Thèse

présentée pour obtenir le grade de docteur

de l'Ecole Nationale Supérieure
des Télécommunications

Spécialité : Electronique et Communications

Céline Durand

Modulations à haute efficacité spectrale pour les transmissions non cohérentes

Soutenue le 20 décembre 2000 devant le jury composé de

Thomas Marzetta	Président
Ezio Biglieri	Rapporteurs
Hikmet Sari	
Juing Fang	Examinateurs
Robert Vallet	
Joseph Boutros	Directeur de thèse

Ecole Nationale Supérieure des Télécommunications, Paris

"Pendant ma première année à l'école navale de Monterey, en Californie, je discutais avec des camarades de la difficulté des programmes. Un des professeurs entendit notre conversation et se chargea de nous rassurer :
– Ne vous inquiétez pas ! Quand vous pensez que vous savez tout, on vous donne votre Licence. Puis, vous vous rendez compte que vous ne savez rien, et on vous donne votre Maîtrise. Et quand vous avez compris que les autres n'en savent pas plus que vous, vous obtenez votre Doctorat."

Blake Huguenin.

"La société humaine, le monde, l'homme tout entier est dans l'alphabet... L'alphabet est une source."

Victor Hugo.

Remerciements

Je tiens à remercier chaleureusement tous ceux qui m'ont aidée, accompagnée et encouragée sur le chemin exigeant qui mène au Doctorat.

Je tiens tout d'abord à exprimer ma profonde gratitude à Monsieur Thomas Marzetta, des *Bell Laboratories*, pour m'avoir fait l'honneur de présider le jury de cette thèse. Son déplacement jusqu'en France pour assister à la soutenance et le soin avec lequel il a tenu son rôle de président m'ont beaucoup touchée. Qu'il en soit vivement remercié.

Toute ma reconnaissance va également à Monsieur Ezio Biglieri, Professeur au *Politecnico* de Turin et à Monsieur Hikmet Sari, Directeur Scientifique de *Pacific Broadband Communications*, pour avoir cordialement accepté d'être les rapporteurs de cette thèse. Leurs réputations scientifiques, associées à leurs commentaires élogieux, honorent mon travail.

Mes plus vifs remerciements s'adressent à Monsieur Juing Fang, d'*Alcatel Space Industries*, et à Monsieur Robert Vallet, Professeur à l'ENST, pour leur participation au jury et l'intérêt qu'ils ont exprimé quand à l'ensemble de mes travaux de recherche.

Un grand merci à mon directeur de thèse, Joseph Boutros. Merci d'avoir supporté mon fort (mauvais !) caractère, mais il en faut pour travailler avec toi, tu en conviendras. Tes compétences techniques et ton excès en tout ont permis à mon travail d'être ce qu'il est, et je t'en suis reconnaissante.

Je n'oublie pas le département Radiocommunications du centre de recherche d'Alcatel CIT, CRC pour les intimes, grâce auquel le contrat CIFRE avec le département Communications et Electronique de l'ENST a pu voir le jour. Je profite de cette occasion pour remercier tous mes compagnons de route "Alcateliens" pour l'ambiance chaleureuse qui a entouré mon passage au CRC : la "CRC team" bien qu'éparpillée, les fidèles au poste contre vents et marées, les midis à la gym et la piste de Kart. Je remercie tout particulièrement Elie Bejjani, initiateur de cette thèse, mon encadrant pendant plus de deux ans, celui grâce auquel les choses sont devenues "cohérentes et utiles" et Marco Fratti, qui a repris le flambeau. Merci à tous les deux pour votre gentillesse, votre professionnalisme et votre soutien sans bornes.

Les derniers mois de ce périple m'ont permis de revenir au département Comelec de l'ENST pour accomplir la tâche souvent ingrate et sans fin qu'est la rédaction d'un mémoire de thèse. Merci à Danielle Childz pour son aide précieuse et à tous les permanents. J'ai une pensée émue pour ce cher bureau A303, qui à coups de déménagements, thés et autres JJG, est devenu ma deuxième maison et pour mes colocataires, de prêt ou de loin : Sabine Leveiller (Le p'tit train...), Sandrine Vialle (trop à dire, merci pour tout), Mhammad Aoude (fan de Laetitia), Christophe Brutel (Cricri pour les intimes), Christophe Gosset (Rabiche), Evguenii Gueorguiev (et sa caméra), Steffan Lauffenberger (oups), Hadi Sawaya (ouh la la), et Cedric "soft"Ware (pour que l'informatique soit toujours un plaisir). Sans oublier tous ceux qui ont d'ores et déjà quitté les lieux mais qui furent présents au cours de ces trois ans : Amal Abou Hassan (to be or not to be... "de souche" ?), François-Xavier Bergot (et les résidus), Loïc Brunel (et sa béquille), Catherine Lamy (Greta et Barbara), Olivier Pothier (Cofinoga) et Seyed Barham Zahir Azami (et ses chevaux).

Je ne saurais finir sans adresser une tendre pensée à Lucile, Maman, Papa, tous mes proches et mes deux soleils. Votre bonheur et votre fierté sont une récompense à la mesure de ces années de travail.

Et Merci Bertrand.

Paris, le 12 janvier 2001

Résumé

Les applications récentes et futures du domaine des télécommunications requièrent toujours plus de bande passante et les débits binaires sont de l'ordre de quelques centaines à quelques milliers de kbits/s. L'accès à de tels services doit être possible depuis un nombre grandissant de réseaux. C'est pourquoi un usage encore plus efficace des ressources est nécessaire.

La mise en œuvre ou non de mécanismes de récupération de la phase permet de distinguer la détection cohérente de la détection non cohérente ; cette dernière se comporte très bien face aux conditions de transmission difficiles et permet la réalisation de terminaux robustes et peu coûteux. Les modulations non cohérentes classiques (Q-FSK, OOK, et leurs variantes) souffrent de leur faible efficacité spectrale, mais celle-ci peut être augmentée à l'aide de signaux multidimensionnels à composantes corrélées alors que tout ou partie de la dégradation des performances est compensée.

Ces travaux mettent l'accent sur des modulations à haute efficacité spectrale pour les transmissions non cohérentes. Nous cherchons et étudions des méthodes de construction d'alphabets non triviaux pour les canaux gaussien et de Rayleigh. Les alphabets multidimensionnels obtenus sont construits à partir de signaux corrélés – signaux d'une modulation FSK ou séquences d'étalement. Trois constructions sont fondées sur les signaux FSK : les réseaux de fréquences dont l'étude repose sur la théorie des réseaux de points, les alphabets codés par une TCM et les BICM pour lesquelles une détection itérative combinée à un décodage souple conduit aux meilleurs résultats. Si des alphabets plus grands sont nécessaires, nous suggérons l'emploi de séquences d'étalement complexes corrélées qui permettent de s'affranchir de toute limite théorique d'efficacité spectrale – hormis la capacité du canal cohérent – et d'approcher par des systèmes de transmission avec détection non cohérente, les performances de la détection cohérente.

Abstract

The rapid expansion in the telecommunications field brings about the evolution of needs. Future applications require more and more bandwidth and transmitted signals exhibit bit rates between several hundred and several thousand kbits/s. Moreover, access to such services should be possible from any type of network. Therefore, transmission resources should be carefully used.

Transmitted signals suffer from several distorsions. When no reliable phase estimation is possible to perform, the detection is called non coherent detection. Its main benefits are the robustness, the lower cost and the relative simplicity of the receiver. Though classical non coherent modulations (FSK modulation, OOK, and derived versions) suffer from their poor spectral efficiency, the use of multidimensional signals with correlated components is a good way to increase the spectral efficiency while compensating for the performance degradation.

This Ph.D. thesis deals with high spectral efficiency modulations for non coherent detection. We propose to search and study new methods for the design of non trivial alphabets for both Gaussian and Rayleigh fading channels. Multidimensional constellations based on correlated signals – either FSK signals or spreading sequences – are considered. Three constructions based on FSK signals are proposed : frequency space lattices that can be analysed using lattice sphere packing theory, TCM encoded alphabets and BICM for which iterative detection combined to soft decoding yields the best results. Moreover, when applications require larger sets, we suggest to use correlated complex spreading sequences. With such nonorthogonal sets, an increase of either the alphabet size or the sequence length always leads to higher spectral efficiency, only limited by the coherent channel capacity. The use of correlated signal sets reduces the gap between coherent and non coherent detection.

Table des matières

Remerciements **i**

Résumé **iii**

Abstract **v**

Table des Matières **vii**

Table des Figures **xi**

Liste des Tableaux **xv**

Liste des Abréviations **xvii**

Introduction **1**

1 Performances optimales ML des modulations Q-FSK **3**

1.1 Modulation de fréquence Q-FSK 4

1.1.1 Principe de la modulation 4

1.1.2 Détection non cohérente optimale à maximum de vraisemblance 5

1.1.3 Expression de la probabilité d'erreur 7

1.1.4 Performances sur différents canaux 12

1.2 Constellations multidimensionnelles à composantes corrélées 14

1.2.1 Principe et intérêt des signaux corrélés 14

1.2.2 Détection non cohérente optimale de signaux multidimensionnels 17

1.2.3 Probabilité d'erreur par paire 22

1.2.4 Exemple : signaux corrélés de diversité 4 28

1.3 Etude de la capacité 30

1.3.1 Capacité des canaux gaussien et de Rayleigh admettant en entrée une modulation 8-FSK 31

1.3.2 Capacité du canal de Rayleigh non cohérent à évanouissements indépendants admettant en entrée un alphabet de signaux multidimensionnels . . 32

1.4 Conclusions 32

1.5 Annexe 1.I : Détection optimale non cohérente sur le canal gaussien 35

1.6 Annexe 1.II : Etude des variations de $P(S_i \to S_j)$ 37

2 Modulations codées à composantes corrélées **39**

2.1 Codage faible latence pour les signaux corrélés 40

2.1.1 Modèle du système 40

2.1.2 Décodage à maximum de vraisemblance . . . 43
2.1.3 Démodulation non cohérente APP et décodage à entrée souple . . . 44
2.1.4 Calcul des APP pour le canal gaussien . . . 46
2.1.5 Calcul des APP pour le canal de Rayleigh . . . 46
2.2 Les modulations codées en treillis . . . 48
2.2.1 Principe . . . 48
2.2.2 Décodage ML : nouvelle métrique pour l'algorithme de Viterbi . . . 51
2.3 Les réseaux de points . . . 52
2.3.1 Définition des paramètres fondamentaux . . . 53
2.3.2 Constructions A et B . . . 58
2.3.3 Les réseaux binaires et les modulations codées en blocs . . . 62
2.3.4 Décodage par sphères . . . 67
2.3.5 Décodage à entrée souple des codes en blocs appliqué au décodage des réseaux de points . . . 70
2.4 Alphabets codés de signaux corrélés sur le canal gaussien . . . 74
2.4.1 Choix du réseau . . . 75
2.4.2 Choix de l'espacement fréquentiel de la FSK, Δf_0 . . . 80
2.4.3 Grande robustesse des schémas codés face à la corrélation . . . 82
2.5 Conclusions . . . 85

3 Signaux corrélés et décodage itératif 87
3.1 Décodage à entrée souple et sortie souple d'un code convolutif . . . 88
3.2 Structure et performances des turbo codes . . . 90
3.2.1 Les turbo codes parallèle . . . 90
3.2.2 Les turbo codes série . . . 92
3.3 Codage forte latence pour les signaux corrélés . . . 94
3.3.1 Modèle du système avec décodage APP simple . . . 94
3.3.2 Modèle du système avec détection itérative et décodage APP . . . 98
3.3.3 Importance du choix de l'étiquetage . . . 101
3.3.4 Choix de l'espacement fréquentiel et du rendement du code . . . 104
3.4 Signaux corrélés et turbo codes . . . 105
3.4.1 Décodage itératif d'un turbo code parallèle . . . 106
3.4.2 Comportement des turbo codes face à la corrélation . . . 107
3.5 Signaux corrélés et codage convolutif . . . 109
3.5.1 Q-FSK non orthogonale codée sur le canal gaussien . . . 109
3.5.2 Alphabet de diversité 4 à composantes corrélées pour le canal de Rayleigh 112
3.6 Conclusions . . . 115

4 Séquences d'étalement à haute efficacité spectrale : étude de la capacité 117
4.1 Séquences d'étalement corrélées à haute efficacité spectrale . . . 118
4.1.1 Principe de construction . . . 118
4.1.2 Séquences de longueur 2 chips . . . 119
4.1.3 Séquences de longueur 8 chips . . . 121
4.1.4 Généralisation : utilisation des codes sphériques . . . 122
4.2 Familles de séquences orthogonales de longueur N . . . 123
4.2.1 Séquences de Walsh-Hadamard . . . 123
4.2.2 Séquences orthogonales complexes . . . 124
4.3 Famille de séquences non orthogonales de longueur N . . . 127

4.3.1 Séquences construites à partir de signaux PSK 127
4.3.2 Séquences complexes purement aléatoires 127
4.3.3 Séquences de Marzetta 128
4.4 Evaluation de la capacité 130
4.4.1 Rappels de théorie de l'information 130
4.4.2 Cas général 132
4.4.3 Capacité des séquences orthogonales 134
4.4.4 Capacité des séquences corrélées 137
4.4.5 Résultats numériques 141
4.5 Exemple : décodage itératif de séquences non orthogonales codées 151
4.5.1 Séquences complexes purement aléatoires et code convolutif 153
4.6 Conclusions 156

Conclusions et Perspectives **158**

Bibliographie **160**

Table des figures

1.1 Probabilité d'erreur par bit d'une modulation BFSK orthogonale sur canal gaussien. 12
1.2 Probabilité d'erreur par bit d'une modulation BFSK orthogonale sur canal de Rayleigh. 13
1.3 Probabilité d'erreur par bit d'une modulation Q-FSK orthogonale sur canal gaussien pour différentes valeurs de Q. 14
1.4 Probabilité d'erreur par bit d'une modulation Q-FSK orthogonale sur canal de Rayleigh pour différentes valeurs de Q. 15
1.5 Probabilité d'erreur par bit d'une modulation BFSK sur canal gaussien pour différentes valeurs de la corrélation normalisée μ. 16
1.6 Probabilité d'erreur par bit d'une modulation BFSK sur canal de Rayleigh pour différentes valeurs de la corrélation normalisée μ. 17
1.7 (a) Subdivision du plan temps-fréquence pour les transmissions non cohérentes. (b) Cas particulier des signaux à composantes corrélées, $Q = 8$, $\Delta f_0 = \frac{1}{4T}$ et $W = \frac{2}{T}$. 18
1.8 Performances comparées de deux alphabets de diversité 4 sur canal de Rayleigh : BFSK orthogonale, $\Delta f_0 = 1/T$ et $B_e = 8$, et $M = 8$ signaux corrélés de longueur $N = 4$, $\Delta f_0 = 0.25/T$, $B_e = 2.66$. 29
1.9 Capacité des canaux gaussien et de Rayleigh avec détection cohérente. La distribution en entrée est gaussienne. 30
1.10 Capacité du canal gaussien non cohérent admettant en entrée une modulation 8-FSK. 32
1.11 Capacité du canal de Rayleigh non cohérent à évanouissements indépendants admettant en entrée une modulation 8-FSK. 33
1.12 Capacité du canal de Rayleigh à évanouissements indépendants admettant en entrée l'alphabet $\mathcal{A}$ de 8 signaux multidimensionnels. 33

2.1 Modèle de transmission. Alphabet FSK multidimensionnel codé. 40
2.2 Structure du récepteur avec décodage à maximum de vraisemblance. 43
2.3 Structure du récepteur avec décodage APP. 44
2.4 Partitionnement et étiquetage d'Ungerboeck d'une modulation 8-PSK. 49
2.5 Partitionnement et étiquetage d'Ungerboeck d'une modulation QAM-16. 50
2.6 Schéma de principe d'une modulation codée en treillis en émission. 50
2.7 Empilement cubique à face centrée (vu de côté). 52
2.8 Le réseau hexagonal A_2 et ses paramètres fondamentaux. 56
2.9 Modèle d'un système de transmission incluant un réseau de points. 56
2.10 Partitionnement de profondeur 1 à 4 de la modulation QAM de taille 64. 65
2.11 Codeur cubique du réseau D_4 d'efficacité spectrale 5.5 bits/symbole. 66
2.12 Codeur cubique du réseau E_8 d'efficacité spectrale 5 bits/symbole. 66

2.13 Codeur cubique du réseau Λ_{16} d'efficacité spectrale 4.5 bits/symbole. 67
2.14 Codeur cubique du réseau Λ_{24} d'efficacité spectrale 4 bits/symbole. 67
2.15 Représentation géométrique de l'algorithme de décodage par sphères. 68
2.16 Codeur cubique du réseau E_8 d'efficacité spectrale 3 bits/symbole. 74
2.17 Constellation cubique N-dimensionnelle. 76
2.18 Projection sur l'axe de l'unique composante distincte de S_i et S_j, $f_{i,1} = 3$ et $f_{j,1} = -1$. 77
2.19 Projection sur les axes des deux composantes distinctes de S_i et S_j, $f_{i,1} = 3$, $f_{i,2} = 5$, $f_{j,1} = 1$ et $f_{j,2} = 1$. 79
2.20 Distribution des erreurs pour une modulation 8-FSK pour différentes valeurs de $\Delta f_0 T = 1, 0.75, 0.42, 0.1$ (de haut en bas) et du rapport signal-à-bruit $E_b/N_0 = 0, 4, 8$dB (de gauche à droite). 81
2.21 Performances d'une modulation 8-FSK non codée pour différentes valeurs de l'espacement fréquentiel $\Delta f_0 T = 1.0, 0.5, 0.42, 0.34, 0.25, 0.1$. 82
2.22 Performances d'une modulation 8-FSK codée par une PAM-8 TCM de rendement 2/3, $\Delta f_0 T = 1.0, 0.5, 0.34$ *vs.* 8-FSK non codée, $\Delta f_0 T = 0.5$. 83
2.23 Performances d'une modulation 8-FSK codée par un réseau de points, $\Delta f_0 T = 1.0, 0.5, 0.34$. 84
2.24 Comparaison des différents schémas codés ou non à bande fixe, *vs.* BFSK orthogonale non codée. 85
2.25 Comparaison des différents schémas codés ou non à efficacité spectrale fixe η, *vs.* BFSK orthogonale non codée, 0.5 bits/s/Hz. 86

3.1 Codeurs du code convolutif (37,21). 88
3.2 Décodeur SISO d'un code convolutif $C(N, K)$. 89
3.3 Structure d'un turbo code parallèle à deux niveaux. 91
3.4 Structure d'un turbo code série. 93
3.5 Alphabet FSK multidimensionnel codé, décodage APP simple. 95
3.6 Alphabet FSK multidimensionnel codé, détection itérative et décodage APP. . . . 98
3.7 Représentation de trois types d'étiquetage et des régions de décision pour chacun des 3 bits de la 8-PSK. (a) Gray, (b) Ungerboeck, (c) mixte. 102
3.8 Equivalence entre la 8-PSK et les quatre constellations BPSK due au décodage itératif avec retour d'informations dures. (a) Etiquetage de Gray, (b) étiquetage d'Ungerboeck, (c) étiquetage mixte. 103
3.9 Probabilité d'erreur binaire en fonction du rendement du code R et $R = \Delta f_0 T$. . 104
3.10 Décodage itératif d'un turbo code à partir des deux SISO des codes constituants. 106
3.11 Modulation 8-FSK codée par un turbo code de rendement 1/2 et 1/3, *vs.* modulation 8-FSK non codée. La bande des systèmes est fixe, dans tous les cas $\Delta f_0 T = 1.0$. 108
3.12 Comparaison à 0.375 bits/s/Hz. 8-FSK non codée orthogonale et 8-FSK codée par un turbo code. 109
3.13 Comparaison des différents types de codage : 8-FSK non codée $\Delta f_0 T = 0.5, 0.34$ *vs.* 8-FSK codée par le réseau de Leech, par une TCM 2/3, 64 états et par un turbo code de rendement 2/3, $\Delta f_0 T = 0.34$. 110
3.14 Décodage SISO d'un code convolutif. 110
3.15 Modulation 8-FSK codée par un code convolutif 1/3, $L = 5, 7, 9$, *vs.* modulation 8-FSK codée par une TCM 2/3, $L = 5, 7$. $\Delta f_0 T = 0.5$. 111
3.16 Modulation 8-FSK codée par un code convolutif 2/3, *vs.* modulation 8-FSK codée par une TCM 2/3, $L = 5, 7$. $\Delta f_0 T = 0.34$. 112

3.17 Alphabet $\mathcal{A}_1$ codé et non codé, $\Delta f_0 = 0.25/T$, *vs.* Alphabet $\mathcal{A}_2$ non codé, $\Delta f_0 = 1.0/T$ 113
3.18 Influence des itérations sur le décodage de deux BICM : alphabet $\mathcal{A}_1$ codé, $\Delta f_0 = 0.1875/T$ et 8-FSK codée, $\Delta f_0 = 0.75/T$. Comparaison avec l'alphabet $\mathcal{A}_1$ décodé par l'algorithme de Viterbi, $\Delta f_0 = 0.1875/T$. 114
3.19 Comparaison à même efficacité spectrale 0.166 bits/s/Hz : alphabet $\mathcal{A}_1$ codé, $\Delta f_0 = 0.1875/T$, 8-FSK codée, $\Delta f_0 = 0.75/T$ et BFSK codée, $\Delta f_0 = 1.0/T$. . . . 115
3.20 Comparaison à même bande : alphabet $\mathcal{A}_1$ codé, $Be = 6$ et 8-FSK codée, $Be = 1.5$, $\Delta f_0 = 0.1875/T$; BFSK codée, $B_e = 6$, $\Delta f_0 = 1.0/T$. 116

4.1 Représentations géométriques des familles 1 (sur le demi cercle) et 2 (sur le cercle).119
4.2 Canal stationnaire, causal et sans mémoire. 130
4.3 Schéma de transmission. 133
4.4 Capacité du canal gaussien en bits/signal pour des alphabets de signaux orthogonaux en entrée. Détection cohérente (gauche) et non cohérente (droite). 142
4.5 Capacité du canal gaussien en bits/s/Hz pour des alphabets de signaux orthogonaux en entrée. Détection cohérente (gauche) et non cohérente (droite). 142
4.6 Capacité du canal de Rayleigh en bits/signal (gauche) et en bits/s/Hz (droite) pour des alphabets de signaux orthogonaux en entrée. Détection non cohérente. . 143
4.7 Capacité du canal gaussien en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux binaires corrélés en entrée. Détection cohérente. 144
4.8 Capacité du canal gaussien non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux de type PSK corrélés de longueur 2, 4 et 8 en entrée. 145
4.9 Capacité du canal de Rayleigh non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux de type PSK corrélés de longueur 2, 4 et 8 en entrée. 146
4.10 Capacité du canal gaussien non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux complexes corrélés de longueur 2, 4 et 8 en entrée. 148
4.11 Capacité du canal de Rayleigh non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux complexes corrélés de longueur 2, 4 et 8 en entrée. 149
4.12 Enveloppe des capacités en bits/s/Hz du canal gaussien non cohérent pour des alphabets de M séquences complexes corrélées de longueur N en entrée. 150
4.13 Enveloppe des capacités en bits/s/Hz du canal de Rayleigh non cohérent pour des alphabets de M séquences complexes corrélées de longueur N en entrée. 150
4.14 Famille codée de séquences non orthogonales : modèle de l'émetteur. 151
4.15 Capacité du canal de Rayleigh non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de séquences complexes corrélées de type Marzetta de longueur 2, 4 et 8 en entrée. 152
4.16 Famille $\mathcal{A}_1$ codée par le code convolutif 16 états C_1 de rendement 2/3. 154
4.17 Famille $\mathcal{A}_1$ codée par le code convolutif 64 états C_2 de rendement 2/3. 155
4.18 Comparaison des comportements des codes C_1 et C_2. 156
4.19 Famille $\mathcal{A}_1$ codée par le code convolutif 16 états C_1 de rendement 1/3. 157
4.20 Famille $\mathcal{A}_1$ codée par le code convolutif 64 états C_2 de rendement 1/3. 157
4.21 Comparaison des comportements des codes C_1 et C_2. 158

Liste des tableaux

2.1 Quelques réseaux de points et leurs paramètres fondamentaux. La dimension N, le nom Λ, la densité Δ, la densité centrée δ ($\log_2(\delta)$ pour $N \geq 32$), le gain γ_{dB} en dB et le coefficient d'erreur $\tau(\Lambda)$. 59
2.2 Exemples de réseaux binaires et leurs formules réelle et complexe. 64

3.1 Codes NRNSC utilisés pour étudier l'influence de l'espacement fréquentiel. 105
3.2 Codes NRNSC utilisés pour le codage d'une modulation 8-FSK corrélée. 111

4.1 Huit séquences d'étalement réelles de 2 chips réparties sur le demi cercle supérieur (famille 1) ou sur le cercle (famille 2). 119
4.2 $|\mu_{i,\ell}|_{i,\ell=1,\ldots,8}$ pour la famille des séquences distribuées sur le demi cercle supérieur. 120
4.3 $|\mu_{i,\ell}|_{i,\ell=1,\ldots,8}$ pour la famille des séquences distribuées sur le cercle. 120
4.4 $|\mu_{i,\ell}|_{i,\ell=1,\ldots,8}$ pour la famille de $M = 8$ séquences complexes construite à partir de la famille 1. 121
4.5 $|\mu_{i,\ell}|_{i,\ell=1,\ldots,8}$ pour la famille de $M = 8$ séquences complexes construite à partir de la famille 2. 122

Liste des abréviations

Pour plus de clarté, la signification d'une abréviation ou d'un acronyme n'est en principe rappelée qu'à sa première apparition dans le texte. Bien souvent, une abréviation existe en français et en anglais. Puisque nous employons toujours la notation la plus usuelle, il est fréquent que le terme anglais soit privilégié, auquel cas nous proposons une traduction.

APP	*A Posteriori* Probability	Probabilité *a posteriori*
ATM	Asynchronous Transfert Mode	Mode de Transfert Asynchrone
AWGN	Additive White Gaussian Noise	Bruit additif blanc gaussien
BFSK	Binary Frequency Shift-Keying	Modulation de fréquence binaire
BICM	Bit Interleaved Coded Modulation	Modulation codée avec entrelacements de bits
BSC	Binary Symmetric Channel	Canal binaire symétrique
CDMA	Code Division Multiple Access	Accès multiple à répartition par codes
CPM	Continuous-Phase Modulation	Modulation à phase continue
D-PSK	Differential Phase Shift-Keying	Modulation de phase différentielle
FB	Forward-Backward (algorithm)	(Algorithme) aller-retour en fréquences
FSK	Frequency Shift-Keying	Modulation de fréquence
MAP	Maximum *A Posteriori*	Maximum *a posteriori*
ML	Maximum Likelihood	Maximum de vraisemblance
NRNSC	Non-Recursive Non-Systematic Convolutional (code)	(Code) convolutif non récursif non systématique
OOK	On-Off Keying (modulation)	(Modulation) par tout ou rien
PAM	Pulse Amplitude Modulation	Modulation d'amplitude en phase
PSK	Phase Shift-Keying	Modulation de phase
QAM	Quadrature Amplitude Modulation	Modulation d'amplitude en quadrature
RSC	Recursive Systematic Convolutional (code)	(Code) convolutif récursif systématique
SISO	Soft-Input Soft-Output (decoder)	(Décodeur) à entrées souples et sorties souples
SNR	Signal-to-Noise Ratio	Rapport signal-à-bruit
TCM	Trellis Coded Modulation	Modulation codée en treillis en temps

Introduction

L'essor du domaine des télécommunications depuis plusieurs années génère continuellement de nouveaux besoins. Les applications récentes et futures – les systèmes d'accès radio aux réseaux ATM (Asynchronous Transfert Mode), les réseaux cellulaires multimédia ou les réseaux sans fil en environnement intérieur (indoor) et extérieur proche (outdoor) par exemple –, se doivent d'être fiables et capables de faire transiter rapidement des volumes importants de données. Elles nécessitent donc une utilisation de plus en plus efficace des ressources disponibles. Les débits binaires des signaux émis sont de l'ordre de quelques centaines à quelques milliers de kbits/s – 150 kbits/s pour le GPRS (General Packet Radio Service), 384 kbits/s pour EDGE (Enhanced Data rates for GSM Evolution) et 2 Mbits/s pour l'UMTS (Universal Mobile Telecommunications System) –. À titre de comparaison, le débit binaire de la norme GSM (Global System for Mobile communications) actuellement utilisée est de 9.6 kbits/s.

Au cours d'une transmission, le signal subit des distorsions : déphasages, atténuations dues aux évanouissements, bruit additif, etc. Lorsque des mécanismes de récupération de la phase, d'estimation de canal ou d'égalisation sont mis en œuvre pour combattre notamment l'interférence entre symboles ou l'effet Doppler, la détection est dite cohérente et toutes les modulations numériques (de phase, d'amplitude ou de fréquence) sont alors envisageables. En contrepartie, le récepteur peut souffrir d'une trop grande complexité ou se révéler peu robuste aux distorsions. En revanche, si aucun mécanisme de récupération de la phase n'est utilisé, la détection est dite non cohérente. Le récepteur ne sera pas en mesure de distinguer une phase aléatoire introduite par le canal d'une phase aléatoire qui provient de l'émetteur. Cette technique, particulièrement robuste face aux conditions difficiles des canaux de transmission, conditionne cependant le choix de la modulation. En effet, hormis l'adaptation de schémas classiques – la D-PSK (Differential Phase Shift Keying) par exemple – ou l'usage des modulations à phase continue (CPM, Continuous Phase Modulation), il existe deux familles de modulations dites non cohérentes : la modulation par tout ou rien (OOK, On-Off Keying) et les signaux orthogonaux, parmi lesquels les modulations de fréquence FSK (Frequency Shift Keying). Bien que très faciles à utiliser, elles présentent le lourd défaut d'être peu efficaces spectralement.

L'ampleur des débits toujours plus importants peut devenir un obstacle à la réalisation de systèmes à détection cohérente. En particulier, les méthodes d'égalisation ou d'estimation de canal sont d'une complexité prohibitive.

Les travaux abordés dans ce document mettent l'accent sur des techniques de transmission avec détection non cohérente et plus particulièrement sur des modulations à haute efficacité spectrale. En pratique, elles ont pour avantage de conduire à une simplicité relative du récepteur qui autorise la réalisation de terminaux à la fois robustes et peu coûteux.

Il a été montré que l'efficacité spectrale des modulations non cohérentes peut être considérablement augmentée à l'aide de signaux multidimensionnels à composantes corrélées [7]. Cette augmentation de l'efficacité spectrale n'est pas obtenue au détriment des performances. Les résultats présentés dans [7] se basent sur le calcul de la probabilité d'erreur par paire de ce type de modulations sur un canal de Rayleigh à évanouissements indépendants. Cependant, aucune méthode de conception d'alphabets n'a été proposée. Ainsi, la recherche et l'étude d'alphabets de signaux corrélés non triviaux tant sur canal gaussien que sur canal de Rayleigh sont ici envisagées.

Le premier chapitre de ce document traite des performances optimales au sens du critère du maximum de vraisemblance (ML, Maximum Likelihood) des modulations FSK. Les principaux éléments nécessaires à leur étude sont rappelés. Suit une modélisation des signaux multidimensionnels à composantes corrélées. La structure du détecteur non cohérent multidimensionnel optimal, ainsi que les expressions des probabilités d'erreur par paire sont établies pour les canaux gaussiens et de Rayleigh. Afin d'obtenir une méthode rigoureuse de conception de constellations multidimensionnelles, nous proposons d'associer les modulations FSK classiques à diverses techniques de codage. Une étude de la capacité complète enfin ces premiers résultats.

Le second chapitre est consacré aux techniques de codage à forte latence. En particulier, les modulations codées en treillis (TCM, Trellis Coded Modulation) [15] et les réseaux de points [26], assimilables à des modulations codées en blocs, sont envisagés. En effet, les constellations multidimensionnelles dérivées de telles méthodes de codage ont toujours fait partie des candidates pertinentes pour une transmission sur les canaux à bruit additif blanc gaussien. La grande densité des réseaux est notamment un paramètre critique affectant les performances du système. Nous proposons un décodage sous-optimal qui associe une démodulation cohérente fondée sur le calcul de probabilités *a posteriori* (APP, *A Posteriori* Probability) et un décodage à entrée souple des modulations codées. Par ailleurs, nous montrons que la densité du réseau influence également les performances lorsque la détection est non cohérente.

À titre de comparaison, des techniques de codage à forte latence sont utilisées dans le chapitre 3. Les modulations FSK sont codées par un code convolutif ou un turbo code parallèle [14]. Une méthode de détection itérative combinée à un décodage APP est proposée. Elle conduit à de meilleurs résultats qu'un décodage APP simple et se révèle particulièrement adaptée au décodage des modulations codées avec entrelacement de bits (BICM, Bit Interleaved Coded Modulation) ainsi conçues.

Finalement, nous choisissons dans le chapitre 4 de ne pas nous restreindre à des modulations sous-jacentes de type FSK. Pour cela, nous construisons des familles de séquences d'étalement complexes corrélées. Une étude précise de la capacité montre que sur canal gaussien ou sur canal de Rayleigh à évanouissements par blocs, l'utilisation de tels alphabets permet de tendre, avec un système non cohérent, vers les performances obtenues en détection cohérente.

Les résultats importants établis au cours de cette étude et les perspectives de travaux futurs sont rassemblés dans le dernier chapitre.

Chapitre 1

Performances optimales ML des modulations Q-FSK *

La détection non cohérente est en général utilisée pour faire face à des conditions de transmission difficiles pour lesquelles une récupération de la phase s'avère complexe et coûteuse. Le choix de ce type de détection, qui consiste à ne s'intéresser qu'au module du signal reçu, conduit par conséquent à l'utilisation exclusive de modulations numériques pour lesquelles aucune information utile n'est transmise sur la phase du signal modulant.

Les familles de modulations numériques qui répondent à ce critère sont au nombre de deux : la modulation OOK et les signaux orthogonaux. Ces modulations non cohérentes sont très faciles à mettre en œuvre mais leur principal défaut réside dans leur faible efficacité spectrale.

La première partie de ce chapitre est consacrée à l'étude des modulations de fréquence Q-FSK, cas particulier des signaux orthogonaux, sur canal à bruit additif blanc gaussien (AWGN, Additive White Gaussian Noise) et sur canal de Rayleigh. Ainsi, nous rappelons leur principe de construction, la structure du détecteur optimal selon le critère du maximum de vraisemblance et leurs performances.

Puis nous nous intéressons à la construction de constellations multidimensionnelles à composantes corrélées, initialement proposées par [7]. Ces dernières sont caractérisées par des composantes de même amplitude et corrélées ; en effet, l'espacement fréquentiel des porteuses est inférieur à celui qui garantit l'orthogonalité. Nous donnons la structure du détecteur optimal et les expressions des probabilités d'erreur par paire pour les deux types de canaux envisagés.

Enfin, nous proposons une étude de la capacité du canal gaussien et de Rayleigh avec détection non cohérente lorsque de tels signaux sont utilisés.

*Une partie de ce chapitre a été présentée au *2000 International Symposium on Information Theory*, Sorrento, Italie, juin 2000.

1.1 Modulation de fréquence Q-FSK

1.1.1 Principe de la modulation

On note $(b_1, b_2, \dots)$ la séquence de bits d'information en entrée du canal de transmission. La modulation, qui est non linéaire et sans mémoire, est constituée d'un alphabet de $Q = 2^k$ signaux, $\{s_0(t), \dots, s_{Q-1}(t)\}$. En bande de base, le signal $s_q(t)$ d'énergie $2E$ et de durée T s'écrit

$$s_q(t) = \sqrt{\frac{2E}{T}} e^{j2\pi f_q t} \quad q = 0, \dots, Q-1 \quad 0 \leq t \leq T$$

La fréquence f_q prend Q valeurs possibles uniformément espacées de Δf_0, l'espacement fréquentiel élémentaire de la modulation FSK. De manière équivalente, on aura $f_q = q \times \Delta f_0$ où $q \in \{0, \dots, Q-1\}$, ou bien $f_q = p_q \times \frac{\Delta f_0}{2}$ où p_q est un entier choisi dans l'ensemble $\{\pm 1, \dots, \pm(Q-1)\}$. Chaque groupe de $k = \log_2(Q)$ bits de la séquence $(b_1, b_2, \dots)$ sélectionne une fréquence parmi les Q possibles, sur laquelle l'émission a lieu.

On définit $\mu_{i,\ell}$ le coefficient d'intercorrélation (ou corrélation) entre les signaux i et ℓ de la modulation par

$$\mu_{i,\ell} = \int_0^T s_i(t) s_\ell^*(t) dt = \frac{2E}{T} \int_0^T e^{j2\pi(f_i - f_\ell)t} dt \tag{1.1}$$

Avec la convention $f_q = q \times \Delta f_0$, on obtient l'expression suivante pour $\mu_{i,\ell}$

$$\mu_{i,\ell} = 2E \times \frac{sin(\pi(i-\ell)\Delta f_0 T)}{\pi(i-\ell)\Delta f_0 T} \times e^{j\pi(i-\ell)\Delta f_0 T}$$

La partie réelle et le module de $\mu_{i,\ell}$ sont donnés par

$$\begin{aligned} Re(\mu_{i,\ell}) &= 2E \times \frac{sin(\pi(i-\ell)\Delta f_0 T)}{\pi(i-\ell)\Delta f_0 T} \times cos(\pi(i-\ell)\Delta f_0 T) \\ &= 2E \times \frac{sin(2\pi(i-\ell)\Delta f_0 T)}{2\pi(i-\ell)\Delta f_0 T} \end{aligned} \tag{1.2}$$

et

$$|\mu_{i,\ell}| = 2E \times \left| \frac{sin(\pi(i-\ell)\Delta f_0 T)}{\pi(i-\ell)\Delta f_0 T} \right| \tag{1.3}$$

Grâce à l'expression (1.2), nous observons tout d'abord que $Re(\mu_{i,\ell}) = 0$ quand $\Delta f_0 = \frac{1}{2T}$ et $i \neq \ell$. Puisque la condition $|i-\ell| = 1$ est vérifiée pour des signaux adjacents, $\Delta f_0 = \frac{1}{2T}$ représente l'espacement fréquentiel minimal qui garantit l'orthogonalité des signaux.

Par ailleurs, on remarquera que $Re(\mu_{i,\ell})$ est nulle pour Δf_0 multiple de $\frac{1}{2T}$ alors que $|\mu_{i,\ell}|$ l'est pour Δf_0 multiple de $\frac{1}{T}$. Si la détection est cohérente, les signaux seront par conséquent orthogonaux avec un écart fréquentiel minimum de $\frac{1}{2T}$, alors que si la détection est non cohérente, un écart fréquentiel minimum de $\frac{1}{T}$ sera nécessaire.

1.1.2 Détection non cohérente optimale à maximum de vraisemblance

En supposant que le signal $s_q(t)$ a été émis, on reçoit

$$r(t) = \alpha e^{j\phi_q} s_q(t) + b(t)$$

où $b(t)$ est un bruit additif blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle ; α est le gain du canal, et ϕ_q une phase aléatoire uniformément répartie sur $[0, 2\pi]$. Pour le canal gaussien, α est une constante. Pour le canal à évanouissements, α suit une loi de Rayleigh ; $p(\alpha) = 2\alpha e^{-\alpha^2}$ et $E[\alpha^2] = 1$.

Nous recherchons le détecteur non cohérent optimal, c'est-à-dire celui capable de fournir, à partir de la seule observation du signal reçu $r(t)$, une décision quant au signal émis qui maximise la probabilité de décision correcte. On note $P(s_q|r)$ la probabilité *a posteriori* du signal $s_q(t)$ et $p(r|s_q)$ la vraisemblance. Ces deux quantités sont reliées par la loi de Bayes [57]

$$P(s_q|r) = \frac{p(r|s_q)P(s_q)}{p(r)} \tag{1.4}$$

où les $P(s_q)$ sont les probabilités *a priori* des signaux $s_q(t)$ et $p(r)$ la densité de probabilité de l'observation $r(t)$.

Si une décision est prise en faveur du signal qui correspond à la plus grande probabilité *a posteriori* $P(s_q|r)$, on parle de détection maximum *a posteriori* (MAP, Maximum *A Posteriori*). Si le signal choisi maximise $p(r|s_q)$, il s'agit d'une détection à maximum de vraisemblance. Nous considérons ici le cas de signaux équiprobables, c'est-à-dire $P(s_q) = \frac{1}{Q}$ pour $q = 0, \ldots, Q-1$; par conséquent, les deux critères de détection sont parfaitement équivalents.

Détecteur optimal sur le canal gaussien

La structure du détecteur optimal sur canal gaussien est connue : nous rappelons dans l'Annexe 1.I de ce chapitre les résultats de [56], Annexe 4.C. Le critère de détection non cohérente optimal est donné par

$$\max_{q=0}^{Q-1} \left| \int_0^T r(t) s_q^*(t) dt \right| \tag{1.5}$$

L'équation (1.5) fournit la structure du détecteur non cohérent optimal ML sur canal gaussien. Il consiste en un banc de Q filtres adaptés à chacune des fréquences de la modulation Q-FSK. Chaque filtre est suivi d'un détecteur d'enveloppe qui justifie l'appellation de détection non cohérente. On choisit ensuite le signal correspondant à l'enveloppe maximale.

Détecteur optimal sur le canal de Rayleigh

La structure du détecteur non cohérent optimal sur canal de Rayleigh est également connue. La démonstration est similaire à celle effectuée pour le canal gaussien. Remarquons que l'équation

(1.57) de l'Annexe 1.I fournit une expression de la densité de probabilité du vecteur $\mathbf{r}_K$ conditionnellement au signal q et à une valeur fixée de l'évanouissement α. Nous la notons $p(\mathbf{r}_K|q,\alpha)$. La loi de α est connue, alors,

$$\begin{aligned}
p(\mathbf{r}_K|q) &= \int_0^\infty p(\mathbf{r}_K|q,\alpha)p(\alpha)d\alpha \\
p(\mathbf{r}_K|q) &= \left(\prod_{k=1}^{K} 2\pi\sigma^2\right) \exp\left(-\sum_{k=1}^{K}\frac{|r_k|^2}{2\sigma^2}\right) \\
&\quad \times \int_0^\infty 2\alpha \exp\left(-\alpha^2\left[1+\sum_{k=1}^{K}\frac{|s_{q,k}|^2}{2\sigma^2}\right]\right) I_0\left(\alpha\left|\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right|\right)d\alpha \qquad (1.6)
\end{aligned}$$

r_k et $s_{q,k}$ sont les $k$ième composantes des développements de Karhunen-Loève de $r(t)$ et $s_q(t)$ respectivement.

L'intégrale ci-dessus est connue et donnée par

$$\int_0^\infty x\exp(-a^2x^2)I_0(bx)dx = \frac{1}{2a^2}\exp\left(\frac{b^2}{4a^2}\right) \qquad (1.7)$$

Notons qu'une expression plus générale de cette intégrale est donnée dans [41] :

$$\int_0^\infty t^{\mu-1}I_\nu(\alpha t)e^{-p^2t^2}dt = \frac{\Gamma\left(\frac{\mu+\nu}{2}\right)\left(\frac{\alpha}{2p}\right)^\nu}{2p^\mu\Gamma(\nu+1)}\exp\left(\frac{\alpha^2}{4p^2}\,{}_1F_1\left(\frac{\nu-\mu}{2}+1,\nu+1;-\frac{\alpha^2}{4p^2}\right)\right)$$

En considérant $\mu=2$, $\nu=0$ et en remarquant que ${}_1F_1(0,1;x)=1$, on obtient (1.7).

En combinant (1.7) et (1.6), on trouve

$$p(\mathbf{r}_K|q) = \frac{\left(\prod_{k=1}^K 2\pi\sigma^2\right)}{1+\sum_{k=1}^K\frac{|s_{q,k}|^2}{2\sigma^2}}\exp\left(-\sum_{k=1}^K\frac{|r_k|^2}{2\sigma^2}\right)\exp\left\{\frac{\left|\sum_{k=1}^K\frac{r_k s_{q,k}^*}{\sigma^2}\right|^2}{4+\sum_{k=1}^K\frac{2|s_{q,k}|^2}{\sigma^2}}\right\} \qquad (1.8)$$

On procède ensuite de la même manière que pour le canal gaussien en substituant (1.8) à (1.57) (Annexe 1.I). En supposant toujours que le bruit additif est blanc gaussien et que les signaux sont équiprobables et de même énergie, les nouvelles expressions des variables de décision sont

$$L_q = \exp\left\{\frac{\left|\int_0^T s_q(t)g_q^*(t)dt\right|^2}{2N_0(2+E)}\right\} \qquad q=0,\ldots,Q-1$$

La fonction exponentielle étant monotone croissante sur $[0,+\infty[$, le critère de détection optimal est le suivant

$$\max_{q=0}^{Q-1}\left|\int_0^T r(t)s_q^*(t)dt\right|^2 \qquad (1.9)$$

On retrouve la structure classique et connue en détection cohérente du détecteur d'enveloppe. La mise en œuvre pratique est similaire au cas du canal gaussien.

1.1.3 Expression de la probabilité d'erreur

Nous venons de voir que le détecteur non cohérent optimal dans le cas de la transmission de signaux Q-aires, c'est-à-dire d'une modulation Q-FSK, est constitué d'un banc de filtres adaptés suivi d'un détecteur d'enveloppe ; ce résultat est valable pour les canaux gaussien et de Rayleigh. Aucune hypothèse particulière quant à l'orthogonalité des signaux n'a été émise : le détecteur est le même que les signaux soient corrélés ($\Delta f_0 < \frac{1}{T}$) ou non ($\Delta f_0 = \frac{1}{T}$).

Nous rappelons maintenant les expressions de la probabilité d'erreur d'une modulation Q-FSK selon que les signaux sont orthogonaux ou non sur canal gaussien et sur canal de Rayleigh.

Signaux orthogonaux sur le canal gaussien

En supposant que le signal $s_0(t)$ a été émis, le signal reçu s'écrit $r(t) = \alpha e^{j\phi_0} s_0(t) + b(t)$. La variable de décision L_0 s'écrit

$$L_0 = \left| \int_0^T r(t) s_0^*(t) dt \right| = \left| 2\alpha e^{j\phi_0} E + b_0 \right|$$

Par orthogonalité des signaux, les autres variables L_q, $q = 1, \ldots, Q-1$ sont constituées d'un terme de bruit uniquement

$$L_q = \left| \int_0^T r(t) s_q^*(t) dt \right| = |b_q|$$

où $b_q = \int_0^T b(t) s_q^*(t) dt$, $q = 0, \ldots, Q-1$ est une variable aléatoire gaussienne complexe de moyenne nulle et de variance par composante réelle $2E\sigma^2 = 2EN_0$. Toujours grâce à l'orthogonalité des signaux, les variables aléatoires b_q sont décorrélées et statistiquement indépendantes.

Ainsi, en tant que module d'une variable aléatoire gaussienne complexe non centrée de variance $2EN_0$, L_0 suit une loi de Rice de paramètre $4\alpha^2 E^2$, tandis que les L_q, $q = 1, \ldots, Q-1$ suivent une loi de Rayleigh (modules de variables aléatoires gaussiennes complexes centrées de variance $2EN_0$) :

$$\begin{aligned} p(\ell_0) &= \frac{\ell_0}{2EN_0} e^{-\frac{\ell_0^2 + 4\alpha^2 E^2}{4EN_0}} I_0\left(\frac{\alpha \ell_0}{N_0}\right) \\ p(\ell_q) &= \frac{\ell_q}{2EN_0} e^{-\frac{\ell_q^2}{4EN_0}} \quad q = 1, \ldots, Q-1 \end{aligned}$$

La probabilité de décision correcte est la probabilité que la variable L_0 soit supérieure à toutes les autres

$$\begin{aligned} P_c &= P(L_1 < L_0, L_2 < L_0, \ldots, L_{Q-1} < L_0) \\ &= \int_0^\infty P(L_1 < L_0, L_2 < L_0, \ldots, L_{Q-1} < L_0 | L_0 = \ell_0) p(\ell_0) d\ell_0 \end{aligned} \tag{1.10}$$

Les variables de décision L_q, $q = 1, \ldots, Q-1$ sont décorrélées, statistiquement indépendantes et ont toutes même densité de probabilité. Alors, la densité de probabilité conjointe conditionnellement à L_0 se factorise en un produit de $Q-1$ termes identiques. L'équation (1.10) devient

$$P_c = \int_0^\infty [P(L_1 < L_0|L_0 = \ell_0)]^{Q-1} p(\ell_0) d\ell_0 \tag{1.11}$$

Calculons $P(L_1 < L_0|L_0 = \ell_0)$.

$$\begin{aligned} P(L_1 < L_0|L_0 = \ell_0) &= \int_0^{\ell_0} p(\ell_1) d\ell_1 \\ &= 1 - e^{-\frac{\ell_0^2}{4EN_0}} \end{aligned} \tag{1.12}$$

Elevée à la puissance $Q-1$, l'expression (1.12) peut se mettre sous la forme

$$(1 - e^{-\frac{\ell_0^2}{4EN_0}})^{Q-1} = \sum_{n=0}^{Q-1} (-1)^n C_{Q-1}^n e^{-\frac{n\ell_0^2}{4EN_0}} \tag{1.13}$$

En reportant (1.13) dans (1.11) et en notant $\gamma = \frac{\alpha^2 E}{N_0}$ le rapport signal-à-bruit, on trouve

$$P_c = \sum_{n=0}^{Q-1} (-1)^n C_{Q-1}^n \frac{e^{-\gamma}}{2EN_0} \int_0^\infty \ell_0 e^{-\frac{\ell_0^2(n+1)}{4EN_0}} I_0\left(\frac{\alpha \ell_0}{N_0}\right) d\ell_0 \tag{1.14}$$

Le résultat de l'équation (1.7) nous permet de calculer l'intégrale dans (1.14)

$$\int_0^\infty \ell_0 e^{-\frac{\ell_0^2(n+1)}{4EN_0}} I_0\left(\frac{\alpha \ell_0}{N_0}\right) d\ell_0 = \frac{2EN_0}{n+1} \exp\left(\frac{\gamma}{n+1}\right) \tag{1.15}$$

Finalement,

$$P_c = \sum_{n=0}^{Q-1} (-1)^n C_{Q-1}^n \frac{1}{n+1} e^{-\frac{\gamma n}{n+1}} \tag{1.16}$$

La probabilité d'erreur par symbole est alors donnée par $P_s = 1 - P_c$, soit

$$P_s = \sum_{n=1}^{Q-1} (-1)^{n+1} C_{Q-1}^n \frac{1}{n+1} e^{-\frac{\gamma n}{n+1}} \tag{1.17}$$

Dans le cas d'une modulation de fréquence de taille $Q = 2$, (BFSK, Binary Frequency Shift-Keying), les probabilités d'erreur par symbole et par bit sont confondues et le rapport signal-à-bruit γ est égal au rapport signal-à-bruit par bit $\gamma_b = \frac{\alpha^2 E_b}{N_0}$. E_b est l'énergie moyenne par bit. Pour un canal gaussien de gain α, l'équation (1.17) devient

$$P_b = \frac{1}{2} e^{-\frac{\alpha^2 E_b}{2N_0}} \tag{1.18}$$

Nous avons vu au paragraphe 1.1.1 que chaque signal est étiqueté par un groupe de $k = \log_2(Q)$ bits. Dans le cas de Q signaux orthogonaux équiprobables, tous les symboles de la modulation sont choisis avec la même probabilité. Par ailleurs, il y a C_k^n possibilités d'avoir n bits erronés parmi k. Le nombre moyen de bits erronés pour un symbole étiqueté par k bits est donc

$$\sum_{n=1}^{k} C_k^n \frac{P_s}{2^k - 1} = k \frac{2^{k-1}}{2^k - 1} P_s$$

La probabilité d'erreur par bit moyenne P_b est donnée par le nombre moyen de bits erronés divisé par le nombre total de bits k. Pour $Q > 2$ signaux, on obtient l'expression de P_b en fonction de P_s suivante [57]

$$P_b = \frac{2^{k-1}}{2^k - 1} P_s \simeq \frac{P_s}{2} \quad \text{pour} \quad k >> 1 \tag{1.19}$$

Signaux non orthogonaux sur le canal gaussien

Nous commençons par donner la probabilité d'erreur par bit d'une modulation BFSK non orthogonale. On note μ la corrélation normalisée entre les deux signaux de la modulation

$$\mu = \frac{\mu_{0,1}}{2E} = \frac{1}{2E} \int_0^T s_0(t) s_1^*(t) dt \tag{1.20}$$

L'hypothèse d'émission du signal $s_0(t)$ reste valable, *i.e.* $r(t) = \alpha e^{j\phi_0} s_0(t) + b(t)$. Les deux variables de décision L_0 et L_1 s'écrivent

$$\begin{aligned} L_0 &= \left| 2\alpha E e^{j\phi_0} + b_0 \right| \\ L_1 &= \left| 2\alpha E \mu e^{j\phi_0} + b_1 \right| \end{aligned}$$

où $b_q = \int_0^T b(t) s_q^*(t) dt$, $q = 0, 1$, est une variable aléatoire gaussienne complexe de moyenne nulle et de variance $2E\sigma^2 = 2EN_0$. L_0 et L_1 suivent une loi de Rice de paramètres respectifs $4\alpha^2 E^2$ et $4\alpha^2 E^2 |\mu|^2$

$$\begin{aligned} p(\ell_0) &= \frac{\ell_0}{2EN_0} e^{-\frac{\ell_0^2 + 4\alpha^2 E^2}{4EN_0}} I_0\left(\frac{\alpha \ell_0}{N_0}\right) \\ p(\ell_1) &= \frac{\ell_1}{2EN_0} e^{-\frac{\ell_1^2 + 4\alpha^2 E^2 |\mu|^2}{4EN_0}} I_0\left(\frac{\alpha |\mu| \ell_1}{N_0}\right) \end{aligned}$$

Deux approches permettent de calculer la probabilité d'erreur par bit $P_b = P(L1 > L0)$. La première méthode consiste à évaluer la densité de probabilité conjointe de L_0 et L_1 [42]. Pour la seconde méthode, il faut remarquer que $P_b = P(L1 > L0) = P(L_0^2 - L_1^2 < 0)$. $L_0^2 - L_1^2 = D$ est un cas particulier de la forme quadratique générale de variables aléatoires complexes définie et évaluée dans [56], annexe 4.B. L'utilisation de ces résultats conduit à une expression de la probabilité d'erreur par bit d'une modulation BFSK non orthogonale

$$P_b = Q(a, b) - \frac{1}{2} e^{-\frac{(a^2 + b^2)}{2}} I_0(ab) \tag{1.21}$$

avec

$$\begin{aligned} a &= \sqrt{\frac{E_b}{2N_0}\left(1-\sqrt{1-|\mu|^2}\right)} \\ b &= \sqrt{\frac{E_b}{2N_0}\left(1+\sqrt{1-|\mu|^2}\right)} \end{aligned}$$

$Q(a,b)$ est la fonction de Marcum généralisée définie par $Q(a,b) \triangleq e^{-\frac{(a^2+b^2)}{2}} \sum_{k=0}^{\infty} \left(\frac{a}{b}\right)^k I_k(ab)$ pour $b > a > 0$.

Passons maintenant au cas général de Q signaux corrélées. Les variables de décision L_q sont données par

$$\begin{aligned} L_0 &= \left|2\alpha E e^{j\phi_0} + b_0\right| \\ L_q &= \left|2\alpha E \mu_{0,q} e^{j\phi_0} + b_q\right| \quad q = 1, \ldots, Q-1 \end{aligned}$$

$\mu_{0,q}$ est toujours la corrélation normalisée entre les signaux 0 et q.

La définition de la probabilité de décision correcte donnée par l'équation (1.10) reste valable. En raison de la non orthogonalité des signaux, les variables aléatoires gaussiennes complexes b_q, et les variables de décision L_q sont maintenant corrélées et statistiquement dépendantes. Il faut alors évaluer la densité de probabilité conjointe de Q variables de Rice corrélées. Il n'existe pas de solution simple à ce calcul. Dans [65], le cas particulier de Q signaux équicorrélés est considéré. Les travaux présentés dans [53] et [52] ont montré de manière heuristique que la probabilité d'erreur est minimale si l'on suppose que la corrélation normalisée $\mu_{i,j}$ est réelle et constante $\forall j \neq i$, c'est-à-dire

$$\mu_{i,j} = \begin{cases} 1 & i = j \\ \mu & i \neq j \text{ et } \mu \text{ réelle positive} \end{cases}$$

Dans ces conditions, la probabilité de décision correcte s'écrit [53]

$$\begin{aligned} P_c &= (1-\mu)\exp\left(\frac{E}{N_0}\right)\int_0^{\infty}\int_0^{\infty} xy\exp\left(-\frac{1}{2}(x^2+y^2)\right) \\ &\quad \times I_0\left(\sqrt{\frac{2E}{N_0}(1-\mu)}x\right) I_0(\sqrt{\mu}xy)[1-Q(\sqrt{\mu}y,x)]^{Q-1}dxdy \end{aligned} \tag{1.22}$$

Remarquons que pour $\mu = 0$ ou $\{\mu = 0$ et $Q = 2\}$, l'équation (1.22) permet de retrouver les formules (1.16) et (1.21) [65].

Signaux orthogonaux sur le canal de Rayleigh

Une fois encore, nous commençons par le cas de la BFSK. Une manière simple d'évaluer la probabilité d'erreur par bit de cette modulation sur canal de Rayleigh avec détection non cohérente est d'utiliser la formule (1.18). En effet, ce calcul fournit une expression de la probabilité d'erreur pour un gain du canal α fixé. (1.18) est alors l'expression de la probabilité d'erreur conditionnellement à une valeur fixée de α que nous notons $P_b(\alpha)$. Il suffit de moyenner cette dernière par rapport à α pour obtenir la probabilité d'erreur P_b. On a

$$P_b = \int_0^\infty P_b(\alpha) p(\alpha) d\alpha \tag{1.23}$$

Le gain du canal α suit une loi de Rayleigh, $p(\alpha) = 2\alpha e^{-\alpha^2}$, avec $E[\alpha^2] = 1$. En combinant (1.18) et (1.23), on obtient facilement

$$P_b = \frac{1}{2 + \frac{E_b}{N_0}} \tag{1.24}$$

On peut procéder de la même manière pour Q signaux à partir du résultat (1.17) que nous notons $P_s(\alpha)$. Alors

$$P_s = \int_0^\infty P_s(\alpha) p(\alpha) d\alpha$$

Le calcul qui se fait aisément donne [65]

$$P_s = \sum_{n=1}^{Q-1} C_{Q-1}^n \frac{(-1)^{n+1}}{n + 1 + n\frac{E}{N_0}} \tag{1.25}$$

On remarquera que dans les expressions (1.24) et (1.25), la probabilité d'erreur n'est plus inversement exponentielle en fonction du rapport signal-à-bruit, comme c'était le cas pour le canal gaussien. Ici, elle est une fonction de l'inverse de $\frac{E}{N_0}$. Cela signifie que pour transmettre sur un canal à évanouissements avec une probabilité d'erreur relativement faible, l'émetteur devra fournir une puissance plus importante que celle nécessaire sur canal gaussien. Pour un grand nombre d'applications, cette contrainte est prohibitive. On peut s'en affranchir grâce à l'utilisation de techniques de diversité qui introduisent une redondance au niveau du canal. Selon la nature des évanouissements, des techniques de diversité temporelle, fréquentielle ou spatiale peuvent être envisagées [65].

Signaux non orthogonaux sur le canal de Rayleigh

On trouve dans la littérature un certain nombre de résultats concernant le cas de signaux non orthogonaux sur le canal de Rayleigh. En particulier, Turin [67] a traité le cas de deux signaux corrélés, $Q = 2$. La probabilité d'erreur correspondante s'écrit

$$P_b = \frac{1}{2}\left(1 - \frac{\beta\sqrt{1 - |\mu|^2}}{\sqrt{1 - \beta^2|\mu|^2}}\right) \tag{1.26}$$

où μ est la corrélation normalisée définie par (1.20) et

$$\beta \triangleq \frac{(E_b/N_0)}{(E_b/N_0) + 2}$$

Pour un nombre de signaux plus grand que deux, les calculs sont relativement complexes, c'est pourquoi nous ne les rapportons pas dans ce paragraphe.

1.1.4 Performances sur différents canaux

Les différents développements que nous venons de rappeler permettent d'illustrer les performances des modulations de fréquence sur le canal gaussien et sur le canal de Rayleigh.

Les figures 1.1 et 1.2 sont consacrées aux performances de la modulation de fréquence orthogonale de taille 2, BFSK, sur chacun de ces deux canaux. Les probabilités d'erreur par bit en détection non cohérente sont comparées à celles obtenues avec détection cohérente. Les expressions de P_b pour une détection cohérente sont données par [57]

$$P_b(\text{AWGN}) = Q\left(\sqrt{\frac{\alpha^2 E_b}{N_0}}\right) \quad \text{et} \quad P_b(\text{Rayleigh}) = \frac{1}{2}\left(1 - \sqrt{\frac{\frac{E_b}{N_0}}{1+\frac{E_b}{N_0}}}\right)$$

Rappelons que la fonction $Q(x)$ est définie par

$$Q(x) \triangleq \int_x^{\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{y^2}{2}\right) dy \tag{1.27}$$

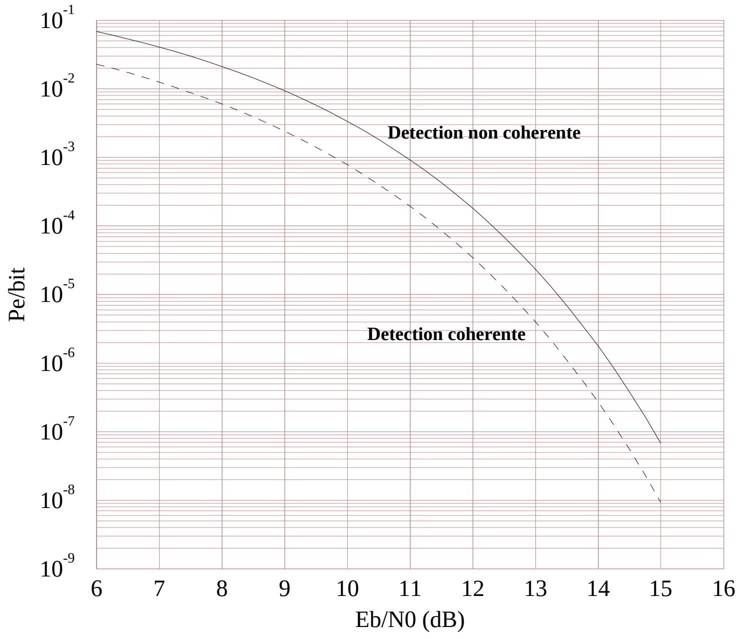


FIG. 1.1 – Probabilité d'erreur par bit d'une modulation BFSK orthogonale sur canal gaussien.

Si la détection non cohérente conduit à une dégradation des performances de 0.75 dB seulement sur canal gaussien pour une probabilité d'erreur par bit $P_b = 10^{-6}$, elle a un impact

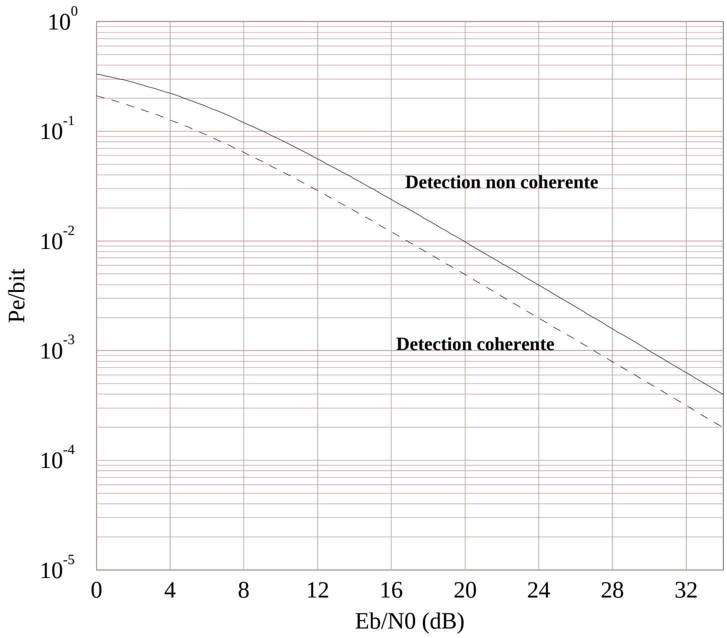


FIG. 1.2 – Probabilité d'erreur par bit d'une modulation BFSK orthogonale sur canal de Rayleigh.

beaucoup plus important sur le canal de Rayleigh : environ 3 dB de perte pour une probabilité d'erreur $P_b = 10^{-3}$.

En contrepartie, les figures 1.3 et 1.4 prouvent que si l'on augmente la taille de l'alphabet Q-FSK, on améliore les performances. Sur canal gaussien, cette amélioration est même considérable pour des valeurs relativement faibles de Q : $Q = 16, 32$. Il a notamment été montré que pour $Q \to \infty$ sur le canal gaussien, on pourra toujours rendre la probabilité d'erreur P_b arbitrairement petite, à condition de travailler avec un rapport signal-à-bruit supérieur à la valeur limite -1.6 dB donnée par Shannon [57]. Malheureusement, augmenter Q revient à une utilisation toujours plus importante de la bande dans le cas de signaux orthogonaux, et donc à une efficacité spectrale moindre.

Une solution consiste à accepter un écart fréquentiel élémentaire inférieur à celui garantissant l'orthogonalité. Les figures 1.5 et 1.6 illustrent l'effet néfaste de la corrélation sur les performances d'une modulation BFSK sur canal gaussien et de Rayleigh. Un écart fréquentiel $\Delta f_0 = \frac{0.5}{T}$, qui correspond à un coefficient de corrélation $\mu = 0.6$, conduit ainsi à une perte de 3.5 dB pour un taux d'erreur de 10^{-6} sur canal gaussien et de 2 dB pour un taux d'erreur de 2×10^{-3} sur canal de Rayleigh. S'il est clair que le principal défaut des modulations de fréquence Q-FSK réside dans leur faible efficacité spectrale, on constate que l'utilisation de fréquences corrélées dans le cas d'une modulation monodimensionnelle (c'est-à-dire une Q-FSK classique) aggrave les performances.

La conception de modulations multidimensionnelles à partir de signaux corrélés permet d'augmenter l'efficacité spectrale [7] tout en compensant cette dégradation des performances. Forts des

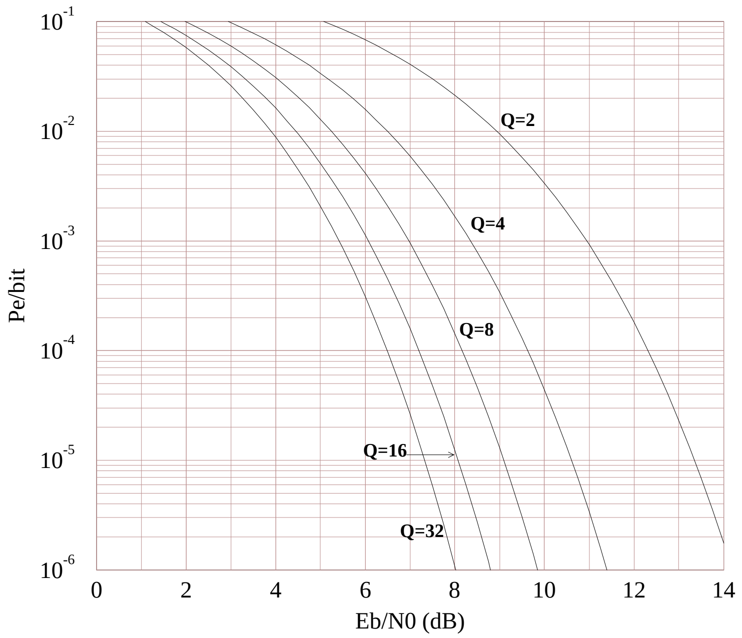


Fig. 1.3 – Probabilité d'erreur par bit d'une modulation Q-FSK orthogonale sur canal gaussien pour différentes valeurs de Q.

résultats connus sur les modulations Q-FSK classiques, nous proposons d'étudier plus en détails ces constructions multidimensionnelles.

1.2 Constellations multidimensionnelles à composantes corrélées

Dans les travaux de [7], deux méthodes sont envisagées : une généralisation de la modulation OOK et une construction de signaux multidimensionnels à composantes corrélées à partir de modulations Q-FSK, solution à laquelle nous nous intéressons ici.

La modélisation présentée dans ce paragraphe permet l'étude de toute transmission de signaux multidimensionnels. On pourra notamment considérer toute méthode de codage ou de diversité comme un cas particulier.

1.2.1 Principe et intérêt des signaux corrélés

Le plan temps-fréquence est divisé en cases rectangulaires de durée T et de largeur de bande W (figure 1.7(a)). Le principe est le suivant : chaque signal est émis dans une case élémentaire du plan temps-fréquence, c'est-à-dire pendant une durée T et à une fréquence donnée. Les signaux successifs ne sont pas nécessairement émis dans des cases adjacentes en temps et/ou en

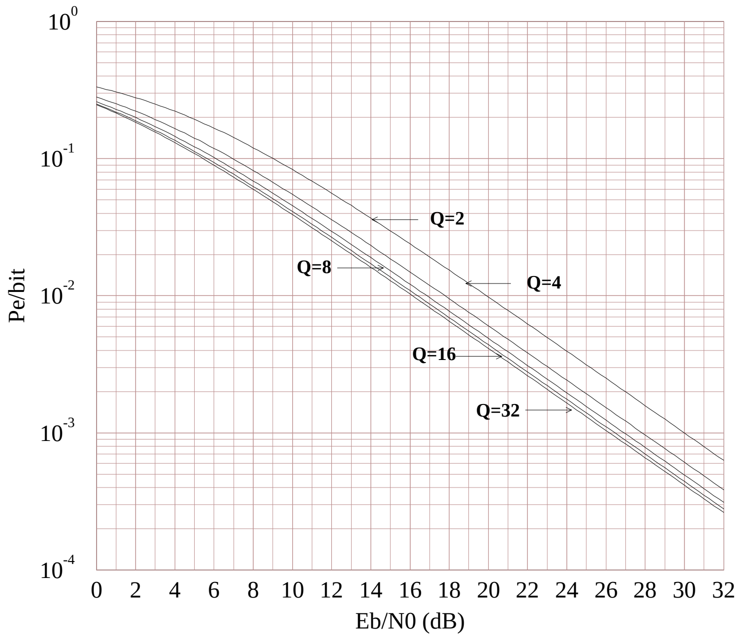


FIG. 1.4 – Probabilité d'erreur par bit d'une modulation Q-FSK orthogonale sur canal de Rayleigh pour différentes valeurs de Q.

fréquence. En particulier, lors d'une émission en diversité, on veillera à utiliser un espacement des cases en temps et/ou en fréquence supérieur au temps et/ou à la bande de cohérence du canal. Une conséquence directe de cette précaution est l'indépendance des évanouissements d'une composante à l'autre. Enfin, notons que les différentes composantes d'un signal multidimensionnel seront émises successivement en temps ou parallèlement sur plusieurs fréquences.

Afin d'assurer l'orthogonalité des signaux lorsque la détection est non cohérente, il est commun de considérer une bande W égale à $\frac{1}{T}$ et d'utiliser des filtres d'émission rectangulaires. Dans chaque case élémentaire, une unique fréquence est disponible. On obtient ainsi le réseau temps-fréquence le plus dense dans un contexte de signaux orthogonaux avec une efficacité spectrale de une composante/s/Hz.

Le principe des constellations multidimensionnelles à composantes corrélées est schématisé figure 1.7(b). Nous ne disposons plus uniquement d'une fréquence mais de Q fréquences différentes dans chaque case. De plus, l'espacement Δf_0 entre les fréquences est inférieur à celui garantissant l'orthogonalité ($Q = 8$ et $\Delta f_0 = \frac{1}{4T}$ sur cette figure). On émet toujours une seule fréquence par case, mais le fait d'avoir le choix parmi plusieurs augmente l'efficacité spectrale du système. Considérons par exemple une bande $W = \frac{2}{T}$ et des signaux à une seule dimension : une seule case élémentaire du plan est utilisée. Avec une modulation 8-FSK identique à celle de la figure 1.7(b), il faut trois bits pour choisir un signal. Cela conduit à une efficacité spectrale de 1.5 bits/s/Hz. En comparaison, une BFSK orthogonale utilise la même bande, mais un bit suffit à choisir un signal de la modulation. Dans ce cas, l'efficacité spectrale est de 0.5 bits/s/Hz seulement. Cet exemple simple prouve que pour une même bande élémentaire, on peut espérer

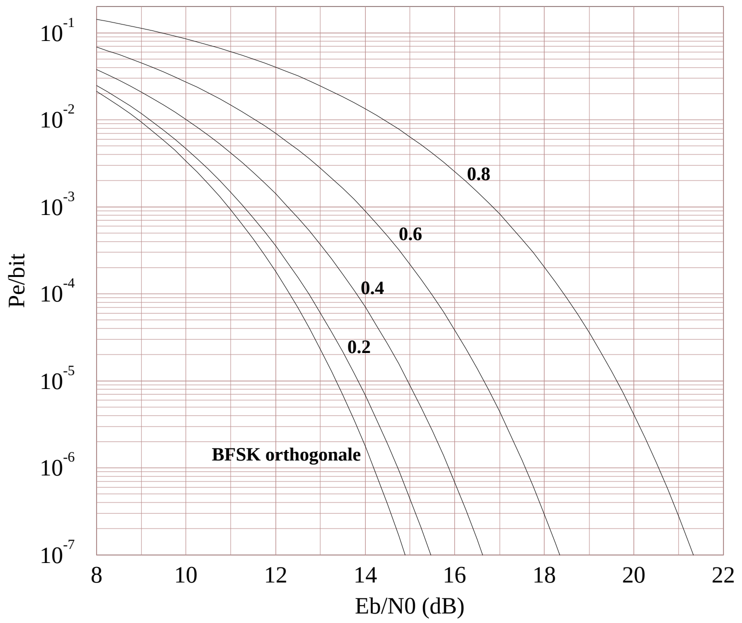


FIG. 1.5 – Probabilité d'erreur par bit d'une modulation BFSK sur canal gaussien pour différentes valeurs de la corrélation normalisée μ.

un gain de l'efficacité spectrale.

