TELECOM PARIS
école nationale supérieure des télécommunications




**Thèse**

présentée pour obtenir le grade de docteur de
l'Ecole Nationale Supérieure des Télécommunications
Spécialité : Électronique et communications

**Ghaya REKAYA-BEN OTHMAN**

# Nouvelles constructions algébriques de codes spatio-temporels atteignant le compromis "multiplexage-diversité"

Soutenue le 17 décembre 2004 devant le jury composé de

| | |
|---|---|
| Ezio Biglieri | Président |
| Giuseppe Caire<br>Mohamed Oussama Damen | Rapporteurs |
| Emanuele Viterbo<br>Olivier Rioul | Examinateurs |
| Jean-Claude Belfiore | Directeur de thèse |

*A mon mari,*

*Pour l'amour, l'attention, l'aide et le soutein qu'il m'a apporté*

*A mes parents,*

*Pour tout l'amour et l'éducation qu'ils m'ont donné*

# Remerciements

Je tiens à exprimer toute ma reconnaissance aux personnes qui m'ont aidée, encouragée, soutenue, pour mener à bien ce travail de thèse.

Je tiens à remercier tout d'abord Monsieur Ezio Biglieri, Professeur au Politecnico de Turin pour m'avoir fait l'immense honneur de présider le jury de ma thèse.

Toute ma gratitude va également à Monsieur Giuseppe Caire, Professeur à l'institut Eurecom de Sophia Antipolis qui a cordialement accepté d'être rapporteur de ce travail, et pour lequel j'éprouve le plus grand respect. Mes plus vifs remerciments s'adressent à Monsieur Mohamed Oussama Damen, Professeur Assistant à l'université de Waterloo de Canada pour sa lecture attentive de mon manuscrit, ses remarques constructives et sa grande gentillesse.

Je remercie également Monsieur Emanuele Viterbo, Professeur au Politecnico de Turin pour sa chaleureuse présence au sein du jury et pour les discussions constructives que nous avons eues ensemble. Emanuele, c'était un plaisir de travailler avec toi. Un très grand merci à Monsieur Olivier Rioul, Maître de Conférences à Télécom Paris, d'avoir accepté d'être membre du jury de ma thèse (à trois jours de la soutenance), ainsi que de sa lecture minisieuse et ses corrections du manuscrit.

Je remercie du fond du coeur mon Directeur de thèse, Monsieur Jean-Claude Belfiore, Professeur à Télécom Paris, qui m'a ouvert les portes de la recherche et m'y a donné goût pour en faire ma carrière. Merci Jean-Claude pour ton écoute, ta disponibilité, ton encadrement, tes conseils précieux et la confiance que tu as su m'accorder. Sans tes idées lunmieuses, ton expérience et ta compétence, ce travail et son aboutissement n'auraient jamais vu le jour. C'était un vrai plaisir de travailler avec toi. Je suis très contente et très fière de t'avoir eu comme Directeur de thèse, et j'espère que cette collaboration fructueuse verra sa continuité dans l'avenir.

Je ne manquerais pas d'adresser ma gratitude à Monsieur Bernard Robinet, Directeur de l'EDITE de Paris, pour tous les conseils précieux qu'il m'a donné tout au long de la thèse.

Je tiens à remercier tous les enseignants-chercheurs du département Comelec, et plus particulièrement, Cedric Ware , Joseph Boutros, Philippe Ciblat et Georges Rodriguez pour leurs écoutes et leurs aides. Un très grand merci à Chantal Cadiat, Danielle Childz et Marie Baquero pour leur aide efficace et leur patience infinie.

Merci à tous mes collégues et amis thésards. Et surtout merci à mes collégues de bureau,

avec qui j'ai passé de très bons moments que je n'oublirai jamais : Stephane, Sabine, Souheil, Ines, Nicolas et Fatma.

# Résumé

Durant ces dernières années, un grand intérêt a été accordé aux systèmes à antennes multiples à cause de leur capacité à augmenter les débits. Une multitude de codes Espace-Temps existent dans la littérature. Les codes Espace-Temps optimaux sont ceux qui satisfont les propriétés suivantes : rendement plein, ordre de diversité maximal, gain de codage optimal. Malheureusement, les meilleurs codes existants souffrent de déterminants minimaux s'évanouissant lorsque l'efficacité spectrale augmente.

Nous proposons deux nouvelles constructions de codes Espace-Temps ayant un rendement plein, une diversité pleine et des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Nous nous basons dans nos constructions sur les algèbres cycliques de division de centre $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$. Les premiers codes construits sont les "codes Quaternioniques". Il s'est avéré que la répartition non uniforme de l'énergie dans la matrice mot de code pénalise leurs performances lorsque le nombre d'antennes à l'émission augmente. Pour pallier ce problème énergétique, nous avons construit une nouvelle famille de codes Espace-Temps, appelée "codes Parfaits". Ces derniers ont une efficacité énergétique qui se traduit par une distribution énergétique uniforme au sein du mot de code et des constellations transmises ne présentant aucune perte de forme par rapport aux constellations émises. Les codes Quaternioniques et les codes Parfaits atteignent le compromis gain de multiplexage-diversité optimal.

La représentation en réseaux de points des codes Quaternioniques et des codes Parfaits permet leur décodage par les décodeurs de réseaux de points. Les décodeurs les plus connus dans la littérature sont le décodeur par sphères et le Schnorr-Euchner. Ces derniers sont utilisés pour décoder des réseaux de points infinis. Étant donné que nous considérons des constellations finies, des versions modifiées des deux algorithmes ont été proposées. La comparaison des complexités correspondants aux deux versions modifiées de ces décodeurs nous a permis de choisir le meilleur, à savoir, le Schnorr-Euchner.

Le décodage des réseaux de points peut être considérablement accéléré en utilisant une réduction de réseaux de points. A ce jour, la réduction n'est appliquée qu'aux réseaux de points infinis . L'utilisation du schéma de codage/décodage en mod-$\Lambda$ rend l'application de la réduction possible en considérant des constellations finies. Nos nouvelles constructions de codes Espace-Temps se basent sur des réseaux de points algébriques. Nous proposons dans ce sens une nouvelle réduction algébrique adaptée aux réseaux de points algébriques pour les systèmes mono-antenne sur canal à évanouissements rapides. Cette méthode sera étendue au cas des systèmes à antennes multiples dans un proche avenir.

# Abstract

A great interest has been accorded to Multi-Input Multi-Output systems due to the large capacity they can offer. A variety of Space-Time codes exists in the literature. Optimal Space-Time codes are full rate, full rank and have optimal coding gain. Unfortunately, the best existing codes suffer from vanishing determinants as spectral efficiency grows.

In our work, we propose two new constructions of Space-Time codes that are full rate, full rank and have non-vanishing determinants. Cyclic division algebras with center $\mathbb{Q}(i)$ and $\mathbb{Q}(j)$ are our essential mathematical tool for these codes' constructions. The first ones are the "Quaternionic ST codes". However, for a number of antennas larger than 2, the non-uniform energy distribution in the codeword penalizes their performances. To alleviate this problem, we have constructed a new family of codes, called "Perfect ST codes". These codes are characterized by a good energy efficiency given by an uniform energy distribution and transmitted constellations have no shaping loss compared to the signal constellation. Quaternionic and Perfect codes achieve the diversity-multiplexing tradeoff.

Quaternonic and Perfect codes are decodable by lattice decoders, Sphere Decoder and Schnorr-Euchner, by considering their lattice representations. These decoders are usually used to decode infinite lattices. As we consider finite constellations, modified versions of both decoders are proposed. By comparing their complexities, we conclude that Schnorr-Euchner is better.

Lattice reduction is used to accelerate the decoding of infinite lattices. Using the coding/decoding mod-$\Lambda$ scheme, it becomes possible to apply lattice reduction when finite constellations are considered. As algebraic lattices are used in our Space-Time codes' construction, we propose a new algebraic lattice reduction for single antenna systems on fast fading channels. The generalization of this result for MIMO systems is under investigation.

# Table des matières

**Remerciements** iii

**Résumé** v

**Abstract** vii

**Table des matières** ix

**Table des figures** xiii

**Liste des tableaux** xiv

**Liste des abréviations** xv

**Liste des notations** xvii

**Introduction** 1

**1 Préliminaires** 5
- 1.1 Présentation du schéma de transmission . . . 5
  - 1.1.1 Modulation / Démodulation . . . 6
  - 1.1.2 Canal de transmission . . . 7
  - 1.1.3 Notion de diversité . . . 8
- 1.2 Définitions et propriétés d'un réseau de points . . . 9
- 1.3 Notions et définitions d'algèbre . . . 11
  - 1.3.1 Notions de base . . . 11
  - 1.3.2 corps de nombres algébriques . . . 16
  - 1.3.3 Algèbre de division . . . 20
    - 1.3.3.1 Algèbre de division commutative (Corps d'extension) . . . 20
    - 1.3.3.2 Algèbre de division non-commutative . . . 21
    - 1.3.3.3 Algèbre cyclique de division . . . 22
    - 1.3.3.4 Algèbre de division sur un corps d'extension . . . 23
    - 1.3.3.5 Algèbre des quaternions . . . 23

**2 État de l'art des codes Espace-Temps** 25
- 2.1 Quelques résultats de la théorie de l'information . . . 25
  - 2.1.1 Cas du canal ergodique . . . 26
    - 2.1.1.1 Canal SISO . . . 26

2.1.1.2 Canal MIMO . . . 26
2.1.2 Probabilité de coupure . . . 28
2.1.3 Compromis de gain de multiplexage-diversité . . . 28
2.2 Critères de construction des codes ST . . . 30
2.3 Différentes Classes de codes ST . . . 32
2.3.1 Codes ST en Treillis . . . 32
2.3.2 Codes ST en blocs . . . 33
2.4 Codes ST orthogonaux . . . 34
2.4.1 Code d'Alamouti . . . 35
2.4.2 Généralisation du code d'Alamouti . . . 36
2.5 Codes ST par couches (layered Space Time codes - LST) . . . 38
2.5.1 V-BLAST . . . 38
2.5.2 D-BLAST . . . 39
2.5.3 "Wrapped" ST code . . . 40
2.6 Codes ST à dispersion linéaire . . . 41
2.7 Codes ST algébriques diagonaux (DAST) . . . 42
2.8 Codes ST algébriques, $n_t = n_r = T$, à rendement plein et diversité pleine . . . 43
2.8.1 Dimension $2 \times 2$ . . . 43
2.8.2 Généralisation . . . 45
2.9 Code TAST . . . 46
2.10 Codes ST algébriques à partir d'algèbres de division . . . 47
2.10.1 Codes ST à partir de corps de nombre . . . 48
2.10.1.1 Extensions cyclotomiques . . . 48
2.10.1.2 Extension à partir de nombres transcendants . . . 49
2.10.2 Codes ST à partir d'algèbres cycliques de division . . . 50
2.11 Codes ST algébriques à partir de rotations réelles . . . 52

**3 Constructions algébriques de codes Espace-Temps en blocs 55**
3.1 Première approche de construction des codes ST . . . 56
3.1.1 Critères de constructions . . . 56
3.1.2 Démarche de la construction . . . 56
3.1.3 Validation de l'approche . . . 58
3.2 Codes Quaternioniques . . . 59
3.2.1 Code quaternionique 2X2 . . . 59
3.2.2 Code quaternionique 3x3 . . . 60
3.2.3 Code quaternionique 4x4 . . . 61
3.2.4 Versions équilibrées des codes quaternioniques . . . 62
3.2.5 Performances des codes quaternioniques . . . 62
3.3 Deuxième approche de construction des codes ST . . . 64
3.3.1 Critères de construction . . . 65
3.3.2 Démarche de la construction . . . 65
3.3.3 Validation de l'approche . . . 67
3.3.3.1 Construction de versions tournées des réseaux de points... . . . 67
3.3.3.2 Déterminant minimal . . . 68
3.4 Codes ST Parfaits . . . 70
3.4.1 Existence des codes parfaits . . . 71
3.4.2 Famille infinie de codes parfaits $2 \times 2$ . . . 72
3.4.3 Code parfait 3x3 . . . 79
3.4.4 Code parfait 4x4 . . . 82

3.4.5 Code parfait 6x6 . . . 86
3.5 Compromis gain de "multiplexage-diversité" . . . 88
3.6 Codes parfaits rectangulaires . . . 91
3.6.1 Construction des codes parfaits rectangulaires . . . 92
3.6.2 Codes parfaits rectangulaires $n_t = 2$ et $T > 2$ . . . 92
3.6.3 Codes parfaits rectangulaires $n_t = 3$ et $T > n_t$ . . . 93

**4 Décodage ML des codes Espace-Temps en blocs 95**
4.1 Représentation en réseau de points des codes ST . . . 96
4.1.1 Système non-codé . . . 96
4.1.2 Système codé . . . 96
4.1.2.1 Codes ST définis sur $\mathbb{Z}[i]$ . . . 97
4.1.2.2 Codes ST définis sur $\mathbb{Z}[j]$ . . . 98
4.2 Algorithmes de décodage des réseaux de points . . . 98
4.3 Décodage des sous-parties finies de réseau par le décodeur par sphères . . . 100
4.3.1 Principe du décodeur par sphères (SD) . . . 100
4.3.2 Choix du rayon de la sphère . . . 103
4.3.3 Décodage des sous-parties finies de réseaux . . . 105
4.3.4 Organigramme du SD modifié . . . 106
4.4 Décodage des sous-parties finies de réseau par le Schnorr-Euchner . . . 108
4.4.1 Principe du Schnorr-Euchner (SE) . . . 108
4.4.2 Rayon de la sphère . . . 110
4.4.3 Décodage des sous-parties finies de réseau . . . 111
4.4.4 Organigramme du SE modifié . . . 112
4.5 Comparaison du SD et du SE . . . 114
4.5.1 Comparaison de point de vue théorique . . . 114
4.5.1.1 Stratégies de parcours . . . 114
4.5.1.2 Rayon de la sphère . . . 115
4.5.1.3 Accélération du temps de recherche . . . 115
4.5.2 Comparaison de point de vue pratique . . . 115
4.5.2.1 Complexité de la phase de prédécodage . . . 116
4.5.2.2 Complexité de la phase de recherche . . . 116
4.5.2.3 Complexité totale . . . 116

**5 Réduction des réseaux de points algébriques pour les canaux FF 119**
5.1 La réduction de réseau de points : définition et principe . . . 120
5.1.1 Définition . . . 120
5.1.2 Principe et intérêt de la réduction de réseau de points . . . 121
5.2 Schéma de Codage/décodage en mod-$\Lambda$ . . . 122
5.3 Méthodes de réduction existantes . . . 124
5.3.1 Réduction de Minkowski . . . 124
5.3.2 Réduction Korkine-Zolotareff (KZ) . . . 125
5.3.3 Réduction Lenstra, Lenstra, Lovasz (LLL) . . . 125
5.4 Nouvelle méthode de réduction : la réduction algébrique . . . 127
5.4.1 Système de transmission considéré . . . 127
5.4.2 Représentation matricielle des éléments de $K$ . . . 128
5.4.3 La réduction algébrique . . . 129
5.4.4 Le décodage du réseau logarithmique . . . 130
5.4.5 L'algorithme de la réduction algébrique . . . 131

5.5 Performances de la réduction algébrique . . . 131
5.5.1 Détection par Forçage à Zero (ZF) . . . 131
5.5.2 Réseauxde points complexe en dimension 2 . . . 132
5.5.3 Réseau de points complexe en dimension 4 . . . 133
5.5.4 Réseau de points en dimension 8 . . . 134
5.6 Comparaison de la réduction algébrique avec la réduction LLL . . . 135
5.7 Accélération des décodeurs de réseaux de points ... . . . 136

**Conclusions et Perspectives** **139**

**Annexes** **140**

**A Rappels de théorie des corps de classe** **143**
A.1 La Valuation . . . 143
A.2 Nombre $p-$adique . . . 143
A.3 Le symbole de norme de Hasse . . . 144

**B $i$ n'est pas une norme dans $\mathbb{Q}(i,\sqrt{p})/\mathbb{Q}(i)$** **147**

**C $j$ et $j^2$ ne sont pas des normes dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$** **149**
C.1 $j$ n'est pas une norme dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$ . . . 149
C.2 $j^2$ n'est pas une norme dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$ . . . 150

**D $-1$ n'est pas une norme dans $\mathbb{Q}(i,2\cos(\frac{2\pi}{15}))/\mathbb{Q}(i)$** **151**

**E $-1$ n'est pas une norme dans $\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},j)/\mathbb{Q}(j)$** **153**

**F Réduction LLL sur $\mathbb{Z}[j]$** **155**

**Bibliographie** **157**

# Table des figures


1.1 Chaîne de transmission . . . . . 6
1.2 Constellations $q$-QAM . . . . . 7
1.3 Constellations $q$-HEX . . . . . 7
1.4 Exemples de réseaux de points en dimension 2 . . . . . 11

2.1 Courbe de la DMG pour $n_t = n_r = 4$ . . . . . 29
2.2 Exemple de code ST en Treillis à 8 états . . . . . 33
2.3 Division en sous-trames et codage de chaque sous-trame . . . . . 38
2.4 Structure d'un mot de code du code V-BLAST . . . . . 38
2.5 Structure d'un mot de code du code D-BLAST . . . . . 40
2.6 Structure d'un mot de code "Wrapped" ST . . . . . 40
2.7 Répartition des couches dans un code TAST . . . . . 46

3.1 Application d'une modulation codée par bloc en sortie du codage Espace-Temps . . 55
3.2 Comparaison du code quaternionique $2 \times 2$ et du meilleure code $2 \times 2$ . . . . . 63
3.3 Comparaison du code quaternionique $3 \times 3$ et du meilleure code $3 \times 3$ . . . . . 64
3.4 Comparaison du code quaternionique $4 \times 4$ et du meilleure code $4 \times 4$ . . . . . 64
3.5 Schéma de transmission MIMO avec une répartition non uniforme de l'énergie . . . 65
3.6 Quelques déterminants de quelques codes parfaits $2 \times 2$ . . . . . 75
3.7 Constellations transmises de quelques codes parfaits $2 \times 2$ . . . . . 77
3.8 Comparaison du Golden code et des meilleurs codes $2 \times 2$ . . . . . 78
3.9 Comparaison du Golden code et de quelques codes parfaits $2 \times 2$ . . . . . 79
3.10 Comparaison du code parfait $3 \times 3$ et du meilleure code $3 \times 3$ . . . . . 82
3.11 Comparaison du code parfait $4 \times 4$ et du meilleur code $4 \times 4$ . . . . . 85
3.12 Choix du code ST en fonction des paramètres du système de transmission . . . . . 91
3.13 Comparaison des performances des codes rectangulaires avec $n_t = n_r = 2$ et $T > 2$ . . 93
3.14 Comparaison des performances des codes rectangulaires avec $n_t = n_r = 3$ et $T > 3$ . . 94

4.1 Représentation géométrique des méthodes de décodage de Pohst et de Kannan . . . 99
4.2 Transformation de la sphère en ellipse dans le nouveau repère . . . . . 101
4.3 Énumération des points du réseau de points $\mathbb{Z}^2$qui sont dans l'ellipse . . . . . 103
4.4 Réseau de points en dimension 2, dont la densité des points est plus forte sur un axe...104
4.5 Temps de recherche en secondes du SD modifié, pour $n = 8$ . . . . . 105
4.6 Décodage d'une constellation 16-QAM . . . . . 105
4.7 Organigramme du décodeur par sphères modifié . . . . . 107
4.8 Projections successives sur les hyperplans composants le réseau de points . . . . . 109
4.9 Temps de recherche en secondes du SE modifié, pour $n = 4$ . . . . . 111

4.10 Organigramme du Schnorr-Euchner modifié . . . . . 113
4.11 Exemple d'arbre de recherche du SD et du SE . . . . . 115
4.12 Comparaison des temps de recherche du SD et du SE modifiés . . . . . 117
4.13 Rapport des temps de recherche SD/SE, pour une constellation 16-QAM . . . . . 117

5.1 Exemples de bases de $\mathbb{Z}^2$ . . . . . 120
5.2 Régions de Voronoï d'un réseau de points avec et sans réduction . . . . . 122
5.3 Codage/décodage en mod-$\Lambda$ pour un canal à évanouissement rapide . . . . . 122
5.4 Décodage de réseau de points complexe en dimension 2 . . . . . 132
5.5 Décodage de réseau de points complexe en dimension 4 . . . . . 134
5.6 Décodage de réseau de points complexe en dimension 8 . . . . . 135
5.7 Temps de recherche du décodage du réseau de points en dimension 8 . . . . . 136

# Liste des tableaux

2.1 Rendements des codes orthogonaux pour différentes dimensions . . . . . 37
2.2 Gains de codage des codes $2 \times 2$ de Damen *et al.*, pour différentes valeur de $\theta$ . . . . 45

# Liste des abréviations

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

| | | |
|---|---|---|
| **AWGN** | Additive White Gaussian Noise | Bruit additif blanc gaussien |
| **FF** | Fast Fading | Évanouissement rapide |
| **SISO** | Single Input Single Output | Entrée unique sortie unique |
| **MIMO** | Multi Input Multi Output | Entrées multiples sorties multiples |
| **QAM** | Quadratique Amplitude Modulation | Modulation d'amplitude en quadratiure de phases |
| **HEX** | Hexagonale | Hexagonale |
| **BPSK** | Binary Phase shift Keying | Modulation de phase binaire |
| **PSK** | Phase shift Keying | Modulation de phase |
| **ST** | Space-Time | Espace-temps |
| **STBC** | Space-Time Block code | Code espace-temps en blocs |
| **LST** | Layered Space-Time code | Code espace temps en couches |
| **LD** | Linear Dispersion code | Code à dispersion linéaire |
| **DAST** | Diagonal Algebraic Space-Time code | Code espace-temps algébrique diagonal |
| **TAST** | Threaded Algebraic Space-Time code | Code espace-temps algébrique en couches |
| **D-MG** | Diversity-Multiplexing Gain | Gain multiplexage-diversité |
| **CQ** | Code Quaternionique | |
| **GC** | Golden Code | |
| **CP** | Code Parfait | |
| **CPR** | Code Parfait Rectangulaire | |
| **MCC** | Meilleur Code Connu | |

| | | |
|---|---|---|
| **ZF** | Zero-Forcing | Forçage à zéro |
| **MMSE** | Minimum Mean Square Error | Erreur quadratique moyenne minimale |
| **SIC** | Successive Interference Cancellation | Suppression successive d'interférence |
| **OSIC** | Ordered Successive Interference Cancellation | Suppression successive d'interférence ordonnée |
| **SD** | Sphere Decoder | Décodeur par sphères |
| **SE** | Schnorr-Euchner | Schnorr-Euchner |
| **ML** | Maximum likelihood | Maximum de vraisemblance |

| | |
|---|---|
| **RSB** | Rapport Signal sur Bruit |
| **iid** | indépendant et identiquement distribué |
| **symbole/u.c.** | Symbole par utilisation canal |

# Liste des notations

Nous avons regroupé ci-dessous les principales notations utilisées dans ce document. Les vecteurs et les matrices seront respectivement notés en minuscules gras et majuscules gras.

| | |
|---|---|
| $\mathbb{N}$ | Ensemble des entiers naturels |
| $\mathbb{Z}$ | Ensemble des entiers relatifs |
| $\mathbb{R}$ | Ensemble des réels |
| $\mathbb{C}$ | Ensemble des nombres complexes |
| $\mathbb{R}^n$ | Espace euclidien réel de dimension $n$ |
| | |
| $M_{l\times c}$ | Matrice à $l$ lignes et $c$ colonnes |
| $I_n$ | Matrice identité de dimension $n$ |
| $\text{diag}(x)$ | Matrice diagonale dont la diagonale est égale au vecteur $x$ |
| | |
| $\mathfrak{R}(x)$ | Partie réelle d'un nombre complexe $x$ |
| $\mathfrak{I}(x)$ | Partie imaginaire d'un nombre complexe $x$ |
| $x^*$ | Conjugué d'un nombre complexe $x$ |
| $x^t$ | Transposé d'un vecteur $x$ |
| $x^H$ | Transposé conjugué d'un vecteur $x$ |
| | |
| $\|\|x\|\|$ | Norme euclidienne d'un vecteur $x$ |

# Introduction

L'intégration de l'internet et des applications multimédia dans les communications sans fil implique une augmentation des débits et par la suite une augmentation de la capacité. Les principales applications en question sont : les "réseaux locaux sans fil", "l'accès radio haut débit" et les systèmes de "quatrième génération". D'un point de vue théorique, ce type d'applications inclut généralement un canal de transmission supposé quasi-statique, non sélectif en fréquence, et pour atteindre ses limites, des antennes multiples à l'émission et à la réception peuvent être utilisées. Cette solution a été approuvée par les calculs de capacité qui prouvent que la capacité d'un canal sans fil augmente linéairement en fonction du nombre minimal d'antennes entre l'émission et la réception. Le codage Espace-Temps (ST) consiste à concevoir des codes pour les systèmes radio à antennes multiples en introduisant une dépendance entre le domaine spatial et temporel dans le but d'apporter, sans sacrifier la bande passante, une diversité spatiale et un gain de codage.

Un code ST est caractérisé par son rendement, son ordre de diversité et son gain de codage. Il existe dans la littérature une multitude de codes ST dont nous citons le fameux code d'Alamouti, déjà intégré dans la norme UMTS. Le code d'Alamouti est optimal pour un système à deux antennes à l'émission et une antenne à la réception atteignant l'ordre de diversité maximal, égal à 2.

Afin d'exploiter d'une façon optimale les ressources spectrales des systèmes de transmission à antennes multiples, des codes ST ayant un rendement plein, une diversité maximale, optimisant le gain de codage ont été construits. Néanmoins, l'optimisation du gain de codage qui revient à maximiser les déterminants minimaux de la différence de deux mots de code n'est valable que pour une efficacité spectrale donnée. Malheureusement, les déterminants minimaux de ces codes s'évanouissent lorsque l'efficacité spectrale augmente. Yao et Wornell ont montré que, pour un système à 2 antennes à l'émission et à la réception, avoir un code ST ayant un déterminant minimal ne s'évanouissant pas est une condition suffisante pour atteindre le compromis gain de multiplexage-diversité optimal. Récemment, il a été démontré que sous certaines hypothèses, avoir des déterminants minimaux ne s'évanouissant pas permet d'atteindre le compromis gain de multiplexage-diversité optimal.

Dans ce travail, nous proposons de nouvelles constructions de codes ST en blocs ayant un rendement plein, une diversité maximale avec en plus des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Dans un premier temps, nous avons construit des codes ST appelés "codes Quaternioniques". Ces codes ont été les premiers codes ST à atteindre le compromis "gain de multiplexage-diversité" optimal. Les performances des codes Quaternioniques sont pénalisées par la répartition non uniforme de l'énergie au sein du

mot de code. Nous avons alors construit une nouvelle famille de codes ST, que nous avons appelés "codes Parfaits" palliant le problème énergétique des codes Quaternioniques. Afin d'augmenter les gains de codage, nous nous sommes basés sur la construction algébrique des codes Parfaits pour construire des codes parfaits rectangulaires (la longueur temporelle du code supérieure au nombre d'antenne à l'émission).

Un décodage à Maximum de Vraisemblance permet l'obtention des performances optimales des codes ST, cependant, sa complexité exponentielle rend impossible son utilisation. Par ailleurs, la représentation en réseaux de points de nos codes ST permet leur décodage par les décodeurs de réseaux de points : le décodage par sphères et le Schnorr-Euchner. Nous proposons des versions modifiées de ces décodeurs adaptées au décodage des sous-parties finies de réseaux de points.

Le décodage des réseaux de points est d'autant plus complexe que la dimension du réseau augmente. Ainsi l'utilisation d'une réduction devient nécessaire pour réduire la complexité des décodeurs. Malheureusement, avec un schéma classique de codage/décodage, la réduction de réseaux de points ne s'applique qu'aux réseaux de points infinis. Cependant il devient possible, en utilisant un schéma de codage/décodage spécifique appelé mod-$\Lambda$, d'appliquer la réduction en considérant des sous parties finies de réseaux de points. Nous proposons dans ce sens une nouvelle méthode de réduction algébrique adaptée à la réduction des réseaux de points algébriques, pour les systèmes mono-antenne sur des canaux à évanouissements rapides employant un précodage linéaire. Cette réduction permet d'obtenir la diversité maximale en employant une simple détection par forçage à zéro.

**Organisation de la thèse :**
Dans le premier chapitre nous présentons les différents paramètres de notre chaîne de transmission et les outils mathématiques indispensables à la compréhension des résultats exposés tout au long de ce mémoire. Nous commençons par une présentation détaillée des différents modules de la chaîne de transmission considérée. Nous définissons la notion de diversité et nous présentons les différents types existants. Nous définissons ensuite les réseaux de points et leurs principales caractéristiques. Nous présentons enfin les notions de base de l'algèbre qui nous seront utiles dans la suite, à savoir, corps de nombres, anneaux des entiers, réseaux logarithmiques, algèbre cyclique de division, etc...

Dans le deuxième chapitre, nous présentons un état de l'art des codes ST en blocs. Nous définissons la capacité d'un canal ergodique, la probabilité de coupure pour un canal à évanouissement par blocs et le compromis "gain de multiplexage-diversité". Nous présentons les critères de construction des codes ST, à savoir, le critère du rang, du déterminant, de l'information mutuelle et de la trace. Suit une présentation détaillée des codes ST en blocs existants dans la littérature : les codes orthogonaux, les codes en couches, les codes à dispersion linéaire, les codes algébriques, les codes construits à partir d'algèbre de division et enfin les codes construits à partir de rotations réelles.

Dans le troisième chapitre, nous proposons deux nouvelles constructions algébriques de codes ST. Nous présentons deux approches dont découle la construction des codes Quaternioniques et des codes Parfaits. Nous détaillons leurs constructions et nous étudions leurs performances. Nous clorons ce chapitre par la présentation des codes parfaits rectangulaires ainsi que leurs performances.

Dans le quatrième chapitre nous traitons le décodage des codes ST construits au chapitre III par les décodeurs de réseaux de points, décodeur par sphères (SD) et Schnorr-Euchner (SE). Nous commençons par la représentation en réseaux de points des systèmes à antennes multiples codés et non-codés. Nous détaillons ensuite le principe de la recherche du point le plus proche dans les réseaux de points et exposons les principaux travaux réalisés sur ce sujet. Par la suite, nous détaillons les algorithmes et les modifications apportées aux deux décodeurs SD et SE pour décoder des sous-parties finies de réseaux de points. Nous étudions et comparons les complexités des deux algorithmes modifiés.

Dans le cinquième chapitre nous proposons une nouvelle méthode de réduction algébrique pour les systèmes mono-antenne sur canal à évanouissements rapides employant un précodage linéaire. Nous exposons dans un premier temps l'intérêt et le principe de la réduction de réseaux de points. Nous présentons ensuite le schéma de codage/décodage en mod-$\Lambda$ nous permettant d'appliquer la réduction en considérant des sous-parties finies de réseaux de points. Après avoir fait le tour des méthodes de réduction existantes dans la littérature, nous présentons notre nouvelle méthode de réduction algébrique. Nous finissons par son application sur des réseaux de points algébriques complexes dans le but d'étudier ses performances et les comparer à celles de la réduction classique LLL.

# Chapitre 1

# Préliminaires

## Introduction

Dans ce chapitre nous exposons le cadre de notre travail et nous dressons le socle théorique des chapitres à venir. Nous définirons dans un premier temps les différents paramètres de la chaîne de transmission considérée et détaillerons ensuite, les différentes notions utilisées.

Nous nous intéressons aux systèmes de transmission à antennes multiples employant un codage Espace-Temps. Nous présenterons dans la première partie de ce chapitre la chaîne de transmission considérée et nous détaillerons les différents modules associés, à savoir, la modulation, le canal de transmission, etc. Nous définirons aussi la notion de diversité et nous présenterons les différents types existants.

Les **réseaux de points** et **la théorie algébrique des nombres** sont les principaux outils mathématiques nécessaires pour établir les résultats exposés tout au long de ce mémoire. Ainsi, nous consacrerons la deuxième partie de ce chapitre aux réseaux de points et leurs principales caractéristiques et la troisième au rappel des différentes définitions algébriques, dont la théorie des nombres algébriques et l'algèbre de division.

## 1.1 Présentation du schéma de transmission

Le schéma de transmission que nous allons considérer dans ce mémoire est un système à antennes multiples (Multi Input Multi Output - **MIMO**) employant un codage Espace-Temps (Space-Time - ST) (figure 1.1), avec $n_t$ antennes à l'émission et $n_r$ antennes à la réception. Le coefficient $h_{ij}$ représente l'évanouissement du trajet entre l'antenne émettrice $i$ et l'antenne réceptrice $j$. A la sortie de la **modulation**, les symboles d'information sont codés par le code ST, et transmis par la suite à travers un **canal de transmission**. A la réception, le décodage du code ST permet la récupération des symboles d'information, qui après **démodulation** génèrent les bits d'informations.

Le mot de code $\mathbf{X}$ est une matrice de dimension $n_t \times T$, avec $T$ la longueur temporelle du code. Chaque composante du mot de code $\mathbf{X}$ est une combinaison linéaire des symboles d'information. Le rendement du code est égal au nombre de symboles transmis par utilisation canal (symboles/uc). Nous parlerons de **code ST infini** si les symboles d'information sont pris

dans un réseaux de points et de **code ST fini** si les symboles d'information sont pris dans un alphabet fini.

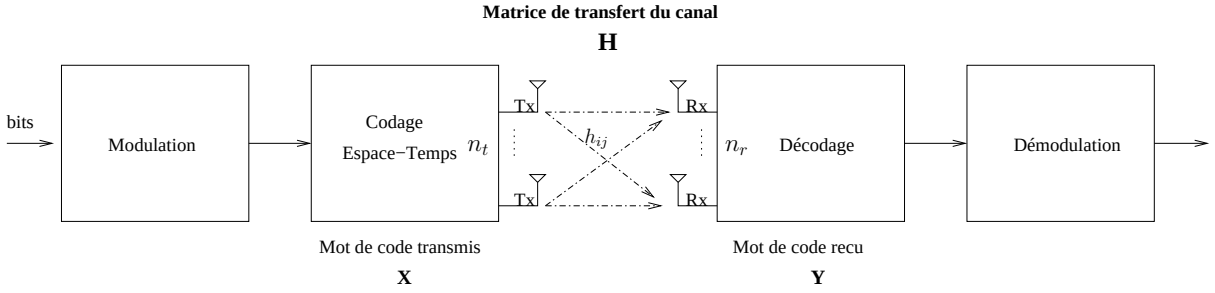



Fig. 1.1: Chaîne de transmission

Le signal reçu par chaque antenne est la superposition des signaux transmis par toutes les antennes émettrices bruité par le canal de transmission. Le mot de code reçu s'écrit alors :

$$\mathbf{Y}_{n_r \times T} = \mathbf{H}_{n_r \times n_t} \cdot \mathbf{X}_{n_t \times T} + \mathbf{W}_{n_r \times T} \tag{1.1}$$

où **H** représente la matrice de transfert du canal de transmission, et **W** le bruit additif blanc Gaussien (Additive White Gaussian Noise - AWGN ). Notons $\mathbf{M}_{r \times t}$ la matrice à $r$ lignes et $t$ colonnes.

Le système de transmission sera dit non-codé si $T = 1$. Le mot de code **x** se réduit alors à un vecteur de symboles de dimension $n_t$ et le vecteur reçu devient :

$$\mathbf{y}_{n_r} = \mathbf{H}_{n_r \times n_t} \cdot \mathbf{x}_{n_t} + \mathbf{w}_{n_r} \tag{1.2}$$

Il existe deux grandes classes de système de transmission suivant la connaissance à priori du canal de transmission au niveau du récepteur. On parle de **système cohérent**, si les coefficients du canal sont supposés être parfaitement connus au niveau du récepteur. Si les coefficients du canal sont inconnus par le récepteur, deux cas sont possibles : le premier correspond au **système non cohérent** qui utilise des techniques d'estimation des coefficients du canal de transmission, comme par exemple l'envoi de séquences d'apprentissage. Le deuxième correspond au **système différentiel** qui décode le code ST sans connaissance du canal.

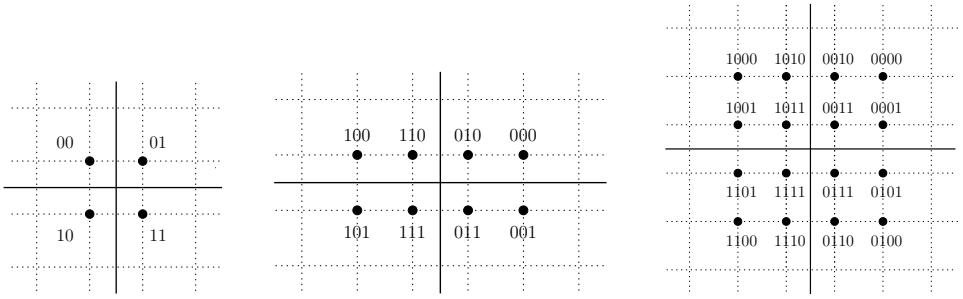
Dans ce travail, nous allons nous intéresser aux systèmes cohérents.

### 1.1.1 Modulation / Démodulation

La modulation est une opération qui consiste à étiqueter les symboles avec les bits d'information. Les deux modulations que nous allons utiliser sont la modulation $q$-QAM et la modulation hexagonale $q$-HEX.

La modulation d'amplitude en quadrature de phases (Quadrature Amplitude Modulation - QAM) est, comme son nom l'indique, une technique qui emploie une combinaison de modulation de phase et d'amplitude. Une constellation QAM est un sous-ensemble fini de $\mathbb{Z}[i]$, obtenue en considérant des points équidistants contenus dans une région donnée de $\mathbb{Z}[i]$.

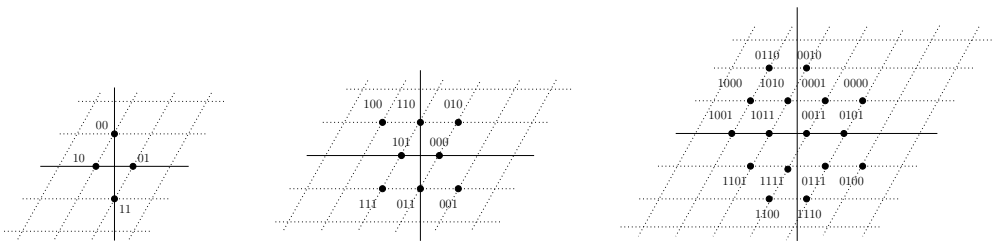
Quelques exemples de constellation $q$-QAM, avec $q$ = 4,8,16, sont présentées dans la figure 1.2. La distance minimale entre deux points adjacents de la constellation est égale à 2. Les énergies moyennes par symbole des 4,8,16 et 64-QAM sont respectivement 2,6,10 et 42.




(a) 4-QAM (b) 8-QAM (c) 16-QAM

Fig. 1.2: Constellations $q$-QAM

Les constellations hexagonales ($q$-HEX) sont des sous-ensembles finis du réseau hexagonal $A_2$, obtenue en considérant des points équidistants contenu dans une région donnée de $A_2$. Le réseau $A_2$ est le réseau le plus dense en dimension 2 et les constellations construites à partir de ce réseau sont très efficaces [1]. Les meilleures constellations hexagonales pour $q$ = 4,8,16 sont présentées dans la figure 1.3. La distance minimale entre deux points adjacents de la constellation est égale à 2. Les énergies moyennes par symbole des 4,8 et 16-HEX sont respectivement 2,4.5 et 8.75. Les constellations 4 et 8-HEX ont été centrées par une translation de 1/2 sur l'axe des abscisses et la constellation 16-HEX a été translatée de 1/4 sur l'axe des abscisses.




(a) 4-HEX (b) 8-HEX (c) 16-HEX

Fig. 1.3: Constellations $q$-HEX

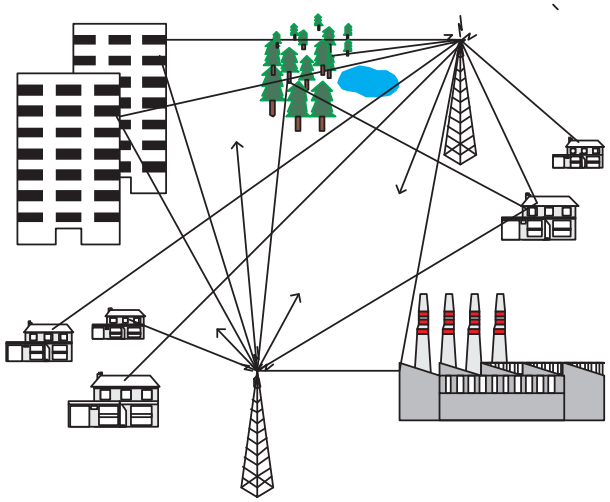
La démodulation est l'opération inverse de la modulation, en faisant l'étiquetage inverse les bits d'information sont reconstitués.

### 1.1.2 Canal de transmission

Ce qui est connu sur le canal de transmission des systèmes radio-mobiles, c'est qu'il souffre d'une limitation due au caractère aléatoire des évanouissements. Cette limitation peut être modélisée par un processus aléatoire Gaussien complexe [2]. Si la moyenne des évanouissements est nulle, alors l'enveloppe suit une loi de Rayleigh et le canal est dit **canal de Rayleigh**. C'est

le modèle de canal que nous allons considérer.

La matrice **H** du canal sera à entrées complexes gaussiennes. Chaque composante dispose d'une partie réelle et une partie imaginaire gaussienne de moyenne nulle et de variance 0.5. Si la moyenne des évanouissements n'est pas nulle le canal est dit canal de Rice.



Il existe trois types de canaux de Rayleigh classés suivant la nature de l'évanouissement.

- **Canal ergodique** - canal FF (Fast-Fading channel) : une réalisation du canal est vue à chaque temps symbole
- **Canal quasi-statique** (Quasi-static fading channel) : le canal reste constant durant la transmission d'une trame ou d'un mot de code.
- **Canal à évanouissement par blocs** (Block-fading channel) : le canal reste constant durant la transmission de $n$ trames. Si $n = 1$, on retrouve le canal quasi-statique.

Au canal de transmission s'ajoute le bruit dû aux divers rayonnements captés par les antennes, les interférences éventuelles entre utilisateurs et le bruit généré par les composants électroniques. Ce bruit est modélisé par un bruit AWGN de moyenne nulle et de variance $\sigma^2$.

Dans la suite, nous considérons comme canal de transmission, un canal de Rayleigh quasi-statique, supposé connu au niveau du récepteur (cas cohérent).

### 1.1.3 Notion de diversité

Il est évident qu'un signal transmis sur un canal radio mobile est fortement affecté par les interférences et les évanouissements liés aux obstacles et aux multi-trajets. En présence de forts évanouissements, l'envoi d'une seule réplique du signal peut être insuffisante pour décoder l'information. Pour pallier ce problème, il serait intéressant de récupérer à la réception diverses répliques du signal affectées par des évanouissements indépendants : cette technique s'appelle **diversité**. La diversité consiste à envoyer sur plusieurs voies indépendantes le même signal de façon à moyenner les évanouissements. L'ordre de diversité est égal au nombre de voies indépendantes à la réception.

Il existe différents types de diversité :

– **la diversité temporelle** : c'est l'envoi en $n$ instants différents du même signal. Les instants sont séparés d'au moins le temps de cohérence du canal afin d'assurer une bonne décorrélation des signaux. Ce type de diversité est intéressant pour les canaux ergodiques.

– **la diversité fréquentielle** : c'est l'envoi sur $n$ fréquences différentes du même signal. Les fréquences sont séparées d'au moins la bande de cohérence du canal. La diversité fréquentielle est utilisée dans les systèmes OFDM (Orthogonal Frequency Division Multiplexing).

– **la diversité d'espace en émission** : c'est l'envoi du même signal sur $n$ antennes différentes séparées d'au moins dix fois la longueur d'onde. A la réception, cette diversité est perçue comme une diversité temporelle.

Ces trois types de diversités sont coûteuses en terme d'efficacité spectrale puisqu'elles nécessitent la répétition du même signal. L'association d'un codage correcteur d'erreurs avec l'un de ces types de diversité permet d'augmenter l'efficacité spectrale, et ainsi d'éviter un gaspillage des ressources spectrales.

– **la diversité d'espace en réception** : c'est la réception du même signal sur $n$ antennes différentes séparées d'au moins dix fois la longueur d'onde. L'ordre de diversité maximal possible est égal à $n$.

– **la diversité de trajets** : c'est la réception de $n$ répliques du même signal issues de $n$ multi-trajets. Un récepteur Rake permet de décorréler les différents trajets. Cette technique est utilisée dans les système DS-CDMA (Direct séquence Code Division Multiples Access).

La combinaison de plusieurs types de diversité permet d'obtenir des ordres de diversité élevés. Elle permet de combattre plus efficacement les effets des évanouissements et augmenter, éventuellement, l'efficacité spectrale. L'ordre de diversité total est le produit des ordres de diversités particuliers.

Dans ce travail, nous allons nous intéresser à deux types de diversité, à savoir, diversité spatio-temporelle. Nous allons considérer un système à antennes multiples à l'émission et à la réception. La diversité à la réception est acquise. Il reste donc à récupérer la diversité à l'émission. Pour cela, différentes techniques de codage spatio-temporels seront utilisées.

## 1.2 Définitions et propriétés d'un réseau de points

Dans cette partie, nous allons définir la notion de "réseau de points" et nous allons expliciter quelques-uns de ses principaux paramètres utiles dans la suite.

**Définition : 1.1** *réseau de points (lattice)*
*Un **réseau de points** est un sous-groupe discret de rang $p$ , $p \leq n$ de l'espace euclidien $\mathbb{R}^n$.*

Autrement dit, un réseau de points est l'ensemble engendré par les vecteurs $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_p}$ de $\mathbb{R}^n$. Soit $\Lambda$ ce réseau de points. Un vecteur $\mathbf{v}$ appartenant à $\Lambda$, s'écrit $\mathbf{v} = a_1\mathbf{v_1} + a_2\mathbf{v_2} + \ldots + a_p\mathbf{v_p}$, avec

$a_1, a_2, \ldots, a_p \in \mathbb{Z}$. La famille de vecteurs $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_p}$ constitue une ***base du réseau de points***, de **dimension** $p$.

**Définition : 1.2** *matrice génératrice d'un réseau de points*
*Soit* $\mathbf{M}$ *la matrice dont les colonnes sont les vecteurs* $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_p}$. $\mathbf{M}$ *est la* ***matrice génératrice*** *du réseau de points. Dans la suite, un réseau de points engendré par la matrice* $\mathbf{M}$ *sera noté* $\Lambda_M$.

Soit $\mathbf{x} = (x_1, x_2, \ldots, x_n)^t$ un point de $\Lambda_M$. Il existe un vecteur $\mathbf{z} = \left(z_1, z_2, \ldots, z_p\right)^t$ de $\mathbb{Z}^p$ tel que $\mathbf{x} = \mathbf{M} \cdot \mathbf{z}$. Le réseau $\Lambda_M$ peut être vu comme une transformation linéaire appliquée au réseau $\mathbb{Z}^p$.

**Définition : 1.3** *matrice de Gram*
*La* ***matrice de Gram*** *du réseau* $\Lambda_M$ *est* $\mathbf{G} = \mathbf{M}^t \cdot \mathbf{M}$.

**Définition : 1.4** *réseau de points équivalent*
*Soit* $\mathbf{Q} \in M_n(\mathbb{R})$, *tel que* $\mathbf{Q} \cdot \mathbf{Q}^t = \mathbf{I_n}$. *Les deux réseaux de points* $\Lambda_M$ *et* $\Lambda_{M \cdot Q}$ *sont équivalents (même réseau).*

**Définition : 1.5** *volume fondamental d'un réseau de points*
*Le* ***parallélotope fondamental*** *d'un réseau de points* $\Lambda_M$ *engendré par l'ensemble des vecteurs* $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_p}$ *de* $\mathbb{R}^n$ *est la région de l'espace*

$$P = \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} = a_1\mathbf{v_1} + a_2\mathbf{v_2} + \ldots + a_p\mathbf{v_p}, 0 \leq a_i < 1, i = 1 \ldots p\}$$

*Le* ***volume fondamental du réseau*** *est le volume fondamental du parallélotope fondamental noté* $vol(\Lambda_\mathbf{M})$. *Si* $p = n$, *le volume fondamental du réseau est* $|\det(\mathbf{M})|$, *qui est aussi* $\sqrt{|\det(\mathbf{G})|}$.

**Définition : 1.6** *cellule de Voronoï*
*La* ***cellule de Voronoï*** *d'un point* $\mathbf{u}$ *d'un réseau de points* $\Lambda$ *est la région de l'espace définie par*

$$\nu(\mathbf{u}) = \{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x} - \mathbf{u}\| \leq \left\|\mathbf{x} - \mathbf{y}\right\|, \mathbf{y} \in \lambda\}$$

Le réseau de points étant géométriquement uniforme, toutes les cellules de Voronoï du réseau sont identiques. On parle alors de **cellule de Voronoï du réseau**. Le volume fondamental du réseau est égal au volume de la cellule de Voronoï.

**Définition : 1.7** *sous-réseau*
*Un* ***sous-réseau*** *d'un réseau de points* $\Lambda$ *est un sous-groupe de* $\Lambda$.

Un réseau est dit entier s'il est un sous-réseau de $\mathbb{Z}^n$. Dans la figure 1.4, nous avons tracé les réseaux de points $A_2$ et $\mathbb{Z}[i]$ avec leurs paramètres élémentaires, à savoir, une base, le parallélotope fondamental et des régions ou cellules de Voronoï.

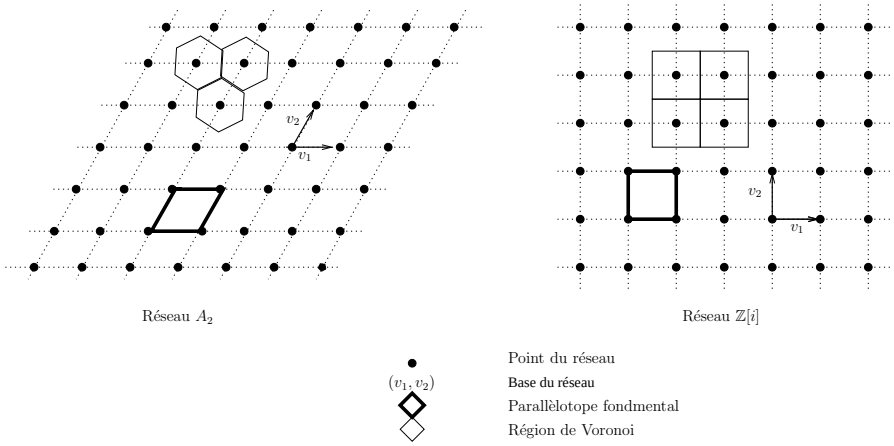



Fig. 1.4: Exemples de réseaux de points en dimension 2

## 1.3 Notions et définitions d'algèbre

Dans cette partie, nous allons rappeler quelques définitions et notions algébriques utiles pour la compréhension des résultats exposés dans ce mémoire. De plus amples détails et définitions peuvent être trouvés dans [3, 4, 5, 6, 7, 8].

Nous commencerons par un rappel des notions de base de l'algèbre. Nous définirons ensuite les corps de nombres algébriques et les notions qui s'y rapportent. Nous développerons enfin la notion d'algèbre cyclique de division et sa représentation matricielle. L'algèbre de division sera notre outil de base dans la construction des codes ST.

### 1.3.1 Notions de base

**Définition : 1.8** *: groupe*
*Un **groupe** G est un ensemble fini ou infini muni d'une loi de composition interne notée* (+) *(généralement appelée addition) vérifiant :*

1. *L'addition est associative,* $\forall\, a,b,c \in G$, $(a + b) + c = a + (b + c)$
2. *L'addition possède un élément neutre n,* $\forall\, a \in G$, $a + n = n + a = a$
3. $\forall\, a \in G$, *a possède un symétrique* $a'$, $a + a' = n$

*Le groupe G muni de sa loi sera noté* (G,+).

Soit (G,+) un groupe :

- G est ***abélien*** (ou commutatif) si sa loi de composition interne est commutative, par exemple $(\mathbb{Z},+)$ et $(\mathbb{R} - \{0\},\times)$ sont des groupes abéliens.
- H est un ***sous-groupe*** de G si $H \subset G$, H est stable par la loi de composition interne de G et H menu de cette loi est un groupe.
- G est ***fini*** s'il possède un nombre fini d'éléments. Son nombre d'éléments est appelé ordre du groupe. Soit H un sous-groupe de G, alors le card(H) divise le card(G). L'***indice*** de H dans G, noté $(G : H)$ est card(G)/card(H).

– $G$ est ***cyclique*** s'il possède un seul générateur et est fini.

**Définition : 1.9** *: anneau (ring)*
*Un **anneau** $A$ est un ensemble muni de deux lois de composition notées $(+)$ et $(\times)$, appelées généralement addition et multiplication et vérifiant :*

1. *$(A,+)$ est un groupe abélien*
2. *la multiplication est associative, $\forall\, a,b,c \in A,\ a \times (b \times c) = (a \times b) \times c$*
3. *la multiplication est distributive (à droite et à gauche) par rapport à l'addition, $\forall\, a,b,c \in A,\ a \times (b + c) = a \times b + a \times c\ (b + c) \times a = b \times a + c \times a$*

Soit $(A, +, \times)$ un anneau.
– $A$ *est* ***unitaire*** s'il possède un élément neutre pour la multiplication.
– $A$ est ***commutatif*** si la multiplication est commutative, par exemple $(\mathbb{Z}, +, \times)$ est un anneau commutatif.
– $A$ est unitaire commutatif, $A$ est alors ***intègre*** (ou sans diviseurs de zéro) si le produit de deux de ses éléments non nuls quelconques est non nul.
– ***l'anneau de polynômes*** à une variable sur $A$ sera noté $A[x]$. Si $A$ est unitaire, $A[x]$ l'est aussi. $A[x]$ est commutatif si et seulement si $A$ l'est.

**Définition : 1.10** *idéal (idéal)*
*Soit $(A, +, \times)$ un anneau commutatif. $I$ est un **idéal** de $A$ s'il est un sous-groupe additif de $(A,+)$ stable par la multiplication : $\forall\, a \in A, \forall\, b \in I,\ a \times b \in I$.*

L'exemple élémentaire d'idéal est l'idéal $n\mathbb{Z}$ de $\mathbb{Z}$, avec $n \in \mathbb{Z}$. Un idéal $I$ possède les propriétés suivantes.
– $I$ est ***premier*** si $a \times b \in I$ et si $a \notin I$ alors $b \in I$ (par exemple si $p$ est un nombre premier alors l'idéal $p\mathbb{Z}$ est premier).
– $I$ est ***irréductible*** s'il ne peut s'écrire comme intersection de deux idéaux.
– $I$ est ***principal*** si $\exists a \in A \mid I = aA = \{a \times x, x \in A\}$, en d'autres termes, l'idéal $I$ est engendré par $a$ et sera noté $(a)$.
– $I$ est ***maximal*** si $J$ est un idéal tel que $I \subset J$, alors soit $J = I$ ou $J = A$ ; en d'autres termes, s'il n'est contenu dans aucun autre idéal. Tout idéal maximal est premier.
– $I$ est ***fini*** s'il est somme d'un nombre fini d'idéaux principaux, est donc engendré par un nombre fini d'éléments.

Il existe plusieurs types d'anneaux dépendants des propriétés de leurs idéaux. On peut citer comme exemples, l'anneau principal, l'anneau noethérien et l'anneau de Dedekind, que nous définissons dans la suite.
– Un anneau $A$ est ***principal*** s'il est intègre et si tout idéal de $A$ est principal.
– Un anneau commutatif dont tout idéal est fini est dit ***noethérien***.
– Un anneau $A$ est ***de Dedekind*** si il est intègre et noethérien et si tout idéal premier non nul de $A$ est maximal. Tout anneau principal est un anneau de Dedekind.
– Soit $A$ un anneau de Dedekind, alors tout idéal dans $A$ se factorise d'une façon unique comme produit d'idéaux premiers (maximaux) de $A$ .
– Soit $I$ un idéal premier de $A$, alors $I = \prod_{l=1}^{q} b_l^{e_l}$ avec $b_l$, $l = 1 \ldots q$ sont des idéaux premiers de $A$. Les $e_l$, $l = 1 \ldots q$ s'appellent **indices de ramification**. On dit que $I$ se ramifie dans $A$ si l'un des indices de ramification est supérieur ou égal à 2.

– Soit $A$ un anneau de Dedekind, tout idéal dans $A$ est engendré par au maximum deux éléments.

**Définition : 1.11** *homomorphisme d'anneaux*
*Soient deux anneaux A et B, d'éléments unités respectifs e et e'. Un homomorphisme $f$ est une application de A dans B vérifiant, pour $a, b \in A$,*

$$\begin{aligned} f(a+b) &= f(a)+f(b) \\ f(ab) &= f(a)f(b) \\ f(e) &= e' \end{aligned}$$

**Définition : 1.12** *corps (skew field)*
*Un **corps** est un anneau dans lequel tout élément non nul admet un symétrique (inverse) pour la multiplication. Un corps est un anneau intègre. Si la multiplication est commutative, le corps est **commutatif**.*

Le terme anglais "field" correspond à corps commutatif.

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps commutatifs, tels que $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Les seuls idéaux d'un corps sont l'idéal nul (0) et le corps tout entier. Réciproquement si $A$ est un anneau ayant comme seuls idéaux l'idéal nul et lui même, alors $A$ est un corps.

**Définition : 1.13** *nombre algébrique*
*Un nombre (réel ou complexe) est dit **algébrique** s'il est solution d'une équation polynômiale du type $P(x) = ax^n + bx^{n-1} + \ldots + cx + p = 0$ avec $a,b,\ldots,c,p \in \mathbb{Z}$. On parle d'**entier algébrique** lorsque le polynôme P est unitaire (i.e. le coefficient du monôme de plus haut degré est égal à 1). Un nombre non algébrique est dit **transcendant**.*

Plus généralement, si $B$ est un sous-anneau d'un anneau commutatif $A$, un élément $x$ de $A$ est dit algébrique sur $B$ s'il existe un polynôme à coefficients dans $B$ dont $x$ est solution. Si le polynôme est unitaire, alors $x$ est dit entier algébrique sur $B$.

Soit $K$ un corps, $K[x]$ est l'anneau des polynômes en l'indéterminé $x$ et à coefficients dans $K$.

**Définition : 1.14** *polynôme minimal*
*Soit K un corps et soit $\theta$ un nombre algébrique sur K. Il existe un unique polynôme irréductible unitaire $\mu_\theta(x) \in K[x]$, ayant $\theta$ comme racine : c'est le **polynôme minimal** de $\theta$ sur K. Le degré de $\theta$ sur K est le degré de son polynôme minimal. Les racines de $\mu_\theta(x)$ sont appelées les conjugués de $\theta$.*

Le complexe $i$ est un entier algébrique de degré 2 dans $\mathbb{Q}$ car il est solution de l'équation $x^2+1=0$. Son conjugué est $-i$. De même $\sqrt{5}$ est un entier algébrique de degré 2 dans $\mathbb{Q}$ puisque il est solution (positive) de l'équation $x^2-5=0$. Son conjugué est $-\sqrt{5}$. Les racines de l'unité, $\zeta_n = e^{2i\pi/n}$, sont des entiers algébriques, de degré $\varphi(n)$ dans $\mathbb{Q}$, $\varphi(\cdot)$ est la fonction d'Euler ($\varphi(n)$ est égale au nombre d'entiers compris entre 1 et $n-1$ et premiers avec $n$). Les conjugués de $\zeta_n$ sont $\zeta_n \cdot e^{4i\pi(l-1)/n}$, $l = 1 \ldots \varphi(n) - 1$. $e$, $e^i$et $\pi$ sont des nombres transcendants.

**Définition : 1.15** *extension de corps*
*Un corps L est une* ***extension d'un corps*** *K si L contient K comme sous-corps.*

**Définition : 1.16** *Extension algébrique simple*
*Soit K un corps et soit $\theta$ algébrique sur K. Si on adjoint $\theta$ à K, on obtient une extension de corps notée $K(\theta)$ ou $K(\theta)/K$. En d'autres termes $K(\theta)$ est le plus petit corps contenant K et $\theta$.*

**Proposition : 1.1** *Soit K un corps, les conditions suivantes sont équivalentes :*
- *tout élément de $K[x]$ de degré strictement supérieur à 0, a une racine dans K*
- *tout élément irréductible de $K[x]$ est de degré 1*
- *toute extension algébrique de K est finie de degré 1 sur K (c'est à dire égale à K).*

**Définition : 1.17** *corps algébriquement clos*
*Un corps K est* ***algébriquement clos*** *s'il vérifie les conditions de la proposition 1.1.*

**Définition : 1.18** *clôture algébrique*
*Soit K une extension algébrique de L, on dit que L est une* ***clôture algébrique*** *de K si L est algébriquement clos.*

Par exemple $\mathbb{R}$ est une extension de $\mathbb{Q}$, et $\mathbb{C}$ est une extension de $\mathbb{R}$. $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

**Définition : 1.19** *espace vectoriel*
*Soit $(K, +, \times)$ un corps commutatif d'élément unité noté 1, soit $(E,+)$ un groupe abélien et soit $(\cdot) : E \times K \to E$ une loi externe sur E. $(E, +, \cdot)$ est un* ***K-espace vectoriel*** *si pour $x,y \in E$ et $a,b \in K$, la loi externe (appelée aussi multiplication scalaire) vérifie :*

1. $a \cdot (x + y) = a \cdot x + a \cdot y$
2. $(a + b) \cdot x = a \cdot x + b \cdot x$
3. $a \cdot (b \cdot x) = ab \cdot x$
4. $1 \cdot x = x$

*Les éléments de K sont appelés des scalaires, et ceux de E des vecteurs. Si K est un anneau commutatif unitaire (sans être un corps), on parle alors de* ***module*** *au lieu d'espace vectoriel.*

**Définition : 1.20** *sous-espace vectoriel*
*Soit K un corps et E un K-espace vectoriel. Soit V un sous-ensemble de E. V est un sous-espace vectoriel si $(V,+)$ est un sous-groupe de $(E,+)$ et pour $a \in K$ et $x \in V$, $a \cdot x \in V$.*

Soient $K$ un corps et $E$ un $K$-espace-vectoriel :

- si $B$ est une partie de $E$ telle que tout élément de $E$ soit combinaison linéaire d'éléments de $B$, on dit que $B$ est une **famille génératrice** de $E$ ou encore que $E$ est engendré par $B$.
- une partie $B$ de $E$ est **libre**, lorsque toute combinaison linéaire nulle d'éléments a tous ses coefficients nuls.
- une partie $B$ de $E$ est dite **base** de $E$ si et seulement si elle est à la fois libre et génératrice. Si $B$ possède un nombre fini d'éléments, on dit que $E$ est un espace vectoriel de dimension finie, égale au cardinal de $B$.
- soit $B = (e_l)_{l=1\ldots n}$ une base de $E$, alors tout élément $x$ de $E$ s'écrit de façon unique sous la forme d'une combinaison linéaire des éléments de $B$. $x = \sum_{l=1\ldots n} \lambda_l \cdot e_l$, les $\lambda_l, l = 1 \ldots n$ sont des scalaires dans $K$ appelés les coordonnées de $x$ dans la base $B$.

Contrairement aux espaces vectoriels sur les corps, un module sur un anneau n'admet pas nécessairement de base. Un module qui possède une base s'appelle un **module libre**.

Soient $K$ un corps et $L = K(\theta)$ une extension algébrique du corps $K$, $L$ peut être considérée comme un espace vectoriel sur $K$. On appelle **degré** de $L$ sur $K$, noté $[L : K]$, la dimension de cet espace vectoriel, qui est le degré du polynôme minimal de $\theta$ sur $K$. Soit $n$ le degré de $L$ sur $K$. Une base de $L$ est $(1,\theta,\theta^2 \ldots,\theta^{n-1})$.

