Décodage à sortie souple des réseaux de points

Soft output decoding of lattices

Catherine LAMY[†] - Joseph BOUTROS[‡]

[†]Motorola Semiconductors Toulouse, France

[‡]Département Communications et Électronique, ENST, 46 rue Barrault 75013 Paris, France

lamyc@com.enst.fr, boutros@com.enst.fr

1er octobre 1998

Résumé

Nous décrivons ici un algorithme universel de décodage de réseaux de points selon le critère MSE valable sur le canal gaussien et le canal de Rayleigh jusqu'en dimension 1024. Cet algorithme permet de décoder des réseaux tournés en grande dimension. Le décodage est réalisé par un égaliseur à retour de décisions et présente une sortie souple permettant de concaténer les réseaux de points avec d'autres types de codes correcteurs d'erreurs. Nous nous intéressons également au problème du choix des rotations, et montrons qu'une rotation aléatoire en grande dimension possède des performances excellentes sur un canal à évanouissements.

Mots clefs : Réseaux de points, rotations aléatoires, diversité, égalisation à retour de décisions, transformée de Fourier rapide.

Abstract

We present a universal MSE algorithm for lattice decoding in dimensions up to 1024 for both Gaussian and Rayleigh fading channels. This algorithm can be applied to decode high diversity multidimensional rotations. The decoding is performed by a decision feedback equalizer and provides soft output which allows a concatenation of the lattice codes with other type of error-correcting codes. The problem of selecting a good rotation is also considered, and we show that a high dimensional random rotation exhibits very good performance on a Rayleigh fading channel.

Key words : Lattices, random rotations, diversity, decision feedback equalization, Fast Fourier Transform.

1 Introduction

Un réseau de points Λ est un sous-groupe discret de rang n dans l'espace n-dimensionnel $\mathbb{R}^n$. Le réseau est un $\mathbb{Z}$-module généré par une base formée de n vecteurs $v_1, v_2, \ldots, v_n$. Les vecteurs de la base forment les colonnes de la matrice génératrice M de Λ et la valeur absolue du déterminant de cette dernière est égale au volume du parallélotope fondamental. Un exemple de réseau de points bi-dimensionnel est montré figure 1.

Le décodage à maximum de vraisemblance (*Maximum Likelihood* ML) d'un réseau de points est équivalent à la minimisation de la distance euclidienne $\|\mathbf{r} - \mathbf{x}\|^2$ entre le point observé $\mathbf{r}$ et le point du réseau $\mathbf{x}$. En très grande dimension, cette tâche est trop complexe et on utilise donc des décodeurs particuliers pour chaque type de réseau. Les réseaux entiers construits par construction A ou B (c'est-à-dire à partir de codes linéaires) peuvent être décodés par étapes (*multistage decoding*) avec décisions souples des codes binaires constituants à chaque étape ([1], [2]), et de nombreux algorithmes de décodage pour le canal gaussien peuvent également être utilisés pour certains réseaux denses ([2], [3], [4]). De plus, un algorithme GMD sous-optimal (*Generalized Minimum Distance*) a été présenté pour le décodage des réseaux entiers sur le canal gaussien ([5]). Le GMD est basé sur le décodage algébrique avec effacements des codes BCH inclus dans la formule du réseau. Tous ces algorithmes ont été développés pour le canal gaussien et reposent principalement sur un décodage à décisions souples des codes linéaires.

Le décodage à maximum de vraisemblance sur un canal de Rayleigh est équivalent à la minimisation de $||\mathbf{r} - \alpha * \mathbf{x}||^2 = \sum_{i=0}^{n-1} |r_i - \alpha_i x_i|^2$, où les coefficients $\{\alpha_i\}$ du canal sont distribués selon une loi de Rayleigh (*flat fading channel*) de distribution $P(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$ et $0 \leq \alpha_i < +\infty$. Sur ce canal, la densité de l'empilement du réseau qui produit un gain positif sur un canal gaussien n'a plus aucun effet. L'efficacité d'un réseau sur le canal de Rayleigh dépend de sa distribution de diversité donnée par le spectre des distances de Hamming entre les points du réseau. Des réseaux tournés à haute diversité ont été pré-

sentés dans [6], [7]. Ces réseaux entiers (ou seulement intégraux pour certains) ne peuvent être décodés par les algorithmes mentionnés ci-dessus. Un moyen de décoder n'importe quel réseau sur un canal avec ou sans évanouissements est l'utilisation du décodeur universel par sphères ([8]) qui est ML mais dont la complexité limite son utilisation à des dimensions inférieures à 32.

Dans cet article, nous présentons un algorithme universel de décodage de réseaux de points jusqu'en dimension 1024, valable sur canal gaussien et de Rayleigh. Cet algorithme, sous-optimal au sens ML, repose sur le critère de minimisation de l'erreur quadratique moyenne (*MSE decoding : minimum mean square error decoding*). Au lieu de minimiser la distance euclidienne, le décodeur MSE minimise l'espérance mathématique de l'erreur quadratique dans l'espace des entiers $\mathbb{Z}^n$ avant d'appliquer la matrice génératrice M du réseau. La première version de cet égaliseur a été présentée dans [9] pour des matrices d'Hadamard et de Fourier sur le canal de Rayleigh. Notre travail généralise le décodage MSE pour tout réseau de points réel ou complexe en dimension n. La sous-optimalité de ce décodeur peut être compensée par une augmentation de l'efficacité spectrale sur le canal gaussien, de la diversité sur le canal de Rayleigh et de la dimension du réseau pour ces deux canaux. Nous expliquons les excellentes performances obtenues dans [9] par le calcul de la distribution de diversité des réseaux tournés (Cf. paragraphe 5). De plus, on notera que de manière très surprenante, ces réseaux tournés de grande dimension (c'est-à-dire les versions tournées des réseaux cubiques $\mathbb{Z}^n$ notés $\mathbb{Z}_{n,L}$ où L est l'ordre de diversité du réseau) peuvent simplement être choisis de manière aléatoire dans le cas du canal de Rayleigh.

