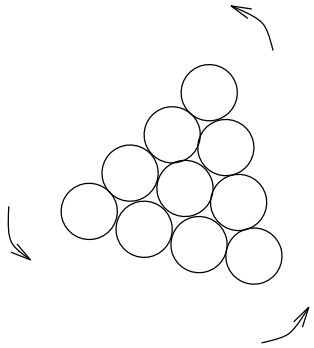
Réseaux de Points pour les Canaux à Evanouissements

Lattice Codes for Rayleigh Fading Channels



Joseph Jean Boutros
Ecole Nationale Supérieure des Télécommunications, Paris

May 28, 1996
french-english version

à Jacqueline Waked
et Jean Berlandier

Sans oublier mon cher père Jean, Paul et Pierre, Rita et Yvette, la patience et l'aide précieuse de Laurence, je dédie ce travail à ma mère Jacqueline qui m'a transmis toute sa volonté, sa persévérance et son courage. Je rappellerai aussi Jean Berlandier qui a su m'imprégner de son savoir et de sa sagesse.

Je remercie tous mes collègues du département Communications de l'ENST et d'autres universités ou laboratoires de recherche, pour leurs conseils et leur soutien. Je citerai par ordre alphabétique : Christine Bachoc, Gérard Battail, Jean-Claude Belfiore, Sergio Benedetto, Ezio Biglieri, Robert Calderbank, Antoine Chouly, Gérard Cohen, Ghassan Kawas-Kaleh, Paul Marinier, Olivier Rioul, Patrick Solé, Robert Vallet, Alexander Vardy et Dominique Ventre.

J'exprime ma profonde gratitude à Emanuele Viterbo et Mario Yubero. Les échanges entre les deux côtés des Alpes et les discussions avec Emanuele ont été très fructueux. Les idées et les travaux de Mario ont eux-aussi contribué à mes recherches.

Je n'oublierai pas le grand soutien de Philippe Gallion, Jany Bats et Laurence Monnot, l'aide et la grande amitié d'Eckhard Papproth, ainsi que les thésards du département Communications : Ralf Haas, Elie Bejjani, Christine Pépin, Georges Rodriguez, and last but not least Emmanuel Lance.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Les réseaux de points connus par les mathématiciens depuis un siècle sont fréquemment utilisés dans les systèmes de communications numériques, surtout depuis l'apparition des modulations codées au début des années 80.

Les réseaux de points servent à construire des modulations à énergie minimale. La grande taille de ces modulations permet la transmission de l'information avec des débits binaires très élevés.

Ainsi, les constellations multidimensionnelles dérivées de réseaux de points ont toujours été le grand candidat à la transmission numérique sur les canaux gaussiens à bruit additif blanc. La grande densité des réseaux était le paramètre critique affectant les performances du système. Le paysage des communications numériques a été fortement modifié et a rajeuni depuis le début des années 90 avec l'explosion de la recherche et des applications dans le domaine des transmissions radiomobiles.

Cette thèse présente donc de nouvelles caractéristiques des réseaux de points, de nouvelles techniques de codage et décodage, afin d'appliquer les réseaux de points aux les systèmes de transmission radiomobile.

Les canaux radiomobiles diffèrent des canaux gaussiens par l'évanouissement dû aux trajets multiples qui vient affecter la partie utile du signal avant l'ajout du bruit. Ainsi, les réseaux de points performants sur le canal gaussien perdent toute leur efficacité sur le canal à évanouissements (canal de Rayleigh), sauf si le réseau de points est doté d'une grande diversité le rendant insensible aux évanouissements. La diversité se traduit par la capacité de récupérer l'information perdue sur les signaux très évanouis en exploitant la redondance qui lie les composantes d'un point du réseau.

Nous avons réussi à construire de nouveaux réseaux à grande diversité. La construction

de ces réseaux fait appel à la théorie algébrique des nombres et utilise le plongement canonique sur un idéal de l'anneau des entiers dans un corps de nombres. Nous avons pu fabriquer de nouveaux réseaux (non connus dans la littérature) ayant une diversité allant de 1 à N, où N est la dimension du réseau. Citons les réseaux $\Lambda_{4,2}$, $\Lambda_{4,4}$, $\Lambda_{5,3}$, $\Lambda_{6,3}$, $\Lambda_{6,6}$, $\Lambda_{8,4}$, $\Lambda_{8,8}$. Ces réseaux sont intégraux mais non entiers. Leur étude nous a permis de construire par la suite de nouvelles versions à grande diversité des réseaux les plus denses : $D_{4,2}$, $E_{8,4}$, $K_{12,6}$, $\Lambda_{16,8}$ et $\Lambda_{24,12}$.

La matrice génératrice des réseaux $\Lambda_{N,N/2}$ est obtenue par application du plongement canonique sur un corps cyclotomique. Nous avons utilisé cette même application pour calculer des rotations multidimensionnelles (les réseaux QAM tournés $\mathbf{Z}_{N,N/2}$). Ces rotations bien spécifiques des constellations multidimensionnelles accroissent la diversité sans modifier les caractéristiques "gaussiennes" du réseau. Nous obtenons ainsi des modulations performantes sur un canal avec ou sans évanouissements.

Le décodage des réseaux de points a été effectué à l'aide d'un nouvel algorithme appelé "Sphere Decoder". Cet algorithme universel ne dépend que de la matrice génératrice du réseau et sa complexité est indépendante de l'efficacité spectrale recherchée (taille de la constellation). Il permet donc de décoder le nouveau réseau obtenu après la rotation appliquée en sortie de l'émetteur et les évanouissements du canal.

Les chapitres sont presque indépendants et le lecteur n'est pas obligé d'en respecter l'ordre. Les experts en réseaux de points peuvent se dispenser de la lecture du chapitre 2. Les experts en théorie algébrique des nombres peuvent se dispenser de la lecture des paragraphes 4.4 et 4.6.1 du chapitre 4.

Le document est organisé de la manière suivante :

- Le chapitre 2 est une introduction aux réseaux de points. Il décrit les paramètres principaux d'un réseau et ses performances sur le canal gaussien. Le paragraphe 2.1 fournit la définition exacte d'un réseau de points. Le paragraphe 2.2 décrit les constructions A et B d'un réseau de points à partir d'un code correcteur d'erreurs. Le partitionnement des réseaux en vue de construire des modulations codées en blocs et les formules des plus importants réseaux sont présentés au paragraphe 2.3. Le dernier paragraphe de ce chapitre montre 4 codeurs de réseaux de points sous la forme d'une modulation codée multiniveaux utilisant des codes en blocs.

- Le décodage universel est expliqué au chapitre 3. Le paragraphe 3.2 décrit l'algorithme "Sphere Decoder" pour le canal gaussien et le paragraphe 3.3 montre comment transformer le Sphere Decoder pour l'adapter au canal de Rayleigh.

- Le plongement canonique (construction algébrique d'un réseau de points) est défini au paragraphe 4.4.2. Ce paragraphe est précédé d'une introduction simple avec quelques exemples d'un corps de nombres et d'une base entière de ce corps. Le paramètre à optimiser par le plongement canonique est la diversité L du réseau. Cette diversité et d'autres paramètres affectant les performances sur le canal de Rayleigh sont introduits dans le paragraphe 4.3. Le théorème le plus important, conséquence directe du plongement canonique, énonce le résultat $L = r_1 + r_2$, où (r_1, r_2) est la signature du corps de nombres.

- Les nouvelles versions des réseaux les plus célèbres (réseaux de Schlafli, Gosset, Coxeter-Todd, Barnes-Wall et Leech) sont présentées au paragraphe 4.6. Les réseaux obtenus ont des diversités allant de 2 à 12. Le sous-paragraphe 4.6.1 redéfinit le plongement canonique appliqué à un idéal inclus dans l'anneau des entiers.

- Le chapitre 5 est divisé en trois parties principales, les paragraphes 5.4, 5.5 et 5.6. Nous montrons au paragraphe 5.4 que le canal de Rayleigh peut être transformé en un canal gaussien si l'on applique une rotation à très grande diversité. Le paragraphe 5.5 présente 3 méthodes différentes pour construire les rotations multidimensionnelles en utilisant la théorie algébrique des nombres. Le calcul des rotations par maximisation de la distance produit minimale (méthode qui ne fait pas appel à la théorie des nombres) est effectué au paragraphe 5.6. Le chapitre se termine par les résultats des simulations qui montrent que le canal de Rayleigh devient gaussien pratiquement à partir d'une diversité égale à 12.

- Le chapitre 6 est une synthèse des travaux présentés dans les chapitres précédents. Les réseaux de points sont comparés à d'autres techniques de codage. Ce chapitre comprend un court exposé de nos perspectives en ce qui concerne les techniques de codage combinées aux réseaux et de nouvelles techniques de décodage moins complexes, éventuellement à sortie souple.

- La liste des publications effectuées dans le cadre de cette thèse est placée à la fin de la bibliographie.

Je vous souhaite une bonne lecture.

Joseph Boutros.

Chapter 2

Définition et Construction des Réseaux de Points

Ce chapitre est un passage obligé pour ceux qui veulent s'initier aux réseaux de points. Des notions relativement avancées sont introduites au paragraphe 2.3. Les 4 paragraphes de ce chapitre forment une synthèse de plusieurs articles et ouvrages traitant de réseaux de points ou de modulations codées. Pour plus d'informations et de références, le lecteur est invité à consulter l'ouvrage encyclopédique de Conway et Sloane [26], ainsi que d'autres articles IEEE et ouvrages dans le domaine des communications numériques et des mathématiques [3] [15] [16] [21] [22] [23] [24] [29] [27] [38] [42] [43] [45] [46] [47] [52] [58] [71] [75] [80].

2.1 Les réseaux de points

Les quatre problèmes classiques, l'empilement des sphères (Sphere Packing), le recouvrement spatial (Space Covering), les boules tangentes (Kissing Number) et la quantification vectorielle, possèdent des caractéristiques communes. Ils ont d'ailleurs souvent été étudiés en parallèle. Dans ce chapitre, nous nous intéressons surtout au problème de rangement de sphères ou "Empilement de Sphères". Un réseau de point (*lattice*) est un empilement particulier possédant une structure de groupe. La théorie des communications numériques est un des grands domaines d'application des réseaux de points où les propriétés géométriques sont bien exploitées, permettant de pousser les limitations pratiques jusqu'aux limites théoriques. Les réseaux les plus denses forment des constellations optimales au sens de la minimisation de la probabilité d'erreur sur un canal de transmission.

2.1.1 Comment ranger des boules ?

Considérons un espace vide (un hangar par exemple) et essayons de déterminer le nombre maximal de boules que l'on peut y entasser. Ce problème classique, toujours non résolu en mathématiques, revient à trouver l'empilement le plus dense de sphères identiques (dans un espace tri-dimensionnel).
La solution serait facile si les boules étaient des cubes. En effet, les cubes s'entassent sans laisser de vide et notre hangar se remplirait alors entièrement avec une densité de remplissage de 100%. Le nombre de cubes rangés est le quotient du volume du hangar par le volume élémentaire d'un cube.

Mais les sphères laissent toujours des zones non remplies entre elles. Quel que soit le rangement utilisé, 25% environ de l'espace restera vide. Un empilement très connu est montré Figures 2.1 et 2.2. Dans ce rangement, les centres des sphères constituent un groupe (au sens algébrique du terme) appelé le réseau cubique à face centrée (*fcc lattice*). Notons que c'est un sous-réseau pair du réseau $\mathbf{Z}^3$.
Dans ce rangement, les boules occupent la fraction $\pi/\sqrt{18} = 0.7405$ de l'espace total. En les empilant de cette façon, le nombre des boules entassées dans le hangar est égal à 0.7405 fois le volume du hangar divisé par le volume d'une boule.
On dira que la densité Δ du réseau fcc est de 0.7405. Continuons en posant une question très intéressante : quelle est la densité maximale que l'on pourrait atteindre ?
Malheureusement, cette fameuse question est un des problèmes ouverts en mathématiques où la réponse n'a pas encore été trouvée. En 1958, Rogers fournit une borne supérieure de 0.7796. En 1986, Lindsey améliora cette borne en remplaçant 0.7796 par 0.7784. Comme Rogers l'avait signalé, "Beaucoup de mathématiciens croient et tous les physiciens savent" que la réponse exacte est 0.7405.
Le problème d'empilement de sphères généralisé revient à trouver la densité maximale d'un rangement dans un espace de dimension N. Sauf indication contraire, notre espace sera toujours euclidien (la métrique utilisée n'est autre que la distance euclidienne).
En pratique, les réseaux de points de dimension $N \geq 3$ ont une importance considérable. Un

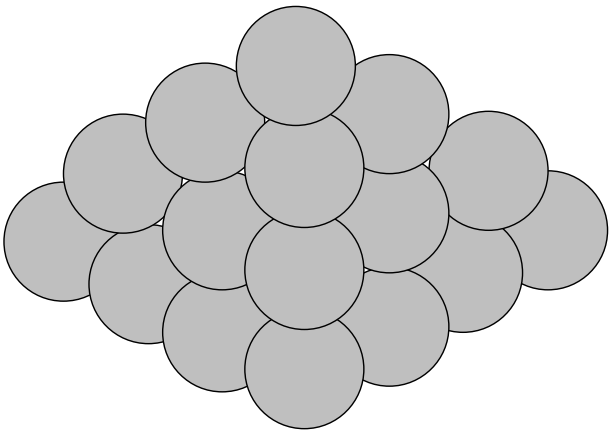


Figure 2.1: L'empilement cubique à faces centrées.

point dans l'espace réel $\mathbf{R}^N$ de dimension N est noté $\mathbf{x} = (x_1, x_2, \ldots, x_N)$ où les composantes x_i sont des éléments de $\mathbf{R}$. Une sphère dans $\mathbf{R}^N$, de rayon ρ et de centre $u = (u_1, u_2, \ldots, u_N)$, est l'ensemble des points $\mathbf{x}$ vérifiant $||\mathbf{x} - \mathbf{u}||^2 = (x_1 - u_1)^2 + (x_2 - u_2)^2 + \ldots + (x_N - u_N)^2 = \rho^2$.

2.1.2 Les empilements groupes

L'empilement des boules montré Figure 2.2 est appelé *groupe* ou *lattice* ou *réseau de points.* La définition exacte d'un réseau de dimension N s'énonce de la façon suivante [71] :

Definition 1 *(Réseau de Points)*
Un sous-groupe discret de rang N de $\mathbf{R}^N$ est appelé réseau *de $\mathbf{R}^N$.*

Ainsi, le réseau noté Λ est un groupe additif formé par les centres des sphères de l'empilement. Le point $\mathbf{0}$ appartient à Λ. Pour tous points $\mathbf{u}$ et $\mathbf{v}$ de Λ, leur somme $\mathbf{u} + \mathbf{v}$ et leur différence $\mathbf{u} - \mathbf{v}$ appartiennent aussi à Λ. "Le réseau est un sous-groupe discret de $\mathbf{R}^N$" signifie que pour tout compact (borné et fermé) $\mathbf{K}$ de $\mathbf{R}^N$, $\mathbf{K} \bigcap \mathbf{R}^N$ est un ensemble fini.
Un exemple typique de réseau est le groupe discret $\mathbf{Z}^N$ où les N composantes d'un point sont toutes entières. Un réseau de points est dit *entier* s'il est un sous-réseau de $\mathbf{Z}^N$.
Pour tout réseau Λ N-dimensionnel, il existe N points (ou N vecteurs) $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ de Λ, tel que $\forall$ le point $\mathbf{x} \in \Lambda$, $\mathbf{x}$ s'écrit sous la forme $\mathbf{x} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_N\mathbf{v}_N$ où les $a_i \in \mathbf{Z}$. En termes algébriques, Λ est un $\mathbf{Z}$-module engendré par N vecteurs linéairement indépendants sur $\mathbf{R}$. La famille des vecteurs $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ est une base du réseau. La région de l'espace $P = \left\{\mathbf{x} \in \mathbf{R}^N \ / \ \mathbf{x} = \alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \ldots + \alpha_N\mathbf{v}_N \ \ avec \ \ \alpha_i \in [0 \ldots 1[\right\}$ est le parallélotope fondamental du réseau.

Definition 2 *(Volume Fondamental)*
On appelle volume fondamental *$vol(\Lambda)$ (ou $det(\Lambda)$) d'un réseau Λ, le volume de son parallélotope fondamental P. Ce volume est indépendant du choix de la base engendrant Λ.*

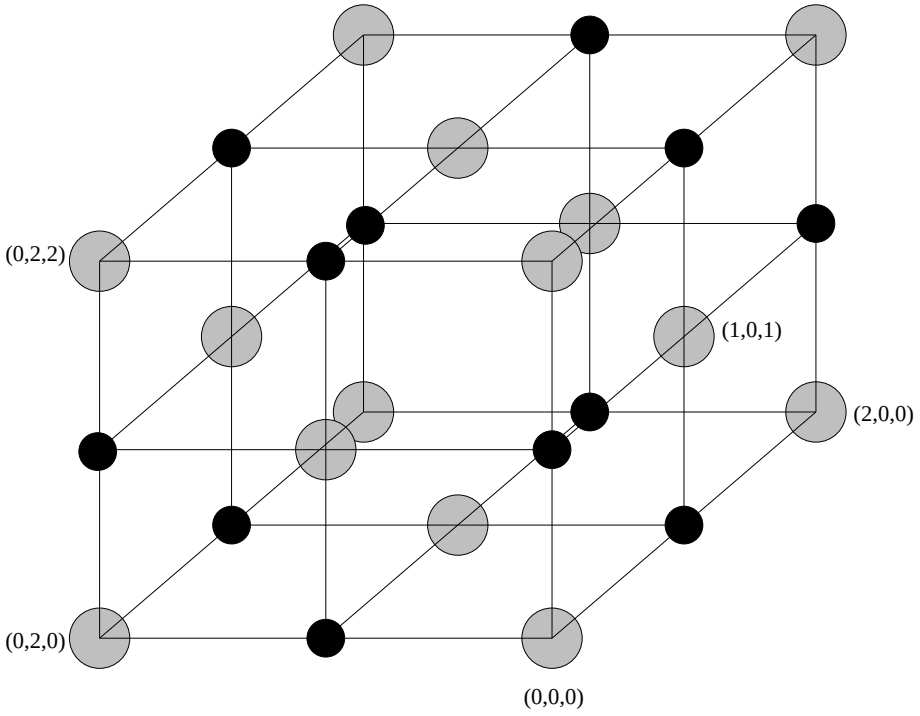


Figure 2.2: Les centres des sphères du réseau fcc.

En effet, un changement de base multiplie le volume fondamental du réseau par $|det(U)|$, où U est la matrice de passage de l'ancienne à la nouvelle base. U est une matrice inversible. Son déterminant $det(U)$ est donc un élément inversible de $\mathbf{Z}$ (Λ est un $\mathbf{Z}$-module). Par conséquent, $det(U) = \pm 1$ et le volume fondamental reste donc le même. Le mot volume dans l'expression $vol(\Lambda)$ est un abus de langage, car le vrai volume (au sens de Lebesgue) du réseau est nul, puisque Λ est un sous-ensemble discret de $\mathbf{R}^N$. La notation $det(\Lambda)$ équivalente à celle de $vol(\Lambda)$ provient de l'égalité $vol(\Lambda) = |det(\mathbf{M})|$ où $\mathbf{M}$ est la matrice génératrice du réseau :

Definition 3 *(Matrice Génératrice)*
Les vecteurs $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ *constituant une base du réseau de points forment les lignes d'une matrice* $\mathbf{M}$ *appelée* matrice génératrice *du réseau* Λ.

Ecrivons $\mathbf{v}_i = (v_{i1}, v_{i2}, \ldots, v_{iN})$ pour $i = 1 \ldots N$. Le réel v_{ij} est la jème composante du vecteur $\mathbf{v}_i$, ainsi $\mathbf{M} = [v_{ij}]$. Un point $\mathbf{x}$ de Λ possède donc une expression matricielle de la forme $\mathbf{x} = \mathbf{aM}$ où $\mathbf{a} = (a_1, a_2, \ldots, a_N)$ est un vecteur de $\mathbf{Z}^N$. Il existe plusieurs choix possibles d'une base $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_N$ du réseau. Par conséquent, la matrice génératrice $\mathbf{M}$ n'est pas unique.

La matrice génératrice $\mathbf{M}$ est une matrice carrée $N \times N$ et la valeur absolue $|det(\mathbf{M})|$ de son déterminant est égale au volume fondamental. En effet, $|det(\mathbf{M})|$ n'est autre que le module du vecteur $\mathbf{V} = \mathbf{v_1} \wedge \mathbf{v_2} \wedge \ldots \wedge \mathbf{v_N}$, produit vectoriel des N vecteurs de la base.

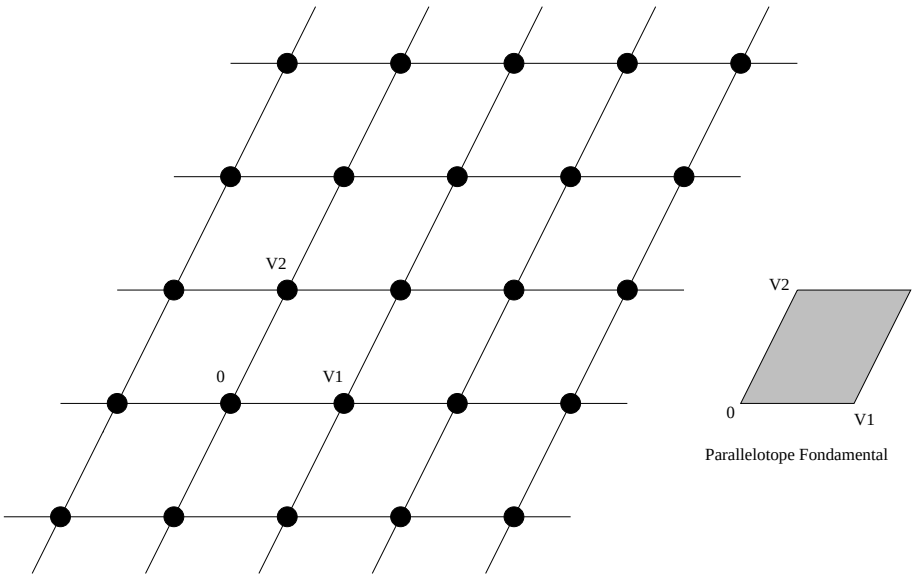


Figure 2.3: Le plan partagé en des régions fondamentales d'un réseau bi-dimensionnel.

Le module du produit vectoriel donne bien le volume de la région limitée par les vecteurs, c'est-à-dire le volume du parallélotope fondamental.

EXEMPLE 2.1
La Figure 2.3 montre un réseau plan (bi-dimensionnel) et son parallélotope fondamental déterminé par la base $\mathbf{v}_1, \mathbf{v}_2$. Des copies du parallélotope fondamental permettent de couvrir l'espace entier avec un seul point appartenant à chaque copie. Le volume fondamental de ce réseau est égal à la surface du parallélogramme ayant comme côtés les deux vecteurs $\mathbf{v}_1$ et $\mathbf{v}_2$. $vol(\Lambda)$ se calcule donc par $vol(\Lambda) = |\mathbf{v}_1 \wedge \mathbf{v}_2| = |v_{11}v_{22} - v_{12}v_{21}| = |det(\mathbf{M})|$. Pour étudier un exemple plus concret, considérons le réseau hexagonal A_2 montré par la Figure 2.4. A_2 est le plus dense rangement dans l'espace $\mathbf{R}^2$. Une matrice génératrice du réseau A_2 pourrait être définie par :

$$M = \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix} . \tag{2.1}$$

On en déduit le volume fondamental de A_2, $vol(A_2) = |det(\mathbf{M})| = \sqrt{3}/2$. La Figure 2.4.c met en évidence les cellules de Voronoi (ou cellules de Dirichlet) du réseau hexagonal. Les frontières d'une cellule de Voronoi sont les médiatrices tracées entre le point au centre de la cellule et tous ses voisins. La définition exacte est la suivante :

Definition 4 *(Cellule de Voronoi)*
Soit $\mathbf{u}$ *un point d'un réseau* Λ. *La région de Voronoi (ou cellule de Dirichlet)* $V(\mathbf{u})$ *associée au point* $\mathbf{u}$ *est l'ensemble de points de* $\mathbf{R}^N$ *défini par*

$$V(\mathbf{u}) = \left\{ \mathbf{x} \in \mathbf{R}^N \ / \ ||\mathbf{x} - \mathbf{u}|| \leq ||\mathbf{x} - \mathbf{y}||, \ \forall \mathbf{y} \in \Lambda \right\}.$$

Le réseau étant un groupe additif, on a la relation triviale $V(\mathbf{0}) + \mathbf{u} = V(\mathbf{u})$. Ainsi, toutes les cellules ont le même volume puisqu'elles sont égales (à une translation près) à la cellule de Voronoi de l'origine $\mathbf{0}$. D'après la structure du réseau, le volume d'une cellule de Voronoi est égal au volume fondamental, $vol(V(\mathbf{0})) = vol(\Lambda)$.

Definition 5 *(Rayon d'Empilement, Rayon de Recouvrement)*
Le rayon d'empilement ρ (resp. rayon de recouvrement R) d'un réseau Λ est le rayon de la plus grande (resp. la plus petite) sphère inscrite (resp. circonscrite) à la région de Voronoi.

Les sphères de l'empilement ont toutes le même rayon ρ. La distance minimale d_{min} entre les points du réseau est donnée par : $d_{min} = 2\rho$. La densité de remplissage d'un réseau est fonction de ρ et de $vol(\Lambda)$:

Definition 6 *(Densité d'un Réseau)*
La densité Δ d'un réseau Λ est donnée par le rapport du volume de la sphère de rayon ρ sur le volume fondamental,

$$\Delta = \frac{volume\ d'une\ sphere}{volume\ fondamental} = \frac{V_N \times \rho^N}{det(\Lambda)} \tag{2.2}$$

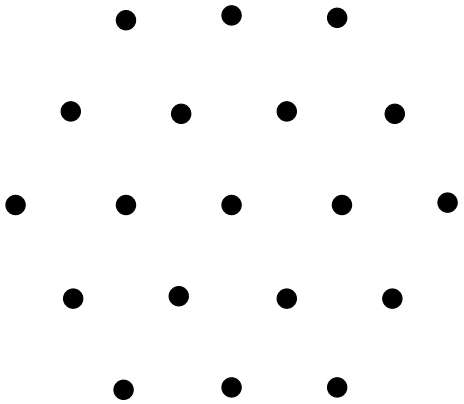
Rappelons que le volume d'une sphère de rayon ρ dans $\mathbf{R}^N$ est proportionnel à ρ^N. Le coefficient de proportionnalité n'est autre que le volume V_N d'une sphère de rayon unité. V_N se calcule à l'aide de l'expression suivante :

$$V_N = \frac{\pi^{N/2}}{\Gamma(N/2+1)} = \begin{cases} \frac{\pi^{N/2}}{(N/2)!} & N\ pair \\ \frac{2^N \pi^{(N-1)/2}((N-1)/2)!}{N!} & N\ impair \end{cases} \tag{2.3}$$

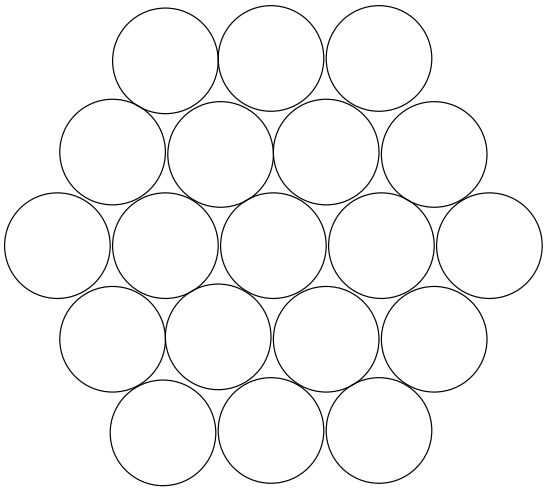
Definition 7 *(Coefficient d'Erreurs)*
Le coefficient d'erreur τ (kissing number) d'un réseau Λ est le nombre de sphères tangentes à une même sphère.

Le coefficient d'erreurs du réseau A_2 est égal à 6. Chaque sphère est entourée par six sphères tangentes (Figure 2.4.b) et chaque point possède six voisins situés à une distance égale à d_{min} (Figure 2.4.a).

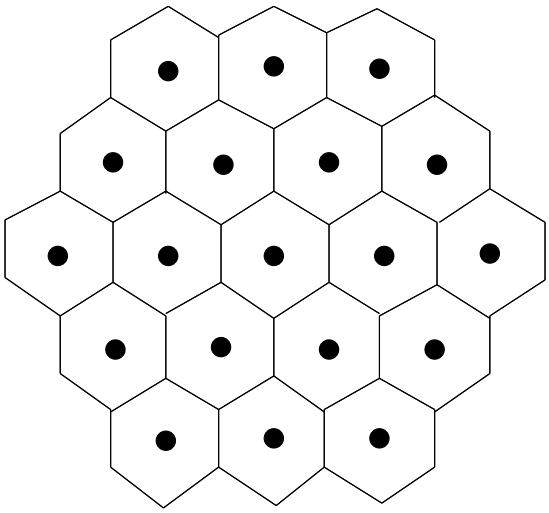
EXEMPLE 2.2
Le Tableau 2.1 fournit une liste des réseaux de points les plus célèbres. Parmi les réseaux les plus importants, citons celui de Schalfli D_4, celui de Gosset E_8, celui de Coxeter-Todd K_{12}, le réseau de Barnes-Wall de dimension 16 Λ_{16} et enfin le fameux réseau de Leech Λ_{24}. Remarquons que la densité Δ est une fonction décroissante de la dimension N, alors que le



(a) Les centres des spheres



(b) Le rangement des spheres



(c) Les cellules de Voronoi

Figure 2.4: Le réseau hexagonal A_2.

coefficient d'erreurs τ est une fonction croissante de N. La 4ème colonne du Tableau 2.1 fournit la densité centrée δ de chaque réseau,

$$\delta = \frac{\Delta}{V_N} = \frac{\rho^N}{det(\Lambda)} \tag{2.4}$$

La densité centrée est souvent plus facile à exprimer que la densité Δ. De plus, lorsque la distance minimale du réseau est égale à 2, l'inverse de la densité centrée nous donne le volume fondamental du réseau.

2.1.3 Performances des réseaux de points

Le but principal de la théorie des réseaux de points dans son application à la théorie des communications numériques est de trouver le réseau le plus dense possible. Cela revient à minimiser l'énergie moyenne de la constellation utilisée et à limiter la probabilité d'erreurs à une borne supérieure fixée par le rayon des sphères (ou bien par la distance minimale). L'espace de travail $\mathbf{R}^N$ étant euclidien, on ne sera donc pas surpris d'avoir de très bonnes performances sur le canal gaussien (canal AWGN).
Supposons qu'un codeur (ou un modulateur) transmette un point $\mathbf{x}$ d'un réseau Λ sur un canal AWGN. Le point reçu $\mathbf{y}$ est donné par $\mathbf{y} = \mathbf{x} + \mathbf{z}$ $(y_i = x_i + z_i,\ i = 1 \dots N)$, où $\mathbf{z}$ est un vecteur représentant le bruit du canal. Les composantes z_i sont des variables gaussiennes de moyenne nulle et de variance σ^2. La constellation C utilisée par le codeur est un sous-ensemble fini du réseau Λ. Ainsi, le volume de cette constellation est fini, d'où une énergie par point bornée. On suppose que C est centrée autour de l'origine pour qu'elle soit une constellation à énergie minimale. A priori, la forme de C est quelconque. Soit n le nombre de points appartenant à C. Ces points seront notés $\mathbf{c}_k$, $k = 1 \dots n$. Sachant qu'un volume fondamental contient un seul point de Λ, le nombre n de points peut être approché par :

$$n = Card(C) \approx \frac{volume\ de\ la\ constellation}{volume\ fondamental} = \frac{vol(C)}{det(\Lambda)} \tag{2.5}$$

Le décodeur placé à l'entrée du récepteur recherche le point de C le plus proche du point reçu $\mathbf{y} = \mathbf{c}_k + \mathbf{z}$. La décision du décodeur reste correcte tant que le point reçu $\mathbf{y}$ appartient à la cellule de Voronoi $V(\mathbf{c}_k)$ du point émis $\mathbf{c}_k$. La probabilité de décision correcte conditionnée par l'émission de $\mathbf{c}_k$ est donnée par :

$$P_c(\mathbf{c}_k emis) = \frac{1}{(\sigma\sqrt{2\pi})^N} \int_{V(\mathbf{c}_k)} e^{-||x-c_k||^2/2\sigma^2} d\mathbf{x} \tag{2.6}$$

Les points de la constellation sont supposés équiprobables, $Prob(\mathbf{c}_k) = 1/n$. Sachant que l'intégrale sur $V(\mathbf{c}_k)$ est égale à l'intégrale sur $V(\mathbf{0})$ (cellule de Voronoi autour de l'origine $\mathbf{0}$), l'expression de la probabilité d'erreurs de la constellation s'écrit sous la forme :

$$P_e = 1 - \frac{1}{(\sigma\sqrt{2\pi})^N} \int_{V(\mathbf{0})} e^{-||x||^2/2\sigma^2} d\mathbf{x} \tag{2.7}$$

N	Λ	Δ	δ	τ
1	$\Lambda_1 = A_1$	1.0	0.5	2
2	$\Lambda_2 = A_2$	0.90690	0.28868	6
3	$\Lambda_3 = D_3$	0.74048	0.17678	12
4	$\Lambda_4 = D_4$	0.61685	0.12500	24
5	$\Lambda_5 = D_5$	0.46526	0.08839	40
6	$\Lambda_6 = E_6$	0.37295	0.07217	72
7	$\Lambda_7 = E_7$	0.29530	0.06250	126
8	$\Lambda_8 = E_8$	0.25367	0.06250	240
10	Λ_{10}	0.09202	0.03608	336
10	P_{10c}	0.09962	0.03906	372
12	Λ_{12}	0.04173	0.03125	648
12	K_{12}	0.04945	0.03704	756
12	P_{12a}	0.04694	0.03516	840
15	Λ_{15}	0.01686	0.04419	2340
16	Λ_{16}	0.01471	0.06250	4320
17	Λ_{17}	0.008811	0.06250	5346
20	Λ_{20}	0.003226	0.12500	17400
24	Λ_{24}	0.001930	1.0	196560
32	Λ_{32}	—	0	208320
32	BW_{32}	—	0	146880
32	Q_{32}	—	1.359	261120
36	Λ_{36}	—	1	—
48	Λ_{48}	—	12	—
64	BW_{64}	—	16	9694080
64	Q_{64}	—	18.719	2611200
64	P_{64c}	—	22	—
128	BW_{128}	—	64	1260230400
128	P_{128b}	—	85	—
128	$\eta(E_8)$	—	88	—
256	BW_{256}	—	192	—
256	$A_{256}^{(22)}$	—	270.89	—
4096	$\eta(\Lambda_{16})$	—	11344	—
65520	$\eta(\Lambda_{24})$	—	311364	—

Table 2.1: Quelques réseaux de points et leurs caractéristiques. La dimension N, le nom Λ, la densité Δ, la densité centrée δ ($log_2(\delta)$ *pour* $N \geq 32$) et le coefficient d'erreur τ.

L'intégrale sur la région $V(\mathbf{0})$ est difficilement calculable (sauf pour quelques réseaux très sympathiques et de faible dimension) et parfois même impossible. Le théorème ci-dessous fournit une expression approchée de P_e valable pour un grand rapport signal à bruit ($\sigma << 1$).

Theorem 1 *(Probabilité d'Erreurs Asymptotique)*
Lorsque la variance σ^2 du bruit gaussien est faible, la probabilité d'erreur de la constellation C s'écrit en fonction de ρ, τ et σ :

$$P_e \approx \frac{\tau}{2} erfc(\frac{\rho}{\sigma\sqrt{2}})$$

Preuve. La formule 2.7 détermine la probabilité d'erreur en intégrant le bruit sur $\mathbf{R}^N - V(\mathbf{0})$ (l'extérieur de la cellule),

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

Soit $\mathbf{u}_j$ ($j = 1 \ldots \tau$) les τ voisins de $\mathbf{0}$. L'hyperplan médiateur de $\mathbf{0} - \mathbf{u}_j$ sépare l'espace $\mathbf{R}^N$ en deux demi-espaces. Le demi-espace contenant $\mathbf{u}_j$ est noté D_j. Le complément de $V(\mathbf{0})$ peut être obtenu par l'union de tous les demi-espaces D_j,

$$\mathbf{R}^N - V(\mathbf{0}) = \bigcup_{j=1\ldots\tau} D_j$$

En appliquant la borne de l'union ($Prob(\bigcup) \leq \sum Prob$), nous majorons P_e par la somme des probabilités,

$$P_e \leq \sum_{j=1}^{\tau} \frac{1}{(\sigma\sqrt{2\pi})^N} \int_{Dj} e^{-||x||^2/2\sigma^2} d\mathbf{x}$$

introduisons la fonction d'erreurs complémentaire,

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-t^2} dt$$

L'origine $\mathbf{0}$ est à une distance ρ de l'hyperplan médiateur le séparant du demi-espace D_j. Par suite, l'intégrale sur D_j s'écrit comme $\frac{1}{2} erfc(\rho/\sigma\sqrt{2})$ et on obtient l'inégalité

$$P_e \leq \frac{\tau}{2} erfc(\frac{\rho}{\sigma\sqrt{2}})$$

L'inégalité se transforme presque en une égalité lorsque σ est très faible (le point reçu reste dans le voisinage très proche du point émis). CQFD.

Le théorème précédent ne met pas en évidence le gain apporté par le réseau de points en termes d'énergie par point ou par bit, pour une probabilité d'erreur fixée. Pour pouvoir

parler d'un gain, il faut comparer les performances de deux réseaux Λ_1 et Λ_2. Nous allons prendre comme référence le réseau entier $\mathbf{Z}^N$. Rappelons que la distance minimale de ce réseau est égale à 1 ($\rho = 1/2$), le coefficient d'erreur $\tau = 2N$ et le volume fondamental $det(\mathbf{Z}^N) = 1$. Le théorème ci-dessous détermine le gain de codage associé à un réseau Λ :

Theorem 2 *(Influence du Rapport Signal à Bruit)*
Soit C une constellation cubique de n points d'un réseau Λ N-dimensionnel. Alors, la probabilité d'erreurs P_e s'écrit en fonction de E_b/N_0 :

$$P_e = \frac{\tau}{2} erfc\left(\sqrt{\frac{3m/N}{2^{2m/N}} \frac{E_b}{N_0} \frac{d_{min}^2}{\sqrt[N/2]{det(\Lambda)}}}\right)$$

où m est le nombre de bits par point de C ($m = log_2(n)$), $N_0/2$ est la densité spectrale du bruit et E_b est l'énergie moyenne par bit.

Preuve. La constellation C est cubique. Elle a la forme d'un cube $[-A, +A]^N$. Pour tous les points $\mathbf{c}_k$, $k = 1 \ldots n$ de C, les composantes $c_{ki}, i = 1 \ldots N$, vérifient $|c_{ki}| < A$. Le volume de C est égal à $(2A)^N$. On obtient donc le nombre de points n en appliquant la formule 2.5,

$$n = \frac{(2A)^N}{det(\Lambda)}$$

Continuons en calculant l'énergie moyenne par point, notée E_p. Cette énergie est l'espérance mathématique de la norme au carré $||\mathbf{c}_k||^2$ des points de C. Mais la constellation C est issue d'un réseau Λ quelconque et il est impossible de trouver l'expression exacte de l'énergie. Ainsi, nous allons approcher E_p par l'énergie moyenne de tous les points $\mathbf{x}$ de $\mathbf{R}^N$ qui appartiennent au cube $[-A, +A]^N$ englobant C,

$$E_p = \int\int\int_{[-A,+A]^N} ||\mathbf{x}||^2 \frac{d\mathbf{x}}{vol(C)} = \int\int\int_{x \in [-A,+A]^N} (x_1^2 + x_2^2 + \ldots + x_N^2) \frac{dx_1 dx_2 \ldots dx_N}{(2A)^N}$$

Cette intégrale est facilement calculable (N intégrale en dimension 1), et nous trouvons

$$E_p = \frac{NA^2}{3}$$

On en déduit l'énergie moyenne par bit,

$$E_b = \frac{E_p}{log_2(n)} = \frac{NA^2}{3m} = \frac{N}{12m} \sqrt[N/2]{2^m det(\Lambda)}$$

Après normalisation du filtre adapté à l'entrée du récepteur, la variance σ^2 d'une composante du bruit additif s'exprime en foncton de la densité spectrale du bruit $N_0/2$ sur le canal par

$$\sigma^2 = \frac{N_0}{2}$$

Les deux dernières formules permettent d'écrire,

$$\frac{E_b}{N_0} = \frac{N \times \sqrt[N/2]{2^m det(\Lambda)}}{24m\sigma^2}$$

Finalement, on applique le théorème 1 en calculant le rapport $\rho/(\sigma\sqrt{2})$,

$$\frac{\rho}{\sigma\sqrt{2}} = \sqrt{\rho^2 \times \frac{1}{2\sigma^2}} = \sqrt{\frac{d_{min}^2}{4} \times \frac{12m/N}{\sqrt[N/2]{2^m det(\Lambda)}} \times \frac{E_b}{N_0}}$$

d'où le résultat énoncé par le théorème. CQFD.

Definition 8 *(Gain Fondamental)*
On appelle gain fondamental *d'un réseau Λ N-dimensionnel, le rapport énergétique*

$$\gamma(\Lambda) = \frac{d_{min}^2}{\sqrt[N/2]{det(\Lambda)}}$$

où d_{min} est la distance minimale de Λ et $det(\Lambda)$ son volume fondamental.

Cette définition est une conséquence directe du théorème 2. En effet, le gain fondamental du réseau $\mathbf{Z}^N$ est $\gamma(\mathbf{Z}^N) = 1$ ($d_{min}(\mathbf{Z}^N) = det(\mathbf{Z}^N) = 1$). Fixons le nombre de bits par dimension (le rapport m/N) et l'énergie par bit (le rapport E_b/N_0). Ainsi, le théorème 2 nous montre que le rapport signal à bruit sous la racine est multiplié par $\gamma(\Lambda)$. Ce gain par rapport au réseau $\mathbf{Z}^N$ dépend uniquement des caractéristiques du réseau, d'où l'appellation gain fondamental. Notons que le gain d'une constellation cubique est lui aussi égal au gain fondamental du réseau Λ. Lorsque la constellation C a une forme non cubique, le gain de C se trouve diminué ou augmenté suivant le moment de second ordre (l'énergie moyenne) de la constellation. Ce moment d'ordre 2 n'est autre que l'énergie E_p calculée au théorème 2. Cette énergie est très liée à la forme de la frontière de $\mathbf{R}^N$ limitant les points de C. Nous allons donc définir le gain total d'une constellation en tenant compte des caractéristiques fondamentales du réseau Λ et de la forme de la constellation :

Definition 9 *(Gain Total)*
Le gain total $\gamma(C)$ *d'une constellation C issue d'un réseau Λ, est le produit du gain fondamental $\gamma(\Lambda)$ par un coefficient $\gamma_s(C)$ appelé* gain de forme,

$$\gamma(C) = \gamma(\Lambda) \times \gamma_s(C)$$

Le gain de forme d'une constellation cubique est égal à 1. Il est évident que la forme sphérique est celle qui minimise l'énergie moyenne de la constellation, puisque les points se trouvent aux endroits les plus proches de l'origine $\mathbf{0}$. Ainsi, le gain de forme $\gamma_s(C)$ est maximal lorsque C possède une forme sphérique. Cette valeur maximale de $\gamma_s(C)$ est

déterminée par le rapport des moments d'ordre 2 (des énergies) d'une sphère (l'intérieur de la sphère) et d'un cube dans l'espace $\mathbf{R}^N$ qui ont le même volume (même nombre de points). Le moment d'ordre 2 d'un cube $[-A,+A]^N$ a été calculé dans la démonstration du théorème 2,

$$||\mathbf{x}||^2_{cube} = \frac{NA^2}{3}$$

Le calcul du moment d'ordre 2 sur le volume de la sphère est moins immédiat. Soit r le rayon de cette sphère qui a le même volume que le cube ($V_N r^N = (2A)^N$), l'énergie moyenne est donnée par :

$$||\mathbf{x}||^2_{sphere} = \int\int\int_{||x||<r} ||\mathbf{x}||^2 \frac{dx_1 dx_2 \ldots dx_N}{vol(sphere)} = \int\int\int_{||x||<r} (x_1^2 + x_2^2 + \ldots + x_N^2) \frac{dx_1 dx_2 \ldots dx_N}{V_N r^N}$$

En utilisant l'intégrale de Dirichlet, et après un changement de variable adéquat ($x = y^2$), nous trouvons

$$||\mathbf{x}||^2_{sphere} = \frac{N \times (V_N r^N)^{2/N} \times (\Gamma(N/2+1))^{2/N}}{\pi \times (N+2)}$$

Rappelons que la fonction $\Gamma(x)$ est définie par

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt \quad x \in \mathbf{R}$$

et qu'elle vérifie les propriétés suivantes :

$$\Gamma(1) = 1 \quad \Gamma(1/2) = \sqrt{\pi} \quad \Gamma(-1/2) = -2\sqrt{\pi}$$

$$\Gamma(x+1) = x\Gamma(x) \quad et \quad \Gamma(n+1) = n! \quad pour\ n\ entier.$$

Rappelons aussi l'intégrale de Dirichlet qui nous a permis de calculer le volume (voir formule 2.3) et le moment d'ordre 2 d'une sphère :

$$\int\int\int_D f(x_1+x_2+\ldots+x_N) x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_N^{\alpha_N} \frac{dx_1 dx_2 \ldots dx_N}{x_1 x_2 \ldots x_N} = \frac{\Gamma(\alpha_1)\Gamma(\alpha_2 \ldots \Gamma(\alpha_N)}{\Gamma(\alpha_1+\alpha_2+\ldots+\alpha_N)} \int_0^1 f(t) t^{\sum \alpha_i - 1} dt$$

l'intégrale N-uple se calcule sur le domaine D de $\mathbf{R}^N$ défini par :

$$D = \left\{ \mathbf{x} \in \mathbf{R}^N \ / \ \mathbf{x} = (x_1, x_2, \ldots, x_N),\ x_1 \geq 0, x_2 \geq 0, \ldots, x_N \geq 0 \ \ et \ \ x_1 + x_2 + \ldots + x_N \leq 1 \right\}$$

Enfin, le gain de forme maximal s'obtient par le rapport :

$$\gamma_s(C)_{max} = \frac{||\mathbf{x}||^2_{cube}}{||\mathbf{x}||^2_{sphere}} = \frac{\pi \times (N+2)}{12 \times \sqrt[N/2]{\Gamma(N/2+1)}} \tag{2.8}$$

Le Tableau 2.2 offre quelques valeurs de $\gamma_s(C)_{max}$ pour des dimensions paires. On montre en appliquant la formule de Stirling ($\sqrt[N]{N!} \rightarrow N/e$) que le gain tend vers $\pi e/6 = 1.53dB$ lorsque N tend vers l'infini.

N	$\gamma_s(C)_{max}$	dB
2	1.05	0.20
4	1.11	0.45
8	1.18	0.73
16	1.25	0.96
24	1.29	1.10
32	1.31	1.17
48	1.34	1.26
64	1.35	1.31

Table 2.2: Le gain de forme maximal.

Λ	$\gamma(\Lambda)(dB)$	$\gamma(\Lambda)+\gamma_s(C)_{max}$
A_2	0.62	0.82
D_4	1.50	1.95
E_8	3.01	3.74
Λ_{16}	4.51	5.47
Λ_{24}	6.02	7.12
Λ_{32} et BW_{32}	6.02	7.19
Q_{32}	6.27	7.44
Λ_{48}	7.52	8.78
BW_{64}	10.39!	11.70!
$Q64$	11.14!	12.45!
$P64c$	12.04!	13.35!

Table 2.3: Gains fondamentaux et gains totaux.

EXEMPLE 2.3
Le gain fondamental $\gamma(\Lambda)$ est invariant si nous transformons Λ par une application composée d'une rotation, d'une symétrie et d'une homothétie : Il est clair que les symétries ou les rotations ne changent pas la distance minimale, ni le volume fondamental. Par contre, une homothétie de rapport α multiplie d_min par α et $det(\Lambda)$ par α^N. Heureusement, le gain fondamental (voir le rapport de la définition 8) reste le même. L'expression du gain fondamental n'est pas facile à utiliser puisqu'il faut déterminer la distance minimale et le volume fondamental du réseau. Ces deux derniers paramètres n'étant pas uniques pour un réseau Λ donné (suite à une transformation de Λ) nous allons exprimer le gain fondamental en fonction de la densité du réseau (la densité d'un réseau est invariante par homothétie, rotation ou symétrie). En combinant la formule 2.4 et la définition 8, nous obtenons :

$$\gamma(\Lambda) = \frac{d_{min}^2}{\sqrt[N/2]{det(\Lambda)}} = 4 \times \sqrt[N/2]{\delta} \tag{2.9}$$

Ainsi, nous formons le Tableau 2.3 qui met en évidence le gain fondamental de quelques réseaux ayant des dimensions paires. La densité centrée δ est extraite du Tableau 2.1. Le gain total maximal est donné par la dernière colonne du Tableau 2.3.

REMARQUE
Le gain effectif d'un réseau est inférieur au gain prévu par le Tableau 2.3, surtout pour les grandes dimensions. En effet, la définition 8 issue du théorème 2 néglige l'influence du coefficient d'erreur τ sur la probabilité d'erreur P_e. Cette dernière est proportionnelle à τ. Signalons que le coefficient d'erreurs est supérieur à 10000 pour $N = 20$ et qu'il est supérieur à 1000000 ! pour $N = 64$. La capacité du canal Gaussien limite le gain réalisable théoriquement à 9dB environ. Par conséquent, les gains fondamentaux des réseaux en dimension 32 et 64 sont fortement atténués par le coefficient d'erreur.

