Successive Minimization of the State Complexity of the Self-dual Lattices Using Korkin-Zolotarev Reduced Basis *

Amir K. Khandani and M. Esmaeili
Dept. of Elec. and Comp. Eng., University of Waterloo, Waterloo, ON, Canada, N2L 3G1

July 5, 2001

Abstract.
This work presents a systematic method to successively minimize the state complexity of the self-dual lattices (in the sense that each section of the trellis has the minimum possible number of states fixing its preceding co-ordinates). This is based on representing the lattice on an orthogonal co-ordinate system corresponding to the Gram-Schmidt (GS) vectors of a Korkin-Zolotarev (KZ) reduced basis. As part of the computations, we give expressions for the GS vectors of a KZ basis of the K_{12}, Λ_{24}, and BW_n lattices. It is also shown that for the complex representation of the Λ_{24} and the BW_n lattices over the set of the Gaussian integers, we have: (i) the corresponding GS vectors are along the standard co-ordinate system, and (ii) the branch complexity at each section of the resulting trellis meets a certain lower bound. This results in a very efficient trellis representation for these lattices over the standard co-ordinate system.

Keywords: Lattice, Self-dual, Korkin-Zolotarev Reduced Basis, State Complexity

1. Introduction

Lattices are widely used in digital communications for the purpose of efficient signaling over band-limited channels (coset coding), or in the quantization of a multi-dimensional source (vector quantization). The major complicated operation in using lattices in such applications is the process of decoding the lattice which is the operation of finding the point of the lattice which has the smallest Euclidean distance to an arbitrary input. The common approach currently used in communication for the decoding of lattices is based on representing the lattice by a state diagram which reflects the underlying group structure. This approach is mainly due to the contributions of Forney (Forney, 1988; Forney, 1994) and Forney and Trott (Forney and Trott, 1993).

Consider the trellis diagram of an n-dimensional (n-D) lattice with respect to a given ordered set of co-ordinate vectors (the k'th section

* This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).
This work is presented in part at *IEEE Int. Symp. Inform. Theory,* (Cambridge, USA), Aug. 1998.

of the trellis, $k = 1, \ldots, n$, corresponds to the k'th co-ordinate vector). It is known that the number of states at a given section of the trellis diagram is equal to the ratio of the volumes of the intersection and projection lattices (to be defined later) with respect to the sub-space spanned by the preceding dimensions. It is also known that by the appropriate selection of the co-ordinate system, one can reduce the state complexity of the underlying trellis diagram (Forney, 1994).

For a lattice Λ, we use a co-ordinate system whose dimensions are along the Gram-Schmidt (GS) vectors of a Korkin-Zolotarev (KZ) reduced basis of Λ. The basic procedure for computing this set of co-ordinates is as follows: the first dimension is selected along a minimum norm vector of the lattice, then the lattice is projected along the orthogonal span of this vector and the procedure is repeated in a recursive manner with respect to the projected lattice. It is shown that in the case of the self-dual lattices, this co-ordinate system successively minimizes the state complexity of the underlying trellis diagram (in the sense that fixing the co-ordinates indexed by $1, \ldots, k$, the $k+1$'th section, $k = 1, \ldots, n$, has the minimum possible number of states). It is worth mentioning that the majority of the lattice used in channel coding applications are self-dual. This includes Barnes-Wall (BW_n) lattices, the Coxeter-Todd (K_{12}) lattice, and the Leech lattice (Λ_{24}) (Forney, 1988).

In this work, we consider lattices which are defined over the set of real, Gaussian, or Eisenstein integers. For the sake of simplicity, most of the discussions are presented in terms of the lattices defined over the set of the real integers; however, the results can be easily generalized to the other cases.

The outline of the article is as follows: Section 2 is devoted to some necessary definitions about lattices. Section 3 explains the procedure used to minimize the state complexity of a self-dual lattice using the GS vectors of a KZ reduced basis. In Section 4, we compute the GS vectors of some of the important lattices used in the communication applications and give numerical results for the resulting state complexities. Finally, Section 5 is devoted to some concluding remarks.

2. Preliminaries

A real n-D lattice Λ is a discrete set of n-D vectors in R^n which form a group under vector addition. The minimum norm vectors of a lattice Λ correspond to the points of Λ which are at the smallest possible distance, denoted by $d_{\min}(\Lambda)$, to the origin.

An n-D lattice Λ is generated by the integer linear combinations of some set of linearly independent n-D vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \Lambda$. In other words, each element $\mathbf{x} \in \Lambda$ can be expressed as: $\mathbf{x} = \sum_{i=1}^{m} z_i \mathbf{b}_i$, $z_i \in Z$, where Z denotes the set of the integers. The set of the vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ is called a basis (or a generator) of the lattice Λ. A lattice is called full rank if $n = m$.

A sub-lattice Λ' is a subset of the elements of Λ that is itself a lattice. A sub-lattice Λ' induces a partition of Λ into equivalence classes modulo Λ'. The order of this partition is shown by $|\Lambda/\Lambda'|$. The lattice Λ is the union of $|\Lambda/\Lambda'|$ cosets of Λ'.

The volume of a lattice Λ, denoted by $V(\Lambda)$, is defined as the volume of the n-D space associated with each lattice point. It can be shown that $V(\Lambda) = \det(\mathbf{\Lambda}\mathbf{\Lambda}^t)$. Note that although the generator matrix $\mathbf{\Lambda}$ is not unique, the quantity $V(\Lambda)$ does not depend on the selection of the specific $\mathbf{\Lambda}$.

The lattice Λ^*, dual to Λ, consists of the elements $\mathbf{x} \in R^n$ satisfying $<\mathbf{x}, \mathbf{y}> \in Z, \forall \mathbf{y} \in \Lambda$, where $<\ .\ >$ denotes the Euclidean inner product on R^n and Z is the set of integers. We have $V(\Lambda) = 1/V(\Lambda^*)$. A lattice is called self-dual if $\Lambda = \Lambda^*$. Hence, for a self-dual lattice, we have $V(\Lambda) = 1$.