Nous commençons cet article en paragraphe 2 par les définitions du gain du réseau sur le canal gaussien et de la diversité d'un réseau sur le canal de Rayleigh. Le paragraphe 3 rappelle le décodage à sortie dure avec l'algorithme du *Sphere Decoder*, alors que le paragraphe 4 présente l'algorithme de décodage à sortie souple avec retour de décisions. Le paragraphe 5 décrit les relations entre les transformées rapides et les rotations algébriques, ainsi que les distributions de diversité de matrices aléatoires de type Hadamard, des matrices de Fourier et des rotations $\mathbb{Z}_{n,n/2}$. Le paragraphe 6 montre les performances d'un décodeur MSE appliqué au réseau de Barnes-Wall BW_{256} et au réseau tourné $\mathbb{Z}_{512,256}$ (équivalent à une rotation complexe en dimension 256) et enfin le paragraphe 7 donne nos conclusions.

2 Rappel des performances d'un réseau de points : densité et diversité

Le schéma de principe d'un système utilisant une constellation issue d'un réseau de points est présenté en figure 2. Sur le canal gaussien, un tel système voit sa probabilité d'erreur par point P_e diminuer exponentiellement avec le rapport signal sur bruit ([7])

$$P_e \approx \frac{\tau}{2}\, erfc\left(\sqrt{\frac{3s}{2^{s+1}} \times \frac{E_b}{N_0} \times \gamma(\Lambda)}\right) \tag{1}$$

où s est le nombre de bits par deux dimensions, τ le nombre de voisins à distance minimale (*kissing number*) d'un point de Λ et $\gamma(\Lambda)$ le gain fondamental du réseau défini ci-dessous. Sur un canal à évanouissements de Rayleigh, la probabilité d'erreur par point diminue avec une pente d'ordre L ([7])

$$P_e \leq \sum_{l=L}^{n} \frac{K_l}{\left(\frac{s}{8}\frac{E_b}{N_0}\right)^l} \tag{2}$$

où les constantes positives K_l dépendent du choix du réseau Λ et où la diversité L du réseau est définie ci-dessous.

Le gain fondamental d'un réseau de points sur le canal gaussien est le rapport énergétique

$$\gamma(\Lambda) = \frac{d_{Emin}^2}{\sqrt[n]{vol(\Lambda)}}$$

où d_{Emin} est la distance euclidienne minimale de Λ et $vol(\Lambda)$ son volume fondamental. Ce gain fondamental est du à la densité du réseau.

L'ordre de diversité L du réseau Λ est le nombre minimum de composantes distinctes entre deux points quelconques du réseau

$$L = \min_{\forall \mathbf{x},\mathbf{y} \in \Lambda} d_H(\mathbf{x},\mathbf{y})$$

où $d_H(\mathbf{x},\mathbf{y})$ est le nombre de x_i différents de y_i, $i = 1 \ldots n$. Maximiser la diversité est la meilleure façon de réduire la probabilité d'erreur sur un canal de Rayleigh. Il a été montré dans [7] que l'utilisation d'une rotation multi-dimensionnelle augmentait la diversité d'un réseau de points. En effet, comme on peut le constater sur la figure 3 dans le cas d'une MAQ-4, une simple rotation augmente la diversité de $L = 1$ à $L = 2$. Notons aussi qu'un système reposant sur des rotations multi-dimensionnelles augmentant la diversité sur le

canal de Rayleigh peut également être utilisé sur le canal gaussien sans aucune perte en terme de performances.

3 Décodage à sortie dure des réseaux de points

Le décodage à maximum de vraisemblance sur un canal gaussien correspond à la minimisation de la métrique $m(\mathbf{x}|\mathbf{r}) = \sum_{i=1}^{n} |r_i - x_i|^2$ où $\mathbf{x} = M\mathbf{z} \in \Lambda$ est le vecteur émis, $\mathbf{r}$ le vecteur reçu, $\mathbf{z}$ un point de $\mathbb{Z}^n$ et M la matrice génératrice du réseau. La minimisation par énumération exhaustive de tous les points de la constellation n'étant pas réalisable en pratique, on peut la simplifier lorsque la structure du réseau de points est connue en utilisant l'algorithme *Sphere Decoder* (décodage par sphères, [8]).

Il s'agit de rechercher tous les points du réseau compris dans une sphère de centre $\mathbf{r}$ et de rayon $\sqrt{C}$ (Cf. figure 4) et de sélectionner le point le plus proche de $\mathbf{r}$. Ceci revient à chercher le plus court vecteur $\mathbf{w}$ dans l'ensemble translaté $\mathbf{r} - \Lambda \in \mathbb{R}^n : \min_{\mathbf{x}\in\Lambda} \|\mathbf{r} - \mathbf{x}\| = \min_{\mathbf{x}\in\mathbf{r}-\Lambda} \|\mathbf{x}\|$. Si l'on introduit $\xi \in \mathbb{R}^n$ tel que $\mathbf{w} = M\xi$ et $G_\Lambda = M^t M$ matrice de Gram de Λ, la recherche des points de Λ se fait alors dans l'ellipsoïde vérifiant $\|\mathbf{w}\|^2 = \xi^t M^t M \xi = \xi^t G_\Lambda \xi \leq C$. La décomposition de Cholesky de G_Λ en $G_\Lambda = R^t R$ (R matrice triangulaire supérieure) nous permet d'exprimer les équations de l'ellipsoïde sous la forme d'un système d'équations triangulaires et donc de déterminer les limites de l'ellipsoïde et d'énumérer simplement les points de Λ compris dans la sphère, et d'en déduire le plus proche voisin de $\mathbf{r}$.

