Finding short vectors in a lattice of Voronoi’s first kind

Robby McKilliam and Alex Grant
Institute for Telecommunications Research, The University of South Australia, SA, 5095

Abstract—we show that for those lattices of Voronoi’s first kind, a vector of shortest nonzero Euclidean length can be computed in polynomial time by computing a minimum cut in a graph.

Index Terms—Lattices, short vectors, minimum cut.

I. INTRODUCTION

A $n$-dimensional lattice, $\Lambda$, is a discrete set of vectors from $\mathbb{R}^n$, $m \geq n$, formed by the integer linear combinations of a set of linearly independent basis vectors $b_1, \ldots, b_n$ from $\mathbb{R}^m$. That is, $\Lambda$, consists of all those vectors, or lattice points, $x \in \mathbb{R}^m$ satisfying

$$x = b_1 u_1 + b_2 u_2 + \cdots + b_n u_n \quad u_1, \ldots, u_n \in \mathbb{Z}.$$ 

An interesting question about a lattice is: ‘What is the shortest distance between any two lattice points?’ Because the origin is a lattice point this question can be equivalently stated as: ‘What is the length of the shortest lattice point not equal to the origin?’ Those points in the lattice with shortest length are called short vectors. The problem of discovering a lattice point of shortest length is called the shortest vector problem and has applications to, for example, cryptography [1]. In general, i.e. for arbitrary lattices, the shortest vector problem is NP-hard [2, 3]. However, for some lattices, the problem is easy to solve. For example, short vectors are relatively easy to determine in highly regular lattices, such as the root lattices $A_n$ and $D_n$, their dual lattices $A^*_n$ and $D^*_n$, and the integer lattice $\mathbb{Z}^n$ [4, Chap. 4].

In this paper we consider a particular class of lattices, those of Voronoi’s first kind [5–7]. We show that a short vector in a lattice of Voronoi’s first kind can be computed in polynomial time by computing a minimum cut in a graph. If the lattice has dimension $n$, this requires $O(n^3)$ operations to deterministically compute a short vector [8], or $O(n^2 \log n)^3$ operations to compute a short vector with high probability [9].

The paper is structured as follows. Section II defines the Voronoi cell and the relevant vectors. Section III defines lattices of Voronoi’s first kind and shows how their short vectors can be found by solving a constrained quadratic program in binary $\{0, 1\}$ variables. Section IV describes how this constrained program can be mapped into that of computing a minimum cut in a weighted graph. Some examples are given in Section V.

1Specifically, the shortest vector problem is known to be hard for NP under what are called reverse unfaithful random reductions [2].

II. VORONOI CELLS, RELEVANT VECTORS, AND SHORT VECTORS

The (open) Voronoi cell, denoted $\text{Vor}(\Lambda)$, of a lattice $\Lambda$ in $\mathbb{R}^n$ is the subset of $\mathbb{R}^n$ containing all points nearer, with respect to a given norm, the lattice point at the origin than any other lattice point. The Voronoi cell is an $n$-dimensional convex polytope that is symmetric about the origin. Here we will always assume the Euclidean norm (or 2-norm), so $\text{Vor}(\Lambda)$ contains those points nearest in Euclidean distance to the origin.

Equivalently the Voronoi cell can be defined as the intersection of the half spaces

$$H_v = \{ x \in \mathbb{R}^n \mid x \cdot v < \frac{1}{2} v \cdot v \}$$

for all $v \in \Lambda \setminus \{0\}$, i.e. all lattice points $v \in \Lambda$ not equal to the origin $0$. Here $x \cdot v$ is the inner product between vectors $x$ and $v$. It is not necessary to consider all $v \in \Lambda \setminus \{0\}$ to define the Voronoi cell. The minimal set of lattice vectors $R$ such that $\text{Vor}(\Lambda) = \cap_{v \in R} H_v$ is called the set of Voronoi relevant vectors or simply relevant vectors [7].

Definition 1. The relevant vectors $v \in \Lambda$ are those for which

$$v \cdot x < x \cdot x$$

for all $x \in \Lambda$ with $x \neq v$ and $x \neq 0$.

