruit additif blanc gaussien

Le modèle du système de transmission utilisant une constellation extraite d'un réseau de point est présenté en figure 1.4. Des bits d'informations, générés par une source binaire non représentée, sont étiquetés avant d'être placé en entrée d'un réseau (ou, comme nous le verrons au chapitre 2, d'une rotation). Ce dernier génère un point $\mathbf{x}$ du réseau qui est émis sur un canal. Nous considérerons dans ce document deux types de canaux : le canal à bruit additif blanc gaussien et le canal de Rayleigh non sélectif à évanouissements indépendants. En sortie du canal, dont l'état (CSI) est fourni ou estimé par le récepteur, on procède à l'opération de détection et de décodage, d'où on tire les bits décodés. Pour notre calcul de performances, nous considérerons que le décodage suit le critère du maximum de vraisemblance (ML).

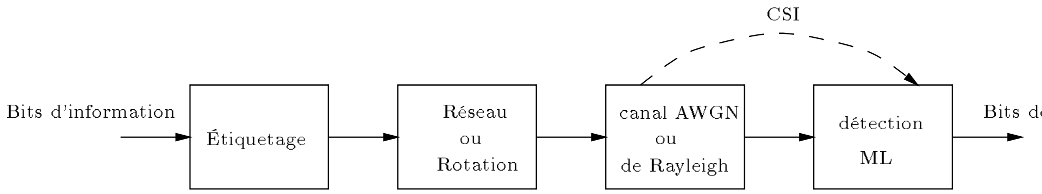


FIG. 1.4: Le système de transmission.

Sur le canal à bruit additif blanc gaussien, la probabilité d'erreur par point P_e d'un tel système décroit exponentiellement lorsque le rapport signal à bruit E_b/N_0 augmente. Pour une constellation cubique, la probabilité d'erreur est bornée par (voir annexe A.1)

$$P_e \leq \tau(\Lambda) Q\left(\sqrt{\frac{d^2_{Emin}}{\sqrt[n/2]{det(\Lambda)}} \frac{E_b}{N_0} \frac{3\eta}{2^\eta}}\right) \tag{1.9}$$

où $Q(x)$ est la fonction erreur définie par $Q(x) = \frac{1}{2}\mathrm{erfc}\left(\frac{x}{\sqrt{2}}\right) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty} e^{-x^2/2}\mathrm{d}x \leq \frac{1}{2}\,e^{-x^2/2}$ et η est l'efficacité spectrale par deux dimensions (soit le nombre de bits d'information émis par deux dimensions).

La borne sur la probabilité d'erreur nous conduit à introduire la notion de gain fondamental d'un réseau.

Définition 1.2.13 *(gain fondamental)*
On appelle **gain fondamental** *d'un réseau en dimension n le rapport*

$$\gamma(\Lambda) = \frac{d^2_{Emin}}{\sqrt[n/2]{det(\Lambda)}} = 4 \times \sqrt[n/2]{\delta} \tag{1.10}$$

où d_{Emin} est la distance euclidienne minimale de Λ, $det(\Lambda)$ son volume fondamental et δ sa densité centrée. Également appelé constante de Hermite [27], (pp. 71–74), ce rapport ne dépend que des caractéristiques du réseau (d'où son nom). Remarquons que $\gamma(\mathbb{Z}^n) = 1$: $\gamma(\Lambda)$ représente le gain du réseau Λ comparativement au réseau des entiers de même dimension. Ce gain, déterminé par la haute densité du réseau, est le facteur crucial pour la probabilité d'erreur d'un réseau sur canal AWGN : plus le gain fondamental sera grand, meilleures pourront être les performances du réseau. On note, avec la deuxième expression du gain fondamental déduite de l'équation (1.6), que la seule connaissance de la densité centrée d'un réseau nous permet de calculer le gain fondamental de Λ : cette densité est connue pour la plupart des réseaux utilisés à ce jour.

La formule (1.9) devient :

$$P_e \leq \tau(\Lambda) Q\left(\sqrt{\frac{3\eta}{2^\eta}\frac{E_b}{N_0}\gamma(\Lambda)}\right) \ . \tag{1.11}$$

Intéressons nous donc plus à ce gain fondamental $\gamma(\Lambda)$: il est invariant si nous transformons Λ par une application composée d'une rotation, d'une symétrie et d'une homothétie : en effet, il est clair que les symétries ou les rotations ne changent pas la distance minimale, ni le volume fondamental. Et par ailleurs, une homothétie de rapport a multiplie d_{Emin} par a et $det(\Lambda)$ par a^n, ce qui fait que le gain fondamental reste le même.

Lorsque la constellation $\mathcal{C}$ a une forme non cubique, le gain de $\mathcal{C}$ se trouve diminué ou augmenté suivant le moment de second ordre de la constellation. Ce moment d'ordre 2 n'est autre que l'énergie E_p (l'énergie moyenne par point) de $\mathcal{C}$. Cette énergie est très liée à la forme de la frontière de $\mathcal{C}$ dans $\mathbb{R}^n$. On peut donc définir un nouveau gain, dit gain total de la constellation, qui tient compte des caractéristiques fondamentales du réseau Λ et de la forme de la constellation.

Définition 1.2.14 *(gain de forme, gain total)*
Le **gain total** *$\gamma(\mathcal{C})$ d'une constellation $\mathcal{C}$ issue d'un réseau de points Λ est le produit du gain fondamental $\gamma(\Lambda)$ par un coefficient $\gamma_s(\mathcal{C})$ appelé* **gain de forme***.*

$$\gamma(\mathcal{C}) = \gamma(\Lambda) \times \gamma_s(\mathcal{C}) \ . \tag{1.12}$$

Par définition, le gain de forme d'une constellation cubique est égal à 1. La forme sphérique minimise l'énergie moyenne de $\mathcal{C}$ en raison de la répartition homogène des distances à l'intérieur d'une hypersphère. Ainsi, le gain de forme $\gamma_s(\mathcal{C})$ est-il maximal lorsque $\mathcal{C}$ possède une forme sphérique. Il s'obtient par le rapport (1.13) (avec utilisation de l'intégrale de Dirichlet pour le calcul de l'énergie moyenne d'une constellation sphérique [16])

$$\gamma_s(\mathcal{C})_{max} = \frac{||\mathbf{x}||^2_{cube}}{||\mathbf{x}||^2_{sphère}} = \frac{\pi \times (n+2)}{12 \times \sqrt[n/2]{\Gamma(n/2+1)}} \ . \tag{1.13}$$

Le tableau 1.1 montre quelques valeurs de $\gamma_s(\mathcal{C})_{max}$ pour différentes dimensions. En appliquant la formule de Stirling ($\sqrt[n]{n!} \sim n/e$), on peut montrer que le gain tend en fait vers

$\pi e/6 \approx 1.533$ dB lorsque n tend vers l'infini. On constate donc que le gain de forme est relativement faible comparé au gain fondamental, ce qui explique pourquoi les constellations sphériques, difficiles à réaliser sont peu utilisées et se voient préférer les constellations cubiques. Par la suite, nous ne considérerons dans ce document que ces constellations.

n	$\gamma_s(\mathcal{C})_{max}$	$\gamma_s(\mathcal{C})_{max}$ (dB)
2	1.0471976	0.200
3	1.0827159	0.345
4	1.1107201	0.456
5	1.1335383	0.544
8	1.1828123	0.729
16	1.2518465	0.976
24	1.2870060	1.096
32	1.3089071	1.169
48	1.3352909	1.256
64	1.3509280	1.306
128	1.3793392	1.397
256	1.3974023	1.453

TAB. 1.1: Quelques valeurs du gain de forme maximal $\gamma_s(\mathcal{C})_{max}$ en fonction de la dimension.

1.2.3 Performances des réseaux de points sur le canal avec évanouissement de Rayleigh

Le système de transmission présenté en figure 1.4 utilisé sur un canal de Rayleigh admet pour borne supérieure de la probabilité d'erreur par paire, i.e. celle de décoder $\mathbf{d} \in \Lambda$ alors que $\mathbf{c} \in \Lambda$ a été effectivement émis lorsque l'on fait abstraction des autres points du réseau (voir annexe A.2)

$$P(\mathbf{c} \rightarrow \mathbf{d}) \leq \frac{1}{2} \prod_{i=1}^{n} \frac{1}{1 + \frac{(c_i - d_i)^2}{8N_0}} \tag{1.14}$$

donc, à haut rapport signal à bruit,

$$P(\mathbf{c} \rightarrow \mathbf{d}) \leq \frac{1}{2} \prod_{c_i \neq d_i} \frac{1}{\frac{(c_i - d_i)^2}{8N_0}} = \frac{1}{2} \frac{1}{\left(\frac{\eta}{8} \frac{E_b}{N_0}\right)^{\ell} d_p^{(\ell)}(\mathbf{c}, \mathbf{d})^2} \tag{1.15}$$

où $d_p^{(\ell)}(\mathbf{c}, \mathbf{d})$ est la distance produit-ℓ normalisée entre deux points $\mathbf{c}$ et $\mathbf{d}$ lorsque ceux-ci diffèrent en ℓ composantes.

$$d_p^{(\ell)}(\mathbf{c}, \mathbf{d})^2 = \frac{\prod_{c_i \neq d_i} (c_i - d_i)^2}{(E/n)^{\ell}} \tag{1.16}$$

où le facteur de normalisation E correspond à deux points soit $E = \frac{\eta}{n} E_b$.

Définition 1.2.15 *(diversité)*
L'ordre de diversité ou **diversité** *L d'un réseau Λ est le nombre minimal de composantes dont deux points quelconques* $\mathbf{c}$ *et* $\mathbf{d}$ *diffèrent*

$$L = min_{\mathbf{c},\mathbf{d}\in\Lambda} d_H(\mathbf{c}, \mathbf{d}) \ . \tag{1.17}$$

L'ensemble des nombres de composantes dont deux points quelconques d'un réseau peuvent différer est appelé **distribution de diversités** *du réseau.*

Utilisant la borne de l'union, on peut donc exprimer la probabilité d'erreur pour une constellation de dimension n extraite du réseau Λ comme

$$P_e \leq \sum_{\mathbf{c},\mathbf{d}\in\Lambda,\mathbf{c}\neq\mathbf{d}} P(\mathbf{c} \rightarrow \mathbf{d}) \ . \tag{1.18}$$

Alors, en remplaçant l'expression de la probabilité d'erreur par paire par sa borne supérieure obtenue dans l'inéquation (1.15) on obtient

$$P_e \leq \frac{1}{2} \sum_{\ell=L}^{n} \frac{K_\ell}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^\ell} \tag{1.19}$$

où $K_\ell = \sum_{d_p^{(\ell)}} \frac{A_{d_p^{(\ell)}}}{(d_p^{(\ell)})^2}$, avec $A_{d_p^{(\ell)}}$ le nombre de points $\mathbf{d}$ à distance produit-ℓ de $\mathbf{c}$. On notera que la série en K_l peut être interprétée comme une série theta du réseau, pour peu qu'on considère la distance produit-ℓ au lieu de la distance euclidienne [79].

Asymptotiquement, la borne sur le logarithme de la probabilité d'erreur P_e décroit linéairement avec une pente L.

1.3 Décodage par sphères

De nombreux algorithmes existent, spécialisés ou non, permettant de décoder les réseaux de points sur le canal AWGN. Citons à titre d'exemple les travaux de Conway *et al.* [26], Sun *et al.* [68], Vardy [75], ou encore l'utilisation de l'algorithme sous-optimal GMD (Generalized minimum distance algorithm [33]). Développés pour le canal gaussien, ces algorithmes reposent principalement sur le décodage souple de codes linéaires, utilisant un treillis ou un calcul sur une valeur de confiance. Applicables au canal de Rayleigh non sélectif, pour lequel les évanouissements multiplient tout simplement les composantes des points émis du réseau, ces algorithmes ne peuvent être utilisés lorsque le réseau est tourné

avant de subir l'évanouissement (par application d'une rotation, comme nous le verrons au chapitre 2). Dans ce cas, du fait de la corrélation liant les symboles et leurs composantes entre eux, le décodage par étages ou le décodage souple des codes correcteurs d'erreurs ne sont plus possibles.
Le seul algorithme qui reste applicable dans tous les cas est le décodeur universel par sphères [78] reposant sur le critère du maximum de vraisemblance (ML). Il est utilisable aussi bien sur le canal AWGN que sur les canaux à évanouissement de Rayleigh, et sa complexité est indépendante de la taille de la constellation utilisée. Néanmoins, sa complexité limite son utilisation à des dimensions du réseau inférieures ou égales à 32. On notera que tout récemment a été proposé une version modifiée de cet algorithme pour le décodage des systèmes d'accès multiple par séquences directes [20][21].

1.3.1 Décodage par sphères en présence d'un bruit blanc gaussien

Plaçons nous tout d'abord dans le cas où le canal est à bruit blanc additif gaussien. Le décodage à maximum de vraisemblance d'un réseau de points Λ quelconque en dimension n utilisé sur ce canal correspond à la recherche, parmi tous les points du réseau, de celui qui est le plus proche du vecteur reçu, soit de celui qui minimise la métrique

$$m(\mathbf{y}|\mathbf{x}) = \|\mathbf{y} - \mathbf{x}\|^2 = \sum_{i=1}^{n} |y_i - x_i|^2 \qquad (1.20)$$

où $\mathbf{x}$ est le point du réseau émis sur le canal, $\mathbf{y} = \mathbf{x} + \mathbf{b}$ le point reçu et $\mathbf{b} = (b_1, \ldots, b_n)^t$ le bruit sur le canal dont les composantes b_i sont des variables aléatoires gaussiennes de moyenne nulle et de variance $\sigma^2 = N_0$. L'ensemble des points du réseau est $M\mathbb{Z}^n$ ou $\{\mathbf{x} \in \mathbb{R}^n | \exists \mathbf{u} \in \mathbb{Z}^n \mathbf{x} = M\mathbf{u}\}$, où M est la matrice génératrice de Λ et où $\mathbf{u} = (u_1, \ldots, u_n)$ est le vecteur à composantes entières associé aux bits d'information.

L'algorithme de décodage par sphères se limite aux points du réseau Λ se trouvant dans une sphère de rayon $\sqrt{C}$ centrée sur le point reçu, comme illustré en figure 1.5.

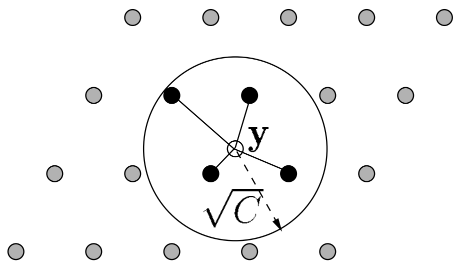


FIG. 1.5: Représentation géométrique de l'algorithme de décodage par sphères.

Le décodeur recherche donc le vecteur $\mathbf{w}$ de plus petite norme possible dans le réseau translaté $\mathbf{y} - \Lambda$ de l'espace euclidien $\mathbb{R}^n$:

$$min_{\mathbf{x}\in\Lambda}\|\mathbf{y} - \mathbf{x}\| = min_{\mathbf{w}\in\mathbf{y}-\Lambda}\|\mathbf{w}\| \ . \qquad (1.21)$$

Définissons les notations suivantes

$$\mathbf{x} = M\mathbf{u} \qquad \mathbf{y} = M\boldsymbol{\rho} \qquad \mathbf{w} = M(\boldsymbol{\rho} - \mathbf{u}) = M\boldsymbol{\xi}$$

avec $\mathbf{u} \in \mathbb{Z}^n$, $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_n) \in \mathbb{R}^n$, $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbb{R}^n$.

Du fait de la présence du bruit sur le canal, les vecteurs $\boldsymbol{\rho}$ et $\boldsymbol{\xi}$ sont en effet des vecteurs réels. De plus, comme $\mathbf{w} = \mathbf{y} - \mathbf{x}$, on a pour tout indice $i, i = 1, \ldots, n$ $\xi_i = \rho_i - u_i$. Le point $\mathbf{w}$ est un point du réseau dont les coordonnées sont exprimées dans le repère translaté centré sur le point reçu $\mathbf{y}$. On veut que $\mathbf{w}$ appartienne à une sphère centrée en $\mathbf{y}$ (i.e. en $\mathbf{0}$ dans le nouveau repère) et de rayon égal à $\sqrt{C}$, ce qui nous amène l'inéquation en ξ :

$$\|\mathbf{w}\|^2 = F(\boldsymbol{\xi}) = \boldsymbol{\xi}^t M^t M \boldsymbol{\xi} = \boldsymbol{\xi}^t G_\Lambda \boldsymbol{\xi} = \sum_{i=1}^{n} \sum_{j=1}^{n} \varsigma_{ij} \xi_i \xi_j \leq C \ . \tag{1.22}$$

Dans ce nouveau système de coordonnées, la sphère de centre $\mathbf{y}$ et de rayon au carré égal à C est transformée en un ellipsoïde centré sur l'origine définie par la forme bilinéaire $F(\xi)$. La factorisation de Cholesky de la matrice de Gram $G_\Lambda = M^t M$ [25] donne $G_\Lambda = R^t R$, où $R = (r_{ij})_{i,j=1,\ldots,n}$ est une matrice triangulaire supérieure, d'où

$$F(\boldsymbol{\xi}) = \boldsymbol{\xi}^t R^t R \boldsymbol{\xi} = \|\boldsymbol{\xi} R\|^2 = \sum_{i=1}^{n} \left(r_{ii}\xi_i + \sum_{j=i+1}^{n} r_{ij}\xi_j \right)^2 \leq C \ . \tag{1.23}$$

En posant

$$f_{ii} = r_{ii}^2 \ , \quad i = 1, \ldots, n$$

$$f_{ij} = \frac{r_{ij}}{r_{ii}} \ , \quad i = 1, \ldots, n \ , \quad j = i+1, \ldots, n$$

on obtient

$$F(\boldsymbol{\xi}) = \sum_{i=1}^{n} f_{ii} \left(\xi_i + \sum_{j=i+1}^{n} f_{ij}\xi_j \right)^2 \leq C \ . \tag{1.24}$$

En s'intéressant tout d'abord à ξ_n et en poursuivant par les $\xi_i, i = n-1, \ldots, 1$, on va déterminer un systèmes de n équations déterminant les limites de l'ellipsoïde :

$$\begin{aligned} f_{nn}\xi_n &\leq C \\ f_{n-1,n-1}\left(\xi_{n-1} + f_{n,n-1}\xi_n\right)^2 + f_{nn}\xi_n^2 &\leq C \\ \forall k, 1 \leq k \leq n \ , \quad \sum_{i=k}^{n} f_{ii} \left(\xi_i + \sum_{j=i+1}^{n} f_{ji}\xi_j \right)^2 &\leq C \ . \end{aligned} \tag{1.25}$$

Les bornes données par l'équation (1.25) nous permettent d'établir la relation générale pour la $i^{ème}$ composante u_i [77][78]

$$\left\lceil -\sqrt{\frac{C}{f_{nn}}} + \rho_n \right\rceil \leq u_n \leq \left\lfloor \sqrt{\frac{C}{f_{nn}}} + \rho_n \right\rfloor$$

$$\left\lceil -\sqrt{\frac{C - f_{nn}\xi_n^2}{f_{n-1,n-1}}} + \rho_{n-1} + f_{n-1,n}\xi_n \right\rceil \leq u_{n-1} \leq \left\lfloor \sqrt{\frac{C - f_{nn}\xi_n^2}{f_{n-1,n-1}}} + \rho_{n-1} + f_{n-1,n}\xi_n \right\rfloor$$

$$\left\lceil -\sqrt{\frac{1}{f_{ii}}\left(C - \sum_{\ell=i+1}^{n} f_{\ell\ell}\left(\xi_\ell + \sum_{j=\ell+1}^{n} f_{\ell j}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} f_{ij}\xi_j \right\rceil \leq u_i$$

$$u_i \leq \left\lfloor \sqrt{\frac{1}{f_{ii}}\left(C - \sum_{\ell=i+1}^{n} f_{\ell\ell}\left(\xi_\ell + \sum_{j=\ell+1}^{n} f_{\ell j}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} f_{ij}\xi_j \right\rfloor \tag{1.26}$$

où $\lceil x \rceil$ est le plus petit entier supérieur à x et $\lfloor x \rfloor$ le plus grand entier inférieur à x.

Les bornes trouvées dans les inéquations de la formule (1.26) nous apprennent que le décodeur par sphères fonctionne avec n compteurs, 1 pour chacun des nombres u_i. Il suffit ensuite de faire varier les valeurs des différents compteurs à l'intérieur des bornes trouvées, en tenant compte du fait que celles-ci dépendent des valeurs des autres compteurs. En pratique, ces bornes sont mises à jour de façon récursive [78]. L'intérêt de cette méthode est que les vecteurs dont la norme est supérieure au rayon donné ne seront jamais testés : la complexité de cet algorithme est donc indépendante de la taille de la constellation considérée. Cette méthode permet donc une estimation ML tout en évitant de façon drastique le nombre de points à tester, en particulier lorsque la dimension augmente.

Le choix du rayon de recherche initial $\sqrt{C}$ est un point crucial de l'algorithme : afin d'être sûrs de toujours trouver un point du réseau à l'intérieur de la sphère nous devons choisir $\sqrt{C}$ égal au rayon de recouvrement du réseau. Pour cela, il est par exemple possible de le choisir égal à la borne supérieure de Rogers [27] (p. 40)

$$\sqrt{C} = \sqrt[n]{(n\log_e n + n\log_e\log_e n + 5n)\frac{\sqrt{det(\Lambda)}}{V_n}} \tag{1.27}$$

où V_n est le volume d'une sphère de rayon 1 en dimension n donné par la formule (1.7) et où le volume fondamental du réseau Λ peut être aisément calculé comme la racine carrée du déterminant de sa matrice de Gram.

En pratique, on ajuste au fur et à mesure le choix de C, le mettant à jour avec la dernière norme euclidienne calculée pour un point de l'ellipsoïde.

Enfin on remarquera que, contrairement aux réseaux de points, la constellation utilisée étant finie, des effets de bord pourront apparaître : au cours de la recherche, il ne faudra pas sélectionner les points qui appartiennent au réseau mais pas à la constellation. La complexité de ce test supplémentaire dépend de la forme de la constellation. Par exemple pour les constellations cubiques, il s'agit seulement de vérifier que toutes les composantes du vecteur appartiennent à un certain intervalle.

1.3.2 Décodage par sphères en présence d'un évanouissement de Rayleigh

Le canal de Rayleigh non sélectif à évanouissements indépendants est une généralisation possible du canal AWGN : il prend en compte la variation de la puissance instantanée reçu et la modélise par des évanouissements indépendants. Le signal reçu s'écrit donc :

$$\mathbf{y} = \boldsymbol{\alpha} \odot \mathbf{x} + \mathbf{b}$$

où $\odot$ représente le produit composante par composante, $\mathbf{x}$ est le vecteur émis et $\mathbf{b} = (b_1, \ldots, b_n)^t$ le bruit sur le canal dont les composantes b_i sont des variables aléatoires gaussiennes de moyenne nulle et de variance $\sigma^2 = N_0$. Les coefficients d'évanouissement $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ ont un moment du second ordre unitaire et leur densité de probabilité est donnée par $p(\alpha_k) = 2\alpha_k \exp(-\alpha_k^2), k = 1, \ldots, n$. Dans la réalité, les évanouissements ne sont pas indépendants : l'état du canal à un instant donné dépend des états aux instants précédents. L'indépendance est alors obtenue en ajoutant un entrelaceur au niveau de l'émetteur : on suppose que la répartition temporelle des bits d'information consécutifs obtenue par l'entrelaceur est suffisamment bonne pour que l'hypothèse d'indépendance soit valide.

Dans ce cas, lorsque le récepteur connait parfaitement l'état du canal (CSI), le décodage ML correspond à la minimisation de la métrique

$$m(\mathbf{y}|\mathbf{x}, \boldsymbol{\alpha}) = \|\mathbf{y} - \boldsymbol{\alpha} \odot \mathbf{x}\|^2 = \sum_{i=1}^{n} |y_i - \alpha_i x_i|^2 \ . \tag{1.28}$$

Soit M la matrice génératrice du réseau Λ considéré. Nous pouvons alors définir le réseau Λ_c de matrice génératrice M_c

$$M_c = M\mathbf{D}(\alpha_1, \ldots, \alpha_n)$$

où $\mathbf{D}(\alpha_1, \ldots, \alpha_n)$ est la matrice diagonale ayant sur sa diagonale principale les valeurs $\alpha_1, \ldots, \alpha_n$.

Le nouveau réseau Λ_c associé à la matrice M_c peut être vu comme le réseau initial considéré dans un repère dans lequel chaque composante a été multipliée par un facteur α_i. Un point de Λ_c s'écrit en effet

$$\mathbf{x}^{(c)} = (x_1^{(c)}, \ldots, x_n^{(c)}) = (\alpha_1 x_1, \ldots, \alpha_n x_n) \ .$$

La métrique à minimiser pour décoder ce réseau est donc, d'après ce qui a été vu au paragraphe précédent,

$$m(\mathbf{y}|\mathbf{x},\boldsymbol{\alpha}) = \sum_{i=1}^{n} |y_i - x_i^{(c)}|^2 \ . \tag{1.29}$$

Ceci signifie [78] que nous pouvons appliquer directement l'algorithme de décodage présenté au paragraphe précédent au réseau Λ_c avec pour point reçu $\mathbf{y}$. Le point décodé $\hat{\mathbf{x}}^{(\mathbf{c})} \in \Lambda_c$ aura les mêmes composantes entières $\hat{\mathbf{u}}$ que le point $\hat{\mathbf{x}} \in \Lambda$.

La complexité supplémentaire introduite par les évanouissements vient du fait que pour chaque point reçu il faut travailler avec un nouveau réseau Λ_c. Il faut donc effectuer une nouvelle décomposition de Cholesky de la matrice de Gram pour chaque nouveau réseau Λ_c. Il faut également calculer l'inverse de la matrice du réseau Λ_c $M_c^{-1} = \mathbf{D}(1/\alpha_1, \ldots, 1/\alpha_n)M^{-1}$ pour calculer les valeurs des coefficients ρ_i, mais ceci ne demande qu'une opération simple de multiplication puisque la matrice M^{-1} peut être précalculée une fois pour toutes.

À nouveau, le choix du rayon C est un point crucial : en effet, lorsque la transmission a lieu dans un milieu à forts évanouissements, le choix d'un grand rayon initial impliquera que de nombreux points vont se trouver à l'intérieur de la sphère et donc le décodage pourra être très lent. Pour éviter cet écueil, il est important de pouvoir adapter le choix de C en fonction des valeurs des coefficients d'évanouissement α_i.

Ayant à notre disposition un algorithme permettant de décoder les réseaux de points tant sur le canal AWGN que sur le canal de Rayleigh non sélectif, nous allons voir comment construire des réseaux de points performants.

1.4 Construction des réseaux de points

Les codes correcteurs d'erreurs peuvent servir à construire des empilements de sphères très denses dans l'espace euclidien $\mathbb{R}^n$ [27]. Bien entendu, d'autres méthodes existent, comme la construction par découpage, par couches ou à partir des corps de nombres (comme nous en verrons un exemple au chapitre 2). Pour plus de précisions sur ces autres méthodes de construction, on se reportera à l'ouvrage encyclopédique de Conway et Sloane [27]. Nous considérerons ici les différentes méthodes les plus classiques de construction, à partir de codes linéaires binaires, soit la construction A, la construction B et la construction D. On notera que si la construction C n'est pas abordée ici, c'est parce que les empilements qu'elle permet de construire ne sont pas en général des réseaux.

À titre d'exemple, le tableau 1.2 fournit une liste des réseaux de points les plus célèbres [27]. Parmi les plus importants on notera le réseau fcc D_3, le réseau de Schalfli D_4, le réseau de Gosset E_8, le réseau de Coxeter-Todd K_{12}, le réseau de Barnes-Wall BW_{16} ou enfin le fameux réseau Leech Λ_{24}. Les caractéristiques principales de ces réseaux s'y trouvent, et on peut ainsi voir que la densité Δ est une fonction décroissante de la dimension n alors que le coefficient d'erreur $\tau(\Lambda)$ en est une fonction croissante.

n	Λ	Δ	δ	γ_{dB}	$\tau(\Lambda)$
1	$\Lambda_1 = A_1$	1.0	0.5	0.0	2
2	$\Lambda_2 = A_2$	0.90690	0.28868	0.62	6
3	$\Lambda_3 = D_3$	0.74048	0.17678	1.00	12
4	$\Lambda_4 = D_4$	0.61685	0.12500	1.51	24
5	$\Lambda_5 = D_5$	0.46526	0.08839	1.81	40
6	$\Lambda_6 = E_6$	0.37295	0.07217	2.22	72
7	$\Lambda_7 = E_7$	0.29530	0.06250	2.58	126
8	$\Lambda_8 = E_8$	0.25367	0.06250	3.01	240
9	Λ_9	0.14577	0.04419	3.01	272
10	Λ_{10}	0.09202	0.03608	3.14	336
11	K_{11}	0.06043	0.03208	3.30	432
12	Λ_{12}	0.04173	0.03125	3.51	648
12	K_{12}	0.04945	0.03704	3.64	756
13	K_{13}	0.02921	0.03208	3.72	918
14	Λ_{14}	0.02162	0.03608	3.96	1422
15	Λ_{15}	0.01686	0.04419	4.21	2340
16	$\Lambda_{16} = BW_{16}$	0.01471	0.06250	4.52	4320
17	Λ_{17}	0.008811	0.06250	4.60	5346
18	Λ_{18}	0.005928	0.07217	4.75	7398
19	Λ_{19}	0.004121	0.08839	4.91	10668
20	Λ_{20}	0.003226	0.12500	5.12	17400
24	Λ_{24}	0.001930	1.0	6.02	196560
32	Λ_{32}	—	0	6.02	208320
32	BW_{32}	—	0	6.02	146880
32	Q_{32}	—	1.359	6.28	261120
36	Λ_{36}	—	1	6.19	234456
48	Λ_{48}	—	12	7.53	—
64	BW_{64}	—	16	7.53	9694080
64	Q_{64}	—	18.719	7.78	2611200
64	P_{64c}	—	22	8.09	—
128	BW_{128}	—	64	9.03	1260230400
128	P_{128b}	—	85	10.02	—
128	$\eta(E_8)$	—	88	10.16	—
256	BW_{256}	—	192	10.54	325139443200

Tab. 1.2: Quelques réseaux de points et leurs caractéristiques. La dimension n, le nom Λ, la densité Δ, la densité centrée δ ($log_2(\delta)$ *pour* $n \geq 32$), le gain en dB γ_{dB} et le coefficient d'erreur $\tau(\Lambda)$.

1.4.1 Constructions A, B et D

Construction A

Il s'agit de l'une des méthodes les plus simples de construction d'un réseau de points. Elle repose sur l'utilisation d'un code linéaire q-aire (en pratique, on prend toujours $q = 2$).

Définition 1.4.1 *(construction A)*
C_0 étant un code linéaire binaire de longueur n, dimension k et distance minimale de Hamming d, on construit un réseau Λ par **construction A** *de la façon suivante : $\mathbf{x} = (x_1, \ldots, x_n)$ est un point du réseau si et seulement si le n-uple $(x_1, \ldots, x_n)$ est congru modulo-2 à un mot du code C_0. On écrit*

$$\Lambda = C_0 + 2\mathbb{Z}^n \ . \tag{1.30}$$

Il est possible d'interpréter cette construction en utilisant la décomposition binaire d'un entier [16].

Définition 1.4.2 *Soit $e \in \mathbb{Z}$. La* **décomposition binaire** *de l'entier e correspond à la projection de e sur la base formée par les puissances de 2, soit*

$$e = \sum_{j=0}^{+\infty} e_j 2^j \ , \quad e_j \in \{0,1\} \ . \tag{1.31}$$

La notation binaire complémentaire est utilisée pour écrire les entiers négatifs.

On peut alors construire la matrice des coordonnées d'un point $\mathbf{x} \in \mathbb{Z}^n$.

Définition 1.4.3 *(Matrice des Coordonnées)*
Soit $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. La **matrice des coordonnées** *de $\mathbf{x}$ est la matrice semi-infinie dont les colonnes sont composées des décompositions binaires des composantes x_i de $\mathbf{x}$. Les lignes de cette matrice, toutes identiques à partir d'un certain rang, sont dites* **ligne mod-2^i**.

Exemple

Considérons le vecteur $\mathbf{x} = (4, 3, 2, 1, 0, -1, -2, -3) \in \mathbb{Z}^8$. La matrice des coordonnées de $\mathbf{x}$ s'écrit

$$\begin{array}{c} \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \end{array} \begin{array}{l} \rightarrow \ ligne\ mod - 2 \\ \rightarrow \ ligne\ mod - 4 \\ \rightarrow \ ligne\ mod - 8 \\ \rightarrow \ ligne\ mod - 16 \\ \ldots\ldots \end{array}$$

Un point $\mathbf{x}$ appartient donc au réseau défini par construction A si et seulement si sa ligne mod-2 appartient au code C_0.

Différentes caractéristiques d'un réseau Λ issu de la construction A à l'aide d'un code linéaire C_0 de longueur n, de dimension k et de distance de Hamming minimale d, noté (n,k,d) sont aisément calculables,

la densité centrée $\qquad \delta = 2^k \rho^n 2^{-n}$

le rayon d'empilement $\qquad \rho = \frac{1}{2} min(2, \sqrt{d})$

le coefficient d'erreurs $\qquad \tau(\Lambda) = \begin{cases} 2^d A_d & si\ d < 4 \\ 2n + 16A_4 & si\ d = 4 \\ 2n & si\ d > 4 \end{cases}$

où A_i est le nombre de mots de poids i dans C_0.

Lorsque la matrice génératrice du code C_0 est de forme systématique, $[I_k|P]$, la matrice génératrice du réseau Λ obtenu par construction A est

$$M = \begin{pmatrix} I_k & P \\ 0 & 2I_{n-k} \end{pmatrix} . \tag{1.32}$$

Cette construction fournit des réseaux de points efficaces pour des dimensions $n \leq 15$. Un exemple de réseaux obtenus par construction A est la famille des réseaux *checkerboard*, notés $D_n = (n, n-1, 2) + 2\mathbb{Z}^n$, obtenus à partir des codes de parité $(n, n-1, 2)$. Parmi ces réseaux, on notera le réseau fcc D_3 et le réseau de Schlafli D_4. Les réseaux D_n sont les plus denses en dimensions $n = 3, 4, 5$ seulement. On notera également que les réseaux les plus denses en dimension 6, 7 et 8 soit E_6, E_7 et E_8 s'obtiennent également par construction A.

Nous donnons en exemple la matrice du réseau fcc

$$M_{D_3} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} . \tag{1.33}$$

Construction B

La construction B ajoute une contrainte supplémentaire sur la ligne mod-4 de la matrice de coordonnées.

Définition 1.4.4 *(construction B)*
C_0 étant un code linéaire binaire de longueur n, dimension k et distance minimale de Hamming d dont tous les mots de codes sont de poids pair, et C_1 étant le code de parité $(n, n-1, 2)$, on construit un réseau Λ par **construction B** *de la façon suivante :* $\mathbf{x} =$

$(x_1, \ldots, x_n)$ est un point du réseau si et seulement si le n-uple $(x_1, \ldots, x_n)$ est congru modulo-2 à un mot du code C_0 et si $\sum_{i=1}^{n} x_i$ est divisible par 4. Lorsque tous les mots de C_0 sont divisibles par 4, on écrit

$$\Lambda = C_0 + 2C_1 + 4\mathbb{Z}^n \ . \tag{1.34}$$

On notera que l'on a $C_0 \subset C_1$ puisque les poids de C_0 sont divisibles par 2. De plus, différentes caractéristiques d'un réseau Λ issu de la construction A à l'aide d'un code linéaire (n, k, d) sont aisément calculables,

la densité centrée $\qquad \delta = 2^k \rho^n 2^{-n-1}$

le rayon d'empilement $\qquad \rho = \frac{1}{2} min(\sqrt{8}, \sqrt{d})$

le coefficient d'erreurs $\qquad \tau(\Lambda) = \begin{cases} 2^{d-1} A_d & si\ d < 8 \\ 2n(n-1) + 128 A_8 & si\ d = 8 \\ 2n(n-1) & si\ d > 8 \end{cases}$

où A_i est le nombre de mots de poids i dans C.

Cette construction est efficace pour des dimensions comprises entre 8 et 24. Grâce à cette construction, nous pouvons par exemple obtenir une nouvelle version du réseau E_8, mais aussi le réseau Λ_9 (le plus dense en dimension 9). En dimension 16, en utilisant le code de Reed-Muller d'ordre 1 on obtient $\Lambda_{16} = 4\mathbb{Z}^{16} + 2(16, 15, 2) + (16, 5, 8)$. On notera que ce réseau est aussi le réseau de Barnes-Wall en dimension 16, comme nous le verrons au paragraphe 1.4.2.

$$M_{\Lambda_{16}} = \left[\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\
0 & & & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & & & & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\
0 & & & & & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\
0 & & & & & & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & & & & & & & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & & & & & & & & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\
0 & & & & & & & & & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\
0 & & & & & & & & & & 0 & 2 & 0 & 0 & 0 & 2 \\
0 & & & & & & & & & & & 0 & 2 & 2 & 2 & 2 \\
0 & & & & & & & & & & & & 0 & 2 & 0 & 2 \\
0 & & & & & & & & & & & & & 0 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4
\end{array}\right] \tag{1.35}$$

Construction D

Généralisant une construction proposée par Barnes et Wall [3], la construction D a été initialement proposée par Barnes et Sloane [4] et s'applique sur une famille de a codes linéaires binaires emboîtés pour produire un réseau dans $\mathbb{R}^n$.

Définition 1.4.5 *(construction D)*
Soit $\gamma = 1$ ou 2. Soient $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_{a-1}$ a codes linéaires binaires, où le code C_i est de longueur n, de dimension k_i et de distance minimale de Hamming $d_i \geq 4^i/\gamma$. Soit également $C_a = (n, k_n = n, 1)$ le code universel sur le corps de Galois $GF(2)$.
Choisissons une base $\mathbf{c}_1, \ldots, \mathbf{c}_n$ de $GF_n(2)$ telle que chaque ensemble de vecteurs $\mathbf{c}_1, \ldots, \mathbf{c}_{k_i}$ forme une base de C_i (familles emboîtées), pour $i = 0, \ldots, a$.
Le réseau de points $\Lambda \subset \mathbb{R}^n$ obtenu par **construction D** *est alors formé par tous les points de la forme*

$$\sum_{i=0}^{a-1} 2^i \sum_{j=1}^{k_i} u^{(i)}[j].c_j + 2^a L \tag{1.36}$$

où $L \in \mathbb{Z}^n$ et $u^{(i)}[j] \in \{0, 1\}$.
On écrit

$$\Lambda = C_0 + 2C_1 + \cdots + 2^{a-1}C_{a-1} + 2^a\mathbb{Z}^n \ . \tag{1.37}$$

Le volume fondamental du réseau Λ, de matrice génératrice M construite à partir de la base $c_1, c_2, \ldots, c_n$, est alors donné par

$$det(\Lambda) = 2^{an - \sum_{i=0}^{a-1} k_i} \ . \tag{1.38}$$

Cette construction est une généralisation des constructions A et B. Il suffit en effet de prendre $a = 1$ pour retrouver la construction A et $a = 2$ pour retrouver la construction B. Elle permet quant à elle de construire des réseaux performants en grandes dimensions. On notera que c'est la propriété d'emboitement de ces codes linéaires qui assure que l'empilement obtenu par construction D est un réseau. Les exemples de réseau précédents peuvent donc également être considérés comme des réseaux obtenus par construction D.

1.4.2 Les réseaux de Barnes-Wall

Construction des réseaux de Barnes-Wall

Nous allons à présent nous intéresser à une famille particulière de réseaux obtenus par construction D, à savoir les réseaux de Barnes-Wall. En effet, d'après [31], on peut utiliser des codes de Reed-Müller pour construire de nombreux réseaux en suivant les équations suivantes :

$$\Lambda(r,m) = 2^{\frac{m-r}{2}}\mathbb{Z}^{2n} + \sum_{\substack{r+1 \leq r' \leq m \\ m-r' \text{ impair}}} RM(r',m+1)2^{\frac{r'-1}{2}} \quad \text{pour } m-r \text{ impair} \tag{1.39}$$

$$\Lambda(r,m) = 2^{\frac{m-r+1}{2}}\mathbb{Z}^{2n} + \sum_{\substack{r+1 \leq r' \leq m \\ m-r' \text{ pair}}} RM(r',m+1)2^{\frac{r'-1}{2}} \quad \text{pour } m-r \text{ pair} \tag{1.40}$$

où la dimension n est donnée par $n = 2^m$ et $RM(r,m)$ désigne le code de Reed-Müller d'ordre r et de longueur m.

En 1959, Barnes et Wall ont isolé une série de réseaux, appelés BW_n, qui en dimension $n = 2^m$ vérifiaient la propriété suivante :

$$\frac{1}{n}\log_2 \Delta \underset{n\to\infty}{\sim} -\frac{1}{4}\log_2 n \ .$$

Il a également été remarqué que les formules des réseaux de Barnes-Wall sont obtenues pour le cas $r = 0$ de la formule générale de construction de réseaux à partir des codes de Reed-Müller. Ainsi obtient-on :

$$\left\{\begin{array}{lcl}
BW_4 & = & 2\mathbb{Z}^4 + (4,3,2) \\
BW_8 & = & 2\mathbb{Z}^8 + (8,4,4) \\
BW_{16} & = & 4\mathbb{Z}^{16} + 2(16,15,2) + (16,5,8) \\
BW_{32} & = & 4\mathbb{Z}^{32} + 2(32,26,4) + (32,6,16) \\
BW_{64} & = & 8\mathbb{Z}^{64} + 4(64,63,2) + 2(64,42,8) + (64,7,32) \\
BW_{128} & = & 8\mathbb{Z}^{128} + 4(128,120,4) + (2(128,64,16) + (128,8,64) \\
BW_{256} & = & 16\mathbb{Z}^{256} + 8(256,255,2) + 4(256,219,8) + 2(256,93,32) + (256,9,128) \\
BW_{512} & = & 16\mathbb{Z}^{512} + 8(512,502,4) + 4(512,382,16) + 2(512,130,64) + (512,10,256) \\
BW_{1024} & = & 32\mathbb{Z}^{1024} + 16(1024,1023,2) + 8(1024,968,8) + 4(1024,638,32) \\
 & & \quad +2(1024,176,128) + (1024,11,512) \\
BW_{2048} & = & 32\mathbb{Z}^{2048} + 16(2048,2036,4) + 8(2048,1816,16) + 4(2048,1024,64) \\
 & & \quad +2(2048,232,256) + (2048,12,1024)
\end{array}\right. \tag{1.41}$$

Les réseaux de Barnes-Wall $BW_n, n = 2^m$ vérifient différentes propriétés bien utiles à qui veut calculer leur gain, densité, ou nombre de voisins (Cf. table 1.4.2) :

$$\frac{1}{n}\log_2 \Delta \underset{n\to\infty}{\sim} -\frac{1}{4}\log_2 n \tag{1.42}$$

$$\delta = 2^{\frac{-5n}{4}} n^{\frac{n}{4}} \tag{1.43}$$

$$\gamma_{dB} = 10\log_{10}(4 \sqrt[\frac{n}{2}]{\delta}) \tag{1.44}$$

$$\tau(\Lambda) = (2+2)(2+2^2)\cdots(2+2^m) \underset{m\to\infty}{\sim} 4.7682^{\frac{m(m+1)}{2}} \tag{1.45}$$

n	Λ	Δ	δ	γ_{dB}	$\tau(\Lambda)$
4	$BW_4 = D_4$	0.61685	0.12500	1.51	24
8	$BW_8 = E_8$	0.25367	0.06250	3.01	240
16	$BW_{16} = \Lambda_{16}$	0.01471	0.06250	4.51	4320
32	BW_{32}	—	0	6.02	146880
64	BW_{64}	—	16	7.52	9694080
128	BW_{128}	—	64	9.03	1260230400
256	BW_{256}	—	192	10.54	325139443200
512	BW_{512}	—	512	12.04	167121673804800
1024	BW_{1024}	—	1280	13.55	167121673804800
2048	BW_{2048}	—	3072	15.05	351507016513635840000

TAB. 1.3: Quelques réseaux de Barnes-Wall et leurs caractéristiques. La dimension n, le nom Λ, la densité Δ, la densité centrée δ (*$log_2(\delta)$ pour $n \geq 32$*), le gain en dB γ_{dB} et le coefficient d'erreur $\tau(\Lambda)$.

Construction des codes de Reed-Müller

Les codes de Reed-Müller forment une famille infinie de codes linéaires, introduits en 1954 par Reed et Müller. Ils sont déterminés par deux paramètres r et m vérifiant l'inégalité $0 \leq r \leq m$.

Définition 1.4.6 *$RM(r,m)$ est constitué de l'ensemble des 2^m-uples binaires qui représentent toutes les fonctions binaires polynomiales de degré inférieur ou égal à r. $RM(r,m)$ est appelé* **code de Reed-Müller d'ordre r**.

$RM(r,m)$ représente un code sur $\{0,1\}^m$ dont la dimension est égale au nombre de polynômes de degré inférieur ou égal à r, i.e. $\sum_{i=0}^{r}\binom{m}{i}$. On notera que les codes de Reed-Müller peuvent également être définis comme des codes cycliques étendus [24]. Les caractéristiques du code linéaire binaire $RM(r,m)$ sont [51] :

- longueur : $n = 2^m$
- dimension : $k = \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$
- distance minimum : $d = 2^{m-r}$

On constate par ailleurs que $RM(m-2,m)$ est le code de Hamming étendu.

La construction d'un code $RM(r,m)$ consiste à prendre les $m+1$ vecteurs de 2^m composantes $v_0, v_1, \ldots, v_m$, choisis de telle façon que

$$\begin{aligned} v_0 &= (1,1,1,\ldots,1), \\ v_i &= (\underbrace{0,\ldots,0}_{2^{i-1}},\underbrace{1,\ldots,1}_{2^{i-1}},\underbrace{0,\ldots,0}_{2^{i-1}},\underbrace{1,\ldots,1}_{2^{i-1}},\ldots,\underbrace{0,\ldots,0}_{2^{i-1}},\underbrace{1,\ldots,1}_{2^{i-1}}) \quad i \leq m. \end{aligned}$$

On peut alors construire la base du code $RM(r,m)$ comme l'ensemble des combinaisons linéaires des vecteurs $v_0, v_1, \ldots, v_m,\ v_1v_2, v_1v_3, \ldots, v_{m-1}v_m, \ldots, v_{m-r+1}v_{m-r+2}\cdots v_m$ (jusqu'au degré r). Donnons un exemple pour $m=4$, les $1+\binom{m}{1}+\cdots+\binom{m}{m}$ vecteurs de base sont

$$\begin{array}{rcccccccccccccccc}
v_0 = & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
v_4 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
v_3 = & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
v_2 = & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
v_1 = & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
v_4 \odot v_3 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
v_4 \odot v_2 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
v_4 \odot v_1 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
v_3 \odot v_2 = & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
v_3 \odot v_1 = & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
v_2 \odot v_1 = & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
v_4 \odot v_3 \odot v_2 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
v_4 \odot v_3 \odot v_1 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
v_4 \odot v_2 \odot v_1 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
v_3 \odot v_2 \odot v_1 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
v_4 \odot v_3 \odot v_2 \odot v_1 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

On notera de plus que par simple permutation de lignes cette matrice est aisément diagonalisable.

