On the bases of $\mathbb{Z}^n$ lattice

Shashank K Mehta[1] and Mahesh Sreekumar Rajasree[2]

[1] skmehta@cse.iitk.ac.in
[2] mahesr@cse.iitk.ac.in
Indian Institute of Technology, Kanpur, India

Abstract. In this paper, we investigate some "good" bases of lattices in which the shortest vector problem and the closest vector problems may be easy to solve. Our focus remains primarily on $\mathbb{Z}^n$. The motivation behind studying such bases for $\mathbb{Z}^n$ is to find better algorithms for the $\mathbb{Z}^n$-isomorphism problem which is known to be in NP $\cap$ Co-NP.

Keywords. Lattices, shortest vector problem, closest vector problem, $\mathbb{Z}^n$-isomorphism, lattice basis, Voronoi cell.

1 Introduction

A lattice is a discrete subgroup of the additive group of $\mathbb{R}^n$. It can be expressed as all the integer linear combinations of a set of linearly independent vectors, i.e., $\mathcal{L}(B) = \{\sum_i \alpha_i b_i | \alpha_i \in \mathbb{Z}\}$. The lattice $\mathbb{Z}^n$ is $\mathcal{L}(\{e_1, \ldots, e_n\})$, where e_i are orthogonal unit vectors. Lattices have been extensively used in computational number theory, cryptanalysis and building post-quantum cryptosystems. Such cryptosystems are built on the hardness of the Shortest-Vector problem (CVP) and Closest Vector problem (CVP) which are NP-hard. $\mathbb{Z}^n$ lattice is the simplest lattice with interesting properties such as existence of an orthonormal basis, the shortest vector has unit norm, CVP can be solved in polynomial time, etc. One of the most interesting problems related to the $\mathbb{Z}^n$ lattice is the $\mathbb{Z}^n$-isomorphism problem which asks whether a given lattice $\mathcal{L}$ is isomorphic to $\mathbb{Z}^n$. Similar to Graph-Isomorphism problem, it is still unknown whether there exists a polynomial time algorithm for $\mathbb{Z}^n$ isomorphism. A trivial solution to this problem is to check whether $\mathcal{L}$ has an orthonormal basis. This motivated us to study various bases of $\mathbb{Z}^n$.

Prior works

There has been numerous work on the study of bases for general lattices. The Korkin-Zolotarev bases are bases with a variety of "good" properties [1] but computing such bases takes super-exponential time [2]. The LLL bases [3] can be computed in polynomial time but the vectors in the bases have norms that are exponentially larger than the shortest vectors. In [4], the author gave a hierarchy of polynomial time lattice basis reduction algorithms that stretch from LLL to Korkine–Zolotareff.

The generalisation of $\mathbb{Z}^n$ isomorphism problem is the lattice isomorphism problem which asks whether two given lattices are isomorphic to each other or not. Haviv and Regev [5] gave an exponential time algorithm to solve this problem. Hunkenschroder [6] shows that $\mathbb{Z}^n$ isomorhpism is in NP $\cap$ Co-NP. Lenstra and Silverberg [7] showed that when the lattice is given with enough symmetry, they can construct a deterministic polynomial-time algorithm to solve $\mathbb{Z}^n$ isomorphism.

Our contributions:-

The following are the major results presented in this paper.

1. We first show that any primitive vector v in $\mathbb{Z}^n$ can be extended to a basis of $\mathbb{Z}^n$ in which all other vectors have smaller norm than v.
2. We reduce SVP in any lattice isomorphic to $\mathbb{Z}^n$ to SVP in $(n-1)$ dimensional sublattice of $\mathbb{Z}^n$.
3. We introduce two new classes of lattice bases called AMDV and AMDS and show that if a basis of $\mathbb{Z}^n$ belongs to both these classes, then it must be $\{e_1, \ldots, e_n\}$. Introducing yet another class of bases, CMB, we give another condition for $\mathbb{Z}^n$ basis to be $\{e_1, \ldots, e_n\}$ however it is only a sufficient condition.
4. We show that any vector that belongs to any SMP (Successive Minima Problem) solution is Voronoi relevant. This result leads to a new lower bound for the norm of the largest Voronoi relevant vector. We also show that a Compact basis of $\mathbb{Z}^n$ can have exponentially large norm and deduce a new upperbound for Compact bases of $\mathbb{Z}^n$.