The short (or minimal) vectors in a lattice are all those lattice points of minimum nonzero Euclidean length, i.e all those of squared length

$$\min_{x \in \Lambda \setminus \{0\}} \|x\|^2.$$ 

Plainly, every short vector is also a relevant vector, because, if a lattice point $s$ is not relevant there exists a lattice point $x \neq s$ such that $x \cdot s < s \cdot s$, implying that $\|x\|^2 < \|s\|^2$, so $s$ is not a short vector.

III. LATTICES OF VORONOI’S FIRST KIND

An $n$-dimensional lattice $\Lambda$ is said to be of Voronoi’s first kind if it has what is called an obtuse superbase [5]. That is, there exists a set of $n + 1$ vectors $b_1, \ldots, b_{n+1}$ such that $b_1, \ldots, b_n$ are a basis for $\Lambda$,

$$b_1 + b_2 + \cdots + b_{n+1} = 0 \quad (1)$$

2These are the ‘strict’ relevant vectors according to Conway and Sloane [5]. If the inequality $v \cdot x < x \cdot x$ is replaced by $v \cdot x \leq x \cdot x$ then this would also include the ‘lax’ relevant vectors. The short vectors are always strict so we only have use of the strict relevant vectors here.
(the superbase condition), and the inner products satisfy,
\[ q_{ij} = b_i \cdot b_j \leq 0, \quad \text{for} \quad i, j = 1, \ldots, n + 1, i \neq j \]
(the obtuse condition). The \( q_{ij} \) are called the Selling parameters. It is known that all lattices in dimensions less than 4 are of Voronoi’s first kind \[5\]. An interesting property of lattices of Voronoi’s first kind is that their relevant vectors have a straightforward description.

**Theorem 1.** (Conway and Sloane \[3\] Theorem 3) The relevant vectors of \( \Lambda \) are of the form,
\[ \sum_{i \in I} b_i \]
where \( I \) is a strict subset of \( \{1, 2, \ldots, n + 1\} \) that is not empty, i.e. \( I \subset \{1, 2, \ldots, n + 1\} \) and \( I \neq \emptyset \).

Because each short vector is also a relevant vector we have the following corollary.

**Corollary 1.** The short vectors in \( \Lambda \) are of the form \( \sum_{i \in I} b_i \) where \( I \subset \{1, 2, \ldots, n + 1\} \) and \( I \neq \emptyset \).

Given this corollary a naïve way to compute a short vector is to compute the squared length \( \| \sum_{i \in C} b_i \|^2 \) for all of the \( 2^n - 2 \) possible \( I \) and return a lattice point with minimum squared length. This procedure requires a number of operations that grows exponentially with the dimension \( n \). We can improve this using a minimum cut algorithm. To facilitate this consider the quadratic form
\[ Q(u) = \| \sum_{i=1}^{n+1} b_i u_i \|^2 = \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} q_{ij} u_i u_j. \quad (2) \]

A short vector is a minimiser of this form under the constraint that the \( u_i \in \{0, 1\} \) and at least one element of \( u \) is equal to 1 and at least one element of \( u \) is equal to 0. The next section will show how this constrained quadratic minimisation problem can be solved by computing a minimum cut in a graph. This technique has appeared previously \[10, 12\] but we include the derivation here so that this paper is self-contained.

**IV. QUADRATIC \{0, 1\} PROGRAMS AND MINIMUM CUTS IN GRAPHS**

Let \( G = \{V, E\} \) be an undirected graph with \( n + 1 \) vertices \( v_1, v_2, \ldots, v_{n+1} \) contained in the set \( V \) and edges \( e_{ij} \in E \) connecting vertex \( v_i \) to vertex \( v_j \). To each edge we assign a weight (or capacity) \( w_{ij} \in \mathbb{R} \). The graph is undirected so the weights are symmetric, i.e. \( w_{ij} = w_{ji} \). A cut in the graph \( G \) is a nonempty subset \( C \subset V \) of vertices with its (also nonempty) complement \( \bar{C} \subset V \).

That is, a cut is the pair \((C, \bar{C})\) such that both \( C \) and \( \bar{C} \) are not empty, \( C \cap \bar{C} = \emptyset \) and \( C \cup \bar{C} = V \).