Exemple : réseau BW_{32}

Nous avons déjà vu l'exemple d'un réseau de Barnes-wall avec le réseau Λ_{16} qui n'est autre que BW_{16} puisque le deuxième code de Reed-Müller permettant de le créer, soit $(16, 15, 2)$ n'est autre que le code à répétition en dimension 16. Donnons ici le réseau de Barnes-Wall en dimension 32, soit $BW_{32} = 4\mathbb{Z}^{32} + 2(32, 26, 4) + (32, 6, 16)$.

$$M_{BW_{32}} =$$
$$\begin{bmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&&0&2&0&0&0&2&0&&0&2&0&0&0&2&0&&0&2&0&0&0&2&0&&0&2&0&0&0&2\\
0&&&0&1&1&1&1&0&&&0&1&1&1&1&0&&&0&1&1&1&1&0&&&0&1&1&1&1\\
0&&&&0&2&0&2&0&&&&0&2&0&2&0&&&&0&2&0&2&0&&&&0&2&0&2\\
0&&&&&0&2&2&0&&&&&0&2&2&0&&&&&0&2&2&0&&&&&0&2&2\\
0&&&&&&0&2&0&0&0&0&0&0&0&2&0&&&&&&0&2&0&0&0&0&0&0&0&2\\
0&&&&&&&0&1&1&1&1&1&1&1&1&0&&&&&&&0&1&1&1&1&1&1&1&1\\
0&&&&&&&&0&2&0&2&0&2&0&2&0&&&&&&&&0&2&0&2&0&2&0&2\\
0&&&&&&&&&0&2&2&0&0&2&2&0&&&&&&&&&0&2&2&0&0&2&2\\
0&&&&&&&&&&0&2&0&0&0&2&0&&&&&&&&&&0&2&0&0&0&2\\
0&&&&&&&&&&&0&2&2&2&2&0&&&&&&&&&&&0&2&2&2&2\\
0&&&&&&&&&&&&0&2&0&2&0&&&&&&&&&&&&0&2&0&2\\
0&&&&&&&&&&&&&0&2&2&0&&&&&&&&&&&&&0&2&2\\
0&&&&&&&&&&&&&&0&4&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&&&&&&&&&&&&&&&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&&&&&&&&&&&&&&&&0&2&0&2&0&2&0&2&0&2&0&2&0&2&0&2\\
0&&&&&&&&&&&&&&&&&0&2&2&0&0&2&2&0&0&2&2&0&0&2&2\\
0&&&&&&&&&&&&&&&&&&0&2&0&0&0&2&0&&0&2&0&0&0&2\\
0&&&&&&&&&&&&&&&&&&&0&2&2&2&2&0&&&0&2&2&2&2\\
0&&&&&&&&&&&&&&&&&&&&0&2&0&2&0&&&&0&2&0&2\\
0&&&&&&&&&&&&&&&&&&&&&0&2&2&0&&&&&0&2&2\\
0&&&&&&&&&&&&&&&&&&&&&&0&4&0&0&0&0&0&0&0&0\\
0&&&&&&&&&&&&&&&&&&&&&&&0&2&2&2&2&2&2&2&2\\
0&&&&&&&&&&&&&&&&&&&&&&&&0&2&0&2&0&2&0&2\\
0&&&&&&&&&&&&&&&&&&&&&&&&&0&2&2&0&0&2&2\\
0&&&&&&&&&&&&&&&&&&&&&&&&&&0&4&0&0&0&0\\
0&&&&&&&&&&&&&&&&&&&&&&&&&&&0&2&2&2&2\\
0&&&&&&&&&&&&&&&&&&&&&&&&&&&&0&4&0&0\\
0&&&&&&&&&&&&&&&&&&&&&&&&&&&&&0&4&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4
\end{bmatrix} \tag{1.46}$$

1.5 Décodage à sortie souple des réseaux de points selon le critère MMSE

Le seul algorithme ML de décodage de réseau de points existant, soit l'algorithme de décodage par sphères rappelé au paragraphe 1.3, étant limité pour des raisons de complexité à des dimensions inférieures ou égales à 32, nous proposons un algorithme sous-optimal de décodage permettant de décoder tout réseau Λ de dimension inférieure ou égale à 1024 sur le canal AWGN et sur le canal de Rayleigh. Cet algorithme repose sur le critère de minimisation de l'erreur quadratique moyenne (critère MMSE). Au lieu de minimiser la distance euclidienne, le décodeur MMSE minimise l'espérance sur l'erreur quadratique dans l'espace $\mathbb{Z}^n$ en entrée du réseau. Nous nous sommes pour cela appuyés sur une première version d'un égaliseur MMSE (employé comme égaliseur à retour de décision (DFE) avec le critère MMSE) présentée dans [60] pour le décodage de matrices de Hadamard et de Fourier sur le canal à évanouissement de Rayleigh. Nous généralisons ici le décodage MMSE à tout réseau réel ou complexe de dimension n.

1.5.1 Détermination du détecteur à retour de décision (DFE)

L'emploi d'égaliseurs dans les systèmes de communications numériques pour réduire l'interférence entre symboles (IES) est très classique lorsque l'on souhaite effectuer une transmission sur un canal à bande limitée [58]. Lorsque la réponse impulsionnelle du canal est courte, il est possible de réaliser une égalisation selon le critère à maximum de vraisemblance en appliquant par exemple l'algorithme de Viterbi sur le treillis du canal. Dans le cas contraire, la réduction des effets de l'IES est obtenue en utilisant des égaliseurs sous-optimaux mais moins complexes reposant sur le critère de minimisation de l'erreur quadratique moyenne [58].

Bien sûr, on pourra se demander, et à juste titre, la relation entre égalisation et décodage de réseaux de points. Un réseau de points Λ est un ensemble discret de points dans un espace de dimension n, $\mathbb{R}^n$ ou $\mathbb{C}^n$, obtenu par transformation linéaire du groupe $\mathbb{Z}^n$, c'est-à-dire que l'on a la relation

$$\Lambda = M\mathbb{Z}^n$$

où $M = (m_{ij})_{i,j=1,\dots,n}$ est la matrice génératrice du réseau. L'effet de cette matrice sur $\mathbb{Z}^n$ est donc comparable à celui d'un canal avec IES : chaque composante d'un point du réseau est une combinaison linéaire de tous les entiers en entrée. Ainsi, l'opération de suppression de l'interférence entre symboles est-elle équivalente à celle du décodage de Λ et le décodage d'un réseau de points peut-il être réalisé à l'aide d'un égaliseur. Du fait de la très grande complexité de l'égalisation avec treillis pour les réseaux de grande dimension, la seule solution possible apparait donc être le décodage à l'aide d'un égaliseur sous-optimal à retour de décision reposant sur le critère de minimisation de l'erreur quadratique moyenne.

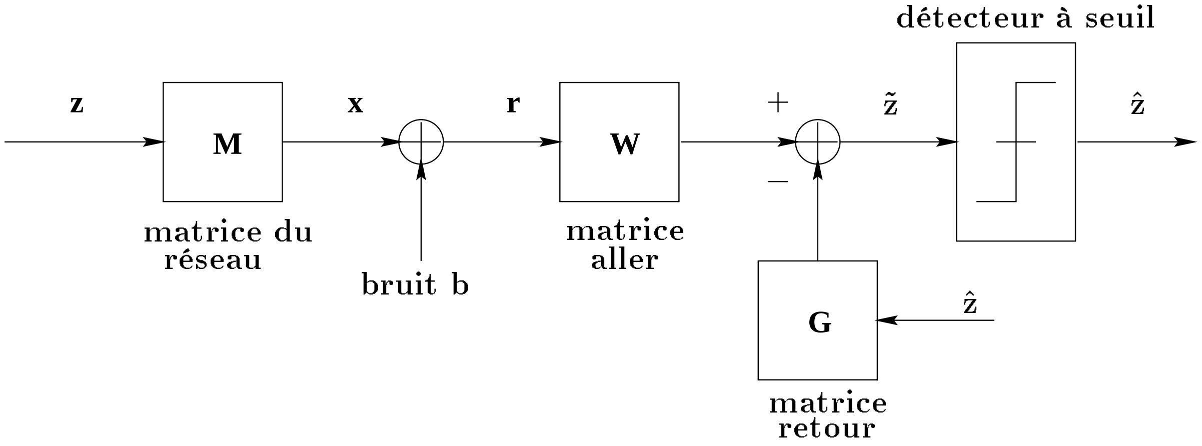


Fig. 1.6: Décodage à retour de décision d'un réseau de points sur canal AWGN.

La figure 1.6 montre le modèle du système de transmission ainsi que l'égaliseur à retour de décision qui comprend une matrice aller W et une matrice de retour G. Le vecteur d'entiers $\mathbf{z}$ ayant été placé en entrée du réseau, le vecteur émis est $\mathbf{x} = M\mathbf{z}$ et le vecteur reçu $\mathbf{y} = \mathbf{x} + \mathbf{b}$. Le bruit $\mathbf{b}$ sur le canal est additif blanc gaussien de moyenne nulle avec une variance de N_0 par composante. L'entrée du détecteur à seuil, soit la version corrigée par la matrice de retour du vecteur reçu est $\tilde{\mathbf{z}}$ et le vecteur estimé, qui est renvoyé en entrée de la matrice de retour G est noté $\hat{\mathbf{z}}$. L'estimation de la $i^{ème}$ composante n'est pas prise en compte dans le calcul de la matrice de retour pour l'égalisation du $i^{ème}$ symbole aussi imposons-nous la condition suivante

$$\forall i \in \{0, \ldots, n-1\} \quad \mid g_{ii} \mid = 0. \tag{1.47}$$

On note σ_z^2 la variance par composante du vecteur d'entiers $\mathbf{z}$. Nous supposerons par la suite que $\sigma_z^2 = 1$, ce qui se fait sans perte de généralité puisqu'au besoin il suffit de remplacer N_0 par N_0/σ_z^2 pour garder correctes les équations trouvées. Nous supposons également que $E[z\hat{z}^h] = \rho I_n$, où I_n la matrice identité en dimension n et ρ est un facteur de corrélation. En pratique, une approximation valable de ρ est donnée par $\rho \approx (1 - P_e(z_i))$. Par conséquent, lorsque le taux d'erreur sur les composantes entières z_i est suffisamment petit, $\rho = 1$. Les notations z^t, z^* et z^h représentent respectivement le transposé, le conjugué et le transconjugué de z. Enfin toute matrice de la forme $\mathbf{D}(\boldsymbol{\xi})$ (respectivement $\mathbf{D}(\boldsymbol{\xi} + a)$, $a \in \mathbb{C}$) représente la matrice diagonale dont les composantes sur la diagonale principale sont $\xi_1, \ldots, \xi_n$ (respectivement $\xi_1 + a, \ldots, \xi_n + a$).

L'égaliseur à retour de décision reposant sur le critère MMSE minimise l'erreur quadratique moyenne (MSE) définie par

$$MSE(W, G) = E[\|\tilde{z} - z\|^2] \ . \tag{1.48}$$

Sachant que lors du calcul de l'égaliseur minimisant l'erreur quadratique moyenne, nous prendrons en compte la condition (1.47) en utilisant les multiplicateurs de Lagrange $(\lambda_i)_{i=1,\dots,n}$. Nous noterons $\boldsymbol{\lambda}$ le vecteur formé par ces multiplicateurs.

La recherche de l'égaliseur minimisant l'expression (1.48) se fait en la dérivant par rapport aux variables W et G afin d'en déterminer les extrema, soit en déterminant le couple (W, G) vérifiant

$$\frac{\partial MSE(W,G)}{\partial W} = \frac{\partial MSE(W,G)}{\partial G} = 0 \ .$$

Pour cela, nous utilisons les règles rappelées ci-dessous

$$\begin{aligned}
\frac{\partial(A^h\Gamma^h\Gamma B)}{\partial\Gamma} &= \Gamma^* A^* B^t \\
\frac{\partial\Gamma^h}{\partial\Gamma} &= 0 \\
\frac{\partial(A^h\Gamma B)}{\partial\Gamma} &= A^* B^t \\
\frac{\partial\|A-\Gamma B\|^2}{\partial\Gamma} &= -A^*B^t + \Gamma^*A^*B^t
\end{aligned} \tag{1.49}$$

où $A = (a_1, \dots, a_n)^t$, $B = (b_1, \dots, b_n)^t$ et $\Gamma = (\gamma_{ij})_{i,j=1,\dots,n}$.

Nous obtenons alors le système suivant (sans contrainte)

$$\left\{ \begin{array}{l} WME[\mathbf{z}\mathbf{z}^h]M^h + WE[\mathbf{b}\mathbf{b}^h] - GE[\hat{\mathbf{z}}\mathbf{z}^h]M^h - E[\mathbf{z}\mathbf{z}^h]M^h = 0 \\ \\ -WME[\mathbf{z}\hat{\mathbf{z}}^h] + GE[\hat{\mathbf{z}}\hat{\mathbf{z}}^h] + E[\mathbf{z}\hat{\mathbf{z}}^h] = 0 \end{array} \right. .$$

Du système d'équations (1.5.1) nous déduisons donc la valeur sans contrainte de G

$$G = \rho WM - \rho I_n \ . \tag{1.50}$$

Il s'agit alors d'introduire ici la contrainte sur les coefficients diagonaux de G donnée par la formule (1.47), ce qui nous donne l'expression de G avec contrainte

$$G = \rho WM - \rho I_n + \mathbf{D}(\boldsymbol{\lambda}) \ . \tag{1.51}$$

Nous en déduisons, avec la première ligne du système (1.5.1) la valeur de W avec contrainte

$$W = \mathbf{D}(\frac{\rho\boldsymbol{\lambda} + (1-\rho^2)}{N_0})M^hV$$

où $V = (v_{ij})_{i,j=1,\dots,n}$ est définie par $\left(\frac{1-\rho^2}{N_0}MM^h + I_n\right)V = I_n$.

En remplaçant cette valeur de W dans l'expression de G donnée par la formule (1.51) nous pouvons calculer la valeur des coefficients multiplicateurs de Lagrange permettant de satisfaire la condition (1.47)

$$\lambda_i = \rho \frac{N_0 + (\rho^2 - 1)B_i}{N_0 + \rho^2 B_i} \tag{1.52}$$

où $B = (B_0, \ldots, B_{n-1})$ avec pour tout $i = 1, \ldots, n$, $B_i = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} m_{ki} v_{kl} m_{li}^*$.

Les expressions finales de W et de G sont donc

$$\begin{cases} W = \mathbf{D}(\frac{1}{\rho^2 B^* + N_0}) M^h V \\ \\ G = \mathbf{D}(\frac{\rho}{\rho^2 B^* + N_0}) M^h V M - \mathbf{D}(\frac{\rho B^*}{\rho^2 B^* + N_0}) \end{cases} . \tag{1.53}$$

1.5.2 Résultats de simulation

Le décodeur DFE sous-optimal trouvé au paragraphe précédent est appliqué au décodage d'un réseau dense en grande dimension, le réseau de Barnes-Wall en dimension 256 sur canal AWGN. L'entrée du filtre de retour est supposée parfaite (ou sans erreur) donc $\rho = 1$.

Le gain fondamental et le coefficient d'erreur du réseau BW_{256} sont donnés par la table 1.4.2, soit $\gamma(BW_{256}) = 10.54$ dB et $\tau(BW_{256}) = 325139443200$ respectivement. La valeur de ce gain fondamental nous apprend qu'une constellation finie extraite de ce réseau sera un bon alphabet de canal pour le canal à bruit additif blanc gaussien. En pratique, le gain effectif sera inférieur aux 10.54 dB théoriques du fait du fort coefficient d'erreur $\tau(BW_{256})$. L'efficacité spectrale à laquelle nous transmettrons est liée à la structure même du réseau BW_{256} : si nous reprenons la formule du réseau donnée en formule (1.41), nous avons $BW_{256} = 16\mathbb{Z}^{256} + 8(256, 255, 2) + 4(256, 219, 8) + 2(256, 93, 32) + (256, 9, 128)$, donc pour émettre un point $\mathbf{x}$ du réseau il nous faudra 255+219+93+9 bits, c'est-à-dire une efficacité spectrale de 2.25 bits par dimension, ou encore $\eta = 4.5$ bits par symbole complexe.

Afin d'estimer les performances du réseau de Barnes-Wall lui-même, soit son efficacité par rapport au meilleur réseau possible en dimension 256, nous plaçons également sur la figure 1.7 une borne des performances optimales sur canal AWGN lorsque la modulation utilisée est un réseau de points en dimension 256, suivant en cela les travaux de Shannon [65].

Afin de comparer nos résultats avec la limite que représente le décodage ML, nous allons utiliser l'inégalité (1.11) qui nous fournit une borne fine sur la probabilité d'erreur par point $P_{e_{point}}$ qu'il est possible d'obtenir théoriquement avec un décodeur ML. Nous en déduisons la probabilité d'erreur par bit $P_{e1_{bit}} = \frac{1}{2} P_{e_{point}}$ pour le cas où l'étiquetage utilisé est aléatoire et la probabilité d'erreur par bit $P_{e2_{bit}} = \frac{1}{128\eta} P_{e_{point}}$ pour le cas où l'étiquetage utilisé est un étiquetage de Gray. Les courbes de $P_{e1_{bit}}$ et de $P_{e2_{bit}}$ sont tracées sur la figure 1.7 pour $\eta = 4.5$ bits par symbole, délimitant la zone hachurée de décodage ML. Cette efficacité spectrale, proche de 2 bits par dimension, nous amène à comparer ces résultats avec les performances d'une MAQ-16. La figure 1.7 nous montre donc, comme nous l'avions prévu, que le gain pratique est bien inférieur au gain théorique puisqu'il est de 5.4 dB.

Les performances du décodeur à retour de décision reposant sur le critère MMSE sont également présentées sur la figure 1.7 lorsqu'utilisé avec une constellation cubique extraite du réseau BW_{256}. Il est indéniable que le décodage selon le critère MMSE est loin d'atteindre les performances ML sur le canal AWGN. Le décodeur MMSE élimine complètement l'interférence entre symboles générée par la structure du réseau, ce que l'on peut observer en comparant ses performances avec le BW_{256} à la courbe de la MAQ-16, mais il ne tire aucun avantage de la densité élevée de l'empilement.

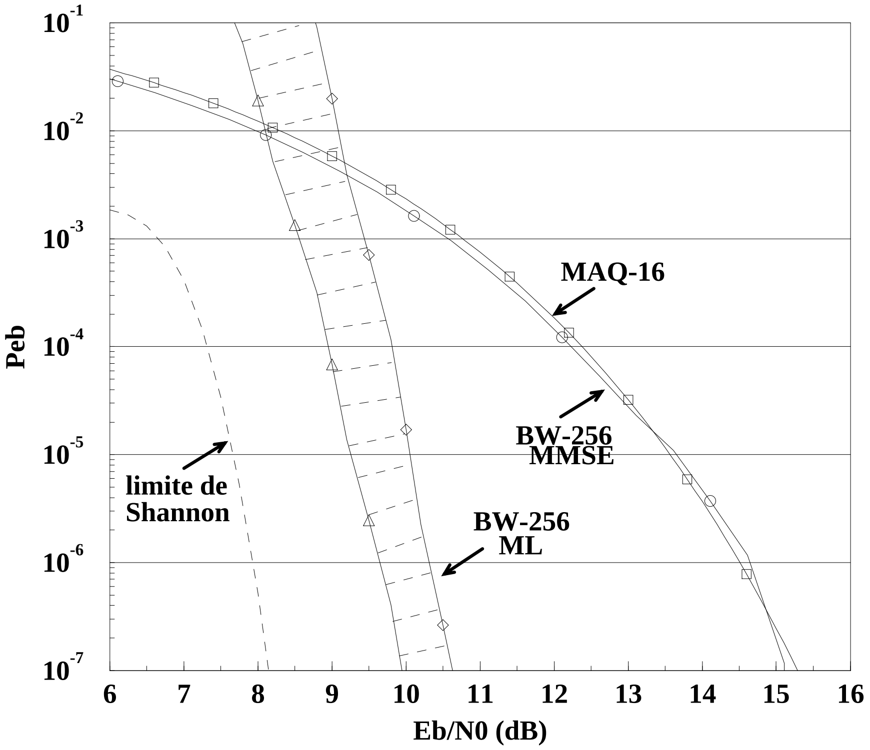


FIG. 1.7: Taux d'erreur binaire pour le réseau de Barnes-Wall BW_{256} avec une efficacité spectrale $\eta/2 = 2.25$ bits par dimension.

1.6 Conclusions

Après avoir rappelé les notions élémentaires de la théorie des réseaux de points, nous nous sommes intéressés dans ce chapitre à leur décodage, rappelant la technique de décodage par sphères, reposant sur le critère ML mais limitée à de petites dimensions, et proposant un nouvel algorithme de décodage par égalisation à retour de décisions selon le critère sous-optimal de minimisation de l'erreur quadratique moyenne. En effet, le critère à maximum de vraisemblance étant inapplicable pour des dimensions élevées pour des raisons numériques évidentes, le critère MMSE apparaît comme un moyen de résoudre le problème du décodage des réseaux de points en grandes dimensions. Cependant, notre DFE présente des performances décevantes sur le canal à bruit additif blanc gaussien. Le gain fondamental du réseau, provenant de la grande densité du réseau, n'est pas exploité par le critère MMSE qui réalise son optimisation dans l'espace des entiers $\mathbf{z}$ et non dans l'espace des points $\mathbf{x}$ du réseau. Le DFE ne peut en fait que supprimer l'interférence entre symboles générée par le réseau lui-même. Nous restons donc malheureusement bien loin des performances optimales des réseaux, dont Urbanke et Rimoldi [73] ont prouvé récemment qu'ils atteignaient la capacité du canal gaussien dans le cas d'un décodage à maximum de vraisemblance.

Un autre axe de recherche sur lequel nous avons commencé à nous pencher est la transformation de l'algorithme de décodage par sphères en un algorithme à entrées et sorties souples, permettant ainsi de fournir une valeur de confiance aux sorties du décodeur, ce qui permettra également à terme de l'inclure dans des systèmes de décodage itératif.

Nous allons à présent nous intéresser au canal à évanouissement de Rayleigh, pour lequel les performances de notre décodeur DFE seront également considérées. Nous nous concentrerons pour ce canal non plus sur les réseaux à grande densité mais les réseaux à grande diversité, et en particulier les rotations, dont on a vu depuis le début des années 1990 qu'elles avaient de très bonnes performances sur les canaux à évanouissement.

Chapitre 2

Les rotations et MAQ multidimensionnelles *

Tournicoti, tournicota
Pollux et Zébulon

2.1 Introduction

Comme nous l'avons vu au chapitre précédent pour le canal à bruit additif blanc gaussien, l'utilisation de constellations extraites de réseaux de points est un moyen connu pour qui veut transmettre à haute efficacité spectrale. Les réseaux de points à grande densité permettent de construire des constellations adaptées à la transmission sur le canal AWGN [27].

L'utilisation de systèmes à grande diversité est par ailleurs classique lorsque l'on considère un canal à évanouissements, car il est bien connu en communications numériques que tirer parti d'une quelconque diversité dans le système de transmission aide à combattre les évanouissements susceptibles de perturber la communication. Ceci explique pourquoi la diversité d'antennes, la diversité en temps ou la diversité en fréquence, bien que coûteuses en terme de bande passante ou d'équipements, sont si populaires. Utiliser la diversité de modulation est une alternative très attrayante dans la mesure où elle ne suppose qu'une complexité supérieure du codeur et du décodeur.

Le défi est donc de combiner les constellations extraites des réseaux de points, à haute efficacité spectrale avec la diversité de modulation. Et c'est dans le cadre de l'approche lancée par Boullé *et al.* [15], Kerpez [45], Viterbo [79], Boutros [16], Giraud *et al.* [38], Da Silva et Souza [29]... que nous allons nous intéresser à des constellations à haute di-

*Certaines parties de ce chapitre ont été publiées dans les journaux *Annales des télécommunications* [82] et *IEEE Transactions on Information Theory* [84].

versité, quelles soient obtenues empiriquement, grâce à la théorie algébrique des nombres, ou encore à partir de polynômes orthogonaux, ou aléatoirement [66]...

Nous nous intéressons donc ici à des modulations améliorant les performances sur le canal de Rayleigh (par augmentation de la diversité grâce à la rotation) mais qui garderont de bonnes performances sur le canal AWGN (une rotation ne modifiant pas la distance euclidienne). Ces constellations pourront donc également être utilisées sur le canal de Rice, qui se trouve entre le canal gaussien et le canal de Rayleigh.

Après présentation du modèle du système et introduction des notations utilisées dans ce chapitre au paragraphe 2.2, nous étudierons différents types de rotations au paragraphe 2.3, parmi lesquelles nous introduisons la transformée de rotation rapide, les rotations construites à partir des polynômes de Tchebicheff ainsi que des rotations aléatoires. Deux types de décodeurs seront alors proposés pour ces rotations, un décodeur à retour de décision reposant sur le critère MMSE au paragraphe 2.6 et un décodeur itératif travaillant sur les probabilités *a posteriori* au paragraphe 2.7. Finalement nous tirerons quelques conclusions au paragraphe 2.8.

2.2 Modèle du système considéré

Pour comprendre l'influence d'une rotation, et avant de nous lancer dans l'étude de systèmes plus complexes, nous proposons tout d'abord de considérer l'expérience toute simple suivante. Observons, à côté de la référence constituée par la sortie d'une canal AWGN dont l'entrée est une BPSK présentée en figure 2.1, la distribution de probabilité du rapport des log-vraisemblances ou LLR en sortie d'un canal de Rayleigh non sélectif à évanouissements indépendants dans les deux cas suivants :

- l'entrée est une modulation BPSK
- l'entrée est une modulation BPSK précédée par une rotation en dimension 2 (angle 31.7°)

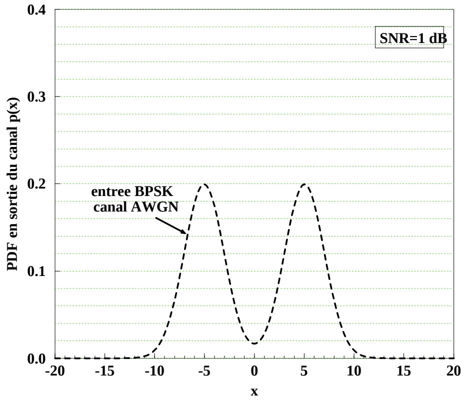
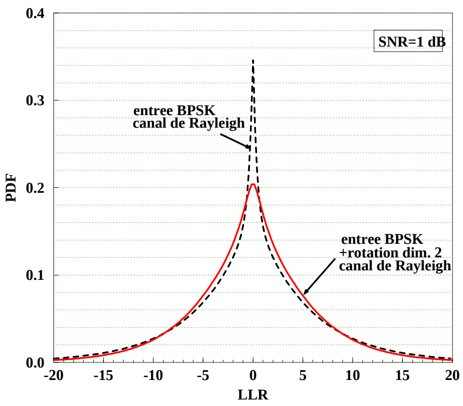
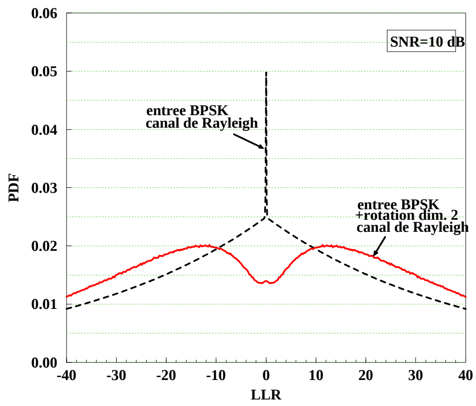


Fig. 2.1: pdf en sortie d'un canal AWGN avec entrée BPSK.

Le résultat de cette expérience est présenté en figure 2.2, et l'on observe très nettement que le pic lié à l'effet des évanouissements sur le canal de Rayleigh commence à se résorber dès les faibles rapport signal à bruit, pour disparaître presque complètement lorsque le rapport signal à bruit est suffisamment important. Sur la courbe de la modulation BPSK tournée à 10 dB, on voit ainsi apparaître deux lobes légèrement déformés, qui nous montrent que la transmission sur le canal n'a perturbé le signal autant que dans le cas de la transmission sans rotation.



(a) : pour un rapport signal à bruit de 1 dB



(b) : pour un rapport signal à bruit de 10 dB

Fig. 2.2: Influence d'une rotation en dimension 2 sur la LLR en sortie d'un canal de Rayleigh indépendant avec entrée BPSK.

L'efficacité de ces modulations tournées vient de leur diversité de modulation, c'est-à-dire du nombre minimal de composantes différentes entre toute paire de points de la constellation considérée. Dans un souci de simplicité, nous parlerons simplement de diversité, et la noterons L. En figure 2.3 nous illustrons cette évolution de la diversité due à la rotation pour une QPSK. Ainsi, si l'on suppose qu'un évanouissement important se produit sur l'une des composantes du point transmis, il est clair que la version évanouie (présentée en cercles blancs) de la constellation avec diversité $L = 2$ offre une protection supérieure contre les effets du bruit, puisque les projections sont toutes distinctes contrairement à ce qui arrive pour la constellation de diversité $L = 1$.

Considérons à présent le schéma du système de transmission présenté en figure 2.4. La source binaire produit les bits en entrée d'un étiqueteur fournissant des éléments $z_i \in \mathbb{Z}^n$ appartenant à une constellation PAM $\{\mathcal{I}_1, \ldots, \mathcal{I}_M\}$, par exemple une BPSK si $M = 2$. Groupant ces éléments par paquets de n, on considère alors en entrée de la rotation un vecteur $\mathbf{z} = (z_1, \ldots, z_n)^t$ appartenant à une constellation MAQ de dimension n qui, après action de la matrice de rotation $R = (r_{ij})_{i,j=1,\ldots,n}$ génère le point $\mathbf{x} = (x_1, \ldots, x_n)^t$ dont

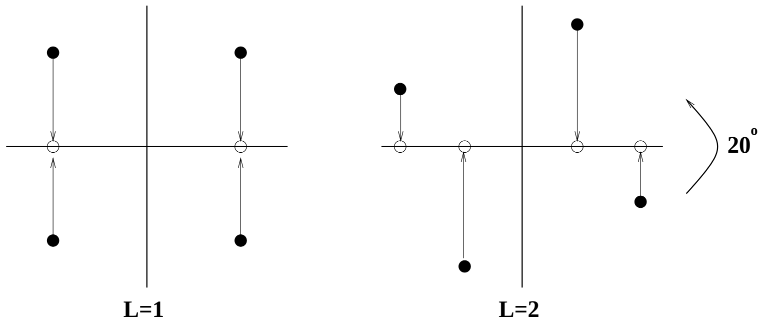


FIG. 2.3: Illustration du gain en diversité par rotation d'une constellation QPSK.

les composantes sont données classiquement par

$$x_i = \sum_{j=1}^{n} r_{ij} z_j \quad i = 1, \ldots, n \ . \tag{2.1}$$

On notera que la rotation n'est autre qu'un réseau de dimension n et de matrice génératrice R. Toute la théorie des réseaux présentée au chapitre précédant reste donc valable ici. La sortie de la rotation est alors émise sur le canal de Rayleigh non sélectif à évanouissements indépendants, ce qui donne en sortie le point reçu $\mathbf{y} = (y_1, \ldots, y_n)^t$ défini par

$$\mathbf{y} = \boldsymbol{\alpha} \odot \mathbf{x} + \mathbf{b} \tag{2.2}$$

où $\mathbf{b} = (b_1, \ldots, b_n)^t$ est un bruit additif blanc gaussien de moyenne nulle et de variance N_0 par composante, où $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)^t$ est le vecteur des coefficients normalisés de l'évanouissement et où $\odot$ représente le produit composante par composante. L'indépendance des composantes de l'évanouissement est assurée par la présence d'un entrelaceur non représenté sur la figure.

Replaçant dans l'équation (2.2) les composantes x_i par leur expression donnée par la formule (2.1), on obtient

$$\mathbf{y} = \mathbf{D}(\boldsymbol{\alpha}) R \mathbf{z} + \mathbf{b} \ . \tag{2.3}$$

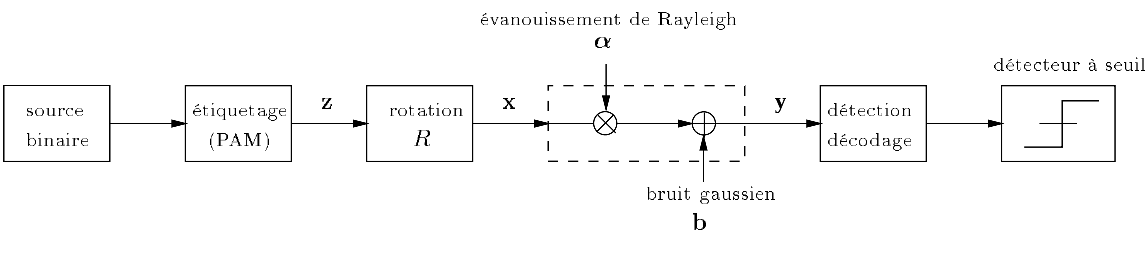


FIG. 2.4: Modèle du système de transmission.

2.3 Choix de la rotation pour le canal à évanouissement de Rayleigh

Utilisant des filtres temporels, appelés précodeurs (*precoders*), Wornell [80] a proposé une méthode pour étaler de l'information à transmettre, la protégeant ainsi des évanouissements sans qu'un entrelacement soit nécessaire. Malheureusement, Wornell s'est limité à un type de filtres linéaires invariants dans le temps qui font que son système ne peut s'adapter en pratique qu'avec l'emploi de filtres finis, qui eux ne sont pas sans pertes. Wornell lui-même souligne que, s'il était possible de trouver des précodeurs qui aient un facteur d'étalement élevé tout en étant sans perte, leurs performances mèneraient asymptotiquement à un canal à bruit additif blanc gaussien sans plus d'évanouissement. En fait, il est aisé de voir qu'une rotation possède ces caractéristiques, puisqu'elles peuvent être vues comme des filtres sans perte et à réponse impulsionnelle finie (FIR) qui étalent l'information sur tous les composantes d'un symbole.

De nombreuses rotations ont été considérées dans la littérature, qui furent optimisées pour satisfaire certains critères comme la maximisation du taux de coupure, de la capacité, ou encore celle de la diversité ou la distribution de diversité de la modulation. En plus de ces rotations déjà connues et établies, nous allons en introduire de nouvelles.

2.3.1 Rotations choisies de manière exhaustive

L'idée de tourner une constellation MAQ n'est pas neuve, puisqu'elle fut présentée en premier lieu par Boullé *et al.* [15] en 1992 dans l'espace réel à deux dimensions $\mathbb{R}^2$. La généralisation de ce résultat en dimensions supérieures est facilité par la propriété suivante :

Théorème 2.3.1 *(Décomposition d'une matrice orthogonale en rotations planes)*
Toute matrice A réelle orthogonale de dimenion n peut être décomposée comme le produit de C_L^2 rotations planes en dimension 2 (ou matrices de Given) et d'une matrice de réflexion.

Preuve – Introduisons tout d'abord les matrices de Given, ou rotations de Given [39].

Définition 2.3.1 *Une* **matrice de Given** $G(i, j, \xi)$, $i < j$, *est une matrice formée à partir de l'identité dont on a remplacé les quatre coefficients* (i, i), (i, j), (j, i) *et* (j, j) *par* *cos(ξ), sin(ξ), $-$sin(ξ) et cos(ξ) respectivement. Matriciellement, on a*

$$G(i,j,\xi) = \begin{array}{cc} \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots & & \vdots \\ 0 & \cdots & \cos\xi & \cdots & \sin\xi & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & -\sin\xi & \cdots & \cos\xi & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{bmatrix} & \begin{array}{c} \\ \\ \leftarrow i \\ \\ \leftarrow j \\ \\ \\ \end{array} \\ \begin{array}{ccccccc} & & \uparrow & & \uparrow & & \\ & & i & & j & & \end{array} & \end{array} . \qquad (2.4)$$

Proposition 1 *Une multiplication à gauche par $G(i,j,\xi)^t$ revient à effectuer une rotation d'un angle ξ dans le sens trigonométrique dans le plan défini par les deux axes de coordonnées $(\mathbf{0}u_i)$ et $(\mathbf{0}u_j)$.*

Preuve – La preuve de cette proposition est immédiate lorsque l'on écrit les coordonnées de tout vecteur $\mathbf{v} = G(i,j,\xi)^t\mathbf{u}$:

$$v_k = \begin{cases} \cos\xi \;\; u_i - \sin\xi \;\; u_j & k = i \\ \sin\xi \;\; u_i + \cos\xi \;\; u_j & k = j \\ u_k & k \neq i,j \end{cases} . \qquad (2.5)$$

De ces formules on déduit qu'il est très facile d'annuler une composante d'un vecteur $\mathbf{u}$ ou de manière similaire un coefficient d'une matrice M en la multipliant par la matrice de Given appropriée, soit en prenant l'angle ξ vérifiant

$$\cos\xi = \frac{u_i}{\sqrt{u_i^2 + u_j^2}} \quad \sin\xi = \frac{-u_j}{\sqrt{u_i^2 + u_j^2}} . \qquad (2.6)$$

Proposition 2 *Si A est une matrice orthogonale $n \times n$, toute décomposition de la forme $A = QV$, où Q est une matrice orthogonale $n \times n$ et V une matrice triangulaire supérieure $n \times n$ permet d'exprimer la matrice Q comme le produit $Q = A\hat{I}$, où $\hat{I}$ est une matrice diagonale dont les éléments diagonaux valent soit 1 soit -1.*

Preuve – Q étant orthogonale par hypothèse, Q^t l'est aussi, donc avec A également orthogonale par hypothèse, $V = Q^tA$ est orthogonale. Or V étant aussi triangulaire supérieure par hypothèse, elle est donc diagonale et chacun de ses éléments diagonaux est de carré 1, soit est égal à 1 ou -1. Introduisons donc $\hat{I} = V$, on a $\hat{I} = Q^tA$ soit $Q = A\hat{I}^{-1}$ et par construction de $\hat{I}$, $\hat{I} = \hat{I}^t = \hat{I}^{-1}$ donc $Q = A\hat{I}$. On notera que $\hat{I}$ définit une réflexion ou une composée de réflexion.

Nous sommes à présent à même de prouver notre théorème de décomposition. Étant donnée une matrice A orthogonale quelconque $n \times n$, on peut, par $n(n-1)/2$ multiplications successives par des matrices de Given transposées, annuler les $n(n-1)/2$ coefficients situés sous la diagonale supérieure de A, comme expliqué dans la preuve de la proposition 1 et donc obtenir une matrice triangulaire supérieure V telle que :

$$V = \prod_{k=1}^{n(n-1)/2} G(i_k, j_k, \xi_k)^t A \ .$$

Le produit de matrices orthogonales étant lui-même orthogonal, la matrice Q définie par $Q = \prod_{k=1}^{n(n-1)/2} G(i_k, j_k, \xi_k)$ est une matrice orthogonale. Utilisant le résultat de la proposition 2, le théorème de décomposition est donc démontré. □

Utilisant le théorème 2.3.1, Da Silva et Sousa [29] ont pu étendre de manière exhaustive les résultats trouvés dans [15] jusqu'à la dimension 5, réalisant une recherche reposant sur l'optimization numérique de la fonction $CFM(\mathcal{C})$ (*constellation figure of merit*) mesurant les performances d'une constellation $\mathcal{C}$ sur un canal de Rayleigh à haut rapport signal à bruit. Directement tirée de la borne ML de la probabilité d'erreur par paire à haut rapport signal à bruit pour une constellation extraite d'un réseau, déterminée dans l'équation (1.15), cette fonction est définie par

$$CFM(\mathcal{C}) = min_{\mathbf{c},\mathbf{d}\in\mathcal{C},\mathbf{c}\neq\mathbf{d}} \prod_{i=1,c_i\neq d_i}^{n} (c_i - d_i)^2 \ . \tag{2.7}$$

Les rotations correspondantes en dimension 4 et 5 sont rappelées dans les tableaux B.1 et B.4. Cette technique devient néanmoins trop complexe pour des dimensions supérieures à 5, ce qui a amené à quitter ce mode de construction.

Des travaux portant sur des transformations linéaires autres que des rotations, menés par Kerpez [45] ont permis la création et l'étude d'un autre type de constellations à haute diversité pouvant être utile pour combattre les effets des évanouissements. Mais, comme montré dans [29], il apparaît que de telles constellations n'offrent pas de meilleurs résultats que les constellations cubiques tournées du fait de leur grande énergie par composante.

Une autre transformation, très liée à notre étude, est la "transformée de diversité" (*diversity transform*) introduite par Rainish [59] qui est construite par optimisation du taux de coupure R_0 [76]. La recherche est dans ce cas-ci également effectuée grâce aux résultats du théorème 2.3.1 à partir de matrices de rotations planes. On notera que s'il est vrai qu'améliorer le taux de coupure ne signifie par pour autant que l'on améliore la capacité ou la diversité, il est certain que le taux de coupure est un critère suffisamment reconnu en communications numériques pour que ces rotations optimisées par Rainish soient pour nous un point de comparaison intéressant. Le critère de recherche sur le taux de coupure est défini par

$$R_0 = \log_2 M - \frac{1}{n}\log_2\left(1 + \frac{1}{M^n}\sum_{\mathbf{x}}\sum_{\mathbf{z}\neq\mathbf{x}}\prod_{j=1}^{n}\frac{1}{1+\frac{E_s}{N_0}A_j}\right) \tag{2.8}$$

où $A_j = \frac{\sum_{i=1}^{n} r_{ij}(x_i - z_i)^2}{4}$. Nous donnons en exemple la rotation optimisée $OP_{2,8}$ en dimension 8, rappelée dans le tableau B.7.

2.3.2 Rotations algébriques

L'emploi de la théorie algébrique des nombres [62] permet de construire des constellations multidimensionnelles extraites de réseaux à grande diversité. Ainsi Boutros et Viterbo [17][19] ont-ils proposé la construction de réseaux dont la diversité est aisément controlable de par leur construction et s'en sont servis pour tourner des constellations MAQ, créant ainsi des MAQ multidimensionnelles à haute diversité. Ont été en particulier considéré deux types de réseaux, soit $\mathbb{Z}_{n,n}$ de diversité garantie par construction égale à la dimension n et $\mathbb{Z}_{n,n/2}$ de diversité garantie par construction égale à $n/2$.

Construction algébrique des réseaux $\mathbb{Z}_{n,n}$

Cette construction repose sur le plongement canonique σ dans les corps de nombres algébriques totalement réels $\mathbb{Q}(2\cos(2\pi/N))$. Appliquant le plongement canonique à un idéal particulier de cet anneau, on obtient une version tournée $\mathbb{Z}_{n,n}$ du réseau entier $\mathbb{Z}^n$. Le choix de ce corps se justifie par le fait qu'étant totalement réel, le corps $\mathbb{Q}(2\cos(2\pi/N))$ garantit une diversité maximale à la constellation obtenue, soit $L = n$ [17]. Il a de plus été montré que différents réseaux tournés de cette famille maximisent la distance produit-ℓ minimale de la constellation [19]. Nous allons rappeler ici les grandes lignes de la procédure utilisée dans [19] pour obtenir $\mathbb{Z}_{n,n}$, puis afin d'aider à la compréhension, nous donnerons un exemple d'application en construisant le réseau tourné $\mathbb{Z}_{5,5}$ dont nous nous servirons également au chapitre 4.

On notera tout d'abord que le degré de $\mathbb{Q}(2\cos(2\pi/N))$ est égal à $\Phi(N)/2$, où $\Phi(\cdot)$ est la fonction d'Euler donnant le nombre d'entiers premiers avec N, ce qui impose certaines limitations sur les dimensions du réseau que nous pouvons obtenir. Les dimensions possibles seront donc de la forme $n = \Phi(N)/2$. La procédure à suivre pour une telle dimension n est alors :

1. Considérer le corps $K = \mathbb{Q}(\beta)$ de discriminant absolu $d_K = p^m$, avec $\beta = 2cos(2\pi/N)$ de polynôme minimal $\mu_\beta(x)$.
2. Factoriser l'idéal principal $(p) = pO_K$, où O_K est l'anneau des entiers de K, sous la forme J^n, où J est un idéal premier.
3. Chercher, en appliquant le plongement canonique successivement à chacun des idéaux J^k, $k = 0, \dots, n$ celui qui permet d'obtenir une matrice génératrice $\Lambda = \sigma(J^k)$ orthogonale, soit la matrice génératrice de $\mathbb{Z}_{n,n}$.

Nous donnons des exemples de ces matrices génératrices en dimension 4, 5 et 8 dans les tableaux B.2, B.5 et B.11.

Exemple : construction de $\mathbb{Z}_{5,5}$

Ayant $\Phi(11)/2 = 5$, on en déduit que le réseau cubique $\mathbb{Z}_{5,5}$ se construit à partir de l'anneau $\mathbb{Q}(2\cos(2\pi/11))$. Calculons à présent le polynôme minimal $\mu_\beta(x)$ de $\beta = 2\cos(2\pi/11)$.

Soit $m(x) = \sum_{k=0}^{2n} a_k x^k$ le polynôme minimal de $\theta = e^{2\pi j/N}$, c'est-à-dire le polynôme cyclotomique de degré $2n = \phi(N)$. On a :

$$m(x) = Q^{(11)}(x) = \sum_{k=0}^{2n} a_k x^k = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \ .$$

Or, le polynôme cyclotomique est réciproque puisqu'il admet également θ^{-1} [10] pour racine car : pour $N \geq 2, x^{\Phi(N)} Q^{(N)}(x^{-1}) = Q^{(N)}(x)$. On peut donc réécrire la relation $\theta^{-n} m(\theta) = 0$, comme

$$\sum_{k=0}^{n} a'_{n-k}(\theta^k + \theta^{-k}) = 0 \tag{2.9}$$

où $a'_k = a_k, k = 0, \ldots, n-1$, et $a'_n = a_n/2$.

On déduit de l'expression de $m(x)$ les valeurs des a'_k, soit

$$(a'_0, a'_1, a'_2, a'_3, a'_4, a'_5) = (1, 1, 1, 1, 1, 1/2) \ .$$

Or, la relation donnée par l'équation (2.9) est par exemple vérifiée par les polynômes $T_k(x)$ de Tchebicheff du premier ordre (voir paragraphe 2.3.4), puisque $(\theta^k + \theta^{-k}) = 2\cos(2\pi k/N) = T_k(\cos 2\pi/N) = 0$. On en déduit donc que le polynôme $\mu(x)$ défini par

$$\mu(x) = \sum_{k=0}^{n} a'_{n-k} T_k(x) = 16x^5 + 8x^4 - 16x^3 - 6x^2 + 3x + 1/2$$

est polynôme minimal de β. Il ne reste plus alors qu'à le réduire, au sens des corps de nombre, pour obtenir le polynôme minimal $\mu_\beta(x)$

$$\mu_\theta(x) = x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1 \ .$$

Connaissant le polynôme minimal, on obtient [25] le discriminant absolu $d_K = 11^4$ dont on déduit la valeur $p = 11$. Nous allons donc factoriser l'idéal $(p) = 11 O_K$ pour construire le réseau $\mathbb{Z}_{5,5} = \sigma(J^3)$ (soit $k = 3$, la seule valeur pour laquelle on obtiendra une matrice orthogonale). La matrice génératrice de l'idéal $\mathcal{G}_{\sigma(J^3)}$ se décompose [17] sous la forme $\mathcal{G}_{\sigma(J^3)} = \mathcal{G} \times T$ où $\mathcal{G}$ est la matrice génératrice du réseau dans O_K et T la matrice de passage entre la base de l'idéal et celle de l'anneau des entiers O_K.

Calculons [25] tout d'abord la matrice génératrice $\mathcal{G}$ du réseau $\Lambda_{5,5} = \sigma(O_K)$. Ses colonnes correspondent au plongement canonique des vecteurs $(\omega_1, \ldots, \omega_n)$ de la base entière de K

$$\mathcal{G} = \begin{bmatrix} 1 & -1.6825 & 2.8308 & -4.7629 & 8.0136 \\ 1 & -0.8308 & 0.6903 & -0.5735 & 0.4765 \\ 1 & 0.2846 & 0.0810 & 0.0231 & 0.0066 \\ 1 & 1.3097 & 1.7154 & 2.2467 & 2.9425 \\ 1 & 1.9190 & 3.6825 & 7.0667 & 13.5609 \end{bmatrix} .$$

Par ailleurs, la décomposition de l'idéal $11O_K$ se fait sous la forme $11O_K = J^5$, où $J = 11O_K + (\theta+2)O_K$, ce qui nous permet de déduire la matrice de transition entre la base de l'idéal premier J et celle de O_K

$$\begin{bmatrix} 11 & 2 & 7 & 8 & 6 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

On en déduit la matrice T entre les coordonnées dans l'idéal J^3 et celles de O_K

$$T = \begin{bmatrix} 11 & 0 & 0 & 8 & 7 \\ 0 & 11 & 0 & 1 & 2 \\ 0 & 0 & 11 & 6 & 9 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

ce qui donne pour matrice génératrice de l'idéal $\mathcal{G}_{\sigma(J^3)} = \mathcal{G} \times T$

$$\mathcal{G}_{\sigma(J^3)} = \begin{bmatrix} 11 & -18.5076 & 31.1391 & 18.5396 & 37.1261 \\ 11 & -9.1391 & 7.5931 & 10.7373 & 12.0273 \\ 11 & 3.1309 & 0.8912 & 8.7938 & 8.3049 \\ 11 & 14.4069 & 18.8691 & 21.8486 & 28.0003 \\ 11 & 21.1088 & 40.5076 & 39.0807 & 57.5414 \end{bmatrix}$$

Cette matrice représente le réseau mais n'est pas sous sa forme réduite (soit normalisée et orthogonale). On va donc chercher la base orthogonale du réseau, utilisant pour cela l'algorithme LLL [48] puisque la base réduite, au sens la minimisation de la forme quadratique associée à la matrice, est la base orthogonale lorsqu'elle existe [25]. On obtient alors, après normalisation, la base orthonormale qui forme la matrice du réseau $\mathbb{Z}_{5,5}$

$$\mathbb{Z}_{5,5} = \begin{bmatrix} -0.4557341407 & -0.5485287320 & -0.5968847877 & -0.3260186796 & 0.1698911240 \\ -0.5968847877 & 0.4557341407 & -0.1698911240 & 0.5485287320 & 0.3260186796 \\ -0.3260186796 & 0.1698911240 & 0.5485287320 & -0.5968847877 & 0.4557341407 \\ -0.1698911240 & 0.5968847877 & -0.3260186796 & -0.4557341407 & -0.5485287320 \\ 0.5485287320 & 0.3260186796 & -0.4557341407 & -0.1698911240 & 0.5968847877 \end{bmatrix}.$$

Construction algébrique des réseaux $\mathbb{Z}_{n,n/2}$

Une autre famille de matrices orthogonales construites grâce à la théorie algébrique des nombres est celle des réseaux $\mathbb{Z}_{n,n/2}$, de diversité $L = n/2$ pour $n = 2^{e_1}3^{e_2}$, $e_1, e_2 =$

$0, 1, 2, \ldots$. On obtient ainsi une rotation multidimensionnelle réelle R de dimension n qui génère la version tournée $\mathbb{Z}_{n,n/2} = R\mathbb{Z}^n$ du réseau entier cubique $\mathbb{Z}$.
On se place dans le corps cyclotomique totalement complexe $K = \mathbb{Q}[j](\theta)$ généré par $\theta = e^{2j\pi/N}$, racine $N^{ème}$ de l'unité (où N est défini par $n = \phi(N)$). La construction se fait alors en appliquant un plongement canonique à l'anneau des entiers $O_K = \mathbb{Z}[j](\theta)$, généré par $(1, \theta, \theta^2, \ldots, \theta^{n/2-1})$, dans K [19]. Si l'on note $\theta_i = \theta \times e^{4j\pi(i-1)/n}$, pour $i = 1, \ldots, n/2$, la rotation obtenue est donnée par la matrice complexe en dimension $n/2$ suivante

$$R = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_{n/2} \\ \vdots & \vdots & & \vdots \\ \theta_1^{n/2-1} & \theta_2^{n/2-1} & \cdots & \theta_{n/2}^{n/2-1} \end{bmatrix} \tag{2.10}$$

Le réseau réel correspondant de dimension n peut être obtenu en remplaçant chaque valeur complexe $a + jb$ de R par la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Comme montré dans [17], ce réseau a une diversité de $L = n/2$.