Using the standard method of Gram-Schmidt (GS) orthogonalization, one can assign to any ordered set of basis vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ of a lattice Λ, a set of Gram-Schmidt vectors $\{\mathbf{g}_1, \ldots, \mathbf{g}_m\}$ satisfying,

$$\begin{aligned} &\mathbf{g}_1 = \mathbf{b}_1, \\ &\mathbf{g}_i = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{g}_j, i = 2, \ldots, n, \quad \mu_{i,j} = \frac{<\mathbf{b}_i, \mathbf{g}_j>}{\|\mathbf{g}_j\|^2}, \quad 1 \le j < i \le n, \end{aligned} \tag{1}$$

where $\|\mathbf{g}_j\|^2 = <\mathbf{g}_j, \mathbf{g}_j>$ is the square norm of $\mathbf{g}_j$.

The projection of a lattice on a given sub-space S, denoted as $P_S[\Lambda]$, is obtained by projecting the elements of Λ on S. The intersection of a lattice with a given sub-space S, denoted as $I_S[\Lambda]$, consists of those elements of Λ which are zero in $S^\perp$, where $S^\perp$ stands for the orthogonal complement of S. We note that the $I_S[\Lambda]$ and the $I_{S^\perp}[\Lambda]$ are sub-lattices of Λ, (Forney, 1994). The basis matrices (and thereby the volumes) of these projection and intersection lattices can be easily computed using the methods explained in (Cohen, 1993) for the computation of the Kernel or image of a basis matrix. It should be mentioned that in general the matrices obtained in this way are composed of vectors which are linearly dependent and to compute the corresponding basis matrix, one has to express them in terms of their Hermite normal form (Nemhauser and Wolsey, 1988). We do not get into these discussions as in our case these volumes can be easily expressed in terms of the product of the lengths of the GS vectors. However, we have used these alternative computational techniques to check the results.

Given an ordered set of orthogonal co-ordinates, say $\mathbf{g}_1, \ldots, \mathbf{g}_n$, we use the notations S_k, $S_k^\perp$, $k = 1, \ldots, n$, to refer to the sub-space spanned by $\mathbf{g}_1, \ldots, \mathbf{g}_k$, and to its orthogonal complement (sub-space spanned by $\mathbf{g}_{k+1}, \ldots, \mathbf{g}_n$), respectively. The following theorems contain some of the key points relevant to the trellis structure of lattices:

Theorem (Forney and Trott, 1993): Consider an ordered set of orthogonal co-ordinate system for R^n used to represent an n-D lattice Λ. The lattice can be represented by a trellis diagram in which the number of states at time index k, $k = 0, \ldots, n$, is equal to,

$$s_k = \frac{V(I_{S_k}[\Lambda])}{V(P_{S_k}[\Lambda])}, \quad k = 1, \ldots, n, \quad \text{and} \quad s_0 = 1. \tag{2}$$

Theorem (Forney, 1994): Consider a sub-space $S \subseteq R^n$ and its orthogonal complement $S^\perp \subseteq R^n$; we have,

$$V(I_S[\Lambda]) \cdot V(P_{S^\perp}[\Lambda]) = V(\Lambda). \tag{3}$$

Theorem (Forney, 1994): Consider a sub-space $S \subseteq R^n$ such that $I_S[\Lambda]$ is of full rank; then the dual lattice to $I_S[\Lambda]$, in S, is $P_S[\Lambda^*]$. Hence,

$$V(I_S[\Lambda]) \cdot V(P_S[\Lambda^*]) = 1. \tag{4}$$

Theorem: Consider an n-D lattice Λ and an ordered set of co-ordinate vectors, say $\mathbf{g}_1, \ldots, \mathbf{g}_n$. Assume that the volume of the intersection of $P_{S_{k-1}^\perp}[\Lambda]$ with $\mathbf{g}_k$ is α_k (this means that α_k is the length of the shortest vector of $P_{S_{k-1}^\perp}[\Lambda]$ in the direction of $\mathbf{g}_k$). We have,

$$V(I_{S_k}[\Lambda]) = \prod_{i=1}^{k} \alpha_k, \quad \text{and} \quad V(P_{S_k^\perp}[\Lambda]) = \frac{V(\Lambda)}{\prod_{i=1}^{k} \alpha_k}. \tag{5}$$

Proof: Using (3), we have,

$$V(I_{S_1}[\Lambda]) = \alpha_1, \quad \text{and} \quad V(P_{S_1^\perp}[\Lambda]) = \frac{V(\Lambda)}{\alpha_1}, \tag{6}$$

where S_1 is the sub-space spanned by $\mathbf{g}_1$. Noting that $P_{S_2^\perp}[\Lambda]$ is obtained by projecting $P_{S_1^\perp}[\Lambda]$ along the orthogonal span of $\mathbf{g}_2$, we obtain

$V(P_{S_1^\perp}[\Lambda]) = \alpha_2 V(P_{S_2^\perp}[\Lambda])$, implying that $V(\Lambda) = \alpha_1\,\alpha_2\,V(P_{S_2^\perp}[\Lambda])$. Continuing the same procedure, we obtain (5). $\square$

3. Using the Korkin-Zolotarev basis to successively minimize the state complexity of the self-dual lattices

Reduction Theory in general deals with the problem of finding a basis for a lattice which is composed of relatively short and nearly orthogonal vectors. There are quite a number of different methods of basis reduction available (Gruber and Lekkerkerker, 1987). In this work, we make use of one of these methods, known as the Korkin-Zolotarev (KZ) basis reduction (Korkine and Zolotareff, 1873) (also refer to (Gruber and Lekkerkerker, 1987), (Lagarias, Lenstra, and Schnorr, 1990), (Kannan, 1987)). The KZ reduced basis of a lattice is used in (Kannan, 1987) to derive bounds on the decoding complexity of a general lattice using a recursive search method over a limited portion of the space.