2 Preliminaries

2.1 Definitions and Notations

In this paper $\mathbb{Z}$ and $\mathbb{R}$ will denote the sets of integers and reals respectively. Vectors will be denoted by small case as in v. Capital boldface letters will denote a set of vectors. These symbols will also be interpreted as matrices in which the member vectors are columns. We will use both interpretations interchangeably for bases. Let $\mathbf{B} = \{b_1, \ldots, b_k\}$ be a set of vectors in $\mathbb{R}^n$. The subspace of $\mathbb{R}^n$ spanned by $\mathbf{B}$ will be denoted by $span(\mathbf{B})$. The norm of a vector $v = (v_1, \ldots, v_n)$ refers to the l_2-norm, i.e., $||v|| = \sqrt{\sum_i v_i^2}$. The norm of $\mathbf{B}$ is defined as $||\mathbf{B}|| = \max\{||b|| \mid b \in \mathbf{B}\}$. For any two sets of vectors $\mathbf{U}$ and $\mathbf{V}$, $\mathbf{U} + \mathbf{V}$ denotes the set $\{u + v \mid u \in \mathbf{U}, v \in \mathbf{V}\}$.

Definition 1 (Lattice). *Given a set of linearly independent vectors $\mathbf{B} = \{b_1, \ldots, b_m\}$ in the vector space $\mathbb{R}^n$, the lattice, $\mathcal{L}(\mathbf{B})$, spanned by $\mathbf{B}$ is the integer span of $\mathbf{B}$, i.e., $\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{m} \alpha_i . b_i | \alpha_i \in \mathbb{Z}\}$. In the matrix notation for $\mathbf{B}$ it is $\{\mathbf{B} \cdot z | z \in \mathbb{Z}^n\}$. $\mathbf{B}$ is called a* basis *for $\mathcal{L}(\mathbf{B})$. The dimension of $\mathcal{L}(\mathbf{B})$ is n and the rank is m. If $\mathcal{L}'$ and $\mathcal{L}$ are lattices such that $\mathcal{L}' \subseteq \mathcal{L}$, then the former is called a sublattice of the latter.*

A vector v in a lattice is called *primitive* if $(1/k).v$ does not belong to the lattice for any integer $|k| > 1$. Let $\mathbf{B}'$ be the result of adding the α (an integer) multiple of the j-th column to the i-th column in $\mathbf{B}$. Then it is easy to verify that $\mathcal{L}(\mathbf{B}') = \mathcal{L}(\mathbf{B})$. More generally, two sets $\mathbf{B}$ and $\mathbf{B}'$ are both bases of the same lattice if and only if $\mathbf{B}' = \mathbf{B} \cdot \mathbf{U}$ where $\mathbf{U}$ is a unimodular matrix.
Let $u, v_1, \ldots, v_k$ be vectors in $\mathbb{R}^n$. If the norm of $u' = u + \sum_{i=1}^{k} \alpha_i.v_i$ is less than $||u||$, where $\alpha_i \in \mathbb{Z}$, then u' is called a *reduction* of u by $\{v_1, \ldots, v_k\}$. Vector u is said to be irreducible by a set of vectors $\mathbf{V}$ if the vectors in $\mathbf{V}$ cannot reduce it.

Definition 2. *$Red(u, \mathbf{V})$ denotes any vector u' which is a reduction of u by $\mathbf{V}$ and it is not further reducible by it. Observe that $Red(u, \mathbf{V})$ is not unique.*

Following is a trivial result.

Lemma 1. *Let $\mathbf{B} = \{b_1, b_2, \ldots . b_n\}$ be a basis of $\mathcal{L}$ and Let $b_i' = Red(b_i, \mathbf{B} \setminus \{b_i\})$. Then $\{b_1, \ldots, b_{i-1}, b_i', b_{i+1}, \ldots, b_n\}$ is also a basis of $\mathcal{L}$.*

A useful property related to lattices is the existence of the dual lattice.