Nous donnons des exemples de ces matrices génératrices en dimensions 4 et 8 dans les tableaux B.3, B.8 et B.9 : ces matrices sont notées $\mathbb{Z}_{4,2,a}$, $\mathbb{Z}_{8,4,a}$ et $\mathbb{Z}_{8,4,b}$.

2.3.3 Transformée de rotation rapide (FRT)

Comme on l'a vu dans le paragraphe précédent, les réseaux tournés par rotation matricielle $\mathbb{Z}_{n,n/2}$ obtenus par Boutros et Viterbo [19] permettent d'augmenter la diversité des constellations utilisées, et ainsi de protéger l'information de l'évanouissement introduit par le canal de Rayleigh. Le principal inconvénient de ces rotations est la complexité du calcul, due à la nécessité de réaliser effectivement des multiplications de matrices de taille $n \times n$. Pour utiliser cette méthode, il faudra donc travailler dans de faibles dimensions si l'on veut profiter de la diversité apportée par ces rotations algébriques sans alourdir trop notre système de transmission. Typiquement, on utilisera des dimensions n de l'ordre de 8 à 32.

Pour atteindre des dimensions supérieures avec ces rotations, nous avons élaboré une "transformée rapide", à l'image de celles bien connues de Fourier (FFT) ou de Hadamard (FHT). Nous allons voir que cette transformation, appelée *transformée de rotation rapide* (*Fast Rotation Transform*, FRT) se déduit aisément des formules obtenues pour les réseaux $\mathbb{Z}_{n,n/2}$ présentés précédemment.

Si nous nous restreignons aux valeurs de n égales à des puissances de 2, nous obtenons $N = 2n$ et les composantes de la matrice de rotation $R = (r_{ik})_{i,k=1,\ldots,n}$ sont donnés par

$$r_{ik} = (\theta.e^{\frac{4j\pi i}{n}})^k = e^{\frac{j\pi k}{n}}.e^{\frac{2j\pi ik}{n/2}} \qquad \forall (i,k) \in 0, \ldots, \frac{n}{2} - 1. \tag{2.11}$$

Appliquons à présent cette rotation à un vecteur $\mathbf{u} = (u_0, \ldots, u_{n/2-1})$, le vecteur résultant est $\mathbf{x} = (x_0, \ldots, x_{n/2-1})$ dont les composantes sont données par

$$x_i = \sum_{k=0}^{\frac{n}{2}-1} (r_{ik} u_k) = \sum_{k=0}^{\frac{n}{2}-1} (e^{\frac{2j\pi ik}{n/2}} u'_k) \qquad \text{avec} \quad u'_k = u_k . e^{\frac{2j\pi k}{2n}} . \tag{2.12}$$

Si l'on compare la formule ci-dessus avec celle de la transformée de Fourier discrète (DFT), il apparaît qu'une rotation algébrique liée au réseau $\mathbb{Z}_{n,n/2}$ revient à l'application d'une transformée de Fourier rapide avec des coefficients déphasés. La fonction de calcul de la FRT à partir d'une FFT est donnée ci-dessous

```
static void FRT(ComplexNum* X, int T, int fid)
/* fid : numéro de la FFT */
{/* begin of FRT() */
 int i;

 if(T==1) { /* transformée directe */
    for(i=0; i<n; i++)
      X[i]=CPLXMUL(X[i], CPLXEXPJ(i*PI/(2.0*n)));

    FFT(X, 1, fid);
   }

 if(T==0) {/* transformée indirecte */
    FFT(X, 0, fid);

    for(i=0; i<n; i++)
      X[i]=CPLXMUL(X[i], CPLXEXPJ(-i*PI/(2.0*n)));
   }

}/* end of FRT() */
```

L'utilisation de la FRT nous garantit donc comme pour les petites dimensions une diversité de $n/2$. On notera qu'elle peut également être utilisée sur des réseaux complexes $\mathbb{Z}_{n/2,n/2}$ construits avec la rotation complexe définie par la formule (2.10).

2.3.4 Rotations construites à partir de familles de polynômes orthogonaux

Classiquement, les polynômes $(Q_k(x))_{k=0}^{+\infty}$, ou famille de polynômes $Q_k(x)$ sont dits orthogonaux sur l'intervalle $[a; b]$ par rapport à la fonction poids $w(x)$ si

$$\forall (i, j) \in \mathbb{N}, i \neq j, \int_a^b w(x) Q_i(x) Q_j(x)\, dx = 0 \ .$$

La fonction poids $w(x)$ détermine le système de polynômes à une constante près, dont la spécification est dite standardisation. Pour des polynômes standardisés on a par définition

$$\begin{aligned} &Q_k(x) = \ell_k x^k + \ell'_k x^{k-1} + \cdots \\ &\text{and } \int_a^b w(x) Q_k^2(x)\, dx = h_k^2 \end{aligned} \tag{2.13}$$

Il est aisé de montrer que les polynômes orthogonaux $Q_k(x)$ de degré k possèdent exactement k racines réelles distinctes $(x_0, x_1, \ldots, x_{k-1})$ sur leur intervalle d'orthogonalité $[a; b]$ [7]. Les polynômes $Q_k(x)$ vérifient également la propriété suivante

$$\begin{aligned} &Q_{k+1}(x) = (a_k + x \times b_k) Q_k(x) - c_k Q_{k-1}(x) \\ &\text{où } b_k = \frac{\ell_{k+1}}{\ell_k},\ a_k = b_k \left(\frac{\ell'_{k+1}}{\ell_{k+1}} - \frac{\ell'_k}{\ell_k} \right),\ c_k = \frac{\ell_{k+1}\ell_{k-1}h_k}{\ell_k^2 h_{k-1}} \text{ , et } Q_{-1} = 0 \end{aligned} \tag{2.14}$$

Utilisant la formule de récurrence (2.14) liant trois polynômes successifs on peut tirer l'expression matricielle suivante

$$\begin{bmatrix} \frac{-a_0}{b_0} & \frac{1}{b_0} & 0 & \cdots & & 0 \\ \frac{c_1}{b_1} & \frac{-a_1}{b_1} & \frac{c_1}{b_1} & & & 0 \\ 0 & \frac{c_2}{b_2} & \frac{-a_2}{b_2} & \frac{1}{b_2} & & 0 \\ \vdots & & \ddots & & & \vdots \\ \vdots & & & \ddots & & \vdots \\ 0 & & \frac{c_{n-1}}{b_{n-1}} & \frac{-a_{n-1}}{b_{n-1}} & \frac{1}{b_{n-1}} & 0 \\ 0 & & & \frac{c_n}{b_n} & \frac{-a_n}{b_n} & \frac{1}{b_n} \end{bmatrix} \begin{bmatrix} Q_0(x) \\ Q_1(x) \\ Q_2(x) \\ \vdots \\ Q_{n-1}(x) \\ Q_n(x) \\ Q_{n+1}(x) \end{bmatrix} = x \begin{bmatrix} Q_0(x) \\ Q_1(x) \\ Q_2(x) \\ \vdots \\ Q_{n-1}(x) \\ Q_n(x) \\ Q_{n+1}(x) \end{bmatrix} \tag{2.15}$$

Replaçant successivement dans l'équation (2.15) la variable x par chacune des $n+1$ racines x_k, $k = 0, \ldots, n$ du polynôme $Q_{n+1}(x)$, on obtient

$$\begin{bmatrix} \frac{-a_0}{b_0} & \frac{1}{b_0} & 0 & \cdots & \\ \frac{c_1}{b_1} & \frac{-a_1}{b_1} & \frac{c_1}{b_1} & & \\ 0 & \frac{c_2}{b_2} & \frac{-a_2}{b_2} & \frac{1}{b_2} & \\ \vdots & & \ddots & & \\ 0 & & \frac{c_{n-1}}{b_{n-1}} & \frac{-a_{n-1}}{b_{n-1}} & \frac{1}{b_{n-1}} \\ 0 & & & \frac{c_n}{b_n} & \frac{-a_n}{b_n} \end{bmatrix} \begin{bmatrix} Q_0(x_k) \\ Q_1(x_k) \\ Q_2(x_k) \\ \vdots \\ Q_{n-1}(x_k) \\ Q_n(x_k) \end{bmatrix} = x_k \begin{bmatrix} Q_0(x_k) \\ Q_1(x_k) \\ Q_2(x_k) \\ \vdots \\ Q_{n-1}(x_k) \\ Q_n(x_k) \end{bmatrix} \tag{2.16}$$

On peut donc en déduire que la matrice dans l'équation (2.15) possède $n+1$ valeurs propres distinctes, à savoir les racines x_k. Ceci implique que la famille des vecteurs propres correspondants $(Q_i(x_k))_{i,k=0,\ldots,n}$ est une base orthogonale de vecteurs à partir de laquelle il est aisé de construire, par simple normalisation, une matrice de rotation R en dimension $n+1$

$$R = \begin{bmatrix} \lambda_0 Q_0(x_0) & \lambda_0 Q_1(x_0) & \cdots & \lambda_0 Q_n(x_0) \\ \lambda_1 Q_0(x_1) & \lambda_1 Q_1(x_1) & \cdots & \lambda_1 Q_n(x_1) \\ \vdots & & & \vdots \\ \lambda_n Q_0(x_n) & \lambda_n Q_1(x_n) & \cdots & \lambda_n Q_n(x_n) \end{bmatrix} \tag{2.17}$$

où $\lambda_k^2 = \left(\sum_{i=0}^{n} Q_i^2(x_k)\right)^{-1}$.

Une des familles les plus connues de polynômes orthogonaux est celle des *polynômes de Tchebicheff du premier ordre* $T_k(x)$ qui sont orthogonaux sur l'intervalle $[-1;1]$ avec la fonction poids $w(x) = (1-x^2)^{-1/2}$ et la normalisation standard $\forall k, T_k(1) = 1$ [61]. Cette technique peut néanmoins être appliquée à d'autres familles de polynômes orthogonaux, comme par exemple ceux présentés dans [1]. À titre d'exemple, nous donnons la matrice de Tchebicheff $Tchebi_8$ en dimension 8 dans le tableau B.6.

2.3.5 D'autres rotations simples à construire : rotations de Hadamard et rotations aléatoires

Figurant parmi les matrices de rotations les plus simples et les plus connues, les matrices de Hadamard sont des matrices calculées récursivement [51] pp. 44–49

$$H_1 = 1, \quad H_{2n} = \frac{1}{\sqrt{2n}} \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \tag{2.18}$$

où nous nous limitons à des dimensions de la forme $n = 2^m, m \in \mathbb{Z}$.

Bien que leur diversité soit égale à 1, nous allons considérer ces matrices de Hadamard car nous verrons notamment au chapitre 4 qu'elles ont des capacités étonnamment bonnes. Notant que ces matrices se comportent à peu près comme des matrices dont les composantes seraient aléatoirement $+1$ ou -1, nous avons généralisé la construction [84] en choisissant des matrices A avec des entrées tirées d'un ensemble de a points ($a \geq 2$) répartis uniforméments sur le cercle unité. Une procédure de Gram-Schmidt est alors appliquée à cette matrice aléatoire de dimension n, qui assure son orthogonalité. Nous avons ainsi tiré aléatoirement différentes matrices dont nous verrons les performances au paragraphe 2.5. Pour des raisons pratiques, nous ne donnons pas les matrices des rotations en dimension supérieure ou égale à 8 donc seule la matrice $\mathbb{Z}_{8,4,random}$ est présentée en annexe dans le tableau B.10.

Dans le cadre de l'étude de la capacité au chapitre 4, nous avons tiré aléatoirement 3000 matrices, avec le paramètre a égal à 8. Nous avons retenu la matrice donnant en moyenne la meilleure capacité, le rapport signal à bruit par bit codé E_c/N_0 prenant trois valeurs : cette matrice appelée $Random_8$ est donnée dans le tableau B.13.

2.4 Étude de la distribution de diversité

Il est bien connu que la distribution des distances euclidiennes du réseau de points Λ a une influence directe sur ses performances sur le canal gaussien (comme nous l'avons vu en établissant la formule (1.11). De même, la distribution de diversité de Λ a une influence directe sur les performances obtenues sur le canal de Rayleigh. Nous allons donc étudier les distributions de diversité de différentes matrices de rotations.

2.4.1 Distribution de diversité de la FRT et de la FFT

Puisque $\mathbf{0}$ appartient au réseau Λ, la distribution de diversité peut être obtenue en comparant tous les points à $\mathbf{0}$. Pour tout $\mathbf{x} \in \Lambda$ choisi aléatoirement, la distribution de diversité donne la probabilité $P(l)$ d'avoir l composantes non nulles dans $\mathbf{x}$, avec $L \leq l \leq n$.

D'après la construction de la FRT à partir de la rotation algébrique du réseau $\mathbb{Z}_{n,n/2}$, la distribution de diversité d'une FRT complexe est donnée tout simplement par

$$\begin{array}{l} P(l) = 0 \quad \text{pour} \quad l = 0, \ldots, n/2 - 1 \\ P(n/2) = 1 \end{array} \tag{2.19}$$

Pour une FFT, le fait de remarquer que le point $(1, 0, 0, \ldots, 0)$ appartient au réseau tourné indique que l'ordre de diversité minimale de la FFT est $L = 1$. Une FFT n'a donc littéralement pas de diversité. Cependant, si l'on trace par simulation sa distribution de diversité pour une BPSK en entrée, on constate qu'elle rejoint celle de la FRT pour de très grandes dimensions, comme montré en figure 2.6. Par conséquent, pour n assez grand, la FFT et la FRT ont les mêmes performances sur le canal de Rayleigh. On notera cependant que pour $n \leq 32$ la FFT donne de mauvais résultats alors qu'une FRT décodée avec le décodeur universel de réseaux de points [78] élimine presque complètement l'impact des évanouissements. Le comportement d'une transformée d'Hadamard rapide (FHT) est identique à celui d'une FFT. Dans le paragraphe suivant, nous allons nous intéresser au calcul de la distribution de diversité d'une matrice aléatoire de type Hadamard et l'on montrera que toute rotation choisie aléatoirement (en grande dimension) donne des performances similaires sur le canal de Rayleigh.

2.4.2 Distribution de diversité de matrices de type Hadamard

Une formule directe et exacte des coefficients h_{ij} d'une matrice d'Hadamard est très difficile à déterminer. Nous allons donc définir une matrice aléatoire *de type Hadamard* H_n qui va nous permettre de calculer une distribution de diversité et d'énergie.

Le calcul de ces distributions est réalisable de manière analytique parce que les composantes des matrices prennent leurs valeurs dans un ensemble de cardinal 2, i.e. ± 1 et ont des lois de probabilité connues. En revanche, la généralisation au cas $a > 2$ pour les matrices aléatoires définies au paragraphe 2.3.5 paraît une tâche très difficile.

La matrice *de type Hadamard* vérifie les conditions suivantes :

- la première ligne et la première colonne de H_n sont remplies avec des *'1'*.
- les autres lignes de H_n sont composées de $n/2$ *'1'* (y compris celui se trouvant dans la première colonne) et $n/2$ *'-1'* répartis aléatoirement.
- on omet volontairement le facteur de normalisation $\frac{1}{\sqrt{n}}$.

On définit également

- $\mathbf{u}$ vecteur d'entrée, et $\mathbf{v}$ vecteur de sortie, vérifiant $\mathbf{v} = H_n\mathbf{u} \quad \mathbf{v} \in \Lambda$
- $U_{k|0}$ est l'ensemble des vecteurs $\mathbf{u}$ avec k composantes égales à *'1'* et $u_1 = 0$. Son cardinal est $|U_{k|0}| = C_{n-1}^{k}$.
- $U_{k|1}$ est l'ensemble des vecteurs $\mathbf{u}$ avec k composantes égales à *'1'* et $u_1 = 1$. Son cardinal est $|U_{k|1}| = C_{n-1}^{k-1}$.
- U étant l'un de ces deux ensembles, et pour $d \in \mathbb{Z}$, on a
$$P(v_i = d \mid \mathbf{u} \in U) = P(v_j = d \mid \mathbf{u} \in U) = P_U(d) \quad \forall (i,j) \in \{1, \dots, n-1\}^2$$
  On remarquera que pour tout vecteur $\mathbf{u}$ non nul, v_0 est non nul.
- $L[l]$ est le nombre de vecteurs de diversité l.

Avec ces notations, nous pouvons écrire le nombre de vecteurs $\mathbf{v}$ de diversité l non nulle pour $\mathbf{u} \in U$
$$L[l]_U = |U| P_U(0)^{n-l}(1 - P_U(0))^{l-1} \tag{2.20}$$

On obtient ainsi la formule de la distribution de diversité de type Hadamard
$$\begin{aligned}
&L[n] = \sum_{k_1'=1}^{n/2} \left(C_{n-1}^{2k_1'}(1 - P_{U_{2k_1'|0}}(0))^{n-1} + C_{n-1}^{2k_1'-1}(1 - P_{U_{2k_1'|1}}(0))^{n-1} + C_{n}^{2k_1'-1} \right) \\
&\text{et } \forall l \in \{1, \dots, n-1\} \\
&L[l] = \sum_{k_1'=1}^{n/2} \left(C_{n-1}^{2k_1'} P_{U_{2k_1'|0}}(0)^{n-l}(1 - P_{U_{2k_1'|0}}(0))^{l-1} + C_{n-1}^{2k_1'-1} P_{U_{2k_1'|1}}(0)^{n-l}(1 - P_{U_{2k_1'|1}}(0))^{l-1} \right)
\end{aligned} \tag{2.21}$$

La distribution des énergies peut être calculée de façon similaire en étudiant le nombre de vecteurs avec $v_i = d$. Si l'on note $D[d^2]$ le nombre de vecteurs d'énergie d, on a
$$\begin{aligned}
&D[0] = \sum_{\substack{0 \le k_1 \le n \\ k_1 \ pair}} C_n^{k_1} \left(P_{U_{k_1|1}}(0) + P_{U_{k_1|0}}(0) \right) \\
&\text{et } \forall d \in \{1, \dots, \frac{n}{2}\} \quad D[d^2] = \sum_{\substack{d \le k_1 \le n \\ k_1 + d \ pair}} C_n^{k_1} \left(P_{U_{k_1|1}}(d) + P_{U_{k_1|0}}(d) + P_{U_{k_1|0}}(-d) + P_{U_{k_1|1}}(-d) \right)
\end{aligned} \tag{2.22}$$

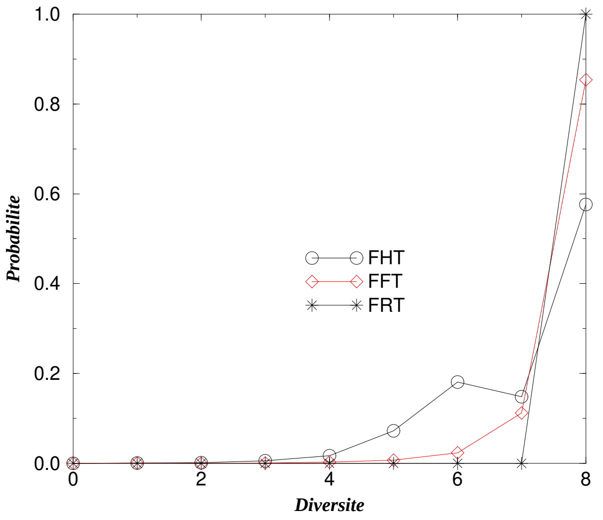


FIG. 2.5: Distribution de diversité pour une FHT, FFT et FRT avec une efficacité spectrale de 1 bit par dimension et une dimension $n = 8$.

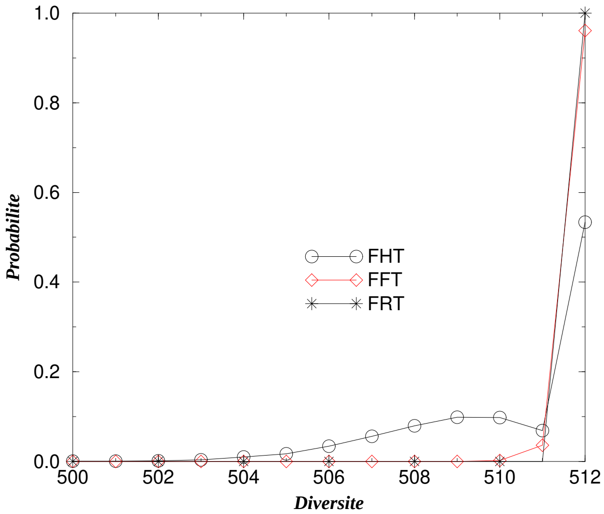


FIG. 2.6: Distribution de diversité pour une FHT, FFT et FRT avec une efficacité spectrale de 1 bit par dimension et une dimension $n = 512$.

La figure 2.6 montre la distribution de diversité pour une FRT complexe en dimension 512, une FFT complexe en dimension 512 et une FHT réelle en dimension 512. La distribution normalisée est obtenue en divisant chaque $L[l]$ par la somme totale $\sum_{l=0}^{n} L[l]$. À titre de comparaison nous présentons également en figure 2.5 les distributions de diversité d'une FHT réelle, FFT complexe et FRT complexe en dimension 8. Il apparaît que les matrices de Hadamard (et il en est de même pour celle de type Hadamard) sont celles qui ont la plus mauvaise distribution de diversité. On en déduit qu'il est indispensable, en faibles dimensions comme la dimension 8 de choisir avec soin la matrice de rotation que l'on utilisera. Au contraire, en grande dimension, comme la dimension 512, les trois distributions sont très proches. On notera à cet effet que l'axe des abscisses débute à $l = 500$. Ceci explique pourquoi pour des dimensions supérieures à 256 ces différentes rotations permettent d'atteindre des taux d'erreur similaires.

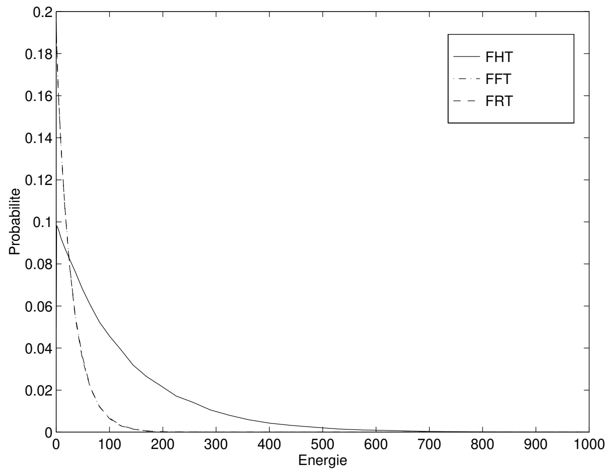


FIG. 2.7: Distribution d'énergie pour une FFT, FHT et FRT avec une efficacité spectrale de 1 bit par dimension et une dimension $n = 256$.

Un exemple de la distribution d'énergie est également donné en figure 2.7. Cette courbe montre que la matrice d'Hadamard a la pire des distributions en terme de distribution d'énergie, alors que les matrices FFT et FRT exhibent des distributions semblables.

2.5 Décodage à sortie souple des rotations en faible dimension selon le critère ML

2.5.1 Performances sur un canal avec CSI estimé parfaitement en réception

L'utilisation du décodeur par sphères rappelé au paragraphe 1.3.2 nous permet de comparer les performances respectives de différentes matrices de rotation en dimension inférieure à 32. Le canal considéré est un canal de Rayleigh non sélectif à évanouissements indépendants, et l'on suppose que le récepteur estime parfaitement le canal. Les quatre matrices aléatoires dont nous avons expliqué la construction au paragraphe 2.3.5 sont

– en dimension 8 la matrice $\mathbb{Z}_{8,4,random}$, de diversité 4, obtenue pour $a = 4$,

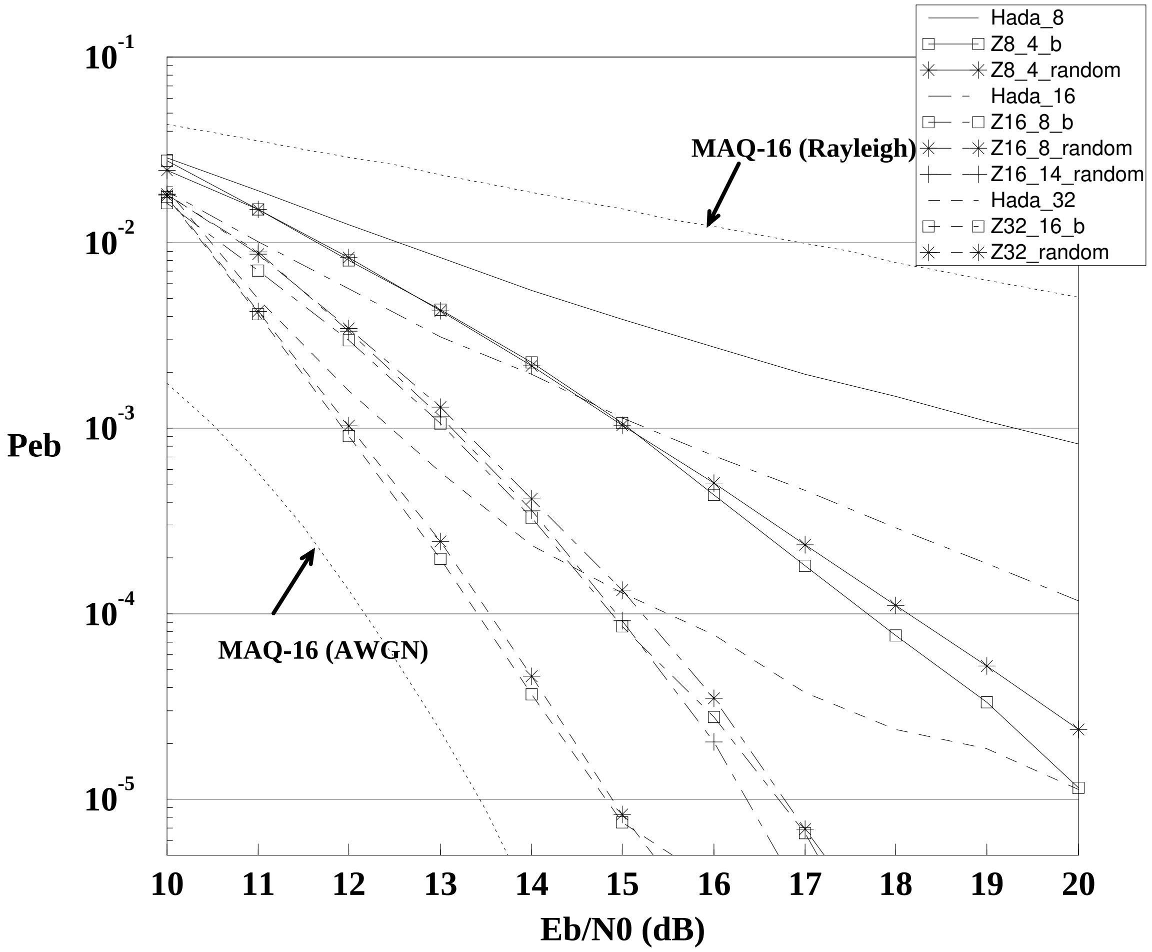


FIG. 2.8: Comparaison des performances respectives des rotations de Hadamard, algébriques et aléatoires sur le canal de Rayleigh avec décodage ML pour une efficacité spectrale de 2 bits par dimension et une parfaite connaissance du canal (CSI parfait).

- en dimension 16, les matrices $\mathbb{Z}_{16,8,random}$ et $\mathbb{Z}_{16,14,random}$, de diversités respectives 8 et 14, obtenues pour $a = 4$ et $a = 16$,
- en dimension 32 la matrice $\mathbb{Z}_{32,random}$, obtenue pour $a = 8$. Sa diversité n'a pas pu être déterminée numériquement du fait de la complexité du calcul.

L'efficacité spectrale choisie étant fixée égale à 2 bits par dimension, nous avons représenté en pointillés les performances de deux courbes de référence, soit les performances de la MAQ-16 non codée sur le canal de Rayleigh et sur le canal à bruit additif blanc gaussien. Le gain obtenu en tournant la constellation est donc évident, pour chacune des rotations simulées. Les performances des matrices de Hadamard sont cependant décevantes, en particulier pour de faibles dimensions ou à fort rapport signal à bruit : en dimension 8, pour une probabilité d'erreur par bit $P_{eb} = 10^{-3}$, les rotations algébrique $\mathbb{Z}_{8,4,b}$ et aléatoire $\mathbb{Z}_{8,4,random}$ gagnent plus de 4 dB sur la matrice d'Hadamard $Hada_8$. On constate par ailleurs que les rotations aléatoires exhibent des résultats aussi bons que les rotations algébriques, ainsi $\mathbb{Z}_{32,random}$ et $\mathbb{Z}_{32,16,b}$ sont-elles à 1.5 dB des performances sur le canal AWGN à $P_{eb} = 10^{-5}$.

2.5.2 Performances sur un canal avec CSI estimé imparfaitement en réception : étude de la robustesse du décodage

Le canal de Rayleigh réel non sélectif est classiquement modélisé par un évanouissement multiplicatif dont les coefficients $\alpha_i, i = 1, \ldots, n$ sont des variables aléatoires suivant une loi de Rayleigh et un bruit blanc additif gaussien $\mathbf{b}$. Si l'on a pu supposer dans un premier temps que l'estimation du canal était parfaite, il est sûr que ce cas idéal est rarement atteint. En effet, le circuit d'estimation de canal compris dans le récepteur commettra des erreurs du fait de la sous-optimalité de la méthode d'estimation (classiquement une interpolation) mais aussi du fait du bruit. Pour modéliser ceci, on introduit un pourcentage err d'erreur dans l'estimation de l'évanouissement sur le canal. On prendra alors au niveau du récepteur non plus le coefficient α_i utilisé à l'émission mais la valeur modifiée

$$\alpha_i * (1 + a_i) \quad i = 1, \ldots, n \tag{2.23}$$

où les a_i sont des variables aléatoires indépendantes uniformément réparties sur $[-err; err]$.

Nous avons tracé ici les courbes avec la rotation algébrique $\mathbb{Z}_{8,4,a}$ et décodage avec le décodeur par sphères en considérant une efficacité spectrale égale à 1 ou 2 bits par dimension en figures 2.9 et 2.10 respectivement. Nous nous sommes en effet restreints à cette seule rotation car les rotations $\mathbb{Z}_{8,4,random}$ et $\mathbb{Z}_{8,8}$ présentent des performances semblables.

Il apparaît qu'au-delà de 4% d'erreur d'estimation de l'évanouissement les performances du système se dégradent énormément. Ce système est donc extrêmement sensible aux erreurs d'estimation de l'état du canal. Cela ne doit pas surprendre : en effet, il s'agit ici d'un décodeur optimal, et ce type de décodeur se révèle toujours plus puissant mais moins robuste que les décodeurs sous-optimaux. Si l'on compare à présent les courbes l'une avec l'autre, on constate que la robustesse est légèrement inférieure lorsque l'on augmente le nombre de bits par dimension. Cela est dû à la plus grande fragilité des courbes d'efficacité spectrale plus élevée et n'est autre que le prix à payer pour transmettre des modulations multi-niveaux.

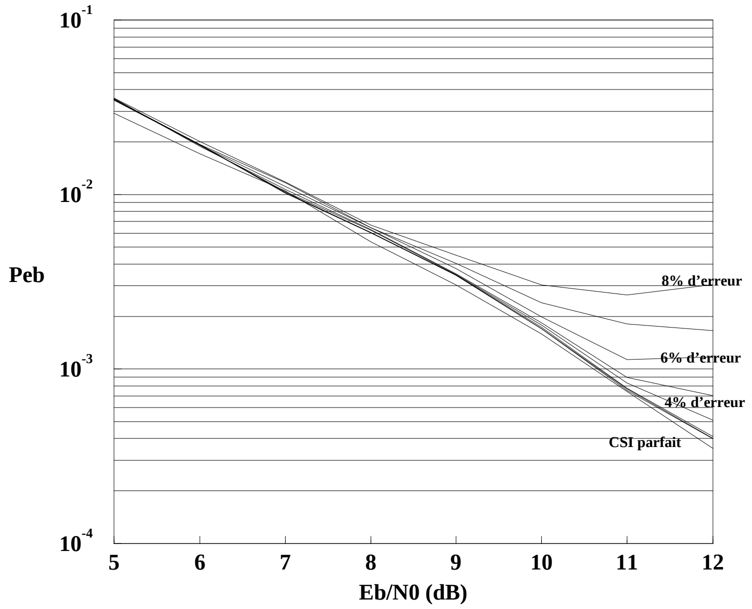


FIG. 2.9: Influence d'une mauvaise estimation de l'évanouissement sur le canal pour la rotation algébrique $\mathbb{Z}_{8,4,a}$ avec 1 bit par dimension et un facteur d'erreur allant de 0 à 8%.

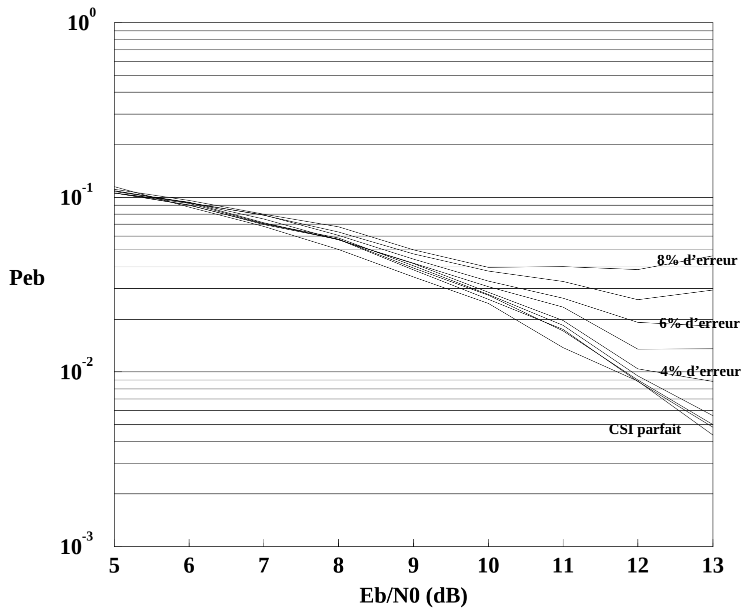


FIG. 2.10: Influence d'une mauvaise estimation de l'évanouissement sur le canal pour la rotation algébrique $\mathbb{Z}_{8,4,a}$ avec 2 bits par dimension et un facteur d'erreur allant de 0 à 8%.

2.6 Décodage à sortie souple des rotations selon le critère MMSE

2.6.1 Détermination de l'égaliseur à retour de décision (DFE) pour une rotation sur canal de Rayleigh

De même que nous avons utilisé un égaliseur à retour de décision pour décoder nous réseaux sur le canal AWGN, l'utilisation d'un DFE apparaît comme une solution intéressante pour éliminer l'interférence entre symboles générée par la rotation sur le canal de Rayleigh à évanouissements indépendants. Nous allons donc décrire dans ce paragraphe une adaptation de la méthode utilisée au chapitre 1 pour les réseaux particuliers que sont les rotations. En effet, l'utilisation d'un égaliseur est naturelle ici encore puisque, comme le montre le schéma de la figure 2.11, on a un émetteur qui applique une transformée orthogonale (rotation) aux symboles à transmettre et un récepteur qui doit supprimer l'interférence entre symboles créée par la rotation. La présence d'évanouissements impose de considérer un égaliseur autre que l'égaliseur ZF (dont le filtre serait tout simplement $R^{-1}\mathbf{D}(\alpha^{-1})$.

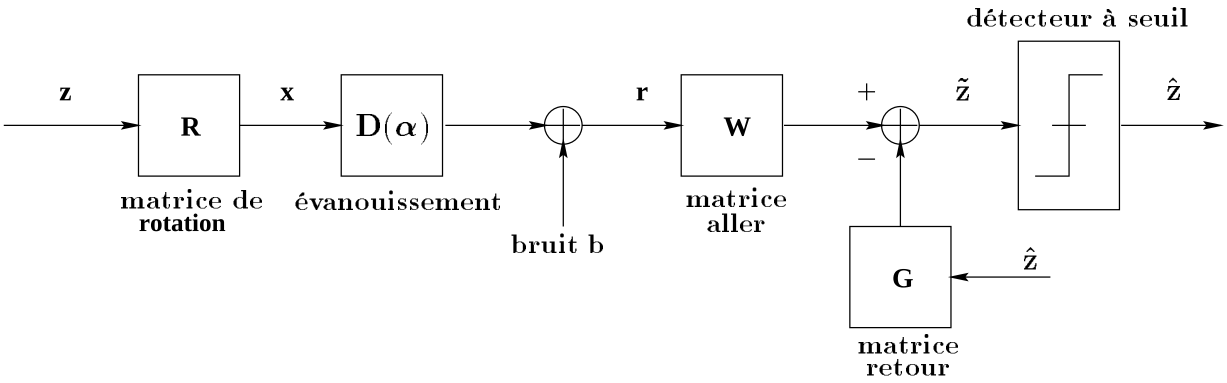


FIG. 2.11: Décodage à retour de décision d'une rotation sur canal de Rayleigh.

Le canal est décrit par une matrice diagonale d'évanouissements $\mathbf{D}(\boldsymbol{\alpha})$ et l'addition d'un vecteur de bruit blanc gaussien de variance $2N_0$ par composante complexe. Le vecteur reçu est d'abord traité par un filtre direct représenté par la matrice W. Le résultat de ce filtrage direct est ajouté à la sortie du filtre indirecte représenté par la matrice G. Le calcul des coefficients des filtres W et G, minimisant l'erreur quadratique moyenne en sortie de l'égaliseur est grandement simplifié par le fait que la matrice du réseau est ici orthogonale. En utilisant la même méthode qu'au paragraphe 1.5.1, on obtient

$$\begin{cases} W = R^{-1}\mathbf{D}(\tilde{\boldsymbol{\alpha}}) \\ G = R^{-1}\mathbf{D}(\boldsymbol{\alpha}\tilde{\boldsymbol{\alpha}})R - \frac{1}{n}trace(\mathbf{D}(\boldsymbol{\alpha}\tilde{\boldsymbol{\alpha}}))I_n \end{cases} \tag{2.24}$$

où les coefficients $\tilde{\alpha}_i$ sont donnés par :

$$\tilde{\alpha}_i = \frac{\alpha_i^*}{\sum_{i=1}^{n} |\alpha_i|^2/n + N_0}$$

On retrouve le compromis inhérent à l'égalisation MSE : la prise en compte du bruit et de la puissance du canal ne permet pas d'annuler l'IES.

2.6.2 Performances sur un canal avec CSI estimé parfaitement en réception

Les performances d'un décodeur MMSE avec une FRT en dimension 256 (la rotation algébrique donnée par le réseau $\mathbb{Z}_{512,256}$) sur le canal de Rayleigh sont montrées en figure 2.12. On peut y comparer les performances de la FRT sur le canal de Rayleigh avec celles d'une MAQ à même efficacité spectrale sur le canal gaussien. Il apparaît clairement que la perte due aux évanouissements a été supprimée : pour une probabilité d'erreur par bit $P_{eb} = 10^{-5}$, la FRT n'est qu'à 0.5 dB de la courbe de la MAQ-16 sur canal AWGN. Le canal de Rayleigh a été converti en un canal gaussien. Ce phénomène est du à l'influence de la distribution de diversité de la FRT (cet argument devenant valable dans les grandes dimensions pour les FFT et FHT également) et compense la sous-optimalité du critère MMSE.

L'égaliseur à retour de décision reposant sur le critère MMSE que nous avons considéré ici est donc un décodeur sous-optimal de très faible complexité, ce qui permet de réaliser un décodage jusqu'à des valeurs de n de l'ordre de 1024. Jusqu'à présent, afin d'en évaluer les performances, nous avons considéré que les valeurs fournies en entrée du filtre de retour G sont parfaites (soit égales aux valeurs d'entrée du codeur). Les résultats de simulation nous prouvent que ce système "parfait" fonctionne très bien, et l'on parvient à transformer le canal de Rayleigh en un canal gaussien.
Le problème qui se pose ensuite est celui du calcul de la valeur "pratique" à introduire en entrée du filtre de retour G. En effet, nous avons pu constater par simulation que la méthode classique qui consiste à faire une première itération avec un seul filtre, soit un filtre aller W seul (dont la formule est alors celle d'un simple égaliseur MSE sans retour de décision) et d'en déduire les entrées à utiliser dès la seconde itération avec le DFE pour W et G ne permet pas, même après de nombreuses itérations du système, d'atteindre les performances souhaitées lorsque le filtre W seul est suivi d'un simple détecteur à seuil. Nous proposons l'introduction d'un code correcteur convolutif dans le schéma du codeur. Ce code correcteur sera décodé à la première itération (W seul) par un algorithme de Viterbi, la sortie de cet algorithme étant introduite dans G avant la sommation avec la sortie retardée de W (W non seul) et un nouveau passage par un décodeur de Viterbi remplaçant le détecteur à seuil précédent. En pratique, on atteint la convergence avec ce système dès la deuxième itération, soit le deuxième Viterbi. Nous présentons un schéma explicatif de ce nouveau système en figure 2.13 dans le cas où il n'y a que deux itérations.

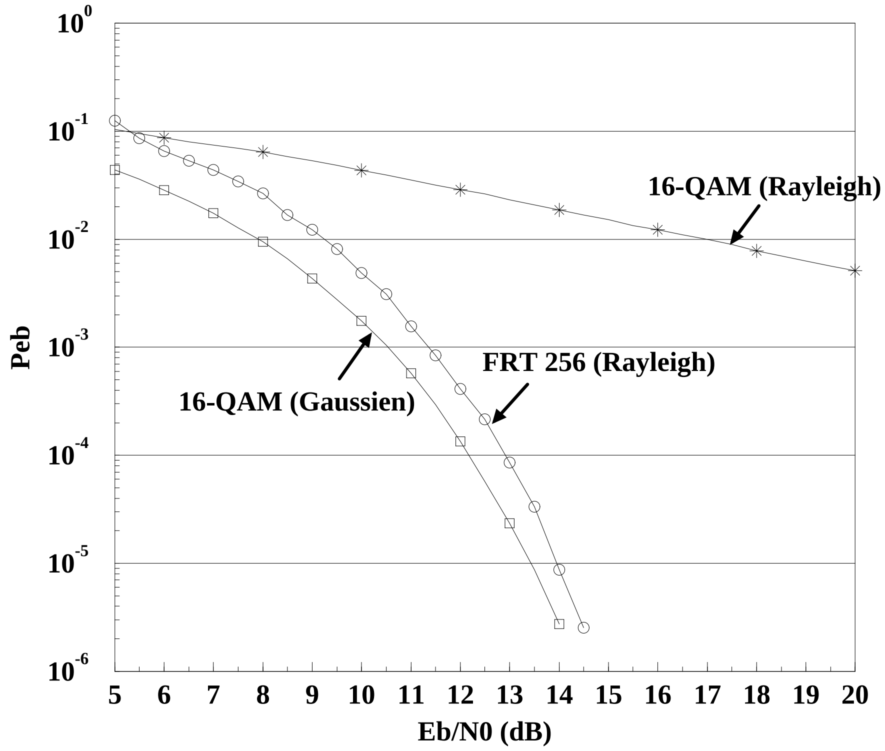


Fig. 2.12: Taux d'erreur binaire pour une FRT de dimension $n = 256$ avec une efficacité spectrale $\eta/2 = 2$ bits par dimension.

On notera que comme toujours lorsque l'on utilise un décodeur de Viterbi une gestion des délais s'impose : il s'agit ici de resynchroniser les sorties de W et de G pour la deuxième itération. On notera également que la matrice W est alternativement celle correspondant à la première itération (W seul), tantôt celle correspondant à la formule (2.24).

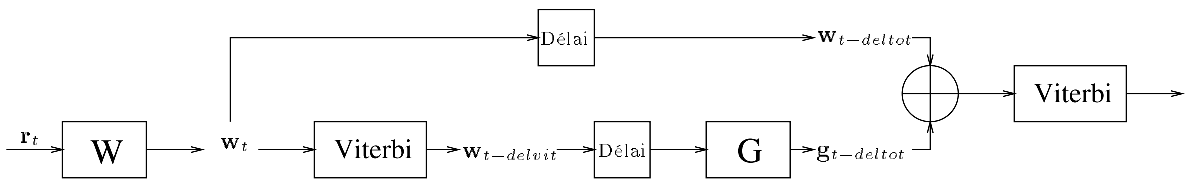


Fig. 2.13: Schéma partiel de l'égaliseur à retour de décisions avec les deux itérations du décodeur de Viterbi interne.

La figure 2.14 montre les performances du système pour une efficacité spectrale de 1 bit par dimension, tout d'abord lorsque l'entrée du filtre de retour est alimentée “parfaitement” et également lorsque le retour se fait avec l'aide d'une modulation PAM-4 de taux 1/2 codée en treillis (TCM) décodée par un algorithme de Viterbi. Le prix à payer est donc une diminution de l'efficacité spectrale (on passe ici à 1/2 bit par dimension) mais la convergence est atteinte grâce à l'introduction du code et de son décodeur de Viterbi. On notera cependant que si le gain reste manifeste comparativement à la $MAQ-4$ seule sur canal de Rayleigh, ce système pratique perd 3.5 dB pour un probabilité d'erreur par bit d'information $P_{eb} = 10^{-6}$ par rapport au cas théorique où l'entrée retour du DFE est "parfaite".

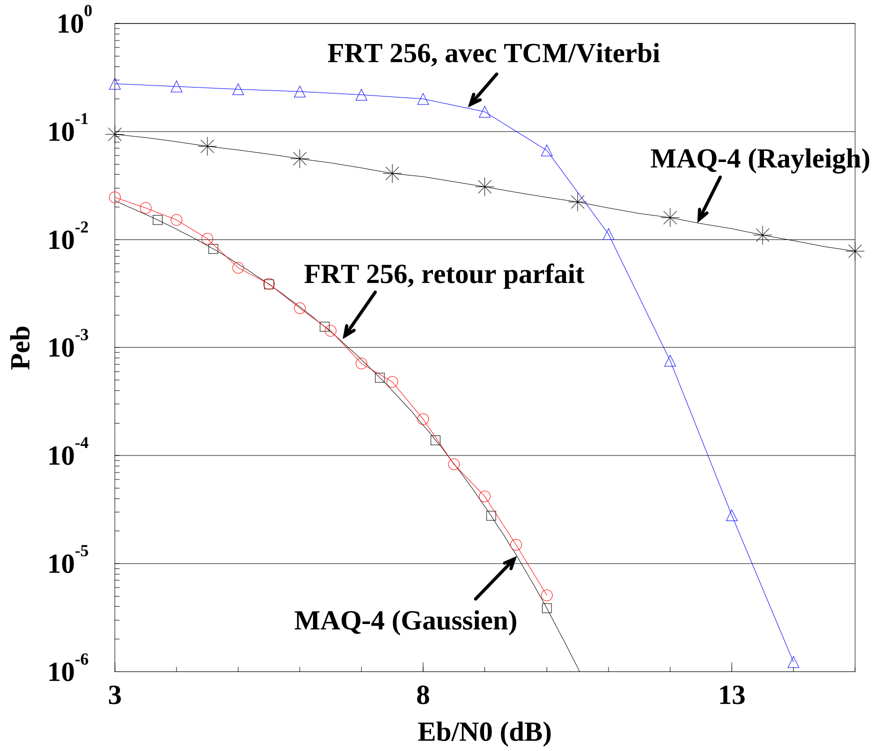


FIG. 2.14: Taux d'erreur binaire pour une FRT de dimension $n = 256$ avec une efficacité spectrale $\eta/2 = 1$ bit par dimension.

