Decoding Complexity and Trellis Structure of Lattices

by

Amir H. Banihashemi

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical Engineering

Waterloo, Ontario, Canada, 1997

The University of Waterloo requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

Decoding operation is the major obstacle associated with using a lattice in communication applications. There are two general methods for lattice decoding: *i*) The integer programming method based on geometry of numbers, and *ii*) The trellis method. This thesis has contributions to both methods, and provides results which make the comparison between the two methods possible.

Regarding method (*i*), Kannan's algorithm, which is currently known as the fastest method for the decoding of a general lattice, is analyzed. Based on a geometrical interpretation of this algorithm, it is shown that it is a special case of a wider category of algorithms, called recursive cube search (RCS) algorithms. In this category, we improve Kannan's algorithm, and establish tight upper and lower bounds on the decoding complexity of lattices. The lower bounds prove that the RCS decoding complexity of any sequence of lattices with possible application in communications increases at least exponentially with dimension and coding gain.

Regarding method (*ii*), we discuss and develop a universal approach to the construction and analysis of the trellis diagrams of lattices using their bases. Based on this approach, we derive tight upper bounds on the trellis complexity of lattices, and study the problem of finding minimal trellis diagrams for lattices. The upper bounds both improve and generalize the previously known similar results. Minimal trellis diagrams for many important lattices are also constructed. These trellises, which are novel in many cases, can be employed to efficiently decode the lattices via the Viterbi algorithm. Moreover, we establish tight lower bounds on the trellis complexity of lattices. For many of the obtained trellises, these lower bounds provide a proof for minimality.

Finally, we derive some results in lattice theory with possible application in communications. These include an upper bound on covering radius of a lattice in terms of its successive minima, and an inequality on the coding gain of densest lattice packings in successive dimensions.

Acknowledgements

I would like to appreciate the valuable efforts of Dr. Ian Blake and Dr. Amir Khandani in supervising this research. I would also like to sincerely thank Dr. Blake for his support and encouragement throughout my Ph.D. program. Interactions with him over the last three years have helped define my views on research.

I am very grateful to Dr. G. David Forney for his interest in this work, and his insightful comments.

I would also like to thank Dr. Daniel J. Costello, Dr. M. Anwar Hasan, Dr. Levent Tuncel, and Dr. Weihua Zhuang for their wilingness to act as examining committee members, and for their helpful comments.

I am grateful to Dr. Joseph Cheriyan and Dr. Levent Tuncel for my education on combinatorial optimization and integer programming.

I am also truly indebted to the government and people of Canada for providing the major part of the funding for this work through Ontario Graduate Scholarships (OGS).

Finally, the support of my family was invaluable. I dedicate this thesis to them.

Contents

List of Tables

List of Figures

Chapter 1

Introduction and motivation

In this thesis, we investigate the decoding complexity and the trellis structure of lattices[1]. Lattices have two main applications in communications: *i*) signaling over band-limited channels, and *ii*) vector quantization. In both applications, a finite subset of points of an n-dimensional (n-D) lattice within a bounded supporting region of $\mathbb{R}^n$ is employed. This collection of points is called a *lattice code*. The major complexity associated with a lattice code is the process of *decoding*, which is finding the point of the code that has the smallest (Euclidean) distance to an input. Presenting an efficient decoding algorithm for a general lattice is one of the purposes of this thesis.

There exist very efficient algorithms for the decoding of well-known lattices with high degree of structure, like the Leech lattice (see [25, pp. 443-448], [33], [74]). Most of these algorithms, however, cannot be applied to a general lattice. There are only two known general purpose methods to decode a lattice: the trellis approach, and the integer programming approach based on geometry of numbers.

[1]The results of this thesis have been partly presented in [4]-[12].

This thesis has contributions related to both methods.

The trellis approach, mainly due to the valuable contributions of Forney [31], [36], [33], is currently one of the common methods in communications for the decoding of lattices. This approach, which can be applied to any lattice with a finite trellis (including rational lattices), is based on representing the lattice by a trellis diagram which reflects the underlying group structure. The Viterbi algorithm [30] is then used to decode the trellis. Many people in the coding community believe that this method can appropriately estimate the effort required for decoding lattices. However, no proof has been given to this effect yet. The results of this thesis provide some strong evidence for verifying this conjecture.

The problem of lattice decoding also lies at the heart of many integer programming problems [42], [39], [2], [43], [38]. The main approach to the decoding of lattices in integer programming is based on using a reduced basis for the lattice. The complexity of such decoding algorithms is composed of two parts: *i*) computing the reduced basis of the lattice, and *ii*) finding the nearest lattice point using this reduced basis. In the decoding problems encountered in communications, the lattice is fixed, so the basis reduction is performed just once and the resulting basis is then stored for subsequent uses. Thus the complexity of solving (*i*) is not of major concern. The fastest lattice decoding algorithm for solving (*ii*) in the context of integer programming appears to be that of Kannan [43].

In this work, a geometrical interpretation of Kannan's algorithm, which clarifies some issues regarding the complexity of the algorithm, is given. Explicit upper and lower bounds on the complexity of Kannan's algorithm for a general lattice are derived. The bounds are in terms of the coding gain (γ) and the dimension (n) of the lattice. For lattices with equal successive minima (ESM), a tighter upper bound and a stronger lower bound are obtained. Recalling that extremal lattices

(including the densest lattices) belong to the category of ESM-lattices, we observe that almost all of the lattices used in signal constellations have ESM. It is also proved that lattices A_n^*, D_n^*, and E_n^* have ESM. This means that the lattices with application in the quantization of uniformly distributed inputs [25, p. 61] are also in the set of ESM-lattices.

To reduce the complexity, we then modify Kannan's algorithm. By the pre-computation of the covering radii of the lattice and its sub-lattices, the modifications could be especially effective for the decoding of lattices used in communication applications. The modified algorithm employs the Korkin-Zolotarev (K-Z) reduced basis, and solves the decoding problem for an n-D lattice by reducing it to some subproblems of dimensionality $n-1$. Explicit upper and lower bounds are derived on the complexity of the algorithm. The complexity results are also improved for ESM-lattices. Using the derived lower bound, it is shown that even by performing some exponential-time pre-computations (for computing the reduced basis, and the covering radii), one cannot decode any sequence of lattices with possible application in communications ($\gamma \geq 1$) in polynomial time. This suggests that the integer programming approach is not going to be practically attractive for the decoding of dense lattices in high dimensions. The lower bound also indicates that our upper bound results cannot be much improved.

In this thesis, we also investigate the trellis structure and the trellis complexity of lattices. Trellis diagrams, which were introduced in the coding literature by Forney [29] in 1967 as a means of describing the Viterbi algorithm for the decoding of convolutional codes, appear to continue playing a very important role in coding theory [28]. They establish close ties between block codes and convolutional codes, between lattices and block codes, and also between the structure of a group code and its decoding complexity. Following the work of [29], the application,

construction and complexity of trellises for block codes was the subject of some significant research [3], [79], [60], [31]. It was however Forney's paper [31] which stimulated the current extensive interest in the area. In particular, the analysis of trellis complexity and the problem of finding minimal trellises for block codes has attracted wide attention (for a list of references, see the related papers in [82], and the references therein). In the appendix of [31], Forney showed that group codes, including lattices, have well defined trellis diagrams. However, unlike block codes, the investigation of trellis diagrams of lattices has not received much attention yet. Except for [31], the works in this area are almost entirely limited to another work of Forney [33], and [69]-[71].

Among other things in [31], Forney gave an algebraic derivation of trellis diagrams for lattices. He also suggested that the trellis complexity and the coding gain of lattices should be studied together. Regarding the complexity of trellises, Forney's main concern was minimizing the number of states [33]. He, however, noticed that for decoding purposes, the number of trellis edges is more important than the number of states [33]. In [33], focusing on the number of trellis states, Forney derived lower bounds on the complexity and constructed trellis diagrams for some important low-dimensional lattices, like Barnes-Wall lattices $D_4, E_8, \Lambda_{16}, \Lambda_{32}$, the Leech lattice Λ_{24}, and the Coxeter-Todd lattice K_{12}. These constructions either met or nearly met the lower bounds.

The problem of investigating the trellis complexity of lattices as a function of coding gain was then attacked by Tarokh and Blake [69], [70]. By introducing three complexity functions which represent state, edge and label group complexities of a trellis, they studied the least amount of decoding effort required to achieve a given coding gain. Their results, which are mainly lower bounds, show that for sufficiently large coding gains γ, the average state and edge complexities of any trellis diagram

of lattices grow at least exponentially with γ. Although their results have shed light on many aspects of the trellis complexity of lattices, there are still some questions unanswered. A major deficiency seems to be the lack of proper upper bounds on the trellis complexity of lattices. Such results enables one to compare the trellis method with the integer programming approach for decoding lattices. Very recently, Tarokh and Vardy in a paper [71], which was received by the author at the final stages of this work, show (by some counter-examples) that the trellis complexity of a general rational lattice cannot be upper bounded by either a function of dimension n or a function of γ. They also derive upper bounds on the trellis complexity of integral lattices in terms of n and the determinant of the lattice. In this thesis, these bounds are both improved and generalized.

For linear block codes, it is well known that although the codes obtained by permuting the coordinates are equivalent, their trellises are not equivalent in general [60]. One is therefore interested in finding a proper permutation of code digits to minimize the trellis complexity. For lattices, it appears that the problem of finding a proper coordinate system to minimize the trellis complexity (in some sense), or more generally speaking, any trellis complexity kind of problem is much more difficult. Nevertheless, the increasing interest in lattice codes for signaling over band-limited channels [35], [18], [16], [17], and for vector quantization [27], [81], [21], and also the capability of lattice codes to achieve the capacity [26], [57], [72], [34], make the study of such problems of some importance.

As a (trellis) coordinate system for an n-D lattice, one should deal with n mutually orthogonal directions in $\mathbb{R}^n$. A search for a proper coordinate system is therefore much more complicated than just looking for a proper permutation. Another significant difference between trellis diagrams of block codes and those of lattices is that, for block codes, in any permuted coordinate system the number of (distinct)

paths in the trellis (N) is fixed and is equal to the number of codewords. For trellis diagrams of lattices, however, N can highly vary with different coordinate systems. This motivates us to consider N as a measure of trellis complexity for lattices. In the present work, focusing on N as the main measure of trellis complexity, we relate the other complexity measures, including the amount of computation required for the Viterbi algorithm, to N. We then discuss how searching for a proper trellis of a lattice (with a small value of N) can be reduced to the problem of finding a proper basis of the lattice. Given a basis of a rational lattice, the construction and analysis of the corresponding trellis is explained in detail. This provides us with a strong tool to search for proper bases which result in less complex trellises.

As a complement to the duality results of [33] on state complexity, we obtain some results which relate the sizes of the label groups, edge complexities and values of N for dual lattices. These duality results are used in both deriving upper bounds on trellis complexity, and finding trellis diagrams with small values of N. We call a trellis of Λ *minimal* if it minimizes N. For many important lattices like Barnes-Wall lattices BW_n, root lattices and their duals D_n, D_n^*, E_n, E_n^*, (A_n, A_n^*, $n \leq 9$), and the Leech lattice Λ_{24}, we obtain basis matrices which result in minimal trellis diagrams. For some other lattices like A_n, A_n^*, $n > 9$, and the Coxeter-Todd lattice K_{12}, trellises with small values of N (probably not minimal) are obtained. The constructed trellises, which are novel in many cases, can be employed to efficiently decode the lattices via the Viterbi algorithm.

We also derive a range of upper bounds on different trellis complexity measures and for different categories of lattices. All the upper bounds are of a constructive nature. For integral lattices, the bounds which are in terms of n, and the successive minima or the determinant of the lattice, are substantially tighter than the similar results of [71]. We are also able to extend our results to the more general category

of rational lattices. In specific, it is shown that for *any* n-D rational lattice Λ, the complexity of the trellis constructed based on *any* basis of Λ can be upper bounded by a function of n and the determinant of Λ. It is worth noting that based on these results, we can find upper bounds on the trellis complexity of all the counter-examples given in [71].

The contents of this thesis are organized as follows: In Chapter 2, we first give an introduction to lattices and their trellis construction. The Viterbi algorithm for the decoding of trellis diagrams of lattices is described next. We then discuss the different trellis complexity measures and their relationships. Chapter 3 contains our contributions to the lattice decoding problem based on the integer programming approach. In Chapters 4 and 5, we develop our results on the trellis structure of lattices. In Chapter 6, we obtain some more results in lattice theory with possible applications in coding. These include an upper bound on the covering radius of a lattice in terms of its successive minima, and an inequality on the coding gain of densest lattice packings in successive dimensions. Finally, Chapter 7 is devoted to concluding remarks and suggestions for future research.

Chapter 2

Preliminaries

In this chapter some definitions and facts about lattices are given. We then discuss the trellis construction of lattices, and explain the application of Viterbi algorithm to the trellis decoding of lattices. Finally the last section of this chapter is devoted to discussions on different trellis complexity measures.

2.1 Background on lattices

Definition 2.1 *A group G is a set that is closed under an associative binary operation $*$, and that has an identity element $e \in G$ and an inverse g^{-1} for every $g \subset G$.*

A group G is called *Abelian* if the operation $*$ is commutative, i.e., if $g * h = h * g$, $\forall g, h \in G$. The *order* $|G|$ of a group G is the number of its elements.

Example 2.1 *The set of integers modulo n, i.e., $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, is an Abelian group under addition modulo n.*

A *subgroup* G_1 of G is a subset of G that is a group under the binary operation of G. A *coset* of a subgroup G_1 in G is a subset $g * G_1 = \{g * g_1 : g_1 \in G_1\}$ of G, where $g \in G$. Two cosets of G_1 are either equal or disjoint. Every element of G belongs to one of these cosets. Hence, the set G/G_1 of the cosets of G_1 in G is a partition of G. All the cosets of G_1 have the same size of $|G_1|$. Thus the number of elements of G/G_1, called the *index* of G_1 in G, is equal to $|G|/|G_1|$. It can be seen that G/G_1 forms a group under the operation $\bullet$ defined by $(g * G_1) \bullet (g' * G_1) = (g * g') * G_1$. This group is called the *quotient group* (of G modulo G_1).

Definition 2.2 *Let G and G' be groups under the operations $*$ and $\circ$, respectively. A group homomorphism $\Psi : G \to G'$ is a mapping such that $\Psi(g * h) = \Psi(g) \circ \Psi(h)$, $\forall g, h \in G$. G and G' are called isomorphic if there exists a group homomorphism $\Psi : G \to G'$ that is both one-to-one and onto.*

Let $\mathbb{R}^m$ be the m-dimensional (m-D) real vector space with the standard inner product $\langle ., . \rangle$, and Euclidean length $\|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle^{\frac{1}{2}}$. The linear subspace generated by some subset of $\mathbb{R}^m$ is denoted by $span(\cdots)$, and its orthogonal complement by $span(\cdots)^{\perp}$. A set of vectors V is called *discrete* if there exists a positive number ρ such that any two vectors of V have distance $\geq \rho$.

Definition 2.3 *A discrete, additive subgroup Λ of $\mathbb{R}^m$ is called a lattice.*

Definition 2.4 *Every lattice Λ is generated as an Abelian group by the integer linear combinations of some set of linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \Lambda$, where the integer $n (\leq m)$ is called the dimension of the lattice Λ. The set of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called a basis of Λ, and the $n \times m$ matrix $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ which has the basis vectors as its rows is called the basis matrix (or generator matrix) of Λ.*

The lattice Λ is also denoted by $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ or $L(B)$. We use the brief notation $span(\Lambda)$ to denote the real span of the set of basis vectors, i.e., $span(\Lambda) = span(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

Definition 2.5 *A lattice Λ is called orthogonal (rectangular) if it has a basis B with mutually orthogonal vectors.*

Definition 2.6 *An n-D lattice $\Lambda \subset \mathbb{R}^m$ is called full-dimensional if $n = m$.*

Definition 2.7 *A fundamental region of a lattice Λ is defined as a building block which, when translated by lattice vectors, partitions $span(\Lambda)$ with just one lattice point in each copy.*

The *Voronoi cell* of a point $\mathbf{v} \in \Lambda$ is an example of a fundamental region for Λ. It consists of those points of $span(\Lambda)$ which are at least as close to $\mathbf{v}$ as to any other lattice point.

It is known that a basis of a lattice is not unique. If $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ is a basis of the lattice Λ, then $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ is also a basis of Λ if and only if (iff) there exists a *unimodular* matrix U (integer matrix with determinant ± 1) such that $UB = B'$.

Definition 2.8 *The determinant (or volume) of a lattice Λ, $det(\Lambda)$, is defined by choosing any basis $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of Λ and setting $det(\Lambda) = [det(BB^T)]^{1/2}$, where B^T denotes the transpose of B.*

For a full-dimensional lattice, $\det(\Lambda) = |\det(B)|$. Geometrically, $\det(\Lambda)$ is the common volume of the (n-D) fundamental regions of Λ, justifying the name "volume" for the determinant.

A *sublattice* Λ_1 of a lattice Λ is a subgroup of Λ. The quotient group Λ/Λ_1 is finite if and only if the dimension of Λ_1 is equal to the dimension of Λ. In this case, $|\Lambda/\Lambda_1| = \det(\Lambda_1)/\det(\Lambda)$.

Definition 2.9 *On the space of n-D lattices, the (B, ϵ)-neighborhood of a lattice Λ with the basis matrix $B = [b_{ij}]$ consists of all lattices having a basis $B' = [b'_{ij}]$, such that*

$$\| B - B' \| \triangleq \max_{i,j}\{|b_{ij} - b'_{ij}|\} < \epsilon \ ,$$

where ϵ is an arbitrary positive number.

Definition 2.10 *The i-th successive minimum $\lambda_i(\Lambda)$ of a lattice Λ is the smallest real number such that there are i linearly independent vectors in Λ of length at most $\lambda_i(\Lambda)$.*

Clearly, we have

$$\lambda_1(\Lambda) \leq \lambda_2(\Lambda) \leq \cdots \leq \lambda_n(\Lambda) \ . \tag{2.1}$$

We call a lattice ESM if its successive minima are equal. Obviously, lattices which are generated by their minimum-length vectors have the ESM property, although to the best of our knowledge the converse to this statement has not been proved. The notation $\lambda(\Lambda) \triangleq \lambda_1(\Lambda)$ is used to denote the length of a shortest nonzero vector in Λ. This is also equal to the minimum distance between lattice points.

Definition 2.11 *Consider an n-D lattice Λ. Assume that an n-D sphere of radius $\lambda(L)/2$ is centered at each lattice point. This arrangement of spheres is called a lattice sphere packing or briefly packing corresponding to the lattice Λ.*

In a lattice-based signal constellation, the constellation points belong to a lattice Λ. As a crude measure of performance of the corresponding lattice code, *coding gain* is defined as

$$\gamma(\Lambda) \triangleq \lambda^2(\Lambda)[\det(\Lambda)]^{-2/n} . \tag{2.2}$$

The quantity $\gamma(\Lambda)$ is the saving in the average energy due to using the lattice Λ for the transmission instead of using a rectangular grid of points with integer components ($\mathbb{Z}^n$ lattice). In fact, $\gamma(\Lambda)$ is a density measure for the packing corresponding to the lattice Λ, [25, p. 73].

As an upper bound on the coding gain γ, *Hermite's constant* γ_n is defined as the supremum value of γ over all n-D lattices. It is known that γ_n is attainable [37, p. 267]. The corresponding lattice, which results in the densest lattice sphere packing in dimension n, is called the *densest* n-D lattice. The value of γ_n is explicitly known only for $n \leq 8$. Minkowski's convex body theorem [37, p. 51] implies that $\gamma_n \leq 4\pi^{-1}\Gamma(n/2+1)^{2/n}$, which yields $\gamma_n \leq 2n/3$ for all $n \geq 2$. For the sake of simplicity, we will usually use the inequality $\gamma_n \leq n$, which holds for all values of n. It is also known that for large values of n, [25, p. 20],

$$\frac{1}{2\pi e} \leq \frac{\gamma_n}{n} \leq \frac{1.744}{2\pi e} . \tag{2.3}$$

We frequently use a famous result, due to Minkowski, which implies that for an n-D lattice Λ, [37, p. 195],

$$\lambda_1(\Lambda)\ldots\lambda_n(\Lambda) \leq \det(\Lambda)\gamma_n^{n/2} . \tag{2.4}$$

The distance between a vector $\mathbf{v}$ and a lattice Λ is defined as the minimum distance between $\mathbf{v}$ and the points of Λ.

Definition 2.12 *The covering radius $\mu(\Lambda)$ of a lattice Λ is the smallest number such that all vectors $\mathbf{v} \in span(\Lambda)$ are at distance at most $\mu(\Lambda)$ from the lattice.*

For every n-D lattice Λ, each Voronoi cell $\mathcal{V}(\mathbf{p})$ of a lattice point $\mathbf{p}$ is an n-D polytope which has at least two vertices at distance $\mu(\Lambda)$ from $\mathbf{p}$. These are called the *deep holes* of Λ corresponding to $\mathbf{p}$.

To any ordered basis of Λ, say $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{R}^m$, one can associate a set of *Gram-Schmidt (G-S)* vectors $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n \in \mathbb{R}^m$, which are computed using the following recursion:

$$\begin{aligned} \hat{\mathbf{b}}_1 &= \mathbf{b}_1 \\ \hat{\mathbf{b}}_i &= \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \hat{\mathbf{b}}_j \quad \text{for} \quad i = 2, \ldots, n \ , \end{aligned} \tag{2.5}$$

where the G-S coefficients, namely $\mu_{i,j}$'s, are equal to:

$$\mu_{i,j} = \frac{\langle \mathbf{b}_i, \hat{\mathbf{b}}_j \rangle}{\langle \hat{\mathbf{b}}_j, \hat{\mathbf{b}}_j \rangle} \ . \tag{2.6}$$

We have $\mu_{i,i} = 1$, $\forall i$, and $\mu_{i,j} = 0$ for $i < j$. Based on the above relationships, the G-S decomposition can be shown in matrix notation as

$$B = [\mu_{i,j}] \hat{B} \ , \tag{2.7}$$

where $\hat{B}$ has $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$ as its rows and $[\mu_{i,j}]$ is the lower triangular matrix of the G-S coefficients. The vector $\hat{\mathbf{b}}_i$ is the projection of $\mathbf{b}_i$ on $span(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$. The vectors $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$ are mutually orthogonal and do not necessarily belong to Λ. In many parts of the thesis, it will be very helpful to think of the basis vectors as being presented in the orthogonal co-ordinate system of the G-S vectors. It can also be seen that

$$\det(\Lambda) = \prod_{i=1}^{n} \|\hat{\mathbf{b}}_i\| \ . \tag{2.8}$$

Using (2.5) and (2.6), we see that if $\mathbf{b}_1, \ldots, \mathbf{b}_n$ have rational co-ordinates, so do the $\hat{\mathbf{b}}_i$'s and they can be computed in polynomial time (with respect to the input size) from $\mathbf{b}_1, \ldots, \mathbf{b}_n$. In this case, the G-S coefficients $\mu_{i,j}$ are rational too.

The following lower bound exists on the length of a shortest nonzero vector of a lattice Λ in terms of the lengths of its G-S vectors [58, p. 18],

$$\lambda(\Lambda) \geq \min\{\|\hat{\mathbf{b}}_1\|, \ldots, \|\hat{\mathbf{b}}_n\|\} \,. \tag{2.9}$$

Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a fixed ordered basis of a lattice Λ. Given $\mathbf{v} \in span(\Lambda)$ and $i \in \{1, \ldots, n\}$, we use the notation $\mathbf{v}(i)$, respectively $\Lambda_{(i)}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$, to denote the orthogonal projection of $\mathbf{v}$, respectively Λ, on the $span(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^{\perp}$. In particular, $\mathbf{v}(1) = \mathbf{v}$ and $\Lambda_{(1)}(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \Lambda$. We also use $\Lambda_{(i)}$ as the short notation for $\Lambda_{(i)}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Clearly, $span(\mathbf{b}_1, \ldots, \mathbf{b}_i) = span(\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_i)$, for $1 \leq i \leq n$, and $\mathbf{b}_i(i), \ldots, \mathbf{b}_n(i)$ is a basis of the lattice $\Lambda_{(i)}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$.

Definition 2.13 *Two lattices Λ_1 and Λ_2 are called equivalent, and demonstrated by $\Lambda_1 \cong \Lambda_2$, if they are the same up to rotation, reflection and scaling. We also refer to Λ_1 and Λ_2 as different versions of the same lattice.*

Two basis matrices B_1 and B_2 define equivalent lattices iff they are related by

$$B_2 = cUB_1O \,,$$

where c is a nonzero constant, U is a unimodular matrix, and O is an orthogonal matrix ($OO^T = I$, where I is the identity matrix).

Definition 2.14 *A parameter of a lattice Λ is called a geometrical invariant of Λ if it remains the same for different versions of Λ.*

Example 2.2 *Neither the minimum distance nor the determinant is a geometrical invariant of a lattice. The coding gain, given in* (2.2)*, however is a geometrical invariant of a lattice.*

Definition 2.15 *A lattice Λ is called rational (respectively integral) if the inner product of any two vectors of Λ is a rational number (respectively an integer).*

A lattice Λ with a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is rational, respectively integral, iff $\langle \mathbf{b}_i, \mathbf{b}_j \rangle \in \mathbb{Q}$, respectively $\mathbb{Z}$, for every $i, j \in \{1, \ldots, n\}$, where $\mathbb{Q}$ is the set of rational numbers.

Integral lattices are a subset of rational lattices. It can be seen that every rational lattice can be transformed to an integral lattice by a proper scaling. Let a rational lattice Λ have a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, and let ζ be the least common multiple (lcm) of the denominators of the rational numbers $\langle \mathbf{b}_i, \mathbf{b}_j \rangle$, $i, j \in \{1, \ldots, n\}$. Also let ν denote the greatest common divisor (gcd) of the integers $\zeta \langle \mathbf{b}_i, \mathbf{b}_j \rangle$, $i, j \in \{1, \ldots, n\}$. Then, the lattice $\sqrt{\zeta/\nu}\ \Lambda$ with the basis $\sqrt{\zeta/\nu}\ \mathbf{b}_1, \ldots, \sqrt{\zeta/\nu}\ \mathbf{b}_n$ is integral (by definition, both the lcm and gcd, and thus both ζ and ν are positive). In fact, $\sqrt{\zeta/\nu}$ is the smallest scaling factor with this property (see Lemma 4.3).

A subset of integral lattices is the set of integer lattices. An n-D lattice is called *integer* if it is a sublattice of $\mathbb{Z}^n$. Many important lattices have integer or integral versions [25].

Example 2.3 *The 2-D hexagonal lattice A_2 is partly shown in Figure 2.1. The following matrix is a basis for a version of A_2.*

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

It can be seen that in this version, $\mu = 1/\sqrt{3}$, $\lambda = 1$, and $det(A_2) = |det(B)| = \sqrt{3}/2$. Using (2.2), we thus have $\gamma(A_2) = 2/\sqrt{3}$. In fact, A_2 is the densest 2-D lattice. From Figure 2.1, it can be seen that each point of A_2 is surrounded by 6 points at distance λ. The lattice therefore has ESM. The Voronoi cells are regular hexagons, and each of them has 6 deep holes. It is also easy to see that this version

of A_2 is rational, but not integral. However, another version of A_2, with the basis matrix $B' = \sqrt{2}B$, is integral.

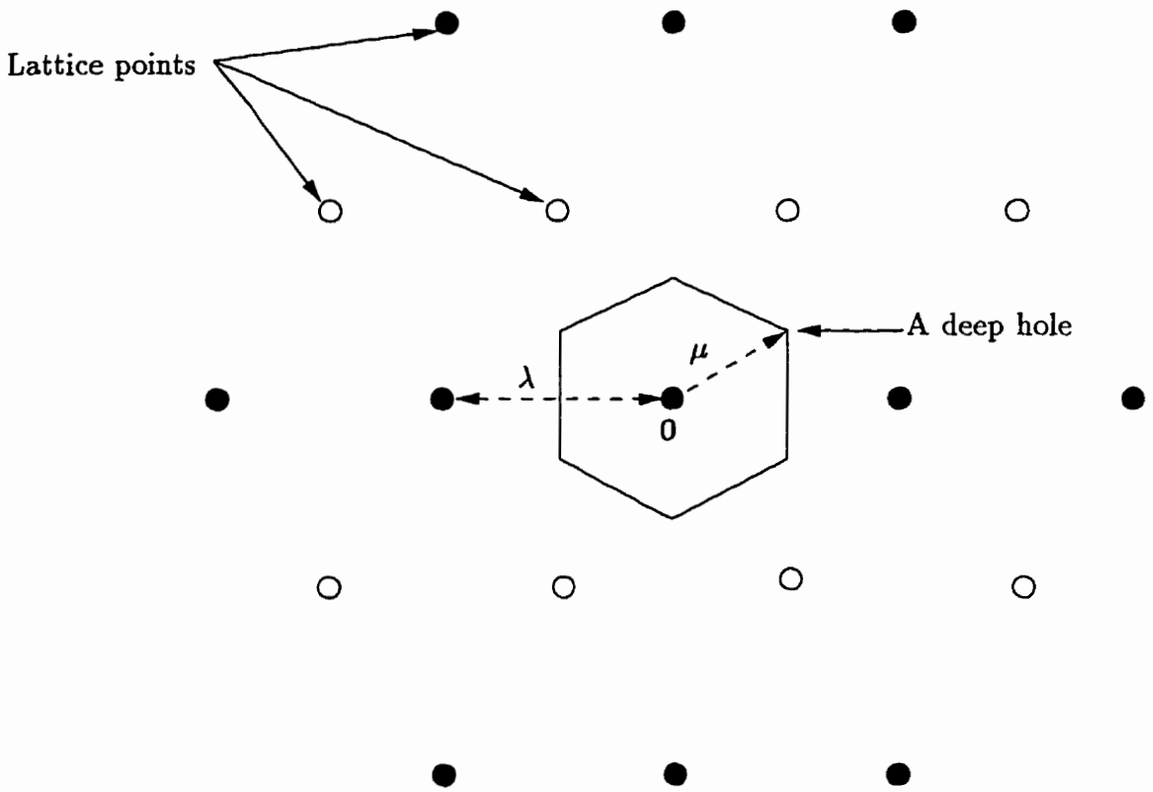

Figure 2.1: The hexagonal lattice A_2, and one of its Voronoi cells.

Definition 2.16 *If Λ is an n-D lattice, then the set of all vectors in span(Λ) whose inner product with all elements of Λ is an integer is an n-D lattice Λ^*, called the dual lattice of Λ.*

A lattice whose dual is itself is called *self-dual*. Let B be a basis for a lattice Λ, then there exists a matrix B' such that $B(B')^T = I$. It can be seen that B' is a basis for Λ^* [19, pp. 23,24]. Thus for a full-dimensional lattice Λ, $(B^{-1})^T$ forms a

basis of Λ^*. For dual lattices, we also have

$$\det(\Lambda^*) = \frac{1}{\det(\Lambda)}. \tag{2.10}$$

Definition 2.17 *Let lattices Λ_1 and Λ_2 have basis matrices B_1 and B_2, respectively. The direct sum lattice $\Lambda_1 \oplus \Lambda_2$ is defined by the following basis matrix:*

$$B = B_1 \oplus B_2 \triangleq \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}. \tag{2.11}$$

We also use the notation Λ^m for the m-fold direct sum of Λ.

It is easy to see that $\det(\Lambda_1 \oplus \Lambda_2) = \det(\Lambda_1)\det(\Lambda_2)$.

Throughout the thesis, we frequently address the properties of some important known lattices such as A_n, A_n^* $(n \geq 1)$, D_n, D_n^* $(n \geq 3)$, E_n, E_n^* $(n = 6, 7, 8)$, BW_n $(n = 2^m,\ m = 2, 3, \ldots)$, K_{12}, and Λ_{24}. For a comprehensive treatment, the reader is referred to the encyclopedic book of Conway and Sloane [25].

2.2 Trellis diagrams of lattices

In the following, to explain the algebraic derivation of trellis diagrams for lattices, we use an exposition similar to [33].

Let $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$ be a sequence of vector spaces with $\dim(V_i) = i$, and let W_i be the orthogonal complement of V_{i-1} in V_i for $1 \leq i \leq n$. Clearly, $\dim(W_i) = 1$. Also, suppose that $\Lambda \subset V_n$ is an n-D lattice. We use the notations $P_i \triangleq P_{V_i}$ and P_{W_i} for the projection operators onto the vector spaces V_i and W_i, respectively. Let $\Lambda_i \triangleq \Lambda \cap V_i$, and $\Lambda_{W_i} \triangleq \Lambda \cap W_i$. It can be seen that Λ_i and Λ_{W_i} have a lattice structure.

To construct the trellis diagram T of the lattice Λ, we define the *state space* $\Sigma_i(\Lambda)$ of Λ at level $i, 0 \leq i \leq n$, as the quotient group $P_i(\Lambda)/\Lambda_i$, and the *label group* $G_i(\Lambda)$ of Λ at trellis section i, $1 \leq i \leq n$, as the quotient group $P_{W_i}(\Lambda)/\Lambda_{W_i}$. The trellis T is then defined as a directed graph whose nodes at each level $i, 0 \leq i \leq n$, are the elements of $\Sigma_i(\Lambda)$. Edges between levels $i-1$ and i (in the trellis section i) are labeled by the elements of $G_i(\Lambda)$. The set of all paths through the trellis corresponds to Λ, i.e., for each lattice point $\mathbf{x} \in \Lambda$, there is a path through T which starts from the initial state $\Sigma_0(\Lambda)$ and ends at the final state $\Sigma_n(\Lambda)$. The path passes through the state sequence $\sigma(\mathbf{x}) = (\sigma_0(\mathbf{x}), \cdots, \sigma_n(\mathbf{x}))$, and the label sequence $\mathbf{g}(\mathbf{x}) = (g_1(\mathbf{x}), \cdots, g_n(\mathbf{x}))$, where $\sigma_i(\mathbf{x}) = \Lambda_i + P_i(\mathbf{x})$, and $g_i(\mathbf{x}) = \Lambda_{W_i} + P_{W_i}(\mathbf{x})$. Clearly, $\sigma_0(\mathbf{x}) = \Sigma_0(\Lambda)$, and $\sigma_n(\mathbf{x}) = \Sigma_n(\Lambda)$.

In the above construction, we call the ordered system of subspaces $\{W_i\}_{i=1}^n$, corresponding to the chain of $V_0, \ldots, V_n$, the *trellis coordinate system* of Λ for T. When no confusion can arise, we omit the word "trellis" in this context. We also use the expression *standard coordinate system* for the coordinate system of the m-D vector space, in which all the vectors are represented. The unit vectors of this coordinate system are denoted by $\{\mathbf{u}_i\}_{i=1}^m$. Note that hereafter, we assume all the trellises to be constructed based on the above construction.

In a trellis of the lattice Λ, the set of all possible state sequences $\sigma(\Lambda)$ is called the *state code*, and the set of all possible label sequences $\mathbf{g}(\Lambda)$ is called the *label code*. It can be seen that $\sigma(\Lambda)$ and $\mathbf{g}(\Lambda)$ are isomorphic [36], and their cardinality, denoted by $N(\Lambda)$, is equal to the number of distinct paths in the trellis. Two paths are called *distinct* if they differ in at least one state.

We illustrate the construction of a trellis diagram by using the following example from [33].

Example 2.4 *Consider the hexagonal lattice A_2 of Example 2.3 shown in Figure 2.1. In the trellis coordinate system of $W_1 = (1,0)$, $W_2 = (0,1)$, A_2 has the trellis of Figure 2.2. The label groups are $G_1 = \Sigma_1 = (1/2)\mathbb{Z}/\mathbb{Z}$, and $G_2 = (\sqrt{3}/2)\mathbb{Z}/(\sqrt{3})\mathbb{Z}$. They are both isomorphic to $\mathbb{Z}_2$. In fact, the state and label codes are also isomorphic to $\mathbb{Z}_2$. Note that the two paths in the trellis correspond to the cosets of the orthogonal sublattice $\mathbb{Z} \oplus \sqrt{3}\mathbb{Z}$ in A_2. These cosets are distinguished by black and white dots in Figure 2.1.*

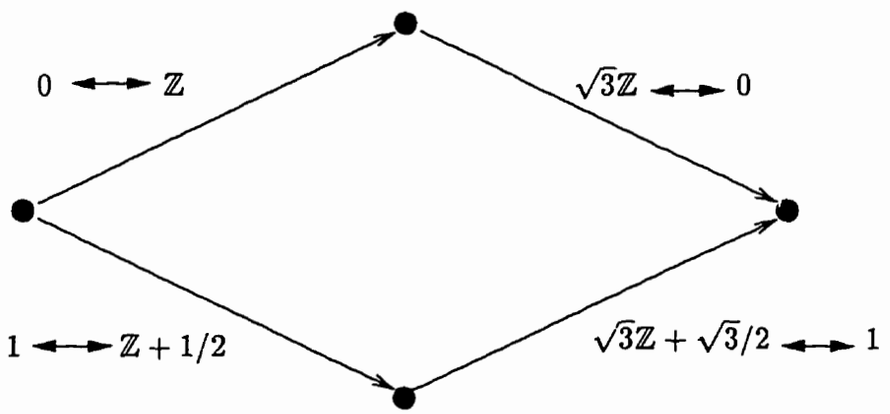

Figure 2.2: A trellis diagram of A_2.

