Tecniche matematiche computazionali per l'analisi ed il progetto di costellazioni a reticolo

Emanuele Viterbo

February 23, 1995

ad Anna

Desidero innanzitutto ringraziare il mio tutore,
Prof. Ezio Biglieri, per la fiducia accordatami e
per gli insegnamenti, la collaborazione ed il
costante incoraggiamento offertimi in questi anni.
Ringrazio Jean-Claude Belfiore e Joseph Boutros,
sia per la proficua collaborazione che per l'amicizia,
l'aiuto e la disponibilità offertemi in occasione
della mia visita all'Ecole Nationale Supérieure
des Télécommunications di Parigi.
E' stato per me di grande stimolo l'interessamento per
il mio lavoro dimostrato dal Prof. Joachim Hagenauer
durante la mia permanenza presso il DLR di Monaco.
Questa è stata possibile grazie alla borsa di studio
concessa dalla SIP.
Ringrazio inoltre mio padre che avendomi introdotto
all'argomento dei reticoli cristallini mi ha dato
lo spunto per avviare questi studi sui reticoli
multidimensionali.
Per le utili discussioni ringrazio infine mio fratello,
Michelangelo ed i miei colleghi dottorandi
Giuseppe Caire e Roberto Garello.

Indice

Elenco delle tabelle

Elenco delle figure

Capitolo 1

Introduzione

Questa tesi raccoglie i risultati del lavoro svolto durante i tre anni del dottorato di ricerca in Elettronica presso il Politecnico di Torino. Parte di questo lavoro è stato portato avanti presso l'Ecole Nationale Supérieure des Télécommunications (E.N.S.T.) di Parigi, Francia e presso l'Istituto per le Telecomunicazioni del centro di riceche aerospaziali DLR di Oberpfaffenhofen, Monaco, Germania.

L'argomento trattato si inquadra nell'ambito della teoria delle comunicazioni digitali con rilavanza sia per la codifica di canale che per quella di sorgente. In entrambi i casi il problema è quello di progettare una costellazione di segnali tale da ottimizzare una opportuna quantità che identifica la qualità del sistema. Nel primo caso si vuole minimizzare la *probabilità di errore* di trasmissione mentre nel secondo si vuole minimizzare l'*errore quadratico medio di quantizzazione*.

Un risultato fondamentale nella teoria dell'informazione, dovuto a Shannon, stabilisce che le prestazioni ottimali di queste costellazioni migliorano al crescere della dimensionalità dello spazio. Purtroppo, questo risultato non è costruttivo nel senso che non fornisce alcun metodo sistematico per ottenere tali costellazioni ottimali. Infatti la dimostrazione del teorema di Shannon sulla codifica di canale è basata sulla tecnica del *random coding* che ora illustreremo. Non avendo a disposizione alcuna tecnica per costruire buoni codici, Shannon considerò uno spazio di codici probabilistico e stimò la probabilità di errore media per questa famiglia di codici. Tale probabilità può essere resa piccola a piacere aumentando la lunghezza dei codici pur di trasmettere ad un tasso *(rate)* inferiore alla capacità del canale. Il teorema di Shannon asserisce quindi che esiste almeno un codice all'interno della famiglia che raggiunge la probabilità di errore media calcolata. La dimostrazione, essendo basata su un ragionamento di media di un insieme di codici, non offre alcun modo per determinare il codice ottimo che fornisce la probabilità suddetta.

La ricerca di costellazioni che abbiano comunque buone prestazioni nei termini sopra citati, risulta inevitabilmente vincolata dalla complessità del metodo di codifica o decodifica (co/decodifica) utilizzato in pratica. Tale complessità, in genere, cresce in modo esponenziale con la dimensione e con il numero totale di segnali della costellazione, tuttavia quando essa presenta una struttura molto regolare la co/decodifica può essere notevolmente semplificata. Ad esempio, la struttura ricca di simmetrie, di alcuni reticoli facilita molto tali operazioni.

La ricerca di buone costellazioni di segnali per la trasmissione, condotta dapprima con la teoria dei codici di correzione d'errore, si è successivamente sviluppata nella teoria delle modulazioni codificate nell'ambito della quale si collocano le costellazioni a reticolo, argomento di questa tesi.

L'interesse per le costellazioni a reticolo per la trasmissione sul canale gaussiano risale ai primi anni Ottanta, anche se la teoria dei reticoli fa parte di alcune branche ormai classiche della matematica quali la geometria dei numeri e la teoria algebrica dei numeri.

In questa tesi si sono esplorati alcuni settori di queste discipline con l'intento di trovare nuove tecniche per l'analisi, il progetto e la co/decodifica di costellazioni a reticolo per la trasmissione su canale gaussiano e su canale con *fading*. In particolare si sono trovate alcune nuove tecniche computazionali che permettono di co/decodificare e calcolare le prestazioni di costellazioni a reticolo qualsiasi.

La tesi è così ripartita. Nel capitolo 2 sono forniti i concetti fondamentali sui reticoli. Partendo dalla definizione di reticolo si illustrano poi i vari problemi fondamentali della teoria dei reticoli quali il problema dell'impacchettamento delle sfere, il problema del ricoprimento dello spazio con sfere, il problema della quantizzazione ed infine il problema della codifica di canale per la trasmissione sul canale gaussiano. In questo capitolo sono infine raccolti i parametri fondamentali di alcuni tra i reticoli più noti.

Nel capitolo 3 viene presentato un algoritmo di decodifica valido per reticoli generici. Dato un punto arbitrario nello spazio l'algoritmo determina il punto del reticolo a minima distanza euclidea. Questo algoritmo risulta utile per la decodifica a massima verosimiglianza nella trasmissione sul canale gaussiano. Con alcune modifiche si è ottenuto un analogo algoritmo valido nella trasmissione sul canale con fading. Questi algoritmi sono stati ampiamente usati per valutare le prestazioni dei nuovi reticoli presentati nel capitolo 5, per i quali non si conosce uno specifico algoritmo di decodifica.

Nel capitolo 4 viene proposto un algoritmo che permette di valutare in modo esatto tutti i parametri fondamentali di un reticolo, costruendo passo a passo la sua regione di Voronoi. Esso è basato sulle tecniche della geometria combinatoria computazionale e partendo da un parallelotopo contenente la regione di Voronoi, lo intaglia come un diamante fino ad ottenere la regione stessa. Come esempio di applicazione di questo algoritmo, si sono calcolati, in modo esatto, i valori di alcune costanti di quantizzazione di reticoli che, pur essendo rilevanti, non presentano particolari simmetrie. La conoscenza della regione di Voronoi del reticolo permette inoltre di valutare in modo piuttosto preciso la probabilità di errore nella trasmissione sul canale gaussiano.

Il capitolo 5 è frutto del lavoro svolto in collaborazione con Joseph Boutros e Jean-Claude Belfiore del Département de Communications del E.N.S.T., Parigi. Questo capitolo costituisce la parte di progetto di costellazioni con buone prestazioni sia sul canale con fading sia sul canale gaussiano. Le costellazioni sono state ottenute utilizzando la costruzione algebrica di reticoli a partire da campi di numeri algebrici. Questi reticoli possiedono una *diversità* intrinseca che li rende efficaci su canali con fading. Utilizzati su un canale gaussiano tuttavia non offrono buone prestazioni a causa della loro bassa densità di impacchettamento. Per ottenere buone prestazioni contemporaneamente sui due tipi di canale si sono seguite due vie differenti, entrambe basate sulla costruzione algebrica. Nel primo caso si sono considerati i reticoli ottenuti per costruzione algebrica a partire da campi di numeri algebrici complessi per i quali la diversità è ridotta, ma la densità di impacchettamento è più elevata. Nel secondo caso si è considerata la costruzione algebrica, dei migliori reticoli noti per il canale gaussiano (D_4, E_6, E_8, K_{12}, Λ_{16}, Λ_{24}), a partire da particolari campi ciclotomici. I reticoli così ottenuti pur mantenendo la loro elevata densità, presentano anche una buona diversità. L'interesse applicativo di queste costellazioni può nascere dalla necessità di trasmettere o ricevere l'informazione contemporaneamente su un canale terrestre, ad esempio radiomobile, tipicamente affetto da fading e su un canale via satellite, in prima approssimazione modellizzabile come un canale gaussiano.

Concludiamo questa breve introduzione con alcune considerazioni e con i possibili sviluppi futuri di questo lavoro. Il grande interesse per le tecniche di modulazione ad alta efficienza spettrale è dettato attualmente dalla necessità di trasmissioni digitali a velocità sempre più elevate su canali radio aventi una risorsa di banda sempre più limitata. Le modulazioni multidimensionali a reticolo, considerate in questa tesi, possono essere efficacemente utilizzate in questo scenario. La solida base teorica sui reticoli ha fornito tecniche di progetto, di decodifica e di valutazione delle prestazioni per alcune particolari costellazioni a reticolo adatte alla trasmissione su canale gaussiano. Il contributo di questa tesi è stato duplice: da una parte si sono considerati i problemi di decodifica e di analisi di costellazioni a reticolo generiche per il canale gaussiano, dall'altra quelli relativi alle costellazioni a reticolo per il canale con fading. Tra i possibili sviluppi futuri di questo lavoro elechiamo i seguenti:

- sviluppo hardware di un decodificatore universale per reticolo;
- valutazione delle prestazioni di costellazioni a reticolo su canale con fading utilizzando la regione di Voronoi;
- ricerca di nuove costellazioni per canali con fading con tecniche algebriche;
- sviluppo di algoritmi sub-ottimi di decodifica per le costellazioni trovate nel capitolo 5.

Chapter 2

Lattices

This chapter collects all the basic definitions and results about lattices which will be used throughout the thesis. Most of the material in this chapter follows the enciclopedic work on lattices by J. H. Conway and N. J. A. Sloane: Sphere packings, lattices and groups [1].

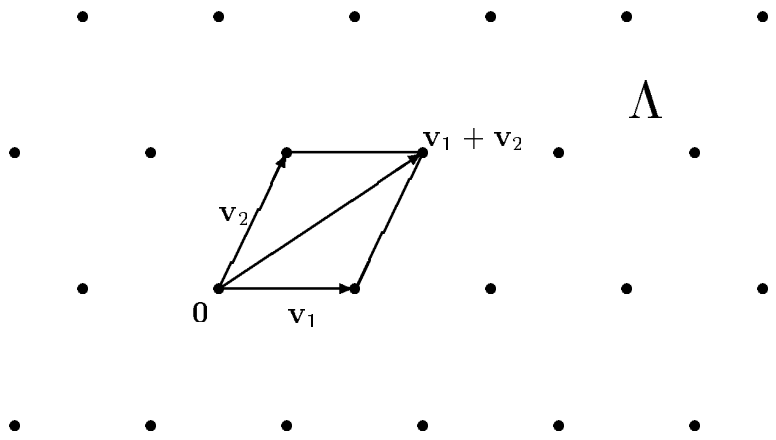

Figure 2.1: An example of a lattice in the plane.

2.1 Preliminary definitions

The following standard notation will be used. $\mathbf{Z}$ is the set of rational integers. $\mathbf{R}^d$ is the d-dimensional Euclidean space. $\mathbf{v} = (v_1, \ldots v_d)$ is a vector (or a point) of $\mathbf{R}^d$ and v_i are the real components with respect to the *canonical basis* $\mathbf{e}_1 = (1, 0, \ldots 0) \cdots \mathbf{e}_n = (0, \ldots 0, 1)$. If $\lambda \in \mathbf{R}$ then $\lambda\mathbf{v}$ denotes a vector with components λv_i. $\|\mathbf{v}\|$ is the Euclidean norm of the vector and $\langle \mathbf{v}, \mathbf{w} \rangle$ the scalar product between the two vectors. The superscript T associated with vectors and matrices denotes transposition.

Definition 1 *Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ be m linearly independent vectors of $\mathbf{R}^d$ ($m \leq d$). A* **lattice** *of $\mathbf{R}^d$ is the set Λ of vectors*

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_m\mathbf{v}_m \qquad \lambda_1, \ldots, \lambda_m \in \mathbf{Z} \ .$$

The set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m\}$ is called a lattice **basis** *and m the* **dimension** *or* **rank** *of Λ. If $m = d$, we talk of a* **full-rank** *lattice (Fig. 2.1).*

It is simple to prove that the vectors of a lattice form an additive group i.e., the sum of two lattice vectors is still a lattice vector, if $\mathbf{w} \in \Lambda$ then $-\mathbf{w} \in \Lambda$ and the null vector $\mathbf{0}$ belongs to Λ. As matter of fact it is possible to define a lattice as discrete sub-group of $\mathbf{R}^d$ of rank m. Conversly, it is possible to prove that all discrete sub-groups of $\mathbf{R}^d$ of finite rank are lattices [41].

The lattice generated by the canonical basis of $\mathbf{R}^d$, consisting of all the vectors having integer components, is called the *integer lattice* $\mathbf{Z}^d$.

Definition 2 *A* **sublattice** *of Λ is a subset of Λ preserving the lattice structure.*

Definition 3 *Let* $\mathbf{v}_i = (v_{i1}, v_{i2}, \ldots, v_{id})$, $i = 1, \ldots, m$ *be the lattice basis vectors. We define the* **generator matrix** *of* Λ *as*

$$M = \begin{pmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_m \end{pmatrix} = \begin{pmatrix} v_{11} & \cdots & v_{1d} \\ \vdots & & \vdots \\ v_{m1} & \cdots & v_{md} \end{pmatrix}$$

With the above definitions can simply write

$$\Lambda = \{\mathbf{u} = \mathbf{x}M : \mathbf{x} \in \mathbf{Z}^m\} \ . \tag{2.1}$$

Written in this form, we can view any lattice Λ as a transformed version of the *integer lattice* $\mathbf{Z}^m$ by means of the linear transformation defined by M. We can imagine that a full-rank lattice Λ is obtained by skewing the coordinate axes of the space containing $\mathbf{Z}^m$. An alternative definition of the generator matrix arranges the basis vectors by columns. In this case we write $\Lambda = \{\mathbf{u}^T = M\mathbf{x}^T : \mathbf{x} \in \mathbf{Z}^m\}$ and all the following definitions need to be slightly modifyed. Throughout this thesis we will adopt Definition 3.

If M generates Λ, then any matrix of the form $M' = TM$, where T is an $m \times m$ integer orthogonal matrix ($\det(T) = \pm 1$), is another generator matrix of the same lattice Λ: in fact T maps isomorphically $\mathbf{Z}^m$ into itself. T is also called an *integer unimodular matrix*. If T is an integer but not unimodular matrix then M' defines a generator matrix of a sublattice of Λ.

Among all the generator matrices of a lattice we are sometimes interested in those representing a so called *reduced basis* of the lattice. A reduced basis is a lattice basis with the shortest possible vectors. We give here a more precise definition of this concept.

Definition 4 *A basis* $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ *of a lattice* Λ *in* $\mathbf{R}^d$ *is reduced (in the sense of Minkowski) if*

- $\mathbf{v}_1 \in \{\mathbf{x} \in \Lambda : \|\mathbf{x}\|$ *is minimal* $\}$
- $\mathbf{v}_{i+1} \in \{\mathbf{x} \in \Lambda : \{\mathbf{v}_1, \ldots, \mathbf{v}_i, \mathbf{x}\}$ *can be extended to a basis and* $\|\mathbf{x}\|$ *is minimal* $\}$

for $i = 1, \ldots, m-1$.

Reduced bases are not unique. In Figure 2.2, $\{\mathbf{w}_1, \mathbf{w}_2\}$ is a non reduced basis of Λ with $\|\mathbf{w}_1\| = 2$ and $\|\mathbf{w}_2\| = \sqrt{10}$, while $\{\mathbf{v}_1, \mathbf{v}_2\}$ with $\|\mathbf{v}_1\| = \sqrt{2}$ and $\|\mathbf{v}_2\| = \sqrt{2}$ is reduced. According to the definition also $\{\mathbf{v}_1, -\mathbf{v}_2\}$ is a reduced basis. Note also that $\{\mathbf{v}_1, \mathbf{w}_2\}$ is not a lattice basis but identifies a sublattice of Λ.

Definition 5 *We say that* Λ_1 *and* Λ_2 *are* **equivalent lattices** *if they differ only by a coordinate rotation or a scaling factor.*

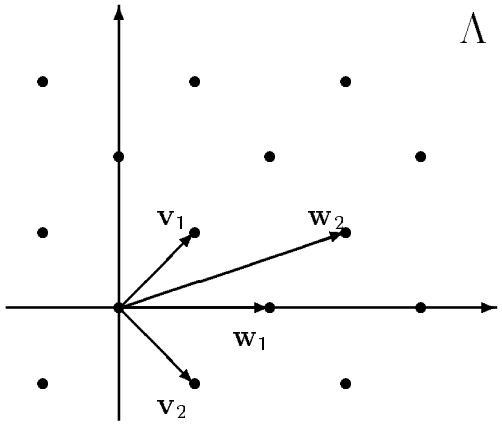

Figure 2.2: An example of reduced basis

The relation between the two generator matrices M_1 and M_2 of the two equivalent lattices is

$$M_1 = cTM_2B \tag{2.2}$$

where B is a rotation matrix (a real orthogonal matrix with determinant ± 1), c the scaling factor and T the integer unimodular matrix which accounts for the possibly different bases of the same lattice. We talk of *scaled lattices*, if B is the identity matrix and $c \neq 1$, and we say that $c\Lambda$ is a scaled version of Λ. If $c = \pm 1$ we have two *congruent lattices*. Finally, if $c = \pm 1$ and T is the identity matrix we have a *rotated lattice*.

Definition 6 *Given a vector* $\mathbf{z} \in \mathbf{R}^d$ *and a lattice* Λ *in* $\mathbf{R}^d$. *We define the* **translated lattice** *as the set of points*

$$\mathbf{z} + \Lambda = \{\mathbf{w} = \mathbf{x}M + \mathbf{z} : \mathbf{x} \in \mathbf{Z}^m\} .$$

We observe that whenever $\mathbf{z} \in \Lambda$, $\mathbf{z} + \Lambda$ is congruent to Λ, and we say that the translation defined by the vector $\mathbf{z}$ is a *translation symmetry* of the lattice.

Definition 7 *The* **fundamental parallelotope** *of* Λ *is the set of points*

$$\{\boldsymbol{\theta} M,\ \boldsymbol{\theta} = (\theta_1, \cdots, \theta_m) \in \mathbf{R}^m, 0 \leq \theta_i < 1\} .$$

The fundamental parallelotope of a lattice is not unique since it depends on the choice of the lattice basis. In the case of full-rank lattices the volume of the fundamental parallelotope is equal to $|\det(M)|$, a number independent of the lattice basis called the *determinant* of Λ. We equivalently indicate it with $\mathbf{d}(\Lambda)$ or with $\mathrm{vol}(\Lambda)$. For non full-rank lattices the volume of the fundamental parallelotope is not well defined since it has zero measure in $\mathbf{R}^d$. We can still define the determinant of the lattice by using the following definition.

Definition 8 *The* **Gram matrix** *of* Λ *is defined as*

$$A = MM^T = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \quad .$$

The elements of the Gram matrix are the Euclidean scalar products of pairs of vectors of the lattice basis, that is, $a_{ij} = \langle \mathbf{v}_i, \mathbf{v}_j \rangle = \sum_k v_{ik} v_{jk}$. A is a real symmetric positive definite matrix. Geometrically, the diagonal elements of A equal the squared norms of the basis vectors, while the other elements account for the intervector angles. The Gram matrix characterizes the lattice independently of the space $\mathbf{R}^d$ in which it is located. Furthermore, the Gram matrix is the same for rotated lattices but generally different for congruent lattices.

For $m = d$, we observe that $\det(A) = \mathbf{d}(\Lambda)^2$. We can use this to define the determinant of Λ when $m < d$, as

$$\mathbf{d}(\Lambda) = \det(A)^{1/2} \ .$$

For scaled versions of Λ we have $\mathbf{d}(c\Lambda) = c^m \mathbf{d}(\Lambda)$.

Definition 9 *Given a lattice* Λ *of* $\mathbf{R}^d$ *we define its* **dual lattice** *as*

$$\Lambda^* = \{\mathbf{x} \in \mathbf{R}^d : \langle \mathbf{x}, \mathbf{u} \rangle \in \mathbf{Z} \qquad \forall \mathbf{u} \in \Lambda\} \ .$$

If A is the Gram matrix of Λ then A^{-1} is the Gram matrix of Λ^*. In the case of a full-rank lattice the generator matrix of Λ^* is $(M^T)^{-1}$.

Definition 10 *A lattice is said to be* **integral** *if the inner product of any two lattice vectors is an integer, or in other words if the Gram matrix has integer entries. Equivalently a lattice is integral if and only if* $\Lambda \subseteq \Lambda^*$. *If* $\Lambda = \Lambda^*$ *we talk of a* **self-dual** *lattice.*

In many cases of interest a lattice, when suitably scaled, becomes an integral lattice.

An alternative approach to lattice theory studies the *quadratic forms* associated with the Gram matrix A of the lattice. The quadratic form

$$Q(\mathbf{x}) = \mathbf{x} A \mathbf{x}^T = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij} x_i x_j \qquad \mathbf{x} = (x_1, \ldots x_m) \in \mathbf{R}^m \tag{2.3}$$

is positive definite, with *discriminant* $\delta(Q)$ =det(A). If we are only interested in the metric properties of a lattice, we can equivalently work on the basis vectors or on the form Q restricted to $\mathbf{Z}^m$. For example, the minimum squared Euclidean distance between any two points of Λ equals the minimum of $Q(\mathbf{x})$ for $\mathbf{x} \in \mathbf{Z}^m \backslash \{\mathbf{0}\}$.

We have seen that the Gram matrix can be uniquely determined from the generator matrix. The converse is not possible: given the Gram matrix A we find an infinite number of different generator matrices which correspond to the rotated versions of the same lattice.

Given the Gram matrix $A = (a_{ij})$ there exists an efficient algorithm which calculates a lower triangular generator matrix

$$L = \begin{pmatrix} l_{11} & & & 0 \\ l_{21} & l_{22} & & \\ \vdots & & \ddots & \\ l_{m1} & l_{m2} & & l_{mm} \end{pmatrix}$$

such that

$$A = L \cdot L^T \ . \tag{2.4}$$

The algorithm solves iteratively the $m(m+1)/2$ equations, obtained from (2.4), in the $m(m+1)/2$ unknowns l_{ij} as follows:

1.

$$l_{11}^2 = a_{11} \quad \Rightarrow \quad l_{11} = \sqrt{a_{11}}$$

2.

$$\begin{array}{rcl} l_{11}l_{21} & = & a_{12} \\ l_{21}^2 + l_{22}^2 & = & a_{22} \end{array} \quad \Rightarrow \quad \begin{array}{rcl} l_{21} & = & a_{12}/l_{11} \\ l_{22} & = & \sqrt{a_{22} - l_{21}^2} = \sqrt{a_{22} - a_{12}^2/a_{11}} \end{array}$$

3.

$$\begin{array}{rcl} l_{11}l_{31} & = & a_{13} \\ l_{21}l_{31} + l_{22}l_{32} & = & a_{23} \\ l_{31}^2 + l_{32}^2 + l_{33}^2 & = & a_{33} \end{array} \quad \Rightarrow \quad \begin{array}{rcl} l_{31} & = & a_{13}/l_{11} \\ l_{32} & = & (a_{23} - l_{21}l_{31})/l_{22} \\ l_{33} & = & \sqrt{a_{33} - l_{31}^2 - l_{32}^2} \end{array}$$

$$\ldots$$

The general equations are given by

$$l_{ii} = \left(a_{ii} - \sum_{k=1}^{i-1} l_{ik}^2 \right)^{1/2}$$

$$l_{ji} = \frac{1}{l_{ii}} \left(a_{ij} - \sum_{k=1}^{i-1} l_{ik} l_{jk} \right) \qquad j = i+1, i+2, \ldots m \ .$$

This procedure is called **Cholesky decomposition** or **Cholesky factorization**.

Definition 11 *Given a discrete set of points Σ in $\mathbf{R}^d$ the Voronoi region of a point $\mathbf{s}_i \in \Sigma$ is the convex set*

$$\mathcal{V}(\mathbf{s}_i) = \{\mathbf{x} \in \mathbf{R}^d : \|\mathbf{x} - \mathbf{s}_i\| \leq \|\mathbf{x} - \mathbf{s}_j\| \quad \textit{for all} \quad i \neq j\} \ .$$

In the following we consider sets of points which form lattices. The Voronoi regions of all the lattice points are congruent due to the translation symmetry of the lattice (see Definition 6). Hence, we can talk of *the* Voronoi cell (or region). This important property has been defined by Forney in [2] as the *geometric uniformity* a lattice.