Definition 3. *Let $\mathcal{L}$ be a lattice of dimension n and rank n and $\mathbf{B}$ be a basis for it. Then $\mathbf{D} = (\mathbf{B}^T)^{-1}$ is called the dual basis of $\mathbf{B}$. The lattice spanned by $\mathbf{D}$ (in the same ambient space), $\mathcal{L}^*$, is independent of the choice of $\mathbf{B}$. That is, $\mathcal{L}^*$ is unique for $\mathcal{L}$ and it is called the* dual *of $\mathcal{L}$. It is easy to see that the dual of the dual is the primal lattice.*

Lattice $\mathbb{Z}^n$ is self dual, i.e., it is its own dual lattice.

2.2 Lattice Related Problems

Some of the interesting problems related to lattices are as follows.

Definition 4 (Shortest Vector Problem (SVP)). *Given a basis $\mathbf{B}$, find a shortest non-zero vector v in the lattice $\mathcal{L}(\mathbf{B})$, i.e., $0 < ||v|| \leq ||u||$ for all $u \in \mathcal{L}(\mathbf{B}) \setminus \{0\}$.*

Definition 5 (Closest Vector Problem (CVP)). *Given a lattice basis $\mathbf{B}$ and an arbitrary vector t in the ambient space, find the vector v in the lattice $\mathcal{L}(\mathbf{B})$ which is closest to t, i.e., $||v - t|| \leq ||u - t||$ for all $u \in \mathcal{L}(\mathbf{B})$.*

Definition 6 (Successive Minima). *The i^{th} successive minimum $\lambda_i(\mathcal{L})$ for a lattice $\mathcal{L}$ is the radius of the smallest sphere centered at the origin containing at least i linearly independent lattice vectors. So*

$$\lambda_i(\mathcal{L}) = inf\,\{r \mid dim(span(\mathcal{L} \cap \mathcal{B}(0, r))) \geq i\}$$

where $\mathcal{B}(0, r)$ (ball of radius r) denotes the set of vectors in the ambient space with norm at most r.

A direct consequence of this definition is as follows.

Claim. Let $S = \{v_1, \ldots, v_k\}$ be a linearly independent set of vectors of a lattice $\mathcal{L}$. Then there exists a $v \in S$ such that $||v|| \geq \lambda_k$.

Definition 7 (Successive Minima Problem (SMP)). *Given a basis* $\mathbf{B}$ *of a lattice* $\mathcal{L}$*, find linearly independent lattice vectors* $s_1, s_2, \ldots, s_n$ *such that* $\forall i, ||s_i|| = \lambda_i(\mathcal{L})$.

Theorem 1 (Corollary 4, [8]). *There is a dimension and rank preserving reduction from SMP to CVP. The reduction calls the CVP oracle* $poly(n, b)$ *times where* b *is the number of input bits.*

Most interesting lattice problems are reducible to SVP and CVP. One of the main challenges in the study of lattices is to find a "good" basis in which SVP and CVP are easy to solve. For example$\{e_1, e_2, \ldots, e_n\}$ is a good basis of $\mathbb{Z}^n$. One way to characterize the concept of "good" basis is that a shortest vector of the lattice belongs to it so SVP becomes a trivial task. Additionally, for any lattice vector v its neighbouring lattice vectors are given by $\{v + \mathbf{B} \cdot z |\ z \in \{-1, 0, 1\}^n\}$. This property makes CVP an easy problem to solve. Most lattices do not have such an ideal basis. But our attempt in this paper is to find bases which are close to the ideal basis.