2.6.3 Performances du DFE sur un canal avec CSI estimé imparfaitement en réception : étude de la robustesse du décodage

Comme dans le décodage ML réalisé avec le décodeur par sphères, nous nous intéressons ici à la robustesse du décodage, observant les performances lorsque l'estimation de l'état du canal n'est pas parfaite. Nous avons tracé ici les courbes avec la FRT en dimension $n = 256$ et un décodage avec l'égaliseur à retour de décision en considérant une efficacité spectrale égale à 1 ou 2 bits par dimension en figures 2.15 et 2.16 respectivement en faisant varier l'estimation des évanouissements $\alpha_i, i = 1, \ldots, n$ selon la formule (2.23).

Il convient néanmoins de souligner la très grande différence existant avec le cas du déco-

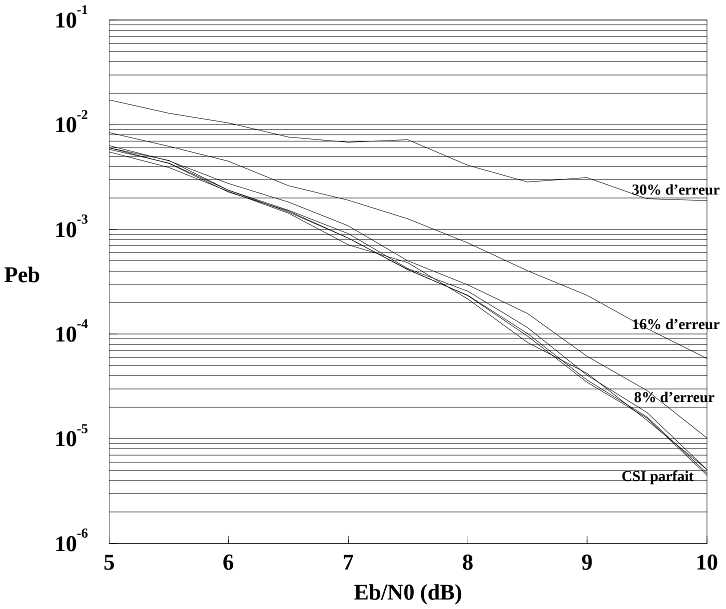


Fig. 2.15: Influence d'une mauvaise estimation de l'évanouissement sur le canal pour une FRT de taille 256 avec 1 bit par dimension et un facteur d'erreur de 0, 1, 2, 4, 8, 16 ou 30%.

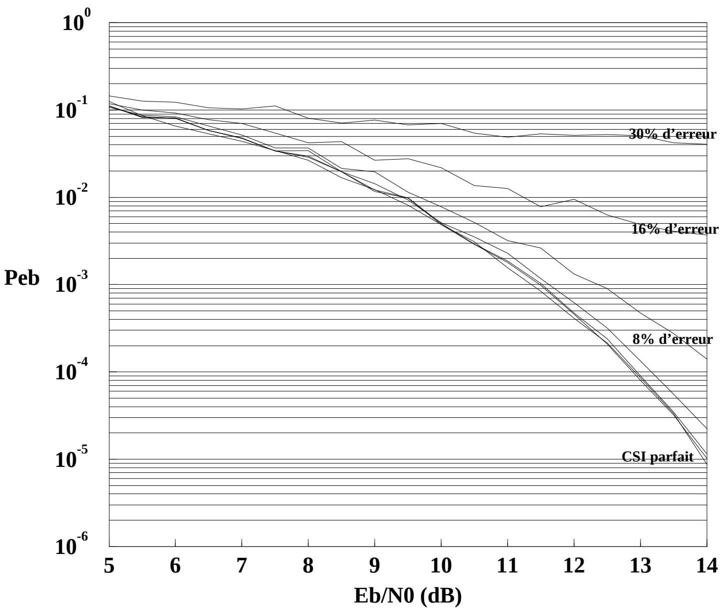


Fig. 2.16: Influence d'une mauvaise estimation de l'évanouissement sur le canal pour une FRT de taille 256 avec 2 bits par dimension et un facteur d'erreur de 0, 1, 2, 4, 8, 16 ou 30%.

deur par sphères : alors que les performances de ce premier système se dégradent dès 4% d'erreur, celle du système FRT+DFE sont encore excellentes avec 8% et ne commencent vraiment à se dégrader qu'à partir de 16% d'erreur. La robustesse du DFE en matière de résistance à une mauvaise estimation du canal est donc un grand point en sa faveur. Comme dans le cas du décodeur par sphères, la robustesse est légèrement inférieure lorsque l'on augmente le nombre de bits par dimension, ceci étant dû à la plus grande fragilité des systèmes d'efficacité spectrale plus élevée et étant le prix à payer pour transmettre des modulations multi-niveaux.

Ayant ainsi pu apprécier les performances du système FRT+DFE lors d'une mauvaise estimation de l'évanouissement, nous avons également étudié son comportement lors d'une mauvaise estimation de la phase. Nous avons en effet jusqu'à présent supposé que la démodulation était cohérente. Or ceci implique une estimation de la phase du signal, c'est-à-dire de la phase de la porteuse mais également de la fréquence doppler ajoutant une phase résiduelle en $2\pi\ f_d\ t$. Du fait du désentrelacement des symboles reçus par le récepteur, l'effet doppler n'est plus modélisable par l'ajout d'une phase linéaire mais par celle d'une phase aléatoire uniformément répartie. L'erreur d'estimation de la phase du signal due à la méthode d'estimation étant également considérée comme une variable aléatoire uniformément répartie, il suffira de considérer le cas d'une erreur de phase aléatoire. On introduit donc une erreur maximale de phase err et pour des signaux complexes, on recevra

$$\alpha(point * e^{ja}) \tag{2.25}$$

où a exprimé en radians est uniformément répartie sur $[-err; err]$, α est le coefficient d'évanouissement (correctement estimé) et $point$ représente le point tourné par la FRT.

Nous avons tracé ici les courbes avec la FRT en dimension $n = 256$ et un décodage avec l'égaliseur à retour de décision en considérant une efficacité spectrale égale à 1 ou 2 bits par dimension en figures 2.17 et 2.18 respectivement en faisant varier l'estimation de la phase selon la méthode expliquée formule (2.25). Dans le cas d'une efficacité spectrale égale à 1 bit par dimension, la robustesse est très grande, puisqu'une erreur de phase de 6 degrés est quasiment sans effet. Pour une efficacité spectrale plus grande, les performances se dégradent un peu mais sans pour autant atteindre des proportions alarmantes.

2.7 Décodage itératif des rotations

Ayant observé que les modulations tournées sur canal de Rayleigh atteignaient des performances proches de celles sur le canal AWGN, et que de manière générale les rotations permettaient d'approcher plus rapidement la capacité sur le canal de Rayleigh (voir chapitre 4), nous avons décidé d'explorer les performances de ces modulations lorsque l'on ajoute un code correcteur d'erreur. Nous nous sommes en particulier intéressés aux codes de haut rendement, correspondant à un taux où la rotation permet théoriquement de forts gains (voir paragraphe 4.3).

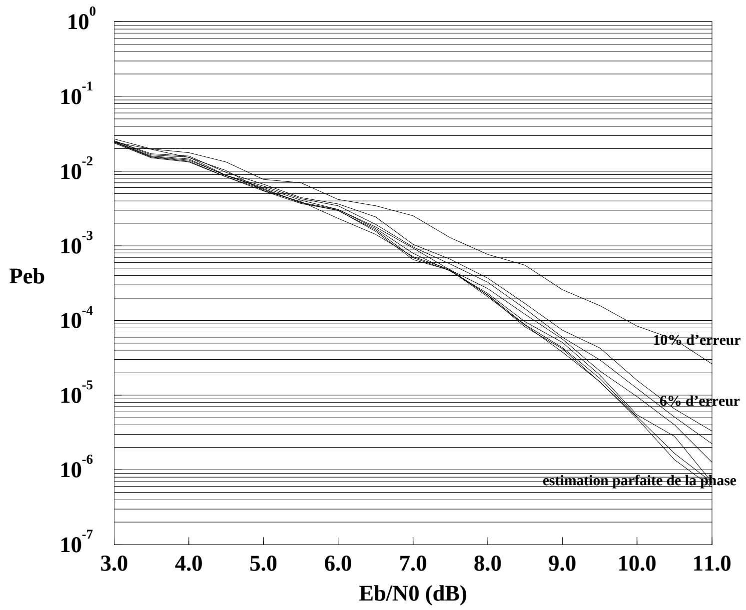


Fig. 2.17: Influence d'une mauvaise estimation de la phase du canal pour une FRT de taille 256 avec 1 bit par dimension et une erreur de phase de 0 à 6 degrés ou 10 degrés.

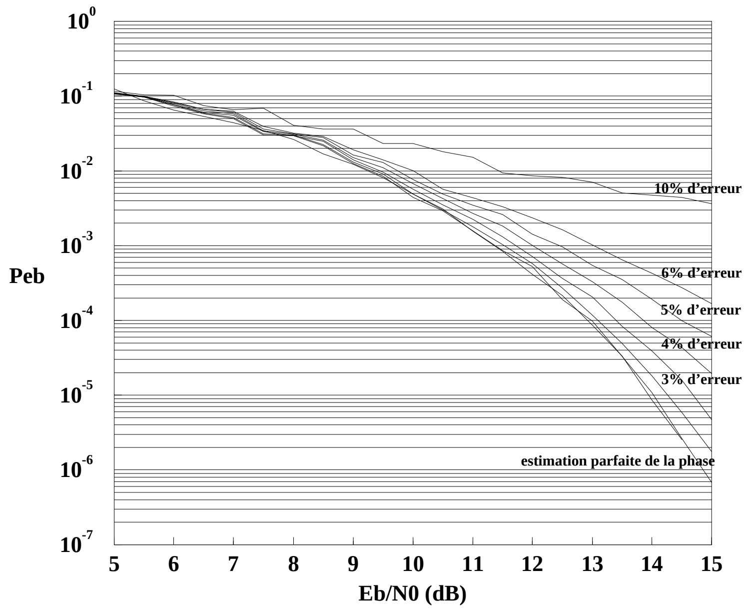


Fig. 2.18: Influence d'une mauvaise estimation de la phase du canal pour une FRT de taille 256 avec 2 bits par dimension et une erreur de phase de 0 à 6 degrés ou 10 degrés.

Or, les performances de notre égaliseur à retour de décision n'apparaissant pas suffisamment bonnes, ne serait-ce qu'en terme d'efficacité spectrale, lorsqu'un code est ajouté, nous proposons d'aborder le problème selon un axe différent, le décodage itératif.

2.7.1 Réalisation du décodage itératif par conversion des observations en probabilités a posteriori (APP)

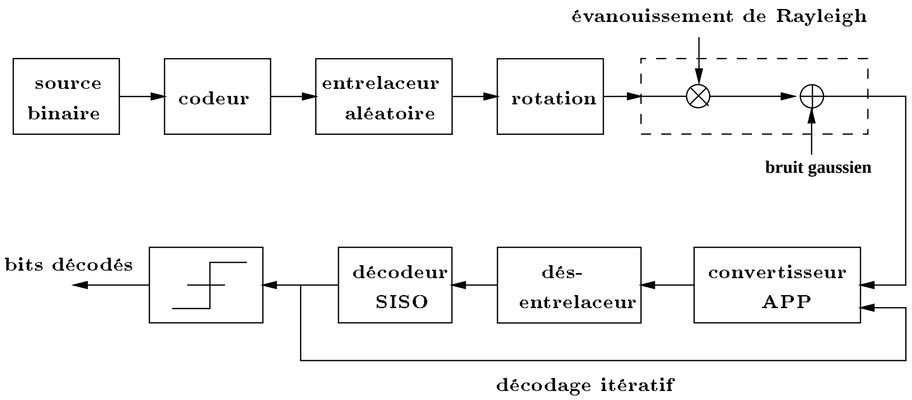


FIG. 2.19: Système combinant rotation et codage.

Considérons donc le codeur présenté en figure 2.7.1. Les bits générés aléatoirement sont codés par un code convolutif classique, puis entrelacés de manière pseudo-aléatoire pour être transmis sur un canal de Rayleigh non sélectif à évanouissements indépendants. Il s'agit donc d'une modulation codée avec entrelacement de bits (BICM) [23] où la rotation fait office de modulateur.

Pour décoder ce système, qui peut être vu comme une concaténation série d'un code extérieur (le code convolutif) et d'un modulateur de canal (la rotation), nous allons utiliser un décodage itératif APP dont les performances dans le décodage de système concaténés sont bien connues [11][40]. L'opération de décodage du canal correspond donc au calcul des probabilités *a posteriori* (APP) des bits codés c_j, $j = 1, \ldots, n$ supposés indépendants entre eux.

$$\begin{aligned} APP(c_j) &= p(c_j|\mathbf{y}) \\ &= \frac{p(\mathbf{y}|c_j) \cdot \pi(c_j)}{p(\mathbf{y})} \qquad j = 1, \ldots, n \\ APP(c_j) &\propto \pi(c_j) \cdot p(\mathbf{y}|c_j) = \pi(c_j) \cdot obs(c_j) \end{aligned} \tag{2.26}$$

où $\pi(c_j)$ est la probabilité *a priori* du bit codé c_j et où l'on définit l'observation sur c_j par $obs(c_j) = p(\mathbf{y}|c_j)$.

La densité de probabilité conditionnelle $p(\mathbf{y}|c_j)$ est obtenue en marginalisant la densité de probabilité jointe de tous les bits codés et de l'observation, en tenant compte du fait que les composantes y_r du vecteur $\mathbf{y}$ reçu sont indépendantes conditionnellement à l'ensemble des bits codés $c_1, \ldots, c_n$

$$
\begin{aligned}
p(\mathbf{y}|c_j) &= \sum_{\substack{c_i \in \{0,1\} \\ i=1,\ldots,n,\, i \neq j}} p(\mathbf{y}, c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_n | c_j) \\
&= \sum_{c_i \in \{0,1\},\, i=1,\ldots,n,\, i \neq j} p(\mathbf{y}|c_1, \ldots, c_n) \prod_{l \neq j} \pi(c_\ell) \\
&= \sum_{\substack{c_i \in \{0,1\} \\ i=1,\ldots,n,\, i \neq j}} \left(\prod_{r=1}^{n} p(y_r|c_1, \ldots, c_n) \prod_{l \neq j} \pi(c_\ell) \right)
\end{aligned}
\tag{2.27}
$$

où la densité de probabilité conditionnelle $p(y_r|c_1, \ldots, c_n)$ est égale à

$$
p(y_r|c_1, \ldots, c_n) = \frac{e^{-\frac{\|y_r - \alpha_r x_r\|^2}{2N_0}}}{(2\pi N_0)} \tag{2.28}
$$

où α_r est l'évanouissement affectant la $r^{ème}$ composante émise x_r.

Ces informations *a posteriori* sont fournies à un décodeur à entrées souples et sorties souples (SISO) [13] qui génère à chaque itération les informations extrinsèques $Ext(c_j)$ équivalentes à de nouvelles probabilités *a priori* $\pi(c_j)$ pour les bits codés c_j. On peut alors fournir ces nouvelles informations *a priori* en entrée du convertisseur APP, ce qui permet d'améliorer l'estimation des probabilités *a posteriori*.

2.7.2 Résultats de simulation

Les figures 2.20 et 2.21 montrent les performances de deux codes non récursifs non systématiques (NRNSC) sur un canal de Rayleigh non sélectif à évanouissements indépendants. Le premier code est de rendement 1/2, de générateurs $(23, 35)$ en octal et de taille d'entrelaceur $N = 2056$, et le second est de rendement 2/3, de générateurs $(27, 75, 72)$ en octal et de taille d'entrelaceur $N = 3072$. Dans les deux cas, les treillis sont ramenés à l'état zéro par utilisation de bits de fermeture (*tail bits*). Nous utilisons pour nos simulations différentes matrices de rotation en dimension 8. On observe entre autres que les rotations $\mathbb{Z}_{8,4,a}$, $OP_{2,8}$ et $\mathbb{Z}_{8,4,random}$ ont des performances quasiment identiques et donnent les meilleurs résultats. Dans un souci de clarté, nous ne représenterons donc que l'une

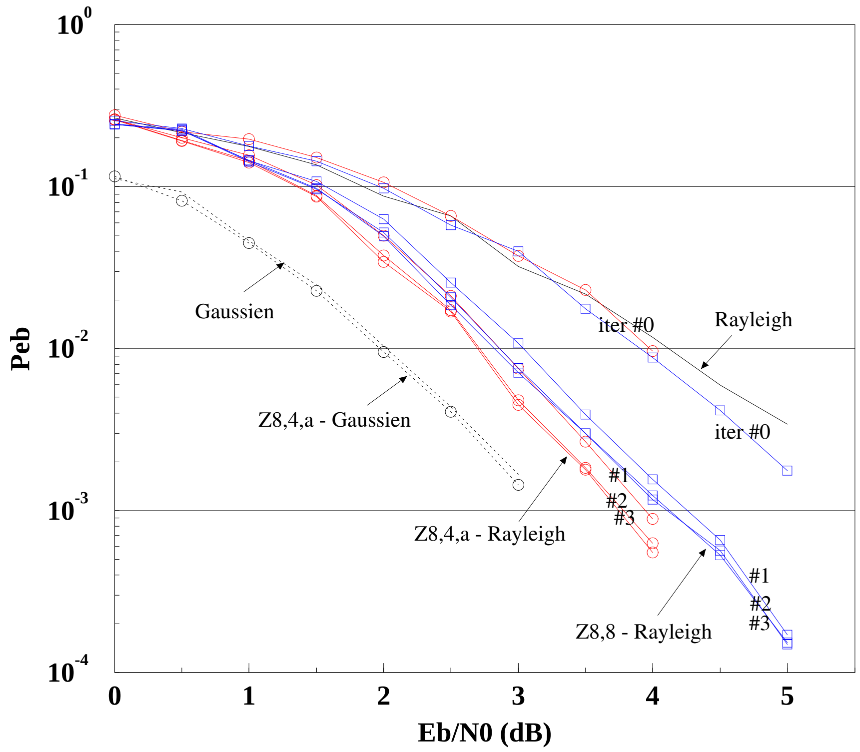


FIG. 2.20: Taux d'erreur binaire pour un code convolutif de rendement $\frac{1}{2}$ combiné avec des rotations en dimension 8.

des trois, soit $\mathbb{Z}_{8,4,a}$. Comme nous le verrons au chapitre 4, si cette rotation n'est pas la meilleure en terme de capacité, elle en est très proche, se situant à environ 0.1 dB de la matrice de rotation $Hada_8$ pour des taux de codage 1/2 et 2/3 (voir figure 4.8).

Le gain obtenu grâce au décodage itératif est évident, et de plus on constate qu'il est atteint presque complètement après seulement trois itérations, ce qui correspond à un délai de traitement raisonnable pour des applications pratiques. D'après la figure 2.20, on observe un gain d'environ 2 dB après la $4^{ème}$ itération pour un taux de codage de 1/2, ce qui place notre code à seulement 0.6 dB des performances sur le canal AWGN pour un taux d'erreur de $5 \cdot 10^{-3}$.

On notera également que le décodage itératif APP ne peut être utilisé ici que parce que la rotation agit comme un second code dans le schéma concaténé : ainsi, les performances sur le canal de Rayleigh lorsque la matrice de rotation est remplacée par l'identité I_8 sont-elles confondues, à toutes les itérations, avec celle d'une BPSK codée sur canal de Rayleigh sans rotation. De même, une rotation n'apporte-t-elle aucun gain sur le canal AWGN, comme le montre la courbe de la rotation $\mathbb{Z}_{8,4,a}$ sur le canal gaussien, superposée à toutes les itérations avec celle d'une BPSK codée sur canal AWGN.

Si nous considérons à présent les résultats obtenus pour un rendement 2/3, où le gain

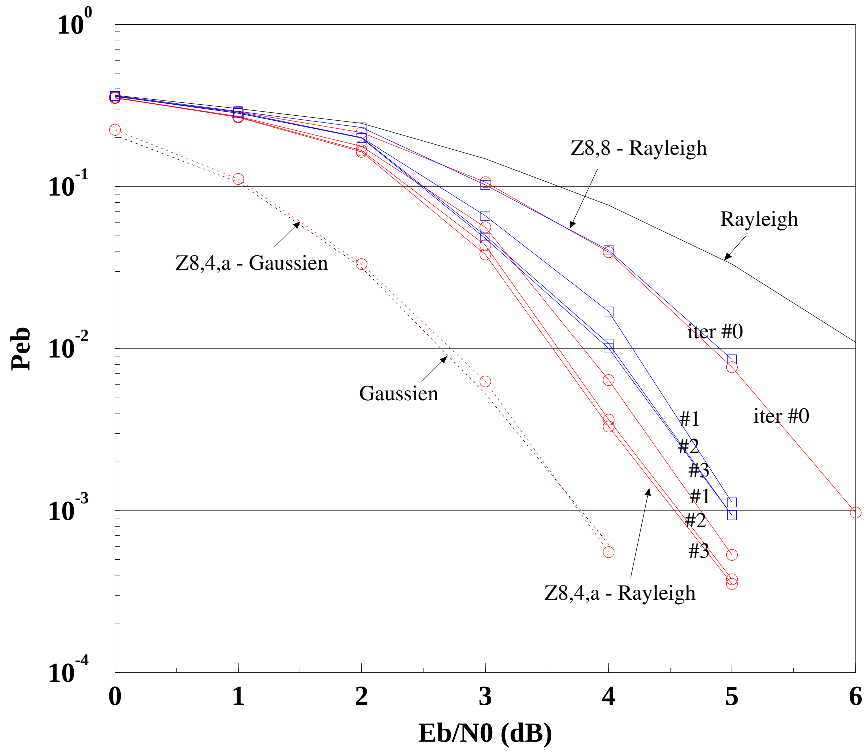


Fig. 2.21: Taux d'erreur binaire pour un code convolutif de rendement $\frac{2}{3}$ combiné avec des rotations en dimension 8.

potentiel, d'après la courbe de capacité des rotations en dimension 8 (voir figure 4.8), les performances tendraient à être meilleures, on observe effectivement un gain plus grand par rapport aux performances du code seul sur canal de Rayleigh. On note en effet que même la première itération améliore-t-elle les résultats de manière significative ! Le gain total est cependant légèrement inférieur à celui obtenu pour un code de rendement 1/2 puisque la modulation tournée sur canal de Rayleigh atteint des performances situées à 0.9 dB de celle sur canal AWGN.

2.8 Conclusions

Après avoir rappelé différents types de rotations existant dans la littérature, nous avons proposé dans ce chapitre une transformation rapide, dite *Transformée de Rotation Rapide* (FRT) qui permet d'utiliser les rotations algébriques $\mathbb{Z}_{n,n/2}$ construites par plongement canonique dans de grandes dimensions. Nous avons également introduit d'autres rotations comme celles construites à partir des polynômes de Tchebicheff, ou les rotations aléatoires construites comme des généralisations des matrices de Hadamard. Nous avons également étudié les distributions de diversité de certaines de ces matrices de rotation, calculant en particulier celle des matrices de type Hadamard.

Ces rotations nous ont permis de générer des MAQ multidimensionnelles tournées non codées pour lesquelles nous avons exploré plusieurs méthodes de décodage. Nous avons ainsi appliqué tout d'abord l'algorithme de décodage par sphères sur le canal de Rayleigh, et abordé le problème de sa robustesse face à une mauvaise estimation du canal. Nous avons également étudié les performances d'un égaliseur à retour de décision reposant sur le critère MMSE pour le décodage des rotations en grande dimension, en particulier de nos FRT. Nous avons proposé d'introduire une modulation codée en treillis décodée par un Viterbi afin d'améliorer considérablement les entrées du filtre de retour. Une étude de la robustesse de cet algorithme face à une mauvaise estimation du canal a également été réalisée. Nous avons enfin proposé un système combinant une rotation en petite dimension et un code correcteur d'erreur, que nous avons décodé de manière itérative. Les performances de ce dernier décodeur, en particulier, sont extrêmement satisfaisantes puisque l'on se situe, à la $4^{ème}$ itération, avec une rotation en dimension 8 et un code de rendement 1/2 ou 2/3, à moins de 1 dB des performances sur le canal AWGN pour un taux d'erreur par bit de $5 \cdot 10^{-3}$.

Chapitre 3

Modulations pour les antennes multiples *

Il ne faut pas mettre tous ses oeufs dans le même panier
proverbe paysan

3.1 Introduction

Les systèmes à antennes multiples, dont un exemple est présenté en figure 3.1, sont d'un intérêt certain lorsqu'on les compare à des systèmes classiques n'utilisant qu'une antenne en émission et en réception. En effet, si l'espacement est suffisant entre les antennes, de manière générale, si elles sont distantes les unes des autres d'au moins une demi-longueur d'onde, les canaux liant les antennes d'émission aux antennes de réception peuvent être considérés comme indépendants les uns des autres, les observations au niveau des différentes antennes de réception étant donc totalement décorrélées : c'est ce qu'on appelle de la *diversité d'antennes*, ici égale au nombre d'antennes de réception.

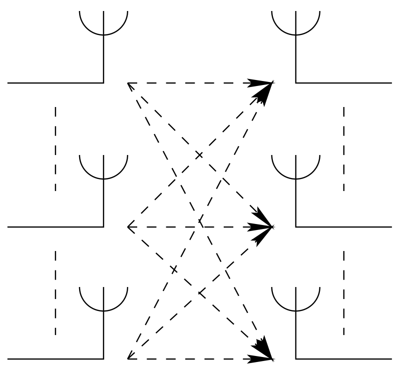


Fig. 3.1: Schéma de principe d'un canal à entrées et sorties multiples.

*Certaines parties de ce chapitre ont été soumis au journal IEEE Transactions on Communications [85].

Pour une même puissance d'émission, on obtient donc plusieurs versions du signal émis. Ainsi, alors que, dans le cas où l'on ne disposait que d'une seule antenne, une position de réception avec un fort évanouissement sur le canal rendait très difficile la récupération de l'information, l'utilisation de plusieurs antennes, avec des répercutions différentes engendrées par les réflexions sur les obstacles, amènera à un résultat bien meilleur, puisque l'on peut statistiquement espérer qu'elles ne seront pas totalement destructrices sur tous les canaux en même temps.

En ce qui concerne les antennes d'émission, différentes approches en terme de transmission de l'information sur les antennes d'émission sont envisageables. Comme nous sommes intéressés par l'augmentation de l'efficacité spectrale effectivement transmise par notre système, le choix trivial d'émettre les mêmes signaux sur chaque antenne, par répartition de la puissance totale d'émission par bit d'information sur toutes les antennes, ne nous intéresse pas. Nous allons en effet utiliser nos différentes antennes d'émission pour émettre des signaux différents, augmentant ainsi notre efficacité spectrale d'un facteur égal à ce nombre d'antennes. Enfin, puisque l'émetteur ne dispose d'aucune connaissance *a priori* du canal, chaque antenne émettra avec la même puissance (allocation uniforme de puissance pour des antennes décorrélées).

Pour une même puissance d'émission, un système avec plusieurs antennes d'émission et de réception apportera donc un gain conséquent à la fois en termes d'efficacité spectrale et de résistance aux évanouissements. Ceci ne se fera bien sûr pas gratuitement, un tel système étant plus coûteux du fait du nombre d'antennes nécessaires. Le traitement des informations sera, quant à lui, plus complexe.
On notera également qu'il n'est pas toujours possible de multiplier les antennes à volonté : ainsi, dans le cas d'une transmission sur le canal radio-mobile, autant est-il relativement aisé d'ajouter plusieurs antennes à la station de base, autant la taille d'un téléphone mobile, important critère de choix pour l'utilisateur moderne, empêche de placer plus de deux à quatre antennes séparées de la demi-longueur d'onde nécessaire pour la décorrélation des canaux. Dans nos exemples numériques, nous nous limiterons donc principalement au cas d'un système symétrique avec deux antennes en émission et deux antennes en réception. Lorsque l'utilisation de plusieurs antennes n'est pas possible, une solution qui pourrait être utilisée serait de suréchantillonner le signal, en s'appuyant sur le fait que le suréchantillonnage temporel et le suréchantillonnage spatial obtenu grâce aux antennes multiples sont mathématiquement équivalents [37].

Le chapitre est organisé comme suit : le modèle du système à entrées et sorties multiples est présenté au paragraphe 3.2. Les performances des systèmes multi-antennes y sont rappelées et le codeur ainsi que les notations utilisées dans le chapitre sont introduites. Nous proposons un décodeur au paragraphe 3.3, en expliquant la méthode de calcul des probabilités *a posteriori* et le processus de détection/décodage itératif utilisés. Nous introduisons au paragraphe 3.4 une méthode d'estimation itérative des paramètres du canal MIMO grâce à l'algorithme EM. Ce système a été simulé pour différents codes correcteurs d'erreur, et des résultats de simulation sont présentés au paragraphe 3.5. Finalement nous tirerons quelques conclusions au paragraphe 3.6.

3.2 Modèle du système à entrées multiples et sorties multiples

3.2.1 Modèle du canal et notations

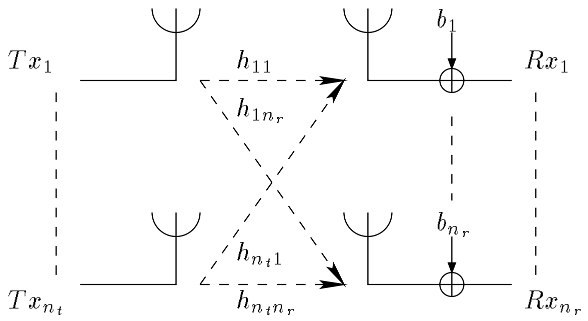


FIG. 3.2: Canal à entrées et sorties multiples avec coefficients du canal.

Le milieu de communication reliant les n_t antennes d'émission (Tx) et les n_r antennes de réception (Rx), présenté en figure 3.2, est un canal de Rayleigh à entrées multiples et sorties multiples. À l'instant $k \in \mathbb{Z}$, i.e. à chaque période symbole, la sortie du canal est constituée de la superposition des n_t symboles transmis pondérés par la réponse impulsionnelle du canal. Ceci peut être exprimé par

$$\mathbf{y}(k) = H(k) \cdot \mathbf{x}(k) + \mathbf{b}(k) \tag{3.1}$$

où, à l'instant k, $\mathbf{y}(k) = (y_i(k))^t{}_{i=1,\ldots,n_r}$ est le vecteur du signal reçu, $\mathbf{x}(k) = (x_j(k))^t{}_{j=1,\ldots,n_t}$ est le vecteur du signal émis, $H(k) = [h_{i,j}(k)]_{i=1,\ldots,n_r,j=1,\ldots,n_t}$ est la matrice du canal et $\mathbf{b}(k) = (b_i(k))^t{}_{i=1,\ldots,n_r}$ est le bruit blanc additif gaussien complexe de moyenne nulle et de variance $2\sigma^2 = 2N_0$ (on notera que σ^2 est la variance de bruit par composante).

Afin de simplifier les notations et de les rendre plus lisibles, nous omettrons par la suite l'indice de temps k lorsqu'il n'est pas indispensable.

Les coefficients du canal $h_{i,j}(k) \in \mathbb{C}$ sont gaussiens, indépendants, et vérifient $E[|h_{i,j}(k)|^2] = 1$. Nous considérerons dans ce chapitre deux types de canaux. Le premier type correspond à un canal de Rayleigh "classique", soit non statique où les coefficients gaussiens complexes $h_{i,j}(k)$ changent aléatoirement et indépendamment à chaque période symbole. Le second type est un canal statique par blocs ou "Rayleigh par blocs" qui garde constantes les valeurs des coefficients $h_{i,j}(k)$ à l'intérieur d'une même trame.

3.2.2 Performances des systèmes multi-antennes

L'emploi d'un système à antennes multiples, ou de manière équivalente l'utilisation de canaux à entrées multiples et sorties multiples (MIMO) permet d'améliorer considérable-

ment les performances et l'efficacité spectrale, et ainsi de fournir des solutions aux besoins modernes en terme de bande passante et de qualité de transmission, comme Tarokh *et al.* l'ont mis en évidence avec des modulations codées en treillis [69][70], ou comme cela a été proposé plus récemment pour des turbo-codes [67].
Avant de présenter le système que nous proposons, qui combine une modulation codée avec entrelacement de bits [81][23] et un canal MIMO, nous proposons tout d'abord quelques rappels sur les performances théoriques des systèmes mono- et multi-antennes afin de comprendre les gains que nous pourrons observer.

Performances d'un système mono-antenne sur un canal AWGN

Rappelons tout d'abord la formule classique de la probabilité d'erreur par bit P_{eb1} d'un système de transmission sans codage sur canal à bruit additif blanc gaussien lorsque la modulation utilisée est une MAQ-M (voir annexe C.1) :

$$P_{eb1} \leq \frac{4}{\log_2 M} Q\left(\sqrt{\frac{2E_b}{N_0}\frac{3\log_2 M}{2(M-1)}}\right) \tag{3.2}$$

où E_b est l'énergie moyenne par bit sur fréquence porteuse, $N_0/2$ la densité spectrale du bruit blanc gaussien sur fréquence porteuse et Q est la fonction d'erreur.

Performances d'un système mono-antenne sur un canal de Rayleigh

Pour le canal de Rayleigh, le calcul de l'espérance mathématique sur tous les évanouissements avec utilisation de l'approximation de la fonction Q nous permet d'obtenir une borne sur la probabilité d'erreur par bit P_{eb2} d'un système de transmission sans codage sur canal à évanouissement de Rayleigh lorsque la modulation utilisée est une MAQ-M (voir annexe C.2) :

$$P_{eb2} \leq \frac{2}{\log_2 M}\left(\frac{3\log_2 M}{2(M-1)} \times \frac{E_b}{N_0} + 1\right)^{-1} . \tag{3.3}$$

Performances d'un système MIMO sur un canal de Rayleigh

Lorsque l'on considère à présent un canal de Rayleigh à entrées et sorties multiples, il apparaît que les antennes de réception (au nombre de n_r) créent une diversité de n_r alors que les antennes d'émission (au nombre de n_t) vont permettre de multiplier le débit binaire par un facteur n_t tout en générant une perte en terme de rapport signal à bruit négligeable. La probabilité d'erreur par paire de décoder $V = (V_1, \ldots, V_{n_t})$ lorsque c'est

$U = (U_1, \ldots, U_{n_t})$ qui a été émis s'écrit : (voir annexe C.3)

$$P(U \to V) \leq \frac{1}{2} \left[\frac{1}{1 + \frac{\sum_{i=1}^{n_t} |V_i - U_i|^2}{8N_0}} \right]^{n_r} . \tag{3.4}$$

D'où une borne sur la probabilité d'erreur par bit d'information

$$P_{eb3} \leq \kappa(M, n_t) \left(\frac{E_b}{N_0} \right)^{-n_r} \tag{3.5}$$

où $\kappa(M, n_t)$ est une constante dépendant uniquement de la constellation MAQ choisie et du nombre d'antennes d'émission n_t.

En présence d'un code correcteur d'erreurs, il est possible d'augmenter l'ordre de diversité de la formule 3.4 jusqu'à la valeur maximale $\ell \times n_r$, où ℓ est la longueur du code considéré.

Performances d'un système MIMO sur un canal de Rayleigh par blocs

Dans le cas où le canal de Rayleigh est constant sur une durée de ℓ blocs, le calcul précédent ne peut être reproduit tel quel. Comme présenté pour la première fois par Tarokh *et al.* [69], il nous faut introduire la matrice hermitienne définie positive $A(U, V) = (A_{pq})_{p,q=1,\ldots,n_t}$ où $A_{pq} = \sum_{k=1}^{\ell} (V_p^k - U_p^k)(V_q^k - U_q^k)^*$ dont les r valeurs propres strictement positives $\lambda_i, i = 1, \ldots, r$ nous permettent d'exprimer la probabilité d'erreur par paire (voir annexe C.4)

$$P(U \to V) \leq \frac{1}{2} \left(\prod_{i=1}^{r} \frac{\lambda_i}{E_b} \right)^{-n_r} \left(\frac{E_b}{8N_0} \right)^{-rn_r} \tag{3.6}$$

où E_b est l'énergie moyenne totale reçue par bit sur fréquence porteuse.

Ce calcul est, comme le précédent, valable pour les systèmes codés ou non-codés, et on voit donc apparaître un gain en diversité, défini comme l'exposant du rapport signal à bruit, soit rn_r, et un gain de codage $\left(\prod_{i=1}^{r} \frac{\lambda_i}{E_s} \right)^{1/n_r}$, défini comme le gain obtenu sur un système non codé ayant le même gain en diversité. Si l'on compare cette formule à celle obtenue pour le canal de Rayleigh indépendant, soit avec $\ell = 1$, on vérifie effectivement que le gain de diversité apporté par les antennes est le même puisque le rang de $A(U, V)$ vérifiant $r \leq min(\ell, n_t)$, on a nécessairement $r = 1$ pour $\ell = 1$.

D'autres travaux de recherche de bornes pour des canaux différents ont été menés dans la littérature, comme par exemple ceux de Malkamäki [52] [53] sur les canaux de Rice par blocs.

3.2.3 Exemple : probabilité d'erreur par bit de la MAQ-4 (ou QPSK) non codée avec deux antennes en émission et deux antennes en réception

On considère la constellation MAQ-4 (ou QPSK) présentée dans l'annexe C en figure C.2 dans le cas d'une transmission avec deux antennes en émission et deux antennes en réception. La formule (3.4) de la probabilité d'erreur par paire devient donc

$$P(U \to V) \leq \frac{1}{2}\left[\frac{1}{1+\frac{|(V_1-U_1)|^2+|(V_2-U_2)|^2}{8N_0}}\right]^2 \approx \frac{1}{2}\left[\frac{|(V_1-U_1)|^2+|(V_2-U_2)|^2}{8N_0}\right]^{-2} .$$

Dans cet exemple, la constellation émise est géométriquement uniforme. Pour une valeur fixée de U, le vecteur V de symboles QPSK prend 15 valeurs possibles. Nous pondérons chaque probabilité d'erreur par paire par le rapport du nombre de bits erronés (i) sur celui des bits émis (4), soit $i/4$. Nous obtenons ainsi la probabilité d'erreur par bit

$$P_{eb}^1 \leq 4\times\frac{1}{4}\times\frac{1}{2}\left[\frac{4A^2}{8N_0}\right]^{-2} + 6\times\frac{2}{4}\times\frac{1}{2}\left[\frac{8A^2}{8N_0}\right]^{-2} + 4\times\frac{3}{4}\times\frac{1}{2}\left[\frac{12A^2}{8N_0}\right]^{-2} + 1\times\frac{4}{4}\times\frac{1}{2}\left[\frac{16A^2}{8N_0}\right]^{-2}$$

$$P_{eb}^1 \leq \frac{1}{2}\left[\frac{A^2}{2N_0}\right]^{-2} + \frac{3}{2}\left[\frac{A^2}{N_0}\right]^{-2} + \frac{3}{2}\left[\frac{3A^2}{2N_0}\right]^{-2} + \frac{1}{2}\left[\frac{2A^2}{N_0}\right]^{-2} \leq \frac{103}{24}\left[\frac{A^2}{N_0}\right]^{-2} .$$

Or, d'après l'équation (C.10) (voir annexe C), l'énergie E_b moyenne totale reçue par bit sur fréquence porteuse est égale à

$$E_b = \frac{4-1}{3\times 2}A^2 \times 2 = A^2 .$$

On en déduit donc l'expression de la probabilité d'erreur par bit de la MAQ-4 sur un canal (2,2)

$$P_{eb}^1 \leq \frac{4.3}{(\frac{E_b}{N_0})^2} . \tag{3.7}$$

Un calcul similaire, pour le cas plus simple du canal à une antenne d'émission et deux antennes de réception, nous donne

$$P_{eb}^2 \leq 2\times\frac{1}{2}\times\frac{1}{2}\left[\frac{4A^2}{8N_0}\right]^{-2} + 1\times\frac{2}{2}\times\frac{1}{2}\left[\frac{8A^2}{8N_0}\right]^{-2}$$

$$P_{eb}^2 \leq \frac{1}{2}\left[\frac{A^2}{2N_0}\right]^{-2} + \frac{1}{2}\left[\frac{A^2}{N_0}\right]^{-2} \leq \frac{5}{2}\left[\frac{A^2}{N_0}\right]^{-2} .$$

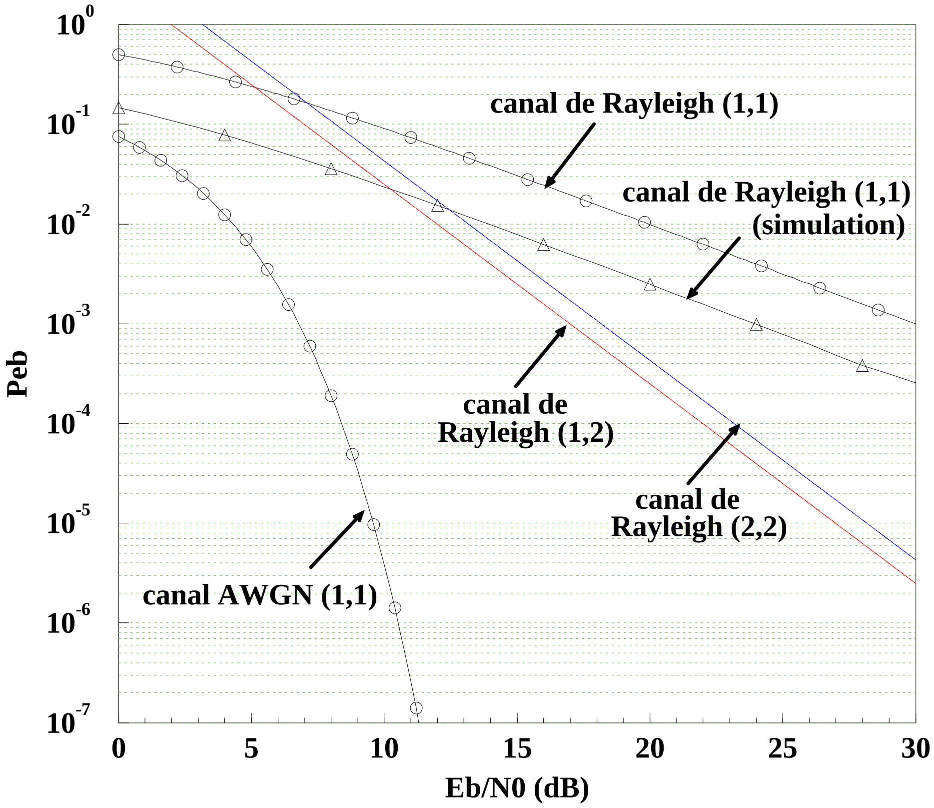


FIG. 3.3: Les bornes de la probabilité d'erreur pour une QPSK non codée sur différents canaux

Comme dans le cas précédent, l'énergie E_b moyenne totale reçue par bit sur fréquence porteuse est égale à

$$E_b = \frac{4-1}{3 \times 2} A^2 \times 2 = A^2$$

d'où l'expression de la probabilité d'erreur par bit de la MAQ-4 sur un canal (1,2)

$$P_{eb}^2 \leq \frac{2.5}{(\frac{E_b}{N_0})^2} \; . \tag{3.8}$$

Nous avons représenté en figure 3.3 les bornes sur la probabilité d'erreur par bit obtenues sur canal AWGN et de Rayleigh mono- ou multi-antennes grâce aux formules précédentes. Si on compare les résultats obtenus avec P_{eb}^1 et P_{eb}^2, il apparaît qu'utiliser deux antennes en émission permet de doubler l'efficacité spectrale au prix d'une simple perte de 1.05 dB. Comparativement à la courbe obtenue sur le canal de Rayleigh non sélectif à coefficients indépendants avec une seule antenne en émission comme en réception, les n_r antennes de réception créent une diversité de n_r, ainsi que le montre la pente de la courbe. Les antennes d'émission permettent quant à elles de multiplier le débit binaire par un facteur n_t.

3.2.4 Description du codeur à entrées multiples et des canaux considérés

Modulation codée avec entrelacement de bits (BICM)

Depuis 1982 et la publication du célèbre article d'Ungerboeck [72], il était généralement considéré que combiner codage et modulation était nécessaire lorsque l'on cherchait à augmenter les performances d'un système. Ce raisonnement tenu sur le canal gaussien fut tout naturellement reporté sur le canal à évanouissements lorsque le développement des communications mobiles a conduit à étudier la faisabilité et les performances des modulations codées sur les canaux de Rayleigh. D'autres pistes furent cependant suivies et ainsi il a été mentionné pour la première fois dans [81] que l'entrelacement de bits, séparant le codage et la modulation, permettait d'augmenter de façon significative les performances sur les canaux à évanouissements. Cette découverte, un premier temps étonnante, vient du fait que, pour les canaux à évanouissements, c'est la distance de Hamming (ou diversité de codage) et non la distance euclidienne du code qui influe sur les performances. Une étude approfondie dans [23], suite aux travaux présentés dans [81] a en effet démontré que le schéma de codage avec une modulation codée avec entrelacement de bits (BICM) atteignait presque la capacité de la modulation lorsque le canal de transmission était à bruit additif blanc gaussien ou à évanouissements de Rayleigh variant lentement.
Nous utilisons donc ici une BICM pour séparer la modulation à forte efficacité spectrale du codage. Cette BICM sera décodée itérativement, comme expliqué dans le paragraphe 3.3.2 grâce à l'utilisation d'un décodeur SISO itératif. Cette méthode constitue donc une avancée certaine face à celle proposée par Li & Ritcey [49] qui ont proposé une méthode de décodage itératif avec retour d'informations dures pour une 8-PSK jumelé à un étiquetage spécifique de leur modulation.

Codeur utilisé

Décrivons à présent le codeur relatif à la BICM considérée : les symboles x_j appartiennent à une constellation à modulation de phase (*PSK*) ou à une constellation à modulation d'amplitude en quadrature (*MAQ*) de taille $M = 2^m$.

La structure de l'émetteur est donnée par la figure 3.4. Les bits d'information $\mathbf{u} = (u_i)_{i=1}^{N_u}$ sont générés par une source binaire et sont codés pour donner N_c bits codés $\mathbf{c} = (c_j)_{j=1}^{N_c}$ qui sont alors entrelacés aléatoirement et étiquetés pour donner les symboles PSK ou MAQ x_j. Le bloc de N_c/m symboles à transmettre est alors divisé en sous-blocs de longueur n_t et émis en parallèle sur les antennes d'émission. Dans le cas du canal de Rayleigh par blocs, cela signifie que les valeurs des coefficients $h_{i,j}(k)$ sont constants pour $k = 1, \ldots, N_c/(mn_t)$. À chaque période symbole, le vecteur des signaux $\mathbf{x}$ est donc une fonction de $m \times n_t$ bits codés

$$\mathbf{x} = (x_1, \ldots, x_{n_t})^t = f(c_1, c_2, \ldots, c_{mn_t}) \ . \tag{3.9}$$

Nous utiliserons dans ce chapitre deux types de codeurs : des codes convolutifs non-récursifs non-systématiques [50] et des turbo codes parallèles [11][12][9]. Comme nous le verrons, le système proposé peut aisément être appliqué à d'autres types de codes correcteurs d'erreurs, pour peu qu'un décodeur à entrées souples et sorties souples existe.

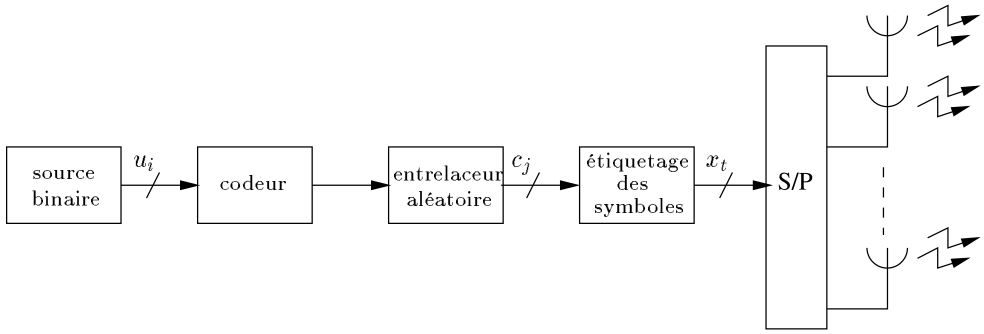


FIG. 3.4: Émetteur pour antennes multiples adapté au codage des éléments binaires.