We say Λ has a finite trellis if there exists a trellis diagram for Λ with a finite number of states (or edges). Clearly, the trellis approach can only be used for the decoding of lattices with finite trellis diagrams. This category of lattices, denoted by $\mathcal{L}$, however, covers a wide range including the rational lattices. For an example of a lattice not in $\mathcal{L}$, see [69]. We also use the notation $\mathcal{L}_n$ to denote the set of n-D lattices with finite trellis diagrams.

In the above trellis construction, the state group $\Sigma_i(\Lambda)$ is finite iff $\dim(\Lambda_i) = i$, and $P_i(\Lambda)$ has a lattice structure, and the label group $G_i(\Lambda)$ is finite iff $\dim(\Lambda_{W_i}) = 1$, and $P_{W_i}(\Lambda)$ has a lattice structure. For a case where these conditions are not

satisfied, see Example 2.5, [1].

It is not difficult to see that a lattice Λ belongs to $\mathcal{L}_n$ iff it has an n-D orthogonal sublattice Λ'. In fact, in a given trellis coordinate system $\{W_i\}_{i=1}^n$, Λ has a finite trellis iff $\dim(\Lambda_{W_i}) = 1$, $\forall i$. In this case, the corresponding sublattice Λ' is equal to the direct sum $\Lambda_{W_1} \oplus \cdots \oplus \Lambda_{W_n}$. The trellis diagram can then be considered as an efficient way of representing Λ as the union of cosets of Λ' in Λ. Each coset is represented by a path through the trellis. The number of cosets, which is the same as the index of Λ' in Λ ($|\Lambda/\Lambda'|$), is therefore equal to $N(\Lambda)$. We consequently have

$$N(\Lambda) = \frac{\det(\Lambda')}{\det(\Lambda)}. \tag{2.12}$$

Example 2.5 *Consider the lattice Λ with the following basis matrix:*

$$B = \begin{pmatrix} 1 & 0 \\ \sqrt{3} & 1 \end{pmatrix}.$$

It is easy to see that the vectors $\mathbf{v}_1 = (2+\sqrt{3}, 1)$ and $\mathbf{v}_2 = (2-\sqrt{3}, -1)$ are orthogonal and belong to Λ. This implies that $\Lambda \in \mathcal{L}_2$. The vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ are also the shortest vectors of Λ in the corresponding directions. Thus in the trellis coordinate system of $\{\mathbf{v}_1, \mathbf{v}_2\}$, the corresponding orthogonal sublattice Λ' has a determinant of $det(\Lambda') = \|\mathbf{v}_1\|\|\mathbf{v}_2\| = 4$, and from (2.12), $N(\Lambda) = 4$.

On the other hand, the G-S vectors of B are $\hat{\mathbf{b}}_1 = (1,0)$ and $\hat{\mathbf{b}}_2 = (0,1)$, and in the (trellis) coordinate system of $\{\hat{\mathbf{b}}_1, \hat{\mathbf{b}}_2\}$, we have $\Lambda_{W_2} = \Lambda \cap span(\hat{\mathbf{b}}_2) = \{\mathbf{0}\}$.

[1] It has been mentioned by some authors, e.g., in [33] and [71], that since an orthogonal projection is a linear transformation, so $P_i(\Lambda)$ and $P_{W_i}(\Lambda)$ are lattices. Using this assumption, it has been concluded in [71] that any trellis of a lattice $\Lambda \in \mathcal{L}$ constructed based on a basis of Λ (this construction is illustrated in detail in Section 4.1) is finite. However, as Example 2.5 shows, this is not true in general. The fact that a projection operator is a linear transformation only results in the group property of $P_i(\Lambda)$ and $P_{W_i}(\Lambda)$, not necessarily in having a discrete structure which is the other requirement for being a lattice.

This implies that the size of the label group $G_2(\Lambda)$ is infinite. It can also be seen that $P_{W_1}(\Lambda) = \{(z_1 + \sqrt{3}z_2)\hat{\mathbf{b}}_1 : z_1, z_2 \in \mathbb{Z}\}$. Using contradiction, this implies that $P_{W_1}(\Lambda)$ does not have a lattice structure, and therefore the sizes of $\Sigma_1(\Lambda)$ and $G_1(\Lambda)$ are infinite too.

We use the following definition from [48], [76].

Definition 2.18 *A trellis is called proper (biproper) if the edges incident from any trellis state (and the set of edges incident to any trellis state) are labeled distinctly.*

Let T be the trellis of a lattice $\Lambda \in \mathcal{L}$ in a given trellis coordinate system. In this coordinate system, it is known that T is the unique trellis of Λ (up to graph isomorphism) with the minimum number of states in each level [36]. Because of its group property, it can be seen that the label code of Λ is *rectangular* [48]. This along with the fact that T has the minimum number of states in each level implies that T is biproper [48]. It is then concluded that T minimizes a wide variety of trellis complexity measures, like the total number of states, the total number of edges, and the number of edges in each trellis section [76]. In fact, counting just the number of additions and comparisons for the Viterbi algorithm[2], it also implies that the trellis T minimizes the Viterbi decoding complexity of the lattice in the given trellis coordinate system [76].

It is however, known that the trellis diagram of a lattice $\Lambda \in \mathcal{L}$ is not unique, i.e., choosing different trellis coordinate systems results in different trellis diagrams. One is therefore interested in finding a less complex trellis (resulting in a more efficient decoding algorithm). One way of measuring the trellis complexity is to

[2]The Viterbi algorithm will be explained in detail in Section 2.3.

consider all the quantities: number of states, number of edges, and the sizes of the label groups [69], [70]. In this work, however, we focus more on $N(\Lambda)$ as the measure of complexity. Although this fundamental geometric measure relates most closely to the complexity of the coset decoding of a lattice (note that the decoding of each coset of Λ' can be performed in polynomial time), it appears that in many cases, minimizing N results in trellises which are simpler (and have a lower Viterbi decoding complexity) than previously known trellis diagrams.

We would like to emphasize a major difference between the trellis diagrams of lattices and those of block codes. The number of distinct paths in one-to-one trellis diagrams [76] (including biproper trellises) of a block code is always fixed and is equal to the number of codewords. This remains true even if one tries to minimize the trellis complexity of a code via permuting the time axis. As we will see later, unlike block codes, for the trellis diagrams of lattices, N depends largely on the selection of the trellis coordinate system. It is therefore natural to search for a coordinate system which minimizes N in the corresponding trellis. Such a trellis is called *minimal*.

It is important to note that permuting the coordinates in a given trellis coordinate system does not change the value of N in the corresponding trellis. It however can affect the other trellis complexity measures as can be seen later in Example 5.6. One can therefore find a low-complexity trellis by first minimizing N, and then minimizing another complexity measure by permuting the coordinates in the obtained coordinate system.

2.3 The Viterbi algorithm

In 1967, the Viterbi algorithm (VA) was originally proposed by Viterbi as a proof technique in the development of exponential error bounds for convolutional codes [78]. Forney subsequently recognized the VA as a maximum-likelihood decoding algorithm for these codes [29]. Later, Omura [63] showed that the VA could be viewed as an instance of the general class of techniques known as "dynamic programming" applied to a trellis. A comprehensive treatment of the VA and its applications can be found in [30], or textbooks like [56]. Here, we only discuss the application of the VA for the trellis decoding of lattices.

Suppose that a trellis diagram T for an n-D lattice $\Lambda \subset \mathbb{R}^n$, and an input $\mathbf{x} \in \mathbb{R}^n$ are given. In the corresponding trellis coordinate system $\{W_i\}_{i=1}^n$, let $\mathbf{v}_i$ be a shortest vector of Λ_{W_i}, i.e., $\Lambda_{W_i} = \mathbb{Z}\mathbf{v}_i$. Also, let $\mathbf{x} = \sum_{i=1}^n x_i \mathbf{v}_i$, where

$$x_i = \frac{\langle \mathbf{x}, \mathbf{v}_i \rangle}{\langle \mathbf{v}_i, \mathbf{v}_i \rangle} . \tag{2.13}$$

In each trellis section $i, 1 \leq i \leq n$, we need to compute a *metric* for each element of the label group G_i. Each edge is then labeled by the metric of the corresponding label group element. Let $(\mathbb{Z} + a_j)\mathbf{v}_i, 1 \leq j \leq |G_i|$, be the elements of G_i, and $c_{ij}\mathbf{v}_i$ denote the closest vector of the j-th element of G_i to $x_i\mathbf{v}_i$. The metric d_{ij}, $1 \leq i \leq n$, $1 \leq j \leq |G_i|$, is defined as $\|(c_{ij} - x_i)\mathbf{v}_i\|^2$, i.e., the squared minimum distance between the elements of $(\mathbb{Z} + a_j)\mathbf{v}_i$ (the j-th element of G_i) and $x_i\mathbf{v}_i$. It is easy to see that

$$c_{ij} = a_j + \lceil x_i - a_j \rfloor , \tag{2.14}$$

where $\lceil t \rfloor$ denotes the closest integer to t. We therefore have

$$d_{ij} = |(x_i - a_j) - \lceil x_i - a_j \rfloor|^2 \|\mathbf{v}_i\|^2 . \tag{2.15}$$

It is easy to see that the following algorithm decodes $\mathbf{x}$ to the nearest point of Λ.

The Viterbi algorithm

step 1: Set $d(\Sigma_0) = 0$, and $sur(\Sigma_0) = \mathbf{0}$, where $\mathbf{0}$ is the origin of $\mathbb{R}^n$, sur is an abbreviation for the *survivor* path, and d denotes the metric for the survivor path. Also set $i = 1$.

step 2: For each state S at level i, denote the set of states at level $i-1$ which are connected to S through an edge by $P(S)$. For each element $S' \in P(S)$, add the metric for the edge connecting S' to S to $d(S')$, and select the minimum value among the results as $d(S)$. If the minimum value corresponds to $\tilde{S} \in P(S)$, and if the edge between $\tilde{S}$ and S is labeled by the j-th element of G_i, then set $sur(S) = sur(\tilde{S}) + c_{ij}\mathbf{v}_i$.

step 3: Increase i by one. If $i \leq n$, go to step 2. Otherwise, output $sur(\Sigma_n)$ as the closest lattice point to $\mathbf{x}$. Clearly, $d(\Sigma_n)$ contains the squared distance between $\mathbf{x}$ and $sur(\Sigma_n)$.

In an efficient implementation of the VA, one does not need to compute the survivor path for every state of the trellis. He only needs to keep track of the survivor paths for the states, and finally construct the output vector by back-tracking the survivor path for Σ_n.

2.4 Trellis complexity measures

Let $\Lambda \in \mathcal{L}_n$ have a finite trellis T with $|\Sigma_i(\Lambda)| = s_i$, for $0 \leq i \leq n$, and $|G_i(\Lambda)| = g_i$, for $1 \leq i \leq n$. Also suppose that T has e_i edges in the trellis section $i, 1 \leq i \leq n$. Define $\mathcal{S}(\Lambda) = (\sum_{i=0}^{n} s_i - 1)/n$, $\mathcal{E}(\Lambda) = (\sum_{i=1}^{n} e_i)/n$, and $\mathcal{G}(\Lambda) = (\sum_{i=1}^{n} g_i)/n$.

These parameters (introduced in [69]), which represent the trellis complexity per dimension, are related to $N(\Lambda)$ by the following lemma.

Lemma 2.1 *Given a finite trellis for a lattice $\Lambda \in \mathcal{L}_n$, and letting the corresponding parameters $N(\Lambda)$, $\mathcal{S}(\Lambda)$, $\mathcal{E}(\Lambda)$, and $\mathcal{G}(\Lambda)$ be defined as above, we have*

$$N(\Lambda)^{\frac{1}{n}} \leq \mathcal{S}(\Lambda) \leq N(\Lambda)\,, \tag{2.16}$$

$$N(\Lambda)^{\frac{2}{n}} \leq \mathcal{E}(\Lambda) \leq N(\Lambda)\,, \tag{2.17}$$

$$N(\Lambda)^{\frac{1}{n}} \leq \mathcal{G}(\Lambda) \leq N(\Lambda)\,. \tag{2.18}$$

Proof: From the construction of the trellis, and the fact that there exists at least one path passing through each state, we have $s_0 = s_n = 1$, and $s_i \leq N(\Lambda)$, for $1 \leq i \leq n-1$. Adding up these relations, subtracting one, and dividing by n, we obtain $\mathcal{S}(\Lambda) \leq [(n-1)N(\Lambda)+1]/n$. This combined with the inequality $1 \leq N(\Lambda)$ results in the upper bound of (2.16). It is easy to see that $N(\Lambda) \leq s_1 \cdots s_n$. The inequality is satisfied with equality iff there is an edge between any two states in any two successive levels of the trellis. Combining this inequality with the arithmetic-geometric mean inequality of

$$(s_1 \cdots s_n)^{\frac{1}{n}} \leq \frac{s_1 + \cdots + s_n}{n}$$

gives the lower bound of (2.16).

It can be seen that $e_i \leq N(\Lambda), 1 \leq i \leq n$. Adding up these inequalities, and dividing the result by n results in the right hand side of (2.17). For the left hand side, let $r_i, 1 \leq i \leq n$, denote the number of edges incident from each state at level $i-1$ (it is known from the group properties that this number is the same for every

state at level $i-1$ [36]). We then have $N(\Lambda) = r_1 \cdots r_n$, and $r_i = e_i/s_{i-1}, 1 \leq i \leq n$. Combining these together and applying the inequality $N(\Lambda) \leq s_0 \cdots s_{n-1}$, we obtain $N^2 \leq e_1 \cdots e_n$. This along with the arithmetic-geometric mean inequality completes the proof.

Regarding (2.18), adding up the relations $g_i \leq e_i \leq N(\Lambda), 1 \leq i \leq n$, and dividing the result by n, results in the upper bound. To get the lower bound, we first combine $N(\Lambda) = r_1 \cdots r_n$ with the inequalities $r_i \leq g_i, 1 \leq i \leq n$, which come from the fact that the trellis is proper. Then the proof follows by applying the arithmetic-geometric mean inequality to the result. □

Note that the bounds given in Lemma 2.1 are tight. In fact, all the bounds are satisfied with equality for the trivial trellis of integer lattice $\mathbb{Z}^n$ consisting of $n+1$ states and n edges such that there is an edge between any two adjacent states.

In the following, we derive lower and upper bounds on the number of computations required for the Viterbi algorithm in terms of $N(\Lambda)$.

Lemma 2.2 *Let a lattice $\Lambda \in \mathcal{L}_n$ have a finite trellis T with the number of distinct paths equal to $N(\Lambda)$. Then the number of computations C required for the Viterbi algorithm to decode Λ using T (also referred to as the Viterbi decoding complexity) satisfies*

$$\begin{aligned} nN(\Lambda)^{2/n} \leq C &\leq n[5\mathcal{G}(\Lambda) + 2\mathcal{E}(\Lambda) - \mathcal{S}(\Lambda) + 4n] \\ &\leq n[7N(\Lambda) - N(\Lambda)^{1/n} + 4n]\,. \end{aligned} \tag{2.19}$$

Proof: It can be seen that $C \geq n\mathcal{E}(\Lambda)$ [69]. Combining this with the lower bound of (2.17) results in the left hand side of (2.19).

To derive the upper bounds, we use the same notations as those employed in Section 2.3. As the first step for the decoding, we need to compute the coefficients

x_i in (2.13). Assuming that the inner products $\langle \mathbf{v}_i, \mathbf{v}_i \rangle$, $1 \leq i \leq n$, have been pre-computed, this step requires at most $2n^2$ arithmetic operations (n multiplications, $n-1$ additions, and one division for each x_i). Also, for metric computations in each trellis section i, $1 \leq i \leq n$, using (2.15), the VA has to perform at most g_i roundings, $2g_i$ subtractions, g_i squarings, and g_i multiplications. For the transition from level i to level $i+1, 0 \leq i \leq n-1$, in addition to metric computations, the VA needs to perform at most e_{i+1} additions, and $(e_{i+1} - s_{i+1})$ two-way comparisons. For the construction of the output vector through the survivor path, based on (2.14), and assuming that the values $\lceil x_i - a_j \rfloor$ for the survivor paths have already been computed and stored (during the computation of metrics), one needs to do at most n^2 multiplications and n^2 additions. Putting all these together results in the first upper bound of (2.19). Applying (2.16)-(2.18) to the first upper bound results in the second one. □

As we already discussed, it is favorable to find orthogonal sublattices of Λ with their indices as small as possible (corresponding to small values of $N(\Lambda)$). This will also tighten all the upper bounds of (2.16)-(2.19).

Chapter 3

Decoding lattices using the K-Z reduced basis

In this chapter, we first talk about some of the important lattices which have ESM. Then an introduction to the idea of basis reduction is presented, and the Korkin-Zolotarev (K-Z) reduced basis is discussed. The proposed decoding algorithm is developed later in the chapter, followed by discussions on its complexity issues. We also explain Kannan's algorithm and establish upper and lower bounds on its complexity.

We concentrate on the problem of using lattices in signal constellations. However, the problems of lattice-based channel coding and lattice-based vector quantization are closely related. In particular, the decoding algorithm discussed here can be used in both of these contexts.

In this chapter, we assume the bases to be rational. This assumption is made only as a matter of computational concern, and all the lemmas, propositions, theorems, and corollaries are valid for a general basis (consisting of vectors with real

elements).

3.1 Extremal and ESM lattices

An n-D lattice Λ_0 is called *extremal* if $\gamma(\Lambda_0)$ is a local maximum, i.e., if in the space of n-D lattices, there exists a neighborhood $\mathcal{N}$ of Λ_0 such that $\gamma(\Lambda) \leq \gamma(\Lambda_0)$, for $\Lambda \in \mathcal{N}$. Extremal lattices have relatively high coding gains and could be favorable in channel coding applications. Clearly, the extremal property of a lattice is invariant under scalings and/or orthogonal transformations of the lattice (it is geometrically invariant). The next theorem, quoted from [37, p. 300], is of great importance in the following discussions.

Theorem 3.1 *Each extremal lattice has ESM.*

As the first corollary, it can be concluded that:

Corollary 3.1 *The densest lattices have ESM.*

Proof: The coding gain of the densest lattices are globally maximum, and therefore locally maximum. (Another proof for this corollary, independent of Theorem 3.1, is given in Appendix A). □

Noting that E_6, E_7, and E_8 are the densest lattices in their corresponding dimensions, it follows from Corollary 3.1 that they are ESM-lattices.

Coxeter proved that lattices A_n and D_n are extremal (see [37, p. 404]). Barnes and Wall constructed another infinite sequence of extremal lattices (BW_n), which are probably the most famous lattices in communications. Two other well-known extremal lattices are Leech (Λ_{24}), and Coxeter-Todd (K_{12}) lattices. We therefore, obtain the following corollary.

Corollary 3.2 *Lattices* A_n $(n \geq 1)$, D_n $(n \geq 3)$, E_n $(n = 6, 7, 8)$, $BW_n(n = 2^m, m = 2, 3, \ldots)$, Λ_{24}, *and* K_{12} *belong to the set of ESM-lattices.*

In spite of what might appear first, the condition of having ESM does not have a strong impact on the achievable coding gain for a lattice. Applying the condition of $\lambda_1 = \cdots = \lambda_n$ to the well-known inequality $\det(\Lambda) \leq \lambda_1 \cdots \lambda_n$, [19, sec. VIII.2], results in the trivial bound of $\gamma \geq 1$ on the coding gain. The bound is achieved for the integer lattice $\mathbb{Z}^n$. On the other hand, it is shown in [13] that, especially in large dimensions, obtaining large coding gains is possible without having ESM.

The following lemma introduces some other groups of ESM-lattices.

Lemma 3.1 *Lattices* A_n^* $(n \geq 1)$, D_n^* $(n \geq 3)$, *and* E_n^* $(n = 6, 7, 8)$ *have ESM.*

Proof: Since the method of the proof is similar for the three groups of lattices, only the proof for A_n^* is given here. Consider the following $n \times (n+1)$ basis matrix for A_n^* [25, p. 115],

$$B = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & -1 & \cdots & 0 & 0 \\ . & . & . & \cdots & . & . \\ 1 & 0 & 0 & \cdots & -1 & 0 \\ \frac{-n}{n+1} & \frac{1}{n+1} & \frac{1}{n+1} & \cdots & \frac{1}{n+1} & \frac{1}{n+1} \end{pmatrix}. \tag{3.1}$$

For this version of A_n^*, we have $\lambda = \sqrt{n/(n+1)}$. It is not difficult to see that the n vectors $\mathbf{b}_n$, $\mathbf{b}_n + \mathbf{b}_1$, $\mathbf{b}_n + \mathbf{b}_2$, $\ldots$, $\mathbf{b}_n + \mathbf{b}_{n-1}$ of the lattice are independent and have length λ. □

Based on the above facts, we conclude that almost all of the lattices currently used in communications, either in channel coding or in quantization applications, have ESM.

3.2 Korkin-Zolotarev (K-Z) reduced basis

The algorithm for finding the closest point of $\mathbb{Z}^n$, the lattice of n-D integer vectors, to an arbitrary point $\mathbf{x} \in \mathbb{R}^n$ is particularly simple. For a real number r, let $\lceil r \rfloor \in \mathbb{Z}$ denote the nearest integer to r. It is not difficult to see that $\lceil \mathbf{x} \rfloor \triangleq (\lceil x_1 \rfloor, \ldots, \lceil x_n \rfloor)$ is the closest point of $\mathbb{Z}^n$ to $\mathbf{x}$. We call this method of decoding the "round-off procedure".

Let Λ be a lattice in $\mathbb{R}^m$ given by basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, and suppose that $\mathbf{x} \in \mathbb{R}^m$ is an arbitrary point. Let $\mathbf{x} = \mathbf{x}' + \mathbf{x}''$ with $\mathbf{x}' \in span(\Lambda)$ and $\mathbf{x}'' \in span(\Lambda)^{\perp}$. Clearly, the nearest point of Λ to $\mathbf{x}$ is the one nearest to $\mathbf{x}'$. Let $\mathbf{x}' = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$. The round-off procedure on basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ in $span(\Lambda)$ decodes $\mathbf{x}'$ to $\mathbf{y} = \sum_{i=1}^{n} \lceil \alpha_i \rfloor \mathbf{b}_i$. Geometrically, this is equivalent to employing a parallelotope decision region[1] spanned by vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$, centered at each lattice point. It can be shown that although the round-off procedure is a polynomial-time algorithm and particularly efficient, it obtains the nearest point of the lattice iff the basis vectors are mutually orthogonal. Unfortunately, for lattices with $\gamma > 1$, there does not exist such a basis (this can be easily proved by contradiction).

The nice properties of orthogonal bases motivate searching for the bases of a lattice which are nearly orthogonal. The problem of transforming a given lattice basis into a basis consisting of vectors which are pairwise nearly orthogonal is called *lattice basis reduction*[2].

The reduction theory, which has its historical roots in the 18-th century, was mainly motivated by the classical question of finding the minima of positive definite

[1]The *decision region* of a point $\mathbf{p}_i$ belonging to a discrete collection of points $\{\mathbf{p}_1, \mathbf{p}_2, \ldots\} \subset span(\Lambda)$, consists of those points of $span(\Lambda)$ which are decoded to $\mathbf{p}_i$.

[2]More generally, the concern of reduction theory is to select a basis with desirable properties from the set of all bases for a lattice.

integral forms. Several distinct notions of reduction have been studied, including those associated to the names Hermite, Minkowski, Korkin-Zolotarev (K-Z), and more recently Lenstra-Lenstra and Lovász (L^3); see e.g., [37, pp. 147-164]. After the introduction of the L^3 reduced basis, which can be computed in polynomial time, reduction theory has found many applications in a variety of areas (see, e.g., [54], [55], [42], [39], [2], [58], [43], [38], [67, pp. 71-74]). It can be shown that for the decoding of lattices, the K-Z reduced basis is a more powerful tool than the L^3 reduced basis [13]. In the following, we explain the K-Z reduced basis which is used in the decoding algorithms we study.

Let $\Lambda \subset \mathbb{Q}^m$ be a lattice with ordered basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, and the corresponding G-S vectors $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$. In the lattice decoding algorithm presented in Subsection 3.3.1, one needs to check the distance between a given vector $\mathbf{x} \in \mathit{span}(\Lambda)$ and a subset of the lattice vectors. The upper bound on the number of candidates needed to be checked depends on the lengths of the G-S vectors. Consequently, it is desirable to make these lengths as small as possible by finding a properly reduced basis of the lattice Λ. By the reduction theory introduced by Korkin and Zolotarev [47] the vectors of a basis can be selected such that the lengths of the corresponding G-S vectors are minimized successively, i.e.,

$$\|\hat{\mathbf{b}}_i\| = \lambda(\Lambda_{(i)}) \quad \text{for} \quad i = 1, \ldots, n\,, \tag{3.2}$$

where $\lambda(\Lambda_{(i)})$ is the length of a shortest vector of the i-th projected lattice $\Lambda_{(i)}$. In particular, $\|\hat{\mathbf{b}}_1\| = \|\mathbf{b}_1\| = \lambda(\Lambda)$. This basis is called a Korkin-Zolotarev (K-Z) reduced basis of Λ.

It can be shown that each lattice has at least one K-Z reduced basis (see [43] or [66]). The K-Z reduced bases are extensively studied in [49]. There is no polynomial-time algorithm known for K-Z reduction. Finding a K-Z reduced basis

of a lattice is actually polynomial-time equivalent to finding a shortest vector of the lattice. The fastest known algorithm for K-Z reduction of a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^m$ with $\varphi = \max(\|\mathbf{b}_1\|^2, \ldots, \|\mathbf{b}_n\|^2)$ and $m = O(n)$ has a theoretic worst case time bound of $\sqrt{n}^{\,n+o(n)} + O(n^4 \log\varphi)$ arithmetic steps on $O(n\log\varphi)$-bit integers and is due to Schnorr [66]. This algorithm is an improved version of Kannan's shortest lattice vector algorithm [43].

Example 3.1 *We obtain the following K-Z reduced bases for the lattices D_4 and E_8.*

$$B_{D_4} = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \end{pmatrix}, \quad B_{E_8} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & -1 & 1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \\ -1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & -1 & 0 & 1 \end{pmatrix}.$$

In the following, we prove a proposition which is of great importance to its subsequent results.

Proposition 3.1 *Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a K-Z reduced basis of a lattice Λ, with Gram-Schmidt orthogonalization $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$. Then, we have*

$$\|\hat{\mathbf{b}}_i\| \leq \lambda_i(\Lambda) \quad \textit{for } i = 1, \ldots, n\,, \tag{3.3}$$

where $\lambda_i(\Lambda)$ is the i-th successive minimum of Λ. All the inequalities are satisfied with equality if the basis is orthogonal.

Proof: By the definition of $\lambda_i(\Lambda)$, there exist i linearly independent vectors of lattice Λ of length at most $\lambda_i(\Lambda)$. Under the projection $\Lambda \longrightarrow \Lambda_{(i)}$, at least one of these vectors, say $\mathbf{v}$, has a nonzero projection $\mathbf{v}(i)$. Therefore, we have $\lambda(\Lambda_{(i)}) \leq \|\mathbf{v}(i)\|$. This inequality combined with the fact that $\|\mathbf{v}(i)\| \leq \|\mathbf{v}\| \leq \lambda_i(\Lambda)$ results in $\lambda(\Lambda_{(i)}) \leq \lambda_i(\Lambda)$. Combining this with (3.2), we obtain $\|\hat{\mathbf{b}}_i\| \leq \lambda_i(\Lambda)$ for $i = 1, \ldots, n$.

If the K-Z basis is orthogonal, we have $\|\hat{\mathbf{b}}_i\| = \|\mathbf{b}_i\|, \ \forall i$, and therefore $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \ldots \leq \|\mathbf{b}_n\|$ (one can obtain a K-Z reduced basis for a lattice Λ with an orthogonal basis simply by arranging the basis vectors in order of increasing length). Combining this with the definition of $\lambda_i(\Lambda)$, we obtain $\lambda_i(\Lambda) \leq \|\mathbf{b}_i\| = \|\hat{\mathbf{b}}_i\|, \ \forall i$. This together with (3.3) results in $\|\hat{\mathbf{b}}_i\| = \lambda_i(\Lambda), \ \forall i$. □

It is not difficult to see that having all the inequalities in (3.3) satisfied with equality does not necessarily result in the orthogonality of the basis (a 2-D rectangular lattice with a non-orthogonal basis is a straight-forward counterexample). It however, does result in the fact that the lattice is rectangular (to prove this, one could use the same approach as the one which will be employed in the last paragraph of the alternative proof for Theorem 6.1).

Corollary 3.3 *If $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a K-Z reduced basis of an ESM-lattice, then*

$$\max_{1 \leq i \leq n} \|\hat{\mathbf{b}}_i\| = \|\hat{\mathbf{b}}_1\| \,. \tag{3.4}$$

Proof: The proof follows by putting the result of Proposition 3.1 together with the facts that for an ESM-lattice $\lambda_1 = \lambda_2 = \cdots = \lambda_n$, and for a K-Z reduced basis $\|\hat{\mathbf{b}}_1\| = \lambda_1$. □

It is interesting to note that the above result can be equivalently expressed as

$$\lambda(\Lambda) = \max\{\|\hat{\mathbf{b}}_1\|, \ldots, \|\hat{\mathbf{b}}_n\|\} \,.$$

Comparing this equality with (2.9) gives another evidence for the strength of K-Z reduction.

As already mentioned, in applications to communication systems, we assume that the computation devoted to finding a reduced basis is performed once (off-line), and we do not consider this computation as a part of the decoding complexity. In the rest of the chapter, the lattices are assumed to be full-dimensional, i.e., $n = m$. Although this assumption simplifies some of the discussions, it does not reduce their generality.

3.3 Lattice decoding problem

In this section, first, we discuss Kannan's decoding algorithm and its complexity. Then, in Subsection 3.3.1, we propose some modifications which increase the efficiency of Kannan's algorithm, especially in communication applications. The complexity bounds for the proposed algorithm are derived in Subsection 3.3.2.

Consider the following lattice decoding problem:

(LDP) Given the vector $\mathbf{x} \in \mathbb{Q}^n$ and lattice $\Lambda = L(\mathbf{b}_1, \ldots, \mathbf{b}_n) \subset \mathbb{Q}^n$, find a lattice vector $\mathbf{b} = \sum_{j=1}^{n} \beta_j \mathbf{b}_j$ such that $\|\mathbf{x} - \mathbf{b}\|$ is minimized. (3.5)

In 1981, Van Emde Boas proved that the problem is NP-hard [73]. A simpler proof was subsequently given by Kannan in 1987, [43]. More recently, it has been shown by Arora et al. that even approximating the solution within any constant factor is NP-hard [1]. Some other relevant results regarding the approximate solutions for LDP can be found in [2], [38], [49].

The fastest (best upper bound on the complexity) known algorithm for solving LDP for a general lattice is due to Kannan [43]. This is an improved version of his

earlier work in [42]. Prior to [43], Helfrich [39] has also made some improvements in the running time of some of the algorithms in [42]. In [43], Kannan uses the same reduced basis as used in this work[3], and shows that for some particular i_1 such that $\|\hat{\mathbf{b}}_{i_1}\| = \max \|\hat{\mathbf{b}}_j\|$, $j \in \{1, \ldots, n\}$, there exists a subset of $\mathbb{Z}^{n-i_1+1}$ of cardinality at most $(n+\sqrt{n})^{(n-i_1+1)}$ that contains the values $(\beta_{i_1}, \ldots, \beta_n)$ of the nearest point. Now, if $\mathbf{b}'$ solves the LDP for the vector $\mathbf{x} - \sum_{j=i_1}^{n} \beta_j \mathbf{b}_j$ and the lattice $L(\mathbf{b}_1, \ldots, \mathbf{b}_{i_1-1})$, then $\mathbf{b}' + \sum_{j=i_1}^{n} \beta_j \mathbf{b}_j$ is a solution candidate of the problem for $\mathbf{x}$ and $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Therefore, the original problem can be reduced to at most $(n+\sqrt{n})^{(n-i_1+1)}$ subproblems, each of dimensionality $i_1 - 1$. In the following, we present a geometrical interpretation for Kannan's algorithm which provides a better understanding of some complexity issues discussed later.

Let indices $i_0, \ldots, i_k$, where $k \leq n$ is a constant integer, be successively defined by $\|\hat{\mathbf{b}}_{i_j}\| = \max_{1 \leq m \leq i_{j-1}-1} \|\hat{\mathbf{b}}_m\|$, for $1 \leq j \leq k$, with $n+1 = i_0 > i_1 > \cdots > i_k = 1$. Here i_1 is the same index as defined in the last paragraph. A careful inspection of Kannan's algorithm [43] reveals that if $i_j \leq q \leq i_{j-1} - 1$, then the algorithm recursively searches for the candidates $\mathbf{b}$ such that the projection length of $(\mathbf{b} - \mathbf{x})$ along the G-S vector $\hat{\mathbf{b}}_q$ is at most $\ell_j = \sqrt{\sum_{m=1}^{i_{j-1}-1} \|\hat{\mathbf{b}}_m\|^2}/2$. Thus the algorithm may be thought of as searching among lattice points in a rectangular parallelepiped centered at $\mathbf{x}$, with edges pointing parallel to the G-S vectors of the lattice. The edge length of the parallelepiped along $\hat{\mathbf{b}}_q$ is $2\ell_j$. (Note that $\ell_1 > \ldots > \ell_k$). For simplicity, we think of such rectangular parallelepipeds as cubes, and we call the algorithms of this type "recursive cube search" (RCS) algorithms. As we will see later, our proposed algorithm also belongs to this category.

[3]The reduced basis used by Kannan has an extra condition on the value of G-S coefficients $\mu_{i,j}$, i.e., $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$. This condition, however, does not affect the G-S orthogonalization of the basis.

The computational complexity of Kannan's algorithm depends on the values of $i_1, \ldots, i_{k-1}$. One can see that $i_1 = 1$ corresponds to the highest complexity. In this case, the original problem is reduced to at most $(n + \sqrt{n})^n$ 0-dimensional subproblems. Each subproblem is solved by just checking the distance between $\mathbf{x}$ and a certain point of the lattice. It can be shown that the number of arithmetic operations for Kannan's algorithm is bounded above by $(2n)^{n+O(1)}$,[4]. This bound is obtained based on the amount of computation required for the worst case of $i_1 = 1$, and the fact that the number of arithmetic operations needed to find a candidate and check its distance to the given vector is polynomially bounded by n.

We are also interested in obtaining lower bounds on the complexity of such algorithms. To emphasize the importance of lower bounds, we pose the following question: "Is there any sequence of lattices with possible application in communications ($\gamma \geq 1$) such that Kannan's algorithm can decode them in polynomial time for an arbitrary $\mathbf{x}$?". As we will see later, using the derived lower bound, the answer to this question is negative even if one finds the best possible basis.

In the following, the number of lattice points $N_p(\cdot)$ that should be checked is defined as the measure of decoding complexity. This can be easily translated in terms of the required number of arithmetic operations in O-notation. For both Kannan's and our proposed algorithm, $N_p(\cdot)$ depends not only on the selection of basis, but also on vector $\mathbf{x}$ and the structure of the lattice itself. The notation

[4]Kannan's result in [43] is, however, slightly different. It is claimed in Theorem 4.5 of [43] that the number of arithmetic operations performed by the algorithm is $O(n^n)$. The author believes that this is an under-estimation, since for the worst case of $i_1 = 1$, even the number of candidates, i.e., $(n + \sqrt{n})^n$, cannot be upper bounded by cn^n, for any positive constant c. The misleading component in the proof turns out to be the wrong assumption that the maximum of $\{(i-1)/(n+\sqrt{n})\}^{(i-1)}$ for $1 \leq i \leq n$ is attained at $i = n$. It is not difficult, however, to see that the maximum is 1, and is obtained for $i = 1$.

$N_p(\mathbf{x}, \Lambda, B)$ is therefore used for the number of candidates, where B is the basis matrix of the lattice. For the sake of simplicity, we sometimes use the notation N_p instead of $N_p(\mathbf{x}, \Lambda, B)$. We also sometimes use the logarithm of the number of candidates (or more generally, the logarithm of the complexity measure) as an index of complexity, referred to hereafter as the *log-complexity* (the base of the logarithm can be selected arbitrarily).

Let $\mathcal{S}$ denote the region of the space that an RCS algorithm searches to solve LDP. As a rough approximation for the complexity measure N_p, one can consider its average value $\bar{N}_p(\Lambda, B)$, averaged over all vectors $\mathbf{x}$ which are uniformly distributed in a fundamental region of Λ. It can be seen that this is equal to

$$\bar{N}_p(\Lambda, B) = \frac{\mathrm{vol}(\mathcal{S})}{\det(\Lambda)}\,, \tag{3.6}$$

where $\mathrm{vol}(\mathcal{S})$ is the volume of $\mathcal{S}$. (Note that $\det(\Lambda)$ is also the volume of a fundamental region of Λ).