2.2 Les réseaux et les codes correcteurs d'erreurs

Les codes correcteurs d'erreurs servent à construire des empilements de sphères dans l'espace euclidien $\mathbf{R}^N$. Des réseaux de points très denses peuvent être construits à partir d'un code correcteur. D'autres méthodes existent, comme la construction par découpage, par couches et à partir des corps de nombres (voir le chapitre 4). Nous nous limitons dans ce paragraphe à la description de la construction A et la construction B permettant de fabriquer un réseau de points entier en utilisant des codes linéaires binaires. Ces deux constructions seront redéfinies et généralisées dans le paragraphe suivant.

Soit e un entier relatif, $e \in \mathbf{Z}$. On projette e sur la base des puissances de 2 où les composantes sur cette base prennent deux valeurs possibles 0 ou 1 :

$$e = \sum_{j=0}^{\infty} e_j 2^j, \quad e_j \in 0, 1 \tag{2.10}$$

La notation binaire complémentaire est utilisée dans cette dernière expression pour écrire les entiers négatifs. Par exemple, les entiers relatifs 3, -1 et -5 se projettent sous la forme :

$$3 = 1 \times 2^0 + 1 \times 2^1 = (110000\ldots)$$

$$-1 = 1 \times 2^0 + 1 \times 2^1 + 1 \times 2^2 + \ldots = (111111\ldots)$$

$$-5 = 1 \times 2^0 + 1 \times 2^1 + 1 \times 2^3 + \ldots = (110111\ldots)$$

Lorsque e est négatif la somme 2.10 est infinie. En pratique, on peut utiliser l'égalité $e = \sum_{j=0}^{k} e_j 2^j \ (mod\ 2^{k+1})$ pour déterminer les composantes e_j par récurrence.

Definition 10 *(Matrice des Coordonnées)*
Soit $\mathbf{x} = (x_1, x_2, \ldots, x_N)$ *un point de* $\mathbf{Z}^N$. *On appelle* matrice des coordonnées *de* $\mathbf{x}$ *la matrice semi-infinie dont les colonnes sont formées par les projections des composantes entières* x_i *sur la base des puissances de 2.*

Un exemple de matrice des coordonnées : Soit $\mathbf{x} = (4, 3, 2, 1, 0, -1, -2, -3)$ un point de $\mathbf{Z}^8$. La matrice des coordonnées de $\mathbf{x}$ s'écrit,

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \begin{matrix} ligne\ mod\ 2 \\ ligne\ mod\ 4 \\ ligne\ mod\ 8 \\ ligne\ mod\ 16 \\ \ldots\ldots \end{matrix}$$

Le nombre de lignes est infini, mais elles deviennent identiques au-dessus d'un certain rang. La ligne numéro i est appelée *ligne mod* 2^i, $i = 1 \ldots \infty$.

Soit C un code binaire (N, K, d). La procédure suivante définit les centres des sphères d'un empilement entier de $\mathbf{R}^N$:

Definition 11 *(Construction A)*
$\mathbf{x} = (x_1, x_2, \ldots, x_N)$ *est un point de l'empilement si et seulement si* $\mathbf{x}$ *est congru modulo 2 à un mot du code* C.

Un point $\mathbf{x}$ appartient à l'empilement défini par la construction A si et seulement si la ligne mod-2 de $\mathbf{x}$ appartient au code C. L'empilement est un réseau de points si C est linéaire. La définition 11 se traduit par une formule liant le réseau Λ à C et $\mathbf{Z}^N$,

$$\Lambda = C + 2\mathbf{Z}^N \tag{2.11}$$

Les caractéristiques d'un réseau issu de la construction A s'énoncent comme suit :

Theorem 3 *Soit* Λ *un réseau défini par la construction A,* $\Lambda = C + 2\mathbf{Z}^N$, *où* C *est un code linéaire binaire* (N, K, d). *Alors, la densité centrée* δ, *le rayon d'empilement* ρ *et le coefficient d'erreur* τ *sont donnés par :*

$$\delta = 2^K \rho^N 2^{-N}$$

$$\rho = \frac{1}{2} min(2, \sqrt{d})$$

$$\tau = \begin{cases} 2^d A_d & si\ d < 4 \\ 2N + 16A_4 & si\ d = 4 \\ 2N & si\ d > 4 \end{cases}$$

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

Preuve. Les mots du code C forment les points de Λ qui appartiennent au cube unité placé à l'origine, $\left\{\mathbf{x} \in \mathbf{R}^N \ / \ 0 \leq x_i \leq 1,\ i = 1 \ldots N\right\}$. Les 2^K mots de code sont situés sur les sommets de ce cube $1 \times 1 \times \ldots \times 1$. Tous les autres points de Λ s'obtiennent en ajoutant des composantes entières paires aux mots de ce code. Cela correspond à la translation du cube unité de 2 dans toutes les directions. Ainsi, un cube $2 \times 2 \times \ldots \times 2$ ne contient que 2^K points de Λ. Chaque point étant le centre d'une sphère de rayon ρ, le volume $2 \times 2 \times \ldots \times 2$ contient exactement 2^K sphères. La densité de Λ en découle,

$$\Delta = \frac{volume\ des\ 2^K\ spheres}{volume\ du\ cube\ 2\times 2\times \ldots \times 2} = \frac{2^K \times V_N \rho^N}{2^N} \text{ et } \delta = \frac{\Delta}{V_N} = 2^K \rho^N 2^{-N}.$$

Si deux points distincts $\mathbf{x}$ et $\mathbf{y}$ de Λ sont congrus modulo 2 au même mot de code ($\mathbf{x}$ et $\mathbf{y}$ ont la même ligne mod-2 dans la matrice des coordonnées), alors la distance entre $\mathbf{x}$ et $\mathbf{y}$ est supérieure ou égale à 2 (c'est la distance minimale dans $2\mathbf{Z}^N$). Si $\mathbf{x}$ et $\mathbf{y}$ sont congrus modulo 2 à deux mots de code différents (les deux lignes mod-2 sont différentes), alors ils doivent avoir au moins d composantes qui diffèrent de 1. Par conséquent, leur distance $||\mathbf{x}-\mathbf{y}||$ est supérieure ou égale à $\sqrt{d}$. En combinant les deux raisonnements, la distance minimale d_{min} de Λ s'écrit comme le minimum de 2 et $\sqrt{d}$,

$$d_{min}(\Lambda) = min(2, \sqrt{d}) \text{ et } \rho = \frac{d_{min}}{2} = \frac{1}{2} min(2, \sqrt{d}).$$

Le coefficient d'erreur est déterminé en calculant le nombre de voisins à distance d_{min} de l'origine $\mathbf{0}$. Il existe $2N$ points à distance 2 de l'origine (les points de la forme $(\pm 2, 0^{n-1})$). Le nombre de mots de code de poids d est égal à A_d. En ajoutant -2 à une composante égale à 1, nous pouvons la transformer en -1. Ainsi, il existe au total $2^d A_d$ points de Λ à une distance $\sqrt{d}$ de l'origine (les points de la forme $(\pm 1^d, 0^{N-d})$). Le résultat énoncé par le théorème s'obtient par une comparaison des deux valeurs possibles ($\sqrt{d}$ et 2) de la distance minimale. CQFD.

Un réseau de points provenant d'une construction A est généré par les K vecteurs de la base du code C et par $N-K$ vecteurs d'une partie de $2\mathbf{Z}^N$. Lorsque la matrice génératrice du code est de forme systématique, $\mathbf{G} = [\mathbf{I}|\mathbf{P}]$, il est facile d'écrire une matrice génératrice du réseau Λ sous la forme,

$$M = \begin{pmatrix} \mathbf{I} & \mathbf{P} \\ \mathbf{0} & 2\mathbf{I} \end{pmatrix}$$

EXEMPLE 2.4

Les réseaux "checkerboard" notés D_N s'obtiennent par construction A à partir d'un code de parité $(N, N-1, 2)$. Parmi ces réseaux, nous citons le réseau fcc D_3 et le réseau de Schlafli D_4. Les réseaux D_N sont les plus denses en dimensions $N = 3, 4, 5$ seulememt. Le plus dense réseau en dimension 6, E_6, s'obtient par une construction A complexe, ou bien par couches à partir de D_3. Voici les propriétés des réseaux D_N :

$$Formule \ : \ D_N = 2\mathbf{Z}^N + (N, N-1, 2)$$

$$Matrice\ Generatrice \ : \ M = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & \dots & 0 \\ 1 & 0 & 1 & \dots & 0 \\ & \dots & & \dots & \\ 1 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$Rayon\ d'Empilement \ : \ \rho = \frac{\sqrt{2}}{2}$$

$$Densite\ Centree\ :\ \delta = 2^{-(N+2)/2}$$
$$Coefficient\ d'Erreur\ :\ \tau = 2N(N-1)$$

Les réseaux E_6, E_7 et E_8 sont les plus denses en dimension 6, 7 et 8 respectivement. Tous les trois s'obtiennent par la construction A. Le code binaire (7,3,4) (le dual du code de Hamming (7,4,3)) est associé à E_7, alors que le Hamming étendu (Reed-Muller) (8,4,4) permet de construire E_8. Voici les propriétés de ces deux réseaux :

Formules :

$$E_7 = 2\mathbf{Z}^7 + (7,3,4)$$
$$E_8 = 2\mathbf{Z}^8 + (8,4,4)$$

Matrices Generatrices :

$$M_{E_7} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$M_{E_8} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$Rayon\ d'Empilement\ :\ \rho(E_7) = \rho(E_8) = 1$$
$$Densites\ Centrees\ :\ \delta(E_7) = \delta(E_8) = 2^{-4}$$
$$Coefficients\ d'Erreur\ :\ \tau(E_7) = 126\ \ et\ \ \tau(E_8) = 240$$

La construction B ajoute une contrainte supplémentaire (par rapport à celle imposée par la construction A sur la ligne mod-2 de la matrice des coordonnées) sur la ligne mod-4. Soit C_0 un code binaire (N, K, d) dont les mots de code sont tous de poids pair. Un empilement de sphères dans $\mathbf{R}^N$ se construit par la procédure,

Definition 12 *(Construction B)*
$\mathbf{x} = (x_1, x_2, \ldots, x_N)$ *est un point de l'empilement si* $\mathbf{x}$ *est congru (modulo 2) à un mot du code* C_0 *et si* $\sum_{i=1}^{N} x_i$ *est divisible par 4.*

Un point $\mathbf{x}$ de $\mathbf{Z}^N$ appartient à l'empilement d'une construction B si et seulement si sa ligne mod-2 est un mot $\mathbf{c}$ appartenant à C_0 et si sa ligne mod-4 a un poids pair lorsque le poids de $\mathbf{c}$ est divisible par 4, ou bien un poids impair lorsque le poids de $\mathbf{c}$ est divisible par 2 et non divisible par 4. L'empilement est un réseau de points si le code est linéaire. Lorsque tous les poids de C_0 sont divisibles par 4, le réseau est donné par la formule

$$\Lambda = C_0 + 2C_1 + 4\mathbf{Z}^N \tag{2.12}$$

où C_1 est le code de parité $(N, N-1, 2)$. De plus, $C_0 \subset C_1$ puisque les poids de C_0 sont divisibles par 2. Les propriétés dérivant de la construction B s'énoncent :

Theorem 4
Soit Λ *un réseau défini par la construction B,* $\Lambda = C_0 + 2C_1 + 4\mathbf{Z}^N$*, où* C_0 *est un code linéaire binaire* (N, K, d) *de poids divisible par 4,* $C_0 \subset C_1$ *et* C_1 *est le code de parité. Alors, la densité centrée* δ*, le rayon d'empilement* ρ *et le coefficient d'erreur* τ *sont donnés par :*

$$\delta = 2^K \rho^N 2^{-N-1}$$

$$\rho = \frac{1}{2} min(\sqrt{8}, \sqrt{d})$$

$$\tau = \begin{cases} 2^{d-1} A_d & si\ d < 8 \\ 2N(N-1) + 128 A_8 & si\ d = 8 \\ 2N(N-1) & si\ d > 8 \end{cases}$$

Preuve. Le nombre de sphères dans le cube $2 \times 2 \times \ldots \times 2$ a été divisé par 2 suite à la contrainte de parité sur la ligne mod-4, d'où $\delta = 2^K \rho^N 2^{-N-1}$. Le rayon d'empilement est déterminé en répétant le même raisonnement que celui du théorème 3. La distance minimale de 2 dans $2\mathbf{Z}^N$ se trouve remplacée par celle de $2C_1$. Deux mots de C_1 diffèrent de 1 dans deux composantes au moins (la distance de Hamming minimale d'un code de parité est 2). La distance minimale dans $2C_1$ est donc égale à $\sqrt{8}$. Le coefficient d'erreurs, comme dans le théorème 3, est déterminé en calculant le nombre de voisins à distance $d_{min}(\Lambda) = 2\rho$ de l'origine $\mathbf{0}$. Il existe $2N(N-1)$ points de la forme $(\pm 2^2, 0^{N-2})$ à une distance $\sqrt{8}$ de l'origine. De plus, le nombre de points à une distance $\sqrt{d}$ est $2^{d-1} A_d$ (les points $(\pm 1^d, 0^{N-d})$ avec un nombre pair de signes - si d est divisible par 4, et un nombre impair de signes - si d est divisible par 2 et non par 4). En comparant d et 8, on trouve le résultat énoncé ci-dessus. CQFD.

EXEMPLE 2.5
Nous appliquons la construction B au code à répétition (8,1,8) formé des deux mots de code 0^8 et 1^8. Nous obtenons de nouveau le réseau E_8. En effet, ce dernier réseau est une version du réseau E_8 obtenu par construction A. Cette version s'écrit :

$$RE_8 = 4\mathbf{Z}^8 + 2(8,7,2) + (8,1,8)$$

où R est l'opérateur rotation défini dans l'Exemple 2.8. Dans l'espace $\mathbf{R}^9$, l'application de la construction B au code formé des deux mots 0^9 et 1^80 donne naissance au réseau Λ_9 (le plus dense connu en dimension 9) :

$$\rho(\Lambda_9) = \sqrt{2} \quad \delta(\Lambda_9) = 2^{-4.5} \quad \tau(\Lambda_9) = 272$$

En dimension 16, le réseau Λ_{16} est formé par le code de Reed-Muller d'ordre 1

$$\Lambda_{16} = 4\mathbf{Z}^{16} + 2(16,15,2) + (16,5,8)$$

$$\rho(\Lambda_{16}) = \sqrt{2} \quad \delta(\Lambda_{16}) = 2^{-4} \quad \tau(\Lambda_{16}) = 4320$$

La matrice génératrice de Λ_{16} s'écrit :

$$M_{\Lambda_{16}} = \begin{bmatrix}
4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 2 & 0 & & & & & & & & & & & & & 0 \\
2 & 0 & 2 & 0 & & & & & & & & & & & & 0 \\
2 & 0 & 0 & 2 & 0 & & & & & & & & & & & 0 \\
2 & 0 & & 0 & 2 & 0 & & & & & & & & & & 0 \\
2 & 0 & & & 0 & 2 & 0 & & & & & & & & & 0 \\
2 & 0 & & & & 0 & 2 & 0 & & & & & & & & 0 \\
2 & 0 & & & & & 0 & 2 & 0 & & & & & & & 0 \\
2 & 0 & & & & & & 0 & 2 & 0 & & & & & & 0 \\
2 & 0 & & & & & & & 0 & 2 & 0 & & & & & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & & & & 0 \\
1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & & & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}$$

Finalement, un réseau très intéressant obtenu par la construction B est le réseau demi-Leech H_{24}. L'union de deux cosets de H_{24} forme une version du réseau Leech Λ_{24} (voir paragraphe 2.3.2). Le réseau demi-Leech s'écrit en fonction du code de Golay étendu (24,12,8) et du code de parité (24,23,2) :

$$H_{24} = 4\mathbf{Z}^{24} + 2(24,23,2) + (24,12,8)$$

$$\rho(H_{24}) = \sqrt{2} \quad \delta(H_{24}) = 1/2 \quad \tau(H_{24}) = 98256$$

2.3 Partitionnement et construction généralisée

La matrice des coordonnées, décrite au paragraphe 2.2, se traduit par le partitionnement du réseau $\mathbf{Z}$ en deux classes d'équivalences. Chacune des deux classes est partitionnée à son tour, et ainsi de suite. La chaine de partitionnement $\mathbf{Z}/2\mathbf{Z}/4\mathbf{Z}/8\mathbf{Z}/\ldots$ permet d'écrire $\mathbf{Z}$ sous la forme d'une séquence de classes d'équivalences (cosets), $\mathbf{Z} = [\mathbf{Z}/2\mathbf{Z}]+[2\mathbf{Z}/4\mathbf{Z}]+[4\mathbf{Z}/8\mathbf{Z}]+\ldots$ Le code C_0 des constructions A et B sélectionne une suite de classes d'équivalence dans le groupe quotient $\mathbf{Z}/2\mathbf{Z}$. Le code C_1 de la construction B, sélectionne une suite de classes dans le groupe $2\mathbf{Z}/4\mathbf{Z}$. Ainsi, l'application d'un code à une ligne mod-2^i de la matrice des coordonnées revient à sélectionner une suite de classe d'équivalence par un code C_{i-1}.
La forme générale de la construction d'un réseau devient :

$$\Lambda = C_0 + 2C_1 + 4C_2 + \ldots + 2^{j-1}C_{j-1} + 2^j\mathbf{Z}^N.$$

Nous présentons au sous-paragraphe 2.3.1 les notions algébriques indispensables à la suite du paragraphe. Nous allons rappeler les principaux résultats de la décomposition des réseaux en classes d'équivalence. La décomposition en classes d'équivalence s'applique à n'importe quel ensemble muni d'une structure de groupe. Cet ensemble peut être un code correcteur d'erreur linéaire ou un réseau de points. La structure de groupe associée à ces ensembles sera toujours additive.

Nous poursuivons le paragraphe par l'étude des réseaux binaires mod-2 et mod-4 et des réseaux complexes. Nous présenterons la construction de Barnes-Wall à partir des codes de Reed-Muller et un tableau de formules des plus importants réseaux.

2.3.1 Le partitionnement des groupes

Soit S un ensemble discret et soit $s \in S$ un élément de S. Les M sous-ensembles disjoints $T(a)$ (où a est une étiquette) forment une partition M-aire de S si leur union est égale à S. Une telle partition sera notée S/T. Le nombre M de sous-ensembles est appelé "ordre de la partition" et sera noté $M = |S/T|$. L'étiquette a est un vecteur formé de K bits lorsque M est une puissance de 2, $M = 2^K$. Si S est un groupe additif, la notation $T(a)$ est remplacée par $T + a$, où T est un sous-groupe de S et a un élément de $S - T$.

Un exemple très simple de partitionnement est celui de l'anneau des entiers relatifs $\mathbf{Z}$. L'anneau est partitionné en deux sous-ensembles, $2\mathbf{Z}$ et $2\mathbf{Z} + 1$, séparant ainsi les nombres pairs des nombres impairs. Cette partition $\mathbf{Z}/2\mathbf{Z}$ est binaire (d'ordre 2). Naturellement, l'étiquette a prend deux valeurs possibles : 0 ou 1.

Une chaine de partitionnement de niveau m, $S_0/S_1/\ldots/S_m$, est obtenue en répétant m fois le partitionnement des sous-ensembles. C'est-à-dire, S_0 est partitionné en $|S_0/S_1|$ sous-ensembles notés $S_1(a_0)$, puis les ensembles $S_1(a_0)$ sont eux-mêmes partitionnés et ainsi de suite. Nous supposons que l'ordre de la partition est identique pour tous les sous-ensembles situés au même niveau. Par suite, l'ordre de la partition totale est le produit des ordres des partitions intermédiaires,

$$|S_0/S_m| = |S_0/S_1| \times |S_1/S_2| \times \ldots \times |S_{m-1}/S_m| \tag{2.13}$$

L'étiquette a de la partition totale S_0/S_m est formée de m composantes, $a = (a_0, a_1, \ldots, a_{m-1})$, où a_j représente l'étiquette associée à la partition S_j/S_{j+1}.
Soit S^N le produit cartésien de l'ensemble S. S^N est l'ensemble de N-uples à composantes dans S. Si T est un sous-ensemble partageant S en $|S/T|$ sous-ensembles, T^N partitionne lui aussi S^N et l'ordre de cette partition vérifie

$$|S^N/T^N| = |S/T|^N \tag{2.14}$$

Definition 13 *(Congruence)*
Soit T un sous-groupe d'un groupe S, et soient s et s' deux éléments de S. s est congru (ou équivalent) à s' modulo T si $s - s' \in T$.

Lorsque s est congru à s' modulo T, on écrira $s = s' \ (modT)$. La relation de congruence est une relation d'équivalence (elle est réflexive, symétrique et transitive). Elle partitionne le groupe S en des classes d'équivalence disjointes. La partition S/T contient $|S/T|$ classes d'équivalence. La classe d'équivalence $T(c)$ d'un élément c de S est $\{s \in S \ / \ s - c \in T\}$. Un élément s de cette classe s'écrit $s = t + c$, où $t \in T$. Par conséquent, la classe $T(c)$ n'est autre que $T + c$.

Definition 14 *(Coset ou Classe d'Equivalence)*
La classe $T + c$ est appelée coset *du sous-groupe T dans le groupe S. L'élément c est appelé "représentant" du coset $T + c$.*

Notons que le représentant d'un coset n'est pas unique (un élément quelconque appartenant au coset). La classe de l'élément 0 du groupe S n'est autre que le coset $T+0 = T$. L'élément nul sera toujours choisi comme représentant du coset T. L'ensemble des représentants des cosets est noté $[S/T]$.
Le groupe S est l'union de $|S/T|$ cosets $T + c$, $c \in [S/T]$. Tout élément s de S est la somme d'un représentant c et d'un élément t de T, $s = t + c$. D'où la formule énoncée par la définition suivante :

Definition 15 *(Décomposition en Cosets)*
Soit T un sous-groupe de S. Le groupe S se décompose en $|S/T|$ cosets de T par la partition S/T et nous pouvons écrire :

$$S = [S/T] + T \tag{2.15}$$

L'ensemble des cosets forme un groupe appelé *groupe quotient*, noté lui aussi par S/T. L'ordre du groupe quotient est égal à celui de la partition. Lorsque S est un groupe d'ordre fini, on a :

$$|S| = |T| \times |S/T| \tag{2.16}$$

et l'ordre du sous-groupe T divise celui de S. Si $|S| = 2^K$, S est dit *groupe binaire*. Les sous-groupes d'un groupe binaire sont tous binaires.

La décomposition en cosets 2.15 se généralise pour une séquence de groupes imbriqués (S_{j+1} sous-groupe de S_j). En effet, la chaine de partitionnement $S_0/S_1/\ldots/S_m$ permet d'écrire la formule :

$$S_0 = [S_0/S_1] + [S_1/S_2] + \ldots + [S_{m-1}/S_m] + S_m \tag{2.17}$$

La chaine de partitionnement est dite *binaire* si $|S_0/S_m| = 2^K$. En appliquant 2.13, on trouve que les partitions intermédiaires sont toutes binaires. Cela se traduit par $|S_j/S_{j+1}| = 2^{K_j}$ et $K = \sum K_j$.

Theorem 5
Soit S un groupe fini binaire, $|S| = 2^K$ $(K > 0)$. Alors, S contient au moins un élément non nul g d'ordre 2. En d'autres termes, le sous-groupe engendré par g est réduit à l'ensemble $\{0, g\}$.

Preuve. Rappelons qu'un élément s de S engendre un sous-groupe par la suite $s, s+s, s+s+s, s+s+s+s, \ldots$. Cette séquence est nécessairement finie puisque les éléments sont en nombre fini dans S. L'expression 2.16 montre en plus que l'ordre de s divise celui de S.
Soit s un élément non nul de S. Considérons la suite $s, 2s, 4s, 6s, \ldots$. Il existe un entier m pour lequel $2ms = 0$ ($ms = s + s + \ldots + s$ m fois) car le nombre d'éléments dans la suite est fini. Posons $g = ms$. L'élément g est non nul et $g + g = 0$. CQFD.

0000	1010	0101	1111
0001	1011	0100	1110
0010	1000	0111	1101
0011	1001	0110	1100

Table 2.4: Décomposition en cosets de $GF(2)^4$.

Theorem 6
Soit S un groupe fini binaire, $|S| = 2^K$ $(K > 0)$. Alors, tout élément s de S s'écrit comme une combinaison linéaire binaire de K éléments de S appelés générateurs *et notés g_k, $k = 0 \ldots K-1$,*

$$s = \sum_{k=0}^{K-1} a_k g_k, \quad avec \quad a_k \in \{0, 1\}$$

Preuve. Soit g_{K-1} un élément d'ordre 2 de S. Posons $T = a_{K-1} g_{K-1} = \{0, g_{K-1}\}$. T est le sous-groupe engendré par g_{K-1}. Décomposons S par la partition S/T, $S = T + [S/T]$. Le sous-groupe $[S/T]$ (ou le groupe quotient S/T) est d'ordre 2^{K-1}. En cherchant un élément g_{K-2} d'ordre 2 de $[S/T]$ et en répétant la même décomposition ($K-1$ fois en total), on trouve le résultat énoncé par le théorème. CQFD.

EXEMPLE 2.6
Soit C le code linéaire de longueur $N = 4$ et de dimension $K = 2$ défini sur $GF(2)$ et engendré par la base $(1, 0, 1, 0)$ et $(0, 1, 0, 1)$. Les quatre mots de code sont formés par les combinaisons linéaires des deux vecteurs de la base

$$C = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$$

C est un sous-espace vectoriel de $GF(2)^4$ et donc un sous-groupe additif de cet espace. Le tableau 2.4 montre la décomposition en cosets de C du groupe $GF(2)^4$.

$$GF(2)^4 = C + [GF(2)^4/C]$$

$$|GF(2)^4| = 16 = |C| \times |GF(2)^4/C| = 4 \times 4$$

Les lignes du tableau 2.4 forment les quatre cosets (la première ligne = le code C) et la première colonne contient le représentant de chaque coset. Ainsi,

$$[GF(2)^4/C] = \{(0000), (0001), (0010), (0011)\}$$

C'est un groupe binaire généré par les deux vecteurs (0001) et (0010).

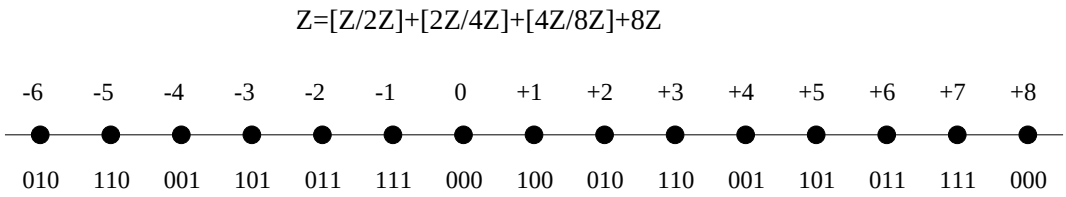


Figure 2.5: Partitionnenemnt de la droite entière.

EXEMPLE 2.7
Considérons l'anneau des entiers relatifs $\mathbf{Z}$. L'ensemble $2\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$. On a ainsi la partition $\mathbf{Z}/2\mathbf{Z}$, ou bien $\mathbf{Z} = 2\mathbf{Z} + [\mathbf{Z}/2\mathbf{Z}]$. Le groupe $[\mathbf{Z}/2\mathbf{Z}]$ contient deux éléments, 0 et 1.
Considérons la chaine de partitionnement binaire $\mathbf{Z}/2\mathbf{Z}/4\mathbf{Z}/8\mathbf{Z}/\ldots$ En appliquant la formule 2.15, la décomposition de $\mathbf{Z}$ se généralise à

$$\mathbf{Z} = [\mathbf{Z}/2\mathbf{Z}] + [2\mathbf{Z}/4\mathbf{Z}] + [4\mathbf{Z}/8\mathbf{Z}] + \ldots$$

Ce partitionnement représente la projection d'un entier sur la base des puissances de 2 (Formule 2.10). De la même manière, la matrice des coordonnées est associée à la décomposition de $\mathbf{Z}^N$ sous la forme

$$\mathbf{Z}^N = [\mathbf{Z}^N/2\mathbf{Z}^N] + [2\mathbf{Z}^N/4\mathbf{Z}^N] + [4\mathbf{Z}^N/8\mathbf{Z}^N] + \ldots$$

La Figure 2.5 montre le partitionnement $\mathbf{Z}/2\mathbf{Z}/4\mathbf{Z}/8\mathbf{Z}$ de niveau 3 d'une constellation entière de 15 points.

Theorem 7
Soit Λ' un sous-réseau d'un réseau de points Λ. Alors, l'ordre de la partition Λ/Λ' est égal au rapport des volumes fondamentaux,

$$det(\Lambda') = |\Lambda/\Lambda'| \times det(\Lambda)$$

Preuve. Le réseau Λ s'écrit $\Lambda = \Lambda' + [\Lambda/\Lambda']$. Il est l'union de $|\Lambda/\Lambda'|$ cosets de Λ'. Dans un volume contenant $|\Lambda/\Lambda'|$ points de Λ, il y a un seul point appartenant à Λ'. D'où le résultat. D'une autre façon, nous pouvons écrire que l'espace global $\mathbf{R}^N$ est donné par

$$\mathbf{R}^N = \Lambda + P(\Lambda)$$

où $P(\Lambda)$ est le parallélotope fondamental de Λ. Ainsi, $\mathbf{R}^N$ est l'union d'un nombre infini de cosets de Λ. En introduisant la partition Λ/Λ', l'espace $\mathbf{R}^N$ devient

$$\mathbf{R}^N = \Lambda' + [\Lambda/\Lambda'] + P(\Lambda) = \Lambda' + P(\Lambda')$$

Nous voyons donc que le parallélotope fondamental de Λ' est l'union de $|\Lambda/\Lambda'|$ copies de $P(\Lambda)$, d'où un volume $|\Lambda/\Lambda'|$ fois plus grand. CQFD.

Une conséquence directe du théorème 7 est la relation $det(\Lambda) = |\mathbf{Z}^N/\Lambda|$, si Λ est un réseau entier N-dimensionnel. Il suffit d'appliquer le théorème 7 sachant que le volume fondamental de $\mathbf{Z}^N$ est égale à 1, $det(\mathbf{Z}^N) = 1$.

EXEMPLE 2.8 (L'Opérateur Rotation)
Nous allons fabriquer une partition binaire du réseau $\mathbf{Z}^2$ (grillage du plan complexe) à partir d'un sous-réseau obtenu par transformation de $\mathbf{Z}^2$. Soit l'opérateur rotation R défini par la matrice 2×2 :

$$R = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Appliquons l'opérateur R au réseau $\mathbf{Z}^2$ pour le transformer en un réseau noté $R\mathbf{Z}^2$. Ce dernier est un sous-réseau de $\mathbf{Z}^2$. La partition $\mathbf{Z}^2/R\mathbf{Z}^2$ est d'ordre 2. Le réseau plan $\mathbf{Z}^2$ est l'union de deux cosets de $R\mathbf{Z}^2$,

$$\mathbf{Z}^2 = R\mathbf{Z}^2 + [\mathbf{Z}^2/R\mathbf{Z}^2] = (R\mathbf{Z}^2 + (0,0)) \bigcup (R\mathbf{Z}^2 + (1,0))$$

Les points noirs de la Figure 2.6 représentent $R\mathbf{Z}^2$ et les points blancs forment son coset $R\mathbf{Z}^2 + (1,0)$. Remarquons d'après cette même figure que $R\mathbf{Z}^2$ est une version de $\mathbf{Z}^2$ (par homothétie et rotation). Il possède donc le même gain fondamental $\gamma(\mathbf{Z}^2) = \gamma(R\mathbf{Z}^2) = 1$. Cela peut être vérifié en calculant directement le gain de $R\mathbf{Z}^2$: $d^2_{min}(R\mathbf{Z}^2) = 2$, $det(R\mathbf{Z}^2) = |\mathbf{Z}^2/R\mathbf{Z}^2| = 2 \implies \gamma(R\mathbf{Z}^2) = 1$.

L'opérateur R vérifie $R^2 = 2I$, où I est la matrice identité. Par suite, $R^2\mathbf{Z}^2 = 2\mathbf{Z}^2$ (R double le carré de la distance). De plus, la matrice R se décompose en un produit

$$R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{bmatrix} \times \sqrt{2} = \begin{bmatrix} \sqrt{2}/2 & \sqrt{2}/2 \\ \sqrt{2}/2 & -\sqrt{2}/2 \end{bmatrix} \times \sqrt{2}$$

La transformation R est ainsi composée d'une homothétie de $\sqrt{2}$, d'une rotation de 45^o et d'une symétrie par rapport à la première bissectrice. Plus simple encore, R est composée d'une homothétie de $\sqrt{2}$ et d'une symétrie par rapport à la droite passant par l'origine et inclinée de 22.5^o.
L'opérateur rotation est défini en dimension $2N$ par l'application de R sur chaque paire de composantes. L'opérateur en dimension 4 par exemple s'écrit :

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

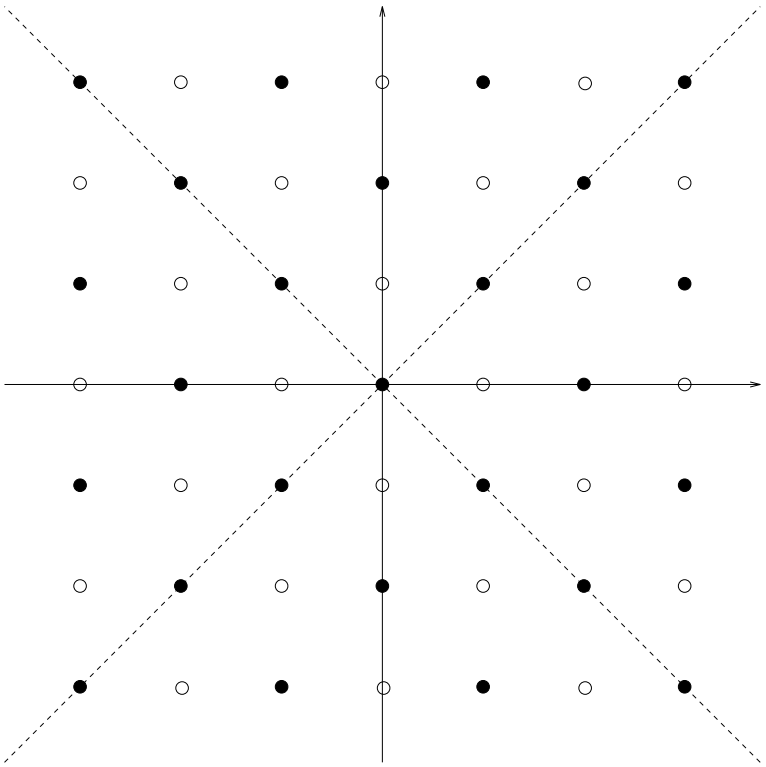


Figure 2.6: La partition $\mathbf{Z}^2/R\mathbf{Z}^2$.

EXEMPLE 2.9 (Le Réseau de Schlafli)
Le réseau D_4 (voir l'Exemple 2.4) est l'ensemble des vecteurs de $\mathbf{Z}^4$ qui possèdent un nombre pair de composantes impaires (ou bien les vecteurs dont le carré de la norme est pair). L'ordre de la partition $\mathbf{Z}^4/D_4$ est 2, car $\mathbf{Z}^4$ est l'union de D_4 et de son coset $D_4+(1,0,0,0)$ (l'ensemble des vecteurs à composantes impaires en nombre impair, c'est-à-dire le carré de la norme est impair). D'après le théorème 7 $det(D_4) = 2$. Il est évident en plus que $d^2_{min}(D_4) = 2$. Par conséquent, $\gamma(D_4) = \sqrt{2} = 1.51dB$.
Le réseau $R\mathbf{Z}^4$ est un sous-réseau de D_4. Cela s'explique par le fait que l'opérateur R double le carré des normes. Tout point de $R\mathbf{Z}^4$ appartient donc à D_4. La chaine de partitionnement $\mathbf{Z}^4/D_4/R\mathbf{Z}^4$ est binaire. En effet,

$$|\mathbf{Z}^4/R\mathbf{Z}^4| = (\sqrt{2})^4 = 4$$

$$|\mathbf{Z}^4/R\mathbf{Z}^4| = |\mathbf{Z}^4/D_4| \times |D_4/R\mathbf{Z}^4| = 2 \times |D_4/R\mathbf{Z}^4|$$
$$=> \quad |D_4/R\mathbf{Z}^4| = 2$$

La chaine de partitionnement se prolonge sans aucune difficulté et devient

$$\mathbf{Z}^4/D_4/R\mathbf{Z}^4/RD_4/2\mathbf{Z}^4/2D_4/2R\mathbf{Z}^4/2RD_4/\ldots$$

Il suffit de remarquer que $D_4 \subset \mathbf{Z}^4 \ => \ RD_4 \subset R\mathbf{Z}^4$ et que $R^2D_4 = 2D_4 \subset R^2\mathbf{Z}^4 = 2\mathbf{Z}^4$, et ainsi de suite.

Definition 16 *(Réseau Complexe)*
On appelle réseau complexe *N-dimensionnel, tout sous-groupe discret de rang N de $\mathbf{C}^N$, où $\mathbf{C}$ est le corps des nombres complexes.*

Tout réseau complexe de dimension N est isomorphe à un réseau réel de dimension $2N$. Le réseau réel s'obtient en décomposant chaque composante complexe en partie réelle et partie imaginaire. Un réseau Λ possède les mêmes propriétés (volume fondamental et distance minimale), qu'il soit considéré réel ou complexe. La seule différence entre réseaux réels et complexes se trouve dans les opérations multiplicatives. Par exemple, le produit scalaire $\mathbf{x}.\mathbf{y} = x_1y_1 + x_2y_2 + \ldots + x_{2N}y_{2N}$ entre deux points $\mathbf{x}$ et $\mathbf{y}$ d'un réseau réel se transforme en un produit hermitien $\mathbf{x}.\mathbf{y} = x_1y_1^* + x_2y_2^* + \ldots + x_Ny_N^*$ dans un réseau complexe.

Definition 17 *(L'Anneau des Gaussiens)*
*Soit $i = \sqrt{-1}$ l'élément imaginaire. L'*anneau gaussien *est un sous-ensemble de $\mathbf{C}$ formé par*

$$\mathbf{G} = \mathbf{Z}[i] = \{a + ib \ / \ a \ et \ b \ \in \mathbf{Z}\}$$

Les éléments de l'anneau gaussien sont appelés *entiers gaussiens*. L'anneau $\mathbf{G}$ est l'exemple le plus simple de réseau complexe. G est un réseau complexe de dimension 1 isomorphe au réseau réel $\mathbf{Z}^2$ de dimension 2. De plus, $\mathbf{G}$ possède une structure d'anneau tout à fait semblable à celle de l'anneau $\mathbf{Z}$. Les unités de $\mathbf{G}$ sont les éléments ± 1 et $\pm i$. Un entier

gaussien est premier s'il est divisible par lui-même et par les unités seulement. L'élément $\phi = 1+i$ est l'entier gaussien premier ayant le plus petit module, $|\phi|^2 = 2$, alors que $\phi^2 = 2i$.

Soit g un entier gaussien. L'ensemble $g\mathbf{G}$ est un sous-réseau de $\mathbf{G}$, et la partition $\mathbf{G}/g\mathbf{G}$ est d'ordre $|g|^2$. Cela est une conséquence du théorème 7, car g augmente le carré de la norme (et donc le volume fondamental de $g\mathbf{G}$) d'un facteur $|g|^2$:

$$|\mathbf{G}/g\mathbf{G}| = |g|^2 \quad \forall g \in \mathbf{G}$$

EXEMPLE 2.10
$\phi\mathbf{G}$ est un sous-ensemble de $\mathbf{G}$ et la partition $\mathbf{G}/\phi\mathbf{G}$ est d'ordre $|\phi|^2 = 2$. $\phi\mathbf{G}$ est le réseau complexe isomorphe au réseau réel $R\mathbf{Z}^2$:

$$\phi \times (a+ib) = (1+i) \times (a+ib) = (a-b) + i(a+b)$$

La multiplication par ϕ correspond à une homothétie de $\sqrt{2}$ et une rotation de 45^o. Le réseau $\mathbf{Z}^2$ étant symétrique par rapport à la première bissectrice, l'opérateur R se confond avec la multiplication par ϕ.
$\phi\mathbf{G}$ est formé par les points de $\mathbf{G}$ dont le carré de la norme (module au carré) est pair. De l'autre côté, $\phi\mathbf{G}+1$ est l'ensemble des entiers gaussiens à norme au carré impaire. L'ensemble des représentants des cosets de la partition $\mathbf{G}/\phi\mathbf{G}$ est $[\mathbf{G}/\phi\mathbf{G}] = 0, 1$.
De façon plus générale, $\phi^\mu\mathbf{G}$ est un sous-réseau de $\mathbf{G}$ qui donne naissance à une partition $\mathbf{G}/\phi^\mu\mathbf{G}$ d'ordre $|\phi|^{2\mu}| = 2^\mu$. L'isomorphisme suivant est évident :

$$\phi^\mu\mathbf{G} \approx R^\mu\mathbf{Z}^2 = \begin{cases} 2^{\mu/2}\mathbf{Z}^2 & si\ \mu\ pair \\ 2^{(\mu-1)/2}\mathbf{Z}^2 & si\ \mu\ impair \end{cases}$$

Le réseau $\phi^\mu\mathbf{G}$ (comme $R^\mu\mathbf{Z}^2$) est constitué des éléments de $\mathbf{G}$ dont le carré de la norme est multiplié par 2^μ. Par suite, $d^2_{min}(\phi^\mu\mathbf{G}) = 2^\mu$.

Theorem 8 *(Décompoistion Binaire d'un Gaussien)*
Soit g un entier gaussien. Alors, g s'écrit comme une combinaison linéaire binaire des puissances de $\phi = 1+i$,

$$g = \sum_{j=0}^{\infty} e_j\phi^j, \quad e_j \in \{0,1\}$$

Preuve.Ce théorème est une extension de la Formule 2.10 au cas complexe. Par analogie avec la chaine $\mathbf{Z}/2\mathbf{Z}/4\mathbf{Z}/\ldots$, nous formons la chaine de partitionnement $\mathbf{G}/\phi\mathbf{G}/\phi^2\mathbf{G}/\phi^3\mathbf{G}/\phi^4\mathbf{G}/\ldots$ (celle-ci est isomorphe à $\mathbf{Z}^2/R\mathbf{Z}^2/2\mathbf{Z}^2/2R\mathbf{Z}^2/4\mathbf{Z}^2/\ldots$). Le partitionnement (total et intermédiaire) de cette chaine est binaire. Nous écrivons l'anneau gaussien sous la forme :

$$\mathbf{G} = [\mathbf{G}/\phi\mathbf{G}] + [\phi\mathbf{G}/\phi^2\mathbf{G}] + [\phi^2\mathbf{G}/\phi^3\mathbf{G}] + \ldots$$

D'après l'Exemple 2.10, $[\mathbf{G}/\phi\mathbf{G}] = \{0, 1\}$, ce qui donne la première composante e_0 de g. De façon identique, $e_1\phi$ est un représentant d'un coset de $\phi^2\mathbf{G}$ dans la partition $\phi\mathbf{G}/\phi^2\mathbf{G}/\ldots$. CQFD.

Remarque
Un réseau Λ réel est un $\mathbf{Z}$-module, où $\pm m\mathbf{x} = \pm(\mathbf{x} + \mathbf{x} + \ldots + \mathbf{x})$ pour tout entier m. Par contre, un réseau Λ complexe n'est pas nécessairement un $\mathbf{G}$-module. En fait, si $g = a + ib$ est un entier gaussien, $g\mathbf{x} = (a\mathbf{x}) + i(b\mathbf{x})$. Le point $g\mathbf{x}$ appartient à Λ si et seulement si $i\Lambda \subset \Lambda$. Mais $i^2\Lambda \subset i\Lambda \implies -\Lambda = \Lambda \subset i\Lambda \subset \Lambda$. Ainsi, Λ est un $\mathbf{G}$-module si et seulement si $i\Lambda = \Lambda$. Un tel réseau complexe est appelé $\mathbf{G}$-réseau.

2.3.2 Les réseaux binaires

Les réseaux binaires constituent une extension des codes correcteurs d'erreurs binaires. C'est la classe la plus intéressante des réseaux adaptés aux applications pratiques. Parmi les réseaux binaires, figurent les réseaux les plus denses ($\mathbf{Z}$, D_4, E_8, $\Lambda_1 6$ et Λ_{24}) en dimension 1, 4, 8, 16 et 24.

Definition 18 *(Réseau Binaire Réel)*
Un réseau Λ de dimension N est dit binaire *s'il existe un entier m tel que $2^m\mathbf{Z}^N \subset \Lambda \subset \mathbf{Z}^N$.*

Le plus petit m vérifiant $2^m\mathbf{Z}^N \subset \Lambda$ est appelé *profondeur-2* du réseau. Nous pouvons définir la chaine de partitionnement $\mathbf{Z}^N/\Lambda/2^m\mathbf{Z}^N$. Lorsque la profondeur-2 du réseau binaire est égale à 1 (resp. 2), on dira que Λ est un réseau mod-2 (resp. mod-4).

Definition 19 *(Réseau Binaire Complexe)*
Un réseau complexe Λ de dimension N est dit binaire, s'il existe un entier μ tel que $\phi^\mu\mathbf{G}^N \subset \Lambda \subset \mathbf{G}^N$ et si Λ est un $\mathbf{G}$-réseau ($\mathbf{G}$-module).

Le plus petit μ vérifiant $\phi^\mu\mathbf{G}^N \subset \Lambda$ est appelé profondeur-ϕ du réseau. Nous pouvons définir la chaine de partitionnement $\mathbf{G}^N/\Lambda/\phi^\mu\mathbf{G}^N$.

Le réseau complexe de dimension N associé à un réseau réel binaire de dimension $2N$ est un réseau complexe binaire, et vice versa. En effet, $2^m\mathbf{Z}^{2N} = \phi^{2m}\mathbf{G}^N \subset \phi^{2m-1}\mathbf{G}^N$. On peut ainsi définir la profondeur ϕ d'un réseau réel. Si m est la profondeur-2 d'un réseau réel $2N$-dimensionnel, sa profondeur-ϕ est égale à $2m$ ou $2m-1$. La profondeur-ϕ sera tout simplement appelée *profondeur*, quelle que soit la nature du réseau (réel ou complexe). La profondeur d'un réseau mod-2 prend les deux valeurs 1 ou 2 et celle d'un réseau mod-4 les deux valeurs 3 ou 4.

L'isomorphisme $\mathbf{Z}^4/D_4/R\mathbf{Z}^4 = \mathbf{G}^2/D_4/\phi\mathbf{G}^2$ montre que le réseau D_4 est un réseau binaire mod-2 avec une profondeur $\mu = 1$.
Puisque l'ordre de la partition $\mathbf{Z}^N/2^m\mathbf{Z}^N$ (resp. $\mathbf{G}^N/\phi^\mu\mathbf{G}^N$) est une puissance de 2, les ordres de $\mathbf{Z}^N/\Lambda$ et de $\Lambda/2^m\mathbf{Z}^N$ (resp. $\mathbf{G}^N/\Lambda$ et de $\Lambda/\phi^\mu\mathbf{G}^N$) doivent être des puissances de 2, car leur produit est égal à $|\mathbf{Z}^N/2^m\mathbf{Z}^N|$ (resp. $|\mathbf{G}^N/\phi^\mu\mathbf{G}^N|$).

Definition 20 *(Redondance d'un Réseau Binaire)*
La redondance $r(\Lambda)$ *d'un réseau binaire est définie comme le logarithme à base 2 de $|\mathbf{Z}^N/\Lambda|$,*

$$|\mathbf{Z}^N/\Lambda| = 2^{r(\Lambda)}$$

D'après le théorème 7, $det(\Lambda) = |\mathbf{Z}^N/\Lambda| = 2^{r(\Lambda)}$. On définit parfois la redondance normalisée par symbole (par 2 dimensions), $\rho(\lambda) = 2r(\Lambda)/N$ où N est la dimension du réseau réel.