Malheureusement, cette augmentation de l'efficacité spectrale s'accompagne d'une dégradation des performances directement liée à la corrélation des fréquences dans une case élémentaire. Nous avons déjà constaté les effets néfastes de la corrélation dans le paragraphe 1.1.4. Nous verrons dans la suite de cette étude que l'utilisation de signaux de grandes dimensions permet de compenser cette dégradation. L'ajout du codage conduit même à des gains supplémentaires.

La constellation se compose de M signaux $\{S_m,\ m = 1, \ldots, M\}$ de dimension N. Ainsi, chaque signal est un vecteur de N composantes $S_m = \{s_{m,1}, \ldots, s_{m,N}\}$. La composante entière $s_{m,n}$ modélise le choix d'une fréquence parmi Q à un instant donné n. Elle correspond à l'émission physique d'un signal $s_{m,n}(t)$

$$s_{m,n}(t) = \sqrt{\frac{2E}{T}} \exp\left(2j\pi f_{m,n} t\right)$$

$n = 1, \ldots, N$, $m = 1, \ldots, M$ et $0 \leq t \leq T$. En accord avec les notations du paragraphe 1.1.1, $2E$ désigne l'énergie du signal $s_{m,n}(t)$ en bande de base. La fréquence élémentaire $f_{m,n}$ est reliée à la composante $s_{m,n}$ par l'une des deux relations suivantes : $f_{m,n} = s_{m,n} \times \Delta f_0$ ou $f_{m,n} = s_{m,n} \times \frac{\Delta f_0}{2}$, selon que $s_{m,n} \in \{0, \ldots, Q-1\}$ ou $s_{m,n} \in \{\pm 1, \ldots, \pm(Q-1)\}$.

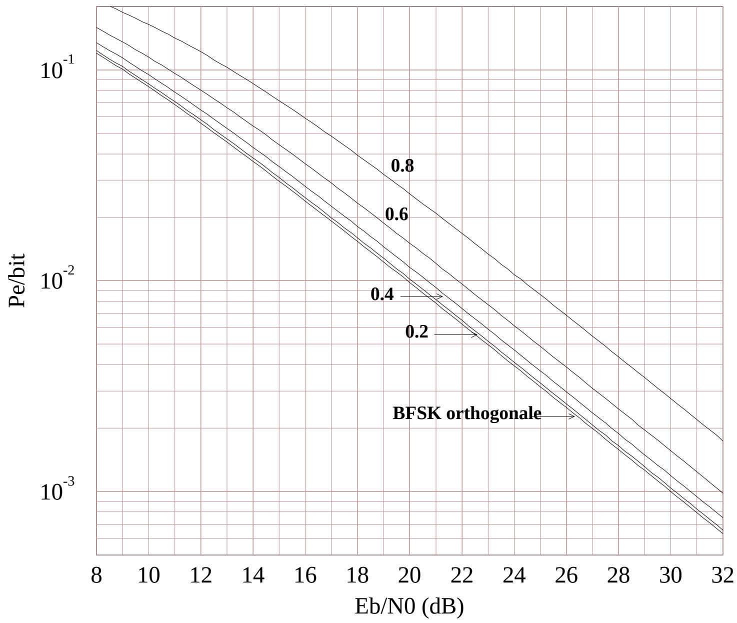


Fig. 1.6 – Probabilité d'erreur par bit d'une modulation BFSK sur canal de Rayleigh pour différentes valeurs de la corrélation normalisée μ.

1.2.2 Détection non cohérente optimale de signaux multidimensionnels

En supposant que le signal S_m a été émis, on reçoit un vecteur $\mathbf{R} = (r_1(t), \ldots, r_N(t))$ de N composantes. Chacune d'entre elles est de la forme

$$r_n(t) = \alpha e^{j\phi_{m,n}} s_{m,n}(t) + b_n(t)$$

où $b_n(t)$ est un bruit additif blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle ; α est le gain du canal et $\phi_{m,n}$ une phase aléatoire uniformément répartie sur $[0, 2\pi]$ de densité de probabilité $p(\phi_{m,n}) = \frac{1}{2\pi}$. $\phi_{m,n}$ est supposée inconnue au niveau du récepteur. Dans le cas du canal gaussien, α est une constante. Dans le cas du canal à évanouissements, α suit une loi de Rayleigh ; $p(\alpha) = 2\alpha e^{-\alpha^2}$ et $E[\alpha^2] = 1$.

Détecteur optimal sur le canal gaussien

En nous inspirant des résultats de [56], Annexe 4.C, nous généralisons au cas N-dimensionnel la recherche du détecteur optimal faite dans l'annexe 1.I. On se place toujours dans l'espace des signaux aléatoires, et les $\{\psi_k(t)\}$ constituent une base de cet espace.

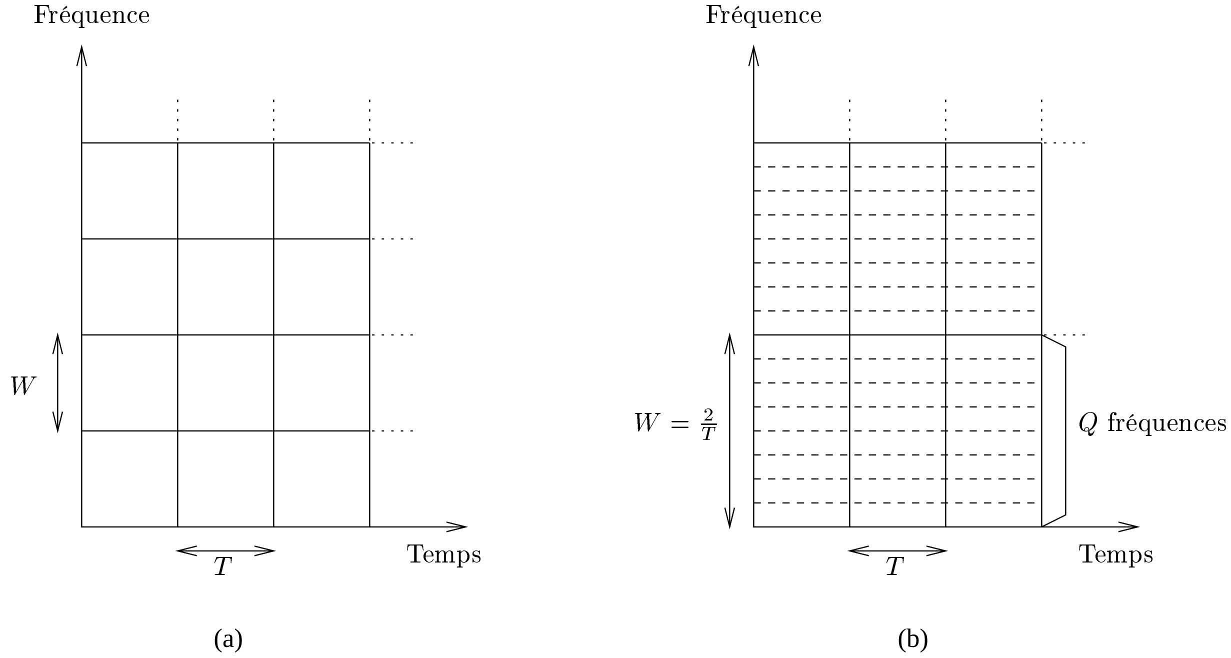


FIG. 1.7 – (a) Subdivision du plan temps-fréquence pour les transmissions non cohérentes. (b) Cas particulier des signaux à composantes corrélées, $Q = 8$, $\Delta f_0 = \frac{1}{4T}$ et $W = \frac{2}{T}$.

Chaque composante $r_n(t)$ admet un développement de Karhunen-Loève

$$r_n(t) = \lim_{K\to\infty} \sum_{k=1}^{K} r_{n,k}\psi_k(t)$$

où les coefficients $r_{n,k}$ sont donnés par $r_{n,k} = \alpha e^{j\phi_{m,n}} s_{m,n,k} + b_{n,k}$, pour $k = 1, 2, \ldots, n = 1, \ldots, N$ et $m = 1, \ldots, M$.

La probabilité $P(m|\mathbf{R})$, probabilité *a posteriori* que le signal S_m soit émis, étant donnée l'observation $\mathbf{R}$, est fournie par

$$P(m|\mathbf{R}) = \frac{p(\mathbf{R}|m)P(m)}{p(\mathbf{R})} = \frac{P(m)}{\sum_{\ell=1}^{M} \Lambda_{\ell m}(\mathbf{R})P(\ell)}$$

où les $P(\ell)$ sont les probabilités *a priori* des signaux S_ℓ et $\Lambda_{\ell m}(\mathbf{R})$ le rapport de vraisemblance de la paire de signaux (ℓ, m), défini par

$$\Lambda_{\ell m}(\mathbf{R}) = \prod_{n=1}^{N} \Lambda_{\ell m}(\mathbf{r}_n) = \prod_{n=1}^{N} \lim_{K\to\infty} \Lambda_{\ell m}(\mathbf{r}_{n,K})$$

Dans l'équation ci-dessus, les vecteurs $\mathbf{r}_{n,K}$ et $\mathbf{r}_n$ désignent respectivement $(r_{n,1}, \ldots, r_{n,K})$ et $(r_{n,1}, r_{n,2}, \ldots)$. $\Lambda_{\ell m}(\mathbf{r}_{n,K})$ est défini comme le rapport des densités de probabilité du vecteur $\mathbf{r}_{n,K}$ conditionnellement à l'émission des signaux S_ℓ et S_m.

Comme précédemment, les coefficients $r_{n,k}$ sont des variables aléatoires gaussiennes complexes de moyenne $m_{r_{n,k}} = \alpha e^{j\phi_{m,n}} s_{m,n,k}$ et de variance $\sigma^2_{r_{n,k}} = \sigma^2$ par composante réelle. La densité de probabilité *a priori* du vecteur $\mathbf{r}_{n,K}$ se calcule comme suit

$$\begin{aligned} p(\mathbf{r}_{n,K}|m,\phi_{n,m}) &= \left(\prod_{k=1}^{K} 2\pi\sigma^2\right)\exp\left(-\sum_{k=1}^{K}|r_{n,k}-\alpha e^{j\phi_{m,n}}s_{m,n,k}|^2/2\sigma^2\right) \\ &= \left(\prod_{k=1}^{K} 2\pi\sigma^2\right)\exp\left(-\sum_{k=1}^{K}(|r_{n,k}|^2-\alpha^2|s_{m,n,k}|^2)/2\sigma^2\right) \\ &\quad\times\exp\left(Re\left[\alpha e^{-j\phi_{m,n}}\sum_{k=1}^{K}\frac{r_{n,k}s^*_{m,n,k}}{\sigma^2}\right]\right) \end{aligned}$$

Les phases $\phi_{m,n}$ sont uniformément distribuées, alors

$$p(\mathbf{r}_{n,K}|m) = \int_0^{2\pi} p(\mathbf{r}_{n,K}|m,\phi_{m,n})\frac{1}{2\pi}d\phi_{m,n} \tag{1.28}$$

Toujours en utilisant (1.56) (Annexe I.1), l'équation (1.28) devient

$$\begin{aligned} p(\mathbf{r}_{n,K}|m) &= \left(\prod_{k=1}^{K} 2\pi\sigma_b^2\right)\exp\left(-\sum_{k=1}^{K}(|r_{n,k}|^2+\alpha^2|s_{m,n,k}|^2)/2\sigma^2\right) \\ &\quad\times I_0\left(\alpha\left|\sum_{k=1}^{K}\frac{r_{n,k}s^*_{m,n,k}}{\sigma^2}\right|\right) \end{aligned} \tag{1.29}$$

À l'aide de la relation (1.29), on peut former le rapport de vraisemblance

$$\begin{aligned} \Lambda_{\ell m}(\mathbf{r}_{n,K}) &= \frac{p(\mathbf{r}_{n,K}|\ell)}{p(\mathbf{r}_{n,K}|m)} \\ &= \exp\left(-\frac{\alpha^2}{2}\sum_{k=1}^{K}(|s_{\ell,n,k}|^2-|s_{m,n,k}|^2)/\sigma^2\right) \\ &\quad\times\frac{I_0\left(\alpha\left|\sum_{k=1}^{K}r_{n,k}s^*_{\ell,n,k}/\sigma^2\right|\right)}{I_0\left(\alpha\left|\sum_{k=1}^{K}r_{n,k}s^*_{m,n,k}/\sigma^2\right|\right)} \end{aligned}$$

La limite de $\Lambda_{\ell m}(\mathbf{r}_{n,K})$ quand $K\to\infty$ est

$$\begin{aligned} \Lambda_{\ell m}(\mathbf{r}_n) &= \exp\left(-\frac{\alpha^2}{2}\left[\int_0^T s_{\ell,n}(t)g^*_{\ell,n}(t)dt-\int_0^T s_{m,n}(t)g^*_{m,n}(t)dt\right]\right) \\ &\quad\times\frac{I_0\left[\alpha|\int_0^T r_n(t)g^*_{\ell,n}(t)dt|\right]}{I_0\left[\alpha|\int_0^T r_n(t)g^*_{m,n}(t)dt|\right]} \end{aligned}$$

Ici encore, les fonctions $g_{m,n}(t)$ sont définies par $g_{m,n}(t)=\lim_{K\to\infty}\sum_{k=1}^{K}\frac{s_{m,n,k}}{\sigma^2}\psi_k(t)=\frac{s_{m,n}(t)}{\sigma^2}$ où la dernière égalité est obtenue par définition du développement de Karhunen-Loève.

La valeur de $\Lambda_{\ell m}(\mathbf{r}_n)$ nous permet d'évaluer $\Lambda_{\ell m}(\mathbf{R})$.

$$\begin{aligned}\Lambda_{\ell m}(\mathbf{R}) &= \exp\left(-\frac{\alpha^2}{2}\sum_{n=1}^{N}\left[\int_0^T s_{\ell,n}(t)g_{\ell,n}^*(t)dt - \int_0^T s_{m,n}(t)g_{m,n}^*(t)dt\right]\right)\\ &\quad \times \prod_{n=1}^{N}\frac{I_0\left[\alpha\left|\int_0^T r_n(t)g_{\ell,n}^*(t)dt\right|\right]}{I_0\left[\alpha\left|\int_0^T r_n(t)g_{m,n}^*(t)dt\right|\right]}\end{aligned}$$

Les M signaux S_m de la constellation sont équiprobables. Maximiser $P(m|\mathbf{R})$ revient donc à maximiser les densités de probabilité conditionnelles $p(\mathbf{R}|m)$. Ceci équivaut au calcul des M variables

$$L_m = \exp\left[-\frac{\alpha^2}{2}\sum_{n=1}^{N}\int_0^T s_{m,n}(t)g_{m,n}^*(t)dt\right]\prod_{n=1}^{N} I_0\left[\alpha\left|\int_0^T r_n(t)g_{m,n}^*(t)dt\right|\right] \quad m = 1,\ldots,M$$

Comme dans le cas monodimensionnel, il suffit alors de choisir parmi les M signaux celui qui maximise L_m. Par ailleurs, les signaux de la constellation ont tous même énergie, et le bruit additif gaussien est blanc. Le terme de la forme $\exp\left[-\frac{\alpha^2}{2}\int_0^T s_{m,n}(t)g_{m,n}^*(t)dt\right]$ est un terme de biais indépendant de l'observation. En effet, dans ces conditions, $g_{m,n}(t) = \frac{s_{m,n}(t)}{\sigma^2}$ devient $\frac{s_{m,n}(t)}{N_0}$ et $\exp\left[-\frac{\alpha^2}{2}\int_0^T s_{m,n}(t)g_{m,n}^*(t)dt\right]$ s'écrit $\exp\left[-\frac{\alpha^2 E}{N_0}\right]$ où $2E$ est l'énergie en bande de base des signaux $s_{m,n}(t)$. Ce terme est commun à tous les L_m et n'intervient pas dans la maximisation.

Par conséquent, le détecteur optimal utilise le critère

$$\max_{m=1}^{M}\prod_{n=1}^{N} I_0\left(\frac{\alpha}{N_0}\left|\int_0^T r_n(t)s_{m,n}^*(t)dt\right|\right) \tag{1.30}$$

L'équation (1.30) décrit la structure du détecteur non cohérent optimal ML pour des signaux multidimensionnels sur le canal gaussien. Le terme $\left|\int_0^T r_n(t)s_{m,n}^*(t)dt\right|$ est obtenu en filtrant la composante $r_n(t)$ par le filtre adapté à la fréquence $s_{m,n}$ et en échantillonnant à l'instant $t = T$. L'observation totale en sortie du banc de filtres adaptés est donnée par M vecteurs $(x_{m,1},\ldots,x_{m,N})$ où

$$x_{m,n} = \int_0^T r_n(t)s_{m,n}^*(t)dt \tag{1.31}$$

Il s'agit ensuite de combiner ces sorties selon (1.30) pour maximiser le critère. On peut remarquer que l'ensemble des $\{x_{m,n}, m = 1,\ldots,M, n = 1,\ldots,N\}$ est redondant. En effet, les composantes des signaux multidimensionnels émis appartiennent à une modulation Q-FSK. Il est suffisant de filtrer chaque composante $r_n(t)$ du signal reçu par les Q filtres adaptés possibles. On obtient une statistique suffisante composée de $Q \times N$ valeurs en sortie du banc de filtres.

Pour simplifier la mise en œuvre pratique de ce détecteur, mais aussi pour mener à bien le calcul de probabilité d'erreur par paire, il est intéressant de chercher une expression simplifiée, équivalente au critère énoncé ci-dessus. $I_0(x) \in [1,+\infty[$ pour tout x réel et la fonction logarithme est strictement croissante sur cet intervalle. Une première étape consiste donc à remplacer le critère (1.30) par

$$\max_{m=1}^{M} \sum_{n=1}^{N} \log \left[I_0 \left(\frac{\alpha}{N_0} \left| \int_0^T r_n(t) s_{m,n}^*(t) dt \right| \right) \right]$$

La fonction de Bessel $I_0(x)$ admet le développement en série suivant :

$$I_0(x) = \sum_{k=0}^{\infty} \frac{(\frac{x}{2})^{2k}}{(k!)^2}$$

On connaît l'équivalent de $I_0(x)$ quand x tend vers l'infini :

$$I_0(x) \sim \frac{e^x}{\sqrt{2\pi x}} \left[1 + O(\frac{1}{x}) \right]$$

Enfin, on peut noter que $I_0(0) = 1$. Ces résultats nous permettent de donner une approximation de $I_0(x)$ pour de faibles ou grandes valeurs de x

$$I_0(x) \simeq \begin{cases} 1 + \frac{x^2}{4} & x \ll 1 \\ \frac{e^x}{\sqrt{x}} & x \gg 1 \end{cases}$$

En pratique, les sorties du banc de filtres adaptés $x_{m,n}$ correspondent à une évaluation du rapport signal-à-bruit. De cette façon, ces deux équivalents représentent les approximations à faible et fort rapport signal-à-bruit de $I_0(x)$. De plus, $\log(1 + x)$ est équivalent à x en 0, et $\log\left(\frac{e^x}{\sqrt{x}}\right) = x - \frac{1}{2}\log(x)$. Quand x est grand, cette dernière égalité devient $\log\left(\frac{e^x}{\sqrt{x}}\right) \simeq x$.

Grâce à ces différents éléments, on dispose de deux nouvelles expressions du critère de détection non cohérent optimal

$$\max_{m=1}^{M} \sum_{n=1}^{N} \left| \int_0^T r_n(t) s_{m,n}^*(t) dt \right|^2 \tag{1.32}$$

pour les faibles valeurs de rapport signal-à-bruit ; et

$$\max_{m=1}^{M} \sum_{n=1}^{N} \left| \int_0^T r_n(t) s_{m,n}^*(t) dt \right| \tag{1.33}$$

pour les fortes valeurs de rapport signal-à-bruit.

Nos résultats de simulation, ainsi que ceux de [58], ont montré que l'usage de l'une des deux approximations, (1.32) ou (1.33), conduit à une dégradation minime des performances par rapport au critère exact de l'équation (1.30). Dans la suite de ce travail, nous utiliserons le critère décrit par l'équation (1.32).

Détecteur optimal sur le canal de Rayleigh

Chaque composante $s_{m,n}(t)$ du signal multidimensionnel S_m est émise dans une case élémentaire du plan temps-fréquence. Le canal est caractérisé par des évanouissements lents et est non sélectif en fréquence. Il peut donc être modélisé par un coefficient multiplicatif $\alpha e^{j\phi_{m,n}}$ constant pour chaque signal de la modulation FSK, $s_{m,n}(t)$. En pratique, il sera toujours possible de satisfaire cette condition en choisissant judicieusement le temps symbole T par rapport à l'étalement des retards du canal T_m, soit $T \gg T_m$. L'entrelacement des composantes du signal est parfait, de telle sorte que les coefficients du canal correspondant aux N composantes peuvent être considérés comme indépendants. De plus, nous supposons qu'il n'existe aucune corrélation entre deux signaux FSK émis dans des cases temps-fréquence adjacentes.

Comme pour le cas monodimensionnel, il est possible de suivre une démarche parfaitement similaire au cas gaussien. La densité de probabilité $p(\mathbf{r}_{n,K}|m)$ donnée par (1.29) est une fois encore considérée comme une densité de probabilité conditionnellement au signal m et à une valeur fixée de l'évanouissement α. On la note $p(\mathbf{r}_{n,K}|m,\alpha)$. Alors,

$$p(\mathbf{r}_{n,K}|m) = \int_0^\infty p(\mathbf{r}_{n,K}|m,\alpha)p(\alpha)d\alpha$$

En utilisant $p(\alpha)$ et (1.7), on obtient

$$p(\mathbf{r}_{n,K}|m) \quad = \quad \frac{\left(\prod_{k=1}^{K} 2\pi\sigma^2\right)}{1+\sum_{k=1}^{K}\frac{|s_{n,m,k}|^2}{2\sigma^2}} \exp\left(-\sum_{k=1}^{K}\frac{|r_{n,k}|^2}{2\sigma^2}\right) \exp\left\{\frac{\left|\sum_{k=1}^{K}\frac{r_{n,k}s_{n,m,k}^*}{\sigma^2}\right|^2}{4+\sum_{k=1}^{K}\frac{2|s_{n,m,k}|^2}{\sigma^2}}\right\} \tag{1.34}$$

Nous substituons simplement (1.34) à (1.29) dans le raisonnement mené pour le canal gaussien. Le bruit additif est toujours blanc gaussien complexe et les signaux multidimensionnels sont équiprobables et de même énergie. Cela nous mène à de nouvelles expressions des variables de décision

$$L_m = \exp\left\{\sum_{n=1}^{N}\frac{\left|\int_0^T s_{m,n}(t)g_{m,n}^*(t)dt\right|^2}{2N_0(2+E)}\right\} \qquad m = 1,\dots,M$$

La fonction exponentielle étant monotone croissante sur $[0,+\infty[$, le critère de détection optimal est le suivant

$$\max_{m=1}^{M}\sum_{n=1}^{N}\left|\int_0^T r_n(t)s_{m,n}^*(t)dt\right|^2 \tag{1.35}$$

On notera que le critère obtenu est le même que celui utilisé sur le canal gaussien.

1.2.3 Probabilité d'erreur par paire

Cas du canal gaussien

La probabilité d'erreur par paire entre deux signaux S_i et S_j de la constellation, notée $P(S_i \to S_j)$, est la probabilité que le signal S_j soit détecté alors que S_i a été émis. En utilisant le critère (1.32), cette probabilité s'écrit

$$P(S_i \rightarrow S_j) = Prob(\sum_{n=1}^{N} |x_{j,n}|^2 > \sum_{n=1}^{N} |x_{i,n}|^2)$$

S_i étant supposé émis, les variables $x_{m,n}$ pour $m = i, j$ et $n = 1, \ldots, N$ sont de la forme

$$\begin{aligned} x_{m,n} &= \int_0^T (\alpha e^{j\phi_{i,n}} s_{i,n}(t) + b_n(t)) s^*_{m,n}(t) dt \\ &= \alpha e^{j\phi_{i,n}} \mu_n^{i,m} + b_{m,n} \end{aligned}$$

$\mu_n^{i,m} = \int_0^T s_{i,n}(t) s^*_{m,n}(t) dt$, $m = i, j$ est la corrélation entre les $n$ièmes composantes des signaux S_i et S_m. $b_{m,n} = \int_0^T b_n(t) s^*_{m,n}(t) dt$ est le bruit additif blanc gaussien complexe en sortie du filtre adapté. Il est de moyenne nulle et de variance $2E\sigma^2$ par composante réelle, où $2E$ est l'énergie des signaux $s_{m,n}(t)$ en bande de base et σ^2 la variance du bruit $b_n(t)$ en entrée du banc de filtres.

Par conséquent, $|x_{m,n}|$ suit une loi de Rice de paramètre $\alpha^2 |\mu_n^{i,m}|^2$ puisque $x_{m,n}$ est une variable aléatoire gaussienne complexe non centrée de variance $\sigma_x^2 = 2E\sigma^2$. Sa densité de probabilité est donnée par

$$p(|x_{m,n}|) = \frac{|x_{m,n}|}{\sigma_x^2} \exp\left(-\frac{|x_{m,n}|^2 + \alpha^2 |\mu_n^{i,m}|^2}{2\sigma_x^2}\right) I_0\left(\frac{\alpha |\mu_n^{i,m}| |x_{m,n}|}{\sigma_x^2}\right) \quad x_{m,n} \geq 0$$

On note $Y_m = \sqrt{\sum_{n=1}^{N} |x_{m,n}|^2}$. Y_m est une variable aléatoire de Rice généralisée d'ordre N [64]. La probabilité d'erreur par paire s'écrit alors

$$P(S_i \rightarrow S_j) = Prob(Y_j^2 > Y_i^2) = Prob(Y_j > Y_i)$$

L'équation (18) de [64] nous donne ainsi la probabilité d'erreur par paire recherchée sur le canal gaussien

$$P(S_i \rightarrow S_j) = \sum_{w=0}^{N-1} g_{N,X_i,1}(w) + \sum_{w=N}^{+\infty} g_{N,X_i,1}(w) \left(1 - \sum_{\ell=0}^{w-N} e^{-X_j} \frac{X_j^\ell}{\ell!}\right) \tag{1.36}$$

où

$$g_{N,X_i,v}(w) = \frac{1}{w!} \left(\frac{v}{1+v}\right)^w \left(\frac{1}{1+v}\right)^N \sum_{k=0}^{+\infty} e^{-X_i} \frac{(N+k+w-1)!}{k!(N+k-1)!} \left(\frac{X_i}{1+v}\right)^k$$

et X_m est défini par [64] comme

$$X_m \triangleq \frac{1}{2} \frac{s^2}{\sigma_{Y_m}^2}$$

s^2 est le paramètre de la variable aléatoire de Rice complexe d'ordre N : il est égal à la somme des N carrés des moyennes des $|x_{m,n}|$ [57], soit $s^2 = \sum_{n=1}^{N} \alpha^2 |\mu_n^{i,m}|^2$. $\sigma_{Y_m}^2$ est la variance par composante réelle des variables gaussiennes complexes sous-jacentes : $\sigma_{Y_m}^2 = \sigma_x^2 = 2E\sigma^2 = 2EN_0$.

Par conséquent, les deux termes X_m, $m = i, j$, s'écrivent

$$X_m = \frac{1}{4EN_0} \sum_{n=1}^{N} \alpha^2 |\mu_n^{i,m}|^2 \quad m = i, j$$

et

$$v = \frac{\sigma_{Y_i}^2}{\sigma_{Y_j}^2} = \frac{\sigma_x^2}{\sigma_x^2} = 1$$

La corrélation $\mu_n^{i,m}$ a déjà été calculée dans le cas de signaux FSK simples (voir équation (1.1)). Dans le cas présent, il nous suffit d'ajouter l'indice de la composante considérée n. On obtient

$$\mu_n^{i,m} = \int_0^T s_{i,n}(t) s_{m,n}^*(t) dt = \frac{2E}{T} \int_0^T e^{2j\pi\Delta f_n t} dt$$

où $\Delta f_n = f_{i,n} - f_{m,n}$ est l'écart de fréquence entre les composantes n de la paire de signaux (i, m). Après intégration, on a

$$\mu_n^{i,m} = 2E \times \frac{sin(\pi\Delta f_n T)}{\pi\Delta f_n T} \times e^{j\pi\Delta f_n T}$$

Ainsi

$$|\mu_n^{i,i}| = 2E \quad \text{et} \quad |\mu_n^{i,j}| = 2E \, \frac{sin(\pi\Delta f_n T)}{\pi\Delta f_n T}$$

On peut donc évaluer plus précisément X_i et X_j

$$X_i = \frac{\alpha^2 NE}{N_0} \tag{1.37}$$

$$X_j = \frac{\alpha^2 E}{N_0} \sum_{n=1}^{N} \left(\frac{sin(\pi\Delta f_n T)}{\pi\Delta f_n T} \right)^2 \tag{1.38}$$

En pratique, la variable X_i est définie par le système de façon définitive, elle ne dépend que de l'énergie des signaux, tandis que X_j dépend des corrélations entre les signaux, c'est-à-dire de la répartition des fréquences. L'étude des variations de la probabilité d'erreur en fonction de ces deux paramètres X_i et X_j est un bon moyen d'aboutir à des critères généraux quant à la construction des signaux multidimensionnels : cette étude est présentée dans l'annexe 1.II. En particulier, nous montrons que la variable X_j décroît lorsque la répartition des fréquences est judicieusement choisie. Dans ce cas, la probabilité d'erreur sera minimisée.

Cas du canal de Rayleigh

La probabilité d'erreur par paire entre les signaux S_1 et S_2 est toujours définie par $P(L_1 < L_2)$, ou de manière équivalente

$$P(S_1 \to S_2) \quad = \quad P\left(\sum_{n=1}^{N} |x_{1,n}|^2 < \sum_{n=1}^{N} |x_{2,n}|^2\right) \tag{1.39}$$

$x_{j,n}$, $j = 1, 2$ désigne la sortie du filtre adapté au signal $s_{j,n}$. Le calcul qui suit généralise celui de [7] au cas de signaux d'énergie E quelconque. Nous définissons le vecteur ρ

$$\rho = (x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2}, \cdots, x_{1,N}, x_{2,N})$$

On note $f = \rho^t F \rho^*$ la forme quadratique hermitienne associée à ρ, avec F matrice carrée $2N \times 2N$ donnée par :

$$F = \begin{bmatrix} 1 & 0 & & & \\ 0 & -1 & & & \\ & & \ddots & & \\ & & & 1 & 0 \\ & & & 0 & -1 \end{bmatrix}$$

La probabilité d'erreur par paire (1.39) n'est autre que la probabilité d'avoir $f < 0$

$$P(S_1 \to S_2) = P(f = \rho^t F \rho^* < 0) \tag{1.40}$$

La fonction caractéristique d'une telle forme quadratique hermitienne est donnée dans [61]

$$\psi_f(j\xi) = E_f\left[e^{j\xi f}\right] = \frac{1}{\det(I - j2\xi R^* F)} \tag{1.41}$$

où $R = \frac{1}{2}E[\rho^t \rho^*]$ est la matrice de covariance du vecteur ρ.

Les deux variables $x_{1,n}$ et $x_{2,n}$ s'écrivent plus précisément :

$$x_{1,n} \quad = \quad 2E\alpha e^{j\phi_n} + b_{1,n} \tag{1.42}$$
$$x_{2,n} \quad = \quad 2E\mu_n \alpha e^{j\phi_n} + b_{2,n} \tag{1.43}$$

où $\mu_n = \frac{\mu_n^{1,2}}{2E}$ est la corrélation normalisée entre les composantes n des signaux S_1 et S_2 et $2E$ est l'énergie de $s_{1,n}(t)$. La corrélation $\mu_n^{1,2}$ a été définie par l'équation (1.1). Toutes les valeurs de la corrélation sont distinctes : $\mu_k \neq \mu_\ell \ \forall\ k, \ell \in \{1, \cdots, N\}$. On note $h_n = \alpha e^{j\phi_n}$ le coefficient multiplicatif modélisant les évanouissements, constant pour chaque signal de la modulation. h_n suit une loi gaussienne centrée de variance σ_h^2 par composante réelle. Les h_n sont indépendants.

Dans ces conditions, les variables aléatoires $x_{1,n}$ et $x_{2,n}$ suivent des lois gaussiennes centrées de variance respective par composante réelle

$$E[|x_{1,n}|^2] = 4E^2\sigma_h^2 + 2E\sigma^2 \tag{1.44}$$

et

$$E[|x_{2,n}|^2] = 4E^2|\mu_n|^2\sigma_h^2 + 2E\sigma^2 \tag{1.45}$$

Par ailleurs, les échantillons de bruit $b_{1,n}$ et $b_{2,n}$ sont corrélés

$$E[b_{1,n}b_{2,n}^*] = 2E\mu_n^*\sigma^2 \tag{1.46}$$

Par conséquent, $x_{1,n}$ et $x_{2,n}$ sont aussi corrélées et

$$E[x_{1,n}x_{2,n}^*] = 2E\mu_n^*(2E\sigma_h^2 + \sigma^2) \tag{1.47}$$

On peut remarquer que les variables aléatoires relatives à deux composantes distinctes ont une corrélation nulle. Les relations (1.44) à (1.47) nous permettent d'écrire la matrice de covariance R du vecteur ρ sous la forme

$$R = \begin{bmatrix} R_1 & 0 & \dots & 0 \\ 0 & R_2 & \dots & 0 \\ & & \ddots & \\ 0 & \dots & 0 & R_N \end{bmatrix}$$

où chaque R_n est une matrice 2×2 donnée par

$$R_n = \begin{bmatrix} 4E^2\sigma_h^2 + 2E\sigma^2 & 2E\mu_n^*(2E\sigma_h^2 + \sigma^2) \\ 2E\mu_n(2E\sigma_h^2 + \sigma^2) & 4E^2|\mu_n|^2\sigma_h^2 + 2E\sigma^2 \end{bmatrix}$$

L'expression de la fonction caractéristique (1.41) devient

$$\psi_f(j\xi) = \frac{1}{\displaystyle\prod_{k=1}^{N} \det(I - j2\xi R_n^* F_n)} \tag{1.48}$$

où F_n est donnée par

$$F_n = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Un calcul direct de $\det(I - j2\xi R_n^* F_n)$ conduit à

$$\det(I - j2\xi R_n^* F_n) = (1 - j2\xi u_n)(1 + j2\xi v_n) \tag{1.49}$$

où

$$u_n = \frac{2E\sigma^2(\gamma + 2N)}{2N}\left[\left(1 - |\mu_n|^2\right)\Gamma + \sqrt{(1 - |\mu_n|^2)\,(1 - |\mu_n|^2\Gamma^2)}\right] \geq 0$$

et

$$v_n = -\frac{2E\sigma^2(\gamma + 2N)}{2N}\left[\left(1 - |\mu_n|^2\right)\Gamma - \sqrt{(1 - |\mu_n|^2)\,(1 - |\mu_n|^2\Gamma^2)}\right] \geq 0$$

Dans les expressions ci-dessus, on définit γ, le rapport signal-à-bruit par symbole, par :

$$\gamma = \frac{2NE\sigma_h^2}{\sigma^2} \tag{1.50}$$

et le paramètre Γ est donné par

$$\Gamma = \frac{\gamma}{\gamma + 2N} \tag{1.51}$$

En utilisant (1.49) dans (1.48), on a

$$\psi_f(j\xi) = \frac{1}{\prod_{n=1}^{N} (1 - j2\xi u_n)(1 + j2\xi v_n)}$$

Puisque $\mu_k \neq \mu_\ell$ pour $k \neq \ell$, nous pouvons décomposer $\psi_f(j\xi)$ en éléments simples

$$\psi_f(j\xi) = \sum_{n=1}^{N} \frac{A_n}{1 - j2\xi u_n} + \sum_{n=1}^{N} \frac{B_n}{1 + j2\xi v_n}$$

où A_n et B_n sont les constantes relatives à chaque fraction simple de la décomposition. Il est alors facile de montrer que la probabilité d'erreur (1.40) s'écrit

$$P(S_1 \to S_2) = \sum_{n=1}^{N} B_n$$

Finalement, un calcul relativement long de B_n fournit une expression de la probabilité d'erreur par paire

$$P(S_1 \to S_2) = \frac{1}{2} \sum_{n=1}^{N} \left\{ \left[1 - \Gamma \sqrt{\frac{1 - |\mu_n|^2}{1 - |\mu_n|^2 \Gamma^2}} \right] \frac{\left(1 - |\mu_n|^2\right)^{N-1}}{\prod_{i=1,\, i \neq n}^{N} (|\mu_i|^2 - |\mu_n|^2)} \right\} \tag{1.52}$$

où Γ est défini par (1.50) et (1.51). L'expression obtenue est la même que celle fournie par [7]. On remarquera cependant que la définition du rapport signal-à-bruit γ diffère et tient compte de l'énergie des signaux E.

Plusieurs résultats supplémentaires également utilisables dans notre cas sont développés dans [7]. On dispose ainsi d'une expression plus simple de l'équation (1.52),

$$P(S_1 \to S_2) = \frac{1}{2} \left[1 - \sum_{n=1}^{N} \Gamma \sqrt{\frac{1 - |\mu_n|^2}{1 - |\mu_n|^2 \Gamma^2}} \frac{\left(1 - |\mu_n|^2\right)^{N-1}}{\prod_{i=1,\, i \neq n}^{N} (|\mu_i|^2 - |\mu_n|^2)} \right] \tag{1.53}$$

d'une expression asymptotique de la relation (1.52) pour les grands rapports signal-à-bruit,

$$P(\gamma \to \infty) = \frac{1}{2} \frac{(2N)!}{(N!)^2} \frac{N^N}{\gamma^N \prod_{n=1}^{N} (1 - |\mu_n|^2)} \tag{1.54}$$

et enfin d'une expression de (1.52) quand les signaux sont équicorrélés, c'est-à-dire $\mu_n = \mu \ \forall n$

$$\begin{aligned} P(S_1 \to S_2) &= \left\{ \frac{1}{2} \left[1 - \Gamma \sqrt{\frac{1-|\mu|^2}{1-|\mu|^2\Gamma^2}} \right] \right\}^N \\ &\times \sum_{n=0}^{N-1} \left\{ \frac{C_{2N-1}^n}{2^{N-1}} \left[1 + \Gamma \sqrt{\frac{1-|\mu|^2}{1-|\mu|^2\Gamma^2}} \right]^n \left[1 - \Gamma \sqrt{\frac{1-|\mu|^2}{1-|\mu|^2\Gamma^2}} \right]^{N-1-n} \right\} \quad (1.55) \end{aligned}$$

1.2.4 Exemple : signaux corrélés de diversité 4

Afin d'illustrer le gain en efficacité spectrale apporté par un alphabet multidimensionnel à composantes corrélées, nous comparons les performances obtenues sur canal de Rayleigh par deux constellations de diversité et de longueur $N = 4$.

Le premier alphabet est formé de deux signaux BFSK orthogonaux de diversité 4 donnés par

$$\begin{aligned} S_1 &= (0,0,0,0) \\ S_2 &= (1,1,1,1) \end{aligned}$$

Chaque composante correspondant à une case temps-fréquence est désignée par le numéro de la fréquence émise. Nous avons le choix entre “0” et “1” pour la BFSK. Les performances de cet alphabet sont obtenues en utilisant la relation (1.55) avec $N = 4$ et $\mu_n = \mu = 0$. L'efficacité spectrale est de 1/8 bits/s/Hz. En effet, il faut 1 bit pour choisir l'un des deux signaux multidimensionnels S_m, $m = 1, 2$, et une approximation de la bande est donnée par $4 \times 2\Delta f_0$ où $\Delta f_0 = 1/T$ puisque les signaux BFSK sont orthogonaux. On note B_e le facteur d'élargissement de bande, défini comme l'inverse de l'efficacité spectrale [7]. Ici, $B_e = 8$.

Le second alphabet est construit à partir d'une modulation 8-FSK. Il est également de longueur et de diversité 4. Ainsi, chaque signal est formé de quatre composantes, émises dans des cases temps-fréquence distinctes et le choix de la fréquence se fait entre les 8 possiblités fournies par la 8-FSK. Une fois encore, chaque composante est représentée par le numéro de la fréquence choisie. Les $M = 8$ signaux de la constellation s'écrivent

$$\begin{aligned} S_1 &= (0,1,0,1) \\ S_2 &= (1,3,2,3) \\ S_3 &= (2,0,4,5) \\ S_4 &= (3,2,6,7) \\ S_5 &= (4,5,3,0) \\ S_6 &= (5,7,5,2) \\ S_7 &= (6,4,7,6) \\ S_8 &= (7,6,1,4) \end{aligned}$$

Cet alphabet, construit de manière heuristique pour optimiser les corrélations entre les signaux a été proposé par [7]. La bande totale nécessaire à l'émission d'un signal S_m est $4 \times 8\Delta f_0$. Les signaux 8-FSK sont corrélés : $\Delta f_0 = 1/4T$. Il faut 3 bits pour choisir l'un des 8 signaux S_m.

L'efficacité spectrale de ce deuxième alphabet vaut donc 3/8 bits/s/Hz, et $Be = 2.66$. L'ordre de diversité 4 de cette constellation est dû au fait que pour tout couple de signaux (S_i, S_j), $i, j = 1, \ldots, 8$, les quatre composantes sont distinctes, c'est-à-dire $s_{i,n}(t) \neq s_{j,n}(t)$, $\forall n = 1, \ldots, 4$. Par ailleurs, il a été montré dans [7] que les deux signaux les plus corrélés sont S_4 et S_7.

Les performances de cet alphabet sont obtenues à partir de la relation (1.52). En effet, il est possible de déduire de la probabilité d'erreur par paire des bornes inférieure et supérieure sur la probabilité d'erreur. Une borne inférieure est donnée par le pire cas de $P(S_i \to S_j)$. On l'obtient pour le couple de signaux les plus corrélés, en l'occurrence (S_4, S_7). Ainsi $P_e \geq P(S_4 \to S_7)$. Par ailleurs, l'application de la borne de l'union fournit une borne supérieure de P_e. Alors $P_e \leq \sum_{(i,j)} P(S_i \to S_j)$, et $\sum_{(i,j)} P(S_i \to S_j) \leq (M-1)P(S_4 \to S_7)$. Finalement,

$$P(S_4 \to S_7) \leq P_e \leq (M-1)P(S_4 \to S_7)$$

La probabilité d'erreur binaire est donnée par $P_b = P_e/2$.

La figure 1.8 illustre ces différents résultats ainsi que les performances obtenues par simulation pour la constellation de signaux corrélés.

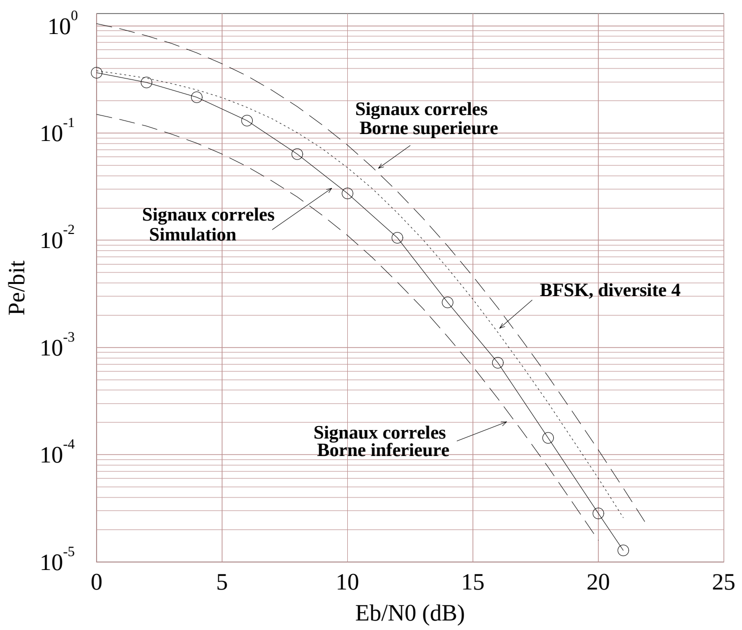


FIG. 1.8 – Performances comparées de deux alphabets de diversité 4 sur canal de Rayleigh : BFSK orthogonale, $\Delta f_0 = 1/T$ et $B_e = 8$, et $M = 8$ signaux corrélés de longueur $N = 4$, $\Delta f_0 = 0.25/T$, $B_e = 2.66$.

On constate que les bornes supérieure et inférieure de la probabilité d'erreur de l'alphabet corrélé sont légitimées par la simulation. Cet alphabet présente un très bon comportement par rapport à la modulation BFSK de diversité 4. En effet, l'efficacité spectrale est multipliée par un facteur 3 et un gain de 1 dB est atteint pour une probabilité d'erreur $P_b = 10^{-4}$. Ces résultats encouragent fortement l'emploi de constellations multidimensionnelles à composantes corrélées.

1.3 Etude de la capacité

La capacité d'un canal de transmission est une mesure de l'aptitude de ce canal à transmettre de l'information. L'information mutuelle moyenne [6][39] permet de quantifier l'information qu'apporte en moyenne la réalisation de la sortie Y sur l'entrée X du canal où X et Y sont deux variables aléatoires indépendantes. La capacité est définie comme le maximum de l'information mutuelle sur toutes les distributions possibles de l'entrée X. L'étude de la capacité permet de fixer les bornes théoriques d'un système de transmission. Nous reviendrons plus précisément sur la capacité en particulier et la théorie de l'information en général dans le dernier chapitre.

Tout système cherche à s'approcher des performances optimales limites ainsi matérialisées par les courbes théoriques de capacité. Dans le cas d'une détection cohérente, sur canal gaussien ou sur canal de Rayleigh à évanouissements indépendants, l'information mutuelle est maximisée pour une distribution gaussienne en entrée du canal. La figure 1.9 illustre la capacité du canal gaussien et du canal de Rayleigh à évanouissements indépendants [16][31][54][39].

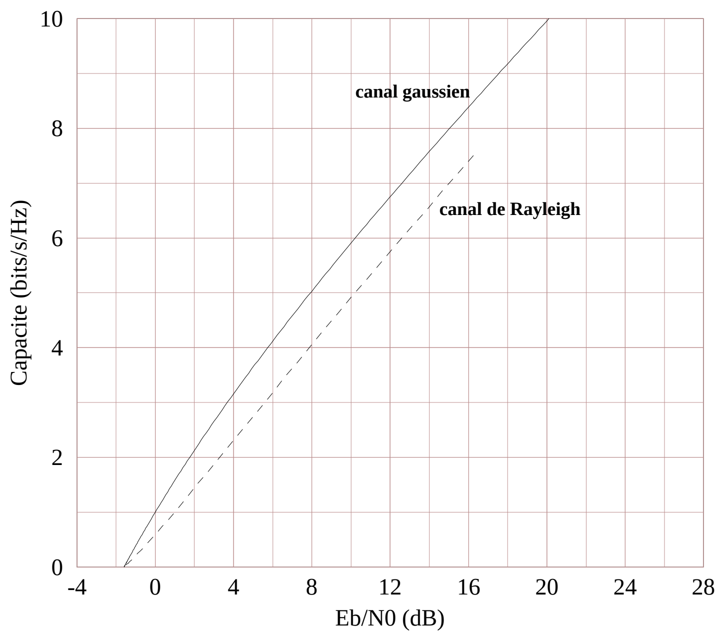


Fig. 1.9 – Capacité des canaux gaussien et de Rayleigh avec détection cohérente. La distribution en entrée est gaussienne.

La capacité théorique du canal de Rayleigh à évanouissements indépendants avec détection non cohérente a été étudiée très précisément dans [1]. Abou Façayl et Shamai ont montré le résultat suivant

Théorème 1.3.1 *(Capacité du canal à évanouissements indépendants avec détection non cohérente)*
La capacité du canal de Rayleigh à évanouissements indépendants utilisé dans un contexte de détection non cohérente est atteinte pour une distribution discrète en entrée. Cette distribution contient un nombre fini de raies, dont obligatoirement une en zéro.

Ce résultat a été énoncé dès 1967 par Richters sous forme de conjecture [59]. La démonstration est apportée par Abou Fayçal et Shamai. Le lecteur se reportera à l'article [1] pour une version détaillée de cette démonstration. L'appelation "raies" de la distribution, par analogie avec un spectre de raies, fait référence au terme anglais "mass point" utilisé par les auteurs. Nous nous contentons de rappeler ici les propriétés de la distribution optimale.

Lemme 1 *(Nombre de raies)*
Le nombre de raies de la distribution qui maximise la capacité du canal de Rayleigh à évanouissements indépendants augmente avec le rapport signal-à-bruit.

Ainsi, pour des valeurs du rapport signal-à-bruit (SNR, Signal-to-Noise Ratio) moyen inférieures à 8 dB, la distribution contient deux raies seulement dont une en zéro. On remarquera que la modulation OOK remplit cette condition. Lorsque le SNR diminue, la probabilité de la raie qui n'est pas en zéro tend vers 0 alors que son amplitude augmente lentement. Gallager a montré qu'asymptotiquement, cette amplitude tend vers l'infini lorsque le SNR tend vers 0 [39](théorème 8.6.1). A fort SNR, le nombre de raies augmente. Une incertitude demeure quant à l'origine des nouvelles raies : est-ce que chaque raie se sépare en deux ou est-ce que de nouvelles raies apparaissent indépendamment ? En observant la condition de Kuhn-Tucker, les auteurs privilégient l'apparition de nouvelles raies à l'infini. On notera enfin qu'une raie donnée a une amplitude d'autant plus grande que sa probabilité est faible.

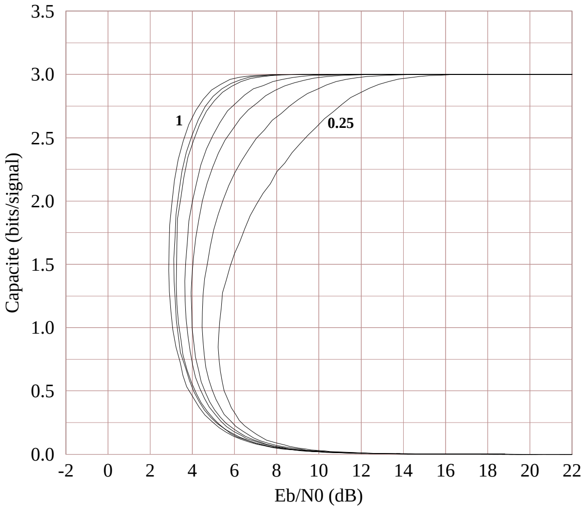
Des travaux récents ont abordé l'étude de la capacité d'un canal de Rayleigh non cohérent à évanouissements plats pour les antennes multiples. La valeur asymptotique de la capacité de ce canal et la forme des signaux qui permettent de l'atteindre sont données dans [51], tandis que [63] généralise ce résultat au cas multi-utilisateurs.

Nous présentons finalement les capacités des canaux gaussien et de Rayleigh non cohérents lorsque nous nous limitons, en entrée du canal, à deux types de modulation : la modulation 8-FSK et un alphabet multidimensionnel construit à partir d'une modulation 8-FSK corrélée, déjà étudié au paragraphe 1.2.4 et noté alphabet $\mathcal{A}$. L'information mutuelle obtenue est abusivement appelée capacité du schéma de modulation. Pour une étude détaillée du calcul de la capacité de ces canaux non cohérents admettant en entrée des alphabets de signaux corrélés, le lecteur se reportera au chapitre 4 de ce document.

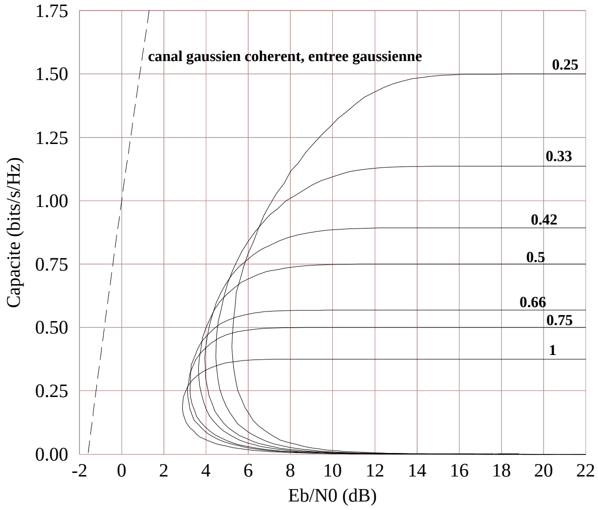
1.3.1 Capacité des canaux gaussien et de Rayleigh admettant en entrée une modulation 8-FSK

Les figures 1.10 et 1.11 représentent respectivement les courbes de capacité des canaux gaussien et de Rayleigh non cohérents. L'entrée du canal est constituée d'une modulation 8-FSK. Différentes valeurs de l'espacement fréquentiel de référence de la modulation sont considérées :

$\Delta f_0 T = 1.0, 0.75, 0.66, 0.5, 0.42, 0.33$ et 0.25. Les figures de gauche (1.10(a) et 1.11(a)) donnent la capacité en bits/signal et celles de droite (1.10(b) et 1.11(b)) la capacité en bits/s/Hz. Enfin, sur ces dernières, la capacité du canal considéré avec détection cohérente est indiquée à titre de comparaison.



(a) Capacité en bits/signal



(b) Capacité en bits/s/Hz

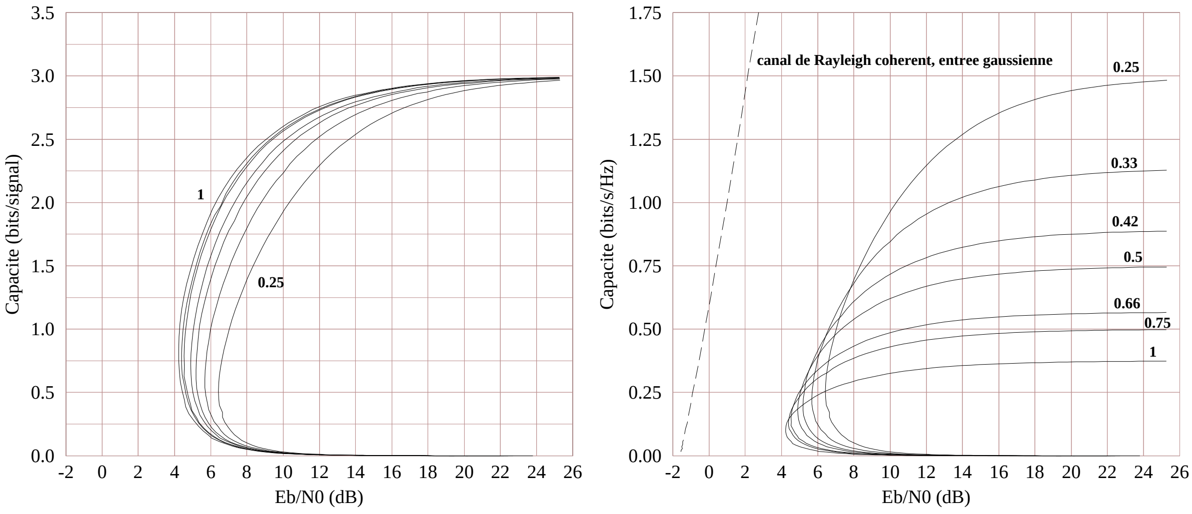
Fig. 1.10 – Capacité du canal gaussien non cohérent admettant en entrée une modulation 8-FSK.

1.3.2 Capacité du canal de Rayleigh non cohérent à évanouissements indépendants admettant en entrée un alphabet de signaux multidimensionnels

La figure 1.12 illustre la capacité du canal de Rayleigh non cohérent à évanouissements indépendants lorsque l'alphabet $\mathcal{A}$ précédemment défini est présenté en entrée. De la même manière que pour la modulation 8-FSK, trois valeurs distinctes de l'espacement fréquentiel de référence sont envisagées : $\Delta f_0 T = 1.0, 0.25$ et 0.1875. La capacité est donnée en bits/signal (figure 1.12(a)) et en bits/s/Hz (figure 1.12(b)). Cette dernière peut être comparée à la capacité du canal de Rayleigh cohérent.

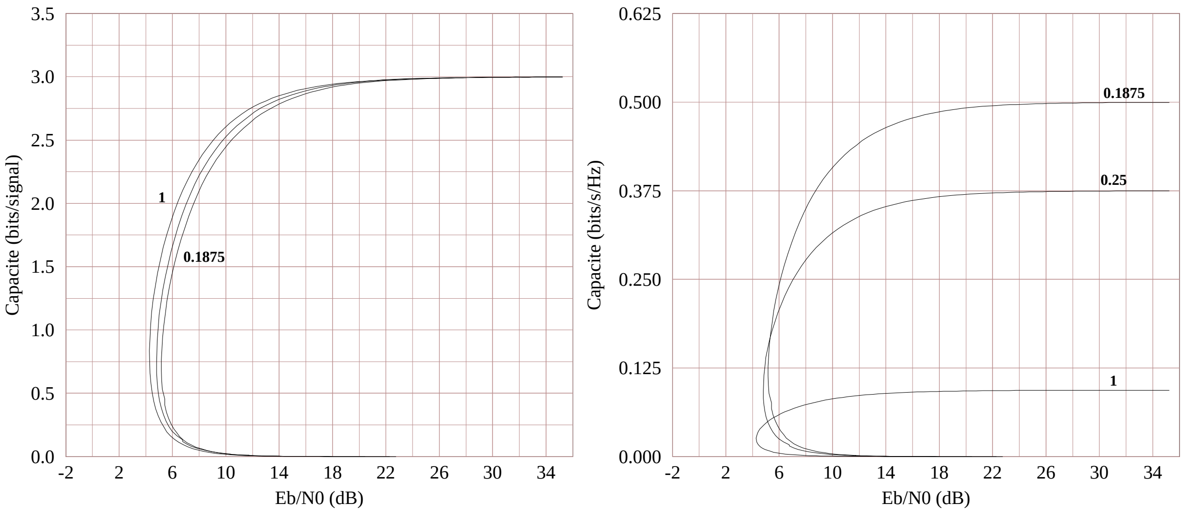
1.4 Conclusions

Dans ce chapitre, nous avons tout d'abord rappelé les résultats existants relatifs aux modulations de fréquence Q-FSK sur canal gaussien et sur canal de Rayleigh. Le principe de construction, la structure des détecteurs optimaux ML ainsi que les performances ont été détaillés. Nous avons



(a) Capacité en bits/signal (b) Capacité en bits/s/Hz

Fig. 1.11 – Capacité du canal de Rayleigh non cohérent à évanouissements indépendants admettant en entrée une modulation 8-FSK.



(a) Capacité en bits/signal (b) Capacité en bits/s/Hz

Fig. 1.12 – Capacité du canal de Rayleigh à évanouissements indépendants admettant en entrée l'alphabet $\mathcal{A}$ de 8 signaux multidimensionnels.

notamment pu observer que ces modulations, très robustes dans un contexte de détection non cohérente, conduisent malheureusement à de faibles efficacités spectrales.

Nous avons alors introduit la notion de constellations multidimensionnelles construites à partir de signaux Q-FSK corrélés. Ces constructions, proposées dans [7], vont à l'encontre de l'approche habituellement choisie : l'exigence d'orthogonalité des signaux est supprimée et permet de réduire la bande utile et par là même d'augmenter l'efficacité spectrale. Les dégradations de performances dues aux corrélations des signaux sont compensées par le caractère multidimensionnel des alphabets utilisés. Nous avons détaillé la structure des détecteurs multidimensionnels optimaux ML, sur canal gaussien et sur canal de Rayleigh, ainsi que l'expression des probabilités d'erreur par paire.

Enfin, nous avons rappelé les principaux résultats connus concernant la capacité des canaux gaussien et de Rayleigh en cas de détection cohérente ou non.

Les alphabets proposés par [7] ont l'avantage d'augmenter la diversité, paramètre important sur canal de Rayleigh. De plus, ils améliorent la capacité, comme nous avons pu le remarquer pour l'alphabet heuristique de 8 signaux de longueur $N = 4$. Par ailleurs, on sait qu'il est possible, lorsque la détection est non cohérente, d'approcher la capacité théorique du canal gaussien cohérent (limite à -1.6 dB) en utilisant un très grand nombre Q de signaux orthogonaux, par exemple des signaux d'une modulation FSK.

Les résultats prometteurs auxquels conduit la constellation heuristique proposée au paragraphe 1.2.4 [7] ainsi que les différents arguments théoriques ici présentés (augmentation de l'efficacité spectrale et de la capacité) ont motivé la recherche de méthodes de construction plus générales d'alphabets multidimensionnels fondés sur des signaux FSK corrélés. Nous avons remarqué que la modélisation multidimensionnelle développée au paragraphe 1.2 peut s'adapter indifféremment à toute méthode de codage ou de diversité. Les travaux de [7] sont relatifs à la diversité, nous proposons dans la suite de ces travaux de nous consacrer à des méthodes de codage.

1.5 Annexe 1.I : Détection optimale non cohérente sur le canal gaussien

Nous travaillons avec une modulation Q-FSK. En supposant que le signal $s_q(t)$ a été émis, on reçoit

$$r(t) = \alpha e^{j\phi_q} s_q(t) + b(t)$$

où $b(t)$ est un bruit additif blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle ; α est le gain du canal, et ϕ_q une phase aléatoire uniformément répartie sur $[0, 2\pi]$ de densité de probabilité $p(\phi_q) = \frac{1}{2\pi}$. Dans le cas du canal gaussien, α est une constante. Dans le cas du canal à évanouissements, α suit une loi de Rayleigh ; $p(\alpha) = 2\alpha e^{-\alpha^2}$ et $E[\alpha^2] = 1$.

Plaçons nous dans l'espace des signaux aléatoires à énergie finie. La famille des $\{\psi_k(t)\}$ est une base orthonormée de cet espace. Le développement de Karhunen-Loève de $r(t)$ sur cette base s'écrit

$$r(t) = \lim_{K\to\infty} \sum_{k=1}^{K} r_k \psi_k(t)$$

où les coefficients r_k sont donnés par $r_k = \alpha e^{j\phi_q} s_{q,k} + b_k$, pour $k = 1, 2, \dots$ et $q = 1, 2, \dots, Q$. On note $\mathbf{r} = (r_1, r_2, \dots)$. Les probabilités $P(q|\mathbf{r}) = P(s_q|\mathbf{r})$, probabilités *a posteriori* que le signal q a été émis, étant donnée l'observation $\mathbf{r}$, sont définies par la loi de Bayes (équation (1.4)). Cette dernière se récrit

$$P(q|\mathbf{r}) = \frac{P(q)}{\sum_{\ell=1}^{Q} \Lambda_{\ell q}(\mathbf{r}) P(\ell)}$$

où $P(\ell)$ est la probabilité *a priori* du signal $s_\ell(t)$ et $\Lambda_{\ell q}(\mathbf{r})$ le rapport de vraisemblance de la paire de signaux (ℓ, q), défini par

$$\Lambda_{\ell q}(\mathbf{r}) = \frac{p(\mathbf{r}|\ell)}{p(\mathbf{r}|q)} = \frac{\int_0^{2\pi} p(\mathbf{r}|\ell, \phi_\ell) p(\phi_\ell) d\phi_\ell}{\int_0^{2\pi} p(\mathbf{r}|q, \phi_q) p(\phi_q) d\phi_q}$$

Les coefficients r_k sont des variables aléatoires complexes gaussiennes de moyenne $m_{r_k} = \alpha e^{j\phi_q} s_{q,k}$ et de variance $\sigma^2_{r_k} = \sigma^2$ par composante réelle. L'indépendance des composantes r_k conduit à l'expression suivante pour la densité de probabilité *a priori* du vecteur $\mathbf{r}_K = (r_1, \dots, r_K)$

$$p(\mathbf{r}_K|q, \phi_q) = \left(\prod_{k=1}^{K} 2\pi\sigma^2 \right) \exp\left(-\sum_{k=1}^{K} \frac{|r_k - \alpha e^{j\phi_q} s_{q,k}|^2}{2\sigma^2} \right) \quad q = 1, \dots, Q$$

Après développement du terme dans l'exponentielle, on obtient

$$p(\mathbf{r}_K|q, \phi_q) = \left(\prod_{k=1}^{K} 2\pi\sigma^2 \right) \exp\left(-\sum_{k=1}^{K} \frac{|r_k|^2 + \alpha^2 |s_{q,k}|^2}{2\sigma^2} \right) \times \exp\left(Re\left[\alpha e^{-j\phi_q} \sum_{k=1}^{K} \frac{r_k s^*_{q,k}}{\sigma^2} \right] \right)$$

Les phases ϕ_q sont uniformément distribuées, alors

$$\begin{aligned} p(\mathbf{r}_K|q) &= \int_0^{2\pi} p(\mathbf{r}_K|q,\phi_q)p(\phi_q)d\phi_q \\ &= \left(\prod_{k=1}^{K} 2\pi\sigma^2\right) \exp\left(-\sum_{k=1}^{K} \frac{(|r_k|^2+\alpha^2|s_{q,k}|^2)}{2\sigma^2}\right) \\ &\times \frac{1}{2\pi}\int_0^{2\pi} \exp\left(Re\left[\alpha e^{-j\phi_q}\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right]\right) d\phi_q \end{aligned}$$

L'intégrale ci-dessus se calcule facilement. En effet, la fonction de Bessel modifiée d'ordre zéro, $I_0(x)$, est définie par [41]

$$I_0(x) \triangleq \frac{1}{2\pi}\int_0^{2\pi} e^{x\cos(\beta+\phi)}d\beta \tag{1.56}$$

En remarquant que

$$Re\left[\alpha e^{-j\phi_q}\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right] = Re\left[\alpha e^{-j\phi_q}\left|\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right| e^{j\phi}\right] = \alpha\left|\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right| cos(-\phi_q+\phi)$$

la densité de probabilité $p(\mathbf{r}_K|q)$ devient

$$\begin{aligned} p(\mathbf{r}_K|q) &= \left(\prod_{k=1}^{K} 2\pi\sigma^2\right) \exp\left(-\sum_{k=1}^{K} \frac{(|r_k|^2+\alpha^2|s_{q,k}|^2)}{2\sigma^2}\right) \\ &\times I_0\left(\alpha\left|\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right|\right) \end{aligned} \tag{1.57}$$

En utilisant la relation (1.57), on peut former le rapport de vraisemblance

$$\begin{aligned} \Lambda_{\ell q}(\mathbf{r}_K) &= \frac{p(\mathbf{r}_K|\ell)}{p(\mathbf{r}_K|q)} \\ &= \exp\left(-\frac{\alpha^2}{2}\sum_{k=1}^{K}\frac{|s_{\ell,k}|^2-|s_{q,k}|^2}{\sigma^2}\right)\frac{I_0\left(\alpha\left|\sum_{k=1}^{K}\frac{r_k s_{\ell,k}^*}{\sigma^2}\right|\right)}{I_0\left(\alpha\left|\sum_{k=1}^{K}\frac{r_k s_{q,k}^*}{\sigma^2}\right|\right)} \end{aligned}$$

Quand $K\to\infty$, $\Lambda_{\ell q}(\mathbf{r}_K)$ tend vers

$$\begin{aligned} \Lambda_{\ell q}(\mathbf{r}) &= \exp\left(-\frac{\alpha^2}{2}\left[\int_0^T s_\ell(t)g_\ell^*(t)dt - \int_0^T s_q(t)g_q^*(t)dt\right]\right) \\ &\times\frac{I_0\left[|\alpha|\int_0^T r(t)g_\ell^*(t)dt|\right]}{I_0\left[|\alpha|\int_0^T r(t)g_q^*(t)dt|\right]} \end{aligned}$$

où les $g_q(t)$ sont définis par $g_q(t) = \lim_{K\to\infty}\sum_{k=1}^{K}\frac{s_{q,k}}{\sigma^2}\psi_k(t) = \frac{s_q(t)}{\sigma^2}$. La dernière égalité est obtenue par définition du développement de Karhunen-Loève.

Lorsque les signaux sont équiprobables, maximiser $P(q|\mathbf{r})$ revient à maximiser les densités de probabilité conditionnelles $p(\mathbf{r}|q)$. Ceci équivaut au calcul des Q variables

$$L_q = \exp\left[-\frac{\alpha^2}{2}\int_0^T s_q(t)g_q^*(t)dt\right] I_0\left[\alpha\left|\int_0^T r(t)g_q^*(t)dt\right|\right] \quad q = 1,\ldots,Q$$

Il suffit ensuite de choisir parmi les Q signaux celui qui maximise L_q. Par ailleurs, les signaux de la modulation Q-FSK sont de même énergie, et le bruit additif gaussien est blanc. Par conséquent, le terme de la forme $\exp\left[-\frac{\alpha^2}{2}\int_0^T s_q(t)g_q^*(t)dt\right]$ est un terme de biais, indépendant de l'observation. En effet, dans ces conditions, $g_q(t) = \frac{s_q(t)}{\sigma^2}$ devient $\frac{s_q(t)}{N_0}$ et $\exp\left[-\frac{\alpha^2}{2}\int_0^T s_q(t)g_q^*(t)dt\right]$ devient $\exp\left[-\frac{\alpha^2 E}{N_0}\right]$. Ce dernier terme est commun à tous les L_q et n'intervient pas dans la maximisation.

D'autre part, la fonction de Bessel modifiée d'ordre zéro est une fonction croissante positive. Rechercher le maximum de $I_0(x)$ équivaut tout simplement à maximiser x. Puisque le facteur $\frac{\alpha}{N_0}$ est constant, le détecteur optimal utilise le critère suivant

$$\max_{q=1}^{Q}\left|\int_0^T r(t)s_q^*(t)dt\right| \tag{1.58}$$

1.6 Annexe 1.II : Etude des variations de $P(S_i \to S_j)$

La probabilité d'erreur par paire de signaux Q-FSK multidimensionnels en détection non cohérente dépend de deux paramètres

$$X_i = \frac{\alpha^2 NE}{N_0} \tag{1.59}$$

et

$$X_j = \frac{\alpha^2 E}{N_0}\sum_{n=1}^{N}\left(\frac{sin(\pi\Delta f_n T)}{\pi\Delta f_n T}\right)^2 \tag{1.60}$$

Dans [64], il est montré que la probabilité d'erreur par paire diminue lorsque X_i augmente – soit une augmentation de l'énergie à corrélation fixe – ou bien lorsque X_j diminue. Dans ce cas, c'est le deuxième terme de la probabilité d'erreur qui diminue.

On note

$$f(X_i, X_j) = \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\left(1 - \sum_{\ell=0}^{w-N} e^{-X_j}\frac{X_j^\ell}{\ell!}\right)$$

Commençons par simplifier l'écriture de $f(X_i, X_j)$.

$$\begin{aligned}
f(X_i,X_j) &= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\left(1-\sum_{\ell=0}^{w-N} e^{-X_j}\frac{X_j^\ell}{\ell!}\right)\\
&= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\left(1-e^{-X_j}\sum_{\ell=0}^{w-N}\frac{X_j^\ell}{\ell!}\right)\\
&= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\left(1-e^{-X_j}\left(e^{X_j}-\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^\ell}{\ell!}\right)\right)\\
&= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\left(1-1+e^{-X_j}\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^\ell}{\ell!})\right)\\
&= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)e^{-X_j}\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^\ell}{\ell!}
\end{aligned}$$

Par définition, X_i et X_j sont positifs. Alors, $g_{N,X_i,1}(w)$ est une somme infinie de termes positifs et $f(X_i, X_j)$ est toujours positive.

Dérivons $f(X_i, X_j)$ par rapport à X_j.

$$\begin{aligned}
\frac{\partial}{\partial X_j}f(X_i,X_j) &= -e^{-X_j}\sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^\ell}{\ell!}+\sum_{w=N}^{+\infty} g_{N,X_i,1}(w)e^{-X_j}\sum_{\ell=w-N+1}^{+\infty}\frac{\ell X_j^{\ell-1}}{\ell!}\\
&= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)e^{-X_j}\left(\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^{\ell-1}}{(\ell-1)!}-\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^\ell}{\ell!}\right)\\
&= \sum_{w=N}^{+\infty} g_{N,X_i,1}(w)e^{-X_j}\left(\sum_{\ell=w-N}^{+\infty}\frac{X_j^\ell}{\ell!}-\sum_{\ell=w-N+1}^{+\infty}\frac{X_j^\ell}{\ell!}\right)\\
&= e^{-X_j}\sum_{w=N}^{+\infty} g_{N,X_i,1}(w)\frac{X_j^{w-N}}{(w-N)!}
\end{aligned}$$

La dérivée de $f(X_i, X_j)$ par rapport à X_j est toujours positive. On en déduit que $f(X_i, X_j)$ est monotone croissante en X_j. Une diminution de X_j, c'est-à-dire un choix judicieux de la répartition des fréquences, réduira $f(X_i, X_j)$. Dans ce cas, la probabilité d'erreur par paire et par suite la probabilité d'erreur seront minimisées.

Par ailleurs, $f(X_i, X_j)$ et la probabilité d'erreur par paire sont toutes deux monotones décroissantes en X_i.

Toute méthode générale de conception d'alphabets de signaux corrélés devra tenir compte de ces deux résultats afin d'optimiser les performances atteintes.