Definition: Consider a basis $\mathbf{\Lambda} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ with the GS vectors $\mathbf{G}[\Lambda] = [\mathbf{g}_1, \ldots, \mathbf{g}_n]$ for Λ, and for $i = 1, \ldots, n$, denote by $P_{S_i^\perp}[\Lambda]$ the orthogonal projection of Λ on the orthogonal complement of the subspace spanned by the basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_i$. Note that $P_{S_i^\perp}[\Lambda]$ is a lattice of rank $n - i$ with the basis vectors $P_{S_i^\perp}[\mathbf{b}_{i+1}], \ldots, P_{S_i^\perp}[\mathbf{b}_n]$. The basis $\mathbf{\Lambda}$ is said to be a KZ basis, if the following two conditions are satisfied,

1. $\mathbf{g}_i$ is a shortest non-zero vector of $P_{S_{i-1}^\perp}[\Lambda]$, for $1 \leq i \leq n$, where $S_0^\perp$ is defined as R^n.

2. $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$, where $\mu_{i,j} = \frac{<\mathbf{b}_i, \mathbf{g}_j>}{||\mathbf{g}_j||^2}$.

Note that these two conditions are independent of each other. In general, a basis satisfying the second condition, i.e., $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq n$, is called proper. It is easy to see that for each $\mathbf{b}_i$, by adding appropriate integer multiples of $\mathbf{b}_j, 1 \leq j \leq i-1$, to it, one is able to satisfy the properness condition (Nemhauser and Wolsey, 1988). This means that any basis which is not proper can be easily transformed into an equivalent proper basis (Nemhauser and Wolsey, 1988). In the present work, we are not concerned if the basis is proper or not, so we can simply drop the second condition from the definition given for the KZ basis.

Example: The following matrix is a KZ basis of the lattice D_4,

$$\mathbf{D}_4 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \tag{7}$$

The set of generator matrices involved in computing the corresponding GS vectors are given in (8). The i'th matrix, $i = 1, \ldots, 4$, from the left corresponds to the generator of the lattice obtained through the projection along the first $i-1$ GS vectors. The GS vectors are shown in bold-face.

$$\begin{vmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{vmatrix} \quad \begin{vmatrix} 0 & 0 & 0 & 0 \\ \mathbf{\frac{1}{2}} & \mathbf{-\frac{1}{2}} & \mathbf{1} & \mathbf{0} \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{vmatrix} \quad \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{\frac{2}{3}} & \mathbf{-\frac{2}{3}} & \mathbf{-\frac{2}{3}} & \mathbf{0} \\ -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 1 \end{vmatrix} \quad \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{vmatrix}. \tag{8}$$

This results in the following matrix as the set of the GS vectors of a KZ basis of D_4,

$$\mathbf{G}[D_4] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 1 & 0 \\ \frac{2}{3} & -\frac{2}{3} & -\frac{2}{3} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{9}$$

It is known that each lattice has at least one KZ reduced basis (Kannan, 1987); however, the KZ basis of a lattice may not be unique. For the rational lattices (where the elements of the generator matrix are rational), the elements of the GS vectors will be also rational (Kannan, 1987).

Consider a lattice Λ with the GS vectors $\mathbf{g}_1, \ldots, \mathbf{g}_n$, of a KZ basis. The volume of the intersection of $P_{S_{k-1}^{\perp}}[\Lambda]$ with $\mathbf{g}_k$ is equal to $\|\mathbf{g}_k\|$. In this case, using (5), we obtain,

$$V(I_{S_k}[\Lambda]) = \prod_{i=1}^{k} \|\mathbf{g}_i\|. \tag{10}$$

It follows that,

$$V(\Lambda) = \prod_{i=1}^{n} \|\mathbf{g}_i\|. \tag{11}$$

Applying (10), it is easy to see that the GS vectors of a KZ basis provide us with a nested set of orthogonal sub-spaces which successively minimize the $V(I_{S_k}[\Lambda])$ for $k = 1, \ldots, n$.

Applying (4) and (10), we obtain,

$$V(P_{S_k}[\Lambda]) = \frac{1}{\prod_{i=1}^{k} \|\mathbf{g}_i^*\|}\ , \tag{12}$$

where $\mathbf{g}_i^*$ are the GS vectors of a KZ basis of Λ^*. It follows from (12) that the GS vectors of a KZ basis of the dual lattice provides us with a nested set of orthogonal sub-spaces which successively maximizes the $V(P_{S_k}[\Lambda])$ for $k = 1, \ldots, n$.

In the case of the self-dual lattices, we have $\mathbf{g}_i^* = \mathbf{g}_i, i = 1, \ldots, n$. Therefore, by replacing (10) and (12) in (2), we obtain the following expression for the state complexity,

$$s_k = \prod_{i=1}^{k} \|\mathbf{g}_i\|^2, \quad k = 1, \ldots, n, \tag{13}$$

which is valid for a self-dual real lattice.

All our previous discussions were formulated in terms of lattices defined over the set of ordinary integers. To generalize the results to the case of the Gaussian or Eisenstein integers, it suffices to replace the norm of the GS vectors by the volume of the equivalent two-dimensional sub-lattices generated by those vectors. For both the Gaussian and the Eisenstein integers, this volume is proportional to the square norm of the corresponding GS vector where the proportionality factor for the Gaussian integers is 1, and for the Eisenstein integers is 3/4, (Forney, 1994). In our case, as we always deal with the ratio of two volumes, the effect of the proportionality factor is simply neglected. This means that for the complex lattices, relationship (13) should be modified to,

$$s_k = \prod_{i=1}^{k} \|\mathbf{g}_i\|^4, \quad k = 1, \ldots, n. \tag{14}$$

It follows from (13) and (14) that for the self-dual lattices, the selected co-ordinate system successively minimizes the state complexity of the underlying trellis diagram. It should be mentioned that our main approach will be valid if the condition of self-duality (resulting in $\mathbf{g}_i^* = \mathbf{g}_i, i = 1, \ldots, n$) is replaced by a milder condition requiring $\mathbf{g}_i^*$ and $\mathbf{g}_i$, $i = 1, \ldots, n$, to be in the same directions.