Using N_p as the measure of complexity, the complexity of Kannan's algorithm for the decoding of a general n-D lattice, and for an arbitrary $\mathbf{x}$ is upper bounded by $(n + \sqrt{n})^n$. This upper bound can be improved for ESM-lattices.

Theorem 3.2 *For an n-D ESM-lattice Λ with coding gain γ and K-Z reduced basis B, and for any given vector $\mathbf{x} \in \mathbb{R}^n$, the complexity of Kannan's algorithm satisfies*

$$N_p(\mathbf{x}, \Lambda, B) \leq (\sqrt{n} + 1)^n \gamma^{n/2}\,. \tag{3.7}$$

Proof: Based on the notations already used in describing Kannan's algorithm, we have an upper bound of $(2\ell_j/\|\hat{\mathbf{b}}_q\|) + 1$ on the number of possible values for each integer β_q, where $i_j \leq q \leq i_{j-1} - 1$. For ESM-lattices, using Corollary 3.3, we

have $k = 1$ ($i_1 = 1$), and each integer $\beta_q, q = 1, \ldots, n$, takes at most $(2\ell_1/\|\hat{\mathbf{b}}_q\|) + 1$ different values. This corresponds to the following upper bound on N_p.

$$N_p \leq \prod_{q=1}^{n} \left(\frac{\sqrt{\sum_{m=1}^{n} \|\hat{\mathbf{b}}_m\|^2}}{\|\hat{\mathbf{b}}_q\|} + 1 \right) \leq \prod_{q=1}^{n} \left(\frac{\sqrt{n}\|\hat{\mathbf{b}}_1\|}{\|\hat{\mathbf{b}}_q\|} + 1 \right) \leq (\sqrt{n} + 1)^n \frac{\|\hat{\mathbf{b}}_1\|^n}{\prod_{q=1}^{n} \|\hat{\mathbf{b}}_q\|}. \tag{3.8}$$

For the last two steps, we have used the fact that $\|\hat{\mathbf{b}}_m\| \leq \|\hat{\mathbf{b}}_1\|$ for $m = 1, \ldots, n$. The proof then follows by applying (2.8), the fact that for a K-Z reduced basis $\|\hat{\mathbf{b}}_1\| = \lambda$, and the definition of coding gain to (3.8). □

In fact, for ESM-lattices, the algorithm searches among the lattice points in the cube centered at $\mathbf{x}$, with its edges of length $2\ell_1$ and along the G-S vectors.

In Subsection 3.3.1, we modify Kannan's algorithm such that the length of each edge of the search cube is reduced. This implies that all the lower bounds derived on the complexity of the modified algorithm are also valid for Kannan's algorithm. The bounds, which are in terms of coding gain and dimension, result in the fact that for any sequence of lattices with possible application in communications ($\gamma \geq 1$), and any selected basis, the complexity of Kannan's algorithm grows at least exponentially with dimension and coding gain.

3.3.1 Modified Kannan's algorithm

Consider the lattice decoding problem defined in (3.5). Based on the definition of covering radius, the candidates for the nearest vector of Λ to a given vector $\mathbf{x}$ are the lattice points inside the sphere of radius $\mu(\Lambda)$, centered at $\mathbf{x}$. There does not, however, exist a good algorithm for finding the lattice points inside a sphere. The proposed approach for solving the LDP is to consider the lattice points inside a properly selected cube, centered at $\mathbf{x}$. To search inside the cube, we devise the

following RCS algorithm.

Modified recursive cube search algorithm

Let $\mathbf{b}$ be a candidate for the nearest vector of $\Lambda = L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ to a given vector $\mathbf{x} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i$, $\alpha_i \in \mathbb{Q}$, $\forall i$, and let $\mathbf{b} = \sum_{i=1}^{n} \beta_i \mathbf{b}_i$, $\beta_i \in \mathbb{Z}$, $\forall i$. The candidates can be checked by enumerating the coefficients β_i from β_n to β_1, successively. This can be performed efficiently by noticing the fact that we just need to search for $\mathbf{b}$ among the lattice points such that

$$\|\mathbf{b} - \mathbf{x}\| \leq \mu(\Lambda) \Longrightarrow \|(\mathbf{b} - \mathbf{x})(n)\| = |\beta_n - \alpha_n| \, \|\hat{\mathbf{b}}_n\| \leq \mu(\Lambda) \,, \tag{3.9}$$

where $(\mathbf{b}-\mathbf{x})(n)$ is the projection of $\mathbf{b}-\mathbf{x}$ along the G-S vector $\hat{\mathbf{b}}_n$. The last inequality in (3.9) enables us to enumerate β_n for the lattice points under consideration. Now, if $\mathbf{b}'$ solves the LDP for the vector $\mathbf{x} - \beta_n \mathbf{b}_n$ and the lattice $L(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$, then $\mathbf{b}' + \beta_n \mathbf{b}_n$ is a solution candidate of the problem for $\mathbf{x}$ and $L(\mathbf{b}_1, \ldots, \mathbf{b}_n)$. Therefore, the original problem can be reduced to several subproblems, each of dimensionality $n - 1$.

Let $\mu_i \triangleq \mu(L(\mathbf{b}_1, \ldots, \mathbf{b}_i))$, for $i = 1, \ldots, n$, and let $\mathcal{S}(\mathbf{x})$ denote the region of $\mathbb{R}^n$ that the algorithm searches to solve LDP for a given vector $\mathbf{x}$. It is not difficult to see that $\mathcal{S}(\mathbf{x})$ is a cube, centered at $\mathbf{x}$ with its edges of length $2\mu_1, \ldots, 2\mu_n$, and along the G-S vectors $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$, respectively. The volume of $\mathcal{S}(\mathbf{x})$ is therefore equal to

$$\mathrm{vol}(\mathcal{S}) = 2^n \prod_{i=1}^{n} \mu_i \,. \tag{3.10}$$

Note that, in general, the inequalities of the form $\mu_i \leq \mu_n = \mu(\Lambda)$, for $i = 1, \ldots, n$, do not hold. Therefore, to reduce the complexity, one can select the edge length of the search cube in the direction of $\hat{\mathbf{b}}_i$ to be the minimum of $2\mu_i$ and $2\mu(\Lambda)$. All the bounds derived later in Subsection 3.3.2 remain valid for this case.

Using the modified RCS algorithm, it appears that we only need to enumerate relatively few candidates from integer n-tuples $(\beta_1, \ldots, \beta_n)$. To derive a proper upper bound on the number of candidates, we first prove the following proposition.

Proposition 3.2 *Let* $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *be an ordered basis of a lattice* Λ*, with G-S orthogonalization* $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$*. Then, we have*

$$\mu(\Lambda) \leq d \triangleq \frac{1}{2}\sqrt{\sum_{i=1}^{n} \|\hat{\mathbf{b}}_i\|^2}\,, \tag{3.11}$$

where the inequality holds with equality if and only if there exists an orthogonal basis for Λ *with the lengths of its vectors equal to* $\|\hat{\mathbf{b}}_i\|, i = 1, \ldots, n$.

Proof: To each lattice point $\mathbf{b}$, we assign a cubic sub-optimum decision region centered at $\mathbf{b}$ with its edges along the G-S co-ordinates $\hat{\mathbf{b}}_1, \ldots, \hat{\mathbf{b}}_n$. The edge lengths are selected as $\|\hat{\mathbf{b}}_1\|, \ldots, \|\hat{\mathbf{b}}_n\|$, respectively. It is not difficult to see that these cubic regions partition the $\mathbb{R}^n$ space (each of them is a fundamental region for the lattice). Using the fact that the maximum distance between a lattice point and the points of its decision region is d and the definition of covering radius, the inequality follows immediately.

It is easy to see that if the basis is orthogonal, the inequality in (3.11) holds with equality. In this case, the Voronoi cells for the lattice points coincide with the aforementioned cubic decision regions. We sketch a proof to show that if $\mu(\Lambda) = d$, then there exists a basis of Λ which is orthogonal. Suppose that such a basis does not exist. Consider an arbitrary lattice point $\mathbf{b}$, and call its corresponding cubic decision region $\mathcal{R}(\mathbf{b})$. Except for the vertices of $\mathcal{R}(\mathbf{b})$, we have $\|\mathbf{b}-\mathbf{v}\| < d$, for every vector $\mathbf{v} \in \mathcal{R}(\mathbf{b})$. Let $\mathbf{p}$ be an arbitrary vertex of $\mathcal{R}(\mathbf{b})$. Since we are assuming that Λ is not rectangular, and because of the congruence of the structure, there should

exist a decision region $\mathcal{R}(\mathbf{b}')$ adjacent to $\mathcal{R}(\mathbf{b})$ which has $\mathbf{p}$ at its intersection with $\mathcal{R}(\mathbf{b})$, but $\mathbf{p}$ is not a vertex of $\mathcal{R}(\mathbf{b}')$, and therefore $\|\mathbf{b}' - \mathbf{p}\| < d$. It can be seen that if such a region does not exist, in other words if all the adjacent cubic regions have $\mathbf{p}$ as their vertex, then for the whole structure all the adjacent cubes coincide in their vertices and consequently, the lattice is rectangular and there should exist an orthogonal basis. This shows that there exists no vector $\mathbf{v} \in \mathbb{R}^n$ such that the distance between $\mathbf{v}$ and the lattice is greater than or equal to d, which results in $\mu(\Lambda) < d$. □

It can be concluded from the proof of Proposition 3.2 that for any given $\mathbf{x} \in \mathbb{R}^n$, there exists a unique $\mathbf{b} \in \Lambda$ such that $\mathbf{x} = \mathbf{b} + \sum_{i=1}^{n} \eta_i \hat{\mathbf{b}}_i$, $-\frac{1}{2} \leq \eta_i < \frac{1}{2}$, $\forall i$, where $\mathbf{x}$ is located inside the cubic decision region of point $\mathbf{b}$.

In the following, we derive lower and upper bounds on $N_p(\mathbf{x}, \Lambda, B)$ for the modified RCS algorithm.

Proposition 3.3 *For any basis B of a lattice Λ, and any $\mathbf{x} \in \mathbb{R}^n$, the number of candidate points $N_p(\mathbf{x}, \Lambda, B)$ of the modified RCS algorithm satisfies*

$$\prod_{i=2}^{n} \left(\frac{2\mu_i}{\|\hat{\mathbf{b}}_i\|} - 1 \right) < N_p(\mathbf{x}, \Lambda, B) \leq \prod_{i=1}^{n} \left(\frac{2\mu_i}{\|\hat{\mathbf{b}}_i\|} + 1 \right) . \tag{3.12}$$

Proof: We enumerate β_i's from β_n to β_1, successively. This means that for each β_i , $i = 1, \ldots, n$, the values taken by $\beta_{i+1}, \ldots, \beta_n$ have been already selected. Starting from β_n, using (3.9) and the fact that β_n is an integer, we obtain the lower bound of $(2\mu_n/\|\hat{\mathbf{b}}_n\|) - 1$ and the upper bound of $(2\mu_n/\|\hat{\mathbf{b}}_n\|) + 1$ on the number of possible values for β_n. Using a similar discussion for every $i = 1, \ldots, n$, the inequality follows. Note that for $i = 1$, $\mu_1 = \|\hat{\mathbf{b}}_1\|/2$, and the number of possible values for β_1 is at least 1. □

Remark: Applying (2.8) and Proposition 3.2 to the upper bound of (3.12), we obtain

$$N_p(\mathbf{x}, \Lambda, B) \leq \frac{\prod_{i=1}^{n}(\sqrt{\sum_{j=1}^{i} \|\hat{\mathbf{b}}_j\|^2} + \|\hat{\mathbf{b}}_i\|)}{\det(\Lambda)} \ . \tag{3.13}$$

For a fixed lattice Λ, $\det(\Lambda)$ has a fixed value, and the bound in (3.13) is just a function of the lengths of the G-S vectors. This justifies the selection of K-Z reduced basis for the decoding algorithm. Note that although the $\|\hat{\mathbf{b}}_i\|$'s are minimized successively for a K-Z reduced basis, this selection does not necessarily result in minimizing the upper bound of (3.13).

The following example shows the superiority of the proposed algorithm over Kannan's method.

Example 3.2 *For E_8, using the K-Z reduced basis given in Example* 3.1, *we obtain the following lengths for the corresponding G-S vectors:* 2.000, 1.732, 1.633, 1.414, 1.414, 1.225, 1.155, 1.000. *Since E_8 has ESM, Kannan's algorithm searches in a cube of edge length $\sqrt{\sum_{m=1}^{8} \|\hat{\mathbf{b}}_m\|^2} = 4.183$, with edges along the G-S vectors. This corresponds to enumerating at most $3, 3, 3, 3, 3, 4, 4$, and 5 different values for $\beta_1, \ldots, \beta_8$, respectively. This results in $N_p \leq 19440$. For the modified algorithm, even by searching in a cube of edge length $2\mu = 2\sqrt{2}$ with edges along the G-S vectors, we enumerate at most $2, 2, 2, 3, 3, 3, 3$, and 3 different values for $\beta_1, \ldots, \beta_8$, respectively. We thus have $N_p \leq 1944$, which is ten times smaller than the bound for Kannan's algorithm.*

In an efficient implementation of the algorithm, one can simply update the distances from point to point, and only keep the nearest vector $\mathbf{b}^* \in \Lambda$ to $\mathbf{x}$ found so far. Noting that the coefficient matrix in (2.7) is triangular, a more efficient implementation is possible if one uses the G-S co-ordinates for representing the

basis vectors. In this work, however, our main concern is the complexity bounds. From this point of view, it is clear that the number of required arithmetic operations for finding a candidate lattice point, and checking its distance to the given vector is polynomially bounded by n. Having selected the values $\beta_{k+1}, \ldots, \beta_n$, one can also use branch-and-bound, and prune any further search of vectors of the form $\mathbf{b} = \mathbf{b}' + \sum_{i=k+1}^{n} \beta_i \mathbf{b}_i$ with $\mathbf{b}' \in L(\mathbf{b}_1, \ldots, \mathbf{b}_k)$, if $\|(\mathbf{b} - \mathbf{x})(k+1)\| \geq \|\mathbf{b}^* - \mathbf{x}\|$, where $(\mathbf{b} - \mathbf{x})(k+1)$ is the orthogonal projection of $\mathbf{b} - \mathbf{x}$ on $span(\mathbf{b}_1, \ldots, \mathbf{b}_k)^{\perp}$. One can also stop enumerating β_1 when $\|\mathbf{b}-\mathbf{x}\|$ starts increasing. Moreover, there is a quick certificate for the closest vector of a lattice Λ to a given vector $\mathbf{x}$, i.e., if for a candidate $\mathbf{b}$, $\|\mathbf{b}-\mathbf{x}\| \leq \lambda(\Lambda)/2$, then $\mathbf{b}$ is the closest vector of Λ to $\mathbf{x}$. This condition can be checked for each candidate, and if satisfied one can stop the algorithm[5]. It is conceivable that by embedding the above points in the algorithm, not every lattice vector in the cubic region $\mathcal{S}(\mathbf{x})$ must be examined. This, in particular, can affect the derived lower bounds on the complexity of RCS algorithms. However, this effect is presumably small, especially for the asymptotics of the algorithm, and in any case it cannot be mathematically analyzed in a reasonable way.

3.3.2 Complexity bounds for the modified RCS algorithm

Upper bounds on complexity

Using Proposition 3.2, it is clear that Kannan's algorithm searches in a larger region of the space as compared to the modified algorithm, and consequently has a larger number of candidate points to check[6]. This implies that the upper bounds derived

[5]This point was suggested by one of the reviewers of [9].

[6]Note that even if we use the upper bounds on μ_i's given by (3.11) instead of the μ_i's themselves, in general, the algorithm still searches in a smaller cube and therefore has a lower com-

for Kannan's algorithm are also valid for the proposed algorithm. Tighter bounds, however, can be found as follows.

Theorem 3.3 *For an n-D lattice Λ with a K-Z reduced basis B, and for any $\mathbf{x} \in \mathbb{R}^n$,*

$$N_p(\mathbf{x}, \Lambda, B) \leq \prod_{i=1}^{n} (\sqrt{i} + 1) {\gamma_n}^{n/2} . \tag{3.14}$$

Proof: Combining (3.3) with (3.13) results in

$$N_p \leq \frac{\prod_{i=1}^{n} (\sqrt{\sum_{j=1}^{i} \lambda_j^2(\Lambda)} + \lambda_i(\Lambda))}{\det(\Lambda)} \leq \frac{\prod_{i=1}^{n} (\sqrt{i} + 1) \lambda_i(\Lambda)}{\det(\Lambda)} , \tag{3.15}$$

where for the last step, we have used (2.1). Inequality (3.15) together with (2.4) completes the proof. □

As a corollary of Theorem 3.3, we obtain the following upper bound on the complexity.

Corollary 3.4 *For an n-D lattice Λ with a K-Z reduced basis B, and for any $\mathbf{x} \in \mathbb{R}^n$,*

$$N_p(\mathbf{x}, \Lambda, B) \leq (\sqrt{n} + 1)^n {\gamma_n}^{n/2} . \tag{3.16}$$

For ESM-lattices, the bound in (3.14) can be improved as follows. The two bounds coincide for the densest lattices.

plexity compared to Kannan's method. In this case, the difference between complexities could be especially large for the decoding of lattices with $\max_i \|\hat{\mathbf{b}}_i\| = \|\hat{\mathbf{b}}_1\|$ (including ESM-lattices).

Theorem 3.4 *For an n-D ESM-lattice Λ with coding gain γ and K-Z reduced basis B, and for any $\mathbf{x} \in \mathbb{R}^n$,*

$$N_p(\mathbf{x}, \Lambda, B) \leq \prod_{i=1}^{n} (\sqrt{i} + 1)\gamma^{n/2} . \tag{3.17}$$

Proof: The result follows by applying $\lambda_1 = \cdots = \lambda_n$ to (3.15), and using (2.2).□

As a corollary of the above theorem, we obtain the same upper bound as given in Theorem 3.2 on the complexity of the algorithm for ESM-lattices. Using $\gamma_n \leq n$, inequality (3.16) corresponds to the bound $(2n)^{n+O(1)}$ for the required number of arithmetic operations, and to the log-complexity of $n \log n + O(n)$. Although this bound cannot be improved for the densest lattices, for most ESM-lattices better complexity bounds can be found based on (3.7).

Example 3.3 *Consider Barnes-Wall lattices $BW_n (n = 2^m, m \geq 2)$, with coding gain $\gamma = \sqrt{n/2}$. Substituting this quantity in (3.7), we obtain $N_p(BW_n) \leq (1 + \sqrt{n})^n (n/2)^{n/4}$. It is not difficult to see that the corresponding log-complexity is $(3n \log n)/4 + O(n)$.*

Lower bounds on complexity

As we already know, solving LDP for a general lattice is NP-hard. Combining this fact with the widely believed conjecture of NP≠P implies that no proposed algorithm can solve LDP for a general lattice in polynomial time. Now, one might ask the following question: "Is it possible to solve LDP in polynomial time in communication applications?". When posing this problem, one might have the idea of doing some pre-computations (e.g. finding an appropriate basis and/or

computing the covering radii of the lattice and its sub-lattices). In the following, we show that for lattices with sufficiently large coding gains (including all the lattices used in communications, with $\gamma \geq 1$), there does not exist any basis such that using the proposed algorithm, and therefore Kannan's algorithm, one can solve LDP in polynomial time. To show this, we first prove the following theorem.

Theorem 3.5 *For an n-D lattice Λ with any basis B,*

$$\bar{N}_p(\Lambda, B) \geq 0.866[1.333\gamma(\Lambda)]^{n/2} . \tag{3.18}$$

Proof: For the modified RCS algorithm, using (3.6) and (3.10), we have

$$\bar{N}_p(\Lambda, B) = \frac{2^n \prod_{i=1}^{n} \mu_i}{\det(\Lambda)} . \tag{3.19}$$

A result, due to Ryškov [64], implies that for an n-D lattice, $\mu/\lambda \geq \sqrt{n/(2n+2)}$. Applying this inequality for dimensions $i = 1, \ldots, n$, to (3.19), and using the fact that $\lambda(L(\mathbf{b}_1, \ldots, \mathbf{b}_i)) \geq \lambda(\Lambda)$, for $i = 1, \ldots, n$, we obtain

$$\bar{N}_p(\Lambda, B) \geq \prod_{i=1}^{n} \sqrt{\frac{2i}{i+1}} \frac{\lambda^n(\Lambda)}{\det(\Lambda)} \geq (1.1547)^{n-1}[\gamma(\Lambda)]^{n/2} . \tag{3.20}$$

For the last step, we have used the definition of $\gamma(\Lambda)$, and the fact that $\sqrt{2i/(i+1)}$ is a uniformly increasing function of i with the value of 1.1547 at $i = 2$. The proof then immediately follows from (3.20). □

Note that for a K-Z reduced basis $\lambda(L(\mathbf{b}_1, \ldots, \mathbf{b}_i)) = \lambda(\Lambda)$, for $i = 1, \ldots, n$. This, however, cannot improve the lower bound of (3.18). The following corollary is a consequence of Theorem 3.5.

Corollary 3.5 *For an n-D lattice Λ with any basis B, there exists some $\mathbf{x} \in \mathbb{R}^n$ such that*

$$N_p(\mathbf{x}, \Lambda, B) \geq 0.866[1.333\gamma(\Lambda)]^{n/2} . \tag{3.21}$$

Inequality (3.21) shows that for lattices with sufficiently large coding gains, and for a general given vector $\mathbf{x}$, the complexity of the modified RCS algorithm grows at least exponentially with n and γ. (Note that $n \geq \gamma$).

As a complement to Theorem 3.4, we derive the following lower bound on the decoding complexity of ESM-lattices which is somehow stronger than Corollary 3.5.

Theorem 3.6 *For an n-D ESM-lattice Λ with coding gain γ and K-Z reduced basis B, and for any $\mathbf{x} \in \mathbb{R}^n$,*

$$N_p(\mathbf{x}, \Lambda, B) > 6.464(0.023\gamma)^{n/2} . \tag{3.22}$$

Proof: Starting from the lower bound of (3.12), we first multiply it by $2\mu_1/\|\hat{\mathbf{b}}_1\| = 1$, then use (2.8), Corollary 3.3, Ryškov's inequality for dimensions $i = 1, \ldots, n$, and finally the fact that for a K-Z reduced basis $\lambda(L(\mathbf{b}_1, \ldots, \mathbf{b}_i)) = \lambda(\Lambda)$, for $i = 1, \ldots, n$, to obtain

$$N_p(\mathbf{x}, \Lambda, B) > \prod_{i=2}^{n} (\sqrt{\frac{2i}{i+1}} - 1) \frac{\lambda^n(\Lambda)}{\det(\Lambda)} . \tag{3.23}$$

Applying (2.2), and substituting $i = 2$ in all the terms in the above product complete the proof. (Note that $\sqrt{2i/(i+1)}$ is a uniformly increasing function of i). □

In the case of densest lattices and for large values of n, combining Theorem 3.6 with the lower bound of (2.3) results in the log-complexity of at least $(n/2)log\ n + O(n)$ for the decoding algorithm.

3.4 Conclusion

Solving the lattice decoding problem (LDP) is the major obstacle associated with using a lattice in communication applications. There exist very efficient algorithms for solving LDP in the case of lattices with strong algebraic structures. This is not, however, the case for a general lattice. In this work, we have obtained some results regarding the complexity of solving LDP for a general lattice. These results relate the decoding complexity to the coding gain γ and the dimension n of the lattice, and are obtained based on a decoding approach which is an improved version of Kannan's algorithm. The complexity results have been improved for the important class of ESM-lattices.

It has been shown that Kannan's algorithm, which is currently the fastest known algorithm for solving LDP for a general lattice, is actually a search method inside a rectangular parallelepiped (cube) with edges along the Gram-Schmidt vectors of the lattice. Explicit lower and upper bounds on the complexity of Kannan's algorithm have been derived.

The proposed algorithm solves the LDP recursively by reducing the dimension of the problem by one in each step. It employs a Korkin-Zolotarev (K-Z) reduced basis of the lattice, and to increase the efficiency for the decoding of lattices in communications, it also uses the knowledge of the covering radii of the lattice and its sub-lattices. It has been shown that the algorithm searches in a similar cube as Kannan's algorithm does, except that the edges of the cube are smaller for the proposed algorithm. Explicit lower and upper bounds in terms of γ and n have been derived on the complexity of the algorithm.

It was proved in [70] that the trellis decoding complexity of lattices grows exponentially with coding gain. In this work, using the derived lower bounds, we have

proved a parallel result for RCS algorithms, i.e., for any selected basis, the decoding complexity of any sequence of lattices with possible application in communications ($\gamma \geq 1$) increases exponentially with dimension and coding gain. This suggests that RCS algorithms are not going to be attractive for the decoding of dense lattices in high dimensions. The lower bound also indicates that our upper bound results cannot be much improved.

Using the derived bounds, we have obtained $n \log n + O(n)$ and $(n/2) \log n + O(n)$ as upper and lower bounds on the decoding log-complexity of the densest lattices, respectively. It has also been shown that tighter upper bounds in terms of dimension can be found for many interesting sequences of ESM-lattices.

Chapter 4

Trellis complexity of lattices

It is described how the problem of finding a proper trellis coordinate system is reduced to the problem of searching for a proper basis of the lattice. We also explain the Hermite Normal Form (HNF) of a lattice and discuss in more detail the construction and analysis of the trellis of a lattice, given its basis. In Section 4.2, some results relating the trellis complexity of dual lattices are established. These results are used later in Section 4.3 to develop upper bounds on the trellis complexity of lattices. They are also employed in Chapter 5 for finding low-complexity trellis diagrams. Moreover, we give lower bounds on the trellis complexity of lattices.

4.1 More on trellis construction

The following lemma, which is of key importance to the rest of this work, shows that the problem of finding a proper orthogonal sublattice (or a proper trellis coordinate system) for a lattice $\Lambda \in \mathcal{L}$ can be reduced to the problem of finding a proper basis of Λ.

Lemma 4.1 *Let $\Lambda \in \mathcal{L}_n$ have a finite trellis defined by the sequence of vector spaces $\{\mathbf{0}\} = V_0 \subset V_1 \subset \cdots \subset V_n = \mathbb{R}^n$, and let $V_i = V_{i-1} \oplus W_i$, $1 \leq i \leq n$. Then there exists a basis $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ of Λ such that $V_i = span(\mathbf{b}_1, \cdots, \mathbf{b}_i)$, and $W_i = span(\hat{\mathbf{b}_i})$, for $1 \leq i \leq n$.*

Proof: We first inductively find vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$, that satisfy the conditions of the lemma, and then prove that they form a basis for Λ.

We begin by selecting $\mathbf{b}_1$ as a shortest vector of the lattice Λ_1. Now suppose that vectors $\mathbf{b}_1, \cdots, \mathbf{b}_i$ have been chosen ($1 \leq i \leq n-1$). We then choose $\mathbf{b}_{i+1}$ to be a lattice vector in Λ_{i+1} with a minimum positive distance to V_i. Note that since $\dim(\Lambda_i) = i$, $1 \leq i \leq n$, the above algorithm succeeds in every stage. By the construction, the n obtained vectors are independent. Moreover, $V_i = span(\mathbf{b}_1, \cdots, \mathbf{b}_i)$, and $W_i = span(\hat{\mathbf{b}_i})$, for $1 \leq i \leq n$. Now let $\mathbf{x}$ be an arbitrary point of Λ. It can be written as $\mathbf{x} = x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n$, where x_i's are real numbers. Let $p_i = x_i - \lfloor x_i \rfloor$, for $i = 1, \ldots, n$, where $\lfloor \xi \rfloor$ denotes the largest integer $\leq \xi$. Clearly, $0 \leq p_i < 1$, $\forall i$. Moreover, $\mathbf{x}' = \sum_{i=1}^{n} \lfloor x_i \rfloor \mathbf{b}_i$, and therefore $\mathbf{x}'' = \mathbf{x} - \mathbf{x}' = \sum_{i=1}^{n} p_i\mathbf{b}_i$ are points of Λ. Now by the choice of $\mathbf{b}_n$, $p_n = 0$. By the choice of $\mathbf{b}_{n-1}$, this implies that $p_{n-1} = 0$, etc.. Thus, the numbers x_i are all integers. This proves that the vectors $\mathbf{b}_1, \cdots, \mathbf{b}_n$ form a basis for Λ. □

Lemma 4.1 also gives an algorithm for finding a basis which corresponds to a given trellis coordinate system. Note that in general, the converse of Lemma 4.1 is not correct, i.e., there exist lattices $\Lambda \in \mathcal{L}$ with a basis matrix B such that the construction of Lemma 4.1 (based on B) does not result in a finite trellis for Λ. For an example, see Example 2.5.

However, for the important category of rational lattices, the following lemma proves that the converse of Lemma 4.1 holds. Note that lattices with rational bases

are special cases of rational lattices.

Lemma 4.2 *Let Λ be an n-D rational lattice. Then based on the construction of Lemma 4.1 for the trellis coordinate system, any basis $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ of Λ results in a finite trellis for Λ.*

Proof: Using (2.5) and (2.6), it can be seen that for any basis $B = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ of a rational lattice Λ, the G-S coefficients $\mu_{i,j}$ are rational for all values of i and j. This implies that the inverse G-S coefficient matrix $[\mu_{i,j}]^{-1}$ in $\hat{B} = [\mu_{i,j}]^{-1}B$ is rational too, which in turn means that for any G-S vector $\hat{\mathbf{b}}_i$, there exists a rational number α_i such that $\alpha_i\hat{\mathbf{b}}_i \in \Lambda$ (the smallest value for α_i is given in Proposition 4.2). Using this, we conclude that Λ has an n-D orthogonal sublattice with its basis along the G-S vectors of B ($\dim(\Lambda_{W_i}) = 1$, $\forall i$), which completes the proof. □

The combination of Lemmas 4.1 and 4.2 implies that for rational lattices the problems of "finding a proper trellis coordinate system" and "finding a proper basis" are equivalent. Note that this equivalence is not one-to-one, i.e., different bases can result in the same coordinate system. Based on the above construction, it is also clear that $N(\Lambda)$ along with the other trellis complexity measures, like $\mathcal{S}(\Lambda)$, $\mathcal{E}(\Lambda)$, and $\mathcal{G}(\Lambda)$, depend on the selected basis for Λ. Thus we sometimes use the notations $N(\Lambda, B)$, $\mathcal{S}(\Lambda, B)$, $\mathcal{E}(\Lambda, B)$, and $\mathcal{G}(\Lambda, B)$ to denote them.

In the following, starting from a basis $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of a lattice $\Lambda \in \mathcal{L}$, we explain in more detail the construction and analysis of the trellis diagram of Λ in the trellis coordinate system $\{W_i\}_{i=1}^n = \{span(\hat{\mathbf{b}}_i)\}_{i=1}^n$. Specifically, we suggest algorithms for finding state spaces, label groups, and the number of distinct paths in the trellis. These algorithms can be easily implemented on a computer for the case of lattices with rational bases. For a general real basis (non-rational), one can

use an approximate rational basis. Note that this is what really happens when we represent a non-rational number on a digital computer. Throughout our discussions, we assume that the necessary and sufficient condition for Λ to have a finite trellis constructed based on B is satisfied, that is, Λ has an n-D orthogonal sublattice Λ' with its basis along the G-S vectors of B.

In [77], ar. algorithm for constructing the trellis diagrams of group codes over finite Abelian groups is given. In the particular case of lattices, this algorithm starts from a given basis matrix of a full-dimensional lattice Λ, and constructs the trellis of Λ in a trellis coordinate system which is the same as the standard coordinate system. This can be considered as a special case of the more general construction presented here. Our approach to the problem is also different from the approach of [77].

As a tool in the rest of this thesis, the *Hermite normal form* (HNF) of a lattice turns out to be very useful.

Definition 4.1 *We call an $n \times n$ rational matrix H, a HNF of an n-D lattice Λ if it is a basis matrix of Λ with the following properties*[1]*:*

i. *H is lower triangular, i.e., $h_{i,j} = 0$, for $i \leq j-1$, $j = 2, \ldots, n$,*

ii. *$h_{i,i} > 0$, for $i = 1, \ldots, n$, and*

iii. *$h_{i,j} \leq 0$ and $|h_{i,j}| < h_{j,j}$, for $i > j$, $j = 1, \ldots, n-1$.*

[1]This definition is slightly different from the standard definition given in textbooks like [62], and [67]. In fact, we have reversed the order of basis vectors to have the G-S vectors along the coordinate vectors. For the sake of simplicity, we have also reversed the order of coordinate vectors. By this selection, the first G-S vector $\hat{\mathbf{b}}_1$ is along the first coordinate vector $\mathbf{u}_1$, $\hat{\mathbf{b}}_2$ is along $\mathbf{u}_2$, and so on.

From the above definition, it is easy to see that $\|\hat{\mathbf{b}}_i\| = h_{i,i}$, $\forall i$, and thus

$$\det(\Lambda) = \prod_{i=1}^{n} h_{i,i} \,. \tag{4.1}$$

It is known that the HNF of a lattice is unique [67]. However in general, different versions of a lattice have different HNF's, e.g., if H is the HNF of a lattice Λ then $c\Lambda (c > 0)$ has cH as its HNF. Starting from an arbitrary $n \times n$ rational basis of Λ, or more generally, an $m \times n$ $(m > n)$ rational matrix of full column rank with Λ as the integer span of its rows, one can always derive H by a series of elementary (unimodular) row operations in polynomial time [62], [67]. The importance of the HNF of a lattice in this work is that its G-S vectors are in the same directions as the coordinate vectors. This implies that, for our applications, the basis does not need to have the condition **iii**. Removing this condition, however, rules out the uniqueness of the HNF.

We also need the following fundamental result.

Lemma 4.3 *For the rational numbers* $p_1/q_1, \ldots, p_k/q_k$, $p_i, q_i \in \mathbb{Z}, q_i \neq 0, \forall i$, *let* $M = lcm(q_1, \ldots, q_k)$. *Then*

$$\zeta = \frac{M}{gcd(Mp_1/q_1, \ldots, Mp_k/q_k)}$$

is the smallest positive number such that $\zeta p_i/q_i \in \mathbb{Z}, \forall i$.

Proof: Without loss of generality, we assume that $p_i, q_i > 0$, for all i. Let ρ be the smallest positive multiplier which results in a vector of integer products $\mathbf{m} = (m_1, \ldots, m_k)$. Assume that $\rho < \zeta$. Also let $\mathbf{n} = (n_1, \ldots, n_k)$ denote the vector of integers obtained by multiplying the rational numbers by ζ. Clearly, $m_i < n_i, \forall i$, and $n_1/m_1 = \cdots = n_k/m_k \stackrel{\Delta}{=} c$. We now claim that $c \in \mathbb{Z}$. Otherwise, consider the

integer vector of the remainders $\mathbf{r} = (r_1, \ldots, r_k)$, which is in the same direction as $\mathbf{m}$ and $\mathbf{n}$, but has a shorter length. This contradicts the definition of ρ.

The integer $c > 1$ is thus a common factor of $n_1, \ldots, n_k$, which is in contradiction with the definition of $\mathbf{n}$. Therefore, $\zeta = \rho$,[2]. □

Corollary 4.1 *For the rational numbers $p_1/q_1, \ldots, p_k/q_k$, $p_i, q_i \in \mathbb{Z}, \forall i$, let p_i and q_i be relatively prime for all i. Also let $M = lcm(q_1, \ldots, q_k)$. Then*

$$\zeta = \frac{M}{gcd(p_1, \ldots, p_k)}$$

is the smallest positive number such that $\zeta p_i/q_i \in \mathbb{Z}, \forall i$.

Proof: The integer numbers $M/q_1, \ldots, M/q_k$, are relatively prime. It is also easy to see that the numbers M/q_i, and $p_j, j = 1, \ldots, k, j \neq i$, are relatively prime for every i in $\{1, \ldots, k\}$. We thus have $\gcd(Mp_1/q_1, \ldots, Mp_k/q_k) = \gcd(p_1, \ldots, p_k)$. This combined with Lemma 4.3 completes the proof. □

In the following, we first describe the lattices $\Lambda_{W_i}, \Lambda_i, P_{W_i}(\Lambda)$, and $P_i(\Lambda)$, as defined in Section 2.2. Let α_i be the smallest positive number such that $\alpha_i \hat{\mathbf{b}}_i \in \Lambda$. Based on the construction given in Lemma 4.1, $\Lambda_{W_i} = \alpha_i \|\hat{\mathbf{b}}_i\| \mathbb{Z}$, $1 \leq i \leq n$. It is also easy to see that $\Lambda_0 = \{\mathbf{0}\}$, and $\Lambda_i = L(\mathbf{b}_1, \cdots, \mathbf{b}_i)$, $1 \leq i \leq n$. Now let $\mathbf{b} = \beta_1 \mathbf{b}_1 + \cdots + \beta_n \mathbf{b}_n$, $\beta_j \in \mathbb{Z}$, $\forall j$, be an arbitrary point of Λ. Then $P_{W_i}(\mathbf{b}) = (\beta_i + \beta_{i+1}\mu_{i+1,i} + \cdots + \beta_n \mu_{n,i})\hat{\mathbf{b}}_i$, where $\mu_{i,j}$ is the element in row i and column j of the G-S coefficient matrix. Suppose that the minimum absolute value of $\beta_i + \beta_{i+1}\mu_{i+1,i} + \cdots + \beta_n \mu_{n,i}$ over all lattice vectors $\mathbf{b}$ is denoted by η_i.