Chapitre 2

Modulations codées à composantes corrélées *

Le chapitre précédent a montré que l'utilisation de signaux corrélés permet d'augmenter l'efficacité spectrale des modulations classiquement utilisées – en particulier les modulations Q-FSK – dans les systèmes de communications avec détection non cohérente. Malheureusement, si l'on se contente de diminuer l'espacement fréquentiel, cette augmentation de l'efficacité spectrale s'accompagne d'une dégradation significative des performances. L'étude de la capacité et un exemple pratique d'alphabet de diversité 4 sur canal de Rayleigh ont montré qu'en construisant des constellations multidimensionnelles à composantes corrélées, il est possible de compenser ces pertes de performances. Enfin, nous avons remarqué que toute technique de codage ou de diversité conduit à de telles constellations. Dans ce chapitre et dans le suivant, nous nous consacrons uniquement à des constructions multidimensionnelles créées grâce à diverses méthodes de codage. Dans un premier temps, le canal considéré est gaussien.

La latence d'un schéma de codage est habituellement reliée au délai ou retard temporel que ce dernier induit. Le délai maximal admissible est parfaitement déterminé par l'application envisagée. Nous considérons des techniques de codage de faible latence : les modulations codées en blocs [12][26][35][37] ou en treillis [15].

Le premier paragraphe décrit le modèle de transmission, ainsi que les deux techniques de décodage envisagées. Le décodage classique à maximum de vraisemblance repose sur le critère multidimensionnel optimal de détection non cohérente déterminé au chapitre 1. Le décodage sous-optimal associe une démodulation non cohérente fondée sur le calcul de probabilités *a posteriori* et un décodage à entrée souple.

De bons résultats sont obtenus sur canal gaussien avec les modulations codées en treillis ou encore les réseaux de points [26] (équivalents à des modulations codées en blocs). Afin d'appréhender au mieux les caractéristiques et les avantages de ces deux méthodes, nous rappelons les résultats importants les concernant.

*Les résultats de ce chapitre ont été présentés au *Sixth Canadian Workshop on Information Theory*, Kingston, Ontario, Canada, juin 1999, et ont été publiés dans *IEEE Communication Letters*, octobre 2000.

Finalement, nous nous intéressons aux performances des systèmes codés. Le choix de l'espacement fréquentiel n'est pas anodin : il est toujours important de veiller à ce que le gain d'efficacité spectrale ne soit pas obtenu au prix d'une dégradation trop importante des performances. Dans le cas des modulations codées en blocs, cet espacement fréquentiel peut être relié aux paramètres fondamentaux du réseau et on montre qu'il faut choisir un réseau dense [26] pour obtenir de meilleures performances.

2.1 Codage faible latence pour les signaux corrélés

2.1.1 Modèle du système

Conformément aux notations introduites au chapitre précédent, Δf_0, T et $2E$ désignent respectivement l'espacement fréquentiel, le temps symbole de la modulation Q-FSK et l'énergie en bande de base des signaux de la Q-FSK.

Le modèle de transmission pour un alphabet FSK multidimensionnel associé à des techniques de codage faible latence est donné figure 2.1.

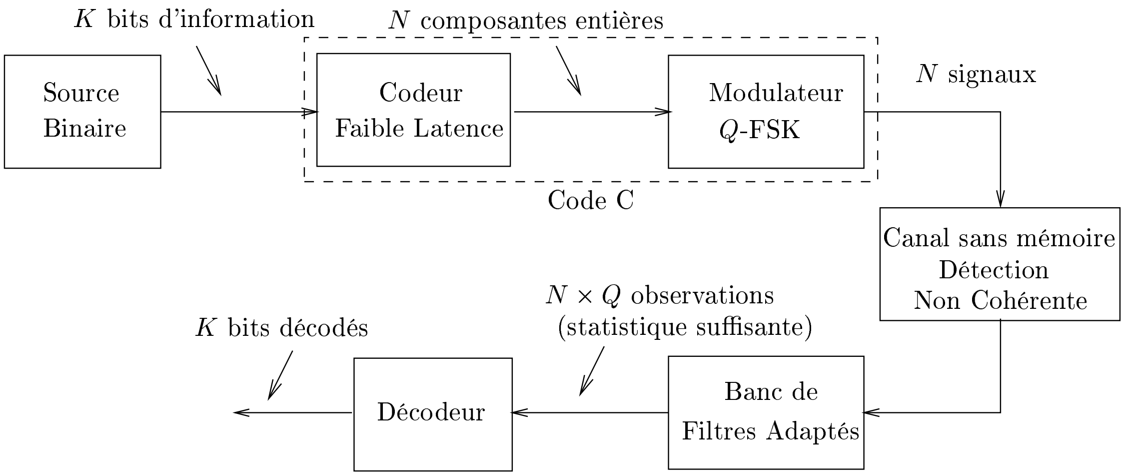


Fig. 2.1 – Modèle de transmission. Alphabet FSK multidimensionnel codé.

Chaque bloc de K bits d'information, $(b_1, b_2, \ldots, b_K)$, est codé et sert à étiqueter N composantes entières p_n, $n = 1, \ldots, N$, chacune d'entre elles appartenant à l'ensemble de taille Q $\{\pm 1, \pm 3, \ldots, \pm(Q-1)\}$. p_n est donc un symbole d'une modulation d'amplitude (PAM, Pulse Amplitude Modulation) de taille Q. Le schéma de codage est composé d'une modulation codée en treillis ou d'un réseau de points (modulation codée en blocs). Les entiers p_n sont groupés pour former un vecteur de dimension N, $P = (p_1, \ldots, p_N)$. Les K bits d'information permettent ainsi de coder $M = 2^K$ points de dimension N que l'on notera P_m, $m = 1, \ldots, M$.

Le vecteur $P_m = (p_{m,1}, \ldots, p_{m,N})$ est alors associé, par l'intermédiaire du modulateur, au signal $S_m = (s_{m,1}, \ldots, s_{m,N})$. Chaque composante $s_{m,n} = p_{m,n}$ représente le choix d'une fréquence parmi les Q possibles à l'instant n. Elle correspond à l'émission physique du signal élémentaire

$s_{m,n}(t)$ issu de la modulation Q-FSK, précédemment défini au paragraphe 1.1.1 par

$$s_{m,n}(t) = \sqrt{\frac{2E}{T}} e^{j2\pi f_{m,n} t} \quad 0 \leq t < T \text{ et } 1 \leq n \leq N$$

La fréquence élémentaire $f_{m,n}$ prend Q valeurs possibles uniformément séparées de Δf_0 et elle est proportionnelle à la $n$ième composante $s_{m,n}$. Puisque $s_{m,n}$ appartient à l'ensemble $\{\pm 1, \pm 3, \ldots, \pm(Q-1)\}$, on a

$$f_{m,n} = p_{m,n} \times \frac{\Delta f_0}{2}$$

La concaténation du codeur faible latence et du modulateur FSK forme ainsi un nouveau code noté C. Ce dernier délivre un signal appartenant à un alphabet FSK multidimensionnel codé de M signaux S_m, $m = 1, \ldots, M$ de longueur N. Les composantes d'un signal multidimensionnel S_m peuvent être émises sur des temps symboles consécutifs lorsqu'une seule porteuse est disponible, ou réparties dans le plan temps-fréquence, lorsque l'on dispose de plusieurs porteuses.

Le canal gaussien sans mémoire est caractérisé par une atténuation constante α, parfaitement connue du récepteur, une phase aléatoire $\phi_{m,n}$ uniformément distribuée sur $[0, 2\pi]$, inconnue du récepteur et un bruit complexe $b_n(t)$ additif blanc gaussien de densité spectrale de puissance $2\sigma_b^2 = 2N_0$.

En supposant que le signal S_i a été émis, on reçoit le vecteur $R(t) = (r_1(t), \ldots, r_N(t))$ où pour tout $n = 1, \ldots, N$

$$r_n(t) = \alpha e^{j\phi_{i,n}} s_{i,n}(t) + b_n(t)$$

Le détecteur non cohérent optimal à maximum de vraisemblance pour des signaux multidimensionnels sur le canal gaussien se compose d'un banc de Q filtres adaptés aux Q fréquences possibles de la modulation FSK comme nous l'avons vu au paragraphe 1.2.2. L'observation totale en sortie du banc de filtres est formée des M vecteurs $(x_{m,1}, x_{m,2}, \ldots, x_{m,N})$ où pour $m = 1, \ldots, M$ et $n = 1, \ldots, N$

$$x_{m,n} = \int_0^T r_n(t) s^*_{m,n}(t) dt = \alpha e^{j\phi_{i,n}} \mu_n^{i,m} + b_{m,n}$$

$\mu_n^{i,m} = \int_0^T s_{i,n}(t) s_{m,n}{}^*(t) dt$ est la corrélation de la $n$ième composante des signaux S_i et S_m, et $b_{m,n} = \int_0^T b(t) s_{m,n}{}^*(t) dt$ est un bruit discret complexe additif blanc gaussien de densité spectrale de puissance $4E\sigma_b^2 = 4N_0 E$.

En pratique, chaque composante $r_n(t)$ du signal $R(t)$ est filtrée par les Q signaux FSK $s_q(t) = \sqrt{2E/T} e^{j2\pi f_q t}$, $q = 0, \ldots, Q-1$. La corrélation en sortie du $q$ième filtre adapté est définie par

$$x_{q,n} = \int_0^T r_n(t) s_q^*(t) dt$$

$|x_n| = (|x_{0,n}|, |x_{1,n}|, \ldots, |x_{Q-1,n}|)$ est l'observation totale pour la composante n. L'ensemble des $N \times Q$ valeurs $|x_{q,n}|$ qui forme une statistique suffisante en sortie du banc de filtres, est utilisée par le décodeur qui délivre alors une estimation des K bits d'information.

Dans le cas de signaux ayant même probabilité *a priori*, le détecteur non cohérent à maximum de vraisemblance est équivalent au détecteur maximum *a posteriori*. Les calculs qui conduisent au critère de détection optimal et à l'expression de la probabilité d'erreur par paire $P(S_i \to S_j)$ sont détaillés aux paragraphes 1.2.2 et 1.2.3. On obtient comme critère

$$\max_{m=1}^{M} \prod_{n=1}^{N} I_0 \left(\frac{\alpha}{N_0} \left| \int_0^T r_n(t) s_{m,n}^*(t) dt \right| \right)$$

dont une expression plus simple et équivalente est donnée par

$$\max_{m=1}^{M} \sum_{n=1}^{N} \left| \int_0^T r_n(t) s_{m,n}^*(t) dt \right|^2 \tag{2.1}$$

tandis que

$$P(S_i \to S_j) = \underbrace{\sum_{w=0}^{N-1} g_{N,X_i}(w)}_{P_1} + \underbrace{\sum_{w=N}^{+\infty} g_{N,X_i}(w) \left(1 - \sum_{\ell=0}^{w-N} e^{-X_j} \frac{(X_j)^\ell}{\ell!} \right)}_{P_2} \tag{2.2}$$

où la fonction $g_{N,X_i}(w)$ est définie par

$$g_{N,X_i}(w) = \frac{1}{2^{w+N} w!} \times \sum_{k=0}^{+\infty} e^{-X_i} \frac{(N+k+w-1)!}{2^k k!(N+k-1)!} (X_i)^k$$

Les paramètres X_i et X_j dépendent des signaux S_i et S_j puisqu'ils sont directement reliés aux coefficients de corrélation. Nous connaissons leurs expressions

$$X_i = \frac{\alpha^2 N E}{N_0} \quad \text{et} \quad X_j = \frac{\alpha^2 E}{N_0} \sum_{n=1}^{N} \left(\frac{\sin(\pi \Delta f_n T)}{\pi \Delta f_n T} \right)^2$$

$\Delta f_n = f_{i,n} - f_{j,n}$ est l'écart de fréquence entre les $n$ièmes composantes des signaux S_i et S_j.

La probabilité d'erreur par paire de l'équation (2.2) est constituée de deux termes. Le premier, noté P_1, est fonction de X_i et dépend de l'énergie du signal émis, tandis que le second, noté P_2, est fonction de X_j et est principalement lié aux corrélations entre les signaux. Lorsque l'espacement fréquentiel de la modulation Q-FSK est égal à $1/T$, les signaux élémentaires $s_{m,n}(t)$ sont orthogonaux et le terme P_2 de l'équation (2.2) est nul. Pour le cas que nous considérons dans ce chapitre, Δf_0 est strictement inférieur à $1/T$; les signaux élémentaires sont corrélés et la bande est réduite. Dans ces conditions, X_j et P_2 sont strictement positifs. Nous veillerons par conséquent à construire des alphabets qui garantissent une bonne distribution des corrélations entre les signaux afin de minimiser P_2.

Le décodage exhaustif fondé sur l'utilisation du critère optimal (2.1) devient très complexe quand on travaille avec des alphabets de grande taille. Selon le schéma de codage choisi, nous proposons deux types de décodeur. Le premier, détaillé au paragraphe 2.1.2, effectue un décodage à maximum de vraisemblance. Le second, décrit au paragraphe 2.1.3 est sous optimal. Il repose sur une démodulation non cohérente qui calcule les probabilités *a posteriori* nécessaires pour le décodeur de réseaux de points.

2.1.2 Décodage à maximum de vraisemblance

Ce premier type de décodage est appliqué aux alphabets FSK muldidimensionnels codés par une modulation codée en treillis. La structure du récepteur est illustrée figure 2.2.

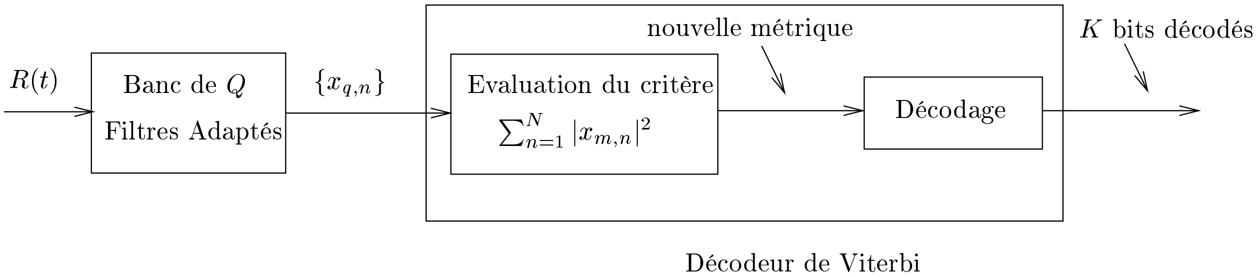


FIG. 2.2 – Structure du récepteur avec décodage à maximum de vraisemblance.

En sortie du banc de filtres adaptés, le critère de détection appliqué est le critère du maximum *a posteriori* par blocs. Puisque tous les signaux émis ont même probabilité *a priori*, celui-ci est en effet parfaitement équivalent au critère du maximum de vraisemblance [11]. Les $N \times Q$ sorties de filtres adaptés $\{x_{q,n}\}$ sont directement utilisées pour calculer les M valeurs du critère de détection optimal $\sum_{n=1}^{N} |x_{m,n}|^2$. En effet, chaque valeur $x_{m,n}$ correspond à une sortie $x_{q,n}$ où $q = s_{m,n}$ est le numéro de la fréquence émise sur la composante n du signal S_m.

Le décodage optimal au sens du maximum de vraisemblance d'un code convolutif est obtenu par la recherche dans le treillis du code de la séquence la plus probable [57] au moyen de l'algorithme de Viterbi [34][72]. Selon la nature de l'estimation fournie par le démodulateur (dure ou souple), les métriques utilisées seront respectivement une métrique de Hamming ou une métrique euclidienne. Une métrique cumulative est évaluée le long du treillis du code. On appelle survivants les chemins conservés à l'étape t du décodage. Il y a un unique survivant par état, et autant de survivants que d'états. Chaque survivant est associé à une valeur de la métrique. A un instant donné, le choix entre deux chemins possibles se fait en conservant celui de métrique minimale. Si deux ou plusieurs chemins ont la même métrique, on en choisit un aléatoirement parmi les candidats possibles.

Soit un code convolutif binaire (k, n) de longueur de contrainte L. Le treillis de ce code comporte $2^{k(L-1)}$ états. L'algorithme nécessite donc la mise en mémoire de $2^{k(L-1)}$ survivants et $2^{k(L-1)}$ métriques à chaque étape. La complexité de l'algorithme de Viterbi varie exponentiellement avec k et L. Afin de ne pas trop souffrir du retard dû au décodage, on peut modifier l'algorithme et effectuer le décodage sur une fenêtre glissante de taille finie W. Si on choisit W de telle sorte que $W > 5L$, les performances du décodage ne sont pas dégradées [57].

Nous utilisons les sorties du banc de filtres adaptés pour évaluer de nouvelles valeurs des métriques. L'algorithme de Viterbi s'appuie ainsi sur le treillis de la modulation codée en treillis, schéma pour lequel nous appliquons cette méthode optimale de décodage. Le paragraphe 2.2.2 décrit plus précisément le calcul des métriques, tandis que les résultats de simulation sont donnés au paragraphe 2.4.

Notons que ce décodage bloc classique convient bien aux TCM car l'étiquetage est optimisé de façon à garantir une distance minimale maximum entre les signaux ou de manière équivalente d'une branche à l'autre du treillis.

2.1.3 Démodulation non cohérente APP et décodage à entrée souple

Cependant, la mise en œuvre du décodage ML n'est pas toujours évidente. Si dans le cas des TCM, cela se traduit par une simple modification du calcul de la métrique dans l'algorithme de Viterbi, les choses deviennent plus complexes pour les réseaux de points. Un décodage ML du code C (concaténation du réseau et de la modulation Q-FSK) revient à évaluer le critère (2.1) de manière exhaustive pour les 2^K points du réseau (K étant le nombre de bits d'information par point). Par exemple, $K = 11$ pour le réseau D_4 de Schlafli en dimension 4 ; $K = 20$ pour le réseau E_8 de Gosset en dimension 8 et $K = 48$ pour le réseau Λ_{24} de Leech en dimension 24. Le nombre de points et par conséquent la complexité du décodage augmentent rapidement. Ces derniers deviennent alors des facteurs prohibitifs à l'utilisation d'une telle technique de décodage. Par ailleurs, on connaît plusieurs algorithmes qui permettent de décoder les réseaux de points sur canal gaussien. Décrites au paragraphe 2.3.5, la plupart de ces techniques reposent sur le décodage à entrée souple des codes en blocs [25]. L'algorithme de décodage par sphères [17][76], quant à lui, est un décodeur ML de faible complexité pour les constellations de réseaux de points. Tous ces algorithmes nécessitent une information souple sur les symboles en entrée.

Si une décision est prise en faveur de la plus grande valeur en module de la sortie du $q$ième filtre adapté pour la $n$ième composante $x_{q,n}$, on obtient une estimation dure du point émis. Nous cherchons ici à associer la démodulation non cohérente aux décodeurs connus de réseaux de points ; il nous faut donc convertir les sorties du banc de filtres adaptés en informations souples sur les symboles émis. La structure du récepteur sous-optimal obtenu est donnée figure 2.3. La sous-optimalité est directement liée au bloc "Convertisseur signal-APP" que nous allons décrire.

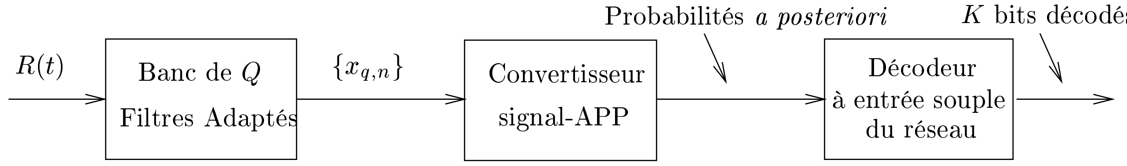


Fig. 2.3 – Structure du récepteur avec décodage APP.

L'entrée souple fournie au décodeur de réseau de points doit être sous la forme d'un vecteur de N composantes. On la note $\tilde{P} = (\tilde{p}_1, \tilde{p}_2, \ldots, \tilde{p}_N)$. Nous proposons de calculer chaque estimation souple $\tilde{p}_n$ comme suit

$$\tilde{p}_n = \sum_{q=0}^{Q-1} (2q - Q + 1)\mathrm{APP}(q, n) \tag{2.3}$$

où $\mathrm{APP}(q, n)$ désigne la probabilité *a posteriori* de la fréquence q à l'instant n. Par définition,

$$\mathrm{APP}(q, n) = p(q/|x_{0,n}|, |x_{1,n}|, ..., |x_{Q-1,n}|)$$

Les Q fréquences de la modulation sont équiprobables et l'observation $|x_n|$ est la même à un instant n donné pour les Q calculs. Par conséquent, une simple application de la loi de Bayes donne

$$\mathrm{APP}(q,n) \propto p(|x_{0,n}|, |x_{1,n}|, \ldots, |x_{Q-1,n}|/q) \tag{2.4}$$

Lorsque les signaux FSK sont orthogonaux, les sorties du banc de filtres adaptés sont parfaitement indépendantes les unes des autres. Dans ce cas, la densité de probabilité conjointe conditionnellement à la fréquence q de l'équation (2.4) s'écrit comme le produit de probabilités conditionnelles marginales. Les simulations ont montré que l'utilisation de cette approximation reste valable lorsque les signaux sont corrélés, c'est-à-dire pour des valeurs de l'espacement fréquentiel $\Delta f_0 < 1/T$. Nous utilisons donc l'expression sous-optimale suivante de la probabilité *a posteriori* $\mathrm{APP}(q,n)$

$$APP(q,n) \propto \prod_{k=0}^{Q-1} p(|x_{k,n}|/q) \tag{2.5}$$

Rappelons que les sorties des filtres adaptés sont données par

$$|x_{k,n}| = \left|\alpha e^{j\phi_{i,n}} \mu_n^{i,k} + b_k\right|$$

Puisque nous supposons que les signaux sont orthogonaux, et si la fréquence q correspond à la fréquence émise sur la composante n du signal (c'est-à-dire $s_{i,n} = q$), la variable aléatoire $|x_{q,n}|$ suit une loi de Rice de paramètre $\beta^2 = 4\alpha^2 E^2$ ($x_{q,n}$ est une variable aléatoire gaussienne complexe non centrée de variance $\sigma^2_{Rice} = 4E^2\sigma^2$)

$$p(|x_{q,n}|/q) = \frac{|x_{q,n}|}{\sigma^2_{Rice}} \exp\left(-\frac{|x_{q,n}|^2 + \beta^2}{2\sigma^2_{Rice}}\right) I_0\left(\frac{|x_{q,n}|\beta}{\sigma^2_{Rice}}\right)$$

tandis que les $Q-1$ variables aléatoires $|x_{k,n}|$, $k \neq q$, suivent une loi de Rayleigh ($x_{k,n}$ est une variable aléatoire gaussienne complexe centrée de variance $\sigma^2_{Rayl} = 4E^2\sigma^2$)

$$p(|x_{k,n}|/q) = \frac{|x_{q,n}|}{\sigma^2_{Rayl}} \exp\left(-\frac{|x_{q,n}|^2}{2\sigma^2_{Rayl}}\right)$$

En effet, par définition, l'autocorrélation $\mu_n^{i,i}$ est égale à l'énergie des signaux FSK en bande de base, soit $2E$. Par ailleurs, le bruit b_k est un bruit filtré. Les valeurs $\mathrm{APP}(q,n)$ décrites par l'équation (2.5) sont ensuite normalisées afin d'assurer des probabilités *a posteriori* comprises entre 0 et 1.

Le bloc “Convertisseur signal-APP” est chargé de mettre en œuvre les opérations ainsi décrites pour chaque composante à l'instant n : calcul des Q vraisemblances $p(|x_{k,n}|/q)$, $k = 0, \ldots, Q-1$, calcul des Q probabilités *a posteriori* $\mathrm{APP}(q,n)$ et normalisation de ces Q valeurs. Après N utilisations de ce bloc, on évalue le point $\tilde{P}$ qui sera présenté en entrée du décodeur de réseau de points.

Décrivons à présent le calcul des probabilités *a posteriori* $\mathrm{APP}(q,n)$ tant dans le cas d'une transmission sur canal gaussien que sur canal de Rayleigh.

2.1.4 Calcul des APP pour le canal gaussien

La transmission est tout d'abord envisagée sur un canal gaussien de gain unitaire $\alpha = 1$. Une expression plus précise de la probabilité *a posteriori* peut alors être calculée par

$$\mathrm{APP}(q,n) \quad \propto \quad \frac{|x_{q,n}|}{4E^2\sigma^2}\exp\left(-\frac{|x_{q,n}|^2+4E^2}{8E^2\sigma^2}\right)I_0\left(\frac{2|x_{q,n}|}{4E\sigma^2}\right)\times\prod_{k=0,k\neq q}^{Q-1}\frac{|x_{k,n}|}{4E^2\sigma^2}\exp\left(-\frac{|x_{k,n}|^2}{8E^2\sigma^2}\right)$$

ou de manière plus compacte

$$\mathrm{APP}(q,n) \quad \propto \quad \left(\prod_{k=0}^{Q-1}\frac{|x_{k,n}|}{4E^2\sigma^2}\right)\times\exp\left(-\frac{1}{2\sigma^2}\right)I_0\left(\frac{|x_{q,n}|}{2E\sigma^2}\right)\times\exp\left(-\sum_{k=0}^{Q-1}\frac{|x_{k,n}|^2}{8E^2\sigma^2}\right)$$

Après normalisation, on obtient

$$\mathrm{APP}(q,n) = \frac{\left(\prod_{k=0}^{Q-1}\frac{|x_{k,n}|}{4E^2\sigma^2}\right)\times\exp\left(-\frac{1}{2\sigma^2}\right)I_0\left(\frac{|x_{q,n}|}{2E\sigma^2}\right)\times\exp\left(-\sum_{k=0}^{Q-1}\frac{|x_{k,n}|^2}{8E^2\sigma^2}\right)}{\sum_{\chi=0}^{Q-1}\left(\prod_{k=0}^{Q-1}\frac{|x_{k,n}|}{4E^2\sigma^2}\right)\times\exp\left(-\frac{1}{2\sigma^2}\right)I_0\left(\frac{|x_{\chi,n}|}{2E\sigma^2}\right)\times\exp\left(-\sum_{k=0}^{Q-1}\frac{|x_{k,n}|^2}{8E^2\sigma^2}\right)}$$

soit

$$\mathrm{APP}(q,n) = \frac{I_0\left(\frac{|x_{q,n}|}{2E\sigma^2}\right)}{\sum_{\chi=0}^{Q-1} I_0\left(\frac{|x_{\chi,n}|}{2E\sigma^2}\right)} \tag{2.6}$$

2.1.5 Calcul des APP pour le canal de Rayleigh

Sur un canal de Rayleigh de gain α, les expressions se récrivent comme suit

$$\mathrm{APP}(q,n/\alpha) \quad \propto \quad \frac{|x_{q,n}|}{4E^2\sigma^2}\exp\left(-\frac{|x_{q,n}|^2+4\alpha^2E^2}{8E^2\sigma^2}\right)I_0\left(\frac{2\alpha|x_{q,n}|}{4E\sigma^2}\right)\times\prod_{k=0,k\neq q}^{Q-1}\frac{|x_{k,n}|}{4E^2\sigma^2}\exp\left(-\frac{|x_{k,n}|^2}{8E^2\sigma^2}\right)$$

Avant normalisation, on obtient

$$\mathrm{APP}(q,n/\alpha) \quad \propto \quad \left(\prod_{k=0}^{Q-1}\frac{|x_{k,n}|}{4E^2\sigma^2}\right)\times\exp\left(-\frac{\alpha^2}{2\sigma^2}\right)I_0\left(\alpha\frac{|x_{q,n}|}{2E\sigma^2}\right)\times\exp\left(-\sum_{k=0}^{Q-1}\frac{|x_{k,n}|^2}{8E^2\sigma^2}\right) \tag{2.7}$$

Lorsque la détection est non cohérente, deux possiblités se présentent. Dans le cas d'évanouissements lents, et bien que la phase soit inconnue du récepteur, on peut envisager d'estimer la puissance reçue. On dispose alors d'une valeur connue du gain du canal α. Ainsi, l'expression de $\mathrm{APP}(q,n/\alpha)$ se simplifie. Tout calcul fait :

$$\mathrm{APP}(q,n) = \frac{I_0\left(\frac{\alpha|x_{q,n}|}{2E\sigma^2}\right)}{\sum_{\chi=0}^{Q-1} I_0\left(\frac{\alpha|x_{\chi,n}|}{2E\sigma^2}\right)} \tag{2.8}$$

En revanche, si les évanouissements sont rapides, on ne pourra plus estimer correctement la puissance reçue. Dans ce cas, il s'agit de moyenner les probabilités *a posteriori* $\mathrm{APP}(q, n/\alpha)$ par rapport à α. L'expression devient

$$\mathrm{APP}(q, n) = \int_0^\infty \mathrm{APP}(q, n/\alpha) p(\alpha) d\alpha$$

où $p(\alpha) = 2\alpha e^{-\alpha^2}$.

Seuls les termes de $\mathrm{APP}(q, n/\alpha)$ contenant α sont importants pour le moyennage. Ainsi, le facteur $\left(\prod_{k=0}^{Q-1} \frac{|x_{k,n}|}{4E^2\sigma^2}\right) \times \exp\left(-\sum_{k=0}^{Q-1} \frac{|x_{k,n}|^2}{8E^2\sigma^2}\right)$ est volontairement oublié dans le calcul qui suit. Alors,

$$\mathrm{APP}(q, n) \propto \int_0^\infty \exp\left(-\frac{\alpha^2}{2\sigma^2}\right) I_0\left(\frac{\alpha |x_{q,n}|}{2E\sigma^2}\right) 2\alpha e^{-\alpha^2} d\alpha$$

En utilisant le changement de variable $u = \alpha^2$, on a

$$\mathrm{APP}(q, n) \propto \int_0^\infty \exp\left(-\left[\frac{1}{2\sigma^2} + 1\right] u\right) I_0\left(\frac{|x_{q,n}|}{2E\sigma^2}\sqrt{u}\right) du \qquad (2.9)$$

L'intégrale ci-dessus est connue et donnée par [41]

$$\int_0^\infty e^{-ax} I_{2\nu}(2\sqrt{\beta x}) dx = \frac{e^{\frac{\beta}{2\alpha}}}{\sqrt{\alpha\beta}} \frac{\Gamma(\nu+1)}{\Gamma(2\nu+1)} M_{-1/2,\nu}\left(\frac{\beta}{\alpha}\right) \quad Re(a) > 0 \text{ et } Re(\nu) > -1 \qquad (2.10)$$

$M_{-1/2,\nu}(t)$ est la fonction de Whittaker. On en connait une expression générale en fonction de $\Phi(t)$, fonction hypergéométrique dégénérée [41]

$$M_{\lambda,\mu}(z) = z^{\mu+\frac{1}{2}} e^{-\frac{z}{2}} \Phi\left(\mu - \lambda + \frac{1}{2}, 2\mu + 1; z\right)$$

L'intégrale de l'équation (2.9) peut être identifiée à celle de (2.10) où $a = 1 + \frac{1}{2\sigma^2}$, $b = \frac{|x_{q,n}|^2}{16E^2\sigma^4}$ et $\nu = 0$. On obtient

$$\mathrm{APP}(q, n) \propto \frac{e^{\frac{b}{2a}}}{\sqrt{ab}} M_{-1/2,0}(\frac{b}{a})$$

En utilisant la propriété $\Phi(\xi, \xi; z) = e^z$, on trouve

$$M_{-1/2,0}\left(\frac{b}{a}\right) = \sqrt{\frac{b}{a}} \exp\left(\frac{b}{2a}\right)$$

Finalement,

$$\mathrm{APP}(q, n) \propto \frac{1}{a} \exp\left(\frac{b}{a}\right)$$

En remplaçant a et b par leur valeur et en simplifiant, on obtient

$$\mathrm{APP}(q, n) \propto \frac{2\sigma^2}{1 + 2\sigma^2} \exp\left(\frac{|x_{q,n}|^2}{8E^2\sigma^2(1 + 2\sigma^2)}\right)$$

Tous les termes volontairement oubliés pour le moyennage sont identiques, quelle que soit la valeur de q. Ainsi, après normalisation, les probabilités *a posteriori* $\mathrm{APP}(q,n)$ pour un canal de Rayleigh variant rapidement sont données par

$$\mathrm{APP}(q,n) = \frac{\exp\left(\frac{|x_{q,n}|^2}{8E^2\sigma^2(1+2\sigma^2)}\right)}{\sum_{\chi=0}^{Q-1}\exp\left(\frac{|x_{\chi,n}|^2}{8E^2\sigma^2(1+2\sigma^2)}\right)} \tag{2.11}$$

En pratique, lorsqu'il est possible de considérer $2\sigma^2 << 1$, une expression plus compacte des APP de la formule (2.11) est

$$\mathrm{APP}(q,n) = \frac{\exp\left(\frac{|x_{q,n}|^2}{8E^2\sigma^2}\right)}{\sum_{\chi=0}^{Q-1}\exp\left(\frac{|x_{\chi,n}|^2}{8E^2\sigma^2}\right)} \tag{2.12}$$

Il s'est révélé nécessaire de modifier légèrement les probabilités *a posteriori* des équations (2.6), (2.8) et (2.12) afin d'obtenir des expressions numériquement stables pour les simulations. C'est pourquoi nous avons utilisé les approximations adéquates de la fonction de Bessel

$$I_0(x) \simeq \begin{cases} 1+\frac{x^2}{4} & x \ll 1 \\ \\ \frac{e^x}{\sqrt{x}} & x \gg 1 \end{cases}$$

Par ailleurs, les rapports faisant intervenir des exponentielles ont été multipliés au numérateur et au dénominateur par une exponentielle de normalisation.

2.2 Les modulations codées en treillis

Les modulations codées en treillis introduites par Ungerboeck [68]-[70] proposent d'intégrer la modulation au processus de codage, ce qui permet d'obtenir un gain significatif et donc d'éviter de gaspiller bande et puissance de canal. Elles sont principalement utilisées dans les modems téléphoniques, les communications par satellite et les transmissions sur faisceaux hertziens.

2.2.1 Principe

La TCM permet d'associer directement le symbole de la modulation à un groupe de bits, selon le critère de maximisation de la distance Euclidienne minimale entre deux mots de code et de minimisation du nombre de voisins à distance fixée. Cette opération repose sur l'étiquetage, par exemple de Gray ou d'Ungerboeck, d'un ensemble partitionné.

Deux exemples de partitionnement sont donnés figures 2.4 et 2.5 pour une modulation de phase de taille 8 (8-PSK, Pulse Shift-Keying) et une modulation d'amplitude en quadrature de taille 16 (QAM-16, Quadrature Amplitude Modulation) respectivement. Chaque sous-ensemble possède une étiquette composée d'autant de bits que le nombre de niveaux le séparant de la modulation initiale. En dernier lieu, chaque point possède une étiquette de $\log_2(M)$ bits, où M est le nombre de points dans la modulation partitionnée. La distance minimale est la même dans tous les sous-ensembles d'un même niveau de partitionnement. Dans le cas de la 8-PSK, l'augmentation n'est pas régentée par une formule particulière. Tandis que dans le cas des modulations rectangulaires de type QAM, la distance minimale au carré double entre deux niveaux, c'est-à-dire $d_{i+1}/d_i = \sqrt{2}$, $\forall i$. En règle générale, on ne descend pas au niveau des singletons de la partition. En effet, le choix du niveau de partitionnement permet de travailler avec des alphabets réduits qui présentent de bonnes propriétés de distance et d'établir ainsi un compromis entre la taille de l'alphabet sélectionné – elle induit une borne supérieure sur la distance minimale – et la complexité du décodeur.

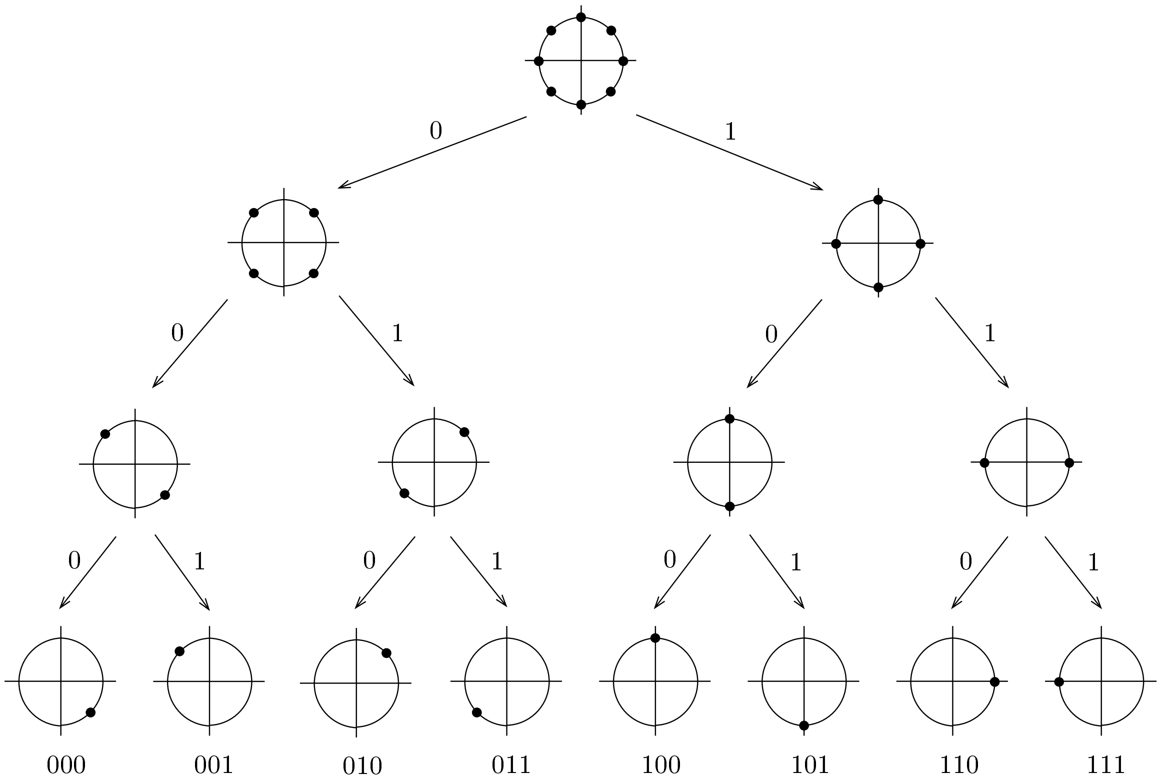


Fig. 2.4 – Partitionnement et étiquetage d'Ungerboeck d'une modulation 8-PSK.

Ce compromis établi, on construit la modulation codée en treillis selon le principe décrit figure 2.6 : les $m = k_1 + k_2$ bits d'information sont répartis en deux groupes

- k_2 bits codés par un code convolutif de rendement k_2/n qui permettent de choisir un sous-ensemble de la partition au niveau considéré.
- k_1 bits non codés qui déterminent le point considéré dans le sous-ensemble choisi.

On calcule classiquement le gain asymptotique d'une TCM en comparant les performances de la modulation codée en treillis à celles d'un système non codé de même efficacité spectrale. Ainsi, une TCM de rendement 2/3 associée à une modulation 8-PSK est-elle comparée à une modulation 4-PSK non codée car elles ont la même efficacité spectrale de 2 bits/symbole ou 2 bits/s/Hz. Selon le type de la modulation sous-jacente utilisée (PSK ou QAM), le gain asymptotique, en

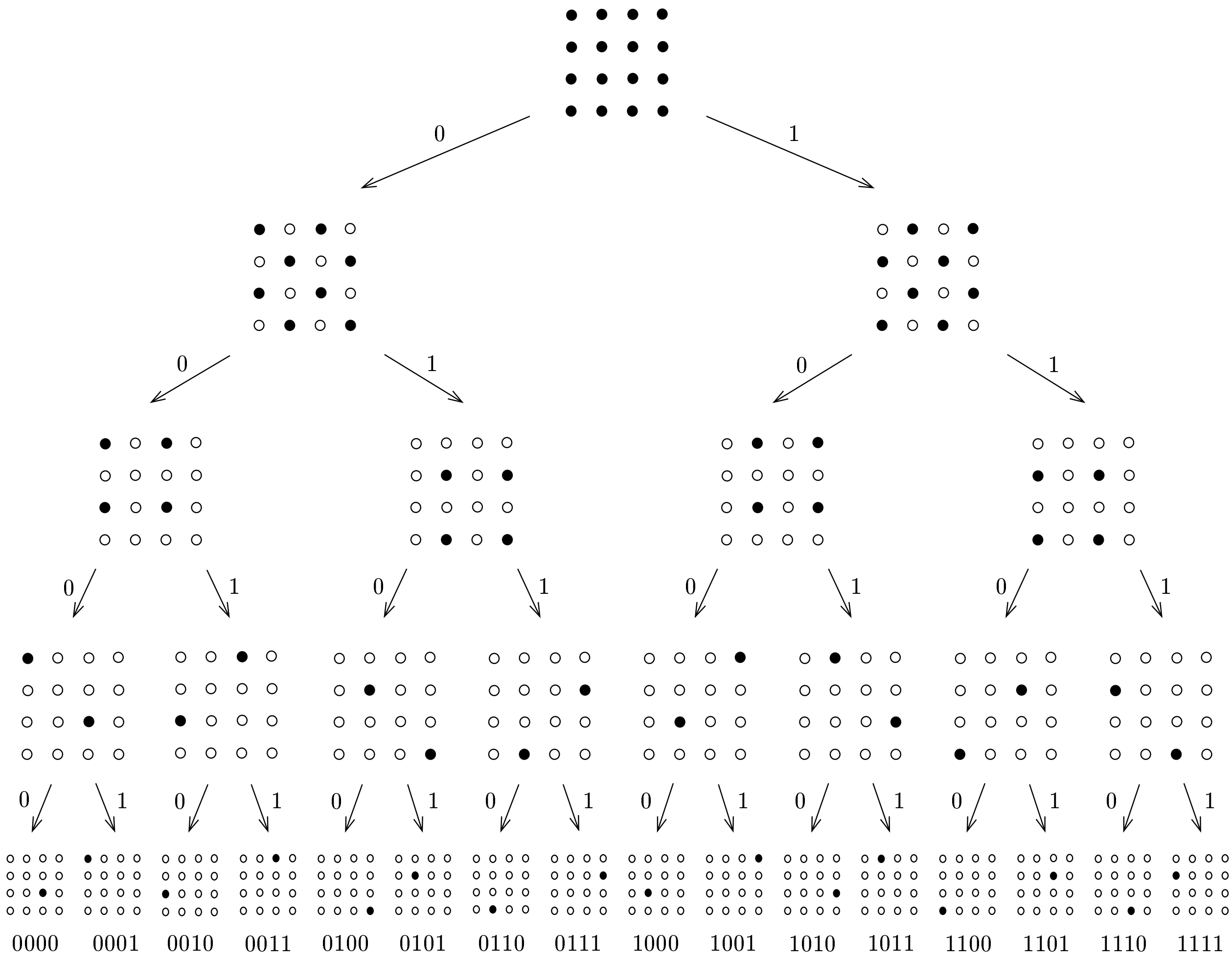


FIG. 2.5 – Partitionnement et étiquetage d'Ungerboeck d'une modulation QAM-16.

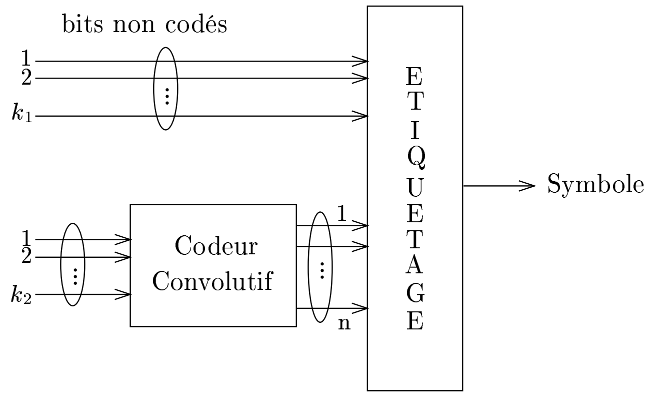


FIG. 2.6 – Schéma de principe d'une modulation codée en treillis en émission.

dB, s'exprime différemment

$$G_{PSK} = 10 \log_{10} \left(\frac{d^2_{min,c}}{d^2_{min,nc}} \right) \quad \text{et} \quad G_{QAM} = 10 \log_{10} \left(\frac{d^2_{min,c}}{d^2_{min,nc}} \times \frac{E_{nc}}{E_c} \right)$$

où les indices c et nc représentent respectivement les systèmes codés et non codés. E désigne l'énergie de la modulation sous-jacente et d^2_{min} la distance minimale au carré. Dans le cas de la TCM, c'est celle des sous-ensembles au niveau considéré dans la partition prise en compte. Par ailleurs, Ungerboeck [57] donne les tables des valeurs de gains asymptotiques pour différentes TCM. On observe qu'il est assez facile d'atteindre un gain de 6 dB. Au delà, les systèmes sont plus complexes à mettre en œuvre ; le peu de gain supplémentaire alors obtenu ne justifie pas une telle complexité.

Particulièrement adaptées aux modulations de type QAM, les TCM présentent un certain nombre d'avantages comme l'ont montré les nombreuses recherches dont elles ont fait l'objet [35][40][69][70][78]. Elles permettent ainsi d'établir un compromis entre le gain de codage obtenu et la complexité de mise en œuvre, tout en offrant la possibilité d'exploiter les propriétés d'invariance rotationnelle, très utiles lorsque la détection est non cohérente.

Nous verrons au paragraphe 2.3 qu'il est possible de construire des modulations codées en blocs [22] en substituant un code en blocs au code convolutif de la figure 2.6. Cette construction est à rapprocher des réseaux de points.

2.2.2 Décodage ML : nouvelle métrique pour l'algorithme de Viterbi

L'utilisation des codes convolutifs dans les schémas de modulations codées permet d'utiliser l'algorithme de Viterbi. Le calcul de la métrique est alors adapté en fonction du schéma de codage. Envisageons le cas simple d'un codage convolutif sur un canal gaussien cohérent de gain unitaire, pour lequel la phase ϕ est connue du récepteur. En supposant que le symbole I_q d'une modulation d'amplitude de taille Q (PAM-Q) a été émis, on reçoit $r(t) = I_q + b(t)$ où le bruit $b(t)$ est additif blanc gaussien réel de moyenne nulle et de variance σ^2. Si le démodulateur fournit une estimation souple du signal émis, on minimisera la distance euclidienne $d_E = ||r(t) - I_q||^2$. Mais si l'estimation est dure, c'est-à-dire sous la forme d'une séquence erronée de bits codés, on minimisera la distance de Hamming $d_H = \sum_{i=1}^{m} r_i - I_{q_i}$ où r_i et I_{q_i} désignent le bit i des étiquettes de r et I_q.

Dans notre cas, le schéma de codage est assimilé à une modulation codée en treillis de rendement R. Chaque groupe de K bits sert à étiqueter N symboles p_n d'une PAM-Q associés à N signaux d'une Q-FSK par l'intermédiaire du modulateur. Lorsque l'algorithme de Viterbi est utilisé pour décoder une modulation codée en treillis, il est commun de considérer que chaque branche du treillis correspond à un des symboles de la modulation. L'algorithme de décodage fournit une estimation des symboles décodés en deux étapes [57]. On en déduit ensuite les bits d'information puisque l'étiquetage bits-symboles est défini. Pour pouvoir procéder de la même façon dans notre modèle, R doit vérifier $K \times R = N \times \log_2(Q)$. Chaque branche du treillis correspondra alors à un symbole de la modulation PAM de taille Q ou de manière équivalente à un signal de la modulation Q-FSK. Dans ces conditions, le critère de l'équation (2.1) est utilisé pour calculer une nouvelle métrique.

L'algorithme de Viterbi effectue la minimisation d'une métrique additive sur tous les chemins possibles dans le treillis. Le critère (2.1) nécessite de maximiser la somme des valeurs de corrélation. La nouvelle métrique du décodeur de Viterbi est

$$\min_m \left\{ -\sum_n |x_{m,n}|^2 \right\}$$

2.3 Les réseaux de points

Outil mathématique connu depuis plus d'un siècle, les réseaux de points ont de nombreuses applications relatives à des domaines diverses. Les mathématiques, où ils sont utilisés dans les travaux sur les groupes, les corps finis ou encore les formes quadratiques ; la cristallographie, où ils servent à modéliser le comportement de certains composés chimiques ; et plus récemment la théorie des communications numériques, désormais grand domaine d'application des réseaux de points. En effet, depuis l'apparition des modulations codées au début des années 1980, les réseaux se sont révélés être un bon moyen pour construire des constellations de grande taille à énergie minimale, candidates aux transmissions à efficacité spectrale élevée. Ces dernières sont utilisées en tant que modulations aussi bien sur le canal gaussien que sur les canaux à évanouissements. Les constellations optimales – au sens de la minimisation de la probabilité d'erreur – construites à partir des réseaux les plus denses, exploitent pleinement leurs propriétés géométriques et conduisent à d'excellentes performances sur canal gaussien. Sur les canaux à évanouissements, ce sont les réseaux à grande diversité qui présentent les meilleurs résultats : la redondance qui lie les composantes d'un point du réseau est utilisée pour récupérer l'information qui a subi les perturbations du canal lors de la transmission.

Le problème de l'empilement de sphères est connu depuis longtemps en mathématiques où la recherche du meilleur empilement – celui qui permet de placer le plus de sphères possible dans un espace de dimension N tout en minimisant le volume des zones non occupées – est l'objet de nombreuses études. La solution en dimension $N = 3$, formalisée par la conjecture de Kepler en 1609, a pu être démontrée très récemment. Elle correspond à l'empilement cubique à face centrée (*fcc*) présenté figure 2.7. Les sphères occupent une portion $\pi/\sqrt{18} \simeq 74,048\%$ de l'espace total appelée densité de l'empilement.

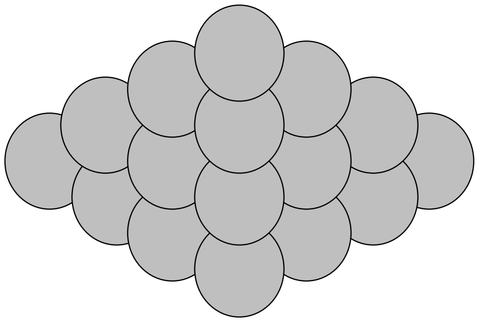


Fig. 2.7 – Empilement cubique à face centrée (vu de côté).

Un réseau de points est un empilement particulier de sphères possédant une structure de groupe [26]. Les sphères de l'empilement ont toutes même rayon. Elles garantissent ainsi une distance minimale entre les centres qui constituent les points du réseau.

Après avoir présenté les paramètres fondamentaux utiles à la définition et à l'étude plus précise des réseaux, nous détaillons deux méthodes de construction de réseaux de points. Puis nous montrons que les réseaux peuvent être, dans certains cas, assimilés à des modulations codées en blocs. Enfin, nous décrivons deux techniques de décodage : le décodage par sphères et le décodage à entrée souple.

2.3.1 Définition des paramètres fondamentaux

$\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{R}$ désignent respectivement les ensembles des entiers naturels, des entiers relatifs et des réels. $\mathbb{R}^N$ est un espace euclidien de dimension N muni d'une distance. Un point ou vecteur de $\mathbb{R}^N$ est noté $\mathbf{x} = (x_1, \ldots, x_N)$, où les composantes x_i sont des éléments de $\mathbb{R}$. La notation $(.)^t$ sur un vecteur ou une matrice indique la transposition. Pour tout réel $a \in \mathbb{R}$, $a\mathbf{x}$ est le vecteur de composantes $(ax_1, \ldots, ax_N)$. La norme euclidienne d'un vecteur $\mathbf{x}$ est notée $||\mathbf{x}||$. Enfin, une sphère de $\mathbb{R}^N$, de rayon ρ et de centre $\mathbf{u} = (u_1, \ldots, u_N)$ désigne l'ensemble des points $\mathbf{x}$ qui vérifient $||\mathbf{x} - \mathbf{u}||^2 = (x_1 - u_1)^2 + (x_2 - u_2)^2 + \cdots + (x_N - u_N)^2 = \rho^2$.

Définition 2.3.1 *(réseau de points)*
Un **réseau de points** *est un sous-groupe discret de rang N de $\mathbb{R}^N$ [60].*

On peut encore définir les réseaux de points complexes.

Définition 2.3.2 *(réseau complexe)*
Un **réseau complexe** *est un sous-groupe discret de rang N de $\mathbb{C}^N$, où $\mathbb{C}$ est le corps des complexes.*

Nous travaillons exclusivement avec des réseaux de rang plein, ainsi, leur dimension N est toujours égale à la dimension de l'espace.

D'un point de vue algébrique, un réseau Λ est un **$\mathbb{Z}$-module**, engendré par une famille de N vecteurs indépendants $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ de $\mathbb{R}^N$. C'est donc l'ensemble des points

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

Par ailleurs, le réseau peut aussi être vu comme le groupe additif formé de l'ensemble des centres des sphères de l'empilement. Par définition d'un groupe additif, l'élément $\mathbf{0}$ appartient à Λ. Et puisque la topologie du groupe est invariante à toute translation, nous pourrons nous restreindre à l'étude de ce qui se passe autour de l'origine $\mathbf{0}$ pour connaître le comportement autour de tout point de Λ.

Définition 2.3.3 *(base du réseau)*
La famille des N vecteurs $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ constitue une **base du réseau** *et N est la* **dimension** *ou le* **rang** *de Λ.*

Définition 2.3.4 *(sous-réseau)*
Un **sous-réseau** *de Λ est un sous-groupe de $\mathbb{R}^N$ ou de $\mathbb{C}^N$ inclus dans Λ.*

Un réseau est dit entier s'il est un sous-réseau du réseau $\mathbb{Z}^N$. Ce dernier est un exemple classique de réseau, chacun de ses points possède N composantes entières. Il est souvent utilisé comme étalon pour comparer les réseaux.

Définition 2.3.5 *(constellation)*
Une **constellation** $\mathcal{C}$ *extraite d'un réseau de points* Λ *est un sous-ensemble fini du réseau* Λ.

Définition 2.3.6 *(matrice génératrice)*
Les vecteurs $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ *de la base du réseau de points forment les lignes d'une matrice appelée* **matrice génératrice** *du réseau.*

Dans toute la suite, nous travaillons en convention "ligne". En notant $\mathbf{v}_i = (v_{i1}, \ldots, v_{iN})$ pour $i = 1, \ldots, N$, la matrice génératrice du réseau est donnée par

$$M = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N)^t = \begin{pmatrix} v_{11} & \cdots & v_{1N} \\ \vdots & & \vdots \\ v_{N1} & \cdots & v_{NN} \end{pmatrix} \tag{2.13}$$

Un point $\mathbf{x} = (x_1, \ldots, x_N)$ du réseau peut donc s'écrire $\mathbf{x} = \mathbf{z}M$ où $\mathbf{z}$ est un vecteur de $\mathbb{Z}^N$. Le réseau Λ correspond dans ce cas au résultat d'une transformation linéaire définie par la matrice M appliquée au réseau cubique $\mathbb{Z}^N$. Notons par ailleurs qu'il existe plusieurs choix possibles de la base $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N)$. Par conséquent, la matrice génératrice du réseau n'est pas unique.

Définition 2.3.7 *(matrice de Gram)*
La **matrice de Gram** G_Λ *du réseau est la matrice définie par*

$$G_\Lambda = MM^t$$

où M *est la matrice génératrice du réseau.*

Par construction, les éléments $g_{ij}, i, j = 1, \ldots, N$ de la matrice de Gram sont les produits scalaires des paires de vecteur de la base, c'est-à-dire $g_{ij} = \mathbf{v}_i.\mathbf{v}_j = \sum_{k=1}^{N} v_{ik}v_{kj}$. La matrice G_Λ est définie positive et symétrique. Ses éléments diagonaux sont égaux au carré des normes des vecteurs de la base.

Définition 2.3.8 *(parallélotope fondamental, volume fondamental)*
La région de l'espace $P = \{\mathbf{x} \in \mathbb{R}^N / \mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_N\mathbf{v}_N,\ 0 \leq a_i < 1\}$ *est le* **parallélotope fondamental** *du réseau. Son* **volume fondamental** *est le volume du parallélotope fondamental, noté* $vol(\Lambda)$.

Le module $|det(M)|$ du déterminant de la matrice génératrice M n'est autre que le module du produit vectoriel $\mathbf{v}_1 \wedge \mathbf{v}_2 \wedge \cdots \wedge \mathbf{v}_N$ des N vecteurs de la base du réseau. Par définition, ce dernier module est encore égal au volume délimité par ces mêmes N vecteurs. Alors, puisque les vecteurs de la base délimitent le parallélotope fondamental, $|det(M)|$ est aussi le volume fondamental du réseau.

Par abus de langage, on note $|det(M)| = det(\Lambda) = vol(\Lambda)$. De plus, en cas de changement de base, la nouvelle matrice génératrice $M' = UM$, où U est la matrice de passage entre l'ancienne et la nouvelle base, est telle que $|det(M')| = |det(U)||det(M)|$. En tant que matrice de passage, U est unitaire, donc $|det(U)| = 1$. Le volume fondamental du réseau reste inchangé. Ainsi, alors que le parallélotope fondamental, directement lié à la base du réseau, n'est pas unique, le volume fondamental est, lui, indépendant du choix de la base.

Définition 2.3.9 *(cellule de Voronoï)*
La région de l'espace associée à un point **u** *du réseau* Λ *définie par*

$$\mathcal{V}(\mathbf{u}) = \{\mathbf{x} \in \mathbb{R}^N / ||\mathbf{x} - \mathbf{u}|| \leq ||\mathbf{x} - \mathbf{y}||, \mathbf{y} \in \Lambda\} \tag{2.14}$$

est appelée **cellule** *ou région* **de Voronoï** *de* **u**.

Les frontières des cellules de Voronoï correspondent aux médiatrices entre le point central de la cellule et chacun de ses voisins. Puisque le réseau est invariant par translation, on constate que toutes les cellules sont identiques et de même volume, égal au volume fondamental du réseau. On parlera de "la cellule de Voronoï" du réseau Λ représentée par $\mathcal{V}(\mathbf{0})$, la cellule centrée sur l'origine. Les différentes cellules de Voronoï constituent un pavage complet de l'espace, à la différence de l'empilement de sphères.

Définition 2.3.10 *(rayon d'empilement, rayon de recouvrement)*
Le **rayon d'empilement** ρ *(respectivement* **rayon de recouvrement** R*) d'un réseau* Λ *est le rayon de la plus grande (respectivement la plus petite) sphère inscrite (respectivement circonscrite) à la région de Voronoï.*

Les sphères d'empilement ont toute même rayon ρ. La distance minimale d_{Emin} entre les points du réseau est alors donnée par

$$d_{Emin} = 2\rho \tag{2.15}$$

La figure 2.8 permet de visualiser tous les paramètres élémentaires définis ci-dessus dans le cadre du réseau hexagonal A_2 de dimension 2, réseau le plus dense dans $\mathbb{R}^2$. Une base est formée des deux vecteurs $\mathbf{v}_1, \mathbf{v}_2$.

Définition 2.3.11 *(densité du réseau)*
La densité de remplissage d'un réseau, ou **densité**, *notée* Δ *est donnée par le rapport du volume de la sphère de l'empilement et du volume fondamental*

$$\Delta = \frac{volume\ d'une\ sph\grave{e}re}{volume\ fondamental} = \frac{V_N \times \rho^N}{vol(\Lambda)} \tag{2.16}$$

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

$$\delta = \frac{\Delta}{V_N} = \frac{\rho^N}{vol(\Lambda)} \tag{2.17}$$

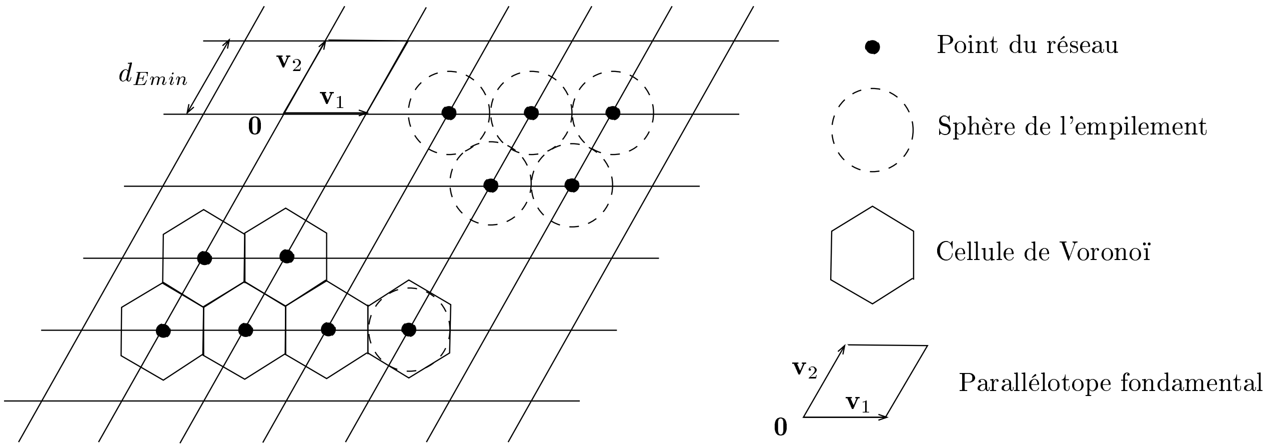


Fig. 2.8 – Le réseau hexagonal A_2 et ses paramètres fondamentaux.

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

$$V_N = \frac{\pi^{N/2}}{\Gamma(N/2+1)} = \begin{cases} \frac{\pi^{N/2}}{(N/2)!} & N \text{ pair} \\ \frac{2^N \pi^{(N-1)/2}((N-1)/2)!}{N!} & N \text{ impair} \end{cases} \tag{2.18}$$

Définition 2.3.12 *(coefficient d'erreur)*
Le **coefficient d'erreur** *$\tau(\Lambda)$ (kissing number) d'un réseau Λ est le nombre de sphères tangentes à une sphère donnée.*

Le réseau étant invariant par translation, la valeur de $\tau(\Lambda)$ ne dépend pas de la sphère considérée. Pour le réseau hexagonal A_2 de la figure 2.8, on a $\tau(A_2) = 6$ puisque chaque point du réseau possède six voisins situés à la distance minimale d_{Emin}.

La figure 2.9 représente le modèle d'un système de transmission mettant en œuvre une constellation issue d'un réseau de point. Les bits d'information, provenant d'une source binaire aléatoire, sont étiquetés afin de choisir le point $\mathbf{x}$ du réseau Λ qui sera émis sur le canal. Nous considérons soit le canal à bruit additif blanc gaussien, soit le canal de Rayleigh non sélectif à évanouissements indépendants.

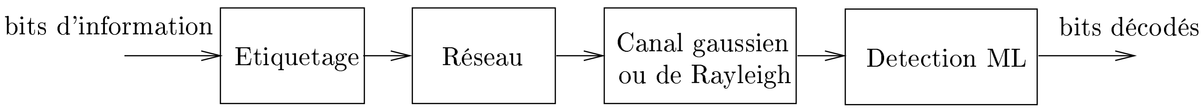


Fig. 2.9 – Modèle d'un système de transmission incluant un réseau de points.

Performances sur canal gaussien

Sur canal gaussien, la probabilité d'erreur par point notée P_e d'un tel système décroit exponentiellement lorsque le rapport signal-à-bruit E_b/N_0 augmente. Dans le cas d'une constellation cubique, la probabilité d'erreur est bornée [17] par :

$$P_e \leq \tau(\Lambda) Q\left(\sqrt{\frac{d^2_{Emin}}{\sqrt[N/2]{det(\Lambda)}} \frac{E_b}{N_0} \frac{3\eta}{2^\eta}}\right) \tag{2.19}$$

où la fonction $Q(x)$ vérifie

$$Q(x) = \frac{1}{2}\text{erfc}\left(\frac{x}{\sqrt{2}}\right) \leq \frac{1}{2}e^{-x^2/2}$$

et η désigne l'efficacité spectrale par deux dimensions, c'est-à-dire le nombre de bits d'information émis par deux dimensions.

L'expression 2.19 nous amène à définir le gain fondamental du réseau.

Définition 2.3.13 *(gain fondamental)*
On appelle **gain fondamental** *d'un réseau en dimension N le rapport*

$$\gamma(\Lambda) = \frac{d^2_{Emin}}{\sqrt[N/2]{vol(\Lambda)}} = 4 \times \sqrt[N/2]{\delta} \tag{2.20}$$

où d_{Emin} est la distance euclidienne minimale de Λ, $vol(\Lambda)$ son volume fondamental et δ sa densité centrée. $\gamma(\Lambda)$ est encore le gain du réseau par rapport au réseau entier $\mathbb{Z}^N$ puisque $\gamma(\mathbb{Z}^N) = 1/1 = 1$. Fonction de la densité du réseau, le gain fondamental influence directement les performances du réseau de points : plus il est élevé, meilleure sera la probabilité d'erreur P_e. On notera que la seule connaissance de la densité centrée δ est suffisante au calcul de γ.

Par ailleurs, il est utile de noter que le gain d'une constellation cubique extraite d'un réseau est égale au gain fondamental du réseau. Toute transformation par rotation, symétrie, homothetie ou composition de la constellation cubique laisse le rapport distance minimale sur volume fondamental inchangé. Dans le cas de constellations de forme non cubique, $\gamma(\Lambda)$ augmente ou diminue suivant le moment de second ordre (c'est-à-dire l'énergie moyenne par point) de la constellation, selon la forme de la frontière de $\mathcal{C}$ dans $\mathbb{R}^N$. On définit alors le gain total du réseau, qui tient compte des caractéristiques fondamentales du réseau Λ et de la forme de la constellation.

Définition 2.3.14 *(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**.

$$\gamma(\mathcal{C}) = \gamma(\Lambda) \times \gamma_s(\mathcal{C}) \tag{2.21}$$

Par définition, le gain de forme d'une constellation cubique est donc égal à 1. Par ailleurs, la forme sphérique minimise l'énergie moyenne de $\mathcal{C}$ grâce à la répartition homogène des points autour de l'origine. Alors, le gain de forme $\gamma(\mathcal{C})$ est maximal lorsque $\mathcal{C}$ est sphérique. On peut montrer que ce gain de forme tend vers $\pi e/6 \approx 1.533$ dB lorsque N tend vers l'infini [17]. Il reste donc relativement faible, ce qui conduit bien souvent à des constellations cubiques beaucoup plus pratiques à utiliser.

Performances sur canal de Rayleigh

Sur canal de Rayleigh, l'application de la borne de l'union et le calcul des probabilités d'erreur par paire permettent d'obtenir une expression de la probabilité d'erreur

$$P_e \leq \frac{1}{2} \sum_{\ell=L}^{N} \frac{K_\ell}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^\ell} \tag{2.22}$$

où K_ℓ est une constante positive qui dépend uniquement des caractéristiques du réseau [46] et où L est la diversité du réseau définie comme suit :

Définition 2.3.15 *(diversité)*
L'ordre de diversité ou **diversité** *L d'un réseau Λ est le nombre minimal de composantes différentes entre deux points quelconques distincts $\mathbf{x}$ et $\mathbf{y}$ du réseau*

$$L = \min_{\substack{\mathbf{x},\mathbf{y}\in\Lambda \\ \mathbf{x}\neq\mathbf{y}}} d_H(\mathbf{x},\mathbf{y}) \tag{2.23}$$

Asymptotiquement, la borne (2.22) décroit linéairement avec la diversité L.

La table (2.1) fournit une liste des paramètres fondamentaux des différents réseaux de points parmi les plus célèbres [26] : leur nom Λ, leur dimension N, leur densité Δ, fonction décroissante de N, leur densité centrée δ, leur gain total γ en dB et enfin leur coefficient d'erreur $\tau(\Lambda)$, fonction croissante de N. Parmi les réseaux les plus importants, on remarquera le réseau fcc D_3, le réseau de Schlafli D_4, le réseau de Gosset E_8, le réseau de Barnes-Wall BW_{16}, ou encore le fameux réseau de Leech Λ_{24}.

2.3.2 Constructions A et B

Les codes correcteurs d'erreurs permettent de construire des empilements de sphères très denses dans l'espace euclidien $\mathbb{R}^N$ [26]. Parmi les autres méthodes, citons par exemple la construction par découpage, par couches ou à partir de corps de nombres. Nous utilisons indirectement ce dernier cas dans le chapitre 4. Pour une description détaillée des méthodes non développées dans ce paragraphe, le lecteur consultera l'ouvrage encyclopédique de Conway et Sloane [26]. Nous nous limitons ici aux constructions A et B classiques qui permettent de fabriquer des réseaux de points entiers à partir des codes linéaires.

Définition 2.3.16 *(décomposition binaire)*
Soit $e \in \mathbb{Z}$. La **décomposition binaire** *de l'entier relatif e est obtenue en le projetant sur la base formée par les puissances de 2, soit*

$$e = \sum_{\ell=0}^{\infty} e_\ell 2^\ell \tag{2.24}$$

où les composantes e_ℓ appartiennent à l'ensemble $\{0,1\}$. La notation binaire complémentaire est utilisée pour écrire les entiers négatifs.

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. 2.1 – Quelques réseaux de points et leurs paramètres fondamentaux. La dimension N, le nom Λ, la densité Δ, la densité centrée δ ($\log_2(\delta)$ pour $N \geq 32$), le gain γ_{dB} en dB et le coefficient d'erreur $\tau(\Lambda)$.

Grâce à la décomposition binaire d'un entier, il est possible de construire la matrice des coordonnées d'un vecteur $\mathbf{x} \in \mathbb{Z}^N$.

Définition 2.3.17 *(matrice des coordonnées)*
Soit $\mathbf{x} = (x_1, \ldots, x_N)$ *un point de* $\mathbb{Z}^N$. *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 sont toutes identiques à partir d'un certain rang. La ligne numéro i est appelée **ligne mod-2^i**.

Considérons par exemple 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

$$\begin{array}{ll} \left[\begin{array}{cccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right] & \begin{array}{l} \rightarrow \text{ligne mod} - 2 \\ \rightarrow \text{ligne mod} - 4 \\ \rightarrow \text{ligne mod} - 8 \\ \rightarrow \text{ligne mod} - 16 \\ \cdots\cdots \end{array} \end{array} \tag{2.25}$$

Ces définitions nous permettent d'interpréter les deux constructions décrites dans la suite.

Construction A

C'est la méthode la plus simple de construction d'un réseau de points. Elle repose sur l'utilisation d'un code linéaire q-aire. Dans la plupart des cas pratiques, on se restreint à $q = 2$.

Définition 2.3.18 *(construction A)*
Soit C_0 un code linéaire binaire de longueur $n = N$, de dimension k et de distance minimale de Hamming d. Un réseau Λ obtenu par construction A peut être décrit de la façon suivante : $\mathbf{x} = (x_1, \ldots, x_N)$ est un point de Λ si et seulement si le N-uple $(x_1, \ldots, x_N)$ est congru modulo 2 à un mot de code de C_0. Alors

$$\Lambda = C_0 + 2\mathbb{Z}^N \tag{2.26}$$

La formule (2.26) nous apprend qu'un réseau de points obtenu par construction A est généré par k vecteurs de la base du code C_0 et $N - k$ vecteurs provenant de $2\mathbb{Z}^N$. Si la matrice génératrice de C_0 est sous forme systématique, soit $[I_k|P]$, alors la matrice génératrice M du réseau Λ est donnée par

$$M = \begin{pmatrix} I_k & P \\ 0 & 2I_{N-k} \end{pmatrix} \tag{2.27}$$

Il est possible de calculer facilement certains paramètres du réseau Λ ainsi construit à partir du code $C_0 = (N, k, d)$ [17].

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

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

le coefficient d'erreur $\qquad \tau(\Lambda) = \left\{ \begin{array}{rl} 2^d A_d & si\ d < 4 \\ 2N + 16A_4 & si\ d = 4 \\ 2N & si\ d > 4 \end{array} \right.$

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

La construction A fournit des réseaux de points efficaces pour des dimensions $N \leq 15$. On citera par exemple les réseaux *checkerboard*, notés $D_N = (N, N-1, 2) + 2\mathbb{Z}^N$, obtenus à partir des codes de parité $(N, N-1, 2)$. Ils donnent le réseau D_3 (ou fcc), le réseau de Schlafli D_4 et D_5 qui sont les réseaux les plus denses en dimension 2, 3 et 4. Par ailleurs, les réseaux les plus denses en dimension 6, 7 et 8, à savoir, E_6, E_7 et le réseau de Gosset E_8 s'obtiennent par construction A. La matrice génératrice du réseau D_3 est donnée à titre d'exemple

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \tag{2.28}$$

Construction B

Cette deuxième construction diffère de la construction A par l'ajout d'une contrainte supplémentaire sur la ligne mod-4 de la matrice des coordonnées.

Définition 2.3.19 *(construction B)*
Soient C_0 un code linéaire binaire de longueur $n = N$, de dimension k et de distance minimale de Hamming d dont tous les mots de codes sont de poids pair, et C_1 le code de parité $(N, N-1, 2)$. Un réseau Λ obtenu par construction B peut être décrit de la façon suivante : $\mathbf{x} = (x_1, \ldots, x_N)$ est un point de Λ 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, alors

$$\Lambda = C_0 + 2C_1 + 4\mathbb{Z}^N \tag{2.29}$$

De plus, $C_0 \subset C_1$ puisque les poids des mots de code de C_0 sont divisibles par 2. De la même façon que pour la construction A, certains paramètres du réseau Λ obtenu par construction B sont facilement calculables [17].

le rayon d'empilement	$\rho = \frac{1}{2} min(\sqrt{8}, \sqrt{d})$
la densité centrée	$\delta = 2^k \rho^N 2^{-N-1}$
le coefficient d'erreur	$\tau(\Lambda) = \begin{cases} 2^{d-1} A_d & si\ d < 8 \\ 2N(N-1) + 128 A_8 & si\ d = 8 \\ 2N(N-1) & si\ d > 8 \end{cases}$
	où A_i est le nombre de mots de poids i dans C_0.