**Définition : 1.21** *Soient E et F des K-espaces vectoriels et $f$ une application de E dans F. $f$ est une application K-linéaire si pour tout x et y dans E et tout $\alpha$ et $\beta$ dans K, $f(\alpha x + \beta y) = \alpha \cdot f(x) + \beta \cdot f(y)$. On note $\mathcal{L}(E,F)$ l'ensemble des applications linéaires de E dans F. On utilise, quand aucune confusion n'est à craindre, le mot "linéaire" à la place de "K-linéaire".*

- *Si $E = F$, $f$ est un endomorphisme. L'ensemble des endomorphismes d'un espace vectoriel E est noté $\mathcal{L}(E)$.*
- *Si $f$ est bijective, $f$ est un isomorphisme.*
- *Si $E = F$ et que $f$ est bijective alors $f$ est un automorphisme. L'ensemble des automorphismes d'un espace vectoriel est noté $GL(E)$ (Groupe linéaire de E).*

**Théorème : 1.1** *soit K un corps de caractéristique 0 (contenant $\mathbb{Z}$ comme sous-anneau et donc contenant $\mathbb{Q}$) ou fini, et soient L une extension algébrique de K de degré n, et C un corps algébriquement clos contenant K. Alors, il existe n K-isomorphismes distincts de L dans C noté $GL(L)$.*

Les conditions suivantes sont équivalentes :

1. $K$ est le corps des invariants du groupe $GL(L)$
2. pour tout $\alpha \in K$, le polynôme minimal de $\alpha$ sur $K$ a toutes ses racines dans $L$
3. $L$ est engendré par les racines d'un polynôme irréductible sur $K$

Si ces conditions sont vérifiées, alors $L$ est dite **extension galoisienne** de $K$, et $GL(L)$ est appelé **groupe de Galois** de $L$ sur $K$ noté $Gal(L/K)$. Si $Gal(L/K)$ est abélien, on dit que $L$ est une extension abélienne de $K$. Et si $Gal(L/K)$ est cyclique, on dit que $L$ est une extension cyclique de $K$.

### 1.3.2 corps de nombres algébriques

**Définition : 1.22** *corps de nombres (number field)*
*On appelle* ***corps de nombres*** *toute extension de degré fini du corps* $\mathbb{Q}$ *des rationnels.*

**Définition : 1.23** *Soit L un corps de nombres. L est aussi un* $\mathbb{Q}$*-espace vectoriel. Il existe donc un nombre algébrique* $\theta \in L$*, appelé* ***élément primitif****, de degré* $n = [L : \mathbb{Q}]$ *tel que* $L = \mathbb{Q}(\theta)$*.* $B = \{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ *est une base de* $\mathbb{Q}(\theta)$*.*

On appelle **corps quadratique** toute extension de degré 2 de $\mathbb{Q}$, et **corps cyclotomique** tout corps de nombres engendré sur $\mathbb{Q}$ par des racines de l'unité. Les corps quadratiques et les corps cyclotomiques sont des extensions galoisiennes de $\mathbb{Q}$.

Un exemple de corps quadratique est $L = \mathbb{Q}(\sqrt{5})$, engendré par la base $B = (1, \sqrt{5})$. Tout élément $x$ de $L$ s'écrit $x = a + b\sqrt{5}$, $a,b \in \mathbb{Q}$. Le polynôme minimal de $\sqrt{5}$ est $P(x) = X^2 - 5$. Les racines de $P$ sont $\sqrt{5}$ et$-\sqrt{5}$. $\mathbb{Q}(\sqrt{5})$ est une extension galoisienne de $\mathbb{Q}$.

**Définition : 1.24** *anneau des entiers (ring of integers)*
*Soit le corps de nombres* $\mathbb{Q}(\theta)$*. L'ensemble des entiers algébriques dans* $\mathbb{Q}(\theta)$ *forme un anneau appelé l'****anneau des entiers,*** *noté* $O_{\mathbb{Q}(\theta)}$*. Il est aussi un module libre de degré n sur* $\mathbb{Z}$*.*
$O_{\mathbb{Q}(\theta)}$ *est appelé aussi ordre maximal (maximal order) de* $\mathbb{Q}(\theta)$ *et tout sous-corps de* $O_{\mathbb{Q}(\theta)}$ *est appelé ordre (order) de* $\mathbb{Q}(\theta)$*.*
*Soit B une base de* $O_{\mathbb{Q}(\theta)}$ *vu comme* $\mathbb{Z}$*-module, B est appelée* ***base intégrale*** *de* $\mathbb{Q}(\theta)$*.*

L'anneau des entiers d'un corps de nombres est un anneau de Dedekind. L'anneau des entiers du corps de nombres $\mathbb{Q}(i)$ est $\mathbb{Z}[i]$, appelé anneau des entiers de Gauss (Gaussian integers). L'anneau des entiers du corps de nombres $\mathbb{Q}(j)$ est $\mathbb{Z}[j]$, appelé anneau des entiers d'Eisenstein (Eisenstein integers).

Continuons sur l'exemple précédent, la base $(1, \sqrt{5})$ n'est pas une base intégrale de $\mathbb{Q}(\sqrt{5})$ parce qu'elle engendre seulement une partie de $O_{\mathbb{Q}(\sqrt{5})}$ et pas $O_{\mathbb{Q}(\sqrt{5})}$ en entier. En effet $\frac{1+\sqrt{5}}{2}$ est un élément primitif de $\mathbb{Q}(\sqrt{5})$ ayant comme polynôme minimal $P(x) = x^2 - x - 1$. Une base intégrale de $\mathbb{Q}(\sqrt{5})$ est $\left(1, \frac{1+\sqrt{5}}{2}\right)$.L'anneau des entiers de $\mathbb{Q}(\sqrt{5})$ est $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{a + b\frac{1+\sqrt{5}}{2}, a,b \in \mathbb{Z}\right\}$.

D'une façon générale, Pour un corps de nombre quadratique $K = \mathbb{Q}(\sqrt{p})$, où $p$ est un entier qui n'est pas un carrée, alors l'anneau des entiers de $K$ est :

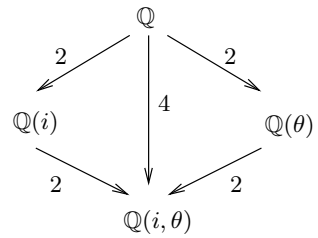
$$O_{\mathbb{Q}(\sqrt{p})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{p}}{2}\right] & \text{si } p \equiv 1 \bmod 4 \\ \mathbb{Z}\left[\sqrt{p}\right] & \text{si } p \equiv 2, 3 \bmod 4 \end{cases}$$

Si $K = \mathbb{Q}(\zeta_n)$ est une extension cyclotomique de $\mathbb{Q}$ alors l'anneau des entiers de $K$ est $O_K = \mathbb{Z}[\zeta_n] = \left\{a_0 + a_1\zeta_n + \cdots + a_{\varphi(n)-1}\zeta_n^{\varphi(n)-1}, a_i \in \mathbb{Z}\ i = 1 \ldots \varphi(n)\right\}$.

**Définition : 1.25** *Soit K un corps. Soient L une extension algébrique de K et M une extension algébrique de L. Alors, M est une extension algébrique de K. Par multiplicativité des degrés, le degré de M est* $[M : K] = [M : L][L : K]$. *Si* $(e_l)_{l\in I}$ *est une base de L sur K et* $(f_l)_{l\in J}$ *une base de M sur L, alors* $(e_l f_k)_{(l,k)\in I\times J}$ *est une base de M sur K.*

**Définition : 1.26** *corps de décomposition*
*Une extension L de K est un* ***corps de décomposition*** *du polynôme P si P est scindé sur L (i.e. tous ses facteurs irréductibles dans* $K[x]$ *sont de degré* 1*) et ses racines sont dans L qui l'engendrent comme une extension de K.*

Soient $\theta = \frac{1+\sqrt{5}}{2}$ et $\bar{\theta} = \frac{1-\sqrt{5}}{2}$. $K = \mathbb{Q}(\theta)$ et $\mathbb{Q}(i)$ sont deux extensions algébriques de $\mathbb{Q}$. Les polynômes minimaux respectifs de $\theta$ et de $i$ sont $P_1 = x^2 - x - 1 = (x-\theta)(x-\bar{\theta})$ et $P_2 = x^2 + 1 = (x-i)(x+i)$. Le polynôme $P_1$ est irréductible sur $\mathbb{Q}(i)$, et $P_2$ est irréductible sur $\mathbb{Q}(\theta)$. $L = \mathbb{Q}(i,\theta)$ est le corps de décomposition de $P_1$ sur $\mathbb{Q}(i)$ et est aussi le corps de décomposition de $P_2$ sur $\mathbb{Q}(\theta)$. $L$ est extension de $\mathbb{Q}$ de degré 4, on parle d'extension absolue, ayant comme base intégrale $B_{L/\mathbb{Q}} = (1,i,\theta,i\theta)$. $L$ est aussi une extension de $\mathbb{Q}(i)$ de degré 2, on parle d'extension relative, ayant comme base intégrale $B_{L/\mathbb{Q}(i)} = (1,\theta)$.




Nous avons défini un corps de nombres et son anneau des entiers. Nous allons maintenant définir quelques propriétés des corps de nombres tels que la signature, le discriminant et le plongement canonique.

**Définition : 1.27** *signature d'un corps de nombres*
*Soit* $L = \mathbb{Q}(\theta)$ *un corps de nombres de degré n. La* ***signature*** *de L notée* $(s,t)$ *est le nombre de racines réelles s et le nombre de paires de racines complexes conjugués t du polynôme minimal de* $\theta$*. Il en découle que* $n = s + 2t$.

D'après le théorème 1.1 il existe exactement $n$ isomorphismes distincts de $L$ dans $\mathbb{C}$, dont $s$ de $L$ dans $\mathbb{R}$ et un nombre paire $2t$ de $L$ dans $\mathbb{C}$.

On parle de **corps de nombres totalement réel** si $t = 0$. Par exemple $\mathbb{Q}(\sqrt{5})$ a comme signature (2,0). On parle de **corps de nombres totalement complexe** si $s = 0$. Par exemple $\mathbb{Q}(i)$ a comme signature (0,1).

**Définition : 1.28** *Soit* $L = \mathbb{Q}(\theta)$ *un corps de nombres de degré n, et soient* $\theta_k$, $k = 1 \ldots n$ *les conjugués de* $\theta$*. Il existe exactement n isomorphismes* $\sigma_k$, $k = 1 \ldots n$ *distincts de K dans* $\mathbb{C}$.

$$x = \sum_{l=0}^{n-1} x_l \theta^l \longmapsto \sigma_k(x) = \sum_{l=0}^{n-1} x_l \theta_k^l$$

*Ces isomorphismes préservent les propriétés algébriques de K. Ils sont appelés aussi des plongements de K dans* $\mathbb{C}$.

**Définition : 1.29** *plongement canonique (canonical embedement)*
*Le* ***plongement canonique*** *de L dans* $\mathbb{R}^s \times \mathbb{C}^t$ *est l'homomorphisme défini par :*

$$\begin{array}{rcl} \sigma : & L & \longmapsto \mathbb{R}^s \times \mathbb{C}^t \\ & x & \longrightarrow (\sigma_1(x), \sigma_2(x), \ldots, \sigma_{s+t}(x)) \end{array}$$

*En identifiant* $\mathbb{R}^s \times \mathbb{C}^t$ *à* $\mathbb{R}^n$*, les coordonnées de* $\sigma(x)$ *dans la base canonique de* $\mathbb{R}$ *sont*

$$(\sigma_1(x), \ldots, \sigma_s(x), \Re(\sigma_{s+1}(x)), \Im(\sigma_{s+1}(x)), \ldots, \Re(\sigma_{s+t}(x)), \Im(\sigma_{s+t}(x)))$$

$\Re(x)$ *et* $\Im(x)$ *sont respectivement la partie réelle et la partie imaginaire de x.*

Continuons sur le même exemple ou $K = \mathbb{Q}(\theta)$, avec $\theta = \frac{1+\sqrt{5}}{2}$. Les deux isomorphismes de $K$ dans $\mathbb{C}$ sont :

$$\begin{array}{rcl} \sigma_1(\theta) & = & \theta \\ \sigma_2(\theta) & = & \bar{\theta} \end{array}$$

Le plongement canonique de $K$ dans $\mathbb{R}^2$est :

$$\begin{array}{rcl} \sigma : & K & \longmapsto \mathbb{R}^2 \\ & x & \longrightarrow (\sigma_1(x), \sigma_2(x)) \end{array}$$

**Définition : 1.30** *Soit* $L = \mathbb{Q}(\theta)$ *un corps de nombres de degré n et* $(\theta^{l-1})_{l=1\ldots n}$ *une base de L sur* $\mathbb{Q}$*, x, y* $\in L$ *et a* $\in \mathbb{Q}$

- *le* ***discriminant*** *de L sur* $\mathbb{Q}$ *est* $d_L = \det\left(((\sigma_k(\theta^{l-1}))^t_{l,k=1\ldots n} \cdot ((\sigma_k(\theta^{l-1}))_{l,k=1\ldots n}\right) \neq 0$.
- *la* ***norme algébrique*** *de x dans L est égale à* $N_{L/\mathbb{Q}}(x) = \prod_{l=1}^{n} \sigma_l(x) \in \mathbb{Q}$*. Si x est un entier algébrique alors* $N_{L/\mathbb{Q}}(x) \in \mathbb{Z}$*. On a pour x,y* $\in L$ *:*

$$\begin{array}{rcl} N_{L/\mathbb{Q}}(xy) & = & N_{L/\mathbb{Q}}(x) N_{L/\mathbb{Q}}(y) \\ N_{L/\mathbb{Q}}(a) & = & a^n \\ N_{L/\mathbb{Q}}(ax) & = & a^n N_{L/\mathbb{Q}}(x) \end{array}$$

- *la* ***trace algébrique*** *de x dans L est égale à* $Tr_{L/\mathbb{Q}}(x) = \sum_{l=1}^{n} \sigma_l(x) \in \mathbb{Q}$*. Si x est un entier algébrique alors* $Tr_{L/\mathbb{Q}}(x) \in \mathbb{Z}$*. On a pour x,y* $\in L$

$$\begin{array}{rcl} Tr_{L/\mathbb{Q}}(x+y) & = & Tr_{L/\mathbb{Q}}(x) + Tr_{L/\mathbb{Q}}(y) \\ Tr_{L/\mathbb{Q}}(ax) & = & a Tr_{L/\mathbb{Q}}(x) \\ Tr_{L/\mathbb{Q}}(a) & = & n \cdot a \end{array}$$

*S'il n'y a pas d'ambiguïté, on notera* $N_{L/\mathbb{Q}}(x) = N(x)$ *et* $Tr_{L/\mathbb{Q}}(x) = Tr(x)$.

Pour notre exemple, le discriminant de $K$ est

$$d_K = \det\left(\begin{bmatrix} 1 & \theta \\ 1 & \bar{\theta} \end{bmatrix}^t \begin{bmatrix} 1 & \theta \\ 1 & \bar{\theta} \end{bmatrix}\right) = 5$$

Soit $x \in K$, $x$ s'écrit $a + b\theta$ avec $a,b \in \mathbb{Q}$, on a

$$\begin{aligned} N_{K/\mathbb{Q}}(x) &= (a+b\theta)(a+b\bar{\theta}) = a^2 - b^2 + ab \in \mathbb{Q} \\ Tr_{L/\mathbb{Q}}(X) &= (a+b\theta) + (a+b\bar{\theta}) = 2a + b \in Q \end{aligned}$$

Des réseaux de points peuvent être construits à partir de corps de nombres et plus précisément à partir des anneaux des entiers des corps de nombres.

**Définition : 1.31** *Soient $L$ un corps de nombres de degré $n$, $\mathcal{O}_L$ l'anneau des entiers de $L$ et $I$ un idéal de $\mathcal{O}_L$. On appelle norme de $I$, notée $N_{L/\mathbb{Q}}(I)$, l'indice de $I$ dans $\mathcal{O}_L$ (card($\mathcal{O}_L$)/card($I$)). Si $I$ est principal, $I = (a)$ avec $a \in \mathcal{O}_L$, alors la norme de $I$ est égale à $\left|N_{L/\mathbb{Q}}(a)\right|$.*

**Définition : 1.32** *Soit $L$ un corps de nombres, si $M$ est un sous-$\mathbb{Z}$-module libre de rang $n$ de $L$ et si $(e_l)_{l=1\ldots n}$ est une $\mathbb{Z}$-base de $M$, alors $\sigma(M)$ est un réseau de points de $\mathbb{R}^n$ dont le volume est $2^{-t}\left|\det(\sigma_k(e_l))_{l,k=1\ldots n}\right|$.*

D'après la définition précédente, on peut déduire que $\sigma(\mathcal{O}_L)$ et $\sigma(I)$ sont des réseaux de points de volume respectifs $2^{-t}\sqrt{|d|}$ et $2^{-t}\sqrt{|d|}N(I)$, $d$ étant le discriminant de $L$. Soit $\theta$ l'élément primitif tel que $L = \mathbb{Q}(\theta)$, $B = \{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ une base de $L$, une matrice génératrice de $\sigma(\mathcal{O}_L)$ est :

$$\mathbf{G} = \begin{bmatrix} \sigma_1(1) & \sigma_1(\theta) & \ldots & \sigma_1(\theta^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_s(1) & \sigma_s(\theta) & \ldots & \sigma_s(\theta^{n-1}) \\ \Re(\sigma_{s+1}(1)) & \Re(\sigma_{s+1}(\theta)) & \ldots & \Re(\sigma_{s+1}(\theta^{n-1})) \\ \Im(\sigma_{s+1}(1)) & \Im(\sigma_{s+1}(\theta)) & \ldots & \Im(\sigma_{s+1}(\theta^{n-1})) \\ \vdots & \vdots & \ddots & \vdots \\ \Re(\sigma_{s+t}(1)) & \Re(\sigma_{s+t}(\theta)) & \ldots & \Re(\sigma_{s+t}(\theta^{n-1})) \\ \Im(\sigma_{s+t}(1)) & \Im(\sigma_{s+t}(\theta)) & \ldots & \Im(\sigma_{s+t}(\theta^{n-1})) \end{bmatrix}$$

Reprenant notre exemple, le réseau de points $\sigma(\mathbb{O}_K)$ a pour matrice génératrice :

$$\mathbf{M} = \begin{bmatrix} 1 & \theta \\ 1 & \bar{\theta} \end{bmatrix}$$

**Définition : 1.33** *unité (unit)*
*Soit $L$ un corps de nombres de degré $n$, et soit $\mathcal{O}_L$ son anneau des entiers. On appelle **unités** de $L$ les éléments inversibles de $\mathcal{O}_L$. Ces unités forment un groupe multiplicatif $U_L$.*

1. *soit $x \in L$, si $x$ est un entier de norme algébrique $\pm 1$ alors $x$ est une unité de $L$.*

2. ***Théorème de Dirichlet*** *: Il existe $r = s + t - 1$ unités $u_l$ de L, avec $l = 1 \dots r$,* ***appelées unités fondamentales****. Toute unité u de L s'écrit de façon unique sous la forme $u = z \cdot u_1^{n_1} \dots u_r^{n_r}$, avec $n_l \in \mathbb{Z}$, $l = 1 \dots r$ et z racine de l'unité. $(u_l)_{l=1\dots r}$ est appelé* ***système d'unités fondamentales*** *de L.*
3. *On appelle* ***plongement logarithmique*** *de $L^* = L \setminus \{0\}$ dans $\mathbb{R}^{s+t}$ l'homomorphisme défini par :*

$$\begin{aligned} \sigma_{log} : \quad L^* &\longmapsto \mathbb{R}^{s+t} \\ x &\longrightarrow (\log(|\sigma_1(x)|), \dots, \log(|\sigma_{s+t}(x)|)) \end{aligned}$$

4. *$\sigma_{log}(U_L)$ est un réseau de points dans $\mathbb{R}^{s+t}$, sa matrice génératrice est :*

$$G = \begin{bmatrix} \log(|\sigma_1(u_1)|) & \log(|\sigma_1(u_2)|) & \dots & \log(|\sigma_1(u_r)|) \\ \log(|\sigma_2(u_1)|) & \log(|\sigma_2(u_2)|) & \dots & \log(|\sigma_2(u_r)|) \\ \vdots & \vdots & \ddots & \vdots \\ \log(|\sigma_{s+t}(u_1)|) & \log(|\sigma_{s+t}(u_2)|) & \dots & \log(|\sigma_{s+t}(u_r)|) \end{bmatrix}$$

Pour notre exemple il existe une seule unité fondamentale ($\theta$), le réseau logarithmique est donc de dimension 1.

### 1.3.3 Algèbre de division

**Définition : 1.34** *algèbre sur un corps*
*Soit K un corps. Une* ***algèbre*** *sur K ou encore une* ***K-algèbre*** *est un espace vectoriel V sur K muni d'une multiplication interne telle que pour tout $f \in K$ et $x,y \in \mathcal{A}$, $f(xy) = x(fy)$.*

- *L'algèbre est dite* ***commutative*** *si la multiplication est commutative. Elle est dite* ***associative*** *si la multiplication est associative.*
- *L'algèbre est dite* ***simple*** *si ses seuls idéaux à gauche et à droite sont (0) et $\mathcal{A}$.*
- *L'algèbre est dite* ***centrale*** *si son centre $\{x \in \mathcal{A} \mid \forall y \in \mathcal{A}, xy = yx\}$ est égal à K.*
- *L'algèbre est dite* ***de division*** *si tout élément non nul de $\mathcal{A}$ a un inverse pour la multiplication.*

Tout corps est une algèbre centrale de division sur lui même. L'ensemble des matrices carrées de dimension $n$ définies sur un corps $K$, noté $\mathcal{M}_n(K)$, forment une algèbre associative. L'ensemble des polynômes sur $K$, $K[x]$, forment une algèbre associative et commutative.

Il existe deux types d'algèbre de division, l'algèbre de division commutative qui correspond simplement à un corps (par exemple les corps d'extension), et l'algèbre de division non-commutative dont nous pouvons citer comme exemple les Quaternions de Hamilton.

Nous allons dans la suite donner la représentation matricielle des algèbres de division définies comme corps d'extension. Nous donnerons aussi la construction d'algèbre de division non-commutative et d'algèbre cyclique de division ainsi que leurs représentations matricielles. Les résultats exposés sont en partie dans [9].

#### 1.3.3.1 Algèbre de division commutative (Corps d'extension)

Soient $L$ un corps et $K$ une extension de $L$ de degré $n$. $K$ est un espace vectoriel de dimension $n$ sur $L$, l'ensemble des transformations linéaires de l'espace vectoriel $K$ sera noté $\mathcal{L}_L(K)$. Soit $A$

une application de $K$ dans $\mathcal{L}_L(K)$, qui associe à tout $k \in K$, la transformation linéaire $\lambda_k$ définie comme suit

$$\begin{array}{rccc} \lambda_k : & K & \to K \\ & u & \mapsto k \cdot u \end{array}$$

Nous pouvons définir une représentation matricielle des éléments de $K$. Soit $(u_1, u_2, \cdots, u_n)$ une base de $K$ et soit $\mathbf{M_i}$ la matrice correspondante à $\lambda_{u_i}$. Alors pour tout $k \in K$, $k = \sum_{i=1}^{n} l_i u_i$, la matrice correspondante à $\lambda_k$ est $\mathbf{M_k} = \sum_{i=1}^{n} l_i \mathbf{M_i}$.

Supposons qu'il existe $\theta$ tel que $K = L(\theta)$, une base de $K$ est $B = (1, \theta, \ldots, \theta^{n-1})$. Soit $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ le polynôme minimal de $\theta$. La matrice correspondante à $\lambda_\theta$ est la matrice compagnon de $P$ :

$$\mathbf{M}_\theta = \begin{bmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & \ldots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-1} \end{bmatrix}$$

Pour tout $k \in K$, la matrice correspondante à $\lambda_k$ s'écrit $\mathbf{M_k} = \sum_{i=1}^{n} l_i \mathbf{M}_\theta^{i-1}$. Le déterminant de la matrice $\mathbf{M_k}$ s'appelle norme réduite de $k$ dans $K$, et sa trace s'appelle trace réduite de $k$ dans $K$.

L'ensemble des matrices $\mathbf{M_k}$ est un plongement de $K$ dans $\mathcal{M}_n(L)$. Soient $\mathbf{M_1}$ et $\mathbf{M_2}$ deux matrices de l'ensemble des matrices $\mathbf{M_k}$. Étant donné que $K$ est une algèbre de division, alors la matrice $(\mathbf{M_1} - \mathbf{M_2})$ est de rang plein.

La représentation matricielle est définie à partir du polynôme minimal. Ainsi d'une forme plus simple du polynôme minimal découlera une représentation matricielle plus simple.

Soit $P = x^n - \gamma$ avec $n \geq 2$ et $\gamma \in L$, irréductible sur $L[X]$, alors $K = L(\sqrt[n]{\gamma}) = L(\theta)$. La matrice $\mathbf{M}_\theta$ s'écrit :

$$\begin{bmatrix} 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \gamma & 0 & \cdots & 0 \end{bmatrix}$$

Pour tout $k \in K$, $k = \sum_{i=1}^{n} l_i \theta^{i-1}$, la matrice correspondante à $\lambda_k$ s'écrit :

$$\mathbf{M_k} = \begin{bmatrix} l_1 & l_2 & \ldots & l_n \\ \gamma l_n & l_1 & \ldots & l_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma l_2 & \gamma l_3 & \ldots & l_1 \end{bmatrix}$$

#### 1.3.3.2 Algèbre de division non-commutative

Soit $L$ un corps. Définir une algèbre de division $\mathcal{A}$ sur $L$ veut dire que le **centre** de $\mathcal{A}$ est égal à $L$. $\mathcal{A}$ est un espace vectoriel sur son centre (donc sur $L$), de dimension un carré parfait, égale à $n^2$. Soit $K$ un sous-corps commutatif de $\mathcal{A}$ tel que $L \subseteq K \subseteq \mathcal{A}$. $K$ est un sous-espace vectoriel de l'espace vectoriel de $\mathcal{A}$ sur $L$, et $[K : L]$ divise $[\mathcal{A} : L]$. Le degré maximal de $K$ sur $L$ est $n$. Si

$[K : L] = n$, alors $K$ est dit **corps maximal** de $\mathcal{A}$.

Afin de définir la représentation matricielle de l'algèbre de division, nous allons définir une application $A$ de $\mathcal{A}$ dans l'ensemble des applications linéaires $\mathcal{L}_L(\mathcal{A})$, qui associe à chaque $d \in \mathcal{A}$, l'application linéaire $\lambda_d$ définie comme suit

$$\begin{array}{rccc} \lambda_d : & \mathcal{A} & \to \mathcal{A} \\ & e & \mapsto d \cdot e \end{array}$$

En utilisant le fait que le centre de $\mathcal{A}$ est $L$, il est facile de vérifier que $\lambda_d$ est une application linéaire. Nous pouvons aussi vérifier que $A$ est un homorphisme d'anneau de $\mathcal{A}$ dans $\mathcal{L}_L(\mathcal{A})$ :

1. $\lambda_{d_1+d_2}(e) = (d1 + d2) \cdot e = d_1e + d_2e = \lambda_{d_1}(e) + \lambda_{d_2}(e)$
2. $\lambda_{d_1d_2} = d_1d_2e = d_1\lambda_{d_2}(e) = \lambda_{d_1} \cdot \lambda_{d_2}(e)$
3. $\lambda_1 = 1 \cdot e = e$

Étant donné que $\mathcal{A}$ est une algèbre de division, $A$ est alors une injection. D'où la possibilité d'un plongement de $\mathcal{A}$ dans $\mathcal{M}_{n^2}(L)$. La représentation matricielle se définit de la même façon que dans le cas de l'algèbre de division commutative.

#### 1.3.3.3 Algèbre cyclique de division

**Définition : 1.35** *Une **algèbre cyclique de division** $\mathcal{A}$ sur un corps $L$ est une algèbre de division qui a un sous-corps maximal $K$, Galois sur $L$. $Gal(K/L)$ est cyclique.*

Soit $\mathcal{A}$ une algèbre cyclique de division de degré $n^2$ sur $L$, tel que $L$ soit son centre et $K/L$ son corps maximal. $Gal(K/L)$ est engendré par $\sigma$, et on a $\sigma^n = 1$. $\mathcal{A}$ est naturellement un espace vectoriel à droite sur $K$ et se décompose de la façon suivante :

$$\mathcal{A} = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K$$

avec $z \in \mathcal{A}$ vérifiant $kz = z\sigma(k)$ pour tout $k \in K$ et $z^n = \gamma$, $\gamma \in L^*$. L'algèbre cyclique de division $\mathcal{A}$ sera noté $\mathcal{A} = (K/L,\sigma,\gamma)$.

D'après la décomposition de $\mathcal{A}$ dans $K$, $(1, z, z^2, \ldots, z^{n-1})$ est une base de $\mathcal{A}$ dans $K$. Soit $d \in \mathcal{A}$, $d$ s'écrit $\sum_{i=1}^{n} z^{i-1}k_i$, $k_i \in K, i = 1 \ldots n$. Afin de construire la matrice de $\lambda_d$, il suffit de calculer les images des éléments de la base de $\mathcal{A}$ par $\lambda_d$. Par exemple :

$$\lambda_d(z) = dz = (\sum_{i=1}^{n} z^{i-1}k_i)z = z\sigma(k_1) + z^2\sigma(k_2) + \cdots + \gamma\sigma(k_n)$$

La matrice de $\lambda_d$ est alors :

$$\mathbf{M_d} = \begin{bmatrix} k_1 & k_2 & \ldots & k_n \\ \gamma\sigma(k_n) & \sigma(k_1) & \ldots & \sigma(k_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n-1}(k_2) & \gamma\sigma^{n-1}(k_3) & \ldots & \sigma^{n-1}(k_1) \end{bmatrix}$$

$K$ étant une extension cyclique de $L$, soit $\theta \in K$ tel que $K = L(\theta)$. Tout $k \in K$ s'écrit $\sum_{i=1}^{n} l_i\theta^{i-1}$, $l_i \in L$, $i = 1 \ldots n$.

Soit $k_i = \sum_{j=1}^{n} l_{i,j}\theta^{j-1}, i = 1 \dots n$ . La matrice de $\lambda_d$ devient :

$$\mathbf{M_d} = \begin{bmatrix} \sum_{i=1}^{n} l_{1,i}\theta^{i-1} & \sum_{i=1}^{n} l_{2,i}\theta^{i-1} & \cdots & \sum_{i=1}^{n} l_{n,i}\theta^{i-1} \\ \gamma\sigma(\sum_{i=1}^{n} l_{n,i}\theta^{i-1}) & \sigma(\sum_{i=1}^{n} l_{1,i}\theta^{i-1}) & \cdots & \sigma(\sum_{i=1}^{n} l_{n-1,i}\theta^{i-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n-1}(\sum_{i=1}^{n} l_{2,i}\theta^{i-1}) & \gamma\sigma^{n-1}(\sum_{i=1}^{n} l_{3,i}\theta^{i-1}) & \cdots & \sigma^{n-1}(\sum_{i=1}^{n} l_{1,i}\theta^{i-1}) \end{bmatrix}$$

Le déterminant de la matrice $\mathbf{M_d}$ s'appelle **norme réduite** de $d$ dans $\mathcal{A}$ et sa trace s'appelle **trace réduite** de $d$ dans $\mathcal{A}$.

**Théorème : 1.2** *Soit $\mathcal{A} = (K/L,\sigma,\gamma)$ une algèbre cyclique, la norme réduite d'un élément de $\mathcal{A}$ est dans $L$.*

#### 1.3.3.4 Algèbre de division sur un corps d'extension

Soit $K$ une extension cyclique d'un corps $L$ de degré $n$. $Gal(K/L)$ est engendré par $\sigma$. Soit $\gamma$ un élément non nul de $L$. Soit l'algèbre $\mathcal{A} = (K/L,\sigma,\gamma) = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K$, $z \in K$ vérifiant $kz = z\sigma(k)$ pour tout $k \in K$ et $z^n = \gamma$. Cette algèbre est cyclique, mais sa construction ne garantit pas qu'elle soit de division. Une contrainte supplémentaire est nécessaire afin qu'elle le devienne.

**Lemme : 1.1** *algèbre de division sur un corps d'extension*
*Une algèbre $\mathcal{A} = (K/L,\sigma,\gamma)$ est une **algèbre cyclique de division** si et seulement si $\gamma, \gamma^2, \dots, \gamma^{n-1}$ne sont pas des normes algébriques d'éléments dans $L$, $\gamma^k \notin N_{L/K}(L)$, $k = 1 \dots n-1$.*

#### 1.3.3.5 Algèbre des quaternions

L'algèbre des quaternions est une d'algèbre cyclique de division. Nous allons dans la suite donner sa définition ainsi que sa représentation matricielle.

**Définition : 1.36** *: algèbre de quaternion*
*Soient K un corps, et $\beta$ et $\gamma$ deux éléments non nuls de K. L'algèbre de quaternion*

$$D_{\beta,\gamma}(K) = \{a + bi + cj + dk \mid a,b,c,d \in K\}$$

*est une algèbre simple centrale sur K. La multiplication est définie par les relations suivantes :*

$$i^2 = \beta, j^2 = \gamma, k = ij = -ji \tag{1.3}$$

*La norme réduite d'un élément $x$ de $D_{\beta,\gamma}(K)$ est $N_{red}(x) = a^2 - \beta b^2 - \gamma c^2 + \beta\gamma d^2 = x \cdot \bar{x}$, avec $\bar{x} = a - bi - cj - dk$ le conjugué de $x$.*

*Une algèbre de quaternion $D_{\beta,\gamma}(K)$ est une algèbre cyclique de division sur K si et seulement si $N_{red}(x) \neq 0$ pour tout élément non nuls $x \in D_{\beta,\gamma}(K)$.*

L'algèbre de quaternion $D_{-1,-1}(\mathbb{R})$ est appelée algèbre des quaternions de Hamilton $\mathbb{H}$. C'est une algèbre cyclique de division sur $\mathbb{R}$, et son corps maximal est $\mathbb{C}$.

On peut obtenir la représentation matricielle des éléments de l'algèbre de quaternion en représentant $i$, $j$ et $k$ définis dans l'équation 1.3 comme suit :

$$\mathbf{i} = \begin{pmatrix} \sqrt{\beta} & 0 \\ 0 & \sqrt{\beta} \end{pmatrix} \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ \gamma & 0 \end{pmatrix} \qquad \mathbf{k} = \mathbf{ij} = \begin{pmatrix} 0 & \sqrt{\beta} \\ -\gamma\sqrt{\beta} & 0 \end{pmatrix}$$

un élément $x$ de $D_{\beta,\gamma}(K)$ s'écrit alors :

$$\mathbf{x} = a + bi + cj + dk = \begin{pmatrix} a + b\sqrt{\beta} & c + d\sqrt{\beta} \\ \gamma(c - d\sqrt{\beta}) & a - b\sqrt{\beta} \end{pmatrix}$$

avec $a$,$b$,$c$,$d \in K$.

En utilisant les notations du paragraphe précédent, l'algèbre des quaternions $D_{-1,-1}(\mathbb{R})$ s'écrit :

$$D_{-1,-1}(\mathbb{R}) = (\mathbb{R}(i)/\mathbb{R},\sigma : i \longmapsto -i, -1)$$

## Conclusion

Ce chapitre a été une introduction aux notions et définitions qui nous seront utiles tout au long de ce mémoire. C'est ainsi que nous nous placerons dans le cas d'un système cohérent où le canal de transmission est supposé connu par le récepteur. Nous supposons le canal quasi-statique non sélectif en fréquence. Nous utiliserons les constellations $q$-QAM et $q$-HEX. Outre la définition des réseaux de points, nous avons détaillé la notion d'algèbre cyclique de division, qui sera notre principal outil dans la construction de codes Espace-Temps.

# Chapitre 2

# État de l'art des codes Espace-Temps

## Introduction

Durant ces dernières d'années, un grand intérêt a été accordé au codage Espace-Temps (ST) grâce à leur capacité à augmenter les débits. Comme mentionné au chapitre précédent, nous allons nous intéresser aux codage ST dans le cas cohérent.

On distingue deux grandes classes de codes ST : les codes ST en Treillis et les codes ST en blocs. Dans ce travail, nous nous intéressons à la deuxième classe de codes ST, les codes ST en blocs.

Il existe dans la littérature une multitude de constructions de codes ST en blocs : les codes orthogonaux [10, 11, 12], les codes en couches [13, 14, 15], les codes à dispersion linéaire [16], les codes algébriques [17, 18, 19, 20], les codes construits à partir d'algèbres de division [9] et enfin les codes construits à partir de rotations réelles [21, 22].

D'une façon générale, les codes ST se caractérisent par leur rendement, ordre de diversité, gain de codage et capacité. Dans [23], des critères de construction permettant d'optimiser l'ordre de diversité et le gain de codage des codes ST ont été établis .

Nous allons commencer par rappeler quelques résultats de la théorie de l'information qui permettront de caractériser les performances des systèmes MIMO. Nous présenterons ensuite les critères de construction des codes ST, à savoir, le critère du rang, du déterminant, de l'information mutuelle et de la trace. Une brève présentation des codes ST en Treillis sera donnée, suivie d'une présentation plus détaillée des codes ST en blocs existant dans la littérature.

## 2.1 Quelques résultats de la théorie de l'information

Un système de transmission est composé d'une source et d'un destinataire, ce dernier essaie de retrouver le signal émis par la source et perturbé par le canal. La question majeure qui se pose est : quelle quantité maximale d'information peut-elle être transmise ? La réponse à cette question se trouve dans la théorie de l'information que l'on va appliquer aux canaux à évanouissements.

L'étude de la capacité permet de fixer les bornes théoriques du système de transmission. Le calcul de la capacité d'un canal MIMO a été réalisé par Telatar dans [24] et Foschini et Gans dans [25] pour les canaux sans mémoire (chaque utilisation du canal définit une réalisation de $H$ indépendante) et pour les canaux ergodiques.

L'information mutuelle $I(\mathbf{X};\mathbf{Y})$ permet de quantifier l'information qu'apporte la réalisation de la sortie $\mathbf{Y}$ sur l'entrée $\mathbf{X}$ du canal, où $\mathbf{X}$ et $\mathbf{Y}$ sont deux variables aléatoires. Pour un canal discret sans mémoire, la capacité est définie comme le maximum de l'information mutuelle sur toutes les distributions possibles de l'entrée $\mathbf{X}$.

$$C = \max_{p(\mathbf{X})} I(\mathbf{X};\mathbf{Y})$$

Pour le canal de transmission radio-mobile réel, modélisé par un canal à évanouissements par blocs, la condition d'ergodicité n'est pas vérifiée et la capacité au sens classique du terme est nulle. Une nouvelle notion a donc été introduite pour ce type de canaux [24, 25, 26, 27], à savoir, une capacité associée à une probabilité de coupure. La capacité est donc considérée comme une variable aléatoire dépendante de la réponse instantanée du canal.

Les canaux à évanouissements par blocs sont aussi caractérisés par leur gain de diversité et leur gain de multiplexage spatial. Malheureusement la maximisation de l'un de ces deux gains n'entraîne pas la maximisation ou même l'obtention de l'autre. Un compromis "gain de multiplexage-diversité" a été établi par Zheng et Tse dans [28].

### 2.1.1 Cas du canal ergodique

Avant de définir la capacité d'un canal MIMO, nous allons définir la capacité d'un canal mono-antennaire (SISO).

#### 2.1.1.1 Canal SISO

La capacité ergodique moyenne d'un canal mono-antennaire s'écrit :

$$C = E_H\left\{\max_{p(x):E\{|x|^2\}\leq P_T} I(x:y)\right\}$$

En considérant le gain complexe $h_{11}$ du canal à évanouissement, la capacité s'écrit [25] :

$$C = E_H\left\{\log_2\left(1+\rho\cdot|h_{11}|^2\right)\right\}$$

où $\rho$ est le rapport signal sur bruit (SNR) moyen en réception. Si $|h_{11}|$ suit une loi de Rayleigh, alors $|h_{11}|^2$ suit une loi du $\chi^2$ d'ordre 2, et la capacité s'écrit [25] :

$$C = E_H\left\{\log\left(1+\rho\cdot x\right)\right\}$$

où $x$ est une variable aléatoire qui suit une loi du $\chi_2$ d'ordre 2.

#### 2.1.1.2 Canal MIMO

La capacité ergodique moyenne d'un canal MIMO s'écrit :

$$C = E_H\left\{\max_{p(\mathbf{X}):\mathbf{Q}\leq P_T} I(\mathbf{X}:\mathbf{Y})\right\}$$

où $\mathbf{Q} = E\left\{\mathbf{X}\mathbf{X}^H\right\}$ est la matrice de covariance du signal d'entrée $\mathbf{X}$. L'énergie totale de transmission est limitée à $P_T$. Choisir $\mathbf{Q} = \frac{P_T}{n_t}\mathbf{I}_{n_t}$ est optimal [24], ce qui correspond au cas décorrélé et de même puissance. La capacité ergodique du canal MIMO AWGN est [24, 25] :

$$C = E_H\left\{\log_2\left(\det\left(\mathbf{I}_{n_r} + \frac{P_T}{\sigma^2 n_t}\mathbf{H}\mathbf{H}^H\right)\right)\right\}$$

qui peut s'écrire aussi :

$$C = E_H\left\{\log_2\left(\det\left(\mathbf{I}_{n_r} + \frac{\rho}{n_t}\mathbf{H}\mathbf{H}^H\right)\right)\right\}$$

où $\rho = \frac{P_T}{\sigma^2}$ est le rapport signal sur bruit moyen (SNR) par antenne de réception.

D'après la loi des grands nombres, $\frac{1}{n_t}\mathbf{H}\mathbf{H}^H \rightarrow \mathbf{I}_{n_r}$ lorsque $n_t$ tend vers l'infini et $n_r$ est constant. Alors la capacité pour un nombre d'antennes à l'émission $n_t$ grand s'écrit [24] :

$$C = n_r \cdot \log_2(1+\rho)$$

Ce qui nous permet de déduire que la capacité du canal MIMO sature pour un nombre d'antennes en réception fixé. Il est donc inutile d'augmenter le nombre d'antennes à l'émission indéfiniment.

Soit la décomposition en valeurs singulières (Singular Value Décomposition - SVD) de la matrice $\mathbf{H}$, $\mathbf{H} = \mathbf{S}\mathbf{D}\mathbf{V}^H$. Les matrices $\mathbf{S}$ et $\mathbf{V}$ sont unitaires et la matrice $\mathbf{D}$ est diagonale composée des valeurs singulières de la matrice $\mathbf{H}$. La capacité devient :

$$\begin{aligned} C &= E_H\left\{\log_2 \det\left(\mathbf{I}_{n_r} + \frac{\rho}{n_t}\mathbf{D}^2\right)\right\} \\ &= E_H\left\{\log_2\left(\prod_{i=1}^{\min(n_t,n_r)}\left(1 + \frac{\rho}{n_t}\lambda_i^2\right)\right)\right\} \\ &= \sum_{i=1}^{\min(n_t,n_r)} E_H\left\{\log_2\left(1 + \frac{\rho}{n_t}\lambda_i^2\right)\right\} \end{aligned}$$

où les $\lambda_i$ sont les valeurs singulières de la matrice $\mathbf{H}$, $\mathbf{H}$ est supposé de rang plein $\min(n_t,n_r)$.

Nous pouvons déduire que la capacité du canal MIMO correspond à la capacité de $\min(n_t,n_r)$ sous-canaux mono-antennaires AWGN. Le canal MIMO ergodique possède $\min(n_t,n_r)$ degrés de liberté.

Pour un canal MIMO $1 \times n_r$, ayant une diversité spatiale à la réception, la capacité peut s'écrire [25] :

$$C = E_H\left\{\log_2(1 + \rho \cdot \mathbf{X})\right\}$$

où $X$ est une variable aléatoire qui suit une loi du $\chi_2$ d'ordre $2n_r$.

Pour un canal MIMO $n_t \times n_r$, et une combinaison optimale entre les $n_r$ antennes à la réception, la capacité s'écrit [25] :

$$C = E_H\left\{n_t \cdot \log_2\left(1 + \frac{\rho}{n_t}\mathbf{X}\right)\right\}$$

où $X$ est une variable aléatoire qui suit une loi du $\chi_2$ d'ordre $2n_r$.

### 2.1.2 Probabilité de coupure

Les canaux MIMO à évanouissements par blocs ont une capacité au sens de Shannon qui est toujours nulle. Une autre façon de mesurer les limites fondamentales de ce canal est la probabilité de coupure. La capacité est considérée comme une variable aléatoire en fonction de la réponse instantanée du canal, qui est constante durant la transmission d'un mot de code de longueur finie.

Si la capacité instantanée est inférieure au rendement utilisé, alors en aucun cas le mot de code transmis ne pourra être décodé sans erreurs, quelque soit le codage/décodage employé. Inversement, si la capacité instantanée est supérieure au rendement utilisé, alors le théorème de Shannon indique qu'il existe un code permettant de transmettre à ce rendement avec une probabilité d'erreurs aussi petite que l'on veut.

**Définition : 2.1** *probabilité de coupure*
*La **probabilité de coupure** (Outage probability) est la probabilité que la capacité du système de transmission devient inférieure au rendement du système R.*

$$Pout(R) = Pr\{C(\mathbf{H}) < R\}$$

La valeur exacte de la probabilité de coupure est difficile à calculer, des approximations ont été proposées dans [26]. On peut prouver que quand $n_t$ et $n_r$ tendent vers l'infini, la capacité $C(\mathbf{H})$ tend vers une variable gaussienne. Soient $\mu_C$ et $\sigma_C^2$ respectivement la moyenne et la variance de la capacité $C(\mathbf{H})$, une approximation de la probabilité de coupure est :

$$Pout \approx Q(\frac{\mu_C - R}{\sigma_C})$$

### 2.1.3 Compromis de gain de multiplexage-diversité

Les canaux à évanouissements par blocs sont caractérisés par leur gain de diversité. Un système MIMO ayant $n_t$ antennes à l'émission et $n_r$ antennes à la réception a un gain de diversité maximal $n_t \cdot n_r$, pour un rendement $R$ fixé. La probabilité d'erreurs moyenne décroît asymptotiquement en $\frac{1}{SNR^{n_t n_r}}$.

D'un autre coté, les canaux ergodiques bénéficient d'un gain de multiplexage spatial, grâce à leur nombre de degrés de liberté égal à $\min(n_t,n_r)$. A fort rapport signal sur bruit, la capacité ergodique est égale à $\min(n_t,n_r)\log(SNR)$. Le gain de multiplexage spatial se traduit par une augmentation du rendement grâce à l'utilisation des canaux spatiaux parallèles.

Il serait intéressant d'augmenter le nombre de degrés de liberté pour les canaux à évanouissements par blocs. Pour cela le gain en diversité à lui seul est insuffisant. Les deux systèmes MIMO correspondant à $n_t \times n_r$ et $n_t n_r \times 1$, ont le même gain de diversité maximal, mais le premier permet d'avoir un meilleur gain de multiplexage spatial.

En effet un système MIMO peut avoir simultanément le gain de diversité et le gain de multiplexage spatial. Mais la maximisation de l'un n'entraîne pas nécessairement la maximisation

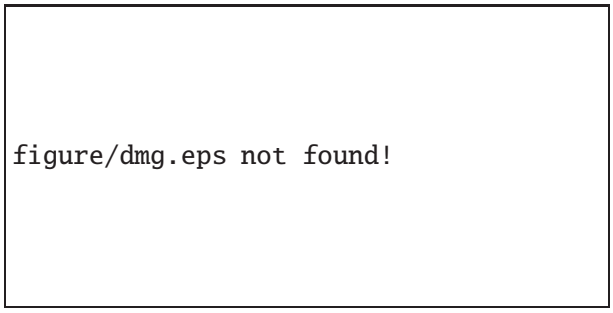



Fig. 2.1: Courbe de la DMG pour $n_t = n_r = 4$

de l'autre. Zheng et Tse dans [28], ont introduit un compromis fondamental entre le gain de diversité et le gain de multiplexage spatial (Diversity Multiplexing Gain tradeoff - DMG).

Le gain de diversité maximal est obtenu pour un rendement fixé $R$. Pour les forts rapports signal sur bruit, ce rendement devient très faible par rapport à la capacité ergodique. Ainsi, pour avoir un gain de multiplexage spatial, il faut considérer des rendements de la forme $R = r\log(SNR)$ correspondants à des fractions de la capacité ergodique, où $r$ est le rendement normalisé et qui représente le gain de multiplexage

Le gain de diversité $d(r)$ correspondant à une transmission avec un rendement normalisé $r$ donné est définit comme suit :

$$d = -\lim_{SNR\to\infty} \frac{\log(P_e)}{\log(SNR)}$$

Le gain de multiplexage maximal est $r_{\max} = \min(n_t,n_r)$ et le gain de diversité maximal est $d_{\max} = n_t n_r$.

Considérons un système MIMO employant un codage Espace-Temps tel que la longueur temporelle du code $T$ vérifie $T \geq n_r + n_t - 1$. Le gain de diversité maximal que peut atteindre le système de transmission pour un gain de multiplexage $r$ donné est [28] :

$$d^*(r) = (n_t - r)(n_r - r)$$

$d^*(r)$ est une courbe linéaire par morceau. La figure 2.1 représente le gain de diversité maximal $d^*(r)$ en fonction du gain de multilexage r pour $n_t = n_r = 4$.

Si $T < n_r + n_t - 1$, des bornes supérieures et inférieures du gain de diversité sont établies dans [28].

Pour un système MIMO avec $n_t = 2$, $n_r \geq 2$, $T \geq 2$, utilisant un codage ST, il a été démontré dans [21, Théorème 1], qu'avoir un déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente, est une condition suffisante (sous certaines conditions) pour atteindre le compromis gain de multiplexage-diversité.

Dans un papier récent de Elia *et al.* [29], Il a été prouvé qu'un système MIMO employant un code ST linéaire ayant un rendement plein et un déterminant minimal ne s'évanouissant

pas lorsque l'efficacité spectrale augmente est optimal du point de vue du compromis gain de multiplexage-diversité.

## 2.2 Critères de construction des codes ST

Tarokh *et al.* dans [23] ont établi des critères de construction des codes ST afin d'augmenter la diversité et le gain de codage. Ces critères ont été établis dans un premier temps pour des canaux à évanouissements indépendants, puis généralisés pour le cas des canaux à évanouissements dépendants. Ils ont aussi établi des critères de construction pour le cas des canaux à évanouissements rapides.

Afin d'établir ces critères il faut calculer la probabilité d'erreurs qu'un décodeur à maximum de vraisemblance (Maximum likelihood - ML) décide d'une façon erronée pour le mot de code $\widehat{\mathbf{X}}$ sachant que $\mathbf{X}$ a été émis, en se plaçant dans le cas des systèmes cohérents. Le système de transmission peut être décrit par l'équation suivante :

$$\mathbf{Y} = \mathbf{H} \cdot \mathbf{X} + \mathbf{W}$$

Le décodeur ML cherche le mot de code $\widehat{\mathbf{X}}$ minimisant $\left\|\mathbf{Y} - \mathbf{H} \cdot \widehat{\mathbf{X}}\right\|^2$. La probabilité que $\widehat{\mathbf{X}} \neq \mathbf{X}$ est égale à :

$$\begin{aligned} Pe &= \text{Prob}\left\{\widehat{\mathbf{X}} \neq \mathbf{X}\right\} \\ &= \sum_{\mathbf{X_l} \in C} \text{Prob}\left\{\mathbf{X_l}\right\} \cdot \text{Prob}\left\{\widehat{\mathbf{X}} \neq \mathbf{X_l} \mid \mathbf{X_l}\right\} \end{aligned}$$

La borne de l'union permet de majorer $\text{Prob}\left\{\widehat{\mathbf{X}} \neq \mathbf{X_l} \mid \mathbf{X_l}\right\}$.

$$\text{Prob}\left\{\widehat{\mathbf{X}} \neq \mathbf{X_l} \mid \mathbf{X_l}\right\} \leq \sum_{\mathbf{T_k} \in C | \mathbf{T_k} \neq \mathbf{X_l}} \text{Prob}\left(\mathbf{X_l} \rightarrow \mathbf{T_k}\right)$$

où $\text{Prob}(\mathbf{X_l} \rightarrow \mathbf{T_k})$ est la probabilité d'erreurs par paire.

$$\begin{aligned} \text{Prob}(\mathbf{X_l} \rightarrow \mathbf{T_k}) &= \text{Prob}\left\{\|\mathbf{Y} - \mathbf{H} \cdot \mathbf{T_k}\|^2 \leq \|\mathbf{Y} - \mathbf{H} \cdot \mathbf{X_l}\|^2 \mid \mathbf{X_l} \text{ émis, } \mathbf{H} \text{ fixé}\right\} \\ &= \text{Prob}\left\{\|\mathbf{H} \cdot (\mathbf{X_l} - \mathbf{T_k}) + \mathbf{W}\|^2 \leq \|\mathbf{W}\|^2 \mid \mathbf{X_l} \text{ émis, } \mathbf{H} \text{ fixé}\right\} \\ &= \text{Prob}\left\{V \leq 0\right\} \end{aligned}$$

où $V = \|\mathbf{H} \cdot (\mathbf{X_l} - \mathbf{T_k})\|^2 + \langle \mathbf{H} \cdot (\mathbf{X_l} - \mathbf{T_k}), \mathbf{W} \rangle$ est une variable gaussienne de moyenne $m_v = \|\mathbf{H} \cdot (\mathbf{X_l} - \mathbf{T_k})\|^2$ et de variance $\sigma_v^2 = 4 \cdot \sigma_W^2 \|\mathbf{H} \cdot (\mathbf{X_l} - \mathbf{T_k})\|^2$. D'où :

$$\begin{aligned} \text{Prob}(\mathbf{X_l} &\rightarrow \mathbf{T_k}) = Q\left(m_v / \sigma_v\right) \\ &= Q\left(\frac{\|\mathbf{H} \cdot (\mathbf{X} - \mathbf{T})\|}{2\sigma_W}\right) \end{aligned}$$

En moyennant par rapport à $\mathbf{H}$ et en utilisant la borne exponentielle, on obtient :

$$\text{Prob}(\mathbf{X_l} \rightarrow \mathbf{T_k}) \leq \exp\left(-\frac{E_H\left(\|\mathbf{H} \cdot (\mathbf{X_l} - \mathbf{T_k})\|^2\right)}{8\sigma_W^2}\right) \tag{2.1}$$

Soit $\mathbf{A} = (\mathbf{X_l} - \mathbf{T_k})(\mathbf{X_l} - \mathbf{T_k})^H$, $\mathbf{A}$ est une matrice hermitienne positive, il existe donc une matrice unitaire $\mathbf{V}$ et une matrice diagonale réelle, positive $\mathbf{D}$ telle que $\mathbf{A} = \mathbf{V}^H\mathbf{D}\mathbf{V}$. Les colonnes de la matrice $\mathbf{V}$ sont les vecteurs propres de $\mathbf{A}$, ils forment une base orthonormale de $\mathbb{C}^n$. Les éléments de $\mathbf{D}$, $\lambda_l \geq 0, l = 1, \ldots, n_t$, sont les valeurs propres de $\mathbf{A}$ en comptant la multiplicité. On a donc :

$$\begin{aligned} E_H\left(\|\mathbf{H}\cdot(\mathbf{X_l}-\mathbf{T_k})\|^2\right) &= tr\ \left(E_H\left(\mathbf{H}\cdot(\mathbf{X_l}-\mathbf{T_k})(\mathbf{X_l}-\mathbf{T_k})^H\cdot\mathbf{H}^H\right)\right) \\ &= tr\left(E_H\left(\mathbf{H}\cdot\mathbf{V}\cdot\mathbf{D}\cdot\mathbf{V}^H\cdot\mathbf{H}^H\right)\right) \\ &= E_H\left(\sum_{i=1}^{n_t}\sum_{j=1}^{n_r}\lambda_i\left|\beta_{ij}\right|^2\right) \\ &= \sum_{i=1}^{n_t}\sum_{j=1}^{n_r}\lambda_i \mathrm{E}\left(\left|\beta_{ij}\right|^2\right) \end{aligned}$$

Soit $h_i$ la $i^{me}$ ligne de $\mathbf{H}$, et $v_j$ la $j^{ime}$ colonne de $\mathbf{V}$, $\beta_{ij} = h_i \cdot v_j$. Étant donné que les $(v_i)_{i=1\ldots n_r}$ forment une base de $\mathbb{C}^{n_r}$ et que les $h_{ij}$ sont des variables gaussiennes de moyennes nulles et de variance 0.5 par dimension réelle, alors $\beta_{ij}$ sont des variables gaussiennes de moyennes nulles et de variance 0.5 par dimension réelle.

Soit $r$ le rang de la matrice $\mathbf{A}$, donc $\mathbf{A}$ possède $r$ valeurs propres non nulles. A fort rapport signal sur bruit la probabilité d'erreurs par paire peut être majorée par.

$$\begin{aligned} \mathrm{Prob}(\mathbf{X_l} &\rightarrow \mathbf{T_k}) \leq \prod_{j=1}^{n_r}\exp\left(-\frac{1}{8\sigma_W^2}\sum_{i=1}^{r}\lambda_i\right) \\ &\leq \left(\frac{1}{\prod_{i=1}^{r}(1+\frac{\lambda_i}{8\sigma_W^2})}\right)^{n_r} \end{aligned}$$

On obtient à la fin :

$$\mathrm{Prob}(\mathbf{X_l} \rightarrow \mathbf{T_k}) \leq \left(\prod_{i=1}^{r}\lambda_i\right)^{-n_r}\left(\frac{1}{8\sigma_W^2}\right)^{-r\cdot n_r}$$

A partir de cette dernière formule les deux critères de construction des codes ST,le critère du rang et le critère du déterminant, peuvent être déduits.

Dans l'expression de la probabilité d'erreur par paire, l'ordre de diversité du système est l'exposant du rapport signal sur bruit. Ceci se traduit asymptotiquement sur la courbe de performance du code ST (probabilité d'erreurs en fonction du rapport signal sur bruit) par une pente égale à l'ordre de diversité. On remarque que la diversité à la réception est acquise, reste donc à récupérer la diversité à l'émission.

**Définition : 2.2** *critère du rang*

*Afin d'atteindre la diversité maximale $n_t \cdot n_r$, la matrice* $\mathbf{A}$ *doit être de rang plein pour tous les mots de code* $\mathbf{X}$ *et* $\mathbf{T}$*. Si la matrice* $\mathbf{A}$ *est de rang r, pour deux mots de codes* $\mathbf{X}$ *et* $\mathbf{T}$*, la diversité atteinte est égale à* $r \cdot n_r$*.*

Le gain de codage permet de mesurer le gain du système codé par rapport au système non-codé, pour un même ordre de diversité.

**Définition : 2.3** *critère du déterminant*
*Afin de maximiser le gain de codage, le déterminant minimal de* $\mathbf{A}$, $\delta(C) = \min_{\mathbf{X},\mathbf{T}\in C,\, \mathbf{X}\neq\mathbf{T}} \det(\mathbf{A})$ *doit être maximisé, pour tous les mots de codes* $\mathbf{X}$ *et* $\mathbf{T}$*.*

Dans [16], un autre critère de construction des codes ST se basant sur la maximisation de l'information mutuelle a été introduit. Ce dernier critère est indépendant du critère du rang et du déterminant. Par conséquent il ne garantit pas à lui seul une diversité maximale.

**Définition : 2.4** *critère de l'information mutuelle*
*Afin d'atteindre la capacité du canal, l'information mutuelle entre le signal émis et celui reçu doit être maximisée.*

$$C = \max_{\mathbf{Q}'\geq 0, tr(\mathbf{Q}')=\mathbf{n_t}} E_H\left\{\log_2\left(\det\left(\mathbf{I}_{n_r} + \frac{\rho}{n_t}\mathbf{H}\mathbf{Q}'\mathbf{H}^H\right)\right)\right\}$$

*où* $\mathbf{Q}' = \frac{n_t}{P_t} E_H\left\{\mathbf{X}\mathbf{X}^H\right\}$.

Dans [30], les auteurs se sont intéressés au cas d'un grand nombre d'antennes à la réception. Dans ce cas de figure les canaux à évanouissements sont équivalents à des canaux AWGN. Les codes ST ayant une distance euclidienne et une distance produit optimales ont de bonnes performances. Les auteurs ont établi un nouveau critère appelé critère de la trace, optimisant la distance euclidienne.

**Définition : 2.5** *critère de la trace*
*Afin de maximiser la distance euclidienne minimale du code, la trace de la matrice* $\mathbf{A}\mathbf{A}^H$*doit être maximisée, pour tous mots de code* $\mathbf{X}$ *et* $\mathbf{T}$*.*

Il est possible qu'un code ST vérifie les critères du rang, du déterminant et de l'information mutuelle en même temps. Si le code est linéaire, alors l'unitarité de la matrice obtenue par vectorisation du mot de code (concatenation des colonnes de la matrice mot de code) est suffisante pour vérifier le critère de l'information mutuelle.

## 2.3 Différentes Classes de codes ST

### 2.3.1 Codes ST en Treillis

Les premiers codes ST en Treillis ont été construits par Tarokh *et al.* dans [23]. C'est une généralisation des codes en Treillis classiques (canal Gaussien) pour les systèmes MIMO.

Dans un code ST en Treillis les symboles à transmettre à chaque instant, par toutes les antennes émettrices, représentent une transition dans le Treillis. Au début du codage d'une trame le codeur doit être à l'état 0. En fonction de l'état du codeur et des bits entrants, une transition est choisie à chaque instant $t$. Si l'étiquette de cette branche est $s_t^1 s_t^2, \ldots, s_t^n$, cela veut dire qu'à l'instant $t$, l'antenne $j$ va transmettre le symbole $s_t^j$. La figure 2.2 illustre un exemple de code en Treillis, pour $n_t = 2$, utilisant une modulation 8-PSK.

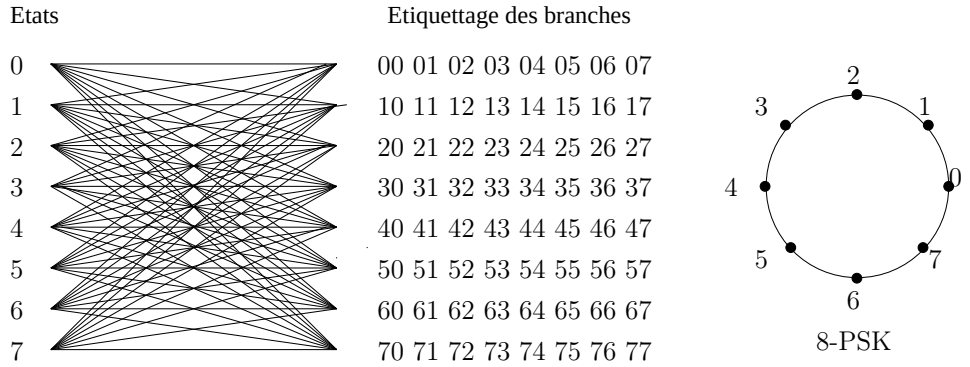



Fig. 2.2: Exemple de code ST en Treillis à 8 états

Soit la trame {0,1,5,7,6,4} de symboles 8-PSK à transmettre, le mot de code s'écrit alors :

$$X = \begin{bmatrix} 0 & 0 & 1 & 5 & 7 & 6 \\ 0 & 1 & 5 & 7 & 6 & 4 \end{bmatrix}$$

Le décodage d'un code en Treillis se fait par l'algorithme de Viterbi. Cet algorithme minimise une métrique additive sur tous les chemins dans le Treillis. La complexité de cet algorithme est exponentielle en fonction du nombre d'états du codeur, ce qui rend les codes en Treillis peu pratiques.

Afin de construire des codes ST en Treillis optimaux, dans [30], les auteurs proposent de vérifier les critères du rang, du déterminant et de la trace. La construction proposée des codes ST en Treillis optimaux consiste à choisir un code en Treillis ayant une distance euclidienne optimale et un multiplexage spatio-temporel des symboles d'information maximisant le gain de codage (afin d'assurer une diversité maximale).

### 2.3.2 Codes ST en blocs

Plusieurs constructions de codes ST en blocs existent dans la littérature, dont quelques unes sont des généralisations d'autres.

Le premier code ST, le fameux code d'Alamouti [10], a trouvé un grand succès grâce à ses propriétés : rendement 1 symbole/uc, diversité pleine et capacité maximale atteinte, pour $n_t = 2$ et $n_r = 1$. Un autre avantage du code d'Alamouti est son décodage linéaire qui est une conséquence de sa structure orthogonale (les colonnes de la matrice mot de code sont orthogonales). Toutes les bonnes propriétés du code d'Alamouti ont été un facteur motivant pour sa généralisation pour des dimensions plus élevées. Malheureusement, ces constructions ont été pénalisées par leurs rendements strictement inférieurs à 1 symbole/uc. En relâchant la

contrainte d'orthogonalité, des codes ST de rendement compris entre 1 et $n_t$ ont été construits.