We have the following lemma and theorem which have essential role in the rest of the paper.

Lemma: Consider the lattice Λ with the KZ basis matrix $\mathbf{\Lambda}$ and let T denote a similarity transformation corresponding to the matrix $\mathbf{T}$ (i.e., $\mathbf{T} = \beta\bar{\mathbf{T}}$ where $\beta > 0$ and matrix $\bar{\mathbf{T}}$ represents an orthonormal transformation). Let $\mathbf{G}$ and $\bar{\mathbf{G}}$ denote the GS vectors corresponding to $\mathbf{\Lambda}$ and $\mathbf{\Lambda T}^t$ which are the basis matrices of the lattices Λ and $T\Lambda$, respectively. Then, $\mathbf{\Lambda T}^t$ is a KZ basis of $T\Lambda$ with the GS vectors $\mathbf{GT}^t$.

Proof: The norms are invariant under the transformation $\bar{\mathbf{T}}$, then $\mathbf{g}_1$ is a minimum norm vector in Λ iff $\mathbf{g}_1\mathbf{T}^t$ is a minimum norm vector in $T\Lambda$. Let $P_{S_i^\perp}$ in each of the two domains (original and transformed) denote the projection along the orthogonal span of the first i of the corresponding GS vectors. Also, let $\mathbf{b}_j$ be the jth row in the matrix $\mathbf{\Lambda}$. Since $<\mathbf{vT}^t, \mathbf{uT}^t>= \beta^2 <\mathbf{u},\mathbf{v}>$, we have

$$\begin{aligned} P_{S_1^\perp}[\mathbf{b}_j\mathbf{T}^t] &= \mathbf{b}_j\mathbf{T}^t - \frac{<\mathbf{b}_j\mathbf{T}^t, \mathbf{g}_1\mathbf{T}^t>}{<\mathbf{g}_1\mathbf{T}^t, \mathbf{g}_1\mathbf{T}^t>}\mathbf{g}_1\mathbf{T}^t \\ &= \left(\mathbf{b}_j - \frac{<\mathbf{b}_j,\mathbf{g}_1>}{<\mathbf{g}_1,\mathbf{g}_1>}\right)\mathbf{T}^t = P_{S_1^\perp}[\mathbf{b}_j]\mathbf{T}^t. \end{aligned} \tag{15}$$

It follows that $P_{S_1^\perp}[\mathbf{\Lambda T}^t] = P_{S_1^\perp}[\mathbf{\Lambda}]\mathbf{T}^t$. This implies that $\mathbf{g}_2$ is a minimum norm vector in $P_{S_1^\perp}[\Lambda]$ iff $\mathbf{g}_2\mathbf{T}^t$ is a minimum norm vector in $P_{S_1^\perp}[T\Lambda]$. The same argument shows that $\mathbf{g}_i$, $i>2$, is a minimum norm vector in $P_{S_{i-1}^\perp}[\Lambda]$ iff $\mathbf{g}_i\mathbf{T}^t$ is a minimum norm vector in $P_{S_{i-1}^\perp}[T\Lambda]$. This shows that $\mathbf{\Lambda T}^t$ is a KZ basis of $T\Lambda$ with the GS vectors $\mathbf{GT}^t$. $\square$

We define the vector $\mathbf{l}[\Lambda]$ as $(\|\mathbf{g}_1\|^2,\ldots,\|\mathbf{g}_n^2\|)$, and the normalized version of $\mathbf{l}[\Lambda]$ (to have unit volume for the lattice) as $\bar{\mathbf{l}}[\Lambda] = \mathbf{l}[\Lambda]/[V(\Lambda)]^{1/n}$. Using the given lemma, it is easy to verify that,

$$\mathbf{l}[R\Lambda] = 2\mathbf{l}[\Lambda], \tag{16}$$

where R is the rotational operator.

Example: Using the lemma and (9), the GS vectors of a KZ basis of RD_4 are computed as,

$$\mathbf{G}[D_4]\mathbf{R} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 1 & 0 \\ \frac{2}{3} & -\frac{2}{3} & -\frac{2}{3} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & \frac{4}{3} & -\frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 1 & -1 \end{bmatrix}. \tag{17}$$

We also have,

$$\mathbf{l}[D_4] = (2,\ 3/2,\ 4/3,\ 1)\,, \quad \text{and} \quad \mathbf{l}[RD_4] = 2\mathbf{l}[D_4] = (4,\ 3,\ 8/3,\ 2)\,. \tag{18}$$

Theorem: Let $T\Lambda$ be a version of lattice Λ obtained through a similarity transformation, and let $\mathbf{\Lambda}$ and $\mathbf{\Lambda T}^t$ be a KZ basis of Λ and $T\Lambda$, respectively. Consider the representation of Λ and $T\Lambda$ on the GS vectors of $\mathbf{\Lambda}$ and $\mathbf{\Lambda T}^t$, respectively. These two representations result in identical trellis diagrams.