La construction B se révèle efficace pour des dimensions N comprises entre 8 et 24. Une nouvelle version du réseau de Gosset E_8 peut être obtenue grâce à cette construction, ainsi que Λ_9, le réseau le plus dense en dimension 9. En dimension 16, l'utilisation du code de Reed-Muller d'ordre 1 conduit au réseau $\Lambda_{16} = (16, 5, 8) + 2(16, 15, 2) + 4\mathbb{Z}^{16}$ qui n'est autre que le réseau de

Barnes-Wall BW_{16}. Sa matrice génératrice s'écrit

$$M = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\
0 & & & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & & & & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\
0 & & & & & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\
0 & & & & & & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\
0 & & & & & & & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & & & & & & & & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\
0 & & & & & & & & & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\
0 & & & & & & & & & & 0 & 2 & 0 & 0 & 0 & 2 \\
0 & & & & & & & & & & & 0 & 2 & 2 & 2 & 2 \\
0 & & & & & & & & & & & & 0 & 2 & 0 & 2 \\
0 & & & & & & & & & & & & & 0 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4
\end{pmatrix} \tag{2.30}$$

2.3.3 Les réseaux binaires et les modulations codées en blocs

On ne saurait clore ces rappels sur les réseaux sans mentionner le lien étroit entre les réseaux de points binaires avec lesquels nous travaillons et les modulations codées en blocs. Les réseaux binaires constituent une extension des codes correcteurs d'erreurs et constituent la classe la plus intéressante des réseaux adaptés aux applications pratiques. Parmi les réseaux binaires, on compte les réseaux les plus denses : $\mathbb{Z}$, D_4, E_8, Λ_{16} et Λ_{24} par exemple. Afin de décrire au mieux ces réseaux binaires, nous proposons d'introduire les définitions diverses qui permettent de généraliser dans l'espace complexe les concepts abordés au paragraphe précédent.

Définition 2.3.20 *(l'anneau des gaussiens)*
*On note $j = \sqrt{-1}$ l'élément imaginaire. L'**anneau gaussien** $\mathbb{G}$ est un sous-ensemble de $\mathbb{C}$ décrit par*

$$\mathbb{G} = \mathbb{Z}[j] = \{a + jb / a, b \in \mathbb{Z}\}$$

*Les éléments de $\mathbb{G}$ sont appelés **entiers gaussiens**.*

L'anneau $\mathbb{G}$, de dimension 1 et isomorphe au réseau $\mathbb{Z}^2$ de dimension 2, est l'exemple le plus simple de réseau complexe. ± 1 et $\pm j$ sont les unités de $\mathbb{G}$. Un entier gaussien est premier s'il est divisible par lui-même et par les unités seulement. Enfin, on peut noter que l'élément $\phi = 1 + j$ est l'entier gaussien premier ayant le plus petit module, $|\phi|^2 = 2$.

Définition 2.3.21 *(décomposition binaire d'un gaussien)*
*Soit $g \in \mathbb{G}$. La **décomposition binaire** de l'entier gaussien g est une combinaison linéaire binaire des puissances de $\phi = 1 + j$, soit*

$$g = \sum_{\ell=0}^{\infty} e_\ell \phi^\ell \tag{2.31}$$

où les composantes e_ℓ appartiennent à l'ensemble $\{0,1\}$.

Ce résultat est une extension directe de la définition 2.3.16.

La définition exacte d'un réseau binaire s'énonce comme suit :

Définition 2.3.22 *(réseau binaire réel)*
Le **réseau** Λ *de dimension* N *est* **binaire** *s'il existe un entier* m *tel que* $2^m\mathbb{Z}^N \subset \Lambda \subset \mathbb{Z}^N$.

Le plus petit entier m qui vérifie $2^m\mathbb{Z}^N \subset \Lambda$ est appelé **profondeur-2** du réseau. Lorsque la profondeur-2 du réseau binaire est égale à 1 (respectivement 2), on dira que Λ est un **réseau mod-2** (respectivement **mod-4**).

Définition 2.3.23 *(réseau binaire complexe)*
Le **réseau complexe** Λ *de dimension* N *est* **binaire** *s'il existe un entier* μ *tel que* $\phi^\mu\mathbb{G}^N \subset \Lambda \subset \mathbb{G}^N$ *et si* Λ *est un* $\mathbb{G}$*-réseau ou* $\mathbb{G}$*-module [17] [60].*

Le plus petit entier ϕ qui vérifie $\phi^\mu\mathbb{G}^N \subset \Lambda$ est appelé **profondeur-ϕ** du réseau.

Ces notions nous permettent de généraliser au cas complexe la construction A détaillée au paragraphe précédent :

Définition 2.3.24 *(construction A complexe)*
Soient Λ *un* $\mathbb{G}$*-réseau complexe de dimension* N, C_1 *un code linéaire binaire* (N,K), *et* C_0 *un sous-code* $(N,J-K)$ *de* C_1. Λ *est un réseau mod-2 obtenu par construction A complexe si et seulement si* Λ *est l'ensemble des* N*-uples d'entiers gaussiens congrus modulo* ϕ^2 *aux* N*-uples de la forme* $\phi\mathbf{c_1}+\mathbf{c_0}$ *où* $\mathbf{c_1}\in C_1$ *et* $\mathbf{c_0}\in C_0$. *Alors*

$$\Lambda = C_0 + \phi C_1 + \phi^2\mathbb{G}^N \tag{2.32}$$

Il est également possible d'énoncer une règle pour les réseaux non mod-2. En effet, si ce n'est pas le cas pour tous, un grand nombre de réseaux non mod-2 sont tout de même décomposables, c'est-à-dire exprimables en fonction de codes binaires seulement.

Définition 2.3.25 *(réseau complexe décomposable)*
Soient $\{C_{\mu-1}, C_{\mu-2}, \ldots, C_0\}$ μ *codes binaires* (N, K_ℓ), $0 \le \ell \le \mu-1$. C_ℓ *est un sous-code de* $C_{\ell+1}$. Λ *est un* **réseau complexe décomposable** *de profondeur* μ *si et seulement si ses éléments sont des* N*-uples d'entiers gaussiens* $\mathbf{x}=(x_1,\ldots,x_N)$ *congrus à* $\phi^{\mu-1}\mathbf{c_{\mu-1}}+\cdots+\phi\mathbf{c_1}+\mathbf{c_0}$ *modulo* ϕ^μ *où* $\mathbf{c}_\ell\in C_\ell$. *Alors*

$$\Lambda = C_0 + \phi C_1 + \cdots + \phi^{\mu-1}C_{\mu-1} + \phi^\mu\mathbb{G}^N \tag{2.33}$$

La table (2.2) donne les formules réelles et complexes des réseaux binaires les plus fréquemment utilisés. La notation $(24,6,16)'$ représente l'ensemble des combinaisons linéaires modulo 4 de six générateurs à composantes entières modulo 4, tels que la norme au carré minimale dans chaque sous ensemble est égale à 16. Puisque nous utilisons ce type de notation uniquement pour des réseaux de dimension 24, les combinaisons linéaires se font toujours modulo 4.

En pratique, on appelle symbole un point du réseau $\mathbb{Z}^2$. Alors, un vecteur de $N/2$ symboles est un point de $\mathbb{Z}^N$. La traduction directe des formules complexes énoncées dans la table (2.2)

Λ	$2N$	Formule Réelle	Formule Complexe
$\mathbb{Z}^2$	2	$\mathbb{Z}^2$	$\mathbb{G}$
$\mathbb{Z}^4$	4	$\mathbb{Z}^4$	$\mathbb{G}^2$
D_4	4	$(4,3,2)+2\mathbb{Z}^4$	$(2,1,2)+\phi\mathbb{G}^2$
$\mathbb{Z}^8$	8	$\mathbb{Z}^8$	$\mathbb{G}^4$
E_8	8	$(8,4,4)+2\mathbb{Z}^8$	$(4,1,4)+\phi(4,3,2)+\phi^2\mathbb{G}^4$
H_{16}	16	$(16,11,4)+2\mathbb{Z}^{16}$	$(8,4,4)+\phi(8,7,2)+\phi^2\mathbb{G}^8$
Λ_{16}	16	$(16,5,8)+2(16,15,2)+4\mathbb{Z}^{16}$	$(8,1,8)+\phi(8,4,4)+$ $\phi^2(8,7,2)+\phi^3\mathbb{G}^8$
H^{24}	24	$(24,12,8)+2(24,23,2)+4\mathbb{Z}^{24}$	$(12,5,8)'+\phi(12,7,4)+$ $\phi^2(12,11,2)+\phi^3\mathbb{G}^{12}$
Λ_{24}	24	$(24,6,16)'+2(24,18,4)+4\mathbb{Z}^{24}$	$(12,1,16)'+\phi(12,5,8)'+\phi^2(12,7,4)+$ $\phi^3(12,11,2)+\phi^4\mathbb{G}^{12}$

TAB. 2.2 – Exemples de réseaux binaires et leurs formules réelle et complexe.

permet de construire les codeurs des réseaux D_4, E_8, Λ_{16} et Λ_{24} à partir d'une modulation QAM codée en blocs. Nous utilisons des partitionnements de plus en plus profonds de cette modulation représentés figure 2.10.

Il est possible de retrouver la valeur du gain fondamental du réseau à partir des propriétés de la modulation codée sous-jacente. En effet, pour choisir un point de la QAM-64, il faut 6 bits en entrée du codeur. De plus, nous avons vu au paragraphe 2.2 que dans le cas des modulations rectangulaires de type QAM, la distance minimale au carré double entre deux niveaux, c'est-à-dire $d_{i+1}/d_i = \sqrt{2}$, $\forall i$. Et enfin, on sait qu'une perte d'efficacité spectrale d'un bit se traduit par une perte d'environ 3 dB. Une approximation du gain peut donc être donnée

$$\gamma_{dB}(\Lambda) = 10\log_{10}(2^i) - 3 \times (6-\eta)$$

où i est la profondeur du partitionnement de la QAM-64 et η l'efficacité spectrale.

Le réseau de Schlafli, D_4

Le schéma du codeur mettant en œuvre la formule complexe du réseau de Schlafli $D_4 = (2,1,2) + \phi\mathbb{G}^2$ est donné figure 2.11. La modulation QAM-64 est partitionnée en deux sous-ensembles notés A et B. Un point de D_4 est un vecteur de quatre composantes réelles ou encore de deux symboles QAM-64, (x_1, x_2). Les deux bits codés fournis par le code à répétition $(2,1,2)$ déterminent le choix du sous-ensemble pour chacun des deux symboles x_1 et x_2. On choisit A si le bit vaut 0, et B, si le bit vaut 1. Les ensembles A et B sont composés de 32 points. On utilise alors 2×5 bits non codés pour choisir un point dans chacun des deux sous-ensembles. Le nombre total de bits d'information est de 11 pour étiqueter deux symboles. Cela correspond à une efficacité spectrale de 5.5 bits/symbole. On retrouve le gain fondamental de D_4, $\gamma_{dB}(D_4) = 10\log_{10}(2) - 3\times 0.5 = 1.5$ dB

Le réseau de Gosset, E_8

De la même manière, la figure 2.12 représente la mise en œuvre pratique de la formule complexe de E_8, $E_8 = (4,1,4) + \phi(4,3,2) + \phi^2\mathbb{G}^4$. On choisit ici un partitionnement de la QAM-64 de profondeur 2 en quatre sous-ensembles $\{A_0, A_1, B_0, B_1\}$ de 16 points. Chacun des quatre symboles du point $\mathbf{x}$ de E_8 appartient à un sous-ensemble Y_i. Les quatre bits fournis par le code à répétition $(4,1,4)$ déterminent le choix de $Y = A$ ou $Y = B$; les quatre bits fournis par le code de

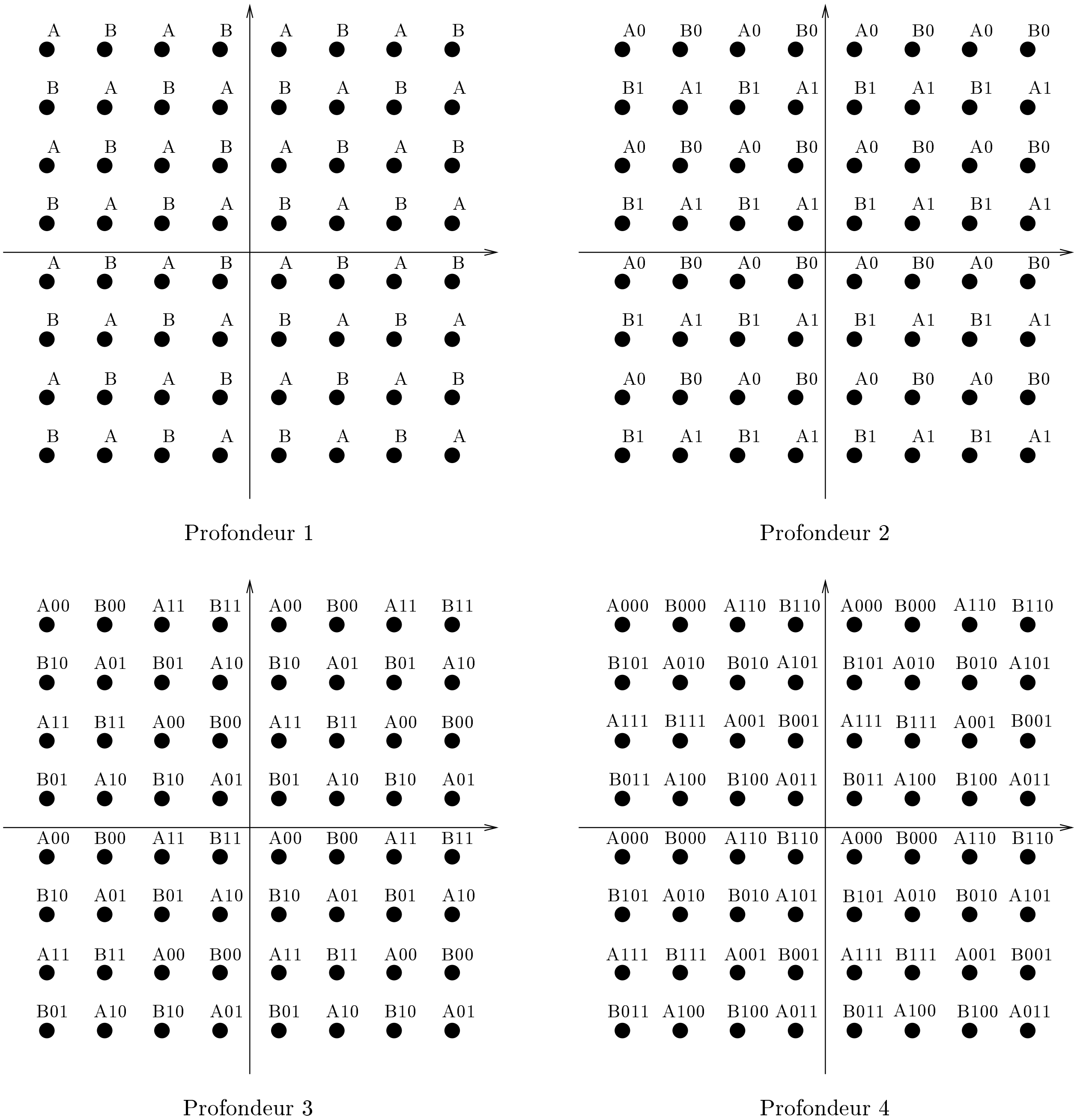


FIG. 2.10 – Partitionnement de profondeur 1 à 4 de la modulation QAM de taille 64.

parité $(4, 3, 2)$ celui des quatre indices i. Il faut ensuite 4 bits supplémentaires pour déterminer chaque symbole dans un sous-ensemble, d'où les 4×4 bits non codés. L'efficacité spectrale est de 5 bits/symbole (20 bits d'information pour 4 symboles) et le gain fondamental est bien $\gamma_{dB}(E_8) = 10 \log_{10}(2^2) - 3 \times 1 = 3$ dB.

Le réseau de Barnes-Wall, Λ_{16}

La formule complexe de Λ_{16} est donnée par $\Lambda_{16} = (8, 1, 8) + \phi(8, 4, 4) + \phi^2(12, 11, 2) + \phi^3\mathbb{G}^{12}$. La figure 2.13 n'est pas la traduction directe de cette formule. Il est plus simple de construire Λ_{16}

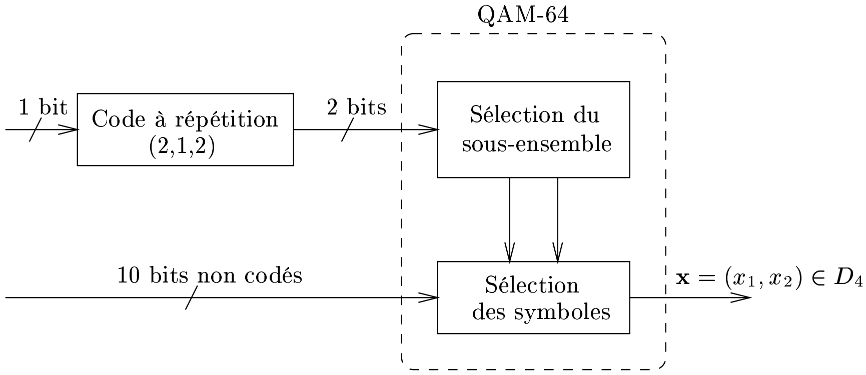


FIG. 2.11 – Codeur cubique du réseau D_4 d'efficacité spectrale 5.5 bits/symbole.

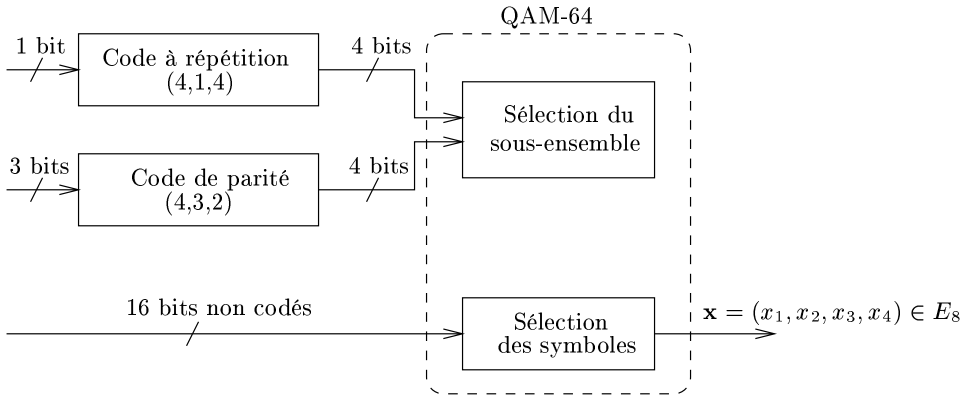


FIG. 2.12 – Codeur cubique du réseau E_8 d'efficacité spectrale 5 bits/symbole.

comme la superposition de deux copies d'un même réseau, l'une des deux étant une simple translation de la première. Le sous-réseau ici considéré est $H_{16} = (16, 11, 4) + 2\mathbb{Z}^{16}$. Alors $\Lambda_{16} = H_{16} \cup (H_{16} + a)$, où a est le vecteur de translation. La QAM-64 est partitionnée en huit sous-ensembles Y_{ij}. Chacune des huit composantes du point de Λ_{16} appartient à l'un d'eux. Le premier niveau de partition correspond aux deux copies de H_{16}. Les huit bits Y sont donnés par le code à répétition $(8, 1, 8)$ et les huit couples (i, j) par le code de Reed-Muller $(16, 11, 4)$. Il manque alors 8×3 bits non codés pour choisir les huit symboles dans les sous-ensembles Y_{ij}. 36 bits d'information servent à coder huit symboles, l'efficacité spectrale de ce codeur est de 4.5 bits/symbole. Une fois encore, on retrouve le gain fondamental de Λ_{16}, $\gamma_{dB}(\Lambda) = 10 \log_{10}(2^3) - 3 \times 1.5 = 4.5$ dB.

Le réseau de Leech, Λ_{24}

Ici encore, le codeur de la figure 2.14 n'est pas la traduction exacte de la formule complexe, $\Lambda_{24} = (12, 1, 16)' + \phi(12, 5, 8)' + \phi^2(12, 7, 4) + \phi^3(12, 11, 2) + \phi^4\mathbb{G}^{12}$. On superpose deux versions (les sous-ensembles A et B) translatées du réseau $H_{24} = (24, 12, 8) + 2(24, 23, 2) + 4\mathbb{Z}^{24}$, soit $\Lambda_{24} = H_{24} \cup (H_{24} + a)$ où a est toujours le vecteur de translation. Le partitionnement de la QAM-64 est cette fois de profondeur 4. Chaque composante x_i du point de Λ appartient à un sous-ensemble Y_{ijk}. Les douze bits Y sont fournis par le code à répétition $(12, 1, 12)$ et les douze couples (i, j) par le code de Golay $(24, 12, 8)$. Les douze bits k sont eux donnés par le code de parité. La parité est paire si $Y = A$ et impaire si $Y = B$. Finalement, il manque 12×2 bits non codés pour déterminer parfaitement les douze symboles. Les 48 bits d'information

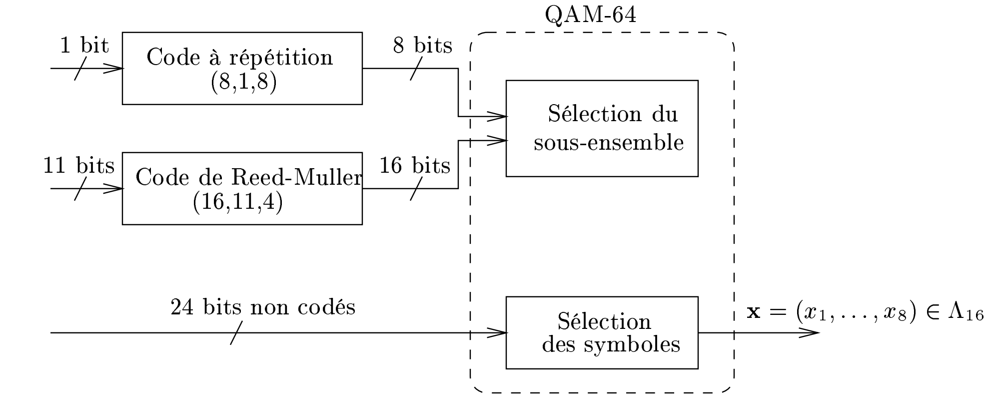


FIG. 2.13 – Codeur cubique du réseau Λ_{16} d'efficacité spectrale 4.5 bits/symbole.

utilisés par ce codeur pour choisir un vecteur de douze composantes mènent à une efficacité spectrale de 4 bits/symbole. Et comme précédemment, on retrouve le gain fondamental de Λ_{24}, $\gamma_{dB}(\Lambda_{24}) = 10\log_{10}(2^4) - 3 \times 2 = 6$ dB.

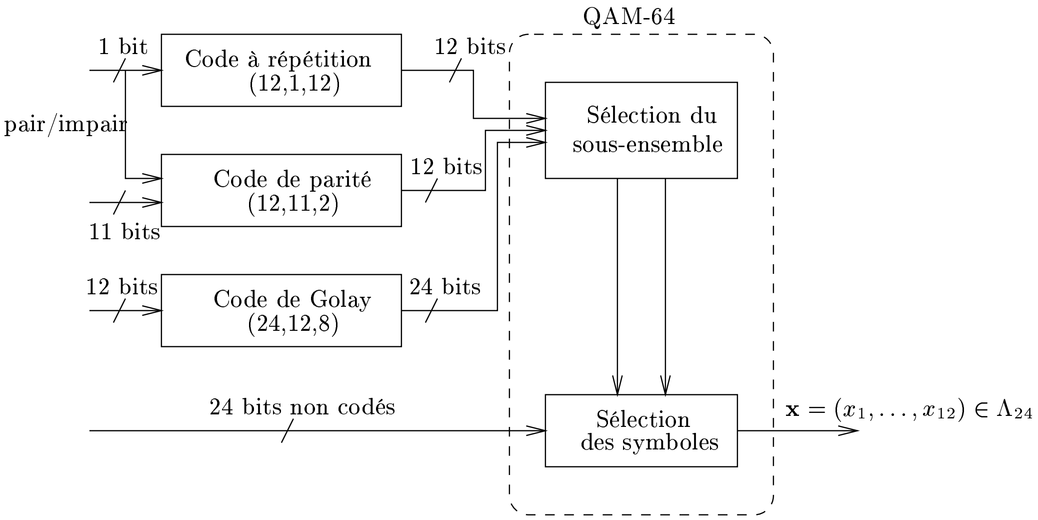


FIG. 2.14 – Codeur cubique du réseau Λ_{24} d'efficacité spectrale 4 bits/symbole.

Nous abordons maintenant les différentes méthodes de décodage qui pourront être associées à ces codeurs, en commençant par le décodage par sphères.

2.3.4 Décodage par sphères

Le décodage par sphères est un algorithme de décodage optimal au sens du maximum de vraisemblance d'un réseau N-dimensionnel Λ quelconque utilisé aussi bien sur un canal à bruit additif blanc gaussien que sur un canal à évanouissements [76]. Nous nous limitons ici au cas du canal gaussien. Le réseau Λ est généré par une matrice réelle M, de taille $N \times N$. Le décodeur ML recherche, parmi tous les points du réseau, celui qui est le plus proche du vecteur reçu. En pratique, cela revient à minimiser la métrique

$$m(\mathbf{y}/\mathbf{x}) = ||\mathbf{y}-\mathbf{x}||^2 = \sum_{i=1}^{N} |y_i - x_i|^2 \tag{2.34}$$

où $\mathbf{x}$ est le point de Λ émis sur le canal, $\mathbf{y} = \mathbf{x} + \mathbf{b}$ le point reçu et $\mathbf{b} = (b_1, \ldots, b_N)$ le vecteur de bruit. 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 donné par $\mathbb{Z}^N M = \{\mathbf{x} \in \mathbb{R}^N / \exists \mathbf{z} \in \mathbb{Z}^N, \mathbf{x} = \mathbf{z}M\}$, où M est la matrice génératrice du réseau et $\mathbf{z} = (z_1, \ldots, z_N)$ le vecteur de composantes entières associé aux bits d'information.

En pratique, l'ensemble des vecteurs $\mathbf{z}$ est limité à un sous-ensemble $\mathcal{A}^N$ de taille finie dans $\mathbb{Z}^N$. Les points du réseau associés à $\mathcal{A}^N$ forment une constellation finie extraite de Λ. Le décodeur ML exhaustif recherche le meilleur point $\mathbf{x}$ parmi tous les points de cette constellation tandis que le décodeur par sphères restreint sa recherche aux points situés dans une sphère de rayon $\sqrt{C}$ et centrée sur le point reçu $\mathbf{y}$. Une représentation géométrique de l'algorithme est illustrée figure 2.15.

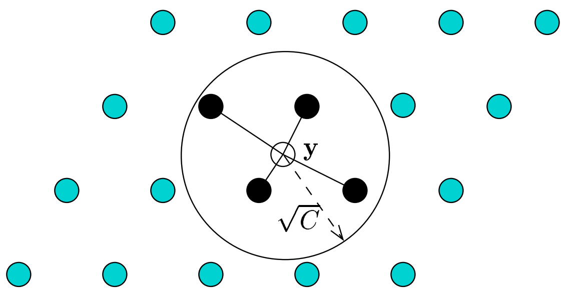


Fig. 2.15 – Représentation géométrique de l'algorithme de décodage par sphères.

Le décodeur recherche ainsi le vecteur $\mathbf{w}$ de norme minimale dans le réseau translaté $\mathbf{y} - \Lambda$ de l'espace eulidien $\mathbb{R}^N$ puisque

$$\min_{\mathbf{x}\in\Lambda} ||\mathbf{y}-\mathbf{x}|| = \min_{\mathbf{w}\in\mathbf{y}-\Lambda} ||\mathbf{w}|| \tag{2.35}$$

Nous travaillons désormais avec les notations suivantes

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

$\mathbf{z} \in \mathbb{Z}^N$, $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_N) \in \mathbb{R}^N$ et $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_N) \in \mathbb{R}^N$.

Du fait de la présence du bruit sur le canal, les vecteurs $\boldsymbol{\rho}$ et $\boldsymbol{\xi}$ sont des vecteurs réels. Par ailleurs, $\mathbf{w} = \mathbf{y} - \mathbf{x}$, alors, $\xi_i = \rho_i - z_i$ pour tout indice $i = 1, \ldots, N$. Le point $\mathbf{w}$ est un point du réseau dont les coordonnées ξ_i sont exprimées dans le repère translaté centré sur le point reçu $\mathbf{y}$. Si $\mathbf{w}$ appartient bien à la sphère centrée en $\mathbf{y}$, c'est-à-dire en $\mathbf{0}$ dans le nouveau repère, de rayon égal à $\sqrt{C}$, alors $\boldsymbol{\xi}$ vérifie la relation suivante

$$||\mathbf{w}||^2 = F(\boldsymbol{\xi}) = \boldsymbol{\xi}MM^t\boldsymbol{\xi}^t = \boldsymbol{\xi}G_\Lambda\boldsymbol{\xi}^t = \sum_{i=1}^{N}\sum_{j=1}^{N} g_{ij}\xi_i\xi_j \leq C \tag{2.36}$$

Dans le nouveau repère, la sphère de centre $\mathbf{y}$ et de rayon $\sqrt{C}$ est transformée en un ellipsoïde centré sur l'origine et défini par la forme bilinéaire $F(\boldsymbol{\xi})$. La factorisation de Cholesky [24] de la matrice de Gram $G_\Lambda = MM^t$ donne $G_\Lambda = AA^t$, où $A = (a_{ij})_{i,j=1,\ldots,N}$ est une matrice triangulaire inférieure. L'inégalité (2.36) devient

$$F(\boldsymbol{\xi}) = \boldsymbol{\xi} AA^t \boldsymbol{\xi}^t = ||A^t\boldsymbol{\xi}^t||^2 = \sum_{i-1}^{N}\left(a_{ii}\xi_i + \sum_{j=i+1}^{N} a_{ji}\xi_j\right)^2$$

En posant

$$\begin{array}{ll} f_{ii} = a_{ii}^2 & i = 1,\ldots,N \\ f_{ij} = \dfrac{a_{ij}}{a_{ii}} & i = 1,\ldots,N,\ i = j+1,\ldots,N \end{array}$$

on obtient

$$F(\boldsymbol{\xi}) = \sum_{i=1}^{N} f_{ii}\left(\xi_i + \sum_{j=i+1}^{N} f_{ji}\xi_j\right)^2 \tag{2.37}$$

En s'intéressant en premier lieu à ξ_N puis en ajoutant une à une les autres composantes ξ_i, $i = N-1,\ldots,1$, on construit un système de N équations qui définissent les limites de l'ellipsoïde

$$\begin{array}{rcl} f_{NN}\xi_N^2 & \leq & C \\ f_{N-1,N-1}(\xi_{N-1} + f_{N,N-1}\xi_N)^2 + f_{NN}\xi_N^2 & \leq & C \\ \forall 1 \leq \ell \leq N \ \displaystyle\sum_{i=\ell}^{N} f_{ii}\left(\xi_i + \sum_{j=i+1}^{N} f_{ji}\xi_j\right)^2 & \leq & C \end{array} \tag{2.38}$$

Les bornes données par le système (2.38) nous permettent d'établir les relations que doivent satisfaire les composantes z_i du vecteur entier $\mathbf{z}$ initial [75][76]

$$\begin{array}{rcl} \left\lceil -\sqrt{\dfrac{C}{f_{NN}}} + \rho_N \right\rceil \leq & z_N & \leq \left\lfloor \sqrt{\dfrac{C}{f_{NN}}} + \rho_N \right\rfloor \\ \left\lceil -\sqrt{\dfrac{C - f_{NN}\xi_N^2}{f_{N-1,N-1}}} + \rho_{N-1} + f_{N,N-1}\xi_N \right\rceil \leq & z_{N-1} & \leq \left\lfloor \sqrt{\dfrac{C - f_{NN}\xi_N^2}{f_{N-1,N-1}}} + \rho_{N-1} + f_{N,N-1}\xi_N \right\rfloor \end{array}$$

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

$$z_i \leq \left\lfloor \sqrt{\frac{1}{f_{ii}}\left(C - \sum_{\ell=i+1}^{N} f_{\ell\ell}\left(\xi_\ell + \sum_{j=\ell+1}^{N} f_{j\ell}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{N} f_{ji}\xi_j \right\rfloor \tag{2.39}$$

où $\lceil x \rceil$ est le plus petit entier supérieur à x et $\lfloor x \rfloor$ le plus grand entier inférieur à x. Grâce aux bornes fournies par les équations (2.39), on constate que le décodeur par sphères fonctionne avec

N compteurs, un pour chaque composante z_i. Il suffit alors de faire varier chacun des différents compteurs sur la plage de variation définie par les bornes, tout en remarquant que les compteurs sont dépendants les uns des autres. En pratique, les bornes sont mises à jour de manière récursive [76].

L'utilisation des compteurs permet d'énumérer de façon exhaustive tous les points entiers $\mathbf{z}$ associés à des points du réseau et situés dans la sphère de rayon $\sqrt{C}$. Les points du réseau situés en dehors de la sphère ne sont ainsi jamais testés. La complexité de l'algorithme est parfaitement indépendante de la taille $|\mathcal{A}|^N$ de la constellation, en revanche, elle est fortement liée au choix de la valeur de C, qui devient par là même un élément crucial de la mise en œuvre de l'algorithme.

Le nombre de points présents dans la sphère de rayon $\sqrt{C}$ augmente avec C. Une valeur de C trop petite peut conduire à une sphère vide, le décodeur ne trouve aucun point. Pour l'éviter, on choisit le rayon $\sqrt{C}$ au moins égal au rayon de recouvrement du réseau. Par ailleurs, si C est trop grand, l'algorithme est fortement ralenti. Une valeur qui satisfait ces deux contraintes est donnée par la borne supérieure de Rogers [26]

$$\sqrt{C} = \sqrt[N]{(N \log N + N \log(\log N) + 5N) \frac{\sqrt{det(\Lambda)}}{V_N}} \tag{2.40}$$

où V_N est le volume d'une sphère de rayon unité en dimension N donné par la formule (2.18).

En pratique, le rayon $\sqrt{C}$ est actualisé régulièrement à la valeur de la dernière norme euclidienne calculée pour un point de l'ellipsoïde. Enfin, on peut remarquer que l'utilisation d'une constellation finie plutôt que celle du réseau entier engendre des effets de bord : on peut être amené à choisir un point du réseau extérieur à la constellation. Ces effets peuvent être évités mais les conséquences de telles techniques de projection sur la complexité globale de l'algorithme dépendent de la forme exacte de la constellation. Par exemple, pour une constellation cubique, il suffit de s'assurer que les composantes du point sélectionné sont bien dans un intervalle donné.

2.3.5 Décodage à entrée souple des codes en blocs appliqué au décodage des réseaux de points

Les deux méthodes de décodage déjà citées, à savoir le décodage ML exhaustif qui recherche le meilleur point dans toute la constellation, et l'algorithme de décodage par sphères qui cherche le meilleur point dans une sphère de rayon fini, nécessitent une importante puissance de calcul. L'avantage du décodage par sphères par rapport au décodage ML exhaustif peut encore être amélioré par des techniques de décodage dites sous-optimales qui offrent pourtant des performances tout à fait correctes. La recherche de tels décodeurs a donné lieu à de nombreux travaux [3][23][25][27][38][66][71]. La plupart de ces méthodes reposent sur des algorithmes de décodage souple des codes en blocs, tel que l'algorithme de Wagner.

Deux décodeurs sous-optimaux du réseau de Gosset E_8 sont décrits dans ce paragraphe : un premier décodeur associé à une construction A complexe de E_8 repose sur l'algorithme de Wagner ; un second, relatif à une construction A réelle, utilise le formalisme des modulations codées et réalise un décodage multiniveaux.

En terme de décodage, un effacement est caractérisé par une amplitude inconnue et une position connue tandis qu'une erreur est d'amplitude inconnue et de position inconnue. La notion d'effacement n'est valable que dans le cas d'un décodage souple. Elle permet justement au décodage souple de codes linéaires de présenter un gain asymptotique par rapport au décodage dur donné par

$$G_{\text{asympt}} = 10\log_{10}(R \times d_{Hmin})$$

où R est le rendement du code. Cette formule n'est valable que pour les codes linéaires mais un code linéaire ou non de distance minimale d_{Hmin} permettra toujours de remplir $\mathcal{T} = d_{Hmin} - 1$ effacements et de corriger $t = \left[\frac{d_{Hmin}-1}{2}\right]$ erreurs.

Considérons l'exemple du code de parité $(6,5,2)$. Ce code est linéaire et binaire. Sa capacité de correction $t = \left[\frac{2-1}{2}\right]$ est nulle mais il peut détecter $\mathcal{T} = 2 - 1 = 1$ erreur, c'est-à-dire remplir un effacement. Dans le cas d'un code de parité, $G_{\text{asympt}} = 10\log_{10}\left(\frac{k}{k+1} \times 2\right)$. Pour le $(6,5,2)$, $G_{\text{asympt}} = 2.22$ dB.

Algorithme de Wagner adapté au décodage de E_8

Soit le code de parité $C(6,5,2)$. Supposons que l'on émette la suite de bits codés (110101), soient modulés par une BPSK (1,1,-1,1,-1,1), sur un canal gaussien et qu'en réception on observe $y = (0.9, -0.2, -0.8, +1.4, -1.1, 0.9)$. Dans le cas d'une simple détection à seuil (décodage dur), le mot décodé (100101) est erroné puisque la parité n'est plus vérifiée. Cependant, la capacité de correction du code étant nulle, on ne pourra pas corriger cette erreur. En revanche, dans le contexte d'un décodage souple, on peut utiliser la parité et l'information souple donnée par y. Ainsi, on sait qu'il y a une erreur et on constate que la valeur -0.2 est la moins fiable de toutes. On décide de complémenter le bit correspondant et on trouve (110101) qui est le mot de code émis. Cet exemple rapide est une application de la règle de Wagner pour les codes de parité.

Définition 2.3.26 *(règle de Wagner)*
Soit $C(n, n-1, 2)$ un code de parité et soit $\mathbf{y} = (y_1, \ldots, y_n)$ le vecteur reçu en sortie du canal de transmission où y_i est une valeur souple. La règle de Wagner consiste à complémenter le bit le moins fiable.

Il est possible de généraliser cette règle au cas d'un code linéaire quelconque, $C(n,k)$. Dans ce cas, on ne complémente plus seulement un bit, mais plusieurs. Le choix des bits concernés est lié au calcul de valeurs de confiance.

Voyons maintenant comment appliquer cette règle au décodage du réseau de Gosset construit à partir de la formule complexe $E_8 = (4,1,4) + \phi(4,3,2) + \phi^2\mathbb{G}^4$. Le partitionnement de la QAM-64 est de profondeur deux et le codeur a été décrit figure 2.10. Le point de E_8 est de la forme $\mathbf{x} = (x_1, x_2, x_3, x_4)$ où chaque composante appartient à un des quatre sous-ensembles de la partition $Y_i \in \{A_0, A_1, B_0, B_1\}$. Comme expliqué précédemment, les quatre bits du code à répétition $(4,1,4)$ permettent de choisir entre les sous-ensembles A et B tandis que les quatre bits du code de parité $(4,3,2)$ fournissent les indices i. En sortie du canal gaussien, on reçoit un vecteur $\mathbf{y}$ de quatre observations complexes. L'algorithme proposé est le suivant :

- recherche d'un candidat possible dans le sous-ensemble A
  - calcul des 16 distances $||\mathbf{y} - \mathbf{a_0}||^2$, $\mathbf{a_0} \in A_0$

    * conserver la plus petite valeur $||\mathbf{y} - \hat{\mathbf{a}}_{\mathbf{0}}||^2$,
    * et le point correspondant $\hat{\mathbf{a}}_{\mathbf{0}}$
  - calcul des 16 distances $||\mathbf{y} - \mathbf{a_1}||^2$, $\mathbf{a_1} \in A_1$
    * conserver la plus petite valeur $||\mathbf{y} - \hat{\mathbf{a}}_{\mathbf{1}}||^2$,
    * et le point correspondant $\hat{\mathbf{a}}_{\mathbf{1}}$
  - calcul de la valeur de confiance dans le sous-ensemble A
    * $m_A = ||\mathbf{y} - \hat{\mathbf{a}}_{\mathbf{1}}||^2 - ||\mathbf{y} - \hat{\mathbf{a}}_{\mathbf{0}}||^2$ est stockée
    * si $m_A > 0$, $\mathbf{y}$ est plus proche de A_0, alors $\hat{\mathbf{a}} = \hat{\mathbf{a}}_{\mathbf{0}}$
    * si $m_A < 0$, $\mathbf{y}$ est plus proche de A_1, alors $\hat{\mathbf{a}} = \hat{\mathbf{a}}_{\mathbf{1}}$

- recherche d'un candidat possible dans le sous-ensemble B
  - calcul des 16 distances $||\mathbf{y} - \mathbf{b_0}||^2$, $\mathbf{b_0} \in B_0$
    * conserver la plus petite valeur $||\mathbf{y} - \hat{\mathbf{b}}_{\mathbf{0}}||^2$,
    * et le point correspondant $\hat{\mathbf{b}}_{\mathbf{0}}$
  - calcul des 16 distances $||\mathbf{y} - \mathbf{b_1}||^2$, $\mathbf{b_1} \in B_1$
    * conserver la plus petite valeur $||\mathbf{y} - \hat{\mathbf{b}}_{\mathbf{1}}||^2$,
    * et le point correspondant $\hat{\mathbf{b}}_{\mathbf{1}}$
  - calcul de la valeur de confiance dans le sous-ensemble B
    * $m_B = ||\mathbf{y} - \hat{\mathbf{b}}_{\mathbf{1}}||^2 - ||\mathbf{y} - \hat{\mathbf{b}}_{\mathbf{0}}||^2$ est stockée
    * si $m_B > 0$, $\mathbf{y}$ est plus proche de B_0, alors $\hat{\mathbf{b}} = \hat{\mathbf{b}}_{\mathbf{0}}$
    * si $m_B < 0$, $\mathbf{y}$ est plus proche de B_1, alors $\hat{\mathbf{b}} = \hat{\mathbf{b}}_{\mathbf{1}}$

- vérification de la parité dans le sous-ensemble A
  - si la parité est vérifiée, le candidat $\hat{\mathbf{a}}$ reste le même.
  - sinon, complémenter le choix, ($\hat{\mathbf{a}} = \hat{\mathbf{a}}_{\mathbf{0}}$ devient $\hat{\mathbf{a}}_{\mathbf{1}}$ et inversement).

- vérification de la parité dans B
  - si la parité est vérifiée, le candidat $\hat{\mathbf{b}}$ reste le même.
  - sinon, complémenter le choix, ($\hat{\mathbf{b}} = \hat{\mathbf{b}}_{\mathbf{0}}$ devient $\hat{\mathbf{b}}_{\mathbf{1}}$ et inversement).

- Choix du point décodé entre le candidat de A et celui de B
  - $||\mathbf{y} - \hat{\mathbf{a}}||^2 > ||\mathbf{y} - \hat{\mathbf{b}}||^2 \Rightarrow \hat{\mathbf{y}} = \hat{\mathbf{a}}$
  - $||\mathbf{y} - \hat{\mathbf{a}}||^2 < ||\mathbf{y} - \hat{\mathbf{b}}||^2 \Rightarrow \hat{\mathbf{y}} = \hat{\mathbf{b}}$

Les deux premières étapes correspondent aux bits non codés du schéma 2.12. Il s'agit de déterminer pour chacun des quatre sous-ensembles, quel point est le plus probablement émis. Les étapes 3 et 4 sont relatives au code de parité. On peut alors choisir entre A_0 et A_1 d'une part et B_0 et B_1 d'autre part. Enfin, l'étape 5 décode le code à répétition et fixe le choix définitif entre A et B.

Il est utile de préciser la manière dont est calculée la valeur de confiance dans chaque sous-ensemble $Y = A$ ou B pour justifier son expression. i désigne le bit de parité. La probabilité *a posteriori* pour les deux valeurs du bit, $i = 0$ et $i = 1$ (c'est-à-dire A_0 et A_1 ou B_0 et B_1), est évaluée puis on en déduit, par exemple pour le cas $Y = A$, une valeur de confiance du type

$$m_Y = \log\left(\frac{\mathrm{APP}(0)}{\mathrm{APP}(1)}\right)$$

Par définition, et en appliquant la règle de Bayes, on a

$$\mathrm{APP}(i) = p(i/\mathbf{y}) = \frac{p(\mathbf{y}/i)P(i)}{P(\mathbf{y})}$$

Et $\mathrm{APP}(i) \propto p(\mathbf{y}/i)$ puisque les deux sous-ensembles sont équiprobables. Les deux sous-constellations A et B sont deux versions translatées d'une même QAM-32. Alors

$$\mathrm{APP}(i) \propto \sum_{\mathbf{a}\in\mathrm{QAM}-32} p(\mathbf{y},\mathbf{a}/i) = \sum_{\mathbf{a}\in\mathrm{QAM}-32} p(\mathbf{y}/\mathbf{a},i)p(\mathbf{a},i) \tag{2.41}$$

où la probabilité $p(\mathbf{a}, i)$ vaut 1 si le point $\mathbf{a}$ est dans la sous-partie A_i de la QAM-32, 0 sinon. La connaissance de $\mathbf{a}$ et de i est redondante. L'équation (2.41) devient

$$\mathrm{APP}(i) \propto \sum_{\mathbf{a}\in\mathrm{QAM}-32/\mathbf{a}\in A_i} p(\mathbf{y}/\mathbf{a})$$

En tenant compte du fait que le canal est gaussien et sans mémoire, on obtient finalement

$$\mathrm{APP}(i) \propto \sum_{\mathbf{a}\in\mathrm{QAM}-32/\mathbf{a}\in A_i} \exp\left(-\frac{||\mathbf{y}-\mathbf{a}||^2}{2N_0}\right) \tag{2.42}$$

Les valeurs des probabilités *a posteriori* ainsi calculées permettent d'évaluer la valeur de confiance de A.

$$m_A = \log\left[\frac{\sum_{\mathbf{a}\in\mathrm{QAM}-32/\mathbf{a}\in A_0}\exp\left(-\frac{||\mathbf{y}-\mathbf{a}||^2}{2N_0}\right)}{\sum_{\mathbf{a}\in\mathrm{QAM}-32/\mathbf{a}\in A_1}\exp\left(-\frac{||\mathbf{y}-\mathbf{a}||^2}{2N_0}\right)}\right] \tag{2.43}$$

Cette valeur exacte de m_A nous oblige à estimer la variance du bruit N_0. Pour simplifier la détection, nous considérons que parmi les 16 exponentielles de la somme $\sum_{\mathbf{a}\in\mathrm{QAM}-32/\mathbf{a}\in A_i}$, celle qui correspond au $\mathbf{a}$ le plus proche de $\mathbf{y}$ est prépondérante. On obtient une approximation de la valeur de confiance pour laquelle l'estimation de N_0 devient inutile. En effet

$$\begin{aligned} m_A &\simeq \log\left[\frac{\exp\left(-\frac{||\mathbf{y}-\mathbf{a_0}||^2}{2N_0}\right)}{\exp\left(-\frac{||\mathbf{y}-\mathbf{a_1}||^2}{2N_0}\right)}\right] \\ m_A &\propto ||\mathbf{y}-\mathbf{a_1}||^2 - ||\mathbf{y}-\mathbf{a_0}||^2 \end{aligned} \tag{2.44}$$

Cette dernière expression est celle utilisée dans l'algorithme de Wagner adapté au décodage du réseau de Gosset.

Décodage multiniveaux

Le second décodeur exploite les propriétés de la modulation codée en blocs qui met en œuvre la formule réelle correspondant à une construction A du réseau de Gosset $E_8 = (8, 4, 4) + 2\mathbb{Z}^8$. Le codeur est donné figure 2.16. On sera attentif au fait que dans ce cas, les composantes x_i du point $\mathbf{x}$ de E_8 appartiennent à une PAM-8 et non plus à une modulation d'amplitude en quadrature. C'est pourquoi $\mathbf{x} = (x_1, \dots, x_8)$.

Le point $\mathbf{x} = \mathbf{c_0} + 2\mathbf{z}$ est supposé émis ; $\mathbf{c_0} \in C_0 = (8, 4, 4)$ et $\mathbf{z} \in \mathbb{Z}^8$. On reçoit $\mathbf{y} = (y_1, \dots, y_8)$. Les composantes x_i et y_i sont réelles dans ce cas. En sortie du codeur, $x_i \in \{0, 1, 2, 3\}$. Le décodage multiniveaux permet de traiter successivement les différents codes utilisés ; dans ce cas, deux codes seulement : le code $(8, 4, 4)$ et le code universel. Pour décoder C_0 en convention ± 1 plutôt que $\{0, 1\}$, on centre artificiellement le réseau : le point reçu est multiplié par 2 et on lui retranche 1. Ainsi, $\tilde{\mathbf{y}} = 2\mathbf{c_0} - 1 + 4\mathbf{z}$.

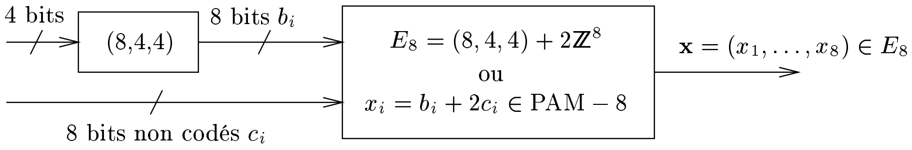


Fig. 2.16 – Codeur cubique du réseau E_8 d'efficacité spectrale 3 bits/symbole.

L'algorithme se déroule comme suit

- translater $\mathbf{y}$ pour pouvoir décoder le code $(8, 4, 4)$ dans $[-1.0, 1.0]$
  - ajouter ou retrancher $4\mathbf{z}$ pour que les composantes soient dans $[-1.0, 3.0[$
  - translater les composantes de $]1.0, 3.0[$ dans $[-1.0, 1.0]$
  - décoder le code $(8, 4, 4)$ de manière exhaustive
  - stocker le candidat $\hat{\mathbf{c}}_\mathbf{0} \in \{0, 1\}$
- retrancher la contribution du code $(8, 4, 4)$ pour pouvoir décoder le code universel $\mathbb{Z}^8$
  - retirer $\hat{\mathbf{c}}_\mathbf{0}$ du mot reçu, et diviser par 2
  - décoder le code universel $\mathbb{Z}^8$ par une détection à seuil
  - stocker le candidat $\hat{\mathbf{z}} \in \{0, 1\}^8$
- reconstruire le point décodé : $\hat{\mathbf{x}} = \hat{\mathbf{c}}_\mathbf{0} + 2\hat{\mathbf{z}}$

Sur canal gaussien, ces deux décodeurs présentent des performances en accord avec la borne théorique donnée par l'équation (2.19)

2.4 Alphabets codés de signaux corrélés sur le canal gaussien

Les rappels que nous venons de faire permettent d'analyser au mieux les résultats obtenus en construisant des alphabets codés de signaux corrélés qui combinent les réseaux ou les TCM et les modulations FSK corrélées. Conformément au schéma 2.1, deux cas sont envisagés : les alphabets multidimensionnels codés par une TCM et ceux codés par un réseau de points.

Afin de pouvoir associer de manière adéquate une TCM à une modulation de fréquence de taille Q, il faut bien choisir le rendement R de la TCM. Les symboles codés et associés aux composantes $s_{m,n}(t)$ via le modulateur sont regroupés par paquets de N. On doit donc coder N symboles, chacun appartenant à une PAM-Q afin d'établir la correspondance avec la Q-FSK. Ces contraintes fournissent une condition jointe sur les variables K, R, N et Q : $K = N \times R \log_2(Q)$. En sortie du canal gaussien, le récepteur est celui donné par la figure 2.2. Les sorties du banc de filtres permettent de décoder l'alphabet multidimensionnel à composantes corrélées avec un décodeur de Viterbi dont la métrique a été adaptée. Comme nous avons déjà pu le constater, cette technique de décodage est particulièrement appropriée aux modulations codées en treillis puisqu'elles ont la propriété de garantir une distance minimale minimum d'une branche à l'autre du treillis.

Lorsque la modulation Q-FSK est codée par un réseau Λ, chaque bloc de K bits b_k correspond au nombre de bits d'information utiles en entrée du codeur. $M = 2^K$ points sont alors disponibles. Le codeur, similaire à ceux présentés plus haut, est choisi de manière à obtenir une constellation cubique de volume $[-(Q-1), +(Q-1)]^N$. Dans tous nos systèmes pratiques, nous travaillons à partir d'une 8-FSK, c'est-à-dire $Q = 8$. Il suffit alors de choisir des codeurs d'efficacité spectrale adéquate. La structure du récepteur a été décrite figure 2.3. Les $N \times Q$ sorties du banc de filtres adaptés sont converties en une information souple qui pourra être délivrée au décodeur de réseau. Rappelons que pour un vecteur $P = (p_1, \ldots, , p_N)$ émis, on note $\tilde{P} = (\tilde{p}_1, \ldots, \tilde{p}_N)$ où

$$\tilde{p}_n = \sum_{q=0}^{Q-1} (2q - Q + 1)\mathrm{APP}(q, n)$$

Le calcul de la valeur des $N \times Q$ probabilités *a posteriori* $\mathrm{APP}(q, n)$ est conditionné par le type de canal. On dispose des trois formules (2.6), (2.8) ou (2.12) selon que le canal est gaussien, de Rayleigh à évanouissements lents ou de Rayleigh à évanouissements rapides. Nous nous limitons dans ce chapire au cas du canal gaussien. Finalement, le vecteur $\tilde{P}$ est présenté à l'entrée d'un décodeur à entrée souple de réseau. Ce pourra être le décodeur par sphères ou l'un des deux décodeurs sous-optimaux. Si le réseau est de dimension raisonnable, $N \leq 8$, on pourra comparer ces résultats à ceux du décodage exhaustif.

Le codage de ces alphabets multidimensionnels est un moyen pour réduire efficacement les erreurs causées par la corrélation des signaux. Le choix du rendement de la TCM est directement lié à la taille de la FSK utilisée. Dans le cas des réseaux, nous allons montrer qu'il faut utiliser un empilement de sphères dense pour atteindre les meilleurs performances.

2.4.1 Choix du réseau

La figure 2.17 illustre le lien entre la constellation cubique $\mathcal{C}$, issue du réseau Λ avec laquelle nous travaillons, et les fréquences. Soit $\mathcal{A}$ l'alphabet multidimensionnel FSK de taille M codé par un réseau de points Λ. M est aussi le nombre de points dans la constellation $\mathcal{C}$ extraite de Λ associée à $\mathcal{A}$. Dans la suite, nous parlerons indifféremment d'alphabet multidimensionnel FSK ou de réseau de fréquences.

On note B la largeur du cube N-dimensionnel relatif à $\mathcal{C}$. B est la bande "artificielle" de la modulation FSK. En la normalisant par l'écart de fréquence élémentaire $\frac{\Delta f_0}{2}$, elle correspond aussi

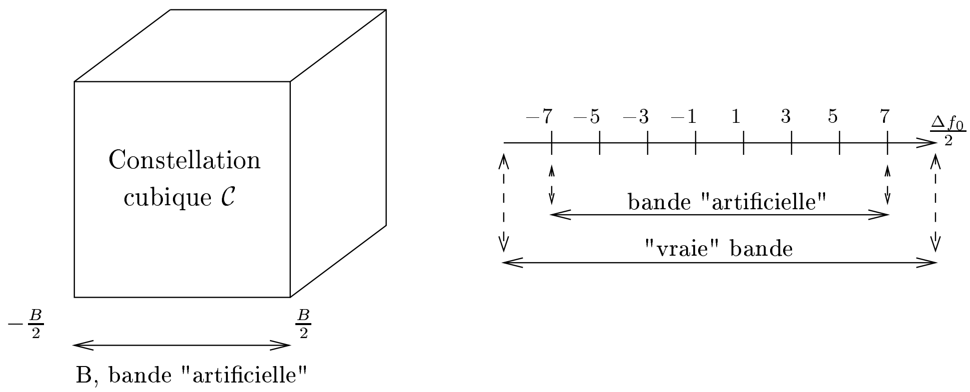


FIG. 2.17 – Constellation cubique N-dimensionnelle.

à l'énergie de la modulation PAM, base du réseau Λ. On remarque que de manière parfaitement équivalente, augmenter le nombre de symboles (resp. fréquences) par dimension dans un réseau de points (resp. fréquences) amplifie l'énergie (resp. la bande totale). Le cardinal de la constellation $\mathcal{C}$, identique à celui de l'alphabet $\mathcal{A}$, peut être exprimé en fonction des paramètres du réseau et de la modulation

$$Card(\mathcal{C}) = M = 2^K = \frac{\left(\frac{B}{\Delta f_0/2}\right)^N}{vol(\Lambda)} \tag{2.45}$$

En effet, le volume fondamental $vol(\Lambda)$ est homogène à des distances plutôt qu'à des écarts de fréquences. K est le nombre de bits d'information par point du réseau. On déduit de l'équation (2.45)

$$B = 2^{\frac{K}{N}} \sqrt[N]{vol(\Lambda)} \frac{\Delta f_0}{2}$$

Cette expression conduit au résultat suivant :

Lemme 2 *Soient $\mathcal{C}$ une constellation cubique extraite d'un réseau Λ et $\mathcal{A}$ l'alphabet N-dimensionnel FSK qui lui est associé dans l'espace des fréquences. Minimiser le volume fondamental du réseau Λ équivaut à minimiser la bande occupée par la modulation FSK.*

Lorque la détection est cohérente, les réseaux les plus denses sont ceux qui obtiennent les meilleures performances sur canal gaussien. Nous montrons que ce résultat est généralisable au cas de la détection non cohérente.

Théorème 2.4.1 *(Optimalité des réseaux denses)*
Soit $\mathcal{A}$ un alphabet N-dimensionnel FSK codé par un réseau Λ. Les performances de $\mathcal{A}$ sur canal gaussien avec détection non cohérente seront d'autant meilleures que Λ sera dense.

Preuve La démonstration de ce théorème repose sur l'analyse des variations de la probabilité d'erreur par paire $P(S_i \to S_j)$ (équation (2.2)) qui dépend des deux paramètres essentiels

$$X_i = \frac{\alpha^2 E}{N_0} \quad \text{et} \quad X_j = \frac{\alpha^2 E}{N_0} \sum_{n=1}^{N} \left(\frac{\sin(\pi \Delta f_n T)}{\pi \Delta f_n T}\right)^2$$

Cette analyse permet de déduire les caractéristiques des meilleurs réseaux et notamment de relier les performances du système codé à la densité du réseau Λ. Nous avons déjà pu remarquer au chapitre 1 que la probabilité d'erreur par paire décroît avec X_j. Sa dépendance en X_i n'est pas influencée par le choix du réseau. Les composantes entières $p_{m,n}$ délivrées par le codeur de réseau et les fréquences élémentaires $f_{m,n}$ des signaux FSK vérifient

$$f_{m,n} = p_{m,n} \times \frac{\Delta f_0}{2}$$

Nous définissons la distance dans l'espace des fréquences entre deux points S_i, S_j de l'alphabet $\mathcal{A}$, notée d_F, par

$$d_F^2 = \sum_{n=1}^{N} \Delta f_n^2, \tag{2.46}$$

où $\Delta f_n = f_{i,n} - f_{j,n}$ est l'écart de fréquences sur la composante n. Cette distance vérifie le lemme 3.

Lemme 3 *La distance d_F dans l'espace des fréquences est proportionnelle au gain fondamental du réseau de points $\gamma(\Lambda)$.*

Deux exemples simples sont d'abord envisagés.

- **S_i et S_j ont une seule composante différente :**
  Alors, il existe un unique indice n pour lequel $s_{i,n}(t) \neq s_{j,n}(t)$, par exemple $n = 1$, c'est-à-dire

  $$|\mu_1^{i,j}| = |\mu_1| = 2E\,\frac{sin(\pi \Delta f_1 T)}{\pi \Delta f_1 T} \quad \text{et} \quad |\mu_n^{i,j}| = 2E,\ \forall n \neq 1$$

  X_j s'écrit

  $$X_j = \underbrace{\frac{\alpha^2}{4EN_0}|\mu_1|^2}_{\text{dépendant du réseau}} + \underbrace{\frac{\alpha^2(N-1)E}{N_0}}_{\text{indépendant du réseau}}$$

  La figure 2.18 illustre l'équivalence réseau de points/réseau de fréquences.

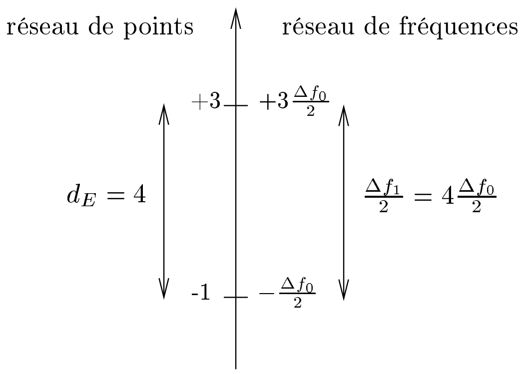


Fig. 2.18 – Projection sur l'axe de l'unique composante distincte de S_i et S_j, $f_{i,1} = 3$ et $f_{j,1} = -1$.

Δf_1 est à la fois proportionnel à la distance euclidienne sur le même axe et à l'écart élémentaire $\frac{\Delta f_0}{2}$. La distance dans l'espace des fréquences définie par $d_F = \sqrt{\Delta f_1^2} = \Delta f_1$ vaut

$$\begin{aligned} d_F &= d_E \, \frac{\Delta f_0}{2} = \frac{d_E}{B} \times B \times \frac{\Delta f_0}{2} \\ &= \frac{d_E}{2^{\frac{K}{N}} \sqrt[N]{vol(\Lambda)} \frac{\Delta f_0}{2}} \times B \times \frac{\Delta f_0}{2} \end{aligned} \tag{2.47}$$

Après simplifications,

$$d_F \propto 2^{-\frac{K}{N}} \, \sqrt{\gamma(\Lambda)} \, B$$

où la distance euclidienne et le gain fondamental vérifient respectivement

$$d_E \propto d_{Emin}(\Lambda) \qquad \text{et} \qquad \gamma(\Lambda) = \frac{d^2_{Emin}(\Lambda)}{\sqrt[\frac{N}{2}]{vol(\Lambda)}}$$

Le lemme 3 est bien vérifié pour ce premier cas particulier.

- **S_i et S_j ont deux composantes différentes :**
  Il existe deux indices n_1 et n_2 pour lesquels $s_{i,n_1}(t) \neq s_{j,n_1}(t)$ et $s_{i,n_2}(t) \neq s_{j,n_2}(t)$, par exemple $n_1 = 1$ et $n_2 = 2$

  $$|\mu_n^{i,j}| = |\mu_n| = 2E \, \frac{sin(\pi \Delta f_n)}{\pi \Delta f_n}, \; n = 1, 2 \qquad \text{et} \qquad |\mu_n^{i,j}| = 2E, \; \forall n \neq 1, 2 \tag{2.48}$$

  X_j s'écrit

  $$X_j = \underbrace{\frac{\alpha^2}{4EN_0}(|\mu_1|^2 + |\mu_2|^2)}_{\text{dépendant du réseau}} + \underbrace{\frac{\alpha^2(N-2)E}{N_0}}_{\text{indépendant du réseau}}$$

  La figure 2.19 illustre le cas de deux composantes distinctes. Comme précédemment, Δf_1 et Δf_2 sont respectivement proportionnels à la distance euclidienne sur leur axe et à $\frac{\Delta f_0}{2}$

  $$\Delta f_1 = d_{E_1} \, \frac{\Delta f_0}{2} \qquad \text{et} \qquad \Delta f_2 = d_{E_2} \, \frac{\Delta f_0}{2} \tag{2.49}$$

  Alors, $d_F = \sqrt{\Delta f_1^2 + \Delta f_2^2}$ vaut

  $$\begin{aligned} d_F &= \sqrt{d^2_{E_1} + d^2_{E_2}} \, \frac{\Delta f_0}{2} \\ &\propto d_{Emin}(\Lambda) \, \frac{\Delta f_0}{2} \\ &\propto 2^{-\frac{K}{N}} \, \sqrt{\gamma(\Lambda)} \, B \end{aligned} \tag{2.50}$$

  Le lemme est encore une fois vérifié.

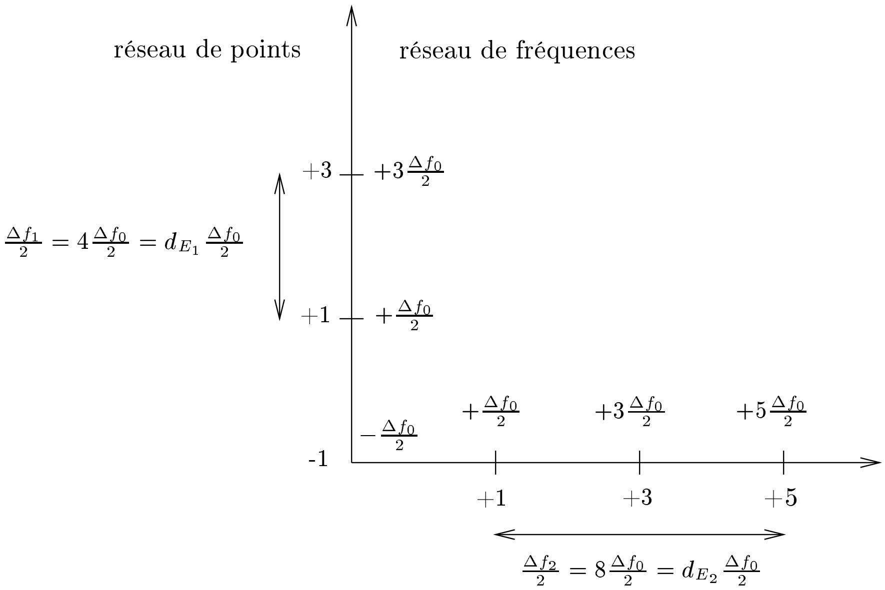


Fig. 2.19 – Projection sur les axes des deux composantes distinctes de S_i et S_j, $f_{i,1} = 3$, $f_{i,2} = 5$, $f_{j,1} = 1$ et $f_{j,2} = 1$.

Ces deux exemples mettent bien en valeur l'équivalence entre les réseaux de points et les réseaux de fréquences ainsi que l'importance du choix du réseau. On peut maintenant généraliser le résultat du lemme 3 à deux points S_i, S_j n'ayant aucune composante commune. X_j s'écrit

$$X_j = \underbrace{\frac{\alpha^2}{4EN_0}(|\mu_1|^2 + |\mu_2|^2 + \ldots + |\mu_N|^2)}_{\text{dépendant du réseau}}$$

Sur chacun des N axes, $\Delta f_n \propto d_{E_n}\ \frac{\Delta f_0}{2}$, soit

$$d_F = \sqrt{\sum_{n=1}^{N} \Delta f_n^2} \propto d_{Emin}(\Lambda)\ \frac{\Delta f_0}{2} \propto 2^{-\frac{K}{N}}\ \sqrt{\gamma(\Lambda)}\ B$$

De plus, la valeur minimale de d_F est donnée par

$$d_{Fmin} = 2^{-\frac{K}{N}} \times \sqrt{\gamma(\Lambda)} \times B \tag{2.51}$$

D'où le lemme 3.

Ce résultat intermédiaire nous permet de démontrer le théorème. En effet la relation (2.51) peut être interprétée comme suit : pour une valeur donnée de l'efficacité spectrale K/N bits par dimension et pour une bande fixe B Hertz, la distance dans l'espace fréquentiel augmente avec la densité du réseau Λ. Par conséquent, en choisissant le réseau le plus dense dans l'espace réel de dimension N, nous maximisons la distance fréquentielle $\sum_{n=1}^{N} \Delta f_n^2$. Ceci équivaut à minimiser le paramètre X_j ; par suite, la contribution de la corrélation dans la probabilité d'erreur par paire, c.q.f.d.

Pour les simulations, nous avons choisi de travailler avec deux cas de réseaux les plus denses : le réseau de Gosset E_8 en dimension 8 et le réseau de Leech Λ_{24} en dimension 24.

2.4.2 Choix de l'espacement fréquentiel de la FSK, Δf_0

Si les réseaux les plus denses sont ceux qui permettent de compenser au mieux les dégradations des performances dues à l'utilisation de signaux corrélés, il faut tout de même veiller au choix de l'espacement fréquentiel. D'une part, Δf_0 intervient (au travers de la bande B) indirectement dans le calcul de l'efficacité spectrale de l'alphabet multidimensionnel FSK codé ; d'autre part, le comportement du réseau ou de la TCM, et notamment le gain de codage réel qu'ils permettent d'atteindre, en dépend fortement. En effet, les réseaux de points et les modulations codées en treillis "voient" le réseau de fréquences.

Soit $\mathcal{C}$ une constellation extraite d'un réseau de points Λ. Elle est construite à partir d'une modulation QAM. Pour ce type de modulation, la notion de voisinage existe et les erreurs ont lieu majoritairement en faveur des voisins les plus proches du point effectivement émis. Dans ces conditions, les réseaux de points se révèlent d'autant plus performants que la dimension et le gain fondamental augmentent. Dans notre cas, les alphabets multidimensionnels associent le codage des réseaux de points aux modulations de fréquence FSK. Lorsque toutes les fréquences sont orthogonales, les signaux sont tous à la même distance c'est-à-dire que la corrélation (notion de distance dans l'espace des fréquences) est la même entre toutes les paires de signaux $(s_i(t), s_j(t))$

$$|\mu_{i,j}| = \begin{cases} 2E & i = j \\ 0 & i \neq j \end{cases}$$

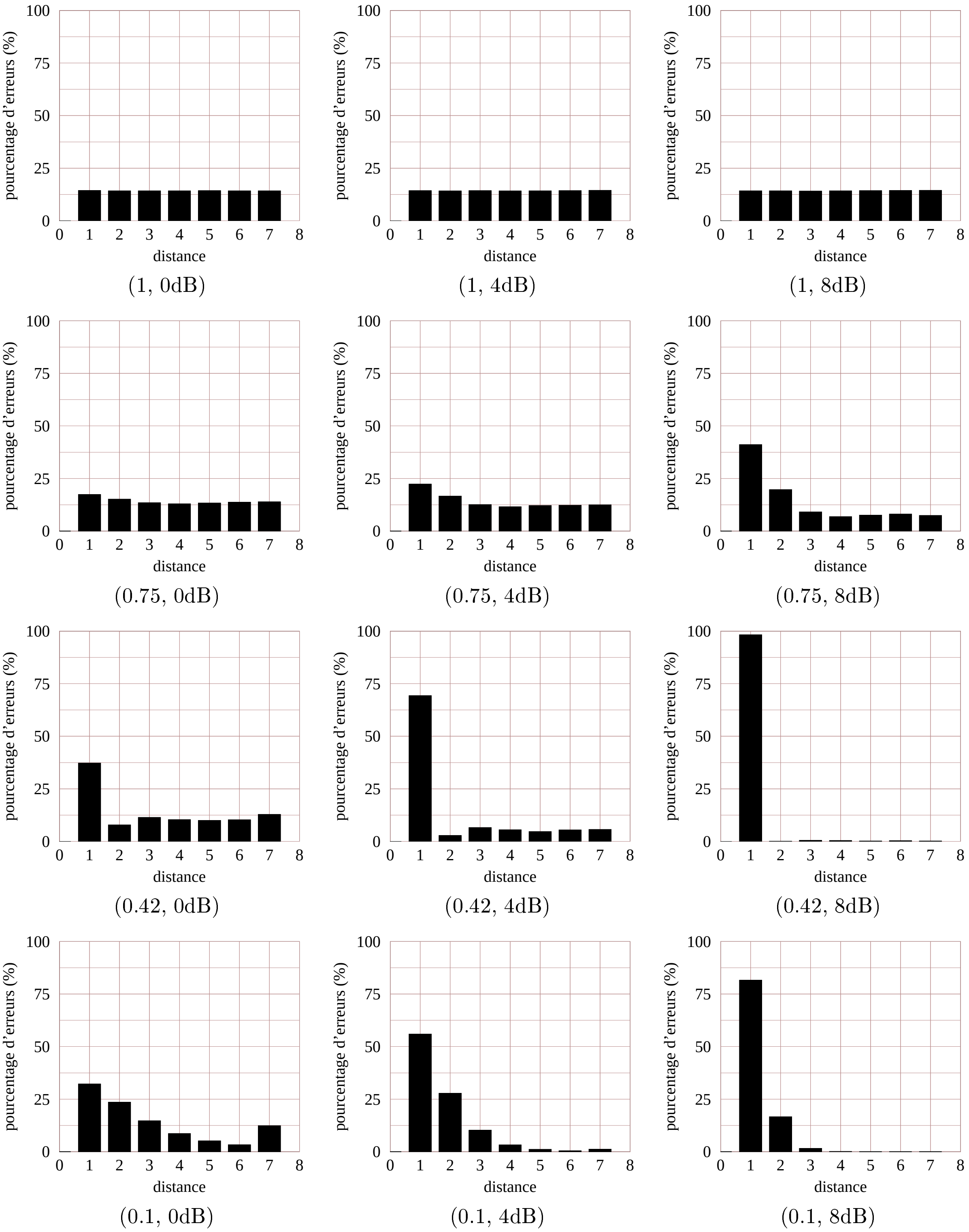
La notion de voisinage n'existe pas pour des modulations de fréquences à signaux orthogonaux. Les erreurs peuvent être faites en faveur de n'importe lequel des signaux FSK et l'effet du réseau est totalement occulté. D'où le résultat suivant

Lemme 4 *Le codage par les réseaux de points d'alphabets N-dimensionnels FSK est utile si et seulement si les signaux FSK sont corrélés, c'est-à-dire que l'espacement fréquentiel élémentaire vérifie $\Delta f_0 < 1/T$.*

En revanche, l'utilisation d'un espacement fréquentiel strictement inférieur à l'inverse du temps symbole introduit un effet de voisinage. La distribution des corrélations permet d'espérer un gain à partir du moment où les plus proches voisins au sens de la corrélation sont vraiment dominants. C'est pourquoi le choix de Δf_0 doit être fait consciencieusement : si $\Delta f_0 T$ est trop proche de 1, tous les signaux sont à la même distance. Si $\Delta f_0 T$ est trop proche de 0, les signaux sont très corrélés et un phénomène de proximité équivalent se manifeste.