La famille des codes ST en couches (layered space-time codes - LST), ont un rendement qui augmente linéairement en fonction du nombre d'antennes, pour des systèmes symétriques ($n_t = n_r$). Un code LST est entièrement défini par le choix du nombre de couches et du codage associé à chacune des couches. Il existe trois types de codes LST : le codage D-BLAST [14], sa version simplifiée VBLAST [13] et le code ST "Wrapped" [15].

Une autre famille de codes ST en blocs existe qui est la famille des codes à dispersion linéaire (linear dispersion code - LD). Un code LD est entièrement défini par le choix du nombre de sous-trames et des matrices de dispersions. La représentation en réseaux de points des codes LD permet leurs décodage par les décodeurs de réseaux de points, décodage par sphères et algorithme Schnorr-Euchner. Ces derniers décodeurs permettent d'obtenir les performances ML, avec une complexité polynômiale. Des codes LD dans [16] ont été construits en maximisant l'information mutuelle. Ce critère à lui seul ne garantit pas la diversité maximale, par la suite, ces codes n'atteignent pas la diversité maximale.

En utilisant les structures des codes LST et LD et des résultats de la théorie algébrique des nombres, des codes ST algébriques atteignant la diversité maximale ont été construits. Le code ST diagonal algébrique (Diagonal Algebraic Space-Time code - DAST) [17], a un rendement égal à 1 symbole/uc et une diversité pleine. Dans [18], un code ST algébrique pour $n_t = 2$ et $n_r \geq 2$ a été construit ayant un rendement plein et une diversité pleine. La généralisation de ce dernier code pour $n_t \geq 3$ a été faite dans [19, 20].

Dans [9] des codes ST ont été construits à partir d'algèbre de division. Une algèbre de division est un anneau dans lequel tout élément non nul admet un inverse pour la multiplication. Il en découle que ces matrices mots de code sont de rang plein et par la suite atteignent la diversité maximale.

Les codes ST dans [18, 20, 19, 9] ont des rendements pleins et des diversités pleines, cependant leurs déterminants minimaux s'évanouissent lorsque l'efficacité spectrale augmente. Rappelons que le gain de codage d'un code ST est le déterminant minimal de la différence de deux mots de code maximisé.

Récemment de nouvelles constructions de code ST algébrique ont été présentées dans [21, 22], pour $n_t = 2$, à partir de rotations réelles optimales au sens de la distance produit minimale. Ces derniers codes ont des déterminants minimaux discrets indépendants de l'efficacité spectrale.

Dans la suite nous détaillerons toutes les constructions de code ST citées, en donnant la structure, le rendement et l'ordre de diversité pour chacun des codes.

## 2.4 Codes ST orthogonaux

Les codes ST orthogonaux sont des codes ST en blocs tels que les mots de code sont des matrices orthogonales ou unitaires [11]. Cette propriété permet un décodage linéaire de ces codes, c'est pourquoi elle est considérée comme leur point fort. Leur faiblesse est un rendement qui s'écroule

lorsque le nombre d'antennes est grand. Le code ST orthogonal ayant le plus grand rendement est le code d'Alamouti.

### 2.4.1 Code d'Alamouti

Alamouti dans [10] a construit un code ST remarquable, qui atteint la diversité maximale et a un rendement égal à 1 symbole/uc. Ce code est optimal pour deux antennes à l'émission et une antenne à la réception, $n_t = 2$, $n_r = 1$. Un mot de code s'écrit :

$$\mathbf{X} = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix}$$

avec $s_1$ et $s_2$ deux symboles d'information. Le vecteur reçu s'écrit :

$$\begin{bmatrix} y_1 & y_2 \end{bmatrix} = \begin{bmatrix} h1 & h2 \end{bmatrix} \cdot \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix} + \begin{bmatrix} w_1 & w_2 \end{bmatrix}$$

Les signaux reçus aux instants $t$ et $t + T$ sont donc

$$\begin{cases} y_1 = h_1 s_1 + h_2 s_2 + w_1 \\ y_2 = -h_1 s_2^* + h_2 s_1^* + w_2 \end{cases}$$

Soient $\mathbf{z} = \begin{bmatrix} y_1 & y_2^* \end{bmatrix}^t$, et $\mathbf{T} = \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}$,on a alors

$$\mathbf{z} = \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2^* \end{bmatrix}$$

et

$$\mathbf{T}^H \cdot \mathbf{z} = \left(|h_1|^2 + |h_2|^2\right) \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} \nu_1 \\ \nu_2 \end{bmatrix}$$

Étant donné que $h_1$ et $h_2$ sont décorrélés alors $\nu_1$ et $\nu_2$ le sont aussi. Une simple détection à seuil permet de retrouver les symboles $s_1$ et $s_2$. Le détecteur ML se réduit donc à une détection à seuil. La diversité maximale est atteinte, et est égale à 2.

Le code d'Alamouti infini peut être obtenu par une construction algébrique. Soit l'algèbre des quaternions de Hamilton, $\mathbb{H} = D_{-1,-1}(\mathbb{R})$, définie dans le chapitre I (def. 1.36). En prenant :

$$i = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix} \quad j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad k = ij = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

$\mathbf{X} \in \mathbb{H}$ s'écrit

$$\mathbf{X} = a + bi + cj + dk = \begin{bmatrix} a + ib & c + id \\ -(c - id) & a - ib \end{bmatrix} = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix}$$

avec $a$,$b$,$c$,$d \in \mathbb{R}$, $s_1 = a + ib$ et $s_2 = c + id$. $\mathbf{X}$ est la version transposée du code d'Alamouti.

Le code d'Alamouti est l'unique code de rendement 1 symbole/uc, de rang plein sur un ensemble fini de $\mathbb{C}$. L'unicité de ce code est due au fait que l'algèbre des quaternions de Hamilton est l'unique algèbre de division qui a comme sous-corps maximal le corps des nombres complexes.

Avec $n_r = 1$, le code d'Alamouti atteint la capacité maximale d'un système MIMO. Mais pour $n_r > 1$, le code n'exploite plus tous les degrés de liberté du système, il a une capacité équivalente à un système MIMO $n_t' = 2n_r$ et $n_r' = 1$. Le code d'Alamouti n'est optimal que pour $n_t = 2$ et $n_r = 1$.

### 2.4.2 Généralisation du code d'Alamouti

La généralisation du code d'Alamouti a été faite par Tarokh *et al.* dans [11] et Tirkkonen et Hottinen dans [31] et [12].

Dans [11], il a été démontré que, pour le cas réel, il existe des constructions orthogonales de code ST seulement pour $n_t = 2$, 4 et 8. Ce problème d'existence de matrice orthogonales réelles est connu en mathématique comme le problème de "Hurwitz-Radon". Par exemple le code pour $n_t = T = 4$ peut être trouvé à partir du code d'Alamouti en passant à la représentation réelle des quaternions de Hamilton. En posant :

$$i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \quad j = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

$\mathbf{X}_{\mathbb{R}}$ s'écrit :

$$\mathbf{X}_{\mathbb{R}} = a + bi + cj + dk = \begin{bmatrix} a & -b & c & -d \\ b & a & d & c \\ -c & -d & a & b \\ d & -c & -b & a \end{bmatrix}$$

Ce dernier résultat a été généralisé aux systèmes dont les symboles appartiennent à des constellations complexes. Considérant un système ayant $n_t$ antennes à l'émission et un nombre quelconque d'antennes à la réception. Durant $T$ temps symbole, le système va transmettre $K$ symboles d'information $s_i$. Un mot de code sera donc une matrice $n_t \times T$ dont les éléments sont des combinaisons linéaires des symboles d'information. Un mot de code orthogonal $\mathbf{C}$ vérifie la relation suivante :

$$\mathbf{C}^H\mathbf{C} = \left(\sum_{i=1}^{K} |s_i|^2\right)\mathbf{I}_{n_t} \tag{2.2}$$

avec $\mathbf{I}_{n_t}$ la matrice identité de dimension $n_t$. La relation 2.2 garantie :

- La saturation du critère du rang : soient $\mathbf{C_1}$ et $\mathbf{C_2}$ deux mots de code, $(\mathbf{C_1} - \mathbf{C_2})$ est une matrice unitaire de rang $n_t$. Ainsi la diversité maximale est atteinte.
- La saturation du critère du déterminant : $\min_{\mathbf{C_1},\mathbf{C_2}\in C}(\det(\mathbf{C_1}-\mathbf{C_2})) = a$, avec $a$ une constante, qui est donc maximisée.
- L'existence d'un décodage linéaire ML.

Un mot de code s'écrit sous la forme suivante :

$$\mathbf{C} = \sum_{l=1}^{K}(a_l\beta_{2l-2} + b_l\beta_{2l-1}) \tag{2.3}$$

avec $s_l = a_l + ib_l, l = 1 \ldots K$, et $\beta_l, l = 0 \ldots 2K-1$ des matrices constantes complexes de dimension $T \times n_t$. Afin de vérifier la relation 2.2, les matrices $\beta_l$ doivent vérifier la condition suivante :

$$\beta_l^H\beta_k + \beta_k^H\beta_l = 2\delta_{lk}\mathbf{I}_{n_t} \tag{2.4}$$

Cette équation est l'extension de l'équation de "Hurwitz-Radon" dans le domaine complexe.

Un code ST $C$, défini à partir de l'équation 2.3 et vérifiant 2.4 a une diversité pleine, et un rendement égal à $K/T$ symboles/uc.

En se restreignant au cas $T = n_t$, et en définissant $\beta_0 = \mathbf{I}_{n_t}$, les matrices $\beta_l, l = 1 \dots 2K-1$ sont alors les générateurs de l'algèbre de Clifford [32]. Grâce aux propriétés des algèbres de Clifford, on peut montrer que les codes ST orthogonaux ont un rendement de la forme $K/n_t$ avec une limitation importante sur la forme de $n_t$ (ceci est dû à la construction même des algèbres de Clifford par produit tensoriel).

Dans [11], il a été prouvé qu'il existe des codes orthogonaux de rendement 1/2, quelque soit le nombre d'antennes. Ces codes atteignent la diversité maximale, mais sacrifient le rendement. Il a été démontré aussi que pour les dimensions 3 et 4, il existe des codes orthogonaux de rendement 3/4. D'une façon plus générale, pour $K$ symboles d'information, il existe un code orthogonal tel que $n_t = 2^{K-1}$ et $T = 2^{K-1}$, ayant un rendement égal à $K/2^{K-1}$.

Exemple d'un code orthogonal [11] pour $n_t = T = 4$ :

$$\mathbf{X} = \begin{bmatrix} s_1 & s_2 & \frac{s_3}{\sqrt{2}} & \frac{s_3}{\sqrt{2}} \\ -s_2^* & s_1^* & \frac{s_3}{\sqrt{2}} & -\frac{s_3}{\sqrt{2}} \\ \frac{s_3^*}{\sqrt{2}} & \frac{s_3^*}{\sqrt{2}} & \frac{(-s_1-s_1^*+s_2-s_2^*)}{2} & \frac{(-s_2-s_2^*+s_1-s_1^*)}{2} \\ \frac{s_3^*}{\sqrt{2}} & -\frac{s_3^*}{\sqrt{2}} & \frac{(s_2+s_2^*+s_1-s_1^*)}{2} & -\frac{(-s_1+s_1^*+s_2-s_2^*)}{2} \end{bmatrix}$$

Afin d'obtenir un code avec une distribution énergétique plus uniforme, une transformation unitaire est proposée dans [31], le code obtenue est :

$$\mathbf{X} = \begin{bmatrix} s_1 & s_2 & s_3 & 0 \\ -s_2^* & s_1^* & 0 & -s_3 \\ -s_3^* & 0 & s_1^* & s_2 \\ 0 & s_3^* & -s_2^* & s_1 \end{bmatrix}$$

Le tableau suivant [12], donne un récapitulatif des rendements des codes orthogonaux en fonction du nombre d'antennes à l'émission.

| $n_t$ | $T$ | nb symboles | rendement |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 2 | 2 | 2 | 2 |
| 3 et 4 | 4 | 3 | 3/4 |
| $2^{K-2}+1 \to 2^{K-1}$ | $2^{K-1}$ | $K$ | $K/2^{K-1}$ |

Tab. 2.1: Rendements des codes orthogonaux pour différentes dimensions

## 2.5 Codes ST par couches (layered Space Time codes - LST)

Le rendement limité des codes orthogonaux a motivé la construction de code ST ayant une plus grande efficacité spectrale. Les codes ST en couches (LST), permettent une augmentation du rendement. Pour les systèmes symétriques (même nombre d'antennes à l'émission et à la réception), leurs rendements augmentent linéairement en fonction du nombre d'antennes. Ces codes exploitent le multiplexage spatio-temporel afin d'augmenter l'ordre de diversité atteint.

Foschini dans [14] a proposé les codes D-BLAST (Diagonal Bell Laboratories Layered Space-Time), et dans [13] Wolniansky *et al.* présentent le code V-BLAST (Vertical Bell Laboratories Layered Space-Time) qui est une version simplifiée du D-BLAST. Dans [15], Caire et Colavolpe présentent un code ST appelé "Wrapped Space-Time code". Les codes V-BLAST et D-BLAST sont des cas particuliers des codes ST "Wrapped".

### 2.5.1 V-BLAST

Une trame de bits d'information est divisée en $n_t$ sous trames, chaque sous trame est modulée par la suite par une modulation $q$-QAM (2.3). Les couches correspondent aux différentes sous-trames.

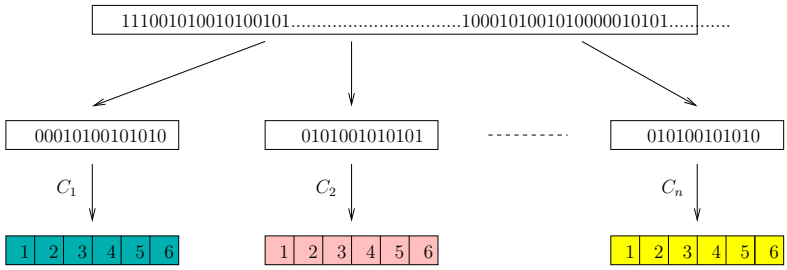



Fig. 2.3: Division en sous-trames et codage de chaque sous-trame

Le codage V-BLAST consiste à associer chaque couche à une antenne émettrice (voir figure 2.4). Le rendement du code est donc $n_t$ symboles/uc. Ce système correspond au système non-codé décrit dans le chapitre précédent par l'équation (1.2).

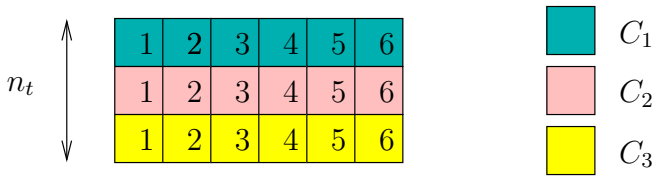



Fig. 2.4: Structure d'un mot de code du code V-BLAST

L'avantage de ce système de transmission apparaît au niveau de son décodage présenté dans [13]. Il s'agit d'un égaliseur à retour de décision adapté à la structure des systèmes MIMO, connu aussi dans la littérature comme "suppression successive de l'interférence" (Successive

Interférence cancellation - SIC). A chaque itération, un symbole d'une couche est décodé en considérant les autres symboles des autres couches comme des interféreurs. Sa contribution dans le signal reçu est par la suite soustraite afin de pouvoir décoder les autres symboles. Ces opérations sont répétées autant de fois qu'il y a de couches. L'annulation peut utiliser soit le critère du forçage à zéro (Zero-Forcing - ZF), soit le critère minimisant l'erreur quadratique moyenne (Minimum Mean Square Error - MMSE).

Étant donné que l'algorithme ne fait pas qu'une annulation, mais aussi une suppression de l'interférence, l'ordre dans lequel les couches sont traitées peut influencer sur les performances. Un classement des couches s'avère nécessaire. L'ordre optimal [13] consiste à traiter à chaque itération la couche ayant le rapport signal sur bruit le plus fort. Tous les symboles appartiennent à la même constellation, ils ont donc la même énergie et sont affectés par le même bruit gaussien. Le classement peut se faire en prenant à chaque fois le $\min(\left\|G_j\right\|^2)$, $G$ étant la matrice d'annulation. L'algorithme de décodage avec classement est appelé "suppression successive d'interférence avec ordonnancement" (Ordered Successive Interference Cancellation - OSIC).

L'algorithme de décodage OSIC est le suivant :

*Algorithme BLAST (ZF-OSIC / MMSE-OSIC) :*

**Entrée :** Signal reçu $\mathbf{y}$, matrice du canal $\mathbf{H}$

**Sortie :** Approximation du vecteur des symboles $\mathbf{s}$

**Initialisation :** Annulation avec ZF, $\mathbf{G} = (\mathbf{H}^H \cdot \mathbf{H})^{-1} \cdot \mathbf{H}^H$ ou annulation avec MMSE, $\mathbf{G} = (\mathbf{H}^H\mathbf{H} - \sigma^2\mathbf{I})^{-1}\mathbf{H}^H$. Choix de la couche ayant le meilleur rapport signal sur bruit, $k_i = \min_j(\left\|\mathbf{G}_j\right\|^2)$, $i = 1$.

**Étape 1** : Annulation de la couche $k_i$, $\mathbf{x}_{k_i} = \mathbf{G}_{k_i}^T \cdot \mathbf{y}$

**Étape 2** : Quantification du symbole $k_i$ approprié à la constellation utilisée, $\hat{\mathbf{s}}_{k_i} = Q(\mathbf{x}_{k_i})$

**Étape 3** : Suppression de la contribution de la couche annulée du signal reçu, $\mathbf{y} = \mathbf{y} - \mathbf{H}_{k_i} \cdot \hat{\mathbf{s}}_{k_i}$, $\mathbf{H}_{k_i}$ la $k_i$ colonne de $\mathbf{H}$ .

**Étape 4** : Définition de $\mathbf{H}_1$ comme étant la matrice $\mathbf{H}$ avec ces colonnes $k_1, k_2, \ldots k_i$ annulées. Recalculer $\mathbf{G}$ en fonction de $\mathbf{H}_1$. Incrémenter $i$.

**Étape 5** : Choix de la prochaine couche à traiter, $k_i = \min_j(\left\|\mathbf{G}_j\right\|^2)$. Aller à l'**Étape 1.**

Cet algorithme permet d'améliorer nettement les performances par rapport à un simple détecteur linéaire ZF ou MMSE, sans trop augmenter la complexité. Comme tous les égaliseurs à retour de décision, son principal inconvénient est la propagation d'erreurs. Si un symbole est mal estimé, une mauvaise contribution est soustraite du signal reçu, ce qui entraîne une mauvaise détection des symboles restants.

### 2.5.2 D-BLAST

L'idée originale de Foschini consiste en un codage diagonal. En effet, les symboles codés de chaque couche sont transmis successivement par chaque antenne émettrice. Les couches occupent alors les diagonales de la matrice mot de code (voir figure 2.5). Le multiplexage spatio-temporel permet d'augmenter l'ordre de diversité atteint par les codes D-BLAST.

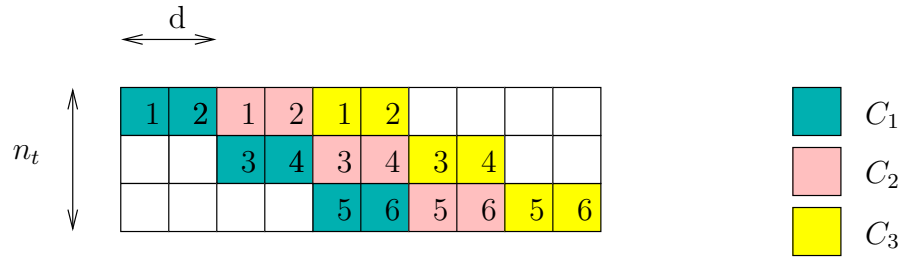



Fig. 2.5: Structure d'un mot de code du code D-BLAST

La longueur des codes utilisés sur chaque couche est égale à $N_1 = n_t d$, où $d$ correspond au délai d'intercalage (interleaving delay). La longueur temporelle du mot de code est donc $T = d(2n_t - 1)$. Pour des raisons de complexité d'implémentation réelle, le nombre d'antennes ne peut pas être très grand. Ainsi, pour obtenir des mots de code long il faut augmenter le délai d'intercalage. Reste que les codes utilisés par les différentes couches sont relativement courts, ce qui pose des problèmes pour certains types de codes comme les codes en Treillis.

Le décodage des codes D-BLAST peut se faire en utilisant l'algorithme OSIC. S'il y a un codage entre couches, alors la complexité de décodage augmente.

Cette architecture, bien qu'elle résiste plus aux effets des évanouissements du canal de transmission, n'a pas eu beaucoup de succès, du moins jusqu'à présent. Cela s'explique par son manque d'efficacité dû à la partie nulle dans la matrice mot de code et surtout à la complexité de son décodage.

### 2.5.3 "Wrapped" ST code

Les codes ST "Wrapped" (WST), ont été proposés dans [15]. Désormais, la construction de code LST ayant une longueur arbitraire et un petit délai d'intercalage entre les couches est possible en utilisant les codes WST. En effet, un seul codage est utilisé pour coder toute la trame de bits. Soit $N_2$ la longueur de ce code. Les symboles codés sont transmis successivement par chaque antenne émettrice (fig. 2.6). La longueur temporelle du mot de code WST est égale à $T = \frac{N_2}{n_t} + (n_t - 1)d$. Ainsi on peut obtenir des codes longs indépendamment du délai d'intercalage. Cette construction résout le problème de la longueur temporelle des codes D-BLAST, tout en conservant la même structure. Le code WST peut être décoder par l'algorithme OSIC.

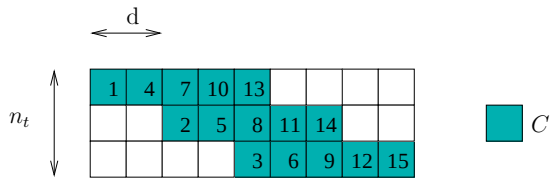



Fig. 2.6: Structure d'un mot de code "Wrapped" ST

Cette construction englobe les codes ST en Treillis et les codes V-BLAST et D-BLAST. En effet, en notant $C$ un code en Treillis, et en fixant $d$ à zéro, le code WST obtenu est un code ST en Treillis. En prenant $C = (C_1 \times C_2 \times \cdots \times C_{n_t})$ (produit cartésien des codes $C_1$,$C_2$,...,$C_{n_t}$), on

retrouve les codes D-BLAST. Quand aux codes V-BLAST, ils sont obtenus en considérant une simple modulation QAM et un délai d'intercalage nul.

## 2.6 Codes ST à dispersion linéaire

Les codes ST présentés jusqu'à présent n'exploitent pas d'une façon optimale les ressources spatio-temporelles qu'offrent un système MIMO. Le code d'Alamouti perd son optimalité pour un nombre d'antennes à la réception supérieur à 1. Les codes orthogonaux, pour un nombre d'antennes émettrices supérieur à 2, sont pénalisés par leurs rendements inférieurs à 1 symbole/uc. Les codes V-BLAST n'exploitent pas le multiplexage spatio-temporel, et par la suite leurs ordres de diversité sont limités. Enfin, les codes D-BLAST et WST, souffrent d'un gaspillage des ressources spectrales dû à la partie nulle dans la matrice mot de code, et d'un décodage plus au moins complexe en fonction du ou des codes utilisés.

Dans [16], Hassibi et Hochwald ont construit des codes ST exploitant le multiplexage spatio-temporel et ayant une structure linéaire. L'idée consiste à transmettre, à chaque instant, par chaque antenne émettrice, une combinaison linéaire de sous-trames. Ces combinaisons linéaires de sous-trames sont ainsi dispersées en espace et en temps, d'où l'appellation de ce code : "code à dispersion linéaire" (Linear Dispersion code - LD). Les codes LD peuvent être construits pour un nombre d'antennes quelconques à l'émission et à la réception.

Soit $N$ le nombre de sous-trames, et soient $s_1, \ldots, s_N$ les symboles obtenus par modulation $q$-QAM ou $q$-PSK (modulation de phase) des sous-trames. Le mot de code $\mathbf{X}$ s'écrit alors :

$$\mathbf{X} = \sum_{n=1}^{N} (\alpha_n \mathbf{A}_n + i\beta_n \mathbf{B}_n) \tag{2.5}$$

les $\alpha_n$ et $\beta_n$ sont respectivement la partie réelle et la partie imaginaire du symboles $s_n$, pour $n = 1 \ldots N$. Le code LD est entièrement défini, pour $n_t$,$n_r$ et $T$ donnés, par la définition du nombre de sous-trames $N$ et des matrices de dispersion $\mathbf{A}_n$ et $\mathbf{B}_n$ pour $n = 1 \ldots N$. On voit dans l'équation 2.5 la linéarité du code LD qui permet son décodage par les décodeurs linéaires. Afin d'éviter un système indécodable, il faut que $N \leq n_r T$.

La construction des codes LD est une construction très générale qui englobe pas mal de constructions de codes ST proposées dans la littérature. Comme exemple de codes LD on peut citer : le code d'Alamouti, les codes orthogonaux et le code V-BLAST. Le code d'Alamouti s'écrit sous la forme de code LD de la façon suivante :

$$X = a_1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + ib_1 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} + a_2 \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + ib_2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Le prix de cette généralité est la difficulté à optimiser les matrices de dispersion. Dans [16], les auteurs se sont basés sur une optimisation de l'information mutuelle afin de construire des codes LD. Le problème est que ce critère à lui seul permet de construire des codes ayant de bonnes performances mais ne garantit pas la diversité maximale. Hassibi et Hochwald dans [16], prouvent que les codes LD construits en imposant plus de contraintes (ce qui réduit l'information mutuelle) ont de meilleures performances, ce qui confirme que l'optimisation de

l'information mutuelle est insuffisante.

Des codes LD ont été construits par la suite, basés sur des structures algébriques, et vérifiant le critère du rang et du déterminant. Différentes constructions algébriques de code LD sont présentées dans la suite.

## 2.7 Codes ST algébriques diagonaux (DAST)

Les constructions des codes LST et LD sont deux "framework" généraux. La première est entièrement définie par le choix du nombre de couches et du codage associé à chacune des couches, et la deuxième est entièrement définie par le choix du nombre de sous-trames et des matrices de dispersion. Ces codes n'atteignent pas toujours l'ordre de diversité maximal.

En utilisant des résultats de la théorie algébriques des nombres, Damen *et al.* ont construit dans [17] un code ST algébrique diagonal appelé code DAST, ayant un rendement égal à 1 symbole/uc et atteignant la diversité maximale. La construction du code DAST se base sur l'utilisation des constellations tournées construites à partir de corps de nombres. Avant de présenter la construction du code DAST, nous allons expliquer l'intérêt de l'utilisation de telles constellations.

En effet, pour combattre les évanouissements, une redondance peut être introduite. Cette redondance va être perçue au niveau du signal reçu comme une augmentation de la dimension de l'espace d'origine. Une alternative à l'introduction d'une telle redondance est l'utilisation des constellations tournées, ce qui revient à augmenter la dimension algébrique de la constellation. Illustrons ça par un exemple. Soit le corps de nombres de degré 2, $K = \mathbb{Q}(\theta)$, avec $\theta = e^{\frac{i\pi}{4}}$. Et soit $\mathbf{M}$ la matrice obtenue par le plongement canonique de $K$ dans $\mathbb{R}^2$ :

$$\mathbf{M} = \begin{bmatrix} 1 & \theta \\ 1 & -\theta \end{bmatrix}$$

$\mathbf{M'} = \frac{1}{\sqrt{2}}\mathbf{M}$ est une matrice unitaire. Posons $\mathbf{s} = (a_1,a_2)$, le vecteur composé par les symboles d'information. Le vecteur obtenu par la rotation du vecteur $\mathbf{s}$ par $\mathbf{M'}$ est aussi de dimension 2, dont chacune de ces composantes est une combinaison linéaire de $a_1$ et $a_2$ appartenant à $K$. $K$ étant un espace vectoriel de dimension 2 sur $\mathbb{Q}$, alors la dimension algébrique de la constellation est augmentée.

Une constellation peut être caractérisée par sa diversité de modulation et sa distance produit. La diversité de modulation est égale à la distance de Hamming minimale entre deux points de la constellation, en d'autres termes elle est égale au nombre de composantes différentes entre deux points de la constellation. Si la constellation est de dimension $n$, alors la diversité maximale de modulation est $l = n$. La distance produit minimale d'une constellation $S$ est définie comme suit :

$$d_{min} \triangleq \min_{y_j = x_1 - x_2, x_1 \neq x_2 \in S} \prod_{j=1}^{l} |y_j|$$

Une **constellation optimale** au sens de la diversité de modulation est une constellation ayant une diversité maximale et une distance produit minimale maximisées. Dans [33, 34], des

constellations quasi-optimales ont été construites à partir de la théorie des nombres.

Le codage DAST consiste à utiliser des constellations tournées avec une transformation de Hadamard. En effet, la constellation optimale garantit la diversité maximale et la transformation de Hadamard permet de répartir les symboles modulés en espace et en temps afin d'avoir un bon gain de codage égale à la distance produit minimale de la constellation. La construction des codes DAST est valable pour $n_t = 1{,}2$ ou multiple de 4.

Une matrice de Hadamard est une matrice carrée dont les coefficient sont tous $-1$ ou 1 et dont les lignes sont toutes orthogonales, il en découle que $\mathbf{H_n}\mathbf{H_n^t} = n \cdot \mathbf{I}_n$. Par exemple, la matrice de Hadamard pour $n = 2$ est la suivante :

$$\mathbf{H_2} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Soit $\mathbf{M}$ une rotation de dimension $n_t$, ayant une diversité maximale, et soit $\mathbf{s} = (a_1, a_2, \ldots, a_{n_t})^T$ le vecteur des symboles d'information. Soit $\mathbf{x} = (x_1, x_2, \ldots, x_{n_t})^T = \mathbf{M} \cdot \mathbf{s}$, le vecteur des symboles d'information tourné par la rotation $\mathbf{M}$. Le mot de code $\mathbf{X}$ s'écrit alors :

$$\mathbf{X} = \frac{1}{\sqrt{n_t}} \cdot \mathbf{H}_{n_t} \cdot \mathrm{diag}(x_1, x_2, \ldots, x_{n_t})$$

$\mathbf{H}_{n_t}$ est la matrice de Hadamard de dimension $n_t$.

## 2.8 Codes ST algébriques, $n_t = n_r = T$, à rendement plein et diversité pleine

Très peu de codes ST dans la littérature ont un rendement plein égal à $r = n_t$ symbole/uc et une diversité pleine égale à $n_t \cdot n_r$. Le code DAST atteint la diversité maximale, mais il a un rendement égal à 1 symbole/uc et son gain de codage dépend de la distance produit minimale de la constellation tournée utilisée.

Dans [18], un code ST pour $n_t = n_r = T = 2$ a été construit, nous le noterons par la suite code $2 \times 2$. Ce code a un rendement plein de 2 symboles/uc, une diversité égale à 4, un gain de codage optimisé et est décodable par les décodeurs de réseaux de points. Une généralisation de ce code pour $n_t = n_r = T$ quelconque a été présentée dans [19, 20]. Nous détaillerons dans la suite les constructions et caractéristiques de ces codes.

### 2.8.1 Dimension $2 \times 2$

Damen *et al.*, dans [18], ont construit le code ST $2 \times 2$ en utilisant la théorie algébrique des nombres. Ce code satisfait les critères du rang, du déterminant et de l'information mutuelle.

Soit $\mathbf{a} = (a_1, a_2, a_3, a_4)$ le vecteur des symboles d'information à transmettre, la constellation utilisée est une $q$-QAM. Et soit $\theta = \exp(i\lambda)$ avec $\lambda \in \mathbb{R}$, et $\phi^2 = \theta$. Le mot de code $\mathbf{X}$ s'écrit

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_1 + \theta a_2 & \phi(a_3 + \theta a_4) \\ \phi(a_3 - \theta a_4) & a_1 - \theta a_2 \end{bmatrix}$$

En prenant les symboles d'information dans $\mathbb{Z}[i]$, le gain de codage du code infini s'écrit :

$$\begin{aligned}\delta_\infty \quad (C) &= \frac{1}{2} \min_{a \neq (0,0,0,0) \in \mathbb{Z}[i]^4} (a_1 + \theta a_2)(a_1 - \theta a_2) - \phi^2 (a_3 + \theta a_4)(a_3 - \theta a_4) \\ &= \frac{1}{2} \min_{a \neq (0,0,0,0) \in \mathbb{Z}[i]^4} (a_1^2 - a_3^2 \theta - a_2^2 \theta^2 + a_4^2 \theta^3)\end{aligned}$$

Le gain de codage du code fini, en prenant les symboles d'information dans $S \subset \mathbb{Z}[i]^4$, s'écrit :

$$\delta(C) = \frac{1}{2} \min_{a = \frac{1}{2}(s_1 - s_2),\ s_1 \neq s_2 \in S} (a_1^2 - a_3^2 \theta - a_2^2 \theta^2 + a_4^2 \theta^3) \geq \delta_\infty(C)$$

Afin de satisfaire le critère du rang et d'assurer par la suite la diversité maximale, $\theta$ doit être choisie tel que $\delta(C) \neq 0$. En plus, il faut que $\theta$ maximise le gain de codage pour une constellation donnée. $\theta$ peut être soit algébrique soit transcendant.

En prenant $\theta$ algébrique de degré supérieur strictement à 3 sur $\mathbb{Q}(i)$ garantit que $\delta(C)$ ne s'annule pas, du fait que $(1, \theta, \theta^2, \theta^3)$ est une base de $\mathbb{Q}(i,\theta)$. Par exemple, pour $\theta = e^{i\frac{\pi}{8}}$, le gain de codage pour une constellation 4-QAM est égal à 0.1304, et pour une constellation 16-QAM il est égal à 0.059.

Si $\theta$ est un nombre algébrique de degré 2 sur $\mathbb{Q}(i)$, pour que $\delta(C)$ ne s'annule pas, il faut que $\theta^2 \in \mathbb{Q}(i)$ et $\theta^2$ ne soit pas un carré dans $\mathbb{Q}(i)$.

$$\delta(C) = \frac{1}{2} \min_{a = \frac{1}{2}(s_1 - s_2),\ s_1 \neq s_2 \in S} ((a_1^2 - a_2^2 \theta^2) - \theta(a_3^2 - a_4^2 \theta^2))$$

Un exemple de $\theta$ algébrique de degré 2 est $e^{i\frac{\pi}{4}}$. Le gain de codage dans ce cas s'écrit :

$$\delta(C) = \frac{1}{2} \min_{a = \frac{1}{2}(s_1 - s_2),\ s_1 \neq s_2 \in S} (N_{\mathbb{Q}(i,\theta)/\mathbb{Q}(i)}(x_1) - \theta N(x_2)_{\mathbb{Q}(i,\theta)/\mathbb{Q}(i)}) \neq 0$$

avec $x_1 = a_1 + a_2\theta$ et $x_2 = a_3 + a_4\theta$.

Soit $\theta = e^{i\lambda}$ est transcendant. Les valeurs de $\lambda$ optimisant le gain de codage pour chaque constellation sont obtenues par une optimisation numérique. Pour une constellation 4-QAM le gain de codage maximal est atteint pour $\lambda = 0.5$, et est égal à 0.2369. Pour une constellation 16-QAM le maximum est atteint pour $\lambda = 0.448$, et est égal à 0.1397. Malheureusement le $\lambda$ donnant le gain de codage optimal pour une constellation 4-QAM donne un gain de codage très faible pour une constellation 16-QAM.

L'utilisation des nombres transcendants permet d'obtenir la valeur optimale du gain de codage pour une constellation donnée, mais ne permet pas de prédire la diminution de ce dernier lorsque l'efficacité spectrale augmente. L'utilisation des nombres algébriques permet d'avoir une borne inférieure du gain de codage, et d'avoir une décroissance plus contrôlée. Le tableau suivant donne un récapitulatif des valeurs du gain de codage pour les constellations 4-QAM et 16-QAM, pour différentes valeurs de $\theta$.

| | $e^{i\frac{\pi}{8}}$ | $e^{\frac{i}{2}}$ | $e^{i0.521}$ | $e^{i\frac{\pi}{4}}$ |
|---|---|---|---|---|
| 4-QAM | 0.1304 | 0.2369 | - | 0.0858 |
| 16-QAM | 0.059 | 0.0367 | 0.1397 | 0.0272 |

TAB. 2.2: Gains de codage des codes $2 \times 2$ de Damen *et al.*, pour différentes valeur de $\theta$

### 2.8.2 Généralisation

Dans [19], un code ST $n_t \times n_t$ de rendement plein et de diversité pleine a été construit, avec une structure semblable à celle du code présenté dans le paragraphe précédent. La construction se base sur les corps de nombres.

Soit $K = \mathbb{Q}(i,\theta)$ une extension cyclotomique sur $\mathbb{Q}(i)$ de degré $n_t$, avec $\theta = \exp(\frac{i\pi}{2n_t})$. $B = (1,\theta,\ldots,\theta^{n_t-1})$ est une base intégrale de $K$. Soit $\sigma$ le générateur du groupe de Galois de $K$. Étant donné que $K$ est un corps de nombre totalement complexe. Le plongement canonique de $B$ dans $\mathbb{C}^{n_t}$ s'écrit :

$$\mathbf{M} = \frac{1}{\sqrt{n_t}} \begin{bmatrix} 1 & \theta & \ldots & \theta^{n_t-1} \\ 1 & \sigma(\theta) & \ldots & \sigma(\theta^{n_t-1}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma^{n_t-1}(\theta) & \ldots & \sigma^{n_t-1}(\theta^{n_t-1}) \end{bmatrix}$$

La matrice $\mathbf{M}$ est une matrice unitaire. Soit $(a_1,\ldots,a_{n_t^2})$ le vecteur de symboles d'information à transmettre, qui va être divisé en $n_t$ vecteurs $\mathbf{v_1},\ldots,\mathbf{v_{n_t}}$ de longueur égale à $n_t$. En multipliant les vecteurs $\mathbf{v_1},\ldots,\mathbf{v_{n_t}}$ par $\mathbf{M}$ on obtient les vecteurs $\beta_1,\ldots,\beta_{n_t}$. Soit $\phi = \exp(\frac{i\pi}{2n_t^2})$, on a $\phi^{n_t} = \theta$. Le mot de code s'écrit :

$$\mathbf{X} = (\phi^{|j-i|}\beta_{i,|j-i+1|})_{1\leq i,j\leq n_t}$$

Par exemple, pour $n_t = 3$, $\theta = \exp(i\frac{\pi}{6})$, $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = j\theta$ et $\sigma_3(\theta) = j^2\theta$, le mot de code $\mathbf{X}$ s'écrit :

$$\mathbf{X} = \begin{bmatrix} \sigma_1(a_1 + \theta a_2 + \theta^2 a_3) & \phi \cdot \sigma_1(a_4 + \theta a_5 + \theta^2 a_6) & \phi^2 \cdot \sigma_1(a_7 + \theta a_8 + \theta^2 a_9) \\ \phi^2 \cdot \sigma_2(a_7 + \theta a_8 + \theta^2 a_9) & \sigma_2(a_1 + \theta a_2 + \theta^2 a_3) & \phi \cdot \sigma_2(a_4 + \theta a_5 + \theta^2 a_6) \\ \phi \cdot \sigma_3(a_4 + \theta a_5 + \theta^2 a_6) & \phi^2 \cdot \sigma_3(a_7 + \theta a_8 + \theta^2 a_9) & \sigma_3(a_1 + \theta a_2 + \theta^2 a_3) \end{bmatrix}$$

Le code tel qu'il a été construit est de rendement plein $n_t$ symboles/uc. Il a été prouvé dans [19] que le code construit vérifie le critère du rang et donc atteint la diversité maximale. Le déterminant d'un mot de code s'écrit :

$$\det(\mathbf{X}) = \min(Tr_{K/Q(i)}(\alpha) + \sum_{j=1}^{n_t} \theta^{j-1} N_{K/Q(i)}(\beta_{j,1}))$$

avec $\alpha$ un entier algébrique fonction des $\beta_{j,k}$, $j,k = 1 \ldots n_t$. Le déterminant dépend de la constellation utilisée, et la construction du code ne donne aucune garantie quand à sa diminution lorsque l'efficacité spectrale augmente.

Le code construit satisfait le critère de l'information mutuelle, puisque la matrice génératrice obtenue par vectorisation de la matrice mot de code une matrice unitaire.

## 2.9 Code TAST

En utilisant le principe du codage LST et la théorie algébrique des nombres, un code ST algébrique en couche, appelé code TAST, a été construit dans [20]. Ce code permet d'avoir un rendement plein, une diversité pleine, et est décodable par les décodeurs de réseaux de points. Un schéma de codage similaire a été présenté dans [35]. Les codes présentés dans le paragraphe précédent, le code $2 \times 2$ et sa généralisation sont des codes TAST.

L'idée du codage TAST consiste à associer à chaque couche un sous-espace algébrique, de telle façon que les couches soient transparentes les unes par rapport aux autres. Ceci permet d'avoir une parfaite suppression de l'interférence. L'utilisation de codes DAST paramétrés sur chaque couche permet d'atteindre la diversité maximale.

Les couches sont construites de façon à ce que chaque couche exploite toute la diversité spatio-temporelle. En effet, pendant chaque temps symbole, chaque couche émet un symbole en utilisant une antenne différente, ainsi toutes les couches sont équivalentes en terme d'utilisation canal. Construire ainsi les couches permet de garantir que l'interférence spatiale observée par une couche ne provient que des autres couches. Une répartition optimale possible des couches est présentée dans la figure 2.7.

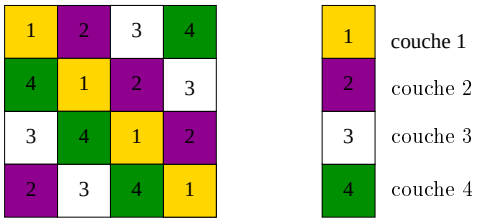



Fig. 2.7: Répartition des couches dans un code TAST

Pour les codes LD, une contrainte est imposée au nombre de sous-trames afin d'avoir un décodage plus simple. En ce qui concerne les codes TAST, pour pouvoir les décoder par un décodeur de réseaux de points ML, il faut que le nombre de couches soit égal à $\min(n_t,n_r)$.

Soit $L$ le nombre de couches. Soit $\mathbf{a} = (a_1,a_2,\ldots,a_K)^T$ le vecteur des symboles d'information divisé en sous vecteur $\mathbf{v_1},\ldots,\mathbf{v_L}$ de longueurs respectifs $K_1,\ldots,K_L$, tel que $K_1+K_2+\cdots+K_L = K$. Soit $\mathbf{M_1},\ldots,\mathbf{M_L}$ des rotations à diversité de modulation pleine et ayant des distances produits minimales maximisées. Les vecteurs de symboles codés correspondant à chaque couche seront :

$$\mathbf{x_j} = \phi_j \cdot \mathbf{M_j}.\mathbf{v_j},\ j = 1\ldots L$$

avec $\phi_1,\ldots,\phi_L \in \mathbb{C}$. Le choix de $\phi_1,\ldots,\phi_L$ est déterminant dans la maximisation de la diversité et du gain de codage.

Il existe deux types de codes TAST, les **codes TAST symétriques** et **les codes TAST asymétriques**. Les codes TAST symétriques sont tels que $K_1 = K_2 = \cdots = K_L = n_t$, et une même rotation est utilisée pour toutes les couches. Le rendement de ces codes est $L$ symboles/uc. Il a été démontré dans [20], que choisir $\phi_1,\ldots,\phi_L$ tels qu'ils ont une mauvaise approximation diophantienne par des nombres algébriques, permet de maximiser le gain de codage. El Gamal et Damen ont établi les deux théorèmes suivants dans [20] donnant des constructions possibles

de codes TAST symétriques.

**Théorème : 2.1** *Le code TAST symétrique, utilisant la matrice de rotation* **M**, *une constellation* $q-QAM$, *et* $\{\phi_1 = 1, \phi_2 = \phi^{1/n_t}, \ldots, \phi_L = \phi^{(L-1)/n_t}\}$ *atteint la diversité maximale si* $\phi$ *est un entier algébrique tel que* $\{1, \phi, \ldots, \phi^{L-1}\}$ *est algébriquement indépendant dans le corps de nombres contenant les éléments de la matrice de rotation* **M**.

**Théorème : 2.2** *Le code TAST symétrique, utilisant la matrice de rotation* **M**, *une constellation* $q-QAM$, *et* $\{\phi_1 = 1, \phi_2 = \phi^{1/n_t}, \ldots, \phi_L = \phi^{(L-1)/n_t}\}$ *atteint la diversité maximale si* $\phi = \exp(i\lambda)$ *avec* $\lambda \neq 0$ *algébrique (par la suite* $\phi$ *est transcendant).*

Le choix de $\phi$ algébrique permet de connaître de façon exacte les limites de l'approximation des $\phi_j$, $j = 1 \ldots L$ par d'autres nombres algébriques, et d'avoir une borne minimale sur le gain de codage.

Les codes TAST asymétriques n'utilisent pas une même rotation pour toutes les couches. Il a été proposé dans [20] d'utiliser des codes DAST pour certaines couches et des codes à répétition pour d'autres. Ces codes ont des rendements fractionnés, et une diversité maximale.

Le gain de codage des codes TAST s'écrit en fonction de l'approximation diophantienne des $\phi_j$, $j = 1 \ldots L$ par des nombres algébriques. Plus la taille de la constellation est grande, mieux l'approximation est et donc plus faible est le gain de codage. Le gain de codage des codes TAST s'évanouit lorsque la taille de la constellation augmente. Par contre, dans quelques cas particuliers, comme le code d'Alamouti (qui est aussi un code TAST), le gain de codage est une somme de normes au carré, donc indépendant de la taille de la constellation.

## 2.10 Codes ST algébriques à partir d'algèbres de division

L'algèbre de division est un outil mathématique très intéressant et très fort qui permet de construire des codes ST ayant une diversité pleine. En effet, une algèbre de division est un anneau dans lequel tout élément non nul a un inverse pour la multiplication. Le premier exemple à citer est le code d'Alamouti qui peut être défini à partir de l'algèbre des quaternions de Hamilton.

Dans le chapitre I, deux classes d'algèbre de division ont été présentées ainsi que leurs représentations matricielles. En utilisant les algèbres de division, Sethuraman et Rajan dans [36, 9], ont construit des codes ST de rendement compris entre 1 et $n_t$ symboles/uc, et de diversité pleine. Deux types de constructions sont proposées. Les constructions basées sur des corps de nombres et les constructions basées sur des algèbres de division non-commutatives construites à partir de corps de nombres. Les extensions utilisées sont choisies en fonction du nombre d'antennes à l'émission $n_t$ et en fonction de l'alphabet utilisé.

Tous les codes ST construits à partir d'algèbre de division sont des codes LD. En effet on peut voir ça directement à partir de la décomposition d'un élément de l'algèbre sous la forme d'une somme de matrices. Cette représentation correspond à la structure d'un code LD avec les matrices $B_i = A_i, i = 1 \cdots n$.

### 2.10.1 Codes ST à partir de corps de nombre

Soit $A$ l'alphabet dans lequel les symboles d'information vont être pris. $A$ est un sous-ensemble fini de $\mathbb{C}$, soit $m$ son cardinal. Le corps de base $F$ sera défini en fonction de l'alphabet, en effet $F$ sera engendré par les éléments de $A$. Par exemple si la constellation utilisée est une $q$-QAM, alors $F = \mathbb{Q}(i)$. Soit $K = F(\alpha)$ une extension de $F$ de degré $n_t$, on a alors :

$$\mathbb{Q} \subset \mathbb{Q}(A) = F \subset \mathbb{Q}(A,\alpha) = F(\alpha) = K$$

$K$ étant un corps, c'est alors une algèbre de division et peut être représenté sur $\mathcal{M}_{n_t}(F)$. Soit $x^{n_t} - \gamma$ un polynôme irréductible sur $F[x]$, avec $\gamma \in F$. Le code ST est défini comme un sous-ensemble fini de $K$ obtenu en restreignant les symboles d'information à $A$. D'après la représentation matricielle des éléments de l'algèbre de division donnée dans le paragraphe 1.3.3.1, un mot de code s'écrit :

$$\mathbf{X} = \begin{bmatrix} f_1 & f_2 & \cdots & f_{n_t} \\ \gamma f_{n_t} & f_1 & \cdots & f_{n_t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma f_2 & \gamma f_3 & \cdots & f_1 \end{bmatrix}$$

avec $f_j \in A$, $j = 1 \ldots n_t$. Le code ST ainsi défini est de rang plein, puisque $K$ est une algèbre de division, et de rendement 1 symbole/uc.

Le paramètre clef dans la construction des codes ST, une fois le corps de nombres $F$ défini, est de trouver un polynôme irréductible de degré $n_t$ sur $F[x]$ afin de construire $K$.

Dans [9], deux types de constructions de codes ST ont été présentées. L'une basée sur des extensions cyclotomiques et l'autre sur des extensions à partir de nombres transcendants. Les rendements de ces codes sont supérieurs ou égaux à 1 symbole/uc.

#### 2.10.1.1 Extensions cyclotomiques

Les codes construits à partir d'extension cyclotomique suppose que la constellation utilisée est une $m$-PSK, d'où $F = \mathbb{Q}(w_m)$, avec $w_m = \exp(i2\pi/m)$ la $m^{\text{ième}}$ racine de l'unité. Reste à trouver $n_t$ tel qu'il existe un polynôme irréductible de degré $n_t$ défini sur $\mathbb{Q}(w_m)$. Il a été prouvé dans [9], que pour tout $n_t$ tel que tous les facteurs premiers qui apparaissent dans la factorisation de $n_t$ forment un sous-ensemble de ceux de $m$, et tout $l$ premier avec $m$, le polynôme $x^{n_t} - w_m^l$ est irréductible sur $\mathbb{Q}(w_m)$.

Par exemple, soit la constellation 6-PSK, le polynôme $x^3 - w_6$ est irréductible sur $\mathbb{Q}(w_6)$. Le mot de code est défini comme suit

$$\mathbf{x} = \begin{bmatrix} s_1 & s_2 & s_3 \\ w_6 s_3 & s_1 & s_2 \\ w_6 s_2 & w_6 s_3 & s_1 \end{bmatrix}$$

avec $s_j$, $j = 1 \ldots 3$ des symboles 6-PSK.

Ce code est caractérisé par le fait qu'il est entièrement défini sur l'alphabet (tous les éléments de la matrice mot de code sont dans l'alphabet), puisqu'il est invariant par multiplication par $w_6$. Étant données les contraintes imposées sur le choix de $n_t$, ce code ne peut être construit pour $n_t$ quelconque. Sethuraman et Rajan ont annulé les contraintes sur le choix de $n_t$, afin de

pouvoir construire des codes ST pour $n_t$ quelconque.

L'idée est de choisir la constellation PSK à utiliser et le nombre d'antennes à l'émission $n_t$ et de chercher le corps $K$. Soit la constellation $M$-PSK, et soit un nombre d'antennes à l'émission $n_t$ fixé. Soit $m$ un entier, tel que les nombres premiers apparaissant dans la factorisation de $M$ et de $n_t$ forment des sous-ensembles dans l'ensemble des nombres premiers apparaissant dans la factorisation de $m$. Et soit $l$ premier avec $m$, alors le polynôme $x^{n_t} - w_m^l$ est irréductible sur $\mathbb{Q}(w_m)$.

Par exemple, soit la constellation 6-PSK, et $n_t = 5$. $m = 30$ est une solution possible. Le polynôme $x^5 - w_{30}$ est irréductible sur $\mathbb{Q}(w_{30})$. En prenant $m$ multiple de 4, par exemple $m = 60$, la constellation utilisée peut être la 16-QAM.

Les codes exposés jusqu'à présent sont de rendement 1 symbole/uc. En exploitant les emboîtements des extensions algébriques, Sethuraman et Rajan ont construit des codes ST ayant des rendements plus élevés.

Soient $M$, $n_t$ et $m$ définis comme précédemment. Comme $M$ divise $m$, alors $\mathbb{Q}(w_M) \subset \mathbb{Q}(w_m)$. Ainsi tout élément $x$ de $\mathbb{Q}(w_m)$ peut s'écrire comme combinaison linéaire de la base de $\mathbb{Q}(w_m)$, $\mathbb{Q}(w_m)$ vu comme espace vectoriel sur $\mathbb{Q}(w_M)$. Pour un rendement $R$ donné, on peut considérer $m$ tel que tous les facteurs premiers de la factorisation de $R$ forment un sous ensemble de ceux de $m$. Alors $\mathbb{Q}(w_m) \subset \mathbb{Q}(w_{mR})$, et tout $x \in \mathbb{Q}(w_{mR})$ s'écrit $x = \sum_{j=0}^{R} f_j w_{mR}^j$. Soit $n_t$ tel que tous ces facteurs premiers forment un sous ensemble de ceux de $mR$. On a alors $x^{n_t} - w_{mR}$ irréductible sur $\mathbb{Q}(w_{mR})$. En prenant comme entrées de la matrice mot de code les éléments de $\mathbb{Q}(w_{mR})$ écrits sous cette forme $\sum_{j=0}^{R} f_j w_{mR}^j$, on obtient un code de rendement $R$ symboles/uc. Cette construction est limitée par toutes les contraintes imposées sur le choix de $R$, $m$ et $n_t$.

#### 2.10.1.2 Extension à partir de nombres transcendants

A cause des limitations rencontrées lors de l'utilisation des nombres algébriques, Sethuraman et Rajan ont pensé à utiliser les nombres transcendants. Ces derniers ont déjà été utilisés dans les constructions des codes présentés dans [18, 20]. Rappelons qu'un nombre transcendant est un nombre qui n'est pas algébrique.

**Proposition : 2.1** *Soient un corps $F$ de caractéristique zéro, et $z$ une indéterminée. $F(z)$ est le corps des fonctions rationnelles en $z$. Tout $x \in F(z)$, s'écrit $x = \frac{p(z)}{q((z)}$, avec $p(z)$ et $q(z)$ deux polynômes définis sur $F$. On a alors pour tout $n \geq 1$, le polynôme $x^n - z$ est irréductible sur $F(z)[x]$. Si $z$ est transcendant sur $\mathbb{Q}$, $z$ est transcendant sur toute extension algébrique de $\mathbb{Q}$.*

Soit la constellation $m$-PSK, et soit $z$ un nombre transcendant sur $\mathbb{Q}$. Le corps d'extension sur lequel le code ST va être construit est $F = \mathbb{Q}(w_m, z)$. D'après la définition précédente $x^{n_t} - z$ est irréductible sur $F$. Le mot de code s'écrit :

$$\mathbf{X} = \begin{bmatrix} f_1 & f_2 & \cdots & f_{n_t} \\ z f_{n_t} & f_1 & \cdots & f_{n_t-1} \\ \vdots & \vdots & \ddots & \vdots \\ z f_2 & z f_3 & \cdots & f_1 \end{bmatrix}$$

Étant donné que l'extension de $\mathbb{Q}(w_m)$ à $\mathbb{Q}(w_m,z)$ est de degré infini, alors tout élément $x \in \mathbb{Q}(w_m,z)$ peut s'écrire $x = \sum_{j=0}^{R} f_j z^j$, avec $f_j \in \mathbb{Q}(w_m)$, $0 \dots R$, $R$ quelconque. En considérant un nombre transcendant quelconque $\gamma$, le mot de code s'écrit :

$$X = \begin{bmatrix} \sum_{j=0}^{R} f_{j,1} z^j & \sum_{j=0}^{R} f_{j,2} z^j & \dots & \sum_{j=0}^{R} f_{j,n_t} z^j \\ \gamma \sum_{j=0}^{R} f_{j,n_t} z^j & \gamma \sum_{j=0}^{R} f_{j,1} z^j & \dots & \sum_{j=0}^{R} f_{j,n_t-1} z^j \\ \vdots & \vdots & \ddots & \vdots \\ \gamma \sum_{j=0}^{R} f_{j,2} z^j & \gamma \sum_{j=0}^{R} f_{j,3} z^j & \dots & \sum_{j=0}^{R} f_{j,1} z^j \end{bmatrix}$$

Soient $s_1$,$s_2$,$s_3$et $s_4$ les symboles d'information appartenant à la constellation 4-PSK. Soit $z$ un nombre transcendant sur $\mathbb{Q}$. Le mot de code s'écrit :

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} s_1 + s_2 z & z(s_3 + s_4 z) \\ s_3 + s_4 z & s_1 + s_2 z \end{bmatrix}$$

Le facteur $1/\sqrt{2}$ permet de normaliser l'énergie transmise par chaque antenne.

Il a été montré dans [36, 9] que le gain de codage des codes ST construits à partir d'extension utilisant des nombres transcendants est supérieur à celui des codes ST construits à partir d'extensions cyclotomiques. Ce qui confirme les résultats de [17, 20].

### 2.10.2 Codes ST à partir d'algèbres cycliques de division

Sethuraman et Rajan ont construit une deuxième classe de codes ST à partir d'algèbre cyclique de division non commutative.

D'après la définition 1.1, si $F$ est un corps et $K$ est une extension galoisienne cyclique de degré $n$ de $F$, $Gal(K/F)$ est engendré par $\sigma$, et $\gamma \in F^*$alors $\mathcal{A} = (K/F,\sigma,\gamma)$ est une algèbre cyclique de division si et seulement si $\gamma,\gamma^2,\dots,\gamma^{n-1}$ ne sont pas des normes sur $K$. Le point critique dans les constructions d'algèbre de division non-commutative à partir d'extension algébrique est donc le choix de $\gamma$. Dans [36, 9], les auteurs ont opté pour le choix de $\gamma$ transcendant et ils ont démontré que $(K(\gamma)/F(\gamma),\sigma,\gamma)$ est une algèbre de division. En étendant l'action de $\sigma$ de $K$ sur $K(\gamma)$, et en définissant $\sigma(\gamma) = 1$, il peut être démontré que $\gamma,\gamma^2,\dots,\gamma^{n-1}$ ne sont pas des normes sur $K(\gamma)$.

Afin d'avoir la même énergie de transmission sur toutes les antennes émettrices, $\gamma$ doit être sur le cercle unité. Une fois $\gamma$ fixé, il reste donc à construire $F(\gamma)$ et son extension cyclique $K(\gamma)$ qui ne dépend que du choix de la constellation.

Soit la constellation $m$-PSK, et soit $n_t$ fixé tel que $m$ soit multiple de $n_t$. Le polynôme $x^{n_t} - w_{mn_t}$ est irréductible sur $F[x]$, alors $F = Q(w_m,\gamma)$, et $K = F(w_{mn_t})$. Le code ST est à présent entièrement défini. Le mot de code $\mathbf{X}$ s'écrit :

$$\mathbf{X} = \begin{bmatrix} k_1 & k_2 & \dots & k_{n_t} \\ \gamma\sigma(k_{n_t}) & \sigma(k_1) & \dots & \sigma(k_{n_t-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n_t-1}(k_2) & \gamma\sigma^{n_t-1}(k_3) & \dots & \sigma^{n_t-1}(k_1) \end{bmatrix}$$

et le rendement est de 1 symbole/uc.

Sachant que $K$ est une extension galoisienne de $F$, et la base de $K$ sur $F$ est $(1,w_m,\ldots,w_m^{n_t-1})$, alors tout $x \in K$ s'écrit $x = \sum_{j=0}^{n_t-1} f_j w_m^j$. En remplaçant dans le mot de code $\mathbf{X}$ les symboles pris dans $K$ par des combinaisons linéaires de symboles pris dans $K$ on obtient un code ST de rendement $n_t$ symboles/uc.

Exemple : soient $n_t = 2$ et $F = \mathbb{Q}(i)$ et soit l'extension cyclique de $F$, $K = \mathbb{Q}(\sqrt{i})$, $\sigma : \sqrt{i} \mapsto -\sqrt{i}$. Soit $\gamma$ transcendant sur $F$. La base de $K$ sur $F$ est $(1, \sqrt{i})$. $(K(\gamma)/F(\gamma),\sigma,\gamma)$ est une algèbre cyclique de division, le code de rendement plein est défini comme suit :

$$\mathbf{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} s_1 + s_2\sqrt{i} & s_3 + s_4\sqrt{i} \\ \gamma(s_3 - s_4\sqrt{i}) & s_1 - s_2\sqrt{i} \end{bmatrix}$$

Dans cette construction le problème du choix de $\gamma$ est résolu, reste le choix de $m$ et $n_t$ qui est assez limité. De la même façon que pour le cas des extensions cyclotomiques, Sethuraman et Rajan ont opté pour l'utilisation des extensions à partir de nombres transcendants utilisant le théorème suivant :

**Théorème : 2.3** *Soit $F = \mathbb{Q}(w_m,z)$ avec $z$ transcendant sur $\mathbb{Q}$, alors $K = F(\sqrt[n]{z})$ est une extension cyclique de $F$ de degré $n$.*

Nous allons illustrer cette construction par l'exemple qui suit. Soient $n_t = 2$ et $t$ transcendant sur $\mathbb{Q}$, et soit la constellation 4-PSK. $F$ est égal à $\mathbb{Q}(i)$, $K = F(\sqrt{t})$ et $\sigma : t \mapsto -t$. Soit $\gamma$ un nombre transcendant sur $\mathbb{Q}$. Le code ST de rendement plein est donné par son mot de code :

$$\mathbf{X} = \begin{bmatrix} s_1 + s_2\sqrt{t} & s_3 + s_4\sqrt{t} \\ \gamma(s_3 - s_4\sqrt{t}) & s_1 - s_2\sqrt{t} \end{bmatrix}$$

Les codes construits à partir d'algèbre cyclique de division utilisant les nombres transcendants généralisent toutes les constructions présentées dans [18, 20] utilisant les nombres transcendants. Pour voir cette généralisation, il faut faire une transformation de ces derniers codes pour les mettre sous la même forme que les codes construits à partir d'algèbre de division. Pour cela, la matrice $\mathbf{T}$, $\mathbf{T} = \mathrm{diag}(\gamma^{n_t-(2k+1)})_{k=0\ldots n_t-1}$, peut être utilisée. Soit $\mathbf{X}$ le mot de code du code ST défini dans [18, 20], le mot de code obtenu par la transformation $T$ est :

$$\mathbf{X}' = \mathbf{T} \cdot \mathbf{X} \cdot \mathbf{T}^{-1}$$

Le déterminant de la matrice $\mathbf{T}$ est égal à 1, alors cette transformation préserve toutes les propriétés du code, le gain de codage et la diversité.

Soit le code $2 \times 2$ présenté dans [18], avec $\theta$ transcendant. Un mot de code $\mathbf{X}$ s'écrit, après transformation par $\mathbf{T}$, sous la forme suivante :

$$\mathbf{X}' = \begin{bmatrix} s_1 + \theta s_2 & \sqrt{\theta} \cdot (s_3 + \theta s_4) \\ \sqrt{\theta} \cdot (s_3 - \theta s_4) & s_1 - \theta s_2 \end{bmatrix}$$

avec $s_j, 1 \ldots 4$ des symboles 4-QAM. $\mathbf{X}'$ correspond exactement au code présenté dans le dernier exemple en prenant $\gamma = t$.

## 2.11 Codes ST algébriques à partir de rotations réelles

Les codes ST DAST, algébrique de [18, 19], TAST et ceux construits à partir d'algèbre de division utilisent des rotations complexes. Dans [21, 22], l'idée est d'utiliser des rotations réelles pour construire des codes ST ayant une diversité pleine, un rendement plein et un déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Les codes construits se limite à la dimension 2, $n_t = 2$ et $n_r \geq 2$.