2.3 Hyperplane Sublattice and Basis

The $(n-1)$-dimensional subspace perpendicular to an integer vector in $\mathbb{R}^n$ is called a *rational subspace*. An $(n-1)$-dimensional subspace of $\mathbb{R}^n$ contains an $(n-1)$-dimensional sublattice of $\mathbb{Z}^n$ if and only if it is a rational subspace. We generalize the terminology to arbitrary lattice. Let $\mathcal{L}$ be any lattice in $\mathbb{R}^n$. An $(n-1)$ dimensional subspace is said to be *pseudo rational* if it contains an $(n-1)$-dimensional sublattice of $\mathcal{L}$. In this section subspace will only refer to $(n-1)$-dimensional subspace. The sublattice contained in a pseudo rational subspace will be called a *hyperplane sublattice*. Let S_0 be a pseudo rational subspace and $\mathcal{L}'$ denote the sublattice contained in it. Let $\mathbf{B}$ be a basis of $\mathcal{L}$ and $\mathbf{B}_1$ be a basis of $\mathcal{L}'$ expressed as an $(n-1) \times (n-1)$ matrix. Then it can be shown that the distance between S_0 and the nearest hyperplane parallel to S_0 that contains at least one lattice point is $Det(\mathbf{B})/Det(\mathbf{B}_1)$. Let the sequence $\ldots, S_{-2}, S_{-1}, S_0, S_1, S_2, \ldots$ denote the successive hyperplanes parallel to S_0 each of which contains at least one $\mathcal{L}$ point. Since a lattice is invariant under the translation from one lattice point to another, the distance between S_i and S_{i+1} is also $Det(\mathbf{B})/Det(\mathbf{B}_1)$ for all i.
There is an important relationship between the bases of $\mathcal{L}$ and the bases of the hyperplane sublatices. If $\mathbf{B}_1 = \{b_2, \ldots, b_n\}$ is a basis of the hyperplane sublattice of S_0 and $b_1 \in S_1 \cap \mathcal{L}$, then $\{b_1, b_2, \ldots, b_n\}$ is a basis of $\mathcal{L}$. Conversely if $\mathbf{B} = \{b_1, \ldots, b_n\}$ is a basis of $\mathcal{L}$ and $\{b_2, \ldots, b_n\}$ spans S_0, then b_1 belongs to the corresponding hyperplane S_1. Such pairs of b_1 and S_0 will be called mutually *compatible*. Some times we may say b_1 is compatible to $\{b_2, \ldots, b_n\}$ or the other way around, where the concerned pseudo-rational subspace is $span(b_2, \ldots, b_n)$ and the vectors, $b_2, \ldots, b_n$, form a basis of the hyperplane sublattice on this pseudo-rational subspace.

Let us show the relation between all compatible vectors to a given pseudo-rational subspace of a lattice. Similarly the relation between the compatible subspaces to a given lattice vector.

Lemma 2. *Let S_0 be a pseudo rational subspace of a lattice with a sublattice basis $\mathbf{B}_1 = [b_2, b_3, \ldots, b_n]$ and b_1 be a lattice vector which are mutually compatible. Then (i) any compatible vector to S_0 is given by $b_1 + \sum_{i=2}^{n} \alpha_i.b_i$ for some integer coefficients α_i. (ii) Every pseudo-rational subspace compatible with b_1 has a sublattice basis $[b_2 - \alpha_1.b_1, b_3 - \alpha_3.b_1, \ldots, b_n - \alpha_n.b_1]$ where α_i are integer coefficients.*

Proof. (i) Suppose $\mathbf{B}' = [b_1', b_2, \ldots, b_n]$ is also a basis of the whole lattice, then b_1' must also belong to S_1, the next parallel hyperplane with lattice points. Then $b_1' = b_1 + v$ where $v \in \mathcal{L}(\mathbf{B}_1)$. So $b_1' = b_1 + \sum_{i=2}^{n} \alpha_i.b_i$ for some $\alpha_i \in \mathbb{Z}$.
(ii) Let $[b_2, \ldots, b_n]$ be compatible with b_1 so $\mathbf{B} = [b_1, b_2, \ldots, b_n]$ is a lattice basis. Its dual is $\mathbf{D} = (\mathbf{B}^T)^{-1} = [d_1, d_2, \ldots, d_n]$. So d_1 is perpendicular to S_0 and b_1 is perpendicular to the subspace of $[d_2, d_3, \ldots, d_n]$. By definition d_1 and the subspace of $[d_2, \ldots, d_n]$ are compatible w.r.t. the dual lattice.
Suppose $\mathbf{B}_1'$ spans the hyperplane sublattice corresponding to another subspace compatible to b_1. Let its normal be d_1'. The dual of $\mathbf{B}' = [b_1, b_2', \ldots, b_n']$ is of the form $[d_1', d_2, \ldots, d_n]$. So $[d_1', d_2, \ldots, d_n]$ is also a basis of the dual lattice $\mathcal{L}^*$. Hence d_1' is another compatible vector for $[d_2, \ldots, d_n]$. From the first part, there exist integers α_i such that $d_1' = d_1 + \sum_{i=2}^{n} \alpha_i.d_i$. The dual of $[d_1 + \sum_{i=2}^{n} \alpha_i.d_i, d_2, \ldots, d_n]$ is $[b_1, b_2 - \alpha_2.b_1, \ldots, b_n - \alpha_n.b_1]$. Then $[b_2', \ldots, b_n']$ and $[b_1, b_2 - \alpha_2.b_1, \ldots, b_n - \alpha_n.b_1]$ are bases of the same hyperplane sublattice, perpendicular to d_1'. □