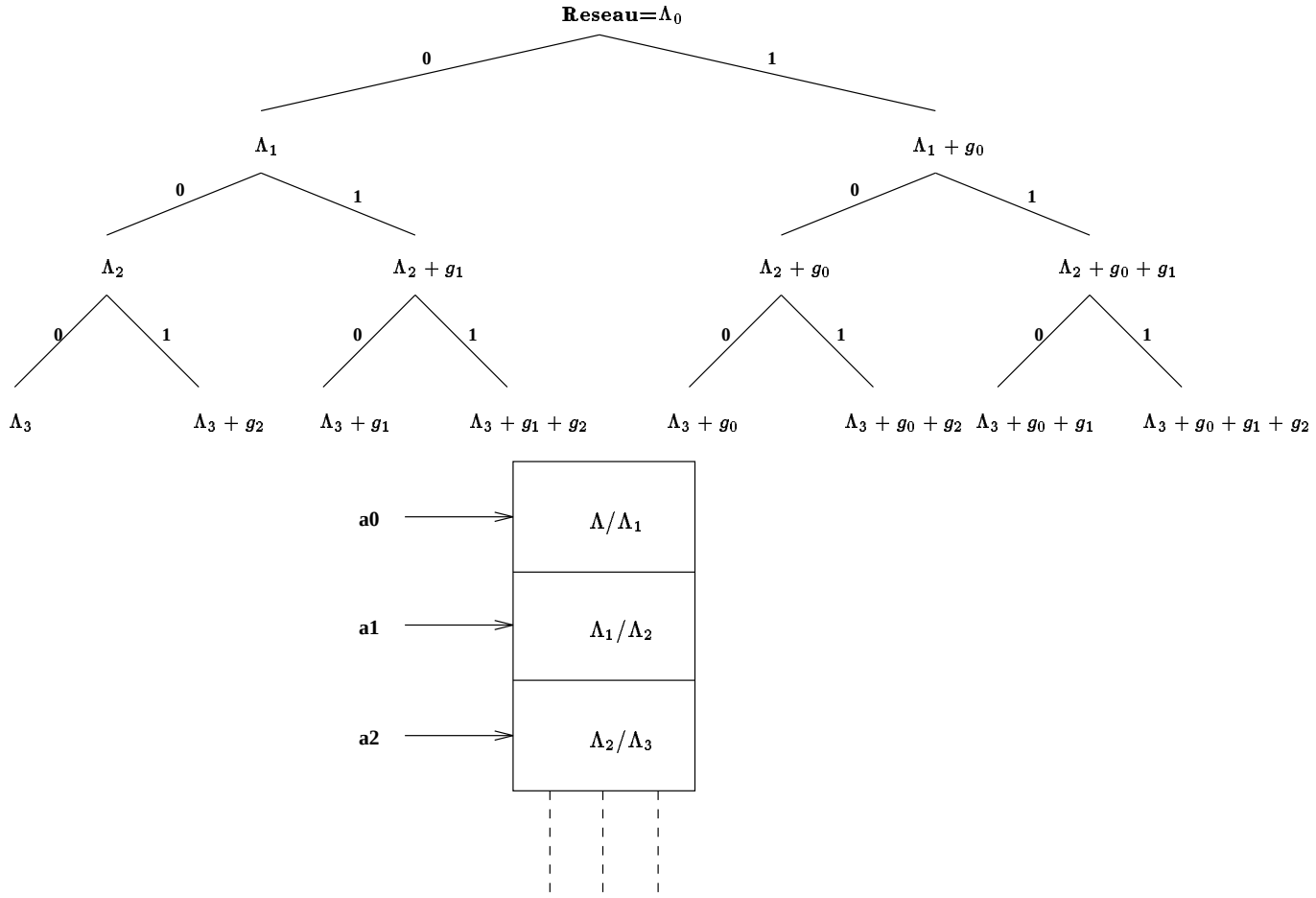


Figure 2.7: Etiquetage d'Ungerboeck.

Soient Λ et Λ' deux réseaux binaires tels que $\Lambda' \subset \Lambda$. Alors, l'ordre de la partition Λ/Λ' est 2^K avec K entier naturel. L'étiquetage des cosets de Λ' se fait par un K-tuple binaire a. Le représentant du coset de Λ' étiqueté par a est noté $c(a)$. Le théorème ci-dessous montre qu'une telle partition se décompose en K partitions d'ordre 2, $\Lambda_k/\Lambda_{k+1},\ 0 \leq k \leq K-1$. De plus, il montre qu'il existe un étiquetage $c(a) = \sum a_k g_k$ où a_k est la kème composante de l'étiquette a, et g_k est un élément de Λ_k n'appartenant pas à Λ_{k+1} tel que les deux vecteurs $\{a_k g_k,\ a_k \in \{0,1\}\}$ forment un système de représentants des cosets de Λ_{k+1} dans la partition binaire Λ_k/Λ_{k+1}. Ainsi, les 2^K combinaisons linéaires $\{\sum a_k g_k\}$ des générateurs g_k forment les représentants $[\Lambda/\Lambda']$ des cosets dans la partition Λ/Λ'.

Theorem 9 *(Etiquetage d'Ungerboeck)*
Soit $\Lambda' \subset \Lambda$ deux réseaux binaires et soit K l'entier défini par $|\Lambda/\Lambda'| = 2^K$. Alors, il existe une suite de réseaux $\Lambda_0 = \Lambda, \Lambda_1, \ldots, \Lambda_K = \Lambda'$ telle que $\Lambda_0/\Lambda_1/\ldots/\Lambda_k$ est une chaine de partitionnement où chaque partition $[\Lambda_k/\Lambda_{k+1}]$ est binaire, $0 \leq k \leq K-1$. Le réseau Λ admet la décomposition

$$\Lambda = \Lambda' + \left\{ \sum_{k=0}^{K-1} a_k g_k \right\}$$

où les $a_k \in \{0,1\}$ et $\{a_k g_k\}$ est l'ensemble des représentants des cosets dans la partition Λ_k/Λ_{k+1}.

Preuve. Le groupe quotient Λ/Λ' est un groupe binaire d'ordre $|\Lambda/\Lambda'| = 2^K$. L'application du théorème 6 suivi de la formule 2.15 donne $\Lambda = \Lambda' + \{\sum a_k g_k\}$ avec K générateurs g_k du groupe quotient. Posons $\Lambda_i = \Lambda' + \left\{\sum_{k=i}^{k=K} a_k g_k\right\}$ pour $i = 1 \ldots K-1$. Le reste de l'énoncé est maintenant trivial. CQFD.

La Figure 2.7 présente l'étiquetage d'Ungerboeck de deux façons différentes : une tour de partitionnement et un arbre binaire. Dans la tour, le premier bit a_0 de l'étiquette a sélectionne un des deux cosets de Λ_1 dans la partition Λ/Λ_1. Le deuxième bit a_1 sélectionne un coset de Λ_2 dans la partition Λ_1/Λ_2, et ainsi de suite. Les deux choix possibles d'un bit a_i se transforment en deux branches issues d'un noeud dans l'arbre binaire. L'étiquetage d'Ungerboeck est imbriqué, c'est-à-dire, les premiers k bits de l'étiquette dans la partition Λ/Λ' forment une étiquette de la partition Λ/Λ_k. Si $\mathbf{x}$ est un point de Λ qui appartient au coset de Λ' étiqueté par a, alors $\mathbf{x}$ est dans le coset de Λ_k étiqueté par les premiers k bits de a.

REMARQUE
Soient $\mathbf{x}$ et $\mathbf{y}$ deux points distincts de Λ situés dans deux cosets de Λ' ayant des étiquettes où les premiers k bits sont identiques. Alors, $d^2(\mathbf{x},\mathbf{y}) = ||\mathbf{x}-\mathbf{y}||^2 \geq d^2_{min}(\Lambda_k)$ car $\mathbf{x}$ et $\mathbf{y}$ appartiennent au même coset de Λ_k.

EXEMPLE 2.11
La Figure 2.8 montre le partitionnement du plan complexe et les étiquettes associées. Le niveau du partitionnement est égal à 4. En notation réelle, la décomposition s'écrit :

$$\mathbf{Z}^2/R\mathbf{Z}^2/2\mathbf{Z}^2/2R\mathbf{Z}^2/4\mathbf{Z}^2$$

$$\mathbf{Z}^2 = 4\mathbf{Z}^2 + [2R\mathbf{Z}^2/4\mathbf{Z}^2] + [2\mathbf{Z}^2/2R\mathbf{Z}^2] + [R\mathbf{Z}^2/2\mathbf{Z}^2] + [\mathbf{Z}^2/R\mathbf{Z}^2]$$

et en notation complexe :

$$\mathbf{G}/\phi\mathbf{G}/\phi^2\mathbf{G}/\phi^3\mathbf{G}/\phi^4\mathbf{G}$$

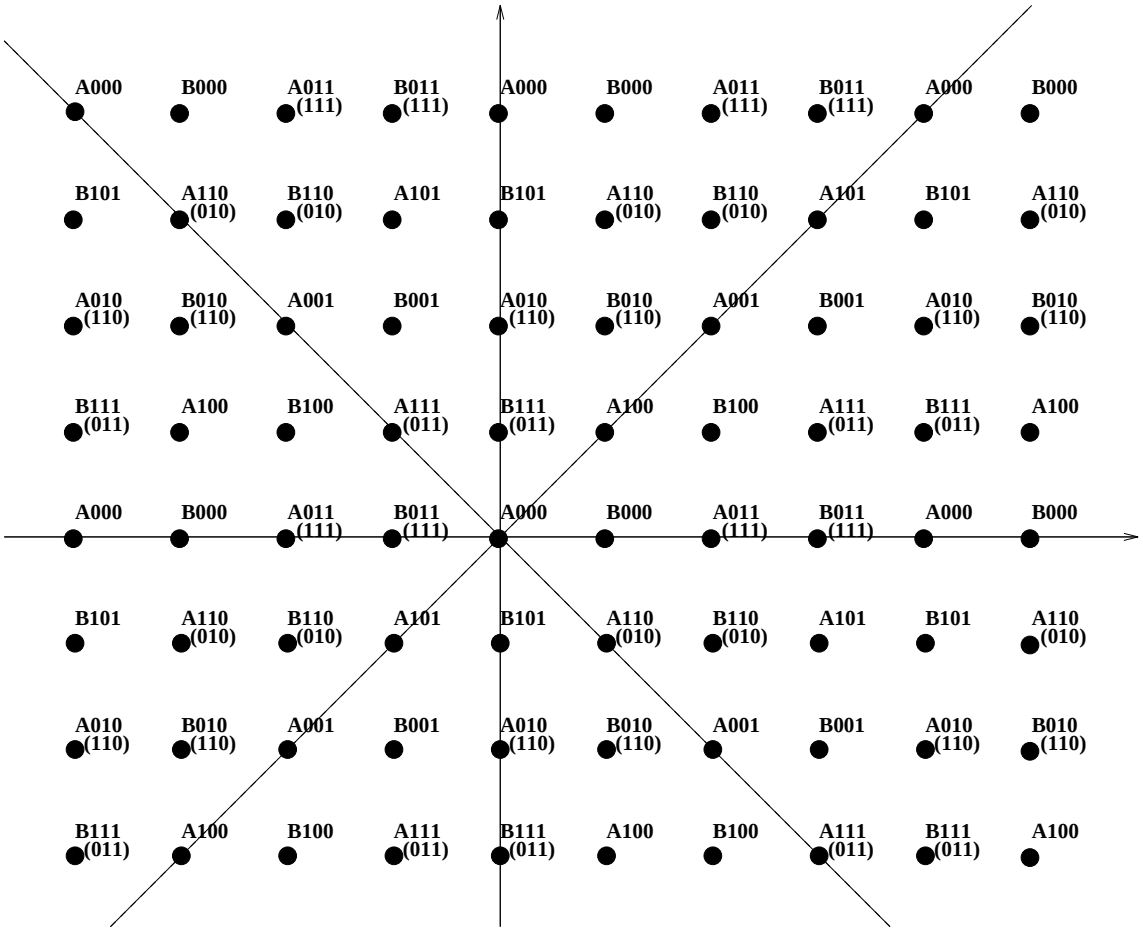


Figure 2.8: Partitionnement de niveau 4 du plan complexe.

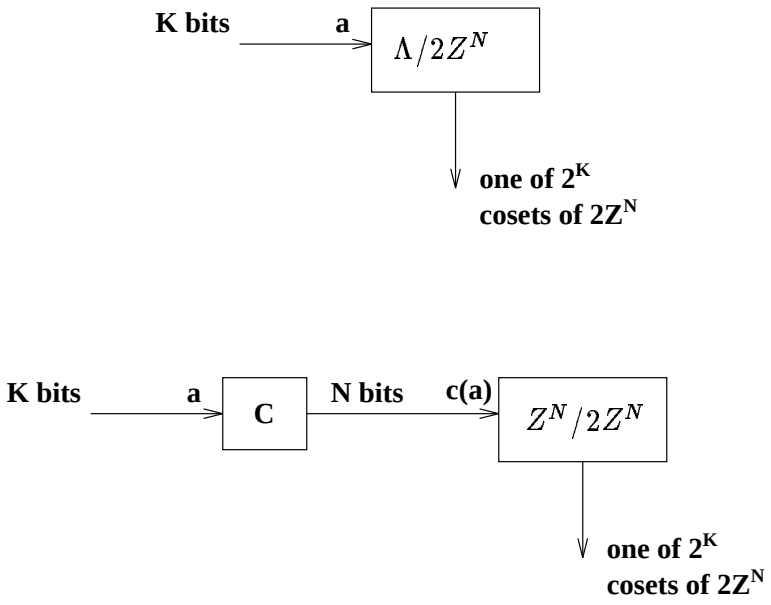


Figure 2.9: Réseau binaire mod-2.

$$\mathbf{G} = \phi^4\mathbf{G} + [\phi^3\mathbf{G}/\phi^4\mathbf{G}] + [\phi^2\mathbf{G}/\phi^3\mathbf{G}] + [\phi\mathbf{G}/\phi^2\mathbf{G}] + [\mathbf{G}/\phi\mathbf{G}]$$

L'étiquetage des cosets de la Figure 2.8 a été fait suivant la méthode d'Ungerboeck. Remarquons qu'un certain nombre de points possède des étiquettes entre parenthèses. Ces étiquettes modifiées remplaceront celle d'Ungerboeck dans la conception des codeurs des réseaux Λ_{16} et Λ_{24}.

Theorem 10 *(Construction A, équivalent au Th. 3)*
Soit Λ un réseau réel entier de dimension N. Λ est un réseau binaire mod-2 si et seulement si les points de Λ sont congrus modulo 2 à un mot d'un code linéaire binaire (N, K, d). La redondance du réseau est $r(\Lambda) = N - K$, et sa distance minimale $d^2_{min} = min(4, d)$.

Preuve. Si Λ est un réseau binaire mod-2, $\mathbf{Z}^N/\Lambda/2\mathbf{Z}^N$ est une chaine de partition. Posons $2^K = |\Lambda/2\mathbf{Z}^N|$, où K est un entier. L'ordre de $\mathbf{Z}^N/\Lambda$ est $|\mathbf{Z}^N/\Lambda| = 2^{N-k}$. Par suite, la redondance de Λ est $r(\Lambda) = N - K$. Λ est l'union de 2^K cosets de $2\mathbf{Z}^N$ dans la partition $\mathbf{Z}^N/2\mathbf{Z}^N$. Les représentants de ces cosets sont des N-uples de 0 et 1. En appliquant le théorème 9, on obtient $\Lambda = 2\mathbf{Z}^N + \{\sum a_k g_k\}$ où les g_k sont des N-uples binaires, $0 \leq k \leq K-1$, et l'addition se fera modulo 2 (à cause du terme $2\mathbf{Z}^N$).

L'ensemble des 2^K représentants $c(a)$ des cosets, $C = \{c(a) = \sum a_k g_k\}$ est un code linéaire (N, K, d). Inversement, si $\Lambda = 2\mathbf{Z}^N + C$, on voit tout de suite que $2\mathbf{Z}^N$ est un sous-réseau de Λ.
Le carré de la distance minimale est égal à 4 dans $2\mathbf{Z}^N$ et à d dans le code C. Par conséquent, le carré de la distance minimale du réseau est le minimum de 4 et d. CQFD.

La Figure 2.9 illustre l'opération de construction d'un réseau Λ mod-2, $\Lambda = 2\mathbf{Z}^N + C$. Nous pouvons sélectionner les cosets de $2\mathbf{Z}^N$ directement dans la partition $\Lambda/2\mathbf{Z}^N$, ou bien dans la partition $\mathbf{Z}^N/2\mathbf{Z}^N$ après l'application du code C sur les K bits d'information. Bien sûr, c'est la deuxième configuration qui sera retenue dans les applications pratiques.

Le code C' associé à un sous-réseau mod-2 Λ' d'un réseau mod-2 Λ est un sous-code du code C associé à Λ.

Les réseaux $\mathbf{Z}^2$, $R\mathbf{Z}^2$ et $2\mathbf{Z}^2$ sont des réseaux mod-2. Ils sont associés respectivement aux codes (2,2,1), (2,1,2) et (2,0,∞). Leurs distances minimales au carré valent 1, 2 et 4. Les réseaux mod-2 $\mathbf{Z}^4$, D_4, $R\mathbf{Z}^4$, RD_4 et $2\mathbf{Z}^4$ correspondent aux codes linéaires binaires (4,4,1), (4,3,2), (4,2,2), (4,1,4) et (4,0,∞) et ont une distance minimale au carré égale à 1, 2, 2, 4 et 4 respectivement.

Les réseaux mod-2 sont limités en distance minimale à $d^2_{min} = 4$ (valeur maximale atteinte lorsque $d = 4$). Par suite, les codes de distance de Hamming minimale 4 ont un intérêt spécial. Parmi ces codes, le code de Reed-Muller (8,4,4) qui s'associe au réseau mod-2 E_8, le réseau de Gosset. $d^2_{min}(E_8) = 4$, $r(E_8) = 4$ et $\gamma(E_8) = 2$ $(3.01dB)$.

Soit Λ un réseau mod-4. Sachant que $4\mathbf{Z}^N$ est un sous-réseau de Λ, le théorème 9 permet d'écrire :

$$\Lambda = 4\mathbf{Z}^N + \left\{\sum a_k g_k\right\} \tag{2.18}$$

Chaque vecteur g_k, $0 \leq k \leq K-1$, est un représentant d'un coset de $4\mathbf{Z}^N$. Le vecteur g_k est un N-uple d'entiers modulo 4, mais l'étiquette $\mathbf{a} = (a_0, a_1, \ldots, a_{K-1})$ est toujours un K-uple formé de 0 et 1. L'addition dans 2.18 se fait modulo 4. Ainsi, Λ est l'union de 2^K cosets de $4\mathbf{Z}^N$. Les représentants des cosets sont $c(a) = \sum a_k g_k \pmod 4$.

Theorem 11 *(Construction d'un Réseau mod-4)*
Soit Λ un réseau binaire mod-4. Alors, Λ se décompose en cosets sous la forme :

$$\Lambda = 4\mathbf{Z}^N + 2C + \left\{\sum a_k g_k\right\}$$

où C est un code binaire linéaire (N, K', d'), et les générateurs g_k, $K' \leq k \leq K-1$, sont des N-uples d'entiers modulo 4. Les composantes d'un générateur g_k ne sont pas toutes paires.

Preuve. Soit Λ_p l'ensemble des points de Λ ayant toutes les composantes paires. Λ_p est un sous-réseau de Λ et admet $4\mathbf{Z}^N$ comme sous-réseau. Ainsi, $\Lambda/\Lambda_p/4\mathbf{Z}^N$ est une chaine de partitionnement. La décomposition en cosets de Λ dans cette partition s'écrit

$$\Lambda = 4\mathbf{Z}^N + [\Lambda_p/4\mathbf{Z}^N] + [\Lambda/\Lambda_p] \tag{2.19}$$

Il est évident que Λ_p est l'homothétie par 2 d'un réseau mod-2 (diviser $\Lambda_p/4\mathbf{Z}^N$ par 2). Donc, il existe un code linéaire (N, K', d') tel que

$$\Lambda_p = 4\mathbf{Z}^N + 2C \tag{2.20}$$

Mais Λ_p décompose Λ par

$$\Lambda = \Lambda_p + [\Lambda/\Lambda_p] = 4\mathbf{Z}^N + 2C + [\Lambda/\Lambda_p] \tag{2.21}$$

En comparant les expressions 2.20 et 2.21, on trouve que $[\Lambda_p/4\mathbf{Z}^N] = 2C = \{2\sum a_k g_k\}$, où les g_k, $0 \leq k \leq K'-1$, sont K' générateurs du code C. $|\Lambda/4\mathbf{Z}^N| = 2^K \implies |\Lambda/\Lambda_p| = 2^{K-K'}$. Posons ainsi $[\Lambda/\Lambda_p] = \{\sum a_k g_k\}$, $K' \leq k \leq K-1$, avec les g_k formant $K-K'$ générateurs du groupe quotient $[\Lambda/\Lambda_p]$. CQFD.

L'ensemble $\{2\sum a_k g_k \ / \ K' \leq k \leq K-1\}$ génère un sous-réseau Λ' de Λ_p. Les points de Λ' sont congrus modulo 4 à un mot $2c'$ d'un code linéaire C' $(N, K-K')$. $C' \subset C$ car $\Lambda' \subset \Lambda_p$. Nous pouvons donc affirmer que $K-K' \leq K'$.

Definition 21 *(Réseau Décomposable)*
Soit Λ un réseau binaire mod-4. Λ *est* décomposable *s'il vérifie*

$$\Lambda = 4\mathbf{Z}^N + 2C_1 + C_0$$

où $C_0 \subset C_1$ sont deux codes linéaires binaires.

Cette définition est une généralisation de la construction B du paragraphe précédent. Elle constitue un cas particulier du théorème 11. En effet, le réseau mod-4 Λ est décomposable si nous arrivons à trouver un ensemble de générateurs $\{g_k \ / \ K' \leq k \leq K-1\}$ de $[\Lambda/\Lambda_p]$ vérifiant : g_k est un N-uple de 0 et de 1, la ligne mod-4 de $g_k + g_{k'}$ est un mot du code C_1. Le code C_0 n'est autre que $[\Lambda/\Lambda_p]$.
La définition 21 traduit l'application d'un code C_0 sur la ligne mod-2 de la matrice des coordonnées et l'application du code C_1 sur la ligne mod-4.

Theorem 12 *(Généralisation du Th. 4)*
Soit Λ un réseau mod-4 décomposable, $\Lambda = 4\mathbf{Z}^N + 2C_1 + C_0$. Alors, la distance minimale de Λ est donnée par :

$$d^2_{min}(\Lambda) = min[16, 4d(C_1), d(C_0)]$$

Preuve. Le carré de la distance minimale dans $4\mathbf{Z}^N$, $2C_1$ et C_0 est égal à 16, $4d(C_1)$ et $d(C_0)$ respectivement. Soit $\mathbf{x}$ un point de Λ congru à $2c_1 + c_0$ modulo 4. Lorsque $c_0 \neq 0$, on a $||\mathbf{x}||^2 \geq d(C_0)$. Si $c_0 = 0$ mais $c_1 \neq 0$, alors $||\mathbf{x}||^2 \geq d(C_1)$. Finalement, si $c_0 = c_1 = 0$ on a $||\mathbf{x}||^2 \geq 16$. CQFD.

Le théorème 12 indique que le rapport $4d(C_1) = d(C_0)$ permet de maximiser la distance minimale d'un réseau mod-4 décomposable. Par exemple, le réseau RE_8 est une version du réseau $E8$. RE_8 est un réseau mod-4 décomposable. Il s'écrit

$$RE_8 = 4\mathbf{Z}^8 + 2(8,7,2) + (8,1,8)$$

Le réseau Leech Λ_{24} est un réseau mod-4 non décomposable. Mais, il peut être considéré comme l'union de deux cosets du réseaux H_{24}. Ce dernier est un réseau mod-4 réel décomposable.

La Figure 2.10.a illustre la décomposition $\Lambda/\Lambda_p/4\mathbf{Z}^N$ d'un réseau mod-4 quelconque. Les K' bits de l'étiquette a_1 sélectionnent un coset de $4\mathbf{Z}^N$ dans la partition $\Lambda_p/4\mathbf{Z}^N$ et les $K - K'$ bits de l'étiquette a_0 sélectionnent un coset de Λ_p dans la partition Λ/Λ_p. Les

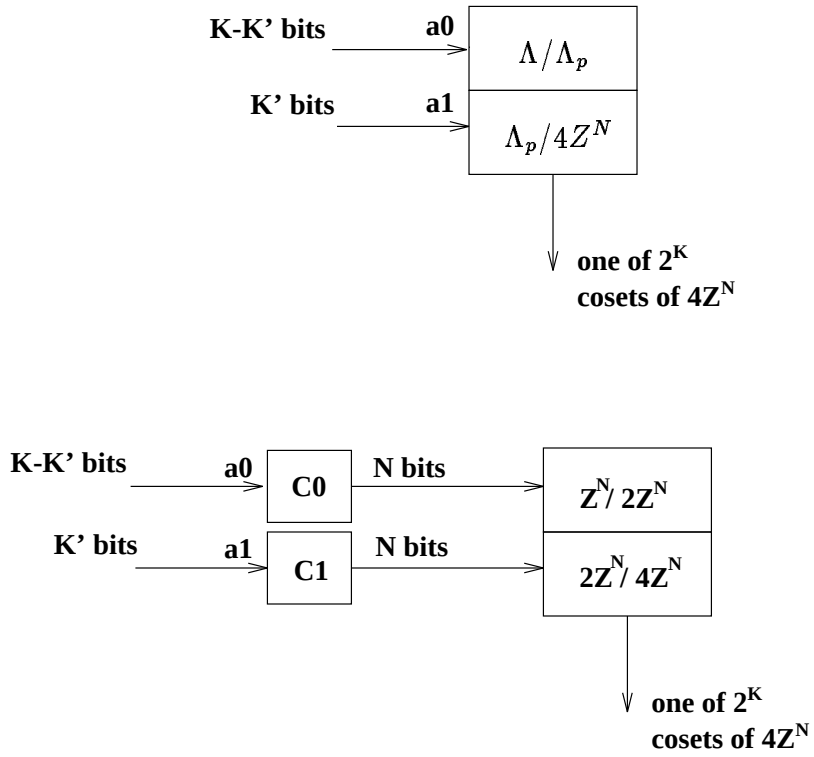


Figure 2.10: Réseau binaire mod-4. a) Quelconque. b) Décomposable.

deux étiquettes groupées désignent un coset de $4\mathbf{Z}^N$ dans la partition $\Lambda/4\mathbf{Z}^N$. La Figure 2.10.b montre la décomposition d'un réseau mod-4 décomposable qui s'écrit par la formule $\Lambda = 4\mathbf{Z}^N + 2C_1 + C_0$. Remarquons que le réseau mod-4 se réduit à un réseau mod-2 si C_1 est le code $(N, N, 1)$. La structure de la Figure 2.10 permet d'étendre la décomposition à un réseau réel binaire de profondeur-2 quelconque en utilisant la chaine de partitionnement $\Lambda/\Lambda_p/\ldots/2^m\mathbf{Z}^N$ formée des sous-réseaux de Λ ayant les composantes dans $2\mathbf{Z}^n$, $4\mathbf{Z}^N$, et ainsi de suite.

La décomposition des réseaux complexes binaires est similaire à celle des réseaux réels. Les réseaux mod-2 complexes sont toujours décomposables et possèdent la formule

$$\Lambda = \phi^2\mathbf{G}^N + \phi C_1 + C_0$$

établie dans le théorème ci-dessous. Les réseaux complexes de profondeur 3 ou plus ne sont pas nécessairement décomposables.

Theorem 13 *(Construction A Complexe)*
Soit Λ un **G***-réseau complexe de dimension N. Alors, Λ est un réseau mod-2 si et seulement si, Λ est l'ensemble des N-uples d'entiers gaussiens congrus modulo ϕ^2 aux N-uples de la forme $\phi c_1 + c_0$, où c_1 est un mot d'un code linéaire binaire $C_1(N,K)$ et c_0 appartient à un sous-code $C_0(N, J-K)$ de C_1.*
La redondance de Λ est donnée par $r(\Lambda) = 2N - J$ et sa distance minimale est

$$d^2_{min}(\Lambda) = min[4, 2d(C_1), d(C_0)]$$

Preuve. Si Λ est un réseau mod-2, $\mathbf{G}^N/\Lambda/2\mathbf{G}^N = \phi^2\mathbf{G}^N$ est une chaine de partitionnement et l'ordre de la partition $\Lambda/2\mathbf{G}^N$ est 2^J, J entier. Sachant que $|\mathbf{G}^N/2\mathbf{G}^N| = 2^{2N}$, on obtient $|\mathbf{G}^N/\Lambda| = 2^{2N-J}$. D'où l'on tire la redondance $r(\Lambda) = 2N - J$. Λ est l'union de 2^J cosets de $2\mathbf{G}^N = \phi^2\mathbf{G}^N$. Nous pouvons ainsi choisir des représentants des cosets sous la forme $\phi c_1 + c_0$ où c_1 et c_0 sont des N-uples binaires. La somme des représentants des cosets est faite modulo $2\mathbf{G}^N$ (ou bien mod 2).
Par analogie avec la démonstration du théorème 11, considérons l'ensemble Λ_ϕ formé des points de Λ dont toutes les composantes sont multiples de ϕ. $\Lambda/\Lambda_\phi/\phi^2\mathbf{G}^N$ est une chaine de partitionnement et la décomposition s'écrit :

$$\Lambda = \phi^2\mathbf{G}^N + [\Lambda_\phi/\phi^2\mathbf{G}^N] + [\Lambda/\Lambda_\phi]$$

Les générateurs de $[\Lambda_\phi/\phi^2\mathbf{G}^N]$ sont notés ϕg_k, $0 \leq k \leq K-1$, g_k est un N-uple binaire et K est un entier. Par conséquent,

$$\Lambda_\phi = \phi^2\mathbf{G}^N + \phi C_1$$

C_1 est un code binaire (N,K) généré par les g_k. De la même façon, les générateurs de $[\Lambda/\Lambda_\phi]$ sont notés g_k, $K \leq k \leq J-1$. La formule de Λ devient

$$\Lambda = \Lambda_\phi + C_0$$

C_0 est un code linéaire binaire $(N, J-K)$. Puisque Λ est un **G**-réseau, $\mathbf{x} \in \Lambda \implies \phi x \in \Lambda$, ce qui montre que C_0 est un sous-code de C_1.
La distance au carré est égale à 4, $2d(C_1)$ et $d(C_0)$ dans $\phi^2\mathbf{G}^N$, ϕC_1 et C_0 respectivement. Ensuite, on répète le même raisonnement que celui du théorème 12 avec un point $\mathbf{x} = \phi c_1 + c_0$. La réciproque ($\Lambda$ est un **G**-réseau contenant $2\mathbf{G}^N$) du théorème est très facile à démontrer. CQFD.

Un réseau mod-2 complexe Λ possède une profondeur de 1 si et seulement si le code C_1 du théorème précédent est le code $(N,N,1)$. La formule de Λ devient $\Lambda = \phi\mathbf{G}^N + C_0$, la profondeur est 2 si C_1 n'est pas le code $(N,N,1)$.

Le réseau de Schlafli D_4 est un réseau complexe mod-2 de profondeur 1, décomposable par la formule $D_4 = \phi\mathbf{G}^2 + (2,1,2)$. De la même façon, le réseau de Gosset est un réseau

complexe mod-2 de profondeur 2 qui se décompose $E_8 = \phi^2\mathbf{G}^4 + \phi(4,3,2) + (4,1,4)$.

Les réseaux complexes non mod-2 ne sont pas nécessairement décomposables, c'est-à-dire exprimables en fonction des codes binaires seulement. Malgré tout, un grand nombre de réseaux non mod-2 utiles sont décomposables.
Considérons la chaine de partitionnement $C_{\mu-1}/C_{\mu-2}/\ldots/C_0$ de μ codes binaires (N, K_j), $0 \leq j \leq \mu - 1$. C_j est un sous-code de C_{j+1}. Soit Λ le réseau complexe binaire dont les éléments sont des N-uples d'entiers gaussiens $\mathbf{x}$ congrus à $\phi^{\mu-1}c_{\mu-1}+\ldots+\phi c_1+c_0$ modulo ϕ^μ, où c_j est un mot du code C_j (les coefficients de ϕ^j dans la représentation binaire complexe de $\mathbf{x}$ forment un mot de C_j) :

Definition 22 *(Réseau Complexe Décomposable)*
Le réseau construit ci-dessus est un réseau complexe décomposable de profondeur μ. Sa formule s'écrit :

$$\Lambda = \phi^\mu\mathbf{G}^N + \phi^{\mu-1}C_{\mu-1} + \ldots + \phi C_1 + C_0$$

Les propriétés d'un réseau complexe décomposable s'énoncent comme ceci :
a) Λ est un $\mathbf{G}$-réseau.
b) La profondeur de Λ est égale à μ $(K_{\mu-1} < N)$.
c) L'ordre de la partition $\Lambda/\phi^\mu\mathbf{G}^N$ est le produit des 2_j^K. La redondance $r(\Lambda) = N\mu - \sum K_j = \sum(N - K_j)$.
d) La distance minimale se calcule par $d^2_{min}(\Lambda) = min[2^\mu, 2^{\mu-1}d(C_{\mu-1}), \ldots, d(C_0)]$.

EXEMPLE 2.12
Notons par $RM(r,m)$ le code de Reed-Muller d'ordre r et de longueur $N = 2^m$. On construit le réseau complexe binaire décomposable $\Lambda(r,m)$ par la formule :

$$\Lambda(r,m) = \phi^{m-r}\mathbf{G}^N + \phi^{m-r-1}RM(m-1,m) + \ldots + RM(r,m)$$

$0 \leq m$ et $0 \leq r \leq m$. Lorsque $r = 0$, $\Lambda(0,m)$ est le réseau de Barnes-Wall de dimension $N = 2^m$ et de profondeur m.

La Table 2.5 fournit les formules réelles et complexes des plus importants réseaux connus en pratique. La Table contient les réseaux $\Lambda(r,m)$, mais aussi le réseau Leech et ses principaux sous-réseaux (des versions) H_{24}, X_{24}, D_{24} et Z^{24}. Λ_{24} et H_{24} sont des réseaux complexes binaires non décomposables, de profondeur 4 et 3 respectivement. Une notation comme $(24,6,16)'$ 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 coset est égale à 16.

(r,m)	Λ	$2N$	μ	Formule Réelle	Formule Complexe
(0,0)	$\mathbf{Z}^2$	2	0	$\mathbf{Z}^2$	$\mathbf{G}$
(1,1)	$\mathbf{Z}^4$	4	0	$\mathbf{Z}^4$	$\mathbf{G}^2$
(0,1)	D_4	4	1	$2\mathbf{Z}^4 + (4,3,2)$	$\phi\mathbf{G}^2 + (2,1,2)$
(2,2)	$\mathbf{Z}^8$	8	0	$\mathbf{Z}^8$	$\mathbf{G}^4$
(1,2)	D_8	8	1	$2\mathbf{Z}^8 + (8,7,2)$	$\phi\mathbf{G}^4 + (4,3,2)$
(0,2)	E_8	8	2	$2\mathbf{Z}^8 + (8,4,4)$	$\phi^2\mathbf{G}^4 + \phi(4,3,2) + (4,1,4)$
(3,3)	$\mathbf{Z}^{16}$	16	0	$\mathbf{Z}^{16}$	$\mathbf{G}^8$
(2,3)	D_{16}	16	1	$2\mathbf{Z}^{16} + (16,15,2)$	$\phi\mathbf{G}^8 + (8,7,2)$
(1,3)	H_{16}	16	2	$2\mathbf{Z}^{16} + (16,11,4)$	$\phi^2\mathbf{G}^8 + \phi(8,7,2) + (8,4,4)$
(0,3)	Λ_{16}	16	3	$4\mathbf{Z}16 + 2(16,15,2) + (16,5,8)$	$\phi^3\mathbf{G}^8 + \phi^2(8,7,2) +$ $\phi(8,4,4) + (8,1,8)$
(4,4)	$\mathbf{Z}^{32}$	32	0	$\mathbf{Z}^{32}$	$\mathbf{G}^{16}$
(3,4)	D_{32}	32	1	$2\mathbf{Z}^{32} + (32,31,2)$	$\phi\mathbf{G}^{16} + (16,15,2)$
(2,4)	X_{32}	32	2	$2\mathbf{Z}^{32} + (32,26,4)$	$\phi^2\mathbf{G}^{16} + \phi(16,15,2) + (16,11,4)$
(1,4)	H_{32}	32	3	$4\mathbf{Z}^{32} + 2(32,31,2) + (32,16,8)$	$\phi^3\mathbf{G}^{16} + \phi^2(16,15,2) +$ $\phi(16,11,4) + (16,5,8)$
(0,4)	Λ_{32}	32	4	$4\mathbf{Z}^{32} + 2(32,26,4) + (32,6,16)$	$\phi^4\mathbf{G}^{16} + \phi^3(16,15,2) + \phi^2(16,11,4) +$ $\phi(16,5,8) + (16,1,16)$
—	$\mathbf{Z}^{24}$	24	0	$\mathbf{Z}^{24}$	$\mathbf{G}^{12}$
—	D_{24}	24	1	$2\mathbf{Z}^{24} + (24,23,2)$	$\phi\mathbf{G}^{12} + (12,11,2)$
—	X_{24}	24	2	$2\mathbf{Z}^{24} + (24,18,4)$	$\phi^2\mathbf{G}^{12} + \phi(12,11,2) + (12,7,4)$
—	H_{24}	24	3	$4\mathbf{Z}^{24} + 2(24,23,2) + (24,12,8)$	$\phi^3\mathbf{G}^{12} + \phi^2(12,11,2) +$ $\phi(12,7,4) + (12,5,8)'$
—	Λ_{24}	24	4	$4\mathbf{Z}^{24} + 2(24,18,4) + (24,6,16)'$	$\phi^4\mathbf{G}^{12} + \phi^3(12,11,2) + \phi^2(12,7,4) +$ $\phi(12,5,8)' + (12,1,16)'$

Table 2.5: Réseaux Binaires et leurs Formules.

2.4 Les modulations codées en blocs

La plupart des modulations d'amplitude utilisées en pratique, sauf les modulations de phase PSK, sont des constellations issues du réseau $\mathbf{Z}^N$ (QAM au sens strict). Dans le langage des communications numériques, un point de $\mathbf{Z}^2$ est appelé un *symbole*. Ainsi, une séquence de $N/2$ symboles forme un point de $\mathbf{Z}^N$. Nous pouvons restreindre ce point à un sous-réseau de $\mathbf{Z}^N$ (réseau entier, mais de densité supérieure) en introduisant une certaine indépendance entre les $N/2$ symboles. Nous réalisons ainsi un gain de codage théorique fourni par le gain fondamental $\gamma(\Lambda) = \frac{d^2_{Emin}(\Lambda)}{\sqrt[N/2]{vol(\Lambda)}}$ défini au paragraphe 2.1.3. Le gain provient surtout du terme en d^2_{Emin}, puisque la corrélation introduite entre les symboles fait augmenter cette distance minimale. Le volume fondamental $vol(\Lambda)$ au dénominateur reflète l'expansion de la constellation issue de Λ par rapport à celle extraite de $\mathbf{Z}^N$.

En se basant sur les résultats de partionnement des réseaux énoncés au paragraphe 2.3.2, et en effectuant une traduction directe de la formule complexes d'un réseau de points, nous allons construire à partir d'une modulation QAM codée en blocs les codeurs de 4 réseaux de points : D_4, E_8, Λ_{16} et Λ_{24}. Toutes les constellations obtenues sont de forme cubique et proviennent de la QAM-64.

D'après le paragraphe précédant le réseau de Schlafli D_4 possède la formule complexe $D_4 = \phi\mathbf{G}^2 + (2,1,2)$. Nous partitionnons donc une QAM-64 en deux sous-ensembles notés A et B. Le partitionnement de niveau 1 est présenté Figure 2.11, alors que le partitionnement jusqu'au niveau 4 est montré sous la forme d'un arbre Figure 2.12 où le symbole X représente A ou B. Les deux sous-ensembles A et B sont deux constellations issues des cosets de $\phi\mathbf{G}$ dans $\mathbf{G}$. Un code à répétition (2,1,2) sélectionne le coset et les bits non codés sélectionnent deux symboles dans le coset.

Le codeur cubique de D_4 est montré Figure 2.16. Les 2 bits provenant du code (2,1,2) choisissent deux symboles de la forme (XX) où $X = A$ si le bit est 0 et $X = B$ si le bit est 1. Sachant que le code à répétition utilise un bit parmi les 6 bits de la QAM-64, le nombre de bits non codés est $2 \times 5 = 10$. Le nombre total de bits d'information est égal à 11 (pour un point de D_4, c'est-à-dire 2 symboles) d'où une efficacité spectrale de 5.5 bits/symbole. Le gain fondamental 1.5dB de D_4 peut être retrouvé en faisant le raisonnement suivant : la nouvelle distance euclidienne minimale au carré est $2d_0^2$, où d_0 est la distance minimale de la QAM-64. Ceci fournit un gain asymptotique de 3dB. Mais la perte de 0.5 bits/symbole en efficacité spectrale coûte 1.5dB environ. Le gain asymptotique total est ainsi égal à 3-1.5=1.5dB.

Le codeur cubique de E_8 est obtenu d'une façon semblable à celui de D_4. Il est montré

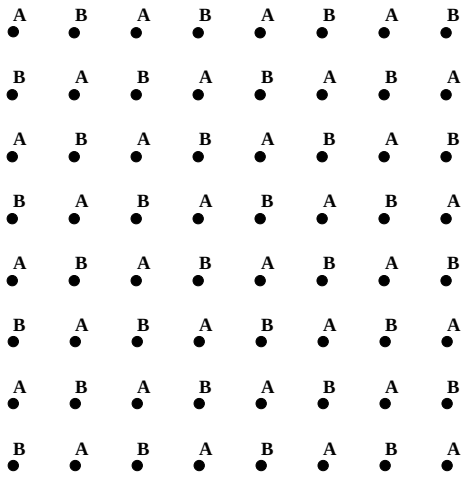


Figure 2.11: Partitionnement de profondeur 1 de la QAM-64.

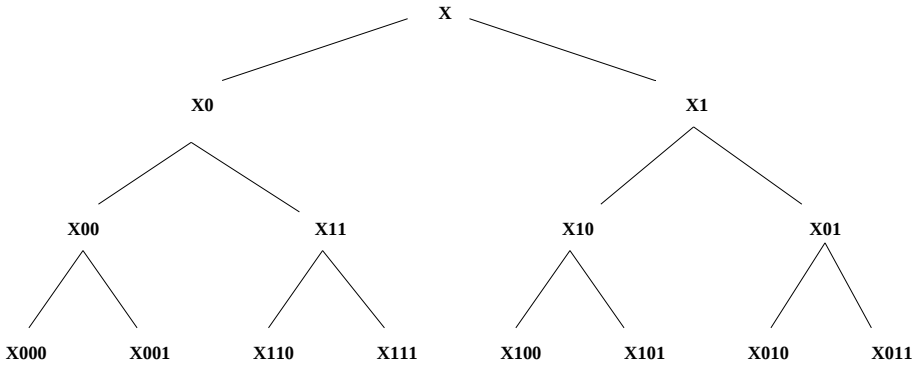


Figure 2.12: Partitionnement jusqu'au niveau 4.

Figure 2.17. La formule complexe de E_8 est $E_8 = \phi^2\mathbf{G}^4 + \phi(4,3,2) + (4,1,4)$. On utilise donc une QAM-64 avec un partitionnement de profondeur 2 (voir Figure 2.13). Les symboles sont notés X_i, où $X = A$ si le bit est 0 et $X = B$ si le bit est 1. Les 4 bits i des 4 symboles sont donnés par le code à parité (4,3,2). Il reste 4 bits non utilisés par symbole de la QAM-64, le nombre de bits non codés est donc $4 \times 4 = 20$ bits. L'efficacité spectrale est de 5 bits/symbole (nombre total de bits d'information divisé par $4 = 20/4$=5). Le gain fondamental de 3dB de E_8 se retrouve ainsi : la nouvelle distance euclidienne minimale est $4d_0^2$. La perte en efficacité spectrale est de 1 bit. Le gain asymptotique final est 6dB-3dB=3dB environ.

Le codeur d'une constellation cubique du réseau Λ_{16} est montré Figure 2.18. La profondeur du partitionnement est égale à 3 (voir Figure 2.14). Les symboles de la QAM-64 sont notés X_{ij}. Les 8 couples d'indices (i,j) sont fournis par le code de Reed-Muller (16,11,4). L'efficacité spectrale est de 4.5 bits/symbole et le gain asymptotique est de 4.5dB (la dis-

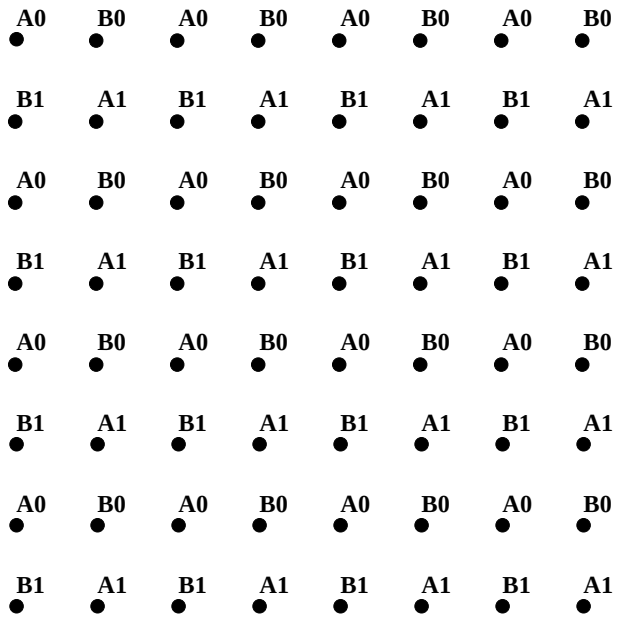


Figure 2.13: Partitionnement de profondeur 2 de la QAM-64.

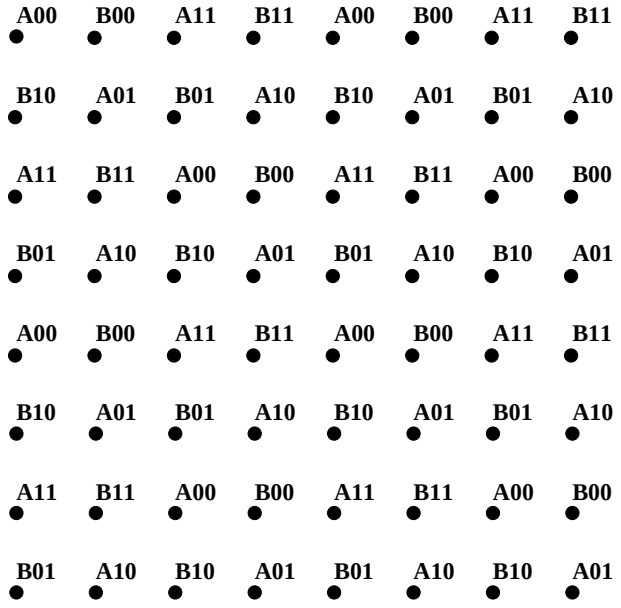


Figure 2.14: Partitionnement de profondeur 3 de la QAM-64.

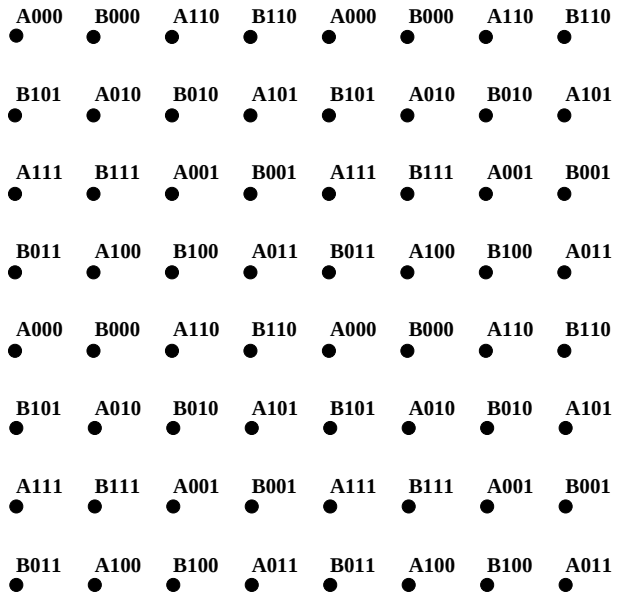


Figure 2.15: Partitionnement de profondeur 4 de la QAM-64.

tance euclidienne minimale est $8d_0^2$).

Le codeur d'une constellation cubique du réseau Leech Λ_{24} est montré Figure 2.18. La profondeur du partitionnement cette fois-ci est égale à 4 (voir Figure 2.15). Les symboles de la QAM-64 sont notés X_{ijk}. Les 12 couples d'indices (i, j) sont fournis par le code de Golay (24,12,8). Les 12 bits k sont fournis par le code de parité (12,11,2). La parité est paire si $X = A$ et impaire si $X = B$. L'efficacité spectrale est de 4 bits/symbole et le gain asymptotique est de 6dB (la distance euclidienne minimale est $16d_0^2$).

Notons enfin que les codeurs de Λ_{16} et Λ_{24} ne constituent pas vraiment une traduction directe des formules complexes des deux réseaux. Ces deux réseaux sont en fait construits en superposant deux copies de leurs demi-réseaux. Le réseau de Barnes-Wall $\Lambda_{16} = H_{16} \bigcup (H_{16} + a)$ est constitué de deux cosets de $H_16 = 2\mathbf{Z}^{16} + (16, 11, 4)$. Les deux cosets sont représentés par les symboles A et les symboles B de la QAM-64. De la même manière, le réseau Leech est l'union de deux cosets d'une version du demi-Leech H_{24}, $\Lambda_{24} = H_{24} \bigcup (H_{24} + b)$.

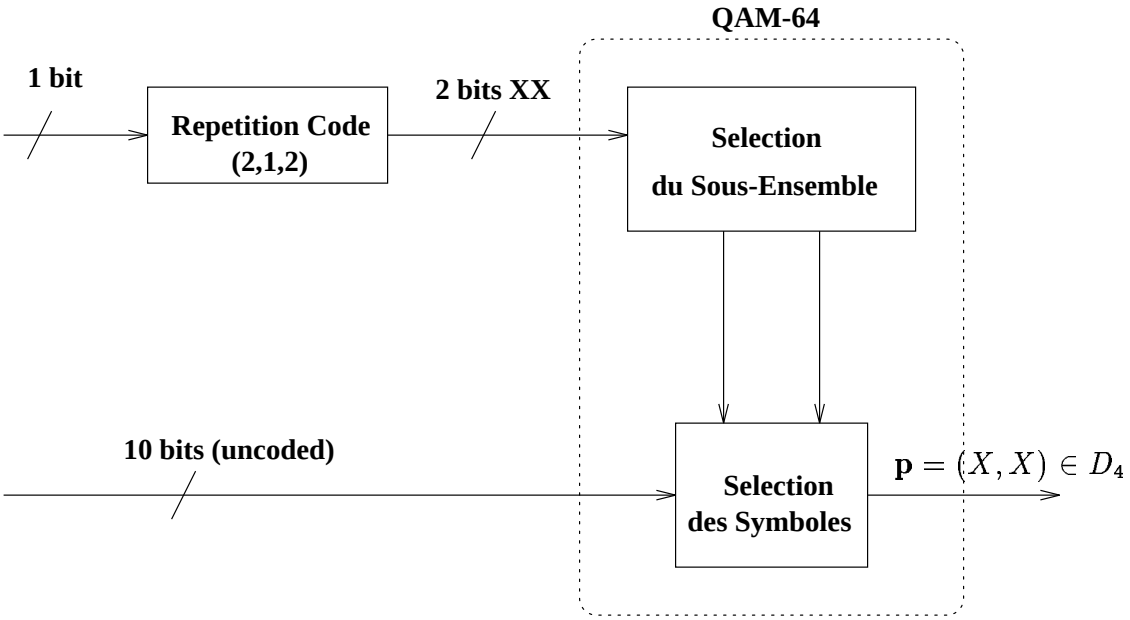


Figure 2.16: Codeur cubique D_4 à 5.5 bits/symbole.