The weight of a cut is
\[ W(C, \bar{C}) = \sum_{i \in I} \sum_{j \in J} w_{ij}, \]
where \( I = \{i \mid v_i \in C\} \) and \( J = \{j \mid v_j \in \bar{C}\} \). That is, \( W(C, \bar{C}) \) is the sum of the weights on the edges crossing from the vertices in \( C \) to the vertices in \( \bar{C} \). If the graph is allowed to contain loops, i.e. edges from a vertex to itself, then the weight of these edges \( w_{ii} \) have no effect on the weight of any cut. We may choose any values for the \( w_{ii} \) without affecting \( W(C, \bar{C}) \).

The minimum cut is the \( C \) and \( \bar{C} \) that minimise the weight \( W(C, \bar{C}) \). Let \( |V| = n + 1 \) and \( |E| \leq 2(n+1)n \) denote the number of vertices and the number of edges in the graph \( G \).

If all of the edge weights \( w_{ij} \) for \( i \neq j \) are nonnegative, a minimum cut can be computed deterministically in order
\[ O(|V||E| + |V|^2 \log |V|) \in O(n^3) \]
operations using the algorithm of Stoer and Wagner \[8\] and with high probability in
\[ O(|V|^2 \log |V|) = O(n^2 \log(n))^3 \]
operations using the randomised algorithm of Karger and Stien \[9\].

We now show how \( W(C, \bar{C}) \) can be represented as a quadratic form. Define the vector \( u \) of length \( n + 1 \) so that
\[ u_i = \begin{cases} 1, & i \in C \\ 0, & i \in \bar{C} \end{cases}. \]

Then
\[ u_i(1 - u_j) = \begin{cases} 1, & i \in C, j \in \bar{C} \\ 0, & \text{otherwise}. \end{cases} \]

The weight can now be written as
\[ W(C, \bar{C}) = \sum_{i \in C} \sum_{j \in \bar{C}} w_{ij} = \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} w_{ij} u_i(1 - u_j) = F(u), \]
say. Finding a minimum cut is equivalent to finding the binary \( \{0, 1\} \) vector \( u \) that minimises \( F(u) \) under the constraint that at least one element in \( u \) is equal to 1 and at least one element in \( u \) is equal to 0. This constraint corresponds to the requirement that both \( C \) and \( \bar{C} \) are nonempty.

Expanding,
\[ F(u) = \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} w_{ij} u_i - \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} w_{ij} u_i u_j = \sum_{i=1}^{n+1} k_i u_i - \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} w_{ij} u_i u_j, \]
where \( k_i = \sum_{j=1}^{n+1} w_{ij} \). Observe the equivalence of \( F(u) \) and \( Q(u) \) from \[10\] when the weights are assigned according to,
\[ q_{ij} = -w_{ij} \quad \text{for} \quad i, j = 1, \ldots, n + 1. \]

Note that with these weights \( k_i = -\sum_{j=0}^{n+2} q_{ij} = 0 \) due to the superbase condition \[11\].

Because the \( q_{ij} \) are nonpositive for \( i \neq j \) the weights \( w_{ij} \) are nonnegative for all \( i \neq j \) with \( i, j \in \{1, n + 1\} \). As discussed the value of the weights \( w_{ii} \) have no effect on the weight of any cut so setting \( q_{ii} = -w_{ii} \) for \( i \in \{1, n + 1\} \) is of no consequence. A vector \( u \) that minimises \( Q(u) \) can be found...
by computing a minimum cut in the graph with these weights. A short vector is then given as $\sum_{i=1}^{n+1} b_i u_i$. This is our main result, so we restate it as a theorem.

**Theorem 2.** Let $\Lambda$ be a $n$-dimensional lattice of Voronoi’s first kind with obtuse superbase $b_1, \ldots, b_{n+1}$ and Selling parameters $q_{ij} = b_i \cdot b_j$. Let $G$ be a graph with $n + 1$ vertices $v_1, \ldots, v_{n+1}$ and edges $e_{ij}$ with weight $-q_{ij}$. Let $(C, C)$ be a minimum cut in the graph $G$. A short vector in the lattice $\Lambda$ is given by $\sum_{i \in I} b_i$ where $I = \{ i \mid v_i \in C \}$. The squared Euclidean length of the short vector is given by the weight of the minimum cut $W(C, C)$.