[2] We first proved the Lemma for the case where the numerator and denominator of each rational number are relatively prime. We then conjectured that the same result is also valid in general, where the numerators and denominators are not necessarily relatively prime. This proof is due to A. Kotlov in response to our conjecture.

It can then be easily seen that $P_{W_i}(\Lambda) = \eta_i \|\hat{\mathbf{b}}_i\| \mathbb{Z}$. We also note that from the definition, $P_i(\Lambda) = L(\mathbf{b}_1, \ldots, \mathbf{b}_i, P_i(\mathbf{b}_{i+1}), \ldots, P_i(\mathbf{b}_n))$, where $L(\cdots)$ denotes the integer linear combinations of the vectors. For the computation of $N(\Lambda, B)$, the following proposition suggests an algorithm.

Proposition 4.1 *Let $\Lambda \in \mathcal{L}_n$ have a trellis constructed based on the basis $B = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$. Let $\{\hat{\mathbf{b}_1}, \cdots, \hat{\mathbf{b}_n}\}$ be the corresponding set of G-S vectors. Suppose that α_i is defined as above. Then $N(\Lambda, B) = \prod_{i=1}^{n} \alpha_i$.*

Proof: Following the previously used notations, we have $\Lambda_{W_i} = \alpha_i \|\hat{\mathbf{b}}_i\| \mathbb{Z}$, $1 \leq i \leq n$. The corresponding orthogonal sublattice Λ' is therefore in the form of $\alpha_1 \|\hat{\mathbf{b}}_1\| \mathbb{Z} \oplus \cdots \oplus \alpha_n \|\hat{\mathbf{b}}_n\| \mathbb{Z}$, and has a determinant equal to $\det(\Lambda') = \prod_{i=1}^{n} \alpha_i \|\hat{\mathbf{b}}_i\|$. Now combining this with (2.8) and (2.12) completes the proof. □

To obtain the numbers α_i, one can use the relation $\hat{B} = [\mu_{i,j}]^{-1} B$. The matrix $[\mu_{i,j}]^{-1}$ is a lower triangular matrix with the elements of the main diagonal equal to one. For rational lattices, $[\mu_{i,j}]^{-1}$ is rational, and the following proposition follows immediately from Lemma 4.3.

Proposition 4.2 *For $[\mu_{i,j}]^{-1}$ rational, suppose that $\theta_1, \cdots, \theta_j, 1$ $(j < i)$, denote its nonzero elements in row i. Let M be the lcm of the denominators of these elements. Then*

$$\alpha_i = \frac{M}{gcd(M\theta_1, \cdots, M\theta_j, M)}. \tag{4.2}$$

In the case of a rational G-S coefficient matrix $[\mu_{i,j}]$, to determine the values of η_i, $1 \leq i \leq n$, in the description of $P_{W_i}(\Lambda)$, we first prove the following lemma.

Lemma 4.4 *Let* $f(\mathbf{x}) = a_1x_1 + \cdots + a_nx_n$ *with* $\mathbf{a}, \mathbf{x} \in \mathbb{Z}^n$, $\mathbf{a} \neq \mathbf{0}$. *Then the minimum of* $|f(\mathbf{x})|$ *over all nonzero* $\mathbf{x} \in \mathbb{Z}^n$ *is equal to* $gcd(a_1, \ldots, a_n)$.

Proof: Using the integer version of Farkas' lemma [62, p. 191], we can see that there does not exist any integer solution $\mathbf{x}$ for the equation $f(\mathbf{x}) = \pm c$, where $c \in \mathbb{Z}$, and $0 < c < \gcd(a_1, \ldots, a_n)$. The same lemma also implies that there is a solution $\mathbf{x} \in \mathbb{Z}^n$ for the equation $f(\mathbf{x}) = \gcd(a_1, \ldots, a_n)$. □

Proposition 4.3 *We have*

$$\eta_i = \frac{gcd(M, M\mu_{i+1,i}, \ldots, M\mu_{n,i})}{M}, \tag{4.3}$$

where M *is either the lcm of the denominators of nonzero elements among the G-S coefficients* $\mu_{i+1,i}, \ldots, \mu_{n,i}$, *if at least one of them is nonzero, or an arbitrary positive integer, otherwise.*

Proof: The proof follows from the definition of η_i and Lemma 4.4. □

Finally, to easily work with the lattice $P_i(\Lambda)$, we also need to find a basis for this lattice. For $[\mu_{i,j}]$ rational, this can be conveniently done by finding the HNF of $P_i(\Lambda)$ in the G-S coordinate system.

After finding cross section lattices Λ_{W_i}, Λ_i, and projection lattices $P_{W_i}(\Lambda)$, $P_i(\Lambda)$, one can easily obtain the state spaces and the label groups for the trellis of Λ. To construct the trellis, one also needs to find out about the connections between states in successive levels of the trellis, and their labelings. This task can be performed by checking some points of the lattice and tracking down their corresponding paths through the trellis, until all the paths are covered. The following example explains the construction of trellis diagrams of lattices, starting from their bases. It also shows how selecting different bases for a lattice can affect the trellis complexity.

Example 4.1 *The following two basis matrices generate the checkerboard lattice* D_4*:*

$$B_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 \end{pmatrix} \quad , \quad B_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

In this version, $\lambda = \sqrt{2}$*, and* $det(D_4) = 2$*. The corresponding G-S coefficient matrices and their inverses are:*

$$[\mu_{i,j}]_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1/2 & 1 & 0 & 0 \\ 1 & 2/3 & 1 & 0 \\ 1 & 2/3 & -1/2 & 1 \end{pmatrix} \quad , \quad [\mu_{i,j}]_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1 \end{pmatrix}.$$

$$[\mu_{i,j}]_1^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1/2 & 1 & 0 & 0 \\ -2/3 & -2/3 & 1 & 0 \\ -1 & -1 & 1/2 & 1 \end{pmatrix} \quad , \quad [\mu_{i,j}]_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 1/2 & -1/2 & -1/2 & 1 \end{pmatrix}.$$

Using Propositions 4.2 *and* 4.3*, it is easy to see that* $\boldsymbol{\alpha}_1 = (1, 2, 3, 2)$*,* $\boldsymbol{\eta}_1 = (1/2, 1/3, 1/2, 1)$*,* $\boldsymbol{\alpha}_2 = (1, 1, 1, 2)$*, and* $\boldsymbol{\eta}_2 = (1/2, 1/2, 1/2, 1)$*. Proposition* 4.1 *then results in* $N(D_4, B_1) = 12$*, and* $N(D_4, B_2) = 2$*. We therefore expect the trellis constructed based on* B_2 *to be less complex than the one constructed based on* B_1*.*

Using quantities $\boldsymbol{\alpha}_1, \boldsymbol{\eta}_1, \boldsymbol{\alpha}_2,$ *and* $\boldsymbol{\eta}_2$ *in* $g_i = \alpha_i/\eta_i$*, for* $1 \leq i \leq 4$*, we have* $\mathbf{g}_1 = (2, 6, 6, 2)$ *and* $\mathbf{g}_2 = (2, 2, 2, 2)$*. Also for the sizes of state spaces, using* $s_i = det(\Lambda_i)/det(P_i(\Lambda))$*,* $1 \leq i \leq 4$*, we obtain* $\mathbf{s}_1 = (1, 2, 3, 2, 1)$ *and* $\mathbf{s}_2 = (1, 2, 2, 2, 1)$*. The corresponding trellis diagrams of* D_4 *are given in Figure* 4.1*. Below each trellis*

section, the corresponding label group is given. If the label group of the trellis section i is isomorphic to Z_m, then the edges of this section are correspondingly labeled with the elements of Z_m. It can be seen that in agreement with our preliminary expectation based on the values of $N(D_4, B_1)$ and $N(D_4, B_2)$, the complexity of trellis (a) *constructed based on B_1 is much more than the complexity of trellis* (b) *built based on B_2. Also note that B_1 and B_2 differ only in the order of basis vectors.*

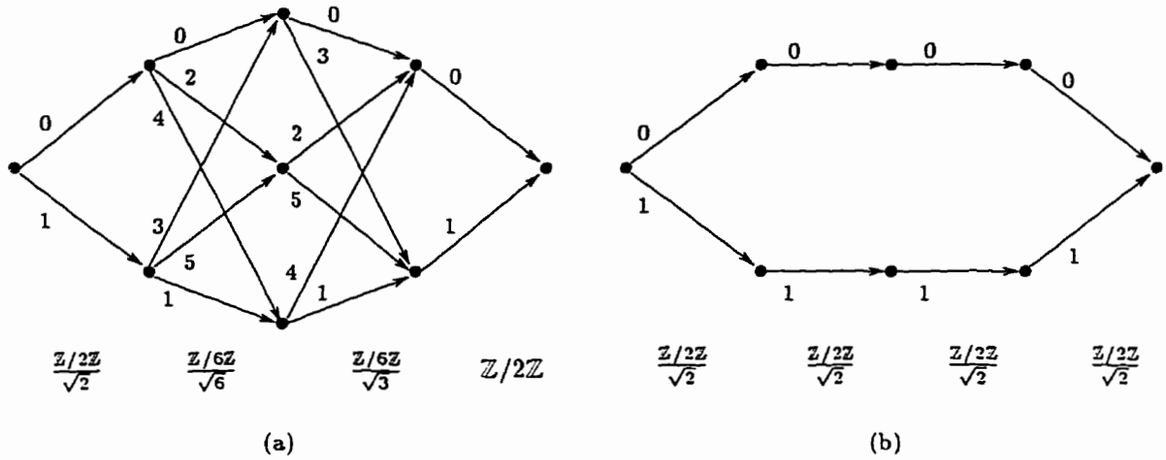

Figure 4.1: Two trellis diagrams of D_4.

Remark: In [33], Forney has also given a trellis with two paths for the version RD_4 of D_4. In Example 4.1, however, we have been able to find a two-path trellis without any need for searching among the different versions of D_4. The following lemma shows that this can be generalized.

Lemma 4.5 *Trellis complexity is a geometrical invariant of a lattice.*

Proof: Before giving a proof, and to resolve any ambiguity, we would like to explain more about the lemma. It states that if we are able to find a trellis for

a version of a lattice, we will also be able to construct the same trellis (up to isomorphism) for any other version of the lattice.

Let $\Lambda_1 \in \mathcal{L}$ have a trellis T_1 constructed based on a basis B_1. Suppose that Λ_2 is a version of Λ_1. It has therefore a form of $\Lambda_2 = c\Lambda_1 O$, where c is a nonzero real number, and O is an orthogonal matrix. It is easy to see that the trellis made based on the basis $B_2 = cB_1O$ for Λ_2 is the same as T_1. □

Remark: We believe that the fundamental result of Lemma 4.5 has been more or less noticed by the researchers in the area. However, because of its importance, we found it useful to state it explicitly.

Example 4.1 shows that the number of distinct paths in different trellis diagrams of a lattice could be very different. In fact, the following simple example shows that for a general basis B of a general lattice Λ, one cannot find a finite upper bound on $N(\Lambda, B)$ in terms of dimension and/or coding gain of the lattice,[3].

Example 4.2 *Consider the integer lattice $\mathbb{Z}^2$. It is easy to see that the following matrix is a basis matrix for $\mathbb{Z}^2$:*

$$B = \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix},$$

where $p \in \mathbb{Z}$ is arbitrary. Then $W_1 = span((p,1))$, $W_2 = span((1,-p))$, and the corresponding orthogonal sublattice Λ' has a determinant of $det(\Lambda') = p^2 + 1$, which results in $N(\mathbb{Z}^2, B) = p^2 + 1$.

Note that in this example N can be easily upper bounded by a function of the input size.

[3]A similar example has been also given in [71].

In [71], it has been shown by some counter-examples that for a general rational lattice, one cannot find any basis such that the complexity of the corresponding trellis is upper bounded by just a function of dimension or coding gain. It is important to note that all the results in [71] are obtained based on having the input size tend to infinity. This fact motivates searching for upper bounds which are directly a function of the input size. Among other things in Section 4.3, we derive upper bounds on the trellis complexity of lattices with rational bases. All the counter-examples of [71] are covered under this category of lattices. The bounds depend on the input basis, the dimension, and the determinant of the lattice.

We continue in the following section by presenting some results on the relation between the trellis complexity of dual lattices.

4.2 Duality results

The following fundamental fact follows from the results of [33]. A proof is also given for the sake of completeness.

Lemma 4.6 *Let $\Lambda \in \mathcal{L}_n$. Then in any trellis coordinate system that Λ has a finite trellis, its dual Λ^* has a finite trellis too.*

Proof: Suppose that Λ has a finite trellis in the coordinate system $\{W_i\}_{i=1}^n$. Then $P_{W_i}(\Lambda)$, and therefore its dual in W_i, $P_{W_i}(\Lambda)^*$, are 1-D lattices for all values of i. From the definition of dual lattices, the inner product of every point of $P_{W_i}(\Lambda)^*$ with every point of $P_{W_i}(\Lambda)$ is an integer. This implies that the inner product of every point $\mathbf{x}$ of $P_{W_i}(\Lambda)^*$ with every point of Λ is also an integer, which concludes that $\mathbf{x} \in \Lambda^*$, and thus $P_{W_i}(\Lambda)^* \subseteq (\Lambda^*)_{W_i}$. This in turn results in the fact that $\dim((\Lambda^*)_{W_i}) = 1$, $\forall i$, which completes the proof. □

In [33], Forney has proved that in any trellis coordinate system, the number of states s_i in any level $i \in \{0, \ldots, n\}$ of the trellises of dual lattices Λ and Λ^* are the same. In the following, we prove a similar result for the sizes of the label groups.

Theorem 4.1 *Let $\Lambda \in \mathcal{L}_n$. Then in any trellis coordinate system, the sizes of the label groups of dual lattices Λ and Λ^* are the same, i.e., $g_i(\Lambda) = g_i(\Lambda^*)$, for $i = 1, \ldots, n$.*

Proof: Let Λ and Λ^* have finite trellises in the given trellis coordinate system. Then for every $i \in \{1, \ldots, n\}$, we have

$$g_i(\Lambda) = |P_{W_i}(\Lambda)/\Lambda_{W_i}| = \frac{\det(\Lambda_{W_i})}{\det(P_{W_i}(\Lambda))} = \frac{\det((\Lambda^*)_{W_i})}{\det(P_{W_i}(\Lambda^*))} = g_i(\Lambda^*) \,.$$

In the second last step, we have used the facts that in $span(W_i)$, $(\Lambda_{W_i})^* = P_{W_i}(\Lambda^*)$, and $(P_{W_i}(\Lambda))^* = (\Lambda^*)_{W_i}$, [33], and also (2.10). □

Despite the nice relations between the state complexity profiles (and label complexity profiles) of dual lattices, it appears that there does not exist such a simple relation either between the number of distinct paths or between the number of edges in the trellises of dual lattices in the same coordinate system. However, we are able to relate these parameters as follows. For $N(\Lambda)$ and $N(\Lambda^*)$, we first prove the following theorem.

Theorem 4.2 *For $\Lambda \in \mathcal{L}_n$, in any trellis coordinate system that Λ and Λ^* have finite trellises, we have*

$$N(\Lambda)N(\Lambda^*) = \prod_{i=1}^{n} g_i \,, \tag{4.4}$$

where g_i is the size of the label group in trellis section i.

Proof: Let Λ' and Λ'' denote the corresponding orthogonal sublattices of Λ and Λ^* in the given coordinate system, respectively. We then have $\det(\Lambda'') = \prod_{i=1}^{n} \det((\Lambda^*)_{W_i})$. Combining this with the facts that $g_i = \det((\Lambda^*)_{W_i})/\det(P_{W_i}(\Lambda^*))$, and $(\Lambda_{W_i})^* = P_{W_i}(\Lambda^*)$, we obtain $\det(\Lambda'') = \prod_{i=1}^{n}(g_i/\det(\Lambda_{W_i}))$. This in turn results in $\det(\Lambda'') = (\prod_{i=1}^{n} g_i)/\det(\Lambda')$. We then have

$$N(\Lambda^*) = \frac{\det(\Lambda'')}{\det(\Lambda^*)} = (\prod_{i=1}^{n} g_i)\frac{\det(\Lambda)}{\det(\Lambda')} = \frac{\prod_{i=1}^{n} g_i}{N(\Lambda)} ,$$

which completes the proof. □

The following corollary is an immediate consequence of Theorem 4.2.

Corollary 4.2 *Let Λ be a self-dual lattice. Then in any coordinate system that Λ has a finite trellis, we have $N(\Lambda) = (\prod_{i=1}^{n} g_i)^{1/2}$.*

Corollary 4.2 also implies that in any coordinate system that a self-dual lattice has a finite trellis, the corresponding quantity $\prod_{i=1}^{n} g_i$ has to be a complete square. For an example, see the trellis of E_8 in Figure 5.1.

Putting the fact that for every $i = 1, \ldots, n$, $g_i \leq N(\Lambda)$, together with Theorem 4.2, we get the following corollary.

Corollary 4.3 *For $\Lambda \in \mathcal{L}_n$, in any coordinate system that Λ and Λ^* have finite trellises, we have $N(\Lambda^*) \leq N(\Lambda)^{n-1}$.*

As we will see later in Proposition 4.4, in many cases the above bound can be improved for integral lattices. We first prove the following lemma.

Lemma 4.7 *Let Λ be an integral lattice in $\mathbb{R}^m$, and let V be an n-D subspace of $\mathbb{R}^m$ such that the lattice $\Lambda_V \triangleq \Lambda \cap V$ has dimension n. Then the projection lattice $P_V(\Lambda)$ is a sublattice of the dual lattice $(\Lambda_V)^*$ in V.*

Proof: For an integral lattice Λ, we have $\Lambda \subseteq \Lambda^*$, and therefore $P_V(\Lambda) \subseteq P_V(\Lambda^*)$. Combining this with $P_V(\Lambda^*) = (\Lambda_V)^*$, [33], completes the proof. □

Corollary 4.4 *Let Λ be a self-dual lattice in $\mathbb{R}^m$, and let V be an n-D subspace of $\mathbb{R}^m$ such that the lattice Λ_V has dimension n. Then $P_V(\Lambda) = (\Lambda_V)^*$.*

Proposition 4.4 *Let $\Lambda \in \mathcal{L}$ be an integral lattice. Then in any coordinate system that Λ and Λ^* have finite trellises, we have $N(\Lambda^*) \leq N(\Lambda) det(\Lambda)^2$.*

Proof: Using Lemma 4.7, we have $\det(P_{W_i}(\Lambda)) \geq \det((\Lambda_{W_i})^*)$, for $i = 1, \ldots, n$. Combining this with $g_i = \det(\Lambda_{W_i})/\det(P_{W_i}(\Lambda))$, $i = 1, \ldots, n$, we obtain $g_i \leq \det(\Lambda_{W_i})/\det((\Lambda_{W_i})^*) = \det(\Lambda_{W_i})^2$, $i = 1, \ldots, n$. Applying these inequalities to the result of Theorem 4.2, and using the fact that $\prod_{i=1}^n \det(\Lambda_{W_i})$ is equal to the determinant of the corresponding orthogonal sublattice Λ' of Λ, lead us to $N(\Lambda)N(\Lambda^*) \leq \det(\Lambda')^2$. The proof then follows by combining this inequality with (2.12). □

Note that for a self-dual lattice, $g_i = \det(\Lambda_{W_i})^2$, $i = 1, \ldots, n$, and the inequality of Proposition 4.4 is satisfied with equality.

In the following, we give an upper bound on $N(\Lambda^*)$ in terms of $\det(\Lambda)$, for Λ an integer lattice.

Proposition 4.5 *For Λ an integer lattice, we have $N(\Lambda^*, H) \leq det(\Lambda)$, where H is the HNF of Λ^*.*

Proof: Since Λ is a sublattice of $\mathbb{Z}^n$, the inner product of any vector of Λ with any vector of $\mathbb{Z}^n$ is integer. This means that $\mathbb{Z}^n \subseteq \Lambda^*$. Now by selecting H as the basis for Λ^*, the spans of G-S vectors $(\{W_i\}_{i=1}^n)$ will be along the vectors of

the standard coordinate system ($\{\mathbf{u}_i\}_{i=1}^n$). This implies that $\det(\Lambda') \leq \det(\mathbb{Z}^n) = 1$, where Λ' is the corresponding orthogonal sublattice of Λ^*. We therefore have $N(\Lambda^*, H) = \det(\Lambda')/\det(\Lambda^*) \leq 1/\det(\Lambda^*) = \det(\Lambda)$, and the proof is complete. □

Note that since $N(\Lambda) \geq 1$, and for an integer lattice, $\det(\Lambda) \geq 1$, the bound in Proposition 4.5 is stronger than the one given in Proposition 4.4. In fact, as we will see in Section 5.4, the bound of Proposition 4.5 is achieved for all D_n^* lattices.

We finish this section by deriving an inequality relating $\mathcal{E}(\Lambda)$ and $\mathcal{E}(\Lambda^*)$ in the same trellis coordinate system.

Theorem 4.3 *For $\Lambda \in \mathcal{L}_n$, in any coordinate system that Λ and Λ^* have finite trellises, we have $\mathcal{E}(\Lambda^*) \leq n\mathcal{E}(\Lambda)^2$.*

Proof: Let for the lattice Λ^*, the trellis parameters $s_i', i = 0, \ldots, n$, and $g_i', r_i', i = 1, \ldots, n$, be defined as in Section 2.4. Then by the definition of $\mathcal{E}$, we have

$$\mathcal{E}(\Lambda^*) = \frac{\sum_{i=1}^n r_i' s_{i-1}'}{n} \leq \frac{\sum_{i=1}^n g_i' s_{i-1}'}{n} \leq \frac{(\sum_{i=1}^n g_i')(\sum_{i=1}^n s_{i-1}')}{n} = n\mathcal{G}(\Lambda^*)\mathcal{S}(\Lambda^*)\,,$$

where we have used $r_i' \leq g_i'$, $i = 1, \ldots, n$, for the second last inequality, and the definition of $\mathcal{G}$ and $\mathcal{S}$ for the last step. It then follows from the identity of state and label complexity profiles of Λ and Λ^* that $\mathcal{E}(\Lambda^*) \leq n\mathcal{G}(\Lambda)\mathcal{S}(\Lambda)$. Combining this with the easily derived inequalities of $\mathcal{G} \leq \mathcal{E}$ and $\mathcal{S} \leq \mathcal{E}$ completes the proof. □

4.3 Bounds on trellis complexity

In this section, we present lower and upper bounds on the trellis complexity of lattices.

4.3.1 Lower bounds on complexity

In the following, a lower bound on $N(\Lambda, B)$ in terms of the coding gain and the dimension of Λ is given. We show that the bound, which was derived in [69], is quite tight, and is achieved by minimal trellises of many important lattices.

Theorem 4.4 *Let a lattice $\Lambda \in \mathcal{L}_n$ with coding gain γ have a finite trellis constructed based on a basis B. Then the number of distinct paths in this trellis, $N(\Lambda, B)$, satisfies*

$$N(\Lambda, B) \geq \gamma^{n/2} . \tag{4.5}$$

The inequality is satisfied with equality iff Λ has n mutually orthogonal vectors with their length equal to $\lambda(\Lambda)$ and along the G-S vectors of B.

Proof: Suppose that Λ' is the corresponding orthogonal sub-lattice of Λ. Also, let $\{\mathbf{b}'_1, \ldots, \mathbf{b}'_n\}$ be a basis of Λ' with mutually orthogonal vectors. It is then easy to see that

$$\det(\Lambda') = \prod_{i=1}^{n} \|\mathbf{b}'_i\| . \tag{4.6}$$

Inequality (4.5) then follows by combining (4.6) with (2.12), and using the fact that $\|\mathbf{b}'_i\| \geq \lambda(\Lambda)$, for $i = 1, \ldots, n$, and finally applying (2.2). □

Example 4.1 (Cont.) *It is easy to see that $N(D_4, B_2)$ satisfies the inequality* (4.5) *with equality. Therefore B_2 is the best basis for D_4 in the sense that it minimizes $N(D_4, B)$, and the trellis of Figure* 4.1(*b*) *is a minimal trellis for D_4.*

Example 4.3 *Using Propositions* 4.1 *and* 4.2, *it can be seen that the "trellis-oriented" basis matrix for the Leech lattice Λ_{24}, given in* [33], *minimizes $N(\Lambda_{24}, B)$ with 2^{24} distinct paths in the trellis.*

The following corollary comes from the fact that N is integer.

Corollary 4.5 *Let a lattice $\Lambda \in \mathcal{L}_n$ with coding gain γ have a finite trellis constructed based on a basis B. Then*

$$N(\Lambda, B) \geq \lceil \gamma^{n/2} \rceil , \tag{4.7}$$

where $\lceil \xi \rceil$ denotes the smallest integer $\geq \xi$.

As we will see later in Chapter 5, the fact that N is an integer number, or in other words $\det(\Lambda)$ divides $\det(\Lambda')$, can more effectively be used if it is combined with the information regarding the structure of the lattice (the arrangement of lattice points). Note that although the condition of vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ being mutually orthogonal is a stronger condition than $\det(\Lambda)$ dividing $\det(\Lambda')$, in many situations it suffices to just use the latter condition.

The following corollary shows that $N(\Lambda, B)$ has at least an exponential growth with $\gamma(\Lambda)$, no matter what the selected basis for Λ is.

Corollary 4.6 *Let $\Lambda \in \mathcal{L}_n$ have a coding gain $\gamma \geq 1$, and a finite trellis constructed based on a basis B. Then*

$$N(\Lambda, B) \geq \gamma^{\gamma/2} . \tag{4.8}$$

Proof: Applying the inequality $n \geq \gamma_n \geq \gamma$ to (4.5) proves the corollary. □

Combining Theorem 4.4 with the lower bound results of Lemmas 2.1 and 2.2, we obtain the following corollary.

Corollary 4.7 *Let $\Lambda \in \mathcal{L}_n$ have a coding gain γ. Then for any finite trellis of Λ, the corresponding parameters $\mathcal{S}(\Lambda), \mathcal{E}(\Lambda), \mathcal{G}(\Lambda)$, and C satisfy*

$$\mathcal{S}(\Lambda) \geq \gamma^{\frac{1}{2}}\,, \tag{4.9}$$

$$\mathcal{E}(\Lambda) \geq \gamma\,, \tag{4.10}$$

$$\mathcal{G}(\Lambda) \geq \gamma^{\frac{1}{2}}\,, \tag{4.11}$$

$$C \geq n\gamma\,. \tag{4.12}$$

Remark: Using the bounds given in (4.9)–(4.11), we can conclude that the trellis complexity functions $\tau_1(\gamma)$, $\tau_2(\gamma)$, and $\tau_3(\gamma)$, as defined in [69], satisfy the inequalities $\tau_1(\gamma) \geq \gamma^{1/2}$, $\tau_2(\gamma) \geq \gamma$, and $\tau_3(\gamma) \geq \gamma^{1/2}$. This is the same result as given in Theorem 3.4 of [69]. It has also been proved in [70] that for large values of γ, τ_1 and τ_2 grow at least exponentially.

Using more elaborate discussions, we are able to improve the lower bound results of this section for some particular lattices. This will be illustrated in Chapter 5.

4.3.2 Upper bounds on complexity

As we already observed in Lemma 4.5, the trellis complexity is a geometrical invariant of a lattice. It is therefore of interest to derive bounds on the trellis complexity which are functions of some other geometrical invariants of the lattice like coding gain. However, in the case of upper bounds and for a general lattice, we know that it is not possible to derive bounds which are just a function of γ or n. In the following, however, we are able to derive a wide range of upper bounds on different trellis complexity measures and for different categories of lattices. In particular,

for integral lattices, the derived bounds which are in terms of n, and the successive minima or the determinant of the lattice are much tighter than the similar bounds of [71].

Since the successive minima (including the minimum distance) and the determinant of a lattice change with scaling, it is reasonable to minimize them by proper scaling while keeping the integral property of the lattice. Combining the fact that a rational lattice always has an integral version with Lemma 4.5, one can extend the application of these upper bound results to rational lattices. We show that the trellis complexity of "any" rational lattice Λ constructed based on "any" basis of Λ can be upper bounded by a function of n and $\det(\Lambda)$. We are also able to improve the bounds for ESM-lattices.

Throughout this section, we give the corresponding bases for the derived upper bounds. All the bounds are thus of a constructive nature. Note that the upper bounds of [71] on the trellis complexity of integral lattices are just existence results.

We first start by the following proposition which can be conveniently used for the derivation of an upper bound on the trellis complexity of an arbitrary lattice given its basis matrix.

Proposition 4.6 *Let a lattice Λ have an $n \times n$ basis matrix B. Suppose that B can be converted to an integer matrix by multiplying column i with the real number x_i, $i = 1, \ldots, n$. Then we have*

$$(\prod_{\substack{i=1 \\ i \neq j}}^{n} x_i) det(\Lambda) \mathbf{u}_j \in \Lambda \,, \tag{4.13}$$

where $\mathbf{u}_j$ is the j-th coordinate vector.

Proof: Let B' denote the matrix obtained from B by the above procedure, and let Δ and Δ' denote the determinant of B and B', respectively. Since B' is integer,

$F \triangleq \Delta'(B')^{-1}$ is an integer matrix too. It then follows that the j-th row of F, $F_j = \Delta' \mathbf{u}_j (B')^{-1}$ is an integer vector. We therefore have $F_j B' = \Delta' \mathbf{u}_j \in L(B')$. It is easy to see that $\mathbf{b} = (b_1, \ldots, b_n) \in L(B')$ iff $(b_1/x_1, \ldots, b_n/x_n) \in \Lambda$. We then have $(\Delta'/x_j)\mathbf{u}_j \in \Lambda$. This combined with the facts that $\Delta' = x_1 \cdots x_n \Delta$, and $\det(\Lambda) = |\Delta|$, completes the proof. □

Using Proposition 4.6, it is easy to see that selecting the trellis coordinate system $\{W_i\}_{i=1}^n$ to be the same as the standard coordinate system, determined by the unit vectors $\{\mathbf{u}_i\}_{i=1}^n$, we have

$$N(\Lambda) \leq (\prod_{j=1}^{n} \prod_{\substack{i=1 \\ i \neq j}}^{n} x_i) \det(\Lambda)^{n-1} . \tag{4.14}$$

The following proposition could be specifically useful for integer lattices.

Proposition 4.7 *Let Λ be an n-D integer lattice, and let H be the HNF of Λ. Then we have*

$$N(\Lambda, H) \leq \prod_{i=1}^{n-1} h_{i,i}^{n-i} . \tag{4.15}$$

Proof: Let $\mathbf{h}_1, \ldots, \mathbf{h}_n$ denote the rows of H. Applying Proposition 4.6 to lattices $L(\mathbf{h}_1, \ldots, \mathbf{h}_j)$, with $x_1 = \cdots = x_j = 1$, and for $j = 1, \ldots, n$, results in $\mathbf{v}_j \triangleq (\prod_{i=1}^{j} h_{i,i})\mathbf{u}_j \in L(\mathbf{h}_1, \ldots, \mathbf{h}_j)$, and therefore $\mathbf{v}_j \in \Lambda$, for $j = 1, \ldots, n$. Now by choosing H as the basis matrix for Λ, the G-S vectors are along the coordinate vectors $\{\mathbf{u}_j\}_{j=1}^n$. This implies that for the corresponding orthogonal sublattice Λ', we have $\det(\Lambda') \leq \|\mathbf{v}_1\| \cdots \|\mathbf{v}_n\|$. This combined with (2.12) and (4.1) completes the proof. □

Using (4.1) combined with the fact that for an integer lattice $h_{i,i}$ is a positive integer for every value of i, we notice that each of the quantities $\|\mathbf{v}_j\|$, $j = 1, \ldots, n$,

in the above proof is upper bounded by $\det(\Lambda)$. Thus we obtain the following simpler upper bound on the number of distinct paths in the trellis of an integer lattice.

Theorem 4.5 *For Λ an n-D integer lattice, we have*

$$N(\Lambda, H) \leq det(\Lambda)^{n-1}\,, \tag{4.16}$$

where H is the HNF of Λ.

The result of Theorem 4.5 can also be obtained from (4.14), or by combining Corollary 4.3 with Proposition 4.5.

Example 4.2 (Cont.) *Using Theorem 4.5, we have $N(\mathbb{Z}^2, H) \leq det(\mathbb{Z}^2)$, which results in $N(\mathbb{Z}^2, H) = 1$, where $H = I_2$ is the HNF of $\mathbb{Z}^2$. We also note that based on Theorem 4.5, $N(\mathbb{Z}^n, I_n) = 1$, $\forall n$, which corresponds to the minimal trellis of $\mathbb{Z}^n$.*

As we will see later in Section 5.3, the bound of (4.16) is also achieved for all D_n lattices.

As can be seen in the following theorem, for Λ an integer lattice, it is possible to derive upper bounds on $\mathcal{S}(\Lambda)$, $\mathcal{E}(\Lambda)$, and $\mathcal{G}(\Lambda)$ which are (in many cases) tighter than the ones obtained by combining (2.16)–(2.18) with (4.16). (Note that for an integer lattice, $\det(\Lambda) \geq 1$).

Theorem 4.6 *For Λ an n-D integer lattice, we have*

$$\mathcal{S}(\Lambda, H) \leq det(\Lambda)\,, \tag{4.17}$$

$$\mathcal{E}(\Lambda, H) \leq n\,det(\Lambda)^2\,, \tag{4.18}$$

$$\mathcal{G}(\Lambda, H) \leq det(\Lambda)\,, \tag{4.19}$$

where H is the HNF of Λ.

Proof: Combining the upper bound of (2.16) with the result of Proposition 4.5, we have $\mathcal{S}(\Lambda^*, H') \leq \det(\Lambda)$, where H' is the HNF of Λ^*. Now if H is the HNF of Λ, then H and H' introduce the same trellis coordinate system, and therefore according to the result of Forney in [33], we obtain $\mathcal{S}(\Lambda^*, H') = \mathcal{S}(\Lambda, H)$. This completes the proof of inequality (4.17).

In a similar way, inequalities (4.18) and (4.19) follow by combining (2.17) and (2.18) with Proposition 4.5 and applying Theorems 4.3 and 4.1, respectively. □

The bounds of Theorem 4.6 are tight. In fact, inequalities (4.17) and (4.19) are both satisfied with equality for $\mathbb{Z}^n$ and D_n lattices.

Remark: From the fact that $\max_i s_i(\Lambda, H) = \max_i s_i(\Lambda^*, H') \leq N(\Lambda^*, H')$, and Proposition 4.5, we can also obtain $\max_i s_i(\Lambda, H) \leq \det(\Lambda)$. Note that in [71], the only bound derived on the trellis complexity of integer lattices is $\min(\max_i s_i) \leq \det(\Lambda)$, where the minimum is taken over all the trellis diagrams of Λ.

In the following, using Theorems 4.5 and 4.6, we derive upper bounds on the trellis complexity of a full-dimensional lattice with a rational basis.

Theorem 4.7 *Let a lattice Λ have a rational $n \times n$ basis matrix B. Let M be the lcm of the denominators of nonzero elements in B, and let $\xi = M/gcd(Mb_{11}, \ldots, Mb_{nn})$. Then we have*

$$N(\Lambda, H) \leq \xi^{n(n-1)} det(\Lambda)^{n-1} ,$$

$$\mathcal{S}(\Lambda, H) \leq \xi^n det(\Lambda) ,$$

$$\mathcal{E}(\Lambda, H) \leq n\xi^{2n} det(\Lambda)^2 ,$$

$$\mathcal{G}(\Lambda, H) \leq \xi^n det(\Lambda) ,$$

where H is the HNF of Λ.

Proof: Since the proofs are similar, we only prove the first inequality. It is easy to see that $\xi B \in \mathbb{Z}^{n\times n}$ (note that based on Lemma 4.3, ξ is the smallest such a number), and therefore $\xi\Lambda$ is an integer lattice. It then follows from Theorem 4.5 that $N(\xi\Lambda, H') \leq \det(\xi\Lambda)^{n-1} = \xi^{n(n-1)}\det(\Lambda)^{n-1}$, where H' is the HNF of the lattice $\xi\Lambda$. At the last step, we have used $\det(\xi\Lambda) = \xi^n\det(\Lambda)$. The HNF of Λ, H. is equal to H'/ξ. This combined with Lemma 4.5 results in $N(\Lambda, H) = N(\xi\Lambda, H')$. Putting this together with the above inequality completes the proof. □

In Theorem 4.7, ξ depends directly on the elements of the basis matrix. Note that using (4.14), one usually obtains a tighter upper bound on N than the one given in Theorem 4.7. The following example illustrates an application of Theorem 4.7.