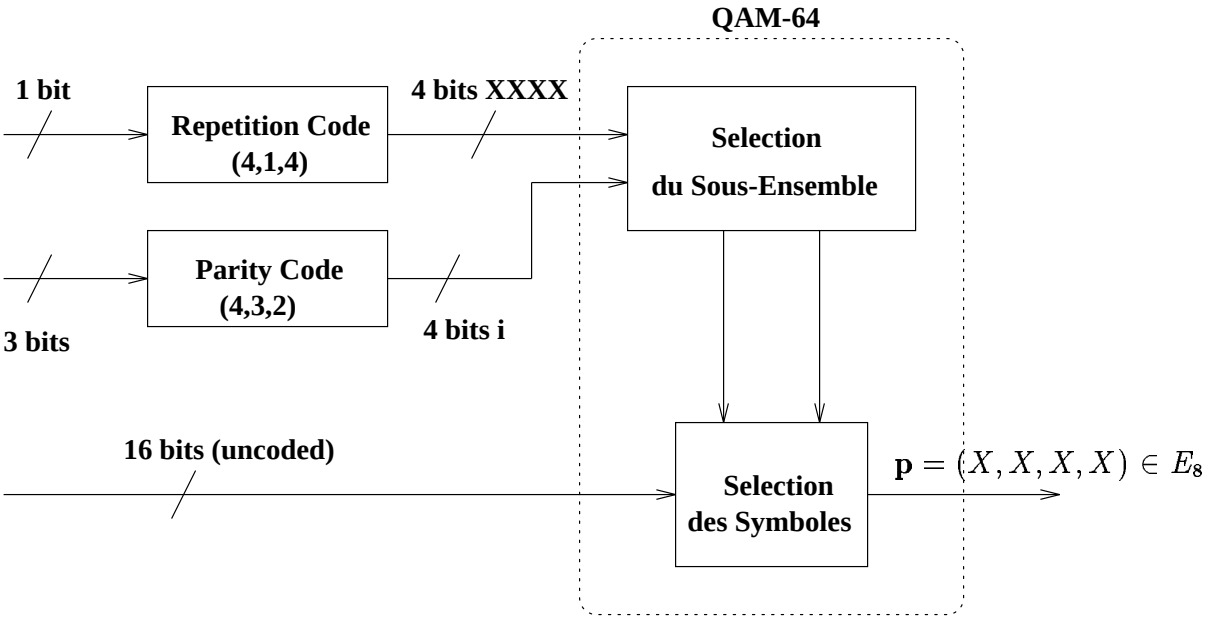


Figure 2.17: Codeur cubique E_8 à 5 bits/symbole.

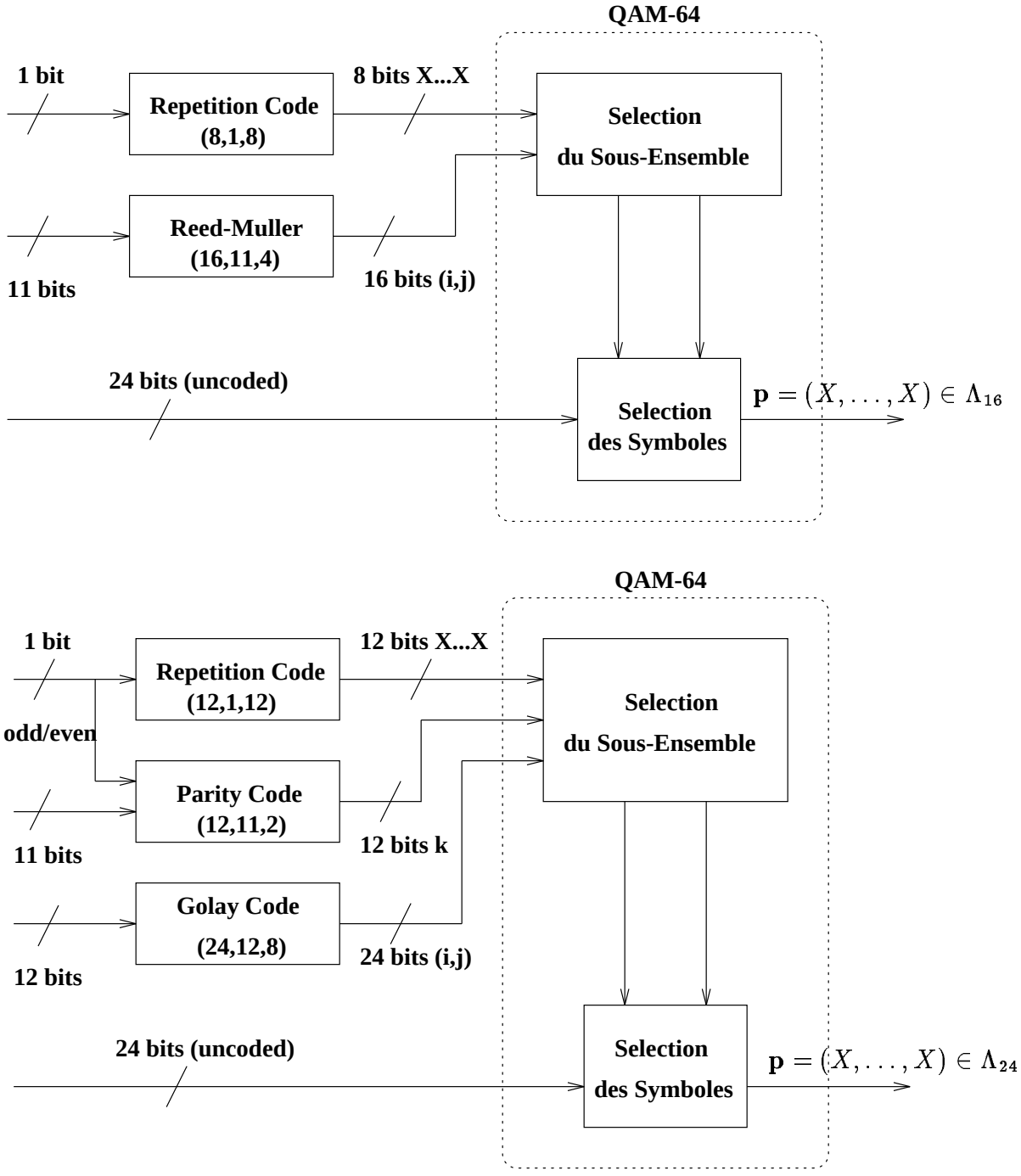


Figure 2.18: Codeurs cubiques Λ_{16} et Λ_{24} à 4.5 et 4 bits/symbole.

Chapter 3

Décodage universel des réseaux de points

Dans ce chapitre nous décrivons un algorithme de décodage de réseaux de points à maximum de vraisemblance. L'algorithme s'applique pour les canaux gaussiens et pour les canaux à évanouissements et ceci quelque soit le réseau. Le décodeur suppose que l'état du canal à évanouissements est parfaitement connu. Il n'existe aucun algorithme dans la littérature pour le décodage de réseaux sur le canal de Rayleigh. Par contre plusieurs dizaines d'algorithmes de décodage de réseaux ou de modulations multiniveaux sur le canal gaussien ont déja été proposés. Ces algorithmes sont basés sur le décodage à décisions souples du code correcteur inclus dans le réseau ou sur le treillis de Forney représentant le réseau ou sur le décodage par étages de la modulation multiniveaux. Citons à titre d'exemples [1] [9] [13] [21] [27] [28] [30] [40] [44] [56] [65] [76] [78] [82] [83] [84]. La représentation d'un réseau de points par un treillis et la complexité de la représentation ont été bien traitées dans des papiers comme [41] [54] [55] [79]. Récemment, le décodage GMD a lui aussi été appliqué aux réseaux de points jusqu'à la dimension 128 [40].

Donc, avec cette batterie d'algorithmes nous devrions être tranquilles en ce qui concerne le décodage. Malheureusement, ce n'est pas le cas. Le problème est simple lorsque l'évanouissement vient multiplier les composantes d'un point du réseau. Il suffit d'introduire les coefficients de l'évanouissement dans la métrique (ou dans la valeur de confiance) associée au point.

La catastrophe se produit lorsque le réseau est tourné (application d'une rotation pour augmenter la diversité) avant de subir l'évanouissement. Le décodage par étages n'est plus possible à cause de la corrélation liant les symboles entre eux. Le réseau n'est plus représentable par un treillis et le décodage souple des codes correcteurs devient lui aussi impossible puisque les composantes de l'espace $\mathbf{Z}^N$ ne sont plus indépendantes. Dans ce cas, le seul algorithme qui puisse fonctionner est le "Sphere Decoder" présenté dans ce chapitre. Nous avons pu appliquer cet algorithme pour décoder les réseaux tournés jusqu'aux dimensions 24 et 32.

3.1 A universal lattice code decoder for fading channels

Lattice codes are used in digital transmission as high rate signal constellations. They are obtained by carving a finite number of points from an n dimensional lattice in the Euclidean space $\mathbf{R}^n$. For the basic notations in lattice theory the reader can refer to [26]. Maximum likelihood (ML) decoding of an arbitrary lattice code used over an additive white Gaussian noise channel is equivalent to finding the closest lattice point to the received point [87, 67, 39].

Recent work on multidimensional modulation schemes for the fading channel show how to construct lattice codes well adapted for such a channel [92].

In the case of independent fading channels, with perfect channel state information (CSI) given to the receiver, ML decoding requires the minimization of the following metric

$$m(\mathbf{x}|\mathbf{r},\boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \tag{3.1}$$

where $\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n}$ is the received vector. The noise vector $\mathbf{n} = (n_1, n_2, \ldots n_n)$ has real, Gaussian distributed independent random variable components, with zero mean and N_0 variance. The random fading coefficients $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ have unit second moment and $*$ represents the component-wise product. $\mathbf{x} = (x_1, x_2, \ldots x_n)$ is one of the transmitted lattice code points. A component interleaver is added to achieve the desired independence of the fading coefficients α_i.

The lattice points can be written as the set $\{\mathbf{x} = \mathbf{u}M\}$ where M is the lattice generator matrix, corresponding to the basis $\{\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_n\}$, and $\mathbf{u} = (u_1, \ldots u_n)$ is the integer component vector to which the information bits are usually mapped. Signal demodulation is assumed to be coherent, so that the fading coefficients can be modeled, after phase elimination, as real random variables with a Rayleigh distribution.

The algorithm proposed in this letter enables to find the closest point of the lattice constellation in terms of metric (3.1).

3.2 The Sphere-Decoder algorithm

We consider first the Gaussian channel case so that we can assume $\alpha_i = 1,\ i = 1, \ldots n$. The lattice decoding algorithm searches through the points of the lattice Λ which are found inside a sphere of given radius $\sqrt{C}$ centered at the received point. This guarantees that only the lattice points within the squared distance C from the received point are considered in the metric minimization.

In the following, it is useful to think of the lattice Λ as the result of a linear transformation, defined by the matrix $M : \mathbf{R}^n \rightarrow \mathbf{R}^n$, when applied to the cubic lattice $\mathbf{Z}^n$.

The problem to solve is the following

$$\min_{\mathbf{x}\in\Lambda} \|\mathbf{r} - \mathbf{x}\| = \min_{\mathbf{w}\in\mathbf{r}-\Lambda} \|\mathbf{w}\|. \tag{3.2}$$

that is, we search for the shortest vector $\mathbf{w}$ in the translated lattice $\mathbf{r}-\Lambda$ in the n-dimensional Euclidean space $\mathbf{R}^n$.

We write $\mathbf{x} = \mathbf{u}M$ with $\mathbf{u} \in \mathbf{Z}^n$, $\mathbf{r} = \boldsymbol{\rho}M$ with $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_n) \in \mathbf{R}^n$, and $\mathbf{w} = \boldsymbol{\xi}M$ with $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbf{R}^n$. Note that $\boldsymbol{\rho}$ and $\boldsymbol{\xi}$ are real vectors. Then we have $\mathbf{w} = \sum_{i=1}^{n} \xi_i \mathbf{v_i}$ where $\xi_i = \rho_i - u_i,\ i = 1, \ldots, n$ define the translated coordinate axes in the space of the integer component vectors $\mathbf{u}$ of the cubic lattice $\mathbf{Z}^n$.

The sphere of square radius C and centered at the received point is transformed into an ellipsoid centered at the origin of the new coordinate system defined by $\boldsymbol{\xi}$:

$$\|\mathbf{w}\|^2 = Q(\boldsymbol{\xi}) = \boldsymbol{\xi}MM^T\boldsymbol{\xi}^T = \boldsymbol{\xi}G\boldsymbol{\xi}^T = \sum_{i=1}^{n}\sum_{j=1}^{n} g_{ij}\xi_i\xi_j \leq C \tag{3.3}$$

Cholesky's factorization of the Gram matrix $G = MM^T$ yields $G = R^TR$, where R is an upper triangular matrix. Then

$$Q(\boldsymbol{\xi}) = \boldsymbol{\xi}R^TR\boldsymbol{\xi}^T = \|R\boldsymbol{\xi}^T\|^2 = \sum_{i=1}^{n}\left(r_{ii}\xi_i + \sum_{j=i+1}^{n} r_{ij}\xi_j\right)^2 \leq C. \tag{3.4}$$

Substituting $q_{ii} = r_{ii}^2$ for $i = 1, \ldots, n$ and $q_{ij} = r_{ij}/r_{ii}$ for $i = 1, \ldots n,\ j = i+1, \ldots, n$, we can write

$$Q(\boldsymbol{\xi}) = \sum_{i=1}^{n} q_{ii}\left(\xi_i + \sum_{j=i+1}^{n} q_{ij}\xi_j\right)^2 \leq C. \tag{3.5}$$

Section 3.5 shows how to compute directly the coefficients q_{ij} of the quadratic form $Q(\boldsymbol{\xi})$.

Starting from ξ_n and working backwards we find the equations of the border of the ellipsoid. The corresponding ranges for the integer components u_n and u_{n-1} are

$$\begin{aligned}
\left\lceil -\sqrt{\frac{C}{q_{nn}}} + \rho_n \right\rceil \leq \quad u_n \quad &\leq \left\lfloor \sqrt{\frac{C}{q_{nn}}} + \rho_n \right\rfloor \\
\left\lceil -\sqrt{\frac{C - q_{nn}\xi_n^2}{q_{n-1,n-1}}} + \rho_{n-1} + q_{n-1,n}\xi_n \right\rceil \leq \quad u_{n-1} \quad &\leq \left\lfloor \sqrt{\frac{C - q_{nn}\xi_n^2}{q_{n-1,n-1}}} + \rho_{n-1} + q_{n-1,n}\xi_n \right\rfloor
\end{aligned}$$

where $\lceil x \rceil$ is the smallest integer greater than x and $\lfloor x \rfloor$ is the greatest integer smaller than x. For the i-th integer component we have

$$\begin{aligned}
&\left\lceil -\sqrt{\frac{1}{q_{ii}}\left(C - \sum_{l=i+1}^{n} q_{il}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} q_{ij}\xi_j \right\rceil \leq u_i \leq \\
&\qquad \leq \left\lfloor \sqrt{\frac{1}{q_{ii}}\left(C - \sum_{l=i+1}^{n} q_{il}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} q_{ij}\xi_j \right\rfloor
\end{aligned} \tag{3.6}$$

The search algorithm proceeds very much like a mixed radix counter on the digits u_i, with the addition that the bounds change whenever there is a carry operation from one digit to the next. In practice, the bounds are updated recursively by using the following equations:

$$\begin{aligned} S_i = S_i(\xi_{i+1}, \ldots, \xi_n) &= \rho_i + \sum_{l=i+1}^{n} q_{il}\xi_l \\ T_{i-1} = T_{i-1}(\xi_i, \ldots, \xi_n) &= C - \sum_{l=i}^{n} q_{i-1,l}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2 = T_i - q_{i,i}\,(S_i - u_i)^2 \end{aligned}$$

When a vector inside the sphere is found, its squared distance from the center (the received point) is given by

$$\hat{d}^2 = C - T_i + q_{11}(S_1 - u_1)^2 \ .$$

This value is compared to the the minimum square distance d^2 (initially set equal to C) found so far in the search. If it is smaller then we have a new candidate closest point and the search continues like this until all the vectors inside the sphere are tested.

The advantage of this method is that we never test vectors with a norm greater than the given radius. Every tested vector requires the computation of its norm, which entails n multiplications and $n-1$ additions. The increase in number of operations needed to update the bounds (3.6) is largely compensated for by the enormous reduction in the number of vectors tested especially when the dimension increases.

In order to be sure to always find a lattice point inside the sphere we must select $\sqrt{C}$ equal to the covering radius of the lattice; otherwise, the decoder can detect a failure if no point is found inside the sphere. A judicious choice of C can greatly speed up the decoder. In practice the choice of C can be adjusted according to the noise variance N_0 so that the probability of a decoding failure is negligible. If a decoding failure is detected the operation can be repeated with a greater radius or an erasure can be declared.

When we deal with a lattice code we must consider the edge effects. During the search in the sphere we discard the points which do not belong to the lattice code; if no code vector is found declare an erasure. The complexity of this additional test depends on the shape of the constellation. For cubic shaped constellations it only entails checking that the vector components lay within a given range.

3.3 The Sphere-Decoder with fading

For ML decoding with perfect CSI at the receiver, the problem is to minimize metric (3.1). Let M be the generator matrix of the lattice Λ and let us consider the lattice Λ_c with generator matrix

$$M_c = M \, \mathrm{diag}(\alpha_1, \ldots \alpha_n) \; .$$

We can imagine this new lattice Λ_c in a space where each component has been compressed or enlarged by a factor α_i. A point of Λ_c can be written as $\mathbf{x}^{(c)} = (x_1^{(c)}, \ldots x_n^{(c)}) = (\alpha_1 x_1, \ldots \alpha_n x_n)$. The metric to minimize is then

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - x_i^{(c)}|^2$$

this means that we can simply apply the lattice decoding algorithm to the lattice Λ_c when the received point is $\mathbf{r}$. The decoded point $\hat{\mathbf{x}}^{(\mathbf{c})} \in \Lambda_c$ has the same integer components $\hat{\mathbf{u}}$ as $\hat{\mathbf{x}} \in \Lambda$.

The additional complexity required by this decoding algorithm comes from the fact that for each received point we have a different compressed lattice Λ_c. So we need to compute a new Cholesky factorization of the Gram matrix for each Λ_c. We also need $M_c^{-1} = \mathrm{diag}(1/\alpha_1, \ldots 1/\alpha_n) M^{-1}$ to find the ρ_i's, but this only requires a vector-matrix multiplication since M^{-1} is precomputed.

The choice of C in this case is more critical. In fact whenever we are in the presence of deep fades then many points fall inside the search sphere and the decoding can be very slow. To overcome this problem it is important to adapt C according to the values of the fading coefficients α_i.

3.4 Conclusions

Decoding arbitrary signal constellations in a fading environment can be a very complex task. When the signal set has no structure it is only possible to perform an exhaustive search through all the constellation points. Some signal constellations, which can be efficiently decoded when used over the Gaussian channel, become hard to decode when used over the fading channel since their structure is destroyed. Fortunately, for lattice constellations this is not the case since the faded constellation still preserves a lattice structure and only a small additional complexity is required.

3.5 Cholesky Decomposition

We briefly summarize the procedure for computing the coefficients $q_{i,j}$ arranged in a matrix Q to be used in (3.5).

```
Q:=A;
for i:=1 to d-1 do
  begin
    for j:=i+1 to d do
      begin
        Q[j,i]:=Q[i,j];
        Q[i,j]:=Q[i,j]/Q[i,i];
      end;
    for k:=i+1 to d do
      for l:=k to d do
        Q[k,l]:=Q[k,l]-Q[k,i]*Q[i,l];
  end;
    for i:=2 to d do
      for j:=1 to i-1 do Q[i,j]:=0;
```

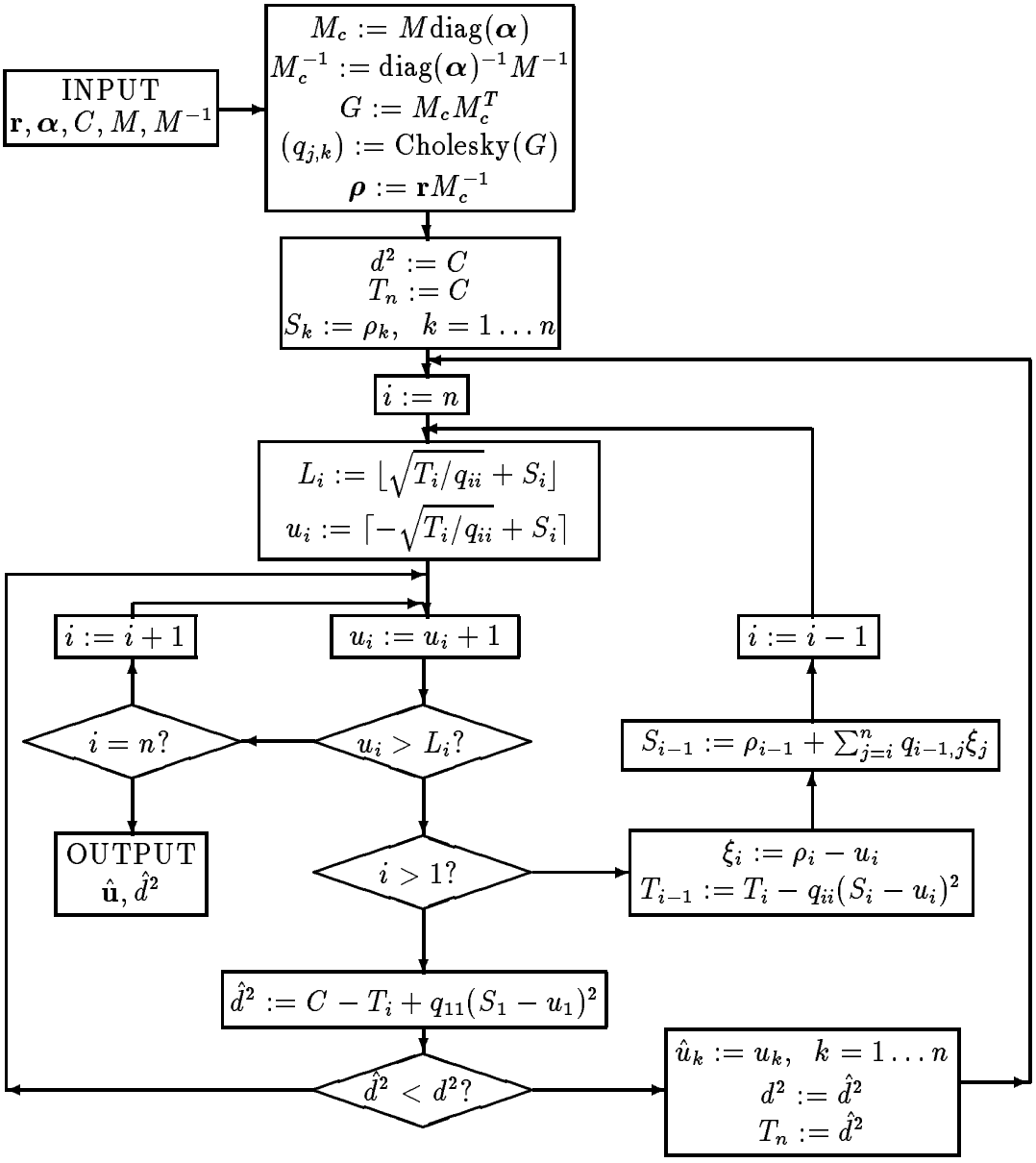


Figure 3.1: Flow chart of the lattice decoding algorithm with fading

Chapter 4

Réseaux de points à grande diversité

Recent work on lattices matched to the Rayleigh fading channel has shown the way to construct good signal constellations with high spectral efficiency. In this chapter we present a new family of lattice constellations, based on complex algebraic number fields, which have good performance on Rayleigh fading channels. Some of these lattices also present a reasonable packing density and thus may be used at the same time over a Gaussian channel. Conversely, we show that particular versions of the best lattice packings ($D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$), constructed from totally complex algebraic cyclotomic fields, present better performance over the Rayleigh fading channel. The practical interest in such signal constellations rises from the need to transmit information at high rates over both terrestrial and satellite links.

4.1 Good lattice constellations for both Rayleigh fading and Gaussian channels

The interest in TCM for fading channels dates back to 1988, when Divsalar and Simon [36] fixed design rules and performance evaluation criteria. Following the ideas in [36], Schlegel and Costello [74] found new 8-PSK trellis codes for the Rayleigh channel. These codes exhibit higher diversity than Ungerboeck's 8-PSK codes, only when the trellis exceeds 64 states.

An alternative method to gain diversity is the use of multidimensional 8-PSK trellis codes proposed by Pietrobon et al. [64]. Although these schemes were designed for the Gaussian channel they show reasonable diversity when the number of states exceeds 16.

All the above TCM schemes have a spectral efficiency of two bits per symbol. The spectral efficiency can be increased by using Ungerboeck's [80] multidimensional QAM trellis codes, but their inherent diversity is very bad due to uncoded bits, which induce parallel transitions in the trellis [36].

Signal constellations having lattice structure are commonly accepted as good means for transmission with high spectral efficiency. The problem of finding good signal constellations for the Gaussian channel can be restated in terms of lattice sphere packings. Good lattice constellations for the Gaussian channel can be carved from lattices with high sphere packing density [26]. The linear and highly symmetrical structure of lattices usually simplifies the decoding task.

For the Rayleigh fading channel the basic ideas remain the same. The problem is to construct signal constellations with minimum average energy for a desired error rate, given the spectral efficiency. A very interesting approach has been recently proposed [17, 48], which makes use of some results of algebraic number theory. Using totally real algebraic number fields, some good lattice constellations matched to the Rayleigh fading channel, up to dimension eight, are found. The effectiveness of these constellations lies in their high degree of diversity, which is actually the maximum possible. By diversity we intend the number of different values in the components of any two distinct points of the constellation.

The signal constellations for the Gaussian channel are usually very bad when used over the Rayleigh fading channel since they have small diversity. Vice versa, the signal constellations in [48] matched to the Rayleigh fading channel are usually very bad when used over the Gaussian channel since the sphere packing density of these lattices is low. In this chapter we search for lattice constellations which have good performance on both Gaussian and Rayleigh fading channel. The same constellations may be used for the Ricean channel which stands in between the Gaussian and the Rayleigh channel.

The practical interest in such signal constellations rises from the need to transmit information over both terrestrial and satellite links. The same modulation/demodulation device can be used to communicate over the terrestrial link (between a mobile and a base station) and over the satellite link (between a mobile and a satellite). Lattice constellations matched to fading channels can also be applied in Wireless Local Area Networks (over the indoor channel) and Asynchronous Digital Subscriber Lines (over the phone line) [2, 89, 62]. The cable channel, combined with a multicarrier modulator and an interleaver, acts as a flat

fading channel.

The chapter outline is the following. In Section 4.2 we show the system model and give the basic definitions. In Section 4.3 we analyze the error probability bounds to find an effective approach to the search of good constellations. The final target of this work is to find good constellations for the Gaussian and the Rayleigh fading channel; we will present two different approaches. The first (Sections 4.4 and 4.5), considers some constellations constructed for the fading channel and trades some of their diversity for a higher asymptotic gain over the Gaussian channel. These constellations are obtained using some results in algebraic number theory, which will be presented in the various subsections. The second approach (Section 4.6) goes in the opposite direction, starting from good constellations for the Gaussian channel we try modifying them to increase their diversity. In this section we will need some further results in algebraic number theory related to ideals and their factorization. Section 4.7 will illustrate the decoding algorithm used with these lattice constellations together with practical results. Finally, in the conclusions we discuss the two different approaches to establish which one is the most effective.

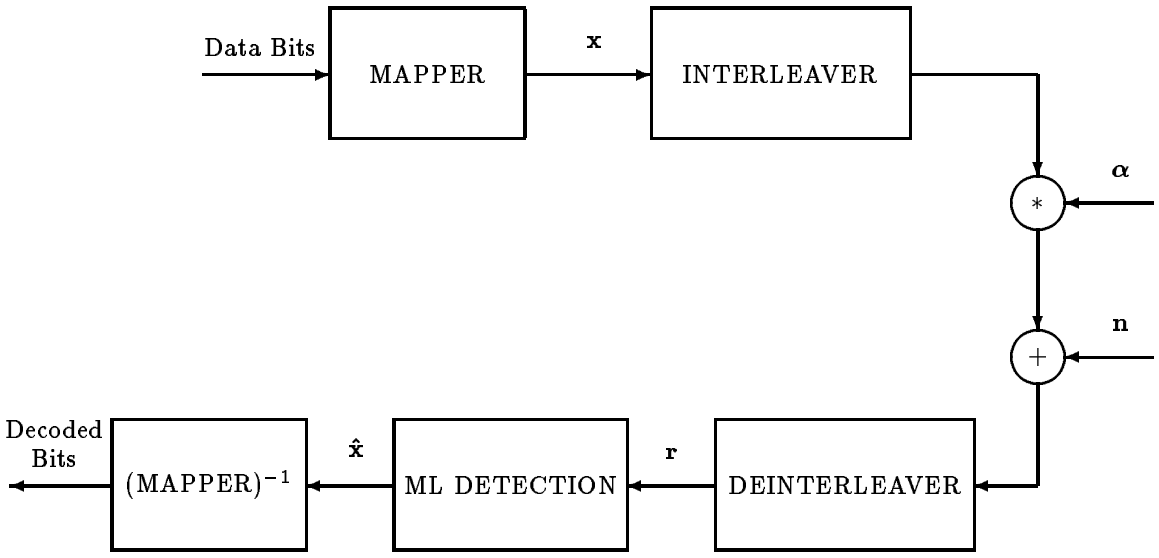


Figure 4.1: The transmission system

4.2 System model and terminology

The baseband transmission system is shown in Figure 4.1. The mapper associates an m-uple of input bits to a signal point $\mathbf{x} = (x_1, x_2, \ldots x_n)$ in the n-dimensional Euclidean space $\mathbf{R}^n$. Let $M = 2^m$ be the total number of signal points in the constellation. An interleaver precedes the channel in the system model. It interleaves the real components of the sequence of mapped points. The constellation points are transmitted either over an additive white Gaussian noise (AWGN) channel, giving $\mathbf{r} = \mathbf{x} + \mathbf{n}$ or over an independent Rayleigh fading channel (RFC) giving $\mathbf{r} = \boldsymbol{\alpha} * \mathbf{x} + \mathbf{n}$, where $\mathbf{r}$ is the received point. $\mathbf{n} = (n_1, n_2, \ldots n_n)$ is a noise vector, whose real components n_i are zero mean, N_0 variance Gaussian distributed independent random variables. $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ are the random fading coefficients with unit second moment and $*$ represents the componentwise product. Signal demodulation is assumed to be coherent, so that the fading coefficients can be modeled after phase elimination, as real random variables with a Rayleigh distribution. The independence of the fading samples represents the situation where the components of the transmitted points are perfectly interleaved. We note that in the case of totally complex lattices (sections 4.4.3 and 4.6), interleaving can be done symbol by symbol instead of componentwise.

The M transmitted signals $\mathbf{x}$ are chosen from a finite constellation S which is carved from a lattice Λ. In particular the points of the constellation are chosen among the first shells of the lattice, so that the signal set approaches the optimal spherical shape. Each point is labeled with an m-bit binary label. The spectral efficiency will be measured in number of

bits per two dimensions

$$\eta = \frac{2m}{n}$$

and the signal to noise ratio per bit is given by

$$SNR = \frac{E_b}{N_0}$$

where E_b is the narrow band average energy per bit and $N_0/2$ is the narrow band noise power spectral density. Let $E = E[\|\mathbf{x}\|^2]$ be the average baseband energy per point of the constellation. The equality $E_b = 0.5 * E/m = E/(n * \eta)$ is very useful to relate the SNR to the constellation's second moment.

After de-interleaving the components of the received points, the maximum likelihood detection criterium imposes the minimization of the following metric

$$m(\mathbf{x}|\mathbf{r}) = \sum_{i=1}^{n} |r_i - x_i|^2 \tag{4.1}$$

for AWGN channel and

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \tag{4.2}$$

for Rayleigh fading channel with perfect side information. Using this criterium we obtain the decoded point $\hat{\mathbf{x}}$ from which the decoded bits are extracted.

4.3 Searching for optimal lattice constellations

To address the search for good constellations we need an estimate of the error probability of the above system.

Since a lattice is *geometrically uniform* we may simply write $P_e(\Lambda) = P_e(\Lambda|\mathbf{x})$ for any transmitted point $\mathbf{x} \in \Lambda$. For convenience, $\mathbf{x}$ is usually taken to be the all zero vector $\mathbf{0}$. We now apply the union bound which gives an upper bound to the point error probability

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{\mathbf{y} \neq \mathbf{x}} P(\mathbf{x} \to \mathbf{y}) \tag{4.3}$$

where $P(\mathbf{x} \to \mathbf{y})$ is the pairwise error probability, the probability that the received point is 'closer' to $\mathbf{y}$ than to $\mathbf{x}$ according to the metric defined in (4.1) or (4.2), when $\mathbf{x}$ is transmitted. The first inequality takes into account the edge effects of the finite constellation S compared to the infinite lattice Λ.

For the AWGN channel equation (4.3) simply becomes [26, Chap. 3]

$$P_e(\Lambda) \leq \frac{\tau}{2} \mathrm{erfc}\left(\frac{d_{Emin}/2}{\sqrt{2N_0}}\right) \tag{4.4}$$

where τ is the *kissing number* and d_{Emin} is the *minimum Euclidean distance* of the lattice. The error probability per point of a cubic constellation can be easily upper bounded (see appendix 4.10) with a function of the signal to noise ratio given by

$$P_e(S) \leq \frac{\tau}{2}\text{erfc}\left(\sqrt{\frac{3\eta}{2^{\eta+1}}\frac{E_b}{N_0}\gamma(\Lambda)}\right) \tag{4.5}$$

where

$$\gamma(\Lambda) = \frac{d^2_{Emin}}{vol(\Lambda)^{2/n}} \tag{4.6}$$

is the *fundamental gain* of Λ. We recall that $\gamma(\mathbf{Z}^n) = 1$ ($\mathbf{Z}^n$ is the n-dimensional integer grid lattice), so that $\gamma(\Lambda)$ is the asymptotic gain of Λ over $\mathbf{Z}^n$. For spherical constellations the total gain should also take into account the shape gain.

For the Rayleigh fading channel, the standard Chernoff bound technique [36] or the direct computation using the Gaussian tail function approximation (see appendix 4.11), give an estimate of the pairwise error probability

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2}\prod_{i=1}^{n}\frac{1}{1+\frac{(x_i-y_i)^2}{8N_0}} \tag{4.7}$$

and for large signal to noise ratios

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2}\prod_{x_i \neq y_i}\frac{1}{\frac{(x_i-y_i)^2}{8N_0}} = \frac{1}{2}\frac{1}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^l d_p^{(l)}(\mathbf{x},\mathbf{y})^2} \tag{4.8}$$

where $d_p^{(l)}(\mathbf{x},\mathbf{y})$ is the (normalized) *l-product distance* of $\mathbf{x}$ from $\mathbf{y}$ when these two points differ in l components

$$d_p^{(l)}(\mathbf{x},\mathbf{y})^2 = \frac{\prod_{x_i \neq y_i}(x_i-y_i)^2}{(E/n)^l}\ . \tag{4.9}$$

Asymptotically, (4.3) is dominated by the term $1/(E_b/N_0)^L$ where L is the minimum number of different components of any two distinct constellation points. L is the so called *diversity* of the signal constellation.

In general rearranging equation (4.3) we obtain

$$P_e(\Lambda) \leq \frac{1}{2}\sum_{l=L}^{n}\frac{K_l}{\left(\frac{\eta}{8}\frac{E_b}{N_0}\right)^l} \tag{4.10}$$

where $K_l = \sum_{d_p^{(l)}}\frac{A_{d_p^{(l)}}}{(d_p^{(l)})^2}$. $A_{d_p^{(l)}}$ is the number of points $\mathbf{y}$ at l-product distance $d_p^{(l)}$ from $\mathbf{x}$ and with l different components, $L \leq l \leq n$. The series in K_l can be interpreted as a *theta series* of the lattice [26], when the product distance is considered instead of the Euclidean distance.

In equation (4.10) we find all the ingredients to obtain a low error probability at a given signal to noise ratio E_b/N_0. In order of relevance we have to :

1. Maximize the diversity $L = \min(l)$.

2. Minimize the average energy per constellation point E.

3. Minimize K_l and especially take care of $d_{p,min} = \min(d_p^{(L)}(\mathbf{x}, \mathbf{y}))$ and $\tau_p = A_{d_p^{(L)}}$ the kissing number for the L-product distance.

The terms in (4.10) clearly become less important when l increases, but the values of $A_{d_p^{(l)}}$ and $d_p^{(l)}(\mathbf{x}, \mathbf{y})$ should be taken into account for non asymptotic considerations.

In fact, the asymptotic coding gain of a system-2 over a reference system-1, having the same spectral efficiency and the same diversity L is given by

$$\gamma_{asympt.} = \left(\frac{K_L(1)}{K_L(2)} \right)^{1/L} \tag{4.11}$$

with the definitions given above. In general, the asymptotic coding gain may not be defined for systems with different diversities L_1 and L_2; in such cases the coding gain varies with the signal to noise ratio.

In the sequel of this chapter, we limit our search for optimal constellations, with high diversity and low energy, to the class of lattices constructed from algebraic number fields.

4.4 Lattices from algebraic number fields

In the following, we will assume that the reader is familiar with the basic definitions on lattices (see Chapter 2 and [26]) and we show the way to construct lattices from algebraic number fields. We will present only the strictly relevant definitions and results in algebraic number theory, which lead to the lattice construction. The exposition is self contained and is based on simple examples, but the interested reader may consult any book on algebraic number theory to quench his thirst for rigour (e.g. [71, 57, 50]). The basic ideas and definitions of section 4 are :

- The number field K and its ring of integers O_K.
- The primitive element θ such that $K = \mathbf{Q}(\theta)$ and its minimal polynomial $\mu_\theta(x)$.
- The integral basis $(\omega_1, \omega_2, \ldots \omega_n)$ of K giving $O_K = \mathbf{Z}[\omega_1, \omega_2, \ldots \omega_n]$.
- The n $\mathbf{Q}$-isomorphisms σ_i defined by $\sigma_i(\theta) = \theta_i$ the ith root of $\mu_\theta(x)$ and the canonical embedding $\sigma : K \rightarrow \mathbf{R}^n$.
- The two special cases of totally real lattices (θ_is totally real) and totally complex lattices (θ_is totally complex).

4.4.1 Algebraic number fields

Let $\mathbf{Z}$ be the ring of rational integers and let K be a field containing $\mathbf{Q}$, the field of rational numbers. Algebraic number theory studies the properties of such fields in relation to the solution of algebraic equations.

Definition 23 – *Let α be an element of K, we say that α is an* **algebraic number** *if it is a root of a monic polynomial with coefficients in $\mathbf{Q}$. Such polynomial with lowest degree is called the minimal polynomial of α and denoted $\mu_\alpha(x)$. If all the elements of K are algebraic we say that K is an* **algebraic extension** *of $\mathbf{Q}$.*

Example 1 - Let us consider the field $K = \{a + b\sqrt{2}$ with $a, b \in \mathbf{Q}\}$. It is simple to see that K is a field containing $\mathbf{Q}$ and that any $\alpha \in K$ is a root of the polynomial $\mu_\alpha(x) = x^2 - 2ax + a^2 - 2b^2$ with rational coefficients. We conclude that K is an algebraic extension of $\mathbf{Q}$.

Definition 24 – *We say that $\alpha \in K$ is an* **algebraic integer** *if it is a root of a monic polynomial with coefficients in $\mathbf{Z}$. The set of algebraic integers of K is a ring called the* **ring of integers** *of K and is indicated with O_K.*

Example 1 (cont.) - In our example, all the algebraic integers will take the form $a + b\sqrt{2}$ with $a, b \in \mathbf{Z}$. Care should be taken in generalizing this result (see Example 3). O_K is a ring contained in K since it is closed under all operations except for the inversion. For example $(2 + 2\sqrt{2})^{-1} = (2 - \sqrt{2})/6$ does not belong to O_K.

Definition 25 – *We define the* **degree** $[K : \mathbf{Q}]$ *of an algebraic extension* K *of* $\mathbf{Q}$ *as the dimension of* K *when considered as a vector space over* $\mathbf{Q}$. *An* **algebraic number field** *is an algebraic extension of* $\mathbf{Q}$ *of finite degree.*

Example 1 (cont.) - K is a vector space over $\mathbf{Q}$ of dimension 2 so it is an algebraic number field of degree 2 (a quadratic field). This is one way of seeing algebraic number fields: as finite dimensional vector spaces over $\mathbf{Q}$.

Result 1 – *Let* K *be an algebraic number field. There exists an element* $\theta \in K$, *called* **primitive element**, *such that the* $\mathbf{Q}$ *vector space* K *is generated by the powers of* θ. *If* K *has degree* n *then* $(1, \theta, \theta^2 \ldots \theta^{n-1})$ *is a* **basis** *of* K *and* $deg(\mu_\theta(x)) = n$. *We will write* $K = \mathbf{Q}(\theta)$.

Example 1 (cont.) - In the above example we have $K = \mathbf{Q}(\sqrt{2})$. $\theta = \sqrt{2}$ is a primitive element since $(1, \sqrt{2})$ form a basis. The minimal polynomial is $\mu_\theta(x) = x^2 - 2$.

Example 2 - Let us consider a slightly more complex example with K generated by $\sqrt{2}$ and $\sqrt{3}$; all its elements may be written as $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ with $a, b, c, d \in \mathbf{Q}$ so that $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a basis of K. If we consider the element $\theta = \sqrt{2} + \sqrt{3}$, we have

$$(1, \theta, \theta^2, \theta^3) = (1, \sqrt{2}, \sqrt{3}, \sqrt{6}) \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

The transition matrix is invertible in $\mathbf{Q}$ proving that we can write $K = \mathbf{Q}(\theta)$. The minimal polynomial of θ is $x^4 - 10x^2 + 1$ and its roots are $\theta = \sqrt{2}+\sqrt{3}, -\sqrt{2}-\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}$. In this particular case they are all primitive elements.

The problem of finding the primitive element given a basis is in general very complex. Usually we start from a field defined by its primitive element.

Result 2 – *There exists a primitive element* θ *which is an algebraic integer of* K. *In other words, the minimal polynomial* $\mu_\theta(x)$ *has coefficients in* $\mathbf{Z}$.

In the above examples θ is not only a primitive element but also an algebraic integer.

4.4.2 Integral basis and canonical embedding

In the special case $K = \mathbf{Q}(\sqrt{2})$, we have seen that the ring of integers O_K was the set of all elements $a + b\sqrt{2}$ with a, b integers. $O_K = \mathbf{Z}(\sqrt{2})$ is a vector space over $\mathbf{Z}$ with $(1, \sqrt{2})$ as a basis. O_K is called a $\mathbf{Z}$-*module*, since $\mathbf{Z}$ is a ring and not a field.

Result 3 – *The ring of integers O_K of K forms a $\mathbf{Z}$-module of rank n (a linear vector space of dimension n over $\mathbf{Z}$).*

Definition 26 – *Let $(\omega_1, \omega_2, \ldots \omega_n)$ be a basis of K. We say that (ω_i) is an* **integral basis** *of K if $O_K = \mathbf{Z}(\omega_1, \omega_2, \ldots \omega_n)$, that is, if (ω_i) is a generating set of the $\mathbf{Z}$-module O_K. So that we can write any element of O_K as $\sum_{i=1}^{n} a_i\omega_i$ with $a_i \in \mathbf{Z}$.*

Example 3 - Take $K = \mathbf{Q}(\sqrt{5})$; we know that any algebraic integer β in K has the form $a + b\sqrt{5}$ with $a, b \in \mathbf{Q}$ such that the polynomial $\mu_\beta(x) = x^2 - 2ax + a^2 - 5b^2$ has integer coefficients. By simple arguments it can be shown that all the elements of O_K take the form $\beta = (u + v\sqrt{5})/2$ with both u, v integers with the same parity. So we can write $\beta = h + k(1+\sqrt{5})/2$ with $h, k \in \mathbf{Z}$. This shows that $(1, (1+\sqrt{5})/2)$ is an integral basis. The basis $(1, \sqrt{5})$ is not integral since $a + b\sqrt{5}$ with $a, b \in \mathbf{Z}$ is only a subset of O_K. Incidently, $(1 + \sqrt{5})/2$ is also a primitive element of K with minimal polynomial $x^2 - x - 1$.

There exist efficient algorithms to find an integral basis of a given algebraic number field in polynomial time [25, 66].

Definition 27 – *Let K and K' be two fields containing $\mathbf{Q}$, we call $\phi : K \to K'$ a* **$\mathbf{Q}$-homomorphism** *if for each $a \in \mathbf{Q}, \phi(a) = a$. If $K' = \mathbf{C}$, the field of complex numbers, a $\mathbf{Q}$-homomorphism $\phi : K \to \mathbf{C}$ is called an* **embedding** *of K into $\mathbf{C}$.*

Result 4 – *Let θ be a primitive element of K and $\mu_\theta(x)$ its minimal polynomial with roots $(\theta_1, \theta_2, \ldots \theta_n)$, $\theta = \theta_1$. There are exactly n embeddings of K into $\mathbf{C}$. Each embedding $\sigma_i : K \to \mathbf{C}$, $\sigma_i(\theta) = \theta_i$, is completely identified by a root $\theta_i \in \mathbf{C}$ of $\mu_\theta(x)$.*

Notice that $\sigma_1(\theta) = \theta_1 = \theta$ and thus σ_1 is the identity mapping, $\sigma_1(K) = K$. When we apply the embedding σ_i to an arbitrary element α of K using the properties of $\mathbf{Q}$-homomorphisms we have

$$\sigma_i(\alpha) = \sigma_i(\sum_{k=1}^{n} a_k\theta^k) = \sum_{k=1}^{n} \sigma_i(a_k)\sigma_i(\theta)^k = \sum_{k=1}^{n} a_k\theta_i^k \in \mathbf{C}$$

and we see that the image of any α under σ_i is uniquely identified by θ_i.

Definition 28 – *The elements $\sigma_1(\alpha), \sigma_2(\alpha), \ldots \sigma_n(\alpha)$ are called the* **conjugates** *of α and*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

is the **algebraic norm** *of α.*

Result 5 – *For any $\alpha \in K$, we have $N(\alpha) \in \mathbf{Q}$. If $\alpha \in O_K$ we have $N(\alpha) \in \mathbf{Z}$.*

Example 1 (cont.) - The roots of the minimal polynomial $x^2 - 2$ are $\theta_1 = \sqrt{2}$ and $\theta_2 = -\sqrt{2}$ then

$$\begin{array}{lll} \sigma_1(\theta) = & \sqrt{2} & \sigma_1(a + b\sqrt{2}) = a + b\sqrt{2} \\ \sigma_2(\theta) = & -\sqrt{2} & \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2} \end{array}$$

The algebraic norm of α is $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = a^2 - 2b^2$ and we can verify the above result.

Definition 29 – *Let $(\omega_1, \omega_2, \ldots \omega_n)$ be an integral basis of K. The* **absolute discriminant** *of K is defined as $d_K = \det[\sigma_j(\omega_i)]^2$.*

Result 6 – *The absolute discriminant belongs to* $\mathbf{Z}$.

Example 3 (cont.) - Applying the 2 $\mathbf{Q}$-homomorphisms to the integral basis ω_1, ω_2, we obtain

$$d_K = \det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 = 5 \ .$$

Definition 30 – *Let $(\sigma_1, \sigma_2, \ldots \sigma_n)$ be the n $\mathbf{Q}$-homomorphisms of K into $\mathbf{C}$. Let r_1 be the number of $\mathbf{Q}$-homomorphisms with image in $\mathbf{R}$, the field of real numbers, and $2r_2$ the number of $\mathbf{Q}$-homomorphisms with image in $\mathbf{C}$ so that*

$$r_1 + 2r_2 = n \ .$$

The pair (r_1, r_2) is called the **signature** *of K. If $r_2 = 0$ we have a* **totally real** *algebraic number field. If $r_1 = 0$ we have a* **totally complex** *algebraic number field. In all other cases we will speak about complex algebraic number field.*

Example 4 - All the previous examples were totally real algebraic number fields with $r_1 = n$. Let us now consider $K = \mathbf{Q}(\sqrt{-3})$. The minimal polynomial of $\sqrt{-3}$ is $x^2 + 3$ and has 2 complex roots so the signature of K is (0, 1). For later use we observe that $(1, \sqrt{-3})$ is not an integral basis. If we take $\theta = e^{\frac{i\pi}{3}} = (1 + i\sqrt{3})/2$ where $i = \sqrt{-1}$, we have $K = \mathbf{Q}(\theta) = \mathbf{Q}(\sqrt{-3})$ and an integral basis is $(1, (1 + i\sqrt{3})/2)$. The minimal polynomial of θ is $x^2 - x + 1$. The ring of integers of this field is also known as the Eisenstein integer ring. This is the most simple example of *cyclotomic field* i.e., a field generated by an m-th root of unity.