Proof: Let $\mathbf{G}$ and $\bar{\mathbf{G}}$ denote the GS-matrices corresponding to $\mathbf{\Lambda}$ and $\mathbf{\Lambda T}^t$, respectively. Representing Λ and $T\Lambda$ on the co-ordinate systems corresponding to the GS vectors of $\mathbf{\Lambda}$ and $\mathbf{\Lambda T}^t$ results in lattices with generator matrices $\mathbf{\Lambda G}^t$ and $(\mathbf{\Lambda T}^t)\bar{\mathbf{G}}^t$, respectively. Applying the lemma, we have $(\mathbf{\Lambda T}^t)\bar{\mathbf{G}}^t = (\mathbf{\Lambda T}^t)(\mathbf{G T}^t)^t$, resulting in $(\mathbf{\Lambda T}^t)\bar{\mathbf{G}}^t = (\mathbf{\Lambda T}^t)(\mathbf{T G}^t) = \beta^2 \mathbf{\Lambda G}^t$. It follows that these two lattices have the same generator matrices within a scale factor, and consequently have identical trellis representations. $\square$

3.1. An inequality on the branch complexity

Consider the representation of a lattice over the GS vectors of a KZ basis. We note that the trellis diagram of the lattice $P_{S_{k-1}^{\perp}}[\Lambda]$ can be simply obtained by merging the states of the original trellis at time index $k-1$ together, and then deleting the first $k-1$ sections. From the structure of the KZ basis, we conclude that the parallel branches at the first section of the resulting trellis correspond to a minimum norm vector of $P_{S_{k-1}^{\perp}}[\Lambda]$, namely $\mathbf{g}_k$. This implies that the minimum distance among the branches merging into any state at time index k of the original trellis is equal to $\|\mathbf{g}_k\|$. Taking the group property into account, we conclude that the number of branches merging into any state at time index k of the original trellis is equal to the ratio of the minimum distance among the parallel branches at the kth section of the original trellis to $\|\mathbf{g}_k\|$. Obviously, the minimum distance among the parallel branches at any section of the original trellis is bounded by the minimum distance of the lattice. This means that,

$$b_k \geq \frac{d_{\min}(\Lambda)}{\|\mathbf{g}_k\|}, \tag{19}$$

where b_k is the number of branches merging into any state at time index k. For the complex lattices, relationship (19) should be modified to,

$$b_k \geq \frac{d_{\min}^2(\Lambda)}{\|\mathbf{g}_k\|^2}. \tag{20}$$

As we will see later, for Λ_{24} and the BW_n lattices there exists a complex KZ basis for which the GS vectors satisfy (20) with equality.

The following section is devoted to computing the GS vectors of a KZ basis, and thereby the trellis complexity, of some of the important lattices. We note that, in general, the computational complexity of finding the KZ basis of a lattice is polynomial time equivalent to finding a minimum norm vector of the lattice which is strongly believed to be *NP* (no polynomial time algorithm known). The fastest algorithm for the KZ reduction of a general lattice given by a set of basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ with $\gamma = \max\{||\mathbf{b}_1||^2, \ldots, ||\mathbf{b}_n||^2\}$ has a complexity bound of $\sqrt{n}^{n+O(n)} + O(n^4 \log \gamma)$ arithmetic steps on integers of $O(n \log \gamma)$ bits (Schnorr, 1987). However, for lattices which have a simple trellis representation, the computation of the KZ basis can be substantially simpler as we will see in the following.

4. Trellis complexity of some important lattices

4.1. Real BW_n lattices

In the following, we first show that the the GS vectors of a KZ basis of the BW_n lattice[1] $\Lambda(0,n)$, $n \geq 2$, can be computed using the recursion,

$$\begin{aligned}\mathbf{G}[\Lambda(0,n)] &= \begin{bmatrix} \mathbf{G}[R\Lambda(0,n-1)] & \mathbf{0} \\ \mathbf{0} & \mathbf{G}[\Lambda(0,n-1)] \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{G}[\Lambda(0,n-1)]\mathbf{R} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}[\Lambda(0,n-1)] \end{bmatrix},\end{aligned} \tag{21}$$

where $\mathbf{G}[\Lambda(0,n-1)]$ denote the GS vectors of a KZ basis of $\Lambda(0,n-1)$. We first establish the result for $n=2$ and 3, and then generalize it for arbitrary value of n.

The GS vectors of $\Lambda(0,2) \equiv E_8$ are obtained by working on the following generator matrix which is based on the squaring construction[2],

$$\mathbf{E_8} = \begin{bmatrix} \mathbf{D_4 R} & \mathbf{0} \\ \mathbf{D_4} & \mathbf{D_4} \end{bmatrix}. \tag{22}$$

The steps of computing the corresponding GS vectors are given in (23).

[1] Refer to (Forney, 1988) for definition.
[2] Refer to (Forney, 1988) for definition.

$$
\begin{array}{cccc|cccc}
2 & 0 & 0 & 0 & & & & \\
1 & 1 & 1 & 1 & & & & \\
2 & 2 & 0 & 0 & & & & \\
2 & 0 & 2 & 0 & & & & \\
\hline
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}
\quad
\begin{array}{cccc|cccc}
\mathbf{2} & \mathbf{0} & \mathbf{0} & \mathbf{0} & & & & \\
1 & 1 & 1 & 1 & & & & \\
2 & 2 & 0 & 0 & & & & \\
2 & 0 & 2 & 0 & & & & \\
\hline
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}
\quad
\begin{array}{cccc|cccc}
0 & 0 & 0 & 0 & & & & \\
\mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} & & & & \\
0 & 2 & 0 & 0 & & & & \\
0 & 0 & 2 & 0 & & & & \\
\hline
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}
.
$$

$$
\begin{array}{cccc|cccc}
0 & 0 & 0 & 0 & & & & \\
0 & 0 & 0 & 0 & & & & \\
\mathbf{0} & \mathbf{\frac{4}{3}} & -\mathbf{\frac{2}{3}} & -\mathbf{\frac{2}{3}} & & & & \\
0 & -\frac{2}{3} & \frac{4}{3} & -\frac{2}{3} & & & & \\
\hline
0 & \frac{2}{3} & -\frac{1}{3} & -\frac{1}{3} & 1 & 1 & 0 & 0 \\
0 & -\frac{1}{3} & \frac{2}{3} & -\frac{1}{3} & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}
\quad
\begin{array}{cccc|cccc}
0 & 0 & 0 & 0 & & & & \\
0 & 0 & 0 & 0 & & & & \\
0 & 0 & 0 & 0 & & & & \\
\mathbf{0} & \mathbf{0} & \mathbf{1} & -\mathbf{1} & & & & \\
\hline
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & \frac{1}{2} & -\frac{1}{2} & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}
\quad
\begin{array}{cccc|cccc}
0 & 0 & 0 & 0 & & & & \\
0 & 0 & 0 & 0 & & & & \\
0 & 0 & 0 & 0 & & & & \\
0 & 0 & 0 & 0 & & & & \\
\hline
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}
\tag{23}
$$