La complexité ne dépend plus de la taille de la constellation, mais seulement de la dimension et de la répartition des points du réseau, ainsi que du paramètre crucial qu'est le rayon $\sqrt{C}$ de la sphère. Pour d^{-1} borne inférieure des valeurs propres de G_Λ, le nombre d'opérations du coeur de l'algorithme est en $O(n^6)$.

4 Décodage MSE à sortie souple des réseaux de points avec un égaliseur à retour de décisions (DFE)

On emploie classiquement des égaliseurs dans les systèmes de communications numériques afin de réduire l'interférence entre symbole (IES) lorsque l'on transmet sur un canal à bande limitée [10]. Lorsque la réponse impulsionnelle du canal est courte, une égalisation à maximum de vraisemblance est réalisable en appliquant l'algorithme de Viterbi au treillis du canal. Dans le cas inverse, la réduction de l'IES est réalisée par des égaliseurs sous-optimaux mais moins complexes fonctionnant selon le principe de minimisation de l'erreur quadratique moyenne (*MSE criterion* [10]).

Examinons la relation existant entre l'égalisation et le décodage des réseaux de points.
Un réseau Λ est un groupe discret de points obtenu par une transformation linéaire (la matrice M) appliquée au groupe $\mathbb{Z}^n$: $\Lambda = M\mathbb{Z}^n$. L'influence de cette matrice sur $\mathbb{Z}^n$ est semblable à celle d'un canal possédant de l'IES puisque chaque composante d'un point du réseau est une combinaison linéaire de tous les entiers d'entrée. Par conséquent, le décodage du réseau Λ est une opération équivalente à celle de la suppression de l'IES et peut donc être réalisé à l'aide d'un égaliseur. Du fait de l'extrême complexité du décodage en treillis pour les grandes dimensions, la seule solution applicable en pratique est le décodage avec un égaliseur MSE à retour de décisions.
En figure 5 se trouve le schéma du décodeur avec une matrice directe W réelle ou complexe de taille $n \times n$ et une matrice de retour G réelle ou complexe de taille $n \times n$. Le bruit blanc gaussien $\mathbf{b}$ a une variance N_0 par composante réelle. L'estimation de la $i^{\text{ème}}$ composante du point émis $\mathbf{x}$ n'est pas utilisée dans le calcul de retour de l'égaliseur du $i^{\text{ème}}$ symbole reçu, ce qui impose la condition suivante sur la diagonale de la matrice G

$$\forall i \in \{0, ...n-1\} \quad g_{ii} = 0 \tag{3}$$

On note le vecteur émis $\mathbf{x} = M\mathbf{z}$ et le vecteur reçu $\mathbf{r} = \mathbf{x} + \mathbf{b}$. Le vecteur $\tilde{\mathbf{z}}$ est l'entrée du détecteur à seuil et $\hat{\mathbf{z}}$ est le vecteur décodé que l'on fournit à l'entrée de la matrice de retour G. Ainsi, le décodeur possède une sortie souple $\tilde{\mathbf{z}}$ et une sortie ferme $\hat{\mathbf{z}}$. Soit σ_z^2 la variance par composante du vecteur entier $\mathbf{z}$. On suppose que $\sigma_z^2 = 1$ (au remplacement

de N_0 par N_0/σ_z^2 près) et que $\mathrm{E}[\mathbf{z}\hat{\mathbf{z}}^h] = \rho I_n$, où ρ est un facteur de corrélation et I_n la matrice identité. On notera $\mathbf{z^t}$ le transposé de $\mathbf{z}$, $\mathbf{z}^*$ son conjugué et $\mathbf{z^h}$ son transconjugué. En pratique, ρ est approximé par $\rho \approx (1 - P_c(z_i))$, où $P_c(z_i)$ est la probabilité d'erreur sur les composantes entières z_i donc on aura $\rho = 1$ lorsque le taux d'erreur est trop faible. L'égaliseur à retour de décisions repose sur le critère de minimisation de l'erreur quadratique moyenne définie par $\mathrm{E}[||z - \tilde{z}||^2]$. La condition (3) devant également être prise en compte, on utilise les multiplicateurs de Lagrange et l'égaliseur devra minimiser

$$\mathrm{E}(\ \| \ z - \tilde{z} \ \|^2 \ ) - \sum_{i=0}^{n-1} \lambda_i g_{ii} \tag{4}$$

La minimisation de l'expression (4) par rapport aux deux matrices W et G fournit la bonne solution

$$\begin{cases} W^* = \frac{1}{N_0} D_{\rho\lambda+(1-\rho^2)} M^t V^* \quad \text{où V est définie par} \quad (\frac{1-\rho^2}{N_0} M^* M^t + I_n).V^* = I_n \\ \\ G^* = \frac{\rho}{N_0} D_{\rho\lambda+(1-\rho^2)} M^t V^* M^* + D_{\lambda-\rho} \end{cases} \tag{5}$$

où la notation D_ξ représente la matrice diagonale $Diag(\xi_0 \ldots \xi_{n-1})$ et où le vecteur $(\lambda_0, \ldots, \lambda_{n-1})$ est noté λ.