Other names from various fields for the Voronoi cell are *Dirichlet cell, Brillouin zone, Wigner-Seitz cell, Wirkungsbereich (domain of action), Wabenzelle (honeycomb), nearest neighbor region, decision region.*

Definition 12 *We define the Voronoi cell $\mathcal{V}(\Lambda)$ of a lattice Λ as the Voronoi region around the origin*

$$\mathcal{V}(\Lambda) = \{\mathbf{x} \in \mathbf{R}^d : \|\mathbf{x}\| \leq \|\mathbf{x} - \mathbf{u}\| \quad \textit{for all non zero } \mathbf{u} \in \Lambda\} \ .$$

In order to simplify the notation we will omit the specification of the lattice when referring to its Voronoi cell. If $\mathbf{u} \neq \mathbf{0} \in \Lambda$, then $\|\mathbf{x}\| = \|\mathbf{x} - \mathbf{u}\|$ defines a hyperplane half-way between $\mathbf{0}$ and $\mathbf{u}$ of equation $\langle \mathbf{x}, \mathbf{u} \rangle = \|\mathbf{u}\|^2/2$, and a half-space $\|\mathbf{x}\| \leq \|\mathbf{x} - \mathbf{u}\|$. $\mathcal{V}$ is an intersection of half-spaces, so it could be a polytope (we must still check if it is bounded). The points $\mathbf{p}$ of the lattice for which the hyperplane between $\mathbf{0}$ and $\mathbf{p}$ contains a facet of $\mathcal{V}$ are called the *Voronoi-relevant points* and the hyperplanes, *Voronoi-relevant hyperplanes.* If $\mathbf{p}$ is Voronoi-relevant also $-\mathbf{p}$ is Voronoi-relevant, so $\mathcal{V}$ is symmetric about the origin. We say that $\mathcal{V}$ is an $\mathbf{0}$-*symmetric convex body.* Since $\mathcal{V}$ cannot contain lattice points $\neq \mathbf{0}$, we are under the hypothesis of Minkowski's fundamental theorem [9, p. 14], which implies that $\mathcal{V}$ is bounded. Thus we can conclude that $\mathcal{V}$ is an $\mathbf{0}$-*symmetric polytope* i.e., a bounded region defined by the intersection of a finite number of closed half-spaces (see Chapter 4 for further details).

Referring to [19] and [20] we also say that $\mathcal{V}$ is a *parallelohedron*, i.e., a *prototile* of a lattice tiling. Like the fundamental parallelotope, the Voronoi cell is a prototile of a lattice tiling (a covering of the entire space by non-overlapping closed sets) and has volume vol(Λ).

Definition 13 *The* **theta series** *of a lattice Λ is defined as*

$$\Theta_\Lambda(z) = \sum_{\mathbf{x} \in \Lambda} q^{\|\mathbf{x}\|^2} = \sum_{m=0}^{\infty} N_m q^m$$

where $q = e^{\pi \imath z}$, $\imath = \sqrt{-1}$.

The theta series is a formal power series in the indeterminate q, where the coefficients N_m are the number of points of the lattice at squared Euclidean distance m from the origin. For integral lattices m is an integer. The theta series can also be viewed as an holomorphic function of the complex variable z in the right complex half-plane. It is interesting to note that the theta series is uniquely determined by its lattice but the converse is not true in general (see Chapter 4, Lattices Is_{5a}, Is_{5b}).

The theta series of the dual lattice Λ^* can be obtained from the theta series of Λ

$$\Theta^*_\Lambda(z) = \mathbf{d}(\Lambda) \left(\frac{\imath}{z}\right)^{n/2} \Theta_\Lambda\left(\frac{-1}{z}\right) \ .$$

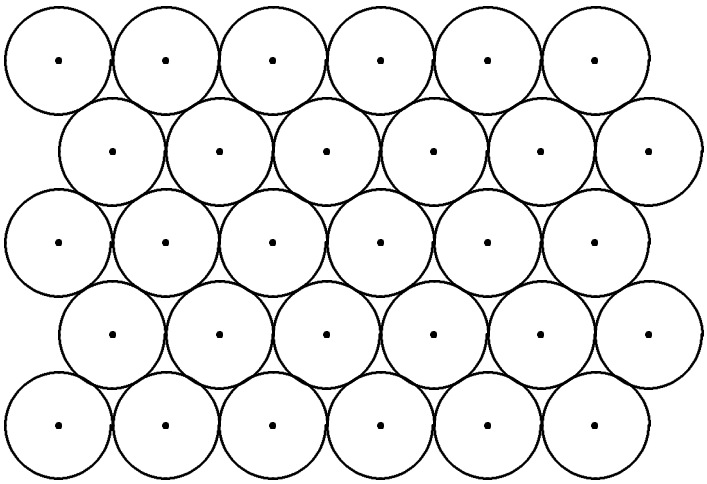

Figure 2.3: The optimal 2-dimensional lattice sphere packing

This formula can be considered as the generalization to lattices of the MacWilliams identities for linear block codes.
For a scaled version of Λ we have $\Theta_{c\Lambda}(z) = \Theta_{\Lambda}(c^2 z)$.

We conclude this section with a useful formula for the volume of a d-dimensional sphere S_r of radius r

$$\mathrm{vol}(S_r) = \frac{\pi^{d/2} r^d}{\Gamma\left(\frac{d}{2}+1\right)} \,. \tag{2.5}$$

For spheres of unit radius this volume is denoted by V_d for each dimension d.

2.2 The sphere packing problem

A very old problem in mathematics asks to stack a large number of identical 3-dimensional spheres in a very large box in the most efficient way, i.e., by maximizing the number of spheres which can fit inside the box. Such arrangements of spheres are called *sphere packings*. The spheres will not fill all the space in the box and whatever arrangement is chosen at least about 25% of the space remains empty. We call *packing density* Δ the percentage of space occupied by the spheres.

The above problem can be generalized to higher or lower dimensions but the optimal or *densest* sphere packing is only known in dimensions 1 and 2 (Fig. 2.3). In all other dimensions we only have some good candidates.

Among all possible packings of spheres we distinguish the *lattice sphere packings* which are obtained by centering at each point of a full-rank lattice Λ, identical spheres with the maximum radius such that they do non penetrate into each other. This particular radius ρ is called *packing radius* of Λ. If we call d_{min} the minimum norm of any non zero lattice point we obviously have $\rho = d_{min}/2$. We observe that the sphere of radius ρ is the largest sphere inscribed in the Voronoi cell of the lattice. If we restrict the problem to lattice sphere

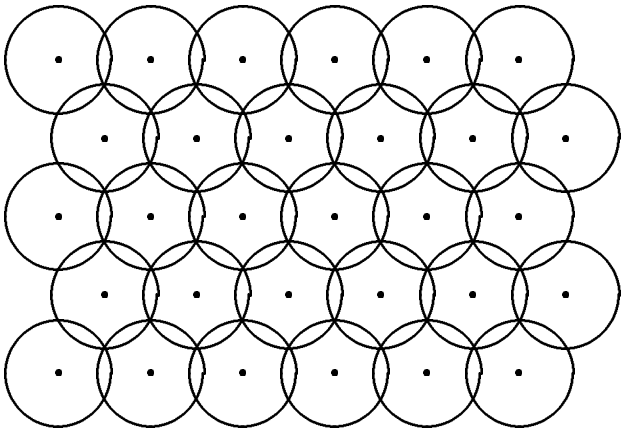

Figure 2.4: The optimal 2-dimensional lattice covering

packings we know the optimal lattice sphere packing up to dimension 8. The packing density of a lattice packing is easily obtained remembering that the Voronoi cell forms a tiling of the entire space

$$\Delta = \frac{\text{Volume of one sphere}}{\text{Volume of the Voronoi cell}} = \frac{V_d \rho^d}{\text{vol}(\Lambda)} \quad \leq 1 \ . \tag{2.6}$$

We also define the *center density*

$$\delta = \frac{\Delta}{V_d} = \frac{\rho^d}{\text{vol}(\Lambda)} \ . \tag{2.7}$$

which gives the number of centers per unit volume and enables one to compare lattices in different dimensions. The density and the center density are independent of the scaling factor of the lattice, whereas the packing radius of $c\Lambda$ is c times the packing radius of Λ.

The number of spheres touching (kissing) one sphere in a sphere packing is called *kissing number*. For an arbitrary packing the kissing number varies from one sphere to another but for lattice packings it is the same for all the spheres. We observe that the kissing number τ gives the number of points of the lattice at the minimum distance d_{min} from the origin, so we can write

$$\Theta_\Lambda(z) = 1 + \tau q^{d_{min}^2} + \cdots = 1 + \tau q^{4\rho^2} + \cdots \ .$$

The optimal lattice packings are known up to dimension 8 and are given by the lattices $\mathbf{Z}$, A_2, A_3, D_4, D_5, E_6, E_7, E_8.

2.3 The covering problem

The *covering problem* asks for the most economical way to cover the entire space with equal overlapping spheres (Fig. 2.4). Here, we will only dicuss lattice coverings for which the centers of the spheres form a lattice. Given a full-rank lattice in $\mathbf{R}^d$ we call *covering radius* R of Λ the smallest radius for which the spheres still cover the entire space. R is also the

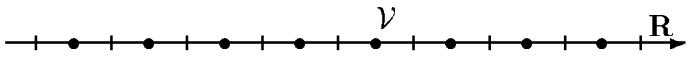

Figure 2.5: The one-dimensional quantizer

distance of the furthest point of $\mathbf{R}^d$ from any lattice point. For a lattice covering we define the *thickness* Θ of the covering as the average number of spheres that contain a point of the space

$$\Theta = \frac{\text{Volume of one sphere}}{\text{Volume of the Voronoi cell}} = \frac{V_d R^d}{\text{vol}(\Lambda)} \geq 1 \ . \tag{2.8}$$

We also define a *normalized thickness* as

$$\theta = \frac{\Theta}{V_d} = \frac{R^d}{\text{vol}(\Lambda)} \ . \tag{2.9}$$

We observe that R is the radius of the smallest sphere containing the Voronoi cell and the vertices of the Voronoi cell on such a sphere are called the *deep holes* of the lattice. The thickness and the normalized thickness are independent of the scaling factor of the lattice, whereas the covering radius of $c\Lambda$ is c times the covering radius of Λ.

The optimal lattice coverings are known up to dimension 5 and are given by the lattices $\mathbf{Z}$, A_2, A_3^*, A_4^*, A_5^*.

2.4 The quantization problem

Quantization consists of representing a continuous space, with the least possible error, by using only a discrete set of points. The number of points used fixes both the quality and the complexity of the quantizer. We illustrate these concepts by means of a simple example.

In the case of a one-dimensional space the quantization process is known as analog-to-digital conversion. The real line can be represented using a discrete set of equally spaced points as shown in Figure 2.5. If we assume that the samples of an input signal are uniformly distributed over $\mathbf{R}$, a measure of the distorsion is given by the average mean square error between the input signal and the quantized point. In order to minimize this distorsion, given a sample $x \in \mathbf{R}$, we 'quantize' it by the closest point of the quantizer. This *encoding* process is equivalent to selecting the quantizer point according to the Voronoi region in which x lays. In this case it is clear that the quality of the quantizer only depends on the number of points per unit length, thus as a measure of quality it is convenient to normalize the average mean square error by the size of the Voronoi region. This quantity is called the one-dimensional normalized second moment and for the uniform quantizer in Figure 2.5 is given by

$$G_1 = \frac{\int_{\mathcal{V}} x^2 dx}{\int_{\mathcal{V}} dx} = \frac{1}{12} = 0.083333\ldots \ .$$

Any other quantizer with non equally spaced points results in a higher normalized second moment, so we say that $\mathbf{Z}$ is the best one-dimensional quantizer.

A fundamental result in information theory states that it is possible to improve the performance by using *vector quantization*, i.e., grouping a certain number d of samples of the input signal and then applying the quantization process with a suitable set of points in a d-dimensional space. Unfortunately this result is non-constructive. The encoding process is performed with the minimum distance criterium, i.e., by selecting the closest quantizer point. The vector quantization problem asks to find the optimal discrete set of points which minimizes the distorsion for a given dimension, assuming a uniform distribution of the input signal. In this thesis we deal with *lattice quantizers* only and the distorsion measure is given by

$$G(\Lambda) = \frac{1}{d} \frac{\int_{\mathcal{V}} \|\mathbf{x}\|^2 d\,\mathbf{x}}{\left(\int_{\mathcal{V}} d\,\mathbf{x}\right)^{1+2/d}} \,. \tag{2.10}$$

This is called *dimensionless second moment* or *quantizing constant* of the lattice Λ.

For each dimension d, it is lower bounded by the quantizing constant of a d-dimensional sphere with the same volume of $\mathcal{V}$ and radius r

$$G(\Lambda) \geq \frac{\Gamma\left(\frac{d}{2}+1\right)^{2/d}}{(d+2)\pi} \,.$$

The optimal lattice quantizer for $\mathbf{R}^2$ is the hexagonal lattice A_2 and for for $\mathbf{R}^3$ is the body-centered cubic lattice A_3^* (see Sec. 2.6). In higher dimension it is conjectured in [1] that the optimal lattice quantizers are the dual lattices of the densest lattice sphere packings. This problem will be further discussed in Chapter 4.

2.5 The channel coding problem

The central problem of coding theory is the following.
A source of information emits a sequence of messages (either continuous signals or discrete sets of symbols from a finite alphabet). These messages need to be transmitted over a channel impaired by noise in such a way that the probability of correct detection at the receiver side is maximized.

It is well known that band-limited signals can be mapped into a multidimensional Euclidean space using Shannon's sampling theorem. While for discrete sets of signals it is always possible to extract a convenient basis, which defines a multidimensional space where each signal is represented by a point or vector $\mathbf{x}$. In both cases the Euclidean norm of $\mathbf{x}$ corresponds to the energy of the trasmitted signal.

We assume that the channel impairments are only due to additive white Gaussian noise (AWGN). The channel bandwidth is larger than the bandwidth of the transmitted messages so that no other type of distorsion appears. AWGN can also be represented as a random vector in the Euclicean space $\mathbf{n} = (n_1, \ldots n_d)$ whose components are independent, Gaussian

distributed, random variables with zero mean and variance σ^2. The received vector can be written as

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \ . \tag{2.11}$$

Let S be a set of code points $\{\mathbf{s}_1, \ldots \mathbf{s}_M\}$ and let $\mathcal{V}(\mathbf{s}_k)$ be the Voronoi region of $\mathbf{s}_k$. If $\mathbf{s}_k$ is transmitted the decoder makes a correct decision if and only if the received vector $\mathbf{y}$ lays inside $\mathcal{V}(\mathbf{s}_k)$. The probability of such event is

$$\frac{1}{(\sigma\sqrt{2\pi})^d} \int_{\mathcal{V}(\mathbf{s}_k)} e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}} d\mathbf{x} \ . \tag{2.12}$$

Assuming that all code points are equally likely to be used, the error probability for this code is

$$P(e) = 1 - \frac{1}{M} \sum_{k=1}^{M} \frac{1}{(\sigma\sqrt{2\pi})^d} \int_{\mathcal{V}(\mathbf{s}_k)} e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}} d\mathbf{x} \ . \tag{2.13}$$

If all the Voronoi cells are congruent, as for lattices, we write

$$P(e) = 1 - \frac{1}{(\sigma\sqrt{2\pi})^d} \int_{\mathcal{V}} e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}} d\mathbf{x} \ . \tag{2.14}$$

For practical applications we will only use a finite number M of points of the lattice within a bounded region containing the origin. This signal constellation is called a *lattice code* or *lattice constellation*. The error probability in (2.14) is exact only for an infinite lattice. When we consider a finite lattice constellation the assumption that the Voronoi regions are all congruent is no longer valid. In fact the points laying on the edge of the constellation have unbounded Voronoi regions while the inner points have the lattice Voronoi regions. Since the unbounded regions contain the Voronoi cell of the lattice, equation (2.14) gives an upper bound to the error probability of a lattice code. The larger the number of points M of the lattice code the tighter is the bound even for low SNR's, since the edge effects become negligible.

The general channel coding problem for the Gaussian channel asks for the code S which minimizes $P(e)$ in (2.13) under the signal energy constraint

$$\|\mathbf{s}_k\|^2 \leq C^2 = \text{const.}$$

The lattice version of the Gaussian channel coding problem is to find, for a given value of σ, the d-dimensional lattice of determinant 1 for which (2.14) is minimized. For a lattice with determinant $\mathbf{d}(\Lambda)$ we can define a *signal-to-noise ratio* as

$$\text{SNR}_{dB} = 10 \log \frac{[\mathbf{d}(\Lambda)]^{2/d}}{4\sigma^2} \tag{2.15}$$

so that the error probability as a function of SNR remains independent of the lattice scaling factor.

The difficulty of the lattice coding problem lays mainly in the complexity of evaluation of the error probability (2.14). To overcome this difficulty we resort to various approximations which possibly cover the range of SNR of interest.

An upper bound to the error probability $P(e)$ of a finite constellation carved from a lattice and used for transmission over the additive white Gaussian noise channel can be derived as follows. We assume that all the points are transmitted with equal probability and the lattice constellation is sufficiently large to neglect edge effects. Due to the geometric uniformity of the lattice [21] it is enough to consider the probability of decoding a point different from $\mathbf{0}$, when $\mathbf{0}$ is transmitted. Let $\mathbf{x}$ be the received vector when $\mathbf{0}$ is transmitted. The components of $\mathbf{x}$, are Gaussian distributed random variables, with zero mean and variance σ^2.

Now let $\mathbf{p}_i$ be the Voronoi-relevant points around $\mathbf{0}$. Using the union bound with all the Voronoi-relevant hyperplanes only, we obtain the upper bound [1, p. 70], [23]

$$\begin{aligned} P(e) &\leq P\left(\bigcup_i \{\langle \mathbf{x}, \mathbf{p}_i\rangle \geq \|\mathbf{p}_i\|^2/2\}\right) \\ &\leq \sum_i P(\langle \mathbf{x}, \mathbf{p}_i\rangle \geq \|\mathbf{p}_i\|^2/2) = \sum_i \frac{1}{2}\mathrm{erfc}\left(\frac{\|\mathbf{p}_i\|/2}{\sqrt{2}\sigma}\right) . \end{aligned} \tag{2.16}$$

where

$$\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt . \tag{2.17}$$

In general this bound is very complex to evaluate, since it is difficult to find all the Voronoi relevant points. This problem will be considered in detail in Chapter 4.

Bound (2.16) may be compared with another upper bound given by

$$P(e) < P(\mathbf{x} \notin S_\rho) = 1 - \Gamma\left(\frac{d}{2}, \frac{\rho^2}{2\sigma^2}\right)/\Gamma\left(\frac{d}{2}\right) \tag{2.18}$$

where S_ρ is a d-dimensional sphere of radius ρ, the packing radius of the lattice, and

$$\Gamma(a, x) = \int_0^x t^{a-1}e^{-t}dt$$

is the incomplete gamma function.

A well-known lower bound [22], is given by

$$P(e) > P(\mathbf{x} \notin S_{r_0}) = 1 - P\left(\frac{d}{2}, \frac{r_0^2}{2\sigma^2}\right)/\Gamma\left(\frac{d}{2}\right) \tag{2.19}$$

where S_{r_0} is a d-dimensional sphere with volume equal to $\mathrm{vol}(\mathcal{V})$ and radius

$$r_0 = (vol(\mathcal{V})/V_d)^{1/d} .$$

In Chapter 4 we present some comparison curves of these bounds.

Λ	$\gamma(\Lambda)(dB)$
A_2	0.62
D_4	1.50
E_8	3.01
Λ_{16}	4.51
Λ_{24}	6.02

Table 2.1: Asymptotic coding gains of some important lattices.

For large SNR's simple estimate of the error probability is given by

$$P(e) \approx \frac{\tau}{2} \operatorname{erfc}\left(\frac{\rho}{\sigma\sqrt{2}}\right) \tag{2.20}$$

where τ is the kissing number, ρ the packing radius. This approximation is obtained from (2.16) by considering only the τ largest terms of the sum.

If we assume that for each code vector $\|\mathbf{s}_k\|^2 \leq C^2$, we can define the signal-to-noise ratio, for sufficiently large values of M, as

$$\mathrm{SNR'}_{dB} = 10 \log \frac{C^2/d}{2\sigma^2 M^{2/d}} \,. \tag{2.21}$$

For a lattice code we can write

$$P(e) \approx \frac{\tau}{2} \operatorname{erfc}\left(\sqrt{\Delta^{2/d} d \cdot \mathrm{SNR'}}\right) \tag{2.22}$$

and with this approximation we reduce the lattice coding problem to the lattice sphere packing problem with the additional requirement of minimizing the kissing number. For $\sigma \to 0$ the term τ can be omitted and the the lattice coding problem coincides with the lattice sphere packing problem.

As a reference lattice we take $\mathbf{Z}^d$ and we define the *fundamental* or *asymptotic coding gain* of a lattice over $\mathbf{Z}^d$ as

$$\gamma(\Lambda) = \frac{d_{min}^2}{\sqrt[d/2]{\mathbf{d}(\Lambda)}} = 4 \sqrt[d/2]{\delta} \tag{2.23}$$

This measure is useful to assess the performance of a lattice code for high signal-to-noise ratios.

Shannon's fundamental result restated in terms of lattice codes establishes that by increasing the dimension d it is possible to find a lattice code which attains any arbitrarily small error probability for a given signal-to-noise ratio. This result is non-costructive, i.e., it gives no method to find such a lattice. Table 2.1 shows the asymptotic coding gains of different lattices which are the best known lattices for the Gaussian channel in each dimension.

The gains clearly increase with the dimension but the delay and the decoding complexity also increase.

Another range of interest for the noise variance is for large σ's (low SNR), when we can use the approximation

$$e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}} \approx 1 - \frac{\|\mathbf{x}\|^2}{2\sigma^2} \tag{2.24}$$

in equation (2.14). With this approximation the lattice coding problem is reduced to the lattice quantization problem. For low SNR's the quantizing constant becomes the relevant factor.

The solution to lattice coding problem is only known in one and two dimensions where the lattices $\mathbf{Z}$ and A_2 are optimal for all values of σ. In general the solution depends on σ but for applications we are interested in the performance for small σ's (large SNR).

2.6 Examples of important lattices

In the following subsections we define some of the most important examples of lattices either giving the generator matrix or the Gram matrix. All the lattice parameters are summarized in Tables 2.2 and 2.3. For those parameters depending on the scaling factor we refer to the specific generator or Gram matrix given in the following subsections.

2.6.1 Integer lattices $\mathbf{Z}^n$

Formally we can write

$$\mathbf{Z}^n = \{(x_1, \ldots x_n) : x_i \in \mathbf{Z}\} \ . \tag{2.25}$$

Both the generator and the Gram matrices are the identity matrix. We note also that the quantizing constant is independent of n and equals to that the one-dimensional quantizer:

$$G(\mathbf{Z}^n) = \frac{1}{12} \ .$$

2.6.2 Lattices A_n

See [1, p. 108]. This lattice has a simple definition in the $(n+1)$-dimensional space as

$$A_n = \{(x_0, x_1, \ldots x_n) \in \mathbf{Z}^{n+1} : \sum_{i=0}^{n} x_i = 0\} \ . \tag{2.26}$$

Its Gram matrix is

$$A = \begin{pmatrix} 2 & -1 & 0 & \cdots & 0 & 0 \\ -1 & 2 & -1 & & 0 & 0 \\ 0 & -1 & 2 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 2 & -1 \\ 0 & 0 & 0 & \cdots & -1 & 2 \end{pmatrix} \ . \tag{2.27}$$

Λ	$\mathbf{d}(\Lambda)$	τ	ρ	R
$\mathbf{Z}^n$	1	$2n$	$1/2$	$\rho\sqrt{n}$
A_n $(n \geq 2)$	$\sqrt{n+1}$	$n(n+1)$	$1/\sqrt{2}$	$\rho\left(\frac{2a(n+1-a)}{n+1}\right)^{1/2}$
A_n^* $(n \geq 2)$	$(n+1)^{(n-1)/2}$	$2n+2$	$\sqrt{n}/2$	$\rho\left(\frac{n+2}{3}\right)^{1/2}$
D_n $(n \geq 3)$	2	$2n(n-1)$	$1/\sqrt{2}$	$\rho\sqrt{2}$ $(n=3)$ $\rho\sqrt{n/2}$ $(n \geq 4)$
D_n^* $(n \geq 5)$	2^{n-1}	$2n$	1	$\sqrt{n/2}$ (n even) $(2n-1)^{1/2}/2$ (n odd)
E_8	1	240	$1/\sqrt{2}$	1
E_7	16	126	1	$\sqrt{3}$
E_7^*	$1/\sqrt{2}$	56	$\sqrt{3/8}$	$\sqrt{7/8}$
E_6	$\sqrt{3}$	72	$1/\sqrt{2}$	$\sqrt{4/3}$
E_6^*	$1/\sqrt{3}$	54	$1/\sqrt{3}$	$\sqrt{2/3}$
K_{12}	27	756	1	$\sqrt{8/3}$
Λ_{16}	16	4320	1	$\sqrt{3}$
Λ_{24}	1	196560	1	$\sqrt{2}$

Table 2.2: Determinant, kissing number, packing radius and covering radius of some important lattices.