Example 4.4 *In [71], as a counter-example for existence of proper upper bounds on the trellis complexity of lattices, the authors consider a sequence of rational 2-D lattices Λ generated by*

$$B = \begin{pmatrix} 1 & 0 \\ p_1/p_2 & p_3/p_4 \end{pmatrix},$$

where p_1, p_2, p_3, and p_4 are distinct primes. They then show that by letting both p_2 and p_4 grow, the number of distinct paths in a minimal trellis of Λ increases without bound.

Now, applying Theorem 4.7 to this example, we have $\xi = p_2p_4$, and consequently $N(\Lambda, H) \leq p_2^2p_3p_4$. A tighter upper bound of the form $N(\Lambda, H) \leq p_2p_3$ can also be obtained using (4.14) with $x_1 = p_2$, and $x_2 = p_4$.

There are different ways of extending the results of Theorem 4.7 to lattices with rational bases which are not full-dimensional, or more generally to rational lattices. One way is to find the smallest scaling factor which transforms the rational lattice to an integral lattice (see Section 2.1), and then use the following upper bounds on

the trellis complexity of integral lattices. Another way is to notice that in the G-S coordinate system, multiplying column i of the basis B of an n-D rational lattice Λ by $\|\hat{\mathbf{b}}_i\|$, for $i = 1, \ldots, n$, results in a rational $n \times n$ matrix. This comes from the fact that for a rational lattice the G-S coefficient matrix and the square norm of the G-S vectors are rational. Now for this matrix, defining ξ in the same way as it was defined in Theorem 4.7, and applying (4.14), we obtain

$$N(\Lambda, B) \leq \xi^{n(n-1)} \det(\Lambda)^{2(n-1)}. \tag{4.20}$$

It is known that for a general rational lattice, there does not exist any basis such that the complexity of the corresponding trellis can be upper bounded by a function of γ or n. Interestingly, inequality (4.20) shows that for "any" rational lattice Λ, the complexity of the trellis constructed based on "any" basis of Λ is upper bounded by a function of n and $\det(\Lambda)$. In (4.20), however, ξ depends directly on the selected basis for the lattice. In the following, we derive upper bounds on the trellis complexity of integral lattices which are just a function of n and the lattice parameters (successive minima or determinant).

To derive upper bounds on the trellis complexity of integral lattices, we employ a basis of the lattice which is reduced in the sense of Korkin and Zolotarev (K-Z reduced basis). Based on Lemma 4.2, it is clear that the corresponding trellis is finite. The following property of K-Z reduced bases has been proved in [49].

Lemma 4.8 *Let* $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ *be a K-Z reduced basis of a lattice* Λ, *then*

$$\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq \left(\gamma_n^n \prod_{i=1}^{n} \frac{i+3}{4} \right)^{1/2} det(\Lambda)\,. \tag{4.21}$$

Note that $\gamma_n^n \prod_{i=1}^{n}(i+3)/4 \leq n^{2n}/(4\pi e^2 + o(1))^n$ for $n \to \infty$ [49].

Remark: All the bounds given in [71] have been obtained using the fact that any n-D lattice Λ has a basis with $\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq (2/\sqrt{3})^{n(n-1)/2}\det(\Lambda)$. Now for large values of n, comparing the logarithms of the bounds on $(\prod_{i=1}^{n} \|\mathbf{b}_i\|)/\det(\Lambda)$ in this inequality and (4.21), we notice that the bound in (4.21) is $O(nlogn)$ while the bound used in [71] is $O(n^2)$. This means that for large values of n, all the bounds of [71] can be improved just by making the assumption of using a K-Z reduced basis for the lattice.

The following lemma is of great importance to its subsequent results.

Lemma 4.9 *Let Λ be an n-D integral lattice with an arbitrary basis $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Then*

$$s_i \leq det(\Lambda_i)^2 \ , \quad for\ i = 1, \ldots, n \ , \tag{4.22}$$

where s_i is the number of states at level i of the trellis of Λ constructed based on B.

Proof: By the definition, $s_i = |P_i(\Lambda)/\Lambda_i| = \det(\Lambda_i)/\det(P_i(\Lambda))$. Using Lemma 4.7, we obtain $\det(P_i(\Lambda)) \geq \det((\Lambda_i)^*)$. Combining these with (2.10) completes the proof. □

Note that the bound of (4.22) is achieved for self-dual lattices.

Remark: In [71], to obtain an upper bound on s_i for an integral lattice, the authors derive and use an inequality of the form $s_i \leq \det(\Lambda_i)^{2i}$. Substituting this inequality with (4.22) can also improve their results substantially.

Proposition 4.8 *Let Λ be an n-D integral lattice with a K-Z reduced basis B, and let N, s_i, e_i, and g_i be the parameters of the trellis of Λ constructed based on B.*

Then

$$N \leq \prod_{j=1}^{n} \lambda_j^{2(n-j)} , \tag{4.23}$$

$$s_i \leq \prod_{j=1}^{i} \lambda_j^2 , \quad for\ i = 1, \ldots, n-1 , \tag{4.24}$$

$$g_i \leq e_i \leq (\prod_{j=1}^{i-1} \lambda_j^4)\lambda_i^2 , for\, i = 2, \ldots, n-1 , \ g_1 \leq e_1 \leq \lambda_1^2 , \ g_n \leq e_n \leq \prod_{j=1}^{n-1} \lambda_j^2, \tag{4.25}$$

where λ_i is the i-th successive minimum of Λ.

Proof: We first prove (4.24) by applying $\det(\Lambda_i) = \|\hat{\mathbf{b}}_1\| \cdots \|\hat{\mathbf{b}}_i\|$, and Proposition 3.1 to (4.22). Inequalities (4.23) and (4.25) then follow from (4.24), using the facts that $N \leq s_1 \cdots s_{n-1}$, and $g_i \leq e_i \leq s_{i-1}s_i$, for $i = 1, \ldots, n$, and $s_0 = s_n = 1$. □

Remark: In [71], the main ingredient in deriving an upper bound on the number of distinct paths in a trellis of an integral lattice Λ is a lemma which proves that if Λ has a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, then it also has an orthogonal sublattice Λ' with $\det(\Lambda') \leq n!(\|\mathbf{b}_1\| \cdots \|\mathbf{b}_n\|)^{2n}$. Based on the above discussions, it is not difficult to see that this inequality can be improved to $\det(\Lambda') \leq (\|\mathbf{b}_1\| \cdots \|\mathbf{b}_n\|)^n$. To prove this, we use the inequality $N(\Lambda, B) \leq \|\hat{\mathbf{b}}_1\|^{2(n-1)}\|\hat{\mathbf{b}}_2\|^{2(n-2)} \cdots \|\hat{\mathbf{b}}_{n-1}\|^2$, which is similar to (4.23) and is valid for any basis of Λ. Multiplying both sides of this inequality with $\det(\Lambda) = \|\hat{\mathbf{b}}_1\| \cdots \|\hat{\mathbf{b}}_n\|$, and using $N\det(\Lambda) = \det(\Lambda')$, we obtain $\det(\Lambda') \leq \|\hat{\mathbf{b}}_1\|^{2n-1}\|\hat{\mathbf{b}}_2\|^{2n-3} \cdots \|\hat{\mathbf{b}}_n\|$. Combining this with $\|\hat{\mathbf{b}}_i\| \leq \|\mathbf{b}_i\|$, for $i = 1, \ldots, n$, and using an assumption that the basis vectors are arranged in increasing norm order complete the proof. Note that the same inequality can also be obtained using an intermediate result of [71] itself. In Lemma 4 of [71], it has been proved that the vectors $\mathbf{x}_1 = \hat{\mathbf{b}}_1$ and $\mathbf{x}_i = \det(\Lambda_{i-1})^2\hat{\mathbf{b}}_i$, $i = 2, \ldots, n$, belong to Λ. Now based on $\det(\Lambda_{i-1}) = \|\hat{\mathbf{b}}_1\| \cdots \|\hat{\mathbf{b}}_{i-1}\|$, and $\|\hat{\mathbf{b}}_i\| \leq \|\mathbf{b}_i\|, \forall i$, we have $\|\mathbf{x}_i\| \leq$

$\|\mathbf{b}_1\|^2 \cdots \|\mathbf{b}_{i-1}\|^2 \|\mathbf{b}_i\|$. This along with the fact that $\det(\Lambda') \leq \|\mathbf{x}_1\| \cdots \|\mathbf{x}_n\|$, and using an assumption that the basis vectors are arranged in increasing norm order lead to the result.

Theorem 4.8 *Let Λ be an n-D integral lattice with a K-Z reduced basis B, and let s_i, e_i, and g_i be the parameters of the trellis of Λ constructed based on B. Then*

$$s_i \leq det(\Lambda)^{2i/n} \gamma_n^i, \quad for \ i = 0, \ldots, n-1, \tag{4.26}$$

$$\begin{aligned} g_i \leq e_i &\leq det(\Lambda)^{4i/n} \gamma_n^{2i}, \quad for \ i = 2, \ldots, n-1, \\ g_1 \leq e_1 &\leq det(\Lambda)^{2/n} \gamma_n, \quad g_n \leq e_n \leq det(\Lambda)^{2(n-1)/n} \gamma_n^{n-1}. \end{aligned} \tag{4.27}$$

Proof: Using (2.1), it is easy to obtain $s_i \leq (\lambda_1 \cdots \lambda_n)^{2i/n}$, for $i = 1, \ldots, n-1$, from (4.24). The result in (4.26) then follows by combining these inequalities with (2.4). It is easy to see that (4.26) is also valid for $i = 0$. To obtain the results of (4.27), we apply the same procedure to (4.25). One more step is required, i.e., since for an integral lattice, $\lambda_i \geq 1$, $i = 1, \ldots, n$, we have $g_i \leq e_i \leq (\lambda_1 \cdots \lambda_i)^4$, for $i = 2, \ldots, n-1$. □

Theorem 4.9 *Let Λ be an n-D integral lattice with ESM. Now if B is a K-Z reduced basis of Λ and s_i, e_i, and g_i are the parameters of the trellis of Λ constructed based on B, then*

$$s_i \leq \lambda^{2i}, \quad for \ i = 0, \ldots, n-1, \tag{4.28}$$

$$g_i \leq e_i \leq \lambda^{4i-2}, \quad for \ i = 1 \ldots, n-1, \quad g_n \leq e_n \leq \lambda^{2(n-1)}, \tag{4.29}$$

where λ is the minimum distance of Λ.

Proof: The results immediately follow by substituting λ for all the successive minima $\lambda_1, \ldots, \lambda_n$ in Proposition 4.8. Note that inequality (4.28) is trivially valid for $i = 0$. □

Theorem 4.10 *Let Λ be an n-D integral lattice with a K-Z reduced basis B. Then*

$$N(\Lambda, B) \leq det(\Lambda)^{n-1} \gamma_n^{n(n-1)/2} , \tag{4.30}$$

$$\mathcal{S}(\Lambda, B) \leq det(\Lambda)^{2(n-1)/n} \gamma_n^{n-1} , \tag{4.31}$$

$$\mathcal{G}(\Lambda, B) \leq \mathcal{E}(\Lambda, B) \leq det(\Lambda)^{4(n-1)/n} \gamma_n^{2(n-1)} . \tag{4.32}$$

Proof: It is not difficult to see that applying the inequalities of (2.1) to (4.23) results in $N(\Lambda, B) \leq (\lambda_1 \cdots \lambda_n)^{n-1}$. This combined with (2.4) completes the proof of (4.30).

To derive the the bounds in (4.31) and (4.32), we use the results of Theorem 4.8 along with the facts that $\mathcal{S} \leq \max_i s_i$, and $\mathcal{G} \leq \mathcal{E} \leq \max_i e_i$. Note that $\gamma_n \geq 1$, $\forall n$, and that for an integral lattice, $\det(\Lambda) \geq 1$. □

For ESM-lattices, the bounds of Theorem 4.10 can be improved as follows.

Theorem 4.11 *Let Λ be an n-D integral lattice with ESM. Then for B a K-Z reduced basis of Λ, we have*

$$N(\Lambda, B) \leq \lambda^{n(n-1)} , \tag{4.33}$$

$$\mathcal{S}(\Lambda, B) \leq \frac{\lambda^{2n} - 1}{n(\lambda^2 - 1)} , \tag{4.34}$$

$$\mathcal{G}(\Lambda, B) \leq \mathcal{E}(\Lambda, B) \leq \frac{(\lambda^{2n} - 1)(\lambda^{2(n-1)} + \lambda^2)}{n(\lambda^4 - 1)} , \tag{4.35}$$

where λ is the minimum distance of Λ.

Proof: Inequality (4.33) follows from substituting λ for all the successive minima in (4.23). Inequalities (4.34) and (4.35) are obtained by applying the results of

Theorem 4.9 to the definitions of $\mathcal{S}$ and $\mathcal{E}$, i.e., $\mathcal{S} = (\sum s_i - 1)/n$, and $\mathcal{E} = (\sum e_i)/n$. □

It can be seen that the bounds of Theorem 4.11 are tighter than the ones in Theorem 4.10. For the densest lattices, the gaps between the bounds become smaller. In particular, the two bounds given in (4.30) and (4.33) coincide for the densest lattices. It should also be noted that in all the upper bounds, γ_n can be replaced by a function of n using the inequalities $\gamma_n \leq n$, or $\gamma_n \leq 2n/3$, for $n \geq 2$. For large values of n, one can also use the upper bound of (2.3).

Finally, we notice that all the upper bounds of Theorems 4.9 and 4.11 are achieved for lattices $\mathbb{Z}^n$ (for inequalities (4.34) and (4.35), one should find the limit of the upper bounds as $\lambda \to 1$. This is equal to 1). In fact, Theorem 4.11 implies that $\mathbb{Z}^n$ is the only n-D integral lattice with ESM which has $\lambda = 1$. Also for the integral version of the hexagonal lattice A_2 with $\lambda(A_2) = \sqrt{2}$, all the inequalities in Theorems 4.9 and 4.11 are satisfied with equality. Note that the minimal trellis of A_2 consists of two paths, and has two states at level one.

Discussion: To compare the derived upper bounds in this thesis with those obtained in [71], we choose two inequalities (4.26) and (4.30), which have correspondences in [71]. The corresponding result of [71] states that for every n-D integral lattice Λ, *there exists* a trellis such that

$$s_i \leq (2/\sqrt{3})^{i^2(n-1)} \det(\Lambda)^{2i^2/n} ,$$

$$N \leq n!\, (2/\sqrt{3})^{n^2(n-1)} \det(\Lambda)^{2n-1} .$$

Based on the fact that for an integral lattice $\det(\Lambda) \geq 1$, one can see the superiority of our bounds over the above results, especially for large values of n. Note that we are still able to improve the bounds of (4.26) and (4.30) for ESM-lattices, as can be seen in (4.28), and (4.33).

4.4 Conclusion

By deriving bounds, we have investigated the trellis complexity of lattices to some extent. The discussions has been based on a universal approach to the construction and analysis of the trellis diagrams of lattices using their bases. Some results relating the trellis complexity of dual lattices have been established. These results have been used in deriving upper bounds on the trellis complexity. The upper bound results both improve and generalize the similar results of [71].

Chapter 5

Minimal trellis diagrams of lattices

For clear reasons, finding low-complexity trellis diagrams for group codes is of importance. There has been a great amount of research devoted to addressing this problem for block codes, e.g., [60], [44], [45],[14],[32],[46],[15]. In most of these works, the authors concentrate on state complexity, and find permutations of the time axis which result in low-complexity trellises for some categories of codes. In continuation to this extensive work on the subject, the general problem area is predicted to remain wide open and active for future research [28].

Despite the situation for block codes, search for low-complexity trellis diagrams of lattices (parallel to the permutation problem for block codes) has not received much attention yet. In fact, the credit for taking the first and perhaps the only step towards this subject goes to Forney for his work in [33]. Here, we continue this mission to a certain extent by devising simple algorithms for finding low-complexity (in many cases, minimal) trellises for a wide range of lattices.

In previous sections and by two examples we gave basis matrices for D_4 and the Leech lattice which result in minimal trellis diagrams for these lattices. In this chapter, we continue by obtaining low-complexity trellis diagrams of some other important lattices. In many cases, like Barnes-Wall lattices BW_n, root lattices and their duals D_n, D_n^*, E_n, E_n^*, and A_n, A_n^*, $n \leq 9$, we are also able to prove that the obtained trellises are minimal. For proof, we either use (4.7), or derive tighter lower bounds on complexity which are achieved by the obtained trellises.

To establish the new lower bounds, we use enumeration techniques which are based on the distance distribution of the shells of lattice points with respect to the origin, the arrangement of points on the first few shells of the lattice, and the fact that the determinant of a lattice divides the determinant of any of its sublattices. Although these techniques are applied to some particular lattices in this thesis, they can also be applied to the other categories of lattices to either improve the lower bound of $\lceil \gamma^{n/2} \rceil$ on the trellis complexity, or search for minimal trellises.

5.1 Preliminaries

It appears that finding a minimal trellis of a general lattice Λ is a very hard problem. To solve it, one can search for n mutually orthogonal vectors of Λ, $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$, which minimize $\prod_{i=1}^{n} \|\mathbf{b}'_i\|$. This is actually the same as minimizing $\det(\Lambda')$, where Λ' is an n-D orthogonal sublattice of Λ with basis vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$. Let Λ be an n-D rational lattice with a given basis B. A trellis of Λ can be constructed based on the basis B (see Section 4.1). Suppose that this trellis has a complexity N_0, and let $\mathbf{x} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i, \alpha_i \in \mathbb{Z}, \forall i$, be a candidate point of Λ for any of the vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$, in the above description. Knowing the value of $\lambda(\Lambda)$, to obtain a trellis of Λ with complexity lower than N_0 (or to show that there does not exist such a

trellis), one only needs to search for $\mathbf{x}$ in the sphere centered at the origin with the radius of $R = N_0 \det(\Lambda)/(\lambda(\Lambda)^{n-1})$. This however could be a difficult task in general. One way of performing this task is to enumerate α_i's from α_n to α_1, successively, and by a method similar to the one presented in Section 3.3. Knowing more about the structure of Λ and the arrangement of its points can usually help to reduce R in the above algorithm, and therefore to make the problem more tractable. Such knowledge can also be employed to improve the bound of (4.7) on trellis complexity. It can even, rather simply, result in finding minimal trellises (without explicitly using the above algorithm), if it is properly combined with an enumeration method which enumerates lattice points on the first few shells of the lattice. These are illustrated in the following sections for some famous lattices.

On the other hand, as we explained in Section 4.1, for rational lattices finding a proper trellis coordinate system, which results in a small value of N, is equivalent to finding a proper basis for the lattice. Thus to obtain a minimal trellis of a lattice Λ, one can search among all the possible bases for Λ. This is clearly a very hard task, even in small dimensionalities. Note that different orderings of basis vectors result in different coordinate systems, and even for only considering the different orderings of a given basis for a lattice, the amount of computation explodes exponentially with dimension.

Having an $n \times m$ basis B of a lattice Λ, any other basis B' of Λ can be constructed (in the same standard coordinate system) by using $B' = UB$, where U is an $n \times n$ unimodular matrix. To show the variety of unimodular operations, we list some of

them below:

i. Interchanging two rows.

ii. Multiplying a row by -1.

iii. Adding an integer multiple of a row to another one.

The corresponding unimodular matrices can be easily constructed [62, p. 192]. Note that the combination of any two unimodular operations (corresponding to the multiplication of the corresponding unimodular matrices) is also a unimodular operation. Despite the intractability of the problem of finding a minimal trellis for a lattice via searching among its bases, it appears that in many cases just starting from a given basis matrix, and reordering the rows gives us good trellis diagrams (sometimes minimal). (See, e.g., Example 4.1). In the following, when we search for a low-complexity trellis of a lattice by working on a given basis, we just permute the basis vectors. This is done as a complete search in small dimensionalities (up to 8), and as a random search for $n \geq 9$. We also notice that minimizing N does not necessarily result in minimizing the other complexity measures of the trellis. In fact, it is not difficult to find examples where two minimal trellises of the same lattice have different values of $\mathcal{S}, \mathcal{G}$, or $\mathcal{E}$ (see, e.g., Example 5.6). Among the minimal trellis diagrams of a lattice, one might be interested in selecting the one which has a lower complexity with respect to another complexity measure, e.g., $\mathcal{S}$. However, no attempt has been made to consider this aspect of the problem here.

For the rest of this work, we need to define matrices R_n, $n = 2m$, $m \geq 1$, by the following recursion:

$$R_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad R_n = R_{n-2} \oplus R_2, \quad n \geq 4,$$

where $\oplus$ denotes the direct sum operation, as defined in (2.11). Note that $R_n = R_n^T$.

We also have $R_n^2 = 2I_n$, which means that $R_n/\sqrt{2}$ is an orthogonal matrix. Let Λ be an n-D lattice ($n = 2m$) with a basis matrix B. We denote a version of Λ by $R\Lambda$ if it has a basis matrix equal to BR_n.

Given a trellis coordinate system $S_1 = \{W_i\}_{i=1}^n$, and a basis B for a lattice Λ, it frequently happens that we need to find another basis B' for Λ such that the two ordered systems $S_2 = \{span(\hat{\mathbf{b}}_i')\}_{i=1}^n$ and S_1 are the same. Let U_1 denote the matrix with its rows equal to the unit vectors of the coordinate system S_1. We first transform B to S_1 by computing $B_1 = B(U_1)^T$. Then by finding the HNF of B_1, we obtain a basis H in S_1 with its G-S vectors along the coordinate system. The basis B' is equal to H transformed back to the original coordinate system, i.e., $B' = HU_1$.

5.2 Barnes-Wall lattices

It can be seen that all the Barnes-Wall lattices $BW_n (n = 2^m,\ m \geq 2)$ have n mutually orthogonal vectors of length λ, [1]. This in conjunction with Theorem 4.4 and Lemma 4.1 indicates that there exists a basis B for each Barnes-Wall lattice BW_n such that $N(BW_n, B) = \gamma^{n/2} = (n/2)^{n/4}$. In the following, starting from a given basis for a Barnes-Wall lattice Λ, we construct another basis which results in a minimal trellis for Λ.

Let G be a matrix with $(1,0)$ and $(1,1)$ as its rows (the order of rows can be selected arbitrarily). Let $G^{\otimes m}$ denote the m-fold Kronecker (tensor) product of G,

[1] Forney has also noticed that certain interesting lattices Λ, including the Barnes-Wall lattices, have this property. Equivalently, he has observed that these lattices have orthogonal sublattices Λ' such that $|\Lambda/\Lambda'| = \gamma(\Lambda)^{n/2}$. This result for Barnes-Wall lattices can also be obtained from the code formulas given in [31].

where the Kronecker product $C \otimes D$ of matrices $C = (c_{ij})$, $1 \leq i \leq p, 1 \leq j \leq q$, and D is defined as

$$\begin{pmatrix} c_{11}D & c_{12}D & \cdots & c_{1q}D \\ \cdot & \cdot & \cdot & \cdots \\ c_{p1}D & c_{p2}D & \cdots & c_{pq}D \end{pmatrix}.$$

A basis matrix for BW_n can be formed by selecting the rows of matrices $G^{\otimes m}$, $2G^{\otimes m}, \ldots, 2^{\lfloor m/2 \rfloor}G^{\otimes m}$ which have a square norm equal to 2^{m-1} or 2^m. In this version, $\lambda(BW_n) = \sqrt{n/2}$ and $\det(BW_n) = (n/2)^{n/4}$, which confirms that $\gamma(BW_n) = \sqrt{n/2}$. Starting from the above basis matrix of BW_n, the following theorem gives an algorithm for finding a basis which minimizes $N(BW_n, B)$.

Theorem 5.1 *Let Λ denote the above version of Barnes-Wall lattice $BW_n (n = 2^m, m \geq 2)$. For m odd, select matrix $\tilde{B}$ to be the HNF of Λ, and for m even, choose it as $\frac{1}{2}HR_n$, where H is the HNF of $R\Lambda$. Then $\tilde{B}$ minimizes $N(\Lambda, B)$, i.e., $N(\Lambda, \tilde{B}) = (n/2)^{n/4}$.*

Proof: We prove the theorem by induction. For $m = 2$, the lattice BW_4 is the same as D_4. As a basis matrix for this version of D_4, we can use either the algorithm stated before, or simply select either one of the matrices B_1 or B_2 given in Example 4.1. Starting from one of these basis matrices as B, we first find the HNF of BR_4. Then by multiplying the result by $\frac{1}{2}R_4$ from the right, we obtain the following basis matrix for D_4:

$$\tilde{B} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & -1 \end{pmatrix}.$$

Using Propositions 4.1 and 4.2, it is easy to see that $N(D_4, \tilde{B}) = 2$.

By Lemma 4.5, the above procedure for finding $\tilde{B}$ implies that using the HNF of RD_4 as the basis matrix minimizes $N(RD_4, B)$. This in turn, by Theorem 4.4, concludes that RD_4 has four of its shortest vectors along the coordinate vectors. Now for every $m \geq 3$, and odd, the induction assumption similarly implies that $RBW_{2^{m-1}}$ has 2^{m-1} of its shortest vectors along the coordinate vectors. It is known that $BW_{2^m} = |BW_{2^{m-1}}/RBW_{2^{m-1}}|^2$, where $|\cdot/\cdot|^2$ denotes the squaring construction [31]. From the squaring construction and the fact that $RBW_{2^{m-1}}$ has 2^{m-1} shortest vectors along the coordinate system, it follows that BW_{2^m} has 2^m of its shortest vectors along the coordinate vectors. Thus the HNF of BW_{2^m} minimizes $N(BW_{2^m}, B)$.

For $m \geq 4$ and even, let the HNF of $BW_{2^{m-1}}$ give the minimum number of distinct paths in the trellis of $BW_{2^{m-1}}$. This implies that $BW_{2^{m-1}}$ has 2^{m-1} shortest vectors along the coordinate vectors. Since $BW_{2^m} = |BW_{2^{m-1}}/RBW_{2^{m-1}}|^2$, it can then be concluded that RBW_{2^m} has 2^m of its shortest vectors along the coordinate vectors. This implies that the HNF of RBW_{2^m}, denoted by H, minimizes $N(RBW_{2^m}, B)$, and therefore the matrix $\frac{1}{2}HR_{2^m}$ minimizes $N(BW_{2^m}, B)$. □

Example 5.1 *The lattice BW_8 is the Gosset lattice E_8. The following basis matrix*

of E_8, which is actually its HNF, minimizes $N(E_8, B)$, i.e., $N(E_8, \tilde{B}) = 16$.

$$\tilde{B} = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & -1 & 1 & 0 & 0 \\ -1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \end{pmatrix}.$$

The corresponding trellis of E_8 is given in Figure 5.1. This trellis corresponds to the "minimal code formula" of $E_8 = 2\mathbb{Z}^8 + (8, 4, 4)$ for E_8, where the linear code $(8, 4, 4)$ is the first order binary Reed-Muller code [59, p. 373]. A trellis of E_8 isomorphic to the trellis of Figure 5.1, and constructed based on the same code formula has been also given in [33]. Note that for another trellis of E_8 given in [33] which minimizes

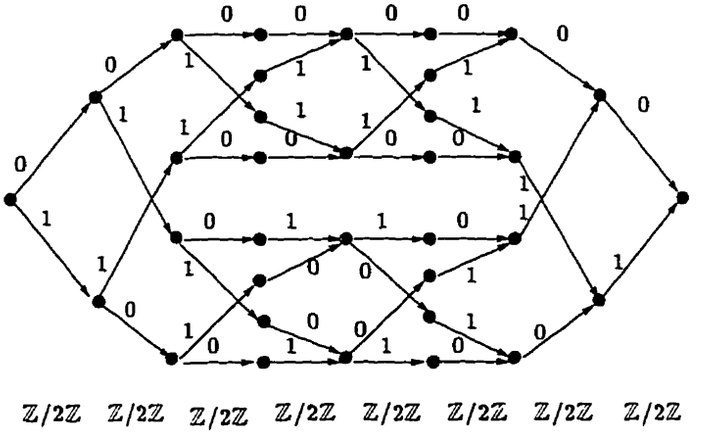

Figure 5.1: A minimal trellis diagram of E_8.

the number of states, we have $N(E_8, B) = 576$, which is much larger than 16. Thus we expect the trellis of Figure 5.1 to decode E_8 more efficiently. This is indeed the

case. The trellis of [33] (with minimum number of states) has $\mathcal{E} = 7$ *and* $\mathcal{G} = 6$, *compared to* $\mathcal{E} = 5.5$ *and* $\mathcal{G} = 2$ *for the above trellis. It also requires* 33 *two-way comparisons for the VA, while this number for the trellis of Figure* 5.1 *is only* 11.

It can be seen that for BW_n, $n \geq 8$, starting from the minimal trellis of D_4, the trellis iteratively constructed based on the two-section trellis of squaring construction [31] is also minimal. To see this, we notice that based on the construction of the two-section trellis, $N(BW_n) = |BW_{n/2}/RBW_{n/2}|N(BW_{n/2})^2$, where we have used the fact that the minimal trellises for $BW_{n/2}$ and $RBW_{n/2}$ have the same number of distinct paths. This combined with $|BW_{n/2}/RBW_{n/2}| = 2^{n/4}$, [31], and the initial condition of $N(D_4) = 2$ results in $N(BW_n) = (n/2)^{n/4}$. The two minimal trellises are however different, and the trellis constructed based on Theorem 5.1 has a lower Viterbi decoding complexity.

5.3 Lattices D_n

For $n \geq 3$, D_n can be represented by the following basis matrix [25, p. 117]:

$$B = \begin{pmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}. \tag{5.1}$$

For this version of D_n, we have $\det(D_n) = 2$, and $\lambda(D_n) = \sqrt{2}$, which result in $\gamma(D_n) = 2^{(n-2)/n}$. Since D_n is an integer lattice, Theorem 4.5 predicts that using the HNF of D_n as the basis matrix, we obtain $N(D_n, H) \leq 2^{n-1}$. In fact, it appears that $N(D_n, H) = 2^{n-1}$. We also note that the construction of D_n based on

the $(n, n-1, 2)$ linear code consisting of all codewords of even weight, and using construction A [25, p. 138], expresses D_n as the union of 2^{n-1} cosets of $2\mathbb{Z}^n$. The conventional trellis of D_n based on this construction is given in Figure 5.2. There is however, some gap between this result and the lower bound of $\gamma^{n/2} = 2^{(n-2)/2}$ given in Theorem 4.4. We already observed in Example 4.1 that the minimal trellis of D_4 achieves the lower bound. The code formula of lattices RD_n, $n = 2^m$, given in [31], which expresses RD_n as the union of $2^{(n-2)/2}$ cosets of $2\mathbb{Z}^n$, also predicts that the above result can be improved (at least for D_n, $n = 2^m$).

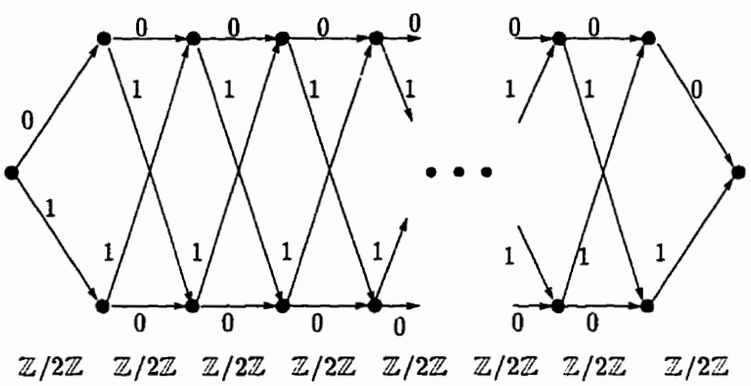

Figure 5.2: Conventional trellis of D_n corresponding to $D_n = 2\mathbb{Z}^n + (n, n-1, 2)$.

5.3.1 n even

Using the basis matrix of (5.1), it can be seen that for n even, the n mutually orthogonal vectors $\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_1 - \mathbf{u}_2, \mathbf{u}_3 + \mathbf{u}_4, \mathbf{u}_3 - \mathbf{u}_4, \ldots, \mathbf{u}_{n-1} + \mathbf{u}_n$, and $\mathbf{u}_{n-1} - \mathbf{u}_n$ belong to the lattice D_n, where $\mathbf{u}_i$ is the i-th coordinate vector. Noticing the fact that all these vectors are shortest vectors of D_n, and using Theorem 4.4 and Lemma 4.1, we conclude that there exists a basis for D_n, n even, that achieves the lower bound of Theorem 4.4. The following theorem gives such a basis.

Theorem 5.2 *For D_n, n even, let H denote the HNF of the lattice RD_n. Then $N(D_n, HR_n/2) = 2^{(n-2)/2}$, i.e., the trellis constructed for D_n based on the basis matrix $HR_n/2$ is a minimal trellis.*

Proof: Using the basis matrix B of (5.1), we can see that for n even, the lattice RD_n with basis matrix BR_n has n vectors of length $\lambda(RD_n) = 2$ along the standard coordinate system. This together with the fact that for a HNF as a basis, the G-S vectors are along the standard coordinate system, and Theorem 4.4 results in $N(RD_n, H) = \gamma(RD_n)^{n/2} = \gamma(D_n)^{n/2}$. Combining this with Lemma 4.5 completes the proof. □

Example 5.2 *Using the basis matrix of Theorem 5.2, we obtain the trellis of Figure 5.3 for D_6. This trellis corresponds tc the minimal code formula $RD_6 = 2\mathbb{Z}^6 +$*

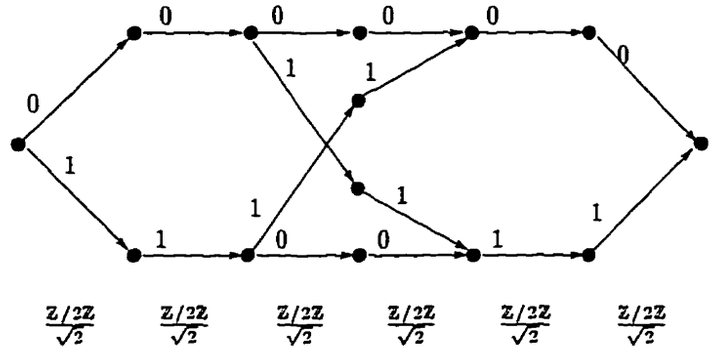

Figure 5.3: A minimal trellis diagram of D_6.

$(6,2,4)$, where the linear code $(6,2,4)$ consists of codewords (000000), (110011), (111100), *and* (001111).

It can be seen that in general, the minimal trellis diagram of D_n, n even, constructed based on the basis introduced in Theorem 5.2, has a form of Figure 5.4(a). An intermediate trellis section for this trellis diagram is given in Figure 5.4(b).

Adding this trellis section to the middle part of the trellis diagram of D_n results in the trellis diagram of D_{n+2}. It is easy to see that in the trellis of Figure 5.4(a), we have $\mathcal{G}(D_n) = 2, \mathcal{S}(D_n) = (3n-5)/n$, and $\mathcal{E}(D_n) = 4(n-2)/n$.

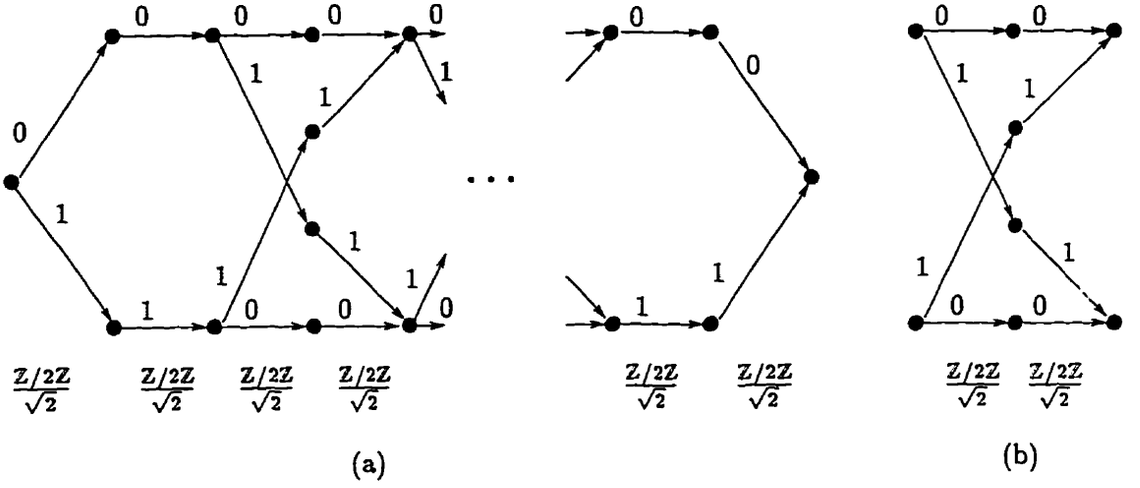

Figure 5.4: (a) A minimal trellis diagram of D_n, n even. (b) A trellis section.

Finally, we notice that the trellis of Figure 5.4(a) corresponds to the minimal code formula of $RD_n = 2\mathbb{Z}^n + (n, \frac{n-2}{2}, 4)$ for RD_n, n even.

5.3.2 n odd

For D_n, n odd, by permuting the basis vectors of (5.1), we are able to obtain trellises with $N = \sqrt{2}\gamma^{n/2}$. This is illustrated in the following theorem.