Toutes nos simulations sont basées sur l'utilisation d'une modulation 8-FSK. L'analyse de la distribution des erreurs d'une modulation FSK en fonction de la valeur de l'espacement fréquentiel Δf_0 peut être faite théoriquement, ou en traçant les histogrammes des erreurs par simulation. Les démarches que nous avons entamées pour la recherche d'histogrammes théoriques se sont révélées infructueuses. Nous proposons tout de même des résultats de simulation. Différentes valeurs de rapport signal-à-bruit sont envisagées : 0 dB, 4 dB et 8 dB. Le schéma de transmission est très simple : la modulation 8-FSK est émise sur un canal gaussien et la détection est non cohérente. Un critère de décision dure permet d'obtenir les distributions des erreurs de la figure 2.20 ; le signal détecté est celui qui présente la plus grande valeur de probabilité *a posteriori*. Le nombre de points transmis est choisi de manière à obtenir les histogrammes avec une précision suffisante.

Notons que les histogrammes ici présentés sont obtenus par rapport à la fréquence zéro. Les huit fréquences de la modulation n'ont pas le même voisinage (un ou deux voisins selon



(1, 0dB) (1, 4dB) (1, 8dB)

(0.75, 0dB) (0.75, 4dB) (0.75, 8dB)

(0.42, 0dB) (0.42, 4dB) (0.42, 8dB)

(0.1, 0dB) (0.1, 4dB) (0.1, 8dB)

Fig. 2.20 – Distribution des erreurs pour une modulation 8-FSK pour différentes valeurs de $\Delta f_0 T = 1, 0.75, 0.42, 0.1$ (de haut en bas) et du rapport signal-à-bruit $E_b/N_0 = 0, 4, 8$dB (de gauche à droite).

que la fréquence est en bordure de la bande ou au centre). Une étude plus précise devra tenir compte des histogrammes obtenus pour chacune des fréquences pour tracer un histogramme moyen. Cependant, la figure 2.20 illustre parfaitement nos suppositions : lorsque les fréquences sont orthogonales, on se trompe indifféremment sur l'un des huit signaux de la 8-FSK. Lorsque l'espacement fréquentiel diminue et que le rapport signal-à-bruit augmente, la modulation FSK tend vers le comportement d'une modulation QAM : on se trompe uniquement en faveur des signaux à la distance minimale. Nous reviendrons sur le choix de l'espacement fréquentiel au chapitre suivant.

2.4.3 Grande robustesse des schémas codés face à la corrélation

Tous les alphabets multidimensionnels considérés sont construits à partir d'une modulation 8-FSK corrélée, d'espacement fréquenciel $\Delta f_0 < 1/T$. La figure 2.21 rappelle l'effet néfaste de la corrélation sur les performances de cette modulation. Nous l'avions déjà remarqué pour une BFSK au chapitre 1. Différentes valeurs de l'espacement fréquentiel sont envisagées : $\Delta f_0 T = 1.0, 0.5, 0.42, 0.34, 0.25, 0.1$. Les valeurs de corrélation correspondantes sont $\mu = 0, 0.64, 0.73, 0.82, 0.9, 0.98$. L'augmentation de l'efficacité spectrale qui en découle se fait au détriment d'une dégradation considérable de ces performances : pour un taux d'erreur de 10^{-4}, multiplier l'efficacité spectrale par un facteur 4 ($\Delta f_0 T = 1.0 \ \rightarrow \ \Delta f_0 T = 0.25$) conduit à une perte de plus de 8 dB.

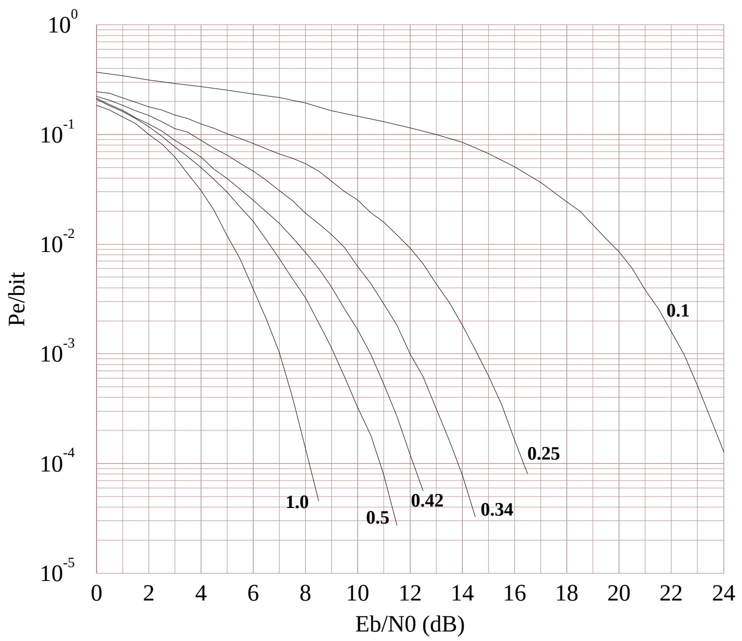
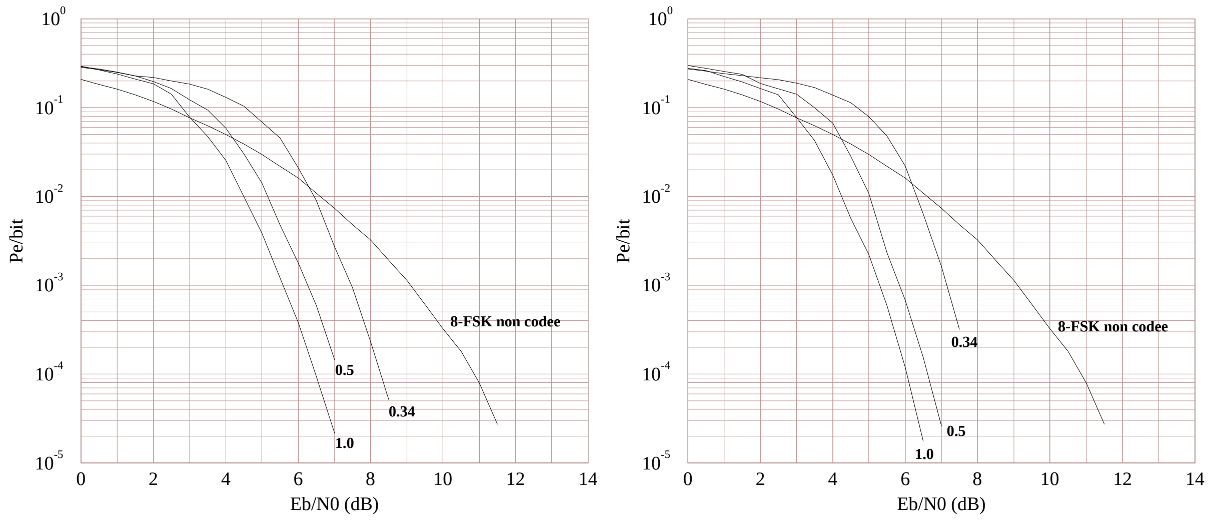


Fig. 2.21 – Performances d'une modulation 8-FSK non codée pour différentes valeurs de l'espacement fréquentiel $\Delta f_0 T = 1.0, 0.5, 0.42, 0.34, 0.25, 0.1$.

Les modulations codées en treillis présentées sont des modulations PAM-8 de rendement 2/3, de longueur de contrainte L et de polynômes générateurs respectifs $L = 5$, $(23, 04, 16)$ et $L = 7$, $(101, 016, 064)$. La structure du décodeur a été décrite au paragraphe 2.1.2. Un système similaire a été proposé par Wittke [79]. Ces travaux se limitent à des modulations Q-FSK de petite taille, $Q \leq 4$, pour lesquelles le gain n'est pas manifeste. Par ailleurs, nous travaillons avec une fenêtre finie dans le treillis pour pouvoir assimiler les alphabets codés TCM à des systèmes de codage faible latence. Wittke considère une fenêtre infinie dans le treillis, le système relève dans ce cas du codage forte latence. La figure 2.22 illustre ainsi les performances d'un alphabet FSK multidimensionnel codé par une TCM 16 états ($L = 5$) et une TCM 64 états ($L = 7$) pour trois valeurs de l'espacement fréquentiel $\Delta f_0 T = 1.0, 0.5, 0.34$. La robustesse d'un tel schéma face à la corrélation est indéniable. Les performances de la modulation 8-FSK non codée avec $\Delta f_0 T = 0.5$ sont données à titre de comparaison. L'alphabet codé TCM, $\Delta f_0 T = 0.5$ et la 8-FSK non codée, $\Delta f_0 T = 0.5$ occupent la même bande. Tandis que l'alphabet codé TCM, $\Delta f_0 T = 0.34$ et la 8-FSK non codée, $\Delta f_0 T = 0.5$ ont la même efficacité spectrale 0.75 bits/s/Hz. Dans les deux cas, le schéma codé apporte un gain pour une probabilité d'erreur de 10^{-3} : 3 dB et 1.75 dB respectivement pour la TCM 2/3, 16 états, 3.25 dB et 2 dB respectivement pour la TCM 2/3, 64 états.

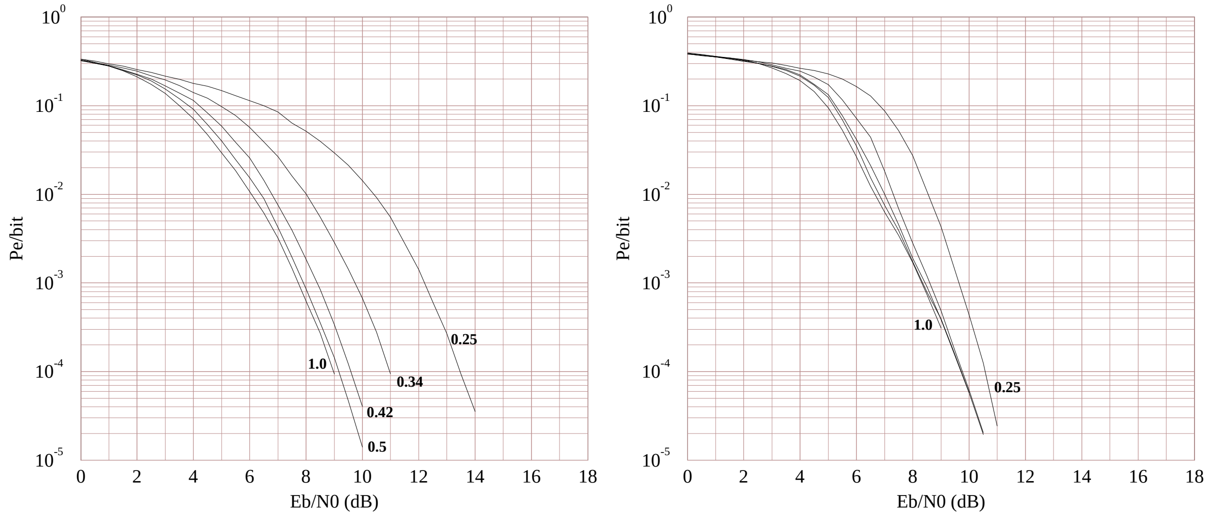


(a) TCM 2/3, 16 états

(b) TCM 2/3, 64 états

Fig. 2.22 – Performances d'une modulation 8-FSK codée par une PAM-8 TCM de rendement 2/3, $\Delta f_0 T = 1.0, 0.5, 0.34$ *vs.* 8-FSK non codée, $\Delta f_0 T = 0.5$.

Un codage par les réseaux de points interdit une démodulation dure. En effet, ne pas exploiter les informations souples fournies par le banc de filtres adaptés équivaut à perdre complètement l'effet du réseau et à ne pas profiter du gain de codage. Nous utilisons le schéma décrit au paragraphe 2.1.3 : une démodulation souple associant un banc de filtres adaptés au convertisseur signal-APP pour canal gaussien et un décodeur de réseaux à entrée souple. Nous nous restreignons ici au décodeur par sphères bien que différents schémas aient été proposés. Ces derniers apporteraient un gain de complexité en cas d'application pratique. Nous donnons les résultats obtenus grâce aux réseaux les plus denses en dimension 8 et 24 : le réseau de Gosset E_8, $\gamma(E_8) = 3$ dB et le réseau de Leech Λ_{24}, $\gamma(\Lambda_{24}) = 6$ dB. Les rendements des codeurs sont respectivement 2.5/3 et 2/3 [26]. La mise en œuvre d'un décodage exhaustif à titre comparatif n'a pas été envisagée. Le nombre de points, 2^{20} et 2^{48} respectivement, conduit à une trop grande complexité. Les performances des alphabets FSK multidimensionnels codés par E_8 et Λ_{24} sont présentées figure 2.23. Les valeurs de l'espacement fréquentiel sont $\Delta f_0 T = 1.0, 0.5, 0.42, 0.34, 0.25$. Comme prévu, le codage par les réseaux est très robuste face à la corrélation et les résultats du réseau de Leech sont meilleurs que ceux du réseau de Gosset. Pour un taux d'erreur de 3×10^{-4}, la perte n'est plus que de 1 dB pour multiplier l'efficacité spectrale par 4 grâce au réseau de Leech.



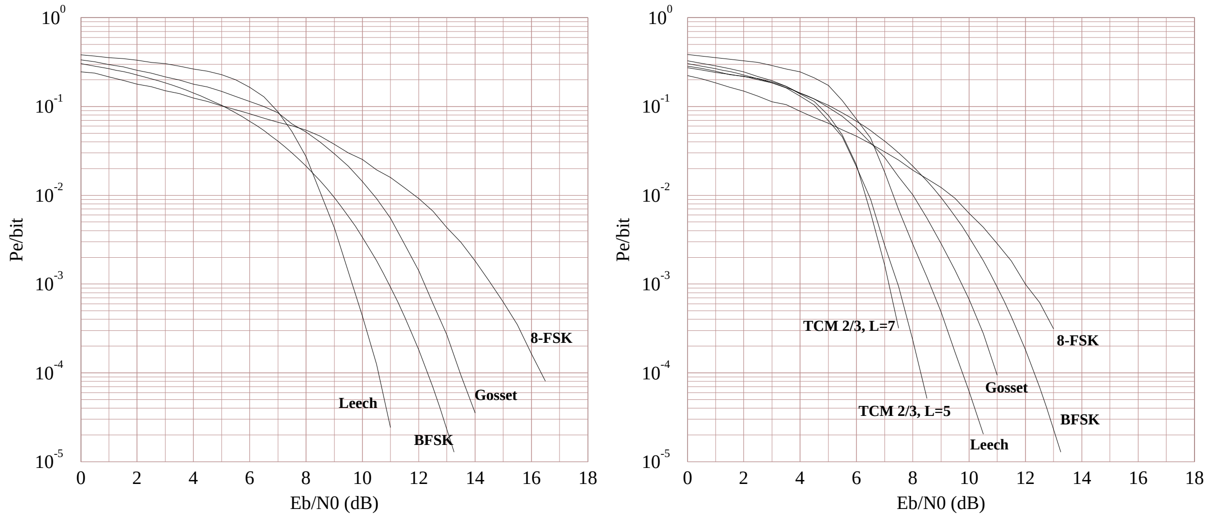
(a) Réseau de Gosset, E_8

(b) Réseau de Leech, Λ_{24}

Fig. 2.23 – Performances d'une modulation 8-FSK codée par un réseau de points, $\Delta f_0 T = 1.0, 0.5, 0.34$.

Les figures 2.24 et 2.25 permettent de comparer les différents systèmes codés ou non à bande fixe ou à efficacité spectrale fixe. L'efficacité spectrale d'une modulation 8-FSK orthogonale non codée est de 0.375 bits/s/Hz. La modulation BFSK orthogonale non codée d'efficacité spectrale 0.5 bits/s/Hz sert de référence. Dans les deux premières figures, on retrouve la modulation 8-FSK non codée et les schémas codés pour $\Delta f_0 T = 0.25$ (a) et $\Delta f_0 T = 0.34$ (b). Tous les systèmes codés se comportent très bien face à la corrélation. Par exemple, l'efficacité spectrale est augmentée de 0.5 à 0.938 bit/s/Hz avec 1.3 dB de gain pour un taux d'erreur de 10^{-4} (E_8, $\Delta f_0 T = 0.34$) et de 0.5 à 0.75 bits/s/Hz avec 2.5 dB de gain pour un taux d'erreur de 2×10^{-5} (Λ_{24}, $\Delta f_0 T = 0.34$).

Les deux dernières figures donnent les résultats pour deux valeurs fixées de l'efficacité spectrale : 0.5 bits/s/Hz (a) et 0.75 bits/s/Hz (b). Ainsi pour la figure 2.25(a), la modulation BFSK non codée est orthogonale et tous les schémas codés supposent une valeur de l'espacement fréquentiel de la 8-FSK égal à $\Delta f_0 T = 0.5$. Pour la figure 2.25(b), on a toujours une BFSK orthogonale, la 8-FSK est telle que $\Delta f_0 T = 0.5$, la 8-FSK codée par le réseau de Gosset suppose



(a) $\Delta f_0 T = 0.25$.

(b) $\Delta f_0 T = 0.34$.

FIG. 2.24 – Comparaison des différents schémas codés ou non à bande fixe, *vs.* BFSK orthogonale non codée.

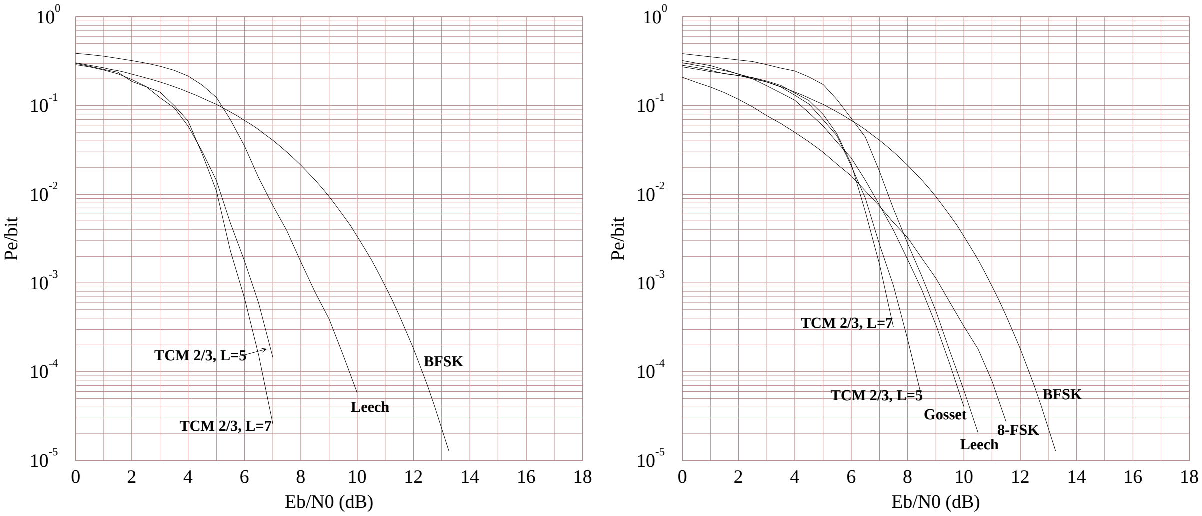
$\Delta f_0 T = 0.42$ tandis que pour tous les autres schémas codés $\Delta f_0 T = 0.34$. Une fois encore, les différents schémas codés se montrent très performants.

2.5 Conclusions

Des TCM et des réseaux de points, le choix du codage faible latence utilisé se fera en fonction des contraintes propres du système pratique. Dans tous les cas, ils ont pour avantage de présenter des complexités de mises en œuvre raisonnables tout en améliorant considérablement les performances de la modulation FSK corrélée sous-jacente. Les réseaux de points, comme les TCM ont la propriété d'optimiser le taux d'erreur par point. Ces systèmes sont par conséquent appropriés aux décodeurs par blocs, aussi bien le décodeur de Viterbi que les décodeurs de réseau. Le traitement des données en réception se fait sur des blocs de N signaux.

Notons que le choix de l'espacement fréquentiel revêt une importance toute particulière lorsque l'on utilise les réseaux de points. Nous généralisons ce résultat dans le chapitre qui suit.

Enfin, nous avons montré et constaté que la densité du réseau conduit à une minimisation du terme P_2 de l'équation (2.2), et donc à de meilleures performances. Le prix à payer pour atteindre effectivement le gain du réseau est une légère perte en efficacité spectrale.



(a) $\eta = 0.5$ bits/s/Hz.

(b) $\eta = 0.75$ bits/s/Hz.

Fig. 2.25 – Comparaison des différents schémas codés ou non à efficacité spectrale fixe η, *vs.* BFSK orthogonale non codée, 0.5 bits/s/Hz.

Chapitre 3

Signaux corrélés et décodage itératif *

Après avoir étudié deux techniques de codage faible latence au chapitre précédent, nous envisageons ici un codage forte latence des alphabets multidimensionnels construits à partir de modulations FSK corrélées. Pour cela, les codes convolutifs et les turbo codes sont considérés. Les codes convolutifs, initialement introduits par Elias [30] comme une alternative aux codes en blocs, ont ensuite donné lieu à de nombreux travaux parmi lesquels [33][44]. Les turbo codes ont été introduits en 1993 par Berrou *et al.* [14].

Depuis l'énoncé du théorème fondamental de codage par Shannon en 1948, le codage de canal en général et la recherche de bons codes en particulier ont fait couler beaucoup d'encre. Des ouvrages de référence sont désormais disponibles [11][50][57][73].

Nous rappelons tout d'abord les principales caractéristiques d'un code convolutif. Par ailleurs, il existe plusieurs méthodes pour les décoder. Nous décrivons au paragraphe 3.1 le décodage à entrée souple et sortie souple (SISO, Soft-Input Soft-Output) qui pourra être utilisé comme brique de base d'un décodage itératif. L'algorithme aller-retour (FB, Forward-Backward) [4] permet de mettre en œuvre l'un de ces décodeurs souples. Nous détaillons ensuite au paragraphe 3.2 la structure ainsi que les performances des turbo codes, avant de passer à la description du système forte latence à proprement dit au paragraphe 3.3.

Deux types de décodage sont envisagés et expliqués. Un décodage APP simple basé sur la concaténation d'un démodulateur APP non cohérent et du décodeur SISO et un décodage constitué d'une détection non cohérente itérative et d'un décodage APP simple.

Finalement, les résultats obtenus avec ces deux types de codes sont explicités aux paragraphes 3.4 et 3.5 : pour les modulations Q-FSK non orthogonales sur canal gaussien et pour un alphabet de diversité 4 à composantes corrélées (cf. chapitre 1) sur canal de Rayleigh.

---

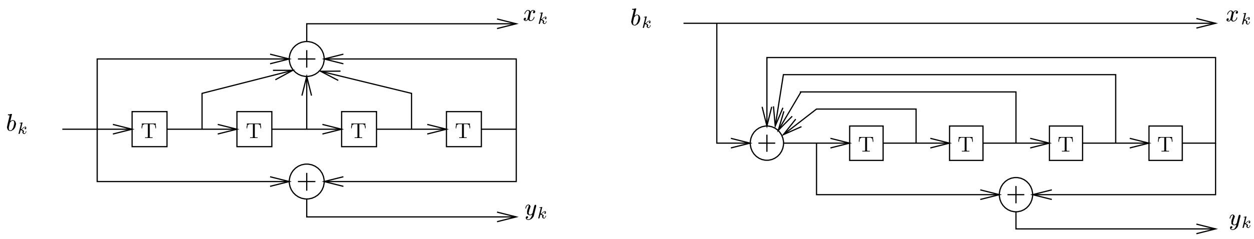
*Les résultats relatifs aux turbo codes ont été présentés au Colloque *Turbo codes in digital broadcasting - Could it double capacity ?*, Londres, novembre 1999, et ont été publiés dans *IEEE Communication Letters*, octobre 2000.

3.1 Décodage à entrée souple et sortie souple d'un code convolutif

Le codeur d'un code convolutif binaire $C(n,k,L)$ admet k bits en entrée et délivre n bits en sortie [57][62]. Il est constitué de k registres à décalage comportant chacun ν cases mémoire où ν et $L = \nu + k$ sont respectivement la mémoire et la longueur de contrainte du code. C est de rendement $R = \frac{k}{n}$. Un code convolutif pourra être décrit par sa matrice génératrice semi-infinie ou par ses polynômes générateurs, en octal dans la plupart des cas, qui lient les n sorties du codeur à ses k entrées. Il existe trois représentations graphiques d'un code convolutif

- *L'arbre* - il est périodique après L étapes ; sa hauteur et sa largeur sont infinies.
- *Le treillis* - sa hauteur est limitée au nombre d'états $2^{k(L-k)}$; sa longueur est infinie et on dénombre 2^k transitions par état.
- *Le diagramme d'état* - il n'est pas périodique, ne possède ni hauteur, ni largeur et permet de trouver la distribution de poids du code.

Le codeur convolutif binaire peut être systématique : à toute suite de k bits en entrée, on associe n bits tels que les k premiers sont une copie des bits d'information et les $n-k$ suivants, les bits codés. Cette propriété n'est pas suffisante. Afin de garantir de bonnes propriétés de distance dans le code, le codeur doit aussi être récursif : les sorties du codeur sont réinjectées en entrée. On identifie alors deux grandes classes de codes convolutifs : les codes convolutifs récursifs systématiques (RSC, Recursive Systematic Convolutional) et les codes convolutifs non récursifs non systématiques (NRNSC, Non-Recursive Non-Systematic Convolutional). Les codes RSC à structure canonique sont de rendement $\frac{k}{k+1}$ et les codes NRNSC de rendement $\frac{k}{n}$. La figure 3.1 représente ainsi deux codeurs possibles pour le code $(2,1,5)$ de polynômes générateurs (37,21).



Code NRNSC Code RSC

FIG. 3.1 – Codeurs du code convolutif (37,21).

Passons maintenant à la description détaillée du décodeur SISO. Le code convolutif $C(n,k,L)$ est utilisé. En considérant une fenêtre de taille finie dans le treillis, il est transformé en un code en blocs linéaire binaire $C(N,K)$. qui contient 2^K mots de longueur N bits. On note $\mathbf{b} = (b_1, \ldots, b_K)$ les K bits d'information en entrée du codeur et $\mathbf{c} = (c_1, \ldots, c_N)$ les N bits codés. Avec un codeur systématique, on retrouve les blocs de bits d'information à l'identique dans la séquence des bits codés. Le vecteur des N échantillons reçus en entrée du décodeur est donné par $\mathbf{x} = (x_1, \ldots, x_N)$. La probabilité *a posteriori*[1] de chacun des N bits codés c_j s'écrit

$$\mathrm{APP}(c_j) = P(c_j/\mathbf{x}) = \sum_{\mathbf{c}\in C} P(c_j, \mathbf{c}/\mathbf{x})$$

[1]Dans ce cas, $\mathrm{APP}(c_j)$ désigne indifféremment $\mathrm{APP}(c_j = 0)$ ou $\mathrm{APP}(c_j = 1)$. La normalisation est faite en divisant par $\mathrm{APP}(c_j = 0) + \mathrm{APP}(c_j = 1)$.

En appliquant la loi de Bayes, on obtient

$$\mathrm{APP}(c_j) = \sum_{\mathbf{c}\in C} \frac{p(\mathbf{x}/c_j,\mathbf{c})P(c_j,\mathbf{c})}{p(\mathbf{x})} \tag{3.1}$$

L'observation $p(\mathbf{x}/c_j,\mathbf{c})$ et la probabilité *a priori* $P(c_j,\mathbf{c})$ sont nulles si le $j$ième bit dans $\mathbf{c}$ est différent de c_j. De plus, si le canal est sans mémoire et que les probabilités *a priori* des bits codés sont indépendantes, alors l'équation (3.1) peut être reformulée

$$\mathrm{APP}(c_j) \propto \sum_{\mathbf{c}\in C/c_j} p(\mathbf{x}/\mathbf{c})P(\mathbf{c}) = \sum_{\mathbf{c}\in C/c_j} \prod_{\ell=1}^{N} p(x_\ell/c_\ell)P(c_\ell) \tag{3.2}$$

$P(c_\ell)$ est la probabilité *a priori* du bit c_ℓ. On la note désormais $\pi(c_\ell)$. Si une information *a priori* est disponible pour chaque bit codé en entrée du codeur, l'APP du bit codé c_j se met sous la forme

$$\mathrm{APP}(c_j) \propto \underbrace{p(x_j/c_j)}_{\text{observation}} \times \underbrace{\pi(c_j)}_{\text{probabilité } a\ priori} \times \underbrace{\sum_{\mathbf{c}\in C/c_j} \prod_{\substack{\ell=1\\ \ell\neq j}}^{N} p(x_\ell/c_\ell)\pi(c_\ell)}_{\text{information extrinsèque}} \tag{3.3}$$

L'information extrinsèque est notée $\mathrm{Ext}(c_j)$. A partir des observations et des probabilités *a priori*, le décodeur SISO est donc capable de fournir deux types d'information souple : les probabilités *a posteriori* $\mathrm{APP}(c_j)$ et les informations extrinsèques $\mathrm{Ext}(c_j)$.

Il existe ainsi plusieurs formes du décodeur SISO selon le nombres de probabilités *a priori* dont on dispose et le nombre d'APP ou informations extrinsèques que l'on calcule. Le schéma général d'un décodeur SISO est représenté figure 3.2.

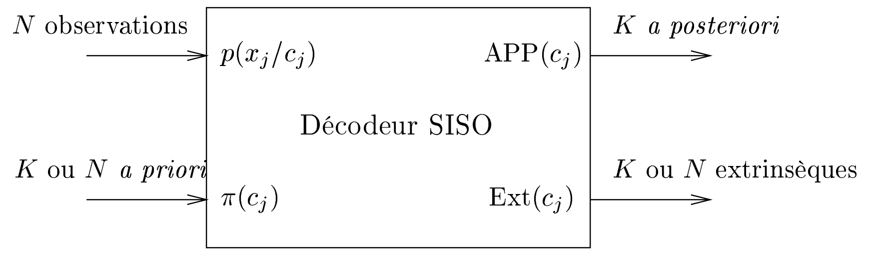


FIG. 3.2 – Décodeur SISO d'un code convolutif $C(N,K)$.

Citons deux exemples d'utilisation. Dans le cas d'un turbo code parallèle à deux niveaux, les K bits d'information sont communs aux deux codes constituants. Le décodeur SISO du premier code délivre K valeurs d'extrinsèques sur les bits d'information seulement. Le second décodeur SISO utilise ces K extrinsèques comme K probabilités *a priori* toujours sur les bits d'information.

Dans le cas d'un turbo code série utilisant un code externe NRNSC et un code interne, le décodeur SISO interne utilise K_2 probabilités *a priori* et délivre K_2 informations extrinsèques sur ses bits d'information, tandis que le décodeur SISO externe utilise N_1 probabilités *a priori* et délivre N_1 informations extrinsèques. En pratique, $N = N_1 = K_2 = N_\Pi$ où N_Π est la taille de l'entrelaceur.

3.2 Structure et performances des turbo codes

Les premiers codes concaténés ont été proposés par Forney en 1966 [32]. Il devenait possible de construire de longs codes en blocs par concaténation série de codes plus courts et plus simples. Depuis, de nombreux travaux ont été accomplis sur la concaténation parallèle [8][9][14] et la concaténation série [10][74]. Les turbo codes, introduits en 1993 par Berrou *et al.* [14], sont un exemple de codes concaténés. Après avoir surpris, ils ont soulevé de nombreuses questions dont certaines ne sont pas encore résolues, par exemple comment mieux comprendre et analyser leurs performances ? Existe-t-il un critère général de construction ?

Le schéma initialement proposé par Berrou *et al.* était formé de la concaténation parallèle de deux codes RSC séparés par un entrelaceur. Cependant, comme pour les autres codages concaténés, il existe deux types de turbo code : les turbo codes parallèle – concaténation parallèle de deux ou plusieurs codes convolutifs séparés par des entrelaceurs – et les turbo codes série – concaténation série de deux codes convolutifs toujours séparés par un entrelaceur. Nous nous limitons au cas simple de deux codes concaténés, aussi bien pour le schéma parallèle que pour le schéma série.

Un turbo code est un code en blocs linéaire binaire. On note R son rendement global et $R_i = \frac{k_i}{n_i}$, $i = 1, 2$ les rendements des codes convolutifs constituants. Dans tous les cas, N_Π est la taille de l'entrelaceur. Ce dernier peut être par exemple pseudo-aléatoire. Il a une influence importante sur les performances globales du turbo code, c'est pourquoi de nombreuses études visant à optimiser le choix de l'entrelaceur ont été menées. On sait notamment que quand N_Π tend vers l'infini, les performances du turbo code se rapprochent de la capacité.

Les performances des différents schémas ont été étudiées en détail [8][9][10]. Les probabilités d'erreur par bit sont évaluées à partir des distribution de poids des codes. Nous ne rappelons ici que les résultats importants.

3.2.1 Les turbo codes parallèle

La structure d'un turbo code parallèle à deux niveaux est décrite figure 3.3. Ce turbo code est un code linéaire binaire de dimension N_Π. Les deux codes C_1 et C_2 peuvent être choisis identiques ou non, mais ce sont toujours des codes RSC. En effet, les turbo codes parallèle construits à partir de codes NRNSC sont beaucoup moins performants : seuls les codes RSC permettent d'avoir un gain d'entrelacement.

Π est la permutation opérée sur les bits d'information. Les N_Π bits d'information sont codés par le premier code C_1. Une version entrelacée par Π de ces mêmes bits est parallèlement codée par le code C_2. Chacun des deux codes RSC C_i délivre $\frac{n_i \times N_\Pi}{k_i}$ bits parmi lesquels les N_Π bits d'information (le code est systématique) et $(n_i - k_i) \times N_\Pi / k_i$ bits codés. Les deux versions des bits d'information ne diffèrent que d'une permutation connue. On pourra choisir de ne transmettre que l'une des deux pour augmenter le rendement global du turbo code.

Le rendement total R peut être exprimé en fonction des rendements R_i des codes constituants. On note $T_i = \lceil \frac{L_i - k_i}{k_i} \rceil$ le nombre de transitions nécessaires à la fermeture du treillis pour le code

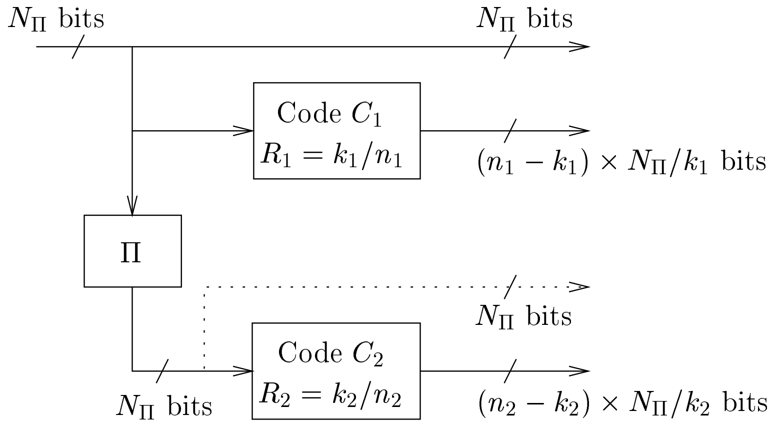


FIG. 3.3 – Structure d'un turbo code parallèle à deux niveaux.

RSC C_i où L_i est sa longueur de contrainte. Alors, en tenant compte de la fermeture du treillis, R est donné par l'expression

$$R = \frac{R_1 R_2}{R_1 + R_2 - R_1 R_2 + \frac{n_1 T_1 + n_2 T_2}{N_\Pi}} \tag{3.4}$$

Lorsque l'on néglige la fermeture du treillis, l'équation (3.4) devient

$$R = \frac{R_1 R_2}{R_1 + R_2 - R_1 R_2}$$

Et si les deux codes constituants ont même rendement $R_1 = R_2$, $R = \frac{R_1}{2-R_1}$. Les turbo codes parallèle les plus fréquemment employés sont les turbo codes de rendement $R = 1/3$ avec $R_1 = R_2 = 1/2$, $R = 1/2$ avec $R_1 = R_2 = 1/2$ où la sortie est poinçonnée et $R = 1/2$ avec $R_1 = R_2 = 2/3$.

Nous donnons ici les performances du turbo code C de rendement $R = 1/3$, où $C_1 = C_2$ et $R_1 = R_2 = 1/2$. La terminaison des treillis est négligée et N_Π désigne toujours la taille de l'entrelaceur. Le polynôme énumérateur de poids du code C_1 est défini par

$$A^{C_1}(W,Z) = \sum_{w=w_{min}}^{N_\Pi} \sum_{z=z_{min}}^{N_\Pi} A^{C_1}_{w,z} W^w Z^z \tag{3.5}$$

où $A^{C_1}_{w,z}$ est le nombre de mots de code de C_1 de poids w sur les bits d'information et z sur les bits de parité. Le polynôme $A^{C_1}(W,Z)$ n'inclut pas le mot tout à zéro du code. Le treillis d'un code RSC commence et se termine à l'état zéro, par conséquent, le poids minimal en entrée est $w_{min} = 2$. Cependant, le poids minimal sur les bits de parité ne correspond pas forcément au poids minimal en entrée. On note $z^{(2)}_{min}$ le poids minimal de la parité associé aux événements d'erreur de poids 2 en entrée. Alors $z_{min} \leq z^{(2)}_{min}$. L'équation (3.5) se récrit

$$A^{C_1}(W,Z) = \sum_{w=w_{min}}^{N_\Pi} W^w A^{C_1}(w,Z) \quad \text{avec} \quad A^{C_1}(w,Z) = \sum_{z=z_{min}}^{N_\Pi} Z^z A^{C_1}_{w,z}$$

$A^{C_1}(w,Z)$ est le polynôme énumérateur de poids conditionnel, puisque le poids w de l'entrée est fixé.

L'entrelaceur choisi est aléatoire. Ainsi, les entrées des deux codeurs sont de même poids tout en étant indépendantes. On montre alors facilement que la distribution de poids conditionnelle pour un poids w en entrée du turbo code C, calculée en moyennant sur tous les entrelaceurs, vérifie [29]

$$A^C(w,Z) = \frac{\left[A^{C_1}(w,Z)\right]^2}{C^w_{N_\Pi}}$$

Sous l'hypothèse d'un décodage à maximum de vraisemblance, une simple application de la borne de l'union fournit une borne supérieure de la probabilité d'erreur par bit

$$P_{eb} \overset{\sim}{\leq} \frac{1}{2} \sum_{w=w_{min}}^{N_\Pi} \frac{w}{N_\Pi} W^w A^C(w,Z) \quad \text{avec} \quad W = Z = e^{-R\frac{E_b}{N_0}}$$

Cette borne diverge pour de faibles valeurs du rapport signal-à-bruit $\frac{E_b}{N_0}$. Grâce à une décomposition des mots de code en événements d'erreur simples, il est possible de trouver une nouvelle borne de la probabilité d'erreur par bit pour un turbo code parallèle construit à partir de deux codes RSC [9]

$$P_{eb} \overset{\sim}{\leq} \frac{1}{2} \sum_{\substack{i=1 \\ i\,pair}}^{N_\Pi} \frac{i}{N_\Pi} \frac{\left(H^{2+2z^{(2)}_{min}}\right)^{\frac{i}{2}}}{\left(1 - H^{z^{(2)}_{min}-2}\right)^i} \quad \text{avec} \quad H = e^{-R\frac{E_b}{N_0}} \tag{3.6}$$

L'observation de (3.6) nous permet de constater que les turbo codes construits à partir de codes RSC présentent un gain d'entrelacement : la probabilité d'erreur par bit décroît en $1/N_\Pi$. Ce n'est pas le cas si les codes constituants sont NRNSC. Par ailleurs, à fort rapport signal-à-bruit, les performances à maximum de vraisemblance d'un code sont conditionnées par sa distance minimale. Asymptotiquement en N_Π, la distance minimale du turbo code, appelée distance effective, est donnée par

$$d_{eff} = 2 + 2z^{(2)}_{min}$$

Pour une taille fixe de l'entrelaceur, on pourra par conséquent améliorer les performances du turbo code si d_{eff} et donc $z^{(2)}_{min}$ sont maximisés.

3.2.2 Les turbo codes série

La structure d'un turbo code série est présentée figure 3.4. Dans ce cas le turbo code est un code en blocs linéaire (J,K). Le code C_1 est appelé code externe et le code C_2 code interne. C_1 peut être choisi indifféremment RSC ou NRNSC. Notons que l'avantage du NRNSC est d'augmenter la distance minimale du turbo code. En revanche, pour les mêmes raisons que dans le cas parallèle, le code interne est toujours RSC.

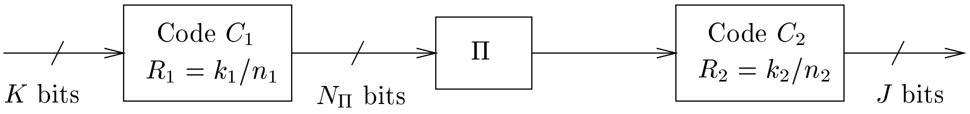


FIG. 3.4 – Structure d'un turbo code série.

Les K bits d'information sont codés par C_1 qui délivre N_Π bits. Ceux-ci sont entrelacés par la permutation Π de taille N_Π. Le code C_2 étant RSC, les J bits codés qu'il délivre contiennent une version permutée des N_Π bits fournis par C_1.

Ici encore, on peut exprimer le rendement R du turbo code en fonction des rendements des constituants. En tenant compte de la fermeture du treillis, on a

$$R = \frac{R_1 R_2}{1 + (n_1 T_1 + n_2 T_2)\frac{R_1 R_2}{K}} \tag{3.7}$$

Si on la néglige, (3.7) devient

$$R = R_1 \times R_2$$

Le turbo code série le plus fréquemment utilisé est de rendement $R = 1/2$ avec $R_1 = 2/3$ et $R_2 = 3/4$. On remarque que pour le même rendement global R, la concaténation série nécessite bien souvent l'usage de codes constituants de rendement et de complexité plus grands que la concaténation parallèle. Cependant, des codes constituants de rendement $R_i = 1/2$ poinçonnés peuvent être envisagés et dans ce cas, la complexité est comparable.

Nous rappelons ici ses performances. Le code externe C_1 est transformé en un code en blocs linéaire binaire (N_Π, K) de rendement $R_1 = k_1/n_1$ et de distance minimale $d_{min} = d_1$; tandis que le code interne C_2 est un code en blocs linéaire binaire (J, N_Π) de rendement $R_2 = k_2/n_2$ et de distance minimale $d_{min} = d_2$. On note C le turbo code série (J, K).

L'expression du polynôme énumérateur de poids du turbo code C s'obtient en faisant le produit de convolution normalisé des polynômes énumérateurs de poids des deux codes constituants

$$A^C(W,Z) = \sum_{\ell=d_1}^{N_\Pi} \frac{A^{C_1}(W,\ell) \times A^{C_2}(\ell,Z)}{C_{N_\Pi}^{\ell}} \tag{3.8}$$

La variable muette Z désigne ici le poids total en sortie du turbo code série C, et non plus seulement le poids de la parité.

De la même manière que précédemment, on décompose $A^C(W,Z)$ à partir du polynôme énumérateur de poids conditionnel $A^C(w,Z)$

$$A^C(W,Z) = \sum_{w=w_{min}}^{K} W^w A^C(w,Z) \quad \text{avec} \quad A^C(w,Z) = \sum_{z=z_{min}}^{J} Z^z A^C_{w,z}$$

Cette nouvelle expression nous permet de trouver une borne supérieure sur la probabilité d'erreur par bit

$$P_{eb} \lesssim \frac{1}{2} \sum_{w=w_{min}}^{K} \frac{w}{K} W^w A^C(w,Z) \quad \text{avec} \quad W = Z = e^{-R\frac{E_b}{N_0}} \tag{3.9}$$

L'étude des performances à partir de la décomposition des mots de code en événements d'erreurs simples conduit à deux résultats importants

- Le turbo code série bénéficie d'un gain d'entrelacement en $1/N_{\Pi}{}^{(d_1+1)/2}$ si et seulement si le code interne C_2 est récursif et systématique. Alors on choisit le code externe C_1 non récursif et non systématique de manière à augmenter d_1, ce qui favorise le gain d'entrelacement.
- La distance minimale ou distance effective du turbo code série est donnée par $d_{eff} = \frac{d_1 d_2}{2}$ si d_1 est paire et $d_{eff} = \frac{(d_1-3)d_2}{2} + z^{(3)}_{C_2,min}$ si d_1 est impaire. $z^{(3)}_{C_2,min}$ désigne le poids minimal de la sortie du code interne C_2 pour un poids 3 dans l'entrelaceur.

Le gain d'entrelacement et la distance minimale du turbo code série sont par conséquent plus grands que ceux du turbo code parallèle. C'est pourquoi les turbo codes série obtiennent de meilleures performances que les turbo codes parallèle mais au prix d'une complexité plus forte, du fait notamment de la taille plus importante des treillis.

3.3 Codage forte latence pour les signaux corrélés

Les différents systèmes présentés ont deux caractéristiques principales. Avant tout, comme nous l'avons déjà précisé, ce sont des alphabets FSK multidimensionnels construits à partir de techniques de codage forte latence. Par ailleurs, la concaténation d'un code, d'un entrelaceur et d'une modulation, c'est-à-dire la composition exacte de nos alphabets, est parfaitement équivalente à une modulation codée avec entrelacement de bits. Bien que depuis l'apparition des modulations codées, il a souvent été considéré que la combinaison du codage et de la modulation est une bonne façon d'améliorer les performances d'un système de transmission, les BICM conduisent à d'excellents résultats. Les premiers travaux conseillant l'utilisation d'un entrelacement des bits sont présentés dans [80]. Il a de plus été montré dans [21] que les BICM permettent d'atteindre la capacité lorsque le canal de transmission est gaussien ou à évanouissements lents.

Le premier modèle que nous proposons met en œuvre un décodage APP simple, tandis que le second tire pleinement profit des propriétés de la BICM grâce à l'association d'une détection itérative avec retour d'informations souples et d'un décodage APP. Ce dernier système, adapté au non cohérent à partir de [46] est à comparer aux travaux de Li & Ritcey [47][49] qui proposent une méthode de décodage itératif avec retour d'informations dures d'une 8-PSK combiné à un étiquetage spécifique de la modulation. Nous étudions plus en détails cette question de l'étiquetage dans le dernier paragraphe de cette partie.

3.3.1 Modèle du système avec décodage APP simple

Les notations définies au chapitre 1 restent valables : Δf_0, T et $2E$ désignent respectivement l'espacement fréquentiel, le temps symbole de la modulation Q-FSK et l'énergie en bande de base des signaux de la Q-FSK. La figure 3.5 illustre le modèle de transmission d'un alphabet multidimensionnel FSK codé issu de l'association d'un code à forte latence et d'une modulation FSK corrélée.

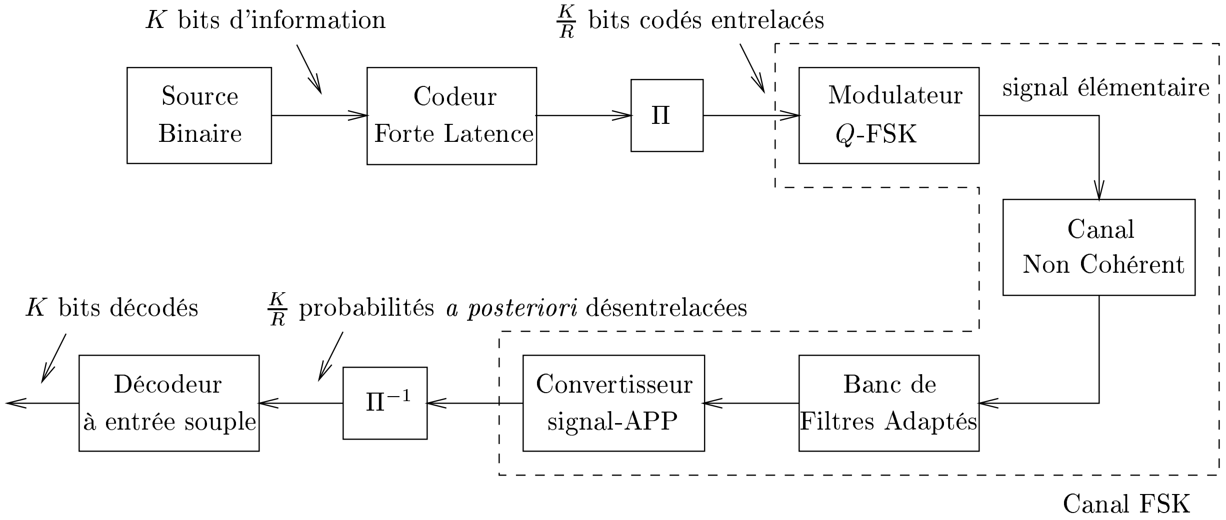


FIG. 3.5 – Alphabet FSK multidimensionnel codé, décodage APP simple.

Chaque bloc de K bits d'information, $b_1, \ldots, b_K$, est codé par un schéma de codage forte latence de rendement R et entrelacé par la permutation Π aléatoire. Les $\frac{K}{R}$ bits codés et entrelacés sont utilisés pour étiqueter N composantes entières p_n, $n = 1, \ldots, N$. Chaque p_n, élément de l'alphabet $\{\pm 1, \pm 3, \ldots, \pm(Q-1)\}$ est un symbole d'une modulation d'amplitude en phase de taille Q. Les grandeurs R, K, N et Q vérifient la relation $K = R \times N \times \log_2(Q)$. Le schéma de codage utilisé est un code convolutif ou un turbo code parallèle.

On note m_n un entier choisi dans l'ensemble $\{0, \ldots, Q-1\}$. Il y a équivalence parfaite entre les composantes p_n et les entiers m_n ; en effet,

$$m_n = \frac{p_n - (Q-1)}{2}$$

Chaque m_n modélise le choix d'une fréquence parmi les Q possibles. Ainsi, dans l'intervalle de temps $[(n-1)T, nT[$, la composante p_n est associée – par l'intermédiaire du modulateur Q-FSK – à l'émission physique du signal élémentaire $s_n(t) = s_{m_n}(t)$ issu d'une modulation Q-FSK et déjà défini au paragraphe 1.1.1

$$s_n(t) = \sqrt{\frac{2E}{T}} e^{2j\pi f_n t} \quad 0 \leq t < T \text{ et } 1 \leq n \leq N$$

ou encore $s_n(t) \in \{s_0(t), \ldots, s_{Q-1}(t)\}$. Par construction, la fréquence élémentaire f_n prend Q valeurs possibles uniformément séparées de Δf_0. Elle est en effet proportionnelle à p_n ou m_n

$$f_n = p_n \times \frac{\Delta f_0}{2} = m_n \times \Delta f_0$$

Contrairement au précédent chapitre, les signaux élémentaires ne sont pas regroupés et traités par blocs de N : $s_n(t)$ est simplement émis dans l'intervalle de temps $[(n-1)T, nT[$. Ainsi, le caractère multidimensionnel de l'alphabet FSK provient de la taille de la fenêtre d'observation en sortie du canal et non plus de la taille N du bloc de données. Bien qu'en théorie des entrelaceurs de taille très grande, voire infinie, existent, en pratique, il n'est pas envisageable de mettre en œuvre de tels systèmes. Pour un alphabet codé par un turbo code, on considérera par exemple un entrelaceur de taille $N = N_{\Pi} = 1024$.

Le canal est sans mémoire et la détection est non cohérente ; dans la suite, nous parlerons de canal non cohérent. Il est caractérisé par une atténuation α et une phase aléatoire ϕ_n inconnue du récepteur. Dans le cas du canal gaussien, α est une constante, nous choisirons simplement $\alpha = 1$. Dans le cas du canal à évanouissements, α suit une loi de Rayleigh ; $p(\alpha) = 2\alpha e^{-\alpha^2}$ et $E[\alpha^2] = 1$. Les phases ϕ_n sont des variables aléatoires uniformément distribuées, c'est-à-dire $p(\phi_n) = \frac{1}{2\pi}$. Le bruit complexe $b_n(t)$ est additif blanc gaussien de densité spectrale de puissance $2\sigma^2 = 2N_0$.

Dans l'intervalle de temps $[(n-1)T, nT[$, le signal $s_n(t)$ est émis. On reçoit

$$r_n(t) = \alpha e^{j\phi_n} s_n(t) + b_n(t) = \alpha e^{j\phi_n} s_{m_n}(t) + b_n(t)$$

Les signaux sont traités séquentiellement en sortie du canal. Le détecteur non cohérent optimal à maximum de vraisemblance pour les signaux monodimensionnels FSK se compose d'un banc de Q filtres adaptés aux Q fréquences possibles de la modulation FSK. Ce résultat est valable pour les deux types de canaux envisagés, à savoir le canal gaussien et le canal de Rayleigh ([57], Annexe 4.C). En pratique, le signal reçu $r_n(t)$ est filtré par les Q signaux FSK $s_q(t) = \sqrt{\frac{2E}{T}} e^{2j\pi f_q t}$, $q = 0, \ldots, Q-1$. En sortie du $q$ième filtre adapté, la corrélation est définie par

$$x_{q,n} = \int_0^T r_n(t) s_q^*(t) dt = \alpha e^{j\phi_n} \mu_n^{m_n,q} + b_{q,n}$$

où $\mu_n^{m_n,q} = \int_0^T s_{m_n}(t) s_q^*(t) dt$ est l'intercorrélation à l'instant n entre les signaux $s_{m_n}(t)$ et $s_q(t)$, déjà définie dans les précédents chapitres. $b_{q,n} = \int_0^T b_n(t) s_q^*(t) dt$ est le bruit filtré par le signal $s_q(t)$. C'est toujours un bruit gaussien complexe de moyenne nulle, sa densité spectrale de puissance devient $4E\sigma^2 = 4EN_0$. L'observation totale en sortie du banc de filtres est formée d'un unique vecteur $|x_n| = (|x_{0,n}|, \ldots, |x_{Q-1,n}|)$.

Le décodeur est un décodeur à entrée souple qui prend une décision bit à bit (il minimise la probabilité d'erreur par symbole au lieu de la probabilité d'erreur par mot), par opposition aux décodeurs utilisés dans le précédent chapitre qui opéraient sur des blocs de N symboles. Le décodage à entrée souple nécessite d'avoir des valeurs de fiabilité sur les bits codés ou les bits d'information, selon le schéma considéré. Chaque signal $s_n(t)$ émis sur le canal non cohérent est étiqueté par $\log_2(Q)$ bits codés que l'on note $c_{j,n}$, $j = 1, \ldots, \log_2(Q)$. $c_{j,n}$ est le $j$ième bit codé sur l'intervalle de temps $[(n-1)T, nT[$. Dans notre cas, il faut convertir les sorties du banc de filtres adaptés $|x_n|$ en $\log_2(Q)$ informations souples sur les bits codés correspondant.

Par définition, la probabilité *a posteriori* du bit $c_{j,n}$ s'écrit

$$\text{APP}(c_{j,n}) = p(c_{j,n}/|x_{0,n}|, \ldots, |x_{Q-1,n}|) \tag{3.10}$$

L'application directe de la loi de Bayes permet de récrire (3.10)

$$\text{APP}(c_{j,n}) = \frac{p(|x_n|/c_{j,n}) P(c_{j,n})}{p(|x_n|)}$$

Si aucune information *a priori* sur les bits codés n'est disponible, l'observation $p(|x_n|/c_{j,n})$ délivrée par le canal est proportionnelle à la probabilité *a posteriori* $\mathrm{APP}(c_{j,n})$

$$\mathrm{APP}(c_{j,n}) \propto p(|x_{0,n}|, \ldots, |x_{Q-1,n}|/c_{j,n})$$

Dans la suite, nous ne distinguons pas ces deux grandeurs. L'opération qui consiste à évaluer les $\log_2(Q)$ informations souples sur les bits codés est effectuée par le bloc "Convertisseur signal-APP". Ces APP seront utilisées comme observations par le décodeur à entrée souple.

L'observation pour le bit $c_{j,n}$ s'écrit

$$p(|x_n|/c_{j,n}) = \sum_{q=0}^{Q-1} p(|x_n|/q, c_{j,n}) p(q/c_{j,n}) \tag{3.11}$$

où $p(q/c_{j,n})$=1 si le $j$ième bit qui étiquète le signal $s_q(t)$ est égal à $c_{j,n}$, 0 sinon.

Alors,

$$\mathrm{APP}(c_{j,n}) \propto \sum_{q/c_{j,n}} p(|x_n|/q) \propto \sum_{q/c_{j,n}} \mathrm{APP}(q,n) \tag{3.12}$$

Après normalisation des APP et puisque tous les signaux de la modulation sont équiprobables, on a $\mathrm{APP}(c_{j,n}) = \sum_{q/c_{j,n}} \mathrm{APP}(q,n)$.

Une première étape consiste à évaluer les probabilités *a posteriori* $\mathrm{APP}(q,n)$ des Q fréquences possibles, ou de manière parfaitement équivalente, des Q signaux $s_q(t)$ de la modulation dans l'intervalle $[(n-1)T, nT[$. Ces Q valeurs ont déjà été définies (paragraphe 2.1.3, équation (2.5)). Trois calculs ont été détaillés selon le type de canal envisagé. Nous ne rappelons ici que les expressions obtenues

- canal gaussien

$$\mathrm{APP}(q,n) = \frac{I_0\left(\frac{|x_{q,n}|}{2E\sigma^2}\right)}{\sum_{\chi=0}^{Q-1} I_0\left(\frac{|x_{\chi,n}|}{2E\sigma^2}\right)}$$

- canal de Rayleigh à évanouissements lents

$$\mathrm{APP}(q,n) = \frac{I_0\left(\frac{\alpha|x_{q,n}|}{2E\sigma^2}\right)}{\sum_{\chi=0}^{Q-1} I_0\left(\frac{\alpha|x_{\chi,n}|}{2E\sigma^2}\right)}$$

- canal de Rayleigh à évanouissements rapides

$$\mathrm{APP}(q,n) = \frac{\exp\left(\frac{|x_{q,n}|^2}{8E^2\sigma^2}\right)}{\sum_{\chi=0}^{Q-1} \exp\left(\frac{|x_{\chi,n}|^2}{8E^2\sigma^2}\right)}$$

Dans un second temps, le bloc "Convertisseur signal-APP" délivre un ensemble de $\log_2(Q)$ probabilités *a posteriori* $\mathrm{APP}(c_{j,n})$ pour chaque intervalle de temps $[nT, (n+1)T[$.

La concaténation des opérations de modulation/démodulation de la Q-FSK et du canal non cohérent forme un nouveau canal à entrée binaire et à sortie souple. La décision bit à bit prise par le décodeur de la figure 3.5 est basée sur l'ensemble des probabilités *a posteriori* sur les bits codés fournies par le canal à entrée binaire et sortie souple aussi appelé canal FSK. Comme prévu, ces APP sont considérées comme des observations à l'entrée du décodeur. Son rôle est alors de calculer de nouvelles valeurs *a posteriori* en utilisant l'information provenant du canal FSK, mais aussi les contraintes du code, pour prendre une décision finale.

Dans la suite, deux cas particuliers sont traités. Le codage de la FSK par un turbo code parallèle conduit à l'utilisation d'un décodage itératif basé sur la mise en cascade des deux décodeurs SISO des codes constituants. En revanche, lorsque seul un code convolutif est utilisé, on se contente d'un simple décodeur SISO, tel que celui décrit au paragraphe 3.1.

3.3.2 Modèle du système avec détection itérative et décodage APP

L'utilisation des itérations, dans un processus de détection ou de décodage, permet de propager des informations souples grâce auxquelles le système sous-jacent affine ses décisions. Pour cela, les entrées et les sorties des entités impliquées doivent être souples.

Par exemple, dans le cas du turbo code, chaque décodeur SISO délivre deux types d'informations souples en sortie : les probabilités *a posteriori* et les informations extrinsèques. Celles-ci sont alors utilisées comme nouvelles probabilités *a priori* par le décodeur suivant, et ainsi de suite. C'est ce qui permet au décodage itératif de converger. Les détails concernant le fonctionnement de ce décodeur sont donnés dans la section suivante.

Nous nous intéressons ici au modèle de transmission illustré figure 3.6.

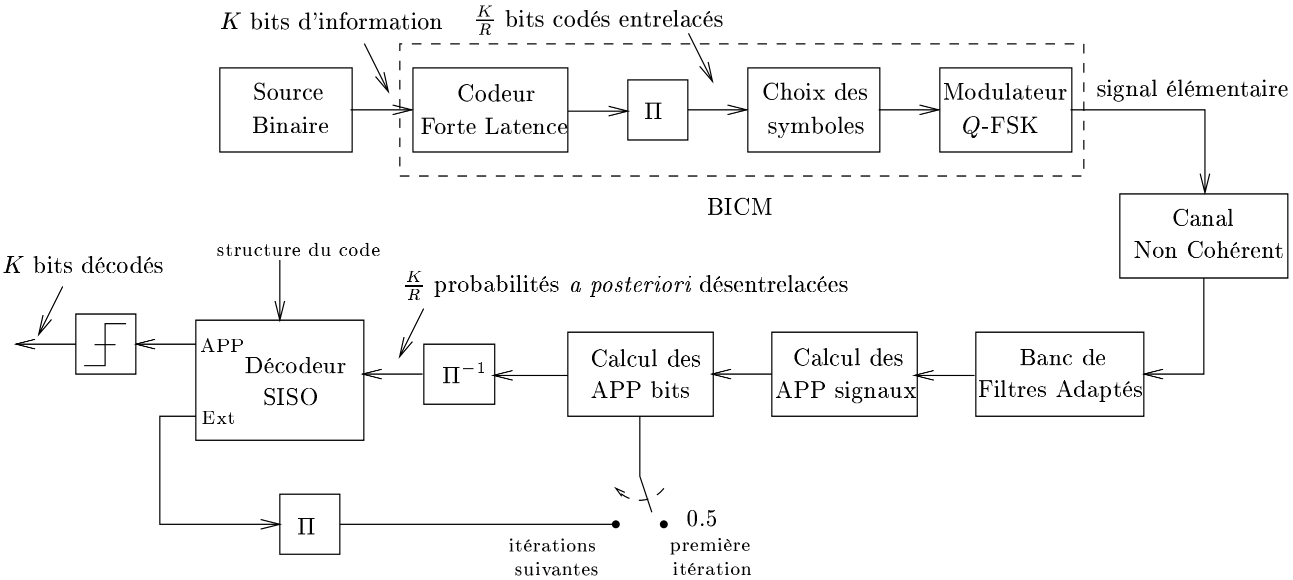


Fig. 3.6 – Alphabet FSK multidimensionnel codé, détection itérative et décodage APP.

La concaténation du codeur forte latence – en pratique, nous nous limitons à un codeur convolutif –, de l'entrelaceur Π, du choix des symboles et de la modulation Q-FSK est équivalente à une BICM. La détection itérative avec retour d'informations souples associée au décodage APP simple permet justement de tirer pleinement profit de ses propriétés. Ce schéma est similaire à celui de la figure 3.5, tout en étant plus général. En effet, si les $\frac{K}{R}$ bits codés étiquètent des symboles d'une modulation PAM-Q, l'émetteur est en tout point identique à celui de la figure 3.5. En revanche, les symboles à émettre peuvent être choisis dans un alphabet multidimensionnel, tel que celui présenté au paragraphe 1.2.4. Les modifications apportées à l'émetteur sont les suivantes

1. Les $\frac{K}{R}$ bits codés permettent de choisir $\frac{N}{N_S}$ symboles de dimension N_S, chacun parmi M, dans un alphabet multidimensionnel $\{S_1, \ldots, S_m\}$.
2. Chaque symbole possible S_m est de dimension N_S où chacune des N_S composantes est issue d'une modulation Q-FSK et correspond au choix de la fréquence m_n, $m_n \in \{0, \ldots, Q-1\}$.
3. Les N_S signaux Q-FSK élémentaires sont émis sur le canal non cohérent sur N_S intervalles de temps $[(n-1)T, nT[$.

On peut toujours lier les principales grandeurs, à savoir le nombre de bits d'information K, le rendement du code R, le nombre de signaux élémentaires traités N, la taille de la modulation FSK sous-jacente Q, la taille M de l'alphabet des symboles S_m et leur dimension N_S. En effet

$$K = R \times \frac{N}{N_S} \times \log_2(M)$$

Si $N_S = 1$, $M = Q$ et on retrouve $K = R \times N \times \log_2(Q)$. A la réception, la différence de l'un quelconque de ces deux schémas par rapport au cas simple du paragraphe précédent réside dans la mise en œuvre du décodage. Les deux entités impliquées dans le processus itératif, à savoir le bloc “Calcul des APP bits” et le décodeur SISO disposent d'entrées et de sorties souples.

Pour conserver toute la généralité du raisonnement, on note c_j, $j = 1, \ldots, \log_2(M)$, les bits codés relatifs à l'émission du symbole S_m sur N_S intervalles de temps, soit une durée totale $N_S \times T$. On remarquera que si l'alphabet de symboles est une PAM-Q, on retrouve la notation des $\log_2(Q)$ bits codés $c_{j,n}$ pendant l'intervalle de temps $[(n-1)T, nT[$ de durée T puisque $N_S = 1$. Le même raisonnement que celui mené précédemment permet d'écrire

$$\mathrm{APP}(c_j) \propto p(|x_1|, \ldots, |x_{N_S}|/c_j) \times \pi(c_j)$$

où $\pi(c_j)$ désigne la probabilité *a priori* du bit c_j. Les N_S vecteurs $\{|x_1|, \ldots, |x_{N_S}|\}$ constituent l'observation, en sortie du banc de filtres adaptés sur un intervalle de durée $N_S \times T$, relative à tout le symbole S_m. On a toujours $|x_n| = (|x_{0,n}|, \ldots, |x_{Q-1,n}|)$.

La densité de probabilité conditionnelle $p(|x_1|, \ldots, |x_{N_S}|/c_j)$ peut être évaluée en marginalisant la densité de probabilité conjointe de tous les symboles de l'alphabet et de l'observation.

$$\begin{aligned}
p(|x_1|, \ldots, |x_{N_S}|/c_j) &= \sum_{m=1}^{M} p(|x_1|, \ldots, |x_{N_S}|, S_m/c_j) \\
p(|x_1|, \ldots, |x_{N_S}|/c_j) &= \sum_{m=1}^{M} p(|x_1|, \ldots, |x_{N_S}|/S_m, c_j) p(S_m/c_j)
\end{aligned}$$

Les $\log_2(M)$ bits codés associés au choix d'un symbole S_m proviennent de l'entrelaceur. Ils sont donc indépendants. Alors

$$p(|x_1|,\ldots,|x_{N_S}|/c_j) = \sum_{m=1}^{M}\left[p(|x_1|,\ldots,|x_{N_S}|/S_m,c_j) \times \prod_{\ell} p(c_\ell/c_j)\right]$$

De plus, on note $p(c_\ell/c_j) = \pi(c_\ell)$. Evidemment, $p(c_j/c_j) = \pi(c_j) = 1$ si le $j$ième bit qui étiquète le symbole S_m vaut c_j, et 0 sinon.

Finalement, après normalisation, et en notant $\mathrm{APP}(S_m) = p(S_m/|x_1|,\ldots,|x_{N_S}|)$,

$$p(|x_1|,\ldots,|x_{N_S}|/c_j) = \sum_{m/c_j}\left[\mathrm{APP}(S_m) \times \prod_{\ell\neq j} \pi(c_\ell)\right] \tag{3.13}$$

Puisque les N_S composantes de chaque symbole S_m sont parfaitement indépendantes

$$\mathrm{APP}(S_m) = p(m_1,\ldots,m_{N_S}/|x_1|,\ldots,|x_{N_S}|) = \prod_{n=1}^{N_S} p(m_n/|x_1|,\ldots,|x_{N_S}|)$$

Seule l'observation $|x_n|$ est pertinente pour la composante m_n. Alors,

$$\mathrm{APP}(S_m) = \prod_{n=1}^{N_S} \mathrm{APP}(m_n,n)$$

En effet, la composante m_n correspondant à l'émission physique d'un signal FSK $\sqrt{\frac{2E}{T}}e^{j2\pi m_n \Delta f_0 t}$, $p(m_n/|x_n|)$ n'est autre que la probabilité *a posteriori* $\mathrm{APP}(m_n,n)$ déjà définie dans les précédents paragraphes.

Les $\log_2(M)$ observations données par la relation (3.13), abusivement appelées APP dans le bloc “Calcul des APP bits”, sont exploitées par le décodeur SISO du code convolutif. Il délivre deux types d'information en sortie :

– $\frac{K}{R} \times \frac{N_S}{N}$ probabilités *a posteriori* sur les bits d'information, $\mathrm{APP}(b_i)$, grâce auxquelles on peut prendre une décision,
– $\log_2(M)$ informations extrinsèques utilisées comme nouvelles informations *a priori* $\{\pi(c_\ell)\}$ à l'itération suivante.

Les $\frac{K}{R} \times \frac{N_S}{N}$ bits b_i sont les bits d'information relatifs aux $\log_2(M)$ bits codés c_j pour une durée $N_S \times T$.

En résumé, le principe de la détection itérative associée au décodage APP est le suivant

- initialisation : initialiser les $\log_2(M)$ probabilités *a priori* $\pi(c_j)$ à $\frac{1}{2}$. Calculer les $Q \times N_S$ $\mathrm{APP}(m_n,n)$, et en déduire les $\log_2(M)$ observations $p(|x_1|,\ldots,|x_{N_S}|/c_j)$.
- à chaque itération :
  – calculer les $\log_2(M)$ observations $p(|x_1|,\ldots,|x_{N_S}|/c_j)$ à partir de l'équation (3.13). Les $Q \times N_S$ probabilités *a posteriori* $\mathrm{APP}(m_n,n)$ sont inchangées et chaque probabilité *a priori* $\pi(c_\ell)$ est prise égale à l'information extrinsèque $\mathrm{Ext}(c_\ell)$ fournie par le décodeur SISO à l'itération précédente.

– appliquer le décodeur SISO qui calcule $\log_2(M)$ nouvelles extrinsèques $\text{Ext}(c_\ell)$ et $\frac{K}{R} \times \frac{N_S}{N}$ nouvelles probabilités *a posteriori* sur les bits d'information $\text{APP}(b_i)$.

- étape finale : à la dernière itération, les APP sur les bits d'information sont traitées par un détecteur à seuil. Si $\text{APP}(b_i = 0) > \text{APP}(b_i = 1)$, $b_i = 0$, sinon, $b_i = 1$.

Ce schéma se révèle très performant en pratique. De plus, nous remarquerons que trois ou quatre itérations suffisent à faire converger le système vers ses meilleures performances. Ce phénomène peut être expliqué grâce à la méthode de la fonction de transfert [20].

3.3.3 Importance du choix de l'étiquetage

Le schéma de modulation codée avec entrelacement de bits initialement proposé par Zehavi [80] conduit à une amélioration significative des performances sur un canal à évanouissements : l'emploi d'un entrelaceur sur les bits plutôt que sur les symboles augmente l'ordre de diversité de la modulation. Cependant, la distance euclidienne minimale est réduite et le décodeur n'exploite pas pleinement les avantages apportés par cet entrelacement des bits. Les travaux de Li & Ritcey [47][49] ont montré que l'on peut s'affranchir de ces inconvénients en procédant à un décodage itératif avec retour d'informations dures. Dans ce cas, les performances dépendent fortement du choix de l'étiquetage. En effet, plus celui-ci permet de maximiser la distance euclidienne minimale de chaque sous-ensemble, plus les résultats de la BICM décodée itérativement sont bons.

La BICM est construite à partir d'une modulation de phase de taille 8. Chaque symbole est ainsi étiqueté par trois bits. Trois types d'étiquetage sont envisagés : l'étiquetage de Gray, l'étiquetage d'Ungerboeck et un étiquetage mixte. La figure 3.7 illustre, pour chaque étiquetage, les sous-ensembles correspondant à chacun des trois bits. Dans tous les cas, la distance euclidienne minimale est la même dans tous les sous-ensembles. En revanche, le nombre de voisins à la distance minimale diffère.

A la première itération, les performances sont d'autant meilleures que le nombre d'erreurs possibles pour chaque bit est réduit. Par ailleurs, pour ce type de modulation, on se trompe majoritairement pour des voisins situés à distance minimale. Observons l'étiquetage de Gray (figure 3.7(a)). Pour chacun des trois bits, il y a respectivement deux, deux et quatre possiblités de prendre une décision erronée, qui correspondent en fait aux nombre de points proches des frontières entre les régions $\{\text{Bit i} = 0\}$ et $\{\text{Bit i} = 1\}$. En procédant à la même observation pour les deux autres méthodes d'étiquetage, il est manifeste que pour ce critère, l'étiquetage de Gray est meilleur que l'étiquetage mixte, lui-même meilleur que l'étiquetage d'Ungerboeck.

C'est pourquoi, dans le cas du décodage classique d'une BICM (sans itération), l'étiquetage de Gray est toujours privilégié [21][80].