Λ	δ	θ	G
$\mathbf{Z}^n$	2^{-n}	$n^{n/2}2^{-n}$	$1/12$
$A_n\ (n \geq 2)$	$2^{-n/2}(n+1)^{-1/2}$	$\frac{[a(n+1-a)]^{n/2}}{(n+1)^{(n+3)/2}}$	$\frac{1}{(n+1)^{1/n}}\left(\frac{1}{12}+\frac{1}{6(n+1)}\right)$
$A_n^*\ (n \geq 2)$	$\frac{n^{n/2}}{2^n(n+1)^{(n-1)/2}}$	$\sqrt{n+1}\left(\frac{n(n+2)}{12(n+1)}\right)^{n/2}$	$\frac{J_{n+1}}{n(n+1)^{1-1/n}}$
$D_n\ (n \geq 3)$	$2^{-(n+2)/2}$	$1/2\ (n=3)$	$\frac{1}{2^{2/n}}\left(\frac{1}{12}+\frac{1}{2n(n+1)}\right)$ $n^{n/2}2^{-(n+1)}\ (n \geq 4)$
$D_n^*\ (n \geq 5)$	$2^{-(n-1)}$	$n^{n/2}\ (n \text{ even})$ $(2n-1)^{n/2}/2^{2n-1}\ (n \text{ odd})$	$\frac{2641}{23040\cdot 2^{3/5}} = 0.0756254\ (n=5)$ $\frac{601\cdot 2^{1/3}}{10080} = 0.0751203\ (n=6)$
E_8	$1/16$	1	$\frac{929}{12960} = 0.0716821$
E_7	$1/16$	$3^{7/2}\cdot 2^{-4}$	$\frac{163}{2016\cdot 2^{1/7}} = 0.0732306$
E_7^*	$3^{7/2}\cdot 2^{-10}$	$7^{7/2}\cdot 2^{-10}$	$\frac{21361\cdot 2^{1/7}}{322560} = 0.0731165$
E_6	$1/8\sqrt{3}$	$2^6\cdot 3^{-7/2}$	$\frac{5}{56\cdot 3^{1/6}} = 0.0743467$
E_6^*	$3^{-5/2}$	$2^3\cdot 3^{-7/2}$	$\frac{12619\cdot 3^{1/6}}{20412 0} = 0.0742437$
K_{12}	$1/27$	$2^{18}\cdot 3^{-9}$	0.070100 ± 0.000024
Λ_{16}	$1/16$	$3^8\cdot 2^{-4}$	0.068299 ± 0.000027
Λ_{24}	1	2^{12}	0.065771 ± 0.000074

Table 2.3: Center density, normalized thickness and quantizing constant of some important lattices

A_2 is self-dual and is known as the *hexagonal lattice*. A_3 is called *face-centered cubic lattice* and corresponds for example to the crystal structure of common salt (NaCl). In Table 2.3 we have posed a equal to the integer part of $(n+1)/2$.

2.6.3 Lattices A_n^*

See [1, p. 115]. The Gram matrix is

$$A = \begin{pmatrix} n & -1 & -1 & \cdots & -1 & -1 \\ -1 & n & -1 & & -1 & -1 \\ -1 & -1 & n & & -1 & -1 \\ \vdots & & & \ddots & & \vdots \\ -1 & -1 & -1 & & n & -1 \\ -1 & -1 & -1 & \cdots & -1 & n \end{pmatrix} . \tag{2.28}$$

A_3^* is called *body-centered cubic lattice* and corresponds for example to the crystal structure of iron. The values of J_n of Table 2.3 are given by

$$J_n = 0, \frac{1}{12}, \frac{5}{18}, \frac{19}{32}, \frac{389}{375}, \frac{1045}{648}, \frac{78077}{33614} \qquad \text{for } n = 0, 1, \ldots 7$$

and the general recursive equation can be found in [1, p. 473].

2.6.4 Lattices D_n

See [1, pp. 117-120]. For $n \geq 3$

$$D_n = \{(x_1, \ldots x_n) \in \mathbf{Z}^n : \sum_{i=0}^{n} x_i \text{ even}\} . \tag{2.29}$$

These lattices are the generalization of the *checkerboard lattice* D_2 shown in Fig. 2.2. The generator matrix is given by

$$M = \begin{pmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & & 0 & 0 \\ 0 & 1 & -1 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & & 1 & -1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix} \tag{2.30}$$

D_2 is self-dual and is equivalent to $\mathbf{Z}^2$, in fact it can be obtained from the integer grid by a rotation of $\pi/4$ and scaling factor $c = \sqrt{2}$. The lattices D_3 and A_3 are both equivalent to the face-centered cubic lattice. D_4 is also self-dual and is known as the *Schläfli lattice*.

2.6.5 Lattices D_n^*

The generator matrix is

$$D_n^* : \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 0 & & 0 & 0 \\ 0 & 0 & 2 & & 0 & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & & 2 & 0 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \tag{2.31}$$

The lattices D_3^* and A_3^* are both equivalent to the *body-centered cubic (bcc) lattice*. The general expression for G is derived in [1, p. 463-472].

2.6.6 The Gosset lattice E_8

See [1, p. 120]. This self-dual lattice is defined as

$$E_8 = \{(x_1, \ldots x_n) : \text{ all } x_i \in \mathbf{Z} \text{ or all } x_i \in \mathbf{Z} + 1/2, \sum_{i=0}^{n} x_i \equiv 0 \bmod 2\} . \tag{2.32}$$

The generator matrix is

$$M = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix} \tag{2.33}$$

2.6.7 Lattices E_7 and E_7^*

See [1, pp. 124-125]. The generator matrix of E_7 and the Gram matrix of E_7^* are respectively

$$M_{E_7} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad A_{E_7^*} = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 3/2 \end{pmatrix} \tag{2.34}$$

The quantizing constant of E_7^* was first computed in a closed form in [27].

2.6.8 Lattices E_6 and E_6^*

See [1, pp. 125-127]. The Gram matrices are

$$A_{E_6} = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix} \qquad A_{E_6^*} = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & -1 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & 0 & 0 \\ 0 & -1 & 0 & 0 & 4/3 & 1 \\ 0 & 0 & -1 & 0 & 1 & 2 \end{pmatrix} \tag{2.35}$$

The quantizing constant of E_6^* was first computed in a closed form in [26].

2.6.9 The Coxeter-Todd lattice K_{12}

See [1, p. 127]. The generator matrix is

$$\mathrm{M} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1/2 & -1/2 & 1 & 0 & 0 & 0 & \sqrt{3}/2 & \sqrt{3}/2 & 0 & 0 & 0 \\ -1/2 & 1 & -1/2 & 0 & 1 & 0 & \sqrt{3}/2 & 0 & \sqrt{3}/2 & 0 & 0 & 0 \\ -1/2 & -1/2 & 1 & 0 & 0 & 1 & \sqrt{3}/2 & \sqrt{3}/2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 0 & 0 & -\sqrt{3}/2 & \sqrt{3}/2 & \sqrt{3}/2 & -\sqrt{3}/2 & 0 & 0 \\ 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & \sqrt{3}/2 & -\sqrt{3}/2 & \sqrt{3}/2 & 0 & -\sqrt{3}/2 & 0 \\ 1/2 & 1/2 & 1/2 & 0 & 0 & 1/2 & \sqrt{3}/2 & \sqrt{3}/2 & -\sqrt{3}/2 & 0 & 0 & -\sqrt{3}/2 \end{pmatrix} \tag{2.36}$$

The value of G has been found by Montecarlo integration [1, pp. 61].

2.6.10 The Barnes-Wall lattice Λ_{16}

See [1, p. 129]. The generator matrix is

$$\mathrm{M} = \frac{1}{\sqrt{2}} \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{2.37}$$

The value of G has been found by Montecarlo integration [1, pp. 61].

2.6.11 The Leech lattice Λ_{24}

See [1, p. 131]. The generator matrix is

$$\mathrm{M} = \frac{1}{\sqrt{8}} \begin{pmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 \\ -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{2.38}$$

The value of G has been found by Montecarlo integration [1, pp. 61].

2.7 Costruction A

This is one of the simplest methods of constructing a lattice using a q-ary linear block code. The properties of such a lattice can be related to the code parameters, which yields a powerful tool for designing lattice codes.

Definition 14 *Given a q-ary linear block code $\mathcal{C}$ with lenght n, dimension k and minimum Hamming distance d, we construct a lattice in the following way: $\mathbf{x}$ is a lattice point if the n-tuple $(x_1, \ldots x_n)$ is congruent modulo q to a codeword of $\mathcal{C}$. We write*

$$\Lambda = q\mathbf{Z}^n + \mathcal{C} \ . \tag{2.39}$$

This construction results in a lattice thanks to the linear stucture of the code. The fact that the sum of two codewords is still a codeword implies that the sum of two vectors of Λ is still in Λ.

If $G = [I|P]$ is generator matrix of the code in the systematic form the lattice generator matrix is

$$M = \begin{pmatrix} I & P \\ 0 & qI \end{pmatrix} \tag{2.40}$$

In the case of binary ($q = 2$) linear codes we have the following results. The packing radius of Λ is

$$\rho = \frac{1}{2}\min\{2, \sqrt{d}\} \tag{2.41}$$

and the center density

$$\delta = 2^k \rho^n 2^{-n} \tag{2.42}$$

While the kissing number is

$$\tau = \begin{cases} 2^d A_d & \text{if } d < 4 \\ 2n + 16A_d & \text{if } d = 4 \\ 2n & \text{if } d > 4 \end{cases} \tag{2.43}$$

where A_d is the number of codewords of $\mathcal{C}$ having Hamming weight d. It is also possible to relate the lattice theta series to the weight enumerator function of the code $\mathcal{C}$ [1, Chap. 7].

We have the covering radius of Λ as

$$R = \max\{1/2\sqrt{n}, R_H\} \tag{2.44}$$

where R_H is the Hamming covering radius of the code. This can be seen noting that the deep holes around the origin can be (a) the vectors with all the components equal to $\pm 1/2$ (b) all permutations of the vectors of the type $((\pm 1)^{R_H} 0^{n-R_H})$ (the exponents are the number of times the component is repeated).

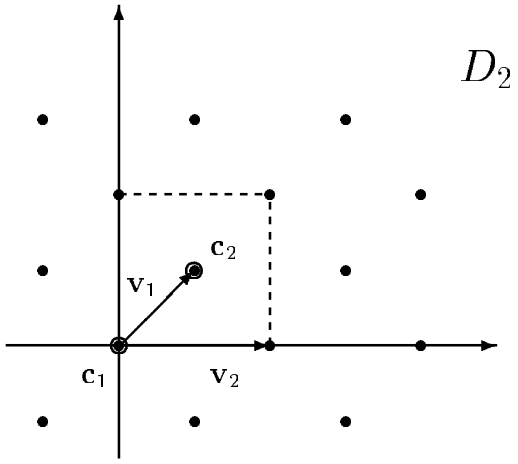

Figure 2.6: Construction A of D_2

Figure 2.6 shows an example of the construction A applied to the binary code $\mathcal{C} = \{\mathbf{c}_1 = (00), \mathbf{c}_2 = (11)\}$. We can imagine that the lattice is obtained by translating all over the plane the square in dashed lines of edge two. The two points $(0,0)$ and $(1,1)$ appear once in every translated square and form the checkerboard lattice. Its basis vectors are $\mathbf{v}_1 = (1,1)$ and $\mathbf{v}_2 = (0,2)$.

Chapter 3

A universal lattice decoding algorithm

Decoding a d-dimensional lattice consists of finding the lattice point closest to any given vector $\mathbf{z}$ *in the Euclidean space* $\mathbf{R}^d$. *Decoding algorithms find applications in vector quantization and in demodulation of multidimensional signal constellations. Here we describe an algorithm that solves the decoding problem for any lattice, irrespective of its particular algebraic structure. This algorithm is also modified to enable maximum-likelihood decoding of lattice codes when used for transmission over a fading channel. Part of this Chapter was presented in [15].*

3.1 Introduction

A lattice code is a finite subset of points of a lattice (or, more generally, of a lattice translate) within a bounded region containing the origin, so that the energy of each signal is bounded. Lattice codes are used in vector quantization, where they provide highly structured codebooks with efficient encoding algorithms [11, p. 470 ff.], and in digital communications, where they generate signal constellations for high-rate transmission (see, e.g., [7] and the references therein). For sufficiently large signal-to-noise ratios, good constellations are usually carved from dense lattices, a selection prompted by De Buda's result that lattice codes asymptotically achieve Shannon's capacity bound [4].

A crucial procedure for both applications of lattice codes is their decoding. Given a d dimensional lattice Λ and a point $\mathbf{z}$ in the d-dimensional Euclidean space $\mathbf{R}^d$ in which Λ is embedded, decoding the lattice amounts to finding the point of Λ closest to $\mathbf{z}$. The problem here is to find this point without incurring the complexity of an exhaustive search. Practical algorithms which efficiently decode some well-known lattices that are attractive for applications ($A_n (n \geq 1)$, $D_n (n \geq 2)$, E_6, E_7, E_8, and their duals) are listed in [3], [1, pp. 443 ff.]. Several Leech lattice decoders have been proposed with ever improving efficiency; a recent review of the subject can be found in [5].

The above algorithms are strictly dependent on the special structure of the lattice being decoded (e.g., its being a binary lattice [6]). Other algorithms [11, pp. 479–481] for general nearest neighbor encoding in vector quantization are valid for any unstructured codebook. They do not take full advantage of the lattice structure which is useful for large bit rates. The algorithm described in section 3 was first created as building block of a general Minkowski's basis reduction [17, 14]. We have adapted it to allow the decoding of any general lattice.

We may also observe here that, since any linear block code $\mathcal{C}$ over $\mathcal{Z}_q$ (the ring of integers modulo q) is in a sense equivalent to a sublattice of $\mathbf{Z}^n$ (see 'Construction A' in [1, Chapter 5]) any general decoding algorithm will also provide a quasi-Maximum Likelihood soft-decoding algorithm for $\mathcal{C}$.

As a preliminary to the decoding problem, we first describe an algorithm for computing the shortest nonzero vector of a lattice. The basic idea in both cases is to restrict the search to a finite number of lattice points which lie within a bounded region. We generally start with a large region and, whenever a shorter vector is found, the region is consequently restricted.

3.2 Shortest nonzero vector in a lattice

The task of determining nonzero vectors of Λ with shortest length was first considered by Gauss and later by Minkowski in his 'Geometry of Numbers'. Minkowski's Fundamental Theorem provides an upper bound to the length of such vector [9]. The first application which tackled the computational aspect of the problem can be found in the study of the lattice structure of pseudo-random numbers generated by the linear congruential method [13].

One of the first algorithms proposed is described in [8]. Here, the search region is defined

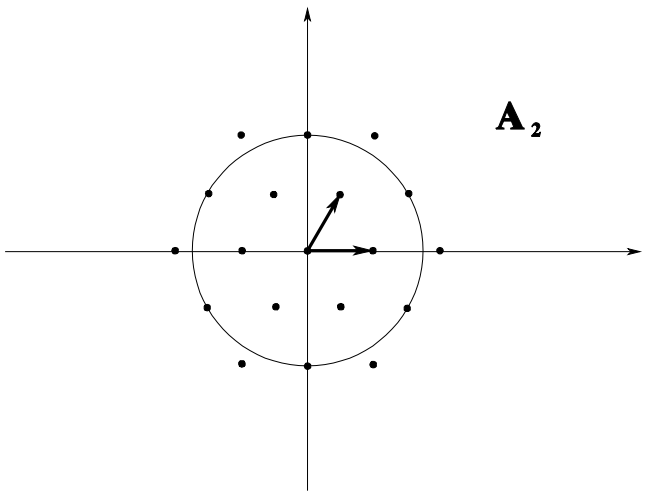

Figure 3.1: The two-dimensional hexagonal lattice.

based on the dual of Λ. A preliminary base reduction can restrict the size of the starting region, but the search becomes prohibitively complex when the lattice dimensionality grows above a certain threshold (around 10).

A substantial improvement was introduced by Pohst in [14] and further analyzed in [17]. We briefly illustrate this algorithm here, and provide some further insight through its geometrical interpretation. Consider a vector $\mathbf{u} \in \mathbf{R}^d$, and let $\|\mathbf{u}\| = \sqrt{\mathbf{u}\mathbf{u}^T}$ denote its Euclidean norm. A *ball* of radius $\sqrt{C}$ is defined by the inequality

$$\|\mathbf{u}\|^2 \leq C. \tag{3.1}$$

If $\mathbf{u}$ is a lattice point, then it can be written in the form $\mathbf{u} = \mathbf{x}M$ for some integer vector $\mathbf{x} \in \mathbf{Z}^d$, and lies inside the ball if

$$\mathbf{x}MM^T\mathbf{x}^T = \mathbf{x}A\mathbf{x}^T = \sum_{i=1}^{d}\sum_{j=1}^{d} a_{ij}x_ix_j \leq C \tag{3.2}$$

If we let the vector $\mathbf{x}$ take on real values, then (3.2) is the equation of an ellipsoid (Figs. 3.1 and 3.2), the lengths of whose semi-axes are directly related to eigenvalues λ_i of the matrix A.

Cholesky's factorization yields $A = R^TR$, where R is an upper triangular matrix with elements $r_{ij} = 0$ for $2 \leq i \leq j \leq d-1$ and $r_{ii} = \sqrt{\lambda_i}$. Then

$$\mathbf{x}A\mathbf{x}^T = \mathbf{x}R^TR\mathbf{x}^T = \|R\mathbf{x}^T\|^2 = \sum_{i=1}^{d}\left(r_{ii}x_i + \sum_{j=i+1}^{d} r_{ij}x_j\right)^2 \leq C. \tag{3.3}$$

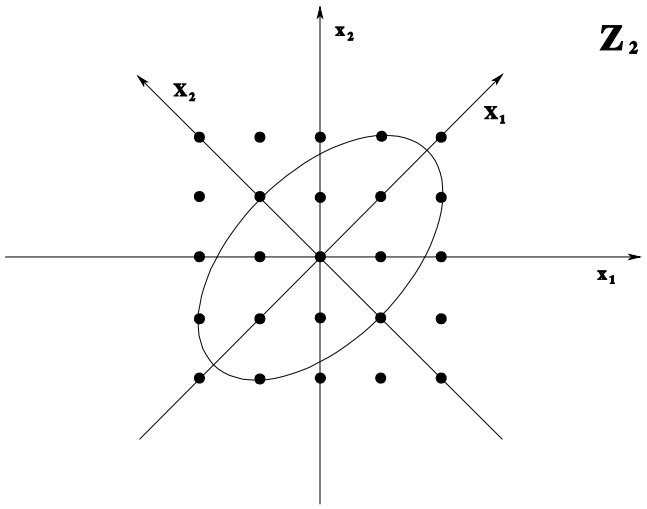

Figure 3.2: The integer lattice with the transformed region.

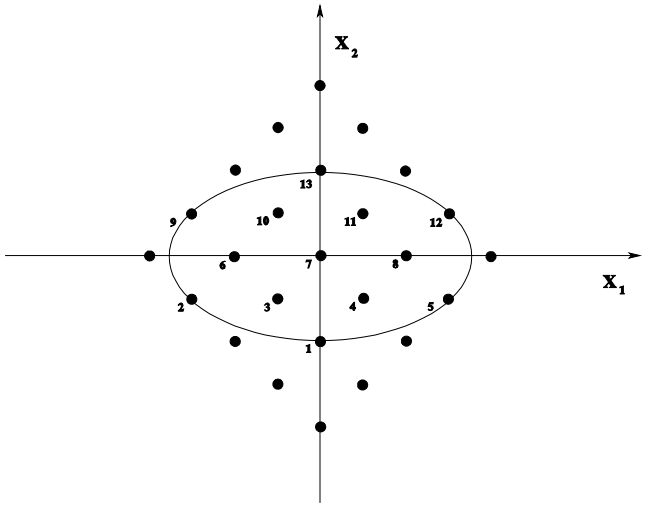

Figure 3.3: The integer lattice in the new coordinate system. The points inside the ellipse are numbered according to the order in which they are tested by the algorithm.

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

$$Q(\mathbf{x}) = \sum_{i=1}^{d} q_{ii} \left(x_i + \sum_{j=i+1}^{d} q_{ij} x_j \right)^2 \leq C. \tag{3.4}$$

The canonical form of this ellipsoid

$$\sum_{i=1}^{d} q_{ii} X_i^2 \leq C \tag{3.5}$$

is obtained by using the coordinate tranformation

$$\begin{pmatrix} X_1 \\ \vdots \\ X_{d-1} \\ X_d \end{pmatrix} = \begin{pmatrix} 1 & q_{12} & \cdots & q_{1d} \\ 0 & 1 & & \vdots \\ \vdots & & 1 & q_{d-1,d} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{d-1} \\ x_d \end{pmatrix}. \tag{3.6}$$

In the new coordinate system $\{X_1, \ldots, X_{d-1}, X_d\}$, based on the axes of the ellipsoid, the value of each component of a point inside the ellipsoid, can be bounded as follows. Starting from the last component, we have

$$|X_d| \leq \sqrt{\frac{C}{q_{dd}}} \tag{3.7}$$

which simply means that the d-th component is bounded by the length of the d-th semi-axis (Figure 3.3). Next, when X_d is chosen in the above range, we have

$$|X_{d-1}| \leq \sqrt{\frac{C - q_{dd} X_d^2}{q_{d-1,d-1}}} \tag{3.8}$$

and in general, once the components $X_{i+1}, \ldots, X_d$ are fixed, we have

$$|X_i| \leq \sqrt{\left(C - \sum_{l=i+1}^{d} q_{il} X_l^2 \right) \frac{1}{q_{ii}}}. \tag{3.9}$$

Substituting equations (3.6) in (3.7), (3.8) and (3.9) we find the bounds for the integer components of $\mathbf{x}$. Starting from x_d and working backwards we find

$$\left\lceil -\sqrt{\frac{C}{q_{dd}}} \right\rceil \leq \quad x_d \quad \leq \left\lfloor \sqrt{\frac{C}{q_{dd}}} \right\rfloor \tag{3.10}$$

$$\left\lceil -\sqrt{\frac{C - q_{dd} x_d^2}{q_{d-1,d-1}}} - q_{d-1,d} x_d \right\rceil \leq \quad x_{d-1} \quad \leq \left\lfloor \sqrt{\frac{C - q_{dd} x_d^2}{q_{d-1,d-1}}} - q_{d-1,d} x_d \right\rfloor \tag{3.11}$$

where $\lceil x \rceil$ is the smallest integer greater or equal to x and $\lfloor x \rfloor$ is the greatest integer less or equal to x. For the i-th integer component we have

$$\left\lceil -\sqrt{\left(C - \sum_{l=i+1}^{d} q_{il}\left(x_l + \sum_{j=l+1}^{d} q_{lj}x_j\right)^2\right)\frac{1}{q_{ii}}} - \sum_{j=i+1}^{d} q_{ij}x_j \right\rceil \leq x_i \leq$$
$$\leq \left\lfloor \sqrt{\left(C - \sum_{l=i+1}^{d} q_{il}\left(x_l + \sum_{j=l+1}^{d} q_{lj}x_j\right)^2\right)\frac{1}{q_{ii}}} - \sum_{j=i+1}^{d} q_{ij}x_j \right\rfloor \tag{3.12}$$

The search algorithm proceeds very much like a mixed radix counter, with the addition that the bounds change whenever there is a carry operation from one digit to the next. (Figure 3.3 shows how the algorithm works. It scans exactly all the points of $\mathbf{Z}^2$ inside the ellipse in the order indicated by the numbers). In practice, the bounds are updated recursively by using the following equations:

$$U_i = U_i(x_{i+1}, \ldots, x_d) = \sum_{l=i+1}^{d} q_{il}x_l \tag{3.13}$$

$$\begin{aligned} T_i = T_i(x_{i+1}, \ldots, x_d) &= C - \sum_{l=i+1}^{d} q_{il}\left(x_l + \sum_{j=l+1}^{d} q_{lj}x_j\right)^2 \\ &= T_{i+1} - q_{i+1,i+1}\left(x_{i+1} + U_{i+1}\right)^2 \end{aligned} \tag{3.14}$$

If a vector $\mathbf{u} = \mathbf{x}M$ for some $\mathbf{x} \in \mathbf{Z}^d$, such that $\|\mathbf{u}\|^2 < C$, is found, then we are able to reduce the radius of the ball. We substitute $\|\mathbf{u}\|^2$ for C, we update all the bounds, and we keep on searching in the smaller ball without restarting from the beginning.