Theorem 5.3 *For D_n, n odd, reordering the basis vectors of B (given in (5.1)), let $\tilde{B} = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_5, \mathbf{b}_4, \mathbf{b}_7, \mathbf{b}_6, \ldots, \mathbf{b}_n, \mathbf{b}_{n-1})$. Then $N(D_n, \tilde{B}) = 2^{(n-1)/2}$.*

Proof: We prove the theorem by induction. It is easy to see that for D_3, the basis $\tilde{B}_3 = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3)$ results in $N(D_3, \tilde{B}_3) = 2$. Now assume that for $n_1 \geq 3$, and

odd, the basis matrix $B \triangleq \tilde{B}_{n_1} = (\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_5, \mathbf{b}_4, \mathbf{b}_7, \mathbf{b}_6, \ldots, \mathbf{b}_{n_1}, \mathbf{b}_{n_1-1})$ results in $N(D_{n_1}, B) = 2^{(n_1-1)/2}$. It can be seen that the lattice D_{n_1+2} has the following basis matrix:

$$B' \triangleq \tilde{B}_{n_1+2} = \begin{pmatrix} & & & & & 0 & 0 \\ & & B & & & \cdot & \cdot \\ & & & & & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & -1 \\ 0 & 0 & \cdots & 0 & 1 & -1 & 0 \end{pmatrix}.$$

Therefore, we have $\hat{\mathbf{b}}'_i = \hat{\mathbf{b}}_i$, for $i = 1, \ldots, n_1$, and consequently, $\alpha'_i = \alpha_i$, for $i = 1, \ldots, n_1$, where α'_i and α_i are defined in Section 4.1, and are the corresponding parameters of lattices D_{n_1} and D_{n_1+2}, respectively. Using Proposition 4.1, we then have $N(D_{n_1+2}, B') = \alpha'_{n_1+1}\alpha'_{n_1+2}N(D_{n_1}, B)$. Based on the above definition of B', it is easy to see that $\hat{\mathbf{b}}'_{n_1+1} = \mathbf{b}'_{n_1+1}$ and $\hat{\mathbf{b}}'_{n_1+2} = (0, \ldots, 0, -1/2, -1/2)$. This combined with the definition of α'_i results in $\alpha'_{n_1+1} = 1$, and $\alpha'_{n_1+2} = 2$. Note that both vectors $\mathbf{b}'_{n_1+1}$ and $2\hat{\mathbf{b}}'_{n_1+2}$ are shortest vectors of D_{n_1+2}. Thus we have $N(D_{n_1+2}, B') = 2N(D_{n_1}, B) = 2^{(n_1+1)/2}$, which completes the proof. □

Note that based on (4.7), we have $N(D_3, B) \geq 2$, which means that the basis $\tilde{B}$ of the above theorem results in a minimal trellis for D_3. The minimal trellis of D_3 has two states in levels one and two. For the other values of n, the lower bound of (4.7) is improved in the following theorem.

Theorem 5.4 *For any trellis diagram of lattices D_n, n odd, we have $N \geq \sqrt{2}\gamma(D_n)^{n/2}$.*

Proof: It is easy to see that for the version of D_n considered here, the lengths of the nonzero vectors in increasing order are [25, p. 118]:

$$\sqrt{2}, 2, \sqrt{6}, \sqrt{8}, \sqrt{10}, \ldots .$$

It can also be seen that it is not possible to find an orthogonal sublattice Λ' of D_n, n odd, such that the lengths of its mutually orthogonal basis vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ are all equal to $\lambda(D_n) = \sqrt{2}$. The reason is that this along with (4.6) results in $\det(\Lambda') = 2^{n/2}$, which is not divisible by $\det(D_n) = 2$, for n odd. Putting this case aside, the next best case for $\det(\Lambda')$ to be minimized is when just one of the vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$ has a length of 2, while the others have still a length of $\sqrt{2}$. This results in $\det(\Lambda') \geq 2^{(n+1)/2}$, and thus $N \geq 2^{(n-1)/2} = \sqrt{2}\gamma(D_n)^{n/2}$, which completes the proof. □

Corollary 5.1 *For lattices D_n, n odd, the trellis diagrams with $N = 2^{(n-1)/2}$, constructed based on the basis $\tilde{B}$ given in Theorem* 5.3, *are minimal.*

Example 5.3 *Using the basis introduced in Theorem* 5.3, *we obtain the minimal trellis diagram of Figure* 5.5 *for D_5. It can be seen that the label code is the linear*

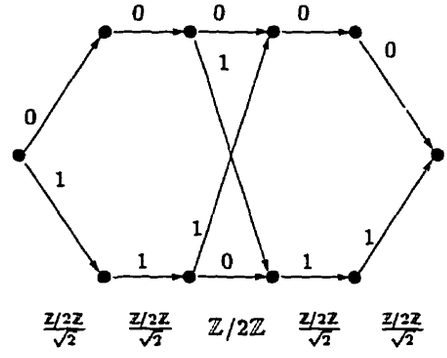

Figure 5.5: A minimal trellis diagram of D_5.

code $(5, 2, 3)$ *consisting of codewords* $(00000), (00111), (11100)$, *and* (11011).

In general, the minimal trellis diagram of D_n, n odd, has the form of Figure 5.6. An intermediate trellis section for this trellis diagram is the same as the one for

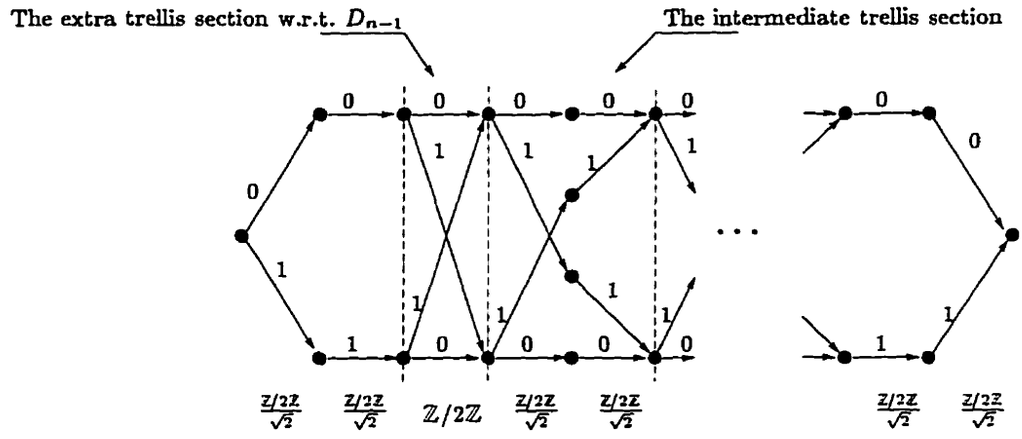

Figure 5.6: A minimal trellis diagram of D_n, n odd.

the trellis of D_n, n even, and is given in Figure 5.4(b). Adding this trellis section to the middle part of the trellis diagram of $D_n, n \geq 5$, results in the trellis diagram of D_{n+2}. Comparing Figures 5.4(a) and 5.6, one realizes that the only difference between trellises is that the trellis of D_n, n odd, has an extra section (as its third section) with respect to the trellis of D_{n-1}. It is also easy to see that in the minimal trellis of Figure 5.6, and for $n \geq 5$, we have $\mathcal{G}(D_n) = 2, \mathcal{S}(D_n) = 3(n-2)/n$, and $\mathcal{E}(D_n) = 4(n-2)/n$. For $n = 3$, we have $\mathcal{G}(D_3) = 2, \mathcal{S}(D_3) = 5/3$, and $\mathcal{E}(D_3) = 2$.

Note that although the conventional trellis of D_n, given in Figure 5.2, minimizes the number of states, it has a higher Viterbi decoding complexity compared to the minimal trellises of D_n obtained here. In specific, the number of two-way comparisons required for the VA to decode the trellis of Figure 5.2 is more than twice what is needed for the decoding of our minimal trellises.

5.4 Lattices D_n^*

The following matrix is a basis for D_n^*, $n \geq 3$, [25, p. 120]:

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ . & . & \cdots & . & . \\ 0 & 0 & \cdots & 1 & 0 \\ 1/2 & 1/2 & \cdots & 1/2 & 1/2 \end{pmatrix}. \tag{5.2}$$

For this version of D_n^*, we have $\det(D_n^*) = 1/2$, and $\lambda = \sqrt{3}/2$, $n = 3$, or $\lambda = 1$, $n \geq 4$. It can be seen that $\gamma(D_3^*) = 1.191$, and $\gamma(D_n^*) = 2^{2/n}$, $n \geq 4$. Using Proposition 4.5, we obtain $N(D_n^*, H) \leq \det(D_n) = 2$, where H is the HNF of D_n^*. On the other hand, based on (4.7), for any basis B' of D_n^*, $N(D_n^*, B') \geq 2$. Combining these results indicates that the trellis constructed based on the HNF of D_n^* is a minimal trellis with two distinct paths. Note that this is in agreement with the fact that $\mathbb{Z}^n$ is a sublattice of D_n^* with index two. In fact, $D_n^* = \mathbb{Z}^n + 1/2(n, 1, n)$, where $(n, 1, n)$ is the binary repetition code. It can be seen that the basis of (5.2) has also its G-S vectors along the coordinate system, we therefore have $N(D_n^*, B) = 2$. The corresponding trellis of D_n^* is given in Figure 5.7.

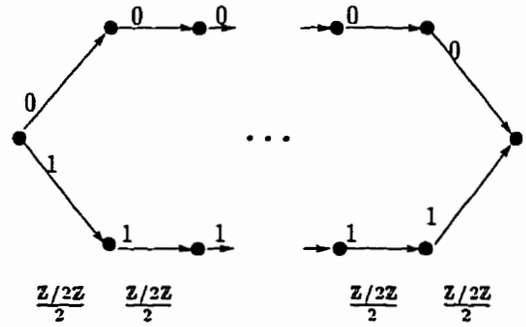

Figure 5.7: A minimal trellis diagram of D_n^*.

The decoding of D_n^* based on the trellis of Figure 5.7 is equivalent to the decoding of the union of two cosets of $\mathbb{Z}^n$ in D_n^*, [22]. The latter is known as the fastest method for the decoding of D_n^*.

5.5 Lattices E_n, E_n^*

In Section 5.2, a minimal trellis and the corresponding basis for $E_8(= E_8^*)$ were given. In the following, we find minimal trellises for lattices E_6, E_6^*, E_7, and E_7^*.

5.5.1 Lattices E_6 and E_6^*

The following basis matrices generate E_6 and E_6^* [25, pp. 126,127]:

$$B = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}, \tag{5.3}$$

$$B^* = \begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}. \tag{5.4}$$

It is known that A_2^3 is a sublattice of E_6 with index 3 [25, p. 447]. This combined with the fact that the minimal trellis of A_2 has two paths indicates that there exists

a trellis diagram for E_6 with $N \leq 24$. Using a permuted version of (5.3) with the order of basis vectors as $(1,3,2,5,4,6)$, we obtain $N(E_6) = 16$. The corresponding trellis is given in Figure 5.8(a). Using this result along with the fact that E_6, as an integral lattice, is a sublattice of E_6^* with index 3, we conclude that there exists a trellis of E_6^* with $N \leq 48$. In fact, Theorem 4.2 along with the result of Figure 5.8(a) for the sizes of the label groups, i.e., $\mathbf{g} = (2,2,4,2,4,2)$, shows that such a trellis has $N = 16$. We are also able to obtain a trellis of E_6^* with $N = 16$ by employing a permuted version of (5.4) with the order of basis vectors as $(1,3,2,5,4,6)$. The corresponding trellis of E_6^* is shown in Figure 5.8(b).

Note that by applying $\gamma(E_6) = 1.665$ and $\gamma(E_6^*) = 1.601$ to (4.7), we obtain $N(E_6, B) \geq 5$ and $N(E_6^*, B') \geq 5$, for any bases B and B' of E_6 and E_6^*, respectively. These lower bounds along with the lengths of nonzero vectors, and the determinants of E_6 and E_6^* are given in Table 5.1. In this table, we also have the new improved lower bound of 16 on the trellis complexity of these lattices. This bound is derived in the following theorem.

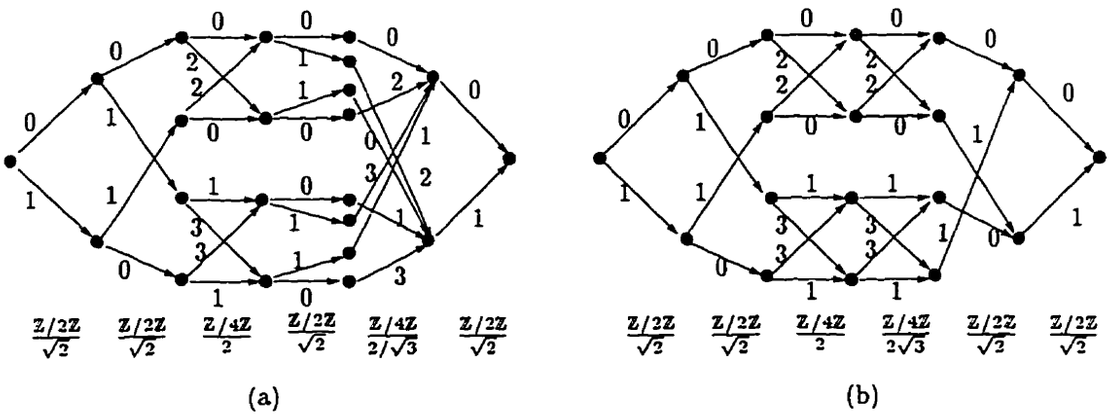

Figure 5.8: (a) A minimal trellis diagram of E_6. (b) A minimal trellis diagram of E_6^*.

Theorem 5.5 *For any trellis diagram of lattices E_6, and E_6^*, we have $N \geq 16$.*

Λ	Lengths of nonzero vectors	$\det(\Lambda)$	$\lceil \gamma^{n/2} \rceil$	New L. B.
E_6	$\sqrt{2}, 2, \sqrt{6}, \sqrt{8}, \sqrt{10}, \sqrt{12}, \sqrt{14}, \ldots$	$\sqrt{3}$	5	16
E_6^*	$2/\sqrt{3}, \sqrt{2}, \sqrt{10/3}, 2, 4/\sqrt{3}, \sqrt{6}, \sqrt{22/3}, \ldots$	$1/\sqrt{3}$	5	16

Table 5.1: Parameters of lattices E_6, and E_6^*, along with the old and new lower bounds on N.

Proof: For any orthogonal sublattice Λ' of E_6, let $\{\mathbf{b}'_1, \ldots, \mathbf{b}'_6\}$ denote the set of mutually orthogonal basis vectors of Λ'. By enumerating the number of basis vectors of length $\lambda(E_6) = \sqrt{2}$, we exhaust all the possibilities for the lengths of these vectors. Examination of the minimal vectors of E_6, given in [25, p. 126], shows that there exist at most four of them which are mutually orthogonal. We therefore start by the cases where four of the basis vectors have length $\sqrt{2}$. By examining the lengths of the vectors of E_6 given in Table 5.1, and using (4.6), we then conclude that for $\det(\Lambda')$ to be the smallest integer multiple of $\det(E_6) = \sqrt{3}$, the best choice for the lengths of the other two vectors is either $\sqrt{6}$ and $\sqrt{8}$, or 2 and $\sqrt{12}$. This results in $\det(\Lambda') \geq (\sqrt{2})^4(4\sqrt{3})$, which together with (2.12) gives $N \geq 16$.

It is not difficult to see that for $\det(E_6) = \sqrt{3}$ to divide $\det(\Lambda')$, there must be at least one basis vector $\mathbf{b}'_i$ of Λ' such that $\|\mathbf{b}'_i\| \geq \sqrt{6}$. For the cases where fewer than four of the basis vectors have length $\sqrt{2}$, this results in $\det(\Lambda') \geq (\sqrt{2})^3(2^2)\sqrt{6}$, and thus $N \geq 16$. This completes the proof of $N(E_6) \geq 16$.

For E_6^*, the result can be proved by just examining the lengths of the vectors of E_6^*, given in Table 5.1. It can be seen that for any orthogonal sublattice Λ' of E_6^*, there must be at least one of its mutually orthogonal basis vectors $\mathbf{b}'_i$ with $\|\mathbf{b}'_i\| \geq 2$. The reason is that it is not possible to select six numbers from the set

of numbers $\{2/\sqrt{3}, \sqrt{2}, \sqrt{10/3}\}$ such that their product forms an integer multiple of $\det(E_6^*) = 1/\sqrt{3}$. Moreover, for E_6^*, there is no orthogonal pair of the vectors of length $2/\sqrt{3}$. If there were, there would be at least one vector of length $2\sqrt{2}/\sqrt{3}$ in E_6^*. Based on these, we then conclude that $\det(\Lambda') \geq (2/\sqrt{3})(2)(\sqrt{2})^4 = 16/\sqrt{3}$, which results in $N(E_6^*) \geq 16$. □

Corollary 5.2 *The trellises of E_6, and E_6^* with $N = 16$, given in Figures 5.8(a) and (b), are minimal.*

5.5.2 Lattices E_7 and E_7^*

It is known that E_7 may be obtained by applying construction A [25, p. 137] to the little Hamming code $(7, 3, 4)$. This corresponds to the code formula $E_7 = 2\mathbb{Z}^7 + (7, 3, 4)$ and the following basis for E_7.

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{5.5}$$

It is then clear that $2\mathbb{Z}^7$ is a sublattice of E_7 with index 8, and therefore $N(E_7, H) \leq 8$, where H is the HNF of E_7. In fact since the G-S vectors of B are also along the coordinate system, we have $N(E_7, B) \leq 8$. On the other hand, applying $\gamma(E_7) = 2^{6/7}$ to Theorem 4.4 results in $N(E_7) \geq 8$, which means that the trellis of E_7 constructed based on (5.5) is a minimal trellis. This trellis is shown in Figure 5.9(a).

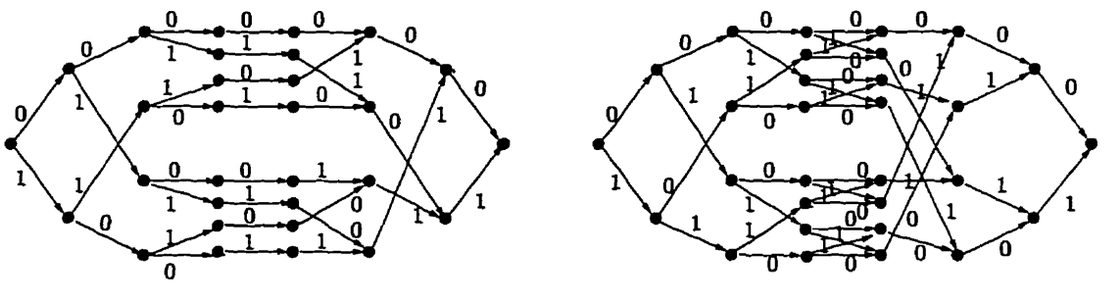

Figure 5.9: (a) A minimal trellis of E_7. (b) A minimal trellis of E_7^*.

Since an integral version of E_7 is a sublattice of E_7^* with index 2 [25, p. 125], the above result for E_7 indicates the existence of a trellis for E_7^* with at most 16 distinct paths. In fact, applying the result of Figure 5.9(a) to Theorem 4.2 implies that constructing a trellis of E_7^* based on its HNF results in $N = 16$. The HNF of E_7^* (as the dual of a version of E_7 with the basis $B/2$, where B is the matrix in (5.5)) is given below:

$$H = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{5.6}$$

The corresponding trellis is shown in Figure 5.9(b). This trellis demonstrates the code formula $E_7^* = 2\mathbb{Z}^7 + (7,4,3)$, where $(7,4,3)$ is the Hamming code. Note that for E_7^*, applying $\gamma = 1.656$ to (4.7) gives the lower bound of $N(E_7^*) \geq 6$. In the following, we tighten this lower bound, and prove that the obtained trellis for E_7^*

is in fact minimal.

Theorem 5.6 *For any trellis diagram of E_7^*, we have $N \geq 16$.*

Proof: Consider a version of E_7^* where the lengths of nonzero vectors in increasing order are equal to [25, p. 125]:

$$\sqrt{3/2}, \sqrt{2}, \sqrt{7/2}, 2, \sqrt{11/2}, \sqrt{6}, \sqrt{15/2}, \ldots .$$

This version has a determinant of $\det(E_7^*) = 1/\sqrt{2}$. Also let Λ' be an orthogonal sublattice of E_7^*. We first notice that there are not any two of the 56 minimal vectors of E_7^*, given in [25, p. 125], which are orthogonal. Thus we just need to discuss two cases where either only one of the basis vectors of Λ' has a length of $\lambda(E_7^*) = \sqrt{3/2}$, or none of the basis vectors has a length of $\sqrt{3/2}$. For the former case, examining the lengths of the vectors of E_7^*, and using the fact that $\det(\Lambda')$ must be an integer multiple of $\det(E_7^*) = 1/\sqrt{2}$, we conclude that there is at least one basis vector $\mathbf{b}_i'$ of Λ' with $\|\mathbf{b}_i'\| \geq \sqrt{6}$. This results in $\det(\Lambda') \geq (\sqrt{3/2})(\sqrt{6})(\sqrt{2})^5$, and therefore $N \geq 24$. For the latter case, it is easy to see that $\det(\Lambda') \geq (\sqrt{2})^7$, and thus $N \geq 16$. □

Corollary 5.3 *The trellis of E_7^* with $N = 16$, shown in Figure 5.9(b), is minimal.*

5.6 Lattices A_n

The lattice A_n, $n \geq 1$, is defined as an integral lattice by the following set of points:

$$A_n = \{(x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1} : x_0 + \cdots + x_n = 0\} . \tag{5.7}$$

The following basis matrix corresponds to the above definition [25, p. 109]:

$$B = \begin{pmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ . & . & . & . & \cdots & . & . \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{pmatrix}. \tag{5.8}$$

For this version of A_n, we have $\lambda = \sqrt{2}$, and $\det(A_n) = \sqrt{n+1}$. Based on Theorem 4.11, constructing a trellis diagram of A_n using a K-Z reduced basis results in $N \leq 2^{n(n-1)/2}$. There is however a big gap between this upper bound and the lower bound of Theorem 4.4, which is $N \geq 2^{n/2}(n+1)^{-1/2}$. Using the basis B given in (5.8), we obtain a trellis with complexity $N(A_n, B) = n!$. In the following, we improve this result by permuting the basis vectors of matrix B, and obtain trellis diagrams with relatively small values of N. Table 5.2 contains the results for A_n, $n \leq 16$. The order of basis vectors is given in the second column. The information of the last column will be used in Section 5.7. From Table 5.2, it is clear that the obtained trellises for lattices $A_1 \cong \mathbb{Z}$, A_2, and $A_3 \cong D_3$ are minimal.

Example 5.4 *The trellis diagrams of A_4 and A_5 constructed based on the bases given in Table* 5.2 *are shown in Figure* 5.10. *Later in this section, we will prove that both of these trellises are minimal.*

It can be seen that for the above version of lattices A_n, $n > 3$, the lengths of nonzero vectors in increasing order are:

$$\sqrt{2}, 2, \sqrt{6}, \sqrt{8}, \sqrt{10}, \sqrt{12}, \ldots .$$

The minimal vectors are all permutations of $(1, -1, 0, \ldots, 0)$, and the vectors with length 2 are all permutations of $(1, 1, -1, -1, 0, \ldots, 0)$. It is easy to see that for

Λ	Basis (B)	$N(\Lambda, B)$	$\lceil \gamma^{n/2} \rceil$	$\prod_{i=1}^{n} g_i$
A_1	(1)	1	1	1
A_2	(1, 2)	2	2	4
A_3	(1, 3, 2)	2	2	8
A_4	(1,3,2,4)	8	2	64
A_5	(1,3,2,5,4)	8	3	128
A_6	(1,3,2,5,4,6)	48	3	2,304
A_7	(1,3,2,7,5,6,4)	16	4	1,024
A_8	(1,2,4,6,5,8,7,3)	96	6	27,648
A_9	(1,3,2,5,7,6,4,9,8)	128	8	32,768
A_{10}	(1,2,4,6,5,8,10,9,7,3)	768	10	589,824
A_{11}	(1,3,2,7,9,5,4,11,10,8,6)	384	14	884,736
A_{12}	(1,3,5,2,7,6,11,9,8,12,10,4)	6912	18	47,775,744
A_{13}	(1,7,11,9,8,3,5,4,13,12,10,2,6)	3072	25	18,874,368
A_{14}	(1,2,5,9,13,4,3,14,7,8,11,10,6,12)	13824	33	573,308,928
A_{15}	(1,2,3,9,13,11,10,5,7,6,15,14,12,4,8)	6144	46	301,989,888
A_{16}	(1,2,6,4,16,10,12,8,5,14,9,13,7,11,3,15)	184320	63	33,973,862,400

Table 5.2: Basis matrices B, the number of distinct paths in the corresponding trellis $N(\Lambda, B)$, the lower bound $\lceil \gamma^{n/2} \rceil$ on N, and the product of the sizes of the label groups for A_n lattices ($n \leq 16$).

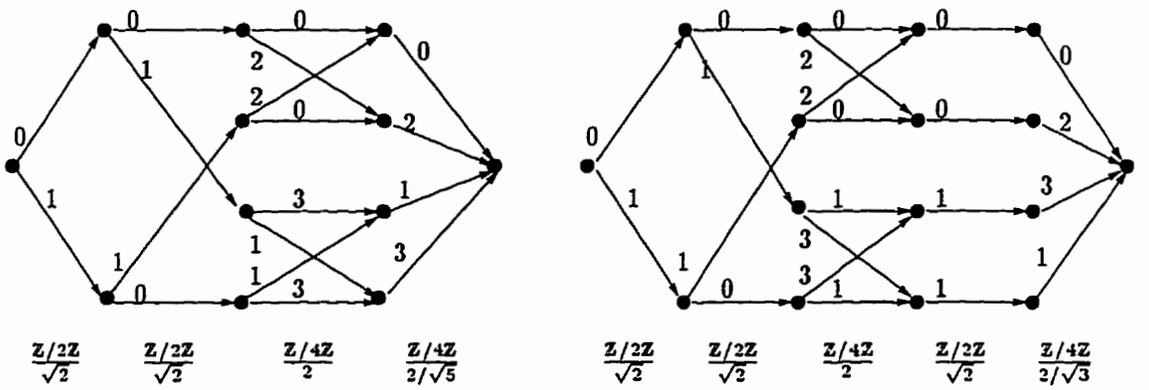

Figure 5.10: (a) A minimal trellis of A_4. (b) A minimal trellis of A_5.

two minimal vectors to be orthogonal, they cannot have any nonzero element in the same coordinate. Thus one can find at most $\lceil n/2 \rceil$ mutually orthogonal minimal vectors of A_n. The following theorem is an immediate result of this, and the fact that the next shortest vector of A_n has a length of at least 2.

Theorem 5.7 *The complexity N of any trellis diagram of lattices A_n satisfies*

$$N \geq \lceil \frac{2^{(3n-1)/4}}{(n+1)^{1/2}} \rceil . \tag{5.9}$$

Proof: Based on the above discussions, for any orthogonal sublattice Λ' of $A_n (n > 3)$, we have $\det(\Lambda') \geq 2^{3n/4}$, for n even, and $\det(\Lambda') \geq 2^{(3n-1)/4}$, for n odd. The proof then follows from this combined with (2.12), and the fact that the lower bound on $\det(\Lambda')$ for n odd is smaller than the one for n even. The lower bound of (5.9) is also achieved for minimal trellises of $A_n, n \leq 3$. □

Comparing the fraction in the lower bound of Theorem 5.7 with $\gamma^{n/2} = 2^{n/2}/(n+1)^{1/2}$ in (4.7) shows the improvement of the bound given in (5.9) over the one in (4.7).

For any specific value of $n > 3$, the lower bound of Theorem 5.7 can be improved using more elaborate discussions involving the arrangement of points of A_n. In the following theorem using enumeration methods, we perform this task for $4 \leq n \leq 9$.

Theorem 5.8 *Any trellis diagram of lattices A_n, $4 \leq n \leq 9$, satisfies $N(A_n) \geq L$, where L is given in Table 5.3.*

Proof: The proofs for A_4, A_5, and A_7 are simple and similar, while it is more complicated to prove the result for A_6, A_8, and A_9. For the sake of brevity, here we just give the proofs for A_4 and A_6.

For A_4, since there are at most 2 minimal vectors which are mutually orthogonal, we start the enumeration by considering the cases where two of the four mutually orthogonal basis vectors of an orthogonal sublattice Λ' have length $\sqrt{2}$. In these cases, for $\det(\Lambda')$ to be an integer multiple of $\det(A_4) = \sqrt{5}$, we need two more vectors of A_4 with the product of their lengths equal to an integer multiple of $\sqrt{5}$. The best choice for the lengths which minimizes $\det(\Lambda')$ is either $\sqrt{8}$ and $\sqrt{10}$, or 2 and $\sqrt{20}$, both resulting in $N \geq 8$. Clearly, for $\det(A_4) = \sqrt{5}$ to divide $\det(\Lambda')$, Λ' must have a basis vector of length at least $\sqrt{10}$. For the cases where fewer than two of the basis vectors have length $\sqrt{2}$, this results in $\det(\Lambda') \geq (\sqrt{2})(2^2)(\sqrt{10})$, and thus $N \geq 8$.

For A_6, to apply the enumeration method, we need the arrangement of vectors on the first few shells of the lattice. It can be seen that the vectors of A_6 with norm $\sqrt{6}$ are all permutations of

$$\pm(2,-1,-1,0,0,0,0), \text{ and } (1,1,1,-1,-1,-1,0),$$

the vectors with norm $\sqrt{8}$ are all permutations of

$$(2,-2,0,0,0,0,0), \text{ and } \pm(2,1,-1,-1,-1,0,0),$$

Lattice (Λ)	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9
$\lceil\gamma(\Lambda)^{n/2}\rceil$	1	2	2	2	3	4	4	6	8
L				8	8	48	16	96	128
$\{m,k\}$		$\{1,0\}$	$\{1,1\}$	$\{3,0\}$	$\{3,1\}$	$\{5,0\}$ $\{3,2\}$	$\{3,3\}$	$\{5,2\}$	$\{7,1\}$

Table 5.3: New (L) and old ($\lceil\gamma(\Lambda)^{n/2}\rceil$) lower bounds on $N(A_n)$, $n \leq 9$, along with the parameters m and k of the proposed algorithm for minimal trellises of A_n.

the vectors with norm $\sqrt{10}$ are all permutations of

$$(2,1,-2,-1,0,0,0), \text{ and } \pm(2,1,1,-1,-1,-1,-1),$$

and finally the vectors with norm $\sqrt{14}$ are all permutations of

$$\pm(3,-2,-1,0,0,0,0),\ \pm(2,2,-2,-1,-1,0,0), \text{ and } \pm(3,1,-1,-1,-1,-1,0).$$

We first enumerate all the possibilities based on the number of mutually orthogonal basis vectors of Λ' with length equal to $\lambda(A_6) = \sqrt{2}$.

a) 3 of the 6 vectors, say $\mathbf{b}'_1, \mathbf{b}'_2$, and $\mathbf{b}'_3$, have length $\sqrt{2}$: We continue by enumerating the possibilities for the number of 3 remaining orthogonal basis vectors with length 2. Examining the vectors of A_6 with lengths $\sqrt{2}$ and 2, it is not difficult to see that one cannot find two orthogonal vectors of length 2 which are orthogonal to 3 mutually orthogonal vectors of length $\sqrt{2}$. We thus need to only consider 2 cases. i) 1 vector, say $\mathbf{b}'_4$, has length 2: In this case, for $\det(\Lambda')$ to be an integer multiple of $\sqrt{7}$, we need two more vectors $\mathbf{b}'_5$ and $\mathbf{b}'_6$ of A_6 such that $\|\mathbf{b}'_5\| \geq \sqrt{6}$, $\|\mathbf{b}'_6\| \geq \sqrt{6}$, and $\|\mathbf{b}'_5\|\|\mathbf{b}'_6\|$ is an integer multiple of $\sqrt{14}$. Examining the vectors of A_6 with lengths $\sqrt{8}$, one realizes that none of them is orthogonal to 3 mutually orthogonal vectors of length $\sqrt{2}$. Also, it is not possible to find any vector of A_6 with length $\sqrt{14}$ which is orthogonal to 4 mutually orthogonal vectors with

lengths $\sqrt{2}, \sqrt{2}, \sqrt{2}$, and 2. Therefore the best choice for $\|\mathbf{b}'_5\|$ and $\|\mathbf{b}'_6\|$ which minimizes $\det(\Lambda')$ is either $\sqrt{18}$ and $\sqrt{28}$, or $\sqrt{12}$ and $\sqrt{42}$, or $\sqrt{6}$ and $\sqrt{84}$. All choices result in $N \geq 48$. **ii)** no vector has length 2: For these cases, we have $\|\mathbf{b}'_4\| \geq \sqrt{6}, \|\mathbf{b}'_5\| \geq \sqrt{6}$, $\|\mathbf{b}'_6\| \geq \sqrt{6}$, and $\|\mathbf{b}'_4\|\|\mathbf{b}'_5\|\|\mathbf{b}'_6\|$ must be an integer multiple of $\sqrt{14}$. Examining the vectors of A_6 with length $\sqrt{6}$ reveals that one cannot find two of them which are orthogonal to each other and also to $\mathbf{b}'_1, \mathbf{b}'_2$, and $\mathbf{b}'_3$. For the cases with just one vector, say $\mathbf{b}'_4$, with length $\sqrt{6}$, the best choice for $\|\mathbf{b}'_5\|$ and $\|\mathbf{b}'_6\|$ to minimize $\det(\Lambda')$, as an integer multiple of $\sqrt{7}$, is either $\sqrt{14}$ and $\sqrt{24}$, or $\sqrt{12}$ and $\sqrt{28}$, or $\sqrt{8}$ and $\sqrt{42}$ (we already saw that this last case is impossible due to orthogonality conditions). All choices result in $N \geq 48$. For the cases with no vector of length $\sqrt{6}$, we need to consider vectors $\mathbf{b}'_4, \mathbf{b}'_5$, and $\mathbf{b}'_6$ of A_6 such that $\|\mathbf{b}'_4\| \geq \sqrt{8}, \|\mathbf{b}'_5\| \geq \sqrt{8}$, $\|\mathbf{b}'_6\| \geq \sqrt{8}$, and $\|\mathbf{b}'_4\|\|\mathbf{b}'_5\|\|\mathbf{b}'_6\|$ is an integer multiple of $\sqrt{14}$. Based on the orthogonality conditions, none of the lengths $\|\mathbf{b}'_4\|, \|\mathbf{b}'_5\|$, or $\|\mathbf{b}'_6\|$ can be equal to $\sqrt{8}$. It is not also possible to have two orthogonal vectors of length $\sqrt{10}$ which are orthogonal to $\mathbf{b}'_1, \mathbf{b}'_2$, and $\mathbf{b}'_3$. The best choice is therefore to have $\|\mathbf{b}'_4\| = \|\mathbf{b}'_5\| = \sqrt{12}$, and $\|\mathbf{b}'_6\| = \sqrt{14}$. This results in $N \geq 48$.

b) 2 of the vectors have length $\sqrt{2}$: For $\sqrt{7}$ to divide $\det(\Lambda')$, we need 4 more vectors with the product of their lengths equal to an integer multiple of $\sqrt{7}$. We enumerate on the number of vectors with length 2. One cannot find 2 orthogonal vectors of A_6 with length 2 which are also orthogonal to 2 vectors of length $\sqrt{2}$. We thus need to consider two cases. **i)** one vector has length 2: In this case, it can be seen that the best situation for minimizing $\det(\Lambda')$, as an integer multiple of $\sqrt{7}$, happens if the 3 remaining vectors have either lengths $\sqrt{6}$, $\sqrt{6}$, and $\sqrt{28}$, or lengths $\sqrt{6}$, $\sqrt{12}$, and $\sqrt{14}$. Both cases result in $N \geq 48$. **ii)** none of the vectors has length 2: The best selection for the lengths of the 4 remaining vectors is $\sqrt{6}$, $\sqrt{6}$, $\sqrt{8}$, and $\sqrt{14}$, which results in $N \geq 48$.

c) Only one vector has length $\sqrt{2}$: We need 5 more mutually orthogonal vectors with the product of their lengths equal to an integer multiple of $\sqrt{14}$, and also orthogonal to the first vector. We enumerate on the number of vectors of length 2. It can be seen that there exist at most 3 mutually orthogonal vectors of length 2 in A_6. We therefore consider the following cases. **i)** 3 vectors have length 2: The best choice for the lengths of the remaining 2 vectors is either 4 and $\sqrt{14}$, or $\sqrt{8}$ and $\sqrt{28}$. Both result in $N \geq 64$. **ii)** 2 vectors or fewer have length 2: For $\sqrt{7}$ to divide $\det(\Lambda')$, there must be at least one basis vector of length at least $\sqrt{14}$. We thus have $\det(\Lambda') \geq \sqrt{2}(2^2)(\sqrt{6})^2\sqrt{14}$, and therefore $N \geq 48$.
d) None of the vectors has length $\sqrt{2}$: Noticing the fact that there exist at most 3 mutually orthogonal vectors of length 2 in A_6, we have $\det(\Lambda') \geq (2^3)(\sqrt{6})^2\sqrt{14}$, and thus $N \geq 68$. □

The same methods can also be applied to the other A_n lattices to improve the lower bound of (5.9). However, by increasing the dimension, the number of enumeration steps required for having a tight lower bound is usually increased as well. This results in complex and lengthy discussions which are difficult to handle.