Soit la rotation réelle **R** :

$$\mathbf{R} = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

Le code proposé par Yao et Wornell utilise deux rotations d'angles respectifs $\theta_1$ et $\theta_2$ sur chaque couche (la structure des couches est celle utilisée pour les codes TAST) . Un mot de code **X** est défini comme suit :

$$\mathbf{X} = \begin{bmatrix} s_1\cos(\theta_1) + s_2\sin(\theta_1) & s_3\cos(\theta_2) + s_4\sin(\theta_2) \\ -s_3\sin(\theta_2) + s_4\cos(\theta_2) & -s_1\sin(\theta_1) + s_2\cos(\theta_1) \end{bmatrix}$$

avec $s_j$, $j = 1 \ldots 4$ des symboles $q$-QAM. Il a été démontré dans [21], par une optimisation numérique que le couple ($\theta_1$,$\theta_2$) maximisant le déterminant minimal est ($\frac{1}{2}$arctan($\frac{1}{2}$),$\frac{1}{2}$arctan(2)). Le déterminant minimal correspondant est :

$$|\det(X_1 - X_2)|_{X_1, X_2 \in C, X_1 \neq X_2} = \sin(2\theta_1)\frac{1}{2\sqrt{5}}$$

Pour le couple ($\frac{1}{2}$arctan($\frac{1}{2}$),$\frac{1}{2}$arctan(2)), il a été prouvé que le déterminant ne s'annule jamais et donc la diversité maximale est atteinte. La construction du code ST ne garantit pas la diversité maximale, c'est plutôt le choix de $\theta_1$et $\theta_2$ qui le détermine. D'autres couples ($\theta_1$,$\theta_2$), tel que $\theta_2 = \frac{\pi}{4} - \theta_1$, ont été donnés permettant d'atteindre la diversité maximale donnant des déterminants minimaux plus faibles.

La construction du code ST faite par Dayal et Varanasi dans [22] est similaire à la construction TAST, remplaçant une rotation complexe par une rotation réelle. La même rotation est utilisée sur les deux couches, et un paramètre $\phi$ permet de les dissocier afin d'atteindre la diversité maximale. Le mot de code s'écrit :

$$\mathbf{X} = \begin{bmatrix} s_1\cos(\theta) + s_2\sin(\theta) & \phi(s_3\cos(\theta) + s_4\sin(\theta)) \\ \phi(-s_3\sin(\theta) + s_4\cos(\theta)) & -s_1\sin(\theta) + s_2\cos(\theta) \end{bmatrix}$$

où $s_j, j = 1 \ldots 4$ des symboles $q$-QAM. Le couple ($\theta$,$\phi$) maximisant le gain de codage, avec $\left|\phi\right| = 1$ préservant une même énergie de transmission pour toutes les antennes, est ($\frac{1}{2}\tan^{-1}(2), -i$). La rotation **R** avec $\theta = \frac{1}{2}\tan^{-1}(2)$ correspond à la rotation optimale au sens de la distance produit minimale. Il a été prouvé dans [22], que pour le couple ($\frac{1}{2}$artan(2), $-i$), la diversité maximale est atteinte, et le déterminant minimal est :

$$|\det(X_1 - X_2)|_{X_1, X_2 \in C, X_1 \neq X_2} = \cos(2\theta)$$

Ces deux constructions aboutissent aux même codes. Ces codes sont intéressants à cause de leurs propriétés : rendement plein, diversité pleine et déterminant minimal indépendant de la constellation utilisée.

## Conclusion

Dans ce chapitre nous avons présenté l'état de l'art des codes ST en blocs. Il s'est avéré que pour une exploitation optimale des ressources spectrales, il serait intéressant d'avoir un rendement plein. Ainsi, en se basant sur ce critère, nous pouvons partager les codes ST en deux groupes. Le premier correspond aux codes ST ayant un rendement qui n'est pas plein, qui inclut le code d'Alamouti, les codes orthogonaux, les codes par couches et les codes DAST. Le deuxième, qui nous intéresse plus, correspond aux codes ST ayant un rendement plein, dans lequel nous trouvons le code algébrique de Damen *et al.* et ses généralisations, le code TAST, les codes construits à partir d'algèbres de division. Ces codes se caractérisent par un ordre de diversité maximal, cependant, leur faiblesse apparaît au niveau du déterminant minimal qui s'évanouit lorsque l'efficacité spectrale augmente.

Dans un travail récent de Elia *et al.* [29], il a été montré, qu'un code ST linéaire, de rendement plein ayant un déterminant minimal ne s'évanouissant lorsque l'efficacité spectrale augmente atteint le compromis gain de multiplexage-diversité. D'où l'importance d'avoir des codes ST ayant des déterminants minimaux ne s'évanouissant pas.

# Chapitre 3

# Constructions algébriques de codes Espace-Temps en blocs

## Introduction

L'état de de l'art sur les codes ST, établi au chapitre précédent, nous a permis de déceler que les meilleurs codes ST [18, 19, 20, 9] dans la littérature sont ceux qui disposent d'un rendement plein et atteignent une diversité maximale pour un nombre d'antennes émettrices égal à la longueur temporelle du code. L'utilisation des nombres transcendants dans la construction de ces codes induit des déterminants minimaux qui s'évanouissent lorsque l'efficacité spectrale augmente. Cette propriété devient pénalisante lorsqu'une modulation codée par bloc est appliquée à la sortie du codeur espace-temps, il serait nécessaire d'augmenter la taille de la constellation en vue de préserver une même efficacité spectrale (fig. 3.1).

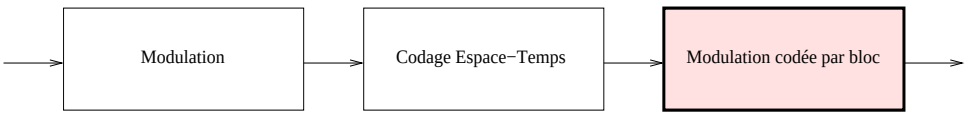



FIG. 3.1: Application d'une modulation codée par bloc en sortie du codage Espace-Temps

Par ailleurs, récemment dans [37, 29], il a été démontré que de point de vue compromis gain de multiplexage-diversité, il est important d'avoir des déterminants minimaux ne s'évanouissant pas.

A partir de ce qui a précédé comme analyses et constatations, construire un code ST en bloc ayant un rendement plein, une diversité maximale avec en plus des déterminants minimaux discrets se révèle du pari, surtout qu'à ce jour, aucun code ST ne réunit de telles propriétés.

La première étape de notre travail a abouti à la construction de nouveaux codes ST appelés "codes quaternioniques". Les performances de ces codes sont fortement pénalisées par la répartition non uniforme de l'énergie au sein du mot de code. Nous avons alors construit une nouvelle famille de codes ST, que nous avons appelés "codes parfaits". Ces derniers disposent des mêmes propriétés que les codes quaternioniques, avec de plus, une bonne efficacité éner-

gétique. En s'inspirant de la construction et de la structure des codes parfaits, nous proposons aussi des "codes parfaits rectangulaires", où la longueur temporelle du code est supérieure aux nombre d'antennes à l'émission.

Après présentation d'une première approche de construction des codes ST ayant des déterminants discrets, nous détaillerons les codes quaternioniques. Nous introduirons par la suite une deuxième approche de construction de codes ST disposant à la fois de déterminants discrets et de bonnes distributions énergétiques. Nous présenterons par la suite la construction algébrique ainsi que les performances des codes parfaits découlant de cette deuxième approche. Suit la preuve montrant que les codes quaternioniques et les codes parfaits atteignent le compromis gain de multiplexage-diversité. La dernière partie sera consacrée à la présentation de la construction et des performances des codes parfaits rectangulaires.

## 3.1 Première approche de construction des codes ST

Avant d'aborder la construction proprement dite des codes ST, nous allons commencer par spécifier les critères que doivent vérifier ces codes. Ces critères concernent le rendement, l'ordre de diversité et le déterminant minimal. Une fois l'approche de la construction définie, nous nous intéresserons à sa validation.

### 3.1.1 Critères de constructions

Nous nous intéressons aux codes ST, tels que la longueur temporelle du code soit égale au nombre d'antennes émettrices, $n_t = T$. Le mot de code est donc une matrice carrée de dimension $n_t \times n_t$. C'est pourquoi nous qualifierons ces codes de "codes carrés".

Nous avons introduit au paragraphe (2.2) les critères de construction des codes ST permettant de maximiser l'ordre de diversité, le gain de codage et la capacité. Ainsi, pour la construction de nos codes ST, nous imposons trois critères basés sur le critère du rang et du déterminant :

1. *Rendement plein* : pour une exploitation optimale des ressources spectrales, le nombre de symboles d'information transmis doit être égal à $n_t \cdot T = n_t^2$.
2. *Diversité pleine* : le code doit vérifier le critère du rang (def. 2.2). Il pourra ainsi atteindre l'ordre de diversité maximal égal à $n_t \cdot n_r$.
3. *Déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente* : le code doit vérifier le critère du déterminant afin de maximiser le gain de codage (def. 2.3) . Nous imposons de plus au code un déterminant minimal ne s'évanouissant pas lorsque la taille de la constellation augmente. Cela se traduit sur les codes ST infinis par un déterminant minimal ne s'annulant pas et une distribution discrète des déterminants.

### 3.1.2 Démarche de la construction

Notre choix concernant la construction des nouveaux codes ST s'est porté sur une méthode algébrique. Ce choix s'est imposé pour deux raisons principales. D'abord, les constructions algébriques des codes ST sont parmi les meilleures dans la littérature. Ensuite, l'utilisation d'outils algébriques permet plus de souplesse dans le contrôle des différents paramètres du code. Ainsi, notre approche se basera sur l'algèbre cyclique de division construite sur des corps de nombres. C'est un outil mathématique très intéressant et suffisamment puissant pour la

construction de codes ST.

Notre approche se compose de 5 étapes :

| |
|---|
| 1 - Choix du corps de base |
| 2- Choix du corps d'extension |
| 3- Définition de l'algèbre cyclique |
| 4- Choix de $\gamma$ |
| 5- Définition du code ST |

Dans [9], des codes ST ont été construits à partir d'algèbres cycliques de division sur des corps transcendants $(K[\gamma]/L[\gamma],\sigma,\gamma)$, où $\gamma$ est un nombre transcendant, $L$ un corps et $K$ une extension cyclique de $L$.

Toutes les définitions d'algèbre nécessaires à l'établissement des résultats de ce chapitre se trouvent au paragraphe (1.3.3).

**1- Choix du corps de base**

Le corps de base représente le corps sur lequel les corps d'extension sont définis et auquel les symboles d'information appartiennent. Nous considérons comme corps de base $L = \mathbb{Q}(i)$ ou $L = \mathbb{Q}(j)$. Nous prenons en conséquence comme constellations une $q$-QAM ou une $q$-HEX puisqu'elles sont des sous-ensembles finis respectivement de $\mathbb{Z}[i]$ et de $\mathbb{Z}[j]$ (fig. 1.2, 1.3).

**2- Choix du corps d'extension**

Le corps d'extension est le corps sur lequel l'algèbre cyclique de division est construite. Dans notre cas, nous devons alors choisir un corps d'extension cyclique $K$ de $L$ de degré $n_t$ sur $L$ (def. 1.15). Définissons $\sigma$ le générateur du groupe de Galois de $K$, $Gal(K/L)$.

**3- Définition de l'algèbre cyclique**

Soit $\gamma \in L$. D'après la définition 1.35, $\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre cyclique de degré $n_t$.

**4- Choix de $\gamma$**

Pour que l'algèbre $\mathcal{A}$ soit une algèbre de division il faut que $\gamma,\gamma^2,\ldots,\gamma^{n_t-1}$ ne soient pas des normes sur $K^*$ (lemme 1.1). De plus, il faut que $\gamma$ soit dans $\mathbb{Z}[i]$ ou dans $\mathbb{Z}[j]$, afin de garantir un déterminant minimal du code ST ne s'évanouissant pas.

**5- Construction du nouveau code ST**

Dans le paragraphe (1.3.3.3), nous avons démontré que l'algèbre cyclique de division a une représentation dans $M_{n_t}(K)$ et nous avons donné la représentation matricielle des éléments de l'algèbre. Soit $(\mathbf{I}_{n_t}, \mathbf{e}, \mathbf{e}^2, \cdots, \mathbf{e}^{n_t-1})$ la base de l'algèbre, avec $\mathbf{e}$ défini comme suit :

$$\mathbf{e} = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & 1 \\ \gamma & 0 & \cdots & 0 \end{bmatrix}$$

Tout élément $\mathbf{X}$ de $K$ s'écrit sous la forme matricielle suivante :

$$\mathbf{X} = \mathbf{x_0 I} + \mathbf{x_1 e} + \cdots + \mathbf{x_{n_t-1} e}^{n_t-1}$$

les $\mathbf{x_i} \in K$, $i = 1 \cdots n_t$, sont les coordonnées de $\mathbf{X}$ dans la base de l'algèbre. $\mathbf{X}$ s'écrit aussi sous la forme suivante :

$$\mathbf{X} = \begin{bmatrix} x_0 & x_1 & \cdots & x_{n_t-1} \\ \gamma\sigma(x_{n_t-1}) & \sigma(x_0) & \cdots & \sigma(x_{n_t-2}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n_t-1}(x_1) & \gamma\sigma^{n_t-1}(x_2) & \cdots & \sigma^{n_t-1}(x_0) \end{bmatrix} \tag{3.1}$$

Nous définissons alors le code ST comme un sous-ensemble fini de l'algèbre de division obtenu en se restreignant à l'anneau des entiers $O_K$ (def. 1.24) ou à un idéal $I$ de l'anneau des entiers. L'équation 3.1 définit alors un mot de code $\mathbf{X}$ du code ST.

### 3.1.3 Validation de l'approche

La démarche présentée ci-dessus a abouti à la définition d'un nouveau code ST. La validation de l'approche passera par la vérification des critères déjà définis.

– **Rendement plein**

Si, dans le mot de code défini dans l'équation 3.1, les $x_i$ représentaient les symboles d'information, le code ST aurait seulement un rendement égal à 1 symbole/uc.

Pour obtenir le rendement plein, il faut s'appuyer sur le fait que $K$ est un espace vectoriel sur $L$. Soit $B = (v_k)_{k=1\ldots n_t}$ une base canonique de $K$. Les $x_i$, $i = 1 \cdots n_t$ s'écrivent alors :

$$x_l = \sum_{k=1}^{n_t} s_{l,k} v_k$$

où $s_{l,k}$,$l$,$k = 1 \cdots n_t$ représentent les symboles d'information pris dans $O_L$. Ainsi, chaque élément de la matrice mot de code est une combinaison linéaire de $n_t$ symboles d'information, et le rendement du code est $n_t$ symboles/u.c. Le mot de code devient alors :

$$\mathbf{X} = \begin{bmatrix} \sum_{i=1}^{n_t} s_{1,i} v_i & \sum_{i=1}^{n_t} s_{2,i} v_i & \cdots & \sum_{i=1}^{n_t} s_{n_t,i} v_i \\ \gamma\sigma(\sum_{i=1}^{n_t} s_{n_t,i} v_i) & \sigma(\sum_{i=1}^{n_t} s_{1,i} v_i) & \cdots & \sigma(\sum_{i=1}^{n_t} s_{n_t-1,i} v_i) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n_t-1}(\sum_{i=1}^{n_t} s_{2,i} v_i) & \gamma\sigma^{n_t-1}(\sum_{i=1}^{n_t} s_{3,i} v_i) & \cdots & \sigma^{n_t-1}(\sum_{i=1}^{n_t} s_{1,i} v_i) \end{bmatrix}$$

– **Diversité maximale**

La diversité maximale est une conséquence directe de l'utilisation des algèbres de division. En effet, par définition, tout élément de l'algèbre de division est inversible. Par conséquent, le code ST construit est de rang plein et la diversité maximale est atteinte.

– **Déterminant minimal discret :**

La construction du code ST sur l'anneau des entiers de $K$ est la clé pour l'obtention des déterminants minimaux discrets. Nous pouvons facilement remarquer que tous les coefficients de la matrice mot de code $\mathbf{X}$ sont dans $O_K$. Cette remarque en résulte de deux points. Le premier est que $\gamma \in O_K$ et le deuxième est que pour tout $x_j \in O_K$, $\sigma^i(x_j)$, pour $i = 1 \cdots n_t - 1$ et $j = 1 \cdots n_t$,

appartient aussi à $\mathcal{O}_K$. Nous déduisons alors que le déterminant de $\mathbf{X}$ appartient aussi à $\mathcal{O}_K$.

D'après le théorème 1.2, la norme réduite de $\mathbf{X}$, qui n'est autre que son déterminant, est dans $L$. Nous déduisons alors, que le déterminant de $\mathbf{X}$ est dans $\mathcal{O}_K \cap L = \mathcal{O}_L$. Afin d'avoir un déterminant minimal discret, il suffit d'avoir $\mathcal{O}_L = \mathbb{Z}[i]$ ou $\mathbb{Z}[j]$.

Pour les petites dimensions, il sera possible d'établir l'expression du déterminant minimal. Cela nous permettra de vérifier plus facilement le fait qu'il soit discret.

## 3.2 Codes Quaternioniques

En se basant sur l'approche présentée au paragraphe précédent, nous avons construit une famille de code ST à rendement plein, diversité pleine et ayant des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Le premier code construit est le code quaternionique en dimension 2. Ce dernier est construit en utilisant les algèbres de quaternions, d'où son appellation "code quaternionique". Les bonnes performances de ce nouveau code comparées à celles du meilleur code ST connu jusqu' à présent dans la littérature en dimension 2 nous ont motivé à traiter d'autres dimensions. Nous avons alors construit les codes quaternioniques pour les dimensions 3 et 4.

Nous détaillons dans la suite la construction algébrique et les performances de ces nouveaux codes.

### 3.2.1 Code quaternionique 2X2

Nous considérons comme corps de base $L = \mathbb{Q}(i)$, et nous choisissons comme corps d'extension $K = \mathbb{Q}(\theta)$, le corps cyclotomique de degré 2 de $\mathbb{Q}(i)$, où $\theta = e^{\frac{i\pi}{4}}$ est la huitième racine de l'unité. Soit $\sigma$ le générateur du groupe de Galois de $K$, $\sigma : \theta \mapsto -\theta$. $K$ étant une extension cyclotomique de $\mathbb{Q}$, son anneau des entiers est égal à $\mathbb{Z}[\theta]$.

Soit $\gamma$ dans $\mathcal{O}_L = \mathbb{Z}[i]$. Nous définissons $\mathcal{A} = (K/L,\sigma,\gamma)$ l'algèbre cyclique de degré 2. D'après la définition 1.36, l'algèbre $\mathcal{A}$ est l'algèbre de quaternion $D_{i,\gamma}(L)$.

$D_{i,\gamma}(L)$ est une algèbre de division si $\gamma$ n'est pas une norme sur $\mathbb{Q}(\theta)/\mathbb{Q}(i)$. Afin de trouver le bon $\gamma$, nous utilisons la factorisation d'idéaux dans l'anneau des entiers de $K$, $\mathcal{O}_K$. On peut voir facilement que l'idéal $5\mathcal{O}_K = 5\mathbb{Z}[i]$ se factorise comme suit :

$$5\mathbb{Z}[i] = (2+i)(2-i)$$

L'idéal $(2+i)$ est premier. Ainsi, choisir $\gamma = 2+i$ garantit que $\gamma$ ne soit pas une norme sur $\mathbb{Q}(\theta)/\mathbb{Q}(i)$.

En considérant la représentation matricielle de l'algèbre de quaternions $D_{\beta,\gamma}(L)$ donnée dans (1.3), nous définissons notre code ST comme un sous-ensemble fini de $D_{i,\gamma}(L)$. Un mot de code s'écrit alors :

$$\mathbf{X} = \begin{bmatrix} s_1 + s_2\theta & s_3 + s_4\theta \\ (2+i)(s_3 - s_4\theta) & s_1 - s_2\theta \end{bmatrix}$$

où $s_1$, $s_2$, $s_3$ et $s_4$ sont les symboles d'information, pris dans $\mathbb{Z}[i]$ pour le code ST infini, et dans une constellation $q$-QAM pour le code ST fini.

Le déterminant du code ST s'écrit :

$$\det_2(C) = N(x_1) - (2+i)N(x_2)$$

où $x_1 = s_1 + s_2\theta$ et $x_2 = s_3 + s_4\theta$. $x_1$ et $x_2$ étant dans $O_K$, il est facile de voir que leurs normes sont dans $O_L = \mathbb{Z}[i]$. Nous déduisons que le déterminant prend ses valeurs dans $O_L = \mathbb{Z}[i]$. Sa valeur minimale est donc égale à 1, obtenue en considérant $x_1 = 1$ et $x_2 = 0$.

### 3.2.2 Code quaternionique 3x3

Pour la construction du code quaternionique en dimension 3, nous allons considérer le corps de base $L = \mathbb{Q}(j)$, et le corps cyclotomique $K = \mathbb{Q}(\theta)$ de $L$ de degré 3, avec $\theta = \exp(i\frac{2\pi}{9}) = \xi_9$ neuvième racine de l'unité. Soit $\sigma$ le générateur du groupe de Galois de $K$, $\sigma : \theta \mapsto j\theta$. L'anneau des entiers de $K$ est égal à $\mathbb{Z}[\theta]$. Soit alors $\gamma \in O_L = \mathbb{Z}[j]$, définissons $\mathcal{A} = (\mathbb{Q}(\theta)/\mathbb{Q}(j),\sigma,\gamma)$ l'algèbre cyclique de degré 3.

Pour que $\mathcal{A}$ soit une algèbre de division, il faut que $\gamma$ et $\gamma^2$ ne soient pas des normes sur $K^*$. Comme pour la dimension 2, nous allons recourir à la factorisation des idéaux afin de trouver un tel $\gamma$. Pour cela nous utilisons le logiciel de calcul algébrique KANT [38].

L'idéal $7\mathbb{Z}[j]$ ne se ramifie pas, il se factorise dans $\mathbb{Z}[j]$ comme suit :

$$7\mathbb{Z}[j] = (7,3+j)\cdot(7,5+j)$$

L'idéal $I = 7\cdot\mathbb{Z}[j] \oplus (3+j)\cdot\mathbb{Z}[j]$ est premier. Or, 7 n'est pas une norme absolue dans $\mathbb{Q}(\theta)$. Ainsi choisir $\gamma = 3 + j$ garantit que $(3+j)$ et $(3+j)^2$ ne soient pas des normes dans $\mathbb{Q}(\theta)/\mathbb{Q}(j)$.

Le code ST est un sous-ensemble fini de l'algèbre de division. Un mot de code $\mathbf{X}$ s'écrit :

$$\mathbf{X} = \begin{bmatrix} s_1 + s_2\theta + s_3\theta^2 & s_4 + s_5\theta + s_6\theta^2 & s_7 + s_8\theta + s_9\theta^2 \\ \gamma\sigma(s_7 + s_8\theta + s_9\theta^2) & \sigma(s_1 + s_2\theta + s_3\theta^2) & \sigma(s_4 + s_5\theta + s_6\theta^2) \\ \gamma\sigma^2(s_4 + s_5\theta + s_6\theta^2) & \gamma\sigma^2(s_7 + s_8\theta + s_9\theta^2) & \sigma^2(s_1 + s_2\theta + s_3\theta^2) \end{bmatrix}$$

où les $s_l$, $l = 1\ldots9$ sont les symboles d'information pris dans $\mathbb{Z}[j]$ pour le code ST infini, et dans une constellation hexagonale $q$-HEX pour le code ST fini. Notons que $(1,\theta,\theta^2)$ est une base de $K$, vue comme espace vectoriel sur $L$.

Le déterminant du code s'écrit :

$$\det_3(C) = N(x_1) + \gamma N(x_2) + \gamma^2 N(x_3) - \gamma Tr\left(x_1\sigma(x_2)\sigma^2(x_3)\right)$$

avec $x_1$, $x_2$et $x_3$ définis comme suit :

$$\begin{aligned} x_1 &= s_1 + s_2\theta + s_3\theta^2 \\ x_2 &= s_4 + s_5\theta + s_6\theta^2 \\ x3 &= s_7 + s_8\theta + s_9\theta^2 \end{aligned}$$

D'après la définition (1.30), pour tout $x \in \mathbb{O}_K$, la norme et la trace de $x$ sont dans $O_L = \mathbb{Z}[j]$. Le déterminant étant une somme de normes et de traces, il prend alors ses valeurs dans $\mathbb{Z}[j]$. Ainsi, le déterminant minimal est égal à 1.

### 3.2.3 Code quaternionique 4x4

Comme pour la dimension 2, nous considérons le corps de base $L = \mathbb{Q}(i)$. Soit $\theta = \exp(i\frac{\pi}{8}) = \xi_{16}$ racine $16^{\text{ième}}$ de l'unité. Nous choisissons comme corps d'extension $K = \mathbb{Q}(\theta)$ l'extension cyclotomique de degré 4 de $\mathbb{Q}(i)$. Soit $\sigma$ le générateur du groupe de Galois de $K$, $\sigma : \theta \mapsto i\theta$. L'anneau des entiers de $K$ est égal à $\mathbb{Z}[\theta]$.

Soit $\gamma \in O_L = \mathbb{Z}[i]$, $\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre cyclique de degré 4. Pour que $\mathcal{A}$ soit une algèbre de division il faut que $\gamma$, $\gamma^2$, $\gamma^3 \notin N_{K/L}(K)$. Pour trouver un tel $\gamma$, nous utilisons la factorisation des idéaux.

En utilisant KANT, nous trouvons que l'idéal $5\mathbb{Z}[i]$ ne se ramifie pas, il se factorise dans $\mathbb{Z}[i]$ comme suit :

$$5\mathbb{Z}[i] = (5,2+i)\cdot(5,3+i)$$

L'idéal $I = 5\cdot\mathbb{Z}[i] \oplus (2+i)\cdot\mathbb{Z}[i]$ étant premier, $(2+i)$, $(2+i)^2$ et $(2+i)^3$ ne sont pas des normes sur $K/L$ car 5 n'est pas une norme absolue.

L'algèbre de division ainsi construite nous permet de déduire le code ST. Un mot de code s'écrit :

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ \gamma\sigma(x_4) & \sigma(x_1) & \sigma(x_2) & \sigma(x_3) \\ \gamma\sigma^2(x_3) & \gamma\sigma^2(x_4) & \sigma^2(x_1) & \sigma^2(x_2) \\ \gamma\sigma^3(x_2) & \gamma\sigma^3(x_3) & \gamma\sigma^3(x_4) & \sigma^3(x_1) \end{bmatrix}$$

avec $x_l \in K$, $l = 1\ldots4$. En fonction des symboles d'information, les $x_l$ s'écrivent dans la base de $K$, $(1,\theta,\theta^2,\theta^3)$ de la façon suivante :

$$\begin{aligned} x_1 &= s_1 + \theta s_2 + \theta^2 s_3 + \theta^3 s_4 \\ x_2 &= s_5 + \theta s_6 + \theta^2 s_7 + \theta^3 s_8 \\ x_3 &= s_9 + \theta s_{10} + \theta^2 s_{11} + \theta^3 s_{12} \\ x_4 &= s_{13} + \theta s_{14} + \theta^2 s_{15} + \theta^3 s_{16} \end{aligned}$$

Pour le code ST infini, les symboles d'information sont pris dans $\mathbb{Z}[i]$, et pour le code ST fini, les symboles d'information sont pris dans une constellation $q$-QAM.

Le déterminant du code s'écrit :

$$\begin{aligned} \det_4(C) = {} & N(x_1) - \gamma N(x_2) + \gamma^2 N(x_3) - \gamma^3 N(x_4) - \gamma Tr\left(x_1\sigma(x_1)\sigma^2(x_2)\sigma^3(x_4)\right) \\ & + \gamma Tr\left(x_1\sigma(x_1)\sigma^2(x_2)\sigma^3(x_3)\right) + \gamma^2 Tr\left(x_1\sigma(x_3)\sigma^2(x_4)\sigma^3(x_4)\right) \\ & - \gamma^2 Tr\left(x_2\sigma(x_3)\sigma^2(x_3)\sigma^3(x_4)\right) + \gamma^2\frac{1}{2}Tr\left(x_4\sigma(x_2)\sigma^2(x_4)\sigma^3(x_2)\right) \\ & - \gamma^2\frac{1}{2}Tr\left(x_1\sigma(x_3)\sigma^2(x_1)\sigma^3(x_3)\right) \end{aligned}$$

Comme pour les dimensions 2 et 3, le déterminant est une somme de normes et de traces. Il prend donc ses valeurs dans $\mathbb{Z}[i]$. Le déterminant minimal est alors égal à 1.

### 3.2.4 Versions équilibrées des codes quaternioniques

Les matrices mots de code relatives aux codes quaternioniques construits pour les dimensions 2, 3 et 4 se caractérisent par une partie triangulaire inférieure multipliée par $\gamma$. Le module non unitaire de $\gamma$ induit un grand déséquilibre énergétique entre la partie supérieure et la partie inférieure du mot de code. Nous proposons alors des versions équilibrées des codes quaternioniques ayant de meilleures distributions énergétiques. Ces nouveaux codes sont obtenus en multipliant la matrice mot de code à droite et à gauche par la matrice diagonale **T** définie comme suit :

$$\mathbf{T} = \mathrm{diag}\left(\gamma^{n_t-(2k+1)}\right)_{k=0\ldots n_t-1}$$

Un mot de code des codes quaternioniques équilibrés s'écrit :

$$\begin{aligned}\mathbf{X}' &= \mathbf{T}\cdot\mathbf{X}\cdot\mathbf{T}^{-1} \\ &= \begin{bmatrix} x_1 & \gamma^{\frac{1}{n_t}}x_2 & \cdots & \gamma^{\frac{n_t-1}{n_t}}x_{n_t} \\ \gamma^{\frac{n_t-1}{n_t}}\sigma(x_{n_t}) & \sigma(x_1) & \cdots & \gamma^{\frac{n_t-2}{n_t}}\sigma(x_{n_t-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{\frac{1}{n_t}}\sigma^{n_t-1}(x_2) & \gamma^{\frac{2}{n_t}}\sigma^{n_t-1}(x_3) & & \sigma^{n_t-1}(x_1) \end{bmatrix}\end{aligned}$$

Étant donné que le déterminant de la matrice **T** est égal à 1, les déterminants minimaux des codes quaternioniques sont préservés.

Écrit sous cette nouvelle forme, les codes quaternioniques ont la même structure que les codes présentés dans [18, 19, 20].

Nous donnons comme exemple, le code quaternionique équilibré en dimension 2.

$$\begin{aligned}\mathbf{X}' &= \begin{bmatrix} \gamma & 0 \\ 0 & \frac{1}{\gamma} \end{bmatrix}\cdot\begin{bmatrix} s_1+s_2\theta & s_3+s_4\theta \\ \gamma(s_3-s_4\theta) & s_1-s_2\theta \end{bmatrix}\cdot\begin{bmatrix} \frac{1}{\gamma} & 0 \\ 0 & \gamma \end{bmatrix} \\ &= \begin{bmatrix} s_1+s_2\theta & \gamma^{1/2}(s_3+s_4\theta) \\ \gamma^{1/2}(s_3-s_4\theta) & s_1-s_2\theta \end{bmatrix}\end{aligned}$$

### 3.2.5 Performances des codes quaternioniques

A ce stade nous avons montré que les codes quaternioniques ont de très bonnes propriétés, à savoir, un rendement plein, une diversité pleine et un déterminant minimal ne s'évanouissant pas. Il nous reste donc à étudier leurs performances et à les comparer aux meilleurs codes ST connus (MCC) jusqu'à présent [18, 19, 20].

Nous avons simulé la chaîne de transmission présentée dans la figure 1.1 en utilisant les codes quaternioniques équilibrés (CQ) ensuite les (MCC). Nous avons utilisé comme décodeur une version modifiée du décodeur Schnorr-Echnner, adaptée à notre application. La présentation complète de ce décodeur avec les modifications effectuées pour décoder les codes ST sera faite dans le chapitre suivant.

Dans la figure 3.2, nous avons tracé le taux d'erreurs par mot de code en fonction du rapport signal sur bruit (RSB= $\frac{E_b}{N_0}$) pour le code quaternionique (CQ) $2\times 2$ et le (MCC) en dimension 2

[18] (tableau récapitulatif 2.2), en utilisant les constellations 4, 16, et 64-QAM. Nous remarquons que le code (CQ) et les (MCC) ont pratiquement les même performances, avec une légère avance pour les codes (CQ).

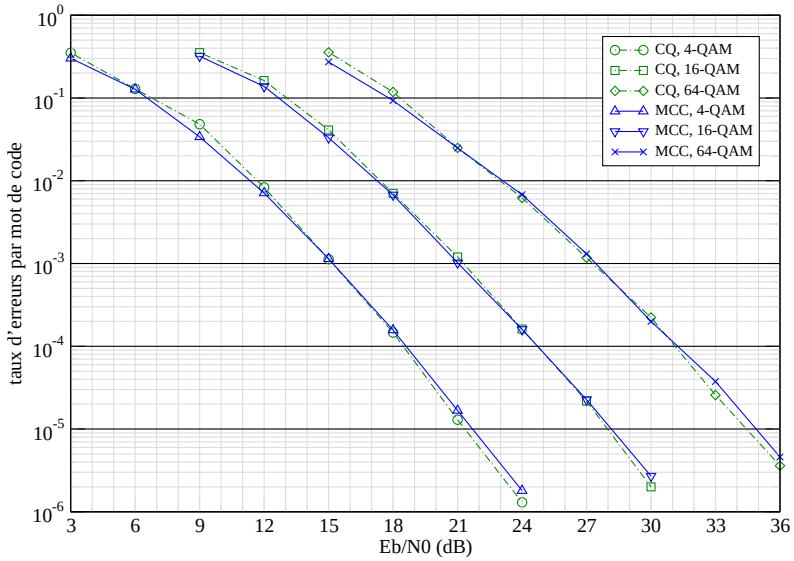



Fig. 3.2: Comparaison du code quaternionique (CQ) 2×2 et du meilleur code connu en dimension 2 (MCC), pour différentes constellations $q$-QAM

Dans les figures 3.3 et 3.4, nous avons tracé le taux d'erreurs par mot de code en fonction du RSB, respectivement, du (CQ) $3 \times 3$ et du (CQ) $4 \times 4$ et des (MCC) [19, 20]. Contrairement à la dimension 2, les codes quaternioniques en dimension 3 et 4 ont des performances moins bonnes que celles des MCC. Cela s'explique par la répartition non uniforme de l'énergie dans le mot de code malgré l'équilibrage énergétique effectué.

La figure (3.5) illustre un exemple de schéma de transmission MIMO avec des énergies différentes sur les antennes émettrices. Une telle transmission entraîne un bon décodage des symboles de forte énergie et inversement, un mauvais décodage des symboles de faible énergie. Ce type de schéma engendre des performances globales plutôt moyennes. Pour pallier à ce problème énergétique, l'idée serait d'utiliser le décodeur SIC ordonné (chapitre I, paragraphe 1.6). Malheureusement, ce décodeur est sous-optimal. Il ne permettra pas donc d'atteindre les performances optimales de notre code.

A cause de ce problème énergétique, nous nous sommes limités à la construction des codes quaternioniques pour les dimensions 2, 3 et 4. Dans un récent papier [39], une généralisation de la construction des codes quaternioniques a été donnée pour les dimensions de la forme suivante : $2^k$, $3.2^k$, $2.3^k$ et $q^k(q-1)/2$ où $q$ est un nombre premier de la forme $(4k+3)$, et $k$ est un entier choisi arbitrairement.

Par ailleurs, nous remarquons un point très intéressant, que plus l'efficacité spectrale augmente, plus l'écart entre les courbes de performance des (CQ) et des (MCC) se réduit. Ce qui montre concrètement l'intérêt d'avoir des codes ayant des déterminants minimaux ne s'évanouissant pas.

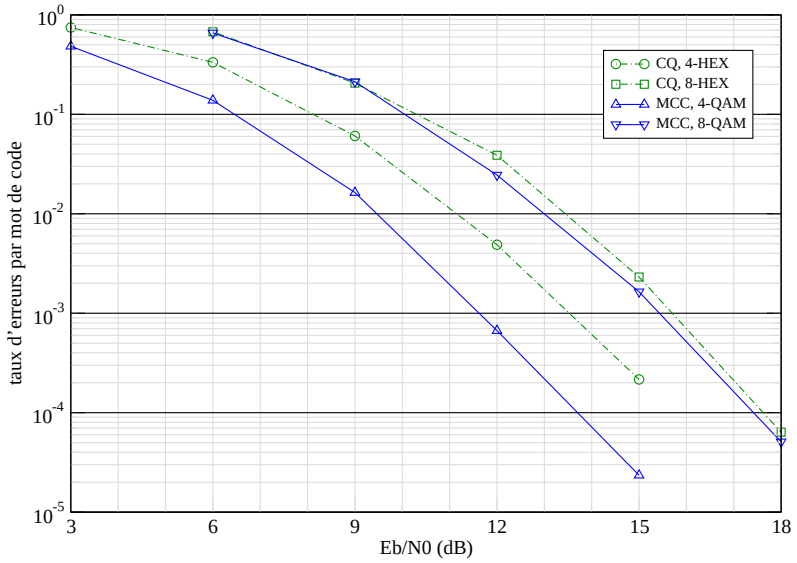



Fig. 3.3: Comparaison du code quaternionique (CQ) $3 \times 3$ et du meilleure code connu en dimension 3 (MCC), pour différentes constellations $q$-QAM et $q$-HEX

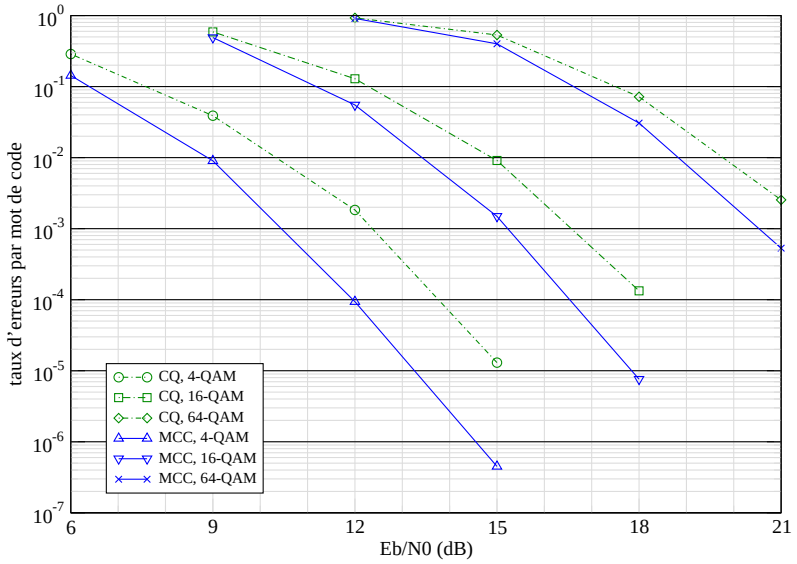



Fig. 3.4: Comparaison du code quaternionique (CQ) 4×4 et du meilleur code connu en dimension 4 (MCC), pour différentes constellations $q$-QAM

## 3.3 Deuxième approche de construction des codes ST

La construction des codes quaternioniques nous a permis d'apprécier l'importance d'avoir des codes ST ayant des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Cette conclusion nous a motivé à construire de nouveaux codes ST conservant les propriétés des codes quaternioniques et palliant au problème énergétique. La construction de ces codes s'effectuera sur la base d'une deuxième approche que nous définirons et validerons.

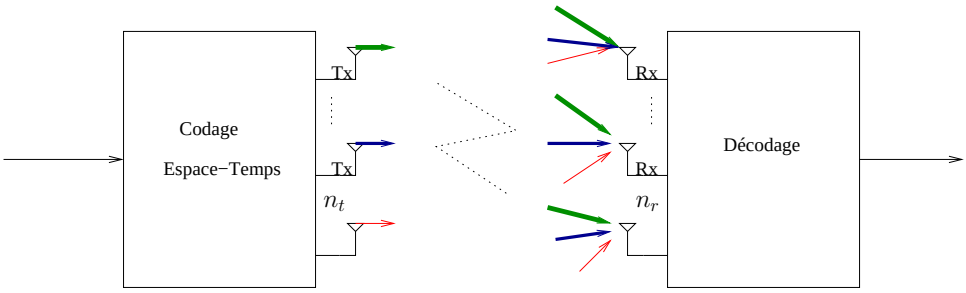



FIG. 3.5: Schéma de transmission MIMO avec une répartition non uniforme de l'énergie sur les antennes émettrices

### 3.3.1 Critères de construction

Les nouveaux codes à construire doivent vérifier les 3 critères relatifs aux codes quaternioniques, ainsi qu'un quatrième lié à l'énergie.

1. Rendement plein
2. Diversité maximale
3. Déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente
4. *Bonne efficacité énergétique : L'énergie moyenne doit être uniformément distribuée dans la matrice mot de code. En plus, une contrainte de forme sur les constellations transmises doit être vérifiée afin d'éviter toute perte de forme par rapport aux constellations émises.* Les codes ST construits à partir d'algèbre de division, comme les codes quaternioniques et les codes construits dans [9], possèdent une structure de couches définie dans [20] (fig. 2.7). Nous allons alors exploiter cette propriété afin d'imposer une contrainte de forme sur les constellations transmises. En effet, étant donné que nous utilisons les constellations $q$-QAM et $q$-HEX qui sont respectivement des sous-ensembles finis de $\mathbb{Z}[i]$ et de $\mathbb{Z}[j]$, il faut alors construire pour chaque couche un réseau de points de la forme $R\mathbb{Z}[i]^{n_t}$ et respectivement un réseau de points de la forme $R\mathbb{Z}[j]^{n_t} = RA_2^{n_t}$, où $R$ est une matrice unitaire complexe, $RR^H = I$ (Notons que lorsqu'on travaille dans $\mathbb{Z}[j]$, la transposition hermitienne utilise la conjugaison dans $\mathbb{Z}[j]$, qui transforme $j$ en $j^2$). Ainsi les constellations transmises seront des versions tournées de $\mathbb{Z}[i]^{n_t}$ et de $A_2^{n_t}$ respectivement. D'après [40, 41] des versions tournées des réseaux de points $\mathbb{Z}^{2n_t}$ ou $A_2^{n_t}$ peuvent être construites comme des réseaux de points algébriques complexes.

### 3.3.2 Démarche de la construction

Nous proposons une approche permettant de construire des codes ST vérifiant les critères cités ci-dessus. Cette approche présente pas mal de similitudes par rapport à la première proposée au paragraphe 3.1, avec quelques différences que nous verrons par la suite. Cette approche se compose de 6 étapes :

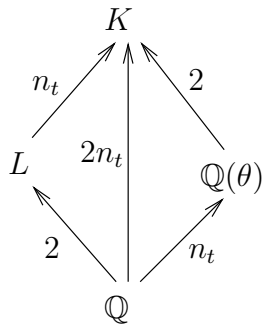
1 - Choix du corps de base
2- Choix du corps de décomposition
3- Définition de l'algèbre cyclique
4- Choix de $\gamma$ tel que $|\gamma| = 1$
5- Choix de l'idéal I
6- Définition du code ST

**1- Choix du corps de base**

Nous considérons comme corps de base $L = \mathbb{Q}(i)$ ou $\mathbb{Q}(j)$. Ainsi, les constellations utilisées seront les constellations $q$-QAM et les constellations $q$-HEX.

**2- Choix du corps de décomposition**

Soit $\theta$ un nombre algébrique, et soit $\mathbb{Q}(\theta)$ un corps de nombres cyclique totalement réel de degré $n_t$ tel que les discriminants de $L$ et de $\mathbb{Q}(\theta)$ sont premiers entre eux. $\left(d_L, d_{\mathbb{Q}(\theta)}\right) = 1$. $K$ est alors le corps de décomposition de $L$ et de $\mathbb{Q}(\theta)$, noté $\mathbb{Q}(i,\theta)$ ( resp.$\mathbb{Q}(j,\theta)$). Définissons $\sigma$ le générateur du groupe de Galois de $K$.




**3- Définition de l'algèbre cyclique**

Soit $\gamma \in L$, $\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre cyclique de degré $n_t$.

**4- Choix de $\gamma$**

Pour que $\mathcal{A}$ soit une algèbre de division, et pour garantir des déterminants minimaux discrets avec une bonne efficacité énergétique, $\gamma$ doit vérifier les propositions suivantes :

- $\gamma, \gamma^2, \ldots, \gamma^{n_t-1}$ ne sont pas des normes de $K^*$
- $\gamma \in O_L = \mathbb{Z}[i]$ ou $\mathbb{Z}[j]$
- $\left|\gamma\right| = 1$.

Ainsi le choix de $\gamma$ se limite à $\{1, i, -1, -i\}$ lorsque $O_L = \mathbb{Z}[i]$ et à $\left\{1, j, j^2, -1, -j, -j^2\right\}$ lorsque $O_L = \mathbb{Z}[j]$ .

**5- Choix de l'idéal**

Il faudrait trouver un idéal $I \subset O_K$ tel que le réseau de points $\Lambda(I)$ (def. 1.32) soit une version tournée du réseau de points complexe $\mathbb{Z}[i]^{n_t}$ (ou resp. $\mathbb{Z}[j]^{n_t}$).

**6- Construction du code ST**

De la même manière que dans la première approche, nous définissons le code ST comme un sous-ensemble fini de l'algèbre de division $\mathcal{A}$ obtenu en se restreignant à l'idéal $I \subset O_K$. Un mot de code s'écrit alors :

$$\mathbf{X} = \begin{bmatrix} \sum_{i=1}^{n_t} s_{1,i} v_i & \sum_{i=1}^{n_t} s_{2,i} v_i & \cdots & \sum_{i=1}^{n_t} s_{n_t,i} v_i \\ \gamma\sigma(\sum_{i=1}^{n_t} s_{n_t,i} v_i) & \sigma(\sum_{i=1}^{n_t} s_{1,i} v_i) & \cdots & \sigma(\sum_{i=1}^{n_t} s_{n_t-1,i} v_i) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n_t}(\sum_{i=1}^{n_t} s_{2,i} v_i) & \gamma\sigma^{n_t}(\sum_{i=1}^{n_t} s_{3,i} v_i) & \cdots & \sigma^{n_t}(\sum_{i=1}^{n_t} s_{1,i} v_i) \end{bmatrix} \tag{3.2}$$

où $B = (v_k)_{k=1\ldots n_t}$ est une base intégrale de l'idéal $I$, et les $s_l$, $l = 1 \cdots n_t^2$ sont les symboles d'information pris dans $O_L$ pour le code ST infini et dans une constellation $q$-QAM ou $q$-HEX pour le code ST fini.

Le mot de code peut s'écrire dans la base de l'algèbre de division $(\mathbf{I}_{n_t}, \mathbf{e}, \cdots, \mathbf{e}^{n_t-1})$ en fonction de la matrice génératrice $\mathbf{M}$ du réseau de points $\Lambda(I)$ sous la forme suivante :

$$\mathbf{X} = \mathrm{diag}\,(\mathbf{M} \cdot \mathbf{x_1}) \cdot \mathbf{I}_{n_t} + \mathrm{diag}\,(\mathbf{M} \cdot \mathbf{x_2}) \cdot \mathbf{e} + \cdots + \mathrm{diag}\,(\mathbf{M} \cdot \mathbf{x_{n_t}}) \cdot \mathbf{e}^{n_t-1}$$

$\mathbf{x_l}$, $l = 1 \cdots n_t$ sont des vecteurs colonnes de taille $n_t$ composés par les $n_t^2$ symboles d'information.

Si l'idéal $I$ est principal (def. 1.10), il est engendré par un seul élément. Soit $\alpha$ cet élément. Tout élément $x$ de $I$ s'écrit alors $x = \alpha y$, avec $y \in O_K$ . Soit $B$ une base intégrale de $O_K$, que nous supposons s'écrit sous la forme suivante $(1, \theta, \theta^2, \cdots, \theta^{n_t-1})$ ($\theta$ n'est pas obligatoirement l'élément primitif de $\mathbb{Q}(\theta)$). La base de l'idéal $I$ est alors $\left(\alpha, \alpha\theta, \alpha\theta^2, \cdots, \alpha\theta^{n_t-1}\right)$ et la matrice génératrice du réseau de points $\Lambda(I)$ est :

$$\mathbf{M} = \begin{bmatrix} \alpha & \alpha\theta & \ldots & \alpha\theta^{n_t-1} \\ \sigma(\alpha) & \sigma(\alpha\theta) & \ldots & \sigma(\alpha\theta^{n_t-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma^{n_t-1}(\alpha) & \sigma^{n_t-1}(\alpha\theta) & \ldots & \sigma^{n_t-1}(\alpha\theta^{n_t-1}) \end{bmatrix} \tag{3.3}$$

Le mot de code s'écrit alors :

$$\mathbf{X} = \begin{bmatrix} \alpha \sum_{i=1}^{n_t} s_{1,i}\theta^{i-1} & \alpha \sum_{i=1}^{n_t} s_{2,i}\theta^{i-1} & \ldots & \alpha \sum_{i=1}^{n_t} s_{n_t,i}\theta^{i-1} \\ \gamma\sigma(\alpha \sum_{i=1}^{n_t} s_{n_t,i}\theta^{i-1}) & \sigma(\alpha \sum_{i=1}^{n_t} s_{1,i}\theta^{i-1}) & \ldots & \sigma(\alpha \sum_{i=1}^{n_t} s_{n_t-1,i}\theta^{i-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n_t-1}(\alpha \sum_{i=1}^{n_t} s_{2,i}\theta^{i-1}) & \gamma\sigma^{n_t-1}(\alpha \sum_{i=1}^{n_t} s_{n_t,i}\theta^{i-1}) & \ldots & \sigma^{n_t-1}(\alpha \sum_{i=1}^{n_t} s_{1,i}\theta^{i-1}) \end{bmatrix} \tag{3.4}$$

### 3.3.3 Validation de l'approche

Le code ST construit de cette façon est bien de rendement plein et de diversité maximale. Afin de valider l'approche proposée, il nous reste à vérifier l'existence d'un idéal permettant de construire des versions tournées de $\mathbb{Z}[i]^{n_t^2}$ ou de $\mathbb{Z}[j]^{n_t^2}$, et de s'assurer que le déterminant minimal du code est bien discret.

#### 3.3.3.1 Construction de versions tournées des réseaux de points $\mathbb{Z}^{2n_t}$ ou $A_2^{n_t}$

Notre objectif est de trouver un idéal $I \subset O_K$ tel que le réseau de points algébrique complexe $\Lambda(I)$ soit une version tournée de $\mathbb{Z}[i]^{n_t}$ ou de $\mathbb{Z}[j]^{n_t}$. Soit $\Lambda^r(I)$ le réseau de points réel obtenu en séparant et vectorisant les parties réelles et imaginaires des vecteurs du réseau de points complexe $\Lambda(I)$. Il en découle que $\Lambda^r(I)$ est une version tournée de $\mathbb{Z}^{2n_t^2}$ ou de $A_2^{n_t^2}$.

Afin de trouver un tel idéal, nous allons utiliser les volumes des réseaux de points $\mathbb{Z}^{2n_t^2}$ et $A_2^{n_t^2}$. En effet, pour que $\Lambda^r(I)$ soit une version homothétique tournée de $\mathbb{Z}^{2n_t^2}$ ou de $A_2^{n_t^2}$ il faut que son volume soit égal à :

$$V(\Lambda^r(I)) = c^{n_t} \quad \text{ou} \quad V(\Lambda^r(I)) = \left(\frac{\sqrt{3}}{2}\right)^{n_t} c^{n_t} \tag{3.5}$$

où $c$ est un entier.

Par définition (def. 1.32) le volume de $\Lambda(I)$ s'écrit en fonction du discriminant de $K/L$ (def. 1.30) :

$$V(\Lambda(I)) = 2^{-n_t} \cdot \sqrt{\left|d_{K/\mathbb{Q}}\right|} \cdot N(I) \tag{3.6}$$

D'après les équations 3.5 et 3.6 nous déduisons la norme de l'idéal $I$ :

$$N(I) = \frac{(2c)^{n_t}}{\sqrt{\left|d_{K/\mathbb{Q}}\right|}} \quad \text{ou} \quad N(I) = \frac{\left(\sqrt{3}c\right)^{n_t}}{\sqrt{\left|d_{K/\mathbb{Q}}\right|}}$$

Soit $d_{K/\mathbb{Q}} = \prod p_k^{r_k}$ la décomposition en facteurs premiers du discriminant. Cette factorisation contient les nombres premiers qui se ramifient dans $O_k$. Soit $p_k O_k = \prod_l I_{k_l}^{e_k}$ avec $e_k > 1$. Il faut donc trouver un idéal sous la forme suivante :

$$I = \prod I_{k_l}^{s_{k_l}}$$

ayant comme norme :

$$N(I) = \prod_{p_k \neq 2} p_k^{n_t - r_k/2} \quad \text{ou} \quad N(I) = \prod_{p_k \neq 3} p_k^{n_t - r_k/2}$$

Cette méthode nous permet de prédire l'idéal à utiliser afin de construire des versions tournées des réseaux de points $\mathbb{Z}^{2n_t}$ et $A_2^{n_t}$ (une réduction peut être nécessaire). Pour valider le résultat, nous calculons la matrice de Gram de la matrice génératrice du réseau de points (en utilisant la bonne transposition hermitienne). La matrice de Gram obtenue doit être égale à la matrice identité.

#### 3.3.3.2 Déterminant minimal

A l'issue de la première approche, nous avons démontré, en utilisant le théorème 1.2 et le fait que $\gamma \in O_K$, que le déterminant minimal du code ST construit sur l'algèbre de division tel que les symboles d'information sont pris dans $O_K$ dispose d'un déterminant minimal discret.

Du fait que les hypothèses de cette démonstration restent aussi valables pour la deuxième approche, nous déduisons que le déterminant minimal du nouveau code construit est aussi discret. Nous nous proposons de calculer la valeur de ce déterminant minimal. Pour cela nous allons distinguer deux cas suivant que l'idéal $I$ soit principal ou non.

**- $I$ est principal**

Soit $\alpha$ l'élément générateur de l'idéal $I$. Le mot de code défini dans l'équation 3.4, se récrit sous la forme suivante :

$$\begin{aligned}\mathbf{X} &= \begin{bmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \sigma(\alpha) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \sigma^{n_t-1}(\alpha) \end{bmatrix} \begin{bmatrix} \sum_{i=1}^{n_t} s_{1,i}\theta^{i-1} & \sum_{i=1}^{n_t} s_{2,i}\theta^{i-1} & \cdots & \sum_{i=1}^{n_t} s_{n_t,i}\theta^{i-1} \\ \gamma\sigma(\sum_{i=1}^{n_t} s_{n_t,i}\theta^{i-1} & \sigma(\sum_{i=1}^{n_t} s_{1,i}\theta^{i-1}) & \cdots & \sigma(\sum_{i=1}^{n_t} s_{n_t-1,i}\theta^{i-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \gamma\sigma^{n_t-1}(\sum_{i=1}^{n_t} s_{2,i}\theta^{i-1}) & \gamma\sigma^{n_t-1}(\sum_{i=1}^{n_t} s_{n_t,i}\theta^{i-1}) & \cdots & \sigma^{n_t-1}(\sum_{i=1}^{n_t} s_{1,i}\theta^{i-1}) \end{bmatrix} \\ &= \mathbf{A}\cdot\mathbf{B}\end{aligned}$$

D'où :

$$\det(\mathbf{X}) = \det(\mathbf{A})\cdot\det(\mathbf{B})$$

La matrice $\mathbf{B}$ correspond exactement au code ST construit en utilisant la première approche, par conséquent son déterminant est dans $O_K$ et sa valeur minimale est égale à 1. Quand à la matrice $\mathbf{A}$, son déterminant est égal à $N_{K/L}(\alpha)$.

Nous déduisons alors que :

$$\delta_{\min}(C_\infty) = \min_{X\in C_\infty, X\neq 0} |\det(X)|^2 = \left|N_{K/L}(\alpha)\right|^2 = N_{K/\mathbb{Q}}(\alpha)$$

Le déterminant minimal peut s'écrire en fonction du discriminant de $d_{\mathbb{Q}(\theta)}$. En effet, le volume du réseau de points $\Lambda(I)$ donne la relation qui relie la norme de l'idéal au discriminant :

$$\mathrm{vol}(\Lambda(I))^2 = 4^{-n_t}\cdot d_K \cdot N_{K/\mathbb{Q}}(I)^2$$

Le discriminant de $K$ s'écrit en fonction de celui de $L$ et de $\mathbb{Q}(\theta)$ :

$$d_K = d_{\mathbb{Q}(\theta)}^2 \cdot d_L^{n_t}$$

avec $d_L = -4$ pour $L = \mathbb{Q}(i)$ et $d_L = -3$ pour $L = \mathbb{Q}(j)$. Le réseau de points $\Lambda^r(I)$ est une version tournée de $\mathbb{Z}^{2nt}$ ou $A_2^{2n_t}$ alors son volume est égal à 1 ou à $\frac{\sqrt{3}}{2}$. Nous avons donc :
Pour $L = \mathbb{Q}(i)$

$$1 = 4^{-n_t}\cdot N_{K/\mathbb{Q}}(\alpha)^2 \cdot d_{\mathbb{Q}(\theta)}^2 \cdot 4^{n_t}$$

Pour $L = \mathbb{Q}(j)$

$$\left(\frac{3}{4}\right)^{n_t} = 4^{-n_t}\cdot N_{K/\mathbb{Q}}(\alpha)^2 \cdot d_{\mathbb{Q}(\theta)}^2 \cdot 3^{n_t}$$

Nous pouvons déduire pour les deux cas que :

$$\delta_{\min}(C_\infty) = N_{K/\mathbb{Q}}(\alpha) = \frac{1}{d_{\mathbb{Q}(\theta)}} \tag{3.7}$$

**- $I$ n'est pas principal**

D'une façon générale, le déterminant minimal du mot de code défini dans l'équation 3.2 s'écrit :

$$\det(\mathbf{X}) = \sum_{s \in S_n} \operatorname{sgn}(s) \prod_{l=1}^{n_t} \mathbf{X}_{l,s(l)}$$

$s_n$ est le groupe des permutations de $n_t$ éléments, et $\mathbf{X}_{l,k}$ est l'élément de la matrice mot de code se trouvant à la $l^{ime}$ ligne et la $k^{ime}$ colonne.

Notons $I^\sigma$ l'action du groupe de Galois sur $I$. Comme $X_{l,s(l)} \in I^{\sigma^{l-1}}$ pour tout $l$, on a [42, p. 118] :

$$\det(\mathbf{X}) \in \prod_{\sigma \in Gal(K/L)} I^\sigma = N_{K/L}(I)\mathcal{O}_K$$

Nous avons démontré que le déterminant minimal est dans $\mathcal{O}_L$. D'où

$$\det(\mathbf{X}) \in \mathcal{O}_L \cap N_{K/L}(I)\mathcal{O}_K = N_{K/L}(I)$$

$L$ étant égal à $\mathbb{Q}(i)$ ou $\mathbb{Q}(j)$, alors $|\det(\mathbf{X})|^2 \in N_{L/\mathbb{Q}}(N_{K/L}(I))$. Par transitivité de la norme [42, p. 99] :

$$\min_{\mathbf{X} \in C_\infty, \mathbf{X} \neq 0} |\det(\mathbf{X})|^2 \in N_{K/\mathbb{Q}}(I) = N(I)\mathbb{Z} \tag{3.8}$$

A partir de cette dernière relation, nous pouvons déduire les bornes inférieures et supérieures du déterminant minimal :

$$N(I) = \frac{1}{d_{\mathbb{Q}(\theta)}} \leq \delta_{\min}(C_\infty) \leq \frac{1}{\operatorname{vol}(\Lambda^r(I))} \min_{x \in I} N_{K/\mathbb{Q}}(x) \tag{3.9}$$

La borne inférieure est immédiate d'après 3.8. La borne supérieure est obtenue en considérant $x_0 \neq 0 \in I$, et $x_l = 0, l = 1 \ldots n_t - 1$. $\frac{1}{\operatorname{vol}(\Lambda^r(I))}$ est un facteur de normalisation.

Si nous voulons valider le cas de l'idéal principal, les bornes inférieures et supérieures dans 3.9 sont égales. Nous retrouvons alors le résultat de l'équation 3.7.

## 3.4 Codes ST Parfaits

En utilisant l'approche présentée dans le paragraphe précédent, nous pouvons construire une nouvelle famille de codes ST. Ces nouveaux codes se caractérisent par des propriétés jamais réunies dans un code ST jusqu'à présent, à savoir : rendement plein, diversité maximale, déterminants minimaux ne s'évanouissant pas et efficacité énergétique. Nous les appelons alors "codes parfaits" .

**Définition : 3.1** *code parfait*

*Un code ST à dispersion linéaire (LD), construit sur une algèbre cyclique de division de centre $\mathbb{Q}(i)$ ou $\mathbb{Q}(j)$, de dimension $n_t \times n_t$, est un code parfait si et seulement si :*

1. *il a un rendement plein : $n_t^2$ symboles d'information q-QAM ou q-HEX sont transmis*
2. *le déterminant minimal ne s'évanouit pas lorsque l'efficacité spectrale augmente*
3. *le réseau de points réel obtenu par vectorisation du mot de code est $Z^{2n_t^2}$ ou $A_2^{n_t^2}$*

Le troixième point de la définition des codes parfaits, nous permet de déduire avant même de construire les codes, qu'ils satisfont le critère de l'information mutuelle par unitarité de la matrice mot de code vectorisé (la vectorisation va être explicité dans le chapitre suivant).

Nous montrons dans la suite que les codes parfaits n'existent que pour les dimensions 2, 3, 4 et 6, et nous donnons les constructions des codes ST parfaits correspondants à ces dimensions.

### 3.4.1 Existence des codes parfaits

Les codes ST parfaits doivent satisfaire beaucoup de contraintes, ce qui induit une restriction sur les dimensions pour lesquelles ils existent.

La contrainte du déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente se traduit pour les codes parfaits infinis par une distribution discrète du déterminant dans $\mathbb{C}$. Nous avons démontré qu'en prenant les symboles d'information dans un idéal $I \subseteq O_K$, et $\gamma \in O_L$, le déterminant du code est dans $O_L$.

Par ailleurs, $O_L$ est discret dans $\mathbb{C}$ si et seulement si $L$ est un corps de nombre quadratique totalement complexe [3]. En d'autres termes, $L = \mathbb{Q}\left(\sqrt{-p}\right)$, avec $p$ un entier positif premier. Ainsi, prendre un corps de base de degré supérieur à 2 impliquera une distribution de déterminants dense dans $\mathbb{C}$.

Considérant $L = \mathbb{Q}\left(\sqrt{-p}\right)$, la contrainte imposée sur le module de $\gamma$, $\left(\left|\gamma\right| = 1\right)$ implique que $\gamma$ est une unité (def. 1.33) dans $L$ du fait que $\left|\gamma\right|^2 = N_{\mathbb{Q}(\sqrt{-p})/\mathbb{Q}}(\gamma) = 1$.

**Lemme : 3.1** *([3], p. 76)*
*Soit p un entier positif libre carré. Les seules unités de* $L = \mathbb{Q}\left(\sqrt{-p}\right)$ *sont* $\pm 1$, *sauf pour* $L = \mathbb{Q}(i)$ *ou* $L = \mathbb{Q}(j)$.

Ainsi, d'après ce dernier lemme, $L$ ne peut être égal qu'à $\mathbb{Q}(i)$ ou $\mathbb{Q}(j)$. Par la suite, $\gamma$ ne peut prendre que les valeurs $-1, \pm i, \pm j, \pm j^2$ qui sont respectivement la $2^{\text{ième}}$, $3^{\text{ième}}$,$4^{\text{ième}}$ et $6^{\text{ième}}$ racines de l'unité.

Afin de garantir que l'algèbre $\mathcal{A} = (K/L,\sigma,\gamma)$ soit une algèbre de division, il faut aussi que, $\gamma^l$, $l = 1 \ldots n_t - 1$, ne soient pas des normes sur $K^*$, ce implique que $n_t \leq 6$.

*Montrons qu'il n'existe pas de code parfait pour la dimension* 5 *:* pour cette dimension, l'unique valeur de $\gamma$ possible est $-j$ et par la suite $L = \mathbb{Q}(j)$. Soit $K$ une extension cyclique de $L$ de degré 5. L'élément $(1 + j)$ appartient à $L$, sa norme est égale à :

$$N_{K/L}(1 + j) = (1 + j)^5 = -j$$

Par conséquent, il n'existe pas d'algèbre de division de degré 5 ayant comme corps de base $\mathbb{Q}(j)$.

En conclusion, les codes parfaits n'existent que pour les dimensions 2, 3, 4, et 6. Dans la suite nous présenterons les constructions algébriques de ces codes ainsi que leurs déterminants minimaux et leurs performances.