The great advantage of this method over [8] lies in the fact that we never test vectors with a norm greater than the given radius. Every vector tested requires the computation of its norm, which entails d multiplications and $d-1$ additions. The increase in number of operations needed to update the bounds (3.12) is largely compensated for by the enormous reduction in the number of vectors tested.

As a byproduct of this algorithm we may obtain the *kissing number* of Λ, that is, the number of lattice points at the minimum distance from the origin.

3.3 Closest lattice point decoder for the Gaussian channel

Here we want to solve the problem

$$\min_{\mathbf{u}\in\Lambda} \|\mathbf{z} - \mathbf{u}\| = \min_{\mathbf{w}\in\mathbf{z}-\Lambda} \|\mathbf{w}\| \ . \tag{3.15}$$

We write $\mathbf{u} = \mathbf{x}M$ with $\mathbf{x} \in \mathbf{Z}^d$, $\mathbf{z} = \boldsymbol{\zeta}\, M$ with $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_d)$, and $\mathbf{w} = \boldsymbol{\xi}\, M$ with $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_d)$, where $\boldsymbol{\zeta}$ and $\boldsymbol{\xi}$ are real vectors. Then we have

$$\mathbf{w} = \sum_{i=1}^{d} \xi_i \mathbf{v_i}$$

where

$$\xi_i = \zeta_i - x_i \qquad i = 1, \ldots, d. \tag{3.16}$$

With the above substitutions we now have to find the shortest nonzero vector of the translated lattice $\mathbf{z} - \Lambda$. As before, we construct a ball of radius $\sqrt{C}$ centered at $\mathbf{z}$ and we test all the lattice points that are inside.

Some additional comments on the choice of $\sqrt{C}$ are appropriate here. In Chapter 2 we have seen that the furthest point of $\mathbf{R}^d$ from a point of Λ is called a *deep hole* of the lattice and that the *covering radius* R of Λ is the smallest distance of a lattice point from a deep hole. If the covering radius of the lattice is known, then we take it as the starting value for $\sqrt{C}$: otherwise we may use Roger's upper bound to the covering radius [18, p. 241]

$$R \leq \left(\frac{\mathbf{d}(\Lambda)}{V_d} (d \log_e d + d \log_e \log_e d + 5d) \right)^{1/d} \tag{3.17}$$

where V_d is the volume of the d-dimensional unit sphere.

In a practical application the radius could be adaptively adjusted according to the noise level in the following way. If no lattice point is detected inside the ball, the radius must be increased and an erasure can be indicated to the higher levels. On the contrary, when the distance $\|\mathbf{w}\|$ of the received point to the lattice point is small, then the radius can be decreased.

3.4 Soft-decoding of the ternary $(12, 6, 6)$ Golay code

As an example of application of the algorithm described before, we study its complexity when used to soft-decode the ternary $(12, 6, 6)$ Golay code. The generator matrix of the corresponding lattice, obtained by construction A, is

$$M = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 2 & 2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\
0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 2 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3
\end{pmatrix} \tag{3.18}$$

which corresponds to periodically repeating in each direction the code vectors contained in a 12-dimensional cube of edge 3. The covering radius of this lattice is not known and the upper bound (3.17) gives $R \leq 2.48$ (we conjecture $R = 2$, a value that has never been exceeded in our computations). The simulation was performed by generating a sequence of vectors $\mathbf{z}$ in the form $\mathbf{x}+\mathbf{n}$, where $\mathbf{n}$ is a zero-mean Gaussian vector with independent, identically distributed components. According to simulation, the average numbers of additions, multiplications and square roots per codeword are about 4900, 3800 and 350. For a complete search through code book we would need 16767 additions and 8748 multiplications, as well as the complete storage of all the 729 ternary codewords. Although square roots are usually considered as lengthy operations, in our case they can be performed with a reduced precision, since they are followed by a floor or ceiling function. Finally we observe that the decoding algorithm is not exactly maximum-likelihood since it can decode a lattice point which is not a code vector. In general this difference is only noticeable for very low signal-to-noise ratios and for small values of q. To better approximate the ML decoding various strategies can be adopted, viz.,

1. Reduce modulo 3 the lattice point coordinates produced by the decoder.

2. During the search in the sphere, discard the points which are not code vectors; if no code vector is found declare an erasure or use strategy 3.

3. Take a hard decision on the information part of the received vector.

Note that when any of the above strategies is adopted, the uniform error property is no longer valid since the decoder is performing some non-linear operation.

3.5 Decoder for the fading channel

Lattices codes, when used over the Gaussian channel can be decoded using the above algorithm. We show how to adapt this lattice decoding algorithm to the fading channel case. This channel model will be described in Chapter 5, section 5.2. For the pourpose of this section we only recall that for maximum-likelihood decoding with perfect side information, the problem is to minimize the metric

$$m(\mathbf{u}|\mathbf{z},\boldsymbol{\alpha}) = \sum_{i=1}^{n} |z_i - \alpha_i u_i|^2 \tag{3.19}$$

Let M be the generator matrix of the lattice Λ and let us consider the lattice Λ_c with generator matrix

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

We can imagine this new lattice Λ_c in a space where each component has been compressed or enlarged by a factor α_i. A point of Λ_c can be written as $\mathbf{w} = (w_1, \ldots w_n) = (\alpha_1 u_1, \ldots \alpha_n u_n)$.

The metric to minimize is then

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

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

As discussed in the previous section, this decoding algorithm is ML only for an infinite lattice. When dealing with a finite constellation, with a given spectral efficiency, some care should be taken. In fact, the decoder may output a lattice point which is not part of the signal set.

The lattice constellations may be constituted by the points of the first shells of the lattice in order to obtain the minimal average energy per point. Since the decoding complexity increses with the search radius of the sphere, this is adaptively selected according to the fading coefficients so that we can always find at least one point of Λ_c inside the sphere. To optimize the decoder whenever the received point lays outside the outermost shell of the costellation we take its projection on this shell.

3.6 Conclusions

The algorithm we have presented shows the advantages offered by the continuous structure of the space in which lattices are embedded. This algorithm was also tested as a Leech lattice decoder and the total number of operations was found to be about 885,000, where additions, multiplications, and square roots were in the same proportions as in the previous example. This result may look discouraging when compared with 8000 operations required by the fastest Leech decoding algorithm known [5]. However, it should be kept in mind that the generality of our procedure enables one to decode lattices for which no *ad hoc* algorithm is known. Finally a the lattice decoding algorithm useful for the Gaussian channel has also been adapted to the fading channel case.

3.7 Appendix

Here we give the procedure for computing directly all the coefficients $q_{i,j}$ arranged in a matrix Q in equation (3.4).

```
Q:=A;
for i:=1 to d-1 do
```

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

Chapter 4

Computing the Voronoi cell: the Diamond Cutting Algorithm

Numerical evaluation of some typical lattice parameters such as density, thickness, dimensionless second moment (quantizing constant) etc., is considered. Computational complexity grows exponentially with the dimension of the lattices and all known results rely on the very regular structure of some of these. In this chapter we present a general algorithm which enables computation of all the common parameters for any given lattice by means of a complete description of its Voronoi cell. Using this algorithm, we have computed previously unknown values of the quantizing constants of some particularly interesting lattices. These results can be used to evaluate the performance of lattice quantizers and lattice signal constellations for the Gaussian channel. As an application we evaluate a tight upper bound for the error probability of a lattice constellation used for transmission over the additive white Gaussian noise channel [30].

4.1 Introduction

The complete geometric structure of a lattice can be found from the description of its Voronoi cell. The knowledge of the Voronoi cell solves at once the problem of the computation of relevant lattice parameters such as packing radius, covering radius, kissing number, center density, thickness, normalized second moment (quantizing constant). The error probability of a lattice constellation, used for transmission over the additive white Gaussian noise channel, can also be effectively evaluated by using some of the above parameters.

The Voronoi cell of certain highly symmetric lattices can be determined analytically. According to [1] the Voronoi cell is completely known for the following lattices: A_n, A_n^*, D_n, D_n^*, $(n \geq 2)$ E_6, E_6^*, E_7, E_7^*, $E_8 \cong E_8^*$, Craig's lattice $A_6^{(2)}$ and the 24-dimensional Leech lattice[1]. No result is available for an arbitrary lattice.

In this chapter we propose an algorithm which computes the Voronoi cell of a full-rank arbitrary lattice. The exact knowledge of the Voronoi cell (i.e., knowledge of the coordinates of its vertices, edges, etc.) enables one to compute all the lattice parameters within any degree of accuracy. Theoretically, this algorithm evaluates a closed-form solution to all the above lattice problems. In practice, due to finite-precision arithmetics, round-off errors limit the accuracy of the calculations, but comparison with known (closed-form) results shows that they do not propagate. Hence, the accuracy of the results can be set *a priori* within the range of the computer floating point precision.

Using this algorithm we have computed some previously unknown values (Table 4.6) of the quantizing constants for some particularly interesting lattices. As these lattices do not improve upon the best known lattice quantizers, the conjecture about the optimal lattice quantizers being the duals of the densest lattices still holds.

Section 4.2 reviews the basic geometric definitions needed to describe the diamond-cutting algorithm (Section 4.3). The name of this algorithm comes from its resemblance to the procedure for cutting a raw diamond into a brilliant. In Section 4.4 we show how to compute all the lattice parameters from the Voronoi cell. Finally, Section 4.5 summarizes all the results obtained with the diamond-cutting algorithm. Of special interest is Table 4.6, where we find the previously unknown quantizing constants for the two locally optimal lattice coverings in $\mathbf{R}^4$ found by Dickson [28] and for a 5-dimensional extreme lattice covering, which belongs to the class introduced by Barnes and Trenerry in [29].

4.2 Polytopes

Definition 15 *For $0 \leq k \leq d$, a k-flat in $\mathbf{R}^d$ is the affine hull (i.e., the set of linear combinations with non-negative coefficients adding up to one) of $k+1$ linearly independent points.*

[1]The normalized second moment is computed by Montecarlo integration using some efficient decoding algorithm of the Leech lattice.

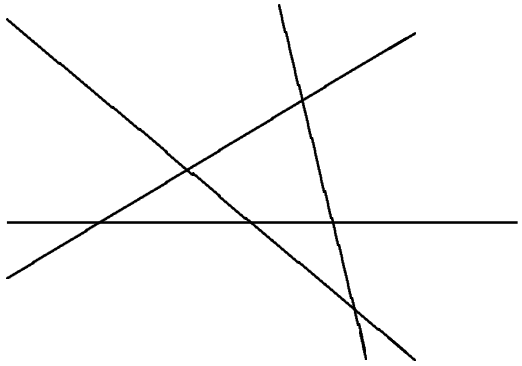

Figure 4.1: Example of two dimensional arrangement of four lines

A 0-flat is a *point*, a 1-flat is called a *line*, a 2-flat is called *plane* and $(d-1)$-flat, $d > 3$, is called *hyperplane*. There is only one d-flat which corresponds to $\mathbf{R}^d$ and for convenience we define the empty set as the (-1)-flat. Equivalently, a k-flat can be defined as the intersection of $d-k$ hyperplanes whose normal vectors are linearly independent.

Definition 16 *Given a finite set H of hyperplanes in $\mathbf{R}^d$ we call arrangement $\mathcal{A}(H)$ of H the dissection of $\mathbf{R}^d$ in connected pieces of various dimensions.*

The two-dimensional arrangement of Fig. 4.1 has 6 intersection points, 8 segments, 8 half-lines, 3 bounded regions and 8 unbounded regions.

Definition 17 *A (convex) polytope $\mathcal{P}$ is the bounded region defined by the intersection of a finite number of closed half-spaces. More specifically, we call $\mathcal{P}$ a k-polytope if it has dimension k, that is, if k is the smallest integer number such that $\mathcal{P}$ is contained in a k-flat.*

In other words we can say that a polytope is a bounded region delimited by a finite number of hyperplanes. The minimum number of hyperplanes needed to define a k-polytope is $k+1$, since this must be bounded. Any bounded region of an arrangement is a polytope, thus it is possible to adapt to polytopes the algorithms designed for arrangements.

Definition 18 *For $0 \leq k \leq d$, a k-face of $\mathcal{P}$ is the set of points of $\mathcal{P}$ contained in k-flat.*

We generally speak of *faces of $\mathcal{P}$* when k is not specified. The 0-faces are called *vertices of $\mathcal{P}$*, the 1-faces, *edges of $\mathcal{P}$* and the $(d-1)$-faces, *facets of $\mathcal{P}$*. For convenience we identify $\mathcal{P}$ with the d-face and the empty set with the (-1)-face.

To give a complete description of a polytope we must know all the relations among its faces. For $-1 \leq k \leq d-1$ a k-face f and a $(k+1)$-face g are *incident upon* each other if f belongs to the boundary of g; in this case, f is called a *subface of g* and g a *superface of f*. The d-face represents the whole polytope and is the only superface of all the facets. The (-1)-face has no subfaces and is the only subface of all the vertices.

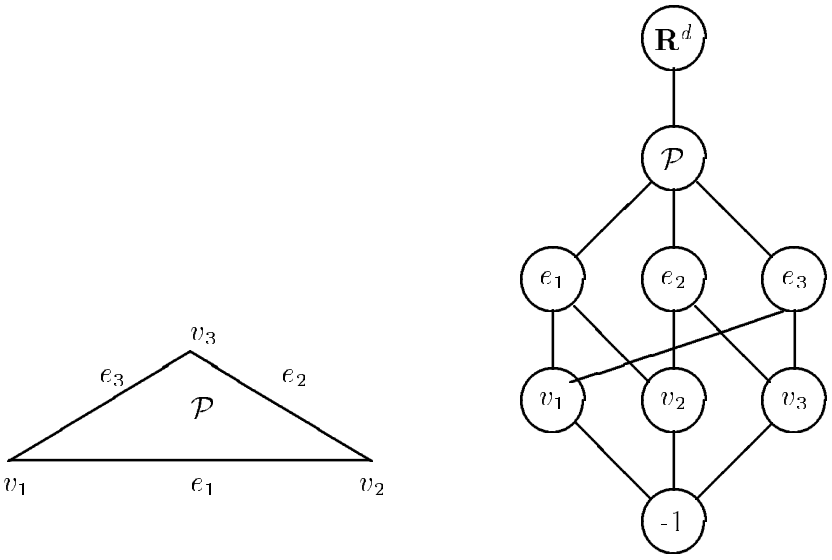

Figure 4.2: Example of the incidence graph of the triangle $\mathcal{P}$.

The *incidence graph* $I(\mathcal{P})$ of $\mathcal{P}$ is an undirected graph defined as follows: for each k-face ($k = -1, 0, 1, \ldots d$) of $\mathcal{P}$, $I(\mathcal{P})$ has a node $\nu(f)$; if f and g are incident upon each other then $\nu(f)$ and $\nu(g)$ are connected by an arc. The incidence graph of a polytope is completed by a node representing the whole Euclidean space $\mathbf{R}^d$ which is connected to the d-face (Fig. 4.2).

In the implementation of the diamond-cutting algorithm, each node $\nu(f)$ of an incidence graph is a record that contains some auxiliary information about the face and two lists containing pointers to the subfaces and the superfaces of f (Fig. 4.3). The auxiliary information stored in a node consists of the coordinates of a point $p(f)$ in f, a component capable of reflecting one of seven colours, the volume of f, the second order moment of f, the square distance of f from the origin and a node number. So $p(f) = f$ if f is a vertex and if $f_1, f_2, \ldots, f_m$ are subfaces of f ($m \geq 2$), then the point

$$p(f) = \frac{1}{m} \sum_{i=1}^{m} p(f_i) \tag{4.1}$$

is the *centroid* of f and it lays always inside f since f is convex. It is important to remark that in general this point does not coincide with the center of gravity (or barycenter) of the face.

We have seen in the discussion following Definition 12 that the Voronoi regions of all the lattice points are congruent polytopes. The Voronoi cell $\mathcal{V}$ is a space-filling parallelohedron with the additional property of being face-to-face, meaning that the intersection of any two distinct tiles is either empty or it is a common k-face for some $k = 0, 1, \ldots d-1$. Minkowski proved that the maximum number of facets of a d-parallelohedron is $2(2^d - 1)$ [18, pp. 88-96 and pp. 164-169]. This gives us already an idea of the exponential complexity of the

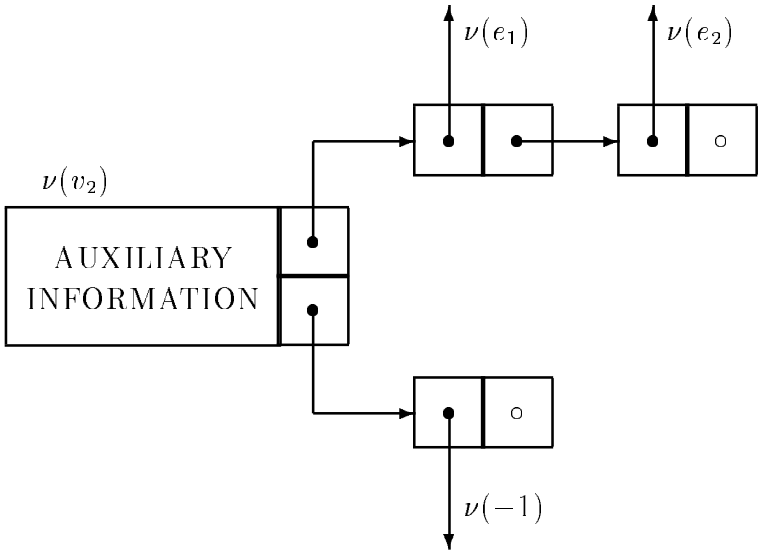

Figure 4.3: Data structure of a node. Each node contains the auxiliary information and the pointers to the heads of the superface and subface lists. Each element of the list contains a pointer to a node and a pointer to the next element in the list.

problem.

Finding the Voronoi region of a lattice is equivalent to determining the Voronoi-relevant points and constructing the polytope bounded by the Voronoi relevant hyperplanes. The Voronoi-relevant points can be found by searching among all the points of the lattice which lie within a sufficently large bounded region around the origin.

4.3 The diamond-cutting algorithm

This algorithm computes the incidence graph of the Voronoi region $\mathcal{V}$ of a lattice. From the incidence graph it is possible to extract all the desired lattice parameters as we shall see in the following section. Let us consider a lattice Λ defined by an arbitrary basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$. Given a point $\mathbf{p}$ we will denote with $h(\mathbf{p})$ the hyperplane passing through the point $\mathbf{p}$ and normal to the vector $\mathbf{p}$. The distance of $h(\mathbf{p})$ from the origin is equal to $\|\mathbf{p}\|$. We can now come to the formal description of the algorithm.

Preparation Given the lattice basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ construct the parallelotope $\mathcal{Q}$ defined by the hyperplanes $h(\pm\frac{1}{2}\mathbf{v}_i)$ for $i = 1, \ldots, d$. $\mathcal{Q}$ contains the Voronoi cell. The corresponding incidence graph $I(\mathcal{Q})$ has 3^d nodes. Finally, set $\mathcal{V} := \mathcal{Q}$.

Cutting Consider all hyperplanes $h(\frac{\lambda_1}{2}\mathbf{v}_1 + \frac{\lambda_2}{2}\mathbf{v}_2 + \cdots \frac{\lambda_d}{2}\mathbf{v}_d)$, with λ_i integers, which cut $\mathcal{V}$ and update $I(\mathcal{V})$ by introducing the nodes corresponding to the new faces and erasing

the ones corresponding to the faces which are left out. For this operation we have adapted Edelsbrunner's algorithm for the incrementation of arrangements [16].

Finish Compute $\mathrm{vol}(\mathcal{V})$, the volume of $\mathcal{V}$. If $\mathrm{vol}(\mathcal{V}) > \det(\Lambda)^{1/2}$ go on cutting, else end the algorithm and output the incidence graph $\mathcal{I}(\mathcal{V})$.

We now describe each step of this algorithm in greater detail.

4.3.1 Preparation

We first construct the incidence graph of a hypercube with edge length 2 centered at the origin. The $p(f)$ vectors of all the k-faces ($k = 0, 1, \ldots d$) of this hypercube have components in the set $\{-1, 0, +1\}$. In particular vertices only have -1 or $+1$ components, edges have one component equal to 0 and the remaining equal to -1 or $+1$, and k-faces have k components equal to 0 and $d-k$ equal to -1 or $+1$. It is now simple to see that a d-dimensional hypercube has $2^{d-k}\binom{d}{k}$ k-faces ($k = 0, 1, \ldots d$) for a total of 3^d faces.

In order to identify the subfaces of a given k-face f it is enough to replace each of the 0 components, in turn, with -1 and $+1$. In this way we find $2k$ subfaces. For the superfaces of f we replace each of the non-zero components, in turn, with a 0, so that we find exactly $d-k$ superfaces. For convenience, these component vectors are considered as base three (digits 0,1,2) numbers and then converted to decimal representation. The number is then used as the node number which uniquely identifies a k-face of $\mathcal{Q}$. An example of this is shown in Figures 4.4 and 4.5.

The parallelotope $\mathcal{Q}$, which is only a slanted and stretched hypercube, has the same incidence graph, except for the $p(f)$ vectors. We only need to calculate the vertices coordinates of the parallelotope then, using (4.1), we recursively obtain all the $p(f)$ vectors of all the faces. The vertices $\mathbf{x}^{(m)}, m = 1, \ldots 2^d$ of $\mathcal{Q}$ are found at the intersection of d hyperplanes

$$\begin{cases} \langle \mathbf{v}_1, \mathbf{x}^{(m)} \rangle = \frac{\lambda_1^{(m)}}{2} \|\mathbf{v}_1\|^2 \\ \langle \mathbf{v}_2, \mathbf{x}^{(m)} \rangle = \frac{\lambda_2^{(m)}}{2} \|\mathbf{v}_2\|^2 \\ \qquad\qquad \vdots \\ \langle \mathbf{v}_d, \mathbf{x}^{(m)} \rangle = \frac{\lambda_d^{(m)}}{2} \|\mathbf{v}_d\|^2 \end{cases} \tag{4.2}$$

where $\lambda_i^{(m)}$, $i = 1, \ldots d$ take on the values -1 and $+1$ of the corresponding components of the m-th vertex in the hypercube. The solution of all these linear systems is found by inverting once for all the generator matrix of the lattice and multiplying it by the vector of the *known terms*.