From (23), we obtain the first four GS vectors of E_8 which form the matrix given in (17). Referring to the last matrix in (23), we conclude that the last four GS vectors of E_8 are the GS vectors of D_4. This results in,

$$
\mathbf{G}[E_8] = \begin{bmatrix} \mathbf{G}[D_4]\mathbf{R} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}[D_4] \end{bmatrix} = \left[\begin{array}{cc}
\begin{array}{cccc} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & \frac{4}{3} & -\frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 1 & -1 \end{array} & \mathbf{0} \\
\mathbf{0} & \begin{array}{cccc} 1 & 1 & 0 & 0 \\ \frac{1}{2} & -\frac{1}{2} & 1 & 0 \\ \frac{2}{3} & -\frac{2}{3} & -\frac{2}{3} & 0 \\ 0 & 0 & 0 & 1 \end{array}
\end{array} \right].
\tag{24}
$$

For $n = 3$, consider the following generator matrix of $\Lambda(0,3) = \Lambda_{16}$,

$$
\mathbf{\Lambda_{16}} = \begin{bmatrix} \mathbf{E}_8\mathbf{R} & \mathbf{0} \\ \mathbf{E}_8 & \mathbf{E}_8 \end{bmatrix} = \begin{bmatrix} 2\mathbf{D}_4 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{D}_4\mathbf{R} & \mathbf{D}_4\mathbf{R} & \mathbf{0} & \mathbf{0} \\ \mathbf{D}_4\mathbf{R} & \mathbf{0} & \mathbf{D}_4\mathbf{R} & \mathbf{0} \\ \mathbf{D}_4 & \mathbf{D}_4 & \mathbf{D}_4 & \mathbf{D}_4 \end{bmatrix}.
\tag{25}
$$

We know that $d^2_{min}(\Lambda_{16}) = 8$ which is equal to $d^2_{min}(2D_4)$. Therefore, the first GS vector of Λ_{16} can be selected as $\mathbf{g}_1(\Lambda_{16}) = (2\mathbf{g}_1(D_4), (0)^{12})$, where $(.)^n$ denotes n times repetition. Now consider the lattice obtained by projecting Λ_{16} along the orthogonal span of this first GS vector. Note that this projection affects just the first block-column (of the last matrix) in (25). Consider different possible integer linear combinations of the four block-rows in (25) for the projected lattice. It is easy to verify that if this integer linear combination involves the fourth block-row, then the resulting minimum squared norm will be at least 6 as generated by the matrix $[\mathbf{D}_4\ \mathbf{D}_4\ \mathbf{D}_4]$ (note that $3d^2_{\min}(D_4) = 6$). However, this is equal to the second largest minimum squared norm of the GS vectors of $2D_4$. This means that the second largest GS vector of Λ_{16} can be obtained by integer linear combination of the first three block-rows only. On the other hand, it is easy to see that a linear integer combination involving all the first three block-rows results in a minimum norm which is larger or equal to the minimum norm obtained through considering the combinations of the first and the second, or the first and the third block-rows only. However, the first and the second (or the first and the third) block-rows in (25) generate the lattice RE_8 for which we have $\mathbf{l}[RE_8] = (\mathbf{l}(2D_4), \mathbf{l}(RD_4))$. This means that the second GS vector can be also selected from $2D_4$. Continuing this procedure, we conclude that one can select $\mathbf{g}_i(\Lambda_{16}) = (2\mathbf{g}_i(D_4), (0)^{12})$, $i = 1, \ldots, 4$. Projecting along the orthogonal span of the first four GS vectors, we are left with a lattice generated by,

$$\begin{bmatrix} \mathbf{D}_4\mathbf{R} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{D}_4\mathbf{R} & \mathbf{0} \\ \mathbf{D}_4 & \mathbf{D}_4 & \mathbf{D}_4 \end{bmatrix}. \tag{26}$$

This generator matrix along with our construction of $\mathbf{G}[E_8]$ complete the proof for $n = 3$.

In the general case, consider the following generator matrix for $\Lambda(0, n+1)$,

$$\mathbf{\Lambda}(0,n+1) = \begin{bmatrix} 2\mathbf{\Lambda}(0,n-1) & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{\Lambda}(0,n-1)\mathbf{R} & \mathbf{\Lambda}(0,n-1)\mathbf{R} & \mathbf{0} & \mathbf{0} \\ \mathbf{\Lambda}(0,n-1)\mathbf{R} & \mathbf{0} & \mathbf{\Lambda}(0,n-1)\mathbf{R} & \mathbf{0} \\ \mathbf{\Lambda}(0,n-1) & \mathbf{\Lambda}(0,n-1) & \mathbf{\Lambda}(0,n-1) & \mathbf{\Lambda}(0,n-1) \end{bmatrix}.$$

Assuming that the statement holds for $n \geq 3$, one can apply a similar argument as used for $\mathbf{\Lambda}_{16}$ to show that it holds for $\Lambda(0, n+1)$. Note that $d^2_{min}(2\Lambda(0, n-1)) = 4d^2_{min}(\Lambda(0, n-1)) = 2d^2_{min}(R\Lambda(0, n-1))$ and $\|\mathbf{g}_i(2\Lambda(0, n-1))\|^2 < \|\mathbf{g}_2(2\Lambda(0, n-1))\|^2 = 3d^2_{\min}(\Lambda(0, n-1))$, $i \geq 3$.