Les multiplicateurs de Lagrange λ_i sont donnés par la contrainte sur G, et l'expression finale de W et G est alors

$$W = D_{\frac{1}{\rho^2 B^* + N_0}} M^h V \text{ et } G = D_{\frac{\rho}{\rho^2 B^* + N_0}} M^h V M - D_{\frac{\rho B^*}{\rho^2 B^* + N_0}}$$

avec $V^* = (v_{ij})$, $M = (M_{ij})$, $B = (B_0, \ldots, B_{n-1})$ et $B_i = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} m_{ki} v_{kl} m_{li}^*$

5 Transformée de rotation rapide pour les canaux à évanouissements

5.1 Des rotations algébriques aux rotations rapides

La recherche d'une rotation garantissant un ordre de diversité supérieur ou égal à L est loin d'être un problème trivial. Une solution a été proposée dans [6], [7], où la rotation retenue est une rotation réelle en dimension n de diversité $L = n/2$ qui génère le réseau

cubique tourné $\mathbb{Z}_{n,L} = R\mathbb{Z}^n$, où R est la matrice de rotation. Le réseau tourné est construit par plongement canonique de l'anneau des entiers dans un corps cyclotomique purement complexe. Ce corps est généré par $\theta = e^{2j\pi/N}$ ($n = \phi(N)$ où ϕ est la fonction d'Euler). Si l'on note $\theta_i = \theta \times e^{4j\pi(i-1)/n}$ pour tout $i = 1...n/2$, la matrice de rotation complexe de taille $n/2$ est alors donnée par

$$R = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \theta_1 & \theta_2 & \dots & \theta_{n/2} \\ \vdots & \vdots & & \vdots \\ \theta_1^{n/2-1} & \theta_2^{n/2-1} & \dots & \theta_{n/2}^{n/2-1} \end{pmatrix} \tag{6}$$

Cette matrice complexe en dimension $n/2$ a pour diversité $n/2$, soit une diversité maximale (*full diversity*) et est équivalente à un réseau réel en dimension n de diversité $n/2$ également. Ce dernier peut-être obtenu en remplaçant chaque valeur complexe $a + jb$ de R par la matrice carrée $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Si l'on s'astreint à choisir les valeurs de n comme puissances de 2, on a $N = 2n$ et on peut donc calculer les coefficients r_{ik} de la matrice de rotation R avec

$$r_{ik} = (\theta.e^{\frac{4j\pi i}{n}})^k = e^{\frac{j\pi k}{n}}.e^{\frac{2j\pi ik}{n/2}} \qquad \forall (i,k) \in 0 \dots \frac{n}{2} - 1 \tag{7}$$

Lorsque cette rotation est appliquée à un vecteur $\mathbf{z} = (z_0, \dots, z_{n/2-1})$, le résultat est le vecteur $\mathbf{x} = (x_0, \dots, x_{n/2-1})$ donné par

$$x_i = \sum_{k=0}^{\frac{n}{2}-1} (r_{ik}.z_k) = \sum_{k=0}^{\frac{n}{2}-1} (e^{\frac{2j\pi ik}{n/2}}.z'_k) \qquad \text{avec} \quad z'_k = z_k.e^{\frac{j\pi k}{2(n/2)}} \tag{8}$$

Si nous comparons la formule ci-dessus et celle de la transformée de Fourier discrète (DFT), nous constatons que la rotation algébrique basée sur le réseau $\mathbb{Z}_{n,n/2}$ est équivalente à $n/2$ changements de phase suivis d'une DFT. Il s'agit donc d'une transformée de rotation rapide (FRT) à diversité maximale, obtenue en combinant des rotations en dimension 2 et une transformation de Fourier rapide (FFT).

Il est bien connu que la distribution des distances euclidiennes du réseau de points Λ a une influence directe sur ses performances sur le canal gaussien (asymptotiquement, elles ne dépendent que de τ et d_{Emin}). De même, la distribution de diversité de Λ a une influence

directe sur les performances obtenues sur le canal de Rayleigh. Puisque $\mathbf{0}$ appartient au réseau Λ, la distribution de diversité peut être obtenue en comparant tous les points à $\mathbf{0}$. Pour tout $\mathbf{x} \in \Lambda$ choisi aléatoirement, la distribution de diversité donne la probabilité $P(l)$ d'avoir l composantes non nulles dans $\mathbf{x}$, avec $L \leq l \leq n$. La distribution de diversité d'une FRT complexe est donnée simplement par $P(l) = 0$ pour $l = 0 \ldots n/2 - 1$ et $P(n/2) = 1$. Pour une FFT, le fait de remarquer que le point $(1, 0, 0, \ldots, 0)$ appartient au réseau tourné indique que l'ordre de diversité minimale de la FFT est $L = 1$. Une FFT n'a donc littéralement pas de diversité, mais on constate que sa distribution de diversité rejoint celle de la FRT pour de très grandes dimensions (Cf. figure 6). Par conséquent, pour n assez grand, la FFT et la FRT ont les mêmes performances sur le canal de Rayleigh. La FFT donne de mauvais résultats pour $n \leq 32$ alors qu'une FRT décodée avec le décodeur universel de réseaux de points [8] élimine presque complètement l'impact des évanouissements. Le comportement d'une transformée d'Hadamard rapide (FHT) est identique à celui d'une FFT. Dans le paragraphe suivant, on calcule la distribution de diversité d'une matrice aléatoire de type Hadamard et l'on montre que toute rotation choisie aléatoirement (en grande dimension) donne des performances similaires sur le canal de Rayleigh.