4.3.2 Cutting

The *raw diamond* is now ready to be cut. Given a hyperplane $h(\mathbf{p})$ cutting $\mathcal{V}$ (i.e., such that $h(\mathbf{p}) \bigcap \mathcal{V} \neq \emptyset$) we construct the incidence graph of the two parts of the dissected polytope:

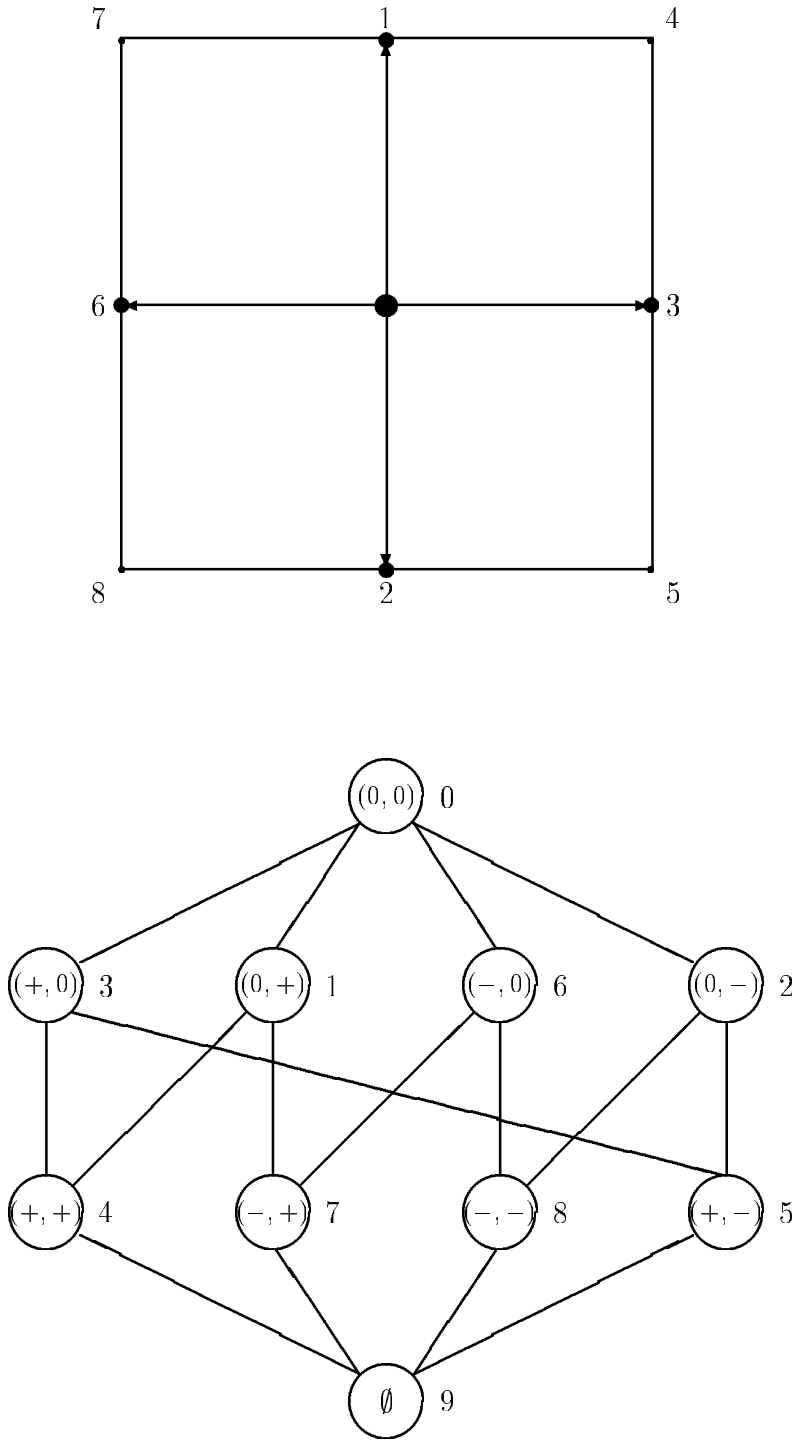

Figure 4.4: Incidence graph of a square ('+' stands for +1 and '-' for -1).

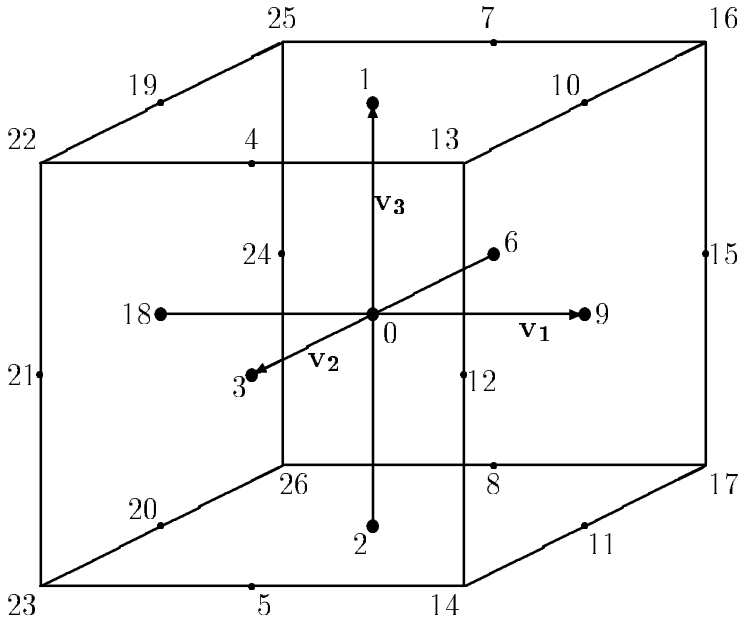

Figure 4.5: Node numbers of a cube.

the main body and the chip. The main body will always contain the origin since the cutting plane does not include the origin. This operation is performed by using the colour conventions and the procedures 7.3–5 described in [16, Ch.7]. Next, the incidence graph is purged from all the nodes representing the chip to obtain the new $\mathcal{I}(\mathcal{V})$.

A key operation in this procedure is to determine whether a given point $\mathbf{x}$ lays on, above, or below the cutting hyperplane. In particular we have:

$$\begin{array}{lcll} \langle \mathbf{p}, \mathbf{x} \rangle & < & \|\mathbf{p}\|^2 & \mathbf{x} \text{ is on the side of the main body} \\ \langle \mathbf{p}, \mathbf{x} \rangle & = & \|\mathbf{p}\|^2 & \mathbf{x} \in h(\mathbf{p}) \\ \langle \mathbf{p}, \mathbf{x} \rangle & > & \|\mathbf{p}\|^2 & \mathbf{x} \text{ is on the side of the chip.} \end{array} \tag{4.3}$$

This operation uses a fixed tolerance value (e.g., 10^{-5}), given as an input, to resolve the three cases.

Another critical procedure is the search for the coordinates of the new vertices. These are given by the intersections between $h(\mathbf{p})$ and the edges of $\mathcal{V}$. A bisection method is used. Starting from a vertex above and a vertex below $h(\mathbf{p})$ we compute the midpoint until such a point is found to lie on $h(\mathbf{p})$. In this case the tolerance should be further reduced in order to overcome some ill-conditioned cases which may be encountered.

4.3.3 Finish

Each cut reduces the volume of the polytope. When this is equal to $\det(\Lambda)^{1/2}$, the volume of the *fundamental parallelotope*, we have obtained the Voronoi region of the lattice. The way to select all the possible cutting hyperplanes is to consider all the lattice points within a given radius C from the origin by using the algorithm proposed in [17]. A safe choice for such radius would be twice the distance from the origin of the furthest vertex of the initial parallelotope $\mathcal{Q}$. In general a less conservative choice will work especially when the lattice basis is not reduced [18, 19]. If the covering radius is already known, then this is also a safe value for C. Whenever C is too small the volume of $\mathcal{V}$ will not reach the value $\det(\Lambda)^{1/2}$, meaning that C should be increased.

4.4 Calculating the lattice parameters

We now see how to evaluate all the lattice parameters once the incidence graph $\mathcal{I}(\mathcal{V})$ of the Voronoi cell is found.

4.4.1 Packing

To calculate the *packing radius* ρ we must find the facet closest to the origin. For this it is sufficient to scan the auxiliary information of the nodes pointed by the subface list of the node $\nu(\mathcal{V})$. At the same time the *kissing number* τ is found (i.e., the number of facets at the packing radius distance from the origin).

The *packing density* Δ is the ratio between the greatest sphere centered at the origin and contained in $\mathcal{V}$ and the volume of $\mathcal{V}$. This sphere has its radius equal to the packing radius. The *center density* δ is equal to the packing density divided by the volume of the unit sphere.

4.4.2 Covering

To calculate the *covering radius* R we must find the vertex of $\mathcal{V}$ with maximum distance from the origin. So it is sufficient to scan the nodes pointed by the superface list of the node $\nu(-1)$.

The *thickness* Θ of a covering of Λ is the ratio between the smallest sphere centered at the origin and contaning $\mathcal{V}$ and the volume of $\mathcal{V}$. This sphere has its radius equal to the covering radius. The *normalized thickness* θ is equal to the thickness divided by the volume of the unit sphere.

4.4.3 Quantization parameters

The *volume* of $\mathcal{V}$ is also given by

$$\mathrm{vol}(\mathcal{V}) = \int_{\mathcal{V}} d\mathbf{x} \tag{4.4}$$

and is equal to the volume of the fundamental parallelotope of Λ. The *second order moment* of $\mathcal{V}$ about $\mathbf{0}$ is defined by

$$U(\mathcal{V}) = \int_{\mathcal{V}} \|\mathbf{x}\|^2 d\mathbf{x} \ . \tag{4.5}$$

In [1, Ch. 21] $\mathrm{vol}(\mathcal{V})$ and $U(\mathcal{V})$ are given in terms of the volume $V_{d-1}(i)$ and of the second-order moment of the facets $U_{d-1}(i)$ about the foot of the perpendicular from $\mathbf{0}$, where i runs over the set of facets of $\mathcal{V}$. Let $h_i^{(d-1)}$ be the distance of the facets of $\mathcal{V}$ from the origin. Then

$$\begin{aligned} \mathrm{vol}(\mathcal{V}) &= \sum_i \frac{h_i^{(d-1)}}{d} V_{d-1}(i) \\ U(\mathcal{V}) &= \sum_i \frac{h_i^{(d-1)}}{d+2} [{h_i^{(d-1)}}^2 V_{d-1}(i) + U_{d-1}(i)] \ . \end{aligned}$$

These equations cannot be used in our algorithm. In fact, the recursive generalization of these equations, which yield the volume and the second-order moment of a k-face in terms of volume and second-order moment of its subfaces, requires an additional hypothesis which is not satisfied in general for arbitrary lattices. Let $\mathbf{c}_i^{(k)}$ be the orthogonal projection of the origin $\mathbf{0}$ on the i-th k-face for $k = 2, \ldots, d-1$. We have $h_i^{(d-1)} = \|\mathbf{c}_i{}^{(d-1)}\|$, where i runs over the set of the facets (subfaces) of $\mathcal{V}$. If we consider the m-th k-face, then we define $h_i^{(k-1)}(m) = \|\mathbf{c}_m^{(k)} - \mathbf{c}_i^{(k-1)}\|$, where i runs over the set of all the subfaces of the m-th k-face. Due to the orthogonality conditions we simply have ${h_i^{(k-1)}(m)}^2 = \|\mathbf{c}_m^{(k)}\|^2 - \|\mathbf{c}_i^{(k-1)}\|^2$.

The general recursions for $k = 1, \ldots d$, are

$$\begin{aligned} V_k(m) &= \sum_i \frac{h_i^{(k-1)}(m)}{d} V_{k-1}(i) \\ U_k(m) &= \sum_i \frac{h_i^{(k-1)}(m)}{d+2} [{h_i^{(k-1)}(m)}^2 V_{k-1}(i) + U_{k-1}(i)] \end{aligned} \tag{4.6}$$

with the initial conditions $V_0(\mathit{vertices}) = 1$ and $U_0(\mathit{vertices}) = 0$.

For the validity of these equations it is crucial to assume that the projections $\mathbf{c}_m^{(k)}$ of the origin on all the faces falls within them. This is certainly true only for the facets ($k = d-1$) of $\mathcal{V}$ which belong to the Voronoi-relevant hyperplanes and are cut by the normal vector connecting $\mathbf{0}$ to the corresponding Voronoi-relevant point. But in general it is not true for an arbitrary lattice.

Equations that may be used to calculate recursively $\mathrm{vol}(\mathcal{V})$ and $U(\mathcal{V})$ for an arbitrary lattice are derived in the following.

Theorem 1 – With the above notations, let g_m be the m-th k-face with barycenter $q(g_m)$, f_i one of its subfaces with barycenter $q(f_i)$. Setting $V_0(\mathit{vertices}) = 1$ and $U_0(\mathit{vertices}) = 0$, for $k = 2, \ldots d$ we have:

$$V_k(m) = \sum_i \frac{a_i^{(k-1)}(m)}{d} V_{k-1}(i)$$

$$U_k(m) \quad = \quad \sum_i \frac{a_i^{(k-1)}(m)}{d+2}[b_i^{(k-1)}(m)^2 V_{k-1}(i) + U_{k-1}(i)] \tag{4.7}$$

where $a_i^{(k-1)}(m)$ is the distance of $q(g_m)$ from the i-th $(k-1)$-face f_i, $b_i^{(k-1)}(m)$ is the distance between $q(g_m)$ and $q(f_i)$, $U_k(m)$ is the second order moment of the g_m about its barycenter $q(g_m)$, and $U_{k-1}(i)$ is the second order moment of f_i about its barycenter $q(f_i)$.

Proof – In this case we always have $q(g_m) \in g_m$ and the face g_m can be decomposed into generalized pyramids of vertex $q(g_m)$ and basis f_i. The proof then follows from elementary calculus by slicing each generalized pyramid into slabs parallel to f_i.

For the use of equation (4.7) in the DCA we need to relate the centroid $p(f)$ to the barycenter $q(f)$ of a face f. This is accomplished recursively using the following equation

$$q(g_m) = \frac{1}{V_k(m)} \sum_i \frac{dq(f_i) + p(g_m)}{d+1} V_k(\mathcal{P}_i) \qquad k = 2 \ldots d$$

where $V_k(\mathcal{P}_i)$ is the volume of the generalized pyramid of vertex $p(g_m)$ and base f_i.

The *dimensionless second moment* or *quantizing constant* of a lattice Λ, defined in Chapter 2, represents the mean-squared quantization errors per point assuming a uniform input distribution to a lattice quantizer

$$G(\Lambda) = G(\mathcal{V}) = \frac{1}{d} \frac{U(\mathcal{V})}{\mathrm{vol}(\mathcal{V})^{1+2/d}} \ . \tag{4.8}$$

This value is independent of the scale and the dimension of the space and depends only on the shape of $\mathcal{V}$.

4.4.4 Error probability

In Caopter 2 we have seen that the exact value of $P(e)$ can be formally written as

$$P(e) = P(\mathbf{x} \notin \mathcal{V}) = 1 - \frac{1}{(\sqrt{2\pi}\sigma)^d} \int_{\mathcal{V}} e^{-\frac{\|\mathbf{x}\|^2}{2\sigma^2}} d\mathbf{x}$$

Using the union bound with all the Voronoi-relevant hyperplanes only, we obtained

$$P(e) \leq \sum_i \frac{1}{2} \mathrm{erfc}\left(\frac{\|\mathbf{p}_i\|/2}{\sqrt{2}\sigma} \right) \ , \tag{4.9}$$

a looser upper bound was given by

$$P(e) < P(\mathbf{x} \notin S_\rho) = 1 - \Gamma\left(\frac{d}{2}, \frac{\rho^2}{2\sigma^2}\right) / \Gamma\left(\frac{d}{2}\right) \tag{4.10}$$

and the equal volume sphere lower bound was

$$P(e) > P(\mathbf{x} \notin S_{r_0}) = 1 - P\left(\frac{d}{2}, \frac{r_0^2}{2\sigma^2}\right) / \Gamma\left(\frac{d}{2}\right) \ . \tag{4.11}$$

4.5 Results

In this section we show some of the results obtained with the Diamond Cutting Algorithm. The algorithm was implemented in standard C and was run on different computers: PC 486, VAX 6000-530 and different UNIX workstations. The best performance in terms of speed was obtained on the workstations.

The major difficulties arise when dimension increases. In fact the amount of memory required may become very high. Using double-precision arithmetics it was estimated that the system needs to allocate, on average, 170 bytes for each node of the incidence graph. The total memory needed to store the final Voronoi cell can be estimated by looking at the total number of nodes (last column of tables). We specify "final" because during the cutting step the incidence graph of the chip as well as that of the main body must be created. For example in the case of E_7 the total memory occupied by the Voronoi cell was about 9MB, while during the cutting operation the peak size of the allocated memory was about 17MB.

The program receives as input the space dimension, the full-rank lattice generator matrix and the tolerance parameter which is used to resolve the position of a point with respect to a hyperplane. This last parameter must be consistent with the accuracy to which the generator matrix is given and approximately determines the final accuracy of the computed parameters. In all cases where the lattices are defined by their Gram matrix A, Cholesky decomposition was applied to A, giving lower triangular generator matrix L (see Chapter 2). The matrix L can then be used as a generator matrix of the lattice. If the lattices are defined by a non-full-rank generator matrix, the Gram matrix is calculated first.

Each lattice appears in two tables. The first one shows all the lattice parameters which are independent of the particular scaling factor, as well as the number N_k of k-faces of the Voronoi cell. The second one gives the parameters which depend on the scaling factor but are still independent of the lattice basis. The column with $\mathrm{vol}(\mathcal{V})$ can be compared with the determinant of the generator matrix of the lattice to check the accuracy of the computations. The facets profile gives the number of facets for each square distance. Here we find the squared packing radius and the kissing number (in boldface). The vertices profile gives the number of vertices for each square distance and here we find the square covering radius (in boldface).

Figures 4.6-4.8 show the bounds (4.9), (4.10) and (4.11) for different six-dimensional lattices. Curves of $P(e)$ are plotted as a function of the signal-to-noise ratio defined in Chapter 2 as

$$SNR_{dB} = 10\log \frac{\sqrt[d]{\mathrm{vol}(\mathcal{V})}}{4\sigma^2} .$$

$G(\Lambda)$ decreases from $\mathbf{Z}^6$ to A_6, to E_6, and to E_6^*, which indicates that the shape of the Voronoi cell becomes more and more spherical. This is reflected in a smaller gap between the upper bound (4.10) and the lower bound (4.11). The improved union bound (4.9) comes also very close to the lower bound.

We now list the generator or Gram matrices of some of the lattices which were tested with the diamond-cutting algorithm, others can be found in Chapter 2. The row vectors

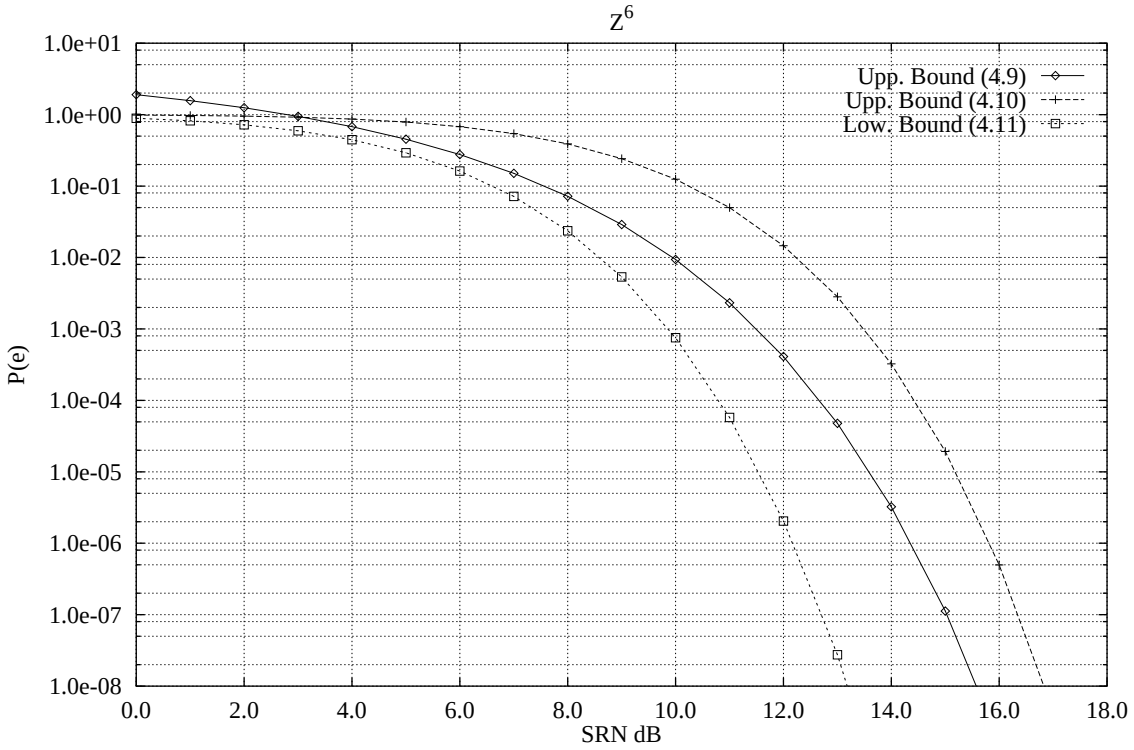

Figure 4.6: Upper and lower bounds to point error probability for $\mathbf{Z}^6$.

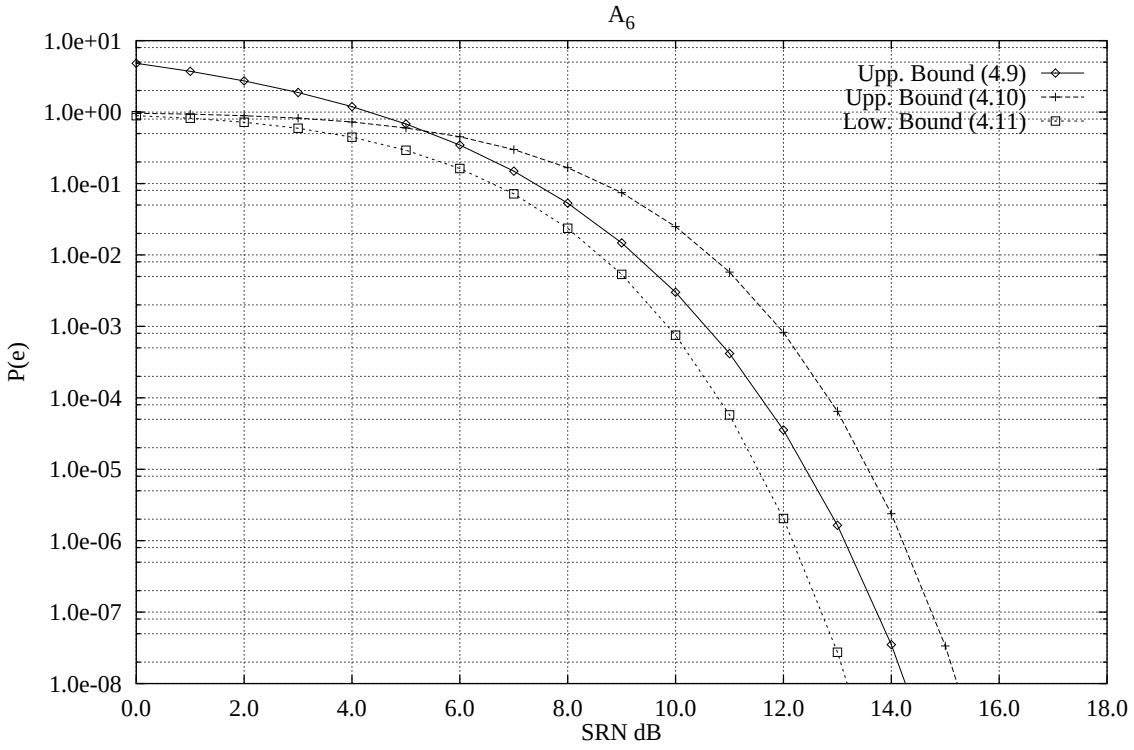

Figure 4.7: Upper and lower bounds to point error probability for A_6.

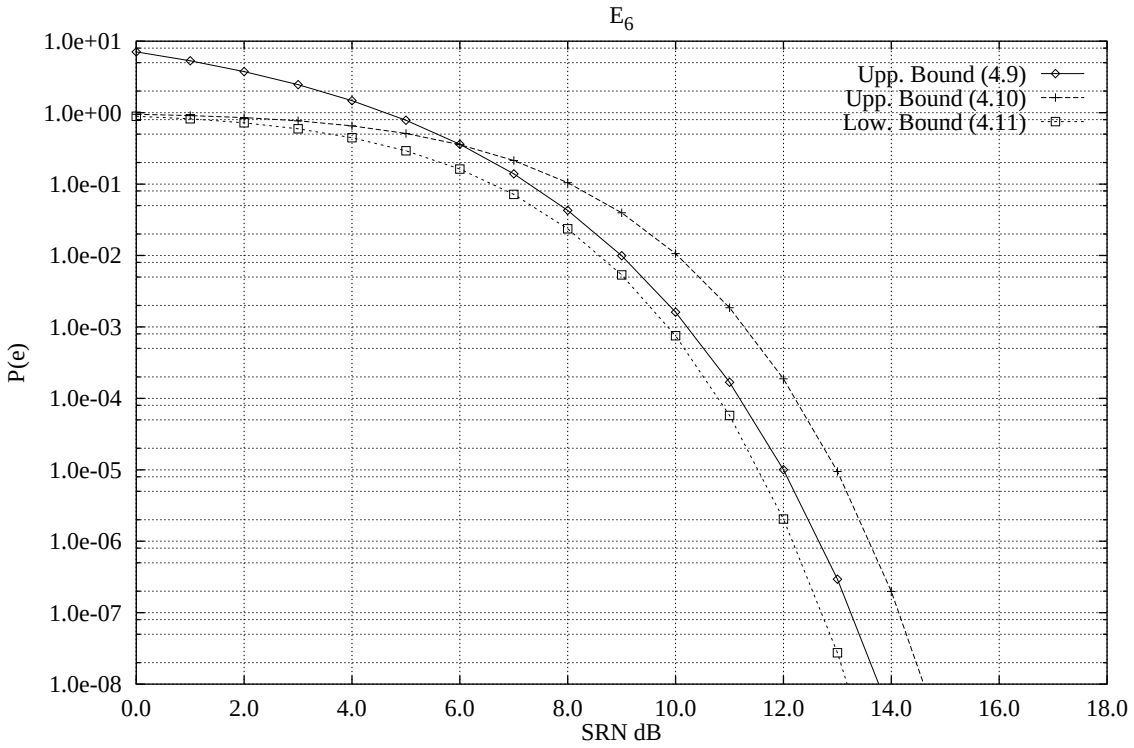

Figure 4.8: Upper and lower bounds to point error probability for E_6.