Definition 31 – *Let us order the σ_i's so that $\sigma_i(\alpha) \in \mathbf{R}$ for $1 \leq i \leq r_1$ and $\sigma_{j+r_2}(\alpha)$ is the complex conjugate of $\sigma_j(\alpha)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. We call* **canonical embedding** *$\sigma : K \to \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ the isomorphism defined by*

$$\sigma(\alpha) = (\sigma_1(\alpha) \ldots \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \ldots \sigma_{r_1+r_2}(\alpha)) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

If we identify $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ *with* $\mathbf{R}^n$*, the canonical embedding can be rewritten as* $\sigma : K \rightarrow \mathbf{R}^n$*,*

$$\sigma(\alpha) = (\sigma_1(\alpha), \ldots \sigma_{r_1}(\alpha), \Re\sigma_{r_1+1}(\alpha), \Im\sigma_{r_1+1}(\alpha), \ldots \Re\sigma_{r_1+r_2}(\alpha), \Im\sigma_{r_1+r_2}(\alpha)) \in \mathbf{R}^n$$

where $\Re$ *is the real part and* $\Im$ *is the imaginary part.*

This definition establishes a one to one correspondence between the elements of an algebraic number field of degree n and the vectors of the n-dimensional Euclidean space. The final step for this algebraic construction of a lattice is given by the following result.

Result 7 – *Let* $(\omega_1, \omega_2, \ldots \omega_n)$ *be an integral basis of* K *and let* d_K *be the absolute discriminant of* K*. The* n *vectors* $\mathbf{v}_i = \sigma(\omega_i) \in \mathbf{R}^n$ *are linearly independent, so they define a full rank lattice* $\Lambda = \sigma(O_K)$ *with generator matrix*

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \ldots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \ldots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \ldots & \sigma_{r_1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \ldots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\omega_n) & \ldots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \ldots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix} \tag{4.12}$$

The vectors $\mathbf{v}_i$ *are the rows of* G*. The volume of the fundamental parallelotope of* Λ *is given by [71]*

$$vol(\Lambda) = |\det(G)| = 2^{-r_2} \times \sqrt{|d_K|} \tag{4.13}$$

4.4.3 Totally real and totally complex number fields

Result 8 *The lattices obtained from the generator matrix (4.12) exhibit a diversity* $L = r_1 + r_2$.

Proof. Let $\mathbf{z} \neq \mathbf{0}$ be an arbitrary point of Λ

$$\mathbf{z} = (z_1, z_2, \ldots z_n) = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i$$

with $\lambda_i \in \mathbf{Z}$ and $\mathbf{v}_i = (v_{ij}) = \sigma(\omega_i)$ the rows of the lattice generator matrix G.

$$\prod_{j=1}^{n} |z_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| = \prod_{j=1}^{r_1} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| \times \prod_{j=r1+1}^{r_1+r_2} \left| \Re\sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| \times \prod_{j=r1+1}^{r_1+r_2} \left| \Im\sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| \tag{4.14}$$

The algebraic integer $\sum_{i=1}^{n} \lambda_i \omega_i$ is non zero because all λ_is are not null together ($z \neq 0$). This implies that $\sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \neq 0$ and so the 1st product at the right side of the above expression contains exactly r_1 non zero factors. The minimum number of non zero factors in the 2nd and the 3rd products is r_2 since the real and imaginary parts of any one of the complex embeddings may not be null together. We then conclude that for such lattices we have a diversity $L \geq r_1 + r_2$. Now, let's take the special element $\alpha = 1$ in O_K. The canonical embedding applied to 1 gives exactly $r_1 + r_2$ non zero terms in the above product ($\sigma_j(1) = 1$ for any j). Hence, we can confirm that $L = r_1 + r_2$, as indicated in [18]. Q.E.D.

In the case of totally real algebraic number fields ($r_2 = 0$), presented in [48], we have

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \ldots & \sigma_n(\omega_1) \\ \sigma_1(\omega_2) & \sigma_2(\omega_2) & \ldots & \sigma_n(\omega_2) \\ \vdots & & & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \ldots & \sigma_n(\omega_n) \end{pmatrix}$$

The lattice Λ constructed in this case attains the maximum degree of diversity $L = n$. The n-product distance of $\mathbf{z}$ from $\mathbf{0}$ is

$$\begin{aligned} d_p^n(\mathbf{0}, \mathbf{z}) &= \prod_{j=1}^{n} |z_j| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i v_{ij} \right| = \prod_{j=1}^{n} \left| \sum_{i=1}^{n} \lambda_i \sigma_j(\omega_i) \right| \\ &= \prod_{j=1}^{n} \left| \sigma_j \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| = \left| N \left(\sum_{i=1}^{n} \lambda_i \omega_i \right) \right| \end{aligned} \tag{4.15}$$

Since $\sum_{i=1}^{n} \lambda_i \omega_i \in O_K$ and it is different from zero, according to result 5, we have

$$d_p^{(n)}(\mathbf{0}, \mathbf{z}) \geq 1 \qquad \forall \mathbf{z} \neq \mathbf{0}$$

The minimum product distance $d_{p,min} = 1$ is given by the elements of K with algebraic norm 1, the so called *units* of K. The fundamental parallelotope has volume

$$vol(\Lambda) = \sqrt{|d_K|} \ .$$

n	$r_2 = 0$	$r_2 = 1$	$r_2 = 2$	$r_2 = 3$	$r_2 = 4$
2	5	-3	—	—	—
3	49	-23	—	—	—
4	725	-275	117	—	—
5	14641	-4511	1609	—	—
6	300125	-92779^*	28037^*	-9747	—
7	20134393	?	?	?	—
8	282300416	?	?	?	1257728^*

Table 4.1: Minimal absolute discriminants. Values with a * are the best known values.

The totally real algebraic number fields with minimum absolute discriminant are known up to dimension 8 (first column Table 4.1) and appear to be the best asymptotically good lattices for the Rayleigh fading channel. In fact, for a fixed number of points M, the energy of constellations carved from these lattices is proportional to $vol(\Lambda)$ and $vol(\Lambda)$ is minimized by selecting the fields with minimum absolute discriminants.

Still two disadvantages are hidden behind the maximal diversity and the minimal absolute discriminant. The fundamental volume can be further reduced if we choose a signature where $r_2 \neq 0$, i.e. if the number field is complex. Equation (4.13) shows that $vol(\Lambda)$ can be divided by 2^{r_2}. We can even maximize r_2 by working in a totally complex field, $r_2 = n/2$. Lattices derived from totally real number fields have bad performance over a Gaussian channel (a negative fundamental gain as shown in Section 4.7) mainly because of their high values of $vol(\Lambda)$ (Table 4.1). The second disadvantage appears over the fading channel and is related to the product kissing number τ_p. We find that the product kissing number is much higher for real fields lattices than for complex fields lattices.

High diversity dense lattices built from complex algebraic number fields have been first proposed in [18]. The totally complex fields are possible only for even degrees since $r_2 = n/2$. The generator matrix is

$$\mathrm{G} = \begin{pmatrix} \Re\sigma_1(\omega_1) & \Im\sigma_1(\omega_1) & \dots & \Re\sigma_{r_2}(\omega_1) & \Im\sigma_{r_2}(\omega_1) \\ \Re\sigma_1(\omega_2) & \Im\sigma_1(\omega_2) & \dots & \Re\sigma_{r_2}(\omega_2) & \Im\sigma_{r_2}(\omega_2) \\ \vdots & & & & \vdots \\ \Re\sigma_1(\omega_n) & \Im\sigma_1(\omega_n) & \dots & \Re\sigma_{r_2}(\omega_n) & \Im\sigma_{r_2}(\omega_n) \end{pmatrix} \tag{4.16}$$

Nothing can be said about the value of the minimum product distance $d_{p,min}$ for complex fields lattices, since it is not related to the algebraic norm as in the totally real case.

Looking at Table 4.1 we immediately notice that the absolute discriminants of the complex fields are comparatively smaller than the ones for the totally real fields. This fact, combined with the fact that $vol(\Lambda)$ is reduced by a factor 2^{-r_2}, results in lower average energy of the constellation S, for complex fields. Of course the price to pay is the reduced

diversity unless we use number fields with higher degrees such as 12, 16 or 24. This lead us to search for good lattices (Λ_{16} or Λ_{24}) adapted to Rayleigh channel and the logical continuation is section 4.6. In the next section, we study in detail some of the lattices constructed by canonical embedding applied to fields in Tables 4.1 and 4.2.

	$\mu_\theta(x)$	$vol(\Lambda_{n,L})$	$\gamma(\Lambda_{n,L})$
$\Lambda_{2,1}$	$x^2 - x + 1$	0.8660	0.624
$\Lambda_{2,2}$	$x^2 - x - 1$	2.2361	-0.484
$\Lambda_{3,2}$	$x^3 - x - 1$	2.3979	0.242
$\Lambda_{3,3}$	$x^3 + x^2 - 2x - 1$	7	-0.862
$\Lambda_{4,2}$	$x^4 - x^3 - x^2 + x + 1$	2.7042	0.850
$\Lambda_{4,3}$	$x^4 - x^3 + 2x - 1$	8.2916	0.178
$\Lambda_{4,4}$	$x^4 - x^3 - 3x^2 + x + 1$	26.9258	-1.130
$\Lambda_{5,3}$	$x^5 - x^3 + x^2 + x - 1$	10.0281	0.597
$\Lambda_{5,4}$	$x^5 - 2x^3 + x^2 - 1$	33.5820	-0.083
$\Lambda_{5,5}$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	121	-1.341
$\Lambda_{6,3}$	$x^6 - 3x^5 + 4x^4 - 4x^3 + 4x^2 - 2x + 1$	12.3409	1.133
$\Lambda_{6,4}$	$x^6 - 2x^5 + 3x^3 - 2x - 1$	41.8606	0.379
$\Lambda_{6,5}$	$x^6 + x^5 - 2x^4 - 3x^3 - x^2 + 2x + 1$	152.2982	-0.285
$\Lambda_{6,6}$	$x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1$	547.8367	-1.347
$\Lambda_{7,7}$	$x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1$	4487.1364	-1.983
$\Lambda_{8,4}$	$x^8 - 2x^7 + 4x^5 - 4x4 + 3x^2 - 2x + 1$	70.0928	1.406
$\Lambda_{8,8}$	$x^8 + 2x^7 - 7x^6 - 8x^5 + 15x^4 + 8x^3 - 9x^2 - 2x + 1$	16801.7980	-1.532

Table 4.2: Reduced minimal polynomials and fundamental volumes and gains (in dB) of the corresponding lattices.

4.5 Lattices from minimal absolute discriminant fields

In Table 4.1 we have all the known minimal absolute discriminant fields up to dimension 8. These fields (especially in dimensions above 4) have been a subject of study of a branch of mathematics known as *computational algebraic number theory*. Computational algebraic number theory has developed powerful algorithmic tools which enable to extend many results, with the aid of computers, to fields of higher degree [25, 66]. Part of this table, up to $n = 6$, can be found in [50] and the references therein. All the totally real fields are reported in [48]. For degree 5 and 6 complex fields see references [51] and [61] respectively. The degree 8, totally complex field of minimal absolute discriminant can be found in [33] together with other 25 totally complex fields of absolute discriminant smaller than 1954287. Table 4.2 gives the *reduced* minimal polynomials of the fields of Table 4.1 along with the fundamental volume of the corresponding lattice obtained from the canonical embedding and their fundamental gains in decibels. A minimal polynomial is called *reduced* if the powers of one of its roots (the primitive element) is an integral basis of the number field. These lattices will be indicated with $\Lambda_{n,L}$.

The main steps for the construction of a lattice from an algebraic number field $K = \mathbf{Q}(\theta)$ can be summarized as follows:

- Find an integral basis of K, which identifies O_K.
- Find the n roots of $\mu_\theta(x)$, which identify the n embeddigs $\sigma_1, \sigma_2, \ldots \sigma_n$.
- Construct the generator matrix applying the canonical embedding.

We show the application of this procedure to some of the lattices of Table 4.2.

$\Lambda_{2,1}$ - $K = \mathbf{Q}(i\sqrt{3})$. From Example 4 we have the integral basis $(1, \frac{1+i\sqrt{3}}{2})$. The 2 embeddings are $\sigma_1(i\sqrt{3}) = i\sqrt{3}$, $\sigma_2(i\sqrt{3}) = -i\sqrt{3}$ and the lattice generator matrix is:

$$G = \begin{pmatrix} \Re\sigma_1(1) & \Im\sigma_1(1) \\ \Re\sigma_1(\frac{1+i\sqrt{3}}{2}) & \Im\sigma_1(\frac{1+i\sqrt{3}}{2}) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

We may recognize in the above matrix the *hexagonal lattice* A_2. The fundamental volume is $vol(\Lambda_{2,1}) = |\det(G)| = \sqrt{3}/2$ and the minimum squared Euclidean distance is $d^2_{Emin} = 1$. $r_1 = 0, r_2 = 1$ and the diversity is $L = 1$ since the vector $(1, 0)$ belongs to the lattice.

$\Lambda_{2,2}$ - $K = \mathbf{Q}(\sqrt{5})$. From Example 3 we have the integral basis $(1, \frac{1+\sqrt{5}}{2})$. The 2 embeddings are $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$ and the lattice generator matrix is:

$$G = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\frac{1+\sqrt{5}}{2}) & \sigma_2(\frac{1+\sqrt{5}}{2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}$$

The fundamental volume is $vol(\Lambda_{2,2}) = |\det(G)| = \sqrt{5}$ and the minimum squared Euclidean distance is $d^2_{Emin} = 2$. $r_1 = 2, r_2 = 0$ and the diversity is $L = 2$.

$\Lambda_{3,2}$ - $K = \mathbf{Q}(\theta)$, where θ is a primitive element with minimal polynomial $x^3 - x - 1$, whose roots are

$$\theta_1 = U + V \quad \theta_{2,3} = -\frac{1}{2}(U+V) \pm i\frac{\sqrt{3}}{2}(U-V)$$

where

$$U = \frac{1}{3}\sqrt[3]{\frac{9+3\sqrt{63}}{2}} \qquad V = \frac{1}{3}\sqrt[3]{\frac{9-3\sqrt{63}}{2}}$$

The primitive element θ coincides with θ_2 and an integral basis is $1, \theta, \theta^2$. The three embeddings are $\sigma_1(\theta) = \theta_1$ (real), $\sigma_2(\theta) = \theta_2$ and $\sigma_3(\theta) = \theta_3$, where σ_2 and σ_3 are conjugates $(r_1 = 1, r_2 = 1)$. We obtain the lattice generator matrix:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 \\ (U+V) & -\frac{1}{2}(U+V) & \frac{\sqrt{3}}{2}(U+V) \\ (U+V)^2 - 4 & -\frac{1}{2}(U^2+V^2-4UV) & -\frac{\sqrt{3}}{2}(U^2-V^2) \end{pmatrix} = \begin{pmatrix} 1.000 & 1.000 & 0.000 \\ 1.325 & -0.662 & 0.562 \\ 1.755 & 0.123 & -0.745 \end{pmatrix}$$

The fundamental volume is $vol(\Lambda_{3,2}) = |\det(G)| = 2.39$ and the minimum squared Euclidean distance is $d^2_{Emin} = 1.895$. The diversity is given by $L = r_1 + r_2 = 2$ since the vector $(1, 1, 0)$ belongs to the lattice and $d^{(2)}_p((0,0,0),(1,1,0)) = 1$.

$\Lambda_{3,3}$ - $K = \mathbf{Q}(\cos(2\pi/7))$. An integral basis is $(2\cos(2\pi/7), 2\cos(4\pi/7), 2\cos(6\pi/7))$. With the following three embeddings $\sigma_1(\cos(2\pi/7)) = \cos(2\pi/7)$, $\sigma_2(\cos(2\pi/7)) = \cos(4\pi/7)$, $\sigma_3(\cos(2\pi/7)) = \cos(6\pi/7)$ we obtain the lattice generator matrix:

$$G = \begin{pmatrix} 2\cos(2\pi/7) & 2\cos(4\pi/7) & 2\cos(6\pi/7) \\ 2\cos(4\pi/7) & 2\cos(6\pi/7) & 2\cos(2\pi/7) \\ 2\cos(6\pi/7) & 2\cos(2\pi/7) & 2\cos(4\pi/7) \end{pmatrix}$$

The fundamental volume is $vol(\Lambda_{3,3}) = |\det(G)| = 7$ and the minimum squared Euclidean distance is $d^2_{Emin} = 3$. The diversity is $L = 3$.

$\Lambda_{4,2}$ - $K = \mathbf{Q}(\theta)$ where θ is a primitive element with minimal polynomial $x^4 + 2x^2 + 13$ and roots

$$\theta_{1,2,3,4} = \pm(R \pm iI) = \pm\left(\sqrt{\frac{\sqrt{13}-1}{2}} \pm i\sqrt{\frac{\sqrt{13}+1}{2}}\right)$$

Taking the following signs for the roots $\theta_1 : (++)$, $\theta_2 = (-+)$, $\theta_3 : (+-)$, $\theta_4 : (--)$ we have the primitive element $\theta = \theta_1$ and the four embeddings $\sigma_1(\theta) = \theta_1$, $\sigma_2(\theta) = \theta_2$, $\sigma_3(\theta) = \theta_3$, $\sigma_4(\theta) = \theta_4$. The canonical embedding is given by $\sigma = (\Re\sigma_1, \Im\sigma_1, \Re\sigma_2, \Im\sigma_2)$, but $(1, \theta, \theta^2, \theta^3)$ is not an integral basis, because $x^4 + 2x^2 + 13$ is not reduced. An integral basis is

$$\left(1,\ \frac{1}{2}(1+\theta),\ \frac{1}{4}(3+\theta^2),\ \frac{1}{8}(1+\theta)(3+\theta^2)\right)$$

We obtain the lattice generator matrix:

$$\mathrm{G} = \begin{pmatrix} 1.000 & 0.000 & 1.000 & 0.000 \\ 1.070 & -0.758 & -0.070 & -0.758 \\ 0.500 & -0.866 & 0.500 & 0.866 \\ -0.121 & -1.306 & 0.621 & -0.440 \end{pmatrix}$$

The fundamental volume is $vol(\Lambda_{4,2}) = |\det(G)| = 2.70$ and the minimum squared Euclidean distance is $d^2_{Emin} = 2$. The diversity is given by $L = r_2 = 2$ since the vector $(1, 0, 1, 0)$ belongs to the lattice and $d^{(2)}_p((0,0,0,0),(1,0,1,0)) = 1$.

$\Lambda_{4,3}$ - $K = \mathbf{Q}(i\sqrt{-3+2\sqrt{5}})$. The roots of the minimal polynomial $x^4 - 6x^2 - 11$ are $\theta_1 = \sqrt{3+2\sqrt{5}}$, $\theta_2 = -\sqrt{3+2\sqrt{5}}$, $\theta_3 = i\sqrt{-3+2\sqrt{5}}$, and $\theta_4 = -i\sqrt{-3+2\sqrt{5}}$. With $\theta = \theta_3$, the four embeddings are $\sigma_1(\theta) = \theta_1$, $\sigma_2(\theta) = \theta_2$, $\sigma_3(\theta) = \theta_3$ and $\sigma_4(\theta) = \theta_4$ and the integral basis has the same form as in $\Lambda_{4,2}$. The canonical embedding is given by $\sigma = (\sigma_1, \sigma_2, \Re\sigma_3, \Im\sigma_3)$. We obtain the lattice generator matrix:

$$G = \begin{pmatrix} 1.000 & 1.000 & 1.000 & 0.000 \\ 1.866 & -0.866 & 0.500 & -0.606 \\ 2.618 & 2.618 & 0.381 & 0.000 \\ 4.887 & -2.269 & 0.190 & -0.231 \end{pmatrix}$$

n	$r_2 = 0$	$r_2 = 1$	$r_2 = 2$	$r_2 = 3$	$r_2 = 4$
2	-0.485	0.625	—	—	—
3	-0.863	0.242	—	—	—
4	-1.130	0.178	0.850	—	—
5	-1.341	-0.084	0.597	—	—
6	-1.347	-0.286	0.380	1.133	—
7	-1.983	?	?	?	—
8	-1.532	?	?	?	1.406

Table 4.3: Asymptotic gains for the Gaussian channel

As an example we show the calculation of the element $(4,2)$ of the above matrix

$$\sigma_2(\frac{1}{8}(1+\theta)(3+\theta^2)) = \sigma_2(\frac{1}{8})\sigma_2(1+\theta)\sigma_2(3+\theta^2) =$$
$$= \sigma_2(\frac{1}{8})(\sigma_2(1)+\sigma_2(\theta))(\sigma_2(3)+\sigma_2(\theta^2)) = \frac{1}{8}(1+\theta_2)(3+\theta_2^2) = -2.269$$

The fundamental volume is $vol(\Lambda_{4,3}) = |\det(G)| = 8.29$ and the minimum squared Euclidean distance is $d^2_{Emin} = 2$. The diversity is given by $L = r_1 + r_2 = 3$ since the vector $(1,1,1,0)$ belongs to the lattice and $d_p^{(3)}((0,0,0,0),(1,1,1,0)) = 1$.

$\Lambda_{4,4}$ - $K = \mathbf{Q}(\sqrt{7+2\sqrt{5}})$. The roots of the minimal polynomial $x^4 - 14x^2 + 29$ are $\theta_1 = \sqrt{7+2\sqrt{5}}$, $\theta_2 = -\sqrt{7+2\sqrt{5}}$, $\theta_3 = \sqrt{7-2\sqrt{5}}$, and $\theta_4 = -\sqrt{7-2\sqrt{5}}$. With $\theta = \theta_1$, the four embeddings are $\sigma_1(\theta) = \theta_1$, $\sigma_2(\theta) = \theta_2$, $\sigma_3(\theta) = \theta_3$, $\sigma_4(\theta) = \theta_4$ and an integral basis has the same form as in $\Lambda_{4,2}$. We obtain the lattice generator matrix:

$$G = \begin{pmatrix} 1.000 & 1.000 & 1.000 & 1.000 \\ -1.193 & -0.294 & 1.294 & 2.193 \\ 3.618 & 1.381 & 1.381 & 3.618 \\ -4.318 & -0.407 & 1.789 & 7.936 \end{pmatrix}$$

The fundamental volume is $vol(\Lambda_{4,4}) = |\det(G)| = 26.92$ and the minimum squared Euclidean distance is $d^2_{Emin} = 4$. According to Section 4.4.3, the diversity is 4 and $d_{p,min} = 1$.

	$\mathbf{Q}(\theta)$	N	Ideals
$D_{4,2}$	θ^4+1	8	$(2,\theta+1)$
$E_{6,3}$	$\theta^6-\theta^3+1$	9	$(3,(\theta+1)^2)$
$E_{8,4}$	$\theta^8-\theta^6+\theta^4-\theta^2+1$	20	$(5,\theta-2)$
$K_{12,6}$	$\theta^{12}-\theta^{11}+\theta^9-\theta^8+$ $+\theta^6-\theta^4+\theta^3-\theta+1$	21	$(7,\theta+3)$
$\Lambda_{16,8}$	$\theta^{16}-\theta^{12}+\theta^8-\theta^4+1$	40	$(2,\theta^4+\theta^3+\theta^2+\theta+1)$ $(5,\theta^2+2)$
$\Lambda_{24,12}$	$\theta^{24}-\theta^{23}+\theta^{21}-\theta^{20}+\theta^{18}-\theta^{17}+\theta^{15}-\theta^{14}$ $+\theta^{12}-\theta^{10}+\theta^9-\theta^7+\theta^6-\theta^4+\theta^3-\theta+1$	39	$(3,\theta^3+\theta^2-1)$ $(3,\theta^3+\theta^2+\theta+1)$ $(13,\theta-3)$

Table 4.4: Some known lattices from cyclotomic fields

4.6 Lattices for the Gaussian channel adapted to the fading channel

The idea of rotating a QAM constellation in order to increase its diversity was first presented in [17]. The advantage of such a technique lays in the fact that the rotated constellation holds its properties over the Gaussian channel. The method proposed was straightforward: find the rotation angle which gives a diversity of 2 and maximizes the minimum product distance. It was found that for a 16-QAM the rotation angle of $\pi/8$ was optimum. Unfortunately, in dimensions greater than 2 this method becomes impracticable.

We have at our disposal the work of Craig [31, 32], who showed how to construct the lattices E_6, E_8, Λ_{24} (Leech lattice) from the totally complex cyclotomic fields $K=\mathbf{Q}(e^{i2\pi/N})$ for $N=9,20,39$. Applying his procedure we found D_4 (Schlafli lattice), K_{12} (Coxeter-Todd's lattice) and Λ_{16} (Barnes-Wall's lattice) from the $8th, 21st$ and the $40th$ root of unity. These lattices are obtained by applying the canonical embedding to particular integral ideals of the above cyclotomic fields. The ideals are given in Table 4.4. The lattices we obtain are actually sublattices of $\sigma(O_K)$. This means that they have the same diversity $L=n/2$ of $\sigma(O_K)$, but a much higher fundamental gain compared to the lattices presented in section 4.5.

To illustrate the construction of the most famous lattice sphere packings, we need a few more results from algebraic number theory.

4.6.1 Ideals in the ring of integers

In the sequel, all given definitions and properties for ideals are true only in number fields and are not necessarily valid in an arbitrary field. For more theoretical details, the reader is invited to consult [71], [25] and [66].

Definition 32 – *Let K be a number field of degree n and O_K its ring of integers. An* **ideal** *I of O_K is a sub-$\mathbf{Z}$-module of O_K such that for every $a \in O_K$ and $b \in I$ we have $ab \in I$, briefly $aI \subset I$ and $bO_K \subset I$.*

The sum and the product of two ideals I and J of O_K, are also ideals of O_K and are defined by

$$\begin{aligned} I+J &= \{x+y, \text{ where } x \in I \text{ and } y \in J\} \\ IJ &= \{\sum_i x_i y_i, \text{ where } x_i \in I \text{ and } y_i \in J\} . \end{aligned}$$

Similarly, the intersection of two ideals is an ideal and we have the inclusions

$$IJ \subset I \cap J \subset I \subset I+J .$$

Definition 33 – *An ideal I of O_K is called* **prime** *(or* **maximal***) if the quotient ring O_K/I is a field. I is called* **principal** *if $I = \alpha O_K$ for some algebraic integer α, in this case we also denote $I = (\alpha)$.*

Result 9 – *Let I be a non-zero ideal of O_K. Then I is a module of maximal rank. The quotient ring O_K/I is finite and its cardinality is called the* **norm** *of the ideal I and denoted $N(I)$, $N(I) = Card(O_K/I) = [O_K : I]$.*

If $\omega_1, \omega_2, \ldots, \omega_n$ is an integral basis of O_K, we can write $O_K = \omega_1\mathbf{Z} + \omega_2\mathbf{Z} + \ldots + \omega_n\mathbf{Z}$. It simply means that the integral basis is a $\mathbf{Z}$-basis and that O_K is a module of maximal rank n. Let x be a non-zero element of I. The following relation $xO_K \subset I \subset O_K$ shows that I is included in a module of rank n and that I contains a module of rank n. Hence, I itself has the maximal rank n. It can be expressed as $I = \gamma_1\mathbf{Z} + \gamma_2\mathbf{Z} + \ldots + \gamma_n\mathbf{Z}$, where γ_i are elements of O_K. The proposition below follows :

Result 10 *Any non-zero ideal I of O_K can be written as $I = \gamma_1\mathbf{Z} + \gamma_2\mathbf{Z} + \ldots + \gamma_n\mathbf{Z}$. The set $\{\gamma_i, i = 1 \ldots n\}$ is called a $\mathbf{Z}$-basis of I.*

After applying the canonical embedding σ to the ideal I included in the ring O_K, we obtain the lattice $\Lambda_I = \sigma(I)$ of rank n included in $\Lambda = \sigma(O_K)$. As a consequence of the two above results, the generator matrix G_I of Λ_I is given by

$$G_I = \begin{pmatrix} \sigma_1(\gamma_1) & \ldots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \ldots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\gamma_n) & \ldots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{pmatrix} \quad (4.17)$$

Logically, we ask for the relation between the two matrices G and G_I. This can be found by comparing O_K and I as $\mathbf{Z}$-modules. Let T be the $n \times n$ matrix associated with the

transition from the first basis to the second basis, i.e.

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = T \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix}$$

Indeed, the γ_i's are algebraic integers and can be written as linear combinations of the ω_i's. $\gamma_i = \sum_{k=1}^{n} t_{ik}\omega_k$ where $t_{ik} \in \mathbf{Z}$. We deduce that $T = [t_{ij}]$ is an integer matrix. T is also known as the **integral matrix representation** of I. Furthermore, we can announce the following result :

Result 11 – *The generator matrix G_I of the lattice Λ_I can be obtained from the generator matrix G of the lattice Λ by applying the transition T between the $\mathbf{Z}$-bases of I and O_K, briefly $G_I = TG$.*

This is derived directly from the formula $\gamma_i = \sum_{k=1}^{n} t_{ik}\omega_k$, which is also valid after taking the real part and the imaginary part of both sides, $\sigma_j(\gamma_i) = \sum_{k=1}^{n} \sigma_j(t_{ik}\omega_k) = \sum_{k=1}^{n} t_{ik}\sigma_j(\omega_k)$. The equality $G_I = TG$ allows us to write $\det G_I = \det T \times \det G$ which means that $vol(\Lambda_I) = |\det T| \times vol(\Lambda)$. The last equation can be used to compute the fundamental volume of Λ_I.

Result 12

$$vol(\Lambda_I) = N(I) \times 2^{-r_2} \times \sqrt{|d_K|} \tag{4.18}$$

Proof. By definition $N(I)$ is equal to the cardinality of O_K/I. But O_K/I is isomorphic to the quotient Λ/Λ_I due to the canonical embedding σ. Thus, they have the same cardinality (or same index as quotient groups). So we have $N(I) = |\Lambda/\Lambda_I|$. But the group partitioning [45], $\Lambda = \Lambda_I + [\Lambda/\Lambda_I]$, shows that a fundamental region of the sub-lattice Λ_I can be constructed as the disjoint union of $|\Lambda/\Lambda_I|$ copies of a fundamental region of Λ, i.e. $vol(\Lambda_I) = |\Lambda/\Lambda_I| \times vol(\Lambda) = N(I) \times vol(\Lambda)$. Finally, equation (4.18) is obtained by combining $vol(\Lambda_I) = N(I) \times vol(\Lambda)$ and equation (4.13). Q.E.D.

Now we can relate T and $N(I)$ with $N(I) = |\det T|$, since $vol(\Lambda_I) = N(I)vol(\Lambda) = |\det T|vol(\Lambda)$. This is very useful especially when I is a principal ideal. In this case, the transition matrix is function of α and will be denoted $T = R(\alpha)$.

Result 13 *Let $I = \alpha O_K$ be a principal ideal. The norm of I is equal to the absolute value of the algebraic norm of its generating element, $N(I) = |N(\alpha)|$.*

Proof. The $\mathbf{Z}$-basis of the principal ideal $I = \alpha O_K$ is the set $\{\alpha\omega_i, i = 1 \ldots n\}$. The transition equation becomes

$$\alpha \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = R(\alpha) \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} \tag{4.19}$$

Recall that $T = R(\alpha)$ and $N(I) = |\det T|$. If we take all the conjugates of the above identity,

$$\sigma_k(\alpha)(\sigma_k(\omega_1), \sigma_k(\omega_2), \ldots \sigma_k(\omega_n))' = R(\alpha)(\sigma_k(\omega_1), \sigma_k(\omega_2), \ldots \sigma_k(\omega_n))'$$

for $k = 1, 2, \ldots n$, where the prime indicates the transposition of the vector. We can write in a concise form

$$\Omega \, \mathrm{diag}(\sigma_1(\alpha), \sigma_2(\alpha), \ldots \sigma_n(\alpha)) = R(\alpha)\Omega$$

where $\Omega = [\sigma_j(\omega_i)]$ for $i, j = 1, \ldots n$. Taking the determinant we obtain $\det R(\alpha) = N(\alpha)$ and finally $N(I) = |det R(\alpha)| = |N(\alpha)|$. Q.E.D.

Example 5 - Let $K = \mathbf{Q}(\sqrt{5})$ and let θ be a primitive element with minimal polynomial $x^2 - x - 1$. Given $\alpha = \theta - 3 \in O_K$, we want to compute the integer transition matrix $T = R(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Using (4.19) with $\omega_i = \theta^{i-1}$ and the identity $\theta^2 = \theta + 1$, derived from the minimal polynomial, we obtain

$$\begin{pmatrix} \theta - 3 \\ -2\theta + 1 \end{pmatrix} = \begin{pmatrix} a + b\theta \\ c + d\theta \end{pmatrix}$$

which gives $R(\alpha) = \begin{pmatrix} -3 & 1 \\ 1 & -2 \end{pmatrix}$. We now have $N(\theta - 3) = N(\frac{-5+\sqrt{5}}{2}) = 5$ which is equal to $\det R(\theta - 3)$. The generator matrix G_I of Λ_I, where $I = \alpha O_K$, is computed by

$$G_I = TG = R(\theta - 3)G = \begin{pmatrix} \frac{-5+\sqrt{5}}{2} & \frac{-5-\sqrt{5}}{2} \\ -\sqrt{5} & \sqrt{5} \end{pmatrix}$$

and equation (4.18) can be easily verified.

We have seen the **Z**-basis representation of an ideal I. This representation was very practical to get properties for the associated lattice $\Lambda_I = \sigma(I)$. Equation (4.18) is very important and will guide us in the construction of Λ_I. We note also that the norm of the product of two ideals in O_K is equal to the product of the norms, $N(IJ) = N(I)N(J)$. This result is closely related to equation (4.18). Sometimes when searching for an ideal of a given norm $N(I)$ to build Λ_I, we start from an ideal H such that $N(H) = cN(I)$ where c is an integer constant. Clearly, we are tempted to search for an ideal $H = IJ$, $c = N(J)$. Hence, we face the problem of factoring an ideal in the ring of integers. The factorization method for principal ideals is given in Result 16. Unfortunately, the factorization is a little bit difficult if we use the **Z**-basis representation of the ideal. The following result shows a new representation of an ideal based on two elements of O_K.

Result 14 *Let I be an ideal of O_K. For any non-zero element $\alpha \in I$ there exists an element $\beta \in I$ such that $I = \alpha O_K + \beta O_K$. α and β are called O_K-**generators** of I. The ideal is denoted $I = (\alpha, \beta)$.*

The above result says that any ideal I in O_K can be expressed as the sum of two principal ideals. What about the $\mathbf{Z}$-basis of $I = \alpha O_K + \beta O_K$? This can be found if we notice that $I = \alpha\omega_1\mathbf{Z} + \ldots + \alpha\omega_n\mathbf{Z} + \beta\omega_1\mathbf{Z} + \ldots + \beta\omega_n\mathbf{Z}$. We obtain $2n$ $\mathbf{Z}$-generators of I. But the transition matrix T is defined only by n $\mathbf{Z}$-generators. So the difficulty is to determine a $\mathbf{Z}$-basis with n elements given a $\mathbf{Z}$-basis with $2n$ elements. This can be done by searching for the $n \times n$ integer matrix T whose rows span the same subgroup of $\mathbf{Z}^n$ generated by the rows of $R(\alpha)$ and $R(\beta)$.

Result 15 *Every ideal I of O_K can be written in a unique way as*

$$I = \prod_J J^{e_J}$$

the product being over a finite set of prime ideals J. The exponents e_J are positive integers.

Result 16 *Let $K = \mathbf{Q}(\theta)$ be a number field, where θ is an algebraic integer, whose minimal polynomial is denoted $\mu(x)$. Let $f = [O_K : \mathbf{Z}[\theta]]$. Then for any prime p not dividing f one can obtain the factorization of the principal ideal $I = pO_K$ as follows. Let*

$$\mu(x) = \prod_{i=1}^{g} \mu_i(x)^{e_i} \pmod p$$

be the decomposition of $\mu(x)$ into irreducible monic factors $\mu_i(x)$ in the ring of polynomials over $GF(p)$, the Galois field of order p. Then

$$I = pO_K = \prod_{i=1}^{g} J_i^{e_i}$$

where $J_i = pO_K + \mu_i(\theta)O_K$.
Furthermore, the index $f_i = [O_K/J_i : GF(p)]$ is equal to the degree of $\mu_i(x)$. We have $deg(K) = n = \sum_{i=1}^{g} e_i f_i$ and the norm of the prime ideal J_i is given by $N(J_i) = p^{f_i}$.

Let us check the norm of $I = pO_K$ in the factorization theorem. All the conjugates $\sigma_i(p)$ of p are equal to p because p is an integer. The algebraic norm of p is $N(p) = \prod_i \sigma_i(p) = p^n = N(I)$. From the decomposition formula we see that $N(I) = \prod_{i=1}^{g} N(J_i^{e_i}) = \prod_{i=1}^{g} p^{e_i f_i} = p^n$. It is clear that the factorization of an ideal requires the factorization of a polynomial in a finite field (modulo p). The above algorithm will be used in the next sub-section to decompose prime ideals while building the lattices of Table 4.4. Note that the ideals in Table 4.4 are defined by two O_K-generators. The last two ideals (for Λ_{16} and Λ_{24}) are given as the product of two and three prime ideals respectively.

4.6.2 Lattices from cyclotomic fields ideals

In this section we assume that K is the cyclotomic field $K = \mathbf{Q}(\theta)$ where $\theta = e^{2i\pi/N}$ denotes a primitive N-th root of unity. Some well known properties of cyclotomic fields are

1. The degree of K is $n = \phi(N)$, where ϕ is the Euler function.
2. The conjugates of θ are the θ^i with $\gcd(i, n) = 1$.
3. The ring of integers is $O_K = \mathbf{Z}[\theta]$ (the index f is 1).
4. The minimal polynomial of θ is

$$p(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

   of degree $n = \phi(N)$. $\mu(i)$ is the Möbius function of the integer i.

5. The absolute discriminant of K is

$$d_K = (-1)^{n/2} N^n / \prod_{p|N} p^{n/(p-1)}$$

Equation (4.18) is used to compute $N(I)$ given the lattice fundamental volume. $vol(\Lambda)$ is replaced by ρ^n/δ, where ρ is the packing radius and δ is the lattice center density [26]. The search for the rotated lattices of Table 4.4 having dimension n and diversity $n/2$ goes through the following steps:

1. Calculate the minimal polynomial of $e^{i2\pi/N}$ which has degree $\phi(N)$.
2. Find all ideals I of O_K with integer norm

$$N(I) = \frac{2^{n/2}}{\sqrt{|d_K|}} \times \frac{\rho^n}{\delta}$$

3. Using the transition matrix T of I compute the generator matrix $G_I = TG$ and evaluate the lattice parameters such as the center density and the kissing number. If they are equal to the parameters of $D_4, E_6, E_8, \Lambda_{12}, \Lambda_{16}$ or Λ_{24}, then we have obtained a rotated version of these lattices. In fact, these lattices are unique with such parameters.

This procedure was applied successfully to obtain a generator matrix for each one of the lattices in Table 4.4. The key operation is the factorization of prime ideals presented in Result 16.

We show as an example the new constructions of $D_{4,2}, K_{12,6}$ and $\Lambda_{16,8}$.

$D_{4,2}$ - We first note that $\phi(8) = 4$ and that the other values of N giving $\phi(N) = 4$ do not result in the rotated version of D_4, whose center density is $1/8$. The minimal polynomial

of $\theta = e^{i2\pi/8}$ is given in Table 4.4 and the absolute discriminant of the field $K = \mathbf{Q}(\theta)$ is $d_K = 2^8$. The signature of K is $(0, 2)$. Using (4.18) we can write

$$N(I) = \frac{2^{4/2}}{\sqrt{2^8}} \cdot \frac{\rho^4}{1/8} = 2^3 \cdot \rho^4$$

and for $N(I) = 2$ we may take $\rho = 1/\sqrt{2}$. The ideals I with norm 2 can be obtained from the factorization of the prime ideal (2), which has norm 2^4

$$(2) = (2, \theta + 1)^4 = I^4 \ .$$

Now I has the desired norm 2. The generator matrix of our lattice is then $G_I = TG$, where T is the integral matrix representation of I

$$\mathrm{T} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

and G is the generator matrix of $\sigma(O_K)$. The lattice generated by G_I has center density $0.125 = 1/8$ and kissing number 24 exactly like D_4. Since D_4 is the unique lattice with these parameters, we have constructed a rotated version of it with diversity equal to 2.

$K_{12,6}$ - We first note that $\phi(21) = 12$ and that the other values of N giving $\phi(N) = 21$ do not result in the rotated version of K_{12}, whose center density is $1/27$. The minimal polynomial of $\theta = e^{i2\pi/12}$ is given in Table 4.4 and the absolute discriminant of the field $K = \mathbf{Q}(\theta)$ is $d_K = 3^6 \cdot 7^{10}$. The signature of K is $(0, 6)$. Using (4.18) we can write

$$N(I) = \frac{2^{12/2}}{\sqrt{3^6 \cdot 7^{10}}} \times \frac{\rho^{12}}{1/27} = \frac{2^6 \cdot \rho^{12}}{7^5}$$

and for $N(I) = 7$ we may take $\rho = \sqrt{7}/\sqrt{2}$. The ideals I with such a norm can be obtained from the factorization of the ideal (7), having norm 7^{12}.

$$(7) = (7, \theta + 3)^6 (7, \theta - 2)^6 = I_1^6 I_2^6$$

In fact $N(I_1) = N(I_2) = 7$ so we may select $I = I_1$, which has the desired norm. The generator matrix of our lattice is then $G_I = TG$, where T is the integral matrix representation of I

$$\mathrm{T} = \begin{pmatrix} 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and G is the generator matrix of $\sigma(O_K)$. The lattice generated by G_I has center density $1/27$ and kissing number 756 exactly like K_{12}. Since K_{12} is the unique lattice with these parameters, we have constructed a rotated version of it with diversity equal to 6.

$\Lambda_{16,8}$ – We first note that $\phi(40) = 16$ and that the other values of N giving $\phi(N) = 16$ did not result in the rotated version of Λ_{16}, whose center density is $1/16$. The minimal polynomial of $\theta = e^{i2\pi/40}$ is given in Table 4.4 and the absolute discriminant of the field $K = \mathbf{Q}(\theta)$ is $d_K = 2^{32} \cdot 5^{12}$. The signature of K is $(0, 8)$. Using (4.18) we can write

$$N(I) = \frac{2^{16/2}}{\sqrt{2^{32} \cdot 5^{12}}} \times \frac{\rho^{16}}{1/16} = \frac{\rho^{16}}{5^6 \cdot 2^4}$$

and for $N(I) = 2^4 \cdot 5^2$ we may take $\rho = \sqrt{2 \cdot 5}$. So we need to find the ideals I with such a norm. These can be obtained from the factorization of the ideals (2) and (5), having norms 2^{16} and 5^{16} respectively.

$$\begin{aligned} (2) &= (2, \theta^4 + \theta^3 + \theta^2 + \theta + 1)^4 = I_1^4 \\ (5) &= (5, \theta^2 + 2)^4 (5, \theta^2 - 2)^4 = I_2^4 I_3^4 \end{aligned}$$

In fact $N(I_1) = 2^4, N(I_2) = 5^2, N(I_3) = 5^2$ so we may select $I = I_1 I_2$ which has the desired norm $N(I) = N(I_1 I_2) = N(I_1)N(I_2) = 2^4 \cdot 5^2$. The generator matrix of our lattice is then $G_I = TG$, where T is the integral matrix representation of I and G is the generator matrix of $\sigma(O_K)$. The lattice generated by G_I has center density 0.0625 and kissing number 4320 exactly like Λ_{16}. Since Λ_{16} is the unique lattice with these parameters, what we have constructed is simply a rotated version of it with diversity equal to 8.

4.7 Decoding and practical results

4.7.1 Decoding algorithm

The lattices codes found in sections 4.5 and 4.6, when used over the Gaussian channel can be decoded using the algorithm shown in [87, 39]. This algorithm searches efficiently for all the lattice points inside a sphere of given radius $\sqrt{C}$ centered at the received vector and then outputs the closest one. It can be summarized as follow :

- Input : A received point r in the n-dimensional real space $\mathbf{R}^n$.
- Output : The lattice point x that minimizes $\sum_{i=1}^{n} |r_i - x_i|^2$.

1. Select a real positive constant C (the squared radius).
2. Enumerate all points in the n-dimensional sphere of radius $\sqrt{C}$ centered at r.
3. Choose the closest point to r.

We show how to adapt this lattice decoding algorithm to the Rayleigh fading channel case. For maximum-likelihood decoding with perfect side information, the problem is to minimize the metric $m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha})$ given in equation (4.2). Let G be the generator matrix of the lattice Λ and let us consider the lattice Λ_c with generator matrix

$$G_c = G\mathrm{diag}(\alpha_1, \ldots \alpha_n)$$

We can imagine this new lattice Λ_c in a space where each component has been compressed or enlarged by a factor α_i. A point of Λ_c can be written as $\mathbf{u} = (u_1, \ldots u_n) = (\alpha_1 x_1, \ldots \alpha_n x_n)$. The metric to minimize is then

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - u_i|^2$$

this means that we can simply apply the lattice decoding algorithm to the lattice Λ_c when the received point is $\mathbf{r}$. The decoded point $\hat{\mathbf{u}} \in \Lambda_c$ has the same integer components (in $\mathbf{Z}^n$) as $\hat{\mathbf{x}} \in \Lambda$. The additional complexity required by this algorithm comes from the fact that for each received point we have a different compressed lattice Λ_c. So we need to compute a new Cholesky factorization of the Gram matrix for each Λ_c [25, 66]. We also need $G_c^{-1} = \mathrm{diag}(1/\alpha_1, \ldots 1/\alpha_n)G^{-1}$ to find the components of the received vector but this only requires a vector-matrix multiplication since G^{-1} can be precomputed.

As discussed in [87], this decoding algorithm is maximum likelihood only for an infinite lattice. When dealing with a finite constellation, with a given spectral efficiency, some care should be taken. In fact, the decoder may output a lattice point which is not part of the signal set. The constellations we have simulated are constituted by the points of the first shells of the lattice in order to obtain the minimal average energy per point. Since the decoding complexity increases with the search radius of the sphere, this is adaptively selected according to the fading coefficients so that we can always find at least a point of Λ_c inside the sphere. To optimize the decoder whenever the received point lays outside the outermost shell of the constellation we take its projection on this shell.

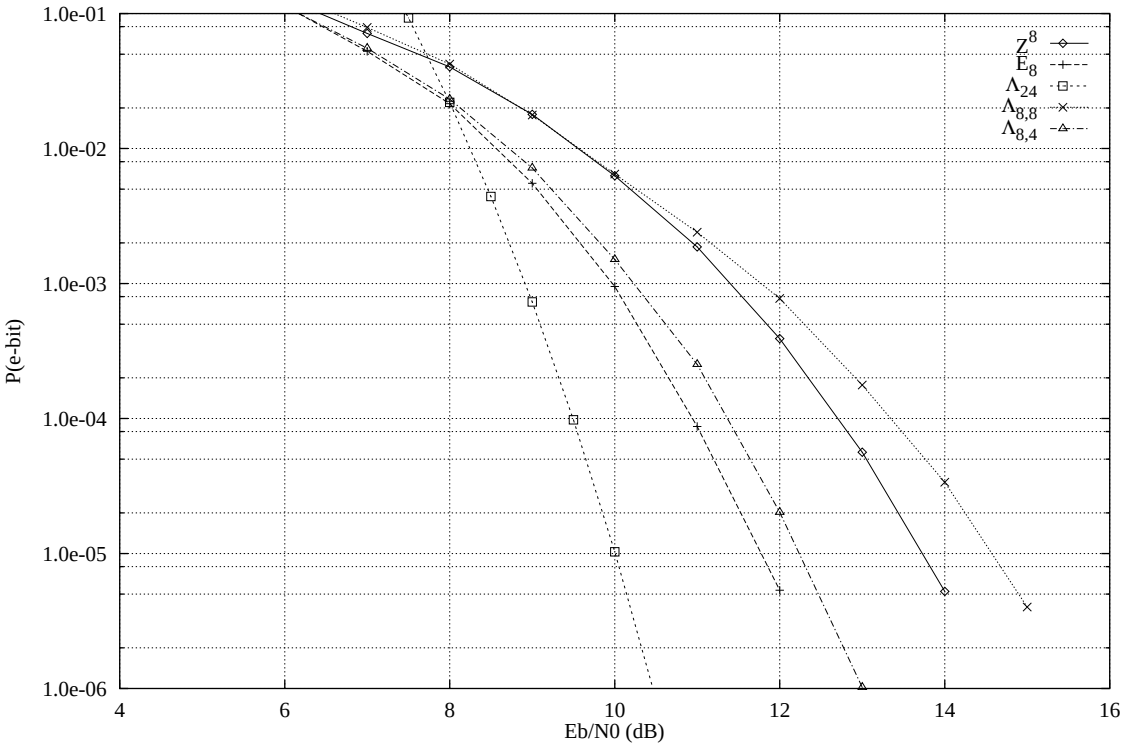


Figure 4.2: Lattice constellations over the Gaussian channel ($\eta = 4$)

4.7.2 Results

We present some simulation results to illustrate and support some of the statements made throughout the chapter. Due to the complexity of the decoding algorithm we have made simulations up to dimension eight while for higher dimensions we have plotted the upper bounds derived in the appendices. All built constellations have a spherical shape. All curves give the bit error probability as a function of E_b/N_0 for $\eta = 4$ bits/symbol. For convenience we will identify the lattice and the lattice constellation carved from it, with the same symbol.

Figure 4.2 shows the performance of different lattice constellations over the Gaussian channel. Taking $\mathbf{Z}^8$ as a reference we can make the following observations.

- E_8 only gains 2dB at 10^{-5} although its asymptotic coding gain is 3dB [26]. This draws the attention to the limitations of the asymptotic coding gain when used as parameter for practical values of the error probability.

- $\Lambda_{8,8}$, from the totally real field with minimal discriminant, loses (curve on the right of $\mathbf{Z}^8$) 0.9dB at 10^{-5} and asymptotically 1.5dB (Table 4.3), showing the weakness of these lattices over the Gaussian channel.

- $\Lambda_{8,4}$, from the totally complex field with minimal discriminant, gains 1.4dB at 10^{-5} and is only 0.6dB at 10^{-5} from E_8, the asymptotically 8-dimensional optimal lattice code for the Gaussian channel.