### 3.4.2 Famille infinie de codes parfaits $2 \times 2$

En utilisant l'approche proposée nous avons construit une famille infinie de codes parfaits en dimension 2 ($n_t = n_r = T = 2$).

Considérons comme corps de base $L = \mathbb{Q}(i)$. Soit $p$ un nombre premier tel que $p \equiv 5(\text{mod}8)$. $K$ est alors le corps de décomposition de $L$ et de $\mathbb{Q}(\sqrt{p})$, $K = \mathbb{Q}(i, \sqrt{p})$. $K$ est une extension relative de $\mathbb{Q}(i)$ de degré 2 et une extension absolue de $\mathbb{Q}$ de degré 4. Le groupe de Galois de $K/\mathbb{Q}(i)$ est engendré par $\sigma$, $\sigma : \sqrt{p} \longmapsto -\sqrt{p}$.

$K$ peut être vu aussi comme un espace-vectoriel sur $L$ ayant comme base $B = (1, \sqrt{p})$. Il s'écrit alors :

$$K = \left\{a + b\sqrt{p} \mid a,b \in L\right\}$$

$B$ n'est pas une base intégrale de $K$ parce qu'elle n'engendre pas tout l'anneau des entiers de $K$ (voir exemple paragraphe 1.3.2 du chapitre I). Sa base intégrale est $(1,\theta)$, où $\theta = \frac{1+\sqrt{p}}{2}$, et son anneau des entiers est $\mathbb{Z}[\theta]$.

$$K = \{a + b\theta \mid a,b \in L\}$$

Soit $\gamma \in O_L$, $\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre cyclique de degré 2.

$\gamma$ doit être pris dans $O_L$, tel que $\left|\gamma\right| = 1$. Le choix de $\gamma$ se limite ainsi à $\{-1,i,-i\}$. Nous choisissons de prendre $\gamma = i$.

Pour finir la construction du code ST, il nous reste donc à :
- montrer que $i$ n'est pas une norme sur $K/L$
- trouver un idéal $I \subseteq O_K$ tel que $\Lambda(I)$ soit une version homothétique tournée de $\mathbb{Z}[i]^2$
- définir le code ST

**Recherche de l'idéal**

Dans le paragraphe (3.3.3.1) nous avons montré qu'en prenant un idéal $I$ de norme $N(I) = \frac{(2c)^2}{\sqrt{|d_{K/\mathbb{Q}}|}}$, le réseau de points $\Lambda(I)$ serait une version homothétique tournée de $\mathbb{Z}[i]^2$.

Notre but est de construire une famille de codes. A chaque code correspond un corps de décomposition $K$ et donc un discriminant. Par conséquent, nous ne pouvons plus nous baser sur la norme de l'idéal pour trouver $I$. Nous allons alors utiliser une autre propriété du réseau de points complexe $\mathbb{Z}[i]^2$.

Le réseau de points $\mathbb{Z}[i]^2$ est l'unique réseau de points unimodulaire en dimension 2 [43]. Par conséquent, il suffit de trouver un idéal $I$ tel que $\Lambda(I)$ soit unimodulaire.

**Définition : 3.2** *réseau de points unimodulaire*
*Un réseau de points est unimodulaire s'il coïncide avec son dual.*

**Définition : 3.3** *réseau de points dual*
*Le réseau de points dual de $\Lambda(I)$ est le réseau de points*

$$\Lambda(I)^\sharp = \{x = a_1v_1 + a_2v_2, a_1, a_2 \in \mathbb{Q}[i] \mid \langle x,y\rangle \in \mathbb{Z}[i], \forall\, y \in \Lambda(I)\}$$

*où $(v_1,v_2)$ est une base du réseau de points $\Lambda(I)$.*

Le produit scalaire des deux vecteurs s'écrit en fonction de la trace algébrique :

$$\langle x,y\rangle = Tr_{K/L}(x\bar{y})$$

D'après le lemme suivant, le réseau de points dual d'un réseau de points algébrique complexe peut être défini explicitement.

**Lemme : 3.2** *Le réseau de points dual $\Lambda(I)^\sharp$ est le réseau de points $\Lambda(I^\sharp)$, où $I^\sharp = \overline{I^{-1}\mathcal{D}_{K/L}^{-1}}$ . $\mathcal{D}_{K/L}^{-1}$ est la codifférente .*

**Définition : 3.4** *codifférente ([44, p. 44] [40])*
*L'ensemble*

$$\mathcal{D}_{K/L}^{-1} = \left\{x \in K \mid \forall \alpha \in \mathcal{O}_K, Tr_{K/L}(x\alpha) \in \mathbb{Z}\right\}$$

*est un idéal fractionnel de $\mathcal{O}_K$ appelé **codifférente**. son idéal inverse $\mathcal{D}_{K/L}$ est un idéal intégral sur $\mathcal{O}_K$ appelé **différente**.*

Le lemme 3.2, découle directement de la définition de la codifférente.

Soit $x \in I^\sharp = \overline{I^{-1}\mathcal{D}_{K/L}^{-1}}$. Afin de montrer que $\Lambda(I)^\sharp = \Lambda(I^\sharp)$, il faut montrer que pour tout $y \in I$, $Tr_{K/L}(x\bar{y}) \in \mathbb{Z}[i]$. Soient $u \in I^{-1}$ et $v \in \mathcal{D}_{K/L}^{-1}$ tels que $x = \overline{uv}$. Nous avons donc $x\bar{y} = \overline{uyv}$, avec $uy \in \mathcal{O}_K$, d'où $Tr_{K/L}(x\bar{y}) \in \mathbb{Z}$.

Afin de trouver un idéal $I$ dans $\mathcal{O}_K$ tel que $\Lambda(I)$ soit unimodulaire, nous allons utiliser un résultat sur la factorisation des idéaux. Pour tout $p$ premier tel que $p \equiv 1(\text{mod}4)$ (cela reste vrai aussi pour $p \equiv 5(\text{mod}8)$), $p$ se factorise dans $\mathcal{O}_K$ comme suit [45] :

$$(p)\mathcal{O}_K = I^2 \cdot \bar{I}^2 \tag{3.10}$$

où $I$ et $\bar{I}$ sont des idéaux premiers conjugués.
Notons aussi que

$$\mathcal{D}_{K/L} = \mathcal{D}_{\mathbb{Q}(i,\sqrt{p})/\mathbb{Q}(\sqrt{p})} = \mathcal{D}_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}} = (\sqrt{p})\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = (\sqrt{p})$$

L'idéal dual de $I$ est :

$$I^\sharp = \overline{I^{-1}}(\sqrt{p})^{-1} = \frac{1}{p}I$$

Soit le réseau de points $(\frac{1}{\sqrt{p}}\Lambda(I))$, son réseau de points dual est :

$$(\frac{1}{\sqrt{p}}\Lambda(I))^\sharp = \sqrt{p}(\Lambda(I)^\sharp) = \frac{1}{\sqrt{p}}\Lambda(I)$$

Le réseau de points $(\frac{1}{\sqrt{p}}\Lambda(I))$ coïncide avec son réseau de points dual, il est alors unimodulaire.

**Choix de $\gamma$**

Pour que $\mathcal{A} = (K/L,\sigma,\gamma)$ soit une algèbre de division, il faut que $i$ ne soit pas une norme sur $K/L$. Tout $x \in K$ s'écrit, $x = a + b\sqrt{p}$, $a, b \in \mathbb{Q}(i)$, et sa norme relative dans $K/L$ s'écrit :

$$N_{K/L}(x) = (a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - pb^2$$

Montrer que $i$ n'est pas une norme sur $K/L$ revient à montrer que l'équation :

$$N_{K/L}(x) = i$$

n'a pas de solution. Pour cela, nous utilisons le corps des nombres $p$-adiques. La démonstration complète est donnée dans l'annexe B.

Nous avons donc prouvé que pour $p \equiv 5(\text{mod}8)$, $i$ n'est pas une norme sur $K/L$.

La preuve donnée dans l'annexe B est aussi valable pour $p \equiv 1(\text{mod}8)$ (en utilisant le fait que $y^{(p-1)/2} = (-1)^{(p-1)/4} = 1$).

Pour justifier notre choix de $p \equiv 5(\text{mod}8)$, nous allons nous appuyer sur un contre exemple écartant le cas $p \equiv 1(\text{mod}8)$.

*Contre exemple* : Prenons $p = 17$, donc $K = \mathbb{Q}(i, \sqrt{17})$. Soit $x = \frac{3(i-1)}{4} - \frac{(i-1)}{4}\sqrt{17} \in K$, la norme relative de $x$ est égale à $i$.

Ayant déterminé tous les paramètres nécessaires à la construction des codes parfaits : corps de base, corps de décomposition, choix de l'idéal et choix de $\gamma$. Nous entamons alors la construction proprement dites du code ST.

**Construction des codes parfaits** $2 \times 2$

Revenons à l'équation 3.10. Nous remarquons que pour $p \equiv 1(\text{mod}4)$, l'idéal $I$ est principal. Cela peut se voir directement de la factorisation de $p$ comme somme de deux carrés :

$$p = u^2 + v^2, u, v \in \mathbb{Z}$$

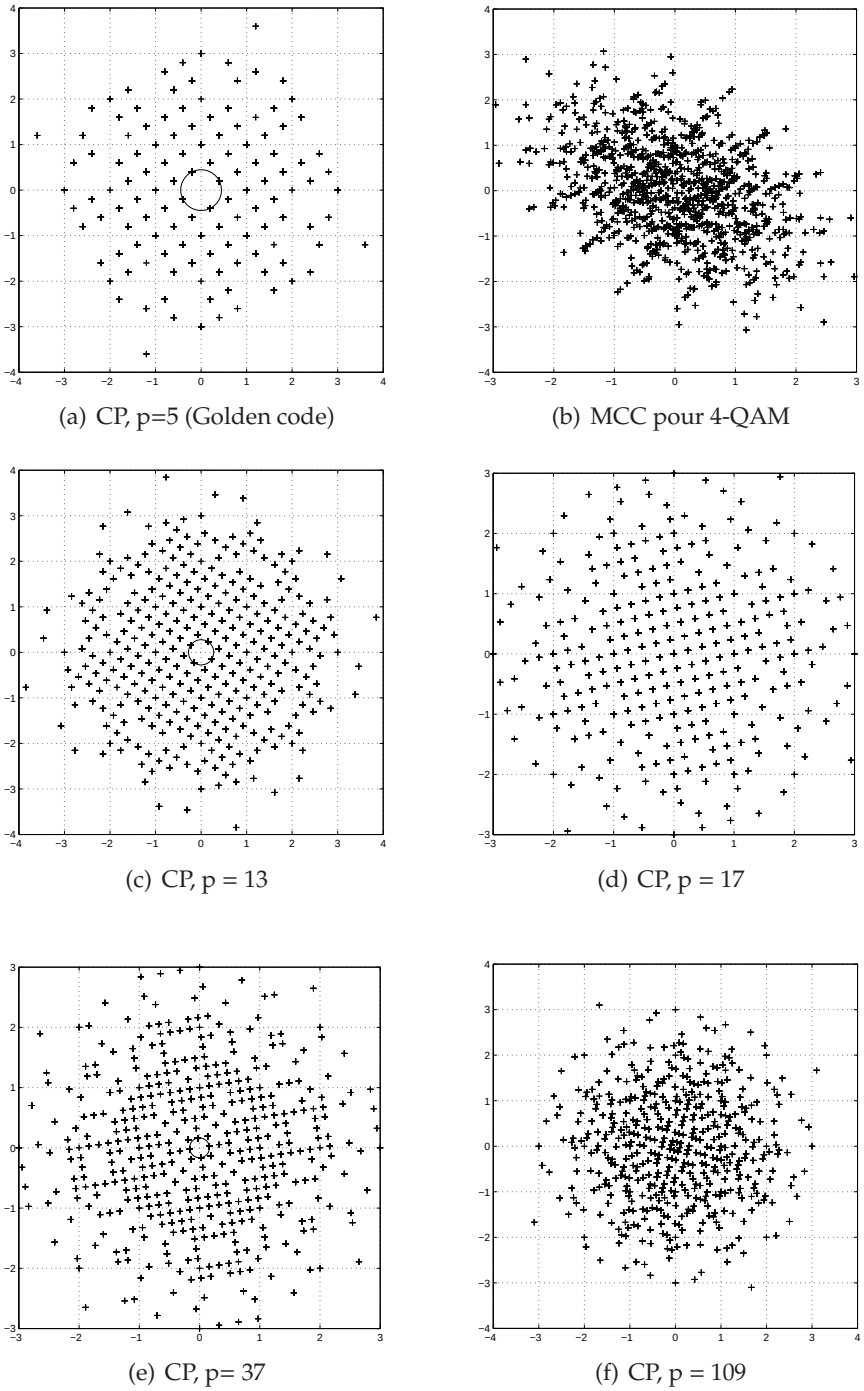
Soit $\alpha = \sqrt{u + iv}$. La norme absolue de $\alpha$ est égale à $N_{K/\mathbb{Q}}(\alpha) = p$. Par conséquent $\alpha \in I$ et sa norme est égale à $p$. $\alpha$ engendre donc $I$, par la suite $I$ est principal. La base de $I$ est ($\alpha$,$\alpha\theta$), et la matrice génératrice du réseau de points $\Lambda(I)$ est d'après (3.3) :

$$\mathbf{M_2} = \begin{bmatrix} \alpha & \alpha\theta \\ \bar{\alpha} & \overline{\alpha\theta} \end{bmatrix}$$

où $\bar{\theta} = \frac{1-\sqrt{d}}{2}$ le conjugué de $\theta$ et $\bar{\alpha}$ est le conjugué de $\alpha$ (étant donné que $\Lambda(I)$ est une version tournée de $\mathbb{Z}[i]^2$, il existe alors une matrice génératrice $\mathbf{M}$ de $\Lambda(I)$ tel que $\mathbf{M}\mathbf{M}^H = \mathbf{I}_2$, qui n'est pas obligatoirement égale à $\mathbf{M_2}$. $\mathbf{M}$ peut être trouvée par réduction de $\mathbf{M_2}$.

Chaque couche du mot de code est codée en multipliant les vecteurs de symboles $(s_1,s_2)^T$ et $(s_3,s_4)^T$ par la matrice $\mathbf{M_2}$. les symboles d'information $s_1$, $s_2$, $s_3$ et $s_4$ sont pris dans $\mathbb{Z}[i]$ pour le code ST infini et dans une constellation $q$-QAM pour le code ST fini. Un mot de code $\mathbf{X}$ s'écrit :

$$\begin{aligned} \mathbf{X} &= \text{diag}\left(\frac{1}{\sqrt{p}}\mathbf{M_2}\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}\right) \cdot \mathbf{I}_2 + \text{diag}\left(\frac{1}{\sqrt{p}}\mathbf{M_2}\begin{bmatrix} s_3 \\ s_4 \end{bmatrix}\right) \cdot \begin{bmatrix} 0 & 1 \\ \gamma & 0 \end{bmatrix} \\ &= \frac{1}{\sqrt{p}}\begin{bmatrix} \alpha(s_1 + \theta s_2) & \alpha(s_3 + \theta s_4) \\ i\bar{\alpha}(s_3 + \bar{\theta} s_4) & \bar{\alpha}(s_1 + \bar{\theta} s_2) \end{bmatrix} \end{aligned}$$



(a) CP, p=5 (Golden code)

(b) MCC pour 4-QAM

(c) CP, p = 13

(d) CP, p = 17

(e) CP, p= 37

(f) CP, p = 109

Fig. 3.6: Quelques déterminants de quelques codes parfaits $2\times2$ et du meilleur code $2\times2$ connu jusqu'à présent

**Déterminant minimal**

$I$ étant principal, nous déduisons d'après l'équation 3.7 le déterminant minimal du code :

$$\delta_{\min}(C_\infty) = \frac{1}{p^2}\left|N_{K/L}(\alpha)\right|^2 = \frac{1}{p}N_{K/\mathbb{Q}}(\alpha) = \frac{1}{p} \tag{3.11}$$

Dans la figure (3.6), nous avons tracé les distributions des déterminants dans le plan complexe des codes parfaits pour $p = 5, 13, 37$ et $109$, du code construit avec $p = 17$ et du meilleur code $2 \times 2$ connu jusqu'à présent pour la constellation 4-QAM (MCC) [18].

Nous voyons bien que les distributions des déterminants des codes parfaits sont discrètes alors que celle du code MCC est dense.

Nous observons aussi un disque vide autour de l'origine pour les codes parfaits, dont le diamètre diminue lorsque $p$ augmente. Le diamètre du disque n'est autre que le déterminant minimal. Pour le code construit avec $p = 17$, la distribution est uniforme autour de l'origine (pas de disque).

**Golden code**

D'après l'équation 3.11, les déterminants minimaux des codes parfaits $2 \times 2$ sont inversement proportionnels à $p$. Ainsi, le meilleur déterminant minimal correspond à $p = 5$, et est égal à $\frac{1}{5}$. Nous avons nommé "Golden code" le meilleur code parfait de la famille, correspondant à $p = 5$. Cette appellation est en relation avec l'utilisation du nombre d'or (Golden number) $\frac{1+\sqrt{5}}{2}$.

Le corps de décomposition sur lequel le "Golden code" est construit est $K = \mathbb{Q}(i, \sqrt{5})$. L'idéal principal $I$ est engendré par $\alpha = 1 + i - i\theta$, où $\theta = \frac{1+\sqrt{5}}{2}$.

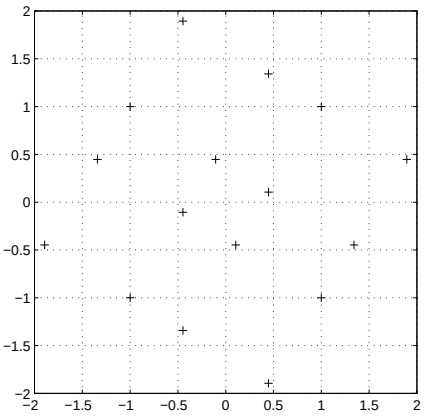
Notons que les codes $2 \times 2$ présentés dans [21, 22] sont des codes isomorphes au Golden code, mais construits par des optimisations respectivement numériques et analytiques.

**Constellations transmises**

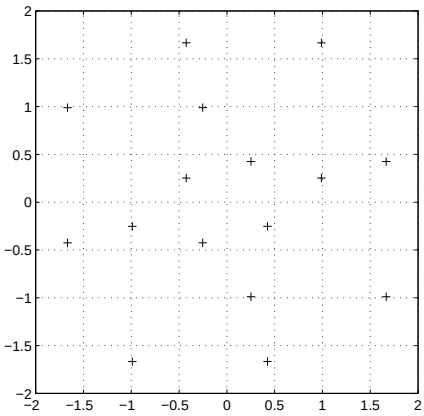
Les codes parfaits ont l'avantage d'avoir une bonne efficacité énergétique grâce au fait qu'ils n'ont pas de perte de forme dans les constellations transmises.

Dans la figure (3.7), nous avons tracé les constellations transmises des codes parfaits avec $p = 5, 13, 37$ et $109$, du code construit avec $p = 17$ et du meilleure code $2 \times 2$ connu jusqu'à présent pour la constellation 4-QAM (MCC) [18]. Les symboles d'information sont pris dans la constellation 4-QAM. Les constellations transmises sont les éléments de la matrice mot de code.

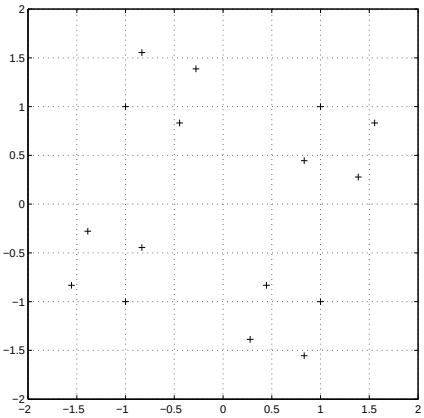
Nous remarquons que pour les codes parfaits et le code avec $p = 17$, les constellations transmises sont des versions tournées et régulièrement espacées de la constellation 16-QAM, alors que la constellation transmise par le code (MCC) est une réunion de 3 constellations PSK.



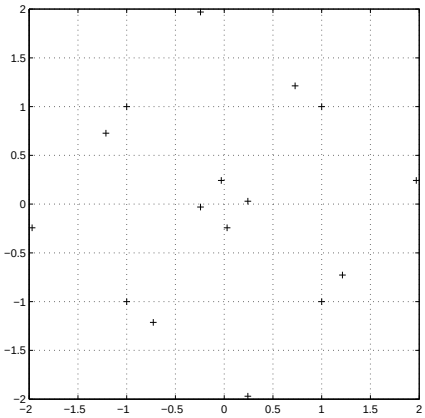
(a) CP, p=5 (Golden code)



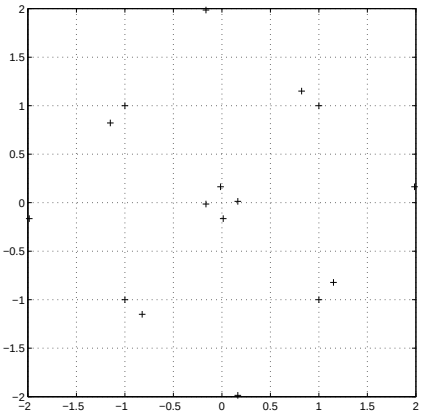
(b) MCC pour 4-QAM



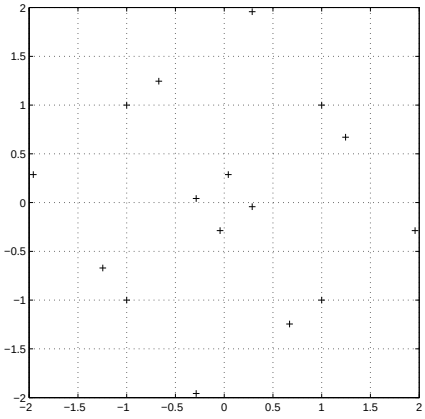
(c) CP, p = 13



(d) CP, p =17



(e) CP, p = 37



(f) CP , p = 109

Fig. 3.7: Constellations transmises de quelques codes parfaits $2 \times 2$ et du meilleur code $2 \times 2$ connu jusqu'à présent, la constellation à l'émission est une $4 - QAM$

**Performances**

Pour achever l'étude de la famille des codes parfaits (CP) en dimension 2, il faudra étudier et comparer les performances de ces codes avec celles des meilleurs codes $2 \times 2$ connus jusqu'à présent (MCC) [18] (voir tableau récapitulatif 2.2). Pour cela, nous avons simulé la chaîne de transmission (fig. 1.1) en utilisant les codes (CP) et les codes (MCC).

Dans la figure 3.8, nous avons tracé, en utilisant les constellations 4, 16, 64-QAM, le taux d'erreurs par mot de code en fonction du RSB= $\frac{E_b}{N_0}$ pour le Golden code (GC) et les (MCC).

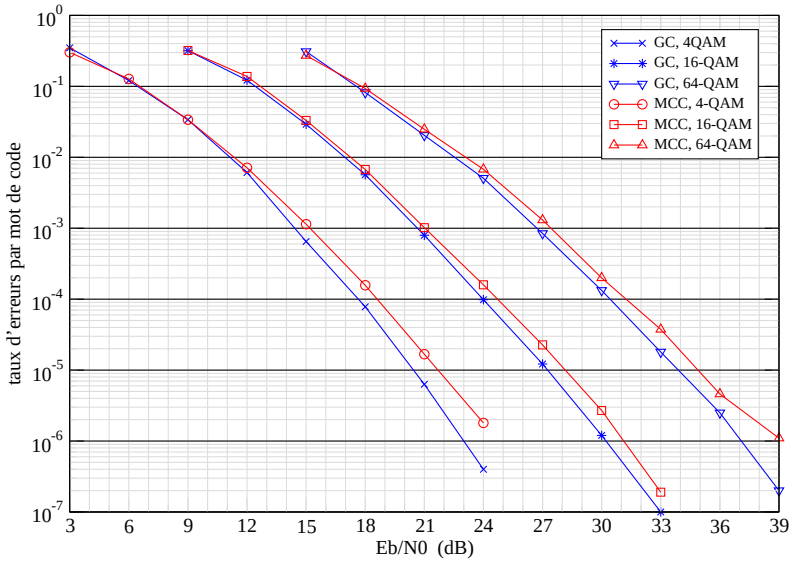



Fig. 3.8: Comparaison du Golden code et des meilleurs codes $2 \times 2$ connus pour différentes constellations $q$-QAM

Le Golden code possède les meilleures performances pour toutes les constellations. Nous remarquons aussi que l'écart entre les courbes de performances du Golden code pour les différentes constellations est constant et est égal à 6 dB. D'après [46], nous pouvons conclure que le Golden code atteint le compromis gain de multiplexage-diversité .

Dans la figure 3.9, nous avons rajouté les performances de quelques codes parfaits pour $p = 13, 37$ et $109$, et du code avec $p = 17$. Nous pouvons noter que les codes parfaits avec $p = 13, 37$ et $109$ ont des performances proches de celles des (MCC). Par ailleurs, le code avec $p = 17$ dispose de moins bonnes performances. Pour ce dernier, nous observons un changement de pente à fort RSB dû à son ordre de diversité qui est égal à 2. Rappelons que pour $p = 17$, nous avons trouvé un $x$ appartenant à $K = \mathbb{Q}(i, \sqrt{17})$ tel que $N_{K/L}(x) = i$. Cela implique que l'algèbre cyclique n'est pas une algèbre de division et le code n'est pas un code parfait. Nous pouvons expliquer le fait que ce code marche bien pour les faibles et moyens RSB et qu'il change de pente à fort RSB par une rare apparition d'un tel $x$.

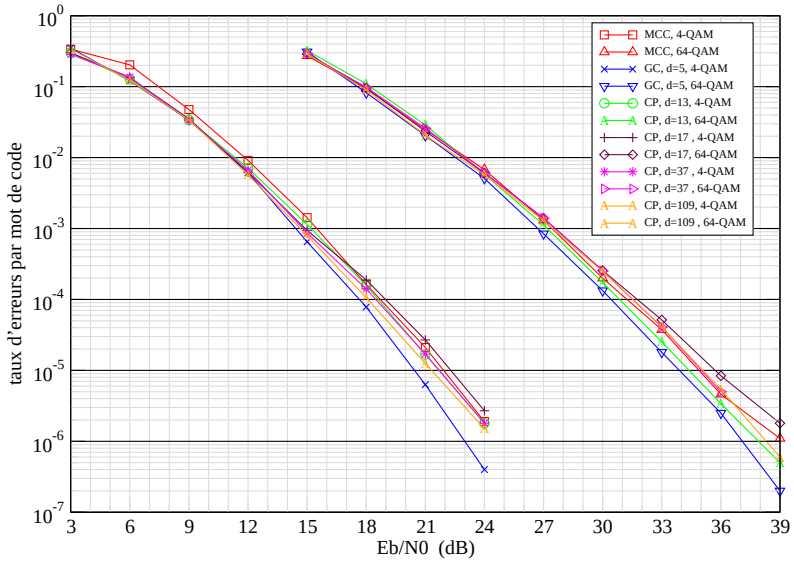



FIG. 3.9: Comparaison du Golden code et de quelques codes parfaits $2\times2$ et des meilleurs codes $2\times2$ connus pour différentes constellations $q$-QAM

### 3.4.3 Code parfait 3x3

Pour construire le code parfait $3\times3$, nous allons considérer comme corps de base $L=\mathbb{Q}(j)$ et utiliser par la suite les constellations $q$-HEX.

Soit $\theta=\zeta_7+\zeta_7^{-1}=2\cos(\frac{2\pi}{7})$, où $\zeta_7=\exp(\frac{i2\pi}{7})$ la $7^{\text{ième}}$ racine de l'unité. $K=\mathbb{Q}(j,\theta)$ est le corps de décomposition de $\mathbb{Q}(j)$ et de $\mathbb{Q}(\theta)$. Il est aussi le sous-corps réel du corps cyclotomique $\mathbb{Q}(\zeta)$. Soit $\sigma$ le générateur du groupe de Galois de $K$ :

$$\sigma:\zeta_7+\zeta_7^{-1}\longmapsto\zeta_7^2+\zeta_7^{-2}$$

$\mathbb{Q}(\theta)$ est une extension de degré 3 de $\mathbb{Q}$, par la suite $K$ est une extension relative de degré 3 de $L$ et est une extension absolue de degré 6 de $\mathbb{Q}$.
$K$ peut être vu aussi comme un espace-vectoriel sur $L$, de base intégrale $B=(1,\theta,\theta^2)$. $K$ s'écrit alors :

$$K=\left\{a+b\theta+c\theta^2\mid a,b,c\in L\right\}$$

Le polynôme minimal de $\theta$ est égal à $x^3+x^2-2x-1=0$.

Soit $\gamma\in\mathcal{O}_K$, $\mathcal{A}=(K/L,\sigma,\gamma)$ est une algèbre cyclique de degré 3.

$\gamma$ doit être pris dans $\mathcal{O}_L$, tel que $\left|\gamma\right|=1$. Ainsi le choix de $\gamma$ se limite à $\left\{-1,\pm j,\pm j^2\right\}$. Nous choisissons de prendre $\gamma=j$.

Pour finir la construction du code parfait ST, il nous reste donc à :
– montrer que $j$, $j^2$ ne sont pas des normes sur $K/L$
– trouver un idéal $I\subseteq\mathcal{O}_K$ tel que $\Lambda(I)$ soit une version homothétique tournée de $A_2^3$
– définir le code ST

**Recherche de l'idéal**

Afin de construire une version tournée de $A_2^3$, nous allons suivre la méthode décrite au paragraphe 3.3.3.1 qui utilise les volumes des réseaux de points.

Le volume du réseau de points $\Lambda(I)$ est :

$$V(\Lambda(I)) = 2^{-3}\sqrt{\left|d_{K/\mathbb{Q}}\right|}N(I)$$

Le discriminant absolu de $K$ est $d_{K/\mathbb{Q}} = -3^3 \cdot 7^4$ et son discriminant relatif est $d_{K/L} = 49 = 7^2$ . Une condition nécessaire pour obtenir une version tournée de $A_2^3$ est l'existence d'un idéal $I \subseteq \mathcal{O}_K$ de norme 7. Le volume de $\Lambda(I)$ devient :

$$V(\Lambda(I)) = 2^{-3} \cdot \sqrt{3^3 \cdot 7^2} = 7^3\left(\frac{\sqrt{3}}{2}\right)^3$$

Nous nous appuyons sur la factorisation des idéaux pour trouver le bon idéal $I$. En utilisant KANT, nous trouvons la factorisation suivante de l'idéal $(7)\mathcal{O}_K$ :

$$(7)\mathcal{O}_K = I_7^3\overline{I_7}^3$$

L'idéal $I = I_7$ est de norme 7, par conséquent $\Lambda(I)$ est une version homothétique tournée de $A_2^3$.

**Choix de $\gamma$**

$\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre de division si et seulement si $j$ et $j^2$ ne sont pas des normes sur $K$.

Montrer que $j$ et $j^2$ ne sont pas des normes sur $K/L$ revient à montrer que les équations

$$\begin{aligned} N_{K/L}(x) &= j \\ N_{K/L}(x) &= j^2 \end{aligned}$$

n'ont pas de solutions. Pour cela, nous utilisons des notions de la théorie des corps de classe. Les preuves complètes sont présentées dans l'annexe C.

**Construction du code Parfait $3 \times 3$**

Le code parfait $3\times3$ est un sous-ensemble fini de l'algèbre cyclique de division $\mathcal{A} = (K/L,\sigma,\gamma)$ obtenu en se restreignant à l'anneau des entiers $\mathcal{O}_K$.

Nous remarquons que $I$ est principal et est engendré par $\alpha = (1 + j) + \theta$. La base de $I$ est alors $(\alpha,\alpha\theta,\alpha\theta^2)$. Cette base n'est pas unitaire. Pour obtenir une base unitaire nous faisons un changement de base en utilisant la matrice $\mathbf{T_3}$ :

$$\mathbf{T_3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 2 & 1 & 0 \end{bmatrix}$$

La nouvelle base de $I$ est $\{v_k\}_{k=1...3} = ((1 + j) + \theta, (-1 - 2j) + j\theta^2, (-1 - 2j) + (1 + j)\theta + (1 + j)\theta^2)$. La matrice génératrice du réseau de points $\Lambda(I)$ est alors :

$$\mathbf{M_3} = \frac{1}{\sqrt{7}}\begin{bmatrix} v_1 & v_2 & v_3 \\ \sigma(v_1) & \sigma(v_2) & \sigma(v_3) \\ \sigma^2(v_1) & \sigma^2(v_2) & \sigma^2(v_3) \end{bmatrix}$$

Pour vérifier que $\Lambda(I)$ est bien une version tournée de $A_2^3$, il faut calculer la matrice de Gram de $\mathbf{M_3}$.
La matrice transposée hermitienne de $\mathbf{M_3}$ se calcule en utilisant la conjugaison dans $\mathbb{Z}[j]$ qui transforme $j$ en $j^2$. La matrice de Gram n'est autre que $\left(\frac{1}{7}Tr_{K/L}(v_k\tau(v_l))\right)_{k,l=1\ldots3}$. En utilisant

$$Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(1) = 3, \quad Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta) = -1, \quad Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2) = 5$$

Nous trouvons que

$$\frac{1}{7}Tr_{K/L}(v_k\tau(v_l)) = \delta_{kl}, k,l = 1\ldots3$$

Nous déduisons que $\mathbf{M_3}$ est unitaire. Pour l'implémentation du code, nous donnons la version numérique de la matrice $\mathbf{M_3}$.

$$\mathbf{M_3} = \frac{1}{\sqrt{7}}\begin{bmatrix} 1.0382 + i0.3273 & -0.4620 - i0.1456 & 0.8326 + i0.2624 \\ -0.1141 + i0.3273 & -0.1423 + i0.4081 & 0.0633 - i0.1816 \\ 0.3987 + i0.3273 & -0.7184 - i0.5898 & -0.8959 - i0.7354 \end{bmatrix}$$

Un mot de code s'écrit alors dans la base de l'algèbre de division $(\mathbf{I}_3,\mathbf{e},\mathbf{e}^2)$ de la façon suivante :

$$\mathbf{X} = \text{diag } (\mathbf{M_3S_1})\,\mathbf{I}_3 + \text{diag } (\mathbf{M_3S_2}) \cdot \mathbf{e} + \text{diag } (\mathbf{M_3S_3}) \cdot \mathbf{e}^2$$

avec

$$\mathbf{e} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \gamma & 0 & 0 \end{bmatrix}$$

Les $\mathbf{S_l} = (s_{l1},s_{l2},s_{l3})^T$, $l = 1\ldots3$ sont les vecteurs composés par les 9 symboles d'information. Les symboles d'information sont pris dans $\mathbb{Z}[j]$ pour le code ST infini et dans une constellation $q$-HEX pour le code ST fini.

**Déterminant minimal**

L'idéal $I$ étant principal, nous déduisons directement le déterminant minimal du code de l'équation (3.7) :

$$\delta_{\min}(C_\infty) = \frac{1}{7^3} \cdot N_{K/\mathbb{Q}}(\alpha) = \frac{7}{7^3} = \frac{1}{49} = \frac{1}{d_{\mathbb{Q}(\theta)}}$$

**Performances**

Afin de pouvoir évaluer et comparer les performances de notre nouveau code, nous avons simulé la chaîne de transmission (fig. 1.1) en utilisant le code parfait (CP) $3 \times 3$ et le meilleur code en dimension 3 connu jusqu'à présent (MCC) [19, 20].

Dans la figure 3.10, nous avons tracé le taux d'erreurs par mot de code en fonction du RSB = $\frac{E_b}{N_0}$ pour les codes (CP) et (MCC) en utilisant les constellations 4, 8, 16-HEX pour les (CP) et les constellations 4, 8, 16-QAM pour les (MCC).

Pour la constellation 4-HEX, nous constatons que les performances du (MCC) sont légèrement meilleures que celles du (CP). Cependant, pour des efficacités spectrales plus élevées, le (CP) prend l'avantage sur le (MCC) grâce à son déterminant qui ne s'évanouit pas lorsque l'efficacité spectrale augmente.

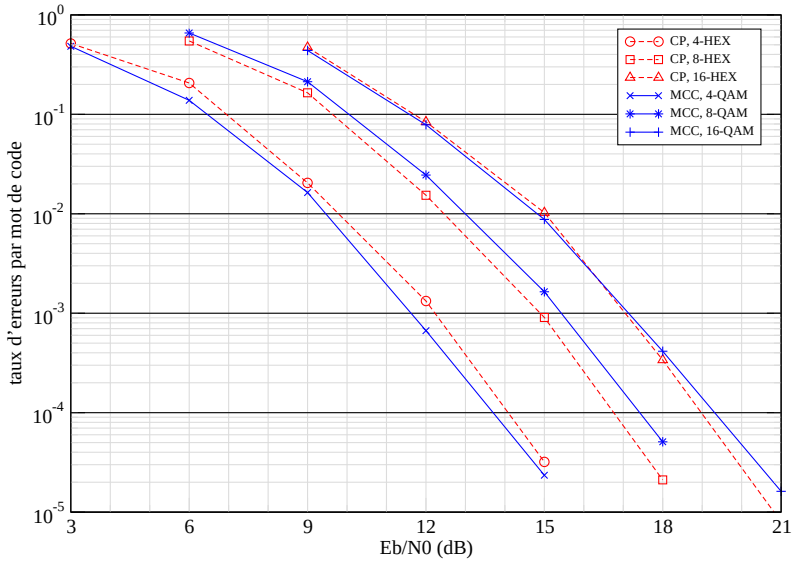



Fig. 3.10: Comparaison du code parfait $3 \times 3$ et du meilleure code $3 \times 3$ connu, pour différentes constellations $q$-HEX et $q$-QAM

### 3.4.4 Code parfait 4x4

Pour le code parfait $4 \times 4$ (comme pour la famille de codes parfaits en dimension 2), notre corps de base sera $L = \mathbb{Q}(i)$. Les constellations utilisées seront par la suite les constellations $q$-QAM.

Soit $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2\cos(\frac{2\pi}{15})$, où $\zeta_{15} = \exp(\frac{i2\pi}{15})$ la $15^{\text{ième}}$ racine de l'unité. $K = \mathbb{Q}(i,\theta)$ est alors le corps de décomposition de $\mathbb{Q}(i)$ et de $\mathbb{Q}(\theta)$. Il est aussi le sous-corps réel du corps cyclotomique $\mathbb{Q}(\zeta_{15})$. Soit $\sigma$ le générateur du groupe de Galois de $K$ :

$$\sigma : \zeta_{15} + \zeta_{15}^{-1} \longmapsto \zeta_{15}^{2} + \zeta_{15}^{-2}$$

$\mathbb{Q}(\theta)$ est une extension de degré 4 de $\mathbb{Q}$, par la suite $K$ est une extension relative de degré 4 de $L = \mathbb{Q}(i)$ et une extension de degré 8 de $\mathbb{Q}$.

$K$ peut être vu aussi comme espace-vectoriel sur $L$, de base intégrale $B = (1,\theta,\theta^2,\theta^3)$. Il s'écrit alors :

$$K = \left\{ a + b\theta + c\theta^2 + d\theta^3 \mid a,b,c,d \in L \right\}$$

Le polynôme minimal de $\theta$ est $x^4 - x^3 - 4x^2 + 4x + 1 = 0$.

Soit $\gamma \in \mathbb{O}_L$, $\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre cyclique de degré 4.

$\gamma$ doit être pris dans $\mathcal{O}_L$, tel que $\left|\gamma\right| = 1$. Ainsi le choix de $\gamma$ se limite à $\{-1,i,-i\}$. Nous choisissons de prendre $\gamma = i$.

Pour finir la construction du code ST, il nous reste donc à :
- montrer que $i, -1, -i$ ne sont pas des normes sur $K/L$
- trouver un idéal $I \subseteq \mathcal{O}_K$ tel que $\Lambda(I)$ soit une version homothétique tournée de $\mathbb{Z}[i]^4$

– construire le code ST

**Recherche de l'idéal**

Afin de construire une version tournée $\mathbb{Z}[i]^4$, nous allons nous baser sur la norme de l'idéal dont l'expression est donnée au paragraphe 3.3.3.1. Le volume du réseau de points $\Lambda(I)$ est :

$$V(\Lambda(I)) = 2^{-4}\sqrt{|d_{K/Q}|}N(I)$$

Le discriminant absolu de $K$ est $d_K = 2^8 \cdot 3^4 \cdot 5^6$ et son discriminant relatif est $d_{K/L} = 1125 = 3^2 \cdot 5^3$. Une condition nécessaire pour obtenir une version tournée de $\mathbb{Z}[i]^4$ est l'existence d'un idéal $I \subseteq \mathbb{O}_K$ tel que :

$$N(I) = 45 = 3^2 \cdot 5$$

Dans ce cas le volume de $\Lambda(I)$ devient :

$$V(\Lambda(I)) = 3^4 \cdot 5^4 = \sqrt{15}^8$$

Géométriquement cela peut s'interpréter par la fait que le parallélotope fondamental du réseau de points est un hypercube dont les cotés sont de longueur $\sqrt{15}$.

Afin de trouver l'idéal $I$, nous allons nous appuyer sur la factorisation des idéaux. En utilisant KANT, nous trouvons les factorisations suivantes des idéaux $(3)\mathcal{O}_K$ et $(5)\mathcal{O}_K$ :

$$\begin{aligned}(3)\mathcal{O}_K &= I_3^2\overline{I_3}^2\\ (5)\mathbb{O}_K &= I_5^4\overline{I_5}^4\end{aligned}$$

L'idéal $I = I_3 \cdot I_5$ est de norme 45. Par la suite $\Lambda(I)$ est bien une version homothétique tournée de $\mathbb{Z}[i]^4$.

**Choix de $\gamma$**

Nous avons choisi $\gamma = i$. Pour que $\mathcal{A} = (K/L,\sigma,\gamma)$ soit une algèbre de division, il faut montrer que $\pm i, -1$ ne sont pas des normes sur $K$,

Pour montrer que $i$ et $-i$ ne sont pas des normes dans $K^*$, nous allons nous appuyer sur l'emboîtement des corps d'extensions et la transitivité de la norme.

**Lemme : 3.3** *Nous avons*

$$\mathbb{Q} \subset \mathbb{Q}(i,\sqrt{5}) \subset K$$

Pour prouver ce résultat, il suffit de montrer que $\mathbb{Q}(i,\sqrt{5})$ est le sous corps fixé par $\left\langle\sigma^2\right\rangle$, le sous groupe d'ordre 2 du groupe de Galois $Gal_{K/L} = \langle\sigma\rangle$.

Soit $\sigma^2 : \zeta_{15} + \zeta_{15}^{-1} \longmapsto \zeta_{15}^4 + \zeta_{15}^{-4}$. Il est facile de voir que pour $x = \sum_{k=0}^{3} a_k(\zeta + \zeta^{-1})^k \in K$, $a_k \in \mathbb{Q}(i)$, tel que $\sigma^2(x) = x$, $x$ est de de la forme $a_0 + a_3(\zeta_{15}^3 + \zeta_{15}^{-3}) = a_0 + a_3\frac{1+\sqrt{5}}{2} \in \mathbb{Q}(i,\sqrt{5})$.

Pour tout $x \in K$, nous avons :

$$N_{K/L}(x) = N_{\mathbb{Q}(i,\sqrt{5})/L}(N_{K/\mathbb{Q}(i,\sqrt{5})}(x))$$

D'où, si $\pm i$ sont des normes sur $K$ alors elles le sont aussi sur $\mathbb{Q}(i,\sqrt{5})$. Or nous savons que pour $p=5$, $\pm i$ ne sont pas des normes sur $\mathbb{Q}(i,\sqrt{5})$ (annexe B). Nous déduisons que $\pm i$ ne sont pas des normes sur $K$.

Nous montrons que $-1$ n'est pas une norme sur $K$ dans l'annexe D.

**Construction du code Parfait** $4\times 4$

Le code parfait $4\times4$ est un sous-ensemble fini de l'algèbre cyclique de division $\mathcal{A}=(K/L,\sigma,\gamma)$ obtenue en se restreignant à l'anneau des entiers $O_K$.

Nous remarquons que l'idéal $I$ est principal, il est engendré par $\alpha=(1-3i)+i\theta^2$. La base de $I$ est alors $(\alpha,\alpha\theta,\alpha\theta^2,\alpha\theta^3)$. Malheureusement cette base n'est pas unitaire. Pour obtenir la base unitaire nous faisons le changement de base en utilisant la matrice $\mathbf{T_4}$ :

$$\mathbf{T_4}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&-3&0&1\\-1&-3&1&1\end{bmatrix}$$

On obtient une nouvelle base de $I$ : $\{v_k\}_{k=1\ldots4}=((1-3i)+i\theta^2,(1-3i)\theta+i\theta^3,-i+(-3+4i)\theta+(1-i)\theta^3,(-1+i)-3\theta+\theta^2+\theta^3)$.

La matrice génératrice du réseau de points $\Lambda(I)$ est alors :

$$\mathbf{M_4}=\frac{1}{\sqrt{15}}\begin{bmatrix}v_1&v_2&v_3&v_4\\\sigma(v_1)&\sigma(v_2)&\sigma(v_3)&\sigma(v_4)\\\sigma^2(v_1)&\sigma^2(v_2)&\sigma^2(v_3)&\sigma^2(v_4)\\\sigma^3(v_1)&\sigma^3(v_2)&\sigma^3(v_3)&\sigma^3(v_4)\end{bmatrix}$$

Pour vérifier que $\Lambda(I)$ est bien une version tournée de $\mathbb{Z}[i]^4$, il faut calculer la matrice de Gram du réseau.

La matrice de Gram n'est autre que $\left(\frac{1}{15}Tr_{K/L}(v_k\overline{v_l})\right)_{k,l=1\ldots4}$. En utilisant :

$$Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta)=1,\quad Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^2)=9,\quad Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^3)=1,\quad Tr_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta^4)=29$$

Nous trouvons que

$$\frac{1}{15}Tr_{K/L}(v_k\overline{v_l})=\delta_{kl},\ k,l=1\ldots4$$

D'où $\mathbf{M_4}$ est unitaire.

Pour l'implémentation du code, nous donnons la version numérique de la matrice $\mathbf{M_4}$.

$$\mathbf{M_4}=\begin{bmatrix}0.2582-0.3122i&0.3455-0.4178i&-0.4178+0.5051i&-0.2136+0.2582i\\0.2582+0.0873i&0.4718+0.1596i&0.1596+0.054i&0.7633+0.2582i\\0.2582+0.2136i&-0.5051-0.4178i&-0.4178-0.3455i&0.3122+0.2582i\\0.2582-0.7633i&-0.054+0.1596i&0.1596-0.4718i&-0.0873+0.2582i\end{bmatrix}$$

Un mot de code s'écrit dans la base de l'algèbre de division $(\mathbf{I_4},\mathbf{e},\mathbf{e}^2,\mathbf{e}^3)$ de la façon suivante :

$$\mathbf{X}=\text{diag}\ (\mathbf{M_4S_1})\,\mathbf{I}_4+\text{diag}\ (\mathbf{M_4S_2})\cdot\mathbf{e}+\text{diag}\ (\mathbf{M_4S_3})\cdot\mathbf{e}^2+\text{diag}\ (\mathbf{M_4S_4})\cdot\mathbf{e}^3$$

avec

$$\mathbf{e} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 \end{bmatrix}$$

$\mathbf{S_l} = (s_{l1}, s_{l2}, s_{l3}, s_{l4})^T$, $l = 1 \dots 4$ sont les vecteurs composés par les 16 symboles d'information. Les symboles d'information sont pris dans $\mathbb{Z}[i]$ pour le code ST infini et dans une constellation $q$-QAM pour le code ST fini.

**Déterminant minimal**

L'idéal $I$ étant principal, nous pouvons déduire directement le déterminant minimal d'après l'équation (3.7) :

$$\delta_{\min}(C_\infty) = \frac{1}{15^4} \cdot N_{K/\mathbb{Q}}(\alpha) = \frac{45}{15^4} = \frac{1}{1125} = \frac{1}{d_{\mathbb{Q}(\theta)}}$$

**Performances**

Afin de pouvoir évaluer et comparer les performances du nouveau code, nous avons simulé la chaîne de transmission (fig. 1.1) en utilisant le code parfait (CP) $4 \times 4$ et le meilleur code en dimension 4 connu jusqu'à présent (MCC) [19, 20] .

Dans la figure 3.11, nous avons tracé le taux d'erreurs par mot de code en fonction du RSB = $\frac{E_b}{N_0}$, pour le (CP) et le (MCC) en utilisant les constellations 4, 16, 64-QAM.

Les performances des deux codes sont très proches. Néanmoins, nous pouvons remarquer qu'en augmentant l'efficacité spectrale, le (CP) l'emporte sur le code (MCC) grâce à son déterminant qui ne s'évanouit pas.

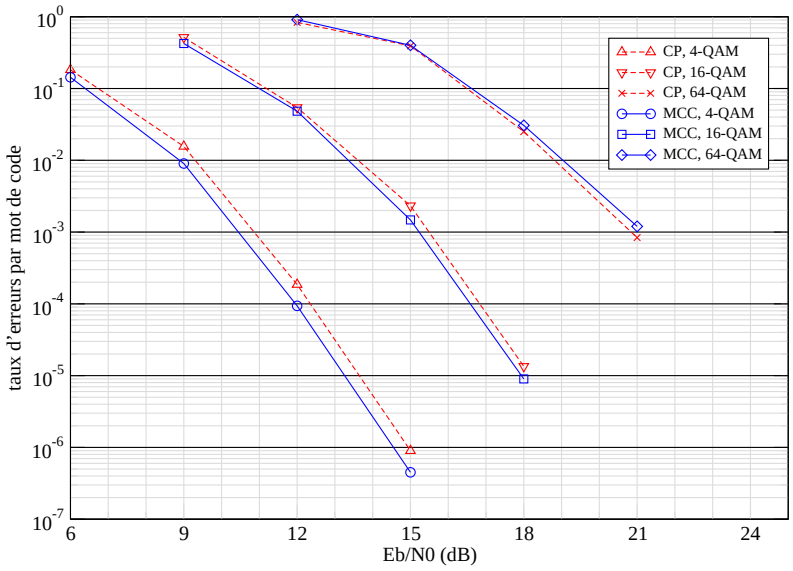



Fig. 3.11: Comparaison du code parfait $4 \times 4$ et du meilleur code $4 \times 4$ connu, pour différentes constellations $q$-QAM

### 3.4.5 Code parfait 6x6

Comme pour le code parfait $3 \times 3$, nous allons considérer comme corps de base $L = \mathbb{Q}(j)$, et utiliser par la suite des constellations $q$-HEX.

Soit $\theta = \zeta_{28} + \zeta_{28}^{-1} = 2\cos(\frac{\pi}{14})$, où $\zeta_{28} = \exp(\frac{i\pi}{14})$ la $28^{\text{ième}}$ racine de l'unité. $K = \mathbb{Q}(j,\theta)$ est le corps de décomposition de $\mathbb{Q}(j)$ et de $\mathbb{Q}(\theta)$. Il est aussi le sous-corps réel du corps cyclotomique $\mathbb{Q}(\zeta_{28})$. Soit $\sigma$ le générateur du groupe de Galois de $K$ :

$$\sigma : \zeta_{28} + \zeta_{28}^{-1} \longmapsto \zeta_{28}^{2} + \zeta_{28}^{-2}$$

$\mathbb{Q}(\theta)$ est une extension de degré 6 de $\mathbb{Q}$, par conséquent $K$ est une extension relative de degré 6 de $L$ et est une extension absolue de degré 12 de $\mathbb{Q}$.

Soit $\gamma \in \mathcal{O}_L$. $\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre cyclique de degré 6.

$\gamma$ doit être pris dans $\mathbb{O}_L$, tel que $\left|\gamma\right| = 1$. Ainsi le choix de $\gamma$ se limite à $\left\{-1, \pm j, \pm j^2\right\}$. Nous choisissons de prendre $\gamma = -j$.

Pour finir la construction du code ST, il nous reste donc à :
- montrer que $\pm j,\ \pm j^2$ et $-1$ ne sont pas des normes sur $K$
- trouver un idéal $I \subseteq \mathcal{O}_K$ tel que $\Lambda(I)$ soit une version homothétique tournée de $A_2^6$
- construire le code ST

**Recherche de l'idéal**

Afin de construire une version tournée de $A_2^6$, nous suivons toujours la méthode utilisant le volume du réseau de points décrite au paragraphe 3.3.3.1 .

Le volume du réseau de points $\Lambda(I)$ est $2^{-6}\sqrt{d_K}N(I)$ et le discriminant absolu de $K$ est $d_K = 2^{12} \cdot 3^6 \cdot 7^{10}$. Une condition nécessaire pour obtenir une version tournée de $A_2^6$ est l'existence d'un idéal $I \subseteq \mathbb{O}_K$ de norme 7. Dans ce cas le volume de $\Lambda(I)$ devient

$$V(\Lambda(I)) = 2^{-6} \cdot 2^6 \cdot 3^3 \cdot 7^5.7 = 2^6 \cdot 7^6 \cdot \left(\frac{\sqrt{3}}{2}\right)^6$$

Comme pour les deux précédentes constructions, nous utilisons la factorisation des idéaux afin de trouver le bon idéal $I$. En effet, l'idéal $(7)\mathcal{O}_K$ se factorise comme suit :

$$(7)\mathcal{O}_K \quad = \quad I_7^6\overline{I_7}^6$$

L'idéal $I = I_7$ est de norme 7, il répond alors au problème.

**Choix de $\gamma$**

$\mathcal{A} = (K/L,\sigma,\gamma)$ est une algèbre de division si et seulement si $\pm j,\ \pm j^2$ et $-1$ ne sont pas des normes sur $K$.

Comme pour la dimension 4, nous allons exploiter l'emboîtement des corps d'extension et la transitivité de la norme pour établir ce dernier résultat.

**Lemme : 3.4** *Nous avons*

$$\mathbb{Q}(j) \subset \mathbb{Q}(j,\zeta_7 + \zeta_7^{-1}) \subset \mathbb{Q}(j,\zeta_{28} + \zeta_{28}^{-1})$$

Ce résultat découle du fait que $\mathbb{Q}(j,\zeta+\zeta_7^{-1})$ est le sous corps fixé par $\left\langle\sigma^2\right\rangle$, le sous groupe d'ordre 2 du groupe de Galois $Gal_{K/L}=\langle\sigma\rangle$. Soit $x\in K$, nous avons donc :

$$N_{K/L}(x)=N_{\mathbb{Q}(j,\zeta_7+\zeta_7^{-1})/L}\left(N_{K/\mathbb{Q}(j,\zeta_7+\zeta_7^{-1})}(x)\right)$$

et puisque $\left[\mathbb{Q}(\zeta_7+\zeta_7^{-1},j):L\right]=3$, nous avons aussi :

$$N_{K/L}(x)=N_{\mathbb{Q}(j,\zeta_7+\zeta_7^{-1})/L}\left(-N_{K/\mathbb{Q}(j,\zeta_7+\zeta_7^{-1})}(x)\right)$$

Si $\pm j$ ou $\pm j^2$sont des normes sur $K$ alors ils le sont aussi sur $\mathbb{Q}(j,\zeta_7+\zeta_7^{-1})$. Or dans l'annexe C nous montrons que $j$ et $j^2$ ne sont pas des normes sur $\mathbb{Q}(j,\zeta_7+\zeta_7^{-1})$. Donc $\pm j$ et $\pm j^2$ ne sont pas des normes sur K.

Nous montrons aussi que $-1$ n'est une norme sur $K$ dans l'annexe E.

**Construction du code Parfait** $6\times 6$

Le code parfait $6\times6$ est un sous-ensemble fini de l'algèbre cyclique de division $\mathcal{A}=(K/L,\sigma,\gamma)$ obtenu en se restreignant à l'anneau des entiers $O_K$.

Contrairement aux précédentes constructions, comme $I$ n'est pas un idéal principal, il devient plus difficile de lui trouver une base. En utilisant KANT, nous déterminons une base numérique de $I$ et nous calculons sa matrice de Gram. Nous réduisons cette dernière par l'algorithme de réduction LLL (Lenstra-Lenstra-Lovasz). Cet algorithme a été modifié (annexe F) pour pouvoir l'appliquer à des réductions de base dans $\mathbb{Z}[j]$. Nous obtenons ainsi la matrice de Gram réduite, ainsi que la matrice de changement de base $\mathbf{T_6}$ :

$$\mathbf{T_6}=\begin{bmatrix}0&1&0&0&0&0\\1+j&0&1&0&0&0\\-1-2j&0&-5&0&1&0\\1+j&0&4&0&-1&0\\0&-3&0&1&0&0\\0&5&0&-5&0&1\end{bmatrix}$$

Nous donnons la matrice génératrice du réseau de points $\Lambda(I)$ sous forme numérique.

$$\mathbf{M_6}=\frac{1}{\sqrt{14}}\begin{bmatrix}1.9498&1.3019-i0.8660&-0.0549-i0.8660&-1.7469-i0.8660&1.5636&0.8677\\0.8677&-1.7469-i0.8660&1.3019-i0.8660&-0.0549-i0.8660&-1.9498&1.5636\\1.5636&-0.0549-i0.8660&-1.7469-i0.8660&1.3019-i0.8660&-0.8677&-1.9498\\-1.9498&1.3019-i0.8660&-0.0549-i0.8660&-1.7469-i0.8660&-1.5636&-0.8677\\-0.8677&-1.7469-i0.8660&1.3019-i0.8660&-0.0549-i0.8660&1.9498&-1.5636\\-1.5636&-0.0549-i0.8660&-1.7469-i0.8660&1.3019-i0.8660&0.8677&1.9498\end{bmatrix}$$

Nous avons bien $\mathbf{M_6}\mathbf{M_6^H}=\mathbf{I}_6$.

Le mot de code s'écrit dans la base de l'algèbre de division comme suit :

$$\mathbf{X}=\sum_{l=1}^{6}\text{diag }\left(\mathbf{M_6}\mathbf{S_l}\right)\mathbf{e}^{l-1}$$

avec

$$\mathbf{e} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Les $\mathbf{S_l} = (s_{l1}, s_{l2}, s_{l3}, s_{l4}, s_{l5}, s_{l6},)^T$, $l = 1 \ldots 63$ sont des vecteurs composés par les 36 symboles d'information. Les symboles d'information sont pris dans $\mathbb{Z}[j]$ pour le code ST infini et dans les constellations $q$-HEX pour le code ST fini.

**Déterminant minimal**

L'idéal $I$ n'est pas principal. Nous déduisons les bornes supérieures et inférieures du déterminant minimal du code infini de l'équation 3.9 :

$$\frac{1}{14^6} N_{K/\mathbb{Q}}(I) = \frac{1}{2^6 \cdot 7^5} = \frac{1}{d_{\mathbb{Q}(\theta)}} \leq \delta_{\min}(C_\infty) \leq \frac{1}{14^6} \min_{x \in I} N_{K/\mathbb{Q}}(x) = \frac{7^2}{2^6 \cdot 7^6}$$

d'où :

$$\frac{1}{2^6 \cdot 7^5} \leq \delta_{\min}(C_\infty) \leq \frac{1}{2^6 \cdot 7^4}$$

## 3.5 Compromis gain de "multiplexage-diversité" des codes Quaternioniques et des codes Parfaits

Les codes Quaternioniques et les codes Parfaits construits dans les précédents paragraphes, ont un rendement plein, une diversité pleine et un déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Cette dernière propriété leur permet d'atteindre le gain de multiplexage-diversité (diversity-multiplexing gain - DMG) optimal.

En effet, dans [29], il a été prouvé que tout code ST construit à partir d'algèbre cyclique de division de centre $\mathbb{Q}$, $\mathbb{Q}(i)$ ou $\mathbb{Q}(j)$, ayant un déterminant minimal ne s'évanouissant pas, atteint la DMG. Ce résultat a été prouvé dans [29, Théorème 1] pour des codes ST vérifiant des contraintes plus générales.

Une notion fondamentale nécessaire pour établir ce résultat est l'alphabet "scalably dense". Un alphabet $A$ est "scalably dense" si sa taille est fonction du RSB en vérifiant les propriétés suivantes :

$$\begin{aligned} |A(RSB)| &\doteq RSB^{\frac{r}{n_t}} \text{ et} \\ a \in A(RSB) &\Rightarrow |a|^2 \dot{\leq} RSB^{\frac{r}{n_t}} \end{aligned} \tag{3.12}$$

où $r$ est le rendement normalisé compris entre 1 et $\min(n_t, n_r)$ défini dans le paragraphe 2.1.3. Les notations $\doteq$ et $\dot{\leq}$ correspondent respectivement aux égalités et inégalités exponentielles définies dans [28]

$$f(RSB) \doteq RSB^b \Leftrightarrow \lim_{RSB \to \infty} \frac{\log f(RSB)}{\log RSB} = b$$

**Théorème : 3.1** *[29, Théorème 1]Soit A un alphabet "scalably dense" . Considérant un code ST, avec $T = n_t$, tel qu'un mot de code X vérifie :*

1. *X est linéaire par rapport aux symboles de A*
2. *X est de rendement plein , i.e., $|X| \doteq RSB^{rT}$*
3. *le déterminant minimal de X ne s'évanouit pas lorsque l'efficacité spectrale augmente*

*Alors le code ST atteint la borne supérieure du compromis gain de multiplexage-diversité.*

Notons que lorsque $n_t = T$, la borne supérieure est la vraie frontière multiplexage-diversité.

Les codes quaternioniques et les codes parfaits satisfont bien le théorème 3.1. En effet, ils sont des codes LD, chaque entrée de la matrice mot de code est combinaison linéaire de $n_t$ symboles d'information $q$-QAM ou $q$-HEX. Leur rendement est plein, $n_t$ symboles/uc, et ont des déterminants minimaux ne s'évanouissant pas. De plus les constellations $q$-QAM et $q$-HEX vérifient la condition 3.12 :

$$R = r \log_2 RSB = n_t \log_2 q$$

d'où :

$$q = RSB^{\frac{r}{n_t}}$$

Nous donnons dans la suite les principales étapes de la démonstration du théorème 3.1 présentée dans [29].

Considérons un code ST, avec $n = n_t = T$, linéaire, de rendement plein, ayant un déterminant minimal ne s'évanouissant pas. Soit $\Delta X = X_i - X_j$ la différence de deux mots de code, et $H$ la matrice de transfert du canal de transmission. Soient $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ et $l_1 \geq l_2 \geq \cdots \geq l_n$ les valeurs propres ordonnées respectives de $H^H H$ et $\Delta X \Delta X^H$. Pour $H$ fixé, le carré de la distance euclidienne s'écrit :

$$d_E^2 = Tr(\theta^2 H \Delta X \Delta X^H H^H)$$

où $\theta$ représente l'énergie d'émission. De façon à avoir $\|\theta X\|_F^2 \dot{\leq} RSB$, il faut choisir $\theta^2 \doteq RSB^{1-\frac{r}{n}}$. En utilisant la décomposition en valeurs propres de $\Delta X \Delta X^H$ et de $H^H H$, ainsi que la "mismatched eigenvalue bound" [29, Théorème 2], une borne inférieure de $d_E^2$ peut être dérivée :

$$d_E^2 \geq \theta^2 \sum_{i=1}^{n} \lambda_i l_i \tag{3.13}$$

Cette dernière inégalité induit $n$ inégalités :

$$d_E^2 \geq \theta^2 \sum_{i=n-j}^{n} \lambda_i l_i,\ j = 0, \cdots, n-1 \tag{3.14}$$

Le déterminant minimal ne s'évanouissant pas lorsque l'efficacité spectrale augmente donne :

$$\lim_{RSB \to \infty} \frac{\log \det_{min}}{\log RSB} = 0 \Leftrightarrow \det_{min} \dot{\leq} RSB^0 \tag{3.15}$$

Soient les $\beta_i$ tels que $l_i = RSB^{-\beta_i}$. En utilisant le fait que $Tr(\Delta X \Delta X^H) = \|\Delta X\|_F^2 \dot{\leq} q \doteq RSB^{\frac{r}{n}}$, et l'équation 3.15 on a :

$$-\sum_{i=n-j}^{n} \beta_i \geq -\frac{r}{n}(n-j-1) \tag{3.16}$$

Soient $\alpha_i$ tels que $\lambda_i = RSB^{-\alpha_i}$. L'ordonnancement des $\lambda_i$ donne $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.