2.4 Some useful facts about $\mathbb{Z}^n$

Finally let us discuss the lattice $\mathbb{Z}^n$ which is the set of all integer vectors. Any set $\mathbf{B}$, of n linearly independent n-dimensional integer vectors, spans a sublattice of $\mathbb{Z}^n$ because its integer-span contains only integer vectors. A necessary and sufficient condition that $\mathcal{L}(\mathbf{B}) = \mathbb{Z}^n$ is that $\mathbf{B}$ contains only integer vectors and the density of lattice points in $\mathcal{L}(\mathbf{B})$ is equal to that of $\mathbb{Z}^n$, which is 1. Hence $\mathcal{L}(\mathbf{B}) = \mathbb{Z}^n$ if and only if $\mathbf{B}$ is an $n \times n$ integer matrix and the $Det(\mathbf{B}) = 1$, i.e., B is a unimodular matrix. Thus it is polynomially decidable whether a given basis generates $\mathbb{Z}^n$.
Now let us consider the case when the basis vectors are not specified in the reference frame $\{e_1, e_2, \ldots, e_n\}$. Suppose $\mathbf{B} = \{b_1, \ldots, b_n\}$ is a basis of $\mathbb{Z}^n$ however in some rotated/reflected reference frame. So there exists an orthonormal matrix R such that $\{R \cdot b_1, \ldots, R \cdot b_n\}$ is a basis of $\mathbb{Z}^n$.

Definition 8 ($\mathbb{Z}^n$ Isomorphism Problem). *Given a linearly independent set of n-dimensional real vectors $\mathbf{B} = \{b_1, \ldots, b_n\}$, the lattice $\mathcal{L}(\mathbf{B})$ is called* isomorphic to $\mathbb{Z}^n$ *if there exists an orthonormal transformation matrix R such that $\mathbf{B}' = \{R \cdot b_1, \ldots, R \cdot b_n\}$ is a basis of $\mathbb{Z}^n$. The $\mathbb{Z}^n$ Isomorphism problem is to determine whether the lattice generated by a given basis is isomorphic to $\mathbb{Z}^n$.*

We have shown that a matrix U is a basis of $\mathbb{Z}^n$ if and only if its is a unimodular matrix. Consider any $\mathcal{L}$, isomorphic to $\mathbb{Z}^n$. A matrix $\mathbf{B}$ is a basis of $\mathcal{L}$ if and only if there exists an orthonormal matrix $\mathbf{R}$ and a unimodular matrix $\mathbf{U}$ such that $\mathbf{B} = \mathbf{R} \cdot \mathbf{U}$.
Before ending this section let us state two necessary conditions for $\mathbb{Z}^n$ isomorphism. We know that $\mathbb{Z}^n$ is self dual because transpose and inverse of a unimodular matrix is also unimodular. If B is a basis of a lattice isomorphic to $\mathbb{Z}^n$ and D is its dual, then self duality implies that $D \subset \mathcal{L}(B)$. We have the following result.

Lemma 3. *Let B be a basis of a full rank lattice in $\mathbb{R}^n$. Then if $Det(B) \neq 1$ or $D \not\subset \mathcal{L}(B)$ where D is dual of B, then $\mathcal{L}(B)$ is not isomorphic to $\mathbb{Z}^n$. Both these conditions can be decided in polynomial time.*

3 Extending a vector into a $\mathbb{Z}^n$ basis

In this section we present results about extending a primitive vector to a basis of $\mathbb{Z}^n$. We first state a result from [9].