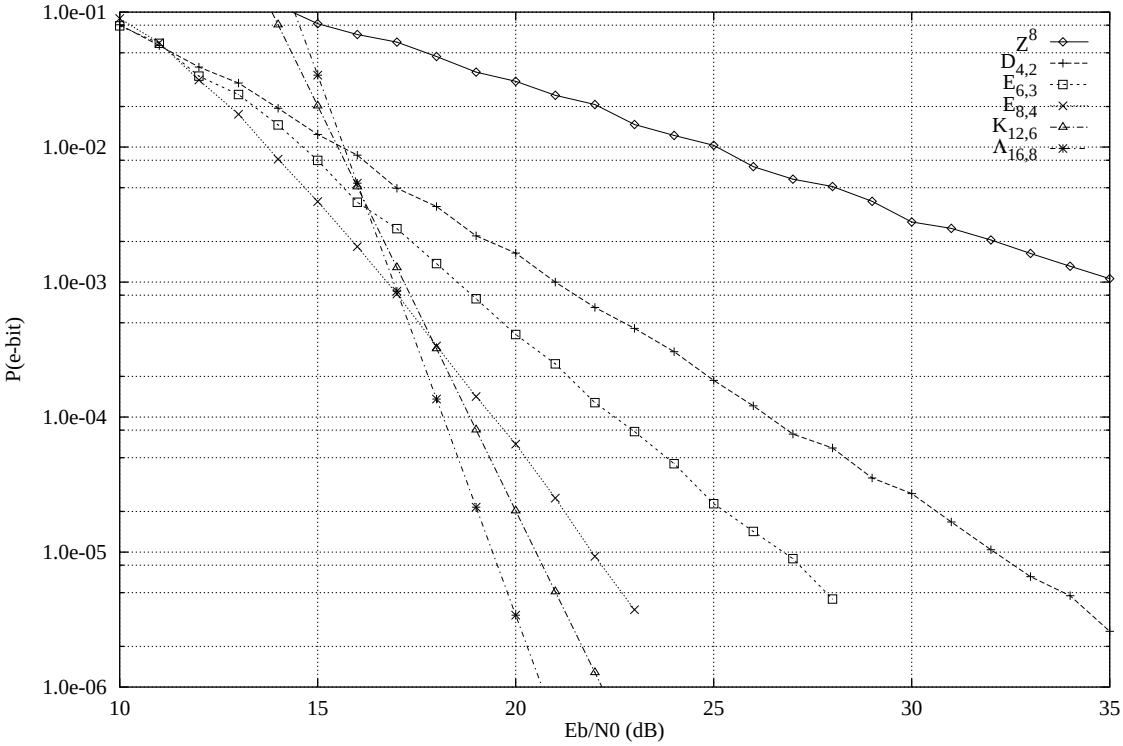


Figure 4.3: Rotated famous lattice constellations over the Rayleigh fading channel ($\eta = 4$)

For comparison, Λ_{24} (at the most left) gains 3.7dB over $\mathbf{Z}^8$ at 10^{-5}. This curve is computed with equation (4.5) after adding 1.10dB of shape gain.

Figure 4.3 shows the performance over the Rayleigh fading channel of the rotated versions of the lattices $D_4, E_6, E_8, K_{12}, \Lambda_{16}$, the last two are upper bounds. As discussed in section 4.3, the slopes of the curves asymptotically correspond to the diversity. For these lattices we can see that this is already true for low bit error probabilities.

- At 10^{-3} the gain over $\mathbf{Z}^8$ is about 17dB and it exceeds 25dB at 10^{-5}.
- $E_{8,4}$ outperforms $D_{4,2}$ with 10dB at 10^{-5}.
- $K_{12,6}$ and $\Lambda_{16,8}$ curves (upperbounds) have been computed using (4.10) after neglecting high diversity terms ($l \geq L + 1$).

Figure 4.4 shows the performance over the Rayleigh fading channel of the lattice constellations from totally real algebraic number fields. These lattices give a good performance over the fading channel but have negative asymptotic gains over the Gaussian channel. The gain of $\Lambda_{8,8}$ (compared to $\mathbf{Z}^8$) on the Rayleigh channel is 19dB at 10^{-3} and >25 at 10^{-5}. Although the theoretical diversities are comparatively higher the actual slopes of the curves do not reach the asymptotic value in the range of interest. For example, $\Lambda_{8,8}$ curve at the most left shows a diversity of 4 instead of 8. An explanation of this fact comes from the high value of the product kissing number for these constellations.

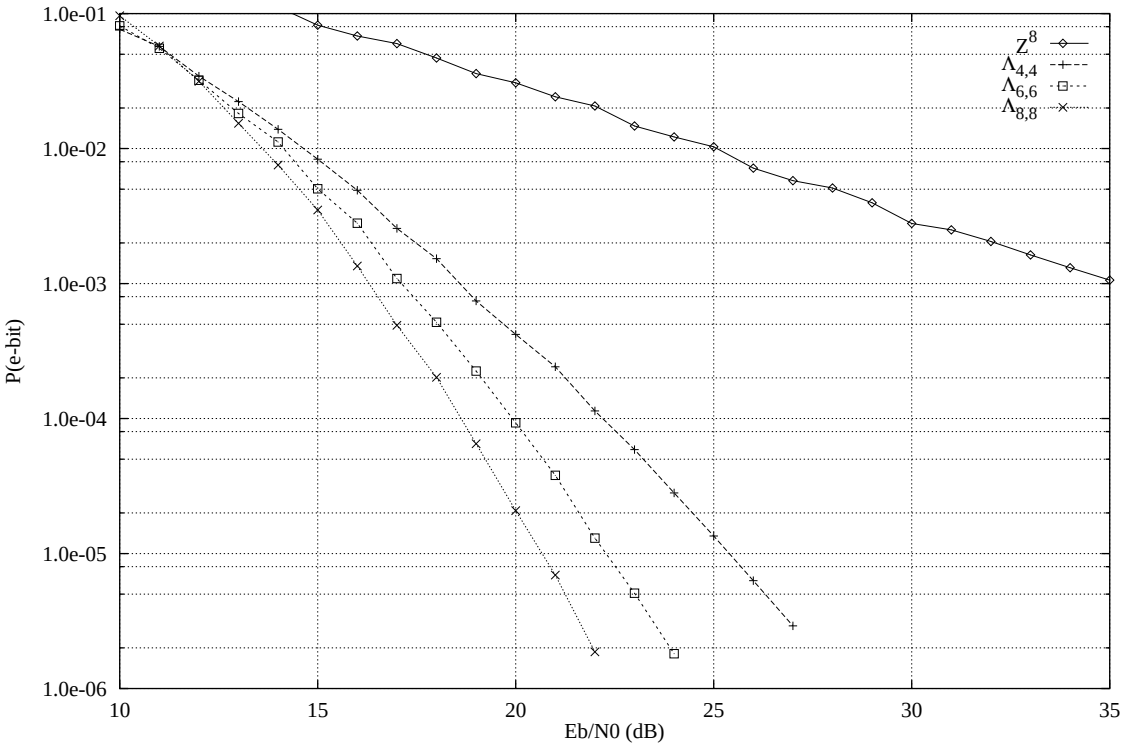


Figure 4.4: Lattice constellations from totally real algebraic number fields of minimal discriminant over the Rayleigh fading channel ($\eta = 4$)

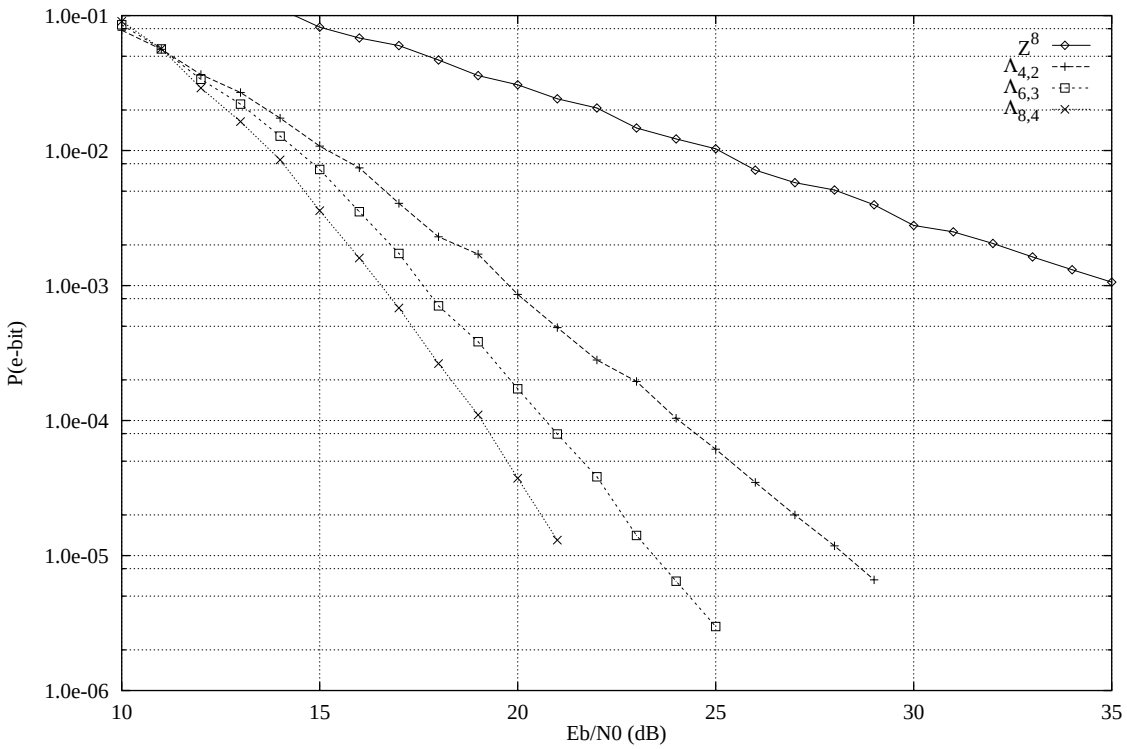


Figure 4.5: Lattice constellations from totally complex algebraic number fields of minimal discriminant over the Rayleigh fading channel ($\eta = 4$)

Figure 4.5 shows the performance over the Rayleigh fading channel of the lattice constellations from totally complex algebraic number fields. The curves achieve quite rapidly the slope corresponding to the diversity and their performance over the fading channel is very close to the one of the corresponding lattices in Figure 4.4.

4.8 Conclusions

Two different approaches (Sections 4.4,4.5 versus Section 4.6) have been used to study two families of lattices in order to achieve good performance over both Gaussian and Rayleigh channels, with high spectral efficiency.

The first family is generated by canonical embedding over the ring of integers of a number field. Among the lattices of this family, we especially gave importance to the classes of totally complex and totally real fields lattices. We found that totally real fields lattices (Λ_{real}) exhibit very good performance on Rayleigh channels with a maximal diversity of n. But they have a negative gain on Gaussian channels caused by their weak packing density. The totally complex fields lattices (Λ_{cplx}) are a compromise between diversity and packing density. They showed a positive gain on Gaussian channels and good performance on Rayleigh channels with a diversity of $n/2$.

The second family of lattices is generated by canonical embedding over special ideals in totally complex cyclotomic fields. This family includes versions of the famous lattice packings D_4, E_6, E_8, K_{12}, Λ_{16} and Λ_{24}. These lattices act in a similar way as the $n/2$ diversity Λ_{cplx} lattices over the Rayleigh channel and thus can achieve a diversity from 2 through 12. Furthermore, these are the best lattices for the Gaussian channel.

The first important point in this conclusion, is the fact that number fields with relatively small (or minimal) absolute discriminants are known only for degrees less or equal to 8. So the diversity of Λ_{real} cannot exceed 8, unless mathematicians find optimal fields with higher degree. On the contrary, the lattices of the second family are less limited in diversity; $\Lambda_{24,12}$ achieves a diversity of 12. Of course we can think about building $\Lambda_{32,16}$ and $\Lambda_{64,32}$ to attain 16 and 32 respective diversities. But we are limited by the ratio of the system's complexity over the practical gain. We cannot forget also that the study of the first family makes it possible for us to construct and understand the second family.

A second non negligible point to be mentioned concerns the practical aspects of lattice encoding/decoding. There exist no efficient algorithms for encoding and decoding the lattices presented in this chapter, especially those of the first family. The universal decoding algorithm presented in the last section has a high complexity in terms of number of arithmetical operations. In fact, we are very pessimistic about finding a fast and a cheap decoding algorithm for the lattices of the first family. It is mainly too difficult to find a simple lattice (such as $\mathbf{Z}^n$) containing these lattices and to make a group partitioning from which a simple encoding/decoding algorithm can be derived. On the contrary, we are very optimistic when it comes to elaborate efficient encoding/decoding algorithms for the $n/2$ diversity lattices of the second family viewed as rotated binary lattices.

4.9 Dedication

This chapter is dedicated to the memory of Catherine Rastello who left us on April 1995.

4.10 Upper bound on the AWGN channel

In this appendix we modify inequality (4.4) to express it as a function of E_b/N_0. We assume that the constellation S has a cubic shape centered at the origin and has volume $(2A)^n$. The components x_i of any point $\mathbf{x}$ in S satisfy the inequality $|x_i| \leq A$. The total number of points in S can be approximated by

$$M \approx \frac{(2A)^n}{vol(\Lambda)}$$

for sufficiently large M. We want to compute the average energy per point $E = E[\|\mathbf{x}\|^2]$ without specifying the particular lattice. Using a continuous approximation for the constellation points, we compute the second order moment of the hyper-cube containing the constellation

$$E \approx \int_{[-A,A]^n} \|\mathbf{x}\|^2 \frac{d\mathbf{x}}{(2A)^n} = \int_{-A}^{A} \cdots \int_{-A}^{A} (x_1^2 + \cdots + x_n^2) \frac{dx_1 \cdots dx_n}{(2A)^n}$$

The above integral is easily computed and gives $E = nA^2/3$.

Since,

$$A^2 = \frac{M^{2/n} vol(\Lambda)^{2/n}}{4} = \frac{2^s vol(\Lambda)^{2/n}}{4}$$

the average energy per bit is

$$E_b = \frac{E}{n \times \eta} = \frac{A^2}{3\eta} = \frac{2^\eta vol(\Lambda)^{2/n}}{12\eta}$$

and

$$\frac{d_{Emin}/2}{\sqrt{2N_0}} = \sqrt{\frac{d_{Emin}^2}{8N_0}} = \sqrt{\frac{3\eta}{2^{\eta+1}} \frac{E_b}{N_0} \frac{d_{Emin}^2}{vol(\Lambda)^{2/n}}} \ .$$

This yields the upper bound (4.5) to the error probability for the AWGN channel.

4.11 Upper bound on the Rayleigh channel

We here derive an upper bound for the pairwise point error probability $P(\mathbf{x} \rightarrow \mathbf{y})$ on the Rayleigh fading channel. The channel power gain is assumed normalized, $E[\alpha_i^2] = 1$. As described in section 2, the components r_i of the received vector are given by $r_i = \alpha_i x_i + n_i$. The received point $\mathbf{r}$ is closer to $\mathbf{y}$ than to $\mathbf{x}$, if $m(\mathbf{y}|\mathbf{r}, \boldsymbol{\alpha}) \leq m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha})$. The conditional pairwise error probability is given by

$$\begin{aligned} P(\mathbf{x} \rightarrow \mathbf{y}|\boldsymbol{\alpha}) &= P(\sum_{i=1}^{n} |r_i - \alpha_i y_i|^2 \leq \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \mid \mathbf{x} \text{ transmitted}) \\ &= P(\sum_{i=1}^{n} |\alpha_i(x_i - y_i) + n_i|^2 \leq \sum_{i=1}^{n} |n_i|^2) \\ &= P(\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2 + 2\sum_{i=1}^{n} \alpha_i (x_i - y_i) n_i \leq 0) \ . \end{aligned}$$

Now, let $\chi = \sum_{i=1}^{n} \alpha_i (x_i - y_i) n_i$. χ is a linear combination of Gaussian random variables (the n_i's). Consequently, χ is Gaussian with zero mean and variance

$$\sigma_\chi^2 = N_0 \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2 \ .$$

Let $A = \frac{1}{2}\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2$ be a constant. We can write the conditional pairwise error probability in terms of χ and A,

$$P(\mathbf{x} \rightarrow \mathbf{y}|\boldsymbol{\alpha}) = P(\chi \geq A) = Q(A/\sigma_\chi)$$

where $Q(x) = (2\pi)^{-1} \int_x^\infty \exp(-t^2/2) dt$ is the Gaussian tail function. The Gaussian tail function can be upper bounded [11] by an exponential $Q(x) \leq \frac{1}{2}\exp(-x^2/2)$. This bound is very tight already for $x \geq 3$. The conditional pairwise error probability becomes

$$P(\mathbf{x} \rightarrow \mathbf{y}|\boldsymbol{\alpha}) \leq \frac{1}{2}\exp(-\frac{A^2}{2\sigma_\chi^2}) = \frac{1}{2}\exp(-\frac{1}{8N_0}\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2) \ .$$

The pairwise error probability $P(\mathbf{x} \rightarrow \mathbf{y})$ is computed by averaging $P(\mathbf{x} \rightarrow \mathbf{y}|\boldsymbol{\alpha})$ over the fading coefficients $\boldsymbol{\alpha}$

$$P(\mathbf{x} \rightarrow \mathbf{y}) = \int P(\mathbf{x} \rightarrow \mathbf{y}|\boldsymbol{\alpha}) \mathbf{p}(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \leq \frac{1}{2}\int \exp(-\frac{1}{8N_0}\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2) \mathbf{p}(\boldsymbol{\alpha}) d\boldsymbol{\alpha}$$

The differential probability is $\mathbf{p}(\boldsymbol{\alpha})d\boldsymbol{\alpha} = p(\alpha_1) \cdots p(\alpha_n) d\alpha_1 \cdots d\alpha_n$, where $p(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$ is the normalized Rayleigh distribution. Replacing in the last inequality we obtain

$$P(\mathbf{x} \rightarrow \mathbf{y}) \leq \frac{1}{2}\prod_{i=1}^{n} I_i$$

where

$$I_i = \int_0^\infty \exp(-\frac{1}{8N_0}\alpha_i^2(x_i - y_i)^2)p(\alpha_i)d\alpha_i = \int_0^\infty 2\alpha_i \exp(-B_i\alpha_i^2)d\alpha_i$$

and $B_i = 1 + (x_i - y_i)^2/(8N_0)$. By simple calculations we obtain $I_i = 1/B_i$ and

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2}\prod_{i=1}^{n}\frac{1}{B_i}$$

which is equation (4.7) in section 4.3. This upper bound is sufficient to derive the optimization criteria for lattices on fading channels. It differs from the classical Chernoff bound by a factor $1/2$ and can be tightened by the use of Gaussian quadratic forms [73] which lead to a coefficient equal to $\begin{pmatrix} 2L-1 \\ L \end{pmatrix}/4^L$ instead of $1/2$.

Chapter 5

Rotations et MAQ multidimensionnelles

The increasing need of high data rate transmissions over time or frequency selective fading channels has drawn the attention to modulation schemes with high spectral efficiency such as QAM. With the aim of increasing the 'diversity order' of the signal set we propose the new multidimensional rotated QAM constellations. Very high diversity orders can be achieved and this results in an almost Gaussian performance over the fading channel. This new multidimensional modulation scheme is essentially uncoded and enables to trade diversity for system complexity, at no expense of power or bandwidth.

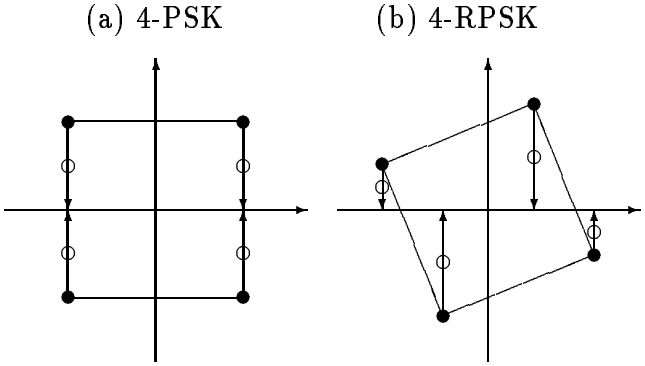


Figure 5.1: How to increase diversity: (a) $L = 1$, (b) $L = 2$.

5.1 Signal Space Diversity: a new power and bandwidth efficient diversity technique for the fading channel

The rapidly growing need of high data rate transmissions over fading channels has stimulated the interest for AM-PM modulation schemes with high spectral efficiency (or throughput). In the fading environment, problems like phase compensation and channel state information (CSI) estimation become harder to tackle when a non-constant envelope modulation scheme is used. Nevertheless, recent work shows that the use of pilot symbols enables to efficiently overcome the above problems even when using a QAM modulation scheme [70]. The pilot symbol technique was combined in different ways with efficient error control coding techniques to achieve conspicuous gains over fading channels [37, 77]. The effectiveness of these transmission schemes basically relies on the good error correcting capabilities of the code. The price to pay for this gain is either a bandwidth expansion or an additional transmission power to accommodate the redundant bits.

In this chapter we present a different approach. We consider uncoded multidimensional modulation schemes with an intrinsic *diversity order*, which achieve substantial coding gains over fading channels. The *diversity order* of a multidimensional signal set is the minimum number of distinct components between any two constellation points. In other words, the diversity order is the minimum Hamming distance between any two coordinate vectors of constellation points.

To distinguish from other well known types of diversity (time, frequency, space, code) we will talk about *modulation diversity* or *signal space diversity*. Throughout the chapter we will use, for simplicity, only the term *diversity* and it will be denoted with the symbol L.

As we will show in the following, the key point to increase the modulation diversity is to apply a certain rotation to a classical signal constellation in such a way that any two points achieve the maximum number of distinct components. Figure 5.1 illustrates this idea on a 4-PSK. In fact, if we suppose that a deep fade hits only one of the components

of the transmitted signal vector, then we can see that the 'compressed' constellation in (b) (empty circles) offers more protection against the effects of noise, since no two points collapse together as would happen with (a). A component interleaver/deinterleaver pair is required to assume that the in-phase and quadrature components of the received symbol are affected by independent fading. This simple operation already results in a gain of $8\,dB$ at 10^{-3} over the traditional 4-PSK (see Fig. 5.13). We will show in this chapter, that the increase in the dimensionality of the signal set produces significant gains in a fading channel, over the corresponding non-rotated signal set.

An interesting feature of the rotation operation is that the rotated signal set has exactly the same performance of the non rotated one when used over a pure AWGN channel. The rotated constellation when used over a Ricean fading channel will show a performance between the two extreme cases of Gaussian and Rayleigh fading channel.

We have used the term 'uncoded' since we are not adding any type of redundancy to the information bit stream. The information bits are grouped into blocks and directly mapped one-to-one onto the multidimensional constellation points. This means that the coding gain is obtained without spending additional power or bandwidth, but only increasing the complexity of the demodulation operation. In fact, demodulation must now be performed on blocks of consecutive symbols.

The scope of this chapter is to analyze in detail all the methods devised to construct high diversity multidimensional QAM constellations carved from a rotated cubic lattice Z^n.

Most of the best known lattices for the Gaussian channel have the property of being integral, i.e. subsets of the cubic lattice $\mathbf{Z}^n$, so this can be used to obtain convenient labelings. In the case of Rayleigh fading channel, no efficient labeling was found for the optimal lattices given in [92], thus limiting their practical use. The rotated multidimensional QAM constellations presented in this chapter can be easily labeled by Gray mapping.

The advantage of these constellations over the ones analyzed in [92] is the simplicity of the bit labeling (Gray mapping).

The chapter is structured as follows. Sections 5.2 and 5.3 introduce the system model and review some elementary concepts of algebraic number theory. In Section 5.4 it is proved theoretically that for large values of diversity the point error probability over a fading channel approaches the one over an AWGN channel. This property is verified through simulation and for values of modulation diversity larger than 12 the bit error rate curves are within 1-2dB from the corresponding Gaussian curve. Section 5.5 presents three different techniques we used to increase the diversity of multidimensional QAM-type signal constellations. Although the most important, diversity is not the only parameter which influences the system performance. It is also important to maximize the *minimum product distance* between any two points of the signal constellation. This problem is considered in Section 5.6. Finally we give our results and conclusions in Sections 5.7 and 5.8 respectively.

5.2 The multidimensional QAM system

We now describe the system model shown in Figure 5.2. An n-dimensional QAM constellation is obtained as the cartesian product of $n/2$ two-dimensional QAM signal sets. A block of m bits is mapped onto the constellation by applying the Gray mapping in each dimension. We obtain an overall Gray mapping which results in a one bit change when moving from one constellation point to any one of its nearest neighbors.

Each group of m/n bits uniquely identifies one of the n components of the multidimensional QAM constellation vector $\mathbf{u} = (u_1, \ldots u_n)$, where $u_i = \pm 1, \pm 3, \ldots$. We will call $\mathbf{u}$ the *integer component vector*. We denote by η the system throughput measured as the number of bits per symbol (two dimensions), so we have $m = \eta n/2$. In the case of odd dimension, one of the symbols should be split between two successive points. The total number of points in this cubic shaped constellations is 2^m and the average energy per bit is simply $E_b = (2^\eta - 1)/3\eta$.

We can view this constellation as carved from a translated and scaled (enlarged by a factor 2) version of the n-dimensional cubic lattice Z^n. In the following, for simplicity, we will consider only the constellations carved form Z^n, so that $u_i = 0, \pm 1, \pm 2, \ldots$. By simple scaling and translation it is possible to revert to the multidimensional QAM constellation.

The point $\mathbf{x}$ of the rotated constellation is obtained by applying the rotation matrix M to $\mathbf{u}$. The set of all points $\{\mathbf{x} = \mathbf{u}M, \mathbf{u} \in Z^n\}$ belongs to the n-dimensional cubic lattice $Z_{n,L}$ with generator matrix M and diversity L. The two lattices Z^n and $Z_{n,L}$ are equivalent in the sense of Section 5.5.1, but exhibit a different modulation diversity. In the following we will identify the lattice with the corresponding constellation.

The channel is modeled as an independent Rayleigh fading channel, separately operating on each component. Perfect phase recovery and CSI are assumed at the receiver. We also assume that the system is unaffected by inter-symbol interference.

To satisfy the assumption of independence we need to introduce a component interleaver which destroys the total correlation among the in-phase and quadrature channel fading coefficients. It should be evident that the component interleaving is the key point in obtaining any gain in the example of Figure 5.1. An undesirable effect of the component interleaver is the fact that it produces non constant envelope transmitted signals [53].

As a result of the above assumptions we will write the received vector as $\mathbf{r} = \boldsymbol{\alpha} \odot \mathbf{x} + \mathbf{n}$, where $\mathbf{n} = (n_1, n_2, \ldots n_n)$ is a noise vector, whose real components n_i are zero mean, N_0 variance Gaussian distributed independent random variables, $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ are the random fading coefficients with unit second moment and $\odot$ represents the component-wise product. Signal demodulation is assumed to be coherent, so that the fading coefficients can be modeled after phase elimination, as real random variables with a Rayleigh distribution. The independence of the fading samples represents the situation where the components of the transmitted points are perfectly interleaved.

After de-interleaving the components of the received points, the maximum likelihood

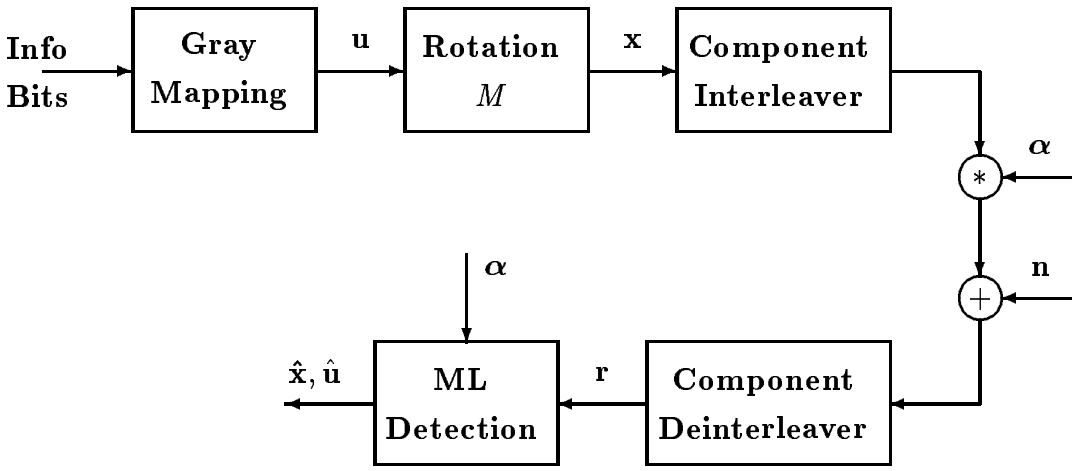


Figure 5.2: System model

(ML) detection criterium with perfect CSI imposes the minimization of the following metric

$$m(\mathbf{x}|\mathbf{r},\boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \tag{5.1}$$

Using this criterium we obtain the decoded point $\hat{\mathbf{x}}$ and the corresponding integer component vector $\hat{\mathbf{u}}$ from which the decoded bits can be extracted.

The minimization of (5.1) can be a very complex operation for an arbitrary signal set with a large number of points. It is shown in [95] how to apply the *Universal lattice decoder* [87] to obtain a more efficient ML detection of lattice constellations in fading channels.

In [92], using the Chernoff bounding technique, we have shown that the point error probability of a multidimensional signal set is essentially dominated by four factors. To improve the performance it is necessary to

1. Minimize the average energy per constellation point.
2. Maximize the diversity L.
3. Maximize the *minimum L-product distance*

$$d_{p,min}^{(L)} = \prod_{x_i \neq y_i}^{(L)} |x_i - y_i|$$

between any two points $\mathbf{x}$ and $\mathbf{y}$ in the constellation.

4. Minimize the *product kissing number* τ_p for the L-product distance i.e., the total number of points at the minimum L-product distance.

In this chapter we have fixed the average energy, since we have selected multidimensional QAM constellations, and we concentrate on the remaining items.

5.3 Algebraic number theory

The idea of rotating a two-dimensional QAM constellation was first presented in [17]. It was found that for a 16-QAM a rotation angle of $\pi/8$ gave a diversity of 2. The effect of this rotation is to spread the information contained in each component over both components of the constellation points. Persuing a similar approach, the optimization of a four-dimensional rotation is found in [53]. The approach to determine such rotations is direct and can not be easily extended to multidimensional constellations.

A more sophisticated mathematical tool is needed to construct lattice multidimensional constellations with high diversity: *algebraic number theory*. A simple introduction to this theory is given in [92] together with a review of the known lattice constellations obtained from the canonical embedding of real and complex algebraic number fields.

Here we will briefly highlight some of the mathematical concepts in algebraic number theory, nevertheless we recommend some further readings on this topic [71, 57, 50].

An algebraic number field $K = \mathbf{Q}(\theta)$ is the set of all possible algebraic combinations $(+, -, *, /)$ of an algebraic number θ (real or complex, irrational and non transcendental) with the rational numbers of $\mathbf{Q}$. This set has all the field properties and is related to an irreducible polynomial over $\mathbf{Q}$, called the *minimal polynomial*, having θ as a root.

From elementary calculus we know that $\mathbf{Q}$ is *dense* in $\mathbf{R}$, the set of real numbers. Then we could state that the set K is 'a little bit denser' in $\mathbf{R}$ if K is a real field, and 'a little bit denser' in $\mathbf{C}$ if K is a complex field.[1] Using a particular mapping, called the *canonical embedding*, it is possible to uniquely represent each element of an algebraic number field with a point in an n-dimensional Euclidean space $\mathbf{R}^n$ just like we represent the elements of $\mathbf{Q}$ on the real line $\mathbf{R}$. This set of points is now only 'dense' in $\mathbf{R}^n$ as $\mathbf{Q}$ was 'dense' in $\mathbf{R}$. In fact we chose n so as to satisfy this condition. n is called the *degree* of the algebraic number field.

The parallel between $\mathbf{Q}$ and K can be further extended. In fact, within $\mathbf{Q}$ we find the set of relative integers $\mathbf{Z}$ which can be represented as a one dimensional lattice Z in $\mathbf{R}$. In K there exists a subset O_K, called the *ring of integers* or *integer ring* of K, which is mapped by the canonical embedding to an n-dimensional lattice, i.e. a discrete group of $\mathbf{R}^n$.

Finally, an *ideal* of $\mathbf{Z}$ can be viewed as a sub-lattice of Z, similarly an ideal of the ring of integers O_K is mapped by the canonical embedding into a sub-lattice of the lattice produced by O_K.

The interest in these lattices lies in the fact that they present a diversity which can be easily controlled by properly selecting the algebraic number field [92].

A key result in [92] shows that it is possible to design lattice constellations with diversity ranging between $n/2$ and n according to the number of real (r_1) and complex $(2r_2)$ roots of the minimal polynomial of the number field. In particular it is proven that $L = r_1 + r_2$. It is then shown that only for $L = n$, the $d_{p,min}$ is related to the particular field properties of K.

[1] We note that this intuitive idea is mathematically unprecise since K has the same density of $\mathbf{Q}$ in $\mathbf{R}$.

5.4 Converting the Rayleigh fading channel into a Gaussian channel

In this section, we show that the multidimensional QAM constellation becomes insensitive to fading when the diversity L is large. This means that the point error probability is the same with or without fading. We focus the proof on the analysis of the pairwise point error probability $P(\mathbf{x} \to \mathbf{y})$, which is the probability of the received point $\mathbf{r}$ to be closer to $\mathbf{y}$ than to $\mathbf{x}$. Assuming that $\mathbf{x}$ is transmitted, the detector selects $\mathbf{y}$ if $m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) \leq m(\mathbf{y}, \mathbf{r}, \boldsymbol{\alpha})$. The conditional pairwise error probability is given by

$$P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) = P(\sum_{i=1}^{n} |r_i - \alpha_i y_i|^2 \leq \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2) = P(X \geq A)$$

where $X = \sum_{i=1}^{n} \alpha_i (x_i - y_i) n_i$ is a Gaussian random variable and $A = \frac{1}{2} \sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2$ is a constant. The mean of X is zero and its variance is $\sigma_X^2 = 2N_0 A$. The conditional pairwise error probability can be written as $P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) = Q(A/\sigma_X)$ and we obtain

$$P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) = \mathrm{Q}\left(\sqrt{\frac{\sum_{i=1}^{n} \alpha_i^2 (x_i - y_i)^2}{4N_0}}\right) \tag{5.2}$$

We recall that the Gaussian tail function is defined as $Q(x) = (2\pi)^{-1/2} \int_x^\infty \exp(-t^2/2) dt$. The pairwise error probability $P(\mathbf{x} \to \mathbf{y})$ is obtained by averaging over the fadings α_i,

$$P(\mathbf{x} \to \mathbf{y}) = \int P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) f(\boldsymbol{\alpha}) d\boldsymbol{\alpha}$$

where $f(\boldsymbol{\alpha})$ is the probability density function of the fading coefficients. The Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is at least L, since L is the modulation diversity of the constellation. For simplicity of notations and without loss of generality, we assume that $|x_i - y_i| = 1$ for the first L components and $|x_i - y_i| = 0$ for the other $n - L$ components. The conditional pairwise error probability given by (5.2) becomes

$$P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) = \mathrm{Q}\left(\sqrt{\frac{\sum_{i=1}^{L} \alpha_i^2}{4N_0}}\right) \quad . \tag{5.3}$$

On a Gaussian channel, expression (5.3) simplifies to

$$P(\mathbf{x} \to \mathbf{y}) = Q\left(\sqrt{\frac{L}{4N_0}}\right) = Q\left(\frac{d_E(\mathbf{x}, \mathbf{y})}{2\sigma}\right) \tag{5.4}$$

where $d_E^2(\mathbf{x}, \mathbf{y}) = L$ is the squared Euclidean distance between $\mathbf{x}$ and $\mathbf{y}$ and $\sigma^2 = N_0$ is the noise variance.

At first sight, one can say that $\sum_{i=1}^{L} \alpha_i^2$ acts as $E[\sum_{i=1}^{L} \alpha_i^2] = L$ when L goes to infinity. This is the *weak law of large numbers*. It states that $\sum_{i=1}^{L} \alpha_i^2 / L$ converges to 1 since the

variance of the sum tends to zero. The probability that the difference is larger than a threshold in absolute value is small. The convergence is very weak and can be proved using the Chebychev inequality. It shows, roughly and intuitively, that (5.3) approaches (5.4) and thus the fading has no effect when L is very large.

The above discussion does not constitute a rigorous proof. The exact proof is found when applying the *strong law of large numbers* (convergence in the sense of probability laws), as done below.

First, let us rewrite the conditional pairwise error probability as

$$P(\mathbf{x} \to \mathbf{y}|\boldsymbol{\alpha}) = \mathrm{Q}\left(\sqrt{\frac{L(1+Y)}{4N_0}}\right) \tag{5.5}$$

where $Y = \frac{\sum_{i=1}^{L}(\alpha_i^2-1)}{L} = \sum_{i=1}^{L} Y_i$. The random variables $Y_i = (\alpha_i^2 - 1)/L$ have a central Chi-square distribution [63] with 2 degrees of freedom, because $\alpha_i^2 = a_i^2 + b_i^2$ where a_i and b_i are two statistically independent and identically distributed Gaussian variables with zero mean and variance 1/2. The mean and the variance of Y_i are respectively $E[Y_i] = 0$ and $E[Y_i^2] = 1/L^2$. As a consequence of the statistical independence of the Y_i, their sum Y is a Chi-square random variable with $2L$ degrees of freedom. Its mean and variance are $E[Y] = 0$ and $E[Y^2] = 1/L$. The probability density function of Y is given by

$$f_Y(y) = \frac{L^L}{(L-1)!}(y+1)^{L-1}\exp(-L(y+1)), \qquad y \geq -1 \tag{5.6}$$

Figure 2 shows equation (5.6) for $L = 2, 4, 8, 12, 16$ and 32. Clearly, we see that $f_Y(y)$ tends to a Dirac impulse $\delta(y)$ when L goes to infinity. We recall that the Dirac impulse satisfies $\delta(0) = +\infty$, $\delta(y) = 0$ for all $y \neq 0$, $\int_{-\infty}^{+\infty} \delta(y)dy = 1$ and $f(y)\delta(y) = f(0)\delta(y)$.

In fact, the characteristic function of Y is

$$\psi_Y(t) = E[\exp(jtY)] = \prod_{i=1}^{L} \psi_{Y_i}(t) = (\psi_{Y_1}(t))^L \tag{5.7}$$

since the Y_i are identically distributed. $\psi_{Y_1}(t)$ expands in a Taylor series as

$$\psi_{Y_1}(t) = 1 + jtE[Y_1] + \frac{(jt)^2}{2}E[Y_1^2] + ... = 1 - \frac{t^2}{2L^2} + O(\frac{1}{L^3})$$

Taking the logarithm of (5.7) we obtain

$$\ln\psi_Y(t) = L \times \ln\left(1 - \frac{t^2}{2L^2} + O(\frac{1}{L^3})\right)$$

and for large values of L, the above expression expands to

$$\ln\psi_Y(t) = L\left(\frac{-t^2}{2L^2} + O(\frac{1}{L^3})\right) = \frac{-t^2}{2L} + O(\frac{1}{L^2})$$

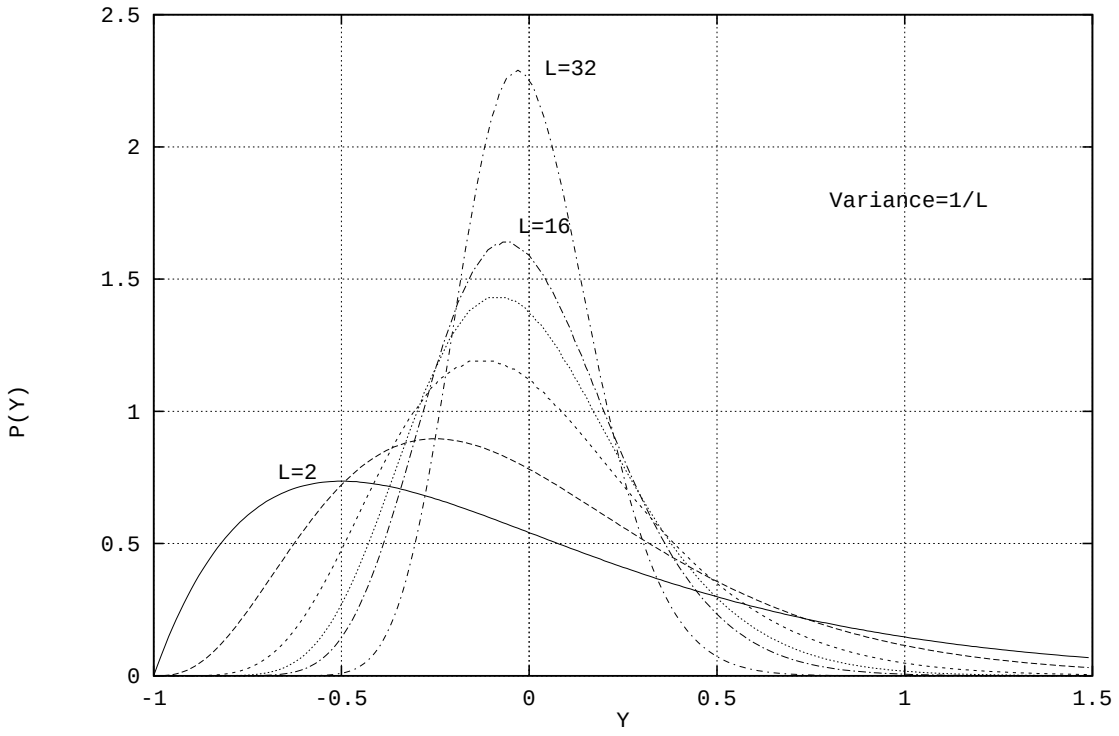


Figure 5.3: Probability density function of Y

When we take the limit as $L \to +\infty$, we obtain $\psi_Y(t) \to 1$ and $f_Y(y) \to \delta(y)$ (Y becomes Gaussian with variance $1/L$). Finally, when L is large $Q(\sqrt{\frac{L(1+y)}{4N_0}})f_Y(y)$ approaches $Q(\sqrt{\frac{L}{4N_0}})\delta(y)$ and thus $P(\mathbf{x} \to \mathbf{y})$ approaches $Q(\sqrt{\frac{L}{4N_0}})$.

Expressions (5.5) and (5.6) can be combined together to yield the pairwise point error probability $P(\mathbf{x} \to \mathbf{y})$,

$$P(\mathbf{x} \to \mathbf{y}) = \int \mathrm{Q}\left(\sqrt{\frac{L(1+Y)}{4N_0}}\right) f_Y(y)dy$$

The computation of the above integral gives $P(\mathbf{x} \to \mathbf{y})$ as a function of the signal-to-noise ratio $SNR = L/N_0$,

$$P(\mathbf{x} \to \mathbf{y}) = \left(\frac{1-\mu}{2}\right)^L \times \sum_{k=0}^{L-1} \binom{L+k-1}{k} \left(\frac{1+\mu}{2}\right)^k \tag{5.8}$$

where μ is given by

$$\mu = \sqrt{\frac{\frac{SNR}{8L}}{1+\frac{SNR}{8L}}}$$

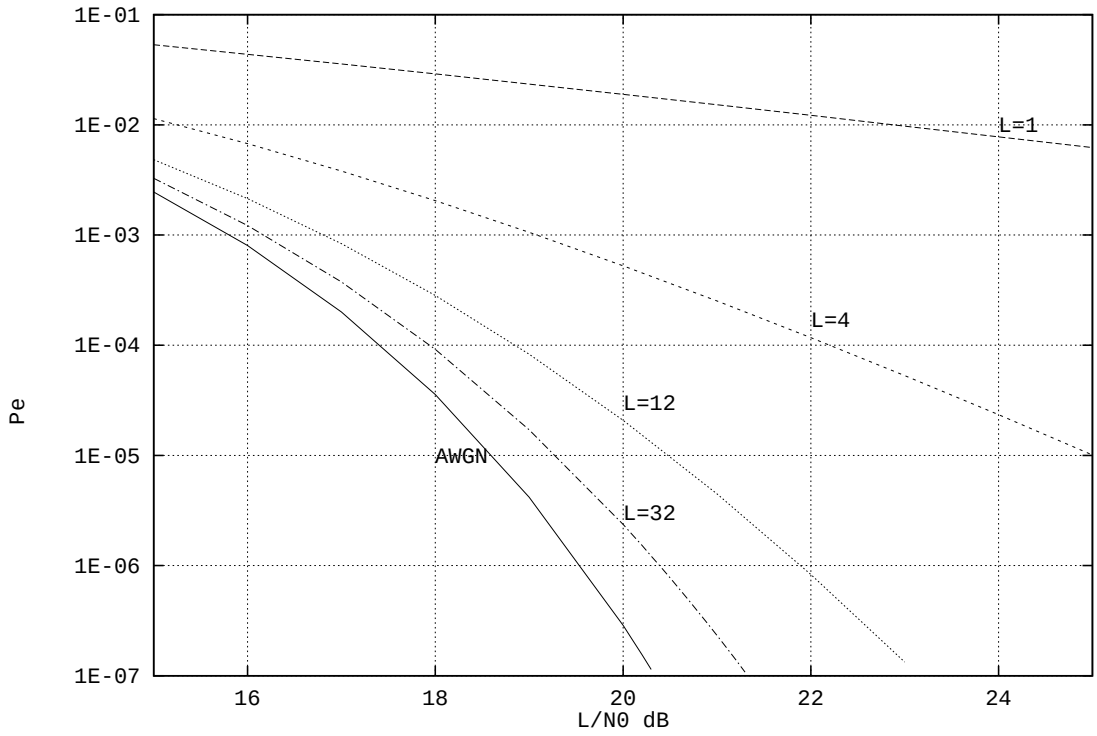


Figure 5.4: Pairwise error probability

The pairwise error probability of (5.8) is plotted in Figure 5.4 for diversities $L = 1$, 4, 12 and 32 on the Rayleigh fading channel. We also plotted in Figure 3 the pairwise error probability of (5.4) on the additive white Gaussian noise channel (AWGN). Practically, the fading effect is reduced when diversity is larger or equal to 12, as shown by Figure 5.4 and confirmed by the simulation results in Section 5.7.

5.5 Rotating the integer lattice Z^n

This section collects the three techniques we have investigated to obtain a rotated multidimensional cubic lattice Z^n with high diversity. Following the notations of [92] we denote with $\Lambda_{n,L}$ an n-dimensional lattice with diversity L.

We observe that the generator matrix M of the rotated lattice Z^n is actually a rotation matrix which transforms all the integer component vectors into a set of vectors with the required diversity.

The rotated cubic lattice constellation can be either used as an uncoded multidimensional modulation scheme or as a base modulation for further coding techniques. For example, we could apply these rotations to any known coding scheme based on QAM modulations to obtain the benefits of diversity together with the coding gain.

5.5.1 Construction of rotated Z^n lattices from known rotated integral lattices

In [92] the rotated versions of the lattices $D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ are found for L equal to half the dimension. Since $D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ are integral lattices (i.e., sub-lattices of Z^n) we expected to find the under-laying rotated Z^n lattice with the same diversity. The following *First Shell Search* (FSS) algorithm determines this rotation (generator) matrix and can be applied to any rotated lattice which admits a basis of vectors taken from its first shell.

We say that two lattices Λ_1 and Λ_2 are *equivalent* if they are equal up to a rotation and a scaling factor. The generator matrices M_1 and M_2 of two equivalent lattices are related by

$$M_2 = \alpha B M_1 R \tag{5.9}$$

where α is the scaling factor, R is the rotation matrix ($\det(R) = \pm 1$) and B is a lattice basis transformation matrix i.e., an integer matrix with $\det(B) = \pm 1$. The matrix B is also known as an integer unimodular matrix.

We denote any one of the non rotated lattices $D_4, E_6, E_8, K_{12}, \Lambda_{16}, \Lambda_{24}$ with $\Lambda_{n,1}$ since it has diversity $L = 1$ and with $\Lambda_{n,n/2}$ the corresponding rotated lattice with diversity $L = n/2$. The two lattices $\Lambda_{n,1}$ and $\Lambda_{n,n/2}$, defined by the generator matrices M_1 and M_2, are equivalent. If we determine the scaling factor α and the matrix B then we are able to obtain the desired rotation matrix R from (5.9).

Taking the absolute value of the determinant of both sides of (5.9) we obtain

$$\alpha = \left(\frac{|\det M_2|}{|\det M_1|} \right)^{1/n} .$$

Without loss of generality we can replace M_2 by $\alpha^{-1} M_2$ and concentrate on finding B. Let us consider the Gram matrices $G_1 = M_1 M_1^T$ and $G_2 = M_2 M_2^T$. Since $M_2 = R M_1 B$ we have $G_2 = B G_1 B^T$. Instead of finding B we search directly for a generator matrix M_1 of the non rotated lattice which results in $G_2 = G_1 = M_1 M_1^T$, implying that B is the identity matrix.

The Gram matrix G_2 is symmetric and its elements g_{ij} are the scalar products $\langle \mathbf{v_i}, \mathbf{v_j} \rangle$ of the lattice basis vectors corresponding to the rows of M_1. The diagonal elements g_{ii} correspond to the square norms of the basis vectors. The algorithm we propose determines the generator matrix M_1 such that the lattice basis vectors satisfy the conditions on the scalar products imposed by G_2.

For the lattices we consider, the diagonal elements g_{ii} of G_2 are all equal to the minimum square distance of the lattice. We can then restrict our search to the generator matrices M_1 formed only by vectors of the first shell of the lattice. The algorithm proceeds by adding the basis vectors one by one into the rows of M_1, after selecting them from a table (SHELL) of all the vectors of the first shell.