En appliquant l'inégalité moyenne arithmétique-moyenne géométrique, aux $n$ inégalités définies dans 3.14, on obtient pour $j = 0, \cdots n-1$ :

$$d_E^2 \doteq RSB^{1-\frac{r}{n}} \cdot RSB^{\left(-\frac{1}{j+1}\sum_{i=n-j}^{n}\alpha_i\right)} \cdot RSB^{\left(-\frac{1}{j+1}\sum_{i=n-j}^{n}\alpha_i\right)}$$

Soit $\alpha = (\alpha_i, \cdots, \alpha_n)$. En utilisant 3.16, on dérive une borne inférieure exponentielle de la distance euclidienne :

$$d_E^2(\alpha) \dot{\geq} RSB^{\delta_j(\alpha)},\ j = 0, \cdots n-1$$

où

$$\delta_j(\alpha) = 1 - \frac{r}{j+1} - \sum_{i=n-j}^{n} \frac{\alpha_i}{j+1}$$

Afin de définir le gain de diversité, on se sert de la distance euclidienne minimale pour calculer une borne de la probabilité d'erreurs pour $H$ fixé, puis on moyenne par rapport à $H$. Il a été montré dans [29] que :

$$d(r) \geq \inf_{\alpha \in \mathcal{B}} \sum_{i=1}^{n} (2i - 1 + n_r - n_t)\alpha_i$$

où l'ensemble $\mathcal{B}$ est défini comme suit :

$$\mathcal{B} = \left\{\alpha : \alpha_i \geq 0 \forall i, \delta_j \leq 0, j = 0, \cdots n-1\right\}$$

Il en découle que pour un rendement $r$ entier donné, le gain de diversité vérifie :

$$d(r) = (n_r - r)(n_t - r)$$

Ce gain de diversité correspond à la borne supérieure optimale de la DMG donnée dans [28]. Donc on peut conclure que le code ST atteint le compromis DMG.

Les codes quaternioniques ont été les premiers codes trouvés qui atteignent le compromis D-MG. Ceci n'est pas suffisant pour garantir des performances optimales du code. Nous avons vu que les performances des codes quaternioniques en dimension 3 et 4 sont moins bonnes que celles des codes présentés dans [20].

Les codes parfaits atteignent le compromis DMG, mais ont en plus une efficacité énergétique qui leur permet d'avoir des performances optimales.

## 3.6 Codes parfaits rectangulaires

Nous nous sommes intéressés jusqu'à présent à des constructions de codes ST ayant une longueur temporelle égale au nombre d'antennes à l'émission, $T = n_t$. En considérant comme canal de transmission le canal de Rayleigh quasi-statique, nous supposons que le canal de transmission est constant durant $T$ temps symbole.

En pratique, le choix du code ST se fait en fonction des paramètres du système de transmission : le nombre d'antennes à l'émission et le temps $T_C$ sur lequel le canal de transmission reste invariant. Deux cas de figure sont possibles, illustrés dans la figure 3.12. Si on dispose d'un nombre d'antennes à l'émission $n_t = T_C$, on peut alors choisir d'utiliser un code ST carré de dimension $T_C \times T_C$. Si le nombre d'antennes à l'émission est strictement inférieur à $T_C$, dans ce cas, on peut utiliser soit un code ST carré de dimension $n_t \times n_t$, soit un code ST de dimension $n_t \times T_C$, qu'on qualifie de code ST rectangulaire.

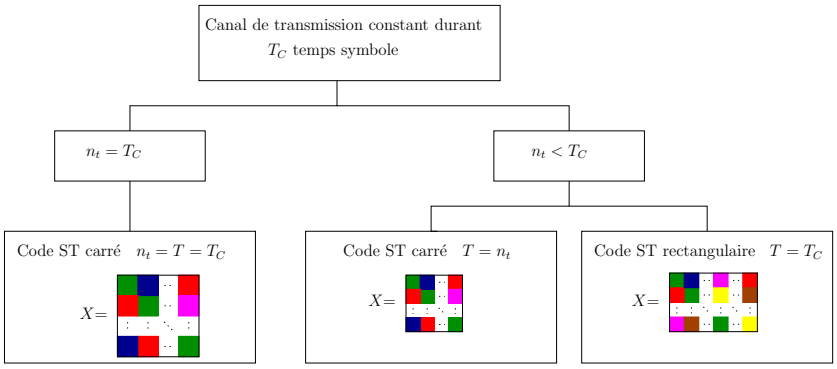



Fig. 3.12: Choix du code ST en fonction des paramètres du système de transmission

Dans le deuxième cas ($n_t < T_C$), l'utilisation des codes rectangulaires s'avère plus attractive. En effet, elle permet de réduire le nombre de mots de code à générer et à transmettre allégeant ainsi les traitements à la réception (synchronisation, amplification, estimation du canal et décodage, etc.). Vu les avantages qu'on peut tirer de ces codes, nous nous sommes proposés de construire des codes ST rectangulaires.

Les codes parfaits sont les meilleurs codes carrés. Ils ont un rendement plein une diversité pleine, des déterminants minimaux ne s'évanouissant pas et une bonne efficacité énergétique. Pour définir la construction des codes rectangulaires, l'idée serait de se baser sur celle des codes carrés parfaits . Nous appelons les nouveaux codes rectangulaires construits "codes parfaits rectangulaires". En construisant des codes parfaits carrés et rectangulaires nous offrons plus de souplesse pour le choix du code ST.

Les codes rectangulaires existants dans la littérature sont les codes ST par couches : VBLAST [13], DBLAST [14] et WST [15], ainsi que les codes TAST asymétriques [20]. Ces codes ont été présentés au chapitre II.

### 3.6.1 Construction des codes parfaits rectangulaires

La construction des codes rectangulaires se base entièrement sur celle des codes parfaits carrés. L'idée est d'exploiter la structure en couches des codes parfaits (fig. 2.7) pour construire des codes parfaits asymétriques, en d'autres termes, pour avoir un nombre de couches supérieur au nombre d'antennes émettrices. C'est le principe des codes TAST asymétriques. Dans la figure 3.12, nous présentons les structures en couches symétriques et asymétriques correspondantes respectivement aux codes carrés et aux codes rectangulaires.

Pour un nombre d'antennes $n_t$ donné, nous considérons les paramètres du code parfait carré $n_t \times n_t$, à savoir, corps de base, corps de décomposition, idéal considéré et $\gamma$ considéré.

Afin d'avoir un rendement plein, il faut transmettre $n_t \cdot T$ symboles d'information. Cela revient à transmettre par chaque antenne, à chaque instant, $n_t$ symboles d'information. En respectant la structure circulaire des lignes de la matrice mot de code (qui permet d'avoir la structure en couches), le mot de code du code parfait rectangulaire s'écrit alors :

$$X = \begin{bmatrix} x_1 & x_2 & \dots & x_{n_t} & \dots & x_T \\ \gamma x_T & x_1 & \cdots & x_{n_t-1} & \dots & x_{T-1} \\ \vdots & \vdots & \ddots & \vdots & & \vdots \\ \gamma x_{T-(n_t-2)} & \gamma x_{T-(n_t-3)} & \dots & x_1 & \dots & x_{T-(n_t-1)} \end{bmatrix}$$

où les $x_i$, $i = 1 \cdots T$ s'écrivent en fonction des symboles d'information comme suit :

$$x_i = \sum_{i=1}^{n_t} s_{1,i} v_i$$

$(v_k)_{k=1\dots n_t}$ est la base de l'idéal considéré. Les symboles d'information sont pris dans des constellations $q$-QAM pour $n_t = 2, 4$ et dans une constellation $q$-HEX pour $n_t = 3, 6$. Le code parfait rectangulaire pour $T = n_t$ n'est autre que le code parfait $n_t \times n_t$.

Le code parfait rectangulaire hérite des propriétés du code parfait carré. Il a alors un rendement plein $n_t$ symboles/u.c. , une diversité maximale $n_t.n_r$ et une bonne efficacité énergétique et offre un gain de codage plus élevé.

### 3.6.2 Codes parfaits rectangulaires $n_t = 2$ et $T > 2$

En utilisant les paramètres du Golden code, nous définissons le code parfait rectangulaire pour $n_t = 2$ et $T > 2$. Le mot de code s'écrit :

$$X = \begin{bmatrix} \alpha(s_1 + \theta s_2) & \alpha(s_3 + \theta s_4) & \dots & \alpha(s_{2T-1} + \theta s_{2T}) \\ \gamma\bar{\alpha}(s_{2T-1} + \bar{\theta} s_{2T}) & \bar{\alpha}(s_1 + \bar{\theta} s_2) & \dots & \bar{\alpha}(s_{2T-3} + \bar{\theta} s_{2T-2}) \end{bmatrix}$$

Les $s_l$, $l = 1 \cdots 2T$, représentent les $2T$ symboles d'information pris dans $\mathbb{Z}[i]$ pour le code infini et dans une constellation $q$-QAM pour le code fini. Rappelons que $\theta = \frac{1+\sqrt{5}}{2}$ , $\alpha = 1+i-i\theta$ et $\gamma = i$.

Afin d'étudier les performances des nouveaux codes rectangulaires construits, nous avons simulé la chaîne de transmission complète présentée dans la figure 3.5 en utilisant les codes rectangulaires.

Dans la figure 3.13, nous avons tracé le taux d'erreurs par symbole en fonction du Rapport signal sur bruit (RSB = $\frac{E_b}{N_0}$) pour le Golden code (GC) et les codes parfaits rectangulaires, en utilisant la constellation 4-QAM, pour $n_t = n_r = 2$ et $T = 3,4,5,6$ (CPR $n_t \times T$). Les codes rectangulaires ont le même ordre de diversité 4 que le Golden Code. A fort RSB, les codes CPR $2 \times 4$ et CPR $2 \times 6$ ont de meilleures performances que le code CPR $2 \times 3$, ce qui traduit le gain de codage apporté par ces codes.

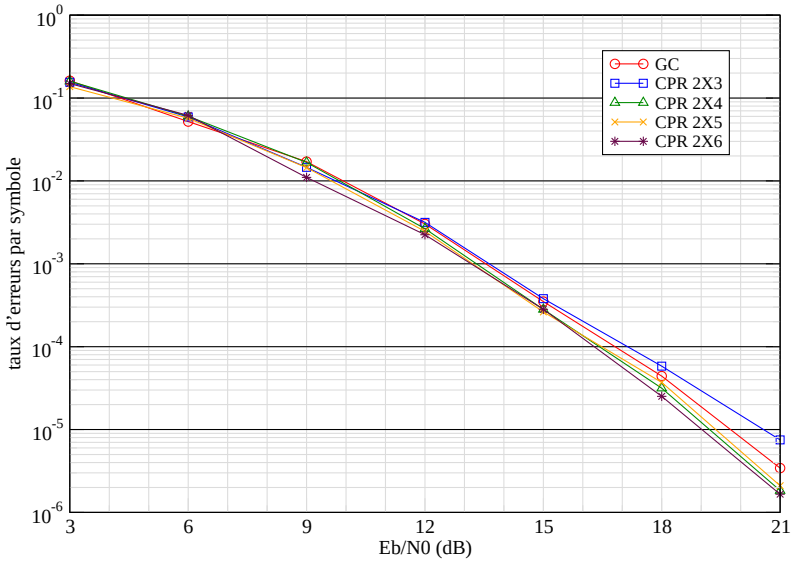



FIG. 3.13: Comparaison des performances des codes rectangulaires avec $n_t = n_r = 2$ et $T > 2$, pour une constellation 4-QAM

### 3.6.3 Codes parfaits rectangulaires $n_t = 3$ et $T > n_t$

En utilisant les paramètres du code parfait 3, nous définissons le code parfait rectangulaire pour $n_t = 3$ et $T > 3$. Le mot de code s'écrit :

$$X = \begin{bmatrix} \alpha(s_1 + \theta s_2 + \theta^2 s_3) & \alpha(s_4 + \theta s_5 + \theta^2 s_6) & \dots & \alpha(s_{2T-2} + \theta s_{2T-1} + \theta^2 s_{2T}) \\ \gamma\sigma(\alpha(s_{2T-2} + \theta s_{2T-1} + \theta^2 s_{2T})) & \sigma(\alpha(s_1 + \theta s_2 + \theta^2 s_3)) & \dots & \sigma(\alpha(s_{2T-5} + \theta s_{2T-4} + \theta^2 s_{2T-3})) \\ \gamma\sigma^2(\alpha(s_{2T-5} + \theta s_{2T-4} + \theta^2 s_{2T-3})) & \gamma\sigma^2(\alpha(s_{2T-2} + \theta s_{2T-1} + \theta^2 s_{2T})) & \dots & \sigma^2(\alpha(s_{2T-8} + \theta s_{2T-7} + \theta^2 s_{2T-6})) \end{bmatrix}$$

où les $s_l$, $l = 1 \cdots 3T$ représentent les $3T$ symboles d'information pris dans $\mathbb{Z}[j]$ pour le code infini et dans une constellation $q$-HEX pour le code fini. Rappelons que $\theta = \zeta_7 + \zeta_7^{-1} = 2cos(\frac{2\pi}{7})$, $\alpha = (1 + j) + \theta$ et $\gamma = j$.

Dans la figure 3.14, nous avons tracé le taux d'erreurs par symbole en fonction du RSB pour le code parfait $3 \times 3$ (CP $3 \times 3$) et les codes rectangulaires pour $n_t = n_r = 3$ et $T = 4,5$ (CPR $n_t \times T$), en utilisant la constellation 4-HEX. Les codes rectangulaires ont le même ordre de diversité que le code carré, à savoir 9. Le CP $3 \times 3$, le CPR $3 \times 4$ et le CPR $3 \times 5$ ont pratiquement les mêmes performances. Cependant, à fort RSB, les codes rectangulaires prennent une petite avance sur le code carré, ce qui représente le gain de codage apporté par ces codes.

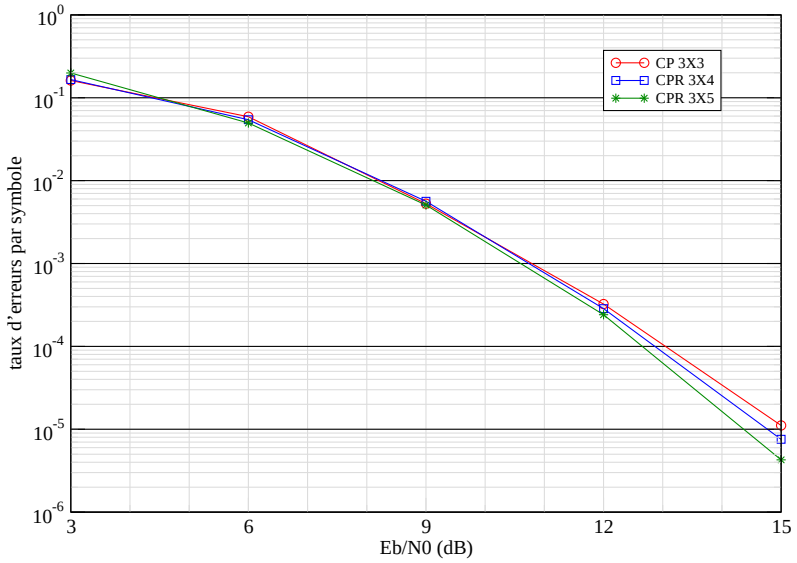



Fig. 3.14: Comparaison des performances des codes rectangulaires avec $n_t = n_r = 3$ et $T > 3$, pour une constellation 4-HEX

## Conclusion

Nous avons présenté dans ce chapitre de nouvelles constructions algébriques de codes ST carrés et rectangulaires. Nous nous sommes basés essentiellement sur les algèbres cycliques de division construites sur les corps de nombres.

Dans un premier temps nous avons construit les codes quaternioniques, qui offrent un rendement plein, une diversité maximale et des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Cependant, la répartition non uniforme de l'énergie dans le mot de code pénalise fortement les performances de ces codes.

Dans un deuxième temps, nous avons construit les codes parfaits préservant toutes les propriétés des codes quaternioniques mais palliant au problème énergétique. Les codes parfaits ont une bonne efficacité énergétique qui se traduit par une répartition uniforme de l'énergie dans le mot de code et des constellations transmises ne présentant aucune perte de forme par rapport à celles émises. Notons que ces codes se distinguent par les meilleures des propriétés relatives aux codes ST jamais réunies par un même code jusqu'à présent. Nous avons montré aussi en s'appuyant sur les récents résultats dans [29] que les codes quaternioniques et les codes parfaits atteignent le compromis gain de multiplexage-diversité.

Pour offrir plus de souplesse dans le choix de code relatif à un système de transmission donné, nous avons construit des codes parfaits rectangulaires inspirés des codes parfaits carrés. Ces nouveaux codes héritent des propriétés des codes carrés et offrent des gain de codage plus élevés.

# Chapitre 4

# Décodage ML des codes Espace-Temps en blocs

## Introduction

Nous avons explicité dans le deuxième chapitre les principales constructions existantes dans la littérature des codes ST en blocs et nous avons construit dans le troisième deux nouvelles familles de code ST, à savoir, les codes quaternioniques et les codes parfaits. Nous avons vu que ces codes disposent de propriétés avantageuses par rapport aux codes existants, résultats confirmés par des simulations comparatives de leurs performances avec celles des meilleurs codes ST en blocs. La comparaison a été effectuée sur la base d'une chaîne de transmission complète entre un émetteur et un récepteur employant chacun des codes ST, ainsi qu'un décodeur choisi en circonstance. C'est au choix de ce décodeur que nous allons nous intéresser dans ce chapitre.

Les codes quaternioniques comme les codes parfaits peuvent avoir une représentation en réseau de points, ce qui permet leur décodage par les décodeurs de réseaux de points. Le décodage ML exhaustif a une complexité qui augmente exponentiellement avec la dimension du réseau, ce qui rend impossible son utilisation. Par ailleurs, il existe des décodeurs de réseaux de points ML ayant une complexité polynomiale, à savoir le "décodeur par sphères" (Sphere Decoder - SD) et l'algorithme de Schnorr-Euchner (SE). Ces derniers ont été utilisés dans la littérature pour décoder des réseaux de points infinis. Ainsi, pour pouvoir décoder des sous-parties finies de réseaux, nous serons amenés à leurs apporter quelques modifications nécessaires.

L'étude et la comparaison des complexités associées à chacun des décodeurs nous permettra de choisir le décodeur le mieux adapté à notre système.

Nous commencerons ce chapitre par la représentation en réseau de points des systèmes MIMO codés et non-codés. Nous détaillerons ensuite le principe de recherche du point le plus proche dans les réseaux de points, notion fondamentale du fonctionnement des décodeurs SD et SE, et nous exposerons en conséquence les principaux travaux réalisés sur ce sujet. La troisième et quatrième parties seront respectivement dédiées aux décodeurs SD et SE : stratégie de recherche et modifications effectuées. Nous clôturons le chapitre par l'étude et la comparaison des complexités des deux algorithmes modifiés.

## 4.1 Représentation en réseau de points des codes ST

Comme nous l'avons déjà vu au chapitre I (paragraphe 1.2), un réseau de points $\Lambda$ est un sous-ensemble discret de $\mathbb{R}^n$ de dimension $n$, entièrement défini par sa matrice génératrice $\mathbf{M}$. Tout point $\mathbf{x}$ de $\Lambda$ s'écrit $\mathbf{x} = \mathbf{zM}$, où $\mathbf{z}$ est un vecteur de $\mathbb{Z}^n$.

La représentation en réseau de points des systèmes MIMO et leur décodage par un décodeur de réseaux de points ont été effectués pour la première fois par Damen *et al.* dans [47].

En séparant les parties réelles et imaginaires et en vectorisant les systèmes MIMO codés et non-codés, nous obtenons leurs représentations en réseau de points. Nous détaillerons dans la suite ces opérations.

### 4.1.1 Système non-codé

Nous considérons un système MIMO avec $n = n_t = n_r$. Le signal reçu s'écrit, en fonction du vecteur de symboles d'information $\mathbf{x}$, de la matrice de transfert du canal $\mathbf{H}$, et du bruit Gaussien, comme suit :

$$\mathbf{y}_n = \mathbf{H}_{n\times n}\mathbf{x}_n + \mathbf{w}_n \tag{4.1}$$

La séparation des parties réelles et des parties imaginaires des vecteurs et de la matrice de l'équation (4.1) et sa transposition donnent :

$$\begin{aligned}
\mathbf{y}_\mathbb{R} &= [\Re(\mathbf{y}^T),\Im(\mathbf{y}^T)] \\
&= [\Re(\mathbf{x}^T),\Im(\mathbf{x}^T)] \cdot \begin{bmatrix} \Re(\mathbf{H}^T) & -\Im(\mathbf{H}^T) \\ \Im(\mathbf{H}^T) & \Re(\mathbf{H}^T) \end{bmatrix} + [\Re(\mathbf{w}^T),\Im(\mathbf{w}^T)] \\
&= \mathbf{x}_\mathbb{R} \cdot \mathbf{H}_\mathbb{R} + \mathbf{w}_\mathbb{R}
\end{aligned}$$

Étant donné que les évanouissements entre toutes les antennes émettrices et les antennes réceptrices (les coefficients de la matrice $\mathbf{H}$) sont indépendants, la probabilité d'avoir deux colonnes de $\mathbf{H}$ dépendantes est nulle. La matrice est donc de rang plein. De même la matrice $\mathbf{H}_\mathbb{R}$ est de rang plein, égal à $2n$.

Nous obtenons ainsi la représentation en réseau de points du système MIMO non-codé. La dimension du réseau de points équivalent est $2n$ et sa matrice génératrice est $\mathbf{H}_\mathbb{R}$.

### 4.1.2 Système codé

Rappelons tout d'abord l'équation représentant le système MIMO codé. En définissant $\mathbf{X}$ le mot de code à transmettre, $\mathbf{H}$ la matrice de transfert du canal et $\mathbf{W}$ le bruit Gaussien. Le mot de code reçu $\mathbf{Y}$ s'écrit :

$$\mathbf{Y}_{n\times T} = \mathbf{H}_{n\times n} \cdot \mathbf{X}_{n\times T} + \mathbf{W}_{n\times T} \tag{4.2}$$

où $T$ est la longueur temporelle du code.

Nous distinguons le cas des codes ST dont le corps de base est $\mathbb{Z}[i]$ et celui dont le corps de base est $\mathbb{Z}[j]$.

#### 4.1.2.1 Codes ST définis sur $\mathbb{Z}[i]$

L'obtention de la représentation en réseau de points des codes ST définis sur $\mathbb{Z}[i]$ se fait en 2 étapes : 1) représenter le code sous la forme d'un système non codé 2) séparer les parties réelles et imaginaires.

Par souci de simplicité et de clarté, nous allons nous baser sur l'exemple du "Golden Code" pour illustrer la représentation en réseau de points des systèmes codés sur $\mathbb{Z}[i]$.
Soit $n = T = 2$. Le mot de code $\mathbf{X}$ s'écrit :

$$\mathbf{X} = \frac{1}{\sqrt{5}} \cdot \begin{bmatrix} \alpha(s_1 + \theta s_2) & \alpha(s_3 + \theta s_4) \\ i\bar{\alpha}(s_3 + \bar{\theta} s_4) & \bar{\alpha}(s_1 + \bar{\theta} s_2) \end{bmatrix}$$

avec $\theta = \frac{1+\sqrt{5}}{2}$, $\bar{\theta} = \frac{1-\sqrt{5}}{2}$, $\alpha = 1 + i - i\theta$, $\overline{\alpha} = 1 + i - i\overline{\theta}$ et $s_l$, $l = 1 \ldots 4$ les symboles d'information appartenant à une constellation $q$-QAM et donc à $\mathbb{Z}[i]$.

– Représentation sous la forme de système non codé
La première étape consiste à vectoriser la matrice mot de code. L'équation (4.2) devient :

$$\begin{aligned} \mathbf{y}_{n \cdot T} &= \frac{1}{\sqrt{5}} \cdot \begin{bmatrix} \mathbf{H} & 0 \\ 0 & \mathbf{H} \end{bmatrix} \cdot \begin{bmatrix} \alpha & \alpha\theta & 0 & 0 \\ 0 & 0 & i\bar{\alpha} & i\bar{\alpha}\bar{\theta} \\ 0 & 0 & \alpha & \alpha\theta \\ \bar{\alpha} & \bar{\alpha}\bar{\theta} & 0 & 0 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} + \mathbf{w} \\ &= \frac{1}{\sqrt{5}} \cdot \mathbf{H}_{n \cdot T} \cdot \mathbf{\Phi}_{n \cdot T} \cdot \mathbf{s}_{n \cdot T} + \mathbf{w}_{n \cdot T} \end{aligned} \tag{4.3}$$

Posons $\mathbf{M_1} = \frac{1}{\sqrt{5}} \cdot \mathbf{H}_{n \cdot T} \cdot \mathbf{\Phi}_{n \cdot T}$, en réécrivant encore une fois l'équation (4.2).

$$\mathbf{y} = \mathbf{M_1} \cdot \mathbf{s} + \mathbf{w} \tag{4.4}$$

Nous obtenons ainsi la représentation en système non-codé.

– Représentation en réseau de points
En appliquant la méthode des systèmes non codés à l'équation (4.4), nous obtenons la représentation en réseau de points du système MIMO codé.
Pour l'implémentation réelle, il serait plus intéressant de séparer les parties réelles et imaginaires des matrices $\mathbf{H}_{n \cdot T}$ et $\mathbf{\Phi}_{n \cdot T}$. L'équation (4.6), s'écrit alors :

$$\mathbf{y}_{\mathbb{R}} = \frac{1}{\sqrt{5}} \cdot \begin{bmatrix} \Re(\mathbf{H}) & 0 & -\Im(\mathbf{H}) & 0 \\ 0 & \Re(\mathbf{H}) & 0 & -\Im(\mathbf{H}) \\ \Im(\mathbf{H}) & 0 & \Re(\mathbf{H}) & 0 \\ 0 & \Im(\mathbf{H}) & 0 & \Re(\mathbf{H}) \end{bmatrix} \cdot \begin{bmatrix} \Re(\mathbf{\Phi}) & -\Im(\mathbf{\Phi}) \\ \Im(\mathbf{\Phi}) & \Re(\mathbf{\Phi}) \end{bmatrix} \begin{bmatrix} \Re(\mathbf{s}) \\ \Im(\mathbf{s}) \end{bmatrix} + \begin{bmatrix} \Re(\mathbf{w}) \\ \Im(\mathbf{w}) \end{bmatrix} \tag{4.5}$$

$$= \frac{1}{\sqrt{5}} \cdot \mathbf{H}_{\mathbb{R}} \cdot \mathbf{\Phi}_{\mathbb{R}} \cdot \mathbf{s}_{\mathbb{R}} + \mathbf{w}_{\mathbb{R}} \tag{4.6}$$

En posant $\mathbf{M} = \frac{1}{\sqrt{5}} \cdot \mathbf{H}_{\mathbb{R}} \cdot \mathbf{\Phi}_{\mathbb{R}}$, et en transposant l'équation (4.6), on obtient :

$$\mathbf{y}_{\mathbb{R}}{}^T = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{M}^T + \mathbf{w}_{\mathbb{R}}{}^T$$

Le réseau de points équivalent a donc pour matrice génératrice $\mathbf{M}$, de dimension égale à 8. Dans le cas général, la dimension du réseau de points équivalent est égale à $2 \cdot n \cdot T$.

#### 4.1.2.2 Codes ST définis sur $\mathbb{Z}[j]$

Traitons maintenant le cas des codes ST de corps de base $\mathbb{Z}[j]$ dont les symboles d'information sont pris dans les constellations hexagonales $q$-HEX. Nous suivrons les mêmes étapes que celles des codes définis sur $\mathbb{Z}[i]$.

– Vectorisation

Comme dans le paragraphe précédent, cette étape consiste à vectoriser le mot de code, et à sortir le vecteur des symboles.

– Séparation des parties en $j$

Étant donné que les éléments de la matrice $\mathbf{\Phi}$ et les symboles d'information sont dans $\mathbb{Z}[j]$, nous allons, commencer par séparer les parties en $j$ et celles qui ne le sont pas. Ensuite, en passant par la base $B$ de $\mathbb{Z}[j]$ dans $\mathbb{Z}[i]$, nous séparons les parties réelles et imaginaires.

$$B = \begin{bmatrix} 1 & -0.5 \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}$$

Après ces deux opérations l'équation 4.2 s'écrit alors dans $\mathbb{Z}$ sous la forme suivante :

$$\begin{aligned} \mathbf{y}_{\mathbb{R}} &= \begin{bmatrix} \mathcal{R}(\mathbf{H}) & \cdots & 0 & -\mathcal{J}(\mathbf{H}) & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{R}(\mathbf{H}) & 0 & \cdots & -\mathcal{J}(\mathbf{H}) \\ \mathcal{J}(\mathbf{H}) & \cdots & 0 & \mathcal{R}(\mathbf{H}) & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \mathcal{J}(\mathbf{H}) & 0 & \cdots & \mathcal{R}(\mathbf{H}) \end{bmatrix} \cdot \begin{bmatrix} 1 & \cdots & 0 & -0.5 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & -0.5 \\ 0 & \cdots & 0 & \frac{\sqrt{3}}{2} & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \frac{\sqrt{3}}{2} \end{bmatrix} \\ &\cdot \begin{bmatrix} R(\mathbf{\Phi}) & -\mathcal{J}(\mathbf{\Phi}) \\ \mathcal{J}(\mathbf{\Phi}) & R(\mathbf{\Phi}) - \mathcal{J}(\mathbf{\Phi}) \end{bmatrix} \begin{bmatrix} R(\mathbf{s}) \\ \mathcal{J}(\mathbf{s}) \end{bmatrix} + \begin{bmatrix} \Re(\mathbf{w}) \\ \Im(\mathbf{w}) \end{bmatrix} \\ &= \mathbf{H}_{\mathbb{R}} \cdot \mathbf{B_1} \cdot \mathbf{\Phi}_{\mathbb{R}} \cdot \mathbf{s}_{\mathbb{R}} + \mathbf{w}_{\mathbb{R}} \end{aligned} \tag{4.7}$$

En posant $\mathbf{M} = \mathbf{H}_{\mathbb{R}} \cdot \mathbf{B_1} \cdot \mathbf{\Phi}_{\mathbb{R}}$, et en transposant l'équation (4.7), on obtient

$$\mathbf{y}_{\mathbb{R}}{}^T = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{M}^T + \mathbf{w}_{\mathbb{R}}{}^T \tag{4.8}$$

D'où la représentation en réseau de points du système MIMO codé.

## 4.2 Algorithmes de décodage des réseaux de points

La théorie des réseaux de points est utilisée dans plusieurs domaines. On peut citer, par exemple, le codage et la cryptographie. Un grand intérêt a été accordé au développement de méthodes de décodage adéquates aux différentes applications, satisfaisant un bon compromis performances-complexité.

Pour les systèmes MIMO, comme nous pouvons le voir dans l'équation 4.8, le vecteur reçu est un point du réseau de points dont la matrice génératrice est $\mathbf{M}^T$ bruité par le bruit Gaussien. Le décodage ML consisterait alors à chercher le point le plus proche du point reçu appartenant au réseau.

**Définition : 4.1** *Point le plus proche (Closest Point)*

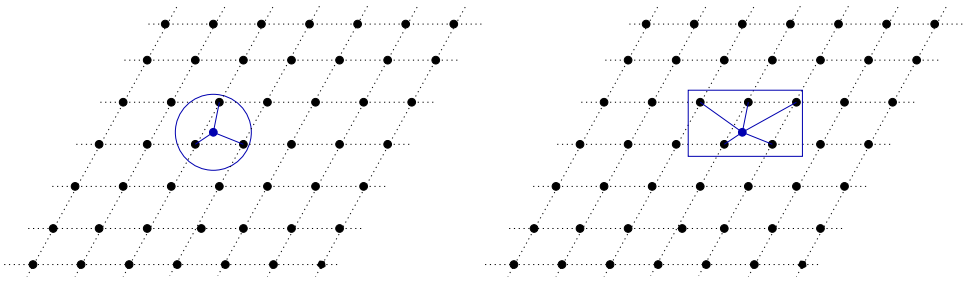
*Soit un réseau de points $\Lambda$, de dimension $n$, et soit le vecteur reçu $\mathbf{x} \in \mathbb{R}^n$. Le point le plus proche du vecteur $\mathbf{x}$ dans le réseau de points $\Lambda$ est le vecteur $\widehat{\mathbf{u}} \in \Lambda$ tel que*

$$\left\|\mathbf{x} - \widehat{\mathbf{u}}\right\| \leq \|\mathbf{x} - \mathbf{u}\| \quad , \textit{pour tout } \mathbf{u} \in \Lambda$$

Intuitivement, on peut affirmer que la recherche du point le plus proche est plus facile et plus rapide pour les réseaux de points ayant des structures particulières. Des méthodes de recherche ont été présentées dans [48] pour la plupart des réseaux de points classiques. Il reste donc à trouver une méthode générale pour décoder un réseau de points quelconque connaissant sa matrice génératrice. Dans ce cas, la méthode de décodage doit être indépendante de toute structure possible du réseau de points.

Une approche commune a été utilisée dans ce sens. Cette approche consiste à définir une région de $\mathbb{R}^n$ incluant le point le plus proche et à parcourir tous les points du réseau contenus dans cette région. Éventuellement, une réduction de la région de recherche peut se faire de manière dynamique [49] au cours de la recherche.

Il existe deux principales branches relatives à la recherche du point le plus proche dans la littérature. La première est celle proposée par Pohst dans [50], considérant comme région de recherche une hypersphère. La deuxième est proposée par Kannan dans [51], considérant comme région de recherche un parallépipéde rectangle. Dans la figure 4.1, nous illustrons les deux régions de recherche dans un plan. Dans la littérature, la méthode de Kannan apparaît comme une méthode théorique, alors que celle de Pohst comme une méthode pratique, et on trouve des implémentations de cet algorithme. Cela s'explique par le fait que le nombre de points considéré dans une hypersphère est inférieur à celui considéré dans un hypercube contenant l'hypersphère, surtout pour les dimensions élevées.



(a) stratégie de Pohst (b) stratégie de Kannan

Fig. 4.1: Représentation géométrique des méthodes de décodage de Pohst et de Kannan

Deux stratégies de recherche ont été développées pour la méthode de Pohst correspondants respectivement aux deux décodeurs connus, à savoir, le décodeur par sphères (Sphere Decoder - SD) et le décodeur de Schnorr-Euchner (SE).

Concernant le SD, l'analyse mathématique a été présentée par Fincke et Pohst dans [52], l'interprétation géométrique par Viterbo et Biglieri dans [53] et l'implémentation pratique pour un canal à évanouissements par Viterbo et Boutros dans [54]. Le principe du SD est de chercher le point le plus proche dans une sphère de rayon donné, centrée sur le point reçu. Si aucun point n'a été trouvé, le rayon de la sphère est agrandi et la recherche est recommencée. Le parcours des points se fait de la surface de la sphère vers l'intérieur.

L'algorithme SE a été présenté par Agrell *et al.* dans [49]. Son principe est d'effectuer des projections successives sur les hyperplans du réseau de points afin de trouver le point le plus proche. Ainsi le parcours des points dans la sphère se fait du centre vers l'extérieur.

Les travaux cités jusqu'à présent s'intéressent au décodage de réseaux de points infinis. Notre intérêt porte plutôt sur le décodage de sous-parties finies de réseau en utilisant les décodeurs de réseaux de points SD et SE.

Nous considérons comme sous-parties finies de réseau les constellations $(q\text{-QAM})^n$ et $(q - \text{HEX})^n$. Nous avons proposé dans [55] des versions modifiées des algorithmes SD et SE tenant compte des bornes des constellations. De récents travaux se sont intéressés au même sujet. Nous citons principalement les travaux de Boutros *et al.* dans [56] et de Damen *et al.* dans [57].

Dans la suite nous détaillons les deux algorithmes et les modifications apportées pour décoder les constellations finies.

## 4.3 Décodage des sous-parties finies de réseau par le décodeur par sphères

### 4.3.1 Principe du décodeur par sphères (SD)

Reprenons l'équation 4.8, qui donne la représentation en réseau de points d'un système MIMO.

$$\mathbf{y}_{\mathbb{R}}{}^T = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{M}^T + \mathbf{w}_{\mathbb{R}}{}^T$$

Considérons le réseau de points $\Lambda$ engendré par la matrice $\mathbf{M}^T$, de dimension $n = 2 \cdot n_t \cdot T$. Soit $\mathbf{x} = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{M}^T \in \mathbb{R}^n$ le point du réseau émis sur le canal Gaussien. Les composantes du vecteur $\mathbf{w}_{\mathbb{R}}{}^T$ sont des variables aléatoires gaussiennes de moyenne nulle et de variance $\sigma^2$. Le décodage consiste à chercher le point le plus proche de $\mathbf{y}$ minimisant la métrique suivante :

$$\min_{\mathbf{x}\in\Lambda} \left\|\mathbf{y}^T - \mathbf{x}\right\| = \min_{\mathbf{z}\in\mathbf{y}-\Lambda} \|\mathbf{z}\|$$

Le problème revient donc à chercher le point le plus proche de $\mathbf{z}$ dans le réseau de points translaté $\mathbf{y} - \Lambda$.

Soient $\mathbf{x}$, $\mathbf{y}$ et $\mathbf{w}$ définis comme suit :

$$\begin{aligned}
\mathbf{x} &= \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{M}^T, \quad \mathbf{u} = \mathbf{s}_{\mathbb{R}}{}^T \in \mathbb{Z}^n \\
\mathbf{y} &= \rho \cdot \mathbf{M}, \quad \rho = (\rho_1, \ldots, \rho_n) \in \mathbb{R}^n \\
\mathbf{w} &= (\rho - \mathbf{u}) \cdot \mathbf{M} = \xi \cdot \mathbf{M}, \quad \xi = (\xi_1, \cdots, \xi_n) \in \mathbb{R}^n
\end{aligned}$$

$\rho$ est le point ZF (Zero Forcing), $\rho = \mathbf{y} \cdot \mathbf{M}^{-1}$. Notons que $\mathbf{w} = \mathbf{y} - \mathbf{x}$, par la suite pour tout $i = 1 \ldots n$, on a $\xi_i = \rho_i - u_i$. Les $\xi_i$ définissent les coordonnées du vecteur $\mathbf{u}$ de $\mathbb{Z}^n$dans le nouveau repère.

Notre objectif est que $\mathbf{w}$ appartienne à une sphère centré sur le point reçu $\mathbf{y}$ de rayon $\sqrt{C}$. Cela se traduit par l'inéquation suivante :

$$\|\mathbf{w}\|^2 = Q(\xi) = \xi \mathbf{M}\mathbf{M}^T \xi^T = \xi \mathbf{G} \xi^T = \sum_{i=1}^{n} \sum_{j=1}^{n} g_{ij} \xi_i \xi_j \leq C \tag{4.9}$$

Dans le nouveau système de coordonnés défini par $\xi$, la sphère de rayon $\sqrt{C}$, centré sur le point reçu, est transformée en un ellipsoïde centré sur l'origine défini par la forme bilinéaire $Q(\xi)$ (fig 4.2).

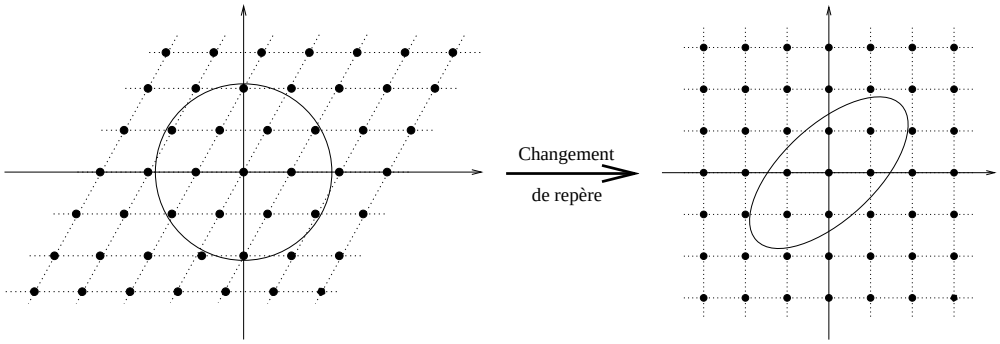



FIG. 4.2: Transformation de la sphère en ellipse dans le nouveau repère

La factorisation de Cholesky de la matrice de Gram $\mathbf{G} = \mathbf{M}\mathbf{M}^T$, donne $\mathbf{G} = \mathbf{R}^T\mathbf{R}$, où $\mathbf{R} = (r_{ij})_{i,j=1\ldots n}$ est une matrice triangulaire supérieure. Réécrivant l'équation (4.9)

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

En posant

$$\begin{aligned} q_{ii} &= r_{ii}^2, i = 1,\ldots,n \\ q_{ij} &= \frac{r_{ij}}{r_{ii}}, i = 1,\ldots,n,\ j = i+1,\ldots,n \end{aligned}$$

On obtient

$$Q(\xi) = \sum_{i=1}^{n} q_{ii}\left(\xi_i + \sum_{j=i+1}^{n} q_{ij}\xi_j\right)^2 \leq C \tag{4.10}$$

Afin de déterminer les limites de l'ellipsoïde il sera judicieux de traiter d'abord $\xi_n$, ensuite les $\xi_i$, $i = n-1,\ldots,1$. D'après l'équation (4.10), on a :

$$q_{nn}\xi_n^2 \leq C \tag{4.11}$$

Par définition $\xi_n = \rho_n - u_n$, en remplaçant dans (4.11)

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

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

Traitons maintenant les $\xi_i$, $i = n-1,\ldots,1$.

$$q_{n-1,n-1}(\xi_{n-1} + q_{n,n-1}\xi_n)^2 + q_{nn}\xi_n^2 \leq C$$

On déduit

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

Pour la $i^{\text{ième}}$ composante $u_i$ on a :

$$\begin{aligned} \left\lceil -\sqrt{\frac{1}{q_{ii}}\left(C - \sum_{l=i+1}^{n} q_{ll}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} q_{ij}\xi_j \right\rceil &\leq u_i \\ \left\lfloor \sqrt{\frac{1}{q_{ii}}\left(C - \sum_{l=i+1}^{n} q_{ll}\left(\xi_l + \sum_{j=l+1}^{n} q_{lj}\xi_j\right)^2\right)} + \rho_i + \sum_{j=i+1}^{n} q_{ij}\xi_j \right\rfloor &\geq u_i \end{aligned} \tag{4.12}$$

Les bornes données dans les inégalités (4.12) montrent que le décodeur par sphères utilise un compteur pour chaque $u_i$. Afin de les simplifier (4.12), on définit les variables suivantes :

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

On a

$$b_{\text{inf}} = \left\lceil -\sqrt{\frac{T_i}{q_{ii}}} + S_i \right\rceil \leq u_i \leq \left\lfloor \sqrt{\frac{T_i}{q_{ii}}} + S_i \right\rfloor = b_{\text{sup}} \tag{4.13}$$

Lorsque un point du réseau de points est trouvé, la distance au carrée qui le sépare du centre (le point reçu) est donnée par :

$$\hat{d}^2 = C - T_1 + q_{11}(S_1 - u_1)^2$$

Le décodeur par sphères calcul pour chaque composante $u_i$ du point $\mathbf{u}$ un intervalle $I_i = [b_{\text{inf},i}, b_{\text{sup},i}]$. Afin de trouver le point le plus proche, l'algorithme parcourt l'intervalle $I_i$ pour chaque composante $u_i$. Pour chaque combinaison de composantes $u_i$ trouvée, la distance $\hat{d}^2$ est évaluée. Chaque point trouvé vérifiant $\hat{d}^2 \leq C$ est stocké. La recherche continue jusqu'à ce que tous les points se trouvant dans la sphère soient parcourus. L'algorithme de recherche implique que le rayon de la sphère ainsi que les bornes $b_{\text{inf},i}$ et $b_{\text{sup},i}$ pour $i = 1 \cdots n$ soient mis à jour dynamiquement au cours de la recherche chaque fois qu'un point est trouvé, i.e. $C = \hat{d}^2$.

Sur un réseau de points en dimension 2, nous illustrons dans la figure (4.3) l'ordre de parcours des points du réseau se trouvant à l'intérieur de la sphère. Nous constatons que les points sont parcourus de haut en bas, et de gauche à droite.

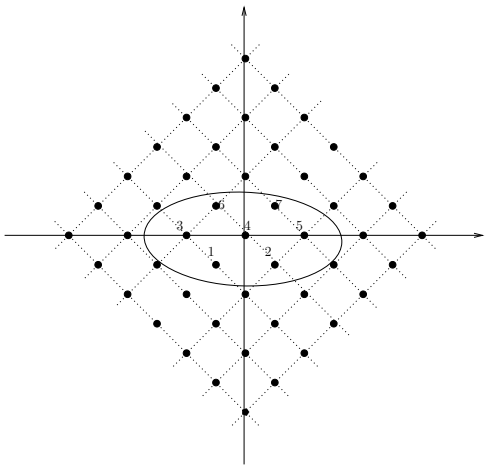



Fig. 4.3: Énumération des points du réseau de points $\mathbb{Z}^2$qui sont dans l'ellipse

### 4.3.2 Choix du rayon de la sphère

A ce stade, nous n'avons pas encore évoqué le choix du rayon initial de la sphère qui est un paramètre critique pour la convergence de l'algorithme. En effet, pour être sûr de trouver un point du réseau à l'intérieur de la sphère, le rayon $\sqrt{C}$ doit être égal au rayon de recouvrement du réseau. Il est possible de le choisir égal à la borne supérieure de Rogers [48], fonction du volume fondamental du réseau de points (définition 1.5).

$$\sqrt{C_1} = \sqrt[n]{(n\log n + n\log\log n + 5n)\frac{\sqrt{\det(\mathbf{M}\mathbf{M}^T)}}{V_n}} \tag{4.14}$$

où $V_n$ est le volume d'une sphère de rayon 1 en dimension $n$.

$$V_n = \begin{cases} \frac{\pi^{n/2}}{(n/2)!} & , n \text{ pair} \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!} & , n \text{ impair} \end{cases}$$

Étant donné que nous manipulons un bruit blanc gaussien, choisir judicieusement un rayon tenant compte du bruit peut accélérer considérablement la recherche du point le plus proche.

Par ailleurs, nous pouvons affirmer intuitivement que, pour les faibles RSB, le point reçu est très affecté par le bruit alors que, pour les forts RSB, le point reçu est très peu affecté par le bruit. Cette constatation nous amène à choisir un grand rayon pour les faibles RSB et un petit rayon pour les forts RSB.

Dans [58], Hassibi et Vikalo ont traité ce point en proposant un rayon fonction de la variance du bruit Gaussien :

$$C = 2 \cdot n \cdot \sigma^2$$

Nous avons vu comment calculer le rayon de la sphère en fonction du bruit Gaussien, il serait intéressant aussi de tenir compte des évanouissements dans le calcul du rayon.

La matrice génératrice $\mathbf{M}$ du réseau de points équivalent représentant le système MIMO est composée de la matrice $\mathbf{H}_{\mathbb{R}}$ et de la matrice $\mathbf{\Phi}_{\mathbb{R}}$. Les éléments de la matrice $\mathbf{H}_{\mathbb{R}}$ sont les évanouissements entre les antennes émettrices et réceptrices. En présence d'un fort évanouissement, le réseau risque d'être plus étiré le long de quelques axes que d'autres. En prenant un grand rayon initial, un grand nombre de points va se trouver à l'intérieur de la sphère.

Dans la figure 4.4, nous illustrons un exemple de réseau de points en dimension 2 dont la densité des points est plus forte sur un axe p que sur l'autre. Il est clair qu'en considérant un grand rayon, le nombre de points à l'intérieur de la sphère est élevé. Par ailleurs, en considérant un petit rayon, très peu de points (voire aucun) se trouveront à l'intérieur de la sphère. Il est donc nécessaire de trouver le bon rayon de la sphère en tenant compte des évanouissements.

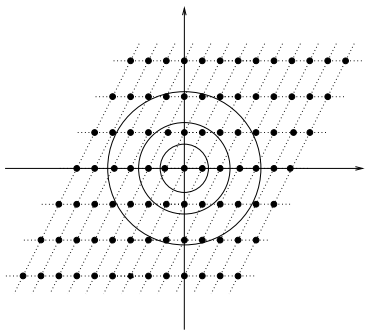


Fig. 4.4: Réseau de points en dimension 2, dont la densité des points est plus forte sur un axe plus que l'autre

L'idée sera donc de prendre le rayon de la sphère égal au minimum de la diagonale de la matrice de Gram de $\mathbf{M}$.

$$C = \min(\text{diag}(\mathbf{M}\mathbf{M}^T))$$

Afin de tenir compte aussi bien du bruit gaussien que des évanouissements, il serait judicieux de prendre comme rayon :

$$C_2 = \min\left(\min(\text{diag}(\mathbf{M}\mathbf{M}^T)), 2 \cdot n \cdot \sigma^2\right) \tag{4.15}$$

Dans la figure 4.5, nous avons tracé le temps de recherche du SD modifié en fonction du RSB = $\frac{E_b}{N_0}$, pour $n_t = 4$ (par la suite $n = 8$), en utilisant une constellation 16-QAM. Nous remarquons qu'à faible et fort RSB, en considérant $C_2$ comme rayon initial de la sphère, le temps de recherche est meilleur. Ce qui montre que le rayon de la sphère est mieux adapté. A moyen RSB, avec un rayon initial $C_1$ ou $C_2$, nous observons des temps de recherche presque identiques.

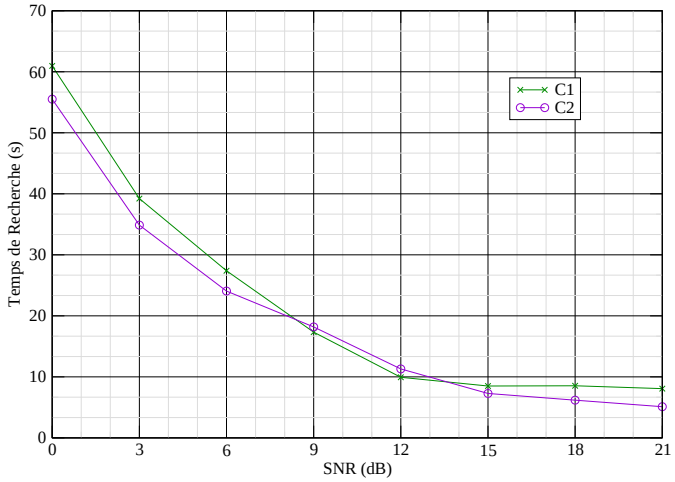



Fig. 4.5: Temps de recherche en secondes du SD modifié, pour $n = 8$, et une constellation 16-QAM

### 4.3.3 Décodage des sous-parties finies de réseaux

Jusqu'à présent, nous avons présenté le SD comme un décodeur de réseaux de points infinis. Or, les symboles d'information du système auquel nous nous intéressons appartiennent à une constellation $q$-QAM ou $q$-HEX. Par la suite le vecteur résultant de la séparation des parties réelles et imaginaires (respectivement des parties en $j$ et des parties pas en $j$) appartient à un sous-ensemble fini de $\mathbb{Z}^n$. Ce qui nous incite alors à modifier le SD pour tenir compte de la constellation.

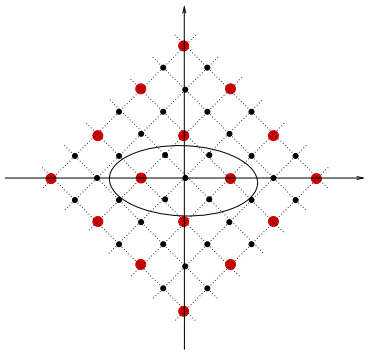


Fig. 4.6: Décodage d'une constellation 16-QAM

La première idée à laquelle nous pouvons penser est de rajouter dans l'algorithme une routine afin de tester chaque fois l'appartenance du point trouvé à la constellation utilisée. Ce qui permet de résoudre le problème, mais qui, malheureusement, entraîne une augmentation de la complexité de l'algorithme.

L'idéal serait donc de décoder la constellation sans augmenter la complexité. L'idée serait de ne parcourir à l'intérieur de la sphère que les points appartenant à la constellation. Pour une

constellation (16-QAM)$^2$, la figure 4.6 illustre les points qu'il faut considérer à l'intérieur de la sphère. Au niveau de l'algorithme, cela se traduit par un calcul des bornes des intervalles $I_i$, $i = 1 \cdots n$, tenant compte des bornes de la constellation.

Soit $I_C = [c_{min}, c_{max}]$, l'intervalle auquel appartiennent les parties réelles et imaginaires (respectivement les parties en $j$ et celles pas en $j$) des symboles de la constellation. Pour une constellation 16-QAM, $I_C = [0,3]$

L'intervalle qu'il faut considérer pour chaque $u_i$ est l'intersection de $I_i$ et de $I_C$.

$$\begin{aligned} I &= I_i \cap I_C \\ &= \left[\sup(b_{inf,i}, c_{min}), \inf(b_{sup,i}, c_{max})\right] \end{aligned}$$

Nous sous-entendons un changement de variable afin de travailler dans un sous-ensemble de $\mathbb{Z}^n$ au lieu de $(2\mathbb{Z})^n$.

Il est à noter que, pour les constellations $q$-HEX (fig. 1.3) et la constellation 8-QAM (fig 1.2), l'ajout d'une routine de test pour ne prendre que les points de la constellation est indispensable.

### 4.3.4 Organigramme du SD modifié

Pour résumer les étapes de l'algorithme SD et illustrer les modifications apportées, nous présentons dans la figure 4.7 l'organigramme du SD modifié. Nous avons conservé les mêmes notations que l'algorithme original présenté dans [54].

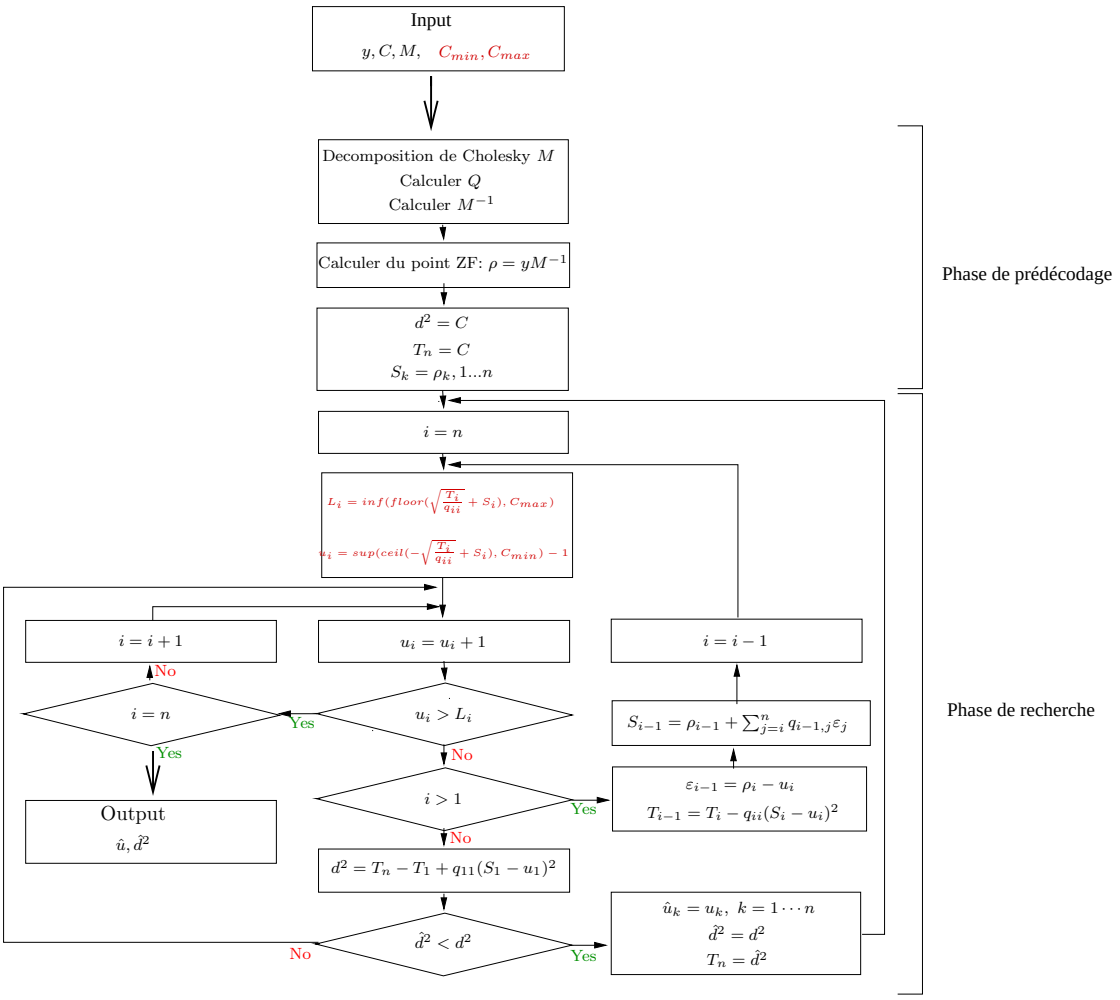



FIG. 4.7: Organigramme du décodeur par sphères modifié

## 4.4 Décodage des sous-parties finies de réseau par le Schnorr-Euchner

### 4.4.1 Principe du Schnorr-Euchner (SE)

La représentation en réseau de points du système MIMO est décrite par l'équation (4.8).

$$\mathbf{y}_{\mathbb{R}}{}^T = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{M}^T + \mathbf{w}_{\mathbb{R}}{}^T$$

L'application de l'algorithme Shnorr-Euchner (SE) pour décoder les réseaux de points nécessite une base triangulaire du réseau. Pour cela, nous allons procéder à une décomposition QR de la matrice génératrice du réseau de points $\mathbf{M}$.

$$\mathbf{M} = \mathbf{Q} \cdot \mathbf{R}$$

où $\mathbf{R}$ est une matrice triangulaire supérieure et $\mathbf{Q}$ est une matrice orthogonale. On a $\mathbf{Q}\mathbf{Q}^T = \mathbf{I}_n$. Réécrivant l'équation (4.8),

$$\mathbf{y}_{\mathbb{R}}{}^T = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{R}^T \cdot \mathbf{Q}^T + \mathbf{w}_{\mathbb{R}}{}^T \tag{4.16}$$

En multipliant les membres de l'égalité par $\mathbf{Q}$, on obtient un réseau de points équivalent (définition 1.4), et l'équation (4.16) devient :

$$\begin{aligned} \mathbf{y}_{\mathbb{R}}{}^T \cdot \mathbf{Q} &= \mathbf{y_1} = \mathbf{s}_{\mathbb{R}}{}^T \cdot \mathbf{R}^T + \mathbf{w}_{\mathbb{R}}{}^T \cdot \mathbf{Q} \\ &= \mathbf{s} \cdot \mathbf{R_1} + \mathbf{w_1} \end{aligned}$$

Cette forme triangulaire de la matrice génératrice du réseau de points permet de voir le réseau comme une superposition de couches. Ces couches vont être la clé de la recherche du point le plus proche $\mathbf{u} = (u_1, u_2, \ldots, u_n)$.

On se propose d'écrire la matrice $\mathbf{R_1}$ sous la forme suivante :

$$\mathbf{R_1} = \begin{bmatrix} \mathbf{R_2} \\ \mathbf{r_n} \end{bmatrix} \tag{4.17}$$

où $\mathbf{R_2}$ est la matrice constituée par les $n-1$ premières lignes de la matrice $\mathbf{R_1}$. On décompose le vecteur $\mathbf{r_n}$ en somme de deux vecteurs $\mathbf{r}_{\|}$ et $\mathbf{r}_{\perp}$, tel que $\mathbf{r}_{\|}$ soit dans l'espace engendré par $\mathbf{R_2}$ et $\mathbf{r}_{\perp}$ dans son espace dual. De cette façon, il est facile de voir que :

$$\begin{aligned} \mathbf{r}_{\|} &= (r_{n,1}, r_{n,2}, \cdots, r_{n,n-1}, 0) \\ \mathbf{r}_{\perp} &= (0, 0, \ldots, 0, r_{n,n}) \end{aligned}$$

En utilisant la décomposition de la matrice $\mathbf{R_1}$ (eq. 4.17), on peut définir le réseau de points sous une forme décomposée [49].

$$\Lambda(\mathbf{R_1}) = \bigcup_{t_n=-\infty}^{+\infty} \left\{ c + t_n \mathbf{r}_{\|} + t_n \mathbf{r}_{\perp}, c \in \Lambda(\mathbf{R_2}) \right\}$$

Ainsi, le réseau de points en dimension $n$ peut se voir comme une réunion infinie de réseaux de points en dimension $n-1$ (qualifiés aussi de couches). $t_n$ indique la couche à laquelle un point du réseau appartient. Comme le vecteur $\mathbf{r}_{\perp}$ soit orthogonal à toutes les couches, nous pouvons déduire que la distance entre deux couches adjacentes est $\|\mathbf{r}_{\perp}\| = |r_{n,n}|$.

Par projection successives sur les hyperplans du réseau de points, un premier point est trouvé. Ce point est le **"Babai point",** il est le point ZF-DFE [57]. Le Babai point est le premier point trouvé par l'algorithme. Il est par la suite le point de départ pour parcourir tous les autres points se trouvant à l'intérieur de la sphère dont le rayon est défini par la distance du Babai point au point reçu. Dans la figure (4.8), nous illustrons la recherche du Babai point dans un réseau de points en dimension 3 par projections successives sur les hyperplans du réseau.

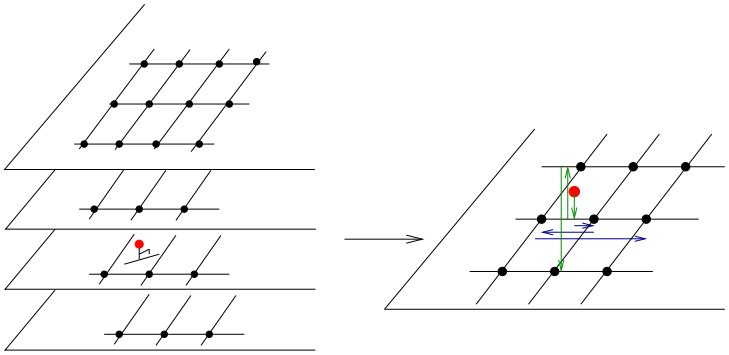


Fig. 4.8: Projections successives sur les hyperplans composants le réseau de points

Trouvons alors le Babai point par le calcul. Soit $\hat{u}_n = \frac{\mathbf{y}\mathbf{r}_\perp}{\|\mathbf{r}_\perp\|^2}$ la projection du vecteur $\mathbf{y}$ sur $\mathbf{r}_\perp$. La distance orthogonale de $\mathbf{y}$ à la couche d'indice $t_n$ est définie comme suit :

$$d_n \triangleq |t_n - \hat{u}_n| \cdot \|\mathbf{r}_\perp\|$$

Soit $u_n = [\hat{u}_n]$ tel que $[x]$ soit l'entier le plus proche de $x$. En considérant le vecteur ZF, $\rho = \mathbf{y} \cdot \mathbf{R_1}^{-1} = (\rho_1, \ldots, \rho_n)$, on a :

$$\begin{aligned} \hat{u}_n &= \rho_n = \frac{y_n}{r_{nn}} \\ d_n &= \left|[\rho_n] - \rho_n\right| \cdot \left|r_{n,n}\right| \end{aligned}$$

Pour calculer $\hat{u}_{n-1}$, il faut considérer le réseau de points en dimension $(n-1)$ engendré par $\mathbf{R_2}$. Ce réseau de points peut être vu comme une réunion infinie de réseaux de points en dimension $(n-2)$. La projection du vecteur $\mathbf{y}$ sur l'espace dual de ces réseaux de points peut se déduire directement de la précédente projection. On a alors :

$$\mathbf{y} = \rho \cdot \mathbf{R_1}$$

On peut donc écrire, pour tout $i = 1 \ldots n$ :

$$y_i = \sum_{j=i}^{n} \rho_j \cdot r_{i,j} = \rho_i \cdot r_{i,i} + \sum_{j=i+1}^{n} \rho_j r_{i,j}$$

En utilisant la décision sur $u_n$, nous déduisons $\rho_{n-1}$ :

$$\rho_{n-1} = \frac{1}{r_{n-1,n-1}}(y_{n-1} - u_n r_{n,n-1})$$

par la suite :

$$\begin{aligned} u_{n-1} &= [\rho_{n-1}] \\ d_{n-1} &= \left|[\rho_{n-1}] - \rho_{n-1}\right| \cdot \left|r_{n-1,n-1}\right| \end{aligned}$$

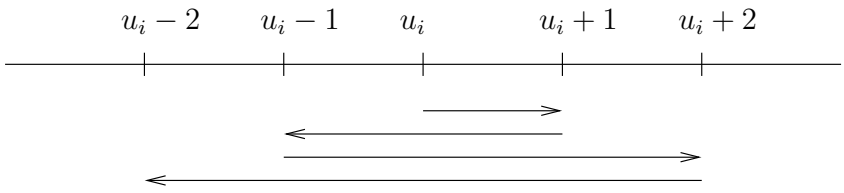
Par substitutions successives, nous pouvons calculer toutes les composantes du Babai point.

$$u_i = [\rho_i] = \left[\frac{1}{r_{i,i}}(y_i - \sum_{j=i+1}^{n} u_j r_{i,j})\right] \tag{4.18}$$

La distance euclidienne entre le Babai point et le point reçu est donc égale à :

$$d^2 = \sum_{i=1}^{n} d_n^2$$

Le Babai point est une première estimation du point le plus proche, sans qu'il lui soit nécessairement égal. Rappelons que le principe du SE est de chercher le point le plus proche dans une hypersphère centrée sur le point reçu. En partant du Babai point, il faudra parcourir tous les points qui sont à l'intérieur de la sphère associée au réseau de points. L'idée originale de l'algorithme de Shnorr-Euchner consiste à tourner autour de chaque composante du Babai point en zigzaguant. Le changement de sens au cours du zigzag est défini par le signe des $d_i$.