3.3 Description du décodeur

3.3.1 Conversion des observations en probabilités *a posteriori* (APP)

Afin de restituer au mieux le flot de bits émis, il nous faut extraire une information souple des signaux reçus, ou plus précisément de la contribution de chaque antenne d'émission. Connaissant l'ensemble des signaux reçus sur tous les instants de temps $k = 1, \ldots, N_c/(mn_t)$, et sachant que les bits codés ont été entrelacés aléatoirement, il est possible de calculer la probabilité qu'un bit codé c_j soit égal à 0 ou 1. Cette probabilité, appelée probabilité *a posteriori* $APP(c_j)$ peut être exprimée comme

$$\begin{aligned} APP(c_j) &= p(c_j|\mathbf{y}) \\ &= \frac{p(\mathbf{y}|c_j) \cdot \pi(c_j)}{p(\mathbf{y})} \quad j = 1, \ldots, mn_t \\ APP(c_j) &\propto \pi(c_j) \cdot p(\mathbf{y}|c_j) = \pi(c_j) \cdot obs(c_j) \end{aligned} \tag{3.10}$$

où $\pi(c_j)$ est la probabilité *a priori* du bit codé c_j et où l'on définit l'observation sur c_j par $obs(c_j) = p(\mathbf{y}|c_j)$.

La densité de probabilité conditionnelle $p(\mathbf{y}|c_j)$ est obtenue en marginalisant la densité de probabilité jointe de tous les bits codés et de l'observation, en tenant compte du fait que les signaux reçus y_r sont indépendants conditionnellement à l'ensemble des bits codés $c_1, \ldots, c_{mn_t}$ supposés indépendants entre eux

$$p(\mathbf{y}|c_j) = \sum_{\substack{c_i \in \{0,1\} \\ i=1,\ldots,mn_t,\, i \neq j}} p(\mathbf{y}, c_1, \ldots, c_{j-1}, c_{j+1}, \ldots, c_{mn_t}|c_j)$$

$$= \sum_{c_i \in \{0,1\},\, i=1,\ldots,mn_t,\, i \neq j} p(\mathbf{y}|c_1,\ldots,c_{mn_t}) \prod_{l \neq j} \pi(c_\ell)$$

$$= \sum_{\substack{c_i \in \{0,1\} \\ i=1,\ldots,mn_t,\, i \neq j}} \left(\prod_{r=1}^{n_r} p(y_r|c_1,\ldots,c_{mn_t}) \prod_{l \neq j} \pi(c_\ell) \right) . \tag{3.11}$$

Or, le canal étant à bruit additif blanc gaussien, la densité de probabilité conditionnelle $p(y_r|c_1,\ldots,c_{mn_t})$ est égale à

$$p(y_r|c_1,\ldots,c_{mn_t}) = \frac{1}{(2\pi\sigma^2)} \exp\left(-\frac{\left\|y_r - \sum_{t=1}^{n_t} h_{t,r} x_t\right\|^2}{2\sigma^2} \right) \tag{3.12}$$

où les signaux x_t sont définis par l'équation (3.9).

On notera qu'il existe une autre méthode, moins complexe mais sous-optimale, pour calculer une approximation des valeurs des APP. Les signaux reçus sont alors traités indépendamment au niveau de chaque antenne de réception pour obtenir plusieurs vraisemblances partielles. L'approximation de l'APP totale est alors

$$APP_{sub}(c_j) \propto \pi(c_j) \cdot \prod_{r=1}^{n_r} p(y_r|c_j) \tag{3.13}$$

où $p(y_r|c_j)$ est calculée en marginalisant la vraisemblance totale d'une façon similaire à celle utilisée dans le calcul de l'équation (3.11). Des simulations ont montré que cette seconde méthode d'évaluation de l'APP était sous-optimale, à la fois en terme de taux d'erreur binaire et en terme de vitesse de convergence pour une diminution de complexité négligeable. En effet, lorsque l'on ne prend pas en compte tout le système, il n'est pas possible de relier correctement toutes les informations partielles, et donc on n'est pas en mesure de fournir la meilleure probabilité *a posteriori* possible au décodeur. Mathématiquement, cette seconde méthode est sous-optimale car les signaux reçus y_r sont corrélés lorsqu'ils ne sont que partiellement conditionnés.

3.3.2 Détection itérative et décodage

L'évaluation de la vraisemblance conditionnelle $p(\mathbf{y}|c_j) = obs(c_j)$ décrite dans le paragraphe précédent correspond à l'étape de détection réalisée au niveau du récepteur. La vraisemblance $obs(c_j)$, appelée *observation* associée au bit c_j, est alors traitée par un décodeur à entrées souples et sorties souples utilisant le treillis du code correcteur d'erreurs considéré. Ce décodeur SISO [13][18], reposant sur le principe du “forward-backward” [2], génère une information extrinsèque $Ext(c_j)$ qui est équivalente à une nouvelle probabilité *a priori* $\pi(c_j)$ pour le bit codé c_j. En conséquence, il convient de retourner cette nouvelle

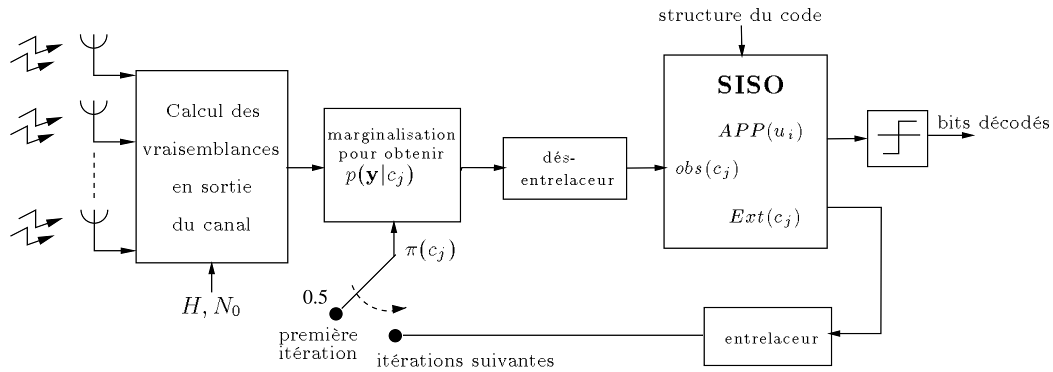


FIG. 3.5: Récepteur pour antennes multiples adapté au codage des éléments binaires.

information *a priori* dans le détecteur défini par l'équation (3.11). C'est ainsi que le processus de détection-décodage itératif est une excellente manière d'améliorer l'estimation des probabilités *a posteriori* : la réinjection de l'information extrinsèque peut bien sûr éloigner temporairement le décodeur itératif des bits codés émis mais dans la plupart des cas, les itérations suivantes, grâce aux autres informations extrinsèques justes, ramèneront le décodeur dans le droit chemin.

La figure 3.5 illustre le processus itératif de détection et de décodage au niveau du récepteur. On notera que le traitement au niveau du récepteur se fait en deux étapes : la première est non itérative et réalise le calcul des probabilités conditionnelles des signaux reçus au niveau de chaque antenne de réception selon la formule (3.12). La deuxième partie est itérative et son entrée dépend aussi des probabilités *a priori* calculées à l'étape précédente. La décision finale se fait à partir des probabilités *a posteriori* générées par le décodeur SISO à sa dernière itération.

Le principe du décodeur itératif peut donc être résumé comme suit :

• initialisation : calculer les $N_c/(mn_t) \times n_r$ vraisemblances $p(y_r|c_1, \ldots, c_{mn_t})$ à partir de la sortie du canal. Initialiser les N_c probabilités *a priori* $\pi(c_j)$ à $1/2$.

• à chaque itération :
- calculer les N_c observations $p(\mathbf{y}|c_j)$ à partir de la sortie du canal en utilisant la formule (3.11) dans laquelle les probabilités *a priori* $\pi(c_\ell)$ sont prises égales à l'information extrinsèque $Ext(c_\ell)$ produite par le décodeur SISO à l'itération précédente.
- appliquer le décodeur SISO, qui calcule $APP(c_j) \propto Ext(c_j) \times obs(c_j), j = 1, \ldots, N_c$ et les probabilités *a posteriori* $APP(u_i), i = 1, \ldots, N_b$.

• étape finale : à la dernière itération, décider que $u_i = 0$ si $APP(u_i = 0) > APP(u_i = 1)$ et $u_i = 1$ sinon. On notera que les bits décodés ne forment pas nécessairement un mot de code.

3.4 Estimation des paramètres du canal

L'algorithme de décodage itératif d'un système à entrées et sorties multiples proposé dans le paragraphe précédent suppose le canal parfaitement connu (amplitude et phase de l'évanouissement, variance du bruit), pour réaliser l'opération de décodage. De telles conditions ne sont bien évidemment pas vérifiées en pratique. Ce paragraphe considère donc le problème du décodage lorsque ces paramètres ne sont pas connus.
En effet, si dans le cas du canal de Rayleigh, les paramètres du canal ne peuvent être estimés du fait de leur indépendance, plusieurs méthodes peuvent être envisagées dans le cas du canal de Rayleigh par blocs.

3.4.1 Choix de la méthode d'estimation

Un des moyens classiques pour estimer le canal est de transmettre des symboles pilotes à l'intérieur de la trame d'information, mais cette pratique présente l'inconvénient de diminuer l'efficacité spectrale transmise à mesure que l'on augmente le nombre de symboles pilotes par trame (et donc que l'on affine l'estimation) : ainsi, si l'on note N_p le nombre des symboles pilotes ajoutés à une trame de longueur originale N, l'efficacité spectrale est réduite d'un facteur $\frac{N_p}{N+N_p}$, ou, de façon symétrique, on observe une perte d'énergie de $10log_{10}(\frac{N+N_p}{N_p})$ dB.

Connaissant ces symboles pilotes, on peut alors utiliser différentes techniques d'estimation afin de déterminer l'état du canal pour les pilotes et ensuite extrapoler à l'ensemble de la trame. La plus classique de ces techniques d'estimation est l'estimation ML (*Maximum Likelihood*) qui revient à maximiser la vraisemblance du signal reçu en fonction des paramètres supposés du canal. Cette méthode ne peut hélas pas être employée lorsque le récepteur est aveugle (aucun symbole pilote n'est transmis), car elle nécessiterait alors une puissance de calcul trop importante pour être réalisable en pratique.

Une autre approche est possible, qui utilise les estimations souples du signal pour estimer les paramètres du canal avec l'aide de quelques symboles pilotes pour initialiser le système. Nous nous proposons en effet de mettre à profit le caractère itératif du décodage pour obtenir des estimations de plus en plus précises des paramètres du canal à l'aide de l'algorithme Expectation-Maximization (EM) [30][74][44][36] et procéder ainsi à une amélioration conjointe de l'estimation du canal et du décodage au fur et à mesure des itérations.

L'algorithme EM est un algorithme général applicable à tous les problèmes dit incomplets. Il est en particulier souvent utilisé pour estimer de manière itérative des paramètres selon le critère à maximum de vraisemblance (ML). Il s'agit d'une approche pragmatique d'un problème dont les données sont incomplètes, où les paramètres sont estimés en utilisant à la première étape des valeurs initiales fournies par l'utilisateur puis les prédictions de l'étape précédente jusqu'à la convergence.

Très général, cet algorithme a donc été utilisé dans de nombreux contextes, allant de l'imagerie médicale à la reconnaissance de la parole en passant par la recherche sur les virus et bien sûr les communications numériques. Ainsi a-t-il par exemple déjà été utilisé pour estimer l'amplitude du signal et la variance du bruit dans le cadre d'un décodage turbo [43], ou pour des modulations à phase continue (CPM) [22].

Ici, l'estimation des paramètres va se faire en utilisant les métriques de l'algorithme Soft-Input Soft-Output. Une fois le canal estimé, le SISO est de nouveau utilisé pour calculer les probabilités *a posteriori* des bits d'information et les probabilités extrinsèques des bits codés comme présenté au paragraphe précédent. L'algorithme SISO est donc utilisé à la fois pour estimer le canal et pour décoder les trames émises, comme présenté dans la figure 3.6.

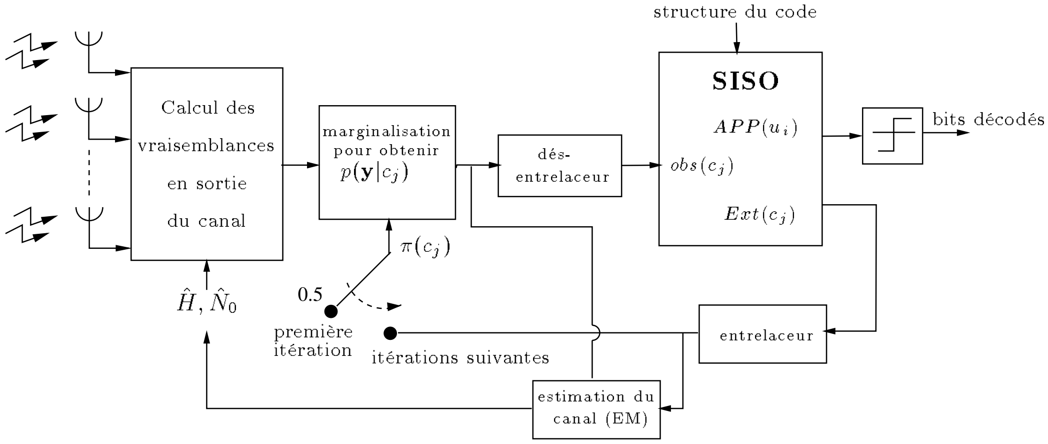


FIG. 3.6: Récepteur pour antennes multiples adapté au codage des éléments binaires avec estimation des paramètres du canal selon l'algorithme EM.

3.4.2 Définition des fonctions et paramètres utilisés

On rappelle que le canal considéré, présenté en figure 3.2, est un canal de Rayleigh par blocs, soit un canal où les coefficients d'évanouissement $h_{ij}(k)$ sont constants sur toute la trame émise : $h_{ij}(k) = h_{ij}, k = 1, \ldots, \frac{N_C}{mn_t}$. L'algorithme EM va travailler sur un tel bloc à coefficients constants, ce qui est tout à fait adapté à notre décodage puisque le récepteur SISO travaille lui aussi par blocs.

On rappelle également que la matrice $H = [h_{i,j}]_{i=1,\ldots,n_r,j=1,\ldots,n_t}$ du canal pour la trame est constituée de coefficients gaussiens indépendants de moyenne nulle et de variance $E[|h_{i,j}|^2] = 1$. Le bruit au niveau de chaque antenne de réception est un bruit additif blanc gaussien de moyenne nulle et de variance $2\sigma^2 = 2N_0$ (σ^2 étant la variance par composante). Ces paramètres du canal, soit l'ensemble des variables que l'on cherche à estimer sont réunis dans le vecteur $\Theta = (N_0, H)$.

La vraisemblance conditionnelle d'une observation $\mathbf{y}$, ou probabilité conditionnelle de $\mathbf{y}$ pour le vecteur Θ sur la trame considérée est alors donnée par

$$p(\mathbf{y}|\Theta) = \sum_{\mathbf{x}_u \in \mathcal{X}} p(\mathbf{y}, \mathbf{x}_u|\Theta) \tag{3.14}$$

où $\mathcal{X}$ est l'ensemble de toutes les séquences $(\mathbf{x}_u)_{u=1,\ldots,|\mathcal{X}|}$ possibles en entrée du convertisseur série-parallèle. Pour une constellation MAQ de taille M, le cardinal de $\mathcal{X}$ est $|\mathcal{X}| = M^{n_t}$.

L'estimation $\hat{\Theta}$ de Θ que nous cherchons est celle qui maximise la vraisemblance de l'observation du canal sur la trame considérée

$$\hat{\Theta} = \arg\max_{\Theta} p(\mathbf{y}|\Theta) \ . \tag{3.15}$$

Trouver une solution à l'équation (3.15) est impossible dans le cas général car cela impliquerait une recherche exhaustive des vraisemblances moyennes de l'observation $\mathbf{y}$ sur toutes les trames possibles de longueur N_c et leur maximisation par rapport à Θ. En outre, rien ne garantit qu'il existe en tout cas une méthode permettant de rendre l'expression définie dans (3.15) maximale. Une solution est donc d'utiliser l'algorithme EM qui améliore son estimation Θ^i au cours des itérations en travaillant avec la fonction $Q(\Theta|\Theta^i)$ donnée par l'espérance mathématique de la log-vraisemblance conditionnelle de l'observation du canal au niveau du récepteur par rapport à la loi des vecteurs émis $\mathbf{x}$

$$Q(\Theta|\Theta^i) = E_{\mathbf{x}}\left[\log\left(p(\mathbf{y}|\mathbf{x},\Theta)\right)|\mathbf{y},\Theta^i\right] \ . \tag{3.16}$$

L'algorithme EM garantit une augmentation monotone de la fonction Q [30] avec la réestimation à l'itération $i+1$ d'une nouvelle valeur Θ^{i+1} à partir de la valeur courante Θ^i.

Une itération de l'algorithme EM inclue les deux étapes suivantes :

- étape E ("Expectation") : calcul de $Q(\Theta|\Theta^i)$,
- étape M ("Maximization") : recherche de la valeur Θ^{i+1} maximisant $Q(\Theta|\Theta^i)$ considérée comme une fonction de Θ.

3.4.3 Séquence de symboles inconnus

Lors de l'étape E on calcule l'expression de la fonction Q à partir de sa définition donnée dans l'équation (3.16), en exprimant l'espérance mathématique sur les vecteurs émis $\mathbf{x}$, en supposant pour cela que les $\mathbf{x}(k)$ et $\mathbf{y}(k)$ sont indépendants entre eux

$$Q(\Theta|\Theta^i) = \sum_{\mathbf{x}_u \in \mathcal{X}} \log\left[p(\mathbf{y}|\mathbf{x}=\mathbf{x}_u,\Theta)\right] p(\mathbf{x}_u|\mathbf{y},\Theta^i) \ . \tag{3.17}$$

Sachant que $\mathbf{x}(k)$ et $\mathbf{y}(k)$ sont les $k^{èmes}$ vecteurs de signaux effectivement émis et reçus sur la trame de longueur N_c bits codés découpée en $\frac{Nc}{mn_t}$ vecteurs, on a

$$Q(\Theta|\Theta^i) = \sum_{k=1}^{\frac{Nc}{mn_t}} \sum_{u=1}^{|\mathcal{X}|} \log\left[p(\mathbf{y}(k)|\mathbf{x}(k) = \mathbf{x}_u, \Theta)\right] p(\mathbf{x}(k) = \mathbf{x}_u|\mathbf{y}(k), \Theta^i) \ . \tag{3.18}$$

Le canal étant supposé à bruit additif blanc gaussien, on obtient

$$Q(\Theta|\Theta^i) = -\sum_{k=1}^{\frac{Nc}{mn_t}} \sum_{u=1}^{|\mathcal{X}|} \left(2\log(N_0) + c^{te} + \frac{||\mathbf{y}(k) - H\mathbf{x}_u||^2}{2N_0}\right) APP_k(\mathbf{x}_u|\Theta^i) \tag{3.19}$$

où $APP_k(\mathbf{x}_u|\Theta^i)$ est la probabilité *a posteriori* que le symbole $\mathbf{x}_u$ ait été émis au temps k sur la trame considérée sachant l'estimation courante Θ^i du canal.

L'étape M peut alors être appliquée en dérivant $Q(\Theta|\Theta^i)$ partiellement par rapport aux deux composantes de Θ. On obtient en annulant ces dérivées et en utilisant les règles rappelées ci-dessous

$$\begin{aligned} \frac{\partial(A^h\Gamma^h\Gamma B)}{\partial\Gamma} &= \Gamma^* A^* B^t \\ \frac{\partial\Gamma^h}{\partial\Gamma} &= 0 \\ \frac{\partial(A^h\Gamma B)}{\partial\Gamma} &= A^* B^t \\ \frac{\partial\|A - \Gamma B\|^2}{\partial\Gamma} &= -A^* B^t + \Gamma^* A^* B^t \end{aligned} \tag{3.20}$$

où $A = (a_1, \ldots, a_n)^t$, $B = (b_1, \ldots, b_n)^t$ et $\Gamma = (\gamma_{ij})_{i,j=1,\ldots,n}$.

la formule de récurrence souhaitée

$$H^{i+1} = \sum_{k=1}^{\frac{Nc}{mn_t}} \sum_{u=1}^{|\mathcal{X}|} \mathbf{y}(k)\mathbf{x}_u^h APP_k(\mathbf{x}_u|\Theta^i) \times \left(\sum_{k=1}^{\frac{Nc}{mn_t}} \sum_{u=1}^{|\mathcal{X}|} \mathbf{x}_u\mathbf{x}_u^h APP_k(\mathbf{x}_u|\Theta^i)\right)^{-1} \tag{3.21}$$

$$N_0^{i+1} = \frac{1}{4\frac{Nc}{mn_t}} \sum_{k=1}^{\frac{Nc}{mn_t}} \sum_{u=1}^{|\mathcal{X}|} APP_k(\mathbf{x}_u|\Theta^i) \cdot ||\mathbf{y}(k) - H^{i+1}\mathbf{x}_u||^2 \ . \tag{3.22}$$

Les simulations ont montré qu'une initialisation aveugle du système ne donnait aucun résultat, aussi la valeur initiale Θ^0 est-elle estimée en utilisant des symboles pilotes, comme décrit dans le paragraphe suivant (typiquement, 11% des symboles émis seront pilotes, comme montré dans le paragraphe 3.5). Pour les autres itérations, il est aisé de voir que l'algorithme EM s'intègre tout naturellement dans les itérations de détection-décodage car il n'a besoin que des observations du canal et des probabilités *a posteriori* des bits codés fournies par le décodeur SISO. En conséquence, l'utilisation de l'algorithme EM n'entraîne qu'une faible augmentation de complexité ou de retard de décision.

3.4.4 Séquence de symboles pilotes

Il apparaît donc nécessaire d'utiliser des symboles pilotes lors de l'initialisation de notre algorithme. Puisque les évanouissements sont constants sur toute la trame, la position des pilotes à l'intérieur de la trame importe peu, et donc il nous est possible de nous ramener au cas simple d'une (sous-)trame composée uniquement de symboles pilotes, pour laquelle l'estimation de Θ peut se faire très facilement selon le critère ML. En effet, connaissant les signaux émis et les observations correspondantes, l'estimation à maximum de vraisemblance $\hat{\Theta}$ est la valeur de Θ qui maximise la probabilité conditionnelle de la trame reçue.

Puisque le récepteur connait les symboles pilotes émis $\tilde{\mathbf{x}}(k), k = 1, \ldots, \frac{N_p}{mn_t}$ et que le canal est à bruit additif blanc gaussien, on a

$$p(\mathbf{y}|H) = p(\mathbf{y}|H, \tilde{\mathbf{x}}(0), \ldots, \tilde{\mathbf{x}}(\frac{N_p}{mn_t})) = \frac{1}{(2\pi N_0)^{2\frac{N_p}{mn_t}}} \exp\left(-\frac{\sum_{k=1}^{\frac{N_p}{mn_t}} ||\mathbf{y}(k) - H\tilde{\mathbf{x}}(k)||^2}{2N_0}\right) \tag{3.23}$$

Il ne reste plus alors qu'à dériver par rapport à H et N_0 pour en déduire le canal estimé grâce aux symboles pilotes, soit $\Theta^0 = (H^0, N_0^0)$

$$\hat{H} = \sum_{k=1}^{\frac{Np}{mn_t}} \mathbf{y}(k)\tilde{\mathbf{x}}^h(k)(\sum_{k=1}^{\frac{Np}{mn_t}} \tilde{\mathbf{x}}(k)\tilde{\mathbf{x}}^h(k))^{-1} = H^0 \tag{3.24}$$

$$\hat{N_0} = \frac{1}{4\frac{N_p}{mn_t}} \sum_{k=1}^{\frac{Np}{mn_t}} ||\mathbf{y}(k) - \hat{H}\tilde{\mathbf{x}}(k)||^2 = N_0^0 \ . \tag{3.25}$$

On notera bien sûr que l'on peut retrouver ces dernières équations en utilisant les formules de récurrence obtenues avec l'algorithme EM sur la sous-trame des pilotes en remplaçant les probabilités *a posteriori* par leurs valeurs (soit 1 lorsqu'il s'agit de la probabilité d'un des pilotes, et 0 sinon). Inversement, partant des formules d'estimation ML, on constate que l'on peut obtenir "intuitivement" les formules d'estimation EM en remplaçant les valeurs des symboles émis par leur vraisemblance.

3.5 Résultats de simulation

Les figures 3.7, 3.9 , 3.10 et 3.12 montrent les performances d'un turbo code et d'un code convolutif non récursif non systématique (NRNSC) sur un canal de Rayleigh non sélectif à évanouissements indépendants et sur un canal de Rayleigh à évanouissements par blocs avec $n_t = 2$ antennes d'émission et $n_r = 2$ antennes de réception.

Le turbo code considéré est formé par la concaténation parallèle de deux codes convolutifs binaires récursifs et systématiques de polynômes générateurs $(23, 35)$ en octal. Il a été simulé en utilisant une longueur de trame de $N_c = 2000$ bits, soit une taille d'entrelaceur égale à 1000. Le code convolutif est binaire non systématique non récursif de polynômes générateurs $(133, 171)$ en octal. Il a été simulé pour des longueurs de trames égales à $N_c = 100$ bits ou $N_c = 200$ bits. Ces choix de longueur de trames correspondent à des valeurs classiques pour le turbo code et le code convolutif dans les conditions que nous considérons.
Dans tous les cas, les treillis du code convolutif $(133, 171)$ et des codes constituants $(23, 35)$ sont terminés, i.e. sont ramenés à l'état zéro après que les N_c bits ont été générés.

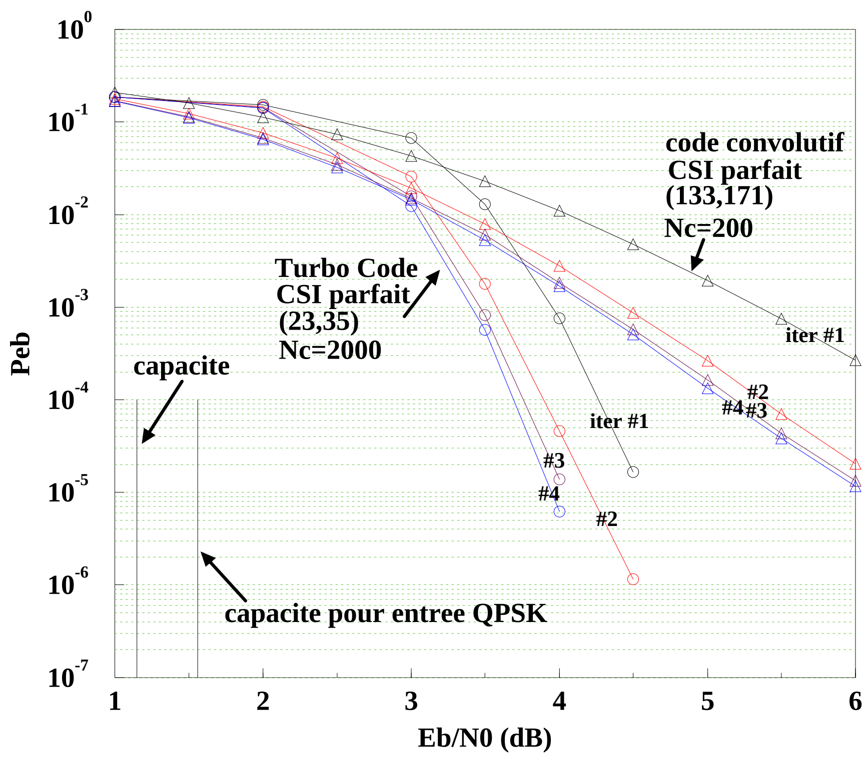


FIG. 3.7: Taux d'erreur binaire pour un turbo code (○) et un code convolutif (△) avec des trames de longueur $N_c = 2000$ et $N_c = 200$ respectivement sur canal de Rayleigh indépendant, $n_t = n_r = 2$ antennes.

Le gain obtenu grâce au décodage itératif est évident, à la fois pour les deux canaux et les deux codes. On notera de plus que le gain est atteint presque complètement après trois

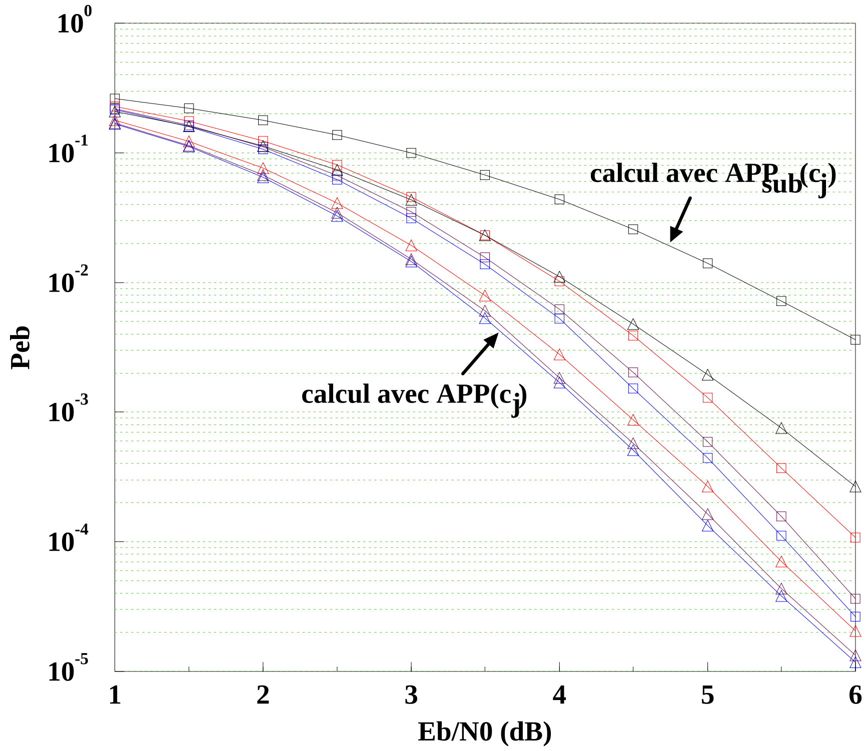


FIG. 3.8: Comparaison du taux d'erreur binaire obtenu pour le code convolutif de générateurs (133, 171) avec des trames de longueur $N_c = 200$ sur canal de Rayleigh indépendant en fonction de la méthode de calcul de l'APP, $n_t = n_r = 2$ antennes.

itérations seulement, ce qui correspond à un délai raisonnable. Alors que sur le canal de Rayleigh indépendant le turbo code obtient de meilleurs résultats que le code convolutif, ce n'est plus le cas sur le canal de Rayleigh par blocs, pour lequel c'est le code convolutif qui montre une meilleure résistance face aux perturbations engendrées par le canal.

À la quatrième itération, le turbo code offre sur le canal de Rayleigh à évanouissements indépendants des performances meilleures que celles du code convolutif de 2 dB pour une probabilité d'erreur par bit $P_{eb} = 10^{-6}$, comme montré par la figure 3.7. Cependant, il apparaît que le turbo code gagne un peu moins d'1 dB au travers des itérations alors que le code convolutif gagne lui plus de 1.5 dB. Cela est dû au fait que le turbo code est lui-même décodé itérativement, dans notre cas 4 itérations sont réalisées dans le turbo décodeur pour chaque itération globale. Le turbo code gagne donc dès la première itération globale beaucoup plus que le code convolutif grâce à ses itérations internes.

Nous présentons également en figure 3.8 une comparaison des résultats du code convolutif ($\triangle$) de la figure 3.7 avec ceux qui sont obtenus lorsque l'on utilise la méthode sous-optimale ($\square$) de calcul de l'APP des bits codés donnée par la formule (3.13). Afin d'alléger les figures, nous ne noterons pas sur les courbes qui suivent les itérations qui se déduisent aisément, comme à la figure 3.7 chacune de la précédente. On note que les itérations

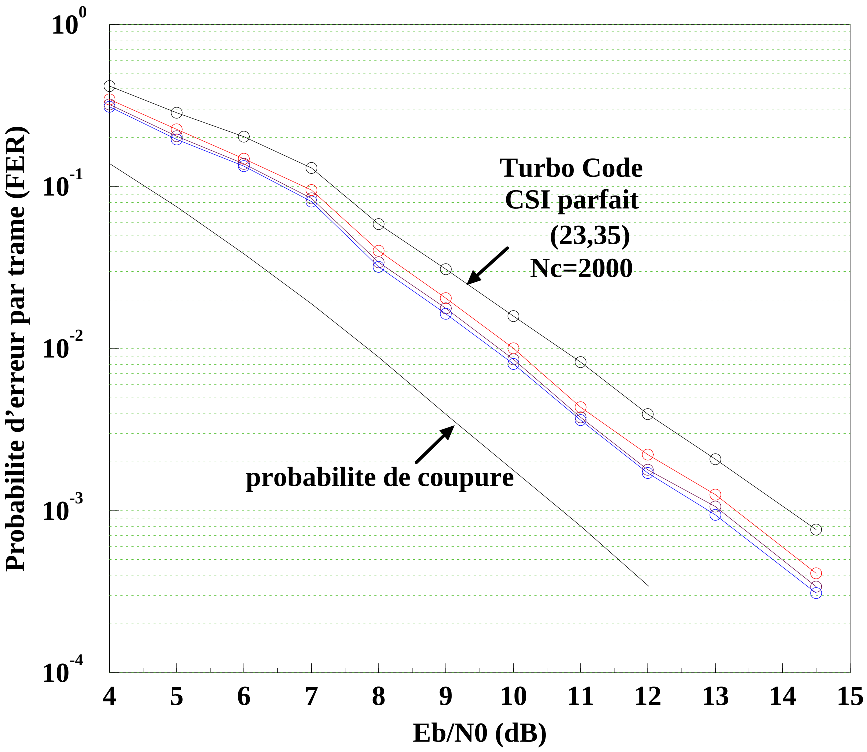


FIG. 3.9: Taux d'erreur par trame pour un turbo code, de codes constituants RSC de générateurs (23,35), avec des trames de longueur $N_c = 2000$ sur un canal de Rayleigh à évanouissements par blocs, $n_t = n_r = 2$ antennes.

de décodage, en particulier les deux premières, sont beaucoup moins efficaces avec cette méthode sous-optimale. Ainsi, alors que trois itérations sont suffisantes pour la méthode "optimale", une supplémentaire s'avère nécessaire pour cette méthode sous-optimale, et même ainsi on observe une perte de 0.5 dB à la quatrième itération.

Sur le canal de Rayleigh par blocs, les courbes des itérations du turbo code et du code convolutif se chevauchant, nous les avons séparé en deux figures 3.9 et 3.10. Le turbo code de codes constituants à 16 états s'améliore d'1 dB après quatre itérations globales mais reste malheureusement moins efficace de 0.7 dB par rapport au code convolutif à 64 états. Ces performances moyennes du turbo code s'expliquent principalement du fait de l'absence de gain d'entrelacement [9] lorsque l'on considère le taux d'erreur par trame (FER). De plus, on se rappellera que le turbo code, pour bien fonctionner, a besoin d'une longueur de trame sensiblement plus grande que le code convolutif, ce qui le rend plus sensible aux erreurs de trames. Il est ainsi à plus de 2 dB de la probabilité de coupure (*outage probability*) pour un taux d'erreur par trame de 10^{-3}. Cette probabilité de coupure (voir paragraphe 4.2.2) nous permet d'estimer les performances atteignables en terme de probabilité d'erreur par trame.

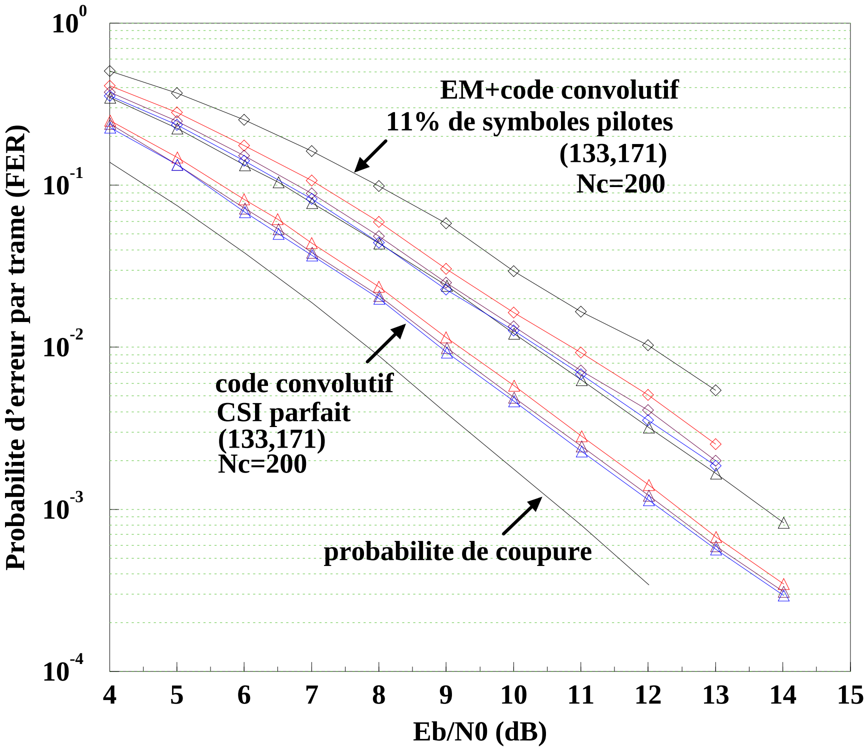


Fig. 3.10: Taux d'erreur par trame pour un code convolutif NRNSC, de générateurs (133, 171), avec des trames de longueur $N_c = 200$ sur un canal de Rayleigh à évanouissements par blocs, $n_t = n_r = 2$ antennes. Comparaison entre le cas d'un CSI parfait et une estimation de canal par l'algorithme EM.

Les différentes simulations que nous avons commentées jusqu'à présent supposaient une connaissance parfaite du canal au niveau du récepteur. La méthode d'estimation des paramètres du canal à l'aide de l'algorithme EM décrite au paragraphe 3.4.1 a été appliquée au code convolutif avec ajout de 12 symboles pilotes à la trame originale, soit $12/112 \approx 11\%$ de symboles pilotes pour $N_c = 200$ bits codés. Prenant en compte la perte d'efficacité spectrale due à l'insertion des pilotes, les courbes ($\diamond$) montrées en figure 3.10 indiquent une perte de 1.5 dB par rapport au cas où l'état du canal est parfaitement connu ($\triangle$) pour un taux d'erreur par trame de 10^{-3}. On notera que l'insertion du même nombre de symboles pilotes sans l'algorithme EM, présenté en figure 3.11, aurait réduit le gain de codage et placé la courbe avec symboles pilotes ($+$) à 2.9 dB de celle avec CSI parfait.

Nous avons également simulé le code convolutif avec l'estimation des paramètres par l'algorithme EM pour une trame de taille $N_c = 100$. Les courbes correspondantes sont représentées en figure 3.12. On observe qu'un nombre trop faible de symboles pilotes ($*$), ne permet pas d'estimer correctement les paramètres du canal : les informations venues de seulement 6 symboles pilotes sont insuffisantes pour déterminer sûrement les 4 coefficients h_{ij}. Si l'on double le nombre de symboles pilotes ($\diamond$), l'estimation se fait correctement et la perte d'efficacité spectrale est compensée par les meilleurs résultats du code pour une

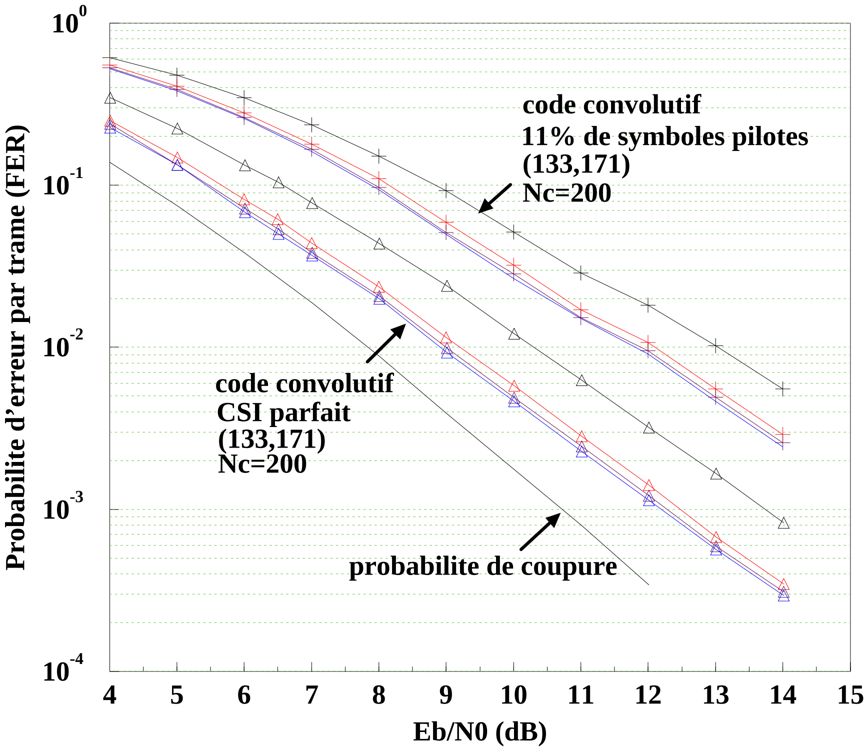


FIG. 3.11: Taux d'erreur par trame pour un code convolutif NRNSC, de générateurs (133, 171), avec des trames de longueur $N_c = 200$ sur un canal de Rayleigh à évanouissements par blocs, $n_t = n_r = 2$ antennes. Comparaison entre le cas d'un CSI parfait et une estimation de canal par ajout de symboles pilotes.

plus petite taille de trame : on retrouve une probabilité d'erreur de $2 \cdot 10^{-3}$ à la quatrième itération pour un décodage avec estimation EM à un rapport signal à bruit de 13 dB.

3.6 Conclusions

Nous avons proposé un schéma de détection et décodage itératif pour des systèmes à antennes d'émission et de réception multiples qui peut être appliqué à des codes correcteurs d'erreurs lorsque le décodage à maximum de vraisemblance n'est pas applicable. L'intérêt principal de ce schéma est que le calcul de l'APP sur lequel il est fondé peut être appliqué à n'importe quel type de code, pour peu qu'un décodeur SISO correspondant soit disponible.

Nous avons également montré que l'estimation des paramètres du canal à l'aide de l'algorithme EM pouvait être intégrée dans le processus de détection. Cette technique pourrait aussi être appliquée dans le cas d'un canal de Rayleigh affecté d'un Doppler avec l'utilisation d'un décodeur SISO à fenêtre glissante qui fournirait alors des estimations locales du canal.

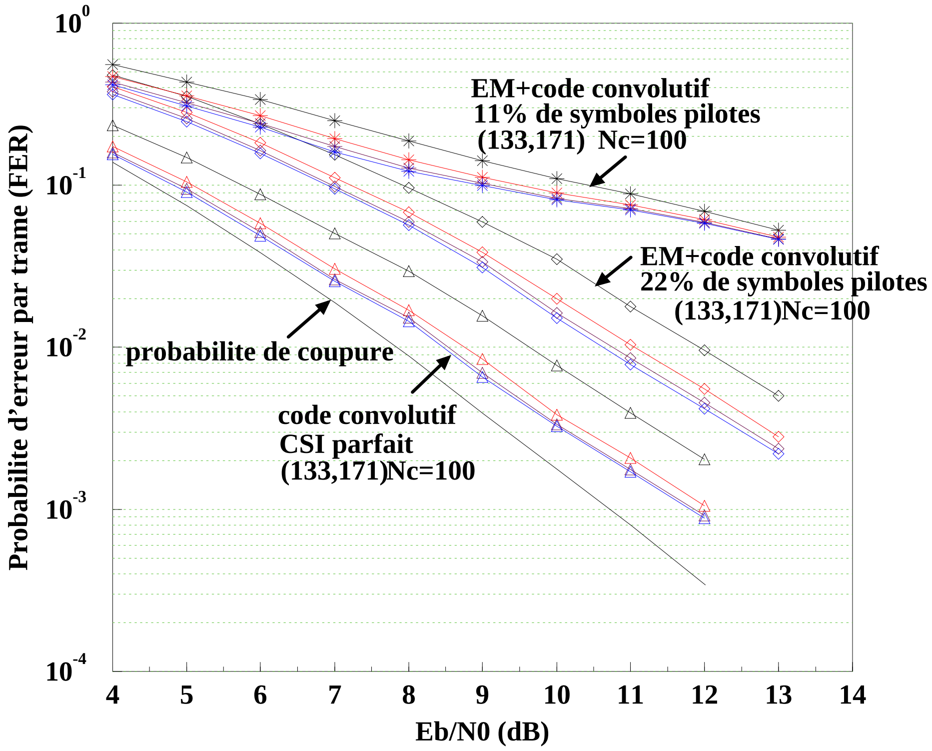


Fig. 3.12: Taux d'erreur par trame pour un code convolutif NRNSC, de générateurs (133, 171), avec des trames de longueur $N_c = 100$ sur un canal de Rayleigh à évanouissements par blocs, $n_t = n_r = 2$ antennes. Comparaison entre le cas d'un CSI parfait et une estimation de canal par l'algorithme EM.

Appliquée à un turbo code parallèle et à un code convolutif, la procédure itérative a montré des résultats performants à la fois sur le canal de Rayleigh à évanouissements indépendants et sur le canal de Rayleigh par blocs. Un petit turbo code, de taille d'entrelaceur 1000 et de rendement total 1/2 atteint un taux d'erreur binaire à 2.5 dB de la capacité. Un code convolutif à 64 états et de rendement 1/2 atteint sur le canal de Rayleigh par blocs un taux d'erreur par trame à 1.5 dB de la probabilité de coupure lorsque l'estimation du canal est parfaite et à 3 dB lorsque l'estimation est faite grâce à l'algorithme EM.

L'algorithme de décodage itératif APP proposé dans ce chapitre a une complexité exponentielle en n_t, le nombre d'antennes d'émission, ce qui devient impossible à utiliser en pratique lorsque n_t est supérieur à 4. Un moyen de réduire considérablement la complexité de l'étape de marginalisation de l'APP serait de considérer le vecteur de signaux de probabilité *a priori* la plus grande et d'en inverser les bits un par un pour en tirer les vraisemblances. Cette conversion sous-optimale aura une complexité linéaire en n_t et ne devrait pas trop dégrader les performances.
Une autre voie d'amélioration possible de ce système serait d'utiliser au niveau des antennes, non plus une allocation de puissance uniforme mais des techniques plus évoluées d'allocation de puissance, comme par exemple le "water filling" [35][28]).

Chapitre 4

Étude de la capacité *

Wer will, der kann
proverbe allemand

It is not possible to transmit at an average rate greater than C
Claude Shannon, 1948

4.1 Introduction

La notion même de communication repose sur l'existence de deux entités A et B et la volonté d'au moins l'une d'elle de transmettre des données à l'autre et celle de cette dernière d'écouter la première. Ce transfert de données de A vers B par exemple est un processus physique, donc sujet à des perturbations dues au bruit thermique ambiant et aux imperfections inévitables du processus de transmission lui-même. La communication est considérée comme réussie si le destinataire B (au besoin après utilisation d'un code correcteur d'erreurs, d'une ou plusieurs retransmissions...) et l'émetteur A sont d'accord sur ce qui a été effectivement transmis.

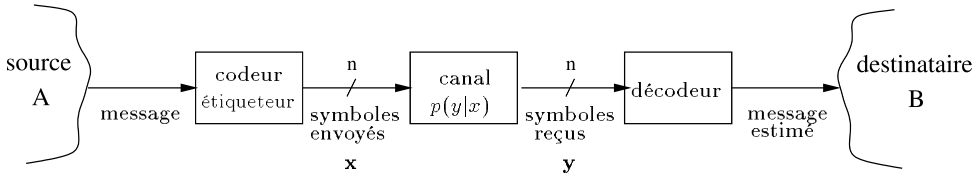


FIG. 4.1: Principe d'un système de communication.

*Certaines parties de ce chapitre ont été soumises au journal IEEE Transactions on Communications [86].

La figure 4.1 représente le modèle théorique d'un tel système de communication. Le canal est caractérisé par sa probabilité de transition $p(y|x)$ qui exprime la probabilité d'observer le symbole y en sortie sachant que le symbole x a été émis. Dans le cadre des communications numériques, le message de la source A est traduit en symboles appartenant à un alphabet fini, dit alphabet de source, et étiquetés en une séquence de n symboles envoyés appartenant à l'alphabet de canal, puis transmis sur celui-ci, ce qui produit en sortie dudit canal une séquence de n symboles reçus réels ou complexes. La sortie du canal est une version dégradée de l'entrée, à partir de laquelle le destinataire B va chercher à reconstituer le message qui a été envoyé, obtenant une estimée du message. Du fait de la dégradation due au canal, deux entrées différentes peuvent produire la même sortie. Il faut donc, pour transmettre correctement, choisir un alphabet portant le moins possible à confusion. Ainsi en étiquetant la source d'une façon appropriée, le message pourra être transmis avec une très faible probabilité d'erreur et il sera possible au destinataire de le reconstruire. Le nombre moyen de symboles émis par la source à chaque utilisation du canal est borné inférieurement par une grandeur appelée *entropie* [76], qui mesure la quantité d'information apportée en moyenne par chaque symbole émis. Les perturbations aléatoires existant sur le canal font que la transmission ne pourra avoir lieu que si l'entropie de la source est inférieure à une grandeur caractéristique du canal, dite *capacité* du canal [64]. Cette capacité mesure la quantité d'information moyenne maximale par symbole entrant dont le canal peut assurer le transfert.