Corollary 5.4 *The trellis diagrams constructed based on the bases given in Table* 5.2 *for* A_n, $4 \leq n \leq 9$, *with* $N = 8, 8, 48, 16, 96,$ *and* 128, *respectively, are minimal.*

Our results on the minimal trellises of $A_n, n \leq 9$, surprisingly suggest that, unlike lattices BW_n, D_n, and D_n^*, it is not likely to find a general structure for the minimal trellis diagrams of all A_n lattices. However, in the following, we propose an efficient systematic algorithm for finding low-complexity trellises for A_n lattices (arbitrary n). The algorithm results in minimal trellises for $n \leq 9$.

The algorithm for trellis construction

Let $n-1=m+k$, for $n \geq 2$, where m and k are non-negative integer numbers. Suppose that lattices A_m and A_k, $m,k \neq 0$, have orthogonal sublattices Λ'_m and Λ'_k with basis vectors $\mathbf{v}_1,\ldots,\mathbf{v}_m$, and $\mathbf{w}_1,\ldots,\mathbf{w}_k$, respectively, where the vectors in each set are mutually orthogonal. Also, for the sake of simple representation, let $A_0=\{\,\}$ be an imaginary lattice with no basis vector. Using the definition (5.7), one can see that the following n mutually orthogonal vectors belong to A_n:

$$\begin{array}{lllllllll}
\mathbf{y}_1 & = (& v_{1,1}\,, & \ldots & , v_{1,m+1} & ; & 0\,, & \ldots & , 0 \quad) \\
 & & & \cdot & & & & \cdot & \\
\mathbf{y}_m & = (& v_{m,1}\,, & \ldots & , v_{m,m+1} & ; & 0\,, & \ldots & , 0 \quad) \\
\mathbf{y}_{m+1} & = (& 0\,, & \ldots & , 0 \quad & ; & w_{1,1}\,, & \ldots & , w_{1,k+1} \quad) \\
 & & & \cdot & & & & \cdot & \\
\mathbf{y}_{n-1} & = (& 0\,, & \ldots & , 0 \quad & ; & w_{k,1}\,, & \ldots & , w_{k,k+1} \quad) \\
\mathbf{y}_n & = (& t\,, & \ldots & , t \quad & ; & -s\,, & \ldots & , -s \quad)\,,
\end{array} \tag{5.10}$$

where $t=(k+1)/g$, $s=(m+1)/g$, and g is the greatest common divisor of $m+1$ and $k+1$. Now, let N_m and N_k be the complexity of trellises constructed based on the quotient groups A_m/Λ'_m and A_k/Λ'_k, respectively ($N_0 \triangleq 1$). We therefore have $N_m = \det(\Lambda'_m)/\sqrt{m+1} = (\prod_{i=1}^{m}\|\mathbf{v}_i\|)/\sqrt{m+1}$, and $N_k = (\prod_{i=1}^{k}\|\mathbf{w}_i\|)/\sqrt{k+1}$. Considering the orthogonal sublattice Λ'_n of A_n with the vectors in (5.10) as its basis vectors, we obtain $\det(\Lambda'_n) = (\prod_{i=1}^{m}\|\mathbf{v}_i\|)(\prod_{i=1}^{k}\|\mathbf{w}_i\|)\|\mathbf{y}_n\|$. Constructing a trellis of $A_n, n=m+k+1$, based on A_n/Λ'_n, we thus see that if A_m and A_k have trellises with complexity N_m and N_k, respectively, then it is always possible to have a trellis of A_n with the following complexity

$$N_n = \frac{\det(\Lambda'_n)}{\sqrt{n+1}} = N_m N_k \left[\frac{(mk+n)\{(k+1)s^2+(m+1)t^2\}}{n+1}\right]^{1/2} = N_m N_k \left(\frac{mk+n}{g}\right). \tag{5.11}$$

Lattice (Λ)	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A_{16}
N in Table 5.2	768	384	6912	3072	13324	6144	184320
New N	768	256	3072	3072	6144	2048	32768
$\{m,k\}$	$\{7,2\}$	$\{7,3\}$	$\{11,0\}$	$\{11,1\}$ $\{7,5\}$	$\{11,2\}$	$\{7,7\}$	$\{15,0\}$

Table 5.4: Old and new values of $N(A_n)$, $10 \leq n \leq 16$, along with the corresponding parameters m, k, in the proposed algorithm.

Now, starting from $n = 2$, and using the facts that A_1 has a minimal trellis with $N_1 = 1$ and that the corresponding sublattice Λ_1' has a basis vector $(1, -1)$, the algorithm finds a trellis of A_2 with complexity $N_2 = 2$, based on the only possibility $\{m, k\} = \{1, 0\}$ which satisfies $m + k = 1$ in the above construction. The corresponding orthogonal sublattice Λ_2' has the mutually orthogonal basis vectors $\mathbf{y}_1 = (1, -1, 0)$, and $\mathbf{y}_2 = (1, 1, -2)$. Similarly, by increasing n by one in each step, the algorithm continues to find a trellis for each A_n, $n > 2$, by enumerating all the $\lfloor (n+1)/2 \rfloor$ possible combinations for m and k in $m + k = n - 1$, and selecting the smallest N_n in (5.11). The corresponding mutually orthogonal basis vectors of Λ_n' are obtained easily based on (5.10), and using the (previously found) results for smaller values of n.

It can be seen that the above algorithm results in the minimal trellises for $n \leq 9$. The corresponding parameters m and k are given in Table 5.3. For $10 \leq n \leq 16$. the results of the algorithm along with the results obtained in Table 5.2 are listed in Table 5.4. One can see the improvement of the former over the latter for values of $n = 11, 12, 14, 15$, and 16. As for the other values of n, it can be proved that the log-complexity ($\log_2 N$) of the trellises obtained by the algorithm is upper bounded

by $(n\log_2 n)/2 + O(n)$. The proof is similar, but more tedious than the proof given below for Theorem 5.9. Note that based on (5.9), the log-complexity of any trellis diagram of A_n is lower bounded by $3n/4+O(\log n)$. The upper bound on complexity can be improved for the special case of $n = 2^p - 1$, where p is a positive integer, or more generally for $n = 2^{p_1} + 2^{p_2} - 1$, where p_1, p_2 are non-negative integers.

Theorem 5.9 *The complexity N_n of the trellis of A_n, $n = 2^p - 1$, $p \in \mathbb{Z}^+$, obtained by the proposed algorithm, satisfies*

$$N_n \leq \frac{2^n}{n+1}. \tag{5.12}$$

Proof: Choosing $m = k = (n-1)/2$ in the algorithm, and using (5.11), we have $N_n \leq N^2_{(n-1)/2}(n+1)/2$. Now since $(n-1)/2 = 2^{p-1} - 1$, $N_{(n-1)/2}$ can also be upper bounded in a similar way. Applying the same procedure $p-1$ times ($p \geq 2$) iteratively, we obtain

$$N_n \leq N_1^{2^{p-1}} \left(\frac{n+1}{2}\right)\left(\frac{n+1}{2^2}\right)^2 \cdots \left(\frac{n+1}{2^{p-1}}\right)^{2^{p-2}} = 2^{2^p - p - 1} = \frac{2^n}{n+1},$$

where at the second last step, we have used $N_1 = 1$, $n+1 = 2^p$, and the arithmetic-geometric series expression for the exponent of 2. It is also easy to see that (5.12) is satisfied for $n = p = 1$. □

The upper bound of (5.12) is quite tight. It is achieved for all the values of n in the form of $2^p - 1$, given in Tables 5.3 and 5.4, i.e., $n = 1, 3, 7, 15$. In fact, using similar methods as those employed in Theorem 5.8, we have been able to prove that the corresponding trellis of A_{15} with $N = 2048$ is minimal (we already saw that the obtained trellises for A_1, A_3, and A_7 are also minimal). This along with the small gap between the upper bound of (5.12) and the lower bound of (5.9) has led us to

conjecture that the algorithm results in minimal trellises for A_n, $n = 2^p - 1$, with complexity $N_n = 2^n/(n+1)$.

As a corollary of Theorem 5.9, we obtain a tight upper bound on the trellis complexity of a more general category of A_n lattices.

Corollary 5.5 *The complexity N_n of the trellis of A_n, $n = 2^{p_1} + 2^{p_2} - 1$, $p_1, p_2 \in \mathbb{Z}^+ \cup \{0\}$, and $p_1 \leq p_2$, obtained by the proposed algorithm, satisfies*

$$N_n \leq 2^{n-p_1-1} . \tag{5.13}$$

Proof: The result is proved by choosing $m = 2^{p_1} - 1$, and $k = 2^{p_2} - 1$, in the algorithm, and applying the result of Theorem 5.9 to (5.11) either for both N_m and N_k, when $p_1, p_2 \geq 1$; or for just N_k, when $p_1 = 0, p_2 \geq 1$. Inequality (5.13) also holds for $n = 1$ ($p_1 = p_2 = 0$). □

Note that (5.13) reduces to (5.12) for $n = 2^p - 1, p \in \mathbb{Z}^+$. The bound of Corollary 5.5 is achieved for $n = 1, 2, 3, 4, 5, 7, 9, 11, 15$, and 16, as can be checked using Tables 5.3, and 5.4. Since $p_1 \geq 0$, it also results in $N_n \leq 2^{n-1}$.

5.7 Lattices A_n^*

The lattice A_n^*, $n \geq 1$, is defined as

$$A_n^* = \{\mathbf{x} = (x_0, \ldots, x_n) : \sum_{i=0}^{n} x_i = 0;\ \mathbf{x} \cdot \mathbf{v} \in \mathbb{Z},\ \forall \mathbf{v} \in A_n\} , \tag{5.14}$$

where A_n has the definition of (5.7). The corresponding basis matrix has been given in (3.1). For this version of A_n^*, we have $\lambda = \sqrt{n/(n+1)}$, and $\det(A_n^*) = 1/\sqrt{n+1}$.

By constructing a trellis of A_n^* based on (3.1), we obtain $N(A_n^*, B) = n!$. However, by permuting the basis vectors, one can get a better result as explained in the following theorem.

Theorem 5.10 *Let* $\tilde{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_{\lfloor n/2 \rfloor}, \mathbf{b}_n, \mathbf{b}_{\lfloor n/2 \rfloor + 1}, \mathbf{b}_{\lfloor n/2 \rfloor + 2}, \ldots, \mathbf{b}_{n-1})$ *be a basis of* A_n^* *obtained from* (3.1) *by permuting its basis vectors. Then* $N(A_n^*, \tilde{B}) = (\lfloor \frac{n+1}{2} \rfloor)!(\lceil \frac{n+1}{2} \rceil)!$.

Proof: Using a method similar to the proof of Theorem 5.3, it can be proved that for the trellis constructed based on $\tilde{B}$, we have $N(A_n^*) = N(A_{n-1}^*)\lceil \frac{n+1}{2} \rceil$. Combining this with the initial condition of $N(A_1^*) = 1$ completes the proof. □

Note that for $n \leq 8$, Theorem 5.10 gives the best result achievable by permuting the basis vectors of (3.1) (all the permutations are tested). For $A_1^* \cong \mathbb{Z}$ and $A_2^* \cong A_2$, the basis of Theorem 5.10 results in a minimal trellis. For A_3^*, the result of this Theorem, which is $N(A_3^*, \tilde{B}) = 4$, can be improved by noticing that $A_3^* \cong D_3^*$, and that the minimal trellis of D_3^* has two distinct paths.

For larger values of n, the result of Theorem 5.10 can be improved by applying the results of Table 5.2 or those of Tables 5.3 and 5.4 (corresponding to the trellis coordinate system of (5.10)) to Theorem 4.2. If A_n has a trellis with $N(A_n)$ distinct paths and label groups with sizes $g_i, i = 1, \ldots, n$, then A_n^* will have a trellis with $(\prod_{i=1}^n g_i)/N(A_n)$ distinct paths (in the same trellis coordinate system). It appears that although for $4 \leq n \leq 10$ and $n = 13$, the coordinates of Table 5.2 and those of Tables 5.3 and 5.4 result in the same $N(A_n^*)$, for the other values of n, the latter results in a smaller $N(A_n^*)$. The best obtained results based on this method are listed in Table 5.5 for $4 \leq n \leq 16$.

It has been tested that the results of Table 5.5 are the best for $n \leq 7$, in the sense that they are the minimum values of $(\prod_{i=1}^n g_i)/N(A_n)$ over all the permutations of

n	$N(A_n^*)$	$\lceil \gamma^{n/2} \rceil$
4	8	2
5	16	2
6	48	2
7	64	2
8	288	2
9	256	2
10	768	3
11	1024	3
12	3072	3
13	6144	3
14	18432	3
15	16384	3
16	32768	3

Table 5.5: Number of distinct paths in the trellis of A_n^*, $4 \leq n \leq 16$, in the same (trellis) coordinate system as the one given in Tables 5.3 and 5.4 for the corresponding A_n.

basis vectors in (5.8). However, for $n = 8$, we are able to find a trellis for A_8^* with $N = 128$. To see this, we notice that a permuted version of (5.8), that is $(\mathbf{b}_1, \mathbf{b}_3, \mathbf{b}_2, \mathbf{b}_5, \mathbf{b}_7, \mathbf{b}_6, \mathbf{b}_4, \mathbf{b}_8)$, results in a trellis with $N = 128$ and $\prod_{i=1}^{8} g_i = 128^2$ for A_8. Combining this with Theorem 4.2 shows that A_8^* has a trellis with $N = 128$ in the same trellis coordinate system. For the other values of $9 \leq n \leq 16$, we have not been able to improve the results of Table 5.5 by this method.

Note that there is also a big gap between the obtained results and the lower bounds of Corollary 4.5, listed in Table 5.5 as well. Later on, in Theorem 5.11, we prove that the obtained trellises for A_4^*, A_5^*, A_6^*, and A_9^*, are minimal. Also for A_7^* and A_8^*, improving the results of Table 5.5, we find (trellis) coordinate systems which result in minimal trellises.

Example 5.5 *Minimal trellises for A_4^* and A_5^* are shown in Figures* 5.11(a) *and* (*b*), *respectively. The trellises are obtained in the same coordinate systems as the ones given in Table* 5.2 *for minimal trellises of A_4 and A_5. The corresponding basis matrices are:*

$$B_{A_4^*} = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{-4}{5} & \frac{1}{5} \end{pmatrix}, \quad B_{A_5^*} = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ \frac{3}{2} & \frac{-1}{2} & \frac{-1}{2} & \frac{-1}{2} & \frac{-1}{2} & \frac{1}{2} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{-5}{6} & \frac{1}{6} & \frac{1}{6} \end{pmatrix}.$$

Note that, as expected, the trellises of Figure 5.11 *have the same state and label complexity profiles as those of Figure* 5.10.

Theorem 5.11 *Minimal trellis diagrams of lattices A_n^*, $4 \leq n \leq 9$, have complexities $N = 8, 16, 48, 32, 48,$ and 256, respectively.*

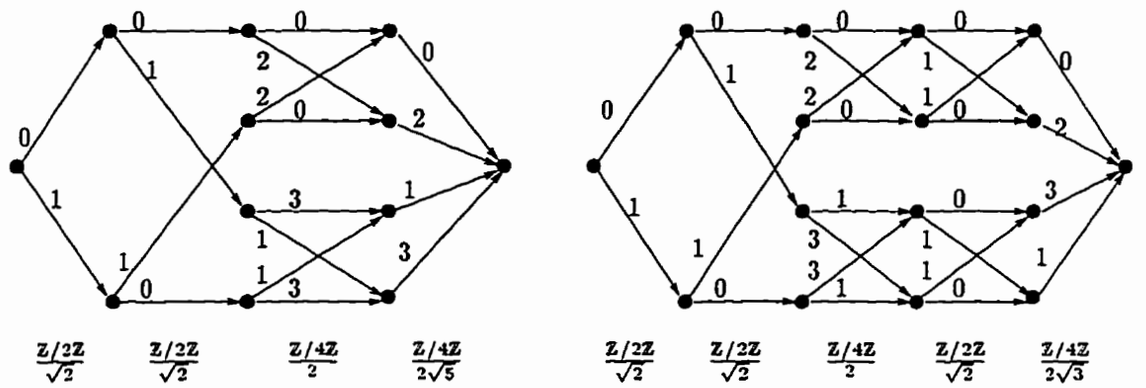

Figure 5.11: (a) A minimal trellis of A_4^*. (b) A minimal trellis of A_5^*.

Proof: The proof is based on direct enumeration of lattice points on the first few shells of A_n^* lattices. On these shells, we search for a set of n mutually orthogonal vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_n$, which minimizes $\det(\Lambda') = \prod_{i=1}^{n} \|\mathbf{b}'_i\|$. To proceed, we need the general forms of the vectors on the shells. Let $\mathbf{x} \in A_n^*$. It can be seen, based on the definition (5.14), that if at least one of the coordinates of $\mathbf{x}$ is zero, then all the coordinates must be integer, and therefore $\mathbf{x} \in A_n$. Knowing the forms of the vectors of A_n, we then continue by listing the vectors of A_n^* in the form of $\mathbf{x} = \mathbf{z}/(n+1)$, and with $\|\mathbf{x}\| \leq M$, where $\mathbf{z} \in \mathbb{Z}^{n+1}$ has no zero coordinates, and M is the distance from the origin of the furthest shell which we are interested in. This "listing process" is performed based on the definition (5.14), and by sequentially checking the cases where $n+1, n, n-1, \ldots, 1$, and 0 of the coordinates of $\mathbf{z}$ are ± 1, and selecting those which result in $\|\mathbf{x}\| \leq M$. Then for the cases where none of the coordinates is ± 1, we continue by checking the instances with $n+1, n, n-1, \ldots, 1$, and 0 of the coordinates of $\mathbf{z}$ equal to ± 2, and so on. The process is stopped for $\pm p$, where p is the smallest integer which satisfies $p > M/\sqrt{n+1}$.

Using the general forms of the vectors, we are then able to study their orthogonality. The resulting knowledge along with the fact that $\det(\Lambda')$ must be an integer multiple of $1/\sqrt{n+1}$, enables us to both obtain orthogonal sublattices Λ' with minimum determinant, and prove their minimality. In the following, we only prove the result for A_4^*. The other proofs are similar, but more tedious.

The lengths of nonzero vectors of A_4^* in increasing order are:

$$2/\sqrt{5}, \sqrt{6/5}, \sqrt{2}, \sqrt{14/5}, 4/\sqrt{5}, 2, \sqrt{24/5}, \ldots .$$

The vectors on the first three shells are all permutations of $\pm(-\frac{4}{5}, \frac{1}{5}^4)$, $\pm(-\frac{3}{5}^2, \frac{2}{5}^3)$, and $(1, -1, 0^3)$, respectively. It can be seen that no pair of vectors from the first two shells are orthogonal. Starting by enumerating the number of vectors of length $2/\sqrt{5}$, we therefore need to consider two cases: a) Only one of the 4 mutually orthogonal vectors has length $2/\sqrt{5}$: We need 3 more vectors which are longer than $\sqrt{6/5}$, with the product of their lengths equal to an integer. All three vectors thus cannot have a length of $\sqrt{2}$. It is possible to have 2 vectors of length $\sqrt{2}$ which are orthogonal to the first vector. In this case, the next smallest integer length is 2, and one can easily find a vector of length 2 which is orthogonal to all the three previously selected vectors (see Table 5.6). This results in $N = 8$. For the cases with fewer than 2 vectors of length $\sqrt{2}$, we have $\det(\Lambda') \geq (2/\sqrt{5})\sqrt{2}(\sqrt{14/5})^2$, and therefore $N \geq 8$. b) None of the vectors has length $2/\sqrt{5}$: If one vector has length $\sqrt{6/5}$, since the product of the lengths must be an integer multiple of $1/\sqrt{5}$, the other three cannot all have a length of $\sqrt{2}$. Thus $\det(\Lambda') \geq (\sqrt{6/5})(\sqrt{2})^2(\sqrt{14/5})$, and $N \geq 9$. If none of the vectors has length $\sqrt{6/5}$, then clearly $\det(\Lambda') \geq (\sqrt{2})^4$, and therefore $N \geq 9$. □

The results of Theorem 5.11 along with the corresponding coordinate systems are given in Table 5.6.

A_n^*	N_{min}	n mutually orthogonal vectors which result in a minimal trellis
A_4^*	8	(−4/5, 1/5, 1/5, 1/5, 1/5), (0, −1, 1, 0, 0) (0, 0, 0, −1, 1), (0, −1, −1, 1, 1)
A_5^*	16	(−4/6, −4/6, 2/6, 2/6, 2/6, 2/6), (−1, 1, 0, 0, 0, 0) (0, 0, −1, 1, 0, 0), (0, 0, 0, 0, −1, 1) (0, 0, −1, −1, 1, 1)
A_6^*	48	(−6/7, 1/7, 1/7, 1/7, 1/7, 1/7, 1/7), (0, −1, 1, 0, 0, 0, 0) (0, 0, 0, −1, 1, 0, 0), (0, 0, 0, 0, 0, −1, 1) (0, 0, 0, −1, −1, 1, 1), (0, −2, −2, 1, 1, 1, 1)
A_7^*	32	(−1, 1, 0, 0, 0, 0, 0, 0) (0, 0, −1, 1, 0, 0, 0, 0) (0, 0, 0, 0, −1, 1, 0, 0) (0, 0, 0, 0, 0, 0, −1, 1) (−1/2, −1/2, −1/2, −1/2, 1/2, 1/2, 1/2, 1/2) (−1/2, −1/2, 1/2, 1/2, 1/2, 1/2, −1/2, −1/2) (1/2, 1/2, −1/2, −1/2, 1/2, 1/2, −1/2, −1/2)
A_8^*	48	(−1, 1, 0, 0, 0, 0, 0, 0, 0) (0, 0, −1, 1, 0, 0, 0, 0, 0) (0, 0, 0, 0, −1, 1, 0, 0, 0) (0, 0, 0, 0, 0, 0, −1, 1, 0) (3/9, 3/9, 3/9, 3/9, 3/9, 3/9, −6/9, −6/9, −6/9) (3/9, 3/9, 3/9, 3/9, −6/9, −6/9, 3/9, 3/9, −6/9) (3/9, 3/9, −6/9, −6/9, 3/9, 3/9, 3/9, 3/9, −6/9) (−6/9, −6/9, 3/9, 3/9, 3/9, 3/9, 3/9, 3/9, −6/9)
A_9^*	256	(−8/10, −8/10, 2/10, 2/10, 2/10, 2/10, 2/10, 2/10, 2/10, 2/10) (−1, 1, 0, 0, 0, 0, 0, 0, 0, 0) (0, 0, −1, 1, 0, 0, 0, 0, 0, 0) (0, 0, 0, 0, −1, 1, 0, 0, 0, 0) (0, 0, 0, 0, 0, 0, −1, 1, 0, 0) (0, 0, 0, 0, 0, 0, 0, 0, −1, 1) (0, 0, −1, −1, 1, 1, 0, 0, 0, 0) (0, 0, 0, 0, 0, 0, −1, −1, 1, 1) (0, 0, −1, −1, −1, −1, 1, 1, 1, 1)

Table 5.6: The complexity N_{min} of minimal trellises for A_n^*, $4 \leq n \leq 9$, and the corresponding trellis coordinate systems.

Example 5.6 *Let* $\mathbf{v}_1 = (0,0,0,-1,1)$, $\mathbf{v}_2 = (0,-1,1,0,0)$, $\mathbf{v}_3 = (0,-1,-1.1,1)$. *and* $\mathbf{v}_4 = (-4/5,1/5,1/5,1/5,1/5)$. *For* A_4^*, *based on Table* 5.6, *the trellis coordinate system* $\{W_i\}_{i=1}^4 = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ *results in a minimal trellis. It can be seen that this trellis is isomorphic to the trellis of Figure* 5.11(a), *and thus has the same state, edge, and label group complexities. However by permuting the coordinates to* $\{W_i\}_{i=1}^4 = \{\mathbf{v}_4, \mathbf{v}_2, \mathbf{v}_1, \mathbf{v}_3\}$, *we find another minimal trellis for* A_4^* *with the following parameters:* $\mathbf{s} = (1,4,8,4,1)$, $\mathbf{e} = (4,8,8,4)$, *and* $\mathbf{g} = (4,2,2,4)$. *Comparing these parameters with those of Figure* 5.11(a) *shows that this second trellis has higher state and edge complexities.*

Note that the results of Theorem 5.11 have a significant improvement over the lower bounds of (4.7). These results also suggest that it is unlikely to find a general structure for minimal trellis diagrams of A_n^* lattices. For larger values of n ($n > 9$), obtaining a minimal trellis by enumeration could be very difficult. One might prefer a simpler approach which results in a low-complexity trellis (without any guarantee for being minimal). As we observed before, one method is to use the same trellis coordinate system which results in a low-complexity trellis for A_n. In this case, using the fact that A_n is a sublattice of A_n^* with index $n+1$, we have $N(A_n^*) \leq (n+1)N(A_n)$. In fact, in the coordinate system (5.10),

$$N(A_n^*) = gN(A_n)\,, \tag{5.15}$$

and the bound can be improved to $N(A_n^*) \leq (n+1)N(A_n)/2$. The reason is that for A_n^*, the shortest vector in the direction of $\mathbf{y}_n$ in (5.10) is $g\mathbf{y}_n/(n+1)$, which has a length of at most $\|\mathbf{y}_n\|/2$.

Applying (5.11) to (5.15), we obtain

$$N(A_n^*) = (m+1)(k+1)N(A_m)N(A_k)\,. \tag{5.16}$$

This suggests minimizing $N(A_n^*)$ in the coordinate systems of the form (5.10) by checking different values of m and k which satisfy $m + k = n - 1$. We however, notice that this search does not improve the results of Table 5.5, except for A_8^*, where choosing $\{m, k\} = \{0, 7\}$ results in $N(A_8^*) = 128$.

Finally, for $n = 2^p - 1$, $p \geq 2$, the results of the above algorithm can be improved by selecting a trellis coordinate system consisting of the $q_1 = (n+1)/2$ vectors (if $q_1 \geq 4$)

$$
\begin{array}{l}
(\ 1, \ -1, \ 0, \ \ 0, \ 0, \ \ldots, \ 0, \ 0, \ \ 0 \ ), \\
(\ 0, \ \ 0, \ 1, \ -1, \ 0, \ \ldots, \ 0, \ 0, \ \ 0 \ ), \\
\qquad\qquad\qquad\qquad \ldots \\
(\ 0, \ \ 0, \ 0, \ \ 0, \ 0, \ \ldots, \ 0, \ 1, \ -1 \ ),
\end{array}
$$

the $q_2 = (n+1)/4$ vectors

$$
\begin{array}{l}
(\ 1^2, \ -1^2, \ 0^2, \ \ 0^2, \ 0^2, \ \ldots, \ 0^2, \ 0^2, \ \ 0^2 \ ), \\
(\ 0^2, \ \ 0^2, \ 1^2, \ -1^2, \ 0^2, \ \ldots, \ 0^2, \ 0^2, \ \ 0^2 \ ), \\
\qquad\qquad\qquad\qquad \ldots \\
(\ 0^2, \ \ 0^2, \ 0^2, \ \ 0^2, \ 0^2, \ \ldots, \ 0^2, \ 1^2, \ -1^2 \ ),
\end{array}
$$

the $q_3 = (n+1)/8$ vectors ..., the $q_{p-2} = 4$ vectors

$$
\begin{array}{l}
(\ 1^{\frac{n+1}{8}}, \ -1^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}} \ ), \\
(\ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 1^{\frac{n+1}{8}}, \ -1^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}} \ ), \\
(\ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 1^{\frac{n+1}{8}}, \ -1^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}} \ ), \\
(\ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 0^{\frac{n+1}{8}}, \ \ 0^{\frac{n+1}{8}}, \ 1^{\frac{n+1}{8}}, \ -1^{\frac{n+1}{8}} \ ),
\end{array}
$$

and the $q_{p-1} = 3$ vectors

$$
\begin{array}{l}
(\ \frac{1}{2}^{(n+1)/4}, \ \ \frac{1}{2}^{(n+1)/4}, \ -\frac{1}{2}^{(n+1)/4}, \ -\frac{1}{2}^{(n+1)/4} \ ), \\
(\ \frac{1}{2}^{(n+1)/4}, \ -\frac{1}{2}^{(n+1)/4}, \ \ \frac{1}{2}^{(n+1)/4}, \ -\frac{1}{2}^{(n+1)/4} \ ), \\
(\ \frac{1}{2}^{(n+1)/4}, \ -\frac{1}{2}^{(n+1)/4}, \ -\frac{1}{2}^{(n+1)/4}, \ \ \frac{1}{2}^{(n+1)/4} \ ).
\end{array}
$$

It is easy to see that all the above vectors belong to A_n^*, and are mutually orthogonal. It can be also seen that the complexity of the corresponding trellis is equal to

$$N(A_n^*) = 2^{n-2} . \tag{5.17}$$

For $n = 15$, this coordinate system results in $N = 8192$, which improves over $N = 16384$, obtained in the best coordinate system of the form (5.10). This method also results in minimal trellises for A_3^* and A_7^*.

It can be seen that the log-complexity of trellises obtained based on the above methods is upper bounded by $(n \log_2 n)/2 + O(n)$. Similar to the situation for A_n lattices, this bound can be improved for some specific values of n. This is illustrated in the following theorem.

Theorem 5.12 *Choosing the trellis with the lowest complexity among the trellises obtained by the above methods, the trellis complexity of A_n^* lattices satisfies*

$$\begin{aligned}
&N(A_n^*) \leq 2^{n-2} , && \text{for } n = 2^p - 1 , \\
&N(A_n^*) \leq 2^{n-1} , && \text{for } n = 2^{p_1} + 2^{p_2} - 1 , \\
&N(A_n^*) \leq n 2^{n-p_1-2} , && \text{for } n = 2^{p_1} + 2^{p_2} , \\
&N(A_n^*) \leq (n-1) 2^{n-p_1-2} , && \text{for } n = 2^{p_1} + 2^{p_2} + 1 , \\
&N(A_n^*) \leq 3(n-2) 2^{n-p_1-3} , && \text{for } n = 2^{p_1} + 2^{p_2} + 2 , \\
&\cdots && \cdots
\end{aligned}$$

where p, p_1, p_2 are non-negative integers, with $p \geq 2$, and $p_1 \leq p_2$.

Proof: The first inequality is a consequence of (5.17). The second inequality is obtained by choosing $\{m, k\} = \{2^{p_1} - 1, 2^{p_2} - 1\}$, and applying Theorem 5.9 to (5.16). The other inequalities are derived by choosing $\{m, k\} = \{0, n-1\}$,

$\{m,k\} = \{1, n-2\}$, $\{m,k\} = \{2, n-3\}$, ... in (5.16), respectively, and applying Corollary 5.5. □

Note that although $n = 2^p - 1$ is a special case of $n = 2^{p_1} + 2^{p_2} - 1$, the first inequality is stronger than the second inequality.

The bounds of Theorem 5.12 are tight. In fact, based on the obtained results, it can be seen that the bounds are attained for $n = 3, 7, 15$, $n = 1, 2, 4, 5, 8, 9, 11, 16$, $n = 2, 4, 6, 8, 12, 16$, $n = 5, 9, 13$, and $n = 6, 10, 14$, respectively. In the following, we also derive a tight lower bound on the trellis complexity of A_n^* lattices for a general value of n. The relatively small gap between the lower bound and the above upper bounds shows the satisfactory performance of the proposed algorithms in finding low-complexity trellises for A_n^*.

Theorem 5.13 *The complexity N of any trellis diagram of A_n^* lattices ($n \geq 4$) satisfies*

$$N \geq \lceil \sqrt{n} 2^{(n-1)/2} \rceil . \tag{5.18}$$

Proof: Since the complexity of minimal trellises for lattices A_n^*, $4 \leq n \leq 9$, satisfies the inequality, the result is proved for $n \leq 9$. It can be seen that for A_n^*, $n \geq 8$, the lengths of nonzero vectors in increasing order are:

$$\sqrt{\frac{n}{n+1}}, \sqrt{\frac{2(n-1)}{n+1}}, \sqrt{2}, \ldots .$$

The vectors on the first two shells are all permutations of $\pm(\frac{-n}{n+1}, \frac{1}{n+1}^n)$, and $\pm(-\frac{n-1}{n+1}^2, \frac{2}{n+1}^{n-1})$, respectively. It is not difficult to see that no pair of these vectors are orthogonal. We therefore have $N \geq \sqrt{n/(n+1)}(\sqrt{2})^{n-1}/\det(A_n^*) = \sqrt{n} 2^{(n-1)/2}$, and the proof is complete. □

Comparing the lower bound of (5.18) with $\gamma^{n/2} = \sqrt{n+1}(n/(n+1))^{n/2}$ shows the considerable improvement of the result given in Theorem 5.13 over the lower bound of (4.7). Also note that the result of Theorem 5.13 corresponds to a lower bound of $n/2 + O(\log n)$ on the log-complexity of any trellis of A_n^*.

5.8 Lattice K_{12}

The following matrix generates the Coxeter-Todd lattice K_{12} [25, p. 128]:

$$B = \begin{pmatrix}
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 0 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\
-\frac{1}{2} & 1 & -\frac{1}{2} & 0 & 1 & 0 & \frac{\sqrt{3}}{2} & 0 & \frac{\sqrt{3}}{2} & 0 & 0 & 0 \\
-\frac{1}{2} & -\frac{1}{2} & 1 & 0 & 0 & 1 & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -\sqrt{3} & 0 & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & 0 & -\frac{\sqrt{3}}{2} & 0 \\
\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} & -\frac{\sqrt{3}}{2} & 0 & 0 & -\frac{\sqrt{3}}{2}
\end{pmatrix}. \tag{5.19}$$

For this version, we have $\lambda = 2$, and $\det(K_{12}) = 27$, which results in $\gamma = 4/\sqrt{3}$. In [33], Forney has considered some trellis constructions of K_{12} as a complex E-lattice. To modify these trellises such that they represent K_{12} as a real lattice, each edge can be replaced by a properly labeled minimal trellis of A_2. The reason is that the set of *Eisenstein integers* E is the complex analog of the real hexagonal

lattice A_2. It is known that K_{12} contains A_2^6 as a sublattice of index 64 [24]. (This corresponds to the complex code formula of $K_{12} = 2E^6 + (6, 3, 4)$ given in [33]). This fact has been used to devise a decoding algorithm for K_{12} in [24]. It also shows that there exists a trellis of K_{12} with $N \leq 64 \times 2^6 = 4096$.

By permuting the rows of (5.19), we obtain a basis for K_{12} with the order of its vectors as $(1, 2, 3, 9, 7, 5, 8, 6, 12, 11, 10, 4)$ which results in a trellis with $N = 4096$. The sizes of the label groups in all trellis sections are 4, and the number of states in different levels of the trellis are $\mathbf{s} = (1, 4, 16, 64, 64, 64, 64, 64, 64, 16, 4, 4, 1)$. Note that for K_{12}, inequality (4.7) results in the lower bound of $N \geq 152$. This lower bound is improved in the following theorem.

Theorem 5.14 *For any trellis diagram of K_{12}, we have $N \geq 512$.*

Proof: Let Λ' be a 12-D orthogonal sublattice of K_{12}. We then proceed by enumerating the number of (mutually orthogonal) basis vectors of Λ' with their length equal to $\lambda(K_{12}) = 2$. For the above version of K_{12}, it can be seen that the lengths of nonzero vectors are [25, p. 129]:

$$2, \sqrt{6}, \sqrt{8}, \sqrt{10}, \sqrt{12}, \sqrt{14}, \ldots .$$

Combining this with the fact that $\det(\Lambda')$ must be an integer multiple of 27, we conclude that for all the cases where the number of basis vectors of length 2 is greater than 6, $\det(\Lambda') \geq (27)(1024)$, and therefore $N \geq 1024$. For the cases where exactly 6 or fewer than 6 of the basis vectors have length 2, we have $\det(\Lambda') \geq (2)^6(\sqrt{6})^6$, and thus $N \geq 512$. □

Note that in the above proof, we have only used the information regarding the lengths of the vectors of K_{12}. More elaborate arguments involving the arrangement of lattice vectors, and their orthogonality conditions can probably result in a tighter lower bound.

5.9 Conclusion

Low-complexity (in many cases minimal) trellis diagrams for some important lattices have been found. For BW_n, D_n, D_n^*, E_n, E_n^*, $(A_n, A_n^*,\ n \leq 9)$, and Λ_{24}, we have obtained basis matrices which result in minimal trellises. The number of distinct paths in some of these minimal trellises is much larger than $\lceil \gamma^{n/2} \rceil$. We have also concluded that, despite the case for BW_n, D_n and D_n^*, it is not likely to find a general structure for the minimal trellises of A_n and A_n^* lattices. We however, propose simple algorithms for finding low-complexity trellis diagrams of A_n and A_n^* in any given dimension n. Except for A_8^*, these algorithms result in minimal trellis diagrams for every other $n \leq 9$. Finally, based on the small gap between the derived upper and lower bounds on the complexity of the trellises obtained by the algorithms, and also the fact that many of these trellises are minimal for $n \leq 9$, we conjecture that many of them are also minimal for $n > 9$ (especially those for A_n).