5.2 Distribution de diversité de matrices aléatoires de type Hadamard

Considérons une efficacité spectrale de 1 bit par dimension ($s = 2$). Dans ce cas, la matrice d'Hadamard (c'est-à-dire la matrice génératrice du réseau Λ correspondant) est multipliée par un vecteur $\mathbf{u}$ à composantes entières à valeurs dans $\{0, 1\}$. Les matrices d'Hadamard sont classiquement calculées récursivement avec (construction de Sylvester où la taille est une puissance de 2)

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

Une formule directe exacte des coefficients h_{ij} d'une matrice d'Hadamard est très difficile à déterminer. Ceci nous amène à définir une matrice aléatoire de type Hadamard H_n qui

va nous permettre de calculer une distribution de diversité

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

On définit également

- $\mathbf{u}$ vecteur d'entrée, et $\mathbf{v}$ vecteur de sortie, vérifiant $\mathbf{v} = H_n\mathbf{u} \quad \in \Lambda$
- $U_{k|0}$ est l'ensemble des vecteurs $\mathbf{u}$ avec k composantes égales à *'1'* et $u_0 = 0$. Son cardinal est $|U_{k|0}| = C_{n-1}^{k}$.
- $U_{k|1}$ est l'ensemble des vecteurs $\mathbf{u}$ avec k composantes égales à *'1'* et $u_0 = 1$. Son cardinal est $|U_{k|1}| = C_{n-1}^{k-1}$.
- U étant l'un de ces deux ensembles, et pour $d \in \mathbb{Z}$, on a

$$P(v_i = d \mid \mathbf{u} \in U) = P(v_j = d \mid \mathbf{u} \in U) = P_U(d) \quad \forall (i,j) \in \{1, ..., n-1\}^2$$

  On remarquera que pour tout $\mathbf{u} \neq \mathbf{0}$, on a $v_0 \neq 0$.
- $L[l]$ est le nombre de vecteurs de diversité l.

Avec ces notations, nous pouvons écrire le nombre de vecteurs $\mathbf{v}$ de diversité l pour $\mathbf{u} \in U$

$$L[l]_U = |U| P_U(0)^{n-l}(1 - P_U(0))^{l-1} \tag{9}$$

On obtient ainsi la formule de la distribution de diversité de ces matrices aléatoires

$$L[n] = \sum_{k_1'=1}^{n/2} \left(C_{n-1}^{2k_1'}(1 - P_{U_{2k_1'|0}}(0))^{n-1} + C_{n-1}^{2k_1'-1}(1 - P_{U_{2k_1'|1}}(0))^{n-1} + C_{n}^{2k_1'-1} \right)$$

et $\forall l \in \{1, ..., n-1\}$

$$L[l] = \sum_{k_1'=1}^{n/2} \left(C_{n-1}^{2k_1'} P_{U_{2k_1'|0}}(0)^{n-l}(1 - P_{U_{2k_1'|0}}(0))^{l-1} + C_{n-1}^{2k_1'-1} P_{U_{2k_1'|1}}(0)^{n-l}(1 - P_{U_{2k_1'|1}}(0))^{l-1} \right) \tag{10}$$

La distribution des énergies peut être calculée de façon similaire en étudiant le nombre de vecteurs avec $v_i = d$. Si l'on note $D[d^2]$ le nombre de vecteurs dont la composante i a

une énergie d, on a

$$D[0] = \sum_{0 \leq k_1 \leq n}^{k_1 \ pair} C_n^{k_1}(P_{U_{k_1}|1}(0) + P_{U_{k_1}|0}(0))$$
$$\text{et } \forall d \in \{1, ..., \frac{n}{2}\} \quad D[d^2] = \sum_{d \leq k_1 \leq n}^{k_1+d \ pair} C_n^{k_1}(P_{U_{k_1}|1}(d) + P_{U_{k_1}|0}(d) + P_{U_{k_1}|0}(-d) + P_{U_{k_1}|1}(-d)) \tag{11}$$

On peut généraliser ces calculs pour des efficacités spectrales supérieures. La figure 6 montre la distribution de diversité pour une FRT complexe en dimension 512, une FFT complexe en dimension 512 et une FHT réelle en dimension 512. La distribution normalisée est obtenue en divisant chaque $L[l]$ par la somme totale $\sum_{l=0}^{n} L[l]$. Un exemple de la distribution d'énergie est également donné en figure 7. Cette courbe montre que la matrice d'Hadamard (ou une matrice aléatoire à composantes dans $\{\pm 1\}$) a la pire des distributions, en particulier en terme de distribution d'énergie. Néanmoins, toutes ces rotations donnent pratiquement le même taux d'erreur pour des dimensions supérieures à 256 puisque les trois familles FFT, FHT et FRT ont une distribution de diversité concentrée au voisinage de n lorsque n est grand.

6 Résultats

Nous illustrons le décodage par un égaliseur à retour de décisions (DFE) sur deux systèmes différents : le réseau de Barnes-Wall de dimension 256 sur le canal gaussien, et le réseau tourné $\mathbb{Z}_{512,256}$ obtenu par une FRT en dimension 256 sur le canal de Rayleigh. Ainsi tirons-nous parti de la diversité de la FRT en l'appliquant sur le canal de Rayleigh et de la distribution de distance du réseau Barnes-Wall en l'appliquant sur le canal gaussien.

Le gain fondamental et le nombre de voisins à distance minimale d'un réseau de Barnes-Wall BW_{256} sont respectivement $\gamma(BW_{256}) = 10.5dB$ et $\tau(BW_{256}) = 325139443200$. Ce réseau est un bon réseau pour le canal gaussien, son gain effectif étant néanmoins inférieur à 10.5 dB du fait de son nombre élevé de voisins. L'équation (1) donne la probabilité d'erreur par point $P_{e_{point}}$ pour un décodeur à maximum de vraisemblance. Si l'étiquetage binaire de la constellation est aléatoire, alors $P_{e1_{bit}} = \frac{1}{2}P_{e_{point}}$, mais si l'étiquetage suit un code de Gray, on a $P_{e2_{bit}} = \frac{1}{128s}P_{e_{point}}$. En figure 8, on trouve les courbes de $P_{e1_{bit}}$