The first row ($i = 1$) of M_1 is set equal to the first vector in SHELL. This satisfies the constraint for g_{11}, as any vector in SHELL. Then we look for a second vector which gives a scalar product with the first equal to g_{12}. In general, if we have chosen $i-1$ vectors we scan the table SHELL to find a vector with the following properties

- it has not been selected before
- its scalar product with the previous $i-1$ vectors gives g_{ij} for $j = 1, 2, \ldots i-1$

If we do not find a vector satisfying the above conditions then we go back to $i-1$ and look for the next admissible vector. With this new vector we repeat the search of the i-th vector starting from the beginning of the table SHELL. When $i = n$ we obtain the desired rotation matrix as $R = M_2 M_1^{-1}$.

The FSS algorithm described above performs an exhaustive search of the possible rotations but considerably reduces the number of combinations to be tested by a brute force combinatorial approach. The FSS algorithm produces many possible rotations for a given lattice (we counted 960 rotations for $D_{4,2}$ and thousands for $E_{8,4}$) because a first shell basis is not unique. The interest in having a choice in the rotation matrices is that some matrices with particular symmetries could possibly simplify the decoding algorithm. For small dimensions (up to 16) the FSS algorithm is relatively fast but for higher dimensions (24 or 32) the execution time is not negligible.

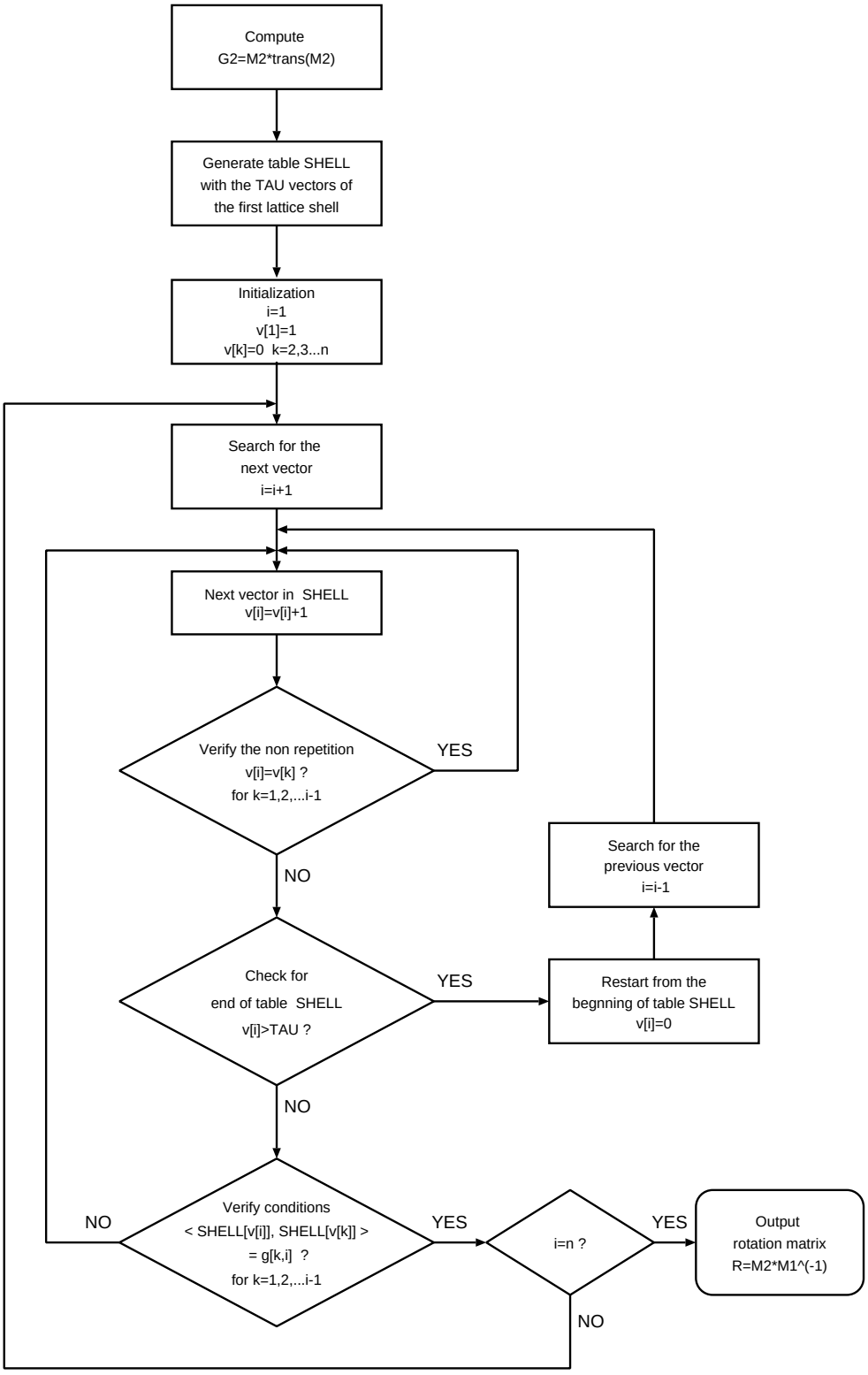


Figure 5.5: Flow chart of the algorithm of Section 5.5.1

5.5.2 Algebraic construction of $Z_{n,n/2}$ lattices

In this section we construct a family of orthogonal matrices with diversity $L = n/2$ for $n = 2^{e_1}3^{e_2}$, $e_1, e_2 = 0, 1, 2, \ldots$ applying the canonical embedding to some totally complex cyclotomic number fields. For the mathematical details about algebraic number fields and the canonical embedding the reader can refer to [92].

The key points used in this section to find $Z_{n,n/2}$ are the following :

- The vectors of the lattice basis are orthogonal.
- The minimal polynomial $\mu_\theta(x)$ has integer coefficients.
- The minimal polynomial $\mu_\theta(x)$ has n distinct complex roots.
- The lattice dimension is $n = \Phi(N)/2$, where $\Phi(\cdot)$ is the Euler function giving the number of integers prime with N [57].

Let us consider the cyclotomic field $K = \mathbf{Q}[j](\theta)$, where $\theta = e^{2\pi j/N}$ is an N-th root of unity. K is an algebraic extension of $\mathbf{Q}[j] = \{a + jb | a, b \in \mathbf{Q}\}$ of degree $\Phi(N)/2$. We recall that this is a totally complex field with signature $(r_1 = 0, r_2 = n/2)$ and minimal polynomial

$$\mu_\theta(x) = \prod_{(k,N)=1} (x - \theta^k) \tag{5.10}$$

where (k, N) is the greatest common divisor of k and N. The minimal polynomial over $\mathbf{Z}[j]$ is denoted by $m(x)$ and defined later in this section.

Let us denote $\theta_1 = \theta, \theta_2, \ldots \theta_{n/2}$ the complex roots of $\mu_\theta(x)$ which define the $n/2$ distinct field $\mathbf{Q}$-homomorphisms

$$\sigma_1(\theta) = \theta_1, \ \sigma_2(\theta) = \theta_2, \ \ldots \ \sigma_{n/2}(\theta) = \theta_{n/2} \ . \tag{5.11}$$

To construct a complex lattice Λ of dimension $n/2$ we apply the canonical embedding to the ring of integers $O_K = \mathbf{Z}[j](\theta)$ generated by $(1, \theta, \theta^2, \ldots \theta^{n/2-1})$. Its generator matrix is given by

$$M = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \theta_1 & \theta_2 & \ldots & \theta_{n/2} \\ \vdots & \vdots & & \vdots \\ \theta_1^{n/2-1} & \theta_2^{n/2-1} & \ldots & \theta_{n/2}^{n/2-1} \end{pmatrix} = \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \\ \vdots \\ \mathbf{v}_{n/2} \end{pmatrix} \tag{5.12}$$

where the complex lattice basis vectors $\mathbf{v}_i$, $i = 1, 2, \ldots n/2$. correspond to the rows of M.

The corresponding real lattice of dimension n can be obtained by replacing each complex entry $a + jb$ of M by a 2×2 matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. As proven in [92] this lattice has diversity $L = n/2 = r_2$.

We are interested in selecting the roots θ_i, $i = 1, 2, \ldots n/2$, or equivalently their minimal polynomial $\mu_\theta(x)$, so that M becomes an orthogonal matrix i.e., a generator matrix for the

complex integer lattice in dimension $n/2$. The orthogonality among the complex vectors implies the orthogonality among the corresponding real vectors. The complex inner product of any two rows $\mathbf{v}_{p+1} = (\theta_1^p, \theta_2^p, \ldots \theta_{n/2}^p)$ and $\mathbf{v}_{q+1} = (\theta_1^q, \theta_2^q, \ldots \theta_{n/2}^q)$, $p, q = 0, 1, \ldots n/2 - 1$ of M must satisfy

$$\langle \mathbf{v}_{p+1}, \mathbf{v}_{q+1} \rangle = \sum_{k=1}^{n/2} (\theta_k)^p (\theta_k^*)^q = \begin{cases} 1 & p = q \\ 0 & p \neq q \end{cases} \tag{5.13}$$

For $p > q$, we have

$$\langle \mathbf{v}_{p+1}, \mathbf{v}_{q+1} \rangle = \sum_{k=1}^{n/2} (\theta_k \theta_k^*)^q (\theta_k)^{p-q} = \sum_{k=1}^{n/2} \|\theta_k\|^q (\theta_k)^{p-q} = 0 \tag{5.14}$$

and since the complex roots θ_i are placed on the unit circle $\|\theta_k\| = 1$

$$\langle \mathbf{v}_{p+1}, \mathbf{v}_{q+1} \rangle = \sum_{k=1}^{n/2} (\theta_k)^m = S_m = 0 \qquad m = 1, 2, , \ldots n/2 - 1 \tag{5.15}$$

In other words, the first $n/2-1$ power symmetric functions S_m of the roots of $\mu_{\theta}(x)$ are null. The polynomial $\mu_{\theta}(x)$, which we want to determine, can be factored into $m(x)m^*(x)$, where we assume that θ_i, $i = 1, 2, \ldots n/2$ are the roots of the polynomial $m(x)$ of degree $n/2$ over the ring of Gaussian integers $\mathbf{Z}[j]$, while $m^*(x)$ takes on the complex conjugate roots.

We can then write

$$m(x) = x^{n/2} - P_1 x^{n/2-1} + \cdots + (-1)^k P_k x^{n/2-k} + \cdots + (-1)^{n/2} P_{n/2} \tag{5.16}$$

where the coefficients P_k of the polynomial are related to the power symmetric functions by the Newton identities

$$\begin{aligned} S_1 &= P_1 \\ S_2 &= P_1^2 - 2P_2 \\ S_3 &= P_1 S_2 - P_2 S_1 + 3P_3 \\ &\cdots \end{aligned}$$

$$S_{n/2} = S_{n/2-1} P_1 - S_{n/2-2} P_2 + S_{n/2-1} P_3 + \cdots - (-1)^{n/2} (n/2) P_{n/2} \tag{5.17}$$

From (5.17) and the orthogonality conditions (5.15) we obtain

$$\begin{aligned} S_1 = 0 &\Rightarrow P_1 = 0 \\ S_2 = 0 &\Rightarrow P_2 = 0 \\ &\cdots \end{aligned}$$

$$S_{n/2} = -(-1)^{n/2} (n/2) P_{n/2} \tag{5.18}$$

and $m(x) = x^{n/2} + P_{n/2}$. Similarly we obtain $m^*(x) = x^{n/2} + P_{n/2}^*$ so that

$$\mu_{\theta}(x) = x^n + (P_{n/2} + P_{n/2}^*) x^{n/2} + 1 \tag{5.19}$$

Now that we have the general form of the minimal polynomial we still need to determine which of the n roots of unity must be chosen to apply the canonical embedding (5.12).

Let $\theta_i = e^{j\phi_i}, i = 1, 2, \ldots n/2$ be the unknown roots of $m(x)$ which we want to determine. $P_{n/2}$ is the product of the $n/2$ roots laying on the unit circle

$$P_{n/2} = e^{j\psi} \qquad -\pi \leq \psi < \pi \tag{5.20}$$

thus

$$m(\theta_i) = e^{j\phi_i n/2} + e^{j\psi} = 0 \tag{5.21}$$

and we obtain exactly $n/2$ distinct values of θ_i with

$$\phi_i = 2\frac{\psi + \pi}{n} + \frac{4\pi(i-1)}{n} \qquad i = 1, 2, \ldots n/2 \tag{5.22}$$

Similarly, for the roots $\theta_{i+n/2} = e^{j\phi_{i+n/2}}$ of $m^*(x)$ satisfy

$$\phi_{i+n/2} = 2\frac{\pi - \psi}{n} + \frac{4\pi(i-1)}{n} \qquad i = 1, 2, \ldots n/2 \tag{5.23}$$

In order to determine the value of ψ we consider the following conditions

- $\mu_\theta(x)$ has exactly n distinct roots, so the roots of $m(x)$ must be different from the roots of $m^*(x)$

$$2\frac{\pi + \psi}{n} \neq 2\frac{\pi - \psi}{n} \quad \Rightarrow \quad \psi \neq 0 \tag{5.24}$$

- $\mu_\theta(x)$ has only complex roots, so

$$\phi_i, \phi_{i+n/2} \neq k\pi \quad \Rightarrow \quad 2\pi i + \pi \pm \psi \neq \frac{n}{2}k\pi \quad \Rightarrow \quad \psi \neq 0 \tag{5.25}$$

- $\mu_\theta(x)$ has integer coefficients

$$P_{n/2} + P^*_{n/2} = e^{j\psi} + e^{-j\psi} = 2\cos\psi \in \mathbf{Z} \tag{5.26}$$

  which implies $\psi = \pm\pi/3, \pm\pi/2, \pm 2\pi/3$.

The possible values for the roots of $m(x)$ are summarized in Table 5.1, where only the negative values of ψ were considered since the positive ones correspond to the roots of $m^*(x)$. The third column (the value of N) is derived from the second one by noting that $\phi_1 = 2\pi/N$ since by definition $\theta = e^{2\pi j/N} = \theta_1 = e^{j\phi_1}$.

Finally, we must solve $\Phi(N) = n$ for $N = 3n/2, 2n, 3n$, to obtain the admissible values of the dimension n of the real lattice. We will make use of the following properties of the Euler function:

- $\Phi(p) = p - 1$ for p prime.

ψ	$\phi_i = 2\frac{\psi+\pi}{n} + \frac{4\pi(i-1)}{n}$	N
$-\frac{\pi}{3}$	$\frac{4\pi}{3n} + \frac{4\pi(i-1)}{n}$	$\frac{3n}{2}$
$-\frac{\pi}{2}$	$\frac{\pi}{n} + \frac{4\pi(i-1)}{n}$	$2n$
$-\frac{2\pi}{3}$	$\frac{2\pi}{3n} + \frac{4\pi(i-1)}{n}$	$3n$

Table 5.1: The admissible values for the roots are $\theta_i = e^{j\phi_i}$, $i = 1, \ldots n/2$

- $\Phi(p^k) = (p-1)p^{k-1}$ for p prime and k positive integer.
- $\Phi(ab) = \Phi(a)\Phi(b)$ iff $(a,b) = 1$ for a, b integers.
- $\Phi(a) \leq a$, equal for $a = 1$ only.

N = 3n/2 — Let $n = 2^{e_1}3^{e_2}P$ where $e_1 = 1, 2, \ldots$, $e_2 = 0, 1, 2, \ldots$, $(2, P) = 1$ and $(3, P) = 1$, then

$$\begin{aligned} \Phi(3n/2) &= n \\ \Phi(2^{e_1-1}3^{e_2+1}P) &= 2^{e_1}3^{e_2}P \\ 2^{e_1-2}2\,3^{e_2}\Phi(P) &= 2^{e_1}3^{e_2}P \\ \Phi(P) &= 2P \qquad \text{no solutions .} \end{aligned}$$

N = 2n — Let $n = 2^{e_1}P$ where $e_1 = 0, 1, 2, \ldots$ and $(2, P) = 1$, then

$$\begin{aligned} \Phi(2n) &= n \\ \Phi(2^{e_1+1}P) &= 2^{e_1}P \\ 2^{e_1}\Phi(P) &= 2^{e_1}P \qquad \text{solutions for } P = 1 \quad \Rightarrow \quad n = 2^{e_1} \ . \end{aligned}$$

N = 3n — Let $n = 2^{e_1}3^{e_2}P$ where $e_1, e_2 = 0, 1, 2, \ldots$, $(2, P) = 1$ and $(3, P) = 1$, then

$$\begin{aligned} \Phi(3n) &= n \\ \Phi(2^{e_1}3^{e_2+1}P) &= 2^{e_1}3^{e_2}P \\ 2^{e_1-1}2\,3^{e_2}\Phi(P) &= 2^{e_1}3^{e_2}P \\ 2^{e_1}3^{e_2}\Phi(P) &= 2^{e_1}3^{e_2}P \qquad \text{solutions for } P = 1 \quad \Rightarrow \quad n = 2^{e_1}3^{e_2} \ . \end{aligned}$$

Finally we can conclude that the admissible values of ψ are $-\pi/2$ and $-2\pi/3$ corresponding to the polynomials of the type $x^n + \epsilon x^{n/2} + 1$ with $\epsilon = 0$ or -1 with $N = 2n$ and $3n$ respectively. Thus, there exist $Z_{n,n/2}$ lattices for all dimensions $n = 2^{e_1}3^{e_2}$, $e_1, e_2 = 0, 1, 2, \ldots$.

5.5.3 Algebraic construction of $Z_{n,n}$ lattices

This construction is based on the totally real algebraic number field $\mathbf{Q}(2\cos(2\pi/N))$. Applying the canonical embedding to a particular ideal in this field we found the rotated cubic lattice $Z_{n,n}$. Since $\mathbf{Q}(2\cos(2\pi/N))$ is a totally real field we know from [92] that the constellation has full diversity $L = n$. The choice of this family of number fields appears to be arbitrary but in the following section we will show that some of these rotated cubic lattices maximize the product distance of the constellation.

We now describe the procedure we used to obtain $Z_{n,n}$. First of all we know that the degree of $\mathbf{Q}(2\cos(2\pi/N))$ is $\Phi(N)/2$ so this imposes some limitations on the lattice dimensions we can obtain ($n = \Phi(N)/2$). All the even dimensions up to 32 do not lead to the desired integer lattice while the odd ones in Table 5.2 do. The procedure is the following:

1. Consider the number field $K = \mathbf{Q}(2\cos(2\pi/N))$ with minimal polynomial $\mu_\theta(x)$ (see Appendix A) and absolute discriminant d_K.

2. Let $d_K = p^m$ be the prime factorization of the absolute discriminant.

3. Factor the principal ideal (p) into I^n, where I is a prime ideal.

4. For $k = 0, \ldots n$ apply the canonical embedding to the ideal I^k and check if the generator matrix is orthogonal i.e., the generator matrix of $Z_{n,n}$.

The last column of Table 5.2 gives the power of the ideal I which produces the full diversity $Z_{n,n}$ lattice. The lattice is given by $Z_{n,n} = \sigma(I^k)$, where σ is the canonical embedding defined by the n real roots of $\mu_\theta(x)$. The fundamental volume of $Z_{n,n}$ can be related to d_K and the algebraic norm $N(I^k) = p^k$ by [92]

$$vol(Z_{n,n}) = N(I^k) * \sqrt{|d_K|}\ .$$

If we introduce a scaling factor $\alpha = (p^k * \sqrt{|d_K|})^{1/n}$, we obtain the unit volume lattice.

As an example, the full diversity cubic lattice $Z_{5,5}$ is found from the field $\mathbf{Q}(2\cos(2\pi/11))$. The absolute discriminant is $d_K = 11^4$ and $Z_{5,5} = \sigma(I^3)$. The prime ideal I is computed by factoring the principal ideal generated by 11: $(11) = (11, \theta+2)^5$ and $I = 11O_K + (\theta+2)O_K$.

n	N	$\mu_\theta(x)$	d_K	k
3	$7, 14$	$x^3 + x^2 - 2x - 1$	7^2	2
	$9, 18$	$x^3 - 3x + 1$	3^4	1
5	$11, 22$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	11^4	3
9	$19, 38$	$x^9 + x^8 - 8x^7 - 7x^6 + 21x^5$ $+15x^4 - 20x^3 - 10x^2 + 5x + 1$	19^8	5
11	$23, 46$	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6$ $-56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$	23^{10}	6
15	$31, 62$	$x^{15} + x^{14} - 14x^{13} - 13x^{12} + 78x^{11} + 66x^{10} -$ $220x^9 - 165x^8 + 330x^7 + 210x^6 - 252x^5 -$ $126x^4 + 84x^3 + 28x^2 - 8x - 1$	31^{14}	8

Table 5.2: Full diversity $Z_{n,n}$ lattices from ideals of the $\mathbf{Q}(2\cos(2\pi/N))$.

5.6 Maximizing the product distance

In the previous section we have shown how to obtain rotated Z^n lattices which guarantee a certain degree of diversity. Although diversity appears to be the most relevant design parameter we are also interested in maximizing the minimal product distance $d_{P,min}$ between any two points of the constellation. In this section we show a construction of $Z_{n,n}$ lattices for some even n which aims at maximizing $d_{P,min}$.

Stating the problem in the most general form, we need to determine an arbitrary rotation matrix, with the highest possible diversity order ($L = n$), which maximizes $d_{P,min}$ of the corresponding signal constellation. This optimization problem becomes rapidly intractable due to the number of variables and the complexity of the constraints. For this reason we restrict our search to a smaller family of rotation matrices which can be parameterized with a reduced number of variables and result in simpler constraints.

We start with dimensions 2 and 3 and then move up to other dimensions of the type $2^{e_1}3^{e_2}$ applying a construction which recalls the one used for Hadamard matrices.

It is important to remind that whenever we are dealing with lattices generated by canonical embedding of totally real number fields $d_{P,min}$ is related to the field norm and is independent of the size of the finite constellation [92]. In all other cases this is not necessarily true.

In the following $d_{P,min}$-optimizing constructions we limited the size of the constellations to the case of $\eta = 4$ bits/symbol. In all cases (except for the three-dimensional one, where it is proven to be true) we verified experimentally that $d_{P,min}$ does not depend on the size of the constellation. We conjecture that in all these cases we are dealing with some lower dimensional sections of a lattice generated by canonical embedding of totally real number fields of higher degree.

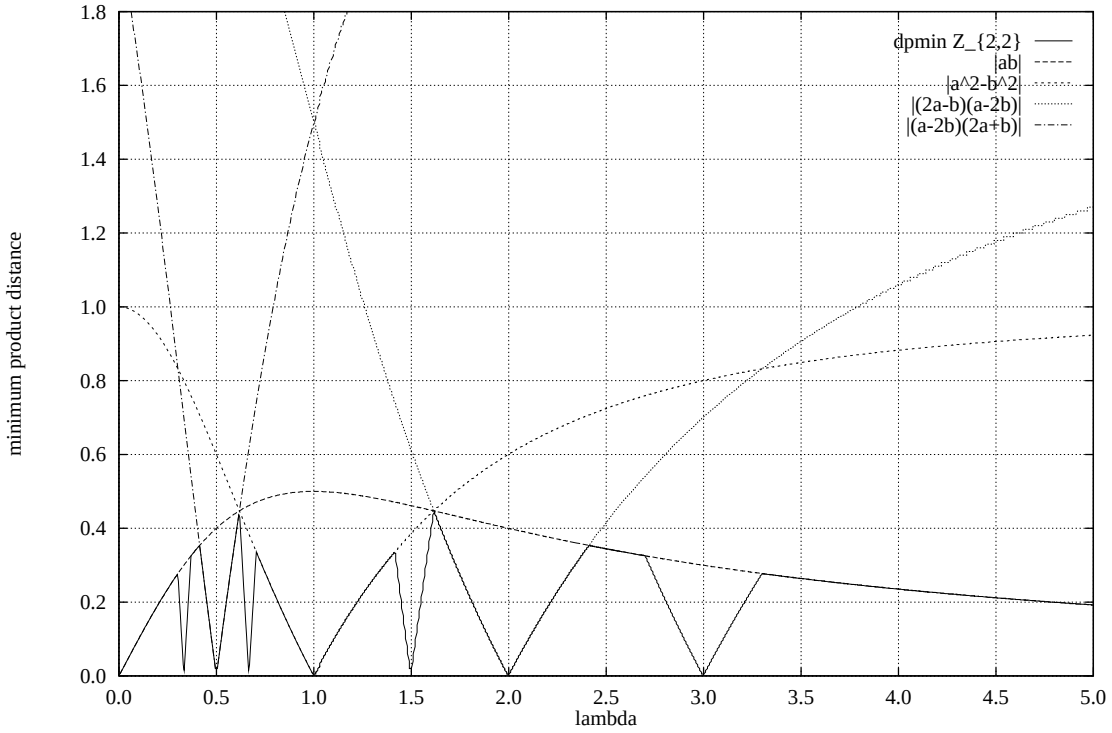


Figure 5.6: $d_{P,min}$ for a family of $Z_{2,2}$ lattices

5.6.1 Dimension 2

All two-dimensional orthogonal matrices have the following structure

$$M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

with the constraint $a^2 + b^2 = 1$.

We parameterize this orthogonal matrix as a function of the single variable λ as follows

$$a = 1/\sqrt{1+\lambda^2} \qquad b = \lambda a \ .$$

Note that the rows of M are the normalized orthogonal lattice basis vectors. Figure 5.6 shows the values of $d_{P,min}$ as a function of λ for a finite constellation ($\eta = 4$ bits/symbol), carved from the lattice generated by M. Only positive values of λ were considered due to the symmetry about the origin and the values of λ resulting in $L = 1$ diversity constellation were skipped. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellation using a small step for λ (e.g. 0.005). In the same figure we also plot the following upper bounds to $d_{P,min}$ (functions of λ)

$$d_{P,min} \leq \begin{cases} |a\,b| & (1,0) \\ |a^2 - b^2| & (1,1) \\ |(2a-b)(a+2b)| & (2,1) \\ |(a-2b)(2a+b)| & (1,2) \end{cases} \tag{5.27}$$

corresponding to the product distances between the origin and the points with the integer components reported in the second column of (5.27). The curve of $d_{P,min}$ could, in principle, be obtained as the minimum of all the bounds of the type (5.27) for all the points of the constellation.

In Figure 5.6 we observe that the highest peaks are found at the intersection of the first and second bound in (5.27) that is for

$$\lambda_{o,2} = \frac{1 \pm \sqrt{5}}{2} \qquad d^{o,2}_{P,min} = \frac{\sqrt{5}}{5} < 0.5 \ . \tag{5.28}$$

The upper bound of 0.5 to $d_{P,min}$ is obtained by assuming that there exists a constellation containing a unit norm vector with all equal components.

A few considerations about the optimal matrix are appropriate here. $\lambda_{o,2}$ is the root of the polynomial $\lambda^2+\lambda-1$ i.e., it belongs to a totally real number field of degree 2. The entries a and b of M then belong to a number field of degree 4. In this case we are not using the canonical embedding lattice but probably some two-dimensional section of it, which gives us a Z^2 lattice constellation with diversity $L = 2$ and maximal $d_{P,min}$. The two dimensional case is the only one where we have obtained the absolute maximum $d_{P,min}$.

5.6.2 Dimension 3

The family of three-dimensional orthogonal matrices we consider here is

$$M = \begin{pmatrix} a & b & c \\ b & c & a \\ -c & -a & -b \end{pmatrix}$$

with the constraints $a^2 + b^2 + c^2 = 1$ and $ab + bc + ac = 0$.

We parameterize this orthogonal matrix as a function of the single variable λ as follows

$$a = \frac{1+\lambda}{1+\lambda+\lambda^2} \qquad b = \lambda a \qquad c = \frac{-\lambda}{1+\lambda} a \ . \tag{5.29}$$

As before the rows of M form the orthonormal lattice basis vectors of a rotated version of Z^3.

Figure 5.7 shows the values of $d_{P,min}$ as a function of λ, for a finite constellation with $\eta = 4$ bits/symbol, carved from the lattice generated by M. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellation for each value of λ. In this case the values of λ were taken in the range $(-4, 4)$ since the $d_{P,min}$ rapidly vanishes outside this interval. The values of λ resulting in diversity less than 3 were skipped. In Figure 5.7 we also plot the following upper bounds to $d_{P,min}$ (functions of λ)

$$d_{P,min} \leq \begin{cases} |a\,b\,c| & (1,0,0) \\ |(a-b)(b-c)(c-a)| & (1,0,1) \\ |(a+b-c)(b+c-a)(c+a-b)| & (1,1,1) \end{cases} \tag{5.30}$$

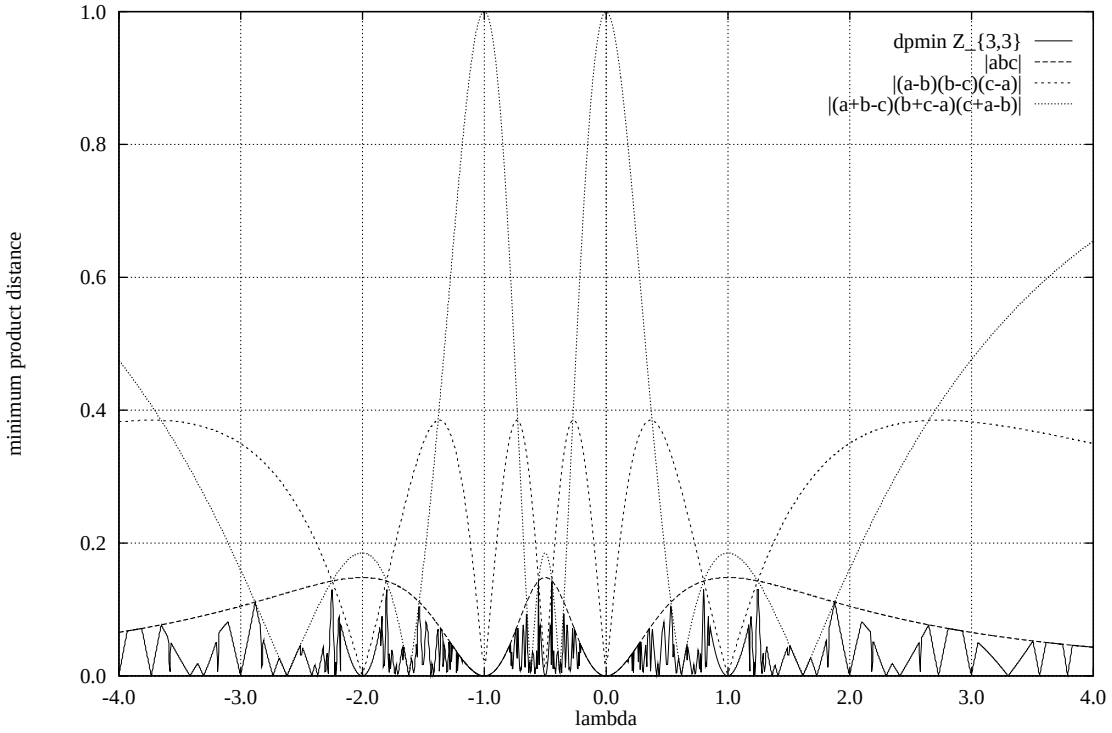


Figure 5.7: $d_{P,min}$ for a family of $Z_{3,3}$ lattices

corresponding to the product distances between the origin and the points with the integer components reported in the second column of (5.30).

In Figure 5.7, we identify the highest peaks at the intersection of the first and second bound in (5.30), that is at the roots of the polynomials

$$\begin{aligned} p_1(\lambda) &= \lambda^3 + 2\lambda^2 - \lambda - 1 \\ p_2(\lambda) &= \lambda^3 + \lambda^2 - 2\lambda - 1 \ . \end{aligned}$$

Surprisingly, these two polynomials happen to be equivalent minimal polynomials of the totally real algebraic number field $\mathbf{Q}(2\cos(2\pi/7))$. The values $\lambda_{o,3}$ of the roots of the above polynomials have the simple expressions:

$$\begin{aligned} p_1 &: \ [2\cos(4\pi/7)]^{-1} = -2.24698, \quad [2\cos(6\pi/7)]^{-1} = -0.55496, \quad [2\cos(2\pi/7)]^{-1} = 0.80194 \\ p_2 &: \ 2\cos(6\pi/7) = -1.80194, \quad 2\cos(4\pi/7) = -0.44504, \quad 2\cos(2\pi/7) = 1.24698 \ . \end{aligned}$$

The values of $a(\lambda_{o,3}), b(\lambda_{o,3})$ and $c(\lambda_{o,3})$ to replace in M can be either computed directly by substitution in equations (5.29) or by applying the field properties of $\mathbf{Q}(2\cos(2\pi/7))$. This second method is preferable since it results in simple polynomial expressions:

$$a(\lambda_{o,3}) = \left[\frac{1+\lambda}{1+\lambda+\lambda^2} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7}(5 + \lambda_{o,3} - \lambda_{o,3}^2)$$

$$b(\lambda_{o,3}) = \left[\frac{\lambda+\lambda^2}{1+\lambda+\lambda^2} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7}(-1+4\lambda_{o,3}+3\lambda_{o,3}^2)$$

$$c(\lambda_{o,3}) = \left[\frac{-\lambda}{1+\lambda+\lambda^2} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7}(3-5\lambda_{o,3}-2\lambda_{o,3}^2) \qquad (i=1,2)\ .$$

Similarly, we can compute the optimal value $d_{P,min}^{o,3}$:

$$d_{P,min}^{o,3} = [|a\,b\,c| \bmod p_i(\lambda)]_{\lambda=\lambda_{o,3}} = \left[\frac{\lambda^2(1+\lambda)^2}{(1+\lambda+\lambda^2)^3} \bmod p_i(\lambda)\right]_{\lambda=\lambda_{o,3}} = \frac{1}{7} < \frac{1}{3} \quad (i=1,2)$$

By direct inspection we find that all these lattices are equivalent to the lattices $Z_{3,3a}$ and $Z_{3,3b}$ of Section 5.5.3.

5.6.3 Construction in higher dimensions

In the two previous subsections we have found the basic building blocks of the rotation matrices we will present here. This construction is based on the special structure of some orthogonal matrices similar to the one used to construct Hadamard matrices. We will illustrate this construction in some details for dimensions 4 and 6. The other rotation matrices for dimensions 8 and 12 are obtained by iterating the same construction.

Dimension 4

The family of four-dimensional orthogonal matrices we consider here is

$$M = \begin{pmatrix} a & b & -c & -d \\ -b & a & d & -c \\ c & d & a & b \\ -d & c & -b & a \end{pmatrix} = \begin{pmatrix} M_1 & -M_2 \\ M_2 & M_1 \end{pmatrix}$$

Let $U^2 = a^2 + b^2 + c^2 + d^2$ be the normalization factor.

If the 2×2 sub-matrix M_1 is fixed to be one of the optimal two-dimensional matrices, then the orthogonality constraints reduce to $ad - bc = 0$. The other 2×2 sub-matrix M_2 is dependent of the parameter λ. The basis vectors are finally normalized by U giving

$$a = \frac{1}{U\sqrt{1+\lambda_{o,2}^2}} \qquad b = \frac{\lambda_{o,2}}{U\sqrt{1+\lambda_{o,2}^2}} \qquad c = \frac{\lambda}{U\lambda_{o,2}} \qquad d = \frac{\lambda}{U}$$

where

$$U = \frac{\sqrt{\lambda_{o,2}^2 + \lambda^2 + \lambda_{o,2}^2\lambda^2}}{\lambda_{o,2}} .$$

Figure 5.8 shows the values of $d_{P,min}$ as a function of λ for a finite constellation ($\eta = 4$ bits/symbol), carved from the lattice generated by M. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellation. The values of λ are shown, with steps of 0.005, in the range $(0, 3)$, since the $d_{P,min}$ rapidly vanishes outside this interval and the curve is symmetric about the origin. The values of λ resulting in diversity less than 4 were skipped. In Figure 5.8 we also plot the following upper bounds to $d_{P,min}$ (functions of λ)

$$d_{P,min} \leq \begin{cases} |a\,b\,c\,d| & (1,0,0,0) \\ |(a^2-c^2)(b^2-d^2)| & (1,0,1,0) \\ |(a-d)^2(b+c)^2| & (1,0,0,1) \\ |(a+d)^2(b-c)^2| & (0,1,1,0) \\ |(-b+c-d)(a+d+c)(d+a-b)(-c+b+a)| & (0,1,1,1) \end{cases} \tag{5.31}$$

corresponding to the product distances between the origin and the points with the given integer components.

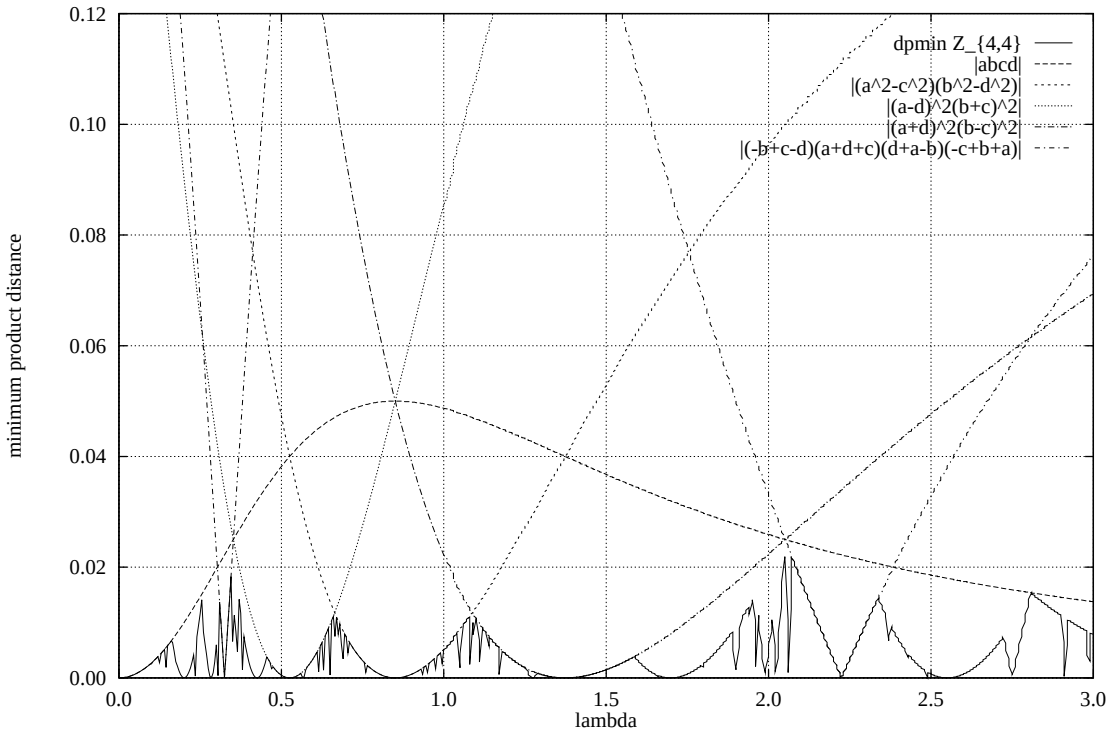


Figure 5.8: $d_{P,min}$ for a family of $Z_{4,4}$ lattices

In Figure 5.8 we find identify the two highest peaks at the intersection of the first and third bound in (5.31)

$$\lambda_{o,4}^{(1)} = \frac{1}{10}(\sqrt{2}-1)\sqrt{50+10\sqrt{2}} = 0.3523511$$

and at the intersection of the first and fourth bound in (5.31)

$$\lambda_{o,4}^{(2)} = \frac{1}{10}(\sqrt{2}+1)\sqrt{50+10\sqrt{2}} = 2.0536527\ .$$

These values can be obtained in a closed for since they are roots of a polynomial of degree 4. The corresponding optimal value for $d_{P,min}$ is $1/40$. Other two lower peaks are found at the intersection of the second and third bound in (5.31) ($\lambda_{so,4}^{(1)} = 0.6641681$) and at the intersection of the second and fourth bound in (5.31) ($\lambda_{so,4}^{(4)} = 1.0894935$). The corresponding sub-optimal value for $d_{P,min}$ is $1/85$. Closed form values of λ_{so}, can also be found.

Dimension 6

The family of six-dimensional orthogonal matrices we consider here is

$$M = \begin{pmatrix} a & b & c & -d & -e & -f \\ b & c & a & -e & -f & -d \\ -c & -a & -b & f & d & e \\ d & e & f & a & b & c \\ e & f & d & b & c & a \\ -f & -d & -e & -c & -a & -b \end{pmatrix} = \begin{pmatrix} M_1 & -M_2 \\ M_2 & M_1 \end{pmatrix}$$

with the normalization factor $U^2 = a^2 + b^2 + c^2 + d^2 + e^2 + f^2$ and the two orthogonality constraints $ae - ce + bf - af + cd - bd = 0$ and $ab + bc + ca + de + ef + fd = 0$.

If the 3×3 sub-matrix M_1 is fixed to be one of the optimal three-dimensional matrices, then the above equations simplify to $U^2 = 1 + d^2 + e^2 + f^2$, $ae - ce + bf - af + cd - bd = 0$ and $de + ef + fd = 0$. The other 3×3 sub-matrix M_2 is determined from the above equations as a function of a single parameter λ. The basis vectors are then normalized so that we obtain:

$$\begin{array}{lll} a = (5 + \lambda_{o,3} - \lambda_{o,3}^2)/(7U) & b = (-1 + 4\lambda_{o,3} + 3\lambda_{o,3}^2)/(7U) & c = (3 - 5\lambda_{o,3} - 2\lambda_{o,3}^2)/(7U) \\ d = \lambda/U & e = \lambda\lambda_{o,3}/U & f = -\lambda(\lambda_{o,3}^2 + \lambda_{o,3} - 1)/U \end{array}$$

where

$$U = \sqrt{1 + \lambda^2(\lambda_{o,3}^2 - \lambda_{o,3} + 2)} \; .$$

Figure 5.9 shows the values of $d_{P,min}$ as a function of λ for a finite constellation ($\eta = 4$ bits/symbol), carved from the lattice generated by M. $d_{P,min}$ was computed by exhaustive search through the points of the finite constellations. The values of λ resulting in diversity less than 6 were skipped. In Figure 5.9 we also plot the following upper bounds to $d_{P,min}$ (functions of λ)

$$d_{P,min} \leq \begin{cases} |a\,b\,c\,d\,e\,f| & (1,0,0,0,0,0) \\ |(a^2 - d^2)(b^2 - e^2)(c^2 - f^2)| & (1,0,0,1,0,0) \\ |(a+e)(b+f)(c+d)(b-d)(c-e)(a-f)| & (1,0,0,0,1,0) \\ |(b+d)(c+e)(a+f)(a-e)(b-f)(c-d)| & (0,1,0,1,0,0) \end{cases} \tag{5.32}$$

corresponding to the product distances between the origin and the points with the integer components reported in the second column of (5.32).

In Figure 5.9 we find the two highest peaks at the intersection of the first and fourth bound in (5.32), corresponding to

$$\lambda_{o,6} = \frac{1}{14}\left[\pm(5 + \lambda_{o,3} - \lambda_{o,3}^2) + \sqrt{35(\lambda_{o,3} + 3)}\right] = \begin{cases} 0.20270605 \\ 0.53069132 \end{cases}$$

The corresponding optimal value for $d_{P,min}$ is

$$d_{P,min}^{o,6} = \frac{1}{7^2\, 5\sqrt{5}} \; .$$

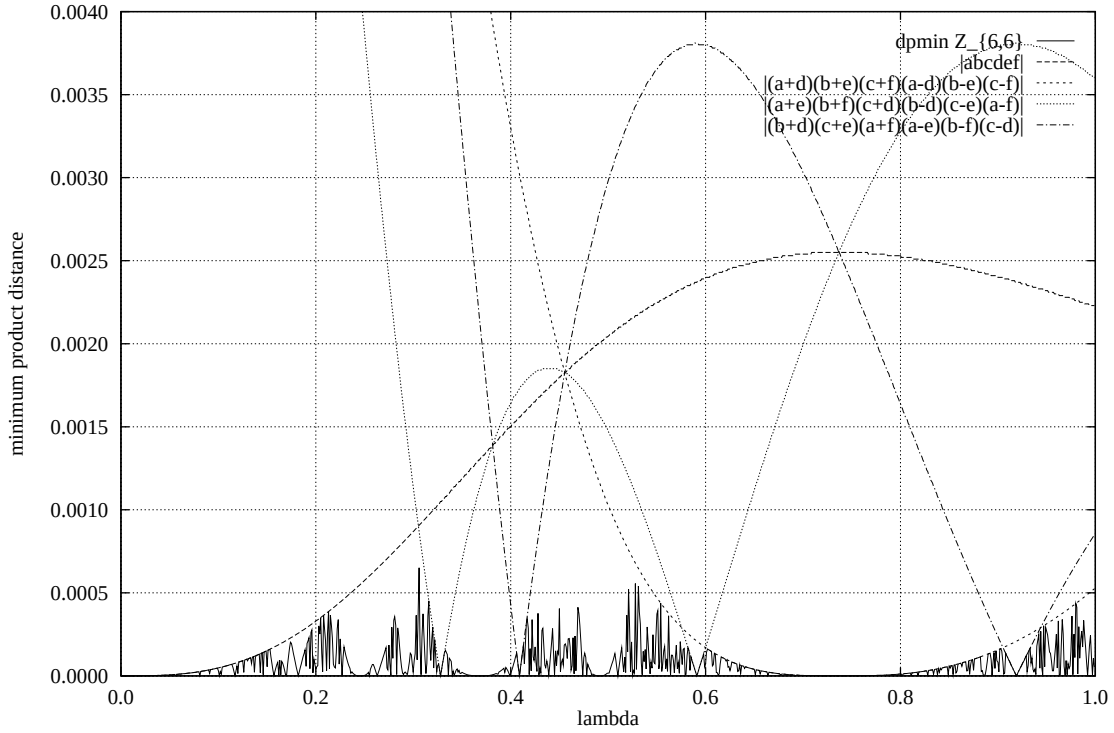


Figure 5.9: $d_{P,min}$ for a family of $Z_{6,6}$ lattices

Other two lower peaks are found at the intersection of the first and third bound in (5.32) corresponding to

$$\lambda_{so,6} = \frac{1}{7}\left[\pm(5+\lambda_{o,3}-\lambda_{o,3}^2)+\sqrt{14(\lambda_{o,3}+3)}\right] = \begin{cases} 0.13585595 \\ 0.79182651 \end{cases}$$

The corresponding suboptimal value for $d_{P,min}$ is

$$d_{P,min}^{so,6} = \frac{1}{7^2\,2^4\,\sqrt{2}}\ .$$

As discussed before the optimal and the suboptimal value of $d_{P,min}$ are computed using the fact that corresponding values of λ lie in an algebraic number field of degree 6.

5.6.4 Other dimensions

In all the previous cases we were able to obtain the closed form expressions for the optimal rotation matrices. If we further increase the dimension a greater number of constraints become non linear and the degree of the polynomial equations giving the optimal values of λ becomes greater than four, which is the ultimate limit for closed form solutions.

In these cases we adopt a purely numerical approach. Unfortunately we are not able to guarantee the absolute optimality of the rotations. We report in Table 5.3 the numerical

n	index					$d_{P,min}$
8	1–4	0.05830052	-0.09433222	0.14074991	-0.22773814	
	5–8	0.19255622	-0.31156250	0.46487183	-0.75217842	$3.685\ 10^{-6}$
12	1–4	-0.15171243	0.34089475	-0.27337636	0.09376344	
	5–8	-0.21068454	0.16895588	0.27514779	0.47206374	
	9–12	0.03331638	-0.08690755	0.23170916	0.58601306	$1.528\ 10^{-10}$

Table 5.3: First rows of the generator matrices of $Z_{8,8}$ and $Z_{12,12}$

values of the first row of the rotation matrix for dimensions 8 and 12. The entire matrix can be easily reconstructed by iterating the construction of the type of the previous sections.

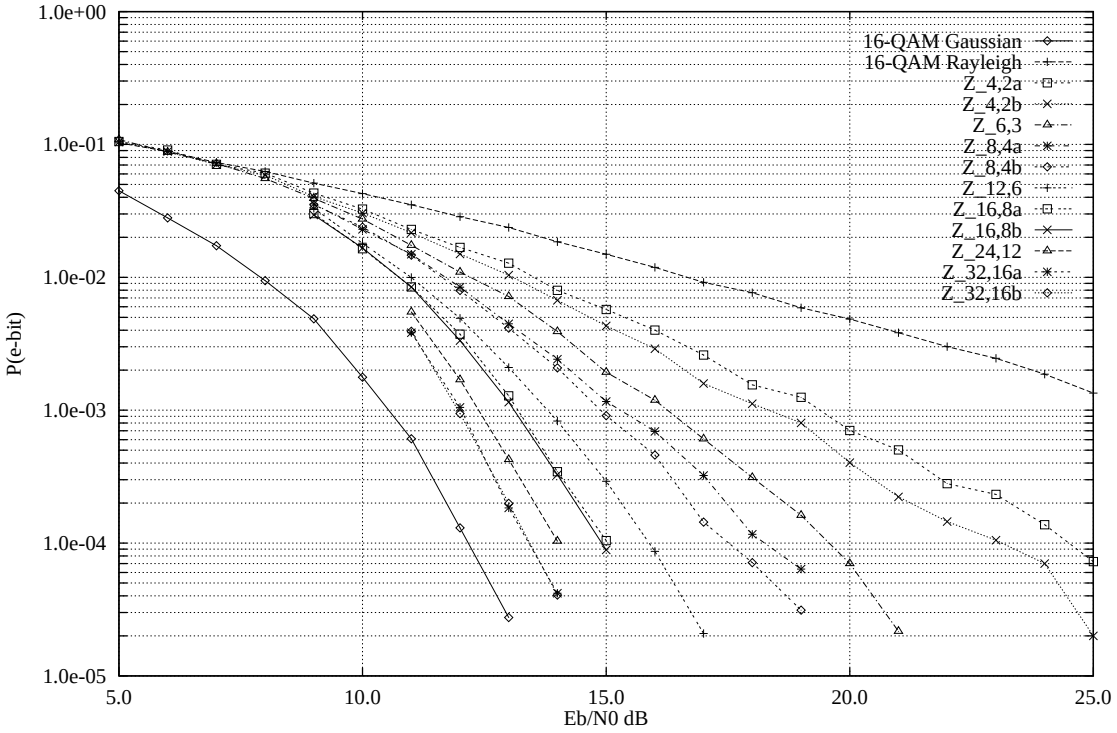


Figure 5.10: Bit error rates for the family of $Z_{n,n/2}$ constellations ($\eta = 4$)

5.7 Simulation results

In this section we give a complete presentation of the performance curves of the rotated constellations that we have constructed in the previous sections.