Au cours des itérations suivantes, les informations dures réinjectées transforment le canal 8-PSK en un canal binaire dans lequel la décision pour chacun des bits est maintenant prise entre deux points d'une BPSK. Ceci est illustré figure 3.8. Par exemple, si la première itération indique que le Bit 2 vaut 0 et que le Bit 3 vaut 1, le choix pour décoder le Bit 1 dans le cas d'un étiquetage de Gray se fait entre le symbole 001 et 101 (figure 3.8(a)). Pour optimiser les

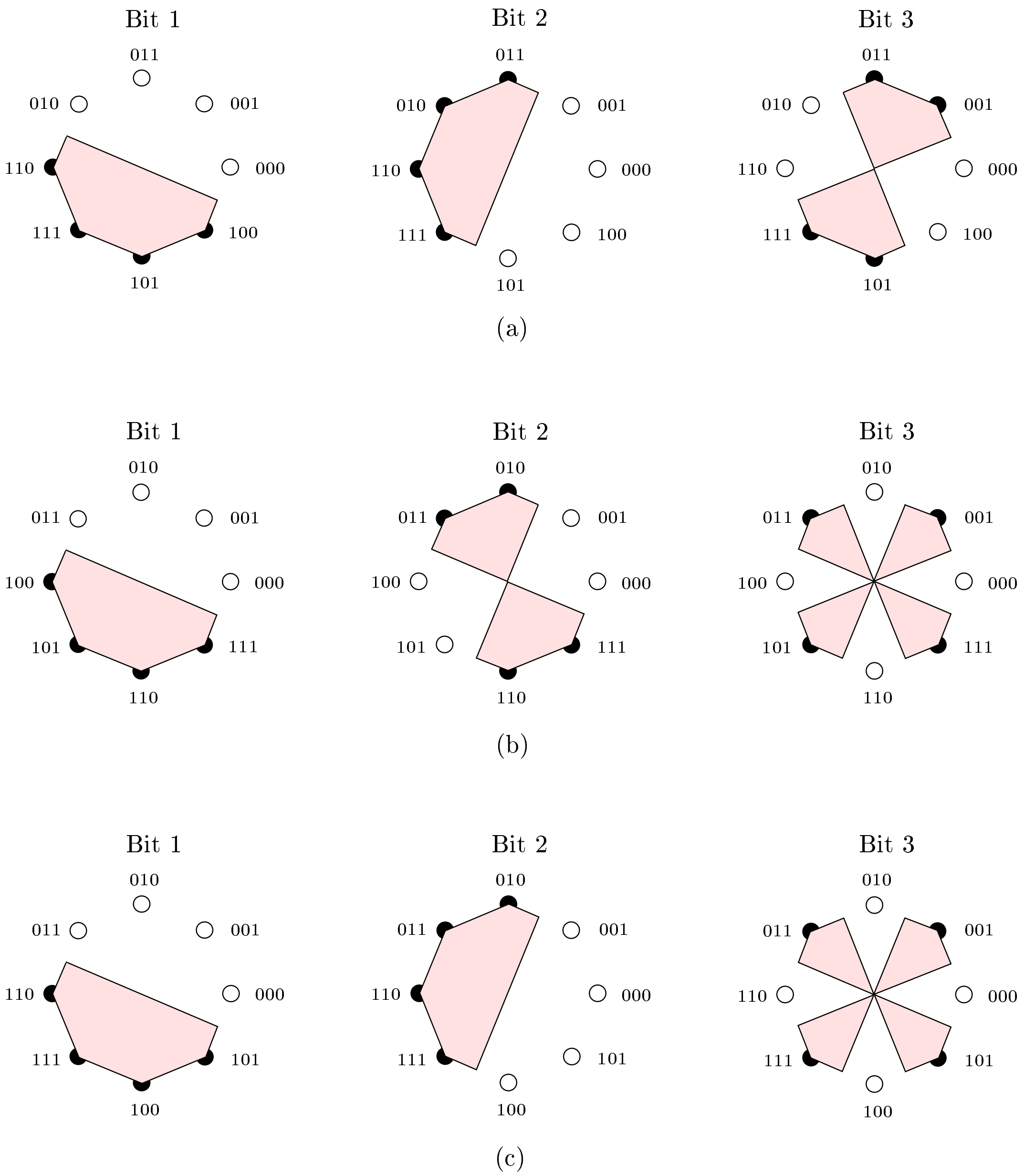


Fig. 3.7 – Représentation de trois types d'étiquetage et des régions de décision pour chacun des 3 bits de la 8-PSK. (a) Gray, (b) Ungerboeck, (c) mixte.

itérations suivantes, il s'agit cette fois de maximiser la distance euclidienne minimale de toutes les paires de signaux BPSK. L'étiquetage d'Ungerboeck répond au mieux à cette attente, suivi de l'étiquetage mixte et enfin de l'étiquetage de Gray.

Des erreurs sont toujours possibles lors du rebouclage des informations dures. C'est pourquoi les performances du décodage itératif dépendent à la fois de celles de l'étiquetage à la première itération et de la robustesse à la propagation d'erreurs de l'étiquetage choisi. L'étiquetage mixte se révèle être un bon compromis [47][49]. On remarquera cependant que cette méthode n'est optimale que pour une détection itérative avec retour d'informations dures.

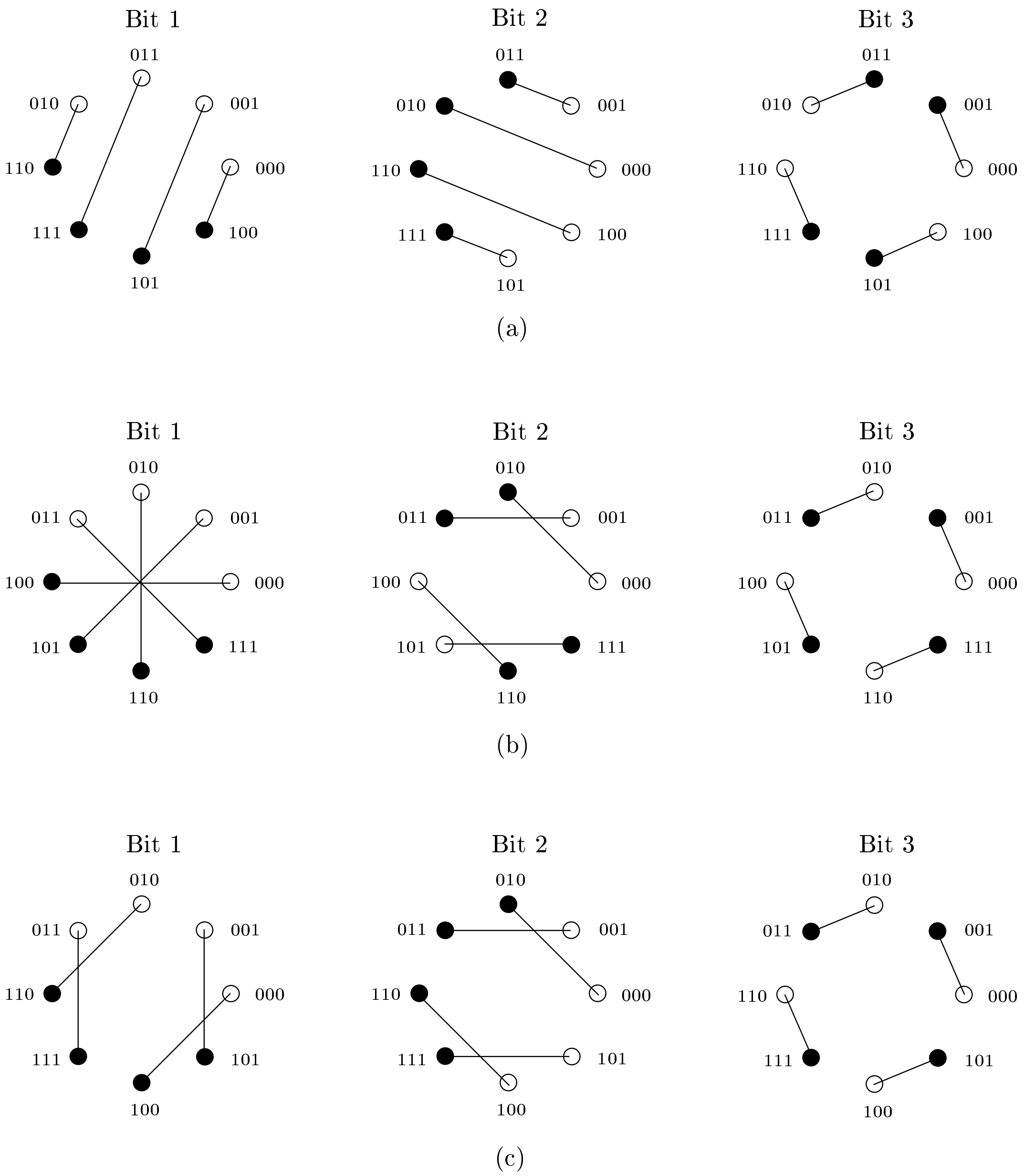


Fig. 3.8 – Equivalence entre la 8-PSK et les quatre constellations BPSK due au décodage itératif avec retour d'informations dures. (a) Etiquetage de Gray, (b) étiquetage d'Ungerboeck, (c) étiquetage mixte.

Revenons maintenant à notre schéma. La détection itérative associée au décodage APP constitue une technique de décodage itératif avec retour d'informations souples. Lors de la première itération, le raisonnement fait par Li & Ritcey reste le même, à savoir que l'étiquetage de Gray est optimal. En revanche, le rebouclage d'informations souples permet, à chaque nouvelle itération, d'être dans un contexte parfaitement similaire à celui de l'itération un. Ainsi, l'étiquetage de Gray reste optimal y compris pour les passes suivantes. Cette conclusion est également renforcée par le fait que l'étiquetage de Gray optimise la capacité. Par ailleurs, Li & Ritcey ont montré que si l'on utilise une technique de rebouclage souple plus élaborée qui minimise la propagation d'erreurs, alors l'étiquetage d'Ungerboeck est optimal [48].

Dans le contexte du schéma de modulation pour lequel nous présentons des résultats de simulation au paragraphe 3.5.2, nous avons observé des performances similaires pour les deux types d'étiquetage, Gray ou Ungerboeck, avec un très léger avantage à l'étiquetage d'Ungerboeck (de l'ordre de 0.1 dB à 10^{-4}). C'est pourquoi seules les courbes obtenues avec étiquetage de Gray seront présentées.

3.3.4 Choix de l'espacement fréquentiel et du rendement du code

Nous avons déjà pu observer au chapitre précédent que le choix de l'espacement fréquentiel de la modulation FSK sous-jacente aux alphabets multidimensionnels est important. En effet, dans le cas des réseaux de points par exemple, nous avons vu que si $\Delta f_0 = 1/T$, aucun gain n'est apporté par le codage du fait de l'effet de voisinage inexistant pour une modulation FSK orthogonale. Par ailleurs, les schémas de codage tels que la TCM de rendement 2/3 ou les réseaux de Gosset E_8 et de Leech Λ_{24} de rendements respectifs 2.5/3 et 2/3 se sont révélés très performants. Nous apportons ici une explication à ce phénomène.

La figure 3.9 nous montre que le choix de l'espacement fréquentiel de la FSK revêt une importance toute particulière.

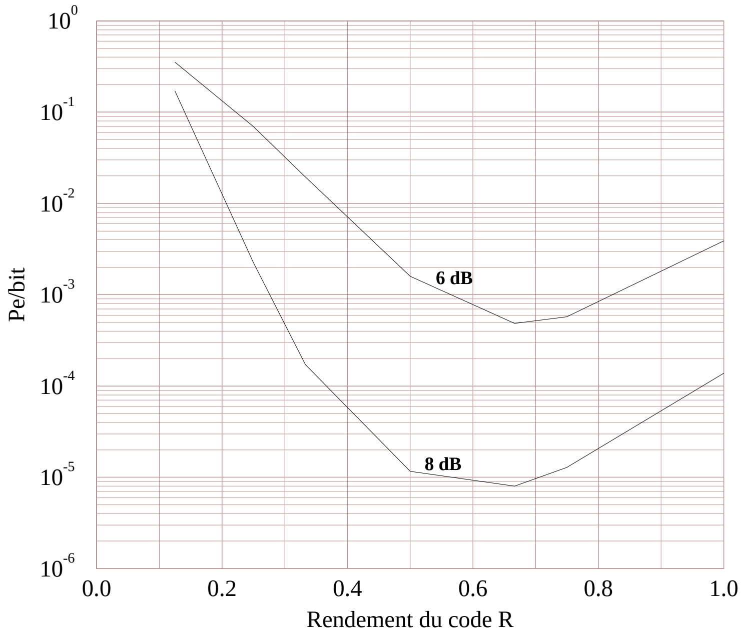


Fig. 3.9 – Probabilité d'erreur binaire en fonction du rendement du code R et $R = \Delta f_0 T$.

Sur cette figure, nous avons tracé la probabilité d'erreur binaire d'une modulation 8-FSK codée par un code convolutif en fonction du rendement R, et ceci pour deux valeurs du rapport signal-à-bruit, 6 et 8 dB. Les différents codes convolutifs considérés sont des codes convolutifs non récursifs non systématiques de complexité de décodage comparable. La table (3.1) résume leurs rendements R, leurs longueurs de contrainte L et leurs polynômes générateurs.

R	L	Polynômes générateurs
1/8	5	$(37, 33, 25, 25, 35, 33, 27, 37)$
1/4	5	$(25, 27, 33, 37)$
1/3	5	$(25, 33, 37)$
1/2	5	$(23, 35)$
2/3	3	$(27, 75, 72)$
3/4	2	$(13, 25, 61, 47)$

Tab. 3.1 – Codes NRNSC utilisés pour étudier l'influence de l'espacement fréquentiel.

Dans tous les cas, l'espacement fréquentiel de la modulation 8-FSK est choisi égal au rendement du code convolutif utilisé pour le codage, $R = \Delta f_0 T$. De cette façon, tous les systèmes codés ont même efficacité spectrale 0.375 bits/s/Hz. Le décodage est effectué à l'aide d'un décodeur SISO utilisant un algorithme aller-retour.

On observe sur la figure 3.9 que l'espacement fréquentiel ou de manière équivalente le rendement optimal, c'est-à-dire celui qui minimise la probabilité d'erreur binaire indépendamment du rapport signal-à-bruit, est $\Delta f_0 T = R = 2/3$. De chaque côté de cette valeur optimale, deux phénomènes se produisent. Lorsque $\Delta f_0 T = R$ se rapproche de 1, les signaux sont de moins en moins corrélés, mais les codes utilisés sont aussi de moins en moins bons, on tend donc vers les performances de la 8-FSK orthogonale non codée. Lorsque $\Delta f_0 T = R$ se rapproche de 0, le code utilisé est de plus en plus performant, mais la corrélation induite par la trop grande réduction de bande ne peut plus être compensée par le gain de codage, les performances se dégradent. Le $\Delta f_0 T = R$ optimal constitue un compromis tant au niveau de la puissance des codes utilisés que de la corrélation autorisée entre les signaux de la modulation 8-FSK.

Cette analyse justifie les bonnes performances obtenues par les schémas de codage présentés au chapitre 2. Dans tous les cas, le rendement du code est en effet proche de ou égal à 2/3. L'espacement fréquentiel a pu être choisi différent de R afin de comparer des systèmes de rendements différents à même efficacité spectrale ou à même bande. Les conclusions tirées de la figure 3.9 restent cependant valables. Notons finalement que les probabilités d'erreur binaire peuvent être réduites en utilisant des schémas de codage plus complexes (par exemple des codes convolutifs de longueur de contrainte plus grande).

3.4 Signaux corrélés et turbo codes

Commençons par étudier les performances obtenues par un schéma associant les turbo codes à une modulation Q-FSK corrélée. Les principaux résultats sur les turbo codes ont été rappelés au paragraphe 3.2. Comme de nombreux autres schémas de codage performants, leur décodage ML est irréalisable en pratique du fait de leur trop grande complexité. Une méthode de décodage itérative basée sur le décodage successif des differents codes constituants est donc envisagée. Cette technique appelée décodage itératif, non optimale au sens ML du terme, permet pourtant d'obtenir d'excellentes performances après un nombre raisonnable d'itérations. A fort rapport signal-à-bruit, les performances du décodage itératif tendent vers celles du décodage ML. Certains travaux se sont notamment intéressés à la rapidité de convergence des turbo codes [19].

Avant d'analyser les performances à proprement parler, nous décrivons brièvement le principe du décodage itératif appliqué à un turbo code parallèle.

3.4.1 Décodage itératif d'un turbo code parallèle

Nous nous restreignons au cas d'un turbo code parallèle construit à partir de deux codes convolutifs récursifs et systématiques. La structure du codeur ici considéré est illustrée figure 3.3. N_Π désigne la taille de l'entrelaceur. Les N_Π bits d'information sont codés par le code C_1 de rendement k_1/n_1 et une version permutée de ces mêmes bits est codée parallèlement par le code C_2 de rendement k_2/n_2.

Le principe du décodage itératif est illustré figure 3.10 : il s'agit de la mise en cascade de deux décodeurs SISO élémentaires tels que celui décrit au paragraphe 3.1. Bien que chacun d'eux soit optimal au sens du critère du maximum *a posteriori*, le décodage itératif ne l'est pas.

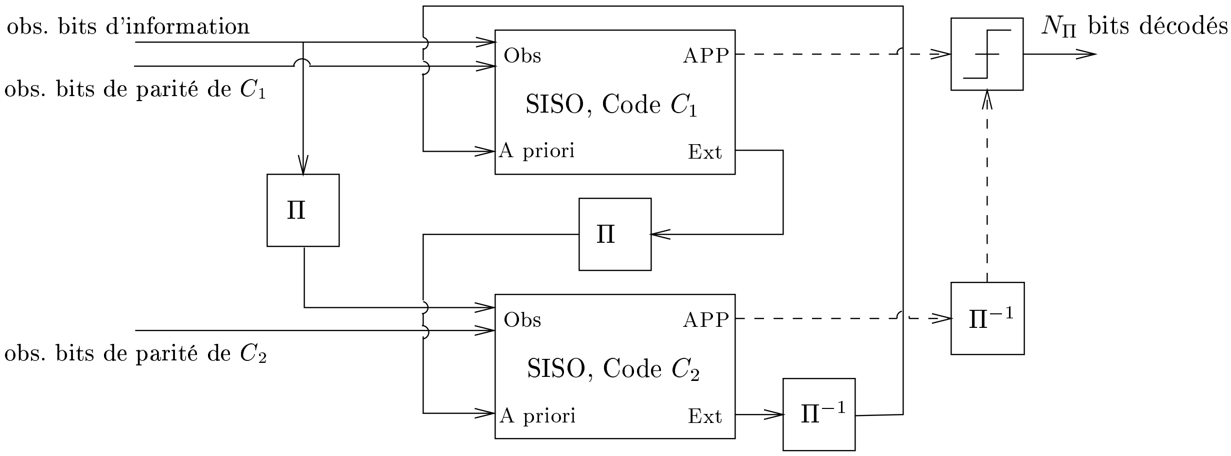


FIG. 3.10 – Décodage itératif d'un turbo code à partir des deux SISO des codes constituants.

Ainsi, chaque décodeur SISO élémentaire utilise

- N_Π observations communes aux deux décodeurs sur les bits d'information et $(n_i - k_i) \times N_\Pi/k_i$ observations relatives à ses bits de parité ; $i = 1, 2$ selon le décodeur concerné
- N_Π probabilités *a priori* sur les bits d'information

et délivre

- N_Π probabilités *a posteriori* sur les bits d'information
- N_Π valeurs d'extrinsèques sur les bits d'information

Dans la suite, SISO1 (resp. SISO2) désigne de décodeur SISO relatif au code C_1 (resp. C_2). Nous pouvons décrire précisément le déroulement du décodage itératif :

- initialisation : initialiser les N_Π probabilités *a priori* du premier décodeur à la valeur 1/2.
- itération 1

  - demie-itération SISO1 : le premier décodeur utilise les observations fournies par le canal pour calculer N_Π probabilités *a posteriori* et N_Π informations extrinsèques.
  - demie-itération SISO2 : le second décodeur utilise une version entrelacée des observations provenant du canal (les mêmes que pour le SISO1). Les N_Π informations extrinsèques délivrées par le SISO1 sont entrelacées et servent d'informations *a priori* au SISO2. Ce dernier délivre N_Π probabilités *a posteriori* et N_Π informations extrinsèques.

- itérations suivantes
  - demie-itération SISO1 : le premier décodeur utilise les N_Π informations extrinsèques obtenues à l'itération précédente désentrelacées comme de nouvelles probabilités *a priori* et procède à une nouvelle demie-itération de décodage.
  - demie-itération SISO2 : la demie-itération du second décodeur est la même, quelle que soit l'itération considérée.

- étape finale : effectuer une détection à seuil sur les probabilités *a posteriori* délivrées par le dernier SISO2 pour obtenir les bits d'information décodés.

Ainsi, chaque décodeur SISO correspond à une demie-itération et une itération complète est effectuée lorsque C_1 et C_2 ont été décodés. A chaque demie-itération, il est possible de prendre une décision sur les bits d'information ; on effectue pour cela une détection à seuil sur les probabilités *a posteriori* disponibles. L'évolution de ces probabilités *a posteriori* et des décisions qui en découlent peut être suivie au fur et à mesure des itérations. On peut notamment les utiliser pour mettre en œuvre un critère d'arrêt de la simulation.

3.4.2 Comportement des turbo codes face à la corrélation

Le système correspondant aux alphabets de signaux corrélés codés par un turbo code est décrit figure 3.5. Le décodage à entrée souple correspond à un décodage itératif d'un turbo code équivalent à celui du paragraphe 3.4.1. Tous les alphabets sont fondés sur une modulation 8-FSK. Le turbo code parallèle de rendement 1/3 utilisé est construit à partir de deux codes convolutifs récursifs et systématiques identiques de rendement 1/2 et de polynômes générateurs $(23, 35)$; l'entrelaceur est de taille 1024. Les turbo codes de rendement 1/2 et 2/3 sont obtenus par perforation du turbo code initial de rendement 1/3. Dans tous les cas, le décodage itératif comporte 12 itérations et chaque décodage SISO utilise un algorithme de type BCJR.

La figure 3.11 illustre le gain apporté par l'emploi des turbo codes pour des systèmes de même bande. En effet, la 8-FSK non codée, ainsi que les deux modulations 8-FSK codées par des turbo codes de rendement respectif $R = 1/2$ et $R = 1/3$ sont orthogonales, $\Delta f_0 T = 1$. Une approximation de la bande de la modulation 8-FSK est toujours $8 \times \Delta f_0$. Les trois schémas de codage, 8-FSK non codée, 8-FSK codée par un turbo code 1/2 et 8-FSK codée par un turbo code 1/3, sont donc d'efficacité spectrale respective 0.375 bits/s/Hz, 0.1875 bits/s/Hz et 0.125 bits/s/Hz. Le turbo code 1/2 apporte un gain de 3.4 dB pour une probabilité d'erreur égale à 10^{-4}, tandis que le turbo code 1/3 permet de gagner 2.9 dB pour cette même probabilité d'erreur.

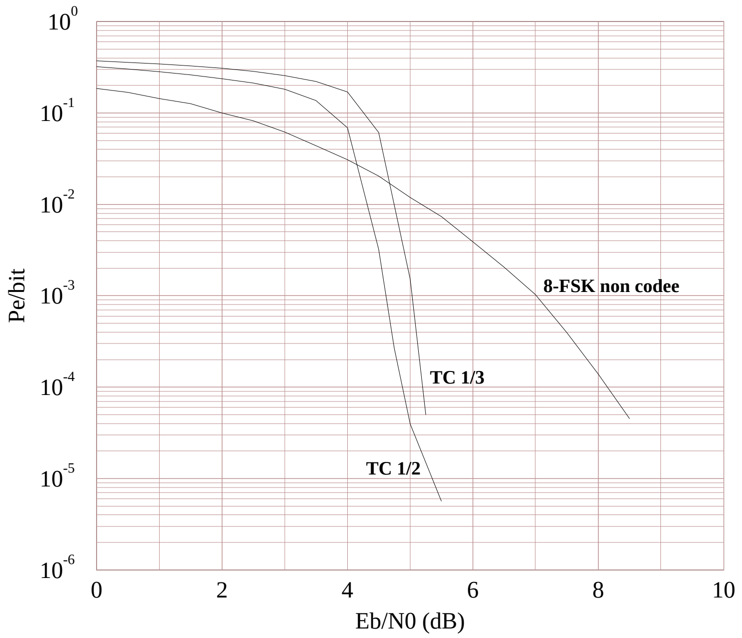
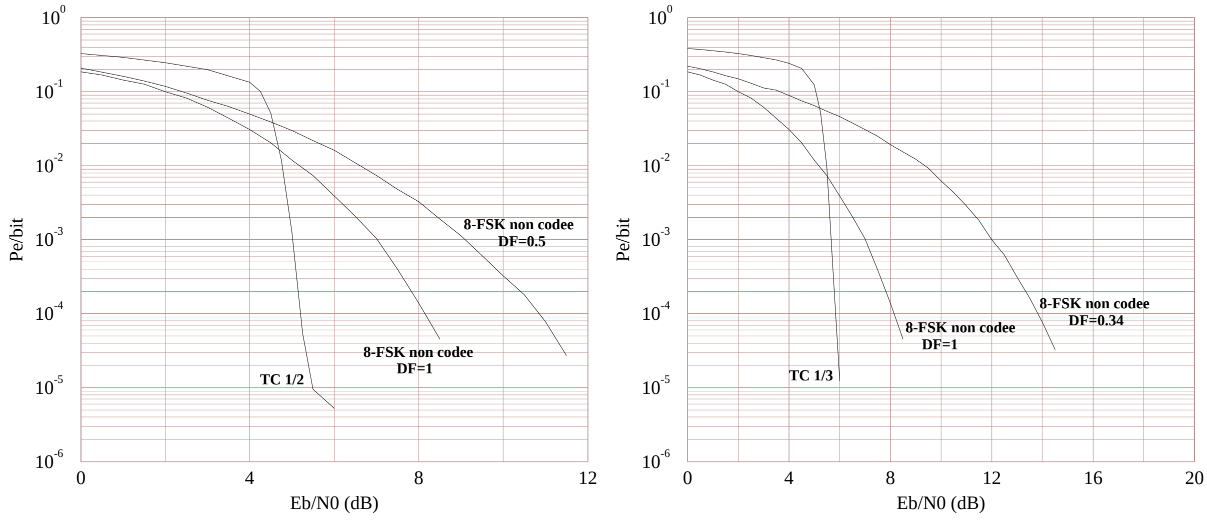


Fig. 3.11 – Modulation 8-FSK codée par un turbo code de rendement $1/2$ et $1/3$, *vs.* modulation 8-FSK non codée. La bande des systèmes est fixe, dans tous les cas $\Delta f_0 T = 1.0$.

Les résultats de simulations résumés figure 3.12 permettent de comparer les systèmes codés et non codés à même efficacité spectrale, soit 0.375 bits/s/Hz et à même bande. Le turbo code employé figure 3.12(a) est de rendement $1/2$, et $\Delta f_0 T = 0.5$. Sur la figure 3.12(b), il est de rendement $1/3$ et $\Delta f_0 T = 0.34$. La modulation 8-FSK orthogonale non codée a même efficacité spectrale que les schémas codés, tandis que les courbes de la 8-FSK non codée avec $\Delta f_0 T = R$, autorisent la comparaison à bande fixe. Dans les deux cas, le turbo code se comporte très bien face à la corrélation et permet de gagner 3 dB pour un taux d'erreur de 10^{-4} pour le rendement $1/2$ (resp. 2.5 dB pour le rendement $1/3$) tout en conservant l'efficacité spectrale de la FSK orthogonale. Lorsque l'on cherche simplement à mieux utiliser la même bande, le gain devient radicalement plus important : 5 dB pour une probabilité d'erreur égale à 3×10^{-3} pour le rendement $1/2$ et 8 dB pour une probabilité d'erreur égale à 10^{-4} pour le rendement $1/3$. En contrepartie, le prix à payer est la réduction de l'efficacité spectrale due au taux de codage.

Finalement, nous proposons de comparer les performances des alphabets codés à l'aide des turbo codes aux résultats obtenus avec les réseaux de points et les TCM. Le tout est rassemblé figure 3.13. Nous rappelons les performances de la 8-FSK non codée avec $\Delta f_0 T = 0.5, 0.34$ et les schémas codés, tous de même rendement $2/3$, sont fondés sur une 8-FSK corrélée, $\Delta f_0 T = 0.34$. Exceptée la 8-FSK non codée, $\Delta f_0 T = 0.34$, d'efficacité spectrale 1.125 bits/s/Hz, tous les alphabets ont même efficacité spectrale de 0.75 bits/s/Hz. Les alphabets multidimensionnels codés sont plus robustes à la corrélation que la modulation non codée. De plus, les très bons résultats des alphabets issus d'un codage faible latence sont encore améliorés par l'emploi des turbo codes : 1 dB d'écart entre le turbo code $2/3$ et la TCM $2/3$, 64 états pour un taux d'erreur de 2×10^{-5} et 3.8 dB entre le turbo code $2/3$ et le réseau de Leech pour un taux d'erreur de



(a) TC 1/2, $\Delta f_0 T = 0.5$ (b) TC 1/3, $\Delta f_0 T = 0.34$

Fig. 3.12 – Comparaison à 0.375 bits/s/Hz. 8-FSK non codée orthogonale et 8-FSK codée par un turbo code.

2×10^{-4}. L'inconvénient est la forte latence du turbo code ; la taille de l'entrelaceur ici égale à 1024 est à comparer aux 48 bits utiles au codage d'un point de Λ_{24} par exemple (cf. figure 2.14, chapitre 2).

3.5 Signaux corrélés et codage convolutif

Enfin, nous nous intéressons aux résultats obtenus par les alphabets FSK codés par un code convolutif. Dans un premier temps, la modulation sous-jacente est une simple FSK. Nous traitons ensuite le cas de l'alphabet multidimensionnel de longueur 4 déjà introduit au chapitre 1.

3.5.1 Q-FSK non orthogonale codée sur le canal gaussien

Le schéma de transmission correspond à la figure 3.5. Le décodeur à entrée souple est le décodeur SISO d'un code convolutif comme rappelé figure 3.14. Les blocs de $\log_2(Q)$ observations sur les bits codés fournis par le canal sont désentrelacés et utilisés par le décodeur SISO. On initialise les probabilités *a priori* à la valeur 1/2. Le SISO délivre alors les probabilités *a posteriori* sur les bits d'information correspondant et une décision est prise par détection à seuil. Les modulations FSK corrélées codées par un code convolutif sont particulièrement adaptées à ce type de décodage. En effet, un décodage ML de type Viterbi pourrait parfaitement être mis en place : chaque branche du treillis serait associée à un signal de la modulation 8-FSK. Une erreur

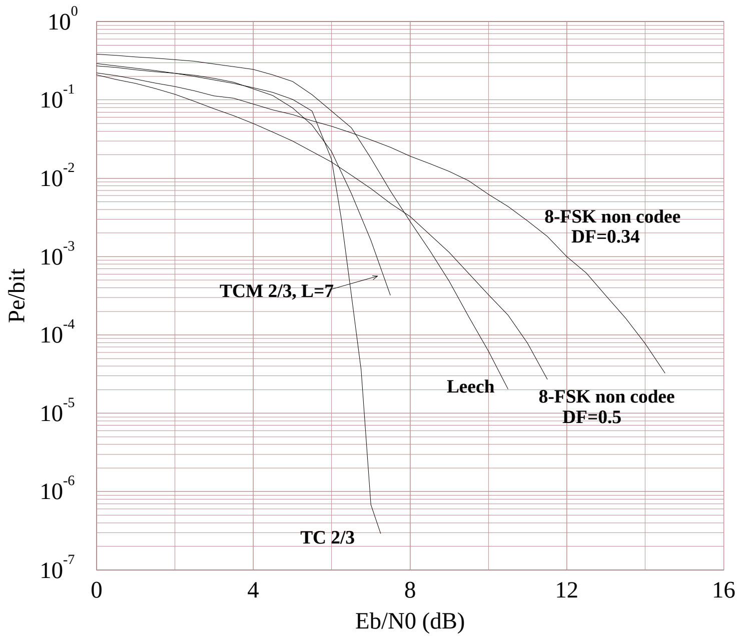


Fig. 3.13 – Comparaison des différents types de codage : 8-FSK non codée $\Delta f_0 T = 0.5, 0.34$ *vs.* 8-FSK codée par le réseau de Leech, par une TCM 2/3, 64 états et par un turbo code de rendement 2/3, $\Delta f_0 T = 0.34$.

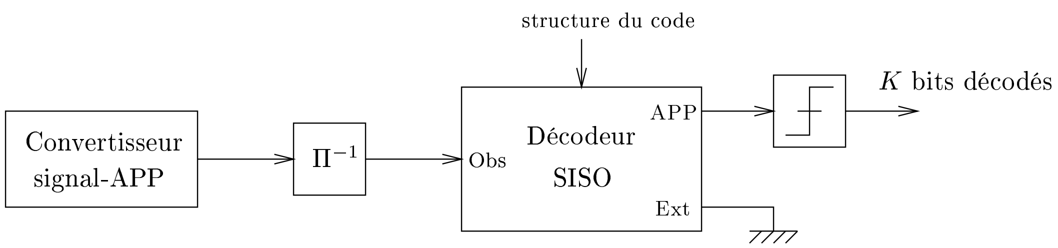


Fig. 3.14 – Décodage SISO d'un code convolutif.

sur la détection d'un signal conduit malheureusement à un groupe de trois erreurs sur les bits codés. Le décodage SISO mettant en œuvre le critère du maximum *a posteriori*, puisqu'il agit directement sur les bits, permet d'éviter les paquets d'erreurs. En effet, les APP des bits codés sont extraites des APP que l'on calcule pour les signaux. Ces dernières sont optimisées au sens du critère du maximum *a posteriori*. Nous avions déjà remarqué cette différence lors de l'analyse des résultats des alphabets multidimensionnels codés par une TCM.

Les caractéristiques (rendement R, longueur de contrainte L et polynômes générateurs) des différents codes NRNSC choisis pour les simulations sont rassemblées dans la table (3.2).

Nous comparons les performances de constellations FSK codées par un code convolutif et par une TCM. Les modulations codées en treillis choisies sont des modulations PAM-8 de rendement

R	L	Polynômes générateurs
1/3	5	$(25, 33, 37)$
1/3	7	$(133, 145, 175)$
1/3	9	$(557, 663, 711)$
2/3	3	$(27, 75, 72)$

Tab. 3.2 – Codes NRNSC utilisés pour le codage d'une modulation 8-FSK corrélée.

2/3 et de polynômes générateurs $(23, 04, 16)$ pour la TCM 2/3 à 16 états ($L = 5$) et $(101, 016, 064)$ pour la TCM 2/3 à 64 états ($L = 7$). Elles sont décodées par l'algorithme de Viterbi modifié proposé au paragraphe 2.1.2. Tous les alphabets d'une même figure occupent la même bande : $\Delta f_0 T = 0.5$ pour la figure 3.15 et $\Delta f_0 T = 0.34$ pour la figure 3.16. On observe sur la figure 3.15

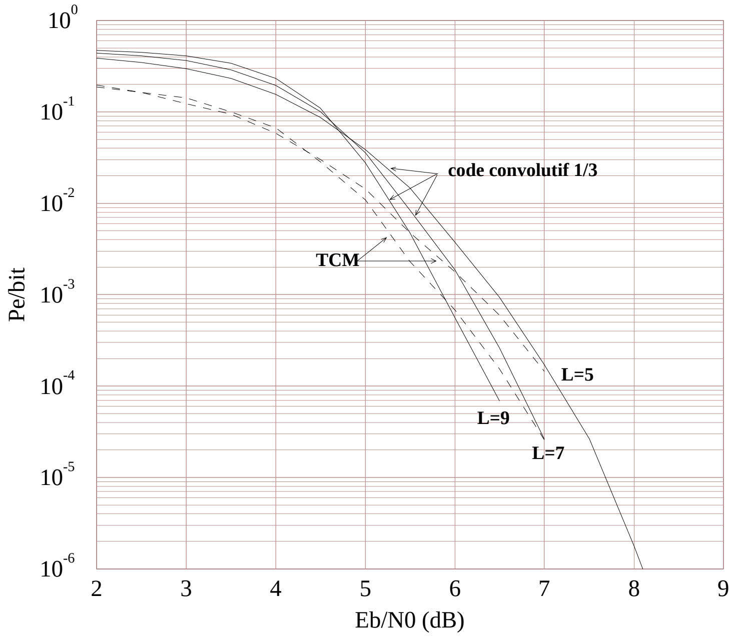


Fig. 3.15 – Modulation 8-FSK codée par un code convolutif 1/3, $L = 5, 7, 9$, *vs.* modulation 8-FSK codée par une TCM 2/3, $L = 5, 7$. $\Delta f_0 T = 0.5$.

que pour une complexité équivalente du treillis, les performances des deux schémas de codage sont comparables, même s'il existe un facteur 2 sur l'efficacité spectrale du fait des rendements choisis. La figure 3.16 confirme cette impression : à efficacité spectrale constante, l'alphabet codé par une TCM se comporte mieux que celui codé par un code NRNSC. Le gain apporté par la TCM est de 1.5 dB environ pour une probabilité d'erreur égale à 10^{-4}. Le seul avantage manifeste d'un code convolutif est la simplicité de mise en œuvre du système de transmission par rapport à tous les autres schémas (à faible ou forte latence) jusqu'ici envisagés.

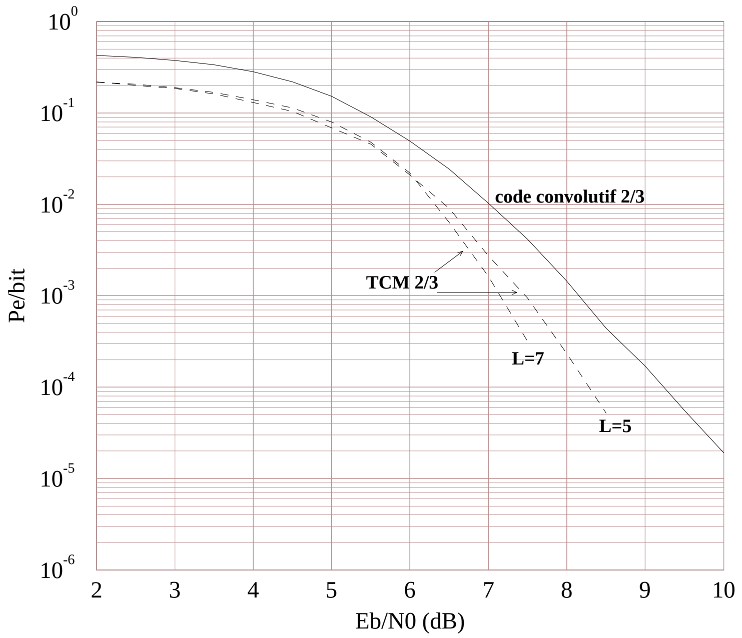


Fig. 3.16 – Modulation 8-FSK codée par un code convolutif 2/3, *vs.* modulation 8-FSK codée par une TCM 2/3, $L = 5, 7$. $\Delta f_0 T = 0.34$.

3.5.2 Alphabet de diversité 4 à composantes corrélées pour le canal de Rayleigh

Nous nous intéressons aux performances sur le canal de Rayleigh de l'alphabet multidimensionnel heuristique présenté au paragraphe 1.2.4. En accord avec les notations du modèle de transmission complet explicité au paragraphe 3.3.2, les $M = 8$ symboles S_m de cet alphabet, noté $\mathcal{A}_1$, sont de longueur $N_S = 4$. Rappelons que $\mathcal{A}_1$ est défini par

$$\begin{array}{rclcrcl} S_1 & = & (0,1,0,1) & \quad & S_5 & = & (4,5,3,0) \\ S_2 & = & (1,3,2,3) & & S_6 & = & (5,7,5,2) \\ S_3 & = & (2,0,4,5) & & S_7 & = & (6,4,7,6) \\ S_4 & = & (3,2,6,7) & & S_8 & = & (7,6,1,4) \end{array}$$

Notons que les performances de l'alphabet $\mathcal{A}_1$ non codé sur canal de Rayleigh ont déjà été comparées à celles d'une modulation BFSK de diversité 4, notée $\mathcal{A}_2$

$$\begin{array}{rcl} S_1 & = & (0,0,0,0) \\ S_2 & = & (1,1,1,1) \end{array}$$

Les différents schémas de codage ici confrontés sont construits à partir de la modulation BFSK, la modulation 8-FSK, l'alphabet $\mathcal{A}_1$ et l'alphabet $\mathcal{A}_2$. Plusieurs valeurs de l'espacement fréquentiel des modulations FSK sous-jacentes sont envisagées : $\Delta f_0 = 1.0/T, 0.75/T, 0.25/T$ et $0.1875/T$. Les courbes de résultats font référence au facteur d'élargissement de bande B_e.

Le code convolutif considéré est un code NRNSC de rendement $R = 1/3$, de longueur de contrainte $L = 5$ et de polynômes générateurs $(25, 33, 37)$. Les alphabets supposent tous l'emploi d'un étiquetage de Gray.

Un décodage à entrée souple simple ainsi que la méthode de détection itérative associée au décodage APP sont envisagés. Dans ce dernier cas, lorsque rien n'est précisé, les résultats présentés sont ceux obtenus à la troisième itération de décodage. Par ailleurs, des trois méthodes de calculs des probabilités *a posteriori* sur canal de Rayleigh proposées au paragraphe 2.1.3, la seconde est naturellement la meilleure ; c'est celle que nous choisissons pour les simulations. En outre, pour les alphabets codés construits selon le modèle de transmission de la figure 3.5, le décodeur à entrée souple correspond à un décodeur de Viterbi classique.

Figure 3.17, l'alphabet $\mathcal{A}_1$, codé ou non, repose sur une 8-FSK corrélée, $\Delta f_0 = 0.25/T$, alors que la modulation BFSK de l'alphabet $\mathcal{A}_2$ est orthogonale. Nous avons déja pu remarquer que l'alphabet $\mathcal{A}_1$ non codé offre un gain de 1 dB par rapport à l'alphabet $\mathcal{A}_2$, alors que l'efficacité spectrale est multipliée par un facteur 3. Par ailleurs, nous observons que ce même alphabet $\mathcal{A}_1$, une fois codé, présente un gain remarquable de 10 dB environ pour une probabilité d'erreur de 10^{-4}, aussi bien par rapport à l'alphabet $\mathcal{A}_1$ non codé (c'est-à-dire à bande fixe) que par rapport à l'alphabet $\mathcal{A}_2$ (c'est-à-dire à efficacité spectrale fixe).

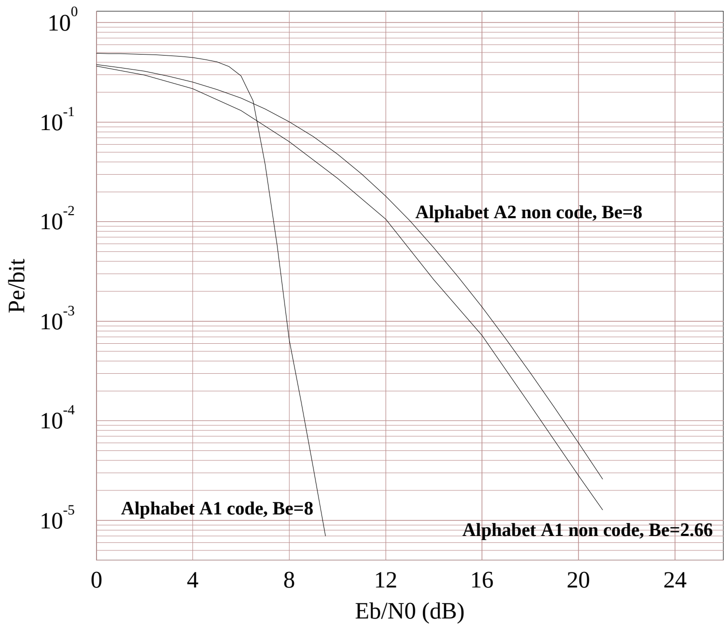


FIG. 3.17 – Alphabet $\mathcal{A}_1$ codé et non codé, $\Delta f_0 = 0.25/T$, *vs.* Alphabet $\mathcal{A}_2$ non codé, $\Delta f_0 = 1.0/T$

La figure 3.18 met en évidence le gain apporté par le décodage itératif lorsque le schéma de transmission considéré est constitué d'une BICM. Deux BICM sont représentées : une modulation 8-FSK simple codée et l'alphabet $\mathcal{A}_1$ codé. Afin que les deux schémas de transmission aient la même efficacité spectrale, les espacements fréquentiels respectifs sont $\Delta f_0 = 0.75/T$ et $\Delta f_0 = 0.1875/T$. Pour l'alphabet $\mathcal{A}_1$ codé, le décodage de Viterbi et le décodage itératif sont représentés. Ainsi, la troisième itération apporte un gain de 2 dB environ pour une probabilité d'erreur de 2×10^{-3} par rapport au décodage de Viterbi. De plus, les performances évoluent de manière non négligeable au cours des itérations : 2 dB (resp. 1.5 dB) de gain entre la première et la troisième itération pour l'alphabet $\mathcal{A}_1$ (resp. la 8-FSK) pour une probabilité d'erreur de 2×10^{-3}. En revanche, il est inutile de considérer plus de trois itérations, le gain entre la seconde et la troisième étant déjà bien moindre qu'entre les deux premières passes.

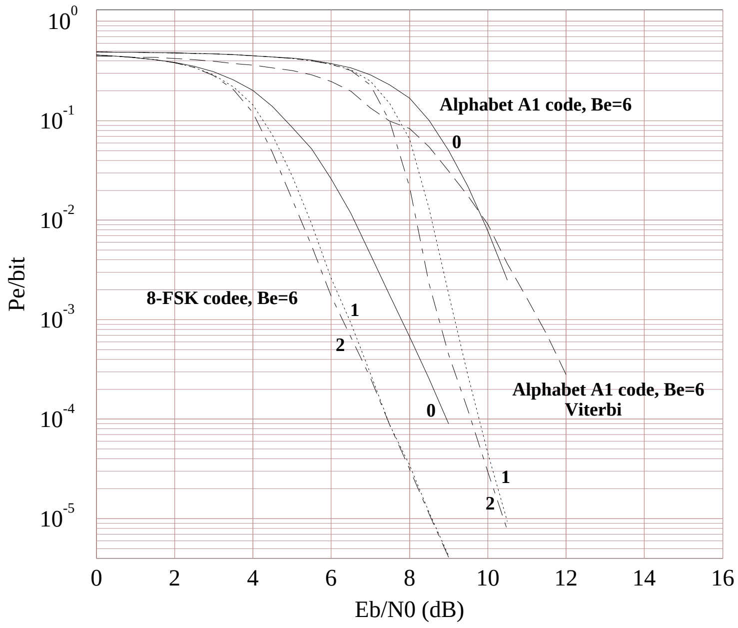


Fig. 3.18 – Influence des itérations sur le décodage de deux BICM : alphabet $\mathcal{A}_1$ codé, $\Delta f_0 = 0.1875/T$ et 8-FSK codée, $\Delta f_0 = 0.75/T$. Comparaison avec l'alphabet $\mathcal{A}_1$ décodé par l'algorithme de Viterbi, $\Delta f_0 = 0.1875/T$.

Finalement, une fois encore, un compromis entre l'occupation de la bande et l'efficacité spectrale disponible est nécessaire. Figure 3.19, l'efficacité spectrale est la même : $\Delta f_0 = 0.75/T$ pour la 8-FSK, $\Delta f_0 = 0.1875/T$ pour $\mathcal{A}_1$ et $\Delta f_0 = 1.0/T$ pour la BFSK. Figure 3.20, la bande est la même : $\Delta f_0 = 0.1875/T$ pour la 8-FSK et $\mathcal{A}_1$, et $\Delta f_0 = 1.0/T$ pour la BFSK. Par conséquent, les deux BICM, BFSK codée et alphabet $\mathcal{A}_1$ codé, ont même efficacité spectrale et occupent la même bande. On remarquera que les résultats de la BFSK codée supposent un décodage de Viterbi. En effet, dans le cas de la BFSK, le signal est aussi le seul bit codé utile. Ainsi, les valeurs des APP des signaux délivrées une fois seulement par le canal sont aussi les APP des bits codés. Il n'y a aucune utilité à itérer le décodage SISO puiqu'aucune information extrinsèque ne pourra être réinjectée dans le calcul de mise à jour des observations (équation (3.13)). Ceci n'est plus vrai dès que deux bits codés au moins servent à étiqueter un signal de la modulation.

Une comparaison des performances illustrées sur ces deux dernières figures conduit aux conclusions suivantes

- Les schémas de codage basés sur les modulations FSK corrélées sont un bon moyen pour augmenter l'efficacité spectrale sur canal de Rayleigh. La dégradation des performances est compensée par l'utilisation du codage.
- A bande fixe, une construction minitieuse de ces alphabets multidimensionnels permet d'apporter un gain supplémentaire.

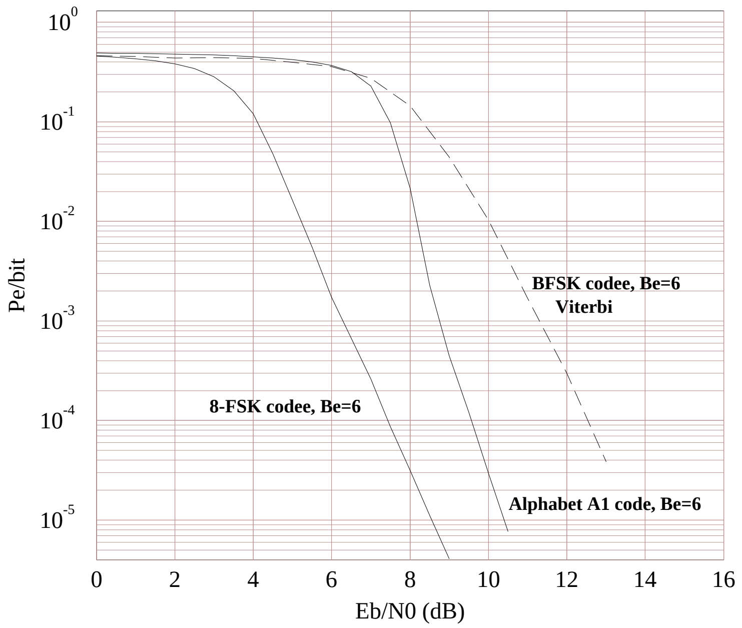


FIG. 3.19 – Comparaison à même efficacité spectrale 0.166 bits/s/Hz : alphabet $\mathcal{A}_1$ codé, $\Delta f_0 = 0.1875/T$, 8-FSK codée, $\Delta f_0 = 0.75/T$ et BFSK codée, $\Delta f_0 = 1.0/T$.

3.6 Conclusions

Dans ce chapitre, nous nous sommes penchés sur des schémas de codage à forte latence tels que les codes convolutifs et les turbo codes qui ont la particularité d'optimiser le taux d'erreur par bit. Par conséquent, ils se sont révélés être tout particulièrement appropriés au décodage SISO, itératif ou non, qui opère bit à bit.

Deux schémas de décodage ont notamment été proposés. Le décodage APP simple utilise un décodeur à entrée souple adapté au code choisi. Ce décodeur sous-optimal au sens ML du terme présente l'avantage considérable d'être adaptable à tout code pour lequel un décodeur à entrée souple existe. Le décodeur associant la détection itérative et le décodage APP a, quant à lui, fait ses preuves ; trois itérations suffisent à obtenir un gain d'environ 2 dB pour une probabilité d'erreur de 2×10^{-3}. La complexité ajoutée est minime.

Enfin, nous avons montré que les alphabets codés à forte latence (codes convolutifs, turbo codes, alphabet de diversité 4) obtiennent des performances encore meilleures que celle des al-

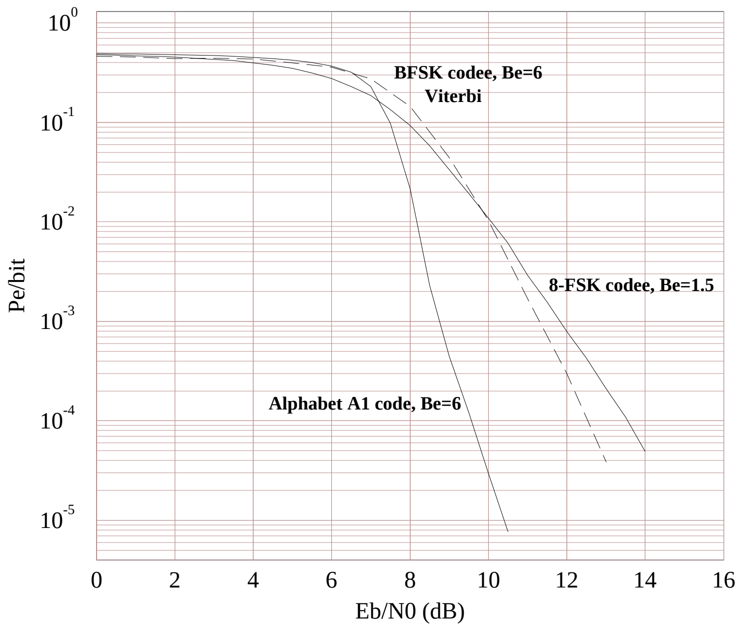


Fig. 3.20 – Comparaison à même bande : alphabet $\mathcal{A}_1$ codé, $Be = 6$ et 8-FSK codée, $Be = 1.5$, $\Delta f_0 = 0.1875/T$; BFSK codée, $B_e = 6$, $\Delta f_0 = 1.0/T$.

phabets codés à faible latence (réseaux de points ou TCM) du chapitre précédent [81][82] . Le choix de la “meilleure” méthode réside dans le compromis entre l’efficacité spectrale ou la bande recherchée et le retard acceptable pour une application donnée. Si la latence n’est pas un obstacle, on privilégiera toujours les alphabets codés par un turbo code.

Chapitre 4

Séquences d'étalement à haute efficacité spectrale : étude de la capacité *

Nous avons consacré les précédents chapitres à l'étude des constellations multidimensionnelles à composantes corrélées reposant sur des signaux Q-FSK non orthogonaux. Il a été montré qu'elles sont un bon moyen pour construire des modulations à haute efficacité spectrale pour la détection non cohérente. L'utilisation d'alphabets de grande dimension associés à du codage permet de compenser la dégradation des performances due à la non orthogonalité des signaux.

On peut cependant regretter la limitation apportée par l'utilisation des modulations FSK. En effet, si l'on souhaite augmenter l'efficacité spectrale de manière encore plus significative, nous devrons choisir des alphabets sous-jacents de plus en plus grands. La conséquence néfaste directe est que la taille du banc de filtres adaptés devient prohibitive (pour $Q >> 8$). Par ailleurs, si l'on a pu trouver un bon choix de réseau sur canal gaussien, nous avons dû nous restreindre à des méthodes de codage forte latence sur canal de Rayleigh. En effet, les meilleurs réseaux sur canal à évanouissements sont des réseaux à composantes non entières. Il est impossible de les étiqueter par des modulations FSK de taille raisonnable.

Nous choisissons par conséquent de nous intéresser désormais aux séquences d'étalement orthogonales ou non. Bien souvent, leurs composantes sont binaires ou entières. Nous relâchons cette contrainte en autorisant l'emploi de composantes non binaires, réelles ou complexes. Cela permet de construire des familles de M séquences d'étalement corrélées de longueur N bien plus grande que la taille de la famille, soit $M >> N$.

Il est important de s'assurer que les valeurs de corrélation entre ces différentes séquences restent aussi maîtrisées que possible. Cette contrainte est nécessairement de plus en plus difficile à satisfaire lorsque le nombre de séquences d'une longueur donnée augmente.

Dans ce chapitre, les principes de base de la construction de telles séquences seront tout d'abord exposés. Puis nous présentons en détail le cas de familles de séquences orthogonales, et non orthogonales de longueur N.

*Les résultats de ce chapitre ont été présentés au *2000 International Symposium on Information Theory and its Applications*, Hawai, novembre 2000.

Nous étudions ensuite la capacité des canaux gaussien et de Rayleigh lorsque ces différents alphabets sont présentés en entrée. On sait par ailleurs que la capacité au sens de Shannon d'un canal de Rayleigh pour lequel les évanouissements sont constants par blocs (block-fading) est nulle. En effet, le théorème de codage [6] nous indique que la capacité d'un canal donné peut être atteinte pour un code arbitrairement long. Malheureusement, dans ce cas, les atténuations subies par le signal sont trop nombreuses sur la durée du code et la probabilité d'erreur ne pourra être rendue arbitrairement petite. Dans notre étude, nous supposons que la taille des trames sur lesquelles les évanouissements sont constants est égale à la longueur N des séquences. Ce schéma, également choisi dans [51], est parfaitement équivalent à un canal de Rayleigh qui varie d'un symbole à l'autre et la capacité n'est pas nulle.

Les résultats théoriques sont finalement comparés à un exemple pratique. Nous appliquons pour cela le décodage itératif proposé au chapitre 3 à des séquences non orthogonales codées par un code convolutif.

4.1 Séquences d'étalement corrélées à haute efficacité spectrale

Dans tout ce chapitre, nous travaillons avec des familles de séquences d'étalement de longueur N. Si l'on exige que ces séquences soient orthogonales et à composantes binaires, il en existe seulement N ; elles sont données par la matrice de Walsh-Hadamard de dimension N. Dans la mesure où nous cherchons à augmenter l'efficacité spectrale, on peut tout d'abord relâcher la contrainte sur l'orthogonalité des signaux. On construit alors des familles de $M > N$ séquences corrélées à composantes binaires, par exemple aléatoirement. Il est cependant plus intéressant de relâcher simultanément les contraintes sur l'orthogonalité et les composantes binaires. Cela revient à chercher M séquences corrélées de longueur N, à composantes binaires ou non. On note $\mathcal{A} = \{\mathbf{s}_1, \ldots, \mathbf{s}_M\}$ l'alphabet des M séquences complexes de longueur N et $\mathbf{s}_m = (s_{m,1}, \ldots, s_{m,N})$.

4.1.1 Principe de construction

Les séquences des familles considérées ont toutes même énergie. D'un point de vue géométrique, cela revient à placer M séquences sur une hypersphère en dimension N, tout en garantissant une bonne répartition de leurs corrélations. Grâce à la distribution sphérique des signaux, l'étiquetage de Gray est parfaitement adapté. Nous pourrons choisir l'un d'entre eux au moyen de $\log_2(M)$ bits d'information.

Les M séquences de la famille correspondent à M points répartis sur l'hypersphère. Les N composantes (c'est-à-dire chips) de $\mathbf{s}_m$, $m = 1, \ldots, M$ sont les coordonnées du point qui lui est associé dans l'espace N-dimensionnel. Par construction, les corrélations entre les séquences sont directement liées aux angles entre les points qui leur correspondent. Si l'on accepte de prendre en compte toute la surface de la sphère, on autorise les points diamétralement opposés : la corrélation maximale pourra atteindre la valeur 1. En revanche, si l'on se limite à la moitié de la sphère, la corrélation maximale ne pourra pas atteindre cette valeur de 1.

Remarquons enfin qu'il est possible de construire facilement des séquences complexes en combinant les séquences réelles. Cela permet de diminuer la corrélation de moitié, en moyenne.

4.1.2 Séquences de longueur 2 chips

Le cas $M = 8$, $N = 2$ correspond à l'exemple d'une famille de 8 séquences de longueur 2 chips. On les note $\{\mathbf{s}_1, \ldots, \mathbf{s}_8\}$. La table 4.1 et la figure 4.1 donne les deux représentations possibles de cette famille selon que l'on choisit de placer les huit points sur le demi cercle unité (famille 1) ou sur le cercle unité (famille 2) en dimension 2.

Séquences	Famille 1	Famille 2
$\mathbf{s}_1$	(1, 0)	(1, 0)
$\mathbf{s}_2$	(0.923, 0.382)	(0.707, 0.707)
$\mathbf{s}_3$	(0 707, 0.707)	(0, 1)
$\mathbf{s}_4$	(0.382, 0.923)	(-0.707, 0.707)
$\mathbf{s}_5$	(0, 1)	(-1, 0)
$\mathbf{s}_6$	(-0.382, 0.923)	(-0.707,-0.707)
$\mathbf{s}_7$	(-0.707, 0.707)	(0,-1)
$\mathbf{s}_8$	(-0.923, 0.382)	(0.707,-0.707)

Tab. 4.1 – Huit séquences d'étalement réelles de 2 chips réparties sur le demi cercle supérieur (famille 1) ou sur le cercle (famille 2).

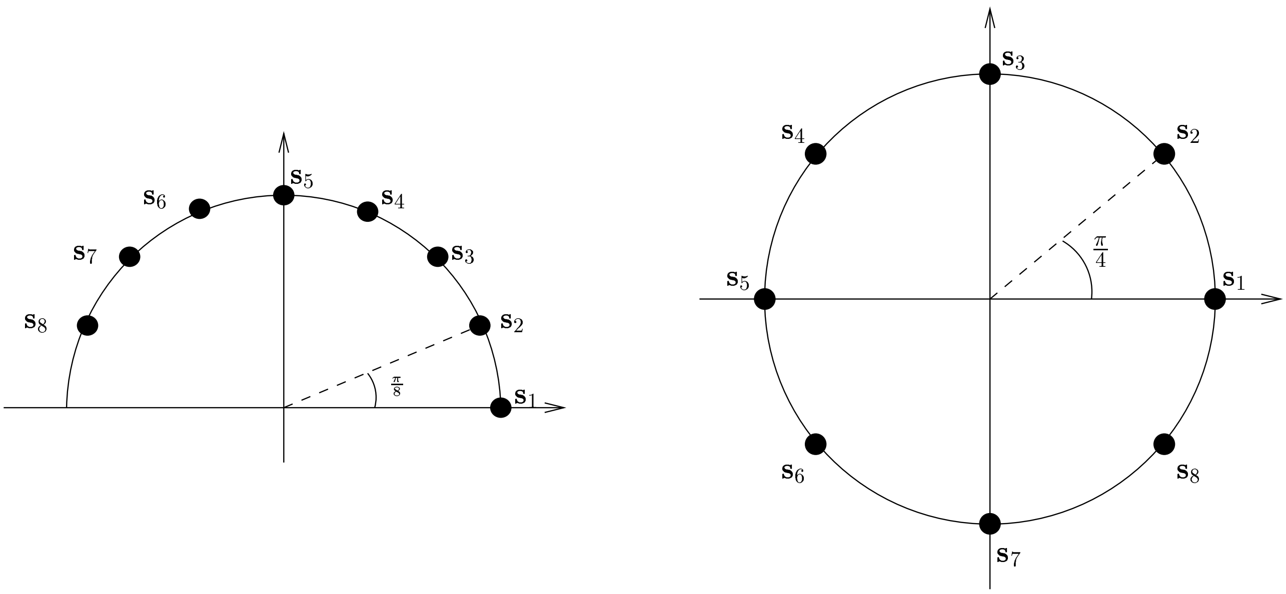


Fig. 4.1 – Représentations géométriques des familles 1 (sur le demi cercle) et 2 (sur le cercle).

La corrélation entre deux séquences $\mathbf{s}_i$ et $\mathbf{s}_\ell$, définie comme le produit scalaire entre les deux vecteurs correspondants aux séquences, est donnée par

$$\mu_{i,\ell} = cos(\alpha_{i,\ell})$$

où $\alpha_{i,\ell}$ est l'angle entre les deux représentations géométriques de $\mathbf{s}_i$ et $\mathbf{s}_\ell$. $\mu_{i,\ell}$ est réelle et la corrélation maximale entre deux séquences distinctes (autre que celle obtenue pour des points diamétralement opposés) est donnée par

$$\mu_{max} = \begin{cases} cos(\frac{\pi}{8}) & \text{pour la famille 1} \\ \\ cos(\frac{\pi}{4}) & \text{pour la famille 2} \end{cases} \tag{4.1}$$

Ceci peut être facilement généralisé au cas de M séquences de longueur $N = 2$. Pour tout couple de vecteurs distincts,

$$\mu_{max} = \begin{cases} cos(\frac{\pi}{M}) & \text{pour } M \text{ séquences sur le demi cercle} \\ \\ cos(\frac{2\pi}{M}) & \text{pour } M \text{ séquences sur le cercle} \end{cases} \tag{4.2}$$

Les équations (4.2) prouvent que la valeur maximale de la corrélation souffre d'une trop forte augmentation du nombre M de séquences d'étalement. Il se trouve que par ailleurs, la valeur de M est directement reliée à l'efficacité spectrale. Trois paramètres importants entrent alors en compte dans le choix de M : l'efficacité spectrale souhaitée, la corrélation maximale obtenue et la distribution des corrélations. Comme pour les Q-FSK, il faut veiller à établir un compromis entre cette efficacité spectrale et la dégradation des performances (due aux corrélations) admissible. On peut par exemple accepter une valeur relativement forte pour μ_{max} si celle-ci est peu fréquente.

Pour chacune des deux familles réelles de notre exemple, les corrélations entre les séquences, données en valeur absolue, sont résumées dans les tableaux 4.2 et 4.3.

Séquences	$\mathbf{s}_1$	$\mathbf{s}_2$	$\mathbf{s}_3$	$\mathbf{s}_4$	$\mathbf{s}_5$	$\mathbf{s}_6$	$\mathbf{s}_7$	$\mathbf{s}_8$
$\mathbf{s}_1$	1	0.923	0.707	0.382	0	0.382	0.707	0.923
$\mathbf{s}_2$	0.923	1	0.923	0.707	0.382	0	0.382	0.707
$\mathbf{s}_3$	0.707	0.923	1	0.923	0.707	0.382	0	0.382
$\mathbf{s}_4$	0.382	0.707	0.923	1	0.923	0.707	0.382	0
$\mathbf{s}_5$	0	0.382	0.707	0.923	1	0.923	0.707	0.382
$\mathbf{s}_6$	0.382	0	0.382	0.707	0.923	1	0.923	0.707
$\mathbf{s}_7$	0.707	0.382	0	0.382	0.707	0.923	1	0.923
$\mathbf{s}_8$	0.923	0.707	0.382	0	0.382	0.707	0.923	1

Tab. 4.2 – $|\mu_{i,\ell}|_{i,\ell=1,\dots,8}$ pour la famille des séquences distribuées sur le demi cercle supérieur.

Séquences	$\mathbf{s}_1$	$\mathbf{s}_2$	$\mathbf{s}_3$	$\mathbf{s}_4$	$\mathbf{s}_5$	$\mathbf{s}_6$	$\mathbf{s}_7$	$\mathbf{s}_8$
$\mathbf{s}_1$	1	0.707	0	0.707	1	0.707	0	0.707
$\mathbf{s}_2$	0.707	1	0.707	0	0.707	1	0.707	0
$\mathbf{s}_3$	0	0.707	1	0.707	0	0.707	1	0.707
$\mathbf{s}_4$	0.707	0	0.707	1	0.707	0	0.707	1
$\mathbf{s}_5$	1	0.707	0	0.707	1	0.707	0	0.707
$\mathbf{s}_6$	0.707	1	0.707	0	0.707	1	0.707	0
$\mathbf{s}_7$	0	0.707	1	0.707	0	0.707	1	0.707
$\mathbf{s}_8$	0.707	0	0.707	1	0.707	0.707	0.707	1

Tab. 4.3 – $|\mu_{i,\ell}|_{i,\ell=1,\dots,8}$ pour la famille des séquences distribuées sur le cercle.

Comme déjà mentionné au paragraphe 4.1.1, la construction de famille de séquences complexes à partir de séquences réelles est envisageable. Par exemple

$$\begin{array}{lcl}\mathbf{S}_1 & \to & \mathbf{s}_1 + j\mathbf{s}_1 \\ \mathbf{S}_2 & \to & \mathbf{s}_2 + j\mathbf{s}_5 \\ \mathbf{S}_3 & \to & \mathbf{s}_3 + j\mathbf{s}_2 \\ \mathbf{S}_4 & \to & \mathbf{s}_4 + j\mathbf{s}_6 \\ \mathbf{S}_5 & \to & \mathbf{s}_5 + j\mathbf{s}_3 \\ \mathbf{S}_6 & \to & \mathbf{s}_6 + j\mathbf{s}_7 \\ \mathbf{S}_7 & \to & \mathbf{s}_7 + j\mathbf{s}_4 \\ \mathbf{S}_8 & \to & \mathbf{s}_8 + j\mathbf{s}_8\end{array}$$

Les $\mathbf{S}_i$, $i = 1, \ldots, 8$ sont les séquences d'étalement complexes.

La corrélation entre deux séquences $\mathbf{S}_i$ et $\mathbf{S}_\ell$ est définie de la façon suivante

$$\mu_{i,\ell} = \frac{1}{2}\mathbf{S}_i\mathbf{S}_\ell^*$$

On la note toujours $\mu_{i,\ell}$ et elle est complexe. Grâce au facteur $\frac{1}{2}$, le module de $\mu_{i,\ell}$ conserve des valeurs comprises entre 0 et 1.

Un calcul similaire à celui effectué précédemment permet d'évaluer les corrélations entre toutes les paires de séquences complexes. Les résultats, en module, sont donnés par les tableaux 4.4 et 4.5.

Séquences	$\mathbf{S}_1$	$\mathbf{S}_2$	$\mathbf{S}_3$	$\mathbf{S}_4$	$\mathbf{S}_5$	$\mathbf{S}_6$	$\mathbf{S}_7$	$\mathbf{S}_8$
$\mathbf{S}_1^*$	1	0.866	0.5	0.707	0.707	0.5	0.5	0.707
$\mathbf{S}_2^*$	0.866	1	0.5	0.923	0.382	0.866	0	0.5
$\mathbf{S}_3^*$	0.5	0.5	1	0.382	0.923	0.707	0.866	0.5
$\mathbf{S}_4^*$	0.707	0.923	0.382	1	0	0.923	0.382	0.707
$\mathbf{S}_5^*$	0.707	0.382	0.923	0	1	0.382	0.923	0.707
$\mathbf{S}_6^*$	0.5	0.866	0.707	0.923	0.382	1	0.5	0.5
$\mathbf{S}_7^*$	0.5	0	0.866	0.382	0.923	0.5	1	0.866
$\mathbf{S}_8^*$	0.707	0.5	0.5	0.707	0.707	0.5	0.866	1

TAB. 4.4 – $|\mu_{i,\ell}|_{i,\ell=1,\ldots,8}$ pour la famille de $M = 8$ séquences complexes construite à partir de la famille 1.

La simple observation des tableaux 4.4 et 4.5 montre que le choix de séquences réelles ou complexes, distribuées sur le cercle ou le demi cercle a des conséquences directes sur la distribution des corrélations, ceci pour une valeur fixe de M.

4.1.3 Séquences de longueur 8 chips

Les codes sphériques construits à partir de réseaux entiers fournissent un exemple de séquences d'étalement réelles de longueur $N = 8$ [26]. Il existe ainsi une façon unique et optimale

Séquences	$\mathbf{S}_1$	$\mathbf{S}_2$	$\mathbf{S}_3$	$\mathbf{S}_4$	$\mathbf{S}_5$	$\mathbf{S}_6$	$\mathbf{S}_7$	$\mathbf{S}_8$
$\mathbf{S}_1^*$	1	0.653	0.822	0.382	0.5	0.568	0.568	0.923
$\mathbf{S}_2^*$	0.653	1	0.669	0.937	0.546	0.742	0.270	0.568
$\mathbf{S}_3^*$	0.822	0.669	1	0.489	0.872	0	0.742	0.568
$\mathbf{S}_4^*$	0.382	0.937	0.489	1	0.653	0.872	0.546	0.5
$\mathbf{S}_5^*$	0.5	0.546	0.872	0.653	1	0.489	0.937	0.382
$\mathbf{S}_6^*$	0.568	0.742	0	0.872	0.489	1	0.669	0.822
$\mathbf{S}_7^*$	0.568	0.270	0.742	0.546	0.937	0.669	1	0.653
$\mathbf{S}_8^*$	0.923	0.568	0.568	0.5	0.382	0.822	0.653	1

Tab. 4.5 – $|\mu_{i,\ell}|_{i,\ell=1,\ldots,8}$ pour la famille de $M = 8$ séquences complexes construite à partir de la famille 2.

de placer 240 points sur une hypersphère de dimension 8, tout en garantissant une corrélation maximale de 0.5 entre les séquences associées à ces points. Dans ce cas, nous avons $M = 240$ séquences d'étalement corrélées de longueur $N = 8$.

Nous avons déjà vu au chapitre 2 que le réseau de Gosset, E_8, est le réseau entier le plus dense en dimension 8. Les points du réseau sont assimilés aux centres des sphères de l'empilement correspondant. Le coefficient d'erreur de E_8, défini comme le nombre de sphères tangentes à une même sphère, est 240 [17][26]. Chaque sphère est ainsi entourée par 240 sphères tangentes, de telle sorte que chaque point du réseau possède 240 voisins situés à une distance égale à la distance minimale du réseau. Ces 240 plus proches voisins constituent la première couronne du réseau de Gosset. Si les sphères sont de rayon unité, les points de E_8 sont tous à distance 2 les uns des autres. Un calcul géométrique simple montre que l'angle qui sépare tout couple de points est égal à $\frac{\pi}{3}$, ce qui conduit à une corrélation maximale de $cos(\frac{\pi}{3}) = 0.5$.

L'ensemble de ces points forme ce que l'on appelle un code sphérique de taille 240. On peut aisément assimiler chacun des 240 points ou mots de code à une séquence de longueur 8 puisque chaque point possède 8 coordonnées. On construit ainsi une famille de $M = 240$ séquences d'étalement corrélées de longueur $N = 8$. Il s'agit bien de la meilleure façon de placer 240 points sur une hypersphère en dimension 8 tout en garantissant une répartition régulière et intéressante des corrélations. L'unicité et l'optimalité de cette famille de séquences proviennent de la structure même du réseau sous-jacent.

La matrice de Walsh-Hadamard fournissant seulement $M = 8$ séquences orthogonales de longueur $N = 8$, les pertes dues à la corrélation non nulle des 240 séquences ci-dessus sont largement compensées par la multiplicité du choix, bien plus important parmi 240 que parmi 8.