**V. SOME EXAMPLES**

As examples we apply this minimum cut approach to finding a short vector in the root lattice $A_n$ and its dual lattice $A^*_n$ [4, pp. 108-117]. An obtuse superbase for $A_n$ is all the cyclic shifts of the vector $[1 \ 1 \ 0 \ 0 \ \cdots \ 0]$ from $\mathbb{R}^{n+1}$. Set the vectors,

$$
b_1 = [1 \ -1 \ 0 \ 0 \ \cdots \ 0], \quad b_2 = [0 \ 1 \ -1 \ 0 \ \cdots \ 0], \quad \cdots, \quad b_{n+1} = [-1 \ 0 \ 0 \ \cdots \ 0 \ 1].
$$

The Selling parameters are

$$q_{ij} = b_i \cdot b_j = \begin{cases} 2, & i = j \\ -1, & i-j \equiv 1 \mod n+1 \\ 0, & \text{otherwise}. \end{cases}$$

The corresponding weighted graph is the cycle graph with $n + 1$ vertices, each edge having weight 1. A minimum cut in this graph is to choose $C$ to contain $c$ consecutive vertices modulo $n + 1$, where $1 \leq c \leq n$. That is, choose

$$C = \{v_1, v_{i+1}, \ldots, v_{i+c}\}$$

for any integer $i$ where the indices are considered modulo $n + 1$. The weight of such a cut is 2. A short vector in $A_n$ is correspondingly of the form

$$\sum_{j=i}^{i+c} b_{j+c} = c_i - c_{i+c}$$

where $c_i \in \mathbb{R}^{n+1}$ denotes a vector of all zeros except the $i$th element which is equal to one. Again, the indices here are considered modulo $n + 1$. The squared Euclidean length of this short vector is 2. It follows that short vectors in $A_n$ are of the form $c_i - c_j$ for $i, j \in \{1, \ldots, n+1\}$, $i \neq j$, a well known fact [4, pp. 108-117]. Figure [I] displays the graph corresponding to the lattice $A_3$.

An obtuse superbase for the dual lattice $A^*_n$ is all cyclic shifts of the vector

$$[\frac{n}{n+1} \ -\frac{1}{n+1} \ \cdots \ -\frac{1}{n+1}] \in \mathbb{R}^{n+1}.$$

Set the vectors,

$$b_1 = \begin{bmatrix} \frac{n}{n+1} & -\frac{1}{n+1} & -\frac{1}{n+1} & \cdots & -\frac{1}{n+1} \end{bmatrix},$$

$$b_2 = \begin{bmatrix} -\frac{1}{n+1} & \frac{n}{n+1} & -\frac{1}{n+1} & \cdots & -\frac{1}{n+1} \end{bmatrix},$$

$$\vdots,$$

$$b_{n+1} = \begin{bmatrix} -\frac{1}{n+1} & -\frac{1}{n+1} & -\frac{1}{n+1} & \cdots & \frac{n}{n+1} \end{bmatrix}.$$

The Selling parameters are

$$q_{ij} = b_i \cdot b_j = \begin{cases} \frac{n}{n+1}, & i = j \\ \frac{1}{n+1}, & \text{otherwise}. \end{cases}$$

The corresponding graph is the complete graph with $n + 1$ vertices and $\frac{n}{2}(n+1)$ edges, each edge having weight $\frac{1}{n+1}$. As each weight is equal and the graph is complete, a minimum cut is given by placing precisely one vertex into $C$ and the remaining vertices into $\bar{C}$. The weight of this cut is $\frac{n}{n+1}$. All the superbase vectors $b_1, \ldots, b_{n+1}$ are short vectors of squared Euclidean length $\frac{n}{n+1}$, again a well known fact [4, pp. 108-117]. Figure [I] shows the graph corresponding to the lattice $A_3^*$.