Rappels de théorie de l'information

Avant d'entamer nos calculs de capacité proprement dits, nous nous proposons de rappeler brièvement les notions et résultats principaux de la théorie de l'information [28][6] dont nous aurons besoin dans ce chapitre. Pour cela, introduisons X et Y, deux variables aléatoires indépendantes de densités de probabilité respectives $p(\mathbf{x}), \mathbf{x} \in \mathcal{X}$ et $p(\mathbf{y}), \mathbf{y} \in \mathcal{Y}$, où $\mathcal{X}$ et $\mathcal{Y}$ sont deux ensembles quelconques. Nous notons dans les deux cas $p(\mathbf{x})$ et $p(\mathbf{y})$ pour les lois de X et Y par souci de simplicité, tout en gardant à l'esprit qu'il s'agit de fonctions distinctes, puisque renvoyant chacune à une variable aléatoire différente. Enfin nous supposerons ici que les variables aléatoires X et Y ont des distributions discrètes. Il est aisé de passer au cas continu en remplaçant dans les formules et définitions ci-dessous les sommes discrètes par des intégrales.

Définition 4.1.1 *L'***entropie** $\mathcal{H}(X)$ *de la variable aléatoire X est l'incertitude liée a la variable X, soit encore la quantité d'information nécessaire à la description de cette variable, soit enfin*

$$\mathcal{H}(X) = E[-\log_2 p(\mathbf{x})] = -\sum_{\mathbf{x}\in\mathcal{X}} p(\mathbf{x}) \log_2 p(\mathbf{x}) \tag{4.1}$$

Définition 4.1.2 *L'***entropie conjointe** *des deux variables aléatoires X et Y est l'in-*

certitude liée à la réalisation conjointe des variables X et Y, soit

$$\mathcal{H}(X,Y) = -\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{y}\in\mathcal{Y}} p(\mathbf{x},\mathbf{y})\log_2 p(\mathbf{x},\mathbf{y}) \tag{4.2}$$

où $p(\mathbf{x},\mathbf{y})$ est la loi conjointe des deux variables aléatoires.

Définition 4.1.3 *L'***entropie conditionnelle** *$\mathcal{H}(Y|X)$ est l'incertitude liée à la réalisation de Y, sachant que X est réalisée, soit*

$$\mathcal{H}(Y|X) = \sum_{\mathbf{x}\in\mathcal{X}} p(\mathbf{x})\mathcal{H}(Y|X=\mathbf{x}) = -\sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{y}\in\mathcal{Y}} p(\mathbf{x},\mathbf{y})\log_2 p(\mathbf{y}|\mathbf{x}) = \mathcal{H}(X,Y) - \mathcal{H}(X) \tag{4.3}$$

Définition 4.1.4 *L'***information mutuelle** *$I(X;Y)$ est l'information (ou la réduction d'incertitude) qu'apporte en moyenne la réalisation de Y sur X, ou aussi l'information qu'apporte en moyenne la réalisation de X sur Y, soit encore la divergence entre la distribution conjointe des deux variables aléatoires et le produit des deux distributions,*

$$I(X;Y) = \sum_{\mathbf{x}\in\mathcal{X}}\sum_{\mathbf{y}\in\mathcal{Y}} p(\mathbf{x},\mathbf{y})\log_2 \frac{p(\mathbf{x},\mathbf{y})}{p(\mathbf{x})p(\mathbf{y})} = \mathcal{H}(X) + \mathcal{H}(Y) - \mathcal{H}(X,Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X) \tag{4.4}$$

où on utilise les conventions (liées à la continuité) $0\log_2(\frac{0}{a}) = 0$ et $a\log_2(\frac{a}{0}) = \infty$.

Définition 4.1.5 *La* **capacité** *C d'un canal discret sans mémoire est le maximum de l'information mutuelle entre son entrée X et sa sortie Y.*

$$C = max_{p(x)} I(X;Y) \tag{4.5}$$

La capacité du canal est donc obtenue par optimisation de la pdf et de l'alphabet de canal. Cette capacité est encore le débit R_D maximum avec lequel on peut transmettre l'information tout en garantissant un taux d'erreur arbitrairement bas. Le débit est égal à $R_D = R \times \log_2 M$, où R est le taux de codage et M la taille de la modulation utilisée. Le théorème de codage, prouvé par Shannon s'énonce alors comme suit :

Théorème 4.1.1 *(Théorème de codage)*
Pout tout débit $R_D < C$, il existe un code tel que sa probabilité d'erreur soit arbitrairement petite. Un code infiniment long, bien choisi, permet donc une communication totalement fiable.

La réciproque du théorème de codage nous apprend qu'inversement, tous les codes dont la probabilité tend asymptotiquement vers zéro vérifient $R_D \leq C$.

Théorème 4.1.2 *(Réciproque du théorème de codage)*
Tous les codes dont la probabilité tend asymptotiquement vers zéro vérifient $R_D \leq C$.

La capacité[1] d'un canal pour une modulation en entrée donnée est donc aussi une mesure de faisabilité de la transmission sur le canal pour cette modulation. Ainsi, déterminer la capacité d'un canal pour les conditions d'une expérience permettra-t-il d'estimer d'une part la qualité de notre codage, mais encore de mesurer la marge de gain potentiel restante. C'est dans cet esprit que nous allons nous intéresser au paragraphe 4.2 au calcul de la capacité sur canal MIMO, pour lequel nous avons proposé un algorithme de décodage APP itératif au chapitre 3.

Nous déterminerons ensuite au paragraphe 4.3 la capacité dans le cas d'un canal de Rayleigh avec pour entrée une modulation tournée, cherchant ainsi à expliquer l'amélioration de performances sur canal de Rayleigh que nous avons pu constaté au chapitre 2. Nous montrerons ainsi que le fait d'utiliser une rotation augmente effectivement la capacité, ce que nous avons illustré en figure 4.2 par une "course des capacités" : plus la dimension de la rotation augmente, meilleure est la capacité obtenue, tendant vers la capacité obtenue pour une distribution gaussienne [47]. Nous présenterons des résultats numériques correspondant à ces calculs au paragraphe 4.4 et finalement nous tirerons quelques conclusions au paragraphe 4.5.

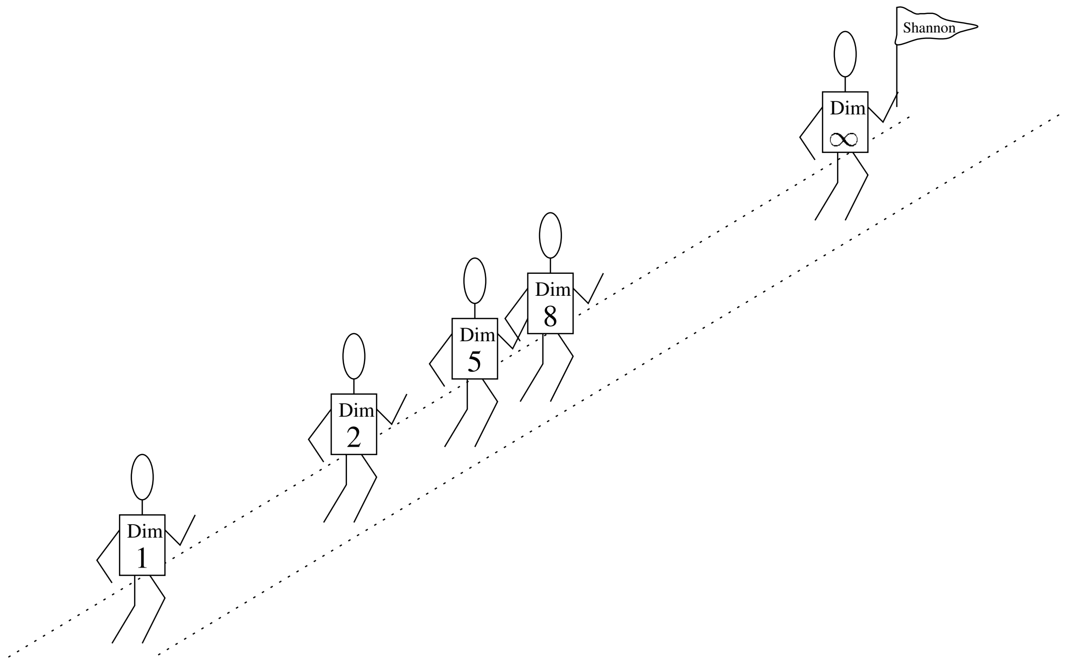


Fig. 4.2: La course des capacités

[1] Par abus de langage et à l'instar d'Ungerboeck [72], nous continuerons à utiliser le terme "capacité" lorsque la distribution $p(\mathbf{x})$ du signal en entrée est fixée.

4.2 Capacité d'un canal à entrées multiples et sorties multiples

4.2.1 Calcul de la capacité d'un canal à entrées multiples et sorties multiples

Le calcul de la capacité C sur un canal à entrées multiples et sorties multiples (n_t, n_r) a été réalisé en parallèle par Telatar [71] et Foschini [34]. Atteinte lorsque le signal d'entrée est gaussien[2], la capacité est égale à l'espérance mathématique de la capacité instantanée $C_{|H}$ calculée pour une valeur fixe H des coefficients du canal, obtenue par la formule (voir annexe D)

$$C_{|H} = \log_2 \left[\det \left(I_{n_r} + \frac{\rho}{n_t} H H^h \right) \right] \quad \text{bits / utilisation du canal} \tag{4.6}$$

où I_{n_r} est la matrice identité de rang n_r, et $\rho = E[\mathbf{x}^h \mathbf{x}]/E[\mathbf{b}^h \mathbf{b}]$ où $\mathbf{x} = (x_1, \ldots, x_{n_t})^t$ est le vecteur des signaux émis sur les n_t antennes et $\mathbf{b} = (b_1, \ldots, b_{n_r})^t$ est le vecteur des bruits blancs gaussiens sur les antennes de réception. ρ est donc égal à $\frac{n_t}{n_r} R \log_2(M) \frac{E_b}{N_0}$.

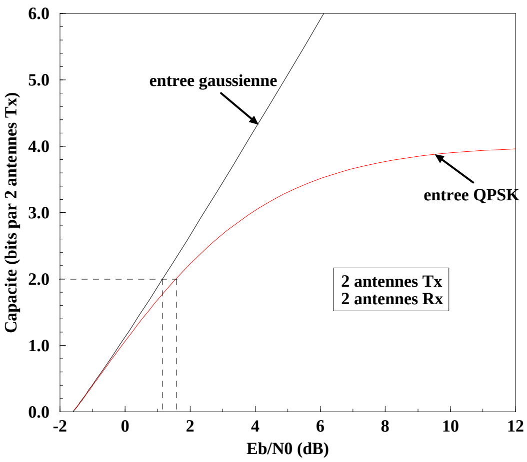
En pratique l'entrée du canal n'est pas gaussienne, on s'intéresse donc au calcul de la capacité d'un canal à entrée discrète $\mathbf{x}$ appartenant à une constellation $\mathcal{X}$ et à sortie continue $\mathbf{y}$. Pour cela, on remplace dans l'équation (4.5) l'information mutuelle moyenne par son expression donnée dans l'équation (4.4), et on obtient

$$C_{|H,\mathcal{X}} = \sum_{\mathbf{x} \in \mathcal{X}} \int_{\mathbf{y}} p(\mathbf{x}) p(\mathbf{y}|\mathbf{x}) \log_2 \left[\frac{p(\mathbf{y}|\mathbf{x})}{\sum_{\mathbf{x}' \in \mathcal{X}} p(\mathbf{x}') p(\mathbf{y}|\mathbf{x}')} \right] \tag{4.7}$$

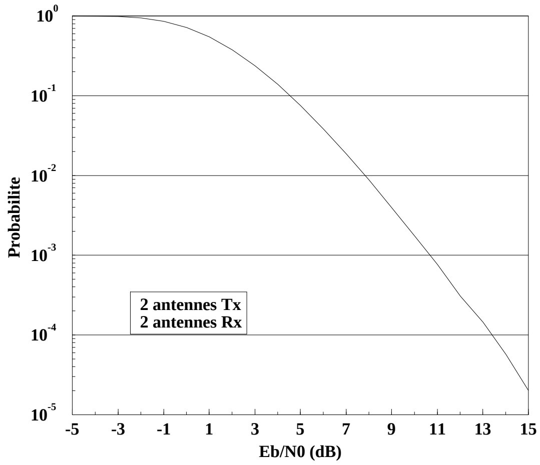
Dans le cas du canal MIMO considéré au paragraphe 3.5, i.e. pour une modulation QPSK (donc une constellation $\mathcal{X}$ de quatre éléments) avec 2 antennes d'émission et 2 antennes de réception, on obtient les courbes de capacités présentées en figure 4.3-a. Ces deux courbes de capacité, à savoir la capacité du canal MIMO $C = E_H[C_{|H}]$ et la capacité du canal pour une modulation QPSK en entrée $C_{QPSK} = E_H[C_{|H,QPSK}]$ correspondant respectivement aux équations (4.6) et (4.7), sont données en fonction du rapport signal à bruit $\frac{E_b}{N_0}$ où E_b est l'énergie totale reçue par le destinataire par bit d'information émis. Les capacités pour une valeur de $2 \times 2 \times \frac{1}{2} = 2$ bits par 2 antennes d'émission sont tracées en pointillés puisqu'elles correspondent au cas considéré dans le chapitre précédent, où les simulations ont été menées pour des QPSK sur 2 antennes d'émission et un taux de codage $R = 1/2$.

On notera que nous nous sommes restreints ici à l'étude de la capacité intéressant nos travaux du chapitre 3. D'autres études menées récemment sur la capacité des canaux

[2]ou plus généralement spécial gaussien comme l'a défini et montré Telatar [71] (voir annexe D)



(a) : capacité



(b) : probabilité de coupure

FIG. 4.3: Capacité et probabilité de coupure pour $R = 1/2$, sur un canal de Rayleigh MIMO, n_t=n_r=2 antennes.

radio-mobiles pourront être consultées pour qui veut en apprendre plus sur ce domaine, comme par exemple ceux de Boixadera *et al.* [14] pour le cas où les antennes ne sont pas décorrélées, ou par Marzetta *et al.* [54] lorsque la matrice du canal est considérée comme inconnue par l'émetteur et le destinataire.

4.2.2 Probabilité de coupure pour les canaux de Rayleigh par blocs

Si la capacité est traditionnellement considérée comme étant un bon moyen d'estimer la quantité d'information pouvant être transmise sur un canal à un taux d'erreur arbitrairement bas, il a été montré dans [55] que ceci n'est plus vrai dans le cas des canaux dont la durée de cohérence est grande devant la taille des blocs de données émis, puisque la condition d'ergodicité du canal n'est alors plus vérifiée.

C'est le cas pour les canaux radio-mobiles, notamment les canaux de Rayleigh par blocs dont la durée de cohérence ne permet pas de considérer que les trames de données transmises voient un ensemble de coefficients statistiquement représentatif. Une notion nouvelle a donc été introduite pour ce type de canaux, à savoir une capacité associée à une probabilité de coupure (*outage probability*), c'est-à-dire un taux de confiance associée à la capacité considérée. La capacité est alors considérée comme une variable aléatoire dépendant de la réponse instantanée du canal (néanmoins constante par bloc). Si la capacité instantanée est au-dessous du taux auquel on essaie de transmettre, en aucun cas le bloc transmis ne pourra être décodé sans erreur, quel que soit le système de codage/décodage employé. Inversement, si la capacité instantanée est au-dessus du taux auquel on essaie de transmettre, le théorème de Shannon nous indique qu'il existe un code permettant de transmettre à ce taux avec une probabilité d'erreur arbitrairement basse.

Cette probabilité de coupure nous permet donc d'estimer les performances possibles sur les canaux non ergodiques [71][34]. Dans le cas du canal MIMO considéré au paragraphe 3.5, soit avec 2 antennes d'émission et 2 antennes de réception et un taux de codage égal à 1/2, on a ainsi la probabilité de coupure

$$P_{out}\left(\frac{E_b}{N_0}\right) = Prob\left(C_{|H}\left(\frac{E_b}{N_0}\right) < 2\right) = \int_{c=0}^{2} p(c)dc \tag{4.8}$$

où $c = C_{|H}(\frac{E_b}{N_0})$ est la capacité instantanée pour une réalisation donnée définie par la formule (4.6). La courbe de cette probabilité de coupure est donnée en figure 4.3-b.

Les courbes présentées en figures 4.3-a et 4.3-b ont ainsi été utilisées au chapitre 3 pour juger les performances des modulations à entrelacement de bits sur canal à entrées et sorties multiples.

4.3 Capacité d'un canal ayant pour entrée une modulation tournée

4.3.1 Modèle du système considéré et notations

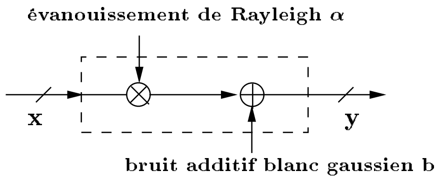


FIG. 4.4: Schéma de principe d'un canal de Rayleigh

On considère un canal de Rayleigh non sélectif avec évanouissements indépendants, comme celui de la figure 4.4. L'entrée $\mathbf{x} = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$ et la sortie $\mathbf{y} = (y_1, \ldots, y_n)^t \in \mathbb{R}^n$, où $\mathbf{u}^t$ représente la version transposée d'un vecteur $\mathbf{u}$, sont liées par la relation

$$\mathbf{y} = \boldsymbol{\alpha} \odot \mathbf{x} + \mathbf{b} \tag{4.9}$$

où $\mathbf{b} = (b_1, \ldots, b_n)^t$ est le vecteur de bruit additif blanc gaussien de moyenne nulle et de variance N_0 par composante réelle, où $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)^t \in \mathbb{R}^{+n}$ est le vecteur des évanouissements sur le canal dont la loi de probabilité est donnée par $p(\alpha_k) = 2\alpha_k \exp(-\alpha_k^2), k = 1, \ldots, n$ et où $\odot$ représente le produit composante par composante de deux vecteurs.

Lorsque l'entrée du canal est la sortie d'une rotation $R = (r_{ij})_{i,j=1,\ldots,n}$ de dimension n, les coefficients $x_i, i = 1, \ldots, n$ sont trivialement donnés par

$$x_i = \sum_{j=1}^{n} r_{ij} z_j \quad i = 1, \ldots, n \tag{4.10}$$

où les entrées $\mathbf{z} = (z_1, \ldots, z_n)$ sont des éléments d'une constellation PAM $\{\mathcal{I}_1, \ldots, \mathcal{I}_M\}$ de taille M. Par exemple, dans le cas d'une BPSK, on a $M = 2$ et $z_i = \pm 1$.

Si l'on remplace dans l'équation (4.9) les coefficients x_i par leur valeur donnée par l'équation (4.10), on obtient l'expression

$$\mathbf{y} = \boldsymbol{\alpha} \odot R\mathbf{z} + \mathbf{b} \tag{4.11}$$

4.3.2 Relation entre capacité et distance produit-ℓ minimale $d_{P,min}^{(\ell)}$

Comme nous l'avons vu dans le paragraphe 2.3.2 de notre chapitre sur les rotations, un des critères de construction des rotations est la distance produit-ℓ minimale $d_{P,min}^{(\ell)}$ entre toute paire de points de la constellation considérée. La recherche de réseaux $\mathbb{Z}_{n,n}$ satisfaisant ce critère a été menée par Boutros [16], chap. 5.

Toute matrice de rotation en dimension 2 peut être caractérisée grâce à un unique paramètre $\lambda, \lambda \in \mathbb{R}$

$$R(\lambda) = \begin{pmatrix} 1/\sqrt{1+\lambda^2} & \lambda/\sqrt{1+\lambda^2} \\ -\lambda/\sqrt{1+\lambda^2} & 1/\sqrt{1+\lambda^2} \end{pmatrix}$$

La figure 4.5 montre les valeurs de $d_{P,min}^{(\ell)}$ pour un ordre de diversité $\ell = 2$ en fonction de λ pour une taille de constellation correspondant à une efficacité spectrale $\eta = 8$ bits/symbole tirée du réseau généré par la rotation $R(\lambda)$. Ces valeurs de $d_{P,min}^{(\ell)}$ ont été déterminées grâce à une recherche exhaustive de tous les points de la constellation finie en utilisant un pas de 0.001 pour λ.

Sur la même figure sont également représentées deux courbes de capacité (voir paragraphe 4.3.4) pour les réseaux générés par la rotation $R(\lambda)$, l'une pour un rapport signal à bruit élevé, $E_c/N_0 = 10$ dB (correspondant à $E_b/N_0 \approx 10$ dB) et l'autre pour un rapport signal à bruit très faible, $E_c/N_0 = -10$ dB (correspondant à $E_b/N_0 \approx -1.0$ dB) et dans les deux cas pour un pas de 0.1 pour λ. Dans ce dernier cas, on constate que les meilleures rotations en terme de capacité, atteintes pour des valeurs de λ proches de 1 (i.e. pour des rotations d'angles proches de 45°) correspondent à une zone pour laquelle les distances produit-ℓ minimales sont très faibles. Il apparaît clairement que le critère de construction fondé sur la maximisation de $d_{P,min}^{(\ell)}$ n'est pas valable pour de faibles rapports signal à bruit. En effet, dans le cas d'un bruit élevé (i.e. pour un faible rapport signal à bruit),

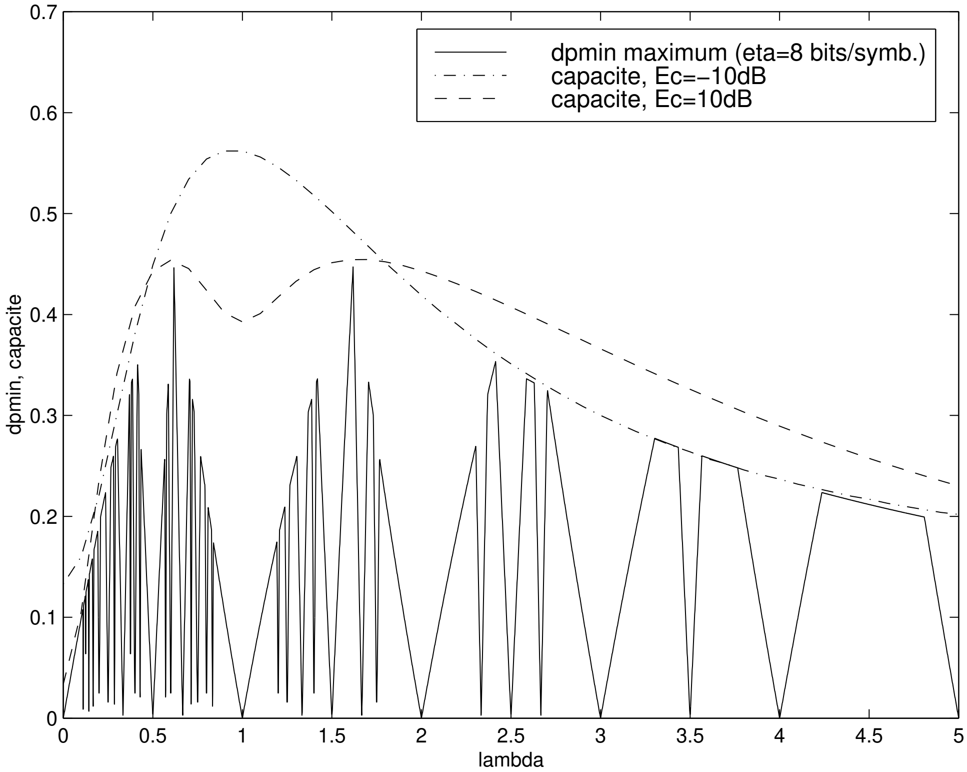


FIG. 4.5: Comparaison des performances d'une rotation en terme de distance produit-ℓ minimale ($d_{P,min}^{(\ell)}$) et de capacité pour différentes valeurs du paramètre λ en dimension 2.

l'approximation permettant de majorer la probabilité d'erreur par paire grâce à la *série théta* du réseau, et donc dépendant en particulier de la distance produit-ℓ minimale du réseau n'est plus applicable. En revanche, lorsque l'on considère un fort rapport signal à bruit, cette majoration de la probabilité d'erreur par paire est pleinement valable et donc on retrouve bien deux pics de capacité pour des valeurs de λ optimales selon le critère de maximisation de la distance produit-ℓ minimale. Ces pics correspondent aux valeurs de $\lambda = \left|\frac{1\pm\sqrt{5}}{2}\right|$, ce qui donne deux angles symétriques par rapport à la première bissectrice 31.7° et 58.3°).

On notera que chacune des échelles des courbes de capacité a fait l'objet d'une modification (translation et homothétie selon l'axe des ordonnées) destinée à nous permettre de comparer leurs résultats. Pour des raisons de symétrie, on a de plus considéré uniquement les valeurs positives du paramètre λ.

De cette comparaison on peut donc déduire que le critère classiquement reconnu de maximisation de la distance produit-ℓ $d_{P,min}^{(\ell)}$ et de l'ordre de diversité pour trouver la meilleure constellation possible en terme de performances amène également à d'excellentes capacités lorsque l'on travaille à une valeur du rapport signal à bruit suffisamment importante. Dans le cas contraire, et comme également observé pour d'autres systèmes ou modulations à forte diversité (par exemple, PSK, FSK avec ordre de diversité $L = 4$ [58], chap. 14), augmenter la diversité à faible rapport signal à bruit tend à dégrader les performances plutôt qu'à les améliorer.

Ayant ainsi vérifié pour la dimension 2 qu'il n'existait pas à proprement parler de lien direct entre la distance produit-ℓ minimale et la capacité, nous allons nous intéresser à un autre critère classique de choix de rotation, à savoir la diversité, et chercher à en apprendre plus sur la relation existant entre capacité et diversité, si elle existe.

4.3.3 Relation entre capacité et diversité pour les modulations tournées : "*gaussianisation*" du canal

Il est bien connu [47] que la capacité d'un canal de Rayleigh non sélectif à coefficients indépendants est atteinte lorsque l'entrée dudit canal a une distribution suivant une loi de probabilité gaussienne. Ceci est d'ailleurs la raison pour laquelle les codes gaussiens sont optimaux. Hélas, ils ne sont pas réalisables en pratique, ce qui nous a amené à nous interroger sur l'existence de transformations aptes à *gaussianiser* un flot que l'on pourrait alors transmettre sur le canal considéré.

Il apparaît que les rotations sont des transformations satisfaisant ce critère, car elles permettent d'augmenter la diversité sur le canal à évanouissement de Rayleigh en répartissant l'information sur plusieurs signaux à transmettre, les "*gaussianisant*". Nous allons montrer ceci dans le cas particulier des matrices d'Hadamard ou plus généralement de type Hadamard.

Une formule directe exacte des composantes h_{ik} de la matrice de Hadamard définie par la formule (2.18), est très difficile à établir. En conséquence, comme au chapitre 2, nous utiliserons une matrice H_n de type Hadamard afin de calculer sa densité de probabilité. Cette matrice de type Hadamard $H_n = (h_{ik})_{i,k=1,\ldots,n}$ est construite en normalisant une matrice remplie de façon pseudo-aléatoire d'éléments ± 1, avec pour contrainte que chaque ligne contient autant d'éléments '+1' que d'éléments '−1' :

$$\forall (i,k) \in \mathbb{N} \quad h_{ik} = \frac{\pm 1}{\sqrt{n}} \; ,$$

$$p(h_{ik} = \tfrac{+1}{\sqrt{n}}) = p(h_{ik} = \tfrac{-1}{\sqrt{n}}) \; .$$

D'après l'équation (4.10), sachant que les $z_k, k = 1, \ldots, n$ sont des symboles équiprobables et appartiennent à une PAM-M, il apparaît que chaque composante $x_i, i = 1, \ldots, n$ a la même probabilité d'être strictement positive ou strictement négative. Sachant de plus que $p(h_{ik} = \frac{+1}{\sqrt{n}}) = p(h_{ik} = \frac{-1}{\sqrt{n}})$, nous pouvons, sans perte de généralité, considérer que x_i est donné par $x_i = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} z_k$, et donc est indépendant de i. Il sera alors possible de déterminer la densité de probabilité pour tout x_i en utilisant les fonctions caractéristiques des z_k.

La densité de probabilité de z_k est donnée par

$$p_{z_k}(z) = \frac{1}{M} \sum_{\ell=1}^{M} \delta(z - \mathcal{I}_\ell) \tag{4.12}$$

où $\delta(\cdot)$ est la fonction de Dirac (ou impulsion de Dirac) qui vérifie

$$\begin{aligned} &\delta(0) = +\infty \\ &\delta(z) = 0 \quad \text{pour tout } z \neq 0 \\ &\textstyle\int_{-\infty}^{+\infty} \delta(z) dz = 1 \\ &p(z)\delta(z) = p(0)\delta(z) \; . \end{aligned} \tag{4.13}$$

En conséquence, la fonction caractéristique $\psi_{z_k}(u)$ de z_k est [56]

$$\psi_{z_k}(u) = E[e^{jz_k u}] = \int_z p_{z_k}(z) e^{jz_k u} dz = \frac{1}{M} \sum_{\ell=1}^{M} e^{j\mathcal{I}_\ell u} \; . \tag{4.14}$$

Ainsi, prenant en considération le fait que pour notre matrice H_n la fonction ψ_{z_k} est indépendante de k, l'expression de ψ_{x_i} est tout naturellement donnée par

$$\psi_{x_i}(u) = \prod_{k=1}^{n} \psi_{\frac{z_k}{\sqrt{n}}}(u) = \prod_{k=1}^{n} \left(\frac{1}{M} \sum_{\ell=1}^{M} e^{j\mathcal{I}_\ell u/\sqrt{n}} \right) = \left(\frac{\sum_{\ell=1}^{M} e^{j\mathcal{I}_\ell u/\sqrt{n}}}{M} \right)^n$$

Dans le cas où la constellation est une BPSK, soit pour $M = 2$, on obtient alors

$$\psi_{x_i}(u) = \left(\frac{\sum_{\ell=1}^{2} e^{j\mathcal{I}_\ell u/\sqrt{n}}}{2} \right)^n = \left(\cos \frac{u}{\sqrt{n}} \right)^n \tag{4.15}$$

où $\frac{u}{\sqrt{n}} \in [-\pi; \pi]$. Par symétrie on se limitera à l'intervalle $[-\pi/2; \pi/2]$.

Au voisinage de 0, $\cos \frac{u}{\sqrt{n}}$ peut être développé selon la formule suivante

$$\cos \frac{u}{\sqrt{n}} = 1 - \frac{u^2}{2n} + O(\frac{u^4}{n^2})$$

Réinjectant cette dernière formule dans l'équation (4.15) et en prenant le logarithme nous trouvons

$$\log \psi_{x_i}(u) = n \times \log \left(1 - \frac{u^2}{2n} + O(\frac{u^4}{n^2}) \right)$$

ce qui devient, pour n grand,

$$\log \psi_{x_i}(u) = n\left(-\frac{u^2}{2n} + O(\frac{u^4}{n^2})\right) = -\frac{u^2}{2} + O(\frac{u^4}{n})$$

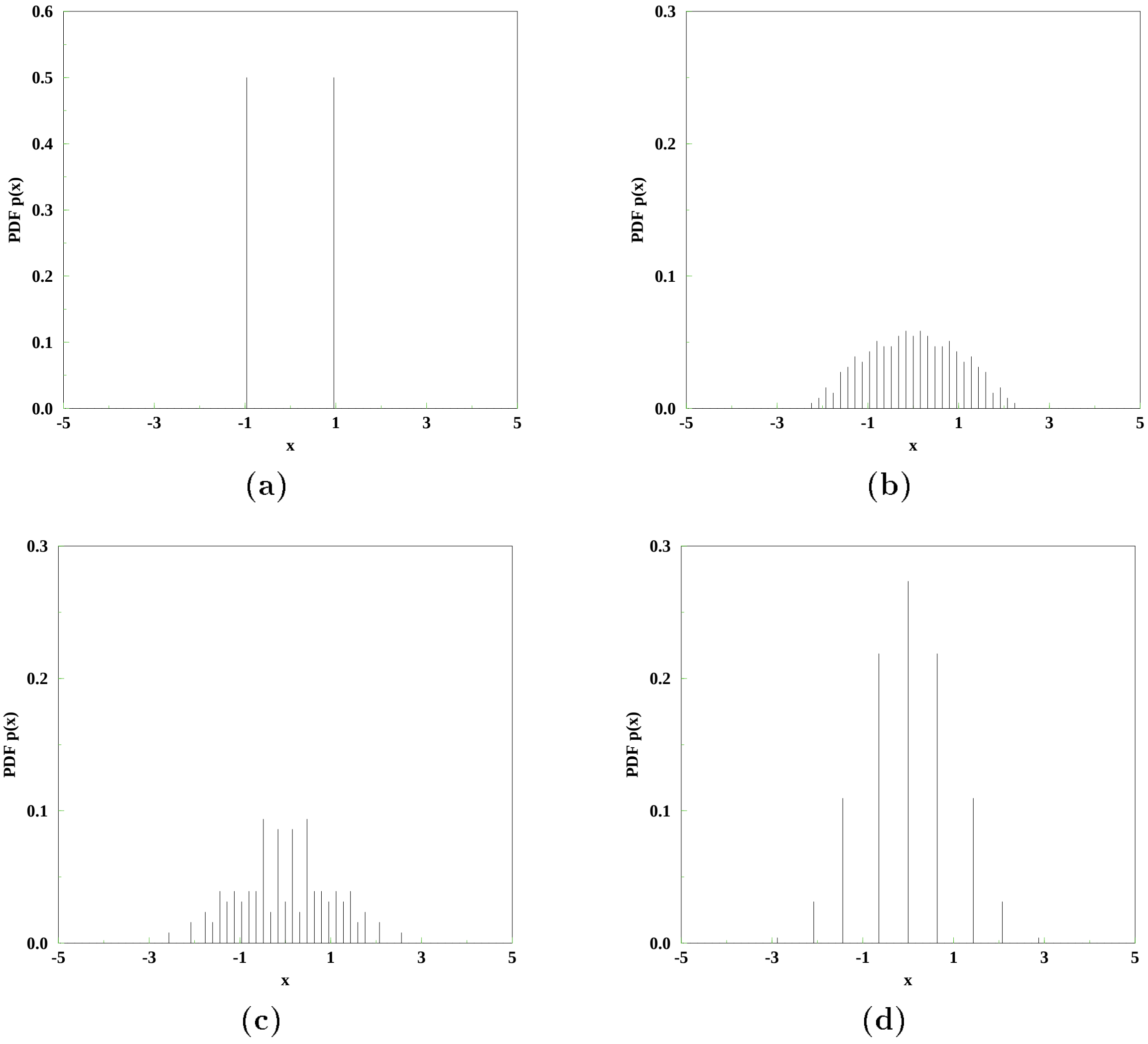


FIG. 4.6: Les raies de la pdf en sortie de plusieurs rotations en dimension 8 pour une entrée BPSK sur chaque composante (a): I_8 (b): $\mathbb{Z}_{8,8}$ (c): $\mathbb{Z}_{8,4,a}$ (d): $Hada_8$.

Lorsque l'on considère la limite de cette formule pour n tendant vers l'infini, on obtient

$$\log \psi_{x_i}(u) \rightarrow_{n\rightarrow+\infty} -\frac{u^2}{2}$$

soit

$$\psi_{x_i}(u) \rightarrow_{n\rightarrow+\infty} \exp\left(-\frac{u^2}{2}\right) .$$

La densité de probabilité d'une composante x_i, obtenue en prenant la transformée de Fourier de la fonction caractéristique tend vers [58]

$$p_{x_i} \rightarrow_{n \to +\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x_i^2}{2}\right)$$

ce qui signifie que x_i devient une gaussienne centrée de variance 1 au sens de la *loi forte des grands nombres* (convergence en lois de probabilité) [56].

La figure 4.6 illustre le calcul précédent en présentant les allures des pdf en sortie de quatre rotations en dimension 8 introduites dans le chapitre 2. On observe bien ici, en les comparant à la courbe sans rotation (ou encore rotation identité) présentée en figure 4.6-a une mise en forme des pdf les rapprochant d'une gaussienne. La discrétisation que l'on observe est due au fait que l'entrée est constituée de symboles BPSK.

4.3.4 Calcul de la capacité d'un canal ayant pour entrée une constellation tournée

La capacité du canal à entrée discrète représenté en figure 4.4 est donnée par [76]

$$\begin{aligned} C &= \max_{p(\mathbf{x})} I(X;Y) = \max_{p(\mathbf{x})} (\mathcal{H}(X) - \mathcal{H}(X|Y)) \\ &= \max_{p(\mathbf{x})} \sum_{\mathbf{x}} \int_{\mathbf{y}} p(\mathbf{x})p(\mathbf{y}|\mathbf{x}) \log_2 \left(\frac{p(\mathbf{y}|\mathbf{x})}{\sum_{\mathbf{x}'} p(\mathbf{x}')p(\mathbf{y}|\mathbf{x}')} \right) d\mathbf{y} \ . \end{aligned} \tag{4.16}$$

Considérons à présent une constellation $\mathcal{X} = \{\mathbf{x}^j\}_{j=1}^M$ composée de M signaux équiprobables où les $\mathbf{x}^j = (x_i^j)_{i=1}^n \in \mathbb{R}^n$ sont les signaux et $M = |\mathcal{X}| = 2^m$. La distribution de probabilité $p(\mathbf{x})$ de ces signaux en entrée est alors donnée par

$$p(\mathbf{x}^j) = 1/M \quad j = 1, \ldots, M \ . \tag{4.17}$$

La capacité du canal ayant une telle constellation en entrée est donc

$$C = I(X;Y) = \mathcal{H}(X) - \mathcal{H}(X|Y) \ . \tag{4.18}$$

L'équation (4.16) devient donc

$$\begin{aligned} C &= m - \frac{1}{M} \sum_{\mathbf{x}} \int_{\mathbf{y}} p(\mathbf{y}|\mathbf{x}) \log_2 \left(\frac{\sum_{\mathbf{x}' \in \mathcal{X}} p(\mathbf{y}|\mathbf{x}')}{p(\mathbf{y}|\mathbf{x})} \right) d\mathbf{y} \\ &= m - \frac{1}{M} \sum_{\mathbf{x}} \int_{\boldsymbol{\alpha}} p(\boldsymbol{\alpha}) \int_{\mathbf{y}} p(\mathbf{y}|\mathbf{x}, \boldsymbol{\alpha}) \log_2 \left(\frac{\sum_{\mathbf{x}' \in \mathcal{X}} p(\mathbf{y}|\mathbf{x}', \boldsymbol{\alpha})}{p(\mathbf{y}|\mathbf{x}, \boldsymbol{\alpha})} \right) d\mathbf{y} d\boldsymbol{\alpha} \end{aligned} \tag{4.19}$$

où, sachant que le bruit sur le canal est gaussien, l'expression de la densité de probabilité de transition sur le canal est, pour un évanouissement $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ donné,

$$p(\mathbf{y}|\mathbf{x}, \boldsymbol{\alpha}) = \frac{1}{(\sqrt{2\pi N_0})^n} \exp\left(-\frac{1}{2N_0}\|\mathbf{y} - \boldsymbol{\alpha} \odot \mathbf{x}\|^2\right)$$

et où la densité de probabilité d'une variable de Rayleigh normalisée $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ est

$$p(\boldsymbol{\alpha}) = \prod_{k=1}^{n} \left[2\alpha_k \exp(-\alpha_k^2)\right]$$

d'où l'expression de la capacité par dimension, en posant $\mathbf{z} = (\mathbf{y} - \boldsymbol{\alpha} \odot \mathbf{x})/(2N_0)$,

$$C_{dim} = \frac{m}{n} - \frac{1}{nM} \sum_{\mathbf{x}} \int_{\mathbb{R}_+^n} \int_{\mathbb{R}^n} \prod_{k=1}^{n} \left[2\alpha_k \exp(-\alpha_k^2)\right] \frac{\exp(-\|\mathbf{z}\|^2)}{(\sqrt{\pi})^n} \log_2 \left(\frac{\sum_{\mathbf{x}' \in \mathcal{X}} \exp(-\|\mathbf{z} + \frac{\boldsymbol{\alpha} \odot (\mathbf{x}' - \mathbf{x})}{\sqrt{2\mathbf{N_0}}}\|^2)}{\exp(-\|\mathbf{z}\|^2)} \right) d\mathbf{z} d\boldsymbol{\alpha} \ . \tag{4.20}$$

Donc dans le cas où les modulations sont des BPSK, on a $M = 2^n$

$$C_{dim} = 1 - \frac{1}{M} \sum_{\mathbf{x}} \int_{\mathbb{R}_+^n} \int_{\mathbb{R}^n} \prod_{k=1}^{n} \left[2\alpha_k \exp(-\alpha_k^2)\right] \frac{\exp(-\|\mathbf{z}\|^2)}{(\sqrt{\pi})^n} \log_2 \left(\frac{\sum_{\mathbf{x}' \in \mathcal{X}} \exp(-\|\mathbf{z} + \frac{\boldsymbol{\alpha} \odot (\mathbf{x}' - \mathbf{x})}{\sqrt{2\mathbf{N_0}}}\|^2)}{\exp(-\|\mathbf{z}\|^2)} \right) d\mathbf{z} d\boldsymbol{\alpha} \ . \tag{4.21}$$

On notera qu'il est important de se rappeler que ce calcul de la capacité par dimension, utile pour comparer les performances de rotations de dimensions différentes, ne peut se faire en considérant chaque dimension de la constellation séparément. En effet, dans la plupart des cas, ces composantes sont corrélées par la diversité engendrée par la matrice de rotation et donc sommer sur toutes les composantes pour obtenir une capacité par dimension moyenne donnerait des résultats totalement faux.

4.4 Résultats numériques

L'expression de la capacité par dimension déterminée par l'équation (4.20) nous permet de comparer les capacités de rotations en dimensions distinctes. Nous considérerons ici différentes rotations en dimensions 2, 4, 5 et 8.

La figure 4.7 montre ainsi des résultats pour des BPSK tournées pour plusieurs dimensions, ainsi que des courbes de référence de la transmission de modulations BPSK ou gaussiennes sur les canaux de Rayleigh ou AWGN.

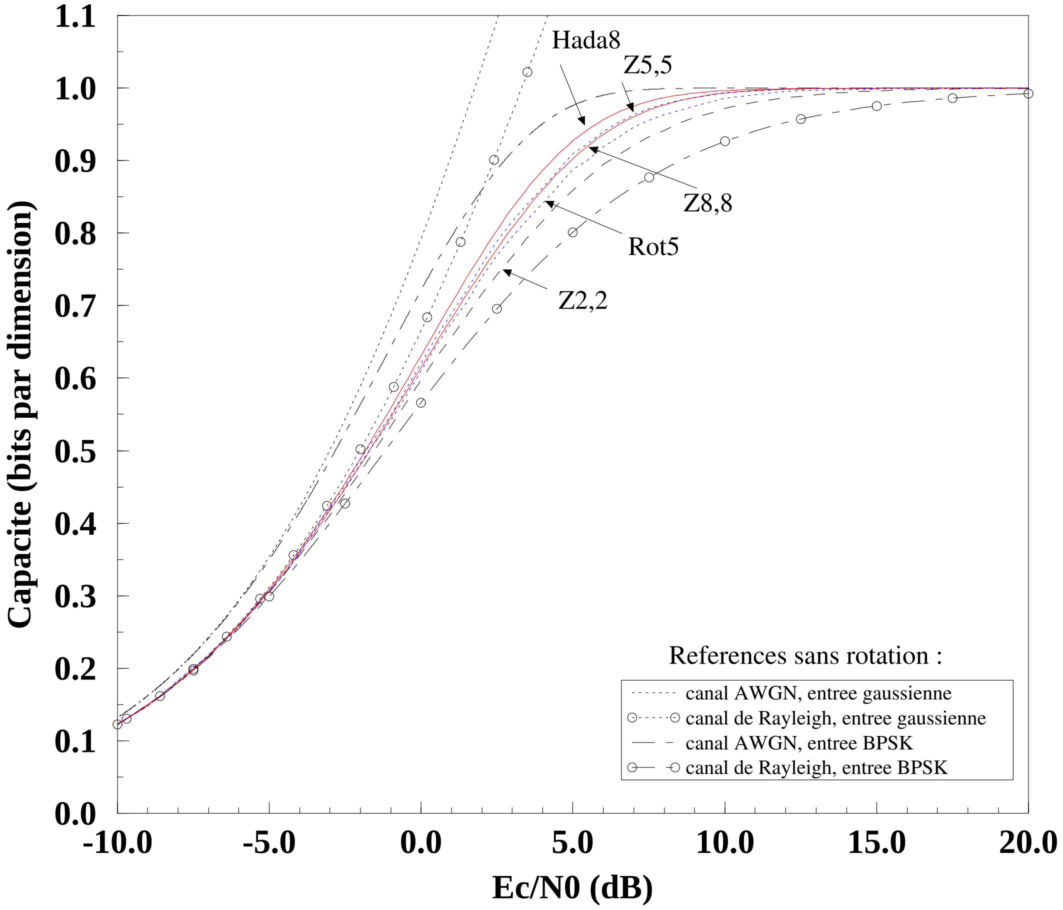


Fig. 4.7: Capacité pour plusieurs rotations en dimensions 2, 5 et 8.

Puisque pour des raisons évidentes, il est impossible de tracer les courbes de toutes les rotations possibles, nous nous sommes restreints à trois valeurs de dimensions, soit 2, 5 et 8 et pour chacune de ces valeurs, nous avons sélectionné parmi les rotations que nous avons pu tester la “meilleure” et la “pire” rotation en terme de capacité. On notera cependant que pour toute dimension la capacité est minorée par la capacité sur canal de Rayleigh avec entrée BPSK et majorée d'une part par la courbe de capacité sur canal de Rayleigh avec entrée gaussienne et d'autre part par la capacité sur canal AWGN avec entrée BPSK.

Les courbes retenues sont celles correspondant à la rotation $\mathbb{Z}_{2,2}$ [19], rotation optimale en terme de diversité et de distance produit-ℓ pour la dimension 2, les rotations Rot_5 [29] et $\mathbb{Z}_{5,5}$ [19] en dimension 5 et les rotations $Hada_8$ et $\mathbb{Z}_{8,8}$ [19] en dimension 8. Par souci de se conformer à la littérature existante, les courbes de capacité de ce paragraphe ont été tracées en fonction de E_c/N_0, soit en fonction du rapport signal à bruit par bit codé. Il est néanmoins aisé de retrouver le rapport signal à bruit par bit d'information correspondant, en se rappelant que $E_c/N_0 = C_{dim} \times E_b/N_0$.

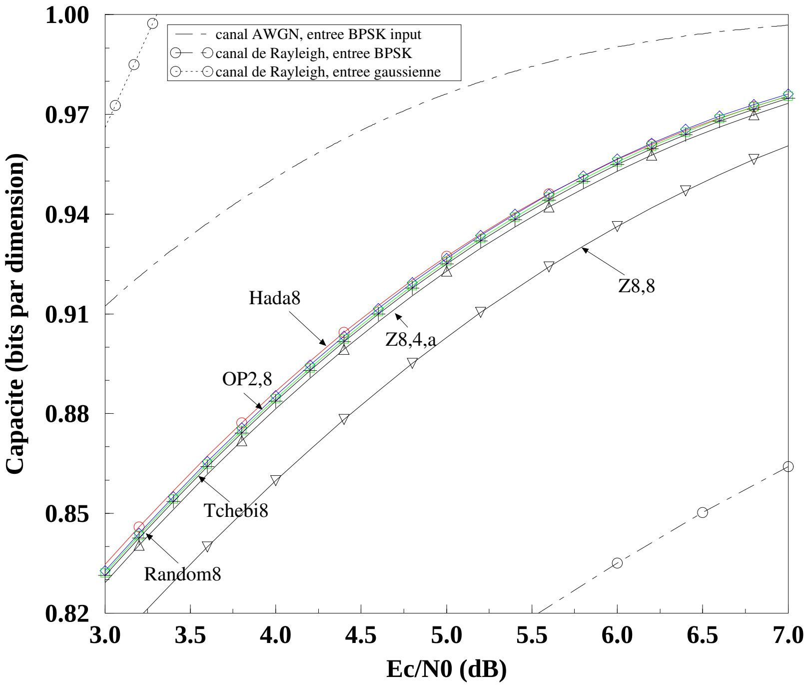


Fig. 4.8: Zoom sur la capacité de plusieurs rotations en dimension 8.