Le paragraphe suivant donne la définition exacte d'un code sphérique et une généralisation de cette méthode.

4.1.4 Généralisation : utilisation des codes sphériques

On note Ω_N la sphère unité de $\mathbb{R}^N$ et $(.,.)$ le produit scalaire usuel. Un code sphérique noté (N, M, s) est un sous-ensemble C de Ω_N de taille M et pour lequel $(u, v) \leq s$ pour tous $u, v \in C$

et $u \neq v$. Le code sphérique utilisé au paragraphe précédent et défini à partir de la première couronne de E_8 est le code (8, 240, 1/2).

Il existe d'autres codes sphériques définis de la même façon à partir de réseaux de points entiers. Ces constructions sont toujours uniques. Citons par exemple le code (24, 196560, 1/2) construit à partir du réseau de Leech, Λ_{24}.

Il est important de signaler que pour une dimension N donnée, les codes sphériques construits de la sorte sont ceux qui fournissent le plus grand nombre de séquences. Toute autre construction basée sur des réseaux entiers conduira à des familles contenant moins de séquences [26]. Par ailleurs, le coefficient d'erreur d'un réseau est rarement égal à une puissance de 2. Il faudra choisir certaines séquences seulement parmi toutes celles du code afin de les étiqueter avec un nombre entier de bits d'information.

Hormis une généralisation possible avec des dimensions N plus grandes, on peut baser la construction des codes sur des réseaux non intégraux [17][26]. On autorise dans ce cas l'utilisation de composantes non binaires et même non entières. Il s'agit alors de placer un nombre arbitraire de points, que l'on pourra choisir comme étant une puissance de 2, sur une hypersphère. Il reste bien entendu primordial de garantir une bonne répartition des corrélations entre les séquences qui leurs seront associées.

4.2 Familles de séquences orthogonales de longueur N

Le principe général de construction proposé au paragraphe 4.1.1 correspond à un grand nombre de familles connues, y compris des familles de séquences orthogonales. Deux types de séquences de longueur N sont détaillés dans ce paragraphe.

4.2.1 Séquences de Walsh-Hadamard

Définition 4.2.1 *Une* **matrice d'Hadamard** *H d'ordre N est une matrice $N \times N$ formée de $+1$ et de -1 et vérifiant $HH^t = NI$.*

La matrice d'Hadamard normalisée [50] est une matrice d'Hadamard dont la première ligne et la première colonne ne contiennent que des $+1$.

$$H_N = \left(\begin{array}{c|ccc} +1 & +1 & \dots & +1 \\ \hline +1 & \dots & \dots & \dots \\ \vdots & \dots & \pm 1 & \dots \\ +1 & \dots & \dots & \dots \end{array}\right)$$

Théorème 4.2.1 *Si une matrice d'Hadamard H d'ordre N existe, alors N vaut 1, 2 ou est multiple de 4.*

La preuve de ce théorème est donnée dans [50]. Par ailleurs, multiplier une ligne ou une colonne de H par -1 fournit une nouvelle matrice d'Hadamard, et deux lignes de H diffèrent en $\frac{N}{2}$ positions exactement [57]. Les N lignes de la matrices sont orthogonales. A une homothétie $\frac{1}{\sqrt{N}}$ près, H est donc une matrice de rotation. La ligne numéro i est une fonction de Walsh.

Il existe plusieurs méthodes de construction, dont la construction de Sylvester. Elle permet de calculer les matrices d'Hadamard d'ordre $N = 2^m$ récursivement [50]

$$H_1 = 1, \quad H_{2N} = \begin{pmatrix} H_N & H_N \\ H_N & -H_N \end{pmatrix} \tag{4.3}$$

Les N lignes de la matrice, notées $\{\mathbf{s}_1, \ldots, \mathbf{s}_N\}$, constituent une famille $\mathcal{A}$ de $M = N$ séquences orthogonales de longueur N à composantes binaires ± 1. Si on normalise la matrice H_N par $\sqrt{N}$, on obtient N séquences orthonormales à composantes réelles distribuées sur une sphère unité en dimension N. H_N est dans ce cas une matrice de rotation.

4.2.2 Séquences orthogonales complexes

Par définition, les lignes ou les colonnes d'une matrice de rotation de taille N forment une base orthonormale. La théorie des nombres permet de construire des matrices de rotation complexes à partir d'un plongement canonique dans un corps de nombres algébriques totalement complexe [18][60]. Seuls les définitions et résultats de la théorie des nombres utiles à cette construction sont ici exposés. Pour une étude plus générale, le lecteur s'intéressera aux travaux de [18].

On note $\mathbb{Z}$ l'anneau des entiers rationnels et K un corps contenant $\mathbb{Q}$ le corps des nombres rationnels.

Définition 4.2.2 *(nombre algébrique)*
Soit α un élément de K. α est un **nombre algébrique** *s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Q}$. Un tel polynôme de degré minimum est appelé* **polynôme minimal** *de α et noté $\mu_\alpha(x)$.*

Définition 4.2.3 *(entier algébrique)*
$\alpha \in K$ est un **entier algébrique** *s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. L'ensemble des entiers algébriques de K est un anneau appelé anneau des entiers de K et noté O_K.*

Si tous les éléments de K sont algébriques, on dit que K est une extension algébrique de $\mathbb{Q}$.

Définition 4.2.4 *(corps de nombres algébriques)*
Le degré $[K : \mathbb{Q}]$ d'une extension algébrique K de $\mathbb{Q}$ est la dimension de K lorsque celui ci est considéré comme un espace vectoriel de $\mathbb{Q}$. Un **corps de nombres algébriques** *est une extension algébrique de $\mathbb{Q}$ de degré fini.*

K désigne maintenant un corps de nombres algébriques. Il existe un élément $\theta \in K$, appelé élément primitif, tel que l'espace vectoriel K de $\mathbb{Q}$ soit généré par les puissances de θ. Si K est de degré d, $(1, \theta, \theta^2, \ldots, \theta^{d-1})$ est une base de K et $\deg(\mu_\theta(x)) = d$. Dans ce cas, nous écrirons $K = \mathbb{Q}(\theta)$. Par ailleurs, il existe un élément primitif θ qui est un entier algébrique de K. Autrement dit, le polynôme minimal $\mu_\theta(x)$ est à coefficients dans $\mathbb{Z}$.

Définition 4.2.5 *(plongement dans un corps de nombres)*
Soient K et K' deux corps contenant $\mathbb{Q}$. $\phi : K \to K'$ est un $\mathbb{Q}$-homomorphisme si pour tout élément $a \in \mathbb{Q}$, $\phi(a) = a$. Dans le cas particulier où $K' = \mathbb{C}$, le corps des nombres complexes, le $\mathbb{Q}$-homomorphisme ϕ est appelé **plongement** *de K dans $\mathbb{C}$.*

θ désigne toujours l'élément primitif de K et $\mu_\theta(x)$ son polynôme minimal de racines $(\theta_1, \theta_2, \ldots, \theta_d)$, $\theta_1 = \theta$. Il existe exactement d plongements de K dans $\mathbb{C}$. Chacun d'entre eux, noté σ_i est complètement identifié par une racine θ_i de $\mu_\theta(x)$

$$\sigma_i : K \to \mathbb{C} \quad \sigma_i(\theta) = \theta_i$$

On remarquera que $\sigma_1(\theta) = \theta_1 = \theta$, par conséquent $\sigma_1(K) = K$. Grâce aux propriétés des homomorphismes, on a aussi $\sigma_i(\theta^k) = (\sigma_i(\theta))^k = \theta_i^k$.

Définition 4.2.6 *(corps de nombres totalement complexe)*
Soient $(\sigma_1, \sigma_2, \ldots, \sigma_d)$ les d $\mathbb{Q}$-homomorphismes de K dans $\mathbb{C}$. On note r_1 le nombre de $\mathbb{Q}$-homomorphismes à image dans $\mathbb{R}$, le corps des nombres réels, et r_2 le nombre de $\mathbb{Q}$-homomorphismes à image dans $\mathbb{C}$ de telle sorte que

$$r_1 + 2r_2 = d$$

La paire (r_1, r_2) est appelée signature de K. Si $r_2 = 0$, K est un **corps de nombres algébriques totalement réel**. *Si $r_1 = 0$, K est un* **corps de nombres algébriques totalement complexe**. *Dans tous les autres cas, on parle d'un corps de nombres algébriques complexe.*

Dans le cas particulier d'un corps totalement complexe de dimension d généré par une racine $n$ième de l'unité, on parle de corps cyclotomique. La dimension du corps d et l'ordre de la racine n sont reliés par la fonction d'Euler $d = \phi(n)$. $\phi(n)$ donne le nombre d'entiers premiers avec n, plus petits que n.

Définition 4.2.7 *(plongement canonique)*
On décide d'ordonner les σ_i comme suit : $\sigma_i(\alpha) \in \mathbb{R}$ pour $1 \le i \le r_1$, et $\sigma_{j+r_2}(\alpha) = \sigma_j^*(\alpha)$ pour $r_1 + 1 \le j \le r_1 + r_2$. L'isomorphisme $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ défini par

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \ldots, \sigma_{r_1+r_2}(\alpha)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

est appelé **plongement canonique**. *En identifiant $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ à $\mathbb{R}^d$, on peut récrire $\sigma : K \to \mathbb{R}^d$ comme*

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), Re\left[\sigma_{r_1+1}(\alpha)\right], Im\left[\sigma_{r_1+1}(\alpha)\right], \ldots, Re\left[\sigma_{r_1+r_2}(\alpha)\right], Im\left[\sigma_{r_1+r_2}(\alpha)\right]) \in \mathbb{R}^d$$

où $Re[.]$ et $Im[.]$ désignent la partie réelle et la partie imaginaire.

Pour toute base $(\omega_1, \omega_2, \ldots, \omega_d)$ de K, les d vecteurs $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^d$ sont linéairement indépendants et définissent une matrice de rang plein

$$\begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \mathrm{Re}[\sigma_{r_1+1}(\omega_1)] & \mathrm{Im}[\sigma_{r_1+1}(\omega_1)] & \ldots & \mathrm{Re}[\sigma_{r_1+r_2}(\omega_1)] & \mathrm{Im}[\sigma_{r_1+r_2}(\omega_1)] \\ \sigma_1(\omega_2) & \ldots & \sigma_{r_1}(\omega_2) & \mathrm{Re}[\sigma_{r_1+1}(\omega_2)] & \mathrm{Im}[\sigma_{r_1+1}(\omega_2)] & \ldots & \mathrm{Re}[\sigma_{r_1+r_2}(\omega_2)] & \mathrm{Im}[\sigma_{r_1+r_2}(\omega_2)] \\ \vdots & & \vdots & & & & & \vdots \\ \sigma_1(\omega_d) & \ldots & \sigma_{r_1}(\omega_d) & \mathrm{Re}[\sigma_{r_1+1}(\omega_d)] & \mathrm{Im}[\sigma_{r_1+1}(\omega_d)] & \ldots & \mathrm{Re}[\sigma_{r_1+r_2}(\omega_d)] & \mathrm{Im}[\sigma_{r_1+r_2}(\omega_d)] \end{pmatrix}$$

Dans le cas d'un corps de nombres algébriques totalement complexe, $r_1 = 0$ et la matrice ci-dessus se simplifie

$$\begin{pmatrix} \mathrm{Re}[\sigma_1(\omega_1)] & \mathrm{Im}[\sigma_1(\omega_1)] & \ldots & \mathrm{Re}[\sigma_{r_2}(\omega_1)] & \mathrm{Im}[\sigma_{r_2}(\omega_1)] \\ \mathrm{Re}[\sigma_1(\omega_2)] & \mathrm{Im}[\sigma_1(\omega_2)] & \ldots & \mathrm{Re}[\sigma_{r_2}(\omega_2)] & \mathrm{Im}[\sigma_{r_2}(\omega_2)] \\ \vdots & & & & \vdots \\ \mathrm{Re}[\sigma_1(\omega_d)] & \mathrm{Im}[\sigma_1(\omega_d)] & \ldots & \mathrm{Re}[\sigma_{r_2}(\omega_d)] & \mathrm{Im}[\sigma_{r_2}(\omega_d)] \end{pmatrix}$$

Si l'on se restreint maintenant à un corps cyclotomique $K = \mathbb{Q}[j](\theta)$ totalement complexe généré par $\theta = e^{2j\pi/n}$, on a toujours $d = \phi(n)$, et les $(\theta_1, \ldots, \theta_d)$ sont les racines du polynôme minimal $\mu_\theta(x)$ associé à θ. Le plongement canonique associé à ce corps est défini par les d isomorphismes $\sigma_i,\ i = 1, \ldots, d$ où chaque σ_i fait correspondre une racine distincte à θ : $\sigma_i(\theta) = \theta_i$. Si on applique ce plongement canonique à l'ensemble $1, \theta, \ldots, \theta^{d/2-1}$ en utilisant $d/2$ isomorphismes parmi d, on obtient une matrice complexe de taille $d/2 \times d/2$

$$R = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \ldots & \sigma_{d/2}(1) \\ \sigma_1(\theta) & \sigma_2(\theta) & \ldots & \sigma_{d/2}(\theta) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\theta^{d/2-1}) & \sigma_2(\theta^{d/2-1}) & \ldots & \sigma_{d/2}(\theta^{d/2-1}) \end{pmatrix} \tag{4.4}$$

Les racines θ_i de $\mu_\theta(x)$ doivent être choisies dans l'ordre suivant

$$\theta_i = \theta \times e^{4j\pi(i-1)/d}, \quad i = 1, \ldots, d/2$$

et le polynôme minimal s'écrit

$$\mu_\theta(x) = x^d + \epsilon x^{d/2} + 1 \tag{4.5}$$

où la variable ϵ prend les valeurs 0 ou 1. On trouve les tables des polynômes pour différentes valeurs de d dans [17].

R est une matrice de rotation. Par définition, ses lignes forment une famille orthonormale de séquences complexes de l'espace de dimension $d/2$. Dans notre cas, nous souhaitons construire une famille de N séquences complexes de longueur N. On choisit par conséquent $N = d/2$. Le corps cyclotomique K de dimension $2N$ est alors généré par $\theta = e^{2j\pi/n}$, et $2N = \phi(n)$: toutes les valeurs de N ne seront pas envisageables. Par identification avec la matrice de rotation de l'équation 4.4 et en utilisant $\sigma_i(\theta^k) = \theta_i^k$, on obtient une matrice de rotation complexe de dimension $N \times N$

$$R = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_N \\ \vdots & \vdots & & \vdots \\ \theta_1^{N-1} & \theta_2^{N-1} & \ldots & \theta_N^{N-1} \end{pmatrix}$$

Les lignes de R constituent la famille $\mathcal{A}$ des $M = N$ séquences complexes recherchées avec

$$\theta = e^{2j\pi/n} \quad \text{et} \quad \theta_i = \theta \times e^{2j\pi(i-1)/N} \; i = 1, \ldots, N$$

4.3 Famille de séquences non orthogonales de longueur N

Nous décrirons ici trois types de familles de séquences complexes non orthogonales, toujours en accord avec le principe donné au paragraphe 4.1.1.

4.3.1 Séquences construites à partir de signaux PSK

Les signaux d'une modulation de phase à M états M-PSK sont de la forme [57]

$$u_m(t) = \exp(j\phi_m) = \exp\left(j\frac{2\pi}{M}(m-1)t\right) \quad m = 1, \ldots, M$$

Les phases ϕ_m appartiennent à $[0, 2\pi]$. Dans notre cas, chaque composante d'une des séquences complexes de l'alphabet est associée à une des M phases d'une M-PSK

$$s_{m,n} = \frac{1}{\sqrt{N}} \exp\left(j\frac{2\pi}{M}((n-1) \times (m-1))[M]\right)$$

où $n[M]$ signifie que la valeur de n est prise modulo M. La phase $\frac{2\pi}{M}((n-1) \times (m-1))[M]$ appartient bien à $[0, 2\pi]$ quand $m = 1, \ldots, M$ et $n = 1, \ldots, N$.

La corrélation entre deux séquences $\mathbf{s}_k$ et $\mathbf{s}_\ell$ est donnée théoriquement par

$$\mu_{k\ell} = E[\mathbf{s}_k \mathbf{s}_\ell^*] = \sum_{n=1}^{N} s_{k,n} s_{\ell,n}^*$$

Tout calcul fait, on a

$$\mu_{k\ell} = \frac{1}{N} \sum_{n=1}^{N} \exp\left\{j\frac{2\pi}{M}\big(((n-1) \times (k-\ell))[M]\big)\right\}$$

En pratique, on constate que la distribution des corrélations est proche d'un sinus cardinal.

4.3.2 Séquences complexes purement aléatoires

Les M séquences complexes purement aléatoires de la famille $\mathcal{A}$ sont de la forme

$$\mathbf{s}_m = \frac{1}{\sqrt{N}}(e^{j\phi_1}, e^{j\phi_2}, \ldots, e^{j\phi_N})$$

Les phases ϕ_n sont choisies aléatoirement de manière uniforme entre 0 et 2π.

4.3.3 Séquences de Marzetta

On ne peut clore cette partie sans évoquer les travaux récents de T. Marzetta et B. Hochwald [51], ainsi que leur généralisation au cas multi-utilisateurs [63]. Ces deux articles abordent le sujet de la capacité d'un canal de Rayleigh non cohérent à évanouissements plats pour les antennes multiples. Une valeur asymptotique de la capacité d'un tel canal et la forme des signaux qui l'atteignent sont notamment données dans [51] ; il nous fournit ainsi une méthode pour construire des alphabets de séquences complexes corrélées les meilleurs possible.

Nous avons rappelé que la capacité d'un canal de Rayleigh à évanouissements par blocs (block-fading) est nulle. Il suffit de travailler avec des mots de codes de longueur égale à la longueur de la trame pour que ce ne soit plus le cas. Dans [51], on dispose de $\mathcal{M}$ antennes d'émission et $\mathcal{N}$ antennes de réception. Chaque utilisateur émet des trames de longueur $\mathcal{T}$ que nous identifions à nos séquences de longueur N, c'est-à-dire $\mathcal{T} = N$. Nous résumons les principaux résultats avant de décrire la méthode de construction plus précisément.

Soient S la matrice $\mathcal{T} \times \mathcal{M}$ des symboles émis, H la matrice $\mathcal{M} \times \mathcal{N}$ des coefficients d'atténuation du canal, W la matrice $\mathcal{T} \times \mathcal{N}$ du bruit additif blanc gaussien et enfin X la matrice $\mathcal{T} \times \mathcal{N}$ des symboles reçus. La variance du bruit N_0 est supposée unitaire et on note γ le rapport signal-à-bruit correspondant à l'énergie reçue en bande de base sur une des antennes de réception. Alors

$$X = \sqrt{\frac{\gamma}{\mathcal{M}}} SH + W$$

On note $p(X/S)$ la densité de probabilité du signal X conditionnellement à l'émission de S. Si $I_{\mathcal{T}}$ désigne la matrice identité $\mathcal{T} \times \mathcal{T}$ et Tr la trace, $p(X/S)$ donnée par [51], équation (4) ; alors,

$$p(X/S) = \frac{\exp\left(-Tr\{[I_{\mathcal{T}} + (\gamma/\mathcal{M})SS^H]^{-1}XX^H\}\right)}{\pi^{\mathcal{T}\mathcal{N}} \det^{\mathcal{N}}[I_{\mathcal{T}} + (\gamma/\mathcal{M})SS^H]}$$

induit ou vérifie les propriétés suivantes

Propriété 1 *La matrice XX^H de taille $\mathcal{T} \times \mathcal{T}$ constitue une statistique suffisante.*

Propriété 2 *La densité de probabilité conditionnelle $p(X/S)$ dépend de la variable S uniquement par l'intermédiaire de SS^H.*

Propriété 3 *Pour toute matrice unitaire Ψ de taille $\mathcal{M} \times \mathcal{M}$, on a*

$$p(X/S\Psi^H) = p(X/S)$$

Propriété 4 *Pour toute matrice unitaire Φ de taille $\mathcal{T} \times \mathcal{T}$, on a*

$$p(\Phi^H X/\Phi S) = p(X/S)$$

L'information mutuelle moyenne entre le signal d'entrée S et le signal reçu X est donnée par

$$I(X;S) = E_{X,S}\left\{\log\left(\frac{p(X/S)}{p(X)}\right)\right\}$$

et la capacité du canal est définie par

$$C = \max_{p(S)} I(X;S)$$

Il est montré que $I(X;S)$ est invariante aux rotations subies par le signal émis S (Lemme 1) et que pour atteindre la capacité, on pourra indifféremment normaliser à 1 l'énergie d'un symbole, celle d'une ligne ou d'une colonne de S ou bien même toute la matrice S (Corollaire 1). On peut alors énoncer les deux principaux résultats :

Théorème 4.3.1 *(La capacité reste inchangée si $\mathcal{M} > \mathcal{T}$ ou $\mathcal{M} = \mathcal{T}$)*
Quels que soient la valeur du temps de cohérence $\mathcal{T}$ du canal et le nombre d'antennes de réception $\mathcal{N}$, la capacité obtenue avec $\mathcal{M} > \mathcal{T}$ antennes d'émission est la même que celle obtenue avec $\mathcal{M} = \mathcal{T}$ antennes d'émission.

Théorème 4.3.2 *(Structure des signaux qui atteignent la capacité)*
La matrice des signaux qui atteignent la capacité peut s'écrire $S = \Phi V$, où Φ est une matrice $\mathcal{T} \times \mathcal{T}$ unitaire isotropique et V une matrice $\mathcal{T} \times \mathcal{M}$ diagonale réelle positive, indépendante de Φ. Par ailleurs, on pourra toujours choisir la densité de probabilité conjointe des éléments diagonaux de V invariante aux réarrangements de ces arguments.

Ainsi, contrairement au cas de la détection cohérente pour lequel la capacité augmente avec le nombre d'antennes d'émission et de réception $(\mathcal{M},\mathcal{N})$, et ce pour toute valeur du temps de cohérence $\mathcal{T}$, [51] montre que lorsque la détection est non cohérente, il est inutile d'émettre sur un nombre d'antennes supérieur au temps de cohérence du canal.

Enfin, [51] donne deux résultats asymptotiques :

Théorème 4.3.3 *(Capacité asymptotique, $\mathcal{T} \to \infty$)*
Soit $\mathcal{M} = \mathcal{N} = 1$. Alors

$$(\log e)e^{1/\gamma}E_1\left(\frac{1}{\gamma}\right) - \mathcal{O}\left(\sqrt{\frac{\log \mathcal{T}}{\mathcal{T}}}\right) \leq \frac{C}{\mathcal{T}} \leq (\log e)e^{1/\gamma}E_1\left(\frac{1}{\gamma}\right)$$

où $E_1(x)$ désigne l'exponentielle intégrale définie par

$$E_1(x) = \int_x^\infty \frac{e^{-y}}{y} dy$$

Théorème 4.3.4 *(Distribution qui atteint la capacité, pour $\mathcal{T} \to \infty$)*
Soit $\mathcal{M} = \mathcal{N} = 1$. Les signaux qui atteignent la capacité sont tels que $v_1/\sqrt{\mathcal{T}}$ converge en distribution vers un Dirac en 1 quand $\mathcal{T} \to \infty$.

où v_1 est ici l'unique élément de la matrice V.

Dans le cas particulier $\mathcal{M} = \mathcal{N} = 1$ qui est le nôtre, on déduit du théorème 4.3.2 une méthode générale de construction de signaux corrélés pouvant atteindre la capacité. Ils sont alors de la forme $S = \Phi v = v\Phi = (s_1, s_2, \ldots, s_N)$ où v est une amplitude de moyenne 1 et Φ un vecteur aléatoire unitaire et isotropique de longueur $\mathcal{T} = N$. N désigne bien ici la longueur de la séquence, on veillera à ne pas le confondre avec $\mathcal{N}$, le nombre d'antennes de réception. En pratique, chaque composante s_n d'une séquence s'écrit $s_n = \rho_n e^{j\phi_n}$. L'amplitude ρ_n suit une loi de Rayleigh de moyenne 1 et ϕ est uniformément distribuée entre 0 et 2π. On construit ainsi M séquences S_m corrélées qui constituent l'alphabet $\mathcal{A}$ cherché. On normalise les séquences de manière à ce que leur énergie moyenne sur l'ensemble de l'alphabet $\mathcal{A}$ soit égale à 1.

Nous nous limitons à des séquences de longueur $N = 8$, bien que le théorème 4.3.3 énonce un résultat asymptotique. Cependant, les résultats numériques de [51] montrent que le choix de séquences plus longues ne se traduira pas par un gain remarquable au niveau des performances : la capacité limite est pratiquement déjà atteinte pour $\mathcal{T} = N \simeq 10$.

4.4 Evaluation de la capacité

4.4.1 Rappels de théorie de l'information

Le propre de la théorie de l'information est de fournir des outils mathématiques permettant l'étude et la compréhension d'un système de communication. Lors d'une transmission sur un canal physique entre une source et un destinataire soucieux de communiquer, le signal subit des perturbations dues au bruit thermique et aux imperfections du système lui même. Deux questions majeures se posent : quelle quantité maximale d'information pourra être transmise ? et avec quel degré de compression ? La communication est un succès si la source et le destinataire sont d'accord sur l'information effectivement transmise. Les principaux résultats [6][28] sont ici exposés avant de passer au calcul de la capacité pour des familles de séquences d'étalement corrélées.

Un canal stationnaire, causal et sans mémoire est représenté figure 4.2. X et Y sont deux variables aléatoires indépendantes désignant l'entrée et la sortie du canal et de densités de probabilité respectives $p_X(x)$ et $p_Y(y)$. Le canal est entièrement défini par les probabilités de transition $Pr(Y/X)$, probabilité d'observer le message Y en sortie si X a été émis.

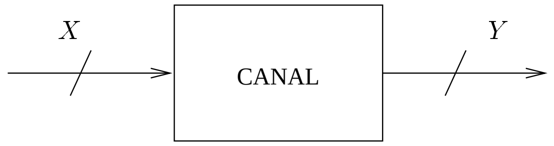


Fig. 4.2 – Canal stationnaire, causal et sans mémoire.

Nous supposons que les variables X et Y ont des distributions continues. Nous appellerons abusivement entropies les différentes entropies différentielles définies ci-dessous.

Définition 4.4.1 *(entropie)*
*L'***entropie** *$\mathcal{H}_d(X)$ de la variable aléatoire X est l'incertitude liée à la variable X, c'est-à-dire*

la quantité d'information nécessaire à la description de cette variable

$$\mathcal{H}_d(X) = -\int p_X(x)\log_2[p_X(x)]dx$$

Définition 4.4.2 *(entropie conjointe)*
*L'***entropie conjointe** $\mathcal{H}_d(X,Y)$ *de deux variables aléatoires* X *et* Y *est l'incertitude liée à la réalisation conjointe des variables* X *et* Y

$$\mathcal{H}_d(X,Y) = -\int\int p_{X,Y}(x,y)\log_2[p_{X,Y}(x,y)]dxdy$$

où $p_{X,Y}(x,y)$ *est la loi conjointe des deux variables aléatoires.*

Définition 4.4.3 *(entropie conditionnelle)*
*L'***entropie conditionnelle** $\mathcal{H}_d(Y|X)$ *est l'incertitude liée à la réalisation de* Y*, sachant que* X *est réalisée*

$$\mathcal{H}_d(Y|X) = -\int\int p_{X,Y}(x,y)\log_2[p_{Y|X}(y|x)]dxdy$$

Grâce à la loi de Bayes, on peut montrer facilement que les diverses entropies sont reliées par la relation

$$\mathcal{H}_d(X,Y) = \mathcal{H}_d(X) + \mathcal{H}_d(Y|X) = \mathcal{H}_d(Y) + \mathcal{H}_d(X|Y)$$

La transmission du message X sur le canal est inutile s'il est à l'avance connu du destinataire. La mesure de l'information est donc une mesure de l'inattendu.

Définition 4.4.4 *(information mutuelle moyenne)*
*L'***information mutuelle moyenne** $I(X;Y)$ *est l'information (ou la réduction d'incertitude) qu'apporte en moyenne la réalisation de* Y *sur* X*, ou de manière parfaitement symétrique l'information qu'apporte en moyenne la réalisation de* X *sur* Y

$$I(X;Y) = \int\int p_{X,Y}(x,y)\log_2\left(\frac{p_{X,Y}(x,y)}{p_X(x)p_Y(y)}\right)dxdy \tag{4.6}$$

Cette quantité n'est pas entièrement caractéristique du canal puisqu'elle dépend aussi de la source choisie. Sa définition entraîne

$$I(X;Y) = \mathcal{H}_d(X) - \mathcal{H}_d(X|Y) = \mathcal{H}_d(Y) - \mathcal{H}_d(Y|X)$$
$$I(X;Y) = \mathcal{H}_d(X) + \mathcal{H}_d(Y) - \mathcal{H}_d(X,Y)$$

Définition 4.4.5 *(capacité)*
La **capacité** C *d'un canal causal et sans mémoire est le maximum de l'information mutuelle moyenne entre son entrée et sa sortie par rapport à toutes les sources stationnaires et ergodiques possibles connectées à son entrée.*

$$C = \max_{p_X(x)} I(X;Y) \tag{4.7}$$

Par suite, la capacité est aussi le débit maximum R_D avec lequel on pourra transmettre l'information sur le canal tout en garantissant une probabilité d'erreur arbitrairement faible. Le débit R_D, le rendement du code utilisé R et la taille de la modulation M sont reliés par $R_D = R \times \log_2(M)$. Le résultat principal de la théorie de l'information est le théorème de codage énoncé par Shannon

Théorème 4.4.1 *(Théorème fondamental du codage de canal)*
Pour tout débit $R_D < C$, où C est la capacité du canal en bits/dimension, il existe un code de longueur N tel que sa probabilité d'erreur est arbitrairement petite lorsque N tend vers l'infini. Un code infiniment long, bien choisi, permet une communication totalement fiable.

Ainsi, la réciproque de ce théorème nous apprend que tous les codes dont la probabilité d'erreur tend asymptotiquement vers zéro vérifient $R_D \leq C$.

La capacité est par conséquent une mesure de l'aptitude du canal à transmettre de l'information. Pour l'évaluer, il convient de trouver la distribution en entrée qui maximise l'information mutuelle. Par exemple, dans le cas du canal binaire symétrique (BSC, Binary Symmetric Channel) à entrée et sortie discrètes, la capacité est atteinte pour une entrée constituée de signaux équiprobables, soit $P(X = 0) = P(X = 1) = \frac{1}{2}$ [57]. Par ailleurs, on sait qu'une entrée gaussienne maximise la capacité du canal gaussien cohérent [57]. Cette dernière exprimée en bits/s/Hz est donnée par

$$C = \frac{1}{2}\log_2(1 + \frac{2E_c}{N0}) = \frac{1}{2}\log_2(1 + \frac{2RE_b}{N0}) \tag{4.8}$$

où $E_c = RE_b$ est l'énergie par bit codé, E_b l'énergie par bit d'information et R le rendement du code utilisé.

Des travaux récents ont permis de montrer que la capacité d'un canal à évanouissements non cohérent est atteinte pour une distribution discrète à valeurs réelles strictement positives en entrée [1][51], nous en avons déjà parlé au chapitre 1. Par ailleurs, une étude très génerale de la capacité pour des canaux de type Rice, Rayleigh ou gaussien, avec ou sans connaissance des coefficients (détection cohérente ou non) et des signaux non nécessairement orthogonaux est donnée dans [21]. Enfin, la capacité d'un canal non cohérent pour des blocs de signaux M-PSK en entrée est présentée dans [55].

Nous détaillons les différentes expressions de la capacité en fonction des hypothèses retenues : type de canal, détection cohérente ou non, signaux orthogonaux ou non ; puis nous comparons les résultats de simulation obtenus par intégration numérique (méthode de Monte Carlo).

4.4.2 Cas général

Nous ne cherchons pas à déterminer la distribution optimale en entrée c'est-à-dire celle qui maximise l'information mutuelle. Au contraire, nous évaluons la capacité d'un canal pour des alphabets de signaux donnés. Alors $C = I(X;Y)$ et la capacité est évaluée en bits/signal.

Les alphabets utilisés sont des familles finies de M séquences de dimension N, orthogonales ($M = N$) ou corrélées ($M > N$). Cela permet de passer rigoureusement de la capacité en bits/signal à la capacité en bits/s/Hz. En effet, quel que soit le type de détection envisagé, on pourra toujours considérer que la bande utilisée par une séquence de longueur N est $B = N/T$

où T est la durée d'un chip. On remarquera que les capacités obtenues pour des familles de séquences orthogonales sont également valides pour tout ensemble de signaux orthogonaux, par exemple une modulation FSK. Cependant, l'évaluation exacte de la bande occupée par une telle modulation ne peut être faite que numériquement. Le passage à la capacité en bits/s/Hz est alors moins précis.

Le schéma général de transmission est représenté figure 4.3. On émet une séquence de longueur N choisie parmi les M possibles de l'alphabet $\mathcal{A} = \{\mathbf{s}_1, \dots \mathbf{s}_M\}$ où $\mathbf{s}_\ell = (s_{\ell,1}, \dots, s_{\ell,N})$. Puisqu'on ne se limite pas à des séquences binaires, les $s_{\ell,n}$ sont réels ou complexes. Par ailleurs, nous supposons que les séquences sont normalisées de telle sorte que leur énergie $E = 1$ en bande de base. En sortie du canal, si le ℓième signal a été émis, on reçoit

$$\mathbf{r} = \alpha e^{j\phi_\ell}\mathbf{s}_\ell + \mathbf{b} \tag{4.9}$$

où $\mathbf{b}$ est un bruit additif blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle ; ϕ_ℓ est une phase aléatoire uniformément répartie sur $[0, 2\pi]$ de densité de probabilité $p(\phi) = \frac{1}{2\pi}$ et α est le gain du canal. Dans le cas du canal gaussien, α est une constante ; nous choisirons $\alpha = 1$. Dans le cas du canal à évanouissements, α suit une loi de Rayleigh ; $p(\alpha) = 2\alpha e^{-\alpha^2}$ et $E[\alpha^2] = 1$.

La sortie $\mathbf{r}$ du canal est une séquence de longueur N, $\mathbf{r} = (r_1, \dots, r_N)$. Le démodulateur est constitué d'un banc de corrélateurs de la même taille que celle de l'alphabet. Envisageons le cas le plus général d'une famille de taille M. En sortie du banc de corrélateurs on dispose du vecteur $\mathbf{x} = (x_1, \dots, x_M)$ où $x_m = \sum_{n=1}^{N} r_n s_{m,n}^*$.

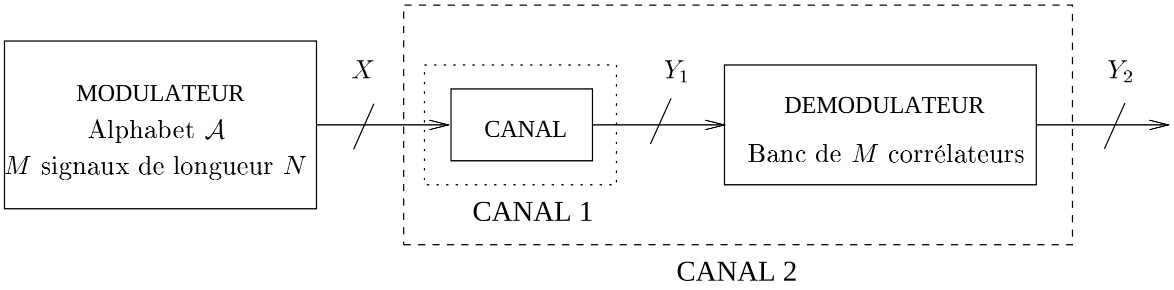


FIG. 4.3 – Schéma de transmission.

Par la suite, nous serons amenés à considérer deux canaux équivalents. Le premier, désigné par CANAL 1 dans la figure 4.3 est uniquement constitué du canal physique sur lequel a lieu la transmission. Son entrée X est discrète : elle appartient à l'alphabet $\mathcal{A}$ des M signaux de longueur N. Sa sortie Y_1 est continue, c'est le vecteur $\mathbf{r}$. Le second, désigné par CANAL 2 est formé de la concaténation du canal physique et du démodulateur. Son entrée X appartient encore à l'alphabet $\mathcal{A}$. Tandis que sa sortie Y_2, continue, est assimilée au vecteur $\mathbf{x}$.

L'information mutuelle moyenne $I(X;Y)$ est donnée par l'équation (4.6). Pour chacun des deux canaux, l'entrée X est discrète et la sortie Y_1 ou Y_2 est continue. La première intégrale sur X se transforme donc en une somme discrète sur tous les signaux de l'alphabet $\mathcal{A}$. De plus

$$p_{X,Y}(x,y) = p_X(x)p_Y(y/x)$$
$$p_X(x) = \textstyle\sum_Y p_{X,Y}(x,y)$$

En utilisant ces quelques propriétés, l'expression (4.6) de $I(X;Y)$ devient

$$I(X;Y) = \sum_{\mathcal{A}} \int_Y p_X(x) p_Y(y/x) \log_2 \left(\frac{p_Y(y/x)}{\sum_{\mathcal{A}} p_{X'}(x') p_Y(y/x')} \right) dy$$

Pour simplifier les notations, nous écrivons désormais $p_X(x) = p(x)$. On obtient une expression plus précise des capacités respectives C_1 et C_2 des deux canaux

$$C_i = I(\mathbf{s};\mathbf{y}_i) = \sum_{\ell=1}^{M} \int_{\mathbf{y}_i} p(\mathbf{s}_\ell) p(\mathbf{y}_i/\mathbf{s}_\ell) \log_2 \left(\frac{p(\mathbf{y}_i/\mathbf{s}_\ell)}{\sum_{k=1}^{M} p(\mathbf{s}_k) p(\mathbf{y}_i/\mathbf{s}_k)} \right) d\mathbf{y}_i$$

où $i = 1, 2$, $\mathbf{y}_1 = \mathbf{r}$ et $\mathbf{y}_2 = \mathbf{x}$.

Les signaux sont supposés équiprobables : $p(\mathbf{s}_\ell) = \frac{1}{M}$ pour tout $\ell = 1, \ldots, M$. Alors

$$C_i = \sum_{\ell=1}^{M} \frac{1}{M} \int_{\mathbf{y}_i} p(\mathbf{y}_i/\mathbf{s}_\ell) \log_2 \left(\frac{p(\mathbf{y}_i/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(\mathbf{y}_i/\mathbf{s}_k)} \right) d\mathbf{y}_i$$

Selon le type de canal, de détection et de signaux utilisés, une expression des probabilités conjointes $\{p(\mathbf{r}/\mathbf{s}_\ell)\}_{\ell=1,\ldots,M}$ peut être déterminée. On remarquera que

$$\int_{\mathbf{y}_i} p(\mathbf{y}_i/\mathbf{s}_\ell) \log_2 \left(\frac{p(\mathbf{y}_i/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(\mathbf{y}_i/\mathbf{s}_k)} \right) d\mathbf{y}_i = E_{\mathbf{y}_i/\mathbf{s}_\ell} \left[\log_2 \left\{ \frac{p(\mathbf{y}_i/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(\mathbf{y}_i/\mathbf{s}_k)} \right\} \right]$$

D'où une expression générale de la capacité des deux canaux

$$C_1 = \sum_{\ell=1}^{M} \frac{1}{M} E_{\mathbf{r}/\mathbf{s}_\ell} \left[\log_2 \left\{ \frac{p(\mathbf{r}/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(\mathbf{r}/\mathbf{s}_k)} \right\} \right] \tag{4.10}$$

et

$$C_2 = \sum_{\ell=1}^{M} \frac{1}{M} E_{\mathbf{x}/\mathbf{s}_\ell} \left[\log_2 \left\{ \frac{p(\mathbf{x}/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(\mathbf{x}/\mathbf{s}_k)} \right\} \right] \tag{4.11}$$

Plusieurs profils d'hypothèses sont envisagés afin de trouver les expressions théoriques exactes des capacités.

4.4.3 Capacité des séquences orthogonales

Seul le cas du canal gaussien ($\alpha = 1$) est traité dans ce paragraphe. Que la détection soit cohérente ou non cohérente, le canal considéré sera de type CANAL 2. Le banc de corrélateurs est constitué des M séquences orthogonales de l'alphabet $\mathcal{A}$. $X \in \mathcal{A}$ et $Y = \mathbf{x} = (x_1, \ldots, x_M)$.

Capacité d'un canal cohérent

Le signal $\mathbf{s}_\ell$ est supposé émis : $\mathbf{r} = e^{j\phi_\ell}\mathbf{s}_\ell + \mathbf{b}$, et

$$x_m = \sum_{i=1}^{N}(e^{j\phi_\ell}s_{\ell,i} + b_i)s^*_{m,i} = e^{j\phi_\ell}\mu_{\ell,m} + b_m$$

où $\mu_{\ell,m}$ est l'intercorrélation entre les séquences ℓ et m et b_m un bruit blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle. Alors x_m est une variable aléatoire gaussienne complexe de moyenne $e^{j\phi_\ell}\mu_{\ell,m}$ et de variance σ^2 par composante réelle. Sa densité de probabilité est donnée par

$$p(x_m/\mathbf{s}_\ell) = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{|x_m - e^{j\phi_\ell}\mu_{\ell,m}|^2}{2\sigma^2}\right)$$

L'orthogonalité des séquences conduit à l'indépendance des variables x_m. Et puisqu'elles sont d'énergie normalisée, $\mu_{\ell,\ell} = E = 1$ et $\mu_{\ell,m} = 0$ pour tout $m \neq \ell$. Enfin, on peut s'affranchir du terme $e^{j\phi_\ell}$ qui est connu du récepteur puisque la détection est cohérente. Ainsi

$$\begin{aligned} p(\mathbf{x}/\mathbf{s}_\ell) &= \prod_{m=1}^{M} p(x_m/\mathbf{s}_\ell) \\ &= \left(\frac{1}{2\pi\sigma^2}\right)^M \exp\left(-\frac{1-2Re(x_\ell)}{2\sigma^2}\right)\exp\left(-\sum_{m=1}^{M}\frac{|x_m|^2}{2\sigma^2}\right) \end{aligned}$$

L'argument du logarithme de l'équation (4.11) devient

$$\frac{p(\mathbf{x}/\mathbf{s}_\ell)}{\sum_{k=1}^{M}\frac{1}{M}p(\mathbf{x}/\mathbf{s}_k)} = \frac{M\left(\frac{1}{2\pi\sigma^2}\right)^M \exp\left(-\frac{1-2Re(x_\ell)}{2\sigma^2}\right)\exp\left(-\sum_{m=1}^{M}\frac{|x_m|^2}{2\sigma^2}\right)}{\sum_{k=1}^{M}\left(\frac{1}{2\pi\sigma^2}\right)^M \exp\left(-\frac{1-2Re(x_k)}{2\sigma^2}\right)\exp\left(-\sum_{m=1}^{M}\frac{|x_m|^2}{2\sigma^2}\right)}$$

Après simplifications, on obtient

$$\frac{p(\mathbf{x}/\mathbf{s}_\ell)}{\sum_{k=1}^{M}\frac{1}{M}p(\mathbf{x}/\mathbf{s}_k)} = \frac{M}{\sum_{k=1}^{M}\exp\left(\frac{Re(x_k - x_\ell)}{\sigma^2}\right)}$$

En reportant dans (4.11), on trouve

$$C = \sum_{\ell=1}^{M}\frac{1}{M}E_{\mathbf{x}/\mathbf{s}_\ell}\left[\log_2(M) - \log_2\left\{\sum_{k=1}^{M}\exp\left(\frac{Re(x_k - x_\ell)}{\sigma^2}\right)\right\}\right]$$

Finalement, on peut remarquer que tous les termes de la somme sur ℓ sont égaux. Il est inutile de tous les calculer : par exemple, celui pour $\ell = 1$ suffit.

L'expression de la capacité du canal gaussien cohérent admettant un alphabet $\mathcal{A}$ de M signaux orthogonaux en entrée est

$$C = \log_2(M) - E_{\mathbf{x}/\mathbf{s}_1}\left[\log_2\left\{\sum_{k=1}^{M}\exp\left(\frac{Re(x_k - x_1)}{\sigma^2}\right)\right\}\right] \tag{4.12}$$

Capacité d'un canal non cohérent

On émet toujours le signal $\mathbf{s}_\ell$, $\mathbf{r} = e^{j\phi_\ell}\mathbf{s}_\ell + \mathbf{b}$. La détection est non cohérente, on s'intéresse au module des M sorties du banc de corrélateurs. Dans ce cas,

$$|x_m| = \left| \sum_{i=1}^{N} (e^{j\phi_\ell} s_{\ell,i} + b_i) s_{m,i}^* \right| = |e^{j\phi_\ell}\mu_{\ell,m} + b_m|$$

où $\mu_{\ell,m}$ est encore l'intercorrélation entre les séquences $\mathbf{s}_\ell$ et $\mathbf{s}_m$ et b_m un bruit blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle. En tant que modules d'une distribution gaussienne complexe non centrée de variance σ^2, $|x_\ell|$ suit une loi de Rice de paramètre $|e^{j\phi_\ell}\mu_{\ell,\ell}| = 1$ tandis que les $|x_m|$, $m \neq \ell$ suivent une loi de Rayleigh. Leurs densités de probabilité respectives sont données par

$$p(|x_\ell|/\mathbf{s}_\ell) = \frac{|x_\ell|}{\sigma^2} \exp\left(-\frac{|x_\ell|^2 + 1}{2\sigma^2}\right) I_0\left(\frac{|x_\ell|}{\sigma^2}\right)$$

et

$$p(|x_m|/\mathbf{s}_\ell) = \frac{|x_m|}{\sigma^2} \exp\left(-\frac{|x_m|^2}{2\sigma^2}\right) \quad \text{pour } m \neq \ell$$

La famille $\mathcal{A}$ est orthogonale, donc les variables $|x_m|$ sont indépendantes.

$$\begin{aligned} p(|\mathbf{x}|/\mathbf{s}_\ell) &= \prod_{m=1}^{M} p(|x_m|/\mathbf{s}_\ell) \\ &= \left(\prod_{m=1}^{M} \frac{|x_m|}{\sigma^2}\right) \exp\left(-\frac{1}{2\sigma^2}\right) \exp\left(-\sum_{m=1}^{M} \frac{|x_m|^2}{2\sigma^2}\right) I_0\left(\frac{|x_\ell|}{\sigma^2}\right) \end{aligned}$$

L'argument du logarithme de l'équation (4.11) devient

$$\frac{p(|\mathbf{x}|/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(|\mathbf{x}|/\mathbf{s}_k)} = \frac{\left(\prod_{m=1}^{M} \frac{|x_m|}{\sigma^2}\right) \exp\left(-\frac{1}{2\sigma^2}\right) \exp\left(-\sum_{m=1}^{M} \frac{|x_m|^2}{2\sigma^2}\right) I_0\left(\frac{|x_\ell|}{\sigma^2}\right)}{\sum_{k=1}^{M} \left(\prod_{m=1}^{M} \frac{|x_m|}{\sigma^2}\right) \exp\left(-\frac{1}{2\sigma^2}\right) \exp\left(-\sum_{m=1}^{M} \frac{|x_m|^2}{2\sigma^2}\right) I_0\left(\frac{|x_k|}{\sigma^2}\right)}$$

Des simplifications entraînent

$$\frac{p(|\mathbf{x}|/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(|\mathbf{x}|/\mathbf{s}_k)} = \frac{M I_0\left(\frac{|x_\ell|}{\sigma^2}\right)}{\sum_{k=1}^{M} I_0\left(\frac{|x_k|}{\sigma^2}\right)}$$

En reportant dans (4.11), on trouve

$$C = \sum_{\ell=1}^{M} \frac{1}{M} E_{|\mathbf{x}|/\mathbf{s}_\ell} \left[\log_2(M) - \log_2 \left\{ \sum_{k=1}^{M} \frac{I_0\left(\frac{|x_k|}{\sigma^2}\right)}{I_0\left(\frac{|x_\ell|}{\sigma^2}\right)} \right\} \right]$$

Comme précédemment, tous les termes de la somme sur ℓ sont symétriques. Le terme $\ell = 1$ suffit.

L'expression de la capacité du canal gaussien non cohérent admettant un alphabet $\mathcal{A}$ de M signaux orthogonaux en entrée s'écrit

$$C = \log_2(M) - E_{|\mathbf{x}|/\mathbf{s}_1}\left[\log_2\left\{\sum_{k=1}^{M}\frac{I_0\left(\frac{|x_k|}{\sigma^2}\right)}{I_0\left(\frac{|x_1|}{\sigma^2}\right)}\right\}\right] \tag{4.13}$$

4.4.4 Capacité des séquences corrélées

Les signaux de l'alphabet $\mathcal{A}$ sont maintenant corrélés. Les deux types de détection – cohérente et non cohérente – sont traités pour le canal gaussien. Dans le cas particulier du canal de Rayleigh, seule la réception non cohérente est présentée.

Capacité d'un canal cohérent

Le modèle de canal équivalent utilisé est encore le CANAL 2. L'alphabet $\mathcal{A}$ contient M séquences corrélées de longueur N. Si les séquences elles-mêmes sont utilisées dans le banc de corrélateurs, les sorties $(x_1, \ldots, x_M)$ ne sont pas indépendantes. L'émission de $\mathbf{s}_\ell$ entraîne une fois encore

$$\mathbf{r} = e^{j\phi_\ell}\mathbf{s}_\ell + \mathbf{b}$$

et les sorties des corrélateurs s'expriment ainsi

$$x_m = \sum_{i=1}^{N}(e^{j\phi_\ell}s_{\ell,i} + b_i)s^*_{m,i} = e^{j\phi_\ell}\mu_{\ell,m} + b_m$$

Les x_m suivent toujours une loi gaussienne complexe de moyenne $e^{j\phi_\ell}\mu_{\ell,m}$ et de variance σ^2 par composante réelle.

$$p(x_m/\mathbf{s}_\ell) = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{|x_m - e^{j\phi_\ell}\mu_{\ell,m}|^2}{2\sigma^2}\right)$$

Et la loi conjointe $p(\mathbf{x}/\mathbf{s}_\ell)$ doit être calculée directement.

$$p(\mathbf{x}/\mathbf{s}_\ell) = \frac{1}{\pi^M det(C_\mathbf{x})}\exp\left\{-(\mathbf{x} - m_{\mathbf{x}/\mathbf{s}_\ell})^H C_\mathbf{x}^{-1}(\mathbf{x} - m_{\mathbf{x}/\mathbf{s}_\ell})\right\}$$

où $m_{\mathbf{x}/\mathbf{s}_\ell} = (e^{j\phi_\ell}\mu_{\ell,1}, \ldots, e^{j\phi_\ell}\mu_{\ell,M})$ est le vecteur moyenne de la variable gaussienne complexe multidimensionnelle $\mathbf{x}/\mathbf{s}_\ell$ et $C_\mathbf{x} = cov(x_\ell, x_k)_{\ell,k=1,\ldots,M}$ est la matrice de covariance des variables gaussiennes complexes élémentaires $x_m, m = 1, \ldots, M$.

En reportant dans (4.11), et en simplifiant, nous obtenons

$$C = \frac{1}{M}\sum_{\ell=1}^{M} E_{\mathbf{x}/\mathbf{s}_\ell}\left[\log_2(M) - \log_2\left\{\sum_{k=1}^{M}\frac{\exp\left\{-(\mathbf{x}-m_{\mathbf{x}/\mathbf{s}_k})^H C_{\mathbf{x}}^{-1}(\mathbf{x}-m_{\mathbf{x}/\mathbf{s}_k})\right\}}{\exp\left\{-(\mathbf{x}-m_{\mathbf{x}/\mathbf{s}_\ell})^H C_{\mathbf{x}}^{-1}(\mathbf{x}-m_{\mathbf{x}/\mathbf{s}_\ell})\right\}}\right\}\right] \tag{4.14}$$

Contrairement au cas orthogonal, les termes ne sont plus symétriques, il faut tous les évaluer.

Il est possible de simplifier ce calcul en remarquant que la projection du signal reçu sur les M séquences de l'alphabet est inutile. La projection sur une base orthogonale de l'espace de dimension N fournit une statistique suffisante, le banc de corrélateurs est alors composé des N filtres correspondant aux N séquences d'Hadamard de longueur N. La réduction de complexité sera d'autant plus importante que l'on utilisera un nombre de séquences M bien plus grand que leur longueur N.

On note $\{\boldsymbol{\psi}_n\}_{n=1,\dots,N}$ la base des N séquences d'Hadamard de longueur N. Les N sorties de corrélateurs sont données par

$$x_n = \sum_{i=1}^{N}(e^{j\phi_\ell}s_{\ell,i} + b_i)\psi_{n,i}^* = e^{j\phi_\ell}s_\ell^n + b_n \quad n = 1,\dots,N \tag{4.15}$$

où s_ℓ^n est la projection de la séquence $\mathbf{s}_\ell$ sur le $n$ième vecteur de la base orthogonale ; $\mathbf{s}_\ell = \sum_{n=1}^{N} s_\ell^n \boldsymbol{\psi}_n$. De cette façon, les x_n sont des variables aléatoires indépendantes et suivent une loi gaussienne de moyenne $e^{j\phi_\ell}s_\ell^n$ et de variance σ^2 par composante réelle.

Comme dans le cas des signaux orthogonaux, il est possible de s'affranchir du terme $e^{j\phi_\ell}$ connu du récepteur.

La loi conjointe $p(\mathbf{x}/\mathbf{s}_\ell)$ s'écrit

$$\begin{aligned} p(\mathbf{x}/\mathbf{s}_\ell) &= \prod_{n=1}^{N} p(x_n/\mathbf{s}_\ell) \\ &= \left(\frac{1}{2\pi\sigma^2}\right)^N \exp\left(-\frac{\sum_{n=1}^{N}|x_n - s_\ell^n|^2}{2\sigma^2}\right) \end{aligned}$$

L'argument du logarithme de l'équation (4.11) devient

$$\frac{p(\mathbf{x}/\mathbf{s}_\ell)}{\sum_{k=1}^{M}\frac{1}{M}p(\mathbf{x}/\mathbf{s}_k)} = \frac{M\left(\frac{1}{2\pi\sigma^2}\right)^N \exp\left(-\frac{\sum_{n=1}^{N}|x_n-s_\ell^n|^2}{2\sigma^2}\right)}{\sum_{k=1}^{M}\left(\frac{1}{2\pi\sigma^2}\right)^N \exp\left(-\frac{\sum_{n=1}^{N}|x_n-s_k^n|^2}{2\sigma^2}\right)}$$

Un calcul direct conduit à

$$\begin{aligned}
\frac{p(\mathbf{x}/\mathbf{s}_\ell)}{\sum_{k=1}^{M}\frac{1}{M}p(\mathbf{x}/\mathbf{s}_k)} &= \frac{M\exp\left(\frac{\sum_{n=1}^{N}|s_\ell^n|^2}{2\sigma^2}\right)\exp\left(\frac{\sum_{n=1}^{N}Re(x_n s_\ell^n)}{\sigma^2}\right)}{\sum_{k=1}^{M}\exp\left(\frac{\sum_{n=1}^{N}|s_k^n|^2}{2\sigma^2}\right)\exp\left(\frac{\sum_{n=1}^{N}Re(x_n s_k^n)}{\sigma^2}\right)} \\
&= \frac{M}{\sum_{k=1}^{M}\exp\left(\frac{\sum_{n=1}^{N}Re[x_n(s_k^n - s_\ell^n)]}{\sigma^2}\right)}
\end{aligned}$$

En effet $\sum_{n=1}^{N}|s_k^n|^2$ définit l'énergie de la séquence $\mathbf{s}_k$ et toutes les séquences sont de même énergie.

Finalement, en reportant dans l'expression (4.11), on obtient la capacité du canal gaussien cohérent pour un alphabet $\mathcal{A}$ de M signaux corrélés en entrée

$$C = \frac{1}{M}\sum_{\ell=1}^{M}E_{\mathbf{x}/\mathbf{s}_\ell}\left[\log_2(M) - \log_2\left\{\exp\left(\frac{\sum_{n=1}^{N}Re[x_n(s_k^n - s_\ell^n)]}{\sigma^2}\right)\right\}\right] \tag{4.16}$$

Cette deuxième expression est celle utilisée pour les simulations.

Capacité d'un canal non cohérent

Intéressons-nous enfin au cas d'une détection non cohérente. Si nous conservons un modèle de canal qui englobe le démodulateur, c'est-à-dire de type CANAL 2, comme précédemment en détection cohérente, nous sommes confrontés à deux problèmes. La projection du signal reçu sur les M signaux corrélés ramène au cas des signaux orthogonaux avec détection non cohérente : les modules des sorties du banc de corrélateurs s'expriment comme suit

$$|x_m| = \left|\sum_{i=1}^{N}(e^{j\phi_\ell}s_{\ell,i} + b_i)s_{m,i}^*\right| = |e^{j\phi_\ell}\mu_{\ell,m} + b_m|$$

Les variables $|x_m|$ ne sont pas indépendantes et chaque $|x_m|$ suit une loi de Rice de paramètre $|e^{j\phi_\ell}\mu_{\ell,m}| = |\mu_{\ell,m}|$. Il faut par conséquent trouver la loi conjointe de M variables de Rice pour mener à bien le calcul de la capacité. Ce problème est particulièrement délicat à résoudre.

Par ailleurs, une projection sur la base orthogonale des N séquences d'Hadamard ne dispense pas de s'intéresser au module des sorties du banc de corrélateurs. Malheureusement, contrairement au cas cohérent, la statistique alors obtenue n'est plus suffisante.

Nous suggérons donc – de manière parfaitement équivalente – de calculer la capacité directement en sortie du canal. Cela correspond au modèle de canal désigné par CANAL 1 dans la figure 4.3.

Émettre $\mathbf{s}_\ell$ entraîne une fois encore

$$\mathbf{r} = \alpha e^{j\phi_\ell}\mathbf{s}_\ell + \mathbf{b}$$

α est le gain gaussien complexe du canal de moyenne $\sqrt{\frac{K}{K+1}}$ et de variance $\frac{1}{2(K+1)}$. Pour le canal gaussien, $K \to \infty$; pour le canal de Rayleigh, $K = 0$ [21]. $K \geq 0$ est le paramètre de Rice défini dans [43]. $\mathbf{b} = (b_1, \ldots, b_N)$ est un vecteur de bruit où chaque variable b_n suit une loi gaussienne complexe centrée de variance σ^2 par composante réelle.

L'équation (4.10) représente la forme la plus générale de la capacité d'un canal non cohérent admettant $X = \mathbf{s}_\ell \in \mathcal{A}$ comme entrée et $Y = \mathbf{r}$ comme sortie. Il faut évaluer $p(\mathbf{r}/\mathbf{s}_\ell)$. On définit $\boldsymbol{\theta} = (\alpha, \phi_\ell)$ comme représentant l'état du canal. Lorsque la détection est non cohérente, $\boldsymbol{\theta}$ n'est pas estimé. Alors, en moyennant sur α et ϕ_ℓ

$$p(\mathbf{r}/\mathbf{s}_\ell) = E_{\boldsymbol{\theta}}\left[p_{\boldsymbol{\theta}}(\mathbf{r}/\mathbf{s}_\ell)\right] \tag{4.17}$$

On obtient [21]

$$p(\mathbf{r}/\mathbf{s}_\ell) \quad = \quad \frac{1}{\pi^N |\Sigma_\mathbf{r}|} \exp\left(-\mathbf{r}\Sigma_\mathbf{r}^{-1}\mathbf{r}^H - \bar{\mathbf{r}}\Sigma_\mathbf{r}^{-1}\bar{\mathbf{r}}^H\right) I_0\left(2\left|\bar{\mathbf{r}}\Sigma_\mathbf{r}^{-1}\mathbf{r}^H\right|\right) \tag{4.18}$$

où

$$\bar{\mathbf{r}} = \sqrt{\frac{K}{K+1}}\mathbf{s}_\ell \quad et \quad \Sigma_\mathbf{r} = \frac{1}{K+1}\mathbf{s}_\ell^H \mathbf{s}_\ell + 2\sigma^2 I_N$$

I_N est la matrice idendité de dimension N et on remarquera que $\Sigma_\mathbf{r} = \Sigma_{\mathbf{r}/\mathbf{s}_\ell}$.

Pour le canal gaussien, $K \to \infty$. Alors $\bar{\mathbf{r}} = \mathbf{s}_\ell$ et $\Sigma_\mathbf{r} = \sigma^2 I_N$. L'équation (4.18) devient

$$p(\mathbf{r}/\mathbf{s}_\ell) \quad = \quad \frac{1}{(2\pi\sigma^2)^N} \exp\left(-\frac{\mathbf{r}\mathbf{r}^H + \mathbf{s}_\ell\mathbf{s}_\ell^H}{2\sigma^2}\right) I_0\left(\frac{|\mathbf{s}_\ell\mathbf{r}^H|}{\sigma^2}\right) \tag{4.19}$$

Plus précisément,

$$p(\mathbf{r}/\mathbf{s}_\ell) \quad = \quad \frac{1}{(2\pi\sigma^2)^N} \exp\left(-\frac{||\mathbf{r}||^2 + ||\mathbf{s}_\ell||^2}{2\sigma^2}\right) I_0\left(\frac{\left|\sum_{i=1}^N s_{\ell,i} r_i^*\right|}{\sigma^2}\right)$$

$s_{\ell,i}$ et r_i désignent la composante numéro i des séquences $\mathbf{s}_\ell$ et $\mathbf{r}$ respectivement.

L'argument du logarithme dans l'équation (4.10) prend la forme

$$\frac{p(\mathbf{r}/\mathbf{s}_\ell)}{\sum_{k=1}^M \frac{1}{M} p(\mathbf{r}/\mathbf{s}_k)} \quad = \quad \frac{M\frac{1}{(2\pi\sigma^2)^N} \exp\left(-\frac{||\mathbf{r}||^2 + ||\mathbf{s}_\ell||^2}{2\sigma^2}\right) I_0\left(\frac{\left|\sum_{i=1}^N s_{\ell,i} r_i^*\right|}{\sigma^2}\right)}{\sum_{k=1}^M \frac{1}{(2\pi\sigma^2)^N} \exp\left(-\frac{||\mathbf{r}||^2 + ||\mathbf{s}_k||^2}{2\sigma^2}\right) I_0\left(\frac{\left|\sum_{i=1}^N s_{k,i} r_i^*\right|}{\sigma^2}\right)}$$

Après simplifications, on a

$$\frac{p(\mathbf{r}/\mathbf{s}_\ell)}{\sum_{k=1}^M \frac{1}{M} p(\mathbf{r}/\mathbf{s}_k)} \quad = \quad \frac{M I_0\left(\frac{\left|\sum_{i=1}^N s_{\ell,i} r_i^*\right|}{\sigma^2}\right)}{\sum_{k=1}^M I_0\left(\frac{\left|\sum_{i=1}^N s_{k,i} r_i^*\right|}{\sigma^2}\right)}$$

En reportant dans l'équation (4.10), nous obtenons la capacité d'un canal gaussien non cohérent admettant un alphabet $\mathcal{A}$ de M séquences corrélées en entrée

$$C = \log_2(M) - \sum_{\ell=1}^{M} \frac{1}{M} E_{\mathbf{r}/\mathbf{s}_\ell} \left[\log_2 \left\{ \sum_{k=1}^{M} \frac{I_0\left(\frac{|\sum_{i=1}^{N} s_{k,i} r_i^*|}{\sigma^2}\right)}{I_0\left(\frac{|\sum_{i=1}^{N} s_{\ell,i} r_i^*|}{\sigma^2}\right)} \right\} \right] \tag{4.20}$$

Pour le canal de Rayleigh, $K = 0$. Alors $\bar{\mathbf{r}} = 0$ et $\Sigma_\mathbf{r} = \Sigma_{\mathbf{r}/\mathbf{s}_\ell} = \mathbf{s}_\ell^H \mathbf{s}_\ell + 2\sigma^2 I_N$. L'équation (4.18) devient

$$p(\mathbf{r}/\mathbf{s}_\ell) = \frac{1}{\pi^N |\mathbf{s}_\ell^H \mathbf{s}_\ell + 2\sigma^2 I_N|} \exp\left(-\mathbf{r}(\mathbf{s}_\ell^H \mathbf{s}_\ell + 2\sigma^2 I_N)^{-1} \mathbf{r}^H\right) \tag{4.21}$$

Alors, l'argument du logarithme de l'équation (4.10) devient

$$\frac{p(\mathbf{r}/\mathbf{s}_\ell)}{\sum_{k=1}^{M} \frac{1}{M} p(\mathbf{r}/\mathbf{s}_k)} = \frac{\frac{M}{\pi^N |\Sigma_{\mathbf{r}/\mathbf{s}_\ell}|} \exp\left(-\mathbf{r}\Sigma_{\mathbf{r}/\mathbf{s}_\ell}^{-1} \mathbf{r}^H\right)}{\sum_{k=1}^{M} \frac{1}{\pi^N |\Sigma_{\mathbf{r}/\mathbf{s}_k}|} \exp\left(-\mathbf{r}\Sigma_{\mathbf{r}/\mathbf{s}_k}^{-1} \mathbf{r}^H\right)}$$

Après simplications et en reportant dans (4.10), la capacité d'un canal de Rayleigh non cohérent admettant une famille $\mathcal{A}$ de M séquences corrélées en entrée est donnée par

$$C = \log_2(M) - \sum_{\ell=1}^{M} \frac{1}{M} E_{\mathbf{r}/\mathbf{s}_\ell} \left[\log_2 \left\{ \sum_{k=1}^{M} \frac{|\Sigma_{\mathbf{r}/\mathbf{s}_\ell}|}{|\Sigma_{\mathbf{r}/\mathbf{s}_k}|} \frac{\exp\left(-\mathbf{r}\Sigma_{\mathbf{r}/\mathbf{s}_k}^{-1} \mathbf{r}^H\right)}{\exp\left(-\mathbf{r}\Sigma_{\mathbf{r}/\mathbf{s}_\ell}^{-1} \mathbf{r}^H\right)} \right\} \right] \tag{4.22}$$

Finalement, on remarquera que la capacité d'un canal de Rice non cohérent admettant un alphabet $\mathcal{A}$ de M séquences corrélés en entrée peut être obtenue en reportant l'expression (4.18) dans l'équation (4.10).

4.4.5 Résultats numériques

Les différentes expressions de capacité établies ci-dessus ont été utilisées pour les simulations. Les moyennes du type

$$E_{\mathbf{y}_i/\mathbf{s}_\ell} \left[\log_2 \left\{ \frac{p(\mathbf{y}_i/\mathbf{s}_\ell)}{p(\mathbf{y}_i)} \right\} \right]$$

où $\mathbf{y}_i = \mathbf{r}$ ou $\mathbf{x}$, ont étés évaluées par intégration numérique (méthode de Monte Carlo). Les résultats sont classés par type d'alphabet utilisé.

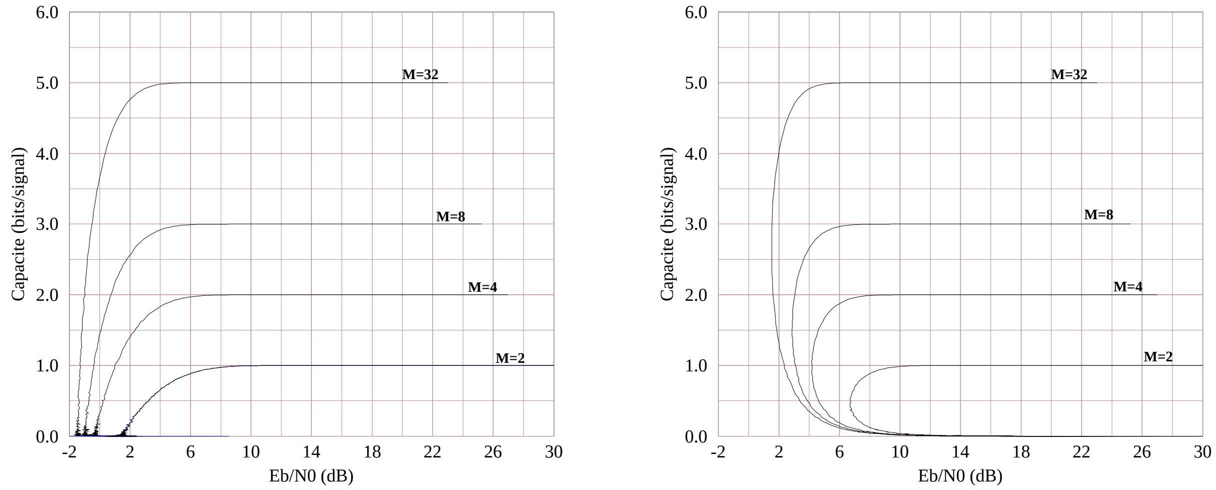


Fig. 4.4 – Capacité du canal gaussien en bits/signal pour des alphabets de signaux orthogonaux en entrée. Détection cohérente (gauche) et non cohérente (droite).

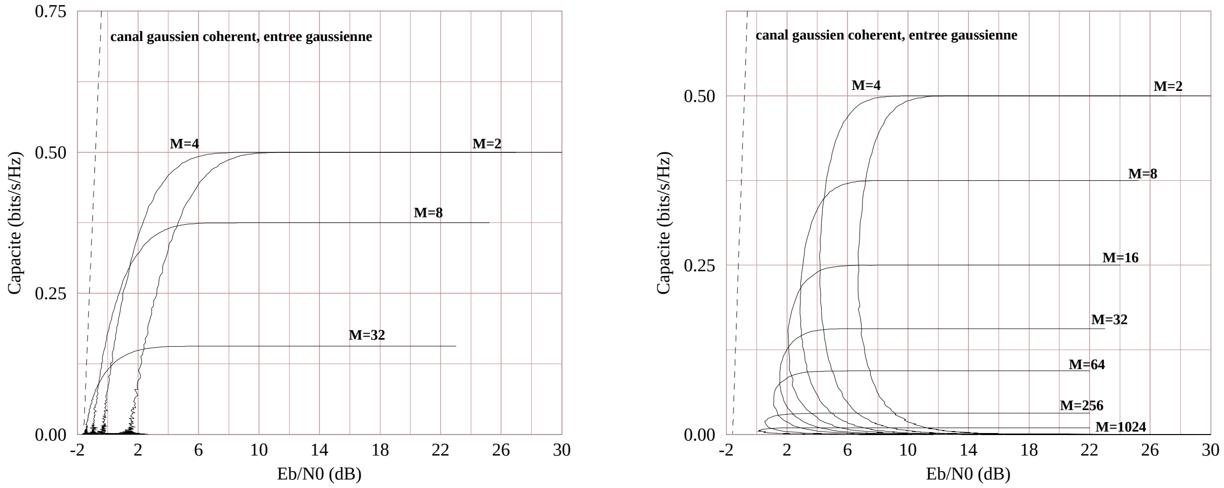


Fig. 4.5 – Capacité du canal gaussien en bits/s/Hz pour des alphabets de signaux orthogonaux en entrée. Détection cohérente (gauche) et non cohérente (droite).

Signaux orthogonaux

Les figures 4.4 et 4.5 présentent les capacités du canal gaussien, avec détection cohérente ou non, admettant en entrée un alphabet de M signaux orthogonaux, respectivement en bits/signal et en bits/s/Hz. Quel que soit le type de détection choisi, le fait d'utiliser des alphabets de plus en plus grands permet de se rapprocher de la capacité du canal gaussien cohérent avec entrée gaussienne. Par ailleurs, les courbes de capacité obtenues pour la détection non cohérente sont une enveloppe des courbes de taux de coupure données dans [57]. On observe bien le même phénomène : il existe un rendement optimal pour chaque taille M d'alphabet. Pour un rapport signal-à-bruit variant de 1 dB environ, on dispose même d'une plage de rendements acceptables. Ce comportement est directement lié à la non linéarité du récepteur non cohérent.

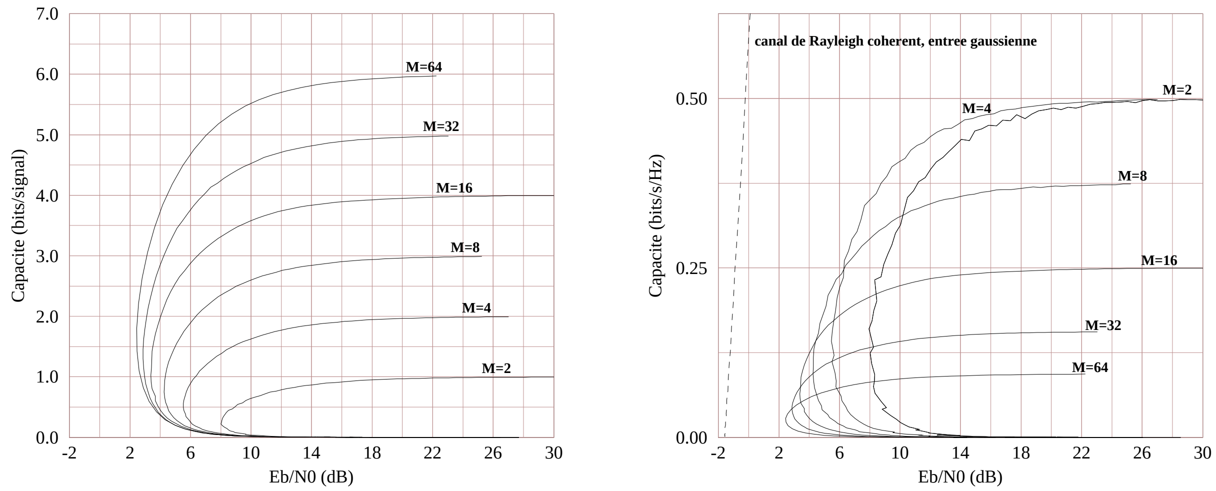


FIG. 4.6 – Capacité du canal de Rayleigh en bits/signal (gauche) et en bits/s/Hz (droite) pour des alphabets de signaux orthogonaux en entrée. Détection non cohérente.