In both of the previous examples short vectors could be obtained by picking one of the vectors $b_1, \ldots, b_{n+1}$ in the obtuse superbase. This is not always the case, as our final example will show. Consider the 3-dimensional lattice with obtuse superbase

$$b_1 = \begin{bmatrix} 1 & -\frac{1}{2} & 0 \end{bmatrix},$$

$$b_2 = \begin{bmatrix} -\frac{1}{2} & 1 & 0 \end{bmatrix},$$

$$b_3 = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix},$$

$$b_4 = \begin{bmatrix} -\frac{1}{2} & -\frac{1}{2} & -1 \end{bmatrix}. \quad (3)$$

The Selling parameters are given in matrix form as

$$[q_{11} \ q_{12} \ q_{13} \ q_{14} \ q_{21} \ q_{22} \ q_{23} \ q_{24} \ q_{31} \ q_{32} \ q_{33} \ q_{34} \ q_{41} \ q_{42} \ q_{43} \ q_{44}] = \begin{bmatrix} \frac{5}{4} & -1 & 0 & -\frac{1}{4} \\ -1 & \frac{5}{4} & 0 & -\frac{1}{4} \\ 0 & 1 & -1 & 0 \\ -\frac{1}{4} & -\frac{1}{4} & -1 & \frac{3}{4} \end{bmatrix}. \quad (4)$$

Figure [I] displays the corresponding graph. The minimum cut is given by choosing $C = \{v_1, v_2\}$ and $\bar{C} = \{v_3, v_4\}$. This corresponds to the short vector

$$b_1 + b_2 = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$$

of squared Euclidean length $\frac{3}{2}$. Note that each of $b_1, b_2, b_3$ and $b_4$ have squared Euclidean length greater than $\frac{3}{2}$ and are therefore not short vectors.

**VI. CONCLUSION**

We have described a method from computing a short vector in a lattice of Voronoi’s first kind. This is achieved by mapping the shortest vector problem into that of computing a minimum cut in a weighted graph. Existing polynomial time algorithms can then be applied [8, 9].
Fig. 1. Graph corresponding to the lattice $A_3$.

Fig. 2. Graph corresponding to the lattice $A_3^*$.

Fig. 3. Graph corresponding to the lattice with superbase given by $\mathbf{B}$.

REFERENCES

[1] D. Micciancio and O. Regev, “Lattice based cryptography,” in Post Quantum Cryptography, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds. Springer, 2009.

[2] D. Micciancio, “The hardness of the closest vector problem with preprocessing,” IEEE Trans. Inform. Theory, vol. 47, no. 3, pp. 1212–1215, 2001.

[3] M. Ajtai, “The shortest vector problem in $L_2$ is NP-hard for randomized reductions,” in Proc. 30th ACM Symposium on Theory of Computing, pp. 10–19, May 1998.

[4] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, Springer, New York, 3rd edition, 1998.

[5] J. H. Conway and N. J. A. Sloane, “Low-dimensional lattices. VI. Voronoi reduction of three-dimensional lattices,” Proceedings: Mathematical and Physical Sciences, vol. 436, no. 1896, pp. 55–68, 1992.

[6] F. Valentin, Sphere coverings, lattices, and tilings (in low dimensions), Ph.D. thesis, Zentrum Mathematik, Technische Universität München, November 2003.

[7] G.F. Voronoï, “Nouvelles applications des paramètres continus à la théorie des formes quadratiques,” Journal für die reine und angewandte Mathematik, pp. 97–178, 1908.

[8] M. Stoer and F. Wagner, “A simple min-cut algorithm,” Journal of the ACM, vol. 44, no. 4, pp. 585–591, 1997.

[9] D. R. Karger and C. Stein, “A new approach to the minimum cut problem,” Journal of the ACM, vol. 43, no. 4, pp. 601–640, 1996.

[10] J. C. Picard and H. D. Ratliff, “Minimum cuts and related problems,” Networks, vol. 5, pp. 357–370, 1974.

[11] C. Sankaran and A. Ephremides, “Solving a class of optimum multiuser detection problems with polynomial complexity,” IEEE Trans. Inform. Theory, vol. 44, no. 5, pp. 1958–1961, Sep. 1998.

[12] S. Ulukus and R.D. Yates, “Optimum multiuser detection is tractable for synchronous CDMA systems using m-sequences,” IEEE Comms. Letters, vol. 2, no. 4, pp. 89–91, Apr. 1998.