et $P_{e2_{bit}}$ pour $s = 4$ bits par symbole (soit par deux dimensions). Si l'on compare les performances de la MAQ-16, on constate que le gain réel d'un décodeur ML est de 5.5 dB. La figure 8 montre également les performances du décodeur MSE sous-optimal. Si l'on compare ses performances aux précédentes, on constate qu'il atteint les performances de la MAQ-16 mais ne parvient pas à les dépasser. Le décodage avec le critère MSE est donc loin d'atteindre les performances du décodage ML sur le canal gaussien, mais il arrive à supprimer complètement l'interférence (virtuelle) introduite par la matrice du réseau.
Les performances d'un décodeur MSE avec une FRT en dimension 256 (la rotation algébrique donnée par le réseau $\mathbb{Z}_{512,256}$) sur le canal de Rayleigh sont montrées en figure 9. On peut y comparer les performances de la FRT sur le canal de Rayleigh avec celles d'une QAM à même efficacité spectrale sur le canal gaussien. Clairement, on constate que la perte due aux évanouissements a été supprimée : le canal de Rayleigh a été converti en un canal gaussien. La distribution de diversité est assez bonne (dans le cas des grandes dimensions pour les FFT et FHT) et compense la sous-optimalité du critère MSE.

7 Conclusions

Le critère MSE est un moyen de résoudre le problème du décodage des réseaux de points en très grande dimension ($n \geq 128$). Néanmoins les performances du décodeur MSE à retour de décisions restent à améliorer sur le canal gaussien. Le critère MSE ne profite pas du gain fondamental du réseau puisqu'il effectue une optimisation sur l'espace des entiers et non sur le réseau lui-même. En revanche, les performances de ce décodeur sont excellentes sur le canal de Rayleigh, sa sous-optimalité ne ruinant pas complètement la grande diversité de la constellation tirée du réseau de points. La sortie souple du DFE précédant le détecteur à seuil permettra d'effectuer un décodage à décisions souples lorsque le réseau est concaténé avec un code correcteur d'erreurs.
Dans le cas du canal de Rayleigh, et lorsque la dimension est assez élevée, (d'après 5.2), on peut choisir le réseau tourné de manière aléatoire (Cf. [11] pour la création de matrices de rotation aléatoires) et les performances de ce réseau seront aussi bonnes que celles d'une rotation algébrique donnée par $\mathbb{Z}_{n,n/2}$.

Références

[1] CONWAY (J.H.), SLOANE (N.J.A.). Sphere packings, lattices and groups. *Springer-Verlag, New York* (2nde édition, 1993), 663 p.

[2] CONWAY (J.H.), SLOANE (N.J.A.). Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice. *IEEE Transactions on Information Theory* (1986), **32**, n°3-4, pp. 111-126.

[3] SUN (F.W.), TILBORG (H.C.A. van). The Leech lattice, the octacode, and decoding algorithms. *IEEE Trans. on Information Theory* (1995),**41**, pp. 1097–1106.

[4] VARDY (A.). Even more efficient bounded-distance decoding of the hexacode, the Golay code, and the Leech lattice. *IEEE Trans. on Information Theory* (1995), **41**, pp. 1495–1499.

[5] FORNEY (G.D.), VARDY (A.). Generalized minimum distance decoding of Euclidean-space codes and lattices. *IEEE-IT workshop, Haifa'96* (1996).

[6] BOUTROS (J.), VITERBO (E.). Signal space diversity: a power and bandwidth efficient diversity technique for the fading channel. *IEEE Trans. on Information Theory* (1998), **44**, n°4.

[7] BOUTROS (J.). Lattice Codes for Rayleigh Fading Channels. *PhD Thesis* (Mai 1996), ENST-Paris, France.

[8] VITERBO (E.), BOUTROS (J.). A universal lattice code decoder for fading channels. *IEEE Transactions on Information Theory*, CLN 96-137, à paraître.

[9] REINHARDT (M.), LINDNER (J.). Transformation of a Rayleigh fading channel; into a set of parallel AWGN channels and its advantage for coded transmission. *Electronics Letters* (Décembre 1995), **31**, pp. 2154-2155.

[10] PROAKIS (J.G.). Digital Communications. *McGraw-Hill* (troisième édition, 1995), 928 p.

[11] SLOANE (N.J.A.). Encrypting by random rotations. *Eurocrypt* (1983).

8 Liste des légendes

Figure 1 :
- Le plan partagé en des régions fondamentales d'un réseau bi-dimensionnel.
- The plane divided in fundamental regions of a two 2-dimensionnal lattice.

Figure 2 :
- Modèle du système de transmission.
- Transmission system model.

Figure 3 :
- Augmentation de l'ordre de diversité par rotation de la constellation.
- Increasing the diversity ordre by rotating the constellation.

Figure 4 :
- Représentation géométrique de l'algorithme *Sphere Decoder*.
- Geometric representation of the Sphere Decoder algorithm.

Figure 5 :
- Décodage à retour de décisions d'un réseau de points.
- Decision feedback decoding of a lattice.

Figure 6 :
- Distribution de diversité en dimension 512 pour $s = 2$.
- Diversity distribution for dimension 512 and 2 bits per symbol.

Figure 7 :
- Distribution d'énergie par composante en dimension 256 pour $s = 2$.
- Energy distribution per component for dimension 256 and 2 bits per symbol.

Figure 8 :
- Probabilité d'erreur binaire pour le réseau BW_{256} sur le canal gaussien à s=4.
- Binary error rate for the lattice BW_{256} on the Gaussian channel with $s = 4$.

Figure 9 :
- Probabilité d'erreur binaire pour une FRT en dimension 256 sur le canal de Rayleigh. (a) : s=2, (b) : s=4.
- Binary error rate for an FRT for dimension 256 on the Rayleigh fading channel. (a) : a=2, (b) : s=4.