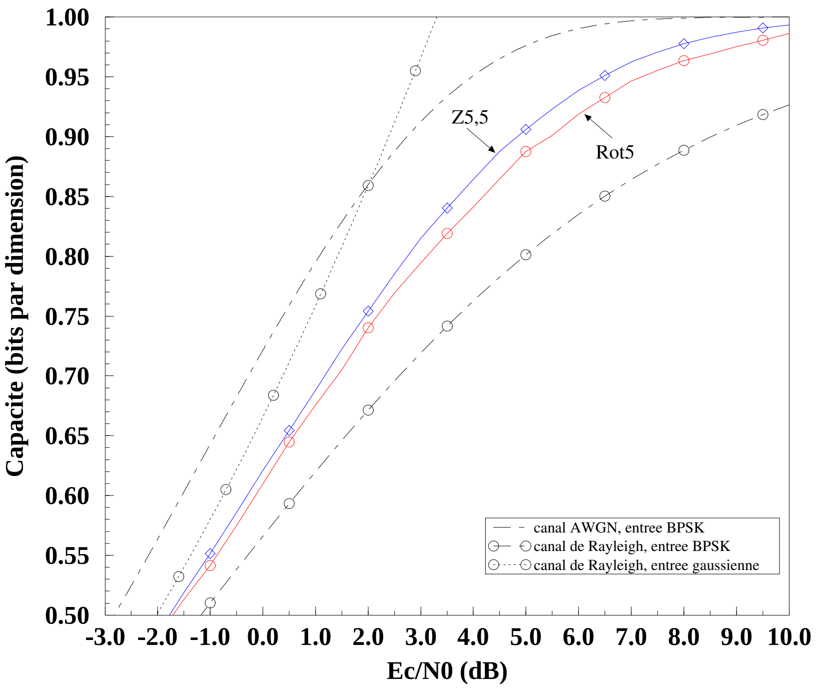


Fig. 4.9: Zoom sur la capacité de plusieurs rotations en dimension 5.

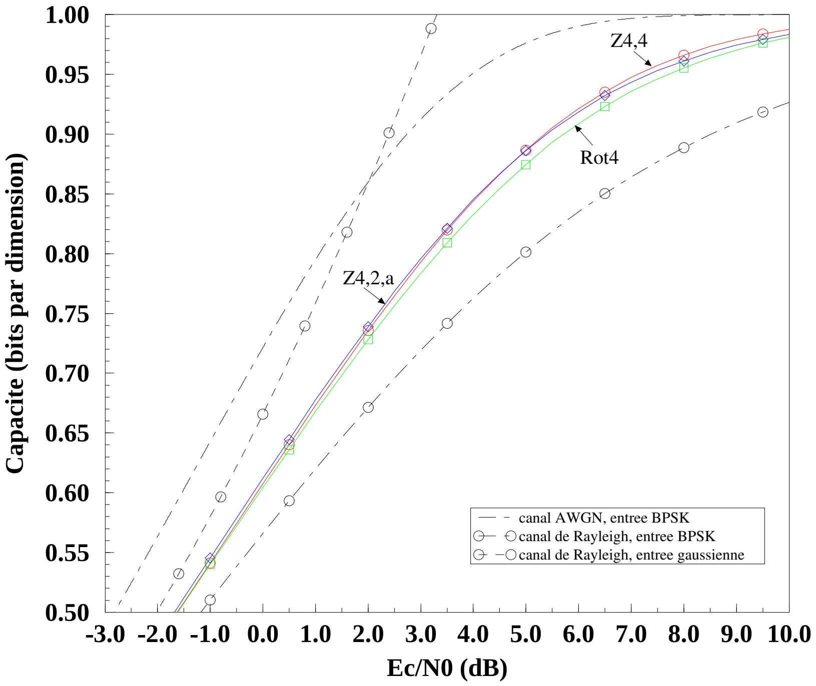


Fig. 4.10: Zoom sur la capacité de plusieurs rotations en dimension 4.

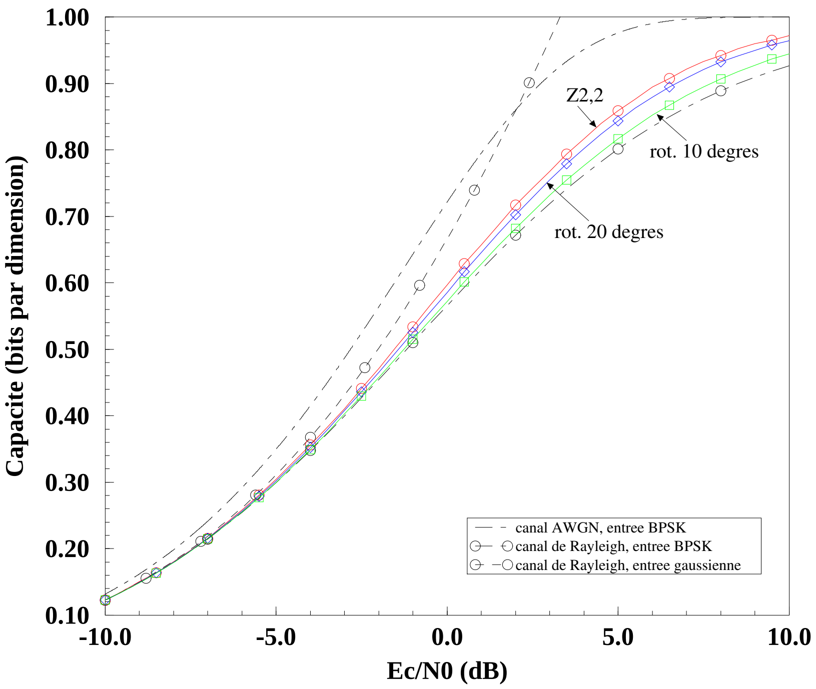


Fig. 4.11: Zoom sur la capacité de plusieurs rotations en dimension 2.

Le choix de la rotation $\mathbb{Z}_{2,2}$ a également été motivé par une recherche numérique sur l'ensemble des rotations $R = \begin{bmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{bmatrix}$ en dimension 2 de la rotation (ou de façon équivalente de son angle de rotation $\theta = \arctan(-\lambda)$ avec λ est le paramètre défini au paragraphe 4.3.2) maximisant la capacité. Réalisant à cet effet une recherche discrétisée avec un pas de 0.1° sur l'angle θ, nous avons obtenu pour angle optimal la valeur $\theta_{opt} = 31.7°$ correspondant à la valeur trouvée analytiquement $\theta = \frac{1}{2}atan(2)$ [29]. La figure 4.11 permet de comparer cette rotation optimale avec d'autres rotations en dimension 2, à savoir celles correspondant à des angles de 20° et 10°. Nous observons ainsi par exemple que cette dernière rotation présente une perte de 0.5 dB pour $R = 2/3$ et de 0.3 dB pour $R = 1/2$ comparativement à la rotation optimale $\mathbb{Z}_{2,2}$.

Ainsi qu'on peut l'observer sur la figure 4.7, le fait d'utiliser une rotation amène un gain dès la dimension 2 : pour un taux de codage $R = 1/2$, et comparé à la transmission classique d'une BPSK sur canal de Rayleigh non sélectif à évanouissements indépendants, $\mathbb{Z}_{2,2}$ gagne 0.3 dB, $\mathbb{Z}_{5,5}$ gagne 0.55 dB, et $Hada_8$ gagne 0.6 dB : seul 0.2 dB la sépare de la limite théorique obtenue avec une entrée gaussienne ! Les gains sont encore plus importants lorsque le taux de codage augmente, puisque pour un taux $R = 2/3$, $\mathbb{Z}_{2,2}$ gagne 0.7 dB, $\mathbb{Z}_{5,5}$ gagne 1.25 dB, et $Hada_8$ gagne 1.4 dB, n'étant plus qu'à 0.5 dB de la limite.

Un autre résultat intéressant est le fait que si la meilleure capacité que l'on peut atteindre augmente avec la dimension, il apparaît également qu'une mauvaise rotation en une dimension m_1 peut avoir une capacité inférieure à celle d'une bonne rotation en dimension $m_2 < m_1$, d'où l'intérêt évident de choisir une "bonne" rotation pour nos systèmes. La figure 4.8 présente les capacités de six rotations en dimension 8, à savoir respectivement dans un ordre décroissant de résultat $Hada_8$, $OP_{2,8}$, $Tchebi_8$, $Random8$, $\mathbb{Z}_{8,4,a}$ et $\mathbb{Z}_{8,8}$ (les matrices de ces rotations sont données dans l'annexe B).
Tout en gardant à l'esprit que les courbes de cinq de ces rotations sont séparées d'au plus 0.2 dB, et donc qu'elles sont de fait toutes de "bonnes" rotations en terme de capacité sur le canal à évanouissements, on notera néanmoins que la meilleure d'entre elles est celle correspondant à la matrice de Hadamard $Hada_8$, qui pour une entrée BPSK est de diversité 4 et, comme nous l'avons montré dans le paragraphe 4.3.3 a une densité de probabilité dont la distribution s'approche d'une gaussienne montrant ainsi que la distribution de diversité importe plus à faible rapport signal à bruit que la diversité minimale. Inversement, on notera que l'une des meilleures rotations en terme de diversité, soit $\mathbb{Z}_{8,8}$ de diversité 8, est de loin la pire des six rotations considérées en terme de capacité. Les figures 4.9 et 4.10 montrent également d'autres rotations présentées au chapitre 2 (leurs matrices se trouvant dans l'annexe B). On constate ainsi que la rotation Rot_4 optimisée en dimension 4 par Da Silva *et al.* [29] présente une perte de 0.1 à 0.15 dB par rapport à la rotation Rot_5 optimisée en dimension 5.

4.5 Conclusions

Après un bref rappel des méthodes de calcul des capacités et de la probabilité de coupure sur un canal MIMO, nous les avons appliqués au cas du système multi-antennes considéré au chapitre précédent et ce faisant obtenant des estimateurs des performances simulées. Nous avons par ailleurs montré que le fait de tourner une constellation MAQ, initialement proposé dans la littérature [5][15][17] pour augmenter la diversité sur le canal de Rayleigh non sélectif à évanouissements indépendants, réalise une "gaussianisation" du signal, augmentant ainsi la capacité. Une méthode de calcul de la capacité pour le canal de Rayleigh ayant en entrée une constellation tournée a été proposée, et nous avons montré que la diversité d'une modulation et sa capacité n'étaient pas directement reliées. Le seul critère de diversité se révèle ainsi mauvais pour déterminer une "bonne" rotation en terme de capacité.

Conclusions et perspectives

Conclusions

L'augmentation de la quantité d'information utile pouvant être transmise sur un système radio-mobile est l'un des enjeux essentiels dans les systèmes de communication actuels ou en cours de développement. Nous avons présenté dans ce document deux méthodes permettant d'augmenter l'efficacité spectrale d'une transmission sur le canal à évanouissements de Rayleigh autrement que par simple augmentation du rapport signal-à-bruit.

La première méthode, présentée au chapitre 2, correspond à l'utilisation de réseaux de points tournés. Reprenant certaines rotations existantes et en introduisant d'autres, nous avons ainsi construit des MAQ multidimensonnelles à haute efficacité spectrale qui sont protégées sur le canal à évanouissements par la diversité induite par la rotation. Nous avons proposé deux méthodes originales de décodage de ces constellations, la première correspondant à l'utilisation d'un égaliseur à retour de décision. Reposant sur le critère MMSE, cet égaliseur permet le décodage des rotations en grande dimension, en particulier de nos transformées de rotation rapide. Cet égaliseur, dont nous avons également proposé une version pour le décodage des réseaux denses sur le canal AWGN au chapitre 1, est relativement robuste mais l' efficacité spectrale de ce système n'est pas aussi grande que prévue puisqu'en pratique nous avons dû lui adjoindre une modulation codée en treillis décodée par un algorithme de Viterbi afin d'améliorer considérablement les entrées du filtre de retour. Le second système proposé combine une rotation en petite dimension avec un code correcteur d'erreur et est décodé de manière itérative. Ce dernier décodeur présente des performances extrêmement satisfaisantes, puisque l'on obtient, à la $4^{ème}$ itération, pour une rotation en dimension 8 et un code de rendement 1/2 ou 2/3, des performances à moins d'1 dB des performances sur le canal AWGN pour un taux d'erreur par bit de $5 \cdot 10^{-3}$.
Nous avons de plus montré au chapitre 4 que le fait de tourner une constellation MAQ avait pour conséquence une "gaussianisation" du signal, qui augmente ainsi sa capacité. Nous avons proposé une méthode de calcul de la capacité sur le canal de Rayleigh ayant en entrée une constellation tournée, montrant que la diversité d'une modulation et sa capacité n'étaient pas directement reliées.

La seconde méthode, présentée au chapitre 3, correspond à l'utilisation d'antennes multiples. Nous avons proposé un schéma de détection et décodage itératif pour des systèmes à antennes multiples en émission et en réception. Reposant sur le calcul des probabilités *a posteriori*, cet algorithme peut être utilisé avec tout code correcteur d'erreurs lorsque le décodage à maximum de vraisemblance n'est pas applicable. Un des intérêts de ce système est la possibilité d'y intégrer une estimation itérative des paramètres du canal à l'aide de l'algorithme EM, l'initialisation étant faite grâce à des symboles pilotes. Appliquée à un turbo code parallèle et à un code convolutif, la procédure itérative a montré des résultats performants à la fois sur le canal de Rayleigh à évanouissements indépendants et sur le canal de Rayleigh par blocs.

Perspectives

Nous envisageons de réaliser une version souple de l'algorithme de décodage par sphères : une valeur de fiabilité accompagnant le point du réseau décodé permettrait ainsi d'améliorer l'estimation en rendant possible son intégration dans un système à décodage itératif.

Il serait également intéressant de diminuer la complexité des algorithmes de décodage APP proposés tant pour les MAQ tournées que pour les systèmes à antennes multiples. Un calcul sous-optimal de l'APP pourrait être utilisé, par exemple en considérant le vecteur de signaux de probabilité *a priori* la plus grande et en inversant les bits un à un pour en tirer les vraisemblances. Enfin, il serait intéressant d'envisager des techniques d'allocation de puissance non uniformes (par exemple le "water filling") pour notre système à antennes multiples afin de gagner en capacité.

Annexe A

Bornes sur la probabilité d'erreur pour les réseaux de points sur canal AWGN ou de Rayleigh*

A.1 Performances sur le canal AWGN

Considérons un point $\mathbf{x} = (x_1, \ldots, x_n)^t$ d'un réseau Λ émis sur un canal AWGN. Le point reçu $\mathbf{y} = (y_1, \ldots, y_n)^t$ est donné par

$$\mathbf{y} = \mathbf{x} + \mathbf{b}$$

où $\mathbf{b} = (b_1, \ldots, b_n)^t$ est le bruit gaussien sur le canal, ses composantes b_i étant des variables gaussiennes de moyenne nulle et de variance $\sigma^2 = N_0$.

En pratique, le réseau Λ étant d'énergie infinie, on n'émettra pas un point de Λ mais un point d'une constellation $\mathcal{C}$ finie (donc d'énergie finie) tirée du réseau. De manière générale, on considérera que $\mathcal{C}$, de forme quelconque, est centrée autour de l'origine afin qu'elle soit à énergie minimale. $\mathcal{C}$ contient n points, notés $\mathbf{c}_k$, $k = 1, \ldots, n$. On note m le nombre de bits nécessaires pour étiqueter les n points de $\mathcal{C}$: en choisissant n comme puissance de 2, on a alors $n = 2^m$.

Le décodeur ML en sortie du canal cherche le point de $\mathcal{C}$ le plus proche du point reçu $\mathbf{y}$. Supposons que c'est le point $\mathbf{c}_k$ qui a été effectivement émis : la décision prise au niveau du récepteur est donc correcte tant que $\mathbf{y}$ appartient à la cellule de Voronoï $\mathcal{V}(\mathbf{c}_k)$. La probabilité d'erreur, sachant $\mathbf{c}_k$ émis et que tous les points de la constellation sont

*Cette annexe est extraite d'un cours que j'ai donné à l'ENST.

équiprobables, est donc

$$P_e = 1 - \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{V(\mathbf{c}_k)} e^{-||\mathbf{x}-\mathbf{c}_k||^2/2\sigma^2} d\mathbf{x} \ . \tag{A.1}$$

Sachant que l'intégrale sur $\mathcal{V}(\mathbf{c}_k)$ est égale à l'intégrale sur $\mathcal{V}(\mathbf{0})$ on obtient

$$P_e = 1 - \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{V(\mathbf{0})} e^{-||\mathbf{x}||^2/2\sigma^2} d\mathbf{x} \ . \tag{A.2}$$

Cette dernière intégrale étant difficilement calculable sauf dans des cas particuliers, on applique alors la borne de l'union aux $\tau(\Lambda)$ plus proches voisins $\mathbf{u}_j$, $j = 1, \ldots, \tau(\Lambda)$ de $\mathbf{0}$, comme illustré en figure A.1.

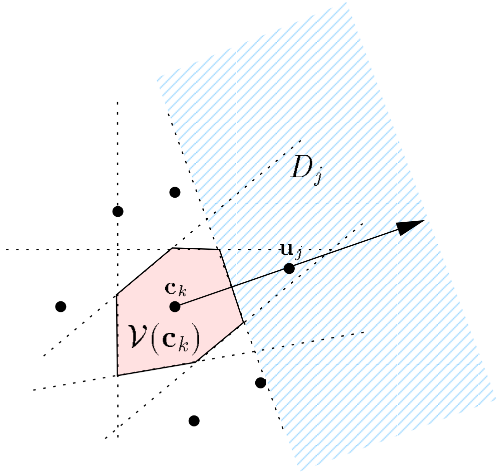


FIG. A.1: Illustration de la signification de la borne de l'union restreinte aux plus proches voisins.

La probabilité d'erreur est donc majorée par la somme des probabilités d'erreur par paire, soit des probabilités d'erreur que l'on obtient en ne considérant que les paires successives $(\mathbf{0}, \mathbf{u}_j)$, $j = 1, \ldots, \tau(\Lambda)$, soit

$$P_e \leq \sum_{j=1}^{\tau(\Lambda)} \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{D_j} e^{-||\mathbf{x}||^2/2\sigma^2} d\mathbf{x} \leq \sum_{j=1}^{\tau(\Lambda)} \frac{1}{(\sigma\sqrt{2\pi})^n} \int_{D_j} e^{-||x_1+\cdots+x_n||^2/2\sigma^2} dx_1 \cdots dx_n \tag{A.3}$$

où D_j est le demi-espace où la décision se fait en faveur de $\mathbf{u}_j$, comme illustré en figure A.1.

On peut supposer (sans perte de généralité) que l'axe $(\mathbf{0}x_1)$ n'est autre que $(\mathbf{0}\mathbf{u}_j)$, et donc que l'on a : $D_j = \{\mathbf{x} \ / \ x_1 \geq \rho_j \ , \ \forall x_2, \ldots, x_n\}$, où ρ_j est la demi-distance entre les points $\mathbf{0}$ et $\mathbf{u}_j$. On obtient alors

$$P_e \leq \sum_{j=1}^{\tau(\Lambda)} \frac{1}{(\sigma\sqrt{2\pi})} \int_{x_1 \geq \rho_j} e^{-||x_1||^2/2\sigma^2} dx_1 \times \left(\frac{1}{(\sigma\sqrt{2\pi})} \int_{-\infty}^{\infty} e^{-||x_i||^2/2\sigma^2} dx_i \right)^{n-1} \tag{A.4}$$

$$\leq \sum_{j=1}^{\tau(\Lambda)} \frac{1}{(\sigma\sqrt{2\pi})} \int_{x_1 \geq \rho_j} e^{-\|x_1\|^2/2\sigma^2} dx_1 \ . \tag{A.5}$$

Majorant chacun des ρ_j par le rayon d'empilement ρ du réseau, et après un changement de variable, on obtient alors

$$\boxed{P_e \leq \frac{\tau(\Lambda)}{\sqrt{\pi}} \int_{\frac{\rho}{\sigma\sqrt{2}}}^{+\infty} e^{-t^2} dt = \tau(\Lambda) Q\left(\frac{\rho}{\sigma}\right) \qquad (A.6)}$$

où Q est la fonction erreur gaussienne définie par $Q(x) = (2\pi)^{-1} \int_x^\infty \exp(-t^2/2)dt$.

Il nous reste à présent à évaluer $\frac{\rho}{\sigma}$, ce que nous allons faire pour le cas le plus classique, soit celui d'une constellation cubique. Une telle constellation a la forme d'un hypercube $[-A; +A]^n$, et en valeur absolue les composantes des points de $\mathcal{C}$ sont donc toutes majorées par A.

Commençons par évaluer A à l'aide des paramètres de la constellation : sachant qu'un volume fondamental contient un seul point de $\mathcal{C}$, le nombre de points n peut être approché par la formule

$$n = 2^m = Card(\mathcal{C}) \approx \frac{\text{volume de la constellation}}{\text{volume fondamental}} = \frac{vol(\mathcal{C})}{det(\Lambda)} \ . \tag{A.7}$$

Or, le volume d'un cube en dimension n de côté $2A$ est trivialement égal à $(2A)^n$, donc on a

$$A^2 = \frac{1}{4} \sqrt[n/2]{2^m det(\Lambda)} \ . \tag{A.8}$$

Calculons ensuite l'énergie par point du réseau E_p afin d'en déduire ensuite E_b : l'énergie moyenne par point, est l'espérance mathématique de la norme au carré $\|\mathbf{c}_k\|^2$ des points de la constellation. $\mathcal{C}$ étant issue d'un réseau Λ quelconque dont on ne connaît pas l'expression exacte de l'énergie, on va devoir réaliser une approximation en la prenant égale à l'énergie moyenne pour tous les points $\mathbf{x}$ de $\mathbb{R}^n$ appartenant au cube $[-A; +A]^n$

$$E_p \approx \frac{\int_{\mathbf{x} \in [-A;+A]^n} \|\mathbf{x}\|^2 d\mathbf{x}}{\int_{[-A;+A]^n} d\mathbf{x}} = \frac{1}{(2A)^n} \int_{\mathbf{x} \in [-A;+A]^n} (x_1^2 + \cdots + x_n^2) dx_1 \cdots dx_n \ . \tag{A.9}$$

Cette intégrale est séparable (car constituée de n intégrales en dimension 1) donc on obtient très facilement

$$E_p = n \frac{A^2}{3} \ . \tag{A.10}$$

On peut alors en déduire l'énergie moyenne par bit E_b

$$E_b = \frac{E_p}{\log_2(n)} = \frac{nA^2}{3m} = \frac{n}{12m} \sqrt[n/2]{2^m det(\Lambda)} \ . \tag{A.11}$$

D'où l'expression de $\sigma^2 = N_0$

$$N_0 = \frac{E_b}{\frac{E_b}{N_0}} = \frac{n}{12m} \sqrt[n/2]{2^m det(\Lambda)} \frac{1}{\frac{E_b}{N_0}} \ . \tag{A.12}$$

Il ne nous reste alors plus qu'à remplacer cette expression dans l'équation (A.6) et, en utilisant la relation (1.4) donnée au chapitre 1 entre d_{Emin} et ρ, on obtient une borne sur la probabilité d'erreur pour une constellation cubique de taille n extraite d'un réseau de points quelconque sur le canal à bruit additif blanc gaussien

$$\boxed{P_e \leq \tau(\Lambda) Q\left(\sqrt{\frac{d_{Emin}^2}{\sqrt[n/2]{det(\Lambda)}} \frac{E_b}{N_0} \frac{3\eta}{2^\eta}}\right) \qquad \text{(A.13)}}$$

où $\eta = \frac{2m}{n}$ est le nombre de bits par deux dimensions (ou efficacité spectrale par deux dimensions).

A.2 Performances sur le canal de Rayleigh

Dans le cas du canal de Rayleigh, pour un point $\mathbf{x} = (x_1, \ldots, x_n)^t$ d'un réseau Λ soit émis sur le canal, le point reçu $\mathbf{y} = (y_1, \ldots, y_n)^t$ est donné par

$$\mathbf{y} = \boldsymbol{\alpha} \odot \mathbf{x} + \mathbf{b}$$

où $\mathbf{b} = (b_1, \ldots, b_n)^t$ est le bruit additif blanc gaussien sur le canal dont les composantes b_i sont des variables gaussiennes de moyenne nulle et de variance $\sigma^2 = N_0$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)^t$ est le vecteur des évanouissements sur le canal, avec $E[\alpha_i] = 1$ (ce qui revient à dire que l'on suppose le gain de puissance sur le canal normalisé) et où $\odot$ représente le produit composante par composante.

Le décodeur ML en sortie du canal cherche le point de $\mathcal{C}$ le plus proche du point reçu $\mathbf{y}$. Comme pour le calcul effectué au paragraphe A.1, le calcul direct de la probabilité d'erreur ne peut s'effectuer dans le cas général et il est nécessaire de recourir à la probabilité d'erreur par paire. La probabilité conditionnelle, pour un évanouissement $\boldsymbol{\alpha}$ connu, que l'on décode $\mathbf{d} = (d_1, \ldots, d_n)^t$ alors que c'est le point $\mathbf{c} = (c_1, \ldots, c_n)^t$ qui a été effectivement émis, dans le cas où l'on ne considère que ces deux points, est donnée par

$$\begin{aligned} P(\mathbf{c} \to \mathbf{d}|\boldsymbol{\alpha}) &= P\left(\sum_{i=1}^{n} |y_i - \alpha_i d_i|^2 \le \sum_{i=1}^{n} |y_i - \alpha_i c_i|^2 \mid \boldsymbol{\alpha}\right) \\ &= P\left(\sum_{i=1}^{n} |\alpha_i(c_i - d_i) + b_i|^2 \le \sum_{i=1}^{n} |b_i|^2 \mid \boldsymbol{\alpha}\right) \\ &= P\left(\sum_{i=1}^{n} \alpha_i^2(c_i - d_i)^2 + 2\sum_{i=1}^{n} \alpha_i(c_i - d_i)b_i \le 0 \mid \boldsymbol{\alpha}\right) . \end{aligned} \tag{A.14}$$

On obtient donc dans l'expression précédente, d'une part une combinaison linéaire de variables aléatoires gaussiennes indépendantes identiquement distribuées (les b_i) soit $\vartheta = \sum_{i=1}^{n} \alpha_i(c_i - d_i)b_i$, dont il est aisé de montrer qu'elle est gaussienne de moyenne nulle et de variance $\sigma_\vartheta^2 = N_0 \sum_{i=1}^{n} \alpha_i^2(c_i - d_i)^2$ et une constante $A = \frac{1}{2}\sum_{i=1}^{n} \alpha_i^2(c_i - d_i)^2$. La probabilité d'erreur par paire conditionnelle s'exprime alors aisément en fonction de A et ϑ :

$$P(\mathbf{c} \to \mathbf{d}|\boldsymbol{\alpha}) = P(\vartheta \ge A) = Q(A/\sigma_\vartheta) . \tag{A.15}$$

La fonction Q peut être majorée [8] par $Q(x) \le \frac{1}{2}\exp(-x^2/2)$. (la borne étant très fine dès $x \ge 3$). La probabilité d'erreur par paire conditionnelle devient alors

$$P(\mathbf{c} \to \mathbf{d}|\boldsymbol{\alpha}) = \frac{1}{2}\exp(-\frac{A^2}{2\sigma_\vartheta^2}) = \frac{1}{2}\exp\left(-\frac{1}{8N_0}\sum_{i=1}^{n} \alpha_i^2(c_i - d_i)^2\right) . \tag{A.16}$$

La probabilité d'erreur par paire $P(\mathbf{c} \to \mathbf{d})$ est alors calculée en moyennant la probabilité d'erreur par paire conditionnelle sur les évanouissements possibles $\boldsymbol{\alpha}$

$$P(\mathbf{c} \to \mathbf{d}) = \int_{\boldsymbol{\alpha}} P(\mathbf{c} \to \mathbf{d}|\boldsymbol{\alpha})p(\boldsymbol{\alpha})d\boldsymbol{\alpha} \le \frac{1}{2}\int_{\boldsymbol{\alpha}} \exp\left(-\frac{1}{8N_0}\sum_{i=1}^{n} \alpha_i^2(c_i - d_i)^2\right) p(\boldsymbol{\alpha})d\boldsymbol{\alpha} \tag{A.17}$$

avec $\mathbf{p}(\boldsymbol{\alpha})d\boldsymbol{\alpha} = p(\alpha_1)\cdots p(\alpha_n)d\alpha_1\cdots d\alpha_n$, où chacune des probabilités conditionnelles $p(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$ suit une loi de Rayleigh normalisée. L'inéquation (A.17) s'écrit donc encore

$$P(\mathbf{c} \to \mathbf{d}) \le \frac{1}{2}\prod_{i=1}^{n}\int_0^{+\infty} \exp\left(-\frac{1}{8N_0}\alpha_i^2(c_i - d_i)^2\right) p(\alpha_i)d\alpha_i . \tag{A.18}$$

Le calcul de ces n intégrales nous donne alors

$$\boxed{P(\mathbf{c} \to \mathbf{d}) \leq \frac{1}{2} \prod_{i=1}^{n} \frac{1}{1 + (c_i - d_i)^2/(8N_0)} \quad \text{(A.19)}}$$

Cette borne supérieure est suffisamment précise pour être un critère efficace d'évaluation et d'optimisation des réseaux de points sur les canaux à évanouissements. On notera qu'elle diffère de la borne de Chernoff classique d'un facteur $\frac{1}{2}$ et qu'au besoin elle peut encore être affinée en utilisant un calcul sur les formes quadratiques gaussiennes [63]

Annexe B

Récapitulatif des matrices des différents réseaux et rotations considérés

Cette annexe a pour but de présenter les différentes matrices des réseaux ou des rotations utilisées au cours de ce document. Le mode de construction de ces différentes matrices est décrit au chapitre 2, et leur provenance est rappelée lorsqu'il s'agit de matrices tirées de la littérature. Pour des raisons pratiques, seules les matrices obtenues pour une dimension inférieure ou égale à 8 seront données.

B.1 Rotations en dimension 4

En dimension 4, trois matrices sont considérées : Rot_4 déterminée par optimisation numérique des performances sur canal de Rayleigh selon la méthode proposée par Da Silva & Souza [29], et la matrice de réseau $Z_{4,4}$ obtenue par maximisation de la distance produit-ℓ en dimension 4 par Boutros [16] et la matrice de réseau $\mathbb{Z}_{4,2,a}$ construite par plongement canonique dans le corps de nombres totalement complexe $\mathbb{Q}[j](e^{2\pi j/8})$.

0.05109452693	0.5185898735	0.6926254321	-0.4987222706
0.2225445479	0.8126200269	-0.3053586993	0.4437101316
0.1954529800	-0.1987550562	0.6460444949	0.7105779837
0.9537617135	-0.1766625671	-0.09824757644	-0.2224327875

TAB. B.1: Rot_4: rotation obtenue par optimisation numérique des performances sur canal de Rayleigh d'après [29].

0.4857122144	0.7858988717	-0.2011885857	-0.3255299698
-0.7858988717	0.4857122144	0.3255299698	-0.2011885857
0.2011885857	0.3255299698	0.4857122144	0.7858988717
-0.3255299698	0.2011885857	-0.7858988717	0.4857122144

TAB. B.2: $\mathbb{Z}_{4,4}$: rotation obtenue par maximisation de la distance produit-ℓ en dimension 4 d'après [16].

0.7071067812	0.0000000000	0.5000000000	0.5000000000
-0.0000000000	0.7071067812	-0.5000000000	0.5000000000
0.7071067812	0.0000000000	-0.5000000000	-0.5000000000
-0.0000000000	0.7071067812	0.5000000000	-0.5000000000

Tab. B.3: $\mathbb{Z}_{4,2,a}$: rotation obtenue par plongement canonique dans le corps de nombres totalement complexe $\mathbb{Q}[j](e^{2\pi j/8})$.

B.2 Rotations en dimension 5

En dimension 5, deux matrices sont considérées : Rot_5 déterminée par optimisation numérique des performances sur canal de Rayleigh selon la méthode proposée par Da Silva & Souza [29], et la matrice de réseau $Z_{5,5}$ dont la construction par plongement canonique dans le corps de nombres totalement réel $\mathbb{Q}(2\cos(2\pi/11))$ est proposé en exemple au paragraphe 2.3.2.

-0.1243255837	-0.1357793743	-0.3821809682	0.5316882905	-0.7330432320
-0.4653152877	-0.1042951070	-0.7657539734	-0.3619991144	0.2349078694
0.1401753897	-0.0469514476	0.0932664896	-0.7656563843	-0.6190461088
0.5705012126	-0.7828658096	-0.1951890540	0.0046570973	0.1533917705
-0.6503107402	-0.5963247253	0.4698522692	-0.0035798846	-0.0268103117

Tab. B.4: Rot_5: rotation obtenue par optimisation numérique des performances sur canal de Rayleigh d'après [29].

-0.4557341407	-0.5485287320	-0.5968847877	-0.3260186796	0.1698911240
-0.5968847877	0.4557341407	-0.1698911240	0.5485287320	0.3260186796
-0.3260186796	0.1698911240	0.5485287320	-0.5968847877	0.4557341407
-0.1698911240	0.5968847877	-0.3260186796	-0.4557341407	-0.5485287320
0.5485287320	0.3260186796	-0.4557341407	-0.1698911240	0.5968847877

Tab. B.5: $\mathbb{Z}_{5,5}$: rotation obtenue obtenue par plongement canonique dans le corps de nombres totalement réel $\mathbb{Q}(2\cos(2\pi/11))$.

B.3 Rotations en dimension 8

Huit matrices sont considérées en dimension 8 : $Tchebi_8$ construite à partir de la famille des polynômes de Tchebicheff du premier ordre $T_k(x)$, $OP_{2,8}$ déterminée par optimisation numérique en fonction du taux de coupure par Rainish [59], $Z_{8,4,a}$ et $Z_{8,4,b}$ construites par plongement canonique dans le corps de nombres totalement complexe $\mathbb{Q}[j](e^{2\pi j/16})$, $\mathbb{Z}_{8,4,random}$ obtenue par tirage aléatoire en dimension 8, $Z_{8,8}$ obtenue par maximisation de la distance produit-ℓ en dimension 8 par Boutros [16], $Hada_8$, matrice de Hadamard normalisée en dimension 8 et $Random_8$ choisie selon le critère d'optimisation de la capacité, comme expliqué au paragraphe 2.3.5.

0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906
0.4903926402	0.4157348062	0.2777851165	0.09754516101	-0.0975451610	-0.2777851165	-0.4157348062	-0.4903926402
0.4619397663	0.1913417162	-0.1913417162	-0.4619397663	-0.4619397663	-0.1913417162	0.1913417162	0.4619397663
0.4157348062	-0.0975451610	-0.4903926402	-0.2777851165	0.2777851165	0.4903926402	0.0975451610	-0.4157348062
0.3535533906	-0.3535533906	-0.3535533906	0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	0.3535533906
0.2777851165	-0.4903926402	0.0975451610	0.4157348062	-0.4157348062	-0.0975451610	0.4903926402	-0.2777851165
0.1913417162	-0.4619397663	0.4619397663	-0.1913417162	-0.1913417162	0.4619397663	-0.4619397663	0.1913417162
0.0975451610	-0.2777851165	0.4157348062	-0.4903926402	0.4903926402	-0.4157348062	0.2777851165	-0.0975451610

TAB. B.6: $Tchebi_8$: rotation construite à partir des polynômes de Tchebicheff.

0.368	0.108	-0.439	-0.394	-0.339	-0.368	-0.395	-0.314
-0.394	0.283	0.363	0.106	-0.413	-0.373	0.285	-0.481
0.129	-0.427	0.362	0.322	0.366	-0.333	-0.456	-0.338
-0.309	0.325	-0.364	0.341	0.140	0.467	-0.342	-0.441
0.453	0.397	0.428	-0.364	0.321	0.304	0.123	-0.333
0.412	-0.457	-0.145	0.292	-0.332	0.317	0.411	-0.368
0.327	0.395	-0.312	0.466	0.344	-0.428	0.341	0.071
0.339	0.315	0.331	0.422	-0.479	0.142	-0.371	0.332

TAB. B.7: $OP_{2,8}$: rotation obtenue par optimisation numérique du taux de coupure [59].

0.5000000000	0.0000000000	0.4619397663	0.1913417162	0.3535533906	0.3535533906	0.1913417162	0.4619397663
-0.0000000000	0.5000000000	-0.1913417162	0.4619397663	-0.3535533906	0.3535533906	-0.4619397663	0.1913417162
0.5000000000	0.0000000000	-0.1913417162	0.4619397663	-0.3535533906	-0.3535533906	0.4619397663	-0.1913417162
-0.0000000000	0.5000000000	-0.4619397663	-0.1913417162	0.3535533906	-0.3535533906	0.1913417162	0.4619397663
0.5000000000	0.0000000000	-0.4619397663	-0.1913417162	0.3535533906	0.3535533906	-0.1913417162	-0.4619397663
-0.0000000000	0.5000000000	0.1913417162	-0.4619397663	-0.3535533906	0.3535533906	0.4619397663	-0.1913417162
0.5000000000	0.0000000000	0.1913417162	-0.4619397663	-0.3535533906	-0.3535533906	-0.4619397663	0.1913417162
-0.0000000000	0.5000000000	0.4619397663	0.1913417162	0.3535533906	-0.3535533906	-0.1913417162	-0.4619397663

TAB. B.8: $\mathbb{Z}_{8,4,a}$: rotation obtenue par plongement canonique dans le corps de nombres totalement complexe $\mathbb{Q}[j](e^{2\pi j/16})$.

0.5000000000	0.0000000000	0.4829629131	0.1294095226	0.4330127019	0.2500000000	0.3535533906	0.3535533906
-0.0000000000	0.5000000000	-0.1294095226	0.4829629131	-0.2500000000	0.4330127019	-0.3535533906	0.3535533906
0.5000000000	0.0000000000	-0.1294095226	0.4829629131	-0.4330127019	-0.2500000000	0.3535533906	-0.3535533906
-0.0000000000	0.5000000000	-0.4829629131	-0.1294095226	0.2500000000	-0.4330127019	0.3535533906	0.3535533906
0.5000000000	0.0000000000	-0.4829629131	-0.1294095226	0.4330127019	0.2500000000	-0.3535533906	-0.3535533906
-0.0000000000	0.5000000000	0.1294095226	-0.4829629131	-0.2500000000	0.4330127019	0.3535533906	-0.3535533906
0.5000000000	0.0000000000	0.1294095226	-0.4829629131	-0.4330127019	-0.2500000000	-0.3535533906	0.3535533906
-0.0000000000	0.5000000000	0.4829629131	0.1294095226	0.2500000000	-0.4330127019	-0.3535533906	-0.3535533906

TAB. B.9: $\mathbb{Z}_{8,4,b}$: rotation obtenue par plongement canonique dans le corps de nombres totalement complexe $\mathbb{Q}[j](e^{2\pi j/16})$.

-0.3535533906	0.3535533906	-0.3535533906	-0.5000000000	-0.5330017909	0.2198997486	-0.0826976770	0.1889822365
-0.3535533906	-0.3535533906	0.3535533906	0.0000000000	-0.3198010745	-0.1099498743	-0.6064496311	-0.3779644730
0.3535533906	-0.3535533906	-0.3535533906	0.0000000000	-0.3198010745	0.3738295726	0.2480930309	-0.5669467095
0.3535533906	-0.3535533906	-0.3535533906	0.0000000000	-0.3198010745	-0.5937293211	-0.1653953539	0.3779644730
0.3535533906	-0.3535533906	0.3535533906	-0.5000000000	0.1066003582	0.4397994971	-0.1653953539	0.3779644730
0.3535533906	0.3535533906	0.3535533906	-0.5000000000	-0.1066003582	-0.4397994971	0.1653953539	-0.3779644730
-0.3535533906	-0.3535533906	-0.3535533906	-0.5000000000	0.5330017909	-0.2198997486	0.0826976770	-0.1889822365
-0.3535533906	-0.3535533906	0.3535533906	0.0000000000	-0.3198010745	-0.1099498743	0.6891473080	0.1889822365

Tab. B.10: $\mathbb{Z}_{8,4,random}$: rotation obtenue par tirage aléatoire en dimension 8.

0.05830052	-0.09433222	0.14074991	-0.22773814	0.19255622	-0.31156250	0.46487183	-0.75217842
0.09433222	0.05830052	0.22773814	0.14074991	0.31156250	0.19255622	0.75217842	0.46487183
-0.14074991	0.22773814	0.05830052	-0.09433222	-0.46487183	0.75217842	0.19255622	-0.31156250
-0.22773814	-0.14074991	0.09433222	0.05830052	-0.75217842	-0.46487183	0.31156250	0.19255622
-0.19255622	0.31156250	-0.46487183	0.75217842	0.05830052	-0.09433222	0.14074991	-0.22773814
-0.31156250	-0.19255622	-0.75217842	-0.46487183	0.09433222	0.05830052	0.22773814	0.14074991
0.46487183	-0.75217842	-0.19255622	0.31156250	-0.14074991	0.22773814	0.05830052	-0.09433222
0.75217842	0.46487183	-0.31156250	-0.19255622	-0.22773814	-0.14074991	0.09433222	0.05830052

Tab. B.11: $\mathbb{Z}_{8,8}$: rotation obtenue par maximisation de la distance produit-ℓ en dimension 8 d'après [16].

0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.3535533906
0.3535533906	-0.3535533906	0.3535533906	-0.3535533906	0.3535533906	-0.3535533906	0.3535533906	-0.3535533906
0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	0.3535533906	0.3535533906	-0.3535533906	-0.3535533906
0.3535533906	-0.3535533906	-0.3535533906	0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	0.3535533906
0.3535533906	0.3535533906	0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	-0.3535533906	-0.3535533906
0.3535533906	-0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	0.3535533906	-0.3535533906	0.3535533906
0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	-0.3535533906	-0.3535533906	0.3535533906	0.3535533906
0.3535533906	-0.3535533906	-0.3535533906	0.3535533906	-0.3535533906	0.3535533906	0.3535533906	-0.3535533906

Tab. B.12: $Hada_8$: matrice de Hadamard normalisée.

0.3535533906	-0.3535533906	0.3535533906	-0.3535533906	0.3668284415	0.1519453155	-0.5715664223	-0.1251452778
0.3535533906	0.3535533906	0.3535533906	0.3535533906	-0.1519453155	0.3668284415	0.1251452778	-0.5715664223
0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	0.3668284415	-0.4558359466	0.1905221408	-0.3483558500
-0.3535533906	0.3535533906	0.3535533906	-0.3535533906	0.4558359466	0.3668284415	0.3483558501	0.1905221408
0.3535533906	0.3535533906	0.3535533906	-0.3535533906	-0.5187737570	-0.2148831260	-0.0462284231	0.4272727047
-0.3535533906	0.3535533906	0.3535533906	0.3535533906	0.2148831259	-0.5187737570	-0.4272727047	-0.0462284231
0.3535533906	0.3535533906	-0.3535533906	0.3535533906	0.3038906310	0.3038906310	-0.2694389954	0.4926495676
-0.3535533906	0.3535533906	-0.3535533906	-0.3535533906	-0.3038906310	0.3038906310	-0.4926495676	-0.2694389954

Tab. B.13: $Random_8$: rotation obtenue par tirage aléatoire puis optimisation numérique de la capacité.

Annexe C

Bornes sur la probabilité d'erreur pour différents canaux

C.1 Probabilité d'erreur d'une MAQ sur un canal AWGN

La probabilité d'erreur par symbole pour une modulation MAQ sur un canal à bruit additif blanc gaussien peut être déterminée en calculant tout d'abord la probabilité d'erreur par symbole d'une modulation PAM [58], pp.278–282. Un exemple d'une telle modulation de taille M est présenté en figure C.1, où $d_{E_{min}} = 2A$ est la distance euclidienne minimale (constante) entre deux points de la constellation.

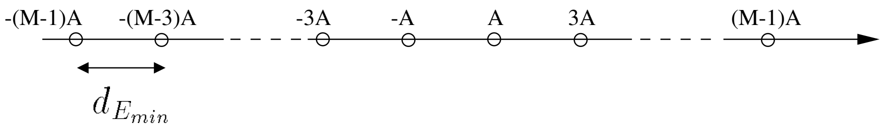


FIG. C.1: Constellation PAM de taille M.

L'énergie moyenne en bande de base de la constellation PAM de taille $M = 2^m$ (ou PAM-M) est donc donnée par

$$\mathcal{E}_{moy} = \frac{1}{M}\sum_{m=1}^{M}\mathcal{E}_m = \frac{1}{M}\sum_{m=1}^{M}(2m - M - 1))^2 A^2 = \frac{1}{M}\left(\frac{1}{3}M(M^2-1)\right)\frac{d^2_{E_{min}}}{4} = \frac{M^2-1}{12}d^2_{E_{min}}$$

où $\mathcal{E}_m$ est l'énergie du $m^{ème}$ point de la constellation, d'abscisse $(2m - M - 1)A$. On peut donc en déduire aisément l'expression de l'énergie moyenne par bit sur fréquence porteuse E_b

$$E_b = \frac{1}{2}\frac{\mathcal{E}_{moy}}{m} = \frac{M^2-1}{24m}d^2_{E_{min}}$$

La probabilité d'erreur par symbole $P_{e_{PAM-M}}$ d'une PAM sur le canal AWGN est la moyenne des probabilités d'erreur, sachant le symbole émis, soit pour un bruit blanc gaussien de variance par composante $N_0 = \sigma^2$

$$P_{e_{PAM-M}} \approx \underbrace{\frac{2}{M} \times Q\left(\frac{d_{E_{min}}}{2\sigma}\right)}_{\text{les extrémités de la PAM}} + \underbrace{\frac{M-2}{M} \times 2\, Q\left(\frac{d_{E_{min}}}{2\sigma}\right)}_{\text{les (M-2) autres points}} = \left(2 - \frac{2}{M}\right) Q\left(\frac{d_{E_{min}}}{2\sigma}\right)$$

où Q est la fonction d'erreur.

On obtient donc la formule classique de la probabilité d'erreur par symbole d'une constellation PAM sur un canal AWGN

$$P_{e_{PAM-M}} \approx \left(2 - \frac{2}{M}\right) Q\left(\sqrt{\frac{2E_b}{N_0}\frac{3\log_2 M}{M^2-1}}\right) \tag{C.1}$$

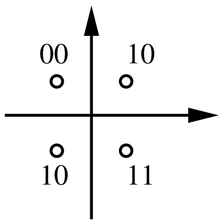


FIG. C.2: Constellation MAQ-4 avec étiquetage de Gray.

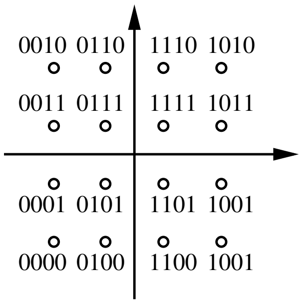


FIG. C.3: Constellation MAQ-16 avec étiquetage de Gray.

Les constellations MAQ rectangulaires de taille M (ou MAQ-M), dont des exemples sont présentés en figures C.2, C.3 et C.4 peuvent être vues comme deux PAM de taille $\sqrt{M}$ en quadrature. Comme les signaux en phase et quadrature peuvent être parfaitement séparés par le démodulateur, la probabilité d'erreur par symbole d'une constellation MAQ s'obtient aisément à partir de celle d'une PAM donnée par l'équation (C.1). Plus spécifiquement, on a :

$$P_{e_{MAQ-M}} = 1 - (1 - P_{e_{PAM-\sqrt{M}}})^2$$

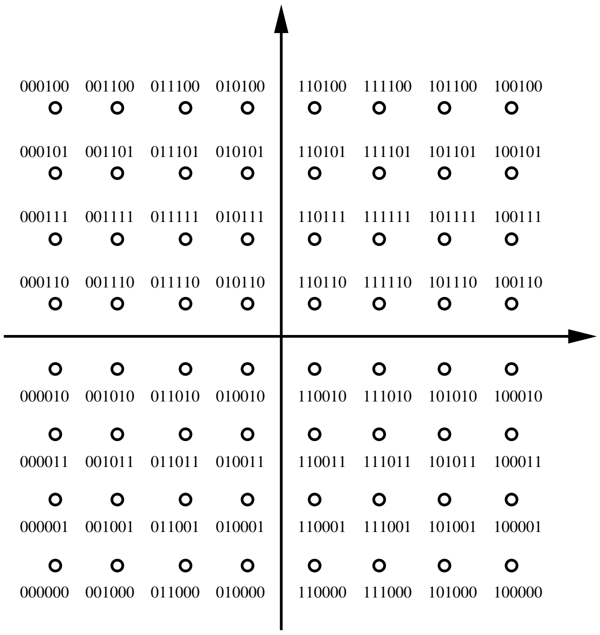


FIG. C.4: Constellation MAQ-64 avec étiquetage de Gray.