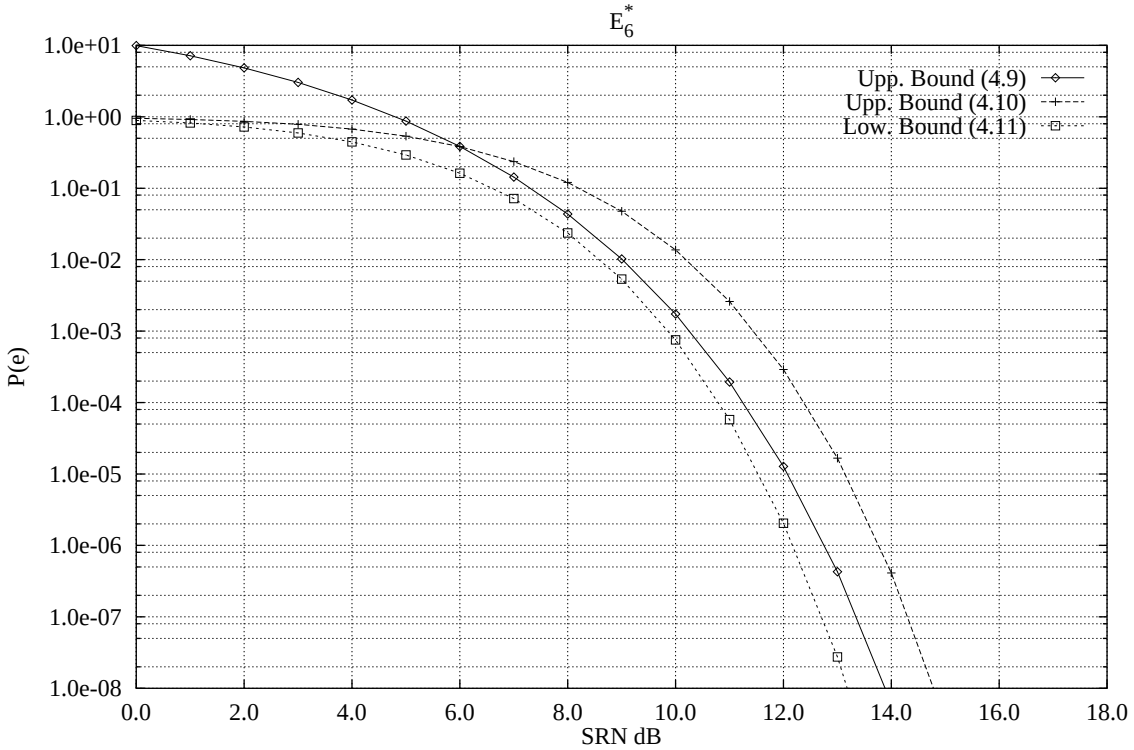

Figure 4.9: Upper and lower bounds to point error probability for E_6^*.

of the generator matrices form the lattice basis. Sometimes a scaled version of the lattices was considered. For the lattices A_n, A_n^*, D_n, D_n^*, $A_6^{(2)}$, E_6, E_6^*, E_7, E_7^* [2] the Voronoi region is known, so the values of the parameters were used to test the accuracy of the program.

4.5.1 New values

The following lattices were considered because they exhibit some interesting feature.

Lattice C_3 (Gram matrix). This lattice was recently proven to be the densest three-dimensional lattice which is geometrically similar to its dual. It is also the thinnest geometrically self-dual covering lattice [1, p. xix]

$$\mathrm{C_3}: \begin{pmatrix} 1+\sqrt{2} & 1 & 1 \\ 1 & 1+\sqrt{2} & 1-\sqrt{2} \\ 1 & 1-\sqrt{2} & 1+\sqrt{2} \end{pmatrix}$$

Lattice Di_{4a} and Di_{4b} (Gram matrices). These two lattices, found by Dickson, together with A_4^* are the three locally optimal lattice coverings in $\mathbf{R}^4$ [28]. The values of $G(\Lambda)$, reported in Table 4.6, answer the question posed in [1, p. 62].

$$\mathrm{Di_{4a}}: \begin{pmatrix} 2 & \alpha & -1 & -1 \\ \alpha & 2 & -1 & -1 \\ -1 & -1 & 2 & 1-\alpha \\ -1 & -1 & 1-\alpha & 2 \end{pmatrix} \qquad \mathrm{Di_{4b}}: \begin{pmatrix} 3-\gamma & \gamma & -1 & -1 \\ \gamma & 3-\gamma & -1 & -1 \\ -1 & -1 & 2+2\beta & -\beta \\ -1 & -1 & -\beta & 2+2\beta \end{pmatrix}$$

where $\alpha = (5-\sqrt{13})/2$ and $\beta \approx 0.544, \gamma \approx 0.499$ are roots of certain polynomials.

Lattices BT_n (Gram matrices) This family of extreme lattice coverings was given by Barnes and Trenerry in [29]. These lattices exhibit a normalized thickness which is slightly larger than the one of the family of best known lattice coverings A_n^*. This property prompted the question in [1, p. 62] and for $n = 5$ we find that we do not improve over the best known lattice quantizer.

For $n \geq 5$ the Gram matrix is given by

$$\mathrm{BT_n}: \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \cdots \\ 0 & n-1 & -1 & -1 & -1 & \\ 0 & -1 & n-1 & -1 & -1 & \\ 0 & -1 & -1 & n-1 & -1 & \\ 0 & -1 & -1 & -1 & n-1 & \\ \vdots & & & & & \ddots \end{pmatrix} + \frac{\beta_n}{4} \begin{pmatrix} n & n-2 & -2 & -2 & \cdots \\ n-2 & n & -2 & -2 & \\ -2 & -2 & & & \\ -2 & -2 & & 4I_{n-2} & \\ \vdots & -2 & & & \end{pmatrix}$$

where I_{n-2} is the $(n-2)$-dimensional identity matrix and β_n is the positive root of

$$3(n-3)x^2 + (n^2-8n-6)x - 4n(n+1) = 0$$

[2] $A_6^{(2)}$ is the self-dual lattice is obtained by using Craig's construction [1, p. 223]. Its normalized second moment was computed exactly by Coulson in [24].

Lattices Is_{5a} and Is_{5b} (Gram matrices) This is a pair of five-dimensional iso-spectral lattices (i.e. inequivalent lattices with the same theta series). See [1, p. xxi].

$$\mathrm{Is_{5a}}: \begin{pmatrix} 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 8 & 4 \\ 2 & 0 & 2 & 4 & 8 \end{pmatrix} \qquad \mathrm{Is_{5b}}: \begin{pmatrix} 2 & 1 & 0 & 2 & 2 \\ 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 6 & 4 & 4 \\ 2 & 2 & 4 & 8 & 4 \\ 2 & 2 & 4 & 4 & 8 \end{pmatrix}$$

4.6 Conclusions

In this chapter we have presented an algorithm which computes the Voronoi cell of an arbitrary lattice. The knowledge of the Voronoi cell enables one to exactly compute all the relevant lattice parameters. Using the diamond-cutting algorithm we have found some previously unknown values of the quantizing constants of some important lattices.

Most of the computational problems related to lattices are either known or conjectured to be NP-hard [1, p. 40]. The principal limitation in the application of the DCA is the exponentially increasing memory requirement. It is enough to recall that the number of nodes required to describe the fundamental parallelotope is 3^d. The final number of nodes for the Voronoi cell greatly varies between different lattices in the same dimension. With 32MB RAM we have reached dimensions between 6 and 8 according to the lattice type. The possibility of reducing the memory requirements appears remote especially if we want to preserve the generality of the algorithm.

	δ	θ	$G(\mathcal{V})$	N_0	N_1	N_2	N_3	N_4	N_5	N_6	N_7	Total
A_2	0.288676	0.384900	0.080188	6	6							12
A_3	0.176777	0.500000	0.078745	14	24	12						50
A_4	0.111803	0.643990	0.078020	30	70	60	20					180
A_5	0.072170	1.125016	0.077648	62	180	210	120	30				602
A_6	0.047246	1.904147	0.077466	126	434	630	490	210	42			1932
A_7	0.031250	4.000000	0.077396	254	1008	1736	1680	980	336	56		6050
A_8	0.020833	8.128842	0.077391	510	2286	4536	5208	3780	1764	504	72	18660

	vol($\mathcal{V}$)	Facet profile (ρ^2, τ)		Vertices profile (R^2)	
A_2	1.732043	**0.499999**	**6**	**0.666664**	6
A_3	1.999991	**0.499999**	**12**	0.749997	8
				0.999999	6
A_4	2.236056	**0.499999**	**20**	0.799997	10
				1.199999	20
A_5	2.449449	**0.499999**	**30**	0.833330	12
				1.333325	30
				1.499999	20
A_6	2.645751	**0.500000**	**42**	0.857143	14
				1.428571	42
				1.714286	70
A_7	2.828427	**0.500000**	**56**	0.875000	16
				1.500000	56
				1.875000	112
				2.000000	70
A_8	3.000000	**0.500000**	**72**	0.888889	18
				1.555556	72
				2.000000	168
				2.222222	252

Table 4.1: Lattices A_n

	δ	θ	$G(\mathcal{V})$	N_0	N_1	N_2	N_3	N_4	N_5	Total
A_2^*	0.288676	0.384900	0.080188	6	6					12
A_3^*	0.162380	0.349385	0.078543	24	36	14				74
A_4^*	0.089444	0.357770	0.077559	120	240	150	30			540
A_5^*	0.048526	0.403566	0.076922	720	1800	1560	540	62		4682
A_6^*	0.026033	0.493668	0.076490	5040	15120	16800	8400	1806	126	47292

	vol($\mathcal{V}$)	Facet profile (ρ^2, τ)		Vertices profile (R^2)	
A_2^*	1.732043	**0.499999**	**6**	**0.666664**	6
A_3^*	3.999995	**0.750000**	**8**	1.249997	24
		0.999991	6		
A_4^*	11.18038	**1.000012**	**10**	**2.000000**	120
		1.499994	20		
A_5^*	36.00000	**1.250000**	**12**	**2.916667**	720
		2.000000	30		
		2.250000	20		
A_6^*	129.6418	**1.500000**	**14**	**4.000000**	5040
		2.500000	42		
		3.000000	70		

Table 4.2: Dual lattices A_n^*

	δ	θ	$G(\mathcal{V})$	N_0	N_1	N_2	N_3	N_4	N_5	N_6	N_7	Total
D_2	0.250000	0.500000	0.083333	4	4							8
D_3	0.176777	0.500000	0.078745	14	24	12						50
D_4	0.125000	0.500000	0.076603	24	96	96	24					240
D_5	0.088388	0.873464	0.075786	42	240	400	240	40				2002
D_6	0.062500	1.687501	0.075591	76	576	1200	1120	480	60			3512
D_7	0.044194	3.544893	0.075686	142	1344	3360	3920	2520	840	84		12210
D_8	0.031250	8.000000	0.075914	272	3072	8960	12544	10080	4928	1344	112	41312

	vol($\mathcal{V}$)	Facet profile (ρ^2, τ)		Vertices profile (R^2)	
D_2	8.000000	**2.000000**	**4**	**4.000000**	4
D_3	16.00000	**2.000000**	**12**	3.000000	8
				4.000000	6
D_4	32.00001	**2.000000**	**24**	**4.000000**	24
D_5	64.00000	**2.000000**	**40**	4.000000	10
				5.000000	32
D_6	127.9999	**2.000000**	**60**	4.000000	12
				6.000000	64
D_7	256.0000	**2.000000**	**84**	4.000000	14
				7.000000	128
D_8	512.0000	**2.000000**	**112**	4.000000	16
				8.000000	256

Table 4.3: Lattices D_n

	δ	θ	$G(\mathcal{V})$	N_0	N_1	N_2	N_3	N_4	N_5	N_6	Total
D_2^*	0.250000	0.500000	0.083333	4	4						8
D_3^*	0.162377	0.349384	0.078543	24	36	14					76
D_4^*	0.125000	0.500000	0.076603	24	96	96	24				240
D_5^*	0.062500	0.474610	0.075625	240	720	720	280	42			2002
D_6^*	0.031250	0.843750	0.075120	160	1440	2880	2160	636	76		7352
D_7^*	0.015625	0.966967	0.074859	2240	10080	17920	15120	6328	1428	142	53258

	vol($\mathcal{V}$)	Facet profile (ρ^2, τ)		Vertices profile (R^2)	
D_2^*	2.000000	**0.500000**	**4**	**1.000000**	4
D_3^*	4.000006	**0.749992**	**8**	**1.249997**	24
		0.999998	6		
D_4^*	8.000000	**1.000000**	**24**	**2.000000**	24
D_5^*	16.00000	**1.000000**	**10**	**2.250001**	240
		1.249999	32		
D_6^*	32.00000	**1.000000**	**12**	**3.000000**	160
		1.500000	64		
D_7^*	63.99999	**1.000000**	**14**	**3.250000**	2240
		1.750000	128		

Table 4.4: Dual lattices D_n^*

	δ	θ	$G(\mathcal{V})$	N_0	N_1	N_2	N_3	N_4	N_5	N_6	Total
$A_6^{(2)}$	0.053995	0.644791	0.075057	798	4368	6944	4452	1176	98		17836
E_6	0.072169	1.368545	0.074347	54	702	2160	2160	720	72		5868
E_6^*	0.064150	0.513201	0.074244	720	6480	10800	6480	1566	126		26172
E_7	0.062500	2.922836	0.073231	632	4788	16128	20160	10080	2016	126	53930
E_7^*	0.045669	0.886223	0.073116	576	10080	40320	50400	23688	4284	182	129530

	vol($\mathcal{V}$)	Facet profile (ρ^2, τ)		Vertices profile (R^2)	
$A_6^{(2)}$	18.520261	**0.999999**	**42**	2.000001	336
		1.500000	56	**2.285715**	462
E_6	1.732037	**0.499998**	**72**	**1.333333**	54
E_6^*	0.577350	**0.333333**	**54**	**0.666667**	720
		0.500000	72		
E_7	16.00000	**1.000000**	**126**	1.750000	576
				3.000000	56
E_7^*	0.707107	**0.375000**	**56**	0.875000	576
		0.500000	126		

Table 4.5: Other lattices

	δ	θ	$G(\mathcal{V})$	N_0	N_1	N_2	N_3	N_4	N_5	Total
C_3	0.165779	0.386206	0.078670	24	36	14				74
Di_{4a}	0.113027	0.390822	0.076993	120	240	150	30			540
Di_{4b}	0.076078	0.381728	0.077465	120	240	150	30			540
BT_5	0.035124	0.423672	0.076278	720	1800	1560	540	62		4682
Is_{5a}	0.018042	1.379132	0.084734	48	120	116	54	12		350
Is_{5b}	0.018042	0.848806	0.082839	114	468	600	288	44		1514

	vol($\mathcal{V}$)	Facet profile (ρ^2, τ)		Vertices profile (R^2)	
C_3	2.828427	**0.603553**	**8**	0.957107	8
		0.707107	4	**1.060660**	16
		1.000000	2		
Di_{4a}	2.211152	**0.499998**	**18**	0.904520	90
		0.651365	6	**0.929606**	30
		0.848671	6		
Di_{4b}	5.138604	**0.625246**	**4**	1.375344	60
		0.771980	6	**1.400553**	60
		0.897196	12		
		1.000956	2		
		1.271960	6		
BT_5	170.8081	**2.047607**	**2**	1.375344	60
		2.638084	10	**5.543897**	720
		3.047608	10		
		3.547607	20		
		4.776172	20		
Is_{5a}	9.797850	**0.499997**	**6**	**2.833313**	48
		0.999999	6		
Is_{5b}	9.797875	**0.499998**	**6**	1.999988	48
		0.999999	18	**2.333330**	66
		1.499996	20		

Table 4.6: Some new values

Chapter 5

Design of lattice constellations for both Rayleigh fading and Gaussian channel

Recent work on lattices matched to the Rayleigh fading channel has shown the way to construct good signal constellations with high spectral efficiency. In this chapter we present a new family of lattice constellations, based on complex algebraic number fields, which have good performance on Rayleigh fading channels. Some of these lattices also exhibit a reasonable packing density and thus may be used at the same time over a Gaussian channel. Conversely, we show that particular versions of the best lattice packings (D_4, E_6, E_8, K_{12}, Λ_{16}, Λ_{24}), constructed from totally complex algebraic cyclotomic fields, exhibit better performance over the Rayleigh fading channel. The practical interest in such signal contellations rises from the need to transmit information at high rates over both terrestrial and satellite links [50].

5.1 Introduction

The interest in TCM for fading channels dates back to 1988, when Divsalar and Simon [31] fixed design rules and performance evaluation criteria. Following the ideas in [31], Schlegel and Costello [32] found new 8-PSK trellis codes for the Rayleigh channel. These codes exhibit higher diversity than Ungerboeck's 8-PSK codes, only when the trellis exceeds 64 states.

An alternative method to gain diversity is the use of multidimensional 8-PSK trellis codes proposed by Pietrobon et al. [33]. Although these schemes were designed for the Gaussian channel they show reasonable diversity when the number of states exceeds 16.

All the above TCM schemes have a spectral efficiency of two bits per symbol. The spectral efficiency can be increased by using Ungerboeck's [34] multidimensional QAM trellis codes, but their inherent diversity is very bad due to uncoded bits, which induce parallel transitions in the trellis [31].

Signal constellations having lattice structure are commonly accepted as good means for transmission with high spectral efficiency. The problem of finding good signal constellations for the Gaussian channel can be restated in terms of lattice sphere packings. Good lattice constellations for the Gaussian channel can be carved from lattices with high sphere packing density [1]. The linear and highly symmetrical structure of lattices usually simplifies the decoding task.

For the Rayleigh fading channel the basic ideas remain the same. The problem is to construct signal constellations with minimum average energy for a desired error rate, given their spectral efficiency. A very interesting approach has been recently proposed [36, 37], which makes use of some results of algebraic number theory. Using totally real algebraic number fields, some good lattice constellations matched to the Rayleigh fading channel, up to dimension eight, are found. The effectiveness of these constellations lies in their high degree of diversity, which is actually the maximum possible. By diversity we intend the number of different values in the components of any two distinct points of the constellation.

The signal constellations for the Gaussian channel are usually very bad when used over the Rayleigh fading channel since they have small diversity. Viceversa, the signal constellations in [37] matched to the Rayleigh fading channel are usually very bad when used over the Gaussian channel since the sphere packing density of these lattices is low. In this chapter we search for lattice constellations which have good performance on both Gaussian and Rayleigh fading channel. The same constellations may be used for the Ricean channel which stands in between the Gaussian and the Rayleigh channel.

The practical interest in such signal contellations rises from the need to transmit information over both terrestrial and satellite links.

The chapter outline is the following. In Section 5.2 we show the system model and give the basic definitions. In Section 5.3 we analyze the error probability bounds to find an effective approach to the search of good constellations. The final target of this work is to find good constellations for the Gaussian and the Rayleigh fading channel; we will present two different approaches. The first (Sections 5.4 and 5.5), considers some constellations constructed for the fading channel and trades some of their diversity for a higher asymptotic gain over the

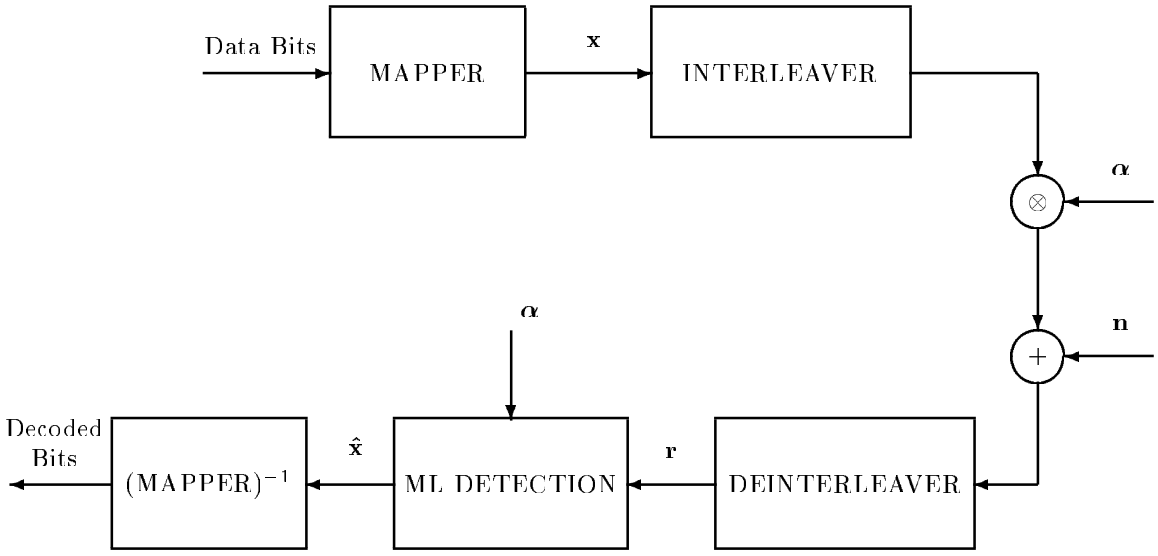

Figure 5.1: The transmission system

Gaussian channel. These constellations are obtained using some results in algebraic number theory, which will be presented in the various subsections. The second approach (Section 5.6) goes in the opposite direction. Starting from good constellations for the Gaussian channel we try modifying them to increase their diversity. In this section we will need some further results in algebraic number theory related to ideals and their factorization. Section 5.7 will illustrate the decoding algorithm used with these lattice constellations together with practical results. Finally, in the conclusions we discuss the two different approaches to establish which one is the most effective.

5.2 System model and terminology

The baseband transmission system is shown in Figure 5.1. The mapper associates an m-uple of input bits with a signal point $\mathbf{x} = (x_1, x_2, \ldots x_n)$ in the n-dimensional Euclidean space $\mathbf{R}^n$. Let $M = 2^m$ be the total number of signal points in the constellation. An interleaver precedes the channel in the system model. It interleaves the real components of the sequence of mapped points. The constellation points are transmitted either over an additive white Gaussian noise (AWGN) channel, giving $\mathbf{r} = \mathbf{x} + \mathbf{n}$, or over an independent Rayleigh fading channel (RFC) giving $\mathbf{r} = \boldsymbol{\alpha} \otimes \mathbf{x} + \mathbf{n}$, where $\mathbf{r}$ is the received point. $\mathbf{n} = (n_1, n_2, \ldots n_n)$ is a noise vector, whose real components n_i are zero mean, N_0-variance Gaussian distributed independent random variables. $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ are the random fading coefficients with unit variance and $\otimes$ represents the componentwise product. Signal demodulation is assumed

to be coherent, so that the fading coefficients can be modeled after phase elimination, as real random variables with a Rayleigh distribution. The independence of the fading samples represents the situation where the components of the transmitted points are perfectly interleaved.

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

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

and the signal-to-noise ratio per bit is given by

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

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

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

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

for AWGN channel and

$$m(\mathbf{x}|\mathbf{r}, \boldsymbol{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2 \tag{5.2}$$

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

5.3 Searching for optimal lattice constellations

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

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

$$P_e(S) \leq P_e(\Lambda) \leq \sum_{\mathbf{y} \neq \mathbf{x}} P(\mathbf{x} \rightarrow \mathbf{y}) \tag{5.3}$$

where $P(\mathbf{x} \rightarrow \mathbf{y})$ is the pairwise error probability, the probability that the received point is 'closer' to $\mathbf{y}$ than to $\mathbf{x}$ according to the metric defined in (5.1) or (5.2), when $\mathbf{x}$ is transmitted.

The first inequality takes into account the edge effects of the finite constellation S compared to the infinite lattice Λ.