Pour chaque combinaison de composantes du vecteur **u**, la distance $d^2$ est calculée. Si elle est inférieure à la précédente distance trouvée, $d^2$ est mise à jour, le point est stocké, et la recherche est poursuivit.

### 4.4.2 Rayon de la sphère

Contrairement au SD, la stratégie de recherche du SE n'impose pas de fixer le rayon initial de la sphère. Dans l'algorithme original proposé dans [49], $d^2$ est initialement égale à l'infini. Une fois le Babai point trouvé, $d^2$ est ajusté.

Dans [56], les auteurs constatent qu'en imposant un rayon fini, calculé de la même façon que celui du SD (4.15), la complexité de décodage est réduite de 30%. Nous avons mesuré par simulation le temps de recherche du point le plus proche en utilisant un rayon initial infini et un deuxième égal à $C_2$. Nous utilisons la version modifiée du SE, avec une constellation 16-QAM et un nombre d'antennes $n_t = 4$ (donc $n = 8$). Les résultats sont présentés dans la figure 4.9. Nous remarquons que les deux courbes sont presque parallèles et le gain est à peu prés égal à 30%.

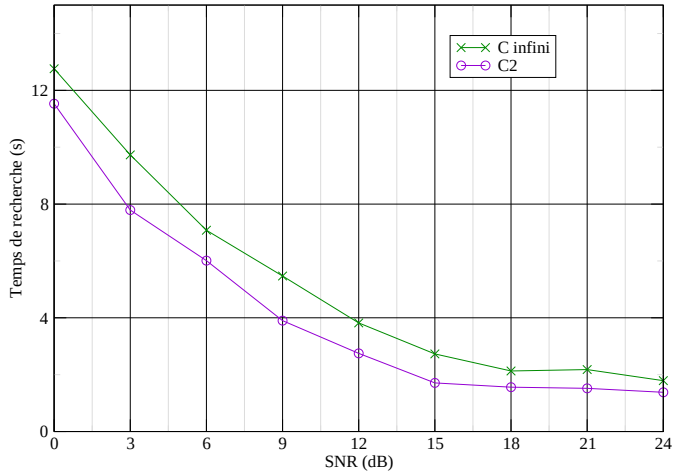



FIG. 4.9: Temps de recherche en secondes du SE modifié, pour $n = 8$ et une constellations 16-QAM

### 4.4.3 Décodage des sous-parties finies de réseau

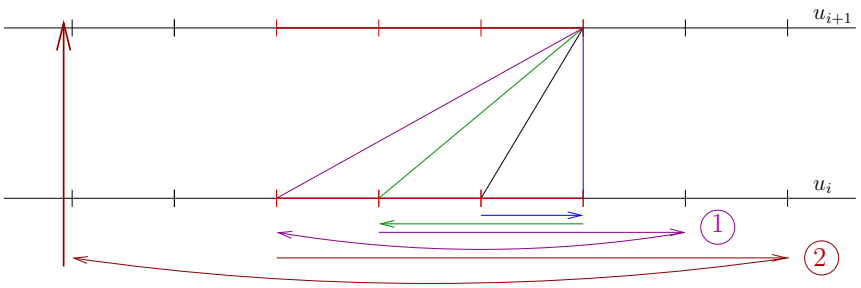
Le décodeur SE présenté ici, est utilisé pour décoder des réseaux de points infinis. Nous l'avons modifié pour pouvoir décoder des constellations $(q\text{-QAM})^n$ et $(q - \text{HEX})^n$. Soit $I_C = [C_{min}, C_{max}]$ l'intervalle auquel appartiennent les parties réelles et imaginaires (respectivement partie en $j$ et pas en $j$) des symboles de la constellation.

Afin de garantir l'aboutissement sur un point de la constellation, il faudra s'assurer que le Babai point appartienne bien à la constellation. Ce qui revient à vérifier que toutes les composantes du Babai point sont dans l'intervalle $I_C$. Pour cela, nous prenons $u_i = in(\hat{u}_i)$ à la place de $u_i = [\hat{u}_i]$. La fonction $in(x)$ est définie comme suit :

$$in(x) = \begin{cases} [x] \\ C_{min} \quad \text{, si } [x] < C_{min} \\ C_{max} \quad \text{, si } [x] > C_{max} \end{cases}$$

Le "zigzag" autour de chaque $u_i$ risque de sortir de l'intervalle $I_C$. Il faut donc revenir dans l'intervalle $I_C$ chaque fois qu'on n'est plus dedans. Deux cas de figures se présentent :

1. Soit on tombe dans l'intervalle $I_C$ , dans ce cas la recherche se poursuit.
2. Soit on ne tombe pas dans l'intervalle $I_C$. Cela veut dire que tous les points de l'intervalle ont été parcourus. Dans ce cas, il faudra remonter à la composante $u_{i+1}$.



Comme pour le décodeur par sphères, nous effectuons un changement de variable afin de travailler dans un sous-ensemble de $\mathbb{Z}^n$ au lieu de $(2\mathbb{Z})^n$. Et nous notons que, pour les constellations $q$-HEX (fig. 1.3) et la constellation 8-QAM (fig 1.2), l'ajout d'une routine de test pour ne prendre que les points de la constellation est indispensable.

### 4.4.4 Organigramme du SE modifié

L'organigramme 4.7 résume l'algorithme SE et les modifications apportées. Nous avons utilisé les mêmes notations que l'algorithme original présenté dans [49].

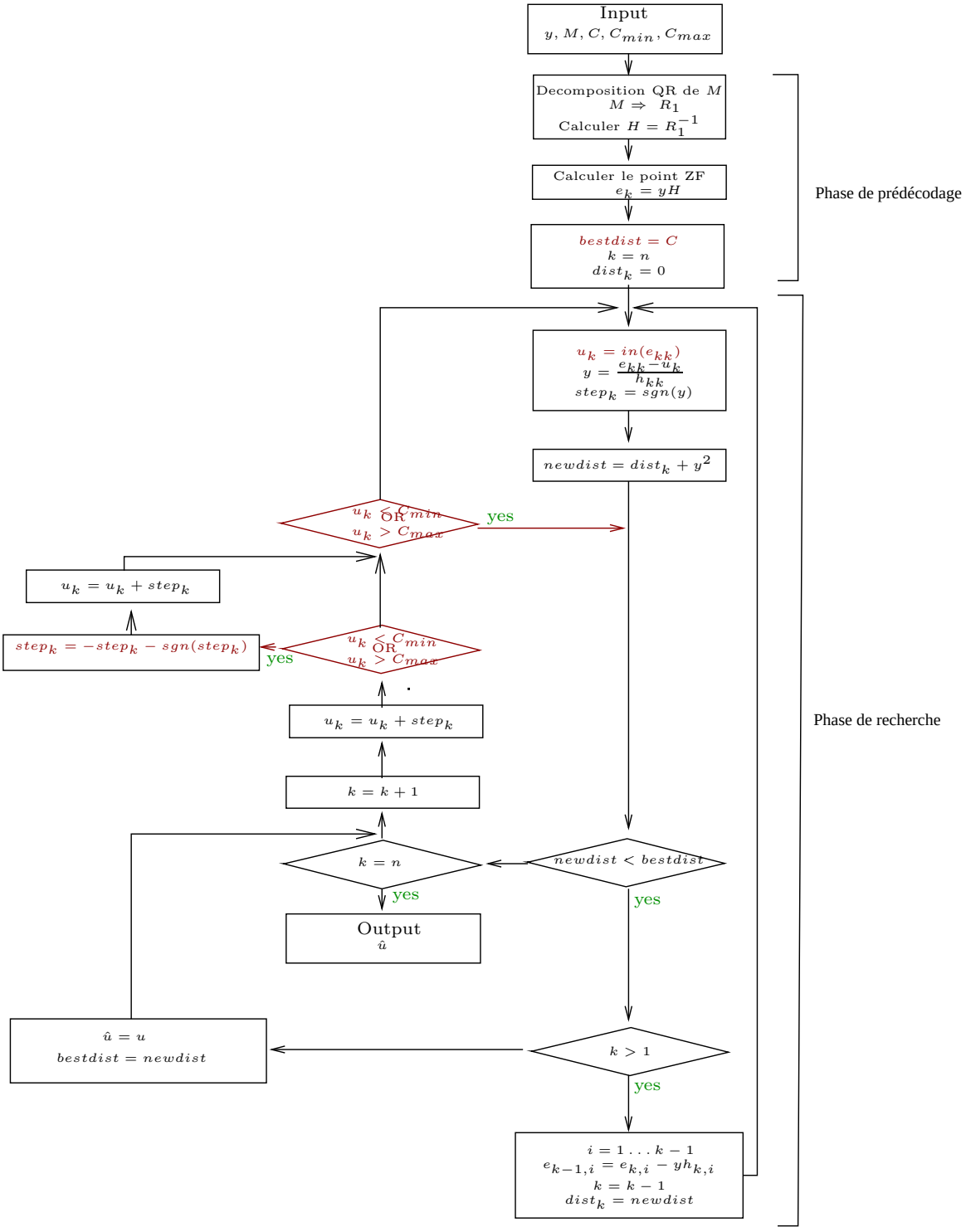



FIG. 4.10: Organigramme du Schnorr-Euchner modifié

## 4.5 Comparaison du SD et du SE

Après avoir présenté les algorithmes de décodage des réseaux de points SD et SE ainsi que les modifications qui leurs ont été apportées pour décoder des sous-parties finies de réseaux, nous nous proposons dans la suite de les comparer afin de choisir celui qui convient le mieux à notre système de transmission.

Il existe dans la littérature différentes études et comparaisons des complexités des décodeurs SD et SE [49, 57, 58, 59]. La complexité étant mesurée soit par le nombre d'opérations arithmétiques soit par le temps de calcul. En général, la recherche du point le plus proche est un problème non-polynomial (NP-hard) en fonction de la dimension [60]. Pour les systèmes MIMO, le point reçu est un point du réseau de points perturbé par un bruit Gaussien dont les propriétés statistiques sont connues. Pour ces systèmes, il a été montré que pour différents RSB, la complexité de décodage est polynomiale [59].

Dans la suite nous étudions et comparons la complexité des versions modifiées du SD et du SE adaptées à notre système de transmission de point de vue théorique (stratégie de recherche) et pratique (temps de recherche).

### 4.5.1 Comparaison de point de vue théorique

Le principe du SD et du SE est de chercher le point le plus proche dans une sphère centrée sur le point reçu. Comme nous l'avons déjà vu précédemment, les deux algorithmes parcourent les points du réseau se trouvant à l'intérieur de la sphère, mais diffèrent dans la stratégie de parcours.

#### 4.5.1.1 Stratégies de parcours

Pour chaque composante $u_i$ du vecteur $u$, le SD parcourt un intervalle $I_i = [B_{inf,i}, B_{sup,i}]$ (eq. 4.13) de bout en bout. Le SE parcourt, pour chaque composante $u_i$, le même intervalle $I_i$ en partant du milieu et en zigzaguant autour. Comme le montre le calcul suivant le $u_i$ considéré par le SE n'est autre que le milieu de l'intervalle $I_i = [B_{inf,i}, B_{sup,i}]$.

$$\begin{aligned} u_i &= \left\lceil \frac{1}{r_{i,i}} (y_i - \sum_{j=i+1}^{n} u_j r_{i,j}) \right\rfloor \\ &= \left\lceil \frac{1}{r_{i,i}} \sum_{j=i}^{n} \rho_i r_{ij} - \sum_{j=i+1}^{n} u_j \frac{r_{i,j}}{r_{i,i}} \right\rfloor \\ &= \left\lceil \rho_i + \sum_{j=i+1}^{n} (\rho_i - u_i) \frac{r_{i,j}}{r_{i,i}} \right\rfloor \end{aligned}$$

Ainsi le SD et le SE parcourent exactement les mêmes points du réseau pour trouver le point le plus proche.

Le parcours des points du réseau de points pour la recherche du point le plus proche, peut se voir comme le parcours d'un arbre de recherche. Dans la figure 4.11, nous avons tracé un exemple d'arbre de recherche du SD et du SE pour un réseau de points en dimension 3 (d'où 3

niveaux de recherche) et une constellation BPSK ($I_C$ = [0,1]). Le point le plus proche correspond donc à un parcours dans l'arbre [57].

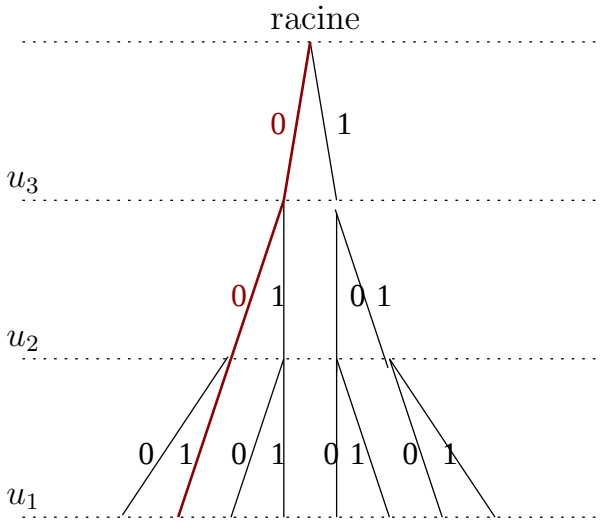



Fig. 4.11: Exemple d'arbre de recherche du SD et du SE

#### 4.5.1.2 Rayon de la sphère

La convergence du SD dépend étroitement du choix du rayon initial. En effet, pour un rayon initial fixé, l'algorithme cherche le point le plus proche dans une sphère bien définie. si aucun point n'a été trouvé, le rayon de la sphère est augmenté et la recherche est recommencée. Par ailleurs, la stratégie de recherche du SE permet de prendre un rayon initial de la sphère infini. Une fois le Babai point trouvé, ce rayon est ajusté. Ainsi la convergence du SE est toujours assurée. En prenant un rayon initial fini, il faut procéder de la même façon que pour le SD.

#### 4.5.1.3 Accélération du temps de recherche

Afin d'accélérer le décodage des réseaux de points, il est proposé dans [49] de réduire la matrice génératrice du réseau de points avant le décodage. En effet la réduction permet d'obtenir une nouvelle base du réseau ayant des vecteurs les plus courts et les plus orthogonaux possibles. Dans [57], il a été proposé de rajouter un ordonnancement des vecteurs de la base réduite afin d'accélérer encore plus la recherche du point le plus proche.

Pour le décodage des constellations finies, l'utilisation d'une réduction fait perdre les bornes de l'hypercube défini par la constellation. Ainsi, il devient impossible de vérifier en sortie du décodeur SD ou SE si le point obtenu appartient bien à la constellation.

### 4.5.2 Comparaison de point de vue pratique

Les algorithmes de décodage SD et SE modifiés comme ceux des non-modifiés se composent de deux phases : une phase de prédécodage et une phase de recherche, tels que le montrent leurs organigrammes respectifs (fig. 4.7, 4.10). Pour étudier et comparer la complexité du SE et SD nous allons étudier la complexité de chacune des phases .

#### 4.5.2.1 Complexité de la phase de prédécodage

Dans la phase de prédécodage, on effectue essentiellement deux opérations : la triangularisation de la matrice génératrice **M** du réseau de points et le calcul du point ZF.

La triangularisation de la matrice génératrice **M** peut être effectuée soit par la décomposition Cholesky, soit par la décomposition QR. Le nombre d'opérations arithmétiques respectifs des deux décompositions sont $\frac{2}{3} \cdot n^3$ et $\frac{1}{6} \cdot n^3 + n$ [61]. Sachant que la décomposition de Cholesky se fait sur la matrice de Gram de la matrice **M**, cela rajoute $n^3$ opérations supplémentaires. Ainsi l'utilisation de la décomposition QR s'avère plus intéressante.

La deuxième opération de la phase de prédécodage est le calcul du point ZF. Pour le SD, cela se fait directement en appliquant la formule $\rho = \mathbf{y} \cdot \mathbf{M}^{-1}$. Pour le SE, on effectue deux multiplications de matrices, $\rho = (\mathbf{y}.\mathbf{Q}) \cdot \mathbf{R}^{-1}$. Au final, les deux calculs restent presque équivalents en terme de nombre d'opérations.

En conclusion, nous pouvons dire que les phases de prédécodage du SD et SE aboutissent pratiquement à la même complexité.




#### 4.5.2.2 Complexité de la phase de recherche

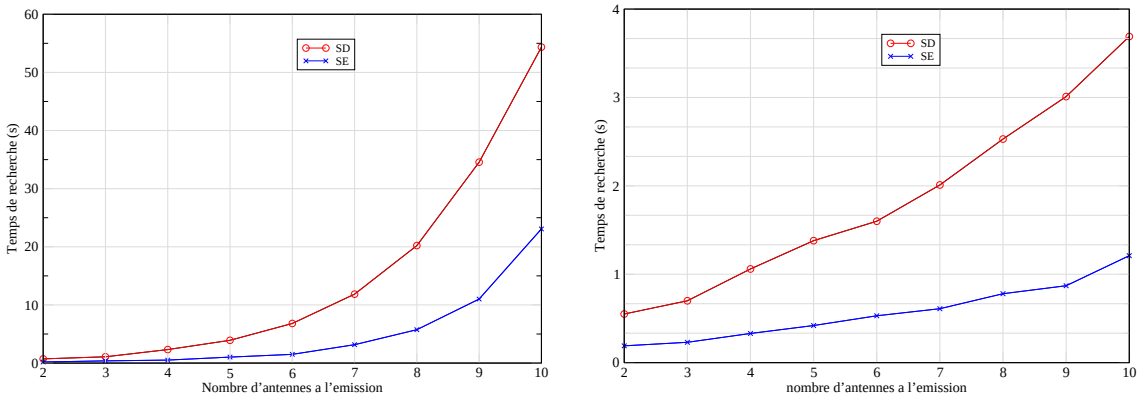
Nous nous proposons d'étudier et de comparer, par simulation, les complexités des phases de recherche des versions modifiées du SD et du SE en fonction du nombre d'antennes. La complexité sera mesurée par le temps de calcul en secondes.

Dans la figure 4.12, nous avons tracé le temps de recherche du SD et du SE en fonction du nombre d'antennes, à RSB=$\frac{E_b}{N}$ = 12 et 20 dB, en utilisant une constellation 16-QAM. Pour ces deux RSB, nous remarquons que la phase de recherche du SE est plus rapide que celle du SD. A moyen RSB, l'écart entre les temps de recherche est plus important qu'à fort RSB, cet écart augmente proportionnellement avec le nombre d'antennes.

#### 4.5.2.3 Complexité totale

Nous avons montré que les phases de prédécodage du SD et du SE sont presque équivalentes en terme de complexité. Par simulation, nous avons trouvé que le SE dispose d'une phase de recherche plus rapide que celle du SD. Nous concluons ainsi que la complexité totale de l'algorithme SE est inférieure à celle du SD.

Dans la figure 4.13, nous avons tracé le rapport du temps total de recherche (correspondant à la phase de prédécodage et la phase de recherche) du SD par SE en fonction du nombre d'antennes pour un RSB = $\frac{E_b}{N_0}$ = 12,20 dB, en utilisant une constellation 16-QAM. Pour les deux RSB, le rapport est presque constant. Par contre, il est un peu plus élevé pour un faible nombre d'antennes. A moyen RSB, le rapport est autour de 1.5, alors que à fort RSB, il est autour de 1.2. On déduit donc que, plus le RSB augmente, plus il est intéressant d'utiliser le SE.




(a) SNR=12 dB (b) SNR= 20 dB

Fig. 4.12: Comparaison des temps de recherche du SD et du SE modifiés, pour une constellation 16-QAM

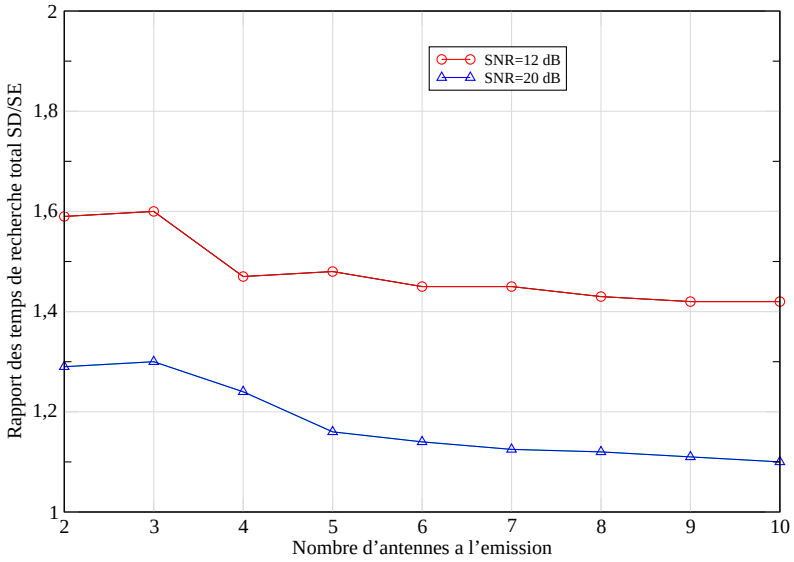



Fig. 4.13: Rapport des temps de recherche SD/SE, pour une constellation 16-QAM

## Conclusion

La représentation en réseau de points des codes ST dont font parties nos codes quaternioniques et parfaits construits au chapitre précédent, permet leur décodage par les décodeurs de réseaux de points donnant ainsi leurs performances optimales.

Au cours de ce chapitre, nous avons présenté les deux algorithmes de décodage ML des réseaux de points, le décodeur par sphères et le Schnorr-Euchner. Ces deux décodeurs ont été utilisés dans la littérature pour décoder les réseaux de points infinis.

Étant donné que nous utilisons les constellations $q$-QAM et $q$-HEX, nous avons été amenés à modifier le décodeur par sphères et le Schnorr-Euchner pour pouvoir décoder les constellations

finies.

L'étude menée sur les deux décodeurs pour le choix du meilleur nous a permis de conclure que les deux décodeurs disposent du même principe de fonctionnement, à savoir, la recherche du point le plus proche dans une sphère centrée sur le point reçu. Néanmoins, ils diffèrent dans la stratégie de parcours. La comparaison des complexités totales des deux décodeurs modifiés révèle que la stratégie de recherche du Schnorr-Euchner est plus rapide que celle du décodeur par sphères. D'où la justification de notre choix du décodeur au chapitre 3.

# Chapitre 5

# Réduction des réseaux de points algébriques pour les canaux à évanouissements rapides

## Introduction

Dans le chapitre précédent nous avons étudié et comparé les décodeurs de réseaux de points, le décodeur par sphères et le Schnorr-Euchner, que nous avons modifiés pour décoder des sous-parties finies de réseau. Sachant que le décodage des réseaux de points est d'autant plus complexe que la dimension du réseau augmente, l'utilisation d'une réduction, dans le but de réduire la complexité des décodeurs de réseaux de points, s'avère intéressante. Malheureusement, avec un schéma classique de codage/décodage de réseaux de points, l'application de la réduction se restreint aux réseaux infinis. Cependant, il est possible, en s'appuyant sur un schéma de codage/décodage spécifique, appelé mod-$\Lambda$ présenté dans [62], d'appliquer la réduction en considérant des sous-parties finies de réseau.

La réduction de réseau de points est un outil mathématique puissant utilisée dans diverses applications. La complexité de la réduction est d'autant plus grande que le résultat est optimal. Dans la littérature, il existe plusieurs algorithmes de réduction, parmi lesquels, nous distinguons la réduction LLL qui offre un résultat suffisamment "acceptable" avec une complexité polynomiale.

Le famille des codes ST en blocs algébriques à laquelle appartiennent nos codes quaternioniques et parfaits construits au chapitre III utilisent des réseaux de points algébriques. Nous nous sommes alors proposés de construire une nouvelle méthode de réduction adaptée aux réseaux de points algébriques, satisfaisant un bon compromis performance-complexité. Nous avons traité dans un premier temps le cas des transmissions sur des canaux à évanouissements rapides utilisant, dans le but d'introduire de la diversité de modulation, un précodage algébrique. Nous espérons généraliser ce résultat dans un futur proche aux cas des systèmes MIMO.

Dans la première partie de ce chapitre, nous définirons la notion de réduction de réseau de points et nous montrerons l'utilité de son application. Nous présenterons ensuite le schéma de codage/décodage en mod-$\Lambda$. La troisième partie sera consacrée à une brève présentation

des méthodes de réduction existantes dans la littérature. Nous présenterons notre nouvelle méthode de réduction algébrique dans la quatrième partie. La cinquième partie sera dédiée aux résultats de la réduction algébrique appliquée à des réseaux de points algébriques complexes. Nous finirons ce chapitre par la comparaison de la réduction algébrique avec la réduction LLL.

## 5.1 La réduction de réseau de points : définition et principe

### 5.1.1 Définition

Tel que nous l'avons défini dans le paragraphe 1.2, un réseau de points est un sous groupe de l'espace euclidien $\mathbb{R}^n$. Un réseau de points $\Lambda$ possède une infinité de bases. Soit $\mathbf{B_1}$ une base de $\Lambda$. $\mathbf{B_2} = \mathbf{B_1} \cdot \mathbf{U}$ est aussi une base de $\Lambda$, si $\mathbf{U}$ est une matrice inversible telle que $\mathbf{U}$ et $\mathbf{U}^{-1}$ sont à entrées entières. Étant donné que $\det(\mathbf{U}^{-1}) = \frac{1}{\det(\mathbf{U})}$, nous déduisons que $\det(\mathbf{U}) = \pm 1$. Le volume fondamental du réseau de points (def. 1.5) est indépendant de la base considérée :

$$V(\Lambda) = \det(\mathbf{B_1}) = \det(\mathbf{B_2} \cdot \mathbf{U}^{-1}) = \pm\det(\mathbf{B_2})$$

Par exemple, $\mathbf{B_1} = (\mathbf{u_1},\mathbf{u_2}) = ((3,2),(2,1))$ et $\mathbf{B_2} = (\mathbf{v_1},\mathbf{v_2}) = ((1,0),(0,1))$ sont deux bases de $\mathbb{Z}^2$(comme illustré dans la figure 5.1). La base $\mathbf{B_2}$ se déduit de la base $\mathbf{B_1}$ par la multiplication de $\mathbf{B_1}$ par $\mathbf{P}$, $\mathbf{B_2} = \mathbf{B_1}\mathbf{P}$.

$$\mathbf{P}^{-1} = \begin{bmatrix} -1 & 2 \\ 2 & -3 \end{bmatrix}$$

$\mathbf{P}$ et $\mathbf{P}^{-1}$ sont bien à entrées entières. Nous pouvons alors dire que $\mathbf{B_2}$ est obtenue par **réduction** de $\mathbf{B_1}$.

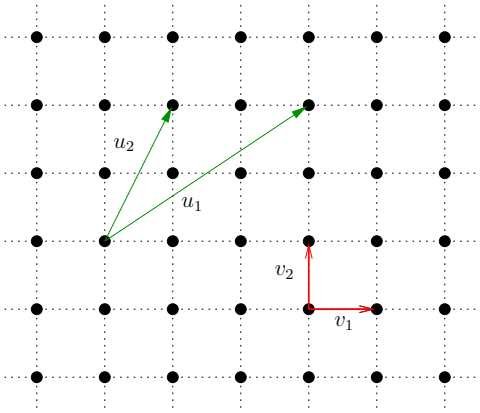



Fig. 5.1: Exemples de bases de $\mathbb{Z}^2$

D'une façon générale, nous pouvons imaginer qu'il existe certains critères permettant de classer toutes les bases d'un réseau de points donné et de déduire la "meilleure" base . Une base est dite **optimale** si les vecteurs qui la composent sont les plus courts et les plus orthogonaux possibles. La **réduction de réseaux de points** consiste alors à chercher la base optimale d'un réseau de points donné.

La matrice de passage $\mathbf{P}$ qui permet de passer d'une base quelconque à la base réduite s'appelle **matrice de réduction**.

### 5.1.2 Principe et intérêt de la réduction de réseau de points

Nous avons vu que la réduction de réseaux de points permet d'obtenir la meilleure base du réseau. Dans [49], les auteurs prouvent que la réduction de réseaux de points permet d'accélérer considérablement son décodage par les décodeurs de réseaux de points.

Afin d'illustrer concrètement l'importance du choix de la base du réseau pour le décodage, nous allons présenter la détection ZF avec et sans réduction d'un réseau de points en dimension 2 présenté dans [63].

Soit le système de transmission décrit par l'équation suivante :

$$\mathbf{y} = \mathbf{H} \cdot \mathbf{x} + \mathbf{w}$$

où $\mathbf{H}$ est la matrice du canal de transmission, $\mathbf{x}$ le vecteur des symboles d'information à composantes entières prises dans l'intervalle $[-N,N]$, où $N$ est un entier suffisamment grand, et $\mathbf{w}$ est un bruit blanc Gaussien.
Supposons que $\mathbf{H}$ est définie comme suit :

$$\mathbf{H} = \begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix}$$

La détection ZF donne :

$$\hat{\mathbf{x}} = [\mathbf{H}^{-1} \cdot \mathbf{y}]$$

où $[x]$ est l'entier le plus proche de $x$.

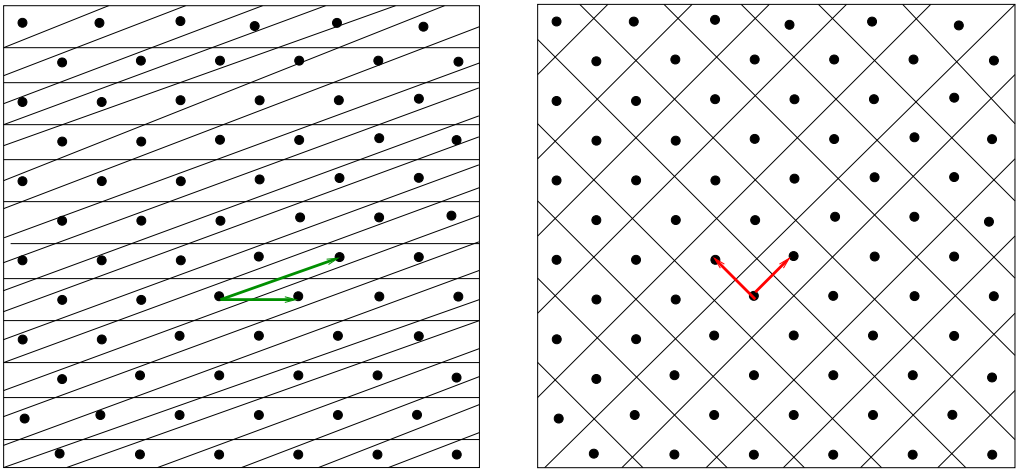
Dans la figure (5.2,a) nous avons présenté les régions de Voronoï (def. 1.6) du réseau de points engendré par $\mathbf{H}$. La détection ZF sera sous-optimale puisque la base utilisée n'est pas orthogonale.

En réduisant la matrice $\mathbf{H}$, on obtient :

$$\mathbf{H_1} = \mathbf{H} \cdot \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Les nouvelles régions de Voronoï du réseau de points sont représentées dans la figure (5.2,b). La nouvelle base est orthogonale. Par conséquent la détection ZF est optimale.

Cette illustration traduit bien le fait qu'une réduction de réseau de points permet d'obtenir les performances ML par une simple détection ZF.



(a) Sans Réduction (b) Avec Réduction

Fig. 5.2: Régions de Voronoï d'un réseau de points avec et sans réduction

## 5.2 Schéma de Codage/décodage en mod-Λ

L'utilisation de la réduction de réseaux de points en considérant des constellations finies s'avère impossible avec un schéma classique de codage/décodage de réseaux de points. Cela s'explique par le fait que la réduction transforme les inégalités qui définissent les bornes de la constellation en un système linéaire d'inégalités difficile à résoudre. Par conséquent, il devient impossible de vérifier l'appartenance d'un point décodé à la constellation en question.

Dans [64], Erez et Zamir proposent un schéma de codage/décodage appelé mod-Λ. Ils montrent que ce schéma permet d'atteindre, en utilisant un décodage de réseaux de points, la capacité d'un canal AWGN, pourvu que le décodeur soit modifié par l'introduction d'un amplificateur et l'ajout à l'émission d'une séquence aléatoire ("Random dither signal"). Il s'agit de la résolution du problème du codage pour le le "dirty paper", c'est-à-dire un canal gaussien avec une interférence connue à l'émetteur. La généralisation du schéma de codage/décodage en mod-Λ pour les systèmes MIMO a été présentée dans [62]. Cette généralisation se caractérise par l'introduction d'un filtre direct (forward filter) et d'un filtre retour (feedback filter) (MMSE-GDFE). Dans la figure 5.3, nous représentons le schéma équivalent dans le cas du canal à évanouissements rapides ("fast fading").

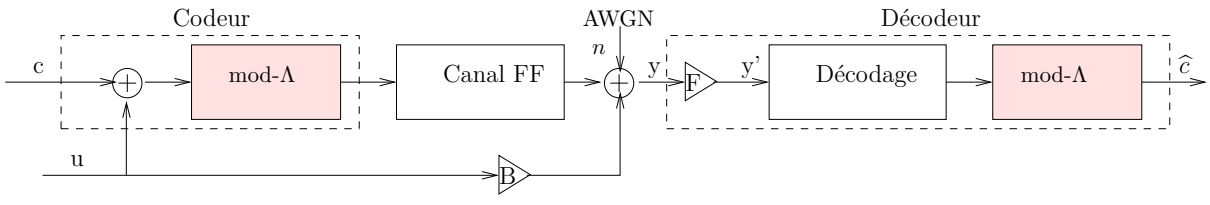



Fig. 5.3: Codage/décodage en mod-Λ pour un canal à évanouissement rapide

Contrairement aux autres cas où le codage/décodage en mod-Λ est utilisé, nous l'utilisons uniquement pour pouvoir résoudre le problème de la sous-partie finie d'un réseau. Afin de dé-

finir le codage/décodage en mod-$\Lambda$, nous aurons besoin de définir le code de Voronoï (Voronoï code ou nested lattice code) tel qu'il est donné dans [62].

**Définition : 5.1** *code de Voronoï*

*Soit $\Lambda_c$ un réseau de points de $\mathbb{R}^n$ et $\Lambda_s$ un sous-réseau de $\Lambda_c$. Le* ***code de Voronoï*** *défini par la partition $\Lambda_c/\Lambda_s$ est :*

$$C = \Lambda_c \cap \nu_s$$

*où $\nu_s$ est la région de Voronoï de $\Lambda_s$. En d'autres termes, C est formé par les représentants des classes (coset leaders) de $\Lambda_s$ dans $\Lambda_c$. Nous définissons aussi la fonction de* ***quantification de réseau de points*** *:*

$$Q_\Lambda(\mathbf{y}) \triangleq argmin_{\lambda\in\Lambda} \left|\mathbf{y} - \lambda\right|$$

*et la fonction* ***modulo-réseau de points*** *:*

$$[\mathbf{y}]\, mod\Lambda \triangleq \mathbf{y} - Q_\Lambda(\mathbf{y})$$

Nous en déduisons à partir de cette définition que, pour le code de Voronoï, l'information est codée dans les classes de $\Lambda_s$ dans $\Lambda_c$.

Soit un code de Voronoï $C$, défini par son réseau de codage (coding lattice) $\Lambda_c$ et son réseau de mise en forme (shaping lattice) $\Lambda_s$. Pour un mot de code de $C$ donné, l'émetteur génère un signal aléatoire $\mathbf{u}$ uniformément distribué dans $\nu_s$ ("dither"). Le signal à transmettre est donc :

$$\mathbf{x} = [\mathbf{c} - \mathbf{u}] \mathrm{mod}\Lambda_s$$

En définissant $\lambda = -Q_\Lambda(\mathbf{c} - \mathbf{u})$, $\mathbf{x}$ s'écrit :

$$\mathbf{x} = \mathbf{c} - \mathbf{u} + \lambda$$

Soit $\mathbf{F}$ et $\mathbf{B}$ respectivement le filtre direct et retour du décodeur MMSE-GDFE. Le vecteur $\mathbf{y}$ (fig. 5.3) s'écrit :

$$\begin{aligned}
\mathbf{y}' &= \mathbf{F}\mathbf{y} + \mathbf{B}\mathbf{u} \\
&= \mathbf{F}(\mathbf{H}(\mathbf{c} - \mathbf{u} + \lambda) + \mathbf{w}) + \mathbf{B}\mathbf{u} \\
&= \mathbf{B}(\mathbf{c} + \lambda) - (\mathbf{B} - \mathbf{F}\mathbf{H})(\mathbf{c} - \mathbf{u} + \lambda) + \mathbf{F}\mathbf{w} \\
&= \mathbf{B}(\mathbf{c} + \lambda) - (\mathbf{B} - \mathbf{F}\mathbf{H})\mathbf{x} + \mathbf{F}\mathbf{w} \\
&= \mathbf{B}(\mathbf{c} + \lambda) + \mathbf{e}'
\end{aligned}$$

Par construction, le vecteur $\mathbf{x}$ est uniformément distribué dans $\nu_s$ et est indépendant de $c$. En posant $\mathbf{c}' = \mathbf{c} + \lambda$, le vecteur $\mathbf{y}'$ se récrit :

$$\mathbf{y}' = \mathbf{B}\mathbf{c}' + \mathbf{e}'$$

Nous remarquons que le signal d'information $\mathbf{c}$ est translaté par un point inconnu $\lambda \in \Lambda_s$. Néanmoins, comme $\mathbf{c}$ et $\mathbf{c}'$ appartiennent à la même classe de $\Lambda_s$ dans $\Lambda_c$, la translation n'induit aucune perte d'information. $\mathbf{e}'$ est l'estimation de l'erreur MMSE indépendante de $\mathbf{c}'$ de matrice de covariance égale à l'identité. Pour retrouver le signal d'information, le décodeur doit

identifier la classe $\Lambda_s + \mathbf{c}$ qui contient $\mathbf{c'}$. Cela se fait en deux étapes. La première consiste à trouver :

$$\hat{\mathbf{z}} = \text{argmin}_{\mathbf{z} \in Z^{2MT}} \left| \mathbf{y'} - \mathbf{BGz} \right|$$

où $\mathbf{G}$ est la matrice génératrice du réseau de codage $\Lambda_c$ et la deuxième à décoder le mot de code. Le mot de code décodé est alors :

$$\hat{\mathbf{c}} = [\mathbf{G}\hat{\mathbf{z}}] \, \text{mod} \Lambda_s$$

Le signal aléatoire $\mathbf{u}$ rend le bruit indépendant du signal transmis asymptotiquement. Cela permet d'avoir une probabilité d'erreurs indépendante du signal transmis en utilisant un décodeur de réseaux de points.

Dans notre cas de figure, la matrice génératrice du réseau de codage est $\mathbf{G} = \mathbf{B\Phi}$, où $\mathbf{B}$ est définie comme suit :

$$\mathbf{B}^H\mathbf{B} = \mathbf{I} + \mathbf{H}^H\mathbf{H}$$

Le schéma de codage/décodage en mod-$\Lambda$ permet de voir que l'information transmise est codée en classes au lieu des points du réseau. Ainsi, une constellation finie va pouvoir être vue comme une constellation infinie et l'application d'une réduction devient possible.

## 5.3 Méthodes de réduction existantes

La théorie de réduction des réseaux de points remonte à plus d'un siècle. Elle découle des travaux effectués sur la réduction des formes quadratiques, telles celles de Hermite et de Korkine Zolotarev [65, 66], et des travaux de Minkowski [67] sur la géométrie des nombres.

Il existe trois grandes classes de méthodes de réduction : la réduction de Minkowski, la réduction de Korkine-Zolotaref et la réduction LLL. Les deux premières permettent d'obtenir une base réduite optimale. Cependant, leurs complexités sont non-polynomiales, ce qui rend peu pratiques leurs utilisations. La réduction Lenstra, Lenstra, Lovasz (LLL) produit une base de vecteurs "relativement" courts et "raisonnablement" orthogonaux avec une complexité polynomiale. C'est la réduction la plus classique et la plus utilisée à l'heure actuelle.

### 5.3.1 Réduction de Minkowski

Le principe de la réduction de Minkowski consiste à trouver une base des vecteurs les plus courts du réseau de points. Évidemment, la base trouvée contient le vecteur le plus court du réseau.

Soit un réseau de points $\Lambda$ et soit $\mathbf{B} = (\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n})$ sa base. $\mathbf{B}$ est le résultat de la réduction de Minkowski si elle vérifie :

1. $\mathbf{b_1}$ est le vecteur le plus court de $\Lambda$
2. pour tout $i = 2 \cdots n$, $\mathbf{b_i}$ est le vecteur le plus court dans $\Lambda$ indépendant de $\mathbf{b_1}, \cdots, \mathbf{b_{i-1}}$, tel que l'ensemble des vecteurs $(\mathbf{b_1}, \cdots, \mathbf{b_i})$ peut être complété de façon à former une base de $\Lambda$. En d'autres termes, $\mathbf{b_i}$ ne peut pas s'écrire comme une combinaison linéaire des vecteurs de la base déjà choisis : $\mathbf{b_1}, \cdots \mathbf{b_{i-1}}, \mathbf{b_i} \neq \sum_{j=1}^{i-1} x_j \mathbf{b_j}$, où $x_j \in \mathbb{Z}$.

Le vecteur le plus court du réseau peut être trouvé par le biais d'une variante de l'algorithme de Schnorr-Euchner présentée dans [49].

Malgré l'application de la réduction de Minkowski dans la théorie des nombres, son utilisation pratique reste restreinte.

### 5.3.2 Réduction Korkine-Zolotareff (KZ)

La réduction Korkine-Zolotareff (KZ) est une variante de la réduction de Minkowski mais plus pratique à utiliser.

Les vecteurs de la base sont les vecteurs les plus courts des réseaux de points orthogonaux complémentaires engendrés par les vecteurs de la base déjà trouvés. De la même façon que la réduction de Minkowski, la base produite contient toujours le vecteur le plus court du réseau.

Considérons un réseau de points $\Lambda$ de base $\mathbf{B} = (\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n})$. $\mathbf{B}$ est résultat de la réduction (KZ) si elle vérifie :

1. $\mathbf{b_1}$ est le vecteur le plus court de $\Lambda$
2. Soit $\Lambda_i$ le réseau de points obtenu par projection de $\Lambda_{i-1}$ sur le sous-espace de $\mathbb{R}^{n-i+1}$ perpendiculaire à $\mathbf{b_{i-1}}$. $\mathbf{b_i}$ est le vecteur le plus court de $\Lambda_i$.

### 5.3.3 Réduction Lenstra, Lenstra, Lovasz (LLL)

L'algorithme de réduction le plus classique est celui proposé par Lenstra, Lenstra et Lovasz (LLL) dans [68]. Il se distingue par sa complexité polynomiale, ce qui justifie ses diverses applications : trouver les facteurs irréductibles de polynômes, trouver le polynôme minimal d'un nombre algébrique, approximation diophantienne simultanée, attaque des systèmes cryptés.

Schnorr dans [69] a généralisé cette réduction et a donné l'implémentation pratique de l'algorithme. Dans [70], une implémentation en virgule flottante a été développée.

Considérons un réseau de points $\Lambda$ de base $\mathbf{B} = (\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n})$. Le principe de la réduction LLL consiste à considérer les vecteurs de la base par couple, où chaque vecteur $\mathbf{b_i}$ de la base doit être le vecteur le plus court dans le réseau de points en dimension 2 engendré par le couple $(\mathbf{b_i}, \mathbf{b_{i+1}})$. Dans [69], Shnorr a présenté l'algorithme de réduction **KZ par blocs** (en considérant des blocs de $k$ vecteurs au lieu de couples de vecteurs) qui est une extension du LLL. Du fait que la réduction LLL soit de nature locale, la base trouvée n'inclut pas obligatoirement le vecteur le plus court, mais une approximation de ce dernier.

Soit $\mathbf{B}^* = (\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*})$ la base obtenue par l'orthogonalisation Gram-Shmidt de $\mathbf{B}$.

$$\begin{aligned} \mathbf{b_i^*} &= \mathbf{b_i} - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b_j^*} \\ \mu_{ij} &= \frac{\left\langle \mathbf{b_i}, \mathbf{b_j^*} \right\rangle}{\left| \mathbf{b_j^*} \right|^2} \end{aligned}$$

La base $\mathbf{B}^*$ est orthogonale, mais n'est pas orthonormale.

Par souci de compréhension, admettons que le réseau de points $\Lambda$ soit de dimension 2. La base ($\mathbf{b_1}$,$\mathbf{b_2}$) de $\Lambda$ est le résultat de la réduction LLL (Gaussien reduced) si elle vérifie :

$$\frac{\langle \mathbf{b_1}, \mathbf{b_2} \rangle}{|\mathbf{b_1}|^2} \leq \frac{1}{2} \tag{5.1}$$

$$|\mathbf{b_1}|^2 \leq |\mathbf{b_2}|^2 \tag{5.2}$$

Afin de garantir une complexité polynomiale de l'algorithme de réduction, la deuxième contrainte 5.2 est relaxée :

$$|\mathbf{b_1}|^2 \leq \frac{4}{3} |\mathbf{b_2}|^2 \tag{5.3}$$

Revenons maintenant au réseau de points $\Lambda$ en dimension $n$. Soit $\Lambda_i$ le réseau de points engendré par le couple de vecteurs ($\mathbf{b_i}$,$\mathbf{b_{i+1}}$). Le réseau de points résultat de la projection orthogonale de $\Lambda_i$ sur $\mathbf{b_1}, \cdots, \mathbf{b_{i-1}}$ a comme base $\mathbf{b_i(i)} = \mathbf{b_i^*}$ et $\mathbf{b_{i+1}(i)} = \mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}$. En appliquant les deux contraintes 5.1 et 5.3 sur les couples de vecteurs adjacents ($\mathbf{b_i}$,$\mathbf{b_{i+1}}$), nous obtenons les conditions pour que $\mathbf{B}$ soit le résultat de la réduction LLL :

$$\left|\mu_{ij}\right| \leq \frac{1}{2}, \text{ for } 1 \leq i < j \leq n \tag{5.4}$$

$$\left|\mathbf{b_i^*}\right|^2 \leq \frac{4}{3} \left|\mathbf{b_{i+1}^*} + \mu_{i+1,i}\mathbf{b_i^*}\right|^2 \tag{5.5}$$

Une base vérifiant la condition 5.4 est appelée "size reduced". L'algorithme LLL s'écrit en utilisant la fonction "SizeReduce" comme suit.

Algorithme LLL

Entrée $B = (b_1, \cdots, b_n)$

Tant que: il existe $i$ ne vérifiant pas la condition 5.3

Echanger $(b_i, b_{i+1})$

Mettre à jour les $\mu_{hk}$ et $b_k^*$

$B \leftarrow \text{SizeReduce}(B)$

Retourner $B$

SizeReduce($B$)

Pour $j = 2 \cdots n$

Pour $i = j - 1 \cdots 1$

$b_j \leftarrow b_j - [\mu_{ji}]\, b_i$

Pour $k = 1 \cdots i$ $\mu_{jk} \leftarrow \mu_{jk} - [\mu_{ji}]\, \mu_{ik}$

Retourner $B$

## 5.4 Nouvelle méthode de réduction : la réduction algébrique

Dans nos constructions de codes ST, nous avons utilisé des réseaux de points algébriques construits sur des corps de nombres. En nous appuyant encore une fois sur les outils algébriques, nous nous sommes proposés de construire une nouvelle méthode de réduction adéquate aux réseaux de points algébriques. Notre méthode va porter dans un premier temps sur les systèmes de transmission mono-antenne sur canaux à évanouissements rapides (Fast-Fading - FF) dans le but de la généraliser pour les systèmes à antennes multiples. La généralisation fera l'objet de futurs travaux.

Avant de présenter le principe et l'algorithme de la réduction algébrique, nous commencerons par la définition du système de transmission considéré.

### 5.4.1 Système de transmission considéré

Considérons un système de transmission mono-antenne sur un canal FF. Pour combattre les évanouissements causés par sa grande variabilité dans le temps, un précodeur apportant de la diversité de modulation peut être utilisé [33, 34]. Le précodage consiste à appliquer une matrice unitaire au vecteur composé de symboles d'information complexes, augmentant ainsi la dimension algébrique de la constellation initiale. Un exemple détaillé en dimension 2 et illustrant l'utilisation des constellations tournées a été présenté dans le paragraphe (2.7).

Soit $\mathbf{\Phi}$ la matrice de précodage de dimension $n \times n$ et $\mathbf{s} = (s_1, s_2, \cdots, s_n)$ le vecteur de symboles d'information. Le vecteur reçu s'écrit :

$$\mathbf{y} = \mathbf{H} \cdot \mathbf{\Phi} \cdot \mathbf{s} + \mathbf{w} \tag{5.6}$$

La matrice du canal $\mathbf{H}$ est une matrice diagonale à entrées indépendantes et identiquement distribuées (i.i.d), de moyenne nulle et de variance 0.5 par composante réelle.

$$\mathbf{H} = \mathrm{diag}(h_1, h_2, \cdots h_n)$$

$\mathbf{w}$ est le vecteur du bruit additif blanc Gaussien de moyenne nulle et de variance $\sigma^2$ par composante réelle.

Dans le paragraphe (5.2), nous avons montré que l'utilisation d'un schéma de codage/décodage en mod-$\Lambda$ rend possible l'application de de la réduction en considérant des constellations finies. Notre objectif étant de construire une nouvelle méthode de réduction algébrique avec un bon compromis complexité-performance, nous allons nous limiter dans la suite, par souci de simplification, aux réseaux de points infinis, en prenant les symboles d'information dans $\mathbb{Z}[i]^n$. L'application du schéma de codage/décodage en mod$\Lambda$ n'altérera pas les performances de la réduction construite.

– **Définition de la matrice de précodage $\phi$**

Notre intérêt portera sur les matrices de précodage définies sur des corps cyclotomiques [33, 34] dont la construction repose sur le plongement canonique dans le corps cyclotomique.

Le corps de base $L$ est choisi égal à $\mathbb{Q}(i)$. Soit $\theta = \zeta_N = e^{\frac{i2\Pi}{N}}$ la $N^{\text{ième}}$ racine de l'unité de degré $\Phi(N) = n$, où $\Phi(N)$ est la fonction d'Euler donnant le nombre d'entiers premiers avec $N$

et plus petits que $N$. $K = L(\theta)$ est le corps cyclotomique de degré $n$ sur $L$. Il est alors totalement complexe de signature $(0,n)$. Soit $\sigma$ le générateur du groupe de Galois de $K$ :

$$\sigma : \zeta_N \longmapsto \zeta_N e^{\frac{i4\Pi}{n}}$$

L'anneau des entiers $O_K = \mathbb{Z}[i,\theta]$ est engendré par la base intégrale $B = (1,\theta,\theta^2,\cdots,\theta^{n-1})$. Le plongement canonique de $O_K$ dans $\mathbb{C}^n$ est l'homomorphisme défini comme suit :

$$\begin{array}{rcl} O_K & \rightarrow & \mathbb{C}^n \\ x & \longmapsto & (\sigma^0(x),\sigma^1(x),\cdots,\sigma^{n-1}(x)) \end{array}$$

En appliquant ce plongement canonique à la base intégrale $B$, on obtient la matrice de rotation complexe engendrant le réseau de points $\Lambda(O_K)$ :

$$\mathbf{\Phi} = \frac{1}{n}\begin{bmatrix} 1 & \theta & \cdots & \theta^{n-1} \\ 1 & \sigma^2(\theta) & \cdots & \sigma^2\left(\theta^{n-1}\right) \\ \vdots & & \ddots & \vdots \\ 1 & \sigma^{n-1}(\theta) & \cdots & \sigma^{n-1}\left(\theta^{n-1}\right) \end{bmatrix} \tag{5.7}$$

### 5.4.2 Représentation matricielle des éléments de $K$

La représentation matricielle des éléments du corps cyclotomique est un outil qui nous sera utile dans la suite pour établir le résultat de la réduction algébrique. C'est pourquoi nous le présentons dès à présent.

A chaque élément $x \in K$, on peut associer une matrice $\mathbf{T}_x \in \mathcal{M}_n(L)$ tel que :

$$\det \mathbf{T}_x = N_{K/L}(x) = \prod_{j=0}^{n-1} \sigma^j(x)$$

vérifiant :

$$\mathrm{diag}(\sigma^j(x)_{j=0\cdots n-1}) \cdot \mathbf{\Phi} = \mathbf{\Phi} \cdot \mathbf{T}_x$$

Si $x$ est dans l'anneau des entiers $O_K$ alors la matrice $\mathbf{T}_x$ est dans $\mathcal{M}_n(O_L)$. Explicitement $\mathbf{T}_x$ s'écrit :

$$\mathbf{T}_x = \frac{1}{n}\begin{bmatrix} Tr(x) & Tr(x\theta) & \cdots & Tr(x\theta^{n-1}) \\ Tr(x\theta^{-1}) & Tr(x) & \cdots & Tr(x\theta^{n-2}) \\ \vdots & \vdots & \ddots & \vdots \\ Tr(x\theta^{-(n-1)}) & Tr(x\theta^{-(n-2)}) & \cdots & Tr(x) \end{bmatrix}$$

Exemple : Soient $\theta = e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}}(1+i)$, $K = \mathbb{Q}(i,\theta)$, et $\sigma(\theta) = -\theta$. Pour tout $z = x + y\theta \in O_L$ où $x,y \in L$, la matrice $\mathbf{T}_z$ associée à $z$ s'écrit :

$$\mathbf{T}_z = \begin{bmatrix} x & iy \\ y & x \end{bmatrix} \in \mathcal{M}_2(L)$$

Cette représentation est aussi un homorphisme de corps car elle conserve au niveau matriciel les propriétés de l'addition et de la multiplication dans $K$.

### 5.4.3 La réduction algébrique

Comme nous l'avions déjà définie au premier paragraphe, la réduction de réseaux de points consiste à chercher une base du réseau composée des vecteurs les plus courts et les plus orthogonaux possibles.

L'idée de la réduction algébrique repose sur la transformation de l'évanouissement en un changement de base, retrouvant ainsi une base quasi-orthogonale du réseau.

Réécrivant la matrice du canal $\mathbf{H}$ sous la forme suivante :

$$\begin{aligned} \mathbf{H} &= \left|\prod_{i=1}^{n} h_i\right|^{\frac{1}{n}} \cdot \mathrm{diag}(a_1, a_2, \ldots, a_n) \\ &= c \cdot \mathbf{H_1} \end{aligned} \tag{5.8}$$

Nous avons donc $\left|\prod_{i=1}^{n} a_i\right| = 1$, par la suite $|\det(\mathbf{H_1})| = 1$. Supposons qu'il existe une unité $u$ de $O_K$, telle que :

$$(|a_1|, |a_2|, \ldots, |a_n|) = (\left|\sigma^0(u)\right|, \left|\sigma^1(u)\right|, \cdots, \left|\sigma^{n-1}(u)\right|) \tag{5.9}$$

Posons pour $k = 1 \cdots n$ :

$$\beta_k = \arg(a_k) - \arg(\sigma^{k-1}(u))$$

Nous avons alors :

$$(a_1, a_2, \ldots, a_n) = (e^{i\beta_1}\sigma^0(u), e^{i\beta_2}\sigma^1(u), \cdots, e^{i\beta_n}\sigma^{n-1}(u)) \tag{5.10}$$

En utilisant les deux équations 5.8 et 5.10, le signal reçu défini dans l'équation 5.6 se récrit :

$$\begin{aligned} \mathbf{y} &= \mathbf{H} \cdot \mathbf{\Phi} \cdot \mathbf{s} + \mathbf{w} \\ &= c \cdot \mathrm{diag}(e^{i\beta_1}, e^{i\beta_2}, \cdots, e^{i\beta_n}) \cdot \mathrm{diag}(\sigma^0(u), \sigma(u), \cdots, \sigma^{n-1}(u)) \cdot \mathbf{\Phi} \cdot \mathbf{s} + \mathbf{w} && (5.11) \\ &= c \cdot \mathbf{\Psi} \cdot \mathbf{U} \cdot \mathbf{\Phi} \cdot \mathbf{s} + \mathbf{w} && (5.12) \end{aligned}$$

En utilisant la représentation matricielle des éléments de $K$ présentée au paragraphe précédent, nous définissons la matrice $\mathbf{T}_u$ correspondante à l'unité $u$. Nous avons alors

$$\mathbf{U} \cdot \mathbf{\Phi} = \mathbf{\Phi} \cdot \mathbf{T}_u$$

En remplaçant dans 5.12, nous obtenons alors :

$$\mathbf{y} = c \cdot \mathbf{\Psi} \cdot \mathbf{\Phi} \cdot \mathbf{T}_u \cdot \mathbf{s} + \mathbf{w} \tag{5.13}$$

$u$ étant une unité, par définition (def. 1.33), sa norme est égale à $\pm 1$ ou $\pm i$. Par la suite le déterminant de la matrice $\mathbf{T}_u$ est égal à $\pm 1$ ou $\pm i$. De plus elle est définie sur $Z[i]$. $\mathbf{T}_u$ est alors matrice unimodulaire. D'où :

$$\mathbf{T}_u \cdot \mathbb{Z}[i]^n = \mathbb{Z}[i]^n$$

Soit le vecteur $\mathbf{z}$ défini comme suit :

$$\mathbf{z} = \mathbf{T}_u \cdot \mathbf{s} \in \mathbb{Z}[i]^n$$

L'équation 5.13, se réécrit en fonction de $\mathbf{z}$ :

$$\mathbf{y} = c \cdot \mathbf{\Psi} \cdot \mathbf{\Phi} \cdot \mathbf{z} + \mathbf{w} \tag{5.14}$$

La matrice $\mathbf{\Psi}$ est diagonale et son déterminant est de module égal à 1. La matrice $\mathbf{\Phi}$ est unitaire. Ainsi, nous avons réduit notre réseau de points et la matrice $\mathbf{T}_u$ est la matrice de réduction.

Cependant, cette réduction n'est possible que lorsqu'il existe une unité $u$ vérifiant 5.10, ce qui n'est pas toujours vrai. Il nous faudra donc chercher une unité $u$ tel que les modules de $u$ et de ses conjuguées approximent au mieux les modules des $a_i$, $i = 1 \cdots n$. Soit $\xi$ la matrice représentant l'erreur d'approximation. Elle est définie comme suit :

$$\xi = \text{diag}(\xi_1, \xi_2, \ldots, \xi_n) = \text{diag}\left( \frac{|a_1|}{\left|\sigma^0(u)\right|}, \frac{|a_2|}{\left|\sigma^1(u)\right|}, \cdots, \frac{|a_n|}{\left|\sigma^{n-1}(u)\right|} \right)$$

Le vecteur reçu s'écrit finalement en tenant compte de l'erreur d'approximation :

$$\mathbf{y} = c \cdot \mathbf{\Psi} \cdot \xi \cdot \mathbf{\Phi} \cdot \mathbf{z} + \mathbf{w}$$

La question qui se pose maintenant : comment trouver la bonne unité $u$ ?. Cette question sera traitée au paragraphe suivant en utilisant le réseau logarithmique (def. 1.33).

### 5.4.4 Le décodage du réseau logarithmique

Il existe $r = s + t - 1$ unités de $K$, $u_l, l = 1 \ldots r$. Toute unité $u$ de $K$ s'écrit d'une façon unique sous la forme :

$$u = \varepsilon \cdot \prod_{i=1}^{s+t-1} u_i^{k_i} \tag{5.15}$$

où $k_l \in \mathbb{Z}$, $l = 1 \ldots r$, $\varepsilon$ est une racine de l'unité et $(u_l)_{l=1\ldots r}$ le système d'unités fondamentales de $K$. En utilisant le plongement logarithmique de $K^*$dans $\mathbb{R}^{s+t}$, nous construisons le réseau logarithmique $\sigma_{log}(u_K)$ dont la matrice génératrice s'écrit de la façon suivante :

$$\mathbf{G} = \begin{bmatrix} \log|\sigma_1(u_1)| & \log|\sigma_2(u_1)| & \cdots & \log|\sigma_{s+t}(u_1)| \\ \log|\sigma_1(u_2)| & \log|\sigma_2(u_2)| & \cdots & \log|\sigma_{s+t}(u_2)| \\ \vdots & \vdots & \ddots & \vdots \\ \log|\sigma_1(u_{s+t-1})| & \log|\sigma_2(u_{r+s-1})| & \cdots & \log|\sigma_{s+t}(u_{s+t-1})| \end{bmatrix}$$

Soit $u$ une unité. Définissons le vecteur $\mathbf{U}$ comme suit :

$$\mathbf{U}_{\log} = (\log|\sigma_1(u)|, \ldots, \log|\sigma_{t+s}(u)|)$$

D'après l'équation 5.15, le vecteur $\mathbf{U}_{\log}$ s'écrit dans le réseau logarithmique $\sigma_{log}(u_K)$ :

$$\mathbf{U}_{\log} = (k_1, k_2, \cdots, k_2) \cdot \mathbf{G}$$

Ainsi le décodage du réseau logarithmique permet de trouver l'unité $u$ tel que le vecteur $(|\sigma_1(u)|, |\sigma_2(u)|, \ldots, |\sigma_n(u)|)$ approxime le vecteur $(|a_1|, |a_2|, \ldots, |a_n|)$. Il peut être accompli par le biais des décodeurs de réseaux de points étudiés au chapitre précédent, le décodeur par sphères et le Schnorr-Euchner. Un décodage sous-optimal peut être aussi utilisé.

### 5.4.5 L'algorithme de la réduction algébrique

L'algorithme de la réduction algébrique peut être résumé en 4 étapes :

1- Normalisation de $H$
2- Sortir les phases de la matrice $H$
3- Approximer la matrice module de $H$ par une unité $u$ et ses conjuguées
$\rightarrow$ Décodage du réseau logarithmique
4- Calculer la matrice de passage $T_u$

La première, la deuxième et la quatrième étapes de la réduction algébrique sont simples et élémentaires. La troisième est le coeur de l'algorithme de réduction, dont dépend la qualité et la complexité de l'algorithme. En effet, la réduction est d'autant plus optimale que l'approximation du vecteur $(|a_1|, |a_2|, \ldots, |a_n|)$ par le vecteur $(|\sigma_1(u)|, |\sigma_2(u)|, \ldots, |\sigma_n(u)|)$ est bonne, avec $u$ une unité de $\mathcal{O}_K$. Cela dépend du décodage du réseau logarithmique ainsi que ses propriétés.

Quant à la complexité de l'algorithme de réduction, elle dépend directement de la complexité de décodage du réseau logarithmique. En remarquant que le réseau logarithmique est réel, la complexité de son décodage par un décodeur de réseaux de points reste raisonnable. Nous pouvons aussi penser à un décodage sous-optimal afin de réduire encore plus la complexité. En conclusion, la complexité de l'algorithme de réduction algébrique reste très raisonnable, ce qui favorise son implémentation pratique.