The real BW_n lattices are self-dual for $n = 2^{2i+1}$, $i = 1, 2, \ldots$ (Forney, 1994). The lengths of the GS vectors of a KZ basis for these lattices can be computed using the recursive relationship $\mathbf{l}[\Lambda(0, n)] =$

$(2\mathbf{l}[\Lambda(0,n-1)], \mathbf{l}[\Lambda(0,n-1)])$ initialized with $\mathbf{l}[\Lambda(0,1)] = \mathbf{l}[D_4] = (2, 3/2, 4/3, 1)$. For instance, we have $\mathbf{l}[E_8] = (4, 3, 8/3, 2, 2, 3/2, 4/3, 1)$ which after the normalization (setting the volume equal to one) results in $\bar{\mathbf{l}}[E_8] = (\sqrt{2}, \sqrt{3/2}, \sqrt{4/3}, 1, 1, \sqrt{3/4}, \sqrt{2/3}, \sqrt{1/2})$. Using (13), this results in the state complexity $(1, 2, 3, 4, 4, 4, 3, 2, 1)$ which is the same as the result reported in (Forney, 1994) based on intuition. Similar computations show that the state complexity for Λ_{32} is equal to,

$$(4, 12, 32, 64, 128, 192, 256, 256, 512, 768, 1024, 1024, 1024, 768, \ldots)$$

which is again the same as the result reported in (Forney, 1994).

4.2. E_8 AND K_{12} AS THE COMPLEX E-LATTICES

The construction of E_8 as an $\mathbf{E}$-lattice (defined over the set of the Eisenstein integers[3]) has the generator matrix,

$$\mathbf{E}_8^{(3)} = \begin{bmatrix} \theta & 0 & 0 & 0 \\ 0 & \theta & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}, \tag{27}$$

where $\theta = \sqrt{-3}$. The corresponding GS matrix is computed as,

$$\mathbf{G}[E_8^{(3)}] = \begin{bmatrix} \theta & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & \frac{\theta}{2} & -\frac{\theta}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{28}$$

It follows that $\mathbf{l}[E_8^{(3)}] = (3, 2, 3/2, 1)$, $\bar{\mathbf{l}}[E_8^{(3)}] = (\sqrt{3}, 2/\sqrt{3}, \sqrt{3}/2, 1/\sqrt{3})$. Using (14), we obtain the state complexity $(1, 3, 4, 3, 1)$ which is the same as the result reported in (Forney, 1994) based on intuition.

The E-lattice K_{12} has the generator matrix,

$$\mathbf{K}_{12} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ \theta & -\theta & 0 & 0 & 0 & 0 \\ 0 & \theta & -\theta & 0 & 0 & 0 \\ 0 & 0 & \theta & -\theta & 0 & 0 \\ 0 & 0 & 0 & \theta & -\theta & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{29}$$

The corresponding GS matrix is computed as,

[3] Refer to (Forney, 1994) for the definition.

$$\mathbf{G}[K_{12}] = \begin{bmatrix} \theta & -\theta & 0 & 0 & 0 & 0 \\ \frac{3}{2} & \frac{3}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & -\theta & 0 & 0 & 0 \\ 0 & 0 & 0 & -\theta & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -\frac{\theta}{2} & \frac{\theta}{2} \end{bmatrix}. \tag{30}$$

This implies $\mathbf{l}[K_{12}] = (6, 9/2, 3, 3, 2, 3/2)$, $\bar{\mathbf{l}}[K_{12}] = (2, 3/2, 1, 1, 2/3, 1/2)$. Applying (14), we obtain the state complexity $(1, 4, 9, 9, 9, 4, 1)$ which is the same as the result reported in (Forney, 1994) based on intuition.

4.3. Complex BW_n lattices

The generator matrix of the BW_n lattice over the Gaussian integers[4], denoted by $\mathbf{\Lambda}_c(0, n)$, can be computed using the recursion,

$$\mathbf{\Lambda}_c(0, n) = \begin{bmatrix} \phi\mathbf{\Lambda}_c(0, n-1) & \mathbf{0} \\ \mathbf{\Lambda}_c(0, n-1) & \mathbf{\Lambda}_c(0, n-1) \end{bmatrix}, \tag{31}$$

where $\phi = 1 + \sqrt{-1}$ and,

$$\mathbf{\Lambda}_c(0, 1) = \begin{bmatrix} \phi & 0 \\ 1 & 1 \end{bmatrix}. \tag{32}$$

Applying the same procedure as in the case of the real BW_n lattices, one can show that the relationship given by (21) is valid in the complex case as well. More precisely, we have,

$$\mathbf{G}[\Lambda_c(0, n)] = \begin{bmatrix} \phi\mathbf{G}[\Lambda_c(0, n-1) & \mathbf{0} \\ \mathbf{0} & \mathbf{G}[\Lambda_c(0, n-1)] \end{bmatrix}, \tag{33}$$

where,

$$\mathbf{G}[\Lambda_c(0, 1)] = \begin{bmatrix} \phi & 0 \\ 0 & 1 \end{bmatrix}. \tag{34}$$

It follows from (33) and (34) that $\mathbf{G}[\Lambda_c(0, n)]$ is a diagonal matrix. This means that the standard co-ordinate system corresponds to the GS vectors of a KZ basis.

It is also easy to show that the complex BW_n lattices contain n orthogonal minimum norm vectors corresponding to all the possible n permutations of the vector $(d_{\min} = \|\mathbf{g}_1\|, (0)^{n-1})$, where $(.)^{n-1}$ denotes $n-1$ times repetition. This can be verified by recursively relating the minimum norm vectors of the lattice generated by $\mathbf{\Lambda}_c(0, n)$ to the minimum norm vectors of the lattice generated by $\phi\mathbf{\Lambda}_c(0, n-1)$. Using this

[4] Refer to (Forney, 1994) for the definition.

fact, we conclude that in the case of the complex BW_n lattices, the lower bound on the branch complexity given in (20) is satisfied with equality.