For the AWGN channel equation (5.3) simply becomes [1, Chap. 3]

$$P_e(\Lambda) \approx \frac{\tau}{2}\mathrm{erfc}\left(\frac{d_{Emin}/2}{\sqrt{2N_0}}\right) \tag{5.4}$$

where τ is the *kissing number* and d_{Emin} is the *minimum Euclidean distance* of the lattice. The error probability per point of a cubic constellation can be easily approximated, for large E_b/N_0, with a function of the signal-to-noise ratio, (see appendix A), given by

$$P_e(S) \approx \frac{\tau}{2}\mathrm{erfc}\left(\sqrt{\frac{3s}{2^{s+1}}\frac{E_b}{N_0}\gamma(\Lambda)}\right) \tag{5.5}$$

where

$$\gamma(\Lambda) = \frac{d^2_{Emin}}{vol(\Lambda)^{2/n}} \tag{5.6}$$

is the *fundamental gain* of Λ defined in Chapter 2. We recall that $\gamma(\mathbf{Z}^n) = 1$, so that $\gamma(\Lambda)$ is the asymptotic gain of Λ over $\mathbf{Z}^n$. For spherical constellations the total gain should also take into account the shape gain.

For the Rayleigh fading channel, the standard Chernoff bound technique [31] or the direct computation using the Gaussian tail function approximation (see appendix B), give an estimate of the pairwise error probability

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2}\prod_{i=1}^{n}\frac{1}{1+\frac{(x_i-y_i)^2}{8N_0}} \tag{5.7}$$

and for large signal-to-noise ratios

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{1}{2}\prod_{x_i \neq y_i}\frac{1}{\frac{(x_i-y_i)^2}{8N_0}} = \frac{1}{2}\frac{1}{\left(\frac{s}{8}\frac{E_b}{N_0}\right)^l d_p^{(l)}(\mathbf{x},\mathbf{y})^2} \tag{5.8}$$

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

$$d_p^{(l)}(\mathbf{x},\mathbf{y})^2 = \frac{\prod_{x_i \neq y_i}(x_i-y_i)^2}{(E/n)^l}\ . \tag{5.9}$$

Asymptotically, (5.3) is dominated by the term $1/(E_b/N_0)^L$ where L is the minimum number of different components of any two distinct constellation points. L is the so called *diversity* of the signal constellation.

In general rearranging equation (5.3) we obtain

$$P_e(\Lambda) \leq \frac{1}{2}\sum_{l=L}^{n}\frac{K_l}{\left(\frac{s}{8}\frac{E_b}{N_0}\right)^l} \tag{5.10}$$

where $K_l = \sum_{d_p^{(l)}} \frac{A_{d_p^{(l)}}}{(d_p^{(l)})^2}$. $A_{d_p^{(l)}}$ is the number of points $\mathbf{y}$ at l-product distance $d_p^{(l)}$ from $\mathbf{x}$ and with l different components, $L \leq l \leq n$. The series in K_l can be interpreted as a *theta series* of the lattice [1], when the product distance is considered instead of the Euclidean distance.

In equation (5.10) we find all the ingredients to obtain a low error probability at a given signal-to-noise ratio E_b/N_0. In order of relevance we have to :

1. Maximize the diversity $L = \min(l)$.
2. Minimize the average energy per constellation point E.
3. Minimize K_l and especially take care of $d_{p,min} = \min(d_p^{(L)}(\mathbf{x}, \mathbf{y}))$ and $\tau_p = A_{d_p^{(L)}}$ the kissing number for the L-product distance.

The terms in (5.10) clearly become less important when l increases, but the values of $A_{d_p^{(l)}}$ and $d_p^{(l)}(\mathbf{x}, \mathbf{y})$ should be taken into account for non asymptotic considerations.

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

$$\gamma_{asympt.} = \left(\frac{K_L(1)}{K_L(2)} \right)^{1/L} \tag{5.11}$$

with the definitions given above. In general, the asymptotic coding gain may not be defined for systems with different diversities L_1 and L_2; in such cases it is still interesting to have an estimate of the coding gain at a given bit error probability $P_b(e)$. Letting $E_{b,2}/N_0$ be the signal-to-noise ratio of the system (2) corresponding to $P_{b,2}(e)$ we have

$$\gamma(E_{b,2}/N_0) = \left(\frac{K_{L_1}(1)}{K_{L_2}(2)} \right)^{1/L_1} \left(\frac{s}{8} \frac{E_{b,2}}{N_0} \right)^{\frac{L_2 - L_1}{L_1}} \tag{5.12}$$

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

5.4 Lattices from algebraic number fields

In the following, we will assume that the reader is familiar with the basic definitions on lattices (see [1]) and we show how to construct lattices from algebraic number fields. We will present only the strictly relevant definitions and results in algebraic number theory, which lead to the lattice construction. The exposition is self-contained and is based on simple examples, but the interested reader may refer to any book on algebraic number theory to quench his thirst for rigour (e.g. [41, 42, 43]).

5.4.1 Algebraic number fields

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

Definition 19 – *Let α be an element of K, we say that α is an* **algebraic number** *if it is a root of a monic polynomial with coefficients in $\mathbf{Q}$. Such polynomial with lowest degree is called the minimal polynomial of α and denoted $\mu_\alpha(x)$. If all the elements of K are algebraic we say that K is an* **algebraic extension** *of $\mathbf{Q}$.*

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

Definition 20 – *We say that $\alpha \in K$ is an* **algebraic integer** *if it is a root of a monic polynomial with coefficients in $\mathbf{Z}$. The set of algebraic integers of K is a ring called the* **ring of integers** *of K and is indicated with O_K.*

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

Definition 21 – *We define the* **degree** $[K : \mathbf{Q}]$ *of an algebraic extension K of $\mathbf{Q}$ as the dimension of K when considered as a vector space over $\mathbf{Q}$. An* **algebraic number field** *is an algebraic extension of $\mathbf{Q}$ of finite degree.*

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

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

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

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

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

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

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

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

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

5.4.2 Integral basis and canonical embedding

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

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

Definition 22 – *Let $(\omega_1, \omega_2, \ldots \omega_n)$ be a basis of K. We say that (ω_i) is an* **integral basis** *of K if $O_K = \mathbf{Z}(\omega_1, \omega_2, \ldots \omega_n)$, that is, if (ω_i) is a generating set of the $\mathbf{Z}$-module O_K. So that we can write any element of O_K as $\sum_{i=1}^{n} a_i\omega_i$ with $a_i \in \mathbf{Z}$.*

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

There exist efficient algorithms to find an integral basis of a given algebraic number field in polynomial time [39, 40].

Definition 23 – *Let K and K' be two number fields containing $\mathbf{Q}$, we call $\phi : K \to K'$ a* **$\mathbf{Q}$-homomorphism** *if $\phi(a) = a$ for each $a \in \mathbf{Q}$. If $K' = \mathbf{C}$, the field of complex numbers, a $\mathbf{Q}$-homomorphism $\phi : K \to \mathbf{C}$ is called an* **embedding** *of K into $\mathbf{C}$.*

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

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

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

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

Definition 24 – *The elements* $\sigma_1(\alpha), \sigma_2(\alpha), \ldots \sigma_n(\alpha)$ *are called the* **conjugates** *of* α *and*

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

is the **algebraic norm** *of* α.

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

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

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

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

Definition 25 – *Let* $(\omega_1, \omega_2, \ldots \omega_n)$ *be an integral basis of* K. *The* **absolute discriminant** *of* K *is defined as* $d_K = \det[\sigma_j(\omega_i)]^2$.

Result 6 – *The absolute discriminant belongs to* **Z**.

Example 3 (cont.) - Applying the 2 **Q**-homomorphisms to the integral basis ω_1, ω_2, we obtain

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

Definition 26 – *Let* $(\sigma_1, \sigma_2, \ldots \sigma_n)$ *be the* n **Q**-*homomorphisms of* K *into* **C**. *Let* r_1 *be the number of* **Q**-*homomorphisms with image in* **R**, *the field of real numbers, and* $2r_2$ *the number of* **Q**-*homomorphisms with image in* **C** *so that*

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

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

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

Definition 27 – *Let us order the σ_i's so that $\sigma_i(\alpha) \in \mathbf{R}$ for $1 \leq i \leq r_1$ and $\sigma_{j+r_2}(\alpha)$ is the complex conjugate of $\sigma_j(\alpha)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. We call* **canonical embedding** *$\sigma : K \longrightarrow \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ the isomorphism defined by*

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

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

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

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

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

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

$$G = \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_{r_1}(\omega_1) & \Re\sigma_{r_1+1}(\omega_1) & \Im\sigma_{r_1+1}(\omega_1) & \dots & \Re\sigma_{r_1+r_2}(\omega_1) & \Im\sigma_{r_1+r_2}(\omega_1) \\ \sigma_1(\omega_2) & \dots & \sigma_{r_1}(\omega_2) & \Re\sigma_{r_1+1}(\omega_2) & \Im\sigma_{r_1+1}(\omega_2) & \dots & \Re\sigma_{r_1+r_2}(\omega_2) & \Im\sigma_{r_1+r_2}(\omega_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\omega_n) & \dots & \sigma_{r_1}(\omega_n) & \Re\sigma_{r_1+1}(\omega_n) & \Im\sigma_{r_1+1}(\omega_n) & \dots & \Re\sigma_{r_1+r_2}(\omega_n) & \Im\sigma_{r_1+r_2}(\omega_n) \end{pmatrix} \quad (5.13)$$

The vectors $\mathbf{v}_i$ are the rows of G. The volume of the fundamental paralletotope of Λ is given by [41]

$$vol(\Lambda) = |\det(G)| = 2^{-r_2} \times \sqrt{|d_K|} \quad (5.14)$$

5.4.3 Totally real and totally complex number fields

Result 8 *The lattices obtained from the generator matrix (5.13) exhibit a diversity $L = r_1 + r_2$.*

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

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

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

$$\prod_{i=1}^{n} |z_i| = \prod_{i=1}^{n} \left| \sum_{j=1}^{n} \lambda_j v_{ij} \right| = \prod_{i=1}^{r_1} \left| \sigma_i \left(\sum_{j=1}^{n} \lambda_j \omega_j \right) \right| \times \prod_{i=r1+1}^{r_1+r_2} \left| \Re\sigma_i \left(\sum_{j=1}^{n} \lambda_j \omega_j \right) \right| \times \prod_{i=r1+1}^{r_1+r_2} \left| \Im\sigma_i \left(\sum_{j=1}^{n} \lambda_j \omega_j \right) \right| \tag{5.15}$$

The minimum number of non-zero factors is $r_1 + r_2$ since the real and imaginary parts of any one of the complex embeddings may not be simultaneously zero. We then conclude that for such lattices we have a diversity $L \geq r_1 + r_2$. Now, let us take the special element $\alpha = 1$ in O_K. The canonical embedding applied to 1 gives exactly $r_1 + r_2$ non zero terms in the above product. Hence, we can confirm that $L = r_1 + r_2$, as conjectured in [38]. Q.E.D.

In the case of totally real algebraic number fields ($r_2 = 0$), presented in [37], we have

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

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

$$\begin{aligned} d_p^{(n)}(\mathbf{0}, \mathbf{z}) &= \prod_{i=1}^{n} |z_i| = \prod_{i=1}^{n} \left| \sum_{j=1}^{n} \lambda_j v_{ij} \right| = \prod_{i=1}^{n} \left| \sum_{j=1}^{n} \lambda_j \sigma_i(\omega_j) \right| \\ &= \prod_{i=1}^{n} \left| \sigma_i \left(\sum_{j=1}^{n} \lambda_j \omega_j \right) \right| = \left| N \left(\sum_{j=1}^{n} \lambda_j \omega_j \right) \right| \end{aligned} \tag{5.16}$$

Since $\sum_{j=1}^{n} \lambda_j \omega_j \in O_K$ and it is different from zero, according to Result 5, we have

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

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

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

The totally real algebraic number fields with minimum absolute discriminant are known up to dimension 8 (first column of Table 5.1) and appear to be the best asymptotically good lattices for the Rayleigh fading channel. In fact, for a fixed number of points M, the energy of

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

Table 5.1: Minimal absolute discriminants. Values with a * are the best known values.

constellations carved from these lattices is is proportional to $vol(\Lambda)$ and $vol(\Lambda)$ is minimized by selecting the fields with minimum absolute discriminants.

Still two drawbacks are hidden behind the maximal diversity and the minimal absolute discriminant. The fundamental volume can be further reduced if we choose a signature where $r_2 \neq 0$, i.e. if the number field is complex. Equation (14) shows that $vol(\Lambda)$ can be divided by 2^{r_2}. We can even maximize r_2 by working in a totally complex field, $r_2 = n/2$. Lattices derived from totally real number fields have bad performance over a Gaussian channel (a negative fundamental gain as shown in Section 5.7) mainly because of their high values of $vol(\Lambda)$ (Table 5.1). The second drawback appears over the fading channel and is related to the product kissing number τ_p. We find that the product kissing number is much higher for real fields lattices than for complex fields lattices.

Lattices built from complex algebraic number fields have been first proposed in [38]. The totally complex fields are possible only for even degrees since $r_2 = n/2$. The generator matrix is

$$\mathrm{G} = \begin{pmatrix} \Re\sigma_1(\omega_1) & \Im\sigma_1(\omega_1) & \dots & \Re\sigma_{r_2}(\omega_1) & \Im\sigma_{r_2}(\omega_1) \\ \Re\sigma_1(\omega_2) & \Im\sigma_1(\omega_2) & \dots & \Re\sigma_{r_2}(\omega_2) & \Im\sigma_{r_2}(\omega_2) \\ \vdots & & & & \vdots \\ \Re\sigma_1(\omega_n) & \Im\sigma_1(\omega_n) & \dots & \Re\sigma_{r_2}(\omega_n) & \Im\sigma_{r_2}(\omega_n) \end{pmatrix} \tag{5.17}$$

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

Looking at Table 5.1 we immediatly notice that the absolute discriminants of the complex fields are comparatively smaller than the ones for the totally real fields. This fact, combined with the fact that $vol(\Lambda)$ is reduced by a factor 2^{-r_2}, results in lower average energy of the constellation S, for complex fields. Of course the price to pay is the reduced diversity unless we use number fields with higher degrees such as 12, 16 or 24. This lead us to search for good lattices (L_{16} or L_{24}) adapted to Rayleigh channel and the logical continuation is section 6. In the next section, we study in detail some of the lattices constructed by canonical embedding applied to fields in Tables 5.1 and 5.2.

	$\mu_\theta(x)$	$vol(\Lambda_{n,L})$
$\Lambda_{2,1}$	$x^2 - x + 1$	0.8660
$\Lambda_{2,2}$	$x^2 - x - 1$	2.2361
$\Lambda_{3,2}$	$x^3 - x - 1$	2.3979
$\Lambda_{3,3}$	$x^3 + x^2 - 2x - 1$	7
$\Lambda_{4,2}$	$x^4 - x^3 - x^2 + x + 1$	2.7042
$\Lambda_{4,3}$	$x^4 - x^3 + 2x - 1$	8.2916
$\Lambda_{4,4}$	$x^4 - x^3 - 3x^2 + x + 1$	26.9258
$\Lambda_{5,3}$	$x^5 - x^3 + x^2 + x - 1$	10.0281
$\Lambda_{5,4}$	$x^5 - 2x^3 + x^2 - 1$	33.5820
$\Lambda_{5,5}$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	121
$\Lambda_{6,3}$	$x^6 - 3x^5 + 4x^4 - 4x^3 + 4x^2 - 2x + 1$	12.3409
$\Lambda_{6,4}$	$x^6 - 2x^5 + 3x^3 - 2x - 1$	41.8606
$\Lambda_{6,5}$	$x^6 + x^5 - 2x^4 - 3x^3 - x^2 + 2x + 1$	152.2982
$\Lambda_{6,6}$	$x^6 - x^5 - 7x^4 + 2x^3 + 7x^2 - 2x - 1$	547.8367
$\Lambda_{7,7}$	$x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1$	4487.1364
$\Lambda_{8,4}$	$x^8 - 2x^7 + 4x^5 - 4x4 + 3x^2 - 2x + 1$	70.0928
$\Lambda_{8,8}$	$x^8 + 2x^7 - 7x^6 - 8x^5 + 15x^4 + 8x^3 - 9x^2 - 2x + 1$	16801.7980

Table 5.2: Reduced minimal polynomials and fundamental volumes of the corresponding lattices.

5.5 Lattices from minimal absolute discriminant fields

In Table 5.1 we have all the known minimal absolute discriminant fields up to dimension 8. These fields (especially in dimensions above 4) have been a subject of study of a branch of mathematics known as *computational algebraic number theory*. Computational algebraic number theory has developed powerfull algorithmic tools which enable to extend many results, with the aid of computers, to fields of higher degree [39, 40]. Part of this table, up to $n = 6$, can be found in [43] and the references therein. All the totally real fields are listed in [37]. For degree 5 and 6 complex fields see references [44] and [45] respectively. The degree 8, totally complex field of minimal absolute discriminant can be found in [46] together with other 25 totally complex fields of absolute discriminant smaller than 1954287. Table 5.2 gives the *reduced* minimal polynomials of the fields of Table 5.1 along with the fundamental volume of the corresponding lattice obtained from the canonical embedding. A minimal polynomial is called *reduced* if the powers of one of its roots (the primitive element) is an integral basis of the number field. These lattices will be indicated with $\Lambda_{n,L}$.

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

- Find an integral basis of K, which identifies O_K.

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

We show the application of this procedure to some of the lattices of Table 5.2.

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

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

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

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

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

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

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

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

where

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

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

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

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

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

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

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

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

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

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

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

We obtain the lattice generator matrix:

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

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

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

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

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

Table 5.3: Asymptotic gains for the Gaussian channel

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

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

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

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

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

The fundamental volume is $vol(\Lambda_{4,4}) = |\det(G)| = 26.92$ and the minimum squared Euclidean distance is $d^2_{Emin} = 4$. According to Section 5.4.3, the diversity is 4 and $d_{p,min} = 1$.

5.6 Lattices for the Gaussian channel adapted to the fading channel

The idea of rotating a QAM costellation in order to increase its diversity was first presented in [36]. The advantage of such a technique lays in the fact that the rotated constellation holds

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

Table 5.4: Some known lattices from cyclotomic fields

its properties over the Gaussian channel. The method proposed was straightforward: find the rotation angle which gives a diversity of 2 and maximizes the minimum product distance. It was found that for a 16 QAM the rotation angle of $\pi/8$ was optimum. Unfortunately, in dimensions greater than 2 this method becomes impractical.

We have at our disposal the work of Craig [47, 48], who showed how to construct the lattices E_6, E_8, Λ_{24} (Leech lattice) from the totally complex cyclotomic fields $K=\mathbf{Q}(e^{i2\pi/N})$ for $N=9,20,39$. Applying his procedure we found D_4 (Schlafli lattice), K_{12} (Coxeter-Todd's lattice) and Λ_{16} (Barnes-Wall's lattice) from the $8th, 21st$ and the $40th$ root of unity. These lattices are obtained by applying the canonical embedding to particular integral ideals of the above cyclotomic fields. The ideals are given in Table 5.4. The lattices we obtain are actually sublattices of $\sigma(O_K)$. This means that they have the same diversity $L=n/2$ of $\sigma(O_K)$, but a much higher fundamental gain compared to the lattices presented in section 5.

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

5.6.1 Ideals in the ring of integers

In the sequel, all given definitions and properties for ideals are true only in number fields and are not necessarily valid in an arbitrary field. For more theoretical details, the reader is invited to refer to [41], [39] and [40].

Definition 28 – *Let K be a number field of degree n and O_K its ring of integers. An* **ideal** *I of O_K is a sub-Z-module of O_K such that for every $a\in O_K$ and $b\in I$ we have $ab\in I$, breefly $aI\subset I$.*

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

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

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

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

Definition 29 – *An ideal I of O_K is called* **prime** *(or* **maximal***) if the quotient ring O_K/I is a field. I is called* **principal** *if $I = \alpha O_K$ for some algebraic integer α, in this case we also denote $I = (\alpha)$.*

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

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

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

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

$$G_I = \begin{pmatrix} \sigma_1(\gamma_1) & \ldots & \sigma_{r_1}(\gamma_1) & \Re\sigma_{r_1+1}(\gamma_1) & \Im\sigma_{r_1+1}(\gamma_1) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_1) & \Im\sigma_{r_1+r_2}(\gamma_1) \\ \sigma_1(\gamma_2) & \ldots & \sigma_{r_1}(\gamma_2) & \Re\sigma_{r_1+1}(\gamma_2) & \Im\sigma_{r_1+1}(\gamma_2) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_2) & \Im\sigma_{r_1+r_2}(\gamma_2) \\ \vdots & & & \vdots & & & & \vdots \\ \sigma_1(\gamma_n) & \ldots & \sigma_{r_1}(\gamma_n) & \Re\sigma_{r_1+1}(\gamma_n) & \Im\sigma_{r_1+1}(\gamma_n) & \ldots & \Re\sigma_{r_1+r_2}(\gamma_n) & \Im\sigma_{r_1+r_2}(\gamma_n) \end{pmatrix} \tag{5.18}$$

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

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

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

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

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

Result 12

$$vol(\Lambda_I) = N(I) \times 2^{-r_2} \times \sqrt{|d_K|} \tag{5.19}$$

Proof. By definition $N(I)$ is equal to the cardinality of O_K/I. But O_K/I is isomorphic to the quotient Λ/Λ_I due to the canonical embedding σ. Thus, they have the same cardinality (or same index as quotient groups). So we have $N(I) = |\Lambda/\Lambda_I|$. But the group partitioning [35], $\Lambda = \Lambda_I + [\Lambda/\Lambda_I]$, shows that a fundamental region of the sub-lattice Λ_I can be constructed as the disjoint union of $|\Lambda/\Lambda_I|$ copies of a fundamental region of Λ, i.e. $vol(\Lambda_I) = |\Lambda/\Lambda_I| \times vol(\Lambda) = N(I) \times vol(\Lambda)$. Finally, equation (5.19) is obtained by combining $vol(\Lambda_I) = N(I) \times vol(\Lambda)$ and equation (5.19). Q.E.D.

Combining Result 10 with equation (5.19) we have $N(I) = \det T$.

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

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

$$\alpha \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = R(\alpha) \times \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} \tag{5.20}$$

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

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

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

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

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

Example 5 - Let $K = \mathbf{Q}(\sqrt{5})$ and let θ be a primitive element with minimal polynomial $x^2 - x - 1$. Given $\alpha = \theta - 3 \in O_K$, we want to compute the integer transition matrix $T = R(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Using (5.20) with $\omega_i = \theta^{i-1}$ and the identity $\theta^2 = \theta + 1$, derived from the minimal polynomial, we obtain

$$\alpha \begin{pmatrix} 1 \\ \theta \end{pmatrix} = R(\alpha) \begin{pmatrix} 1 \\ \theta \end{pmatrix} \quad \rightarrow \quad \begin{pmatrix} \theta - 3 \\ -2\theta + 1 \end{pmatrix} = \begin{pmatrix} a + b\theta \\ c + d\theta \end{pmatrix}$$

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

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

and equation (5.19) can be easily verified.

We have seen the $\mathbf{Z}$-basis representation of an ideal I. This representation was very practical to get properties for the associated lattice $\Lambda_I = \sigma(I)$. Equation (5.19) is very important and will guide us in the construction of Λ_I. We note also that the norm of the product of two ideals in O_K is equal to the product of the norms, $N(IJ) = N(I)N(J)$. This result is closely related to equation (5.19). Sometimes when searching for an ideal of a given norm $N(I)$ to build Λ_I, we start from an ideal H such that $N(H) = cN(I)$ where c is an integer constant. Clearly, we are tempted to search for an ideal $H = IJ$, $c = N(J)$. Hence, we face the problem of factoring an ideal in the ring of integers. The factorization method for principal ideals is given in Result 16. Unfortunately, the factorization is a litte bit difficult if we use the $\mathbf{Z}$-basis representation of the ideal. The following result shows a new representation of an ideal based on two elements of O_K.

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

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

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

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

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

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

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

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

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

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

Let us check the norm of $I = pO_K$ in the factorization theorem. All the conjugates $\sigma_i(p)$ of p are equal to p because p is an integer. The algebraic norm of p is $N(p) = \prod_i \sigma_i(p) = p^n = N(I)$. From the decomposition formula we see that $N(I) = \prod_{i=1}^{g} N(J_i^{e_i}) = \prod_{i=1}^{g} p^{e_i f_i} = p^n$. It is clear that the factorization of an ideal requires the factorization of a polynomial in a finite field (modulo p). The above algorithm will be used in the next sub-section to decompose prime ideals while building the lattices of Table 5.4. Note that the ideals in Table 5.4 are defined by two O_K-generators. The last two ideals (for Λ_{16} and Λ_{24}) are given as the product of two and three prime ideals respectively.