## 5.5 Performances de la réduction algébrique

Nous considérons un système mono-antenne sur canal à évanouissements rapides employant un précodage linéaire. Après application de la réduction algébrique, le signal reçu s'écrit :

$$\mathbf{y} = c \cdot \mathbf{\Psi} \cdot \xi \cdot \mathbf{\Phi} \cdot \mathbf{z} + \mathbf{w} \tag{5.16}$$

Notre objectif étant d'étudier les performances de la réduction algébrique, nous employons, pour compléter notre chaîne de transmission, une détection par Forçage à Zéro (ZF) pour décoder $\mathbf{y}$. Notre étude portera sur les réseaux de points en dimension $n = 2$, 4 et 8.

### 5.5.1 Détection par Forçage à Zero (ZF)

Reprenons l'équation 5.16. Du fait que les matrices $\mathbf{\Psi}$ et $\xi$ sont diagonales et la matrice $\mathbf{\Phi}$ unitaire, une simple détection ZF peut être utilisée pour décoder le vecteur $\mathbf{s}$ émis.

La détection ZF consiste à l'inversion du canal suivie d'une détection à seuil. La sortie du détecteur ZF s'écrit :

$$\begin{aligned} \rho &= \left[\frac{1}{c} \cdot \mathbf{\Phi}^H \cdot \xi^{-1} \cdot \mathbf{\Psi}^H \cdot \mathbf{y}\right] \\ &= \left[z + \frac{1}{c} \cdot \mathbf{\Phi}^H \cdot \xi^{-1} \cdot \mathbf{\Psi}^H \cdot \mathbf{w}\right] \\ &= [\mathbf{T}_u \cdot \mathbf{s} + \mathbf{w_1}] \end{aligned}$$

où $\mathbf{w_1}$ reste un vecteur Gaussien. $[x]$ est l'entier le plus proche de $x$. Retrouver $\hat{\mathbf{s}}$ à partir de $\rho$ reste évident puisque $\mathbf{T}_u \in \mathbb{Z}^n$ :

$$\hat{\mathbf{s}} = \mathbf{T}_u^{-1} \cdot \rho$$

On conjecture que la réduction algébrique suivie d'une simple détection ZF permet l'obtention d'une diversité maximale. En effet, la matrice représentant l'erreur d'approximation est bornée par le rayon de recouvrement du réseau logarithmique.

### 5.5.2 Réseauxde points complexe en dimension 2

Nous considérons comme matrice de précodage la matrice $\mathbf{\Phi}$ construite sur le corps cyclotomique de degré 2, $K = \mathbb{Q}(\theta)$, où $\theta = e^{\frac{i\pi}{4}}$

$$\mathbf{\Phi} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \theta \\ 1 & -\theta \end{bmatrix}$$

La signature du corps $K$ est égale (0,2), par la suite, son système d'unités fondamentales se réduit à une unité : $u_1 = 1 + i - ie^{\frac{i\pi}{4}} = \theta^2 - \theta + 1$ et son réseau logarithmique à $\Lambda \cong \mathbb{Z}$.

Nous avons simulé le système de transmission décrit par l'équation 5.6 en utilisant notre réduction algébrique. Dans la figure 5.4, nous avons tracé le taux d'erreurs par mot (vecteur $\mathbf{s}$) en fonction du RSB = $\frac{E_s}{N_0}$, pour la détection ZF sans réduction, la détection ZF après réduction algébrique et le décodeur ML.

Nous remarquons que la réduction algébrique avec une simple détection ZF permet de récupérer la diversité maximale, égale à 2. Le réseau logarithmique étant de dimension 1, son décodage est élémentaire. Ainsi, la complexité de la réduction algébrique suivie d'une détection ZF est négligeable par rapport à celle du décodeur ML, tout en gardant quasiment les mêmes performances.

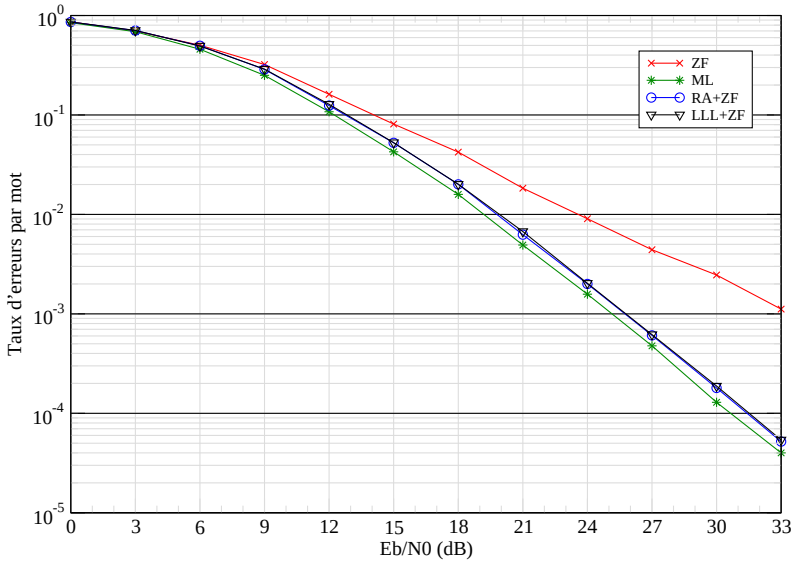



Fig. 5.4: Décodage de réseau de points complexe en dimension 2

### 5.5.3 Réseau de points complexe en dimension 4

Nous considérons le corps cyclotomique de degré 4 sur $\mathbb{Q}(i)$, $K = \mathbb{Q}(\theta)$, où $\theta = e^{\frac{i\pi}{8}}$. La matrice de précodage $\mathbf{\Phi}$ est telle que définie dans l'équation 5.7.

$$\mathbf{\Phi} = \frac{1}{2}\begin{bmatrix} 1 & e^{\frac{i\pi}{8}} & e^{\frac{i\pi}{4}} & e^{\frac{i3\pi}{8}} \\ 1 & ie^{\frac{i\pi}{8}} & -e^{\frac{i\pi}{4}} & -ie^{\frac{i3\pi}{8}} \\ 1 & -e^{\frac{i\pi}{8}} & e^{\frac{i\pi}{4}} & -e^{\frac{i3\pi}{8}} \\ 1 & -ie^{\frac{i\pi}{8}} & -e^{\frac{i\pi}{4}} & ie^{\frac{i3\pi}{8}} \end{bmatrix}$$

La signature du corps $K$ est égale (0,4). Par la suite, son système d'unités fondamentales se compose de 3 unités :

$$\begin{aligned} u_1 &= -1 + i - i\theta^2 \\ u_2 &= 1 + i\theta^2 + \theta^3 \\ u_3 &= -1 - i\theta + \theta^2 + (1+i)\theta^3 \end{aligned}$$

La matrice génératrice du réseau logarithmique s'écrit :

$$\mathbf{G_4} = \begin{bmatrix} -0.88 & 0.88 & -0.88 & 0.88 \\ 0.56 & -0.16 & -1.44 & 1.04 \\ 1.04 & 0.56 & -0.16 & -1.44 \end{bmatrix}$$

Nous avons simulé le système de transmission décrit par l'équation 5.6 en utilisant notre réduction algébrique. Dans la figure 5.4, nous avons tracé le taux d'erreurs par mot (vecteur $\mathbf{s}$) en fonction du RSB = $\frac{E_s}{N_0}$, pour le détection ZF sans réduction, la détection ZF après réduction algébrique et le décodeur ML.

Nous remarquons, comme en dimension 2, que la réduction algébrique suivie d'une simple détection ZF permet d'obtenir la diversité maximale, égale à 4. Les performances de la réduction algébrique suivie d'une détection ZF sont à moins de 3dB des performances ML. Néanmoins, la complexité est très faible par rapport à celle du décodeur ML.

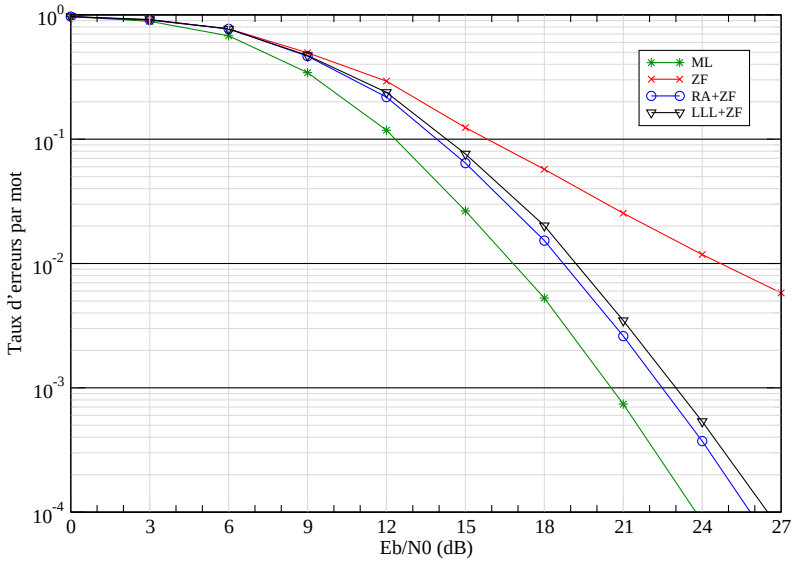



Fig. 5.5: Décodage de réseau de points complexe en dimension 4

### 5.5.4 Réseau de points en dimension 8

Nous considérons le corps cyclotomique de degré 8 sur $\mathbb{Q}(i)$, $K = \mathbb{Q}(\theta)$, où $\theta = e^{\frac{i\pi}{16}}$. La matrice de précodage $\mathbf{\Phi}$ est définie dans l'équation 5.7. La signature du corps $K$ est égale (0,8). Par la suite, son système d'unités fondamentales se compose de 7 unités :

$$\begin{aligned}
u_1 &= -\theta^2 + \theta^5 - i\theta^7 \\
u_2 &= i + i\theta^2 + \theta^6 \\
u_3 &= -(1+i)\theta^2 - \theta^6 \\
u_4 &= (-1+i)(1+\theta+\theta^2+\theta^3) + i(\theta^4+\theta^5+\theta^6) + (1+i)\theta^7 \\
u_5 &= -\theta^5 + i\theta^6 + \theta^7 \\
u_6 &= i - i\theta^2 + i\theta^4 - (1+i)\theta^6 \\
u_7 &= 1 - i\theta^6 + i\theta^7
\end{aligned}$$

La matrice génératrice du réseau logarithmique s'écrit :

$$\mathbf{G_8} = \begin{bmatrix}
-0.41 & 1.08 & -2.19 & -0.49 & 0.97 & -0.03 & 0.74 & 0.32 \\
1.04 & -1.44 & -0.16 & 0.56 & 1.04 & -1.44 & -0.16 & 0.56 \\
0.88 & -0.88 & 0.88 & -0.88 & 0.88 & -0.88 & 0.88 & -0.88 \\
2.27 & -1.57 & 0.13 & -0.21 & -1.23 & 0.12 & -0.29 & 0.78 \\
0.32 & 0.97 & 1.08 & 0.74 & -0.49 & -0.41 & -0.03 & -2.19 \\
-0.56 & -1.04 & 1.44 & 0.16 & -0.56 & -1.04 & 1.44 & 0.16 \\
-0.03 & -2.19 & 0.32 & 0.97 & 1.08 & 0.74 & -0.49 & -0.41
\end{bmatrix}$$

Nous avons simulé le système de transmission décrit par l'équation 5.6 en utilisant notre réduction algébrique. Dans la figure 5.6, nous avons tracé le taux d'erreurs par mot (vecteur $\mathbf{s}$) en fonction du RSB = $\frac{E_s}{N_0}$, pour la détection ZF sans réduction, la détection ZF après réduction algébrique et le décodeur ML.

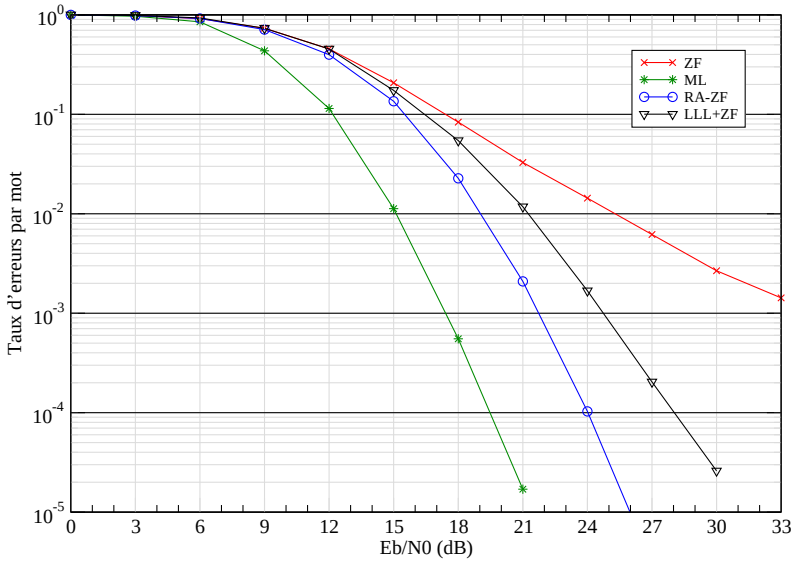



Fig. 5.6: Décodage de réseau de points complexe en dimension 8

La réduction algébrique suivie d'une détection ZF permet l'obtention de la diversité maximale, égale à 8. Les performances obtenues sont à moins de 4dB de celles du ML.

## 5.6 Comparaison de la réduction algébrique avec la réduction LLL

Comme nous l'avons déjà vu au paragraphe 5.3.3, la réduction LLL est un algorithme simple et efficace et dispose d'une complexité polynomiale. La base du réseau de points obtenue par cette réduction se compose de vecteurs les "plus courts possible" et "raisonnablement" orthogonaux. La base du réseau de points obtenue par la réduction algébrique est la plus orthogonale possible. Cette différence dans les propriétés des deux réductions nous permet de prédire, à priori, qu'avec une détection ZF, la réduction algébrique prend l'avantage sur la réduction LLL étant donné que la détection ZF ne dépend que de l'orthogonalité de la base.

Dans les figures 5.4, 5.5 et 5.6, nous avons tracé aussi les performances de la réduction LLL suivie d'une détection ZF, respectivement des réseaux de points complexes en dimension 2, 4 et 8.

En dimension 2, les deux réductions affichent quasiment les mêmes performances. En dimension 4, la réduction algébrique prend l'avantage sur la réduction LLL et permet d'obtenir de meilleures performances. En dimension 8, l'écart se creuse en faveur de la réduction algébrique. Cela s'explique par le fait que la réduction LLL ne permet pas d'atteindre la diversité maximale, alors que la réduction algébrique l'atteint toujours.

Au delà de l'aspect performance, la complexité de la réduction algébrique est très raisonnable et son implémentation demeure très simple et mieux adapté aux réseaux de points algébriques.

## 5.7 Accélération des décodeurs de réseaux de points en utilisant la réduction algébrique

Dans le chapitre 4, nous avons évoqué la réduction de réseau de points comme un outil permettant d'accélérer le décodage par les décodeurs de réseaux de points, décodage par sphères et Schnorr-Euchner. Afin de confirmer ce résultat, nous avons mesuré le temps de recherche du Schnorr-Euchner avec et sans réduction.

Nous avons tracé dans la figure 5.7 le temps de recherche du décodage du réseau de points en dimension 8, par le Schnorr-Euchner avec et sans réduction, en fonction du RSB = $\frac{E_b}{N_0}$ (dB). Nous avons utilisé la réduction LLL et la réduction algébrique. Les résultats des simulations confirment le gain en temps de recherche apporté par l'application d'une réduction avant le décodage du réseau. Le gain est plus important pour les faibles et moyens RSB.

Le gain en temps de recherche apporté par la réduction algébrique par rapport à la réduction LLL, à faible et fort RSB confirme que le résultat de la réduction algébrique est meilleur que celui de la réduction LLL.

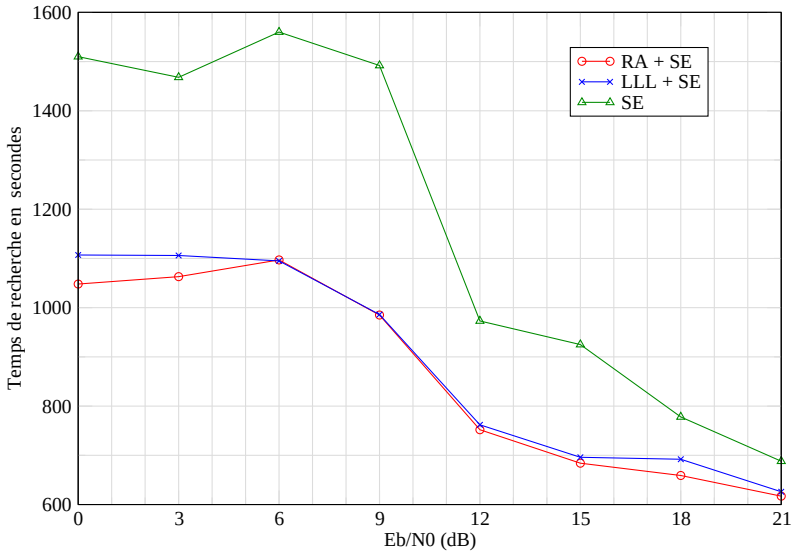



Fig. 5.7: Temps de recherche du décodage du réseau de point complexe en dimension 8 par le Schnorr-Euchner avec et sans réduction

## Conclusion

La réduction de réseau de points consiste à trouver une base optimale du réseau composée de vecteurs "les plus courts" et les "plus orthogonaux" possibles. Dans la littérature, il existe trois méthodes de réduction de réseau de points. La plus classique et la plus utilisée est la réduction LLL qui se distingue par sa simplicité et sa complexité polynomiale.

Dans ce chapitre nous avons proposé une nouvelle méthode de réduction algébrique pour un système mono-antenne sur un canal à évanouissements rapides utilisant, dans le but d'in-

troduire de la diversité de modulation, un précodage linéaire. L'utilisation du schéma de codage/décodage en mod$\Lambda$ rend l'application de la réduction possible en considérant des constellations finies.

La réduction algébrique suivie d'une simple détection ZF permet d'atteindre l'ordre de diversité maximal. En dimension élevée, la détection ZF s'avère insuffisante pour atteindre les performances ML. On pourrait penser que l'approximation du vecteur des amplitudes par une unité et ses conjuguées n'est plus suffisamment bonne.

Pour clore ce chapitre, nous pouvons dire que différentes améliorations restent à faire sur cette nouvelle méthode de réduction algébrique, parmi lesquelles nous citons :

- Exploiter la structure du réseau logarithmique afin de mieux le décoder
- Prouver que pour une dimension quelconque la diversité maximale est atteinte
- Appliquer la réduction à des constellations finies en utilisant le schéma de codage/décodage en mod$\Lambda$
- Étendre la réduction algébrique aux cas des systèmes MIMO.

# Conclusions et Perspectives

## Conclusions

Dans ce mémoire, nous avons étudié le codage et décodage Espace-Temps (ST) des systèmes à antennes multiples dans le cas cohérent, considérant un canal quasi-statique non sélectif en fréquence.

Au niveau du codage ST, nous avons proposé deux nouvelles constructions de codes ST en blocs pour une longueur temporelle du code égale au nombre d'antennes à l'émission : les codes Quaternioniques et les codes Parfaits. Ces nouveaux codes se distinguent par un rendement plein, une diversité pleine et des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente. Nous rappelons que le gain de codage des codes ST est le déterminant minimal de la différence de deux mots de code maximisé. Les constructions effectuées sont algébriques, se basant essentiellement sur les algèbres cycliques de division de centre $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$. Dans un premier temps, nous avons construit les codes Quaternioniques pour les dimensions 2, 3 et 4. Il s'est avéré que leurs performances, pour les dimensions 3 et 4, se dégradaient à cause de la répartition non uniforme de l'énergie dans le mot de code. Nous avons alors construit les codes Parfaits, palliant au problème énergétique. Ces codes ont une efficacité énergétique qui se traduit par une même énergie moyenne de transmission à chaque instant par chaque antenne émettrice, et des constellations transmisses ne présentant aucune perte de forme par rapport aux constellations émises. Les codes parfaits existent pour les dimensions 2, 3, 4 et 6. Pour la dimension 2, il existe une famille infinie de codes Parfaits. Nous avons appelé "Golden code" le meilleur code de cette famille en terme de déterminant minimal. En s'inspirant de la construction des codes Parfaits, nous avons construit les codes parfaits rectangulaires. Ces codes se caractérisent par des longueurs temporelles supérieures au nombre d'antennes à l'émission et offrent des gains de codage plus élevés.

Par ailleurs, il a été démontré récemment que les codes ST construits sur les algèbres cycliques de division de centre $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$, admettant des déterminants minimaux ne s'évanouissant pas lorsque l'efficacité spectrale augmente, atteignent le compromis gain de multiplexage-diversité. Évidemment, nous pouvons facilement conclure que nos codes Quaternioniques et Parfaits atteignent bien cette frontière multiplexage-diversité. Les codes Quaternioniques ont été les premiers codes à atteindre cette frontière.

Au niveau décodage, nous avons modifié les deux décodeurs de réseaux de points, décodage par sphères et Schnorr-Euchner, pour pouvoir décoder des constellations finies. Cela nous permettait, moyennant un passage à la représentation en réseaux de points des codes ST, de les

appliquer à notre schéma de transmission. L'utilisation de ces décodeurs s'avère intéressante du fait qu'ils offrent les performances ML avec une complexité mesurée. L'étude et la comparaison des complexités des versions modifiées des deux décodeurs nous ont permis de statuer sur le décodeur à choisir, à savoir, le Schnorr-Euchner.

La réduction des réseaux de points permet l'accélération de leur décodage en leur offrant une meilleure base composée de vecteurs les "plus courts" et les "plus orthogonaux" possibles. En utilisant le schéma de codage/décodage en mod-$\Lambda$, l'application de la réduction devient possible en considérant des constellations finies. Nous avons proposé une nouvelle méthode de réduction algébrique pour un système mono-antenne sur un canal à évanouissements rapides utilisant un précodage linéaire. La réduction algébrique suivie d'une simple détection ZF permet d'atteindre l'ordre de diversité maximal. De plus, sa complexité est très raisonnable favorisant ainsi son implémentation pratique.

## Perspectives

Plusieurs améliorations peuvent être apportées à la réduction algébrique afin d'optimiser ses performances et réduire sa complexité. D'un côté, les performances de la réduction sont étroitement liées à la finesse de l'approximation des évanouissements normalisés par une unité et ses conjugués, d'un autre côté, la qualité de l'approximation ne dépend que des caractéristiques du réseau logarithmique. Cela laisse à penser qu'en choisissant le réseau logarithmique selon des critères bien choisis, nous pouvons améliorer les performances de la réduction algébrique. Par ailleurs, en analysant en profondeur les exemples des réseaux logarithmiques proposés dans ce mémoire, nous remarquons l'existence d'une structure circulaire entre les lignes de la matrice génératrice. L'exploitation d'une éventuelle structure du réseau logarithmique pourrait aider à accélérer son décodage et ainsi accélérer la réduction elle même. Le point le plus important qui reste à traiter demeure la généralisation de la réduction algébrique pour le cas des systèmes à antennes multiples employant un codage ST algébrique en blocs.

Des codes rectangulaires cohérents ont déjà été utilisés dans les systèmes MIMO non cohérents [71]. Les bonnes propriétés des codes parfaits laissent envisager de bonnes performances pour leur version non cohérente.

Actuellement, il y a un regain d'intérêt dans la communauté "Théorie de l'information" pour les couches autres que la couche physique ("cross-layers") sur les systèmes sans fil. Le compromis "multiplexage-diversité" est un moyen assez simple d'étudier les limites de tels systèmes. On peut citer des applications au canal à accès multiple [72], à l'ARQ [73] ou aux communications avec relai [74]. On sait que ce compromis peut être atteint sur le canal MIMO soit par des codes longs [75] soit par nos codes (codes quaternioniques et parfaits). Nous pensons que les méthodes utilisées dans nos constructions peuvent être étendue à ces cas.

# Annexes

# Annexe A

# Rappels de théorie des corps de classe

Plusieurs notions issues de la théorie des corps de classe (Class field theory) sont essentielles pour établir les résultats des démonstrations des différentes annexes. Parmi ces notions nous citons : la valuation, les nombres $p$-adiques et le symbole de norme de Hasse (”Hasse Norm Symbol”) et ses propriétés.

## A.1 La Valuation

Soit un corps $K$. Une valuation dans $K$ à valeur dans un groupe abélien $G$ (généralement égal à $\mathbb{Z}$ ou $\mathbb{R}$), est une application :

$$v : K \to G \cup \{\infty\}$$

vérifiant les propriétés suivantes, pour tout $a$,$b \in K$ :

1. $v(0) = \infty$
2. $v(ab) = v(a) + v(b)$ (équivalent à dire que $v$ est un homomorphisme de groupe)
3. $v(a + b) \geq \min\{v(a),v(b)\}$, il y a égalité si $v(a) \neq v(b)$ (c'est une translation de l'inégalité triangulaire dans les espaces métriques)

On appelle anneau de valuation :

$$A = \{a \in K^* \mid v(a) \geq 0\} \cup \{0\}$$

## A.2 Nombre $p-$adique

Pour tout nombre premier $p$, l'ensemble des nombres $p$-adiques est une complétion du corps des rationnels décrit par Kurt Hensel en 1897. Ces ensembles ont été utilisés pour résoudre des problèmes de la théorie des nombres en appliquant le principe local-global de Helmut Hasse, qui stipule sommairement, qu'une équation peut être résolue sur le corps des rationnels si et seulement si elle peut être résolue sur le corps des réels et sur l'ensemble des nombres $p$-adiques, pour tout les nombres premiers $p$.

Un nombre rationnel $x \in \mathbb{Q}$ peut s'écrire :

$$x = \frac{p^a r}{s}$$

où $p$ est un nombre premier. $r$, $s$ des entiers indivisibles par $p$ et $a$ un entier unique.

La norme $p$-adique d'un élément $x$ de $\mathbb{Q}$ est :

$$|x|_p = p^{-a}$$

et on a $|0|_p = 0$.

La valuation $p$-adique est une valuation sur le corps $K = \mathbb{Q}$ à valeurs dans $\mathbb{Z}$ :

$$v_p(x) = a$$

La norme $p$-adique définit une métrique dans $\mathbb{Q}$, soit :

$$d_p(x,y) = \left|x - y\right|_p$$

En considérant la métrique usuelle donnée par la valeur absolue, le corps des nombres rationnels n'est pas complet. Par exemple la série définie par $x_1 = 1$ et $x_{n+1} = \frac{x_n}{2} + \frac{1}{x_n}$ est une série de Cauchy de nombres rationnels mais qui ne converge pas vers une limite rationnelle. Elle converge vers $\sqrt{2}$.

En considérant la métrique "valeur absolue", l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$ sont complets . Pour un nombre premier $p$ donné, l'ensemble des nombres $p$-adiques $\mathbb{Q}_p$ est complet. En considérant la métrique $p$-adique, $\mathbb{Q}_p$ complète $\mathbb{Q}$ . De la même façon, $\mathbb{R}$ complète $\mathbb{Q}$ en utilisant la métrique usuelle "valeur absolue".

L'ensemble des entiers $p$-adiques $\mathbb{Z}_p$ forme un sous-anneau de $\mathbb{Q}_p$.

Tout $x \in \mathbb{Q}_p$ peut être écrit d'une façon unique sous la forme suivante :

$$x = \sum_{i=k}^{\infty} a_i p^i$$

où $k$ est un entier, et les $a_i \in \{0, \cdots, p-1\}$. Cette série converge vers $x$ en considérant la métrique $d_p$.

## A.3 Le symbole de norme de Hasse

Nous introduisons la notion "symbole de norme de Hasse" [76] qui permet de vérifier si un élément est une norme.

Dans la suite, $K/F$ sera un corps d'extension d'un corps de nombres, que nous supposons abélien. Notons $K_\nu$ la complétion de $K$ relativement à la valuation $\nu$. Soit $i_\nu$ le plongement de $K$ dans $K_\nu$.

**Définition : A.1** *[76, p. 105] $K/F$ un corps d'extension abélien d'un corps de nombres, et $Gal(K/F)$ son groupe de Galois. Le "*symbole de norme de Hasse*" est :*

$$\begin{array}{rccc} \left(\frac{\bullet, K/F}{\nu}\right): & K^* & \to & Gal(K/F) \\ & x & \mapsto & \left(\frac{i_\nu(x), K/F}{\nu}\right) \end{array}$$

La propriété principale de ce symbole est le fait qu'il permet de vérifier si un élément est une norme locale [76, p. 106,107].

**Théorème : A.1** *Nous avons* $\left(\frac{x,K/F}{v}\right) = 1$ *si et seulement si x est une norme locale à v pour K/F.*

Pour pouvoir calculer le "symbole de norme de Hasse", nous aurons besoin de connaître certaines de ses propriétés.

**Théorème : A.2** *Nous avons*

$$\left(\frac{xy,K/F}{v}\right) = \left(\frac{x,K/F}{v}\right)\left(\frac{y,K/F}{v}\right)$$

**Théorème : A.3** *Si v ne se ramifie pas dans K/F, alors pour tout* $x \in F^*$ *:*

$$\left(\frac{x,K/F}{v}\right) = \left(\frac{K/F}{v}\right)^{v(x)}$$

*où* $\left(\frac{K/F}{v}\right)$ *est le Frobenius de v pour K/F, et* $v(x)$ *est la valuation de x.*

Pour la suite, il est suffisant de savoir que le Frobenius$\left(\frac{K/F}{v}\right)$ est un élément du groupe de Galois de $K/F$ (nous n'avons pas besoin de connaître sa valeur exacte). Une définition plus précise est donnée dans [76, p. 107]

**Corollaire : A.1** *Si v ne se ramifie pas, alors une unité est toujours une norme.*

Cela est évident du fait que la valuation d'une unité est nulle.

**Théorème : A.4** *[76, p. 113] Soit K/F une extension finie. Pour tout* $x \in F^*$ *nous avons :*

$$\prod_v \left(\frac{x,K/F}{v}\right) = 1,$$

*où le produit est défini sur tous les places v.*

D'après le corollaire A.1, une unité est toujours une norme locale si $v$ ne se ramifie pas. Étant donné que nous nous intéressons à montrer qu'une unité $\gamma$ n'est pas une norme, il suffirait de trouver une contradiction pour un $v$ ne se ramifiant pas.

# Annexe B

# $i$ n'est pas une norme dans $\mathbb{Q}(i, \sqrt{p})/\mathbb{Q}(i)$

---

Dans cette annexe, en utilisant les nombres $p$-adiques, nous montrons que $i$ n'est pas une norme dans $\mathbb{Q}(i, \sqrt{p})/\mathbb{Q}(i)$.

Rappelons d'abord la caractérisation d'un carré dans un corps fini. Soit $p$ un nombre premier et notons $GF(p)$ le corps fini composé de $p$ éléments.

**Proposition : B.1** *[77] Soit $x \in GF(p)^*$. Nous avons :*

$$x \text{ est un carré } \Leftrightarrow x^{\frac{p-1}{2}} = 1$$

**Corollaire : B.1** *Si $p \equiv 1(mod4)$ alors $-1$ est un carré dans $GF(p)$.*

Dans notre cas, $p$ est un nombre premier tel que $p \equiv 5(\text{mod}8)$ et $K = \mathbb{Q}(i, \sqrt{p})$ une extension relative de $\mathbb{Q}(i)$. Soit $x \in K$, alors $x$ s'écrit $x = a + b\sqrt{p}$, avec $a,b \in \mathbb{Q}(i)$. La norme relative de $x$ dans $K/\mathbb{Q}(i)$ s'écrit :

$$N_{K/\mathbb{Q}(i)}(x) = (a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - pb^2 \tag{B.1}$$

Notre objectif est de montrer que l'équation :

$$N_{K/\mathbb{Q}(i)}(x) = i$$

n'a pas de solution.

Nous allons montrer que cette équation n'a pas de solution dans le corps des nombres $p$-adiques $\mathbb{Q}_p$ et par la suite n'a pas de solution dans $K$.

Soit $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$ l'anneau de valuation de $\mathbb{Q}_p$.$v_p(x)$ est la valuation de $x$ dans $p$. Nous allons tout d'abord vérifier que $i \in \mathbb{Z}_p$. En effet, il existe un plongement de $\mathbb{Q}(i)$ dans $\mathbb{Q}_p$ si le polynôme minimal de $i$, $x^2 + 1$ a des racines dans $\mathbb{Z}_p$. En utilisant le lemme de Hensel [78, p. 75], il suffit de vérifier que $-1$ est un carré dans $GF(p)$.

Par hypothèse $p \equiv 5(\text{mod}8)$, par la suite $p \equiv 1(\text{mod}4)$. D'après le corollaire B.1, $-1$ est un carré dans $GF(p)$.

**Proposition : B.2** *L'unité $i \in \mathbb{Z}[i]$ n'est pas une norme, i.e. il n'existe pas de $x \in K$ tel que $N_{K/\mathbb{Q}(i)}(x) = i$ , où $K = \mathbb{Q}(i, \sqrt{p})$ avec $p \equiv 5(mod8)$.*

Afin de prouver la proposition, il suffira, d'après l'équation B.1, de prouver que l'équation :

$$a^2 - pb^2 = i, a,b \in \mathbb{Q}(i) \tag{B.2}$$

n'a pas de solution.

En utilisant le plongement de $\mathbb{Q}(i)$ dans $\mathbb{Q}_p$, cette équation peut s'écrire dans $\mathbb{Q}_p$ comme suit :

$$a^2 - pb^2 = y + px, a,b \in \mathbb{Q}(i), x,y \in \mathbb{Z}_p \tag{B.3}$$

où $y^2 = -1$. Si l'équation B.2 a une solution, alors cette solution reste valable dans $\mathbb{Q}_p$. Par la suite, montrer que l'équation B.3 n'a pas de solution permet de prouver la proposition B.2 , et clore par la suite la démonstration.
En terme de valuation, nous avons :

$$v_p(a^2 - pb^2) = v_p(y + px)$$

Comme $x \in \mathbb{Z}_p$ et $y$ est une unité, nous avons alors :

$$v_p(y + px) \geq \inf\{v_p(y), v_p(x) + 1\} = 0$$

Et puisque les valuations sont distinctes, nous obtenons l'égalité suivante :

$$v_p(a^2 - pb^2) = \inf\{v_p(y), v_p(x) + 1\} = 0$$

L'unique cas possible est $v_p(a) = 0$ ce qui implique que $a \in \mathbb{Z}_p$. Par conséquent $b \in \mathbb{Z}_p$. Nous avons alors :

$$a^2 - pb^2 = y + px, a,b,x,y \in \mathbb{Z}_p \tag{B.4}$$

En réduisant l'équation B.4 (mod$p\mathbb{Z}_p$), nous remarquons que $y$ doit être un carré dans $GF(p)$. Comme $y^2 = -1$ et $p \equiv 5(\text{mod}8)$ alors $y^{(p-1)/2} = (-1)^{p-1)/4} = -1$. D'après la proposition B.1, $y$ n'est pas un carré, d'où une contradiction.

**$-i$ n'est pas une norme dans $\mathbb{Q}(i, \sqrt{p})/\mathbb{Q}(i)$**

De la même façon, nous pouvons montré que $-i$ n'est pas une norme dans $K$ . L'équation B.3 devient :

$$a^2 - pb^2 = -y + px, a,b,x,y \in \mathbb{Z}_p$$

En réduisant cette dernière équation mod($p$), nous pouvons voir que, pour avoir une solution $y$ doit être un carré dans $GF(p)$. Comme $(-y)^{(p-1)/2} = (-y)^2 = y^2 = -1$, $y$ ne peut pas être un carré, d'où la contradiction.

# Annexe C

# $j$ et $j^2$ ne sont pas des normes dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$

Dans cette annexe, nous prouvons que $j$ et $j^2$ ne sont pas des normes dans $\mathbb{K} = \mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$. Pour cela, nous montrons, en calculant leurs symboles de norme de Hasse, qu'ils ne sont pas des normes locales. La preuve correspondate à $j$ et celle correspondante à $j^2$ étant similaires, nous détaillerons dans la suite que la première et nous donnerons les principaux points de la deuxième.

## C.1 $j$ n'est pas une norme dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$

**Proposition : C.1** *L'unité $j$ n'est pas une norme dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$.*

Dans notre cas, $K = \mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))$ est une extension relative de $\mathbb{Q}(j)$. Nous avons :

$$7\mathbb{Z}[j] = (j-2)(j+3) = \mathfrak{p}_7\mathfrak{q}_7.$$

Pour montrer que $j$ n'est pas une norme dans $K$, il suffira de montrer que $j$ n'est pas une norme locale dans $\mathfrak{p}_7$.

Nous cherchons un $y$ satisfaisant :

$$y \equiv 1 \pmod{j-2} \tag{C.1}$$
$$jy \equiv 1 \pmod{j+3} \tag{C.2}$$

En utilisant le théorème du reste chinois appliqué à $\mathbb{Z}[j]$, nous trouvons $y = 7 - 3j$ avec $(y)Z[j] = \mathfrak{p}_{79}$. Soit $\left(\frac{x,K/F}{\nu}\right)$ le symbole de norme de Hasse. En appliquant la formule du produit (Th. A.4) nous avons :

$$\prod_{\nu}\left(\frac{jy,K/F}{\nu}\right) = \prod_{\nu \text{ se ramifie}}\left(\frac{jy,K/F}{\nu}\right)\prod_{\nu \text{ ne se ramifie pas}}\left(\frac{jy,K/F}{\nu}\right) = 1. \tag{C.3}$$

Étant donné que la ramification dans $K/\mathbb{Q}(j)$ est uniquement en 7, le produit dans les places ramifiées donne $\left(\frac{jy,K/F}{\mathfrak{p}_7}\right)\left(\frac{jy,K/F}{\mathfrak{q}_7}\right)$. Par linéarité (Th. A.2), nous avons $\left(\frac{xy,K/F}{\nu}\right) = \left(\frac{x,K/F}{\nu}\right)\left(\frac{y,K/F}{\nu}\right)$.

Puisque $y \in \mathfrak{p}_{79}$, sa valuation est nulle pour $\nu \neq \mathfrak{p}_{79}$. Nous savons aussi que la valuation d'une unité est nulle. Nous déduisons alors que le produit sur les places non ramifiées s'écrit :

$$\prod_{\nu \text{ ne se ramifie pas}} \left(\frac{jy,K/F}{\nu}\right) = \prod_{\nu \text{ ne se ramifie pas}} \left(\frac{j,K/F}{\nu}\right)\left(\frac{y,K/F}{\nu}\right) = \left(\frac{y,K/F}{\mathfrak{p}_{79}}\right).$$

La simplification de l'équation C.3 donne :

$$\left(\frac{j,K/F}{\mathfrak{p}_7}\right)\left(\frac{y,K/F}{\mathfrak{p}_7}\right)\left(\frac{jy,K/F}{\mathfrak{q}_7}\right)\left(\frac{y,K/F}{\mathfrak{p}_{79}}\right) = 1.$$

Le choix de $y$ (équations C.1 et C.2) implique que le deuxième et le troisième termes sont égaux à 1 . Finalement nous avons :

$$\left(\frac{j,K/F}{\mathfrak{p}_7}\right)\left(\frac{y,K/F}{\mathfrak{p}_{79}}\right) = 1.$$

Comme $\mathfrak{p}_{79}$ est inerte, le second terme est différent de 1. Par la suite $\left(\frac{j,K/F}{\mathfrak{p}_7}\right) \neq 1$, ce qui veut dire que $j$ n'est pas une norme dans $\mathfrak{p}_7$.

## C.2 $j^2$ n'est pas une norme dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$

**Proposition : C.2** *L'unité $j^2$ n'est pas une norme dans $\mathbb{Q}(j,2\cos\left(\frac{2\pi}{7}\right))/\mathbb{Q}(j)$.*

Nous gardons les mêmes notations que la démonstration précédente. Nous montrons que $j^2$ n'est pas une norme locale dans $\mathfrak{p}_7$, et par la suite elle n'est pas une norme dans $K$.

Soit $y = 5j - 9$ vérifiant :

$$y \equiv 1 \pmod{j-2} \tag{C.4}$$
$$j^2 y \equiv 1 \pmod{3+j} \tag{C.5}$$

Nous avons $(y)\mathbb{Z}[j] = \mathfrak{p}_{151}$. En reprenant le même calcul que dans la démonstration précédente, nous obtenons :

$$\left(\frac{j^2,K/F}{\mathfrak{p}_7}\right)\left(\frac{y,K/F}{\mathfrak{p}_{151}}\right) = 1,$$

$\mathfrak{p}_{151}$ est inerte, d'où $j^2$ n'est pas une norme dans $K$.

# Annexe D

# $-1$ n'est pas une norme dans $\mathbb{Q}(i,2\cos(\frac{2\pi}{15}))/\mathbb{Q}(i)$

Nous montrons dans cette annexe que $i^2 = -1$ n'est pas une norme dans $K = \mathbb{Q}(i,2\cos(\frac{2\pi}{15}))/\mathbb{Q}(i)$. La démarche générale de la preuve est la même que celles présentées dans l'annexe précédente. Toutefois, il faut être plus prudent, puisque la ramification dans $\mathbb{Q}(i,2\cos(\frac{2\pi}{15}))/\mathbb{Q}(i)$ apparaît dans deux nombres premiers.

**Proposition : D.1** *L'unité* $-1$ *n'est pas une norme dans* $\mathbb{Q}(i,2\cos(\frac{2\pi}{15}))/\mathbb{Q}(i)$.

Nous avons :

$$5\mathbb{Z}[i] = (i+2)(i-2) = \mathfrak{p}_5\mathfrak{q}_5 \text{ et } 3\mathbb{Z}[i] = 3 = \mathfrak{p}_3.$$

Pour montrer que$-1$ n'est une norme dans $K$, il suffira de monter que $-1$ n'est pas une norme locale dans $\mathfrak{p}_5$.

Nous cherchons $y$ dans $\mathbb{Z}[i]$ vérifiant :

$$y \equiv 1 \pmod{i+2} \tag{D.1}$$
$$-y \equiv 1 \pmod{i-2} \tag{D.2}$$
$$-y \equiv 1 \pmod{3} \tag{D.3}$$

En utilisant le théorème du reste chinois à $\mathbb{Z}[i]$, nous trouvons $y = 12i - 25$ avec $(y)\mathbb{Z}[j] = \mathfrak{p}_{769}$. Soit $\left(\frac{x,K/F}{\nu}\right)$ le symbole de norme de Hasse. La formule du produit (Th. A.4) donne :

$$\prod_{\nu}\left(\frac{-y,K/F}{\nu}\right) = 1. \tag{D.4}$$

Étant donné que la ramification dans $K/\mathbb{Q}(i)$ est uniquement en 3 et 5, le produit dans les nombres premiers ramifié est $\left(\frac{-y,K/F}{\mathfrak{p}_5}\right)\left(\frac{-y,K/F}{\mathfrak{q}_5}\right)\left(\frac{-y,K/F}{\mathfrak{p}_3}\right)$.

Comme $y \in \mathfrak{p}_{769}$ , sa valuation est nulle pour $\nu \neq \mathfrak{p}_{769}$. Nous avons aussi que la valuation d'une unité est nulle. Nous déduisons alors que le produit dans les nombres premiers qui ne se ramifient pas est :

$$\prod_{\nu \text{ ne se ramifie pas}}\left(\frac{-y,K/F}{\nu}\right) = \prod_{\nu \text{ ne se ramifie pas}}\left(\frac{-1,K/F}{\nu}\right)\left(\frac{y,K/F}{\nu}\right) = \left(\frac{y,K/F}{\mathfrak{p}_{769}}\right).$$

La simplification de l'équation D.4 donne :

$$\left(\frac{-y,K/F}{\mathfrak{p}_3}\right)\left(\frac{y,K/F}{\mathfrak{p}_5}\right)\left(\frac{-1,K/F}{\mathfrak{p}_5}\right)\left(\frac{-y,K/F}{\mathfrak{q}_5}\right)\left(\frac{y,K/F}{\mathfrak{p}_{769}}\right) = 1.$$

Le premier, le deuxième et le quatrième termes sont égaux à 1 du fait que $y$ vérifie les équations D.1,D.2 et D.3. Finalement nous avons :

$$\left(\frac{-1,K/F}{\mathfrak{p}_5}\right)\left(\frac{y,K/F}{\mathfrak{p}_{769}}\right) = 1.$$

Puisque $\mathfrak{p}_{769}$ n'est pas complètement scindé (Split), le second terme est différent de 1. Par la suite nous avons $\left(\frac{-1,K/F}{\mathfrak{p}_5}\right) \neq 1$. Ce qui nous permet de conclure que $-1$ n'est pas une norme sur $K$.

# Annexe E

# $-1$ n'est pas une norme dans $\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},j)/\mathbb{Q}(j)$

Nous prouvons dans cette annexe que $(-j)^3=-1$ n'est pas une norme dans $\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},j)/\mathbb{Q}(j)$. La preuve est similaire aux preuves présentées dans les annexes précédentes.

**Proposition : E.1** *L'unité* $-1$ *n'est pas une norme dans* $\mathbb{Q}(\zeta_{28}+\zeta_{28}^{-1},j)/\mathbb{Q}(j)$.

Nous avons :

$$7\mathbb{Z}[j]=(j-2)(j+3)=\mathfrak{p}_7\mathfrak{q}_7 \text{ et } 2\mathbb{Z}[j]=2=\mathfrak{p}_2.$$

Pour monter que $-1$ n'est pas une norme dans $K$, il suffira de montrer que$-1$ n'est pas une norme locale dans $\mathfrak{p}_7$,

Nous cherchons $y$ dans $\mathbb{Z}[i]$ vérifiant :

$$y \equiv 1 \pmod{j-2} \tag{E.1}$$
$$-y \equiv 1 \pmod{3+j} \tag{E.2}$$
$$-y \equiv 1 \pmod{2} \tag{E.3}$$

En utilisant le Théorème du reste chinois à $\mathbb{Z}[i]$, nous trouvons $y=3-8j$ avec $(y)\mathbb{Z}[j]=\mathfrak{p}_{97}$. Soit $\left(\frac{x,K/F}{\nu}\right)$ le symbole de norme de Hasse. La formule du produit (Th. A.4 ) donne :

$$\prod_{\nu}\left(\frac{-y,K/F}{\nu}\right)=1. \tag{E.4}$$

Étant donné que la ramification dans $K/\mathbb{Q}(i)$ est uniquement en 2 et 7, le produit dans les nombres premiers ramifiés est $\left(\frac{-y,K/F}{\mathfrak{p}_7}\right)\left(\frac{-y,K/F}{\mathfrak{q}_7}\right)\left(\frac{-y,K/F}{\mathfrak{p}_2}\right)$.

Comme $y\in\mathfrak{p}_{97}$, sa valuation est nulle pour $\nu\neq\mathfrak{p}_{97}$. En plus, nous avons la valuation d'une unité est nulle. Nous déduisons alors que le produit dans les nombres premiers qui ne se ramifient pas est :

$$\prod_{\nu \text{ ne se ramifie pas}}\left(\frac{-y,K/F}{\nu}\right)=\prod_{\nu \text{ ne se ramifie pas}}\left(\frac{-1,K/F}{\nu}\right)\left(\frac{y,K/F}{\nu}\right)=\left(\frac{y,K/F}{\mathfrak{p}_{97}}\right).$$

La simplification de l'équation E.4 donne :

$$\left(\frac{-y,K/F}{\mathfrak{p}_2}\right)\left(\frac{y,K/F}{\mathfrak{p}_7}\right)\left(\frac{-1,K/F}{\mathfrak{p}_7}\right)\left(\frac{-y,K/F}{\mathfrak{q}_7}\right)\left(\frac{y,K/F}{\mathfrak{p}_{97}}\right) = 1.$$

Le premier, le deuxième et le quatrième termes sont égaux à 1 du fait que $y$ vérifie les équations E.1,E.2 et E.3. Finalement nous avons :

$$\left(\frac{-1,K/F}{\mathfrak{p}_7}\right)\left(\frac{y,K/F}{\mathfrak{p}_{97}}\right) = 1.$$

Puisque $\mathfrak{p}_{97}$ n'est pas complètement scindé (Split), le second terme est différent de 1. Par la suite nous avons $\left(\frac{-1,K/F}{\mathfrak{p}_7}\right) \neq 1$ .Ce qui nous permet de conclure que $-1$ n'est pas une norme sur $K$.

# Annexe F

# Réduction LLL sur $\mathbb{Z}[j]$

L'algorithme LLL standard sur $\mathbb{Z}$ peut être facilement modifié pour être appliqué dans $\mathbb{Z}[j]$ [79]. Les deux principaux points sur lesquels il faut être vigilant sont :

- La division euclidienne : Le quotient de la division euclidienne sur $\mathbb{Z}[j]$ est défini de la façon suivante : Soit $x = x_1 + jx_2$ et $y = y_1 + jy_2$, $x_1$,$x_2$,$y_1$,$y_2 \in \mathbb{Z}$. La division de $x$ par $y$ donne $\frac{x}{y} = z_1 + jz_2$, avec $z_1$,$z_2 \in \mathbb{Q}$. Alors, nous avons $x = yq + r$, où $q = [z_1] + j[z_2]$.
- La conjugaison : la conjugaison complexe usuelle est remplacée par la conjugaison dans $\mathbb{Z}[j]$ qui transforme $j$ en $j^2$.

# Bibliographie


[1] G. D. Forney, R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Efficient Modulation for Band-Limited Channels," *IEEE Journal on Selected Areas in Comuunications*, vol. 2, pp. 632–647, September 1984.

[2] J. G. Proakis, "Digital Communications." McGraw-Hill Series in Electrical and Computer Engineering, 1995. 4th edition.

[3] P. Samuel, "Théorie algébrique des nombres." Hermann, Editeur des sciencees et des arts, 2003. 293 rue lecourbe, 75015 Paris.

[4] M.-A. Knus, A. Merkurje, M. Rost, and J.-P. Tignol, "The book of Involutions." American Mathematical Society Colloquium Publications, 1998. http ://www.ams.org/.

[5] S. Johansson, "A description of Quaternion Algebras." citeseer.ist.psu.edu/331138.html.

[6] E. W. Weisstein, "Fibonacci Numbers." From *Mathworld* A Wolfram Web Resource. http ://mathworld.wolfram.com/FibonacciNumber.html.

[7] D. W. Morris, "Introduction to Arithmetic Groups," February 2003. Preliminary version.

[8] R. Elkik, "Cours d'algèbre." ellipses, novembre 2002. 32, rue Bargue 75740 Paris cedex 15.

[9] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-Diversity, High-Rate Space-Time Block Codes From Division Algebras," *IEEE Transactions on Information Theory*, vol. 49, pp. 2596–2616, October 2003.

[10] S. Alamouti, "Space-Time block coding : A simple transmitter diversity technique for wireless communications," *IEEE Journal On Select Areas In Communications*, vol. 16, pp. 1451–1458, October 1998.

[11] V.Tarokh, H. Jafarkhani, and R. A. Calderbank, "Space-Time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, pp. 1456–1467, July 1999.

[12] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space-time block codes for complex signal constellations," *IEEE Transactions on Information Theory*, vol. 48, pp. 384–395, February 2002.

[13] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-BLAST : An Architecture for Realizing Very High Data Rates Over the Rich-Scattering Wireless Channel," Bell Laboratories, Lucent Technologies, Crawford Hill Laboratory 791 Holmdel-Keyport RD., Holmdel, NJ07733.

[14] G. J. Foschini, "Layerd space-time architecture for wireless communication in a fading environment when using multiple antennas," *Bell Laboratories Technical Journal*, vol. 1, no. 2, pp. 41–59, 1996.

[15] G. Caire and G. Colavolpe, "On space-time coding for quasi-static multiple-antenna channels," *IEEE Global Telecommunications Conference*, vol. 2, pp. 1078–1082, March 2001.

[16] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Transactions on Information Theory*, vol. 48, pp. 1804–1824, July 2002.

[17] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Transactions on Information Theory*, vol. 48, pp. 628–636, March 2002.

[18] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A Construction of a Space-Time Code Based on Number Theory," *IEEE Transactions on Information Theory*, vol. 48, pp. 753–760, March 2002.

[19] S. Galliou and J.-C. Belfiore, "A New Familly of Full Rate, Fully Diverse Space-Time Codes Based on Galois Theory," in *Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland*, p. 419, July 2002.

[20] H. E. Gamal and M. O. Damen, "Universal Space-Time Coding," *IEEE Transactions On Information Theory*, January 2002.

[21] H. Yao and G. W. Wornell, "Achieving the Full MIMO Diversity-Multiplexing Frontier with Rotation-Based Space-Time Codes," *in Proceedings Allerton Conference on Communication, Control, and Computing, (Illinois)*, October 2003.

[22] P. Dayal and M. K. Varanasi, "An Optimal Two Transmit Antenna Space-Time Code and its Stacked Extensions," *in Proceedings of Asilomar Conference on Signals, Systems and Computers, Montery,CA*.

[23] V.Tarokh, N. Seshadri, and A. R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communication : Performance Criterion and Code Construction," *IEEE Transactions On Information Theory*, vol. 44, pp. 744–765, March 1998.

[24] E. Telatar, "Capacity of Multi-antenna Gaussian Channels," *Internal technical report*, June 1995. Bell Laboratories http ://mars.bell-labs.com/papers/.

[25] G. J. Foschini and M. J. Gans, "On limits of wireless Communication in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol. 6, pp. 311–335, March 1998.

[26] E. Biglieri and G. Taricco, "How far away is infinity ? Using asymptotic analyses in multiple-antenna capacity calculations," *JWCC Barolo, Italy*, Novembre 2002.

[27] E. Biglieri, J. Proakis, and S. Shamai, "Fading Channels : Information-Theoretic and Communications Aspects," *IEEE Transactions on Information Theory*, vol. 44, pp. 2619–2692, October 1998.

[28] L. Zheng and D. Tse, "Diversity and multiplexing : A fundamental tradeoff in multiple antenna channels," *IEEE Transactions on Information Theory*, vol. 49, pp. 1073–1096, May 2003.

[29] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H. f Lu, "Explicit, Minimum-Delay Space-Time Codes Achieving The Diversity-Multiplexing Gain Tradeoff," *submitted to IEEE Transactions on Information Theory*.

[30] D. Aktas, H. E. Gamal, and M. P. Fitz, "Towards Optimal Space-Time Coding," *in Proceedings of Asilomar Conference on Signals, Systems and Computers*, vol. 2, pp. 1137–1141, November 2002.

[31] O. Tirkkonen and A. Hottinen, "Complex Space-Time Block Codes for four Tx," *in Proceedings of IEEE Global Telecommunications Conference*, vol. 2, pp. 1005–1009, November 2000.

[32] P. Lounesto, "Cliffod algebras and spinors." Cambridge University Press.

[33] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic Tools to build Modulation Schemes for Fading Channels," *IEEE Transactions on Information Theory*, vol. 43, pp. 938–952, May 1997.

[34] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels," *IEEE Transactions On Information Theory*, vol. 42, pp. 502–518, March 1996.

[35] X. Ma and G. B. Giannakis, "Full-Diversity Full-Rate Complex-Field Space-Time Coding," *IEEE Transactions on Signal Processing*, vol. 51, pp. 2917–2930, Novembre 2003.

[36] B. A. Sethuraman and B. S. Rajan, "Full-Rank Space-Time Block Codes from Division Algebras," *Technical Report*, October 2002. Indian Institute of Science Bangalore.

[37] P. Elia, P. V. Kumar, S. A. Pawar, R. R. Kumar, B. S. Rajan, and H. F. Lu, "Diversity-multiplexing tradeoff analysis of few algebraic space-time constructions," *in Proceedings Allerton Conference on Communication, Control, and Computing, (Illinois)*, 2004.

[38] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger, "Kant V4," *J.Symbolic Comp.*, vol. 24, pp. 267–283, 1997.

[39] T. Kiran and B. S. Rajan, "STBC-schemes with Non-Vanishing Determinant for Certain Number of Transmit Antennas," *submitted to IEEE Transactions On Information Theory*, 2004.

[40] E. Bayer, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$ lattice constellations for the Rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 50, pp. 702–714, April 2004.

[41] E. Bayer, F. Oggier, and E. Viterbo, "Algebraic lattice constellations : Bounds on performance," *submitted to IEEE Transaction on Information Theory*, April 2004.

[42] A. Fröhlich and M. Taylor, "Algebraic number theory." Cambridge University Press, 1991.

[43] A. Schiemann, "Classification of hermitian forms with the neighbour method," *J. Symbolic Computation*, vol. 26, pp. 487–508, 1998.

[44] H. P. F. Swinnerton-Dyer, "A brief guide to algebraic number theory." Combridge University Press, 2001.

[45] H. Cohn, "Advanced Number Theory." Dover Publications Inc. New York, 1980.

[46] V. Shashidhar, B. S. Rajan, and P. V. Kumar, "STBC with Optimal Diversity-Multiplexing Tradeoff for 2, 3 and 4 Transmit antennas," *in Proceedings of IEEE International Symposium on Information Theory, Chicago, USA*, Juin 2004.

[47] M. O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice Code Decoder for Space-Time Codes," *IEEE Communications Letters*, vol. 4, pp. 161–163, May 2000.

[48] J. H. Conway and N. J. A. Sloane, "Sphere Packings, Lattices and Groups." Grundlehren der mathematischen Wissenschaften, New York Berlin : Springer-Verlag, 1988. 2nd edition.

[49] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Transactions on Information Theory*, vol. 48, pp. 2201–2214, August 2002.

[50] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced basis with applications," *ACM SIGSAM Bulletin*, vol. 15, pp. 37–44, February 1981.

[51] R. Kannan, "Improved algorithms for integer programming an related lattice problems," *in Proceedings of the ACM Symposium on Theory of computing, Boston*, pp. 193–206, April 1983.

[52] U. Fincke and 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.

[53] E. Viterbo and E. Biglieri, "A universal lattice decoder," in *GRETSI* $14^{eme}$ *colloque*, (Juan les Pins), September 1993.

[54] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Transactions on Information Theory*, vol. 45, pp. 1639–1642, July 1999.

[55] G.Rekaya and J.-C. Belfiore, "On the complexity of ML lattice decoders for decoding linear full rate space-time codes," *in Proceedings of IEEE International Symposium on Information Theory, Yokohama, Japon*, p. 206, July 2003.

[56] J. Boutros, N. Gresset, L. Brunel, and M. Fossorier, "Soft-input soft-output lattice sphere decoder for linear channels," *in Proceedings of IEEE Global Telecommunications Conference*, pp. 1583–1587, 2003.

[57] M. O. Damen, H. E. Gamal, and G. Caire, "On Maximum-Likelihood Detection and the search for the Closest Lattice Point," *IEEE Transactions on Information Theory*, vol. 49, pp. 2389–2402, October 2003.

[58] B. Hassibi and H. Vikalo, "On the expected complexity of sphere decoding," *in proceedings of Asilomar Conference on Signals, Systems and Computers*, vol. 2, pp. 1051–1055, 2001.

[59] H. Vikalo and B. Hassibi, "On the sphere decoding algorithm, part i : the expected complexity, part ii : generalizations, second-order statistics and applications to communications," *submitted to IEEE Transactions on Signal Processing*.

[60] P. V. Emde-Boas, "Another NP-complete partition problem and the complexity of computing short vectors in a lattice," *Repport 81-04, Mathematisch Institut, Amsterdam, Netherlands*, April 1981.

[61] "Numerical Recipes." http ://www.nr.com.

[62] H. E. Gamal, G. Caire, and M. O. Damen, "Lattice coding and decoding achieve the optimal diversity-vs-multiplexing tradeoff of MIMO channels," *IEEE Transactions on Information Theory*, vol. 50, pp. 968–985, June 2004.

[63] H. Yao and G. w. Wornell, "Lattice-Reduction-Aided Detectors for MIMO Communication Systems," *in Proceedings of IEEE Global Telecommunications Conference*, November 2002.

[64] U. Erez and R. Zamir, "Lattice decoding can achieve $\frac{1}{2}log(1 + snr)$ on the AWGN channel using nested codes," *in Proceedings of IEEE Symposium on Information Theory, Washington DC, USA*, p. 125, June 2001.

[65] A. Korkine and G. Zolotareff, "Sur les formes quadratiques positives ternaires," *Mathematische Annalen*, vol. 5, pp. 581–583, 1872.

[66] A. Korkine and G. Zolotareff, "Sur les formes quadratiques," *Mathematische Annalen*, vol. 6, pp. 336–389, 1873.

[67] H. Minkowski, "Geometrie der zahlen," *Teubnner-Verlag, Leipzig*, 1896.

[68] A. K. Lenstra, H. W. Lenstra, and L. Lovasz, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, pp. 515–534, 1982.

[69] C. P. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms," *Theoretical Computer Science*, vol. 53, pp. 201–224, 1987.

[70] C. P. Schnorr and M. Euchner, "Lattice Basis Reduction : Improved Parctical Algorithms and Solving Subset Sum Problems," *Mathematical Programming*, vol. 66, pp. 181–199, 1994.

[71] I. Kammoun and J.-C. Belfiore, "A new family of Grassmann Space-Time codes for non-coherent MIMO systems," *IEEE Communications Letters*, 2003.

[72] D. Tse, P. Viswanath, and L. Zheng, "Diversity-Multiplexing Tradeoff in Multiple Access Channels," *IEEE Transactions on Information Theory*, vol. 50, pp. 1859–1874, September 2004.

[73] H. El Gamal, G. Caire, and M. O. Damen, "The Diversity-Multiplexing-Delay Tradeoff of the MIMO-ARQ channel." submitted to IEEE Transactions on Information Theory, 2004.

[74] K. A. Yazdi, H. E. Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half duplex cooperative channels," in *in Proceedings Allerton Conference on Communication, Control, and Computing, (Illinois)*, October 2004.

[75] H. E. Gamal, G. Caire, and M. O. Damen, "Lattice Coding and Decoding Achieve the Optimal Diversity-vs-Multiplexing Tredeoff of MIMO," *submitted on IEEE Transactions On Information Theory*, November 2003.

[76] G. Gras, "Class Field Theory." Springer Verlag, 2003.

[77] Liedl and Niederreiter, "Finite Fields and its applications."

[78] F. Q. Gouvêa, "*p*-adic numbers : An introduction." Universitext, Springer, second edition, 1997.

[79] H. Napias, "A generalisation of the LLL algorithm over Euclidean rings or orders," *Journal de Théorie des Nombres de Bordeaux*, vol. 8, pp. 387–396, 1996.

# Publications

[1] G. Rekaya and J-C Belfiore, "On the complexity of ML lattice decoders for decoding linear full rate space-time codes", in Proceedings of IEEE International Symposium on Information Theory, Yokohama, Japon, p. 206, July 2003.

[2] G. Rekaya and J-C Belfiore, "Complexity of ML lattice decoders for decoding linear full rate space-time codes", Accepted for Publication as a correspondance in IEEE Transactions on Wireless Communications.

[3] J-C Belfiore and G. Rekaya, "Quaternionic lattices for Space-Time coding", in Proceedings of IEEE Workshop on Information Theory, Paris, France, p. 267-270, March 2003.

[4] J-C Belfiore, G. Rekaya and E. Viterbo, "The Golden Code : A $2 \times 2$ Full-Rate Space-Time Code with Non-Vanishing Determinants", in Proceedings of IEEE International Symposium on Information Theory, Chicago, USA, July 2004.

[5] J-C Belfiore, G. Rekaya and E. Viterbo, "The Golden Code : A $2 \times 2$ Full-Rate Space-Time Code with Non-Vnishing Determinants", submitted to IEEE Transactions on Information Theory, 2004.

[6] G. Rekaya, J-C Belfiore and E. Viterbo, "Algebraic $3 \times 3$, $4 \times 4$ and $6 \times 6$ Space-Time Codes with Non-Vanishing Determinants", in Proceedings of IEEE International Symposium on Information Theory and its Applications, Parma, Italy, October 2004.

[7] F. Oggier, G. Rekaya, J-C Belfiore and E. Viterbo, "Perfect Space-Time Block Codes", submitted to IEEE Transactions on Information Theory, 2004.

[8] G. Rekaya, J-C Belfiore and E. Viterbo, "A Very Efficient Reduction Tool on Fast Fading Channels", in Proceedings of IEEE International Symposium on Information Theory and its Applications, Parma, Italy, October 2004.