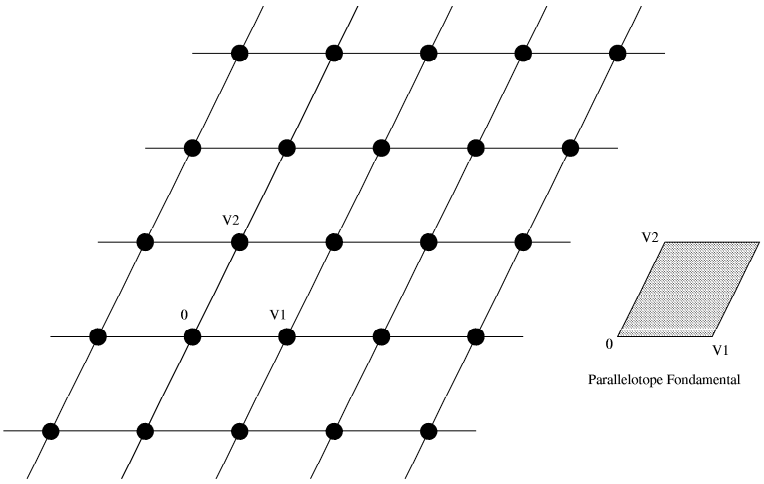

FIG. 1 – *Le plan partagé en des régions fondamentales d'un réseau bi-dimensionnel.*

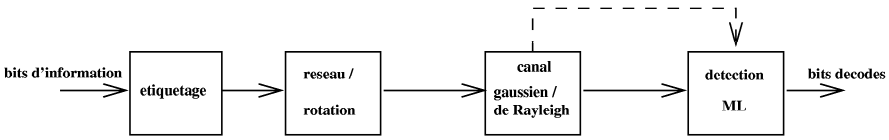

FIG. 2 – *Modèle du système de transmission.*

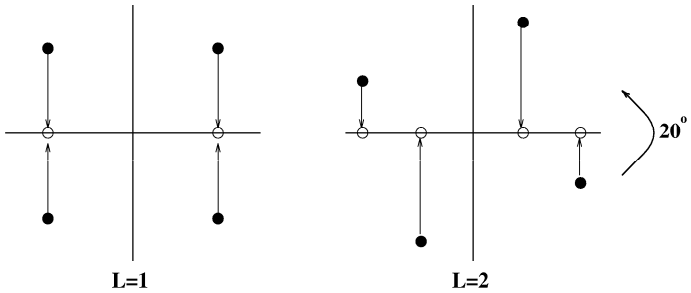

FIG. 3 – *Augmentation de l'ordre de diversité par rotation de la constellation.*

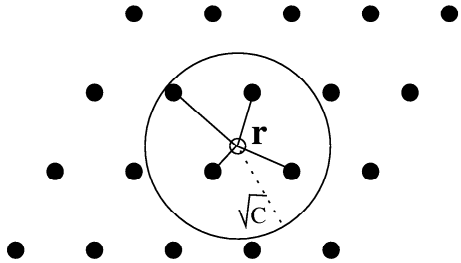

FIG. 4 – *Représentation géométrique de l'algorithme* Sphere Decoder.

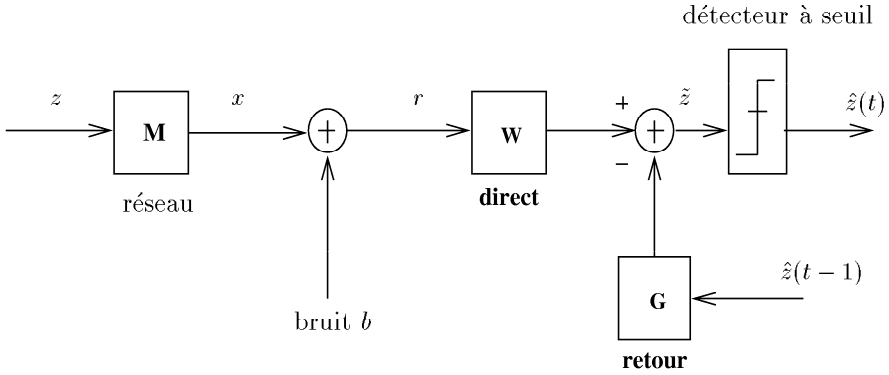

FIG. 5 *Décodage à retour de décisions d'un réseau de points.*

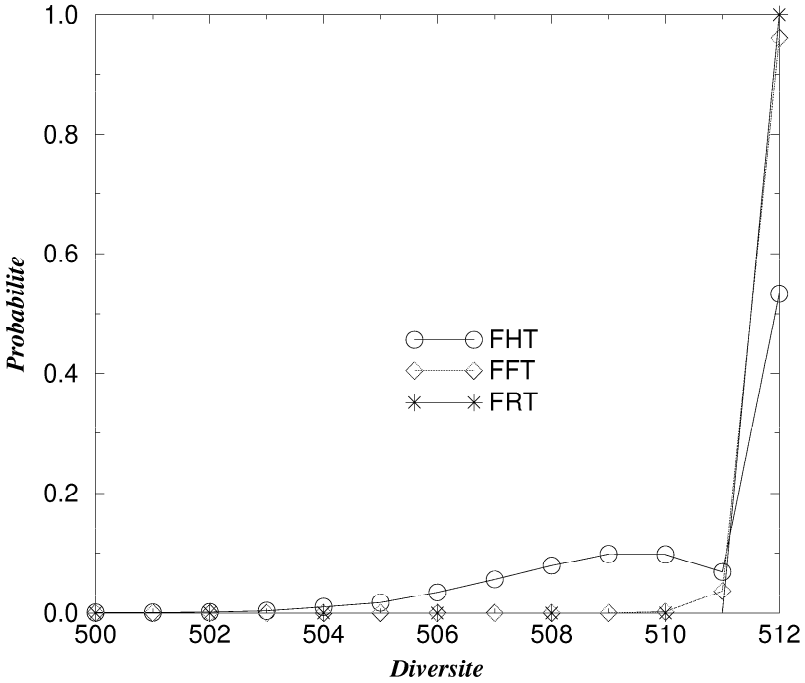

FIG. 6 – *Distribution de diversité en dimension 512 pour* $s = 2$.