We first consider a throughput of $\eta = 4$ bit/symbol so that we will compare the performance with a traditional 16-QAM modulation scheme. In all the figures we plot the BER curve of the 16-QAM over the Gaussian channel and over the independent Rayleigh fading channel. These two curves bound the region of potential gain over the fading channel, when the rotated multidimensional uncoded schemes are used.

The first family of curves (Fig. 5.10) corresponds to constellations in dimensions n up to 32 and diversity $L = n/2$ (Sec. 5.5.2). As the diversity increases the bit error rate curves approach the one for the Gaussian channel. For the largest value of diversity the gap to the Gaussian BER curve is only about 1.5 dB between 10^{-3} and 10^{-4}. These constellations can be easily constructed for any dimension $n = 2^{e_1}3^{e_2}$, $e_1, e_2 = 0, 1, 2 \ldots$. The only limitation in going beyond dimension 32 is the decoder complexity.

The second family of curves (Fig. 5.11) corresponds to constellations in dimensions n up to 15 and diversity $L = n$ (Sec. 5.5.3). As the diversity increases ($L = 3, 5, 9, 11, 15$) the bit error rate curves approach the one for the Gaussian channel. For the largest value of diversity the gap to the Gaussian BER curve is about 3 dB between 10^{-3} and 10^{-4}. If we compare these curves with the previous ones we observe that for similar dimensions (e.g. 15 and 16)

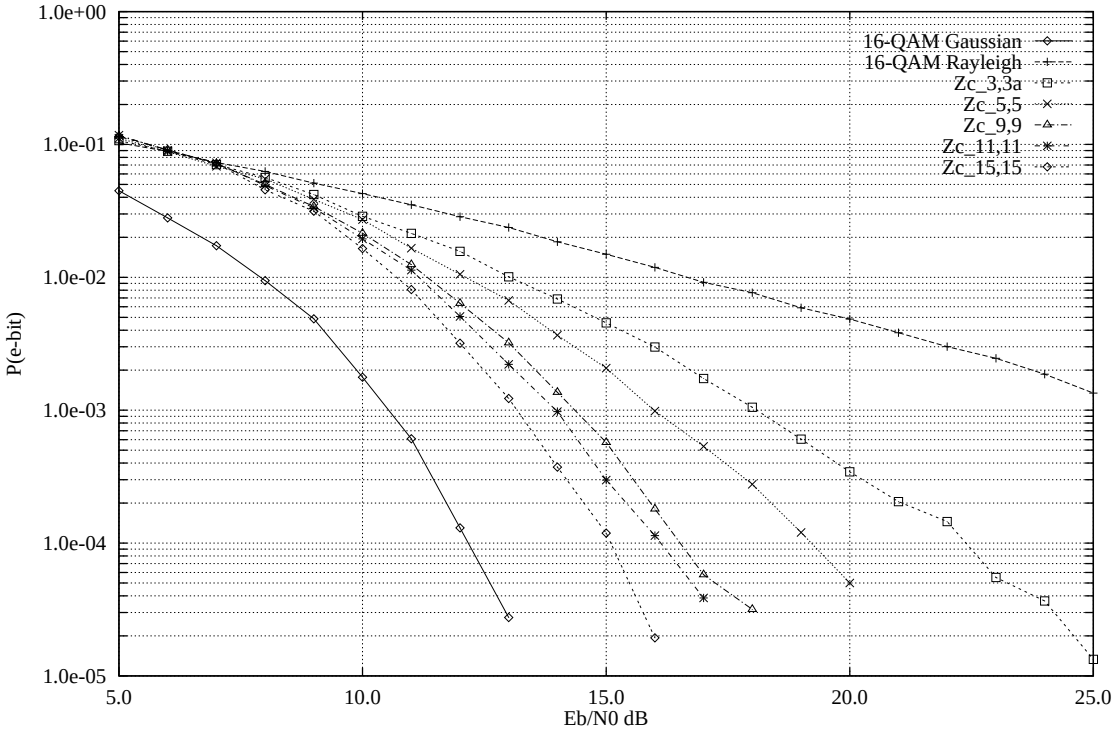


Figure 5.11: Bit error rates for the family of $Z_{n,n}$ constellations from $\mathbf{Q}(2\cos(2\pi/N))$ ($\eta = 4$)

the performance is similar. This shows that the doubling of the diversity is not sufficient to increase the performance. We have verified experimentally that for these constellations the product kissing number τ_p is much larger and we believe that this is the limiting factor to improving the performance by simply increasing the diversity.

The third family of curves (Fig. 5.12) corresponds to constellations in dimensions n up to 12 and full diversity $L = n$ (Sec. 5.6). As the diversity increases ($L = 3, 4, 6, 8, 12$) the bit error rate curves approach the one for the Gaussian channel. For the largest value of diversity the gap to the Gaussian BER curve is about 4dB between 10^{-3} and 10^{-4}. The computational complexity of finding these rotations is the limiting factor in increasing dimension. Having optimized the minimum product distance we expected a performance improvement. Unfortunately, the product kissing number is again the limiting factor. For the four-dimensional case we have plotted the curves for two distinct rotations corresponding to different values of the minimum product distance (see Section 5.6.3). In this case doubling $d_{p,min}$ only improves by a few tenths of a dB.

Finally we show in Figure 5.13 the case of $\eta = 2$ bits/symbol which can be compared to the traditional 4-PSK modulation scheme. We considered the case of $Z_{n,n/2}$ rotations. In this case the gap to the Gaussian BER curve is less than 1 dB between 10^{-3} and 10^{-4}.

This figure is also useful for comparison with the coded system proposed in [53] with 2 bits/symbol. There, a rate 1/2 trellis coded rotated 16-QAM is used and BER of 10^{-4} is achieved with $E_b/N_0 = 19$ dB. Our uncoded system provides the same performance using

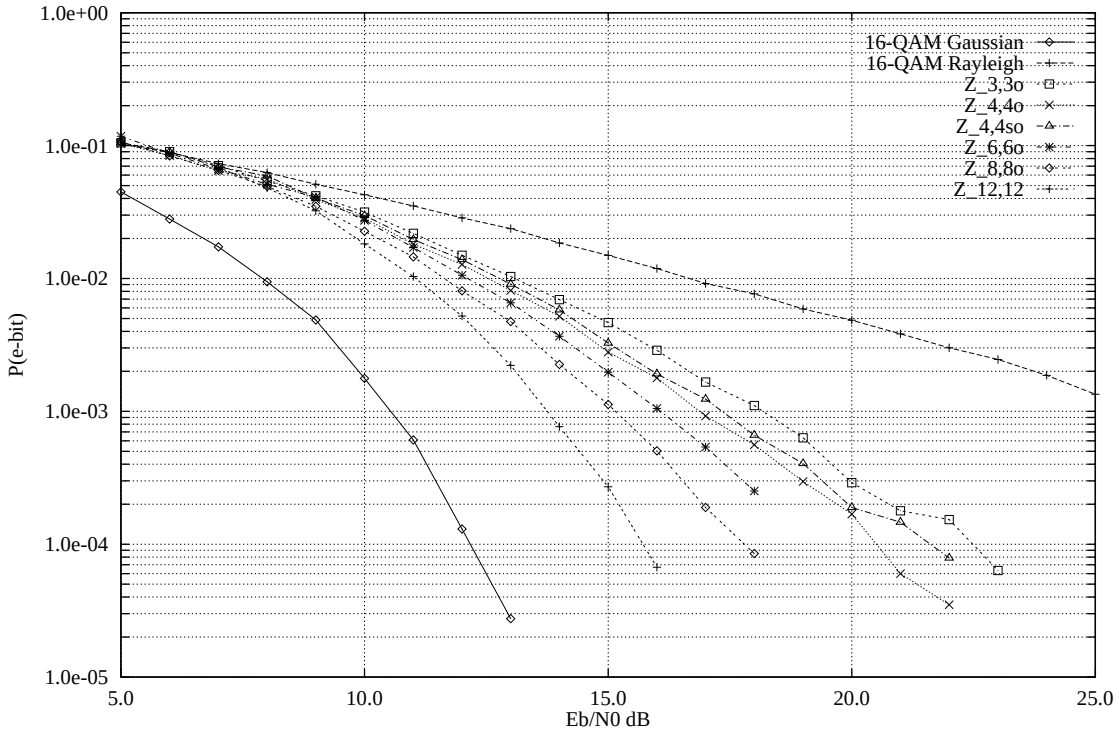


Figure 5.12: Bit error rates for the family of $Z_{n,n}$ constellations which maximize the minimum product distance ($\eta = 4$)

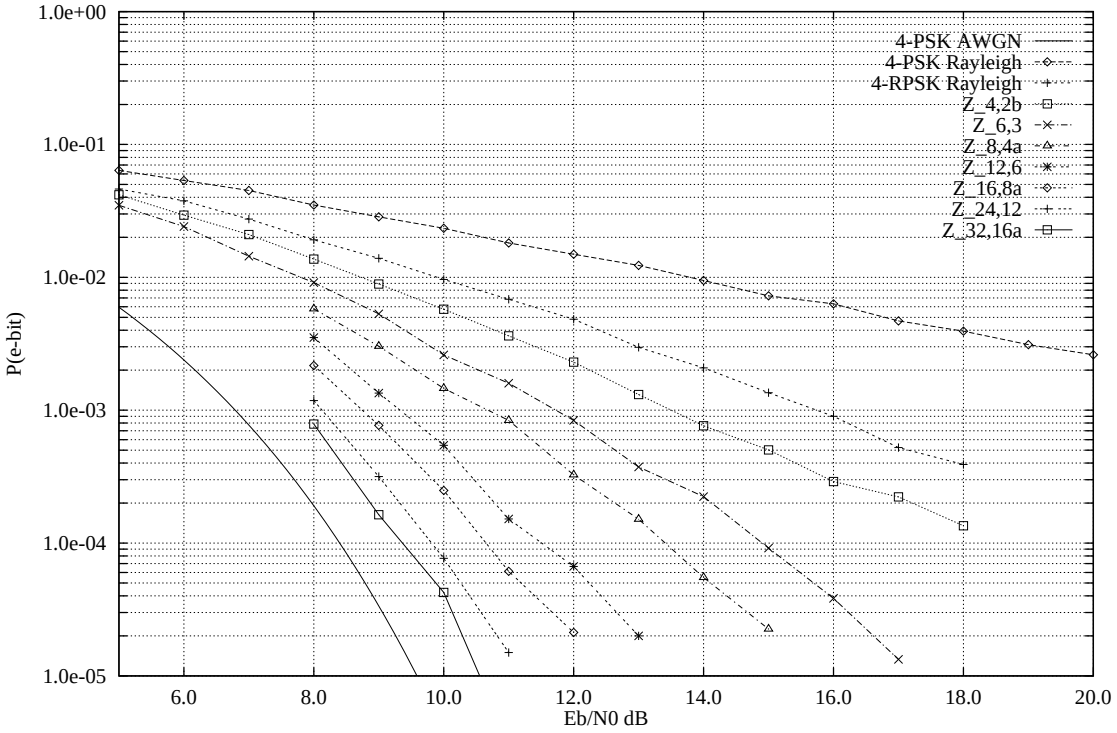


Figure 5.13: Bit error rates for the family of $Z_{n,n/2}$ constellations ($\eta = 2$)

only a four-dimensional constellation and greater gains can be obtained by increasing the dimension.

5.8 Conclusions

In this chapter we have considered a new diversity technique. We have constructed high diversity modulation schemes which exhibit an almost Gaussian performance over the fading channel.

The great advantage of this type of diversity is that it is traded only for a higher demodulator complexity. No additional power or bandwidth is required, since no type of redundancy is added.

We have verified that the diversity order L and the minimum product distance $d_{p,min}$ are not the only important design parameters. The product kissing number τ_p is also a critical design parameter. The constellation design which takes into account τ_p is still an open problem.

Using the *Universal lattice decoder* the ML detection complexity is independent of the system throughput: only increasing the number of dimensions slows down the demodulation operation.

Future developments of this work include the analysis of additional error control coding techniques, the effects of imperfect CSI estimation, performance analysis with correlated fading channels.

5.9 The minimal polynomial of $2\cos(2\pi/N)$

This appendix gives two different methods to compute the minimal polynomials $\mu(x)$ of $2\cos(2\pi/N)$ for any N.

Proof 1 – Let $m(x)$ be the minimal polynomial of $\theta = e^{2\pi j/N}$ (i.e., the cyclotomic polynomial of degree $\phi(N)$) and let $x = 2\cos(2\pi/N) = \theta + 1/\theta$ then

$$\theta^2 - x\theta + 1 = 0 \quad \text{and} \quad \theta_{1,2} = \frac{x \pm \sqrt{x^2-4}}{2}$$

We now consider the polynomial with integer coefficients $g(x) = m(\theta_1)m(\theta_2)$. This polynomial has degree $\Phi(N)$ and must contain a factor of degree $\Phi(N)/2$ which is the minimal polynomial we are looking for. This implies that $g(x) = \mu(x)^2$ so that the minimal polynomial can be obtained using Euclid's algorithm to compute the greatest common divisor between $g(x)$ and its derivative $g'(x) = 2\mu(x)\mu'(x)$.

Proof 2 – Let $m(x) = \sum_{k=0}^{n} a_k x^k$ be the minimal polynomial of $\theta = e^{2\pi j/N}$ i.e., the cyclotomic polynomial of degree $n = \phi(N)$.

Using the fact that $m(x)$ is reciprocal since it also admits θ^{-1} as a root, we can write the relation $\theta^{-n/2}m(\theta) = 0$ as

$$\sum_{k=0}^{n/2} a'_{n/2-k}(\theta^k + \theta^{-k}) = 0$$

where $a'_k = a_k$ except $a'_{n/2} = a_{n/2}/2$. Noting that $(\theta^k + \theta^{-k}) = 2\cos(2\pi k/N) = T_k(\cos 2\pi/N)$ where $T_k(x)$ is the k-th Chebychev polynomial of the first kind, we obtain

$$\mu(x) = \sum_{k=0}^{n/2} a'_{n/2-k} T_k(x) = 0 \ .$$

To show that $\mu(x)$ is the minimal polynomial of $x = 2\cos(2\pi/N)$ it is enough to show that it is irreducible. Indeed, if it were reducible, then going backwards from the relation $\mu(x) = 0$ gives a non trivial factorization of $\Phi_N(\theta)$ over $\mathbf{Q}$, which is impossible.

We can conclude that the minimal polynomial of x over $\mathbf{Q}$ is given above and has degree $n/2$.

Using the above proof it is easy to show that if N is odd, since $\Phi_{2N}(\theta) = \Phi_N(-\theta)$, $\mu_{2N}(x) = \mu_N(-x)$: the minimal polynomial for $x = \cos 2\pi/2N$ is obtained from the minimal polynomial of $x = \cos 2\pi/N$ by changing the sign of x.

Chapter 6

Conclusions et perspectives

Nous avons vu au chapitre précédent que les QAM tournées permettent de réduire presque entièrement la perte due aux évanouissements. Le comportement des performances devient quasi gaussien. Ne crions pas victoire pour autant ! Le duel entre codes en blocs et codes en treillis n'est toujours pas terminé. Il a même engendré l'affrontement entre les réseaux de points (ou les modulations codées en blocs en général) et les modulations codées en treillis (ou tout codage même pragmatique basé sur les codes convolutifs). Les combinaisons entre réseaux de points et codage en treillis [22] [24] [88] [97] ont donné encore plus d'importances à cette course de performances à moindre complexité.

Essayons d'être objectifs : les modulations codées en treillis sont très populaires, très efficaces sur les canaux gaussiens et efficaces sur les canaux de Rayleigh. Les réseaux de points sont peu populaires, mais efficaces sur les canaux gaussiens et les canaux de Rayleigh. Les réseaux de points sont plus adaptés aux transmissions par trames que les codes en treillis. De plus, les décodeurs gaussiens de réseaux de points peuvent monter à des débits inaccessibles par les codes convolutifs.

La comparaison entre bloc et convolutif s'arrête-t-elle ici ? Non puisque plusieurs découvertes récentes ont modifié le cours de la recherche en communications numériques. La nouveauté vient du décodage à sortie souple et non du décodage à entrée souple. Depuis les premiers articles sur le décodage à sortie souple [4] [7] [20] [49] [60], les codes parallèles concaténés (les Turbo-Codes) ont montré des performances imbattables sur les canaux gaussiens et d'excellentes performances sur les canaux de Rayleigh [7] [5] [6] [10] [12] [35] [59] [69].

Malgré les derniers travaux intéressants en matière de réseaux de points ou d'empilements de sphères [40] [78] [81] [82] [85] [87] [95] [94], des performances imbattables sur les canaux de Rayleigh et les canaux gaussiens peuvent être obtenues si un décodeur de réseau à sortie souple est disponible.

Ce chapitre est une synthèse de nos travaux sur les réseaux tournés avec une simple comparaison entre réseaux et PAM codées en treillis. Remarquons que l'approche classique de la théorie de l'information sur les limites des canaux de Rayleigh, comme dans l'analyse

effectuée par [19], n'a pas été utilisée ni mentionnée dans cette thèse, ceci pour réserver la place à des procédures plus techniques et plus proche de l'application. Nous espérons que, dans un avenir proche, nous allons pouvoir effectuer le décodage à sortie souple des rotations multidimensionnelles, malgré les quelques essais non concluants effectués jusqu'à maintenant. Les perspectives et quelques idées originales sont exposées au paragraphe 6.4. La Figure 6.2 est un bon récapitulatif de tous nos travaux sur les réseaux de points où le point de départ est la construction algébrique par le plongement canonique.

6.1 New Approach for Transmission over Fading Channels

New lattice constellations matched to Gaussian and fading channels have been published recently [92]. These lattices were found to be efficient on Rayleigh fading channels because they exhibit a very high diversity order $(8, 12, 16, ...)$. The same lattices have good performance on Gaussian channels due to their high density (asymptotic gain of 3.0, 4.5 or 6.0 dB). The study of these lattices led us to a new diversity technique that improves the performance on the Rayleigh fading channel without any redundancy and with no loss in performance on the Gaussian channel. This technique is simply described as a multidimensional rotation which increases the diversity order of the signal constellation.

We assume that the transmitter uses a quadrature amplitude modulation. The bidimensional QAM constellation associated to the modulation is viewed as a finite subset extracted from the integer lattice $\mathbf{Z}^2$. A point $\mathbf{p}$ in the real n-dimensional space is built by grouping $n/2$ bidimensional QAM symbols. This point $\mathbf{p}$ is rotated and its components are interleaved before being transmitted over the fading channel. The transmitted vector is $\mathbf{x} = \mathbf{Rp}$ where $\mathbf{R}$ is an $n \times n$ rotation matrix, $\mathbf{R}^t = \mathbf{R}^{-1}$). We assume that the Rayleigh channel coefficients are independent and perfectly known by the receiver.

6.2 High Diversity Rotations

The effect of the rotation matrix $\mathbf{R}$ is to spread the same information on different space axes. Thus, when deep fading occurs on one of the n axes, the information is still extracted from unfaded axes. The probabilty that a deep fading occurs at the same time on the n components is almost zero.

The most difficult problem is the search of a rotation matrix that guarantees the diversity order for any size of the QAM constellation, i.e. for any number of bits per symbol. This problem can be simplified if we look at a rotation of dimension n and diversity order L as the generator matrix of the rotated integer lattice $\mathbf{Z}_{n,L} = \mathbf{RZ}^n$. The diversity is guaranteed if the minimum Hamming distance between the lattice points is equal to L [92]. One possible solution [96] is to build the lattice $\mathbf{Z}_{n,L}$ by applying a complex canonical embedding to the ring of integers in a cyclotomic number field.

Let us define the canonical embedding and see how to compute the rotations. First, the number field $K = \mathbf{Q}(\theta)$ is defined by a minimal polynomial $\mu_\theta(x)$ of degree n whose roots are $\theta = \theta_1, \theta_2, ..., \theta_n$. It has been shown [92] that the diversity of a lattice derived from K is $L = r_1 + r_2$ where r_1 is the number of real roots and $2r_2$ is the number of complex roots $(r_1 + 2r_2 = n)$. We restrict our search to totally complex fields generated by $\theta = e^{2j\pi/N}$ (cyclotomic fields) where the lattice dimension and the root order are related by the Euler function, $n = \phi(N)$. In this case, $r_1 = 0$ and $2r_2 = n$ and so the lattice diversity is equal to half of the dimension, $L = n/2$. The canonical embedding in the field described above is defined by n isomorphisms $\sigma_i, i = 1...n$. Each isomorphism σ_i associates a distinct

n	N	$\mu_\theta(x)$
4	8	x^4+1
	12	x^4-x^2+1
8	16	x^8+1
	24	x^8-x^4+1
12	36	$x^{12}-x^6+1$
16	32	$x^{16}+1$
	48	$x^{16}-x^8+1$
24	72	$x^{24}-x^{12}+1$
32	64	$x^{32}+1$
	96	$x^{32}-x^{16}+1$

Table 6.1: $Z_{n,n/2}$ lattices from cyclotomic fields $\mathbf{Q}(e^{2j\pi/N})$.

root to the generator element, $\sigma_i(\theta)=\theta_i$. If we apply the canonical embedding to the set $1,\theta,\theta^2,...,\theta^{n/2-1}$ using $n/2$ isomorphisms out of n, we obtain an $n/2\times n/2$ complex matrix

$$R=\begin{pmatrix} \sigma_1(1) & \sigma_2(1) & \dots & \sigma_{n/2}(1) \\ \sigma_1(\theta) & \sigma_2(\theta) & \dots & \sigma_{n/2}(\theta) \\ \vdots & \vdots & & \vdots \\ \sigma_1(\theta^{n/2-1}) & \sigma_2(\theta^{n/2-1}) & \dots & \sigma_{n/2}(\theta^{n/2-1}) \end{pmatrix} \tag{6.1}$$

The matrix written above in complex form is the generator matrix of the lattice $\mathbf{Z}_{n,n/2}$ under some conditions [96]. The roots must be chosen in the following order,

$$\theta_i=\theta\times e^{4j\pi(i-1)/n}, i=1...n/2$$

and the minimal polynomial must be written as

$$\mu_\theta(x)=x^n+\epsilon x^{n/2}+1$$

where the constant ϵ takes the values 0 or -1 (see Table 6.1). The real matrix form of size $n\times n$ is obtained by splitting each complex entry into a 2×2 real matrix. As an example, for $n=24$ and $N=72$, we build a 24-dimensional rotation with diversity order equal to 12. The diversity is sufficiently high to convert the Rayleigh channel into a Gaussian channel [93]. Figure 6.1 shows the performance of the lattice $\mathbf{Z}_{24,12}$ on the Rayleigh channel for a spectral efficiency of 2 bits/dimension and the performance of the 16-QAM on the Gaussian channel.

ν	Generators in octal systematic recursive	Diversity
3	11, 02, 16	2
4	23, 12, 16	3
5	41, 52, 34	3
6	117, 52, 164	4

Table 6.2: Optimal codes for the 8-PAM modulation.

6.3 Lattices versus TCMs

Let us compare the rotated constellations to trellis coded modulations. It is obvious that rotated QAMs have no gain on the Gaussian channel. A trellis coded modulation may have a gain up to 6 dB over the Gaussian channel.

The diversity order of a TCM is equal to the minimum Hamming distance between all the possible signal sequences in the trellis. If we consider an n-dimensional TCM, its diversity L can be bounded by $n \leq L \leq n \times (\nu/k+1)$ when the trellis has 2^ν states and the convolutional encoder is of rate $k/(k+1)$. The lower bound is reached if the trellis contains parallel transitions and the upper one is reached if we found a special trellis encoder where the minimum length of a diverging path is $(\nu/k)+1$ and all the n-dimensional points are distinct.

For one dimensional TCMs, the diversity is practically limited to 6 or 7 (2048 states for 2 bits/dimension). For higher dimensions, the trellis diversity is also limited by its size, and in all dimensions higher than 4 parallel transitions are needed to reduce the number of states. In these cases the diversity is still limited by the dimension of the coded set ($L \leq 8$ if we rotate the Wei 8-dimensional TCM).

Nevertheless, for comparison reasons on the Rayleigh channel, we computed the best trellis coded 8-PAM modulations shown in Table 6.2. The 64 states 8-PAM ($L = 4$) exhibits a good performance on the Rayleigh channel. If we compare the slopes of the 8-PAM and the $\mathbf{Z}_{24,12}$ curves, it is possible to compute the signal-to-noise ratio for which the maximum diversity is reached (the curve becomes a straight line). The diversity 4 is reached by the 64 states 8-PAM at 9.4 dB and the diversity 12 by the 24-dimensional rotated QAM at 14.5 dB. Rotating the 8-dimensional Wei TCM gives a gain of 7 dB at 10^{-3} on the Rayleigh channel compared to the same TCM without rotation. The performance are identical to that of a 16-dimensional uncoded rotation and still 3 dB away from that of the Gaussian channel.

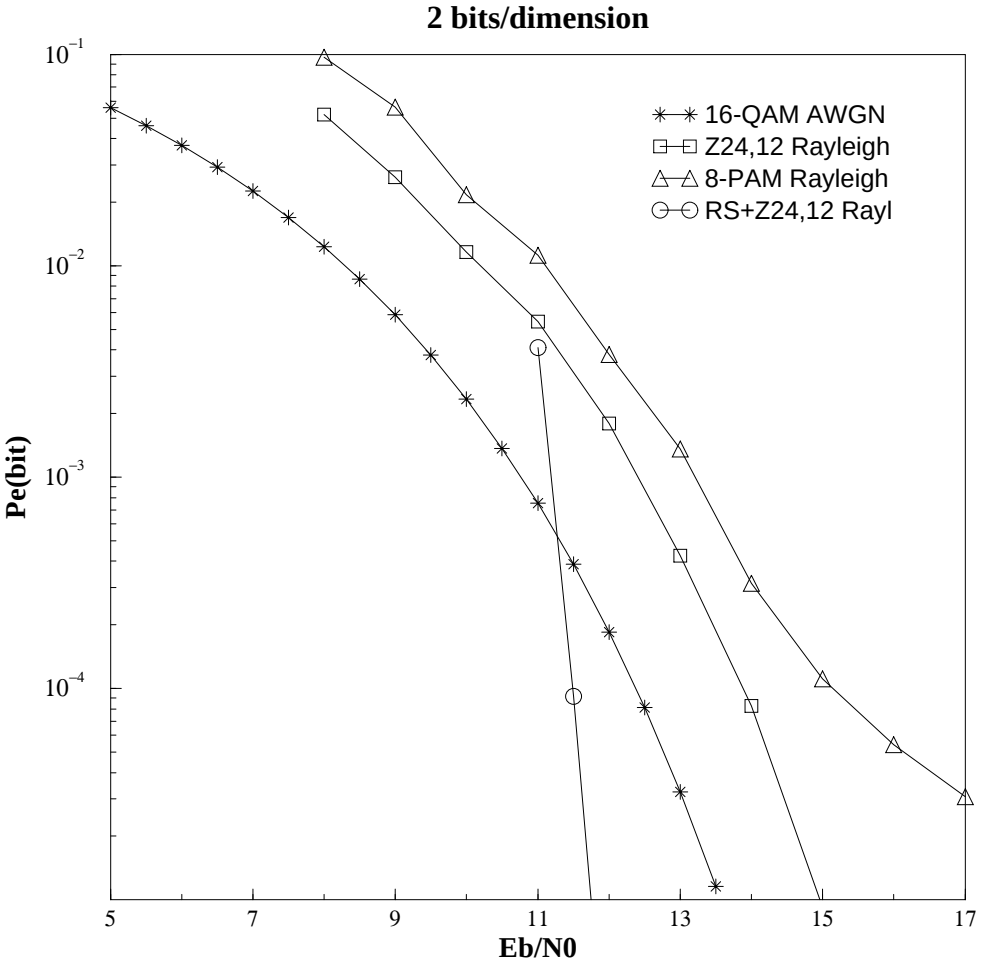


Figure 6.1: Performance over the Rayleigh channel.

6.4 Beyond the Gaussian Channel

We have seen that a high diversity rotation converts the Rayleigh channel into a Gaussian channel. Practically, with $\mathbf{Z}_{24,12}$ the performance are still 1.5 dB away. An interesting question arises : On the Rayleigh channel, how can we achieve a performance better than the Gaussian channel ?

We propose 3 different schemes. The first technique is to rotate a lattice with a positive fundamental gain, such as the Leech lattice. It is known that the Leech lattice Λ_{24} has an asymptotic gain of 6 dB on the Gaussian channel. Thus theoretically, the performance should go 6 dB beyond the Gaussian channel if we rotate Λ_{24} into $\Lambda_{24,12}$. Practically, we gain 3 or 4 dB instead of 6 because of the relatively high kissing number and the finite diversity order.

The second scheme is the rotation of a trellis coded modulation. In this scheme, the lattice decoder is combined with the Viterbi decoder and hence a soft output lattice decoder must be available.

The third scheme is the simplest one. It is possible to push the rotated lattice performance beyond the Gaussian channel by adding a high rate error control code. As an example, we concatenate the 24-dimensional rotation with a (252,220) Reed-Solomon code. As shown in Figure 6.1 the gain is 3 dB at 10^{-5}. The price to pay is a bandwidth expansion factor of 1.14 .

6.5 Conclusions

It is possible to improve the performance on the Rayleigh fading channel with a multidimensional uncoded rotation. The fading effect becomes negligible when very high diversity rotations are applied. It is even possible to go beyond the Gaussian channel with some price to pay (complexity or bandwidth expansion).

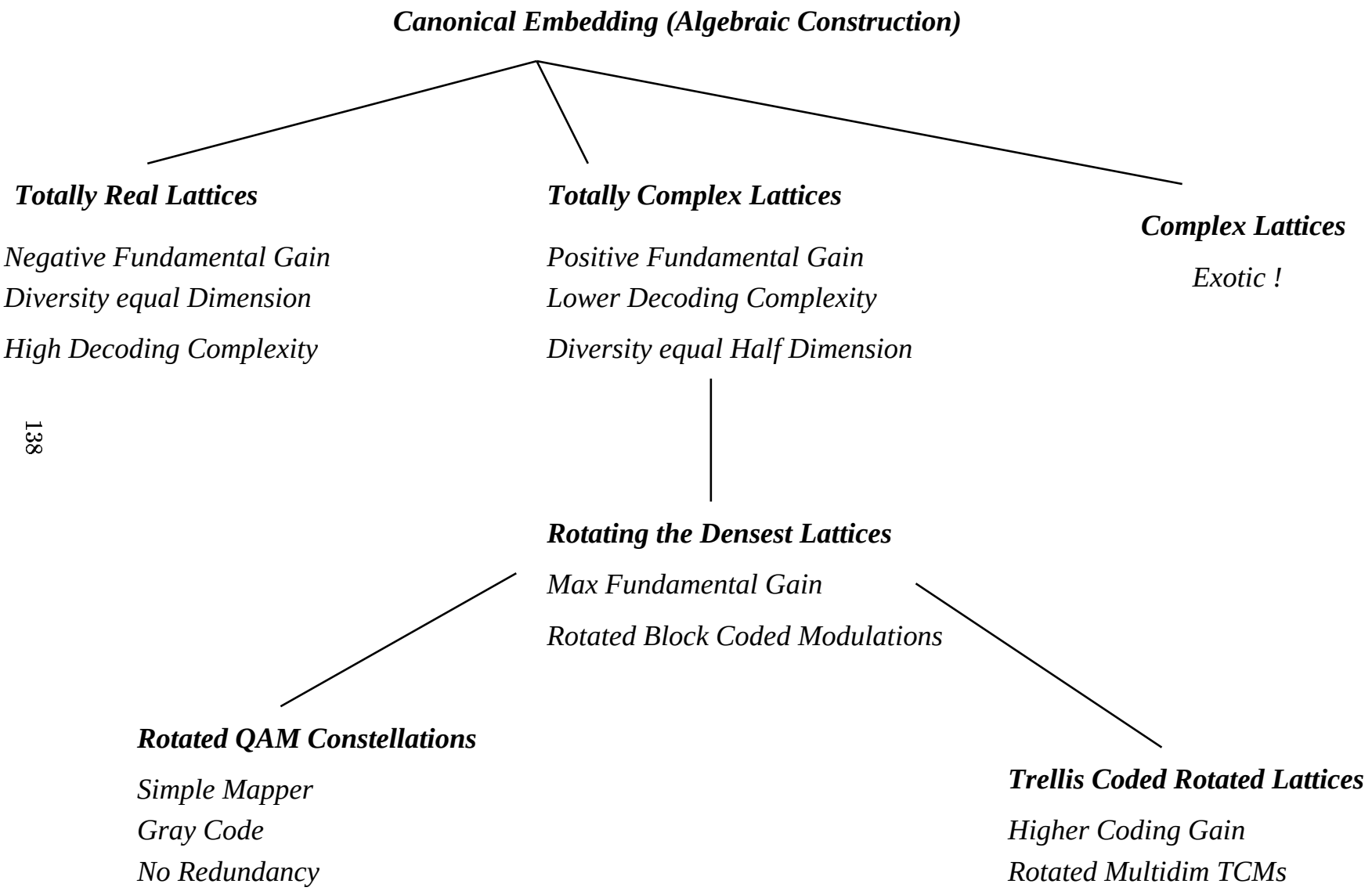


Figure 6.2: Lattices for fading channels : a brief summary.

Bibliography

[1] 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 Trans. on Information Theory*, vol. 40, pp. 1030–1043, 1994.

[2] ANSI Asymmetric Digital Subscriber Line (ADSL) Working Draft Standard, T1E1.4/94-091R4, Sept. 1994.

[3] C. Bachoc, C. Batut: "Etude algorithmique de réseaux construits avec la forme trace," Experim. Math. 1, pp. 184–190, 1992.

[4] L.R. Bahl, J. Cocke, F. Jelinek, J. Raviv: "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. on Information Theory*, vol. 20, pp. 284–287, March 1974.

[5] G. Battail: "Codage convolutif récursif pseudo aléatoire," *Annales des Télécommunications*, vol. 50, no. 9-10, pp. 779–789, 1995.

[6] G. Battail, C. Berrou, A. Glavieux: "Pseudo-random recursive convolutional coding for near-capacity performance," *Proceedings of GlobeCom'93*, Houston, pp. 23-27, 1993.

[7] G. Battail: "Pondération des symboles décodés par l'algorithme de Viterbi," *Annales des Télécommunications*, vol. 42, no. 1-2, pp. 1–8, Jan.-Feb. 1987.

[8] C. Batut, H.G. Quebbemann, R. Scharlau: "Computations of cyclotomic lattices," Sonderforschungsbereich 343, Universität Bielefeld, Preprint 1995.

[9] Y. Be'ery, B. Shahar: "Fast decoding of the Leech lattice," *IEEE. J. Select. Areas Comm.*, vol. 7, pp. 959–967, 1989.

[10] S. Benedetto, G. Montorsi: "Unveiling turbo-codes: some results on parallel concatenated coding schemes," *IEEE Trans. on Information Theory*, vol. 42, no. 2, pp. 409–428, March 1996.

[11] S. Benedetto, E. Biglieri, V. Castellani: *Digital Transmission Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1987.

[12] C. Berrou, A. Glavieux, P. Thitimajshima: "Near Shannon limit error-correcting coding and decoding : turbo-codes," *Proceedings of ICC'93*, Genève, pp. 1064-1070, Mai 1993.

[13] E. Biglieri: "Parallel demodulation of multidimensional signals," *IEEE Trans. on Communications*, vol. 40, no. 10, pp. 1581–1587, October 1992.

[14] E. Biglieri, D. Divsalar, P.J. McLane, M.K. Simon: *Introduction to trellis coded modulation with applications*, new York, Macmillan, 1991.

[15] E. Biglieri, M. Elia: "Multidimensional modulation and coding for band-limited digital channels," *IEEE Trans. on Information Theory*, vol. 34., no. 4, pp. 803–809, July 1988.

[16] A. Bonnecaze, P. Solé, A.R. Calderbank: "Quaternary quadratic residue codes and unimodular lattices," February 1994.

[17] K. Boullé, J. C. Belfiore: "Modulation scheme designed for the Rayleigh fading channel," CISS'92, Princeton, March 1992.

[18] J. Boutros: "Constellations optimales par plongement canonique", Mémoire de fin d'études, E.N.S.T. Paris, June 1992.

[19] R. Buz: "Information theoretic limits on communications over multipath fading channels with ideal and non-ideal channel state information," *Preprint March 1995*, presented in part at the IEEE International Symposium on Information Theory, Whistler, British Columbia, September 1995.

[20] G. Caire, G. Taricco, E. Biglieri: "On the Convergence of the Iterated Decoding Algorithm." *Proc. IEEE Int. Symposium on Information Theory*, Whistler, September 1995.

[21] A.R. Calderbank: "Multilevel codes and multistage decoding," *IEEE Trans. on Communications*, vol. 37, no. 3, March 1989.

[22] A.R. Calderbank, N.J.A. Sloane: "New trellis codes based on lattices and cosets," *IEEE Trans. on Information Theory*, vol. 33, no. 2, pp. 177–195, March 1987.

[23] A.R. Calderbank, N.J.A. Sloane: "An eight-dimensional trellis code," *Proceedings IEEE*, vol. 74, pp. 757–759, 1986.

[24] A.R. Calderbank, N.J.A. Sloane: "Four-dimensional modulation with an eight-state trellis code," *Bell Systems Technical Journal*, vol. 64, pp. 1005–1018, 1985.

[25] H. Cohen: *Computational algebraic number theory*, Springer Verlag 1993.

[26] J. H. Conway, N. J. Sloane: *Sphere packings, lattices and groups*, 2nd ed., 1993, Springer-Verlag, New York.

[27] J.H. Conway, N.J.A. Sloane : "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice" *IEEE Transactions on Information Theory*, vol. 32, pp. 41–50, 1986.

[28] J.H. Conway, N.J.A. Sloane : "Fast quantizing and decoding algorithms for lattice quantizers and codes" *IEEE Transactions on Information Theory*, vol. 28, no. 2, March 1982, pp. 211–226.

[29] J.H. Conway, N.J.A. Sloane : "Voronoi regions of lattices, second moments of polytopes, and quantization," *IEEE Trans. on Information Theory*, vol. 28, pp. 211–226, 1982.

[30] M.A.O. de Costa e Silva and R. Palazzo: "A bounded-distance decoding algorithm for lattices obtained from a generalized code formula," *IEEE Trans. on Information Theory*, vol. 40, pp. 2075–2082, 1994.

[31] M. Craig: "Extreme forms and cyclotomy," *Mathematika*, vol. 25, pp. 44-56, 1978.

[32] M. Craig: "A cyclotomic construction for Leech's lattice," *Mathematika*, vol. 25, pp. 236-241, 1978.

[33] F. Diaz y Diaz: "Petits discriminants des corps de nombres totalement imaginaires de degré 8," *J. of Number Theory*, vol. 25, no. 1,pp. 34–52, Jan. 1987.

[34] U. Dieter: "How to calculate shortest vectors in a lattice," *Mathematics of Computation*, vol. 29, July 1975, pp. 827–833.

[35] D. Divsalar, F. Pollara: "Turbo codes for PCS applications," *Proceedings of ICC'95*, Seattle, June 1995.

[36] D. Divsalar, M. K. Simon: "The design of trellis coded MPSK for fading channels: performance criteria," *IEEE Trans. on Communications*, vol. 36, pp. 1004–1012, Sept. 1988.

[37] J. Du, B. Vucetic: "Trellis coded 16-QAM for fading channels," *European Trans. Telecom.*, vol. 4, no. 3, pp. 335–341, May-June 1993.

[38] M.V. Eyuboglu, G.D. Forney: "Lattices and trellis quantization with lattice and trellis-bounded code-books," *IEEE Trans. on Information Theory*, vol. 39, pp. 46–59, 1993.

[39] U. Fincke, M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of computation*, vol. 44, pp. 463–471, April 1985.

[40] G.D. Forney, A. Vardy: "Generalized minimum distance decoding of Euclidean-space codes and lattices," *Preprint January 1996*, presented in part at the IEEE-IT workshop, Haifa, June 1996.

[41] G.D. Forney: "Density/length profiles and trellis complexity of lattices," *IEEE Trans. on Information Theory*, vol. 40, pp. 1753–1772, 1995.

[42] G.D. Forney: "Geometrically uniform codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1241–1260, September 1991.

[43] G. D. Forney, Jr.: "Multidimensional constellations — Part II: Voronoi constellations," *IEEE J. Select. Areas Comm.*, vol. 7, no. 4, August 1989, pp. 941–958.

[44] G. D. Forney, Jr.: "A bounded distance-decoding algorithm for the Leech lattice, with generalizations," *IEEE Transactions on Information Theory*, vol. 35, no. 4, July/August 1989, pp. 906–909.

[45] G. D. Forney: "Coset codes I: introduction and geometrical classification,", *IEEE Trans. on Information Theory*, vol. 34, pp. 1123–1151, 1988.

[46] G. D. Forney, Jr., "Coset codes — Part II: Binary lattices and related codes," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152–1187, September 1988.

[47] G. D. Forney, R.G. Gallager, G.R. Lang, F.M. Longstaff, S.U. Qureshi: "Efficient modulation for band-limited channels," *IEEE J. Select. Areas Comm.*, vol. 2, pp. 632–647, 1984.

[48] X. Giraud: "Constellations pour le canal à evanouissements", PhD thesis, E.N.S.T. Paris, May 1994.

[49] J. Hagenauer, P. Hoeher: "A Viterbi algorithm with soft-decision outputs and its applications," *Proceedings IEEE GlobeCom'89*, Dallas, Texas, pp. 47.1.1–47.1.7, Nov. 1989.

[50] H. Hasse: *Number Theory*, Springer Verlag, 1980.

[51] J. Hunter: "The minimum discriminants of quintic fields," *Proc. Glasgow Math. Assoc.*, vol. 3, pp. 57–67, 1957.

[52] H. Imai, S. Hirakawa: "Multilevel coding method using error-correcting codes," *IEEE Trans. on Information Theory*, vol. 23, pp. 371–377, 1977.

[53] B. D. Jeličić, S. Roy: "Design of a trellis coded QAM for flat fading and AWGN channels," *IEEE Trans. on Vehicular technology*, vol. 44, n. 1, Feb. 1995.

[54] A. Lafourcade, A. Vardy: "Lower bounds on trellis complexity of block codes," Preprint, April 1995.

[55] A. Lafourcade, A. Vardy: "Optimal sectionalization of a trellis," Preprint, April 1995.

[56] G.R. Lang, F.M. Longstaff: "A Leech lattice modem," *IEEE J. Select. Areas Comm.*, vol. 7, pp. 968–973, 1989.

[57] S. Lang: *Algebraic Number Fields*, Addison Wesley, 1971.

[58] J. Leech: "Notes on sphere packings," *Canadian Journal of Mathematics*, vol. 19, pp. 251–267, 1967.

[59] S. Le Goff, A. Glavieux, C, Berrou: "Turbo-codes and high spectral efficiency modulation," *Proceedings ICC'94*, New Orleans, pp. 645–649, May 1994.

[60] Y. Li, B. Vucetic, Y. Sato: "Optimum Soft-Output Detection for Channels with Intersymbol Interference," *IEEE Trans. on Information Theory*, vol. 41, no. 3, May 1995.

[61] J. Liang, H. Zassenhaus: "The minimum discriminant of sixth degree totally complex algebraic number fields," *J. of Number Theory*, vol. 9, pp. 16–35, Jan. 1977.

[62] K. Pahlavan, A.H. Levesque: *Wireless Information Networks*, Wiley Interscience, New York, 1995.

[63] A. Papoulis: *Probability, random variables, and stochastic processes*, New York, McGraw Hill, 3rd edition, 1991.

[64] S. S. Pietrobon, R.H. Deng, A. Lafanechere, G. Ungerboeck, D.J. Costello: "Trellis coded multidimensional phase modulation," *IEEE Trans. on Information Theory*, vol. 36, no. 1, pp. 63–89, Jan. 1990.

[65] V.S. Pless: "Decoding the Golay codes," *IEEE Trans. on Information Theory*, vol. 32, no. 4, pp. 561–567, 1986.

[66] M. E. Pohst: *Computational algebraic number theory*, DMV Seminar, vol. 21, Birkhäuser Verlag, 1993.

[67] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced basis with applications," *ACM SIGSAM Bulletin*, vol. 15, 1981, pp. 37–44.

[68] J.G. Proakis: *Digital Communications*, New York, McGraw Hill, 3rd edition, 1995.

[69] P. Robertson: "Illuminating the structure of code and decoder of parallel concatenated recursive systematic (turbo) codes," *Proceeeding of GlobeCom'94*, San Francisco, pp. 1298–1303, 1994.

[70] S. Sampei, T. Sunaga: "Rayleigh fading compensation for QAM in land mobile radio communications," *IEEE Trans. on Veh. Technol.*, vol. 42, no. 2, pp. 137–147, May 1993.

[71] P. Samuel: *Algebraic theory of numbers*, Paris: Hermann 1971.

[72] N. Seshadri, C-E.W. Sundberg : "Multilevel Trellis Coded Modulations for the Rayleigh Fading Channel," *IEEE Trans. on Communications*, vol. 41, no. 9, September 1993.

[73] C. Schlegel: "Trellis coded modulation on time-selective fading channels," *IEEE Trans. on Communications*, vol. 42, pp. 1617–1627, Feb/March/April 1994.

[74] C. Schlegel, D. J. Costello: "Bandwidth efficient coding for fading channels: code construction and performance analysis," *IEEE J. on Selected Areas in Communications*, vol. 7, no. 9, Dec. 1989.

[75] N.J.A. Sloane : "Tables of sphere packings and spherical codes," *IEEE Trans. on Information Theory*, vol. 27, pp. 327–338, 1981.

[76] J. Snyders, Y. Be'ery: "Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes," *IEEE Trans. on Information Theory*, vol. 35, 1989.

[77] D. Subasinghe-Dias, K. Feher: "A coded 16-QAM scheme for fast fading mobile radio channels," *IEEE Trans. Commun.*, vol. 43, no. 5, pp. 1906–1916, May 1995.

[78] F.W. Sun, H.C.A. van Tilborg: "The Leech lattice, the octacode, and decoding algorithms," *IEEE Trans. on Information Theory*, vol. 41, pp. 1097–1106, 1995.

[79] V. Tarokh: "Trellis complexity vs. the coding gain of lattice-based communication systems," *PHD Thesis*, University of Waterloo, Ontario, Canada, 1995.

[80] G. Ungerboeck: "Trellis-coded modulation with redundant signal sets, Part II," *IEEE Communications Magazine*, vol. 25, no. 2, Feb. 1987.

[81] A. Vardy: "A new sphere packing in 20 dimensions," *Inventiones mathematicae 121*, 119-133, 1995.

[82] A. Vardy: "Even more efficient bounded-distance decoding of the hexacode, the Golay code, and the Leech lattice," *IEEE Trans. on Information Theory*, vol. 41, pp. 1495–1499, 1995.

[83] A. Vardy, Y. Be'ery: "More efficient maximum likelihood decoding of the Leech lattice," *IEEE Trans. on Information Theory*, vol. 39, pp. 1435–1444, 1993.

[84] A. Vardy, Y. Be'ery: "More efficient soft decision decoding of the Golay codes," *IEEE Trans. on Information Theory*, vol. 37, pp. 667–672, 1991.

[85] E. Viterbo: "Techniche matematiche computazionali per l'analisi ed il progetto di costellazioni a reticolo," *PHD Thesis*, Politecnico di Torino, Italy, February 1995.

[86] E. Viterbo, E. Biglieri: "Computing the Voronoi cell of a lattice: The diamond-cutting algorithm," *IEEE Trans. on Information Theory*, January 1996.

[87] E. Viterbo, E. Biglieri: "A universal lattice decoder," 14^{eme} Colloque GRETSI, Juan-les-Pins, pp. 611–614, Sept. 1993.

[88] L.F. Wei: "Trellis-coded modulation with multidimensional constellations," *IEEE Trans. on Information Theory*, vol. 33, no. 4, pp. 483–501, July 1987.

[89] IEEE Working Group 802.11, P802.11-93/20b0, Update of Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, March 1994.

[90] L. Zhang, B. Vucetic: "Multilevel Block Codes for Rayleigh Fading Channels," *IEEE Trans. on Communications*, vol. 43, no. 1, January 1995.

List of Publications

[91] J. Boutros, E. Viterbo: "High diversity lattices," *Proceedings Int. Symposium on Information Theory*, Whistler, September 1995.

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

[93] J. Boutros, M. Yubero: "Converting the Rayleigh fading channel into a Gaussian channel," *Mediterranean Workshop on Coding and Information Integrity*, Palma, February 1996.

[94] J. Boutros, E. Viterbo: "Signal space diversity: a new power and bandwidth efficient diversity technique for the fading channel," submitted to *IEEE Trans. on Information Theory*, April 1996.

[95] E. Viterbo, J. Boutros: "A universal lattice code decoder for fading channels," submitted to *IEEE Trans. on Information Theory*, April 1996.

[96] J. Boutros, E. Viterbo: "Rotated Multidimensional QAM constellations", *IEEE Workshop on Information Theory*, Haifa, June 1996.

[97] J. Boutros, E. Viterbo: "Trellis coded rotated lattices,", *International Union of radio Science*, URSI-96, Lille, Août 1996.

[98] G. Battail, J. Boutros: "On communication over fading channels," *International Conference on Universal Personal Communications*, Boston, October 1996.

[99] J. Boutros, E. Viterbo: "New approach for transmission over fading channels," *International Conference on Universal Personal Communications*, Boston, October 1996.