All the complex BW_n lattices are self-dual (Forney, 1994). For these lattices, we have the recursive relationship $\mathbf{l}[\Lambda(0,n)] = (2\mathbf{l}[\Lambda(0,n-1)], \mathbf{l}[\Lambda(0,n-1)])$ initialized with $\mathbf{l}[\Lambda(0,1)] = \mathbf{l}[D_4] = (2,1)$, on the lengths of the GS vectors. As an example, for the E_8 lattice we have $\bar{\mathbf{l}}[E_8] = (2,1,1,1/2)$ resulting in the state complexity $(1,4,4,4,1)$ and the branch complexity $(1,2,2,4)$. For Λ_{16}, we have

$$\bar{\mathbf{l}}[\Lambda_{16}] = (2\sqrt{2}, \sqrt{2}, \sqrt{2}, \sqrt{2}/2, \sqrt{2}, \sqrt{2}/2, \sqrt{2}/2, \sqrt{2}/4)$$

resulting in the state complexity $(1,8,16,32,16,32,16,8,1)$ and the branch complexity $(1,2,2,4,2,4,4,8)$.

Note that if in the expression $\mathbf{l}[\Lambda_{16}] = (2\mathbf{l}[E_8], \mathbf{l}[E_8])$, we replace $\mathbf{l}[E_8]$ by $\mathbf{l}[E_8^{(3)}]$ (as given in Section 4.2), and substitute the result in (14), we obtain the values of $(1,6,16,24,16,24,16,6,1)$ which is the same as the bound given in (Forney, 1994) on the state complexity of Λ_{16}. However, we note that the squaring construction, and consequently the relationship $\mathbf{l}[\Lambda_{16}] = (2\mathbf{l}[E_8], \mathbf{l}[E_8])$, is not valid any more for this representation.

4.4. The Leech Lattice (Λ_{24})

Considering the Leech lattice obtained by applying the cubic construction[5] to the partition chain $2E_8/RE_8/E_8$, and using a similar approach as used for the BW_n lattices, it is straight-forward to show that the GS vectors of a KZ basis of Λ_{24} can be computed from,

$$\mathbf{G}[\Lambda_{24}] = \begin{bmatrix} 2\mathbf{G}[E_8] & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{G}[E_8]\mathbf{R} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{G}[E_8] \end{bmatrix}. \tag{35}$$

This results in $\mathbf{l}[\Lambda_{24}] = (4\mathbf{l}[E_8], 2\mathbf{l}[E_8], \mathbf{l}[E_8])$. By replacing $\mathbf{l}[E_8]$ in the expression given for $\mathbf{l}[\Lambda_{24}]$, we obtain the state complexity

$$(1,4,12,32,64,128,192,256,256,512,768,1024,1024,\ldots)$$

which is the same as the result reported in (Forney, 1994) based on intuition.

As an alternative, we could represent the underlying E_8 lattices via their complex (Gaussian) representation which would diagonalize (35), resulting in the standard co-ordinate system for the GS vectors of a

[5] Refer to (Forney, 1988) for definition.

KZ basis of Λ_{24}. We note that the cubic construction (which serves as the basis to derive the GS vectors of Λ_{24}) is still valid for this representation. Note that in this case the inequality in (20) is satisfied with equality. For this representation, we have $\mathbf{l}[E_8] = (4, 2, 2, 1)$ which results in $\bar{\mathbf{l}}[\Lambda_{24}] = (4, 2, 2, 1, 2, 1, 1, 0.5, 1, 0.5, 0.5, 0.25)$. Replacing $\bar{\mathbf{l}}[\Lambda_{24}]$ in (14) and (20), we obtain the state complexity

$$(1, 16, 64, 256, 256, 1024, 1024, \ldots),$$

and the branch complexity,

$$(1, 2, 2, 4, 2, 4, 4, 8, 4, 8, 8, 16).$$

5. Concluding remarks:

We have presented a systematic method for successive minimization of the state complexity of the self-dual lattices. This is based on the representation of lattices on the Gram-Schmidt vectors of one of their KZ reduced basis. We have given expressions for the corresponding co-ordinate system (and the resulting state complexity) for the K_{12}, Λ_{24}, and BW_n lattices. Using the proposed method, we have re-derived the trellis diagrams given in (Forney, 1994) based on intuition, in a systematic and unified approach. It is shown that for the complex Λ_{24} and BW_n lattices, the standard co-ordinate system successively minimizes the state complexity, while the resulting branch complexity at each section of the trellis meets certain lower bound. This results in a very efficient trellis representation for the complex Λ_{24} and BW_n lattices. Overall, it seems very unlikely that one can reduce the complexity of the trellis decoding of these lattices by a change of the co-ordinate system.

References

Forney, G. D., Coset codes–Part II: Binary lattices and related codes, *IEEE Trans. Inform. Theory,* vol. IT–34, pages 1152–1187, Sept. 1988.

Forney, G. D., Density/length profiles and trellis complexity of lattices, *IEEE Trans. Inform. Theory,* vol. IT–40, pages 1753–1772, Nov. 1994.

Forney, G. D., and Trott, M. D., The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders, *IEEE Trans. Inform. Theory,* vol. IT–39, pages 1491–1513, Sept. 1993.

Nemhauser, G. L., and Wolsey, L. A., *Integer and combinatorial optimization,* John Wiley & Sons Ltd. , 1988.

Cohen, H. "A course in computational algebraic number theory," Springer-Verlag, 1993.

Gruber, P. M. and Lekkerkerker, C. G., *Geometry of numbers*, Amsterdam : North-Holland, 1987.

Korkine, A., and Zolotareff, G., "Sure les formes quadratiques," *Math. Ann. 6*, pages 366-389, 1873.

Lagarias, J. C., Lenstra, H. W., and Schnorr, C. P., "Korkine Zolotareff bases and successive minima of a lattice and its reciprocal," *Combinatorica 10*, pages 333-348, 1990.

Kannan, P., "Minkowski's convex body theory and integer programming," *Mathematics of Operations Research,* vol. 12, No. 3, August 1987.

Schnorr, C. P., "A hierarchy of polynomial time lattice basis reduction algorithms," *Theoretical Computer Science 53*, pages 201-224, 1987.