5.6.2 Lattices from cyclotomic fields ideals

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

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

4. The minimal polynomial of θ is

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

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

5. The absolute discriminant of K is

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

Equation (5.19) is used to compute $N(I)$ given the lattice fundamental volume. $vol(\Lambda)$ is replaced by ρ^n/δ, where ρ is the packing radius and δ is the lattice center density [1]. The search for the rotated lattices of Table 5.4 having dimension n and diversity $n/2$ goes through the following steps:

1. Calculate the minimal polynomial of $e^{i2\pi/N}$ which has degree $\phi(N)$.

2. Find all ideals I of O_K with integer norm

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

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

This procedure was applied succesfully to obtain a generator matrix for each one of the lattices in Table 5.4. The key operation is the factorization of prime ideals presented in Result 16.

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

$D_{4,2}$ – We first note that $\phi(8) = 4$ and that the other values of N giving $\phi(N) = 4$ do not result in the rotated version of D_4, whose center density is $1/8$. The minimal polynomial of $\theta = e^{i2\pi/8}$ is given in Table 5.4 and the absolute discriminant of the field $K = \mathbf{Q}(\theta)$ is $d_K = 2^8$. The signature of K is $(0, 2)$. Using (5.19) we can write

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

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

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

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

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

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

$K_{12,6}$ – We first note that $\phi(21) = 12$ and that the other values of N giving $\phi(N) = 21$ do not result in the rotated version of K_{12}, whose center density is $1/27$. The minimal polynomial of $\theta = e^{i2\pi/12}$ is given in Table 5.4 and the absolute discriminant of the field $K = \mathbf{Q}(\theta)$ is $d_K = 3^6 \cdot 7^{10}$. The signature of K is $(0, 6)$. Using (5.19) we can write

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

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

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

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

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

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

$\Lambda_{16,8}$ – We first note that $\phi(40) = 16$ and that the other values of N giving $\phi(N) = 16$ did not result in the rotated version of Λ_{16}, whose center density is $1/16$. The minimal

polynomial of $\theta = e^{i2\pi/40}$ is given in Table 5.4 and the absolute discriminant of the field $K = \mathbf{Q}(\theta)$ is $d_K = 2^{32} \cdot 5^{12}$. The signature of K is $(0, 8)$. Using (5.19) we can write

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

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

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

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

5.7 Results

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

Figure 5.2 shows the performance of different lattice constellations over the Gaussian channel. Taking $\mathbf{Z}^8$ as a reference we can make the following observations.

- E_8 only gains 2dB at 10^{-5} although its asymptotic coding gain is 3dB [1]. This draws the attention to the limitations of the asymptotic coding gain when used as parameter for practical values of the error probability.

- $\Lambda_{8,8}$, from the totally real field with minimal discriminant, loses (curve on the right of $\mathbf{Z}^8$) 0.9dB at 10^{-5} and asymptotically 1.5dB (Table 5.3), showing the weakness of these lattices over the Gaussian channel.

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

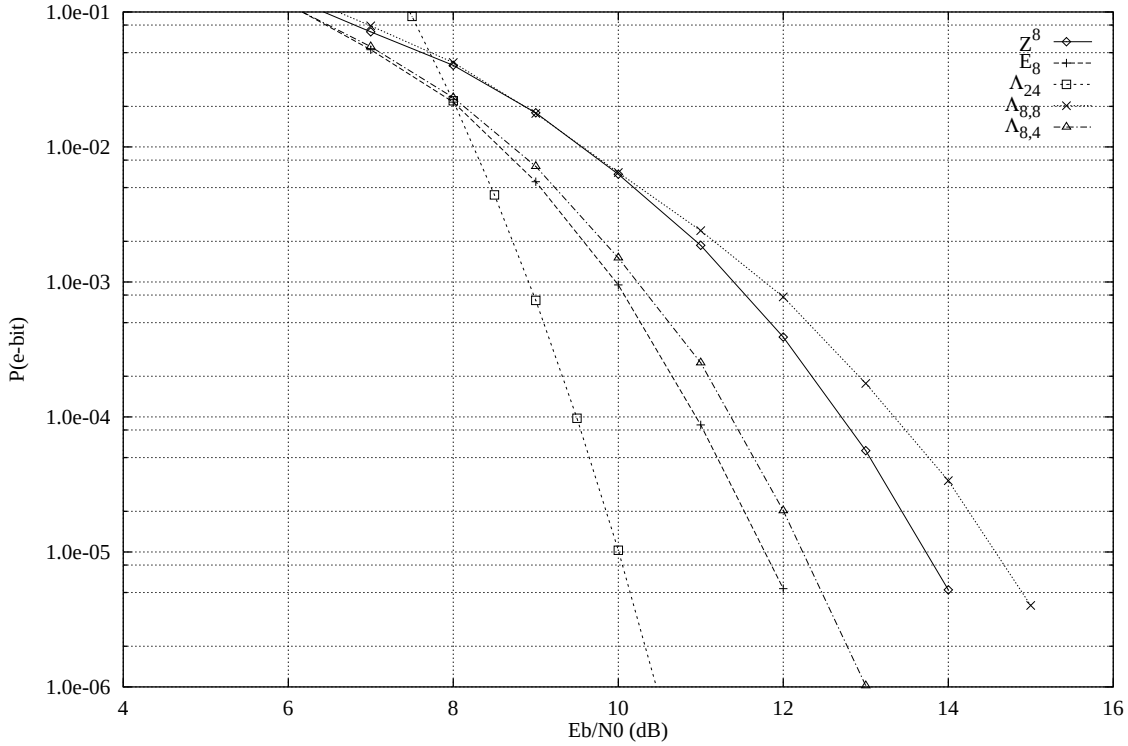

Figure 5.2: Lattice constellations over the Gaussian channel ($s = 4$)

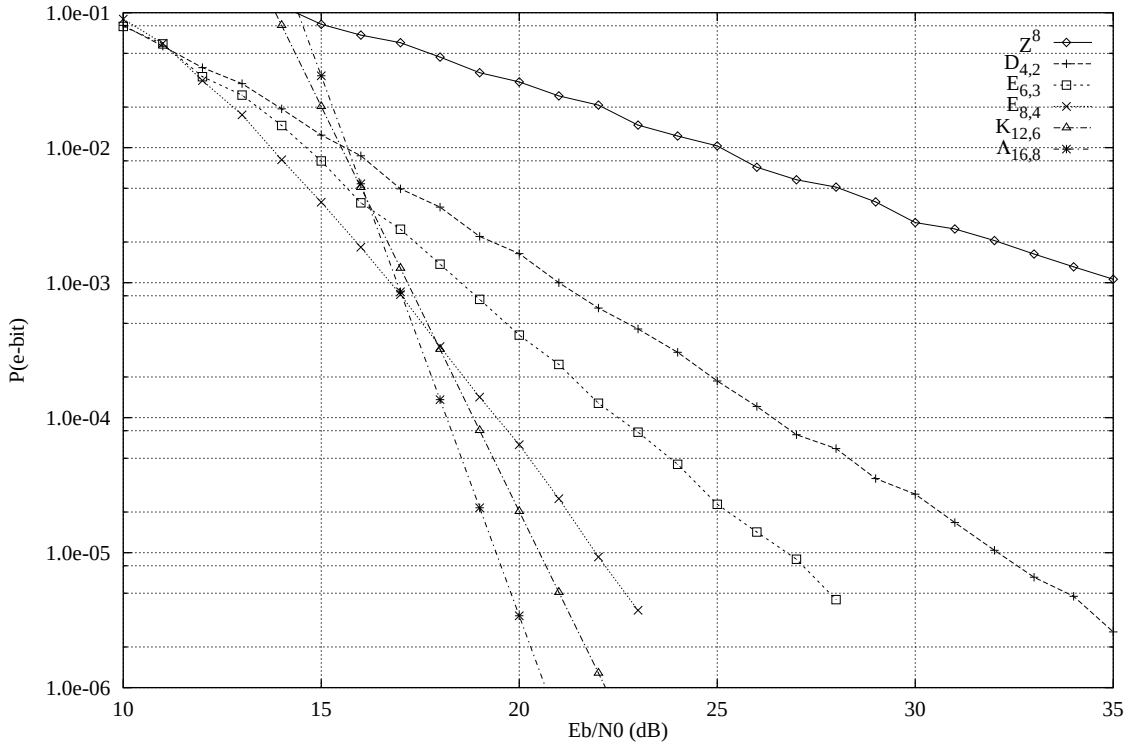

Figure 5.3: Rotated famous lattice constellations over the Rayleigh fading channel ($s = 4$)

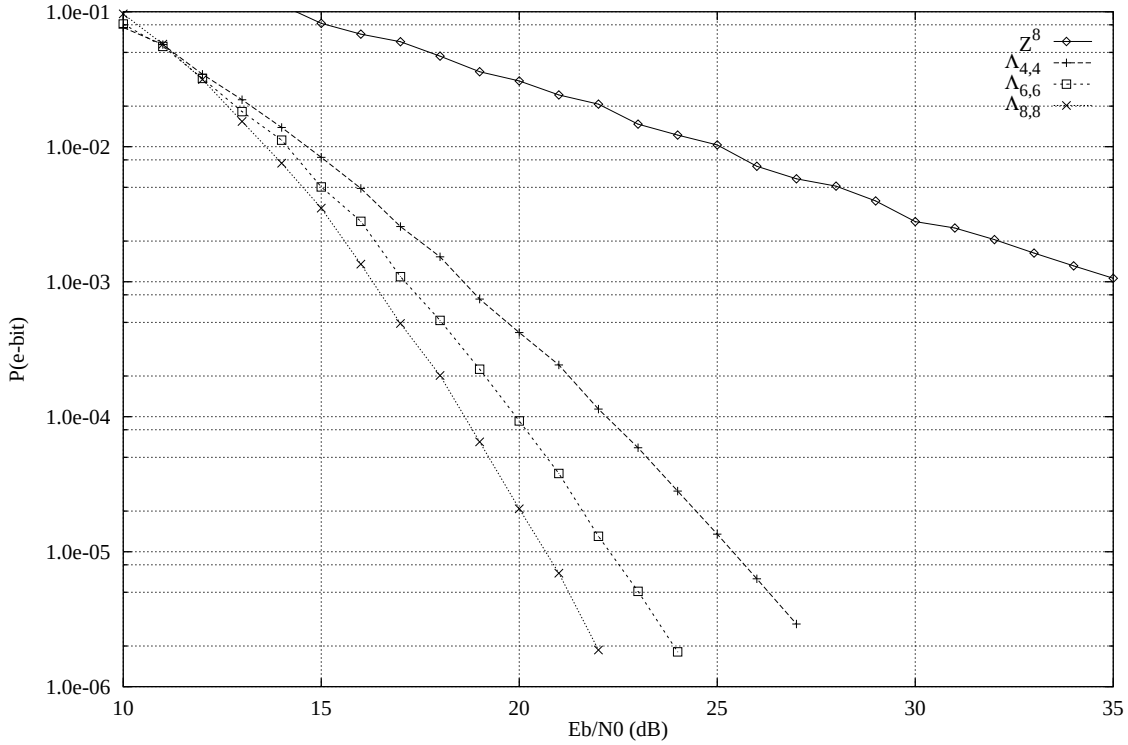

Figure 5.4: Lattice constellations from totally real algebraic number fields of minimal discriminant over the Rayleigh fadind channel ($s = 4$)

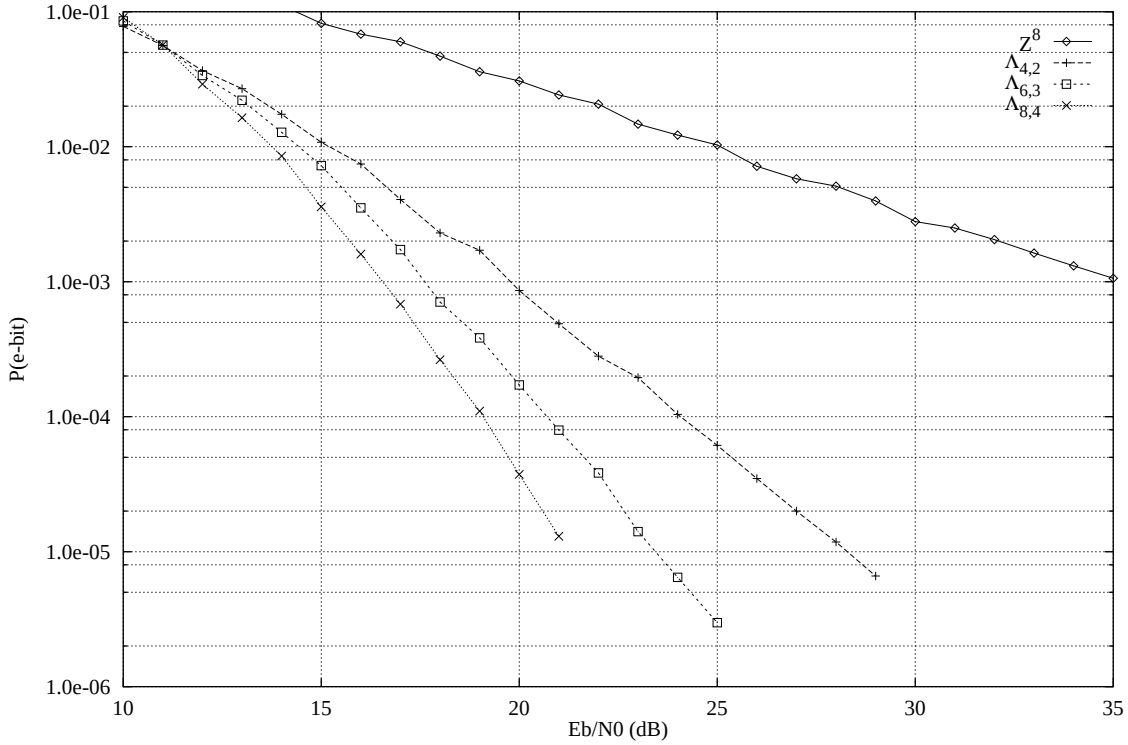

Figure 5.5: Lattice constellations from totally complex algebraic number fields of minimal discriminant over the Rayleigh fadind channel ($s = 4$)

For comparison we have plotted the upper bound (5.5) for the Leach lattice Λ_{24} which gains 3.7dB at 10^{-5}, although its asymptotic coding gain is 6dB [1].

Figure 5.3 shows the performance over the Rayleigh fading channel of the rotated versions of the lattices D_4, E_6, E_8, K_{12}, Λ_{16} (the last two are upper bounds). As discussed in section 5.3, the slopes of the curves asympotically correspond to the diversity. For these lattices we can see that this is already true for low bit error probabilities.

Figure 5.4 shows the performance over the Rayleigh fading of the lattice constellations from totally real algebraic number fields. These lattices give the best performance over the fading channel but have negative asymptotic gains over the Gaussian channel. Although the diversities are comparatively higher the actual slopes of the curves do not reach the asymptotic value in the range of interest. An explanation of this fact comes from the high value of the product kissing number for these constellations.

Figure 5.5 shows the performance over the Rayleigh fading of the lattice constellations from totally complex algebraic number fields. The curves achieve quite rapidly the slope corresponding to the diversity and their performance over the fading channel is very close to the one of the corresponding lattices in Figure 5.4.

5.8 Conclusions

Two different approaches (Sections 5.4, 5.5 versus Section 5.6) have been used to study two families of lattices in order to achieve good performance over both Gaussian and Rayleigh channels, with high spectral efficiency.

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

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

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

over the practical gain. We cannot forget also that the study of the first family makes it possible for us to construct and understand the second family.

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

5.9 Appendix A – Upper bound on the AWGN channel

In this appendix we modify inequality (4) to express it as a function of E_b/N_0. We assume that the constellation S has a cubic shape centered at the origin and has volume $(2A)^n$. The components x_i of any point $\mathbf{x}$ in S satisfy the inequality $|x_i| \leq A$. The total number of points in S can be approximated by

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

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

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

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

Since,

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

the average energy per bit is

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

and

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

This yields the upper bound (5) to the error probability for the AWGN channel.

5.10 Appendix B – Upper bound on the Rayleigh channel

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

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

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

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

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

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

where $Q(x) = (2\pi)^{-1} \int_x^\infty \exp(-t^2/2) dt$ is the Gaussian tail function. The Gaussian tail function can be upper bounded [49] by an exponential $Q(x) \leq \frac{1}{2}\exp(-x^2/2)$. This bound is very tight already for $x \geq 3$. The conditional pairwise error probability becomes

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

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

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

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

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

where

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

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

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

which is equation (7) in section 3. This differs from the classical Chernoff bound by a factor $1/2$ and results in a tighter bound (for small diversities) due to the small slopes of the error probability curves.

Bibliography

[1] J. H. Conway, N. J. Sloane: *Sphere packings, lattices and groups*, 2nd ed., 1993, Springer-Verlag, New York.

[2] G. D. Forney, Jr., "Geometrically uniform codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1241–1260, September 1991.

[3] J. H. Conway, N. J. A. Sloane, "Fast quantizing and decoding algorithms for lattice quantizers and codes" *IEEE Transactions on Information Theory*, vol. 28, no. 2, March 1982, pp. 211–226.

[4] R. de Buda, "Some optimal codes have structure" *IEEE J. Select. Areas Comm.*, vol. 7, August 1989, pp. 893–899.

[5] G. D. Forney, Jr., "A bounded distance-decoding algorithm for the Leech lattice, with generalizations," *IEEE Transactions on Information Theory*, vol. 35, no. 4, July/August 1989, pp. 906–909.

[6] G. D. Forney, Jr., "Coset codes — Part II: Binary lattices and related codes," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1152–1187, September 1988.

[7] G. D. Forney, Jr., "Multidimensional constellations — Part II: Voronoi constellations," *IEEE J. Select. Areas Comm.*, vol. 7, no. 4, August 1989, pp. 941–958.

[8] U. Dieter, "How to calculate shortest vectors in a lattice," *Mathematics of Computation*, vol. 29, July 1975, pp. 827–833.

[9] P. Erdös, P. M. Gruber, J. Hammer, *Lattice points*. Essex, England: Longman Scientific & Technical, 1989.

[10] U. Fincke, M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of computation*, vol. 44, April 1985, pp. 463–471.

[11] A. Gersho and R. M. Gray, *Vector Quantization and Signal Compression*. Boston, MA: Kluwer, 1992.

[12] P. M. Gruber, C. G. Lekkerkerker, *Geometry of Numbers,* (2nd ed.), Amsterdam: North-Holland, 1987.

[13] D. E. Knuth, *The Art of Computer Programming,* Vol II, 2nd ed., Addison-Wesley, 1981, pp. 89–105.

[14] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced basis with applications," *ACM SIGSAM Bulletin*, vol. 15, 1981, pp. 37–44.

[15] E. Viterbo, E Biglieri:"A universal lattice decoder", 14-ème Colloque GRETSI, Juan-les-Pins, Sept. 1993.

[16] H. Edelsbrunner, *Algorithms in combinatorial geometry.* Berlin: Springer-Verlag, 1987.

[17] U. Fincke, M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Mathematics of computation*, vol. 44, pp. 463–471, April 1985.

[18] P. M. Gruber, C. G. Lekkerkerker, *Geometry of numbers,* (2nd ed.). Amsterdam: North–Holland, 1987.

[19] P. M. Gruber, "Geometry of numbers" in *Handbook of convex geometry, Vol. B* , ed. P. M. Gruber, J. M. Wills, pp. 737–764, Amsterdam: Elsevier Science Publishers B.V., 1993.

[20] E. Schulte, "Tilings" in *Handbook of convex geometry*, Vol. B, ed. P. M. Gruber, J. M. Wills, pp. 899–932, Amsterdam: Elsevier Science Publishers B.V., 1993.

[21] G. D. Forney, "Geometrically uniform codes", *IEEE Trans. Inform. Theory*, vol. 37, n. 5, pp. 1241–1260, Sept. 1991.

[22] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *The Bell System Technical Journal*, vol. 38, n. 3, May 1959.

[23] E. Biglieri, A. Sandri, A. Spalvieri, "Computing upper bounds to error probability of coded modulation schemes," pp.650–654, *Proceedings ICC'94*, New Orleans, May 1994.

[24] D. Coulson, "The dual lattice of an extreme six-dimensional lattice," *Journal of the Australian Mathematical Society (Series A)*, vol. 50, 1991, pp. 373–383.

[25] J. H. Conway, N. J. A. Sloane, "On the Voronoi regions of certain lattices," *SIAM Journal on algebraic and discrete methods*, vol. 5, n. 3, Sept. 1984, pp. 294–305.

[26] R. T. Worley, "The Voronoi region of E_6^*," *Journal of the Australian Mathematical Society (Series A)*, vol. 43, 1987, pp. 268–278.

[27] R. T. Worley, "The Voronoi region of E_7^*," *SIAM Journal of Discrete Mathematics*, vol. 1, n. 1, Feb. 1988, pp. 134–141.

[28] T. J. Dickson, "The extreme coverings of 4-space by sphres," *Journal of the Australian Mathematical Society*, vol. 7, 1967, pp. 490–496.

[29] E. S. Barnes, D. W. Trenerry, "A class of extreme lattice-coverings of n-space by sphres," *Journal of the Australian Mathematical Society*, vol. 14, 1972, pp. 247–256.

[30] E. Viterbo, E. Biglieri: "Computing the Voronoi cell of a lattice: The diamond-cutting algorithm," submitted to *IEEE Transactions on Information Theory*, Sept. 1994.

[31] D. Divsalar, M. K. Simon: "The design of trellis coded MPSK for fading channels: performance criteria," *IEEE Trans. on Communications*, vol. 36, pp. 1004–1012, Sept. 1988.

[32] C. Schlegel, D. J. Costello: "Bandwidth efficient coding for fading channels: code construction and performance analysis," *IEEE J. on Selected Areas in Communications*, vol. 7, no. 9, Dec. 1989.

[33] S. S. Pietrobon, R.H. Deng, A. Lafanechere, G. Ungerboeck, D.J. Costello: "Trellis coded multidimensional phase modulation," *IEEE Trans. on Information Theory*, vol. 36, no. 1, pp. 63–89, Jan. 1990.

[34] G. Ungerboeck: "Trellis-coded modulation with redundant signal sets, Part II," *IEEE Communications Magazine*, vol. 25, no. 2, Feb. 1987.

[35] G. D. Forney: "Coset codes I: introduction and geometrical classification,", *IEEE Trans. on Information Theory*, vol. 34, pp. 1123–1151, 1988.

[36] K. Boullé, J. C. Belfiore: "Modulation scheme designed for the Rayleigh fading channel," CISS'92, Princeton, March 1992.

[37] X. Giraud: "Constellations pour le canal à evanouissements", PhD thesis, E.N.S.T. Paris, May 1994, paper submitted to *IEEE Trans. Information Theory.*

[38] J. Boutros: "Constellations optimales par plongement canonique", Mémoire de fin d'études, E.N.S.T. Paris, June 1992.

[39] H. Cohen: *Computational algebraic number theory*, Springer Verlag 1993.

[40] M. E. Pohst: *Computational algebraic number theory*, DMV Seminar, vol. 21, Birkhäuser Verlag, 1993.

[41] P. Samuel: *Algebraic theory of numbers*, Paris: Hermann 1971.

[42] S. Lang: *Algebraic Number Fields*, Addison Wesley, 1971.

[43] H. Hasse: *Number Theory*, Springer Verlag, 1980.

[44] J. Hunter: "The minimum discriminants of quintic fields," *Proc. Glasgow Math. Assoc.*, vol. 3, pp. 57–67, 1957.

[45] J. Liang, H. Zassenhaus: "The minimum discriminant of sixth degree totally complex algebraic number fields," *J. of Number Theory*, vol. 9, pp. 16–35, Jan. 1977. .

[46] F. Diaz y Diaz: "Petits discriminants des corps de nombres totalement imaginaires de degré 8," *J. of Number Theory*, vol. 25, no. 1,pp. 34–52, Jan. 1987.

[47] M. Craig: "Extreme forms and cyclotomy," *Mathematika*, vol. 25, pp. 44-56, 1978.

[48] M. Craig: "A cyclotomic construction for Leech's lattice," *Mathematika*, vol. 25, pp. 236-241, 1978.

[49] S. Benedetto, E. Biglieri, V. Castellani: *Digital Transmission Theory*, Prentice-Hall, Englewood Cliffs, New Jersey, 1987.

[50] J. Boutros, E. Viterbo, C. Rastello, J.C. Belfiore: "Good constellations for both Rayleigh fading and Gaussian channels," submitted to *IEEE Transactions on Information Theory*, October 1994.