Ce calcul, exact lorsqu'une modulation PAM de taille $\sqrt{M}$ existe bel et bien, soit lorsque la constellation MAQ est de taille $M = 2^m$ avec m pair, est supposé valable pour les entiers m impairs (il suffit de se rapporter au critère ML directement), d'où la formule bien connue de la probabilité d'erreur par symbole pour une constellation MAQ sur un canal AWGN (et la borne qui s'en déduit)

$$P_{e_{MAQ-M}} \approx 1 - \left(1 - (2 - \frac{2}{\sqrt{M}})\ Q\left(\sqrt{\frac{3\log_2 M}{M-1}\frac{E_b}{N_0}}\right)\right)^2 \leq 4\ Q\left(\sqrt{\frac{3\log_2 M}{M-1}\frac{E_b}{N_0}}\right) \tag{C.2}$$

Si l'on suppose l'existence d'un étiquetage de Gray (comme présenté en exemple dans les figures C.2, C.3 et C.4), la probabilité d'erreur par bit d'une constellation MAQ sur un canal AWGN est alors bornée par

$$\boxed{P_{eb_{MAQ-M}} \leq \frac{4}{\log_2 M}\ Q\left(\sqrt{\frac{2E_b}{N_0}\frac{3\log_2 M}{2(M-1)}}\right) \quad \text{(C.3)}}$$

C.2 Probabilité d'erreur d'une MAQ sur un canal de Rayleigh

Si l'on considère à présent un canal de Rayleigh cohérent, caractérisé par :
- un coefficient α réel suivant une loi de Rayleigh normalisée et affaiblissant le symbole complexe émis
- l'ajout de bruit blanc gaussien à l'entrée du récepteur comme pour le canal AWGN un bruit additif blanc gaussien complexe de variance par composante N_0

La probabilité d'erreur conditionnelle à α fixé est donc, d'après la formule (C.2)

$$P'_{e_{MAQ-M|\alpha}} \approx 4Q\left(\sqrt{\frac{3\log_2 M}{M-1}\frac{\alpha^2 E_b}{N_0}}\right)$$

Le coefficient α suivant une loi de Rayleigh, sa loi de probabilité est donc donnée par $p(\alpha) = 2\alpha \exp -\alpha^2$, la probabilité d'erreur de la MAQ-M sur un canal de Rayleigh est obtenue en moyennant sur toutes les valeurs de l'évanouissement

$$P'_{e_{MAQ-M}} = E_\alpha\left[P'_{e_{MAQ-M|\alpha}}\right] = \int_0^{+\infty} p(\alpha) P'_{e_{MAQ-M|\alpha}} d\alpha$$

La fonction Q peut être majorée par $Q(x) \leq \frac{1}{2} e^{-x^2/2} \leq 1$, cette borne étant très fine dès que $x \geq 3$ [58], d'où

$$P'_{e_{MAQ-M}} \leq \int_0^{+\infty} p(\alpha)\left[4\frac{1}{2}\exp\left(-\frac{3\log_2 M}{2(M-1)}\frac{\alpha^2 E_b}{N_0}\right)\right] d\alpha$$

$$P'_{e_{MAQ-M}} \leq 2\int_0^{+\infty} 2\alpha \exp\left(\left(-\frac{3\log_2 M}{2(M-1)}\frac{E_b}{N_0} - 1\right)\alpha^2\right) d\alpha$$

D'où une borne de la probabilité d'erreur par symbole pour une MAQ-M sur le canal de Rayleigh

$$P'_{e_{MAQ-M}} \leq 2\left(\frac{3\log_2 M}{2(M-1)}\frac{E_b}{N_0} + 1\right)^{-1} \tag{C.4}$$

Si l'on suppose l'existence d'un étiquetage de Gray, la probabilité d'erreur par bit d'une constellation MAQ sur un canal AWGN est alors bornée par

$$\boxed{P'_{eb_{MAQ-M}} \leq \frac{2}{\log_2 M}\left(\frac{3\log_2 M}{2(M-1)} \times \frac{E_b}{N_0} + 1\right)^{-1} \quad \text{(C.5)}}$$

On notera que cette borne a perdu de sa finesse du fait des approximations successives, et montre, par rapport à la courbe que l'on peut obtenir par simulation avec décodage ML et étiquetage de Gray, une perte de 3 à 5 dB pour les MAQ-4, MAQ-16 ou MAQ-64.

C.3 Probabilité d'erreur d'une MAQ sur canal de Rayleigh MIMO

Calcul de la probabilité d'erreur par paire $P(U \to V)$

Nous considérons à présent le cas d'un système équipé de n_t antennes d'émission et de n_r antennes de réception, comme présenté au chapitre 3 en figure 3.2. Le modulateur MAQ-M émet en parallèle n_t symboles différents $x_i, i = 1, \ldots, n_t$ appartenant à la constellation sur les n_t antennes. On notera $\mathbf{x} = (x_i)^t_{i=1,\ldots,n_t}$. Le récepteur reçoit une observation $\mathbf{y} = (y_j)^t_{j=1,\ldots,n_r}$ composée de n_r échantillons complexes. Le canal MIMO est caractérisé par n_r bruits blancs gaussiens $b_j, j = 1, \ldots, n_r$ complexes indépendants de variance $2N_0$ (soit N_0 par composante) et $n_t \times n_r$ coefficients complexes $h_{ij}, i = 1, \ldots, n_t, j = 1, \ldots, n_r$ supposés parfaitement connus par le détecteur. Le coefficient h_{ij} suit une loi gaussienne complexe de moyenne nulle et de variance unitaire, et correspond au lien entre l'antenne émettrice i et l'antenne réceptrice j. On notera $H = (h_{ij})^{j=1,\ldots,n_r}_{i=1,\ldots,n_t}$. On a donc

$$\forall j \in \{1, \ldots, n_r\} \quad y_j = \sum_{i=1}^{n_t} h_{ij} x_i + b_j$$

Pour une réalisation du canal fixée H, on considère deux vecteurs $U = (U_i)^t_{i=1,\ldots,n_t}$ et $V = (V_i)^t_{i=1,\ldots,n_t}$ contenant chacun n_t symboles de la constellation MAQ-M choisie. Si de plus on pose $\mathbf{z}^U = \sum_{i=1}^{n_t} h_{ij} U_i$ et $\mathbf{z}^V = \sum_{i=1}^{n_t} h_{ij} V_i$, le détecteur cohérent ML minimise la métrique $m(\mathbf{x})$ définie par

$$m(\mathbf{x}) = \|\mathbf{y} - \mathbf{z}^{\mathbf{x}}\|^2 = \sum_{j=1}^{n_r} \|y_j - \sum_{i=1}^{n_t} h_{ij} x_i\|^2 \tag{C.6}$$

Supposons à présent que c'est U qui a été émis, soit que $x_i = U_i \, i = 1, \ldots, n_t$. La probabilité d'erreur conditionnelle par paire $P(U \to V|H)$, i.e. la probabilité que le détecteur ML choisisse le vecteur V ignorant les $M^{n_t} - 2$ autres vecteurs possibles alors que c'est le vecteur U qui a été émis pour une valeur fixée H du canal est donnée par

$$P(U \to V|H) = P(m(U) > m(V)|H) = P\left(\sum_{j=1}^{n_r} \|b_j\|^2 > \sum_{j=1}^{n_r} \| \sum_{i=1}^{n_t} h_{ij}(U_i - V_i) + b_j\|^2 |H\right)$$

$$P(U \to V|H) = P\left(\Re\left(\sum_{j=1}^{n_r} b_j^* \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\right) > \frac{1}{2} \sum_{j=1}^{n_r} \| \sum_{i=1}^{n_t} h_{ij}(U_i - V_i)\|^2 |H\right)$$

Posant $W = \Re(\sum_{j=1}^{n_r} b_j^* \sum_{i=1}^{n_t} h_{ij}(V_i - U_i))$ et $w = \frac{1}{2}\sum_{j=1}^{n_r} \| \sum_{i=1}^{n_t} h_{ij}(U_i - V_i)\|^2$, la probabilité d'erreur conditionnelle s'écrit donc comme la probabilité pour la variable aléatoire W de variance σ_W^2 d'être supérieure à la constante w. W étant clairement une variable gaussienne réelle de moyenne nulle, on a donc

$$P(U \to V|H) = P(W > w) = Q\left(\frac{w}{\sigma_W}\right)$$

Il reste donc à calculer la variance de la variable aléatoire W. H, U et V étant fixés, $\sum_{i=1}^{n_t} h_{ij}(V_i - U_i)$ est une constante, alors que les bruits b_j sont informément répartis sur l'espace des phases. Donc

$$\sigma_W^2 = E[W^2|H,U,V] = E\left[\Re\left(\sum_{j=1}^{n_r} b_j^* \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\right)^2\right] = \frac{1}{2}E_{\mathrm{b}}\left[\left(\sum_{j=1}^{n_r} b_j^* \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\right)^2\right]$$

$$\sigma_W^2 = \frac{1}{2}\sum_{j=1}^{n_r}\left(\| \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\|^2 E_{\mathrm{b}}\left[|b_j|^2\right]\right) = \frac{1}{2}(2w)(2N_0) = 2N_0 w$$

On peut donc exprimer la probabilité d'erreur conditionnelle comme

$$P(U \to V|H) = Q\left(\sqrt{\frac{\sum_{j=1}^{n_r} \| \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\|^2}{4N_0}}\right) \tag{C.7}$$

Utilisant l'approximation de la fonction Q par sa borne supérieure exponentielle classique, on obtient

$$P(U \to V|H) \leq \frac{1}{2}\exp\left(-\frac{\sum_{j=1}^{n_r} \| \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\|^2}{8N_0}\right) \tag{C.8}$$

Définissons à présent les variables aléatoires α_j suivantes

$$\alpha_j = \| \sum_{i=1}^{n_t} h_{ij}(V_i - U_i)\|^2 \quad \forall j \in \{1, \ldots, n_r\}$$

Sachant que les évanouissements h_{ij} sont des variables aléatoires gaussiennes complexes indépendantes de moyenne nulle et de variance 1 et que les symboles U_i et V_i sont fixés, il apparaît que les variables aléatoires α_j sont des modules au carré de sommes de gaussiennes complexes indépendantes. Les α_j sont donc par définition des variables aléatoires de Rayleigh indépendantes de variance $E[\alpha_j^2] = \sum_{i=1}^{n_t} \|(V_i - U_i)\|^2$. L'inégalité (C.8) nous permet d'écrire

$$P(U \to V) = E_H[P(U \to V|H)] \leq \frac{1}{2}\int_0^{+\infty} .. \int_0^{+\infty} p(\alpha_1)..p(\alpha_{n_r})\exp(-\frac{\alpha_1^2}{8N_0})..\exp(-\frac{\alpha_{n_r}^2}{8N_0})d\alpha_1..d\alpha_{n_r}$$

L'indépendance des variables α_j nous permet d'écrire

$$P(U \to V) \leq \frac{1}{2}\left[\int_0^{+\infty} p(\alpha_1)\exp(-\frac{\alpha_1^2}{8N_0})d\alpha_1\right]^{n_r} = \frac{1}{2}\left[\int_0^{+\infty} p(\alpha)\exp(-(\sum_{i=1}^{n_t}\|(V_i-U_i)\|^2)\frac{\alpha^2}{8N_0})d\alpha\right]^{n_r}$$

où α est une version normalisée de la variable aléatoire α_1 : $\alpha = \alpha_1/E[\alpha_1^2]$.
Le calcul de l'intégrale nous permet d'obtenir la relation suivante

$$\boxed{P(U \to V) \leq \frac{1}{2}\left[\frac{1}{1+\frac{\sum_{i=1}^{n_t}\|V_i-U_i\|^2}{8N_0}}\right]^{n_r} \qquad \text{(C.9)}}$$

Expression de l'énergie E_b moyenne totale reçue par bit sur fréquence porteuse

Calculons l'énergie moyenne par bit reçue sur fréquence porteuse pour une constellation MAQ de taille $M = 2^m$ sur notre système MIMO avec n_t antennes d'émission et n_r antennes d'émission. L'énergie moyenne en bande de base d'un point de la constellation est donc donnée par

$$\mathcal{E}_{moy} = \frac{2(M-1)}{3}A^2$$

Or, au niveau des antennes de réception, tout se passe comme si l'on avait placé un code à répétition de longueur n_r puisque l'on observe une amplification de la puissance reçue d'un facteur n_r (pour une puissance P émise, on reçoit n_rP en démodulation parfaitement cohérente). Par ailleurs, gardant la même distance d_{min} entre deux points de la constellation, on a transmis au total n_t fois plus d'énergie que dans le cas classique mono-antenne, cette énergie ayant également permis de transmettre n_t symboles donc l'énergie moyenne totale reçue sur fréquence porteuse est

$$E_s = \frac{\mathcal{E}_{moy}}{2}n_tn_r$$

d'où l'expression de l'énergie moyenne par bit sur fréquence porteuse

$$E_b = \frac{E_s}{mn_t} = \frac{\mathcal{E}_{moy}}{2m}n_r = \frac{M-1}{3m}A^2n_r \qquad \text{(C.10)}$$

Expression de la probabilité d'erreur par bit

La probabilité d'erreur par symbole se déduit de la probabilité d'erreur par paire en utilisant la borne de l'union [76][58]

$$P''_{e_{MAQ-M}} \leq \sum_U \left(p(U)\sum_{V,V\neq U} P(U \to V)\right)$$

D'où, en pondérant chacune de ces probabilité d'erreur par paire par le nombre de bits erronés correspondant, la probabilité d'erreur par bit correspondante

$$P''_{eb_{MAQ-M}} \leq \sum_{U} \left(p(U) \sum_{V, V \neq U} \frac{d_H(U,V)}{mn_t} P(U \to V) \right)$$

Or, à fort rapport signal à bruit, l'équation (C.9) peut être approximée par

$$P(U \to V) \leq \frac{1}{2} \left[\frac{\sum_{i=1}^{n_t} |(V_i - U_i)|^2}{8N_0} \right]^{-n_r}$$

où pour tout $i, i = 1, \ldots, n_t$, U_i et V_i, $\forall i \in \{1, \ldots, n_t\}$ sont des symboles de la constellation MAQ, soit $|(V_i - U_i)|^2 = K_i A^2$ donc où $\sum_{i=1}^{n_t} |(V_i - U_i)|^2 = KA^2$, avec $K, K_1, \ldots, K_{n_t}$ des constantes dépendant uniquement de M et de la forme de la constellation. Tenant compte de l'expression de l'énergie E_b moyenne totale reçue par bit sur fréquence porteuse donnée par l'équation (C.10) on a donc

$$\boxed{P''_{eb_{MAQ-M}} \leq \kappa(M, n_t) \left(\frac{E_b}{N_0} \right)^{-n_r} \qquad \text{(C.11)}}$$

où $\kappa(M, n_t)$ est une constante dépendant uniquement de la constellation MAQ choisie et du nombre d'antennes d'émission n_t.

On notera que si l'on souhaite déterminer une borne sur la probabilité d'erreur dans le cas où un code (n_c, k_c, d_{min_c}) est placé avant le modulateur émettant sur le canal, le calcul de la probabilité d'erreur par paire donnée par la formule (C.9) reste valable. La majoration avec la borne de l'union faisant apparaître une somme sur toutes les distances entre deux points $\mathbf{d} = \sum_{i=1}^{n_t} |(V_i - U_i)|^2$, on aura alors recours au polynôme énumérateur de poids du code considéré pour exprimer la borne et la calculer, ainsi qu'expliqué par exemple dans [76].

C.4 Probabilité d'erreur d'une MAQ sur un canal de Rayleigh par blocs MIMO

Reprenons le calcul précédent dans le cas où le canal de Rayleigh est constant sur une durée de ℓ périodes symboles. Ce type de calcul a notamment été déjà réalisé par *Tarokh et al.* [69] et nous nous en inspirons donc considérablement ici.

Le canal étant constant sur le bloc de $\ell \times n_t$ symboles, le détecteur cohérent ML va lui aussi travailler par ℓ paquets, soit considérer que l'on aura émis un vecteur de symboles $\mathbf{x} = x_1^1, x_2^1, \ldots, x_{n_t}^1, x_1^2, x_2^2, \ldots, x_{n_t}^2, \ldots, x_1^\ell, x_2^\ell, \ldots, x_{n_t}^\ell = ((x_i^u)_{i=1,\ldots,n_t}^{u=1,\ldots,\ell})^t$
et reçu $\mathbf{y} = y_1^1, y_2^1, \ldots, y_{n_r}^1, y_1^2, y_2^2, \ldots, y_{n_r}^2, \ldots, y_1^\ell, y_2^\ell, \ldots, y_{n_r}^\ell = ((y_i^u)_{i=1,\ldots,n_r}^{u=1,\ldots,\ell})^t$.

Pour une réalisation du canal fixée H, on considère les deux vecteurs $U = ((U_i^u)_{i=1,\ldots,n_t}^{u=1,\ldots,\ell})^t$ et $V = ((V_i^u)_{i=1,\ldots,n_t}^{u=1,\ldots,\ell})^t$ contenant chacun $\ell \times n_t$ symboles de la constellation MAQ-M choisie. Le détecteur cohérent ML minimise alors la métrique $m_2(\mathbf{x})$ définie par

$$m_2(\mathbf{x}) = \sum_{j=1}^{n_r} \sum_{u=1}^{\ell} |y_j^u - \sum_{i=1}^{n_t} h_{ij} x_i^u|^2 \tag{C.12}$$

Supposons à présent que c'est U qui a été émis, de façon similaire au cas précédent, on obtient une borne sur la probabilité d'erreur par paire conditionnelle avec

$$P(U \to V|H) \leq \frac{1}{2} \exp\left(-\frac{\sum_{j=1}^{n_r} \sum_{u=1}^{\ell} |\sum_{i=1}^{n_t} h_{ij}(V_i^u - U_i^u)|^2}{8N_0}\right) \tag{C.13}$$

où N_0 est la variance du bruit par dimension.

La différence avec le paragraphe précédent est que les coefficients h_{ij} sont constants pour toutes les valeurs de $u, u = 1, \ldots, \ell$. Nous allons donc introduire de nouvelles variables aléatoires α_j, définies par $\alpha_j = \sum_{u=1}^{\ell} \| \sum_{i=1}^{n_t} h_{ij}(V_i^u - U_i^u)\|^2$. Les α_j ne définissent donc plus des variables de Rayleigh mais nous allons les modifier afin de nous ramener au raisonnement du cas précédent en regroupant les coefficients h_{ij} entre eux. Pour cela, nous introduisons la matrice $A(U,V) = (A_{pq})_{p=1,\ldots,n_t}^{q=1,\ldots,n_t}$ où $A_{pq} = \sum_{u=1}^{\ell}(V_p^u - U_p^u)(V_q^u - U_q^u)^h$ et les vecteurs $k_j = (h_{1j}, \ldots, h_{n_t j}), j = 1, \ldots, n_r$, ce qui nous permet de réécrire l'équation (C.13) de la façon suivante

$$P(U \to V|H) \leq \frac{1}{2} \exp\left(-\frac{\sum_{j=1}^{n_r} k_j A(U,V) {k_j}^h}{8N_0}\right) = \frac{1}{2} \prod_{j=1}^{n_r} \exp\left(-\frac{k_j A(U,V) {k_j}^h}{8N_0}\right)$$

On notera tout d'abord que la matrice $A(U,V)$ est hermitienne, puisqu'il est évident que $A(U,V) = A(U,V)^h$. Elle est donc diagonalisable et que ses valeurs propres $\lambda_i, i = 1, \ldots, n_t$ sont positives ou nulles [42]. Si l'on note $\mathcal{V}$ sa matrice de passage, $\mathcal{V} = (v_{pq})_{p=1,\ldots,n_t}^{q=1,\ldots,n_t}$ est unitaire et vérifie $\mathcal{V}A(U,V)\mathcal{V}^h = Diag(\lambda_1, \ldots, \lambda_{n_t})$. On peut alors définir les variables aléatoires β_{ij} suivantes

$$\forall i \in \{1, \ldots n_t\} \; \forall j \in \{1, \ldots n_r\} \quad \beta_{ij} = \sum_{p=1}^{n_t} h_{pj} v_{pi}$$

L'expression de la probabilité d'erreur par paire devient alors

$$P(U \to V|H) \leq \frac{1}{2} \prod_{j=1}^{n_r} \exp\left(-\frac{\sum_{i=1}^{n_t} \lambda_i |\beta_{ij}|^2}{8N_0}\right)$$

Or, sachant que les évanouissements h_{ij} sont des variables aléatoires gaussiennes indépendantes de variance 1 (ou encore 1/2 par dimension) et de moyenne nulle, et que la matrice $\mathcal{V}$ est unitaire, donc forme une base orthonormale de $\mathbb{C}^{n_t}$, les variables aléatoires

β_{ij} sont elles aussi des gaussiennes indépendantes de moyenne nulle et de variance 1. L'opération de diagonalisation réalisée sur $A(U,V)$ nous permet donc d'avoir, comme au paragraphe précédent, des coefficients $\lambda_i|\beta_{ij}|^2$ de l'exponentielle majorante égaux qui sont des variables aléatoires de Rayleigh indépendantes. La variance de chaque $\lambda_i|\beta_{ij}|^2$ étant égale à λ_i ($\lambda_i \geq 0$), on obtient

$$P(U \to V) \leq \frac{1}{2}\left(\frac{1}{\prod_{i=1}^{n_t}(1+\frac{\lambda_i}{8N_0})}\right)^{n_r}$$

Si l'on note à présent r le rang de la matrice $A(U,V)$ [42], l'équation devient à fort rapport signal à bruit

$$\boxed{P(U \to V) \leq \frac{1}{2}\left(\prod_{i=1}^{r}\frac{\lambda_i}{E_b}\right)^{-n_r}\left(\frac{E_b}{8N_0}\right)^{-rn_r} \qquad \text{(C.14)}}$$

On voit donc apparaître un gain en diversité, défini comme la puissance du rapport signal à bruit, soit rn_r, et un gain de codage, défini comme le gain obtenu sur un système non codé ayant le même gain en diversité, soit $\left(\prod_{i=1}^{r}\frac{\lambda_i}{E_s}\right)^{1/n_r}$. Si l'on compare cette formule à celle obtenue pour le canal de Rayleigh indépendant, soit avec $\ell = 1$, on vérifie effectivement que le gain de diversité est identique, puisque le rang de $A(U,V)$ vérifiant par définition $r \leq min(\ell, n_t)$, on a nécessairement $r = 1$ pour $\ell = 1$.

Comme au paragraphe précédent, la probabilité d'erreur par bit se déduira en utilisant la borne de l'union.

Annexe D

Expression de la capacité d'un canal à entrées multiples et sorties multiples

Le calcul de la capacité sur canal à entrées et sorties multiples a été mené en parallèle par Telatar [71] et Foschini [34]. Nous présentons ici les grandes lignes de celle réalisée par Telatar, qui se trouve être la plus complète théoriquement parlant. Certaines démonstrations, non directement utiles au raisonnement, ont été omises ici. On les trouvera dans l'article original [71].

La démarche suivie est la suivante : après avoir introduit les entrées complexes dites gaussiennes spéciales, on montrera qu'elles sont à maximum d'entropie et on en déduira la capacité du canal MIMO

$$C = E_{\mathbf{H}}\left[\log_2 \det(I_{n_r} + \frac{\rho}{n_t}\mathbf{H}\mathbf{H}^h)\right]$$

lorsque l'on suppose que le canal est à bande étroite, où ρ est donc égal au rapport entre la puissance totale émise par les antennes d'émission et la variance du bruit.

D.1 Notations et définitions

Nous considérons ici un canal de transmission tel que celui de la figure 3.2 du chapitre 3 avec n_t antennes d'émission et n_r antennes de réception. Le vecteur reçu $\mathbf{y}$ étant donné par

$$\mathbf{y} = H\mathbf{x} + \mathbf{b}$$

où $\mathbf{x} = (x_j)^t_{j=1,\ldots,n_t}$ est le vecteur du signal émis, $H = [h_{ij}]_{i=1,\ldots,n_r,j=1,\ldots,n_t}$ est la matrice complexe du canal et $\mathbf{b} = (b_i)^t{}_{i=1,\ldots,n_r}$ est le bruit blanc additif gaussien complexe. Par souci de simplification, on supposera dans tout notre calcul que l'on a $E[\mathbf{bb}^h] = I_{n_r}$, ce qui se fait sans perte de généralité considérant que l'autocorrélation $E[\mathbf{xx}^h]$ du signal émis a elle aussi été divisée par le facteur $2N_0$ correspondant (variance du bruit complexe). La puissance totale émise $E[\mathbf{x}^h\mathbf{x}]$ sur les n_t antennes d'émission sera bornée supérieurement par $\rho = \frac{P}{2N_0}$.

De plus, ayant remarqué que pour $\mathbf{x}$ vérifiant la limitation en puissance $E[\mathbf{x}^h\mathbf{x}] \leq \rho$, $\mathbf{x} - E[\mathbf{x}]$ la vérifie aussi, nous nous limiterons à des vecteurs $\mathbf{x}$ de moyenne nulle.

Définition D.1.1 *Un vecteur* $\mathbf{x} \in \mathbb{C}^n$ *est dit* **spécial gaussien** *si*

- *le vecteur réel* $\hat{\mathbf{x}} = \begin{bmatrix} \Re(\mathbf{x}) \\ \Im(\mathbf{x}) \end{bmatrix} \in \mathbb{R}^{2n}$ *est gaussien*
- *la matrice de covariance de* $\hat{\mathbf{x}}$ *a la structure spéciale suivante :*

$$E[(\hat{\mathbf{x}} - E[\hat{\mathbf{x}}])(\hat{\mathbf{x}} - E[\hat{\mathbf{x}}])^h] = \frac{1}{2} \begin{bmatrix} \Re(Q) & -\Im(Q) \\ \Im(Q) & \Re(Q) \end{bmatrix}$$

où la matrice $Q \in \mathbb{C}^{n\times n}$ *de covariance de* $\mathbf{x}$ *est hermitienne définie positive.*

On notera que les différentes conditions imposées au vecteur $\mathbf{x}$ pour qu'il soit spécial gaussien seront par exemple vérifiées lorsque ses composantes de $\hat{\mathbf{x}}$ sont des gaussiennes réelles décorrélées identiquement distribuées.

Pour tous $\mathbf{z} \in \mathbb{C}^n$ et $A \in \mathbb{C}^{n\times n}$ on notera

$$\hat{\mathbf{z}} = \begin{bmatrix} \Re(\mathbf{z}) \\ \Im(\mathbf{z}) \end{bmatrix}$$

et

$$\hat{A} = \begin{bmatrix} \Re(A) & -\Im(A) \\ \Im(A) & \Re(A) \end{bmatrix}$$

Définition D.1.2 *La* **densité de probabilité** *(selon la mesure de Lebesgue) sur* $\mathbb{C}^n$ *d'un vecteur* $\mathbf{x} \in \mathbb{C}^n$ *de moyenne* $\boldsymbol{\mu}$ *et de covariance* Q *est donnée par*

$$\gamma_{\mu,Q}(\mathbf{x}) = \det(\pi\hat{Q})^{-1/2} \exp(-(\hat{\mathbf{x}} - \hat{\boldsymbol{\mu}})^h \hat{Q}^{-1} (\hat{\mathbf{x}} - \hat{\boldsymbol{\mu}}))$$

D.2 Propriétés des vecteurs spéciaux gaussiens

Les vecteurs spéciaux gaussiens vérifient les différentes propriétés suivantes [71]

Propriété 1 *La densité de probabilité d'un vecteur spécial gaussien est égale à*

$$\gamma_{\mu,Q}(\mathbf{x}) = \det(\pi Q)^{-1} \exp(-(\mathbf{x} - \boldsymbol{\mu})^h Q^{-1} (\mathbf{x} - \boldsymbol{\mu}))$$

Propriété 2 *L'entropie différentielle $\mathcal{H}(\gamma_{\mu,Q}(\mathbf{x}))$ d'un vecteur spécial gaussien $\mathbf{x}$ de moyenne $\boldsymbol{\mu}$ et de covariance Q, que l'on notera par simplicité $\mathcal{H}(\mathbf{x})$, est donnée par*

$$\mathcal{H}(\mathbf{x}) = \log_2 \det(\pi e Q)$$

Proposition 3 *Soit $\mathbf{x} \in \mathbb{C}^n$ un vecteur complexe de moyenne nulle et de matrice de covariance $E[\mathbf{x}\mathbf{x}^h] = Q$, soit $E[x_i x_j^*] = Q_{ij}, 1 \leq i, j \leq n$. L'entropie de $\mathbf{x}$ vérifie $\mathcal{H}(\mathbf{x}) \leq \log_2 \det(\pi e Q)$, avec égalité si et seulement si x est un vecteur spécial gaussien.*

Propriété 3 *Tout vecteur résultant d'une transformation linéaire d'un vecteur spécial gaussien est spécial gaussien.*

Propriété 4 *La somme de deux vecteurs spéciaux gaussiens indépendants est spéciale gaussienne.*

D.3 Capacité pour une valeur de H fixée

Nous allons tout d'abord considérer le cas d'un canal H déterminé. La capacité correspondante $C(H, \rho)$ est classiquement obtenue en maximisant l'information mutuelle moyenne entre l'entrée $\mathbf{x}$ et la sortie $\mathbf{y}$ du canal :

$$I(\mathbf{x}; \mathbf{y}) = \mathcal{H}(\mathbf{y}) - \mathcal{H}(\mathbf{y}|\mathbf{x}) = \mathcal{H}(\mathbf{y}) - \mathcal{H}(\mathbf{b})$$

donc maximiser $I(\mathbf{x}; \mathbf{y})$ revient à maximiser $\mathcal{H}(\mathbf{y})$. Nous omettrons donc le facteur $\mathcal{H}(\mathbf{b})$ dans la suite de nos calculs. Or, pour $\mathbf{x}$ de moyenne nulle et de covariance Q, $\mathbf{y}$ est de moyenne nulle et de covariance $E[\mathbf{y}\mathbf{y}^h] = HQH^h + I_{n_r}$ donc, par proposition 3 est d'entropie maximale lorsqu'il est spécial gaussien. D'après les propriétés 3 et 4, avoir $\mathbf{y}$ spécial gaussien implique que $\mathbf{x}$ l'est également. On en déduit donc la propriété suivante :

Proposition 4 *La capacité sur un canal à entrées et sorties multiples à H fixée est maximale lorsque l'entrée est spéciale gaussienne.*

En nous restreignant donc à des entrées $\mathbf{x}$ spéciales gaussiennes, il s'agit de maximiser

$$I(\mathbf{x}; \mathbf{y}) = \mathcal{H}(\mathbf{y}) \propto \log_2 \det(I_{n_r} + HQH^h) = \Psi(Q, H)$$

On peut montrer, en utilisant le technique du "water-filling" [28][71] et en diagonalisant la matrice hermitienne $HH^h = U^h \Lambda U$ où U est une matrice unitaire et Λ une matrice diagonale $\Lambda = \mathbf{D}(\lambda_1, \ldots, \lambda_{n_t})$, que l'on obtient

$$C(H, \rho) = \sum_{i,\ \omega\lambda_i > 1} \log_2(\omega.\lambda_i) \tag{D.1}$$

où ω représente le niveau du "water-filling".

D.4 Capacité d'un canal de Rayleigh MIMO

On suppose à présent que la matrice H n'est plus fixée, mais est une matrice aléatoire $\mathbf{H}$, indépendante de $\mathbf{x}$ et de $\mathbf{b}$. Les composantes de $\mathbf{H}$ sont indépendantes, gaussiennes de moyenne nulle et leurs parties réelles et imaginaires indépendantes entre elles sont de variance 1/2. Enfin, la réalisation H de $\mathbf{H}$ est supposée connue du récepteur mais pas de l'émetteur.

Proposition 5 *Soit* $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$ *une matrice gaussienne complexe de composantes réelles et imaginaires indépendantes identiquement distribuées et de moyenne nulle. Alors, pour toutes matrices* $U \in \mathbb{C}^{n_r \times n_r}$ *et* $V \in \mathbb{C}^{n_t \times n_t}$ *unitaires, la distribution de* $U\mathbf{H}V^h$ *est la même que celle de* $\mathbf{H}$.

La matrice $\mathbf{H}$ est donc invariante par des transformation unitaires.

Puisque le récepteur connaît la réalisation de $\mathbf{H}$, la sortie du canal est à présent le couple $(\mathbf{y}, \mathbf{H}) = (\mathbf{Hx} + \mathbf{b}, \mathbf{H})$. L'information mutuelle entre l'entrée et la sortie du canal est donc

$$I(\mathbf{x}; (\mathbf{y}, \mathbf{H})) = I(\mathbf{x}; \mathbf{H}) + I(\mathbf{x}; \mathbf{y}|\mathbf{H}) = I(\mathbf{x}; \mathbf{y}|\mathbf{H}) = E_{\mathbf{H}}[I(\mathbf{x}; \mathbf{y}|\mathbf{H} = H)]$$

D'après les résultats trouvés au paragraphe précédent pour le cas où H est fixé, on sait que, Q étant la matrice de covariance de $\mathbf{x}$, le choix de $\mathbf{x}$ qui maximise $I(\mathbf{x}; \mathbf{y}|\mathbf{H} = H)$ est un vecteur spécial gaussien complexe et que l'information mutuelle maximale correspondante est $\Psi(Q, H)$. Il faut donc à présent maximiser la fonction $\Psi(Q)$ suivante

$$\Psi(Q) = E_{\mathbf{H}}[\Psi(Q, \mathbf{H})] = E_{\mathbf{H}}[\log_2 \det(I_{n_r} + \mathbf{H}Q\mathbf{H}^h)] \tag{D.2}$$

pour Q matrice hermitienne définie positive vérifiant $tr(Q) \leq \rho$.

Q étant hermitienne définie positive, elle est diagonalisable : il existe une matrice U unitaire et une matrice diagonale D positive telles que $Q = UDU^h$. On obtient donc

$$\Psi(Q) = E_{\mathbf{H}}[\log_2 \det(I_{n_r} + (\mathbf{H}U)D(\mathbf{H}U)^h)]$$

Or, la distribution de $\mathbf{H}U$ est la même que celle de $\mathbf{H}$ par proposition 5, on a $\Psi(Q) = \Psi(D)$ et on peut donc se restreindre au cas où Q est diagonale positive.

Considérons une telle matrice Q et introduisons une matrice de permutation Π, et la matrice $Q_\Pi = \Pi Q \Pi^h$: de la proposition 5, on déduit que l'on a $\Psi(Q) = \Psi(Q_\Pi)$.
Par ailleurs, l'application $Q \to I_{n_r} + HQH^h$ étant linéaire et conservant le caractère positif de la matrice d'entrée Q, et sachant que le logarithme du déterminant d'une matrice est une fonction concave sur l'ensemble des matrices définies positives [71], on déduit que la fonction $Q \to \Psi(Q)$ est concave.

Si l'on considère alors la matrice $\tilde{Q}$ définie comme la moyenne arithmétique de toutes les matrices de permutation possible, soit

$$\tilde{Q} = \frac{1}{n_t!} \sum_{\Pi} Q_{\Pi} = \frac{tr(Q)}{n_t} I_{n_t}$$

on a alors $\Psi(\tilde{Q}) \geq \Psi(Q_{\Pi})$ et $tr(\tilde{Q}) = tr(Q)$. Ainsi, la matrice Q qui maximise la fonction Ψ est-elle un multiple de l'identité, avec pour coefficient de proportionnalité le plus grand possible, soit $\frac{\rho}{n_t}$.

Théorème D.4.1 *La capacité d'un canal à entrées et sorties multiples est atteinte lorsque le signal d'entrée est spécial gaussien, de moyenne nulle, et de covariance $\frac{\rho}{n_t} I_{n_t}$. La capacité vaut alors :*

$$C = E_{\mathbf{H}} \left[\log_2 \det(I_{n_r} + \frac{\rho}{n_t} \mathbf{H}\mathbf{H}^h) \right]$$

Bibliographie

[1] M. Abramovitz, I. A. Stegun, *Handbook of Mathematical Functions.* New York: Dover, 1972, sec. 22, pp.773–802.

[2] L. R. Bahl, J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Transactions on Information Theory*, vol. 20, pp. 284–287, March 1974.

[3] E. S. Barnes and G. E. Wall, "Some extreme forms defined in terms of Abelian groups," *Journal of the Australian Mathematical Society*, vol. 1, pp. 47–63, 1959.

[4] E. S. Barnes and N. J. A. Sloane, "New lattice packings of spheres," *Canadian Journal of Mathematics*, vol. 35, pp. 117–130, 1983.

[5] G. Battail, "Rotating a redundant constellation in signal space against channel fluctuations," ENST, Paris, France, rapport interne, 1989.

[6] G. Battail, *Théorie de l'information.* Paris: Masson, 1997.

[7] P. Beckmann, *Orthogonal Polynomials for Engineers and Physicists.* Boulder, Colorado: The Golem Press, 1973.

[8] S. Benedetto, E. Biglieri, V. Castellani, *Digital Transmission Theory.* New Jersey: Prentice-Hall, Englewood Cliffs, 1987.

[9] S. Benedetto and G. Montorsi, "Design of parallel concatenated convolutional codes," *IEEE Transactions on Communications*, vol. 44, no. 5, pp. 591–600, May 1996.

[10] E. R. Berlekamp, *Algebraic coding theory.* Laguna Hill, California: Aegean Park Press, revised edition, 1984.

[11] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: turbo-codes," *Proceedings of ICC'93*, Genève, pp. 1064–1070, May 1993.

[12] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *IEEE Transactions on Communications*, vol. 44, pp. 1261–1271, October 1996.

[13] S. Benedetto, G. Montorsi and F Pollara, "A Soft-Input Soft-Output APP Module for Iterative Decoding of Concatenated Codes," *IEEE Communications Letters*, vol. 1, no. 1, pp. 22-24, January 1997.

[14] F. Boixadera and J. Boutros, "Capacity considerations for wireless multiple-input multiple-output channels," *Proceedings of Workshop on Multiaccess, Mobility and Teletraffic for Wireless Communications*, Venice, Italy, 6-8 October 1999.

[15] K. Boullé, J-C. Belfiore, "Modulation scheme designed for the Rayleigh fading channel," *Proceedings of CISS'92*, Princeton NJ, pp. 288-293, March 1992.

[16] J. Boutros, "Lattice Codes for Rayleigh Fading Channels," Ph.D. dissertation, École Nationale Supérieure des Télécommunications, Paris, France, Juin 1996.

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

[18] J. Boutros, "Les turbo codes parallèles et séries, décodage SISO itératif et performances ML," cours ENST, *http://www.comelec.enst.fr/turbocodes.*

[19] J. Boutros, E. Viterbo, "Signal Space Diversity: a power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1453–1467, July 1998.

[20] L. Brunel, "Algorithmes de décodage de canal pour l'accès multiple à étalement de spectre," Ph.D. dissertation, École Nationale Supérieure des Télécommunications, Paris, France, Décembre 1999.

[21] L. Brunel and J. Boutros,, "Euclidean space lattice decoding for joint detection in CDMA systems," *Proceedings of of ITW'99*, Kruger National Park, South Africa, p. 129, June 1999.

[22] C. Brutel, J. Boutros and P. Mège, "Iterative joint channel estimation and detection of coded CPM," *Proceedings of the 2000 International Zürich Seminar on Broadband Communications*, February 15-17 2000, ETH Zürich, Switzerland.

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

[24] G. Cohen, J. L. Dornstetter, P. Godlewski, *Codes correcteurs d'erreurs.* Paris: Masson, Collection technique et scientifique des télécommunications, 1992.

[25] H. Cohen, *A course in computational algebraic number theory.* New York: Springer-Verlag, 1993.

[26] J. H. Conway and N. J. A. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Transactions on Information Theory*, vol. IT-32, pp. 41–50, 1986.

[27] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups.* New York: Springer-Verlag, 3rd edition, 1998.

[28] T. M. Cover and J. A. Thomas, *Elements of Information Theory.* New York: John Wiley & Sons, 1991.

[29] V. M. DaSilva, E. S. Sousa, "Fading-Resistant Modulation Using Several Transmitter Antennas," *IEEE Transactions on Communications*, vol. 45, no. 10, pp. 1236–1244, October 1997.

[30] A. P. Dempster, N. M. Laird and D. B. Rubin, "Maximum likelihood from incomplete data via the EM algorithm," *J. Roy. Stat. Soc.* , no. 39, pp. 1–38, 1977.

[31] G.D. Forney, "Coset Codes — PartII: Binary Lattices and Related Codes," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152–1187, September 1988.

[32] G. D. Forney Jr. , "Geometrically uniform codes," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 211–226, March 1982.

[33] G. D. Forney Jr. and A. Vardy, "Generalized minimum distance decoding of Euclidean-space codes and lattices," *IEEE Transactions Information Theory*, vol. 42, pp. 1992–2026, 1996.

[34] G. J. Foschini, Jr. and M. J. Gans, "On limits of wireless communication in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol. 6, no. 3, pp. 311–335, March 1998.

[35] R. G. Gallager, *Information theory and reliable communications.* New York: John Wiley & Sons, 1968.

[36] C. N. Georghiades and J. C. Han, "Sequence estimation in the presence of random parameters via the EM algorithm," *IEEE Transactions on Communications*, vol. 45, no. 3, pp. 300–308, March 1997.

[37] D. Gesbert, "Égalisation et identification multi-voies : méthodes auto-adaptatives au second ordre," Ph.D. dissertation, École Nationale Supérieure des Télécommunications, Paris, France, Mars 1997.

[38] X. Giraud, E. Boutillon and J-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 938–952, May 1997.

[39] G. H. Golub and C. F. Van Loan, *Matrix computations.* Baltimore, Maryland: The Johns Hopkins University Press, 2nd edition, 1989.

[40] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 429–445, March 1996.

[41] T. Hales, "The Kepler Conjecture," *http://www.math.lsa.umich.edu/ hales/countdown.*

[42] R. A. Horn and C. R. Johnson, *Matrix Analysis.* Cambridge: Cambridge University Press, 1985-1993.

[43] N. Ibrahim, "Codage et décodage de canal pour un système de communication à accès multiple," Ph.D. dissertation, École Nationale Supérieure des Télécommunications, Paris, France, Mars 1999.

[44] G. Kawas Kaleh and R. Vallet, "Joint Parameter Estimation and Symbol Detection for Linear and Nonlinear Unknown Channels," *IEEE Transactions on Communications*, vol. 42, no. 7, pp. 2406–2413, July 1994.

[45] K. J. Kerpez, "Constellations for good diversity performance," *IEEE Transactions on Communications*, vol. 41, no. 9, pp. 1412–1421, Sept. 1993.

[46] G. R. Lang and F.M. Longstaff, "A Leech lattice modem," *IEEE Journal of Selected Areas in Communications*, vol. 7, pp. 968–973, August 1989.

[47] W. C. Y. Lee, "Estimate of channel capacity in Rayleigh fading environment," *IEEE Transactions on Vehicular Technology*, vol. 39, pp. 187–189, August 1990.

[48] A. K. Lenstra, H. W. Lenstra and L. Lovàsz, "Factoring polynomials with rational coefficients," *Math. Ann.*, vol. 261, pp. 515–534, 1982.

[49] X. Li, J. A. Ricey, "Bit-interleaved coded modulation with iterative decoding," *IEEE Communications Letters*, vol. 1, no. 6, pp.169–171, November 1997.

[50] S. Lin and D. J. Costello, "Error Control Coding: Fundamentals and applications," Englewood Cliffs, NJ, Prentice-Hall, 1983.

[51] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[52] E. Malkamäki, "Coded diversity on Block-Fading Channels," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp.771–782, March 1999.

[53] E. Malkamäki, "Evaluating the performance of convolutional codes over block fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp.1643–1646, July 1999.

[54] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in rayleigh flat fading," *IEEE Transactions on Information Theory*, vol. 45, no. 1, pp. 139–157, January 1999.

[55] L. H. Ozarow, S. Shamai (Shitz) and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Transactions on Vehicular Technology*, vol. 43, pp. 359–378, May 1994.

[56] A. Papoulis, *Probability, random variables, and stochastic processes*. New York: Mac Graw Hill, 3rd edition, 1991.

[57] C. Pöppe, "La conjecture de Kepler démontrée," *Pour la science*, no. 259, Mai 1999.

[58] J.G. Proakis, *Digital Communications*. New York: McGraw-Hill, 3rd edition, 1995.

[59] D. Rainish, "Diversity Transform for Fading Channels," *IEEE Transactions on Information Theory*, vol. 44, no. 12, December 1996.

[60] M. Reinhardt and J. Lindner, "Transformation of a Rayleigh fading channel into a set of parallel AWGN channels and its advantage for coded transmission," *Electronics Letters*, vol. 31, pp. 2154–2155, December 1995.

[61] T. J. Rivlin, *Chebyshev Polynonials: from Approximation Theory to Algebra and Number Theory*. New York: John Wiley & Sons, Inc., 2nd ed., 1990

[62] P. Samuel, *Algebraic theory of numbers*. Paris: Hermann, 1971.

[63] C. Schlegel, "Trellis coded modulation on time-selective fading channels," *IEEE Transactions on Communications*, vol. 42, pp. 1617–1627, April 1994.

[64] C. E. Shannon, "A Mathematical Theory of Communication," *Bell system technical journal*, vol. 27, no. 3-4, pp. 379–423 and 623–656, 1948.

[65] C. Shannon, “Probability of error for optimal codes in a Gaussian channel,” *Bell Systems Technical Journal*, vol. 38, pp. 611–656, May 1959.

[66] N. J. A. Sloane : “Encrypting by random rotations,” *Eurocrypt*, 1983.

[67] A. Stefanov and T. M. Duman, “Turbo coded modulation for systems with transmit and receive antenna diversity,” *Proceedings of the 1999 Global Telecommunications Conference,* Dec. 5-9, 1999, Rio de Janeiro, Brazil, pp. 2336–2340.

[68] F. W. Sun and H. C. A. Van Tilborg, “The Leech lattice, the octacode, and decoding algorithms,” *IEEE Transactions on Information Theory*, vol. IT-41, pp. 1097–1106, 1995.

[69] V. Tarokh, N. Seshadri and A. R. Calderbank, “Space-time codes for high data rate wireless communication: Performance criterion and code construction,” *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp.744–765, March 1998.

[70] V. Tarokh A. Naguib, N. Seshadri and A. R. Calderbank, “Space-time codes for high data rate wireless communication: Performance criteria in the presence of channel estimation errors, mobility, and multiple paths,” *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp.199–207, March 1998.

[71] E. Telatar, “Capacity of multi-antenna Gaussian channels,” *AT&T Bell Laboratories Internal Tech. Memo.* , June 1995.

[72] G. Ungerboeck, “Channel coding with multilevel/phase signals,” *IEEE Transactions on Information Theory*, vol. 28, pp. 56–67, January 1982.

[73] R. Urbanke and R. Rimoldi, “Lattices codes can achieve capacity on the AWGN channel,” *IEEE transactions on Information Theory*, vol. 44, no. 1, pp. 273–278, January 1998.

[74] R. Vallet, “Applications de l’identification des modèles de Markov cachés aux communications numériques,” Ph.D. dissertation, École Nationale Supérieure des Télécommunications, Paris, France, October 1991.

[75] A. Vardy, “Even more efficient bounded-distance decoding of the hexacode, the Golay code, and the Leech lattice,” *IEEE Transactions on Information Theory*, vol. IT-41, pp. 1495–1499, 1995.

[76] A. J. Viterbi and J. K. Omura, *Principles of digital communications and coding.* New York: McGraw-Hill, 1979.

[77] E. Viterbo and E. Biglieri, “A universal lattice decoder,” *Proceedings of* 14^{th} *Colloque GRETSI*, Juan-les-Pins, pp. 611–614, Septermber 1993.

[78] E. Viterbo and J. Boutros, “A universal lattice code decoder for fading channels,” *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1639–1642, July 1999.

[79] E. Viterbo, “Tecniche matematiche computazionali per l’analisi ed il progetto di costellazioni a reticolo,” Ph.D. dissertation, Politecnico di Torino, Torino, Italy, February 1995.

[80] G. W. Wornell, “Spread-response precoding for communication over fading channels,” *IEEE Transactions on Information Theory*, vol. 42, pp. 488–501, Mars 1996.

[81] E. Zehavi, "8-PSK trellis codes for a rayleigh channel," *IEEE Transactions on Communications*, vol. 40, pp. 873–884, May 1992.

Liste de publications

(à télécharger à l'adresse `http://www.comelec.enst.fr/publications`)

[82] C. Lamy and J. Boutros, "Décodage à sortie souple des réseaux de points," *Annales des Télécommunications*, vol. 53, n. 9-10, pp. 353–360, Octobre 1998.

[83] C. Lamy and J. Boutros, "Soft-Output MSE Decoding of Lattices," *Proceedings of the 5-th Int. Symposium on Digital Signal Processing for Communications Systems (DSPCS'99)*, Perth, Australia, 2–4 February 1999.

[84] C. Lamy and J. Boutros, "On Random Rotations Diversity and Minimum MSE Decoding of Lattices," to appear in *IEEE Transactions on Information Theory*, July 2000.

[85] C. Lamy, F. Boixadera and J. Boutros, "Iterative APP decoding and channel estimation for multiple-input multiple-output channels," submitted to *IEEE Transactions on Communications*, 2000.

[86] C. Lamy, J. Boutros and E. Viterbo "Capacity of rotated modulations on the Rayleigh fading channel," in preparation for the *IEEE Transactions on Communications*, 2000.