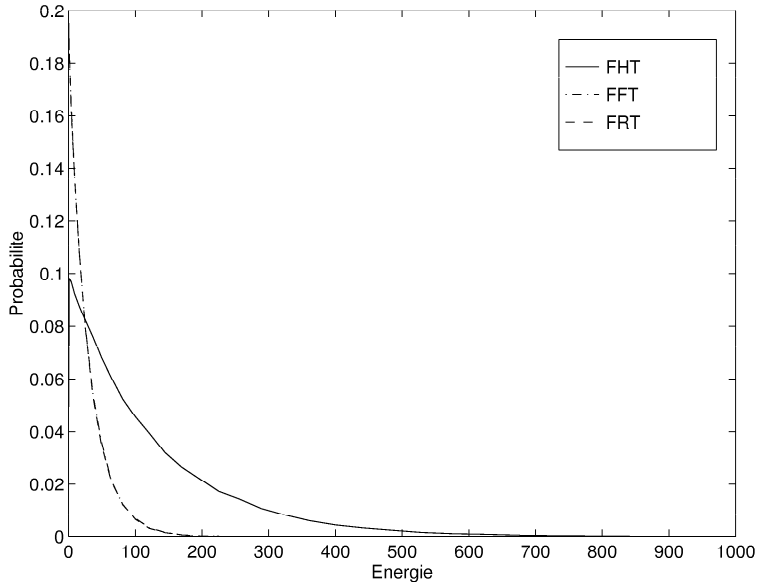

FIG. 7 – *Distribution d'énergie par composante en dimension 256 pour* $s = 2$.

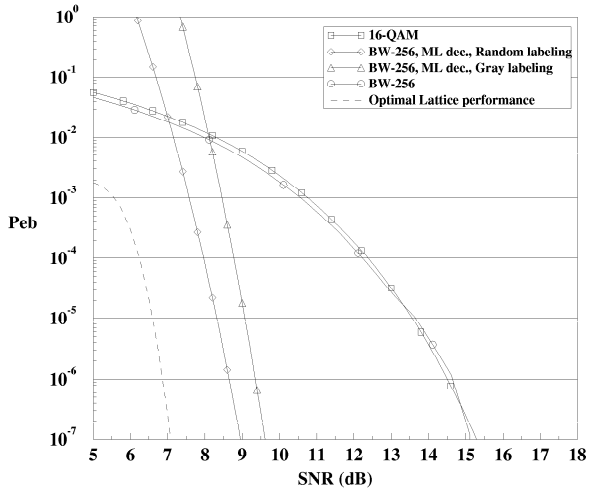

FIG. 8 – *Probabilité d'erreur binaire pour le réseau* BW_{256} *sur le canal gaussien à s=4.*

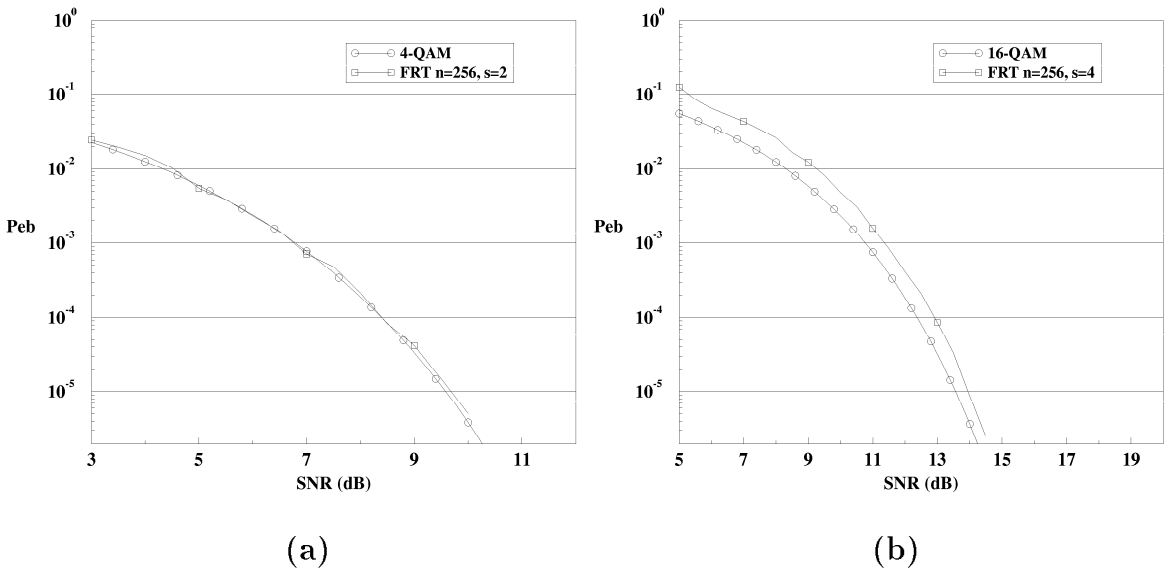

FIG. 9 – *Probabilité d'erreur binaire pour une FRT en dimension 256 sur le canal de Rayleigh. (a) : s=2, (b) : s=4.*