Lemma 4 (Theorem 2, [9]). *Let $\{a_1, \ldots, a_n\}$ be a multiset of positive integers. Let $m = max\{a_1, \ldots, a_n\}$ and $g_k = gcd(a_k, \ldots, a_n)$, then there exists an integer solution to the equation $x_1a_1 + \cdots + x_na_n = g_1$ which satisfies $-\frac{g_{j+1}}{2g_j} < x_j \leq \frac{g_{j+1}}{2g_j}, \forall j \in [n-1]$ and $|x_n| \leq max(\frac{m}{2g_1}, 1)$.*

Corollary 1. *Let $gcd(a_1, a_2) = g$ and $x_1a_1 + x_2a_2 = g$. Then*

$$|x_1| \begin{cases} = 1 & \text{if } |a_1| = 1 \\ \leq |\frac{a_2}{2g}| & \text{if } |a_1| > 1 \end{cases} \tag{1}$$

Corollary 2. *Let b_1 be a primitive vector of $\mathbb{Z}^n$. Then, there exists a primitive vector $d_1 \in \mathbb{Z}^n$ such that $b_1.d_1 = 1$ and $||d_1|| \leq \max\{1, ||b_1||/2\}$.*

Proof. Without loss of generality, we can assume that the entries of $b_1 = [a_1, \ldots, a_n]$ are all positive integers and $1 \leq a_n \leq \cdots \leq a_1$. If $a_i = 1$, then $d_1 = e_i$ will suffice. Now we only need to consider the case that $a_i \geq 2$ for all i. Using Lemma 4, we know that there exists x_i such that $x_1a_1 + \cdots + x_na_n = 1$, where $|x_j| \leq g_{j+1}/(2g_j) \leq a_{j+1}/2, \forall j \in [n-1]$, and $|x_n| \leq a_1/2$.
Therefore, we have $x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \leq \frac{a_2^2 + \cdots + a_n^2 + a_1^2}{4} \leq ||b_1||^2/4$
The fact that $b_1 \cdot d_1 = 1$ implies that d_1 is primitive. □

Following is the main result of this section.

Theorem 2. *Let $v \in \mathbb{Z}^n$ be primitive vector such that $||v||^2 > 1$. Then, there exists a $\mathbb{Z}^n$-basis $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$ such that $b_n = v$ and $||b_n||^2 > ||b_i||^2, \forall i \in [n-1]$.*

Proof is in the Appendix.

4 Shortest vector in hyperplane lattice

In [10], the author showed that SVP is NP-complete in ℓ_∞ norm. Let $\mathcal{L}$ be a lattice isomorphic to $\mathbb{Z}^n$. In this section we will show that SVP in $\mathcal{L}$ can be polynomially reduced to SVP in hyperplane sublattice of $\mathcal{L}$. This result reduces the $\mathbb{Z}^n$ isomorphism problem into SVP on hyperplane sublattices.

Lemma 5. *Let $\mathcal{L}$ be a lattice isomorphic to $\mathbb{Z}^n$ where $n \geq 4$ and b be an arbitrary vector in $\mathcal{L}$. Let $\mathcal{L}_1$ denote the hyperplane sublattice of $\mathcal{L}$ on subspace perpendicular to b. Then the shortest vector v in $\mathcal{L}_1$ is either a unit vector or $||v|| \leq ||b||/\sqrt{2}$.*

Proof. To prove this claim we will work in the reference frame in which $\mathcal{L}$ is $\mathbb{Z}^n$. Let $b = (a_1, a_2, \ldots, a_n)$. Consider the case where $a_i = 0$ for some i. Then $e_i \in \mathcal{L}_1$
Now consider the case where all the components of b are non-zero. Let a_i and a_j be the two magnitude-wise smallest components of b, i.e., $|a_i| \leq |a_j| \leq |a_k|$ for all $k \in [n] \setminus \{i, j\}$. Let $u = (0, \ldots, -a_j, 0 \ldots, 0, a_i, 0, \ldots)$ where the i-th component is $-a_j$ and the j-th component is a_i. Clearly u is perpendicular to b so u belongs to $\mathcal{L}_1$. Further, $||u||^2 = a_i^2 + a_j^2 \leq (2/n)||b||^2 \leq (1/2)||b||^2$. □

This result suggests an algorithm to compute a shortest vector in any lattice isomorphic to $\mathbb{Z}^n$ by iteratively computing the *shortest vector* on hyperplane sublattices. Start with an arbitrary vector, b, from $\mathcal{L}$. If b is a unit vector then the task is over. Otherwise compute the hyperplane sublattice, $\mathcal{L}