Les performances de ces mêmes alphabets sur canal de Rayleigh non cohérent sont illustrées figure 4.6. Ici encore, l'augmentation de la taille de l'alphabet M permet de tendre vers la capacité du canal de Rayleigh cohérent avec entrée gaussienne. Avec une famille de $M = 64$ signaux, on se situe au mieux à 4 dB de cette capacité alors que sur canal gaussien, l'alphabet de $M = 1024$ signaux est à 1.8 dB seulement de la capacité maximale.

Cependant, les alphabets de séquences orthogonales sont limités à une efficacité spectrale de 0.5 bits/s/Hz. En utilisant des séquences corrélées, nous cherchons à conserver, voire à améliorer les capacités envisageables tout en garantissant une efficacité spectrale bien meilleure pour une taille d'alphabet et/ou une longueur de séquences données.

La suite des résultats concerne des ensembles de signaux corrélés.

Séquences binaires corrélées

Dans un premier temps, nous relâchons seulement la contrainte d'orthogonalité. On peut facilement choisir aléatoirement M séquences de longueur N parmi les 2^N séquences binaires possibles pour construire des alphabets de $M > N$ séquences binaires corrélées. L'efficacité spectrale obtenue est supérieure à 0.5 bits/s/Hz. Un exemple est présenté figure 4.7 pour des séquences de longueur $N = 8$ avec détection cohérente en bits/signal et en bits/s/Hz respectivement. À des fins de comparaison, apparaissent aussi sur ces graphiques les performances d'ensemble de signaux orthogonaux – ici, les familles d'Hadamard de longueur $N = 2$ et $N = 8$ –; ainsi que la famille composée des 8 séquences réelles de longueur $N = 2$ précédemment nommée famille 1.

Il est manifeste que l'on peut alors atteindre des efficacités spectrales plus importantes mais

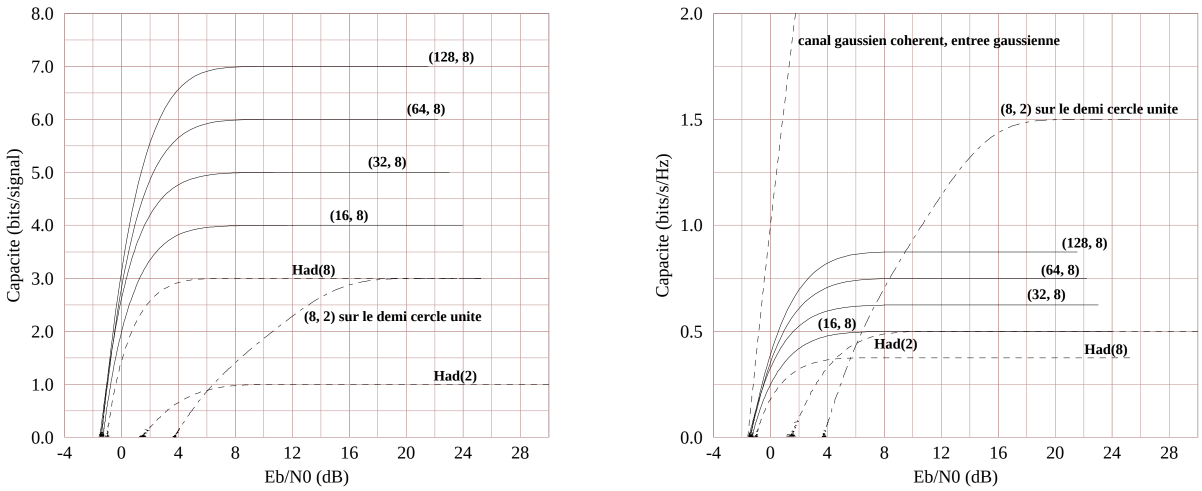


Fig. 4.7 – Capacité du canal gaussien en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux binaires corrélés en entrée. Détection cohérente.

pour de fortes valeurs du rapport signal-à-bruit seulement. Voyons comment l'utilisation de séquences corrélées à composantes non binaires peut nous conduire à une meilleure capacité pour de plus faibles rapports signal-à-bruit.

Séquences construites à partir de signaux PSK

La construction de ces séquences est décrite au paragraphe 4.3.1. Sur les figures 4.8 et 4.9, on peut comparer leurs performances pour des longueurs différentes $N = 2, 4, 8$, en bits/signal et en bits/s/Hz, pour le canal gaussien et le canal de Rayleigh respectivement. La détection est non cohérente.

D'une part, l'augmentation de la taille M de l'alphabet à longueur N fixe conduit à des efficacités spectrales plus grandes. D'autre part, quand la longueur N augmente, les familles de courbes pour N donné se rapprochent de la capacité du canal à entrée gaussienne. Cette constatation est valable pour les deux types de canaux envisagés et est visible sur les courbes pour lesquelles la capacité est donnée en bits/s/Hz. Remarquons aussi que par construction le cas $(N, M = N)$ nous ramène aux séquences d'Hadamard de longueur N. On notera cependant que les courbes correspondant aux familles de plus de 16 séquences sont très “écrasées” sur le haut, et le gain potentiel en efficacité spectrale sera atteint uniquement pour de très fortes valeurs du rapport signal-à-bruit. Il sera donc plus judicieux d'utiliser ce type de séquences lorsque l'on aura besoin d'alphabets de petites tailles, soit $M = 4, 8$.

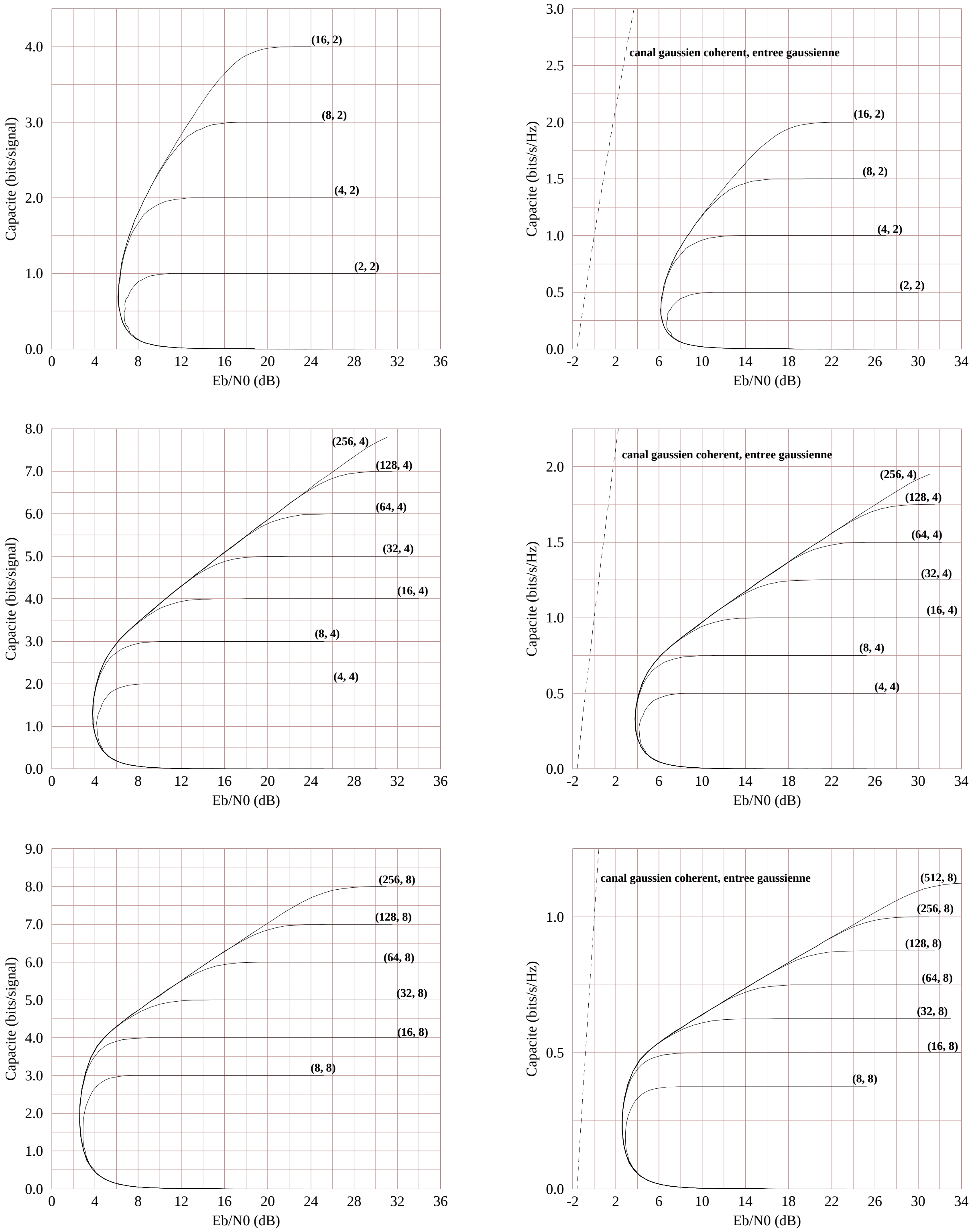


Fig. 4.8 – Capacité du canal gaussien non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux de type PSK corrélés de longueur 2, 4 et 8 en entrée.

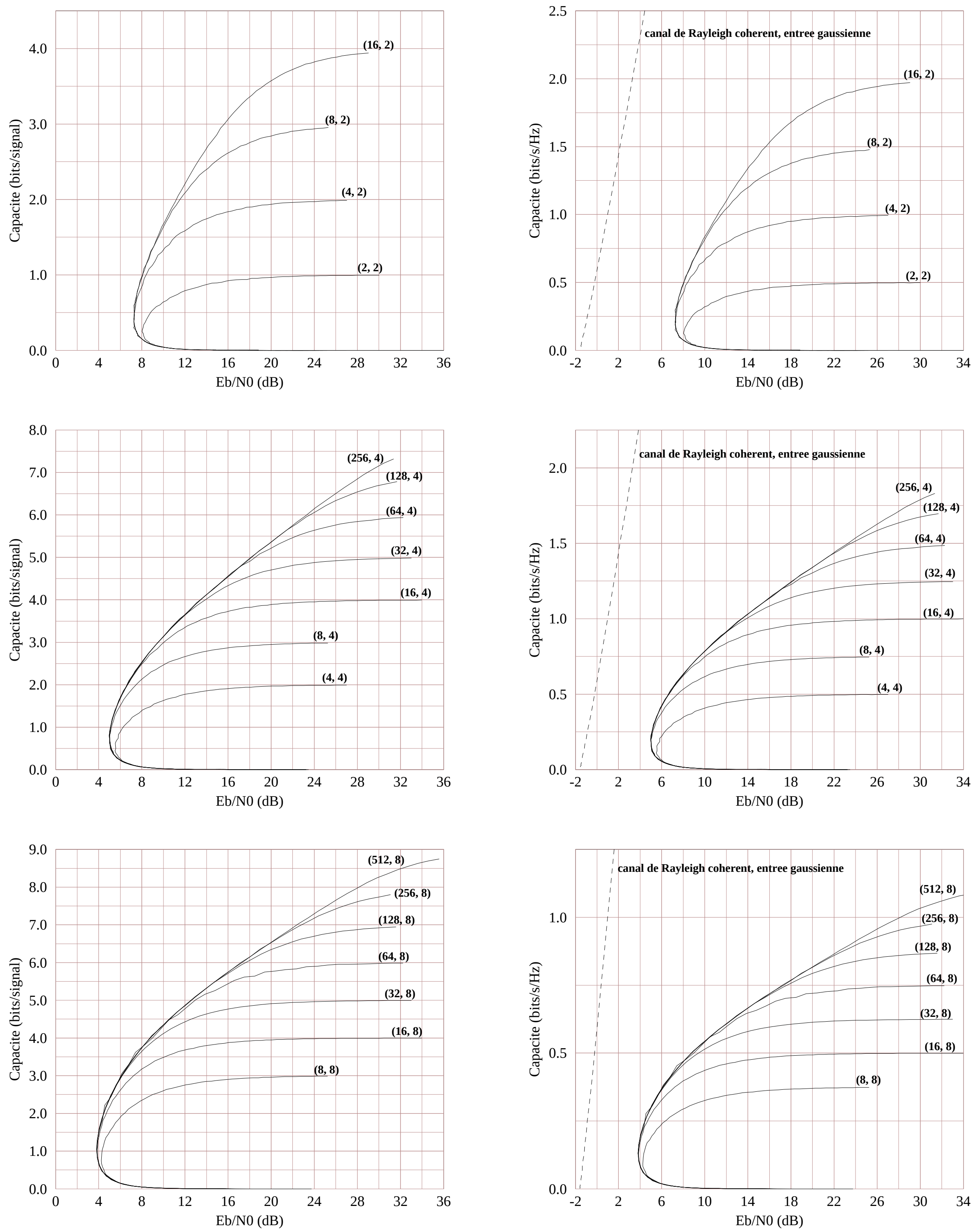


Fig. 4.9 – Capacité du canal de Rayleigh non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux de type PSK corrélés de longueur 2, 4 et 8 en entrée.

Séquences complexes purement aléatoires

Tous les résultats relatifs aux séquences complexes corrélées choisies aléatoirement sont rassemblés sur les figures 4.10 et 4.11. Bien que les principaux commentaires possibles soient similaires à ce qui a été dit pour les séquences de type PSK, on observe un meilleur comportement des séquences purement aléatoires pour des tailles d'alphabets plus importantes, $M = 32$ à 256, et ce d'autant plus que la longueur N est grande. Par exemple, une famille de 256 séquences de longueur 8 atteint une capacité de 0.5 bits/s/Hz avec une perte de seulement 3 dB par rapport à la capacité du canal gaussien cohérent alors que la famille $(256, 8)$ de séquences de type PSK et la famille d'Hadamard de longueur 4 atteignent cette même valeur de la capacité avec une perte de 6 et 8 dB respectivement.

Lorsque la détection est non cohérente, l'utilisation de familles de signaux orthogonaux de plus en plus longs permettra de tendre vers la capacité théorique du canal gaussien pour des efficacités spectrales très petites. En revanche, si l'on souhaite tendre vers la capacité du canal gaussien tout en travaillant à des efficacités spectrales raisonnables, il faudra utiliser des familles de plus en plus grandes de signaux corrélés de plus en plus longs. Cette dernière remarque est parfaitement illustrée par les figures 4.12 et 4.13 sur canal gaussien et canal de Rayleigh respectivement. Nous y avons tracé les enveloppes des courbes de capacité obtenues pour différentes valeurs de N en fonction du rapport signal-à-bruit. L'enveloppe correspondant aux familles de séquences orthogonales y figure également, ainsi que la capacité du canal cohérent choisi avec entrée gaussienne. Ce dernier graphique constitue une limite supérieure de la capacité. Toutes les courbes sont une fois encore données en bits/s/Hz.

Une famille de $M = 1024$ séquences corrélées de longueur $N = 8$ atteint ainsi une capacité de 1 bits/s/Hz au prix de 3 dB de perte par rapport à la capacité du canal gaussien cohérent, et 0.5 bits/s/Hz avec 3.5 dB de perte par rapport à la capacité du canal de Rayleigh cohérent. Sur les deux figures, il est clair qu'aucun alphabet de séquences orthogonales ne pourra dépasser une capacité de 0.5 bits/s/Hz. Ce maximum est atteint par les familles d'Hadamard $N = 2, 4$ mais pour des valeurs de rapport signal-à-bruit très éloignées des capacités des canaux cohérents (8 dB sur canal gaussien et 16 dB sur canal de Rayleigh).

Du point de vue de la capacité à proprement parler, l'utilisation de familles de grandes tailles s'impose. Si l'on veut se rapprocher du cas cohérent, c'est bien le nombre de séquences qui importe. Un compromis entre l'augmentation de l'efficacité spectrale et la complexité de mise en œuvre de l'alphabet devra donc être fait.

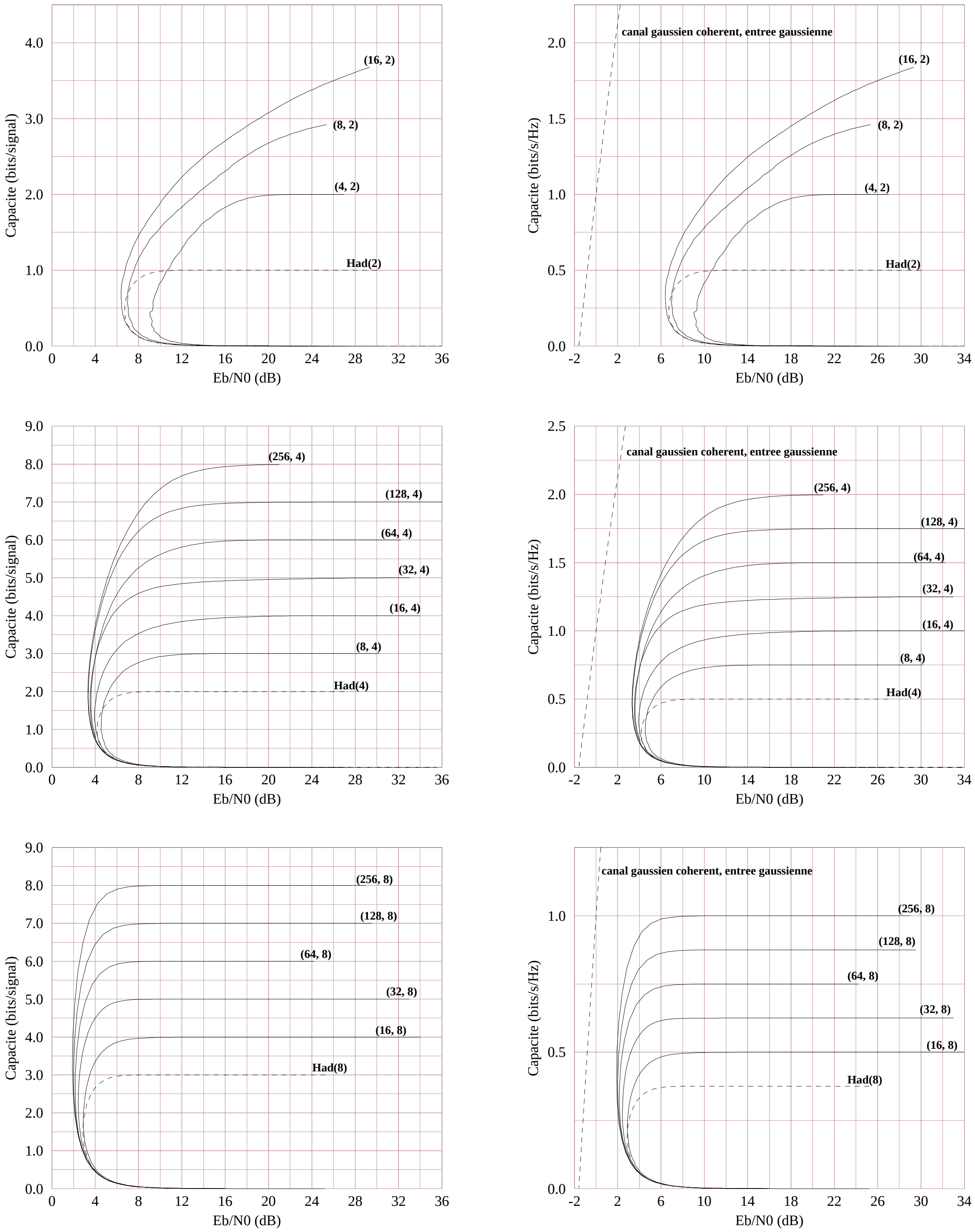


Fig. 4.10 – Capacité du canal gaussien non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux complexes corrélés de longueur 2, 4 et 8 en entrée.

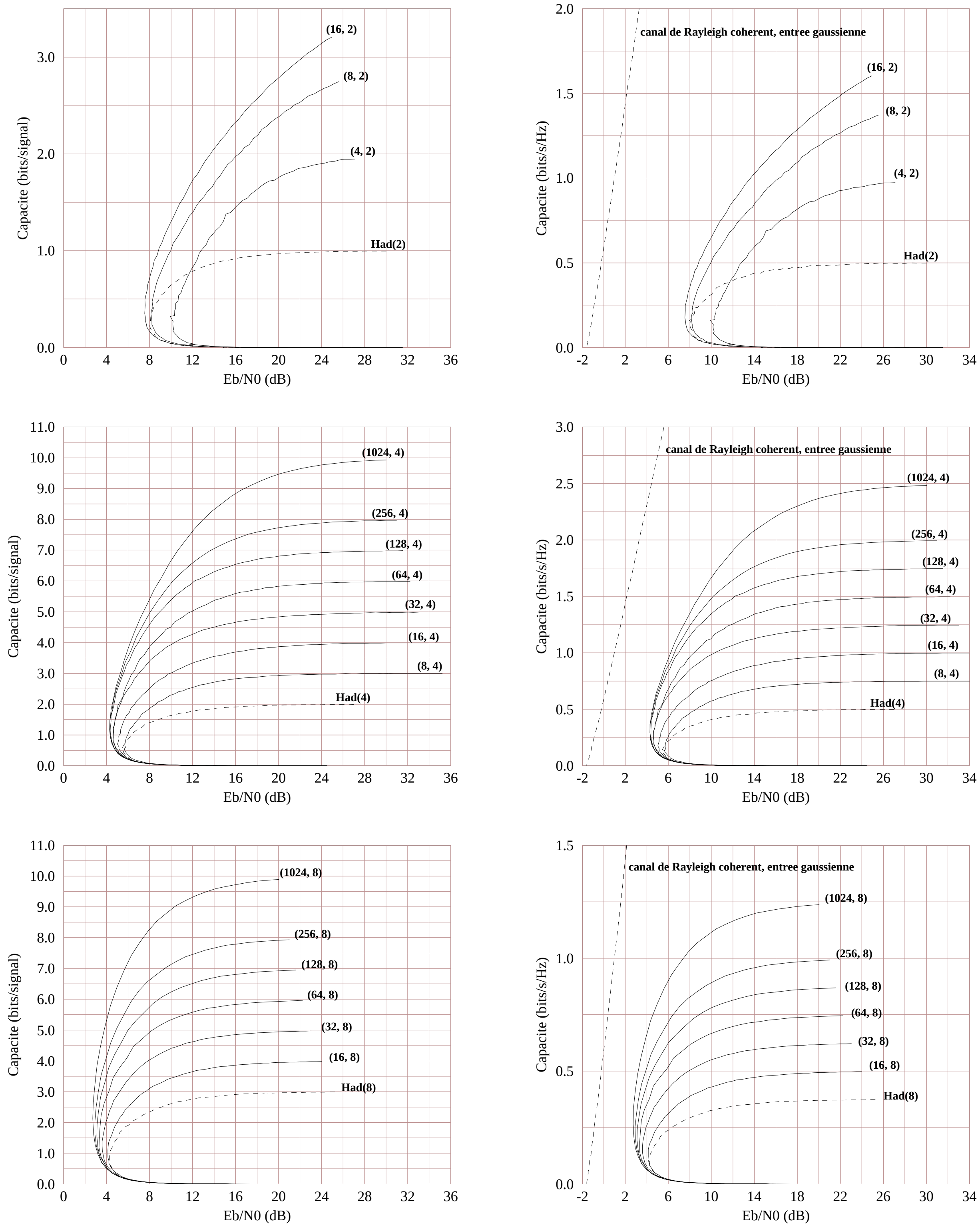


Fig. 4.11 – Capacité du canal de Rayleigh non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de signaux complexes corrélés de longueur 2, 4 et 8 en entrée.

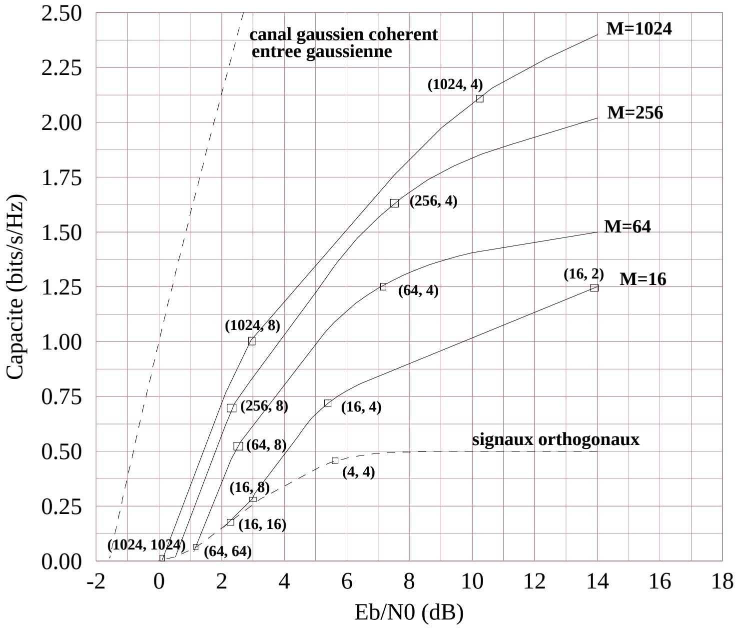


Fig. 4.12 – Enveloppe des capacités en bits/s/Hz du canal gaussien non cohérent pour des alphabets de M séquences complexes corrélées de longueur N en entrée.

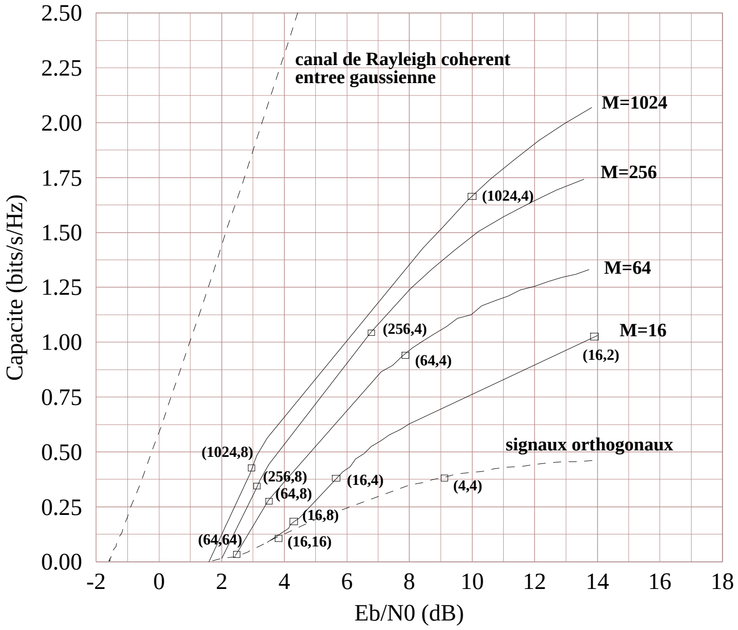


Fig. 4.13 – Enveloppe des capacités en bits/s/Hz du canal de Rayleigh non cohérent pour des alphabets de M séquences complexes corrélées de longueur N en entrée.

Séquences de Marzetta

Enfin, la figure 4.15 illustre les performances des séquences de type Marzetta. Rappelons que, de manière asymptotique, ces séquences sont celles qui atteignent la capacité du canal de Rayleigh à entrées et sorties multiples avec détection non cohérente. En effet, le phénomène d"'écrasement" observé sur le haut des courbes pour les autres séquences à des degrés plus ou moins importants est moins marqué. Cependant, on pourra remarquer que leurs performances sont en tout point similaires à celles des séquences complexes purement aléatoires, du moins pour les tailles d'ensemble M et les longueurs N considérées. Les séquences purement aléatoires constituent donc une bonne manière d'approcher la capacité quel que soit le type de canal choisi avec l'hypothèse d'une détection non cohérente.

4.5 Exemple : décodage itératif de séquences non orthogonales codées

Nous souhaitons comparer des exemples pratiques aux résultats théoriques présentés dans les paragraphes précédents. Pour cela, nous choisissons une famille $\mathcal{A}$ de M séquences de longueur N parmi les différentes constructions envisagées. Utilisée sans codage, cette famille permet d'atteindre au mieux une efficacité spectrale égale à

$$\eta = \frac{\log_2(M)}{N} \text{ bits/s/Hz}$$

Lorsque l'on rajoute un schéma de codage de rendement R, la relation $C = R \times \eta$ existe entre l'efficacité spectrale, la capacité C du canal obtenue avec la famille $\mathcal{A}$ en entrée et le rendement du code. Le choix de la famille conditionne η. Il est donc simple d'en déduire le rendement du code que nous devons considérer.

Le modèle de transmission est identique à celui explicité au paragraphe 3.3.2. Seul l'émetteur est légèrement modifié puisque nous n'utilisons plus de modulateur Q-FSK. La figure 4.14 illustre les quelques modifications apportées à la BICM. Par ailleurs, le banc de filtres adaptés est remplacé par un banc de corrélateurs.

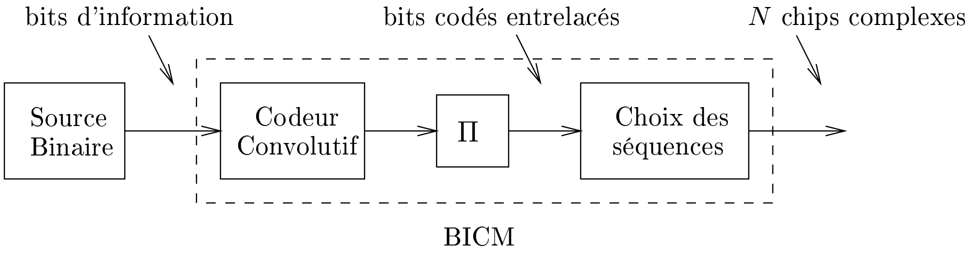


FIG. 4.14 – Famille codée de séquences non orthogonales : modèle de l'émetteur.

En accord avec les notations utilisées tout au long de ce chapitre, les M séquences de la famille $\mathcal{A}$ s'écrivent $\{\mathbf{s}_1, \ldots, \mathbf{s}_M\}$ où $\mathbf{s}_m = (s_{m,1}, \ldots, s_{m,N})$.

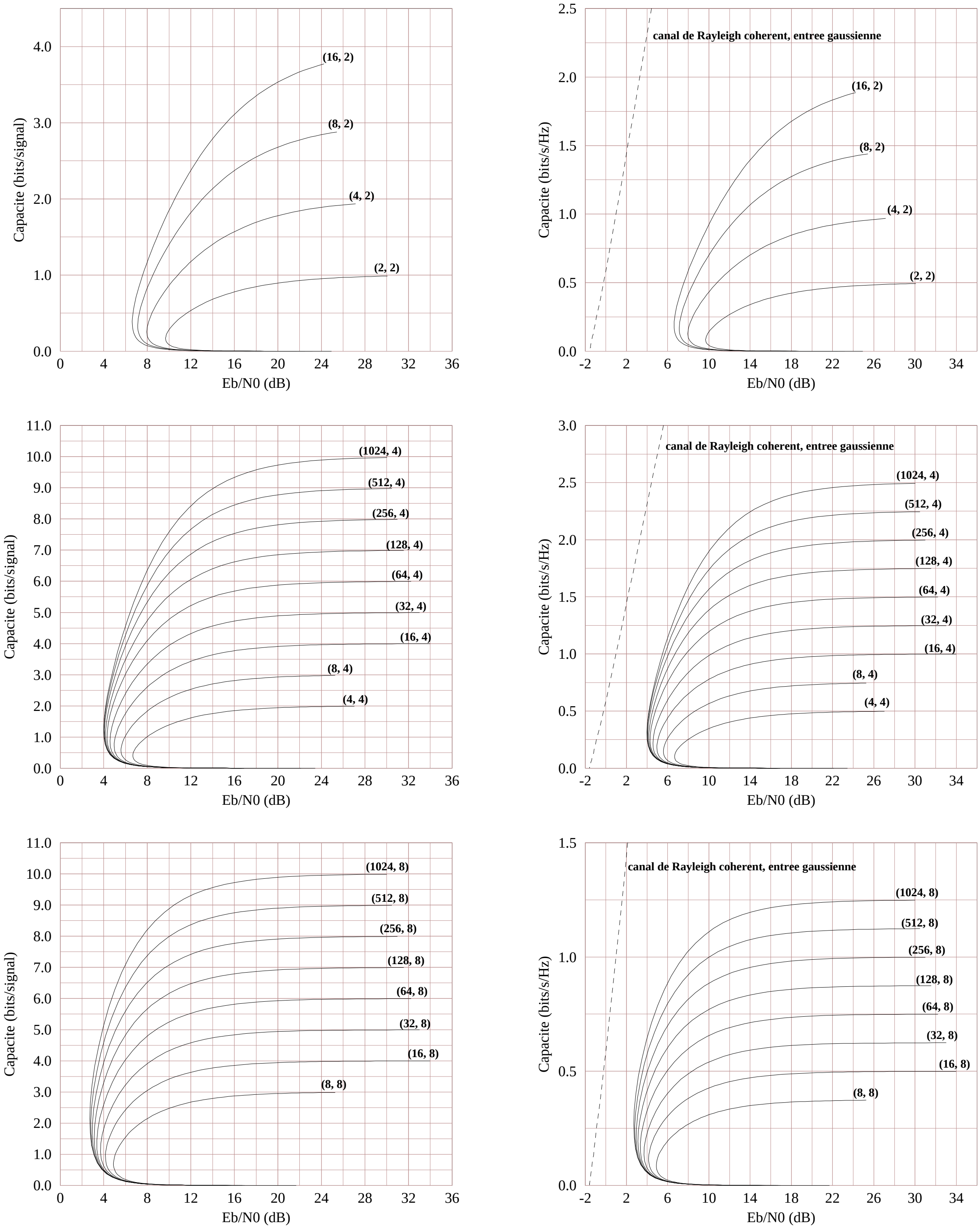


Fig. 4.15 – Capacité du canal de Rayleigh non cohérent en bits/signal (gauche) et bits/s/Hz (droite) pour des alphabets de séquences complexes corrélées de type Marzetta de longueur 2, 4 et 8 en entrée.

Le canal sans mémoire est toujours caractérisé par une phase aléatoire ϕ uniformément distribuée sur $[0, 2\pi[$, inconnue du récepteur puisque la détection est non cohérente, un gain α et un bruit $\mathbf{b}$ additif blanc gaussien complexe de moyenne nulle et de variance σ^2 par composante réelle. Sur canal gaussien, la constante α est supposée égale à 1 et sur canal à évanouissements, α suit une loi de Rayleigh ; $p(\alpha) = 2\alpha e^{-\alpha^2}$ et $E[\alpha^2] = 1$.

Si la séquence $\mathbf{s}_\ell$ est émise, on reçoit $\mathbf{r} = \alpha e^{j\phi_\ell}\mathbf{s}_\ell + \mathbf{b}$ où chaque composante ou chip du vecteur $\mathbf{r}$ est donnée par $r_n = \alpha e^{j\phi_\ell} s_{\ell,n} + b_n$. En sortie du banc de corrélateurs, on dispose d'un vecteur de M corrélations $\mathbf{x} = (x_1, \ldots, x_M)$ avec $x_m = \sum_{n=1}^{N} r_n s_{m,n}^*$. Afin de calculer les M APP des séquences (bloc "Calcul des APP signaux"), nous utilisons la formule directe de la densité de probabilité de l'observation $\mathbf{r}$ conditionnellement à l'émission de la séquence $\mathbf{s}_\ell$ donnée par l'équation (4.18) [21]. Dans le cas du canal gaussien, $p(\mathbf{r}/\mathbf{s}_\ell)$ est fonction des sorties $\{x_m\}$ du banc de corrélateurs (équation (4.19)), dans le cas du canal de Rayleigh, l'expression est donnée par l'équation (4.21).

L'APP d'une séquence $\mathbf{s}_\ell$ est définie par $\mathrm{APP}(\mathbf{s}_\ell) = p(\mathbf{s}_\ell/\mathbf{r})$. L'application directe de la loi de Bayes permet de récrire

$$\mathrm{APP}(\mathbf{s}_\ell) \propto p(\mathbf{r}/\mathbf{s}_\ell)$$

puisque toutes les séquences de la famille $\mathcal{A}$ sont équiprobables. Comme précédemment, nous appelons abusivement APP la valeur normalisée de l'observation, soit

$$\mathrm{APP}(\mathbf{s}_\ell) = \frac{p(\mathbf{r}/\mathbf{s}_\ell)}{\sum_{k=1}^{M} p(\mathbf{r}/\mathbf{s}_k)}$$

Le fonctionnement du bloc "Calcul des APP bits" a été détaillé au paragraphe 3.3.2. Les $\log_2(M)$ observations sur les bits codés qui étiquètent la séquence $\mathbf{s}_\ell$ sont évaluées à l'aide de la formule (3.13) dans laquelle les APP des signaux multidimensionnels $\mathrm{APP}(S_m)$ sont remplacées par les APP des séquences $\mathrm{APP}(\mathbf{s}_m)$.

Ces $\log_2(M)$ observations abusivement appelées APP sont utilisées par le décodeur SISO et nous nous limitons à quatre itérations de décodage. Par ailleurs, l'étiquetage de Gray est employé.

Nous comparons les performances d'une famille de $M = 64$ séquences complexes purement aléatoires de longueur $N = 8$ codée à sa capacité sur canal gaussien et sur canal de Rayleigh.

4.5.1 Séquences complexes purement aléatoires et code convolutif

Dans la suite, la famille de 64 séquences complexes purement aléatoires de longueur 8 est indifféremment notée $\mathcal{A}_1$ ou $(64, 8)$.

Séquences complexes purement aléatoires et code convolutif sur le canal gaussien

La capacité de la famille $\mathcal{A}_1$ sur canal gaussien est illustrée sur le dernier graphique en bas à droite sur la figure 4.10. On constate qu'elle atteint une capacité $C = 0.5$ bits/s/Hz pour un rapport signal-à-bruit $E_b/N_0 = 2.5$ dB. Par ailleurs, $\eta = \frac{\log_2(64)}{8} = 3/4$. Il faut donc choisir un code convolutif de rendement $R = 2/3$. En toute logique, plus le code choisi sera puissant, plus la probabilité d'erreur de l'alphabet codé devra tendre vers 0 pour un rapport signal-à-bruit proche de 2.5 dB.

Deux codes convolutifs de rendement 2/3 ont été utilisés pour les simulations : le code C_1 de longueur de contrainte $L = 3$ (16 états), de polynômes générateurs $(27, 75, 72)$ et de distance libre $d_{\text{free}} = 5$ ainsi que le code C_2 de longueur de contrainte $L = 4$ (64 états), de polynômes générateurs $(236, 155, 337)$ et de distance libre $d_{\text{free}} = 7$.

Les figures 4.16 et 4.17 résument les performances obtenues avec la famille $\mathcal{A}_1$ codée. Les quatre itérations de décodage sont représentées. A titre de comparaison, sont également rappelées la référence de capacité (0.5 bits/s/Hz à 2.5 dB ici) et les performances d'une famille de huit signaux orthogonaux non codés sur canal gaussien non cohérent. On constate qu'en pratique, l'utilisation d'un code de complexité raisonnable (le code C_1, 16 états) permet de faire tendre la probabilité d'erreur vers 0 à environ 1.75 dB de la capacité. En effet, ce premier schéma atteint une probabilité d'erreur $P_e = 10^{-6}$ pour un rapport signal-à-bruit $E_b/N_0 = 4.25$ dB. L'emploi d'un code plus complexe (le code C_2, 64 états) ne permet pas d'améliorer les résultats puisque l'on atteint dans ce cas une probabilité d'erreur $P_e = 7 \times 10^{-4}$ seulement pour le même rapport signal-à-bruit $E_b/N_0 = 4.25$ dB. Ainsi, les résultats obtenus pour ce cas pratique sont très encourageants.

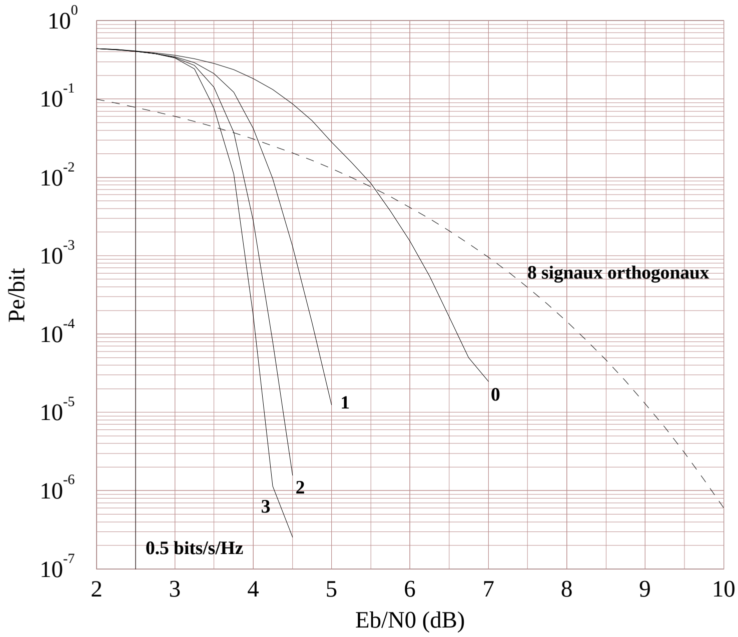


Fig. 4.16 – Famille $\mathcal{A}_1$ codée par le code convolutif 16 états C_1 de rendement 2/3.

Par ailleurs, la figure 4.18 permet de comparer les comportements des deux codes. On remarque sur les courbes des itérations deux et trois que pour des rapports signal-à-bruit compris entre 0 et 4 dB, le code C_1, 16 états obtient de meilleurs résultats avant d'être rattrapé par le code C_2 pour des rapports signal-à-bruit supérieurs à 4 dB. Une explication peut être apportée :

à fort E_b/N_0, c'est la distance minimale d'un code qui influence ses performances, tandis qu'à faible E_b/N_0, le nombre de voisins devient le paramètre important.

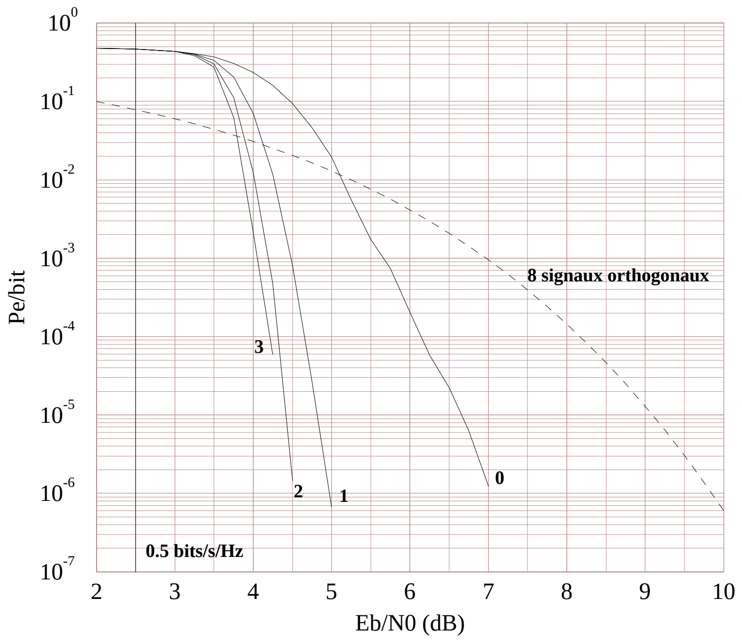


Fig. 4.17 – Famille $\mathcal{A}_1$ codée par le code convolutif 64 états C_2 de rendement 2/3.

Séquences complexes purement aléatoires et code convolutif sur le canal de Rayleigh

La capacité de cette même famille $\mathcal{A}_1$ sur canal de Rayleigh est illustrée sur le dernier graphique en bas à droite sur la figure 4.11. On constate qu'elle atteint une capacité $C = 0.25$ bits/s/Hz pour un rapport signal-à-bruit $E_b/N_0 = 3.5$ dB. On a toujours $\eta = \frac{\log_2(64)}{8} = 3/4$. Il nous faut donc cette fois choisir un code convolutif de rendement $R = 1/3$. De la même manière, on espère que plus le code choisi sera puissant, plus la probabilité d'erreur de l'alphabet codé devra tendre vers 0 pour un rapport signal-à-bruit proche de 3.5 dB.

Deux codes convolutifs de rendement 1/3 sont utilisés pour les simulations : le code C_1 de longueur de contrainte $L = 5$ (16 états), de polynômes générateurs $(25, 33, 37)$ et de distance libre $d_{\text{free}} = 12$ ainsi que le code C_2 de longueur de contrainte $L = 7$ (64 états), de polynômes générateurs $(133, 145, 175)$ et de distance libre $d_{\text{free}} = 15$.

Les figures 4.19 et 4.20 résument les performances obtenues avec la famille $\mathcal{A}_1$ codée. Les quatre itérations de décodage sont représentées. A titre de comparaison, sont également rappelées la référence de capacité (0.25 bits/s/Hz à 3.5 dB ici) et les performances d'une famille de huit signaux orthogonaux non codés sur canal de Rayleigh non cohérent. L'utilisation d'un code de complexité raisonnable (le code C_1, 16 états) permet cette fois de faire tendre la probabilité d'erreur vers 0 à environ 2.5 dB de la capacité. En effet, ce premier schéma atteint une probabilité d'erreur $P_e = 3 \times 10^{-5}$ pour un rapport signal-à-bruit $E_b/N_0 = 6$ dB. L'emploi d'un code

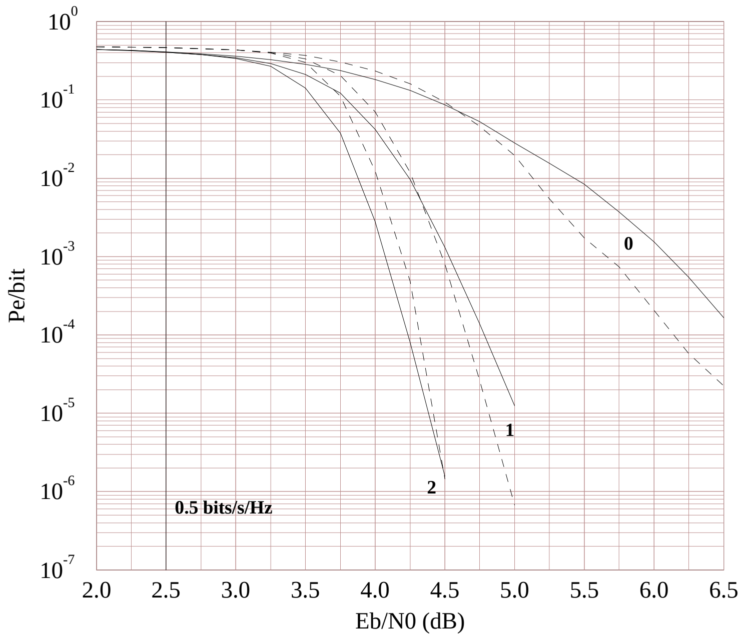


Fig. 4.18 – Comparaison des comportements des codes C_1 et C_2.

plus complexe (le code C_2, 64 états) ne permet toujours pas d'améliorer les résultats puisque l'on atteint dans ce cas une probabilité d'erreur $P_e = 7 \times 10^{-5}$ pour un rapport signal-à-bruit $E_b/N_0 = 5.75$ dB comme pour le code C_1. Malgré cela, les résultats obtenus pour ce cas pratique sont ici encore très encourageants.

Un raisonnement en tout point similaire à celui de l'exemple du canal gaussien peut être mené pour expliquer les différences de comportements des deux codes convolutifs de même rendements utilisés. Les courbes sont rassemblées figure 4.21. Le code C_2 devient plus performant au delà d'un rapport signal-à-bruit de 5.75 dB pour les deuxième et troisième itérations.

4.6 Conclusions

Dans ce chapitre, nous avons tout d'abord présenté différentes constructions possibles menant à des familles de $M >> N$ séquences d'étalement réelles ou complexes de longueur N. Certaines sont connues, comme les séquences d'Hadamard par exemple. Par ailleurs, nous avons pu montré que le principe général exposé au paragraphe 4.1.1 permet en fait de décrire à la fois des familles nouvelles et des familles existantes.

Nous avons étudié la capacité des différents alphabets sur canal gaussien et sur un canal de Rayleigh à évanouissements par blocs. Un grand nombre de résultats numériques obtenus par simulation à l'aide de la méthode d'intégration de Monté Carlo sont présentés. Deux conclusions importantes peuvent en être tirées.

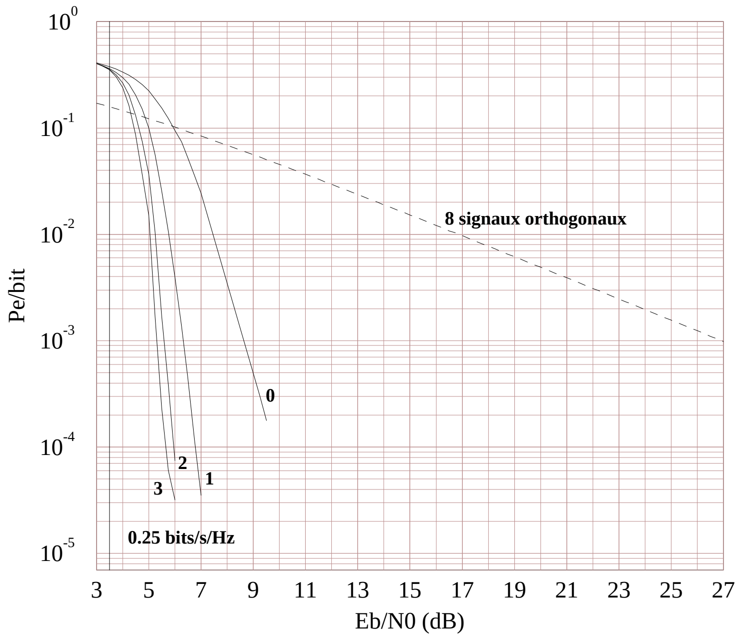


Fig. 4.19 – Famille $\mathcal{A}_1$ codée par le code convolutif 16 états C_1 de rendement 1/3.

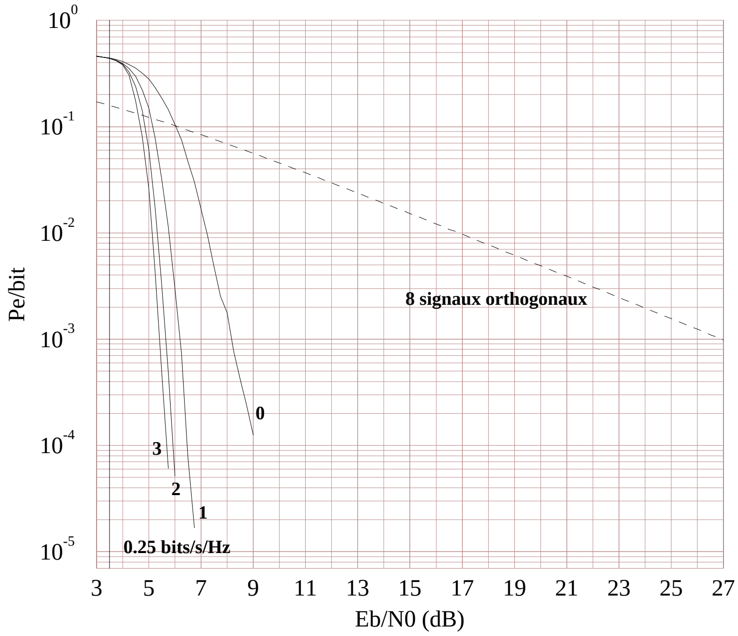


Fig. 4.20 – Famille $\mathcal{A}_1$ codée par le code convolutif 64 états C_2 de rendement 1/3.

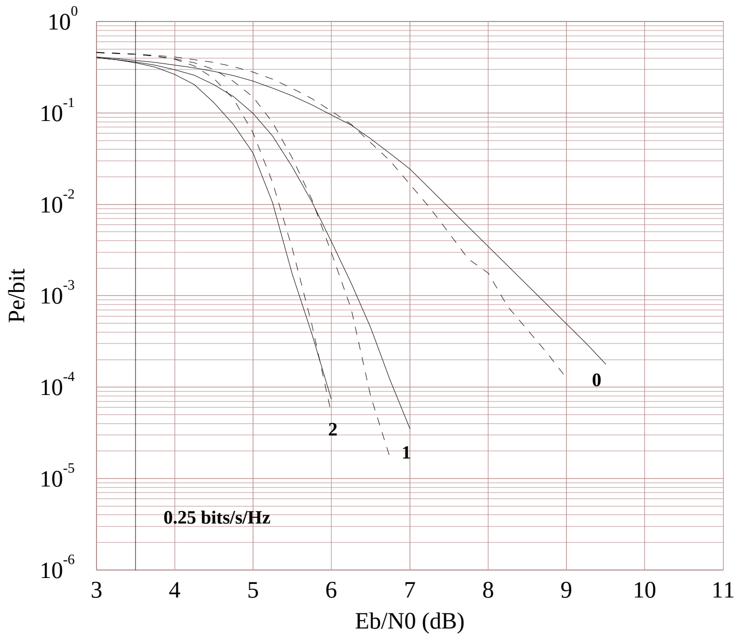


Fig. 4.21 – Comparaison des comportements des codes C_1 et C_2.

Aucune famille de séquences orthogonales ne permet d'atteindre une efficacité spectrale supérieure à 0.5 bits/s/Hz. Ce maximum est atteint pour $N = 2, 4$ seulement, à très fort rapport signal-à-bruit. En augmentant la taille M des alphabets non orthogonaux et la longueur N des séquences de ces même alphabets, aucune limite d'efficacité spectrale n'existe en théorie. Evidemment, dans tout système pratique, on veillera à effectuer un compromis entre l'efficacité spectrale souhaitée et la complexité relative de l'alphabet nécessaire.

Enfin, tant sur canal gaussien que sur canal de Rayleigh, l'emploi de grandes familles de séquences corrélées permet de tendre vers la capacité en détection cohérente du canal correspondant. En théorie, l'usage d'alphabets corrélés appropriés et construits avec attention permet ainsi d'approcher les performances de la détection cohérente avec une détection non cohérente.

Conclusions et perspectives

Conclusions

Les alphabets multidimensionnels étudiés dans ce document sont construits à partir de signaux corrélés – signaux d'une modulation Q-FSK ou séquences d'étalement. Cette approche va à l'encontre des hypothèses habituellement émises et des résultats connus. Nous avons pourtant montré qu'en associant le codage et/ou la diversité à des modulations non orthogonales, l'efficacité spectrale des modulations multidimensionnelles qui en résultent est considérablement augmentée tandis que tout ou partie de la dégradation des performances est compensée.

Le critère N-dimensionnel optimal de détection non cohérente est le même sur les canaux gaussien et de Rayleigh. Le détecteur est constitué d'un banc de filtres adaptés à tous les candidats possibles sur chaque composante – par exemple les Q signaux d'une modulation Q-FSK. Le critère maximise, sur les M signaux de l'alphabet multidimensionnel, la somme de N contributions au carré. Chaque contribution n'est autre que le module de la sortie du filtre adapté à la composante émise.

Les constructions proposées à partir des modulations FSK sont au nombre de trois :

• les réseaux de fréquences

Il existe une parfaite correspondance entre les composantes entières d'un point du réseau de points et les fréquences émises sur chaque composante d'un point du réseau de fréquences. En choisissant un réseau de points dense, d'excellents résultats sont obtenus sur canal gaussien.

• les alphabets codés par une TCM

De la même manière, chaque signal de la modulation PAM ou PSK sous-jacente permet de choisir un signal FSK. Ces alphabets conduisent à des systèmes peu complexes et particulièrement robustes.

• les BICM

Contrairement aux schémas communément utilisés, la modulation sous-jacente est une FSK classique ou une FSK de diversité supérieure à 1. L'emploi des turbo codes permet d'atteindre les meilleures performances – par rapport aux différentes constructions envisagées – mais le retard introduit par la latence de ce type de codage ne sera pas toujours admissible en pratique.

Dans tous les cas, le choix de l'espacement fréquentiel élémentaire de la modulation FSK revêt une importance particulière : la valeur $\Delta f_0 = 2/3T$ établit le meilleur compromis entre le gain d'efficacité spectrale dû à la réduction de la bande et la dégradation des performances qui doit être compensée par le schéma de codage.

Nous avons défini un schéma sous-optimal de décodage : il associe une démodulation non cohérente APP à un décodage à entrée souple. La démodulation non cohérente APP consiste à transformer judicieusement les sorties du banc de filtres en informations souples délivrées au décodeur à entrée souple (décodeur par sphères, décodeur multiniveaux, décodeur SISO, etc.). Ce mécanisme de décodage fait ainsi preuve d'une grande souplesse, il peut être utilisé pour tous les alphabets que nous avons étudiés. Pour les BICM, le schéma sous-optimal peut être amélioré à l'aide d'une détection itérative.

Enfin, lorsque les applications nécessitent des alphabets de taille plus grande, nous suggérons l'utilisation de séquences d'étalement complexes corrélées. Nous avons établi un principe de construction très général : les séquences sont identifiées à des points répartis judicieusement sur une hypersphère en dimension N. Aucune famille de séquences orthogonales ne permet d'atteindre une efficacité spectrale supérieure à 0.5 bits/s/Hz, et ce maximum est atteint pour N valant 2 ou 4 seulement, à très fort rapport signal-à-bruit. En revanche, en augmentant simultanément la taille des alphabets non orthogonaux et la longueur des séquences qui les composent, on s'affranchit de toute limite théorique d'efficacité spectrale. En pratique, on veillera à établir un compromis entre l'efficacité spectrale souhaitée et la complexité de mise en œuvre correspondante.

Les résultats, encourageants, prouvent que l'usage d'alphabets corrélés appropriés et construits avec attention, dans des systèmes de transmission avec détection non cohérente, permet d'approcher les performances de la détection cohérente.

Perspectives

Nous avons pu observer que l'étude des expressions des probabilités d'erreur par paire permet de déterminer des critères de conception des modulations multidimensionnelles. Il faudrait poursuivre la démarche et déterminer une expression des probabilités d'erreur.

De nouvelles méthodes de construction pourraient également être explorées. En particulier, il serait bon d'exploiter la forme de la distribution d'entrée qui permet d'atteindre la capacité du canal de Rayleigh en détection non cohérente [1].

Par ailleurs, l'intégralité de cette étude est restreinte au cas de transmissions mono-antenne. Il serait intéressant de généraliser ces résultats à un canal à entrées multiples et sorties multiples sur le modèle des travaux de T.L. Marzetta et B. Hockwald [51].

Enfin, les séquences corrélées des alphabets décrits dans le dernier chapitre pourraient être exploitées en tant que nouvelles signatures dans un système à accès multiple de type CDMA (Code Division Multiple Access). Il s'agira alors d'optimiser l'affectation de ces séquences aux différents utilisateurs. La minimisation des interférences entre utilisateurs, liée à la répartition des corrélations, sera privilégiée afin d'améliorer au mieux les performances du système global.

Bibliographie

[1] I.C. Abou Faycal, M.D. Trott, S. Shamai (Shitz). «The capacity of discrete-time Rayleigh fading channels». *Proceedings of the International Symposium on Information Theory (ISIT'97)*, pp. 473, Ulm, Germany, 1997.

[2] M. Abramowitz, I. Stegun. *Handbook of mathematical functions.* Dover Publications Inc., New York, 9th printing, 1972.

[3] O. Amrani, Y. Be'ery, A. Vardy, F.W. Sun, H.C.A. van Tilborg. «The Leech lattice and the Golay code : bounded-distance decoding and multilevel constructions». *IEEE Transactions on Information Theory*, vol. 40, pp. 1030-1043, 1994.

[4] L.R. Bahl, J. Cocke, F. Jelinek, J. Raviv. «Optimal decoding of linear codes for minimizing symbol error rate». *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 284-287, March 1974.

[5] G. Battail. «Description polynomiale des codes en blocs linéaires». *Annales des Télécommunications*, vol. 38, no. 1-2, pp. 3-15.

[6] G. Battail, *Théorie de l'information*, Masson, Paris, 1997.

[7] E. Bejjani, *Techniques de transmission pour les canaux très dispersifs*, Thèse de doctorat, ENST, 1997.

[8] S. Benedetto, G. Montorsi. «Unveiling turbo-codes : some results on parallel concatenated coding schemes». *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 409-429, March 1996.

[9] S. Benedetto, G. Montorsi. «Design of parallel concatenated convolutional codes». *IEEE Transactions on Communications*, vol. 44, no. 5, pp. 591-600, May 1996.

[10] S. Benedetto, G. Montorsi, D. Divsalar, F. Pollara. «Serial concatenation of interleaved codes : Performance analysis, design and iterative decoding». *TDA Progress Report 42-126*, JPL, August 1996.

[11] S. Benedetto, E. Biglieri, V. Castellani. *Digital Transmission Theory.* Prentice-Hall, Englewood Cliffs, New Jersey, 1987.

[12] S. Benedetto, E. Biglieri. *Principals of Digital Transmission : with Wireless Applications.* Plenum Press, 1998.

[13] E.R. Berlekamp. «The technology of error-correcting codes». *Proceedings of the IEEE*, vol. 68, no. 8, pp. 564-593, May 1980.

[14] C. Berrou, A. Glavieux, P. Thitimajshima. «Near Shannon limit error-correcting coding and decoding : turbo-codes». *Proceedings of ICC'93*, Genève, pp. 1064-1070, May 1993.

[15] E. Biglieri, D. Divsalar, P.J. McLane, M.K. Simon. *Introduction to trellis coded modulation with applications.* MacMillan, New York, 1991.

[16] E. Biglieri, J.G. Proakis, S. Shamai (Shitz). «Fading Channels : Information-Theoretic and Communications Aspects». *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2619-2692, October 1998.

[17] J. Boutros. *Réseaux de points pour les canaux à évanouissements.* Thèse de doctorat, ENST, 1996.

[18] J. Boutros, E. Viterbo, C. Rastello, J-C. Belfiore. «Good Lattice Constellations for both Rayleigh Fading and Gaussian Channels». *IEEE Transactions on Information Theory*, vol. 42, no. 2, pp. 502-518, March 1996.

[19] J. Boutros, O. Pothier. «Convergence analysis of turbo decoding». *Proceedings of the Canadian Workshop on Information Theory (CWIT'97)*, Toronto, Canada, June 1997.

[20] J. Boutros. «APP Decoding of Linear Transformations». *Proceedings of 2000 International Symposium on Information Theory and its Applications (ISITA2000)*, Honolulu, Hawai, Etats-Unis, November 2000.

[21] G. Caire, G. Taricco, E. Biglieri. «Bit-Interleaved Coded Modulation». *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 927-946, May 1998.

[22] A.R. Calderbank, N.J. Sloane. «New Trellis Codes Based on Lattices and Cosets». *IEEE Transactions on Information Theory*, vol. 33, no. 2, pp. 177-195, March 1987.

[23] A.R. Calderbank. «Multilevel codes and multistage decoding». *IEEE Transactions on Communications*, vol. 37, no. 3, pp. 222-229, March 1989.

[24] H. Cohen. *Computational algebraic numbre theory.* Springer-Verlag, New York, 1993.

[25] J.H. Conway, N.J. Sloane. «Soft Decoding Techniques for Codes and Lattices, Including the Golay Code and Leech Lattice». *IEEE Transactions on Information Theory*, vol. 32, no. 1, pp. 41-50, January 1986.

[26] J.H. Conway, N.J. Sloane. *Sphere packings, lattices and groups*, 3rd edition. Springer-Verlag, New York, 1998.

[27] M.A.O. de Costa e Silva, R. Palazzo. «A bounded-distance decoding algorithm for lattices obtained from a generalized code formula». *IEEE Transactions on Information Theory*, vol. 40, no. 6, pp. 2075-2082, November 1994.

[28] T.M. Cover, J.A. Thomas. *Elements of Information Theory.* John Wiley & Sons, New York, 1991.

[29] D. Divsalar, S. Dolinar, R.J. McEliece, F. Pollara. «Transfer function bounds on the performance of turbo codes». *TDA Progress Report 42-122*, JPL, April-June 1995.

[30] P. Elias. «Coding for noisy channels». *IRE Conv. Rec.*, Pt. 4, pp. 37-47, 1955.

[31] T. Ericson. «A Gaussian Channel with Slow Fading». *IEEE Transactions on Information Theory*, vol. 16, no. 3, pp. 353-355, May 1970.

[32] G.D. Forney. *Concatenated Codes.* Cambridge, MIT Press, 1966.

[33] G.D. Forney. «Convolutional codes, part I : Algebraic structure». *IEEE Transactions on Information Theory*, vol. 16, no. 6, pp. 720-738, November 1970.

[34] G.D. Forney. «The Viterbi algorithm». *Proceedings of the IEEE*, vol. 61, no. 3, pp. 268-278, March 1973.

[35] G.D. Forney, R.G. Gallager, G.R. Lang, F.M. Longstaff, S.U. Qureshi. «Efficient modulations for band-limited channels». *IEEE Journal on Selected Areas in Communications*, vol. 2, pp. 632-647, September 1984.

[36] G.D. Forney. «Coset codes - Part I : Introduction and geometrical classification». *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1123-1151, September 1988.

[37] G.D. Forney. «Coset codes - Part II : Binary lattices and related codes». *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152-1187, September 1988.

[38] G.D. Forney, A. Vardy. «Generalized minimum-distance decoding for Euclidian-space codes and lattices». *IEEE Transactions on Information Theory*, vol. 42, no. 6, part 1, pp. 1992-2026, November 1996.

[39] R.G. Gallager. *Information Theory and Reliable Communication.* John Wiley & Sons, 1968.

[40] A. Gersho, V.B. Lawrence. «Multidimensional Signal Constellations for Voiceband Data Transmission». *IEEE Journal on Selected Areas in Communications*, vol. 2, pp. 687-702, September 1984.

[41] I.S. Gradshteyn, I.M. Ryzhik. *Tables of integrals, series and products*, 5th edition. Academic Press, 1980.

[42] C.W. Helstrom. «The Resolution of Signals in White Gaussian Noise». *Proceedings of the IRE*, vol. 43, pp. 1111-1118, September 1955.

[43] S.H. Jamali, T. Le-Ngoc. *Coded-Modulation Techniques for Fading Channels.* Kluwer, New York, 1994.

[44] R. Johannesson, Z.-X. Wan. «A linear algebra approach to minimal convolutional encoders». *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1219-1233, July 1993.

[45] K.J. Kerpez. «Constellations for Good Diversity Performance». *IEEE Transactions on Communications*, vol. 41, no. 9, pp. 1412-1421, September 1993.

[46] C. Lamy. *Communications à grande efficacité spectrale sur le canal à évanouissements.* Thèse de doctorat, ENST, 2000.

[47] X. Li, J.A. Ritcey. «Bit-Interleaved Coded Modulation with Iterative Decoding». *IEEE Communication Letters*, vol. 1, no. 6, pp. 169-171, November 1997.

[48] X. Li, J.A. Ritcey. «Bit-Interleaved Coded Modulation with Iterative Decoding - Approaching Turbo-TCM Performance without Code Concatenation». *Proceedings of CISS'98*, March 1998.

[49] X. Li, J.A. Ritcey. «Trellis-Coded Modulation with Bit Interleaving and Iterative Decoding». *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 4, pp. 715-724, April 1999.

[50] F.J. MacWilliams, N.J.A. Sloane. *The theory of error-correcting codes.* North-Holland, Englewood Cliffs, 8th impression, 1993.

[51] T.L. Marzetta, B. 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.

[52] A.N Nutall. «Error Probabilities for Nonorthogonal M-ary Signals under Phase-Coherent and Phase-Incoherent Reception». Waltham, MA : Litton Systems Inc., Tech Report TR-61-1-BF, June 1961.

[53] A.H Nutall. «Error Probabilities for Equicorrelated M-ary Signals under Phase-Coherent and Phase-Incoherent Reception». *IRE Transactions on Information Theory*, pp. 305-314, July 1962.

[54] L. Ozarow, S. Shamai (Shitz), A.D. Wyner. «Information Rates for the Two-Ray Mobile Communications Channel». *IEEE Transactions on Vehicular Technologies*, vol. 43, no. 2, pp. 359-378, May 1994.

[55] M. Peleg, S. Shamai (Shitz). «On the Capacity of the Blockwise Incoherent MPSK Channel». *IEEE Transactions on Communications*, vol. 46, no. 5, pp. 603-609, May 1998.

[56] J.G. Proakis. *Digital communications*, 2nd edition. McGraw-Hill, New York, 1989.

[57] J.G. Proakis : *Digital Communications*, 3rd edition. McGraw Hill, New York, 1995.

[58] D. Raphaeli. «Noncoherent Coded Modulation». *IEEE Transactions on Communications*, vol. 44, no. 2, pp. 172-183, February 1996.

[59] J.S. Richters. «Communication Over Fading Dispersive Channels». *MIT Research Laboratory of Electronics*, Technical Report 464, November 1967.

[60] P. Samuel. *Algebraic theory of numbers.* Hermann, Paris, 1971.

[61] M. Schwartz, W.R. Bennet, S. Stein. *Communication Systems and Techniques.* McGraw-Hill, 1966.

[62] C. Schlegel. *Trellis Coding.* IEEE Press, New York, 1997.

[63] S. Shamai (Shitz), T.L. Marzetta. «Multiuser Capacity in Block Fading with no Channel State Information». *Proceedings of the International Symposium on Information Theory (ISIT2000)*, Sorrento, Italy, June 2000.

[64] D.A. Shnidman. «Two Noncentral Chi-Square Generalizations». *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 283-285, January 1996.

[65] M.K Simon, S.M. Hinedi, W.C. Lindsey *Digital Communications Techniques - Signal Design and Detection.* PTR Prentice Hall, 1995.

[66] F.W. Sun, H.C.A. van Tiborg. «The Leech lattice, the octacode, and decoding algorithms». *IEEE Transactions on Information Theory*, vol. 41, no. 4, pp. 1097-1106, July 1995.

[67] G.L Turin. «Error Probabilities for Binary Symmetric Ideal Reception through Nonselective Slow Fading and Noise». *Proceedings of the IRE*, vol. 46, pp. 1603-1619, September 1958.

[68] G. Ungerboeck. «Channel Coding with Multilevel/Phase Signals». *IEEE Transactions on Information Theory*, vol. 28, no. 1, pp. 55-67, January 1982.

[69] G. Ungerboeck. «Trellis-Coded Modulation with Redundant Signals Sets, Part I : Introduction». *IEEE Communication Magazine*, vol. 25, no. 2, pp. 5-11, February 1987.

[70] G. Ungerboeck. «Trellis-Coded Modulation with Redundant Signals Sets, Part II : State of the art». *IEEE Communication Magazine*, vol. 25, no. 2, pp. 12-21, February 1987.

[71] A. Vardy. «Even more efficient bounded-distance decoding of the hexacode, the Golay code and the Leech lattice». *IEEE Transactions on Information Theory*, vol. 41, no. 5, pp. 1495-1499, September 1995.

[72] A.J. Viterbi. «Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm». *IEEE Transactions on Information Theory*, vol. 13, no. 2, pp. 260-269, April 1967.

[73] A.J. Viterbi, J.K. Omura. *Principles of digital communications and coding.* McGraw-Hill, New York, 1979.

[74] A.J. Viterbi, A.M. Viterbi, J. Nicolas, N.T. Sindhushayana. «Perspectives on interleaved concatenated codes with iterative soft-output decoding». *International Symposium on Turbo Codes*, Brest, septembre 1997.

[75] E. Viterbo, E. Biglieri. «A universal lattice decoder». *Proceedings du* $14^{ième}$ *Colloque GRETSI*, Juan-les-Pins, pp. 611-614, septembre 1993.

[76] E. Viterbo, J. Boutros. «A Universal Lattice Code Decoder for Fading Channels». *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1639-1642, July 1999.

[77] M. Greferath, E. Viterbo. «Algebraic Construction of Good Collision Resistant Signal Sets». *Proceedings of the Workshop on Coding and Cryptography (WCC'99)*, pp. 213-224, Paris, January 1999.

[78] L.F. Wei. «Trellis-Coded Modulation with Multi-Dimensional Constellations». *IEEE Transactions on Information Theory*, vol. 33, no. 4, pp. 483-501, July 1987.

[79] P.H. Wittke, Y. Ming Lam, M.J. Schefter. «The Performance of Trellis-Coded Nonorthogonal Noncoherent FSK in Noise and Jamming,». *IEEE Transactions on Communications*, vol. 43, no. 2/3/4, pp. 635-645, February/March/April 1995.

[80] E. Zehavi. «8-PSK trellis codes for a Rayleigh channel». *IEEE Transactions on Communications*, vol. 40, no. 5, pp. 873-884, May 1992.

Publications

[81] C. Durand, E. Bejjani, J. Boutros. «Frequency Space Lattice Encoding for Noncoherent Detection with Correlated Signals». *Proceedings of the Sixth Canadian Workshop on Information Theory (CWIT'99)*, Kingston, Canada, June 1999.

[82] C. Durand, E. Bejjani, J. Boutros. «Forward Error Correction of FSK Alphabets for Wireless Noncoherent Transmissions». *Colloquium Digest «Turbo-codes in digital broadcasting - could it double capacity»*, London, November 1999.

[83] C. Durand, E. Bejjani, J. Boutros. «Multidimensional Signals with Correlated Frequencies for Noncoherent Detection over the Rayleigh Channel». *Proceedings of 2000 International Symposium on Information Theory (ISIT2000)*, pp. 160, Sorrento, Italy, June 2000.

[84] C. Durand, E. Bejjani, J. Boutros. «Forward Error Correction of FSK Alphabets for Noncoherent Transmissions over AWGN Channel». *IEEE Communications Letters*, October 2000.

[85] C. Durand, E. Bejjani, J. Boutros. «Non-Coherent Detection with Nonorthogonal Signals from an Information Theory Perspective». *Proceedings of 2000 International Symposium on Information Theory and its Applications (ISITA2000)*, Honolulu, Hawai, Etats-Unis, November 2000.