Chapter 6

Some results on lattice theory

Covering radius, successive minima, and coding gain are important structural parameters of a lattice. In the following two sections, we derive inequalities which relate the covering radius of a lattice to its successive minima, and the coding gains of densest lattices in two successive dimensions together.

6.1 An upper bound on covering radius

The inhomogeneous minimum and successive minima of a convex body with respect to a lattice [37, pp. 123,124] play essential roles in the geometry of numbers. A well-known inequality connecting these parameters, for a bounded o-symmetric convex body K with respect to a lattice Λ in $\mathbb{R}^n$, is the following [41]:

$$\mu(K,\Lambda) \leq \frac{1}{2}\sum_{i=1}^{n} \lambda_i(K,\Lambda)\,, \tag{6.1}$$

where $\mu(K,\Lambda)$ and $\lambda_i(K,\Lambda)$ are the inhomogeneous minimum and the i-th successive minimum of the body K with respect to the lattice Λ, respectively. Inequality

(6.1) has been used by other researchers to derive upper bounds on $\mu(K,\Lambda)$ in terms of $\lambda_1(K,\Lambda)$ and the volume of the body K, [20], [65], [68]. Further classical results of this type are due to Mahler, Hlawka, Kneser, Birch and others, see [37, pp. 98-107].

In this work, we give an analogue of (6.1) for the case that K is the n-D unit sphere S_n centered at the origin. In this case, $\mu(S_n,\Lambda)$ and $\lambda_i(S_n,\Lambda)$ are the so-called covering radius and the i-th successive minimum of the lattice Λ, abbreviated by $\mu(\Lambda)$ and $\lambda_i(\Lambda)$, respectively. The derived bound which is tighter than (6.1) is given in the following Theorem. It is achieved only in the case of orthogonal lattices. Two alternate proofs, which are basically geometrical, are given.

Theorem 6.1 *The covering radius $\mu(\Lambda)$ of an n-D lattice Λ satisfies*

$$\mu(\Lambda) \leq \frac{1}{2}\sqrt{\sum_{i=1}^{n} \lambda_i(\Lambda)^2}\,, \tag{6.2}$$

where $\lambda_i(\Lambda)$ is the i-th successive minimum of Λ. The inequality holds with equality iff there exists an orthogonal basis for Λ.

Proof: As the first proof, we use Propositions 3.1 and 3.2 together with the fact that every lattice has a K-Z reduced basis. □

We also present an alternative proof for Theorem 6.1 which does not depend on the concept of basis reduction. To do so, we need the following fact from basic geometry of numbers [37, p. 19].

Proposition 6.1 *Let $\mathbf{y}_1,\ldots,\mathbf{y}_n$ be n independent points of a given n-D lattice Λ. Then there exists a basis $\mathbf{b}_1,\ldots,\mathbf{b}_n$ of Λ, such that*

$$\mathbf{y}_i \in L(\mathbf{b}_1,\ldots,\mathbf{b}_i) \quad \textit{for} \quad i = 1,\ldots,n\,.$$

Alternative proof: Define a sequence of lattices $\Lambda^{(i)}$, $i = 1, \ldots, n$, such that $\Lambda^{(1)} = \Lambda$, and $\Lambda^{(i+1)}$, $i = 1, \ldots, n-1$, is the orthogonal projection of $\Lambda^{(i)}$ to $span(\mathbf{v}_i)^\perp$, where $\mathbf{v}_i \in \Lambda^{(i)}$ satisfies $\|\mathbf{v}_i\| = \lambda(\Lambda^{(i)})$. We first prove that

$$\mu(\Lambda^{(i)})^2 \leq \frac{1}{4}\lambda(\Lambda^{(i)})^2 + \mu(\Lambda^{(i+1)})^2 \quad \text{for } i = 1, \ldots, n-1\,. \tag{6.3}$$

For any $\mathbf{w} \in span(\Lambda^{(i)})$, let $\mathbf{w} = \mathbf{w}' + \mathbf{w}''$, where $\mathbf{w}' \in span(\mathbf{v}_i)$ and $\mathbf{w}'' \in span(\mathbf{v}_i)^\perp$. Let $\mathbf{x} \in span(\Lambda^{(i)})$. By the definition of $\mu(\Lambda^{(i+1)})$, there exists $\mathbf{b} \in \Lambda^{(i)}$ such that $\|(\mathbf{x}-\mathbf{b})''\| \leq \mu(\Lambda^{(i+1)})$. There also exists an integer k such that $\|(\mathbf{x}-\mathbf{b})' - k\mathbf{v}_i\| \leq \lambda(\Lambda^{(i)})/2$. Therefore $\mathbf{u} \stackrel{\Delta}{=} \mathbf{b} + k\mathbf{v}_i$ is a point of the lattice $\Lambda^{(i)}$ satisfying

$$\begin{aligned} \|\mathbf{x}-\mathbf{u}\|^2 &= \|(\mathbf{x}-\mathbf{u})'\|^2 + \|(\mathbf{x}-\mathbf{u})''\|^2 = \|(\mathbf{x}-\mathbf{b})' - k\mathbf{v}_i\|^2 + \|(\mathbf{x}-\mathbf{b})''\|^2 \\ &\leq \tfrac{1}{4}\lambda(\Lambda^{(i)})^2 + \mu(\Lambda^{(i+1)})^2\,, \end{aligned}$$

which proves (6.3).

Starting from $i = 1$, by combining the inequalities in (6.3) successively, and using the fact that $\mu(\Lambda^{(n)}) = \frac{1}{2}\lambda(\Lambda^{(n)})$ for the 1-D lattice $\Lambda^{(n)}$, we obtain

$$\mu(\Lambda) \leq \frac{1}{2}\sqrt{\sum_{i=1}^{n} \lambda(\Lambda^{(i)})^2}\,. \tag{6.4}$$

By the same discussion as given in the proof of Proposition 3.1, we also have $\lambda(\Lambda^{(i)}) \leq \lambda_i(\Lambda)$. This combined with (6.4) proves (6.2).

Suppose that Λ has an orthogonal basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$. It is not difficult to see that arranging the basis vectors in order of increasing length, we obtain $\|\hat{\mathbf{b}}_i\| = \|\mathbf{b}_i\| = \lambda_i(\Lambda)$ for $i = 1, \ldots, n$. Combining this fact with Proposition 3.2, we have $\mu(\Lambda) = 1/2\sqrt{\sum_{i=1}^{n} \lambda_i(\Lambda)^2}$.

To prove the "only if" part, we note that if (6.2) holds with equality, then $\lambda(\Lambda^{(i)}) = \lambda_i(\Lambda)$, for all i, and for any set of vectors $\{\mathbf{v}_i : \mathbf{v}_i \in \Lambda^{(i)}, \|\mathbf{v}_i\| = \lambda(\Lambda^{(i)}) ; i = 1, \ldots, n-1\}$. This results in the fact that there exist mutually orthogonal vectors $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \Lambda$ such that $\|\mathbf{y}_i\| = \lambda_i(\Lambda), \forall i$. Applying Proposition 6.1 for successive values of i, starting from $i = 1$, and using the definition of successive minima along with the fact that $\mathbf{y}_i \perp \mathbf{y}_j$, for $i \neq j$, we conclude that there exists a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ for Λ such that $\mathbf{b}_i = \pm\mathbf{y}_i, \forall i$. □

For ESM-lattices, inequality (6.2) reduces to

$$\mu(\Lambda) \leq \frac{\sqrt{n}}{2}\lambda(\Lambda) . \tag{6.5}$$

Inequality (6.5) is satisfied with equality only for the cubic lattices which are equivalent to the lattice $\mathbb{Z}^n$. This results in a characterization of the $\mathbb{Z}^n$ lattice, i.e., $\mathbb{Z}^n$ is the only n-D ESM-lattice (up to equivalence) which satisfies (6.5) with equality, or equivalently, $\mathbb{Z}^n$ has the largest covering radius in the set of n-D ESM-lattices.

For an n-D ESM-lattice Λ, there is a well-known conjecture in the geometry of numbers which asserts that the covering radius $\mu(\Lambda)$ satisfies

$$\mu(\Lambda) \leq \frac{\sqrt{n}}{2}\det(\Lambda)^{1/n} . \tag{6.6}$$

This conjecture has only been proved for dimensions $n \leq 6$ (see [37, p. 617]). Selecting a K-Z reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ for an n-D ESM-lattice Λ, and using Proposition 3.1, we have $\det(\Lambda) = \prod_{i=1}^{n} \|\hat{\mathbf{b}}_i\| \leq \lambda(\Lambda)^n$. This indicates that the bound in (6.6) is tighter than the one in (6.5). The two bounds coincide for cubic lattices.

6.2 An inequality on Hermite's constants in successive dimensions

The problem of finding dense lattice packings (large γ) is of great importance in both mathematics and communications [37, pp. 385-411], [25, pp. 66-74]. The maximum value of γ in a given dimension n is denoted as γ_n, and is called Hermite's constant. The value of γ_n is known only for the dimensions $n \leq 8$ [37, p. 410]. It has never been proved that γ_n is an increasing function of n, although this is very likely to be true. In this work, we establish a lower bound on γ_n in terms of γ_{n-1} and n. The bound is derived using a densely constructed n-D lattice which is composed of parallel layers. Each layer is a translated version of a densest $(n-1)$-D lattice. The layers are placed such that the lattice points in one layer are orthogonally projected to the deep holes of the two adjacent layers. This, along with the proper adjustment of the spacing between the layers, helps to increase the coding gain.

In deriving the bound on γ_n, we make use of a lower bound on the covering radius of a lattice (μ) in terms of its minimum distance (λ) and dimension (n) which is due to Ryškov [64]. For large values of n, the derived bound on γ_n is improved through establishing a lower bound on μ in terms of λ and n which is tighter than Ryškov's bound (for $n > 42$).

It should also be noted that Mordell and Oppenheim, independent of each other, have obtained an upper bound of the form $(\gamma_{n-1})^{(n-1)/(n-2)}$ on γ_n, see [37, p. 376]. This, in conjunction with the lower bound presented here, provides a tight range for γ_n in terms of γ_{n-1}.

It is known how to build up a packing in $\mathbb{R}^n$ from a given lattice packing (corresponding to a lattice Λ) in $\mathbb{R}^{n-1}$ by extending the latter to a layer of spheres

in $\mathbb{R}^n$ (with centers at the points of Λ), and stacking congruent layers as densely as possible [50]-[53], [23]. In fact, it appears that the densest lattices in dimensions $n \leq 8$ have a layer structure, see e.g., [25, p. 164]. In the above construction, we call the lattice Λ the *base* for the resulting packing. As explained before, we select the base to be a densest $(n-1)$-D lattice. To preserve the lattice property, we form the successive layers by translating the base with a fixed n-D vector, called the *generator vector*, successively. The generator vector is selected such that the density (coding gain) of the resulting lattice is as large as possible.

6.2.1 Preliminaries

In the following, we give a simple proof for a lower bound on covering radius μ in terms of minimum distance λ which is helpful in following the rest of this work. The original proof, due to Ryškov [64], is more complicated and applies to a general uniform system of points. We need the following lemma from [64]:

Lemma 6.1 *The length of the smallest edge of an arbitrary n-D simplex located inside an n-D sphere of radius r is upper bounded by $[2(n+1)/n]^{1/2}r$. This bound is achieved only for a regular simplex inscribed in the sphere.*

Theorem 6.2 *For an n-D lattice Λ, we have*

$$\mu(\Lambda) \geq \sqrt{\frac{n}{2(n+1)}}\lambda(\Lambda)\,. \tag{6.7}$$

Proof: Consider a sphere $\mathcal{S}(\mathbf{v})$ of radius $\mu(\Lambda)$ centered at an arbitrary deep hole $\mathbf{v}$ of the lattice Λ. Since $\mathbf{v}$ is the common vertex of some adjacent n-D polytopes

(Voronoi cells of Λ), it is located at the intersection of at least n hyper-planes (which are the facets of the corresponding Voronoi cells). It is not then difficult to see that $\mathbf{v}$ is the deep hole corresponding to at least $n+1$ adjacent Voronoi cells. This means that there exist at least $n+1$ lattice points on the surface of $\mathcal{S}(\mathbf{v})$. Let the minimum distance between these points be denoted by d. We have $\lambda(\Lambda) \leq d$. Considering the aforementioned $n+1$ lattice points as the vertices of a simplex, and using Lemma 6.1, we obtain $d \leq [2(n+1)/n]^{1/2}\mu(\Lambda)$. Combining these inequalities proves the theorem. □

It is interesting to note that (6.7) is satisfied with equality for the densest one- and two-dimensional lattices, i.e., the integer lattice $\mathbb{Z}$ and the hexagonal lattice.

Inequality (6.7) could be also obtained by combining the upper bound on the density of packings given by Rogers (see [25, p. 19]), with the lower bound on the thickness of coverings due to Coxeter, Few and Rogers (C-F-R) (see [25, p. 40]).[1] It is clear from the above observation that by tightening either bound, one can improve the inequality given in (6.7). Rogers' bound is the best known bound for $n \leq 42$, [25, p. 20]. For $n > 42$, the Kabatiansky-Levenshtein (K-L) bound (see [25, pp. 264-265]) takes over [25, p. 20]. There does not, however, exist a simple expression for the K-L bound except for large values of n. Combining K-L and C-F-R bounds for large values of n, as given in [25, p. 19] and [25, p. 40], respectively, we obtain

$$\mu(\Lambda) \geq 0.7573 \left(\frac{n}{e\sqrt{e}}\right)^{1/n} \lambda(\Lambda)\,, \tag{6.8}$$

which is tighter than (6.7).

[1]Note that both of these results had been available quite a while before the publication of Ryškov's bound in [64].

6.2.2 Main result

Let Λ_b be an $(n-1)$-D lattice with basis $\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}$, where $\mathbf{b}_i = (b_{i,1}, \ldots, b_{i,n-1})$, and let $\mathbf{v} = (v_1, \ldots, v_{n-1})$ be a deep hole of Λ_b. We construct an n-D lattice Λ using the following generator matrix

$$B' = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n-1} & 0 \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n-1} & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ b_{n-1,1} & b_{n-1,2} & \cdots & b_{n-1,n-1} & 0 \\ v_1 & v_2 & \cdots & v_{n-1} & h \end{pmatrix},$$

where h is a properly selected positive number. It is easy to see that the lattice Λ has a layer structure with the base lattice Λ_b, and the generator vector $\mathbf{b}'_n = (v_1, \ldots, v_{n-1}, h)$. As we will see later, the selection of $\mathbf{v}$ as a deep hole helps to increase the coding gain (density) of Λ. It is easy to show that

$$\det(\Lambda) = h \det(\Lambda_b) . \tag{6.9}$$

To maximize the coding gain of Λ, we would like to select h as the smallest number such that $\lambda' \triangleq \lambda(\Lambda) = \lambda(\Lambda_b) \triangleq \lambda$. Choosing a proper value for h requires checking the distance between lattice points in different layers. The value of h also depends on the values of $\mu \triangleq \mu(\Lambda_b)$ and λ. We select Λ_b to be a densest $(n-1)$-D lattice, denoted by L_{n-1}. Since we do not know much about the structure of L_{n-1}, for a general value of n, we choose

$$h \geq \frac{\lambda}{2} . \tag{6.10}$$

This selection guarantees that, except for the lattice points in two adjacent layers, the distance between the other lattice points is at least λ. It is easy to see that the minimum distance between lattice points in two adjacent layers is $\sqrt{\mu^2 + h^2}$.

Therefore, to keep λ' equal to λ, we also need

$$h^2 \geq \lambda^2 - \mu^2 \,. \tag{6.11}$$

The value of h is selected as the smallest number satisfying both (6.10) and (6.11). The corresponding value is denoted by h_0. We have

$$h_0 = \begin{cases} \sqrt{\lambda^2 - \mu^2} & \text{if } \mu \leq \frac{\sqrt{3}}{2}\lambda, \\ \lambda/2 & \text{otherwise}\,. \end{cases} \tag{6.12}$$

According to (6.12), the value of h_0 depends on the range of μ (as determined by λ). However, later in Proposition 6.3, we will present an upper bound on h_0 which depends only on λ and n. This upper bound will be used in conjunction with the following proposition to derive our main result.

Proposition 6.2 *We have*

$$\gamma(\Lambda) = \left(\frac{\lambda}{h_0}\right)^{\frac{2}{n}} \gamma(\Lambda_b)^{\frac{n-1}{n}} \,.$$

Proof: The proof follows using the definition (2.2), and the facts that $\lambda' = \lambda$ and (6.9). □

Proposition 6.3 *We have*

$$h_0 \leq \sqrt{\frac{n+1}{2n}}\lambda \,. \tag{6.13}$$

Proof: We consider the following two cases:

i) $\mu \leq \sqrt{3}\lambda/2$. In this case, the result follows by applying inequality (6.7) to the

first expression of (6.12).

ii) $\mu > \sqrt{3}\lambda/2$. In this case, using (6.12), we obtain $h_0 = \lambda/2$ which also satisfies (6.13). □

Theorem 6.3 (main result) *We have*

$$\gamma_n \geq \left(\frac{2n}{n+1}\right)^{\frac{1}{n}} \gamma_{n-1}^{\frac{n-1}{n}} . \tag{6.14}$$

Proof: Using Proposition 6.2, and the facts that $\Lambda_b = L_{n-1}$, and $\gamma_n \geq \gamma(\Lambda)$, we obtain

$$\gamma_n \geq \left(\frac{\lambda}{h_0}\right)^{\frac{2}{n}} \gamma_{n-1}^{\frac{n-1}{n}} . \tag{6.15}$$

The proof then follows by applying (6.13) to (6.15). □

Note that inequality (6.14) is satisfied with equality for $n = 2$.

For large values of n, applying (6.8), and using the same arguments as in the proofs of Proposition 6.3 and Theorem 6.3, we can find a tighter bound than (6.14) as

$$\gamma_n \geq \left[1 - (0.7573)^2 \left(\frac{n-1}{e\sqrt{e}}\right)^{\frac{2}{n-1}}\right]^{\frac{n-1}{n}} \gamma_{n-1}^{\frac{n-1}{n}} > (2.345)^{\frac{1}{n}} \gamma_{n-1}^{\frac{n-1}{n}} . \tag{6.16}$$

It can be seen that the expression $2n/(n+1)$ in (6.14) is always less than 2. This, unfortunately, implies that the inequality (6.14) cannot result in the proof of $\gamma_n \geq \gamma_{n-1}$ for any interesting values of n, i.e., $n \geq 10$. The reason is that to conclude such a result from (6.14), we need to have $\gamma_{n-1} \leq 2n/(n+1) < 2$. However, referring to Tables 1.2 and 1.3 of [25], we observe that there already exist lattices in dimensions $n \geq 9$ which have coding gains larger than 2. It is not difficult to see that combining K-L and C-F-R bounds for $n > 42$ cannot help either.

It seems, however, natural that one tries to prove $\gamma_n \geq \gamma_{n-1}$ for certain values of $n \geq 10$ by the proper improvement of inequality (6.7) for the corresponding densest lattices. For the densest lattices in dimensions $n \geq 9$, we expect the number of lattice points on the surface of $\mathcal{S}(\mathbf{v})$, as defined in Theorem 6.2, to be larger than $n+1$. To make inequality (6.7) tighter for these lattices, one might be able to use a well-quantified version of this argument to improve the bound given in Lemma 6.1.

Chapter 7

Concluding remarks

This thesis has made contributions to solving the lattice decoding problem and investigating its complexity. It has also contributed to the exploration of the trellis structure and the trellis complexity of lattices. Some results on lattice theory with possible coding applications have also been developed.

The upper bounds derived in this thesis on the complexity of RCS algorithms, which are in terms of the dimension n and the coding gain γ of the lattice, are so far the best known bounds on the decoding complexity of a general lattice. As for the trellis method, however, there does not exist an upper bound on the trellis complexity of lattices which is just a function of n or γ. There are also some lattices which do not have a finite trellis, and therefore cannot be decoded by the trellis method. Despite these facts, based on the results developed in this thesis, we are able to compare the RCS and trellis methods for each specific lattice with a finite trellis diagram.

As an example, using RCS algorithms, the decoding log-complexity of D_n lattices is bounded above and below by $n \log n/2 + O(n)$ and $O(n)$, respectively. Ap-

plying the Viterbi algorithm to the minimal trellis of D_n, it can be seen, based on the first upper bound of (2.19), that the decoding log-complexity of D_n is upper bounded by $2\log n + O(1)$. Comparison of the bounds shows that the trellis method is more efficient than RCS methods for the decoding of D_n, especially for large values of n. A similar result also holds for D_n^*. As another example, we consider the sequence of Barnes-Wall lattices BW_n. When decoded by RCS algorithms, BW_n has a decoding log-complexity which is upper bounded by $(3n\log n)/4 + O(n)$. By applying the trellis method to a minimal trellis of BW_n, even by using the second upper bound of (2.19), the bound on log-complexity is reduced to $(n\log n)/4 + O(n)$. Note that for RCS methods, this is a lower bound on the decoding log-complexity of BW_n.

The above examples provide evidence that the Viterbi algorithm, when applied to a minimal trellis of a lattice with strong algebraic structure, can outperform the RCS methods. This is mainly due to the fact that RCS algorithms are not able to employ such a structure to reduce the complexity. They however remain the fastest algorithms for the decoding of a *general* lattice.

There are a few directions in which the contributions of this work can be extended. Improving the bounds on the complexity of RCS algorithms is of definite interest, although our results imply that this is not very likely.

Developing efficient algorithms to find minimal trellis diagrams of lattices is an important and challenging problem. In particular, a continuation of this work could be to find minimal trellises for K_{12}, and the other A_n and A_n^* lattices. Forney has also suggested the extension of our arguments to complex lattices. In particular, he has posed some problems on the investigation of minimal trellis diagrams for complex lattices.

It has been proved in [40] that the problem of finding a coordinate permutation that minimizes the number of states at a given level in the trellis of a binary linear block code is NP-hard. We conjecture that the problem of finding a minimal trellis of a lattice, given its basis, is also NP-hard.

Another problem would be to find a trellis among the minimal trellises of a lattice which minimizes another complexity measure (in addition to the number of distinct paths N). One can also study the problem of minimizing the other trellis complexity measures like the number of edges, instead of minimizing N. Improvements over the bounds on the trellis complexity of lattices is also of great interest.

It has been shown in [71] that the trellis complexity of rational lattices cannot be upper bounded by either a function of n or a function of γ. A more natural and challenging problem is to answer the following question: "Is it possible to upper bound the trellis complexity of rational lattices by a function of n (and/or γ), and the size of the basis?".

Investigating the interplay between the performance and the decoding complexity of lattice codes is an important fundamental problem. With this regard, devising approximate decoding algorithms which are practically simple is an interesting research area. One might also want to look into the problem of constructing lattices with simple trellis structures.

A very interesting and extremely difficult problem is, of course, to prove or disprove that γ_n is an increasing function of n.

Appendix A

An independent proof for Corollary 3.1

Corollary 3.1 *The densest lattices have ESM.*

Proof: Suppose Λ to be an arbitrary n-D lattice with successive minima $\lambda_1, \ldots, \lambda_n$. Combining (2.4) with the fact that $\lambda_1 \leq \lambda_i$ for $1 \leq i \leq n-1$, results in $\lambda_1^{n-1}\lambda_n \leq \det(\Lambda)\gamma_n^{n/2}$. Dividing both sides of the last inequality by λ_1^n and using (2.2), we obtain $\lambda_n/\lambda_1 \leq \{\gamma_n/\gamma(\Lambda)\}^{n/2}$. For the densest lattice(s), we have $\gamma(\Lambda) = \gamma_n$, and the inequality results in $\lambda_n \leq \lambda_1$. Comparing this with (2.1) proves the corollary. □

Bibliography

[1] S. Arora, L. Babai, J. Stern and Z. Sweedyk, "The hardness of approximate optima in lattices, codes, and systems of linear equations," in *Proc. 34th IEEE Symp. on Foundations of Computer Science,* pp. 724-733, 1993.

[2] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem," *Combinatorica 6,* pp. 1-13, 1986.

[3] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory,* vol. IT-20, pp. 284-287, 1974.

[4] A. H. Banihashemi and I. F. Blake, "Trellis complexity and minimal trellis diagrams of lattices," submitted to *IEEE Trans. Inform. Theory,* Oct. 1996.

[5] —— ——, "On the trellis complexity of root lattices and their duals," submitted to *IEEE Trans. Inform. Theory,* April 1997.

[6] —— ——, "New upper bounds on trellis complexity of lattices," accepted for presentation at the *1997 IEEE International Symposium on Information Theory,* Ulm, Germany, June 29–July 4, 1997.

[7] —— ——, "Minimal trellis diagrams of lattices," accepted for presentation at the *1997 IEEE International Symposium on Information Theory*, Ulm, Germany, June 29–July 4, 1997.

[8] —— ——, "On the trellis complexity of root lattices and their duals," accepted for presentation at the *1997 IEEE Information Theory Workshop*, Longyearbyen, Svalbard, Norway, July 6–12, 1997.

[9] —— and A. K. Khandani, "On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis," accepted for publication in *IEEE Trans. Inform. Theory*, Dec. 1995.

[10] —— ——, "An inequality on the coding gain of densest lattice packings," presented at the *30th Annual Conference on Information Sciences and Systems*, Princeton Univ., Princeton, NJ, March 20–22, 1996.

[11] —— ——, "Lattice decoding using the Korkin-Zolotarev reduced basis," presented at the *30th Annual Conference on Information Sciences and Systems*, Princeton Univ., Princeton, NJ, March 20–22, 1996.

[12] —— ——, "An inequality on the coding gain of densest lattice packings," submitted to *Designs, Codes and Cryptography*, Oct. 1996.

[13] —— ——, "Lattice decoding using the Korkin-Zolotarev reduced basis," *Tech. Report UW-E&CE* 95 – 12, Dept. of Elec. and Comp. Eng., Univ. of Waterloo, 1995.

[14] Y. Berger and Y. Be'ery, "Bounds on the trellis size of linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-39, no. 1, pp. 203-209, Jan. 1993.

[15] —— ——, "The twisted squaring construction, trellis complexity, and generalized weights of BCH and QR codes," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 6, pp. 1817-1827, Nov. 1996.

[16] E. Biglieri and A. Spalvieri, "Performance evaluation of coded modulation schemes based on binary lattices," *IEEE Trans. Comm.,* vol. 43, pp. 269-276, 1995.

[17] J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh Fading and Gaussian channels," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 2, pp. 502-518, March 1996.

[18] A. R. Calderbank and N. J. A. Sloane, "New trellis codes based on lattices and codes," *IEEE Trans. Inform. Theory,* vol. IT-33, no. 2, pp. 177-195. March 1987.

[19] J. W. S. Cassels, *An introduction to the geometry of numbers,* Springer Verlag, Berlin, 1971.

[20] C. Chabauty, *Sur les minima arithmétiques des formes,* Annales Sci. Ecole Normale Sup. (3), vol. 66, pp. 367-394, 1949.

[21] F. Chen, Z. Gao, and J. Villasenor, "Lattice vector quantization of generalized Gaussian sources," *IEEE Trans. Inform. Theory,* vol. IT-43, no. 1, pp. 92-103, Jan. 1997.

[22] J. H. Conway and N. J. A. Sloane, "Fast quantizing and decoding algorithms for lattice quantizers and codes," *IEEE Trans. Inform. Theory,* vol. IT-28, no. 2, March 1982.

[23] —— ——, Laminated lattices, *Annals Math.* 116, pp. 593-620, 1982.

[24] —— ——, "On the Voronoi regions of certain lattices," *SIAM J. Alg. Disc. Math.*, vol. 5, no. 3, Sept. 1984.

[25] —— ——, *Sphere packings, lattices and groups*, 2nd ed. New York: Springer-Verlag, 1993.

[26] R. de Buda, "Some optimal codes have structure," *IEEE J. Select. Areas Comm.*, vol. 7, no. 6, pp. 893-899, Aug. 1989.

[27] M. V. Eyuboglu and G. D. Forney, Jr., "Lattice and trellis quantization with lattice- and trellis-bounded codebooks—High-rate theory for memoryless sources," *IEEE Trans. Inform. Theory*, vol. IT-39, no. 1, pp. 46-59, Jan. 1993.

[28] J. Feigenbaum, G. D. Forney, Jr., B. H. Markus, R. J. McEliece, and A. Vardy, "Introduction to the special issue on codes and complexity," *IEEE Trans. Inform. Theory*, vol. IT-42, no. 6, pp. 1649-1657, Nov. 1996.

[29] G. D. Forney, Jr., "Final report on a coding system design for advanced solar missions," Contract NAS2-3637, NASA Ames Research Center, Moffet Field, CA, Dec. 1967.

[30] ——, "The Viterbi algorithm," *Proc. IEEE*, vol. 61, pp. 268-278, 1973.

[31] ——, "Coset codes - part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. IT-34, no. 5, pp. 1152-1187, Sept. 1988.

[32] ——, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-40, no. 6, pp. 1741-1752, Nov. 1994.

[33] ——, "Density/length profiles and trellis complexity of lattices," *IEEE Trans. Inform. Theory*, vol. IT-40, no. 6, pp. 1753-1772, Nov. 1994.

[34] —— "Approaching the capacity of the AWGN channel with coset codes and multilevel coset codes," preprint, Sept. 1996.

[35] ——, R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi, "Efficient modulation for band-limited channels," *IEEE J. Select. Areas Comm.*, vol. SAC-2, no. 5, pp. 632-647, Sept. 1984.

[36] —— and M. D. Trott, "The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders," *IEEE Trans. Inform. Theory*, vol. IT-39. no. 9, pp. 1491-1513, Sept. 1993.

[37] P. M. Gruber and C. G. Lekkerkerker, *Geometry of numbers*, 2nd ed. North-Holland, Amsterdam: Elsevier Science Publishers B.V., 1987.

[38] J. Hastad, "Dual vectors and lower bounds for the nearest lattice point problem," *Combinatorica 8*, pp. 75-81, 1988.

[39] B. Helfrich, "Algorithms to construct Minkowski reduced and Hermite reduced lattice bases," *Theoretical Computer Sci. 41*, pp. 125-139, 1985.

[40] G. B. Horn and F. R. Kschischang, "On the intractability of permuting a block code to minimize trellis complexity," *IEEE Trans. Inform. Theory*, vol. IT-42, no. 6, pp. 2042-2048, Nov. 1996.

[41] V. Jarnik, *Zwei Bemerkungen zur Geometrie der Zahlen*, Věstnik Královské České Společn. Nauk, 12pp, 1941.

[42] R. Kannan, "Improved algorithms on integer programming and related lattice problems," *Proc. 15th Annual ACM Symp. on Theory of Computing,* pp. 193-206, 1983.

[43] ——, "Minkowski's convex body theorem and integer programming," *Mathematics of Operations Research,* vol. 12, no.3, pp. 415-440, Aug. 1987.

[44] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes," *IEEE Trans. Inform. Theory,* vol. IT-39, no. 1, pp. 242-245. Jan. 1993.

[45] —— —— —— ——, "On complexity of trellis structure of linear block codes," *IEEE Trans. Inform. Theory,* vol. IT-39, no. 3, pp. 1057-1064, May 1993.

[46] A. B. Kiely, S. J. Dolinar, R. J. McEliece, L. L. Ekroot, and W. Lin, "Trellis decoding complexity of linear block codes," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 6, pp. 1687-1697, Nov. 1996.

[47] A. Korkin and G. Zolotarev, "Sur les formes quadratiques," *Math. Ann. 6,* pp. 366-389, 1873.

[48] F. R. Kschischang, "The trellis structure of maximal fixed-cost codes," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 6, pp. 1828-1838, Nov. 1996.

[49] J. C. Lagarias, H. W. Lenstra and C. P. Schnorr, "Korkin Zolotarev bases and successive minima of a lattice and its reciprocal," *Combinatorica 10,* pp. 333-348, 1990.

[50] J. Leech, Some sphere packings in higher space, *Can. J. Math.* 16, pp. 657-682, 1964.

[51] J. Leech, Five dimensional non-lattice sphere packings, *Canad. Math. Bull.* 10, pp. 387-393, 1967.

[52] J. Leech, Six and seven dimensional non-lattice sphere packings, *Canad. Math. Bull.* 12, pp. 151-155, 1969.

[53] J. Leech and N. J. A. Sloane, Sphere packings and error-correcting codes, *Can. J. Math.* 23, pp. 718-745, 1971.

[54] H. W. Lenstra, "Integer programming with a fixed number of variables," First announcement (1979), *Mathematics of Operations Research,* vol 8, no. 4, pp. 538-548, Nov. 1983.

[55] A. K. Lenstra, H. W. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen 261,* pp. 513-534, 1982.

[56] S. Lin and D. J. Costello, Jr., *Error control coding: fundamentals and applications,* Prentice-Hall Inc., 1983.

[57] T. Linder, C. Schlegel, and K. Zeger, "Corrected proof of de Buda's theorem," *IEEE Trans. Inform. Theory,* vol. IT-39, no. 5, pp. 1735-1737, Sept. 1993.

[58] L. Lovász, "An algorithmic theory of numbers, graphs and convexity," *NSF-CBMS Regional Conference Series in Applied Mathematics 50,* SIAM, Philadelphia, Pennsylvania, 1986.

[59] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes, 2nd ed.* North-Holland Publishing Company, 1978.

[60] J. L. Massey, "Foundation and methods of channel encoding," *Proc. Int. Conf. Information Theory and Systems*, NTG-Fachberichte vol. 65, pp. 148-157, Berlin, 1978.

[61] R. J. McEliece, "On the BCJR trellis for linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-42, pp. 1072-1092, July 1996.

[62] G. L. Nemhauser, and L. A. Wolsey, *Integer and combinatorial optimization.* John Wiley & Sons, 1988.

[63] J. K. Omura, "On the Viterbi decoding algorithm," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 177-179, Jan. 1969.

[64] S. S. Ryškov, "Density of an (r, R)-system," *Mat. Zametki*, vol. 16, no. 3, pp. 447-454, Sept. 1974; English translation in *Math. Notes of the Academy of Sciences of the USSR*, vol. 16, pp. 855-858, 1975.

[65] P. Scherk, *Convex bodies off center*, Archiv Math. 3, p. 303, 1950.

[66] C. P. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms," *Theoretical Computer Science 53*, pp. 201-224, 1987.

[67] A. Schrijver, *Theory of linear and integer programming*, New York: Wiley, 1986.

[68] H. Störmer and G. Walter, *Verschärfung eines Satzes von Mahler über konvexe Körper in inhomogener Lage*, Archiv Math. 2, pp. 346-348, 1950.

[69] V. Tarokh and I. F. Blake, "Trellis complexity versus the coding gain of lattices I," *IEEE Trans. Inform. Theory*, vol. IT-42, no. 6, pp. 1796-1807, Nov. 1996.

[70] —— ——, "Trellis complexity versus the coding gain of lattices II," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 6, pp. 1808-1816, Nov. 1996.

[71] —— and A. Vardy, "Upper bounds on trellis complexity of lattices," preprint, received Aug. 1996.

[72] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," submitted to *IEEE Trans. Inform. Theory,* Sept. 1995.

[73] P. van Emde Boas, "Another NP-complete partition problem and the complexity of computing short vectors in a lattice," *Report 81-04,* Dept. of Mathematics, Univ. of Amsterdam, 1981.

[74] A. Vardy, "Even more efficient bounded-distance decoding of the hexacode, the Golay code, and the Leech lattice," *IEEE Trans. Inform. Theory,* vol. IT-41, no. 5, pp. 1495-1499, Sept. 1995.

[75] —— and Y. Be'ery, "Maximum-likelihood soft decision decoding of BCH codes," *IEEE Trans. Inform. Theory,* vol. IT-40, no. 2, pp. 546-554, March 1994.

[76] —— and F. R. Kschischang, "Proof of a conjecture of McEliece regarding the expansion index of the minimal trellis," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 6, pp. 2027-2034, Nov. 1996.

[77] V. V. Vazirani, H. Saran, and B. S. Rajan, "An efficient algorithm for constructing minimal trellises for codes over finite abelian groups," *IEEE Trans. Inform. Theory,* vol. IT-42, no. 6, pp. 1839-1854, Nov. 1996.

[78] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 260-269, Apr. 1967.

[79] J. K. Wolf, "Efficient maximum-likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 76-80, 1978.

[80] Ø. Ytrehus, "On the trellis complexity of certain binary linear block codes," *IEEE Trans. Inform. Theory*, vol. IT-41, no. 2, pp. 559-560, March 1995.

[81] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Trans. Inform. Theory*, vol. IT-42, no. 4, pp. 1152-1159, July 1996.

[82] "Special issue on codes and complexity–Part I," *IEEE Trans. Inform. Theory*, vol. IT-42, no. 6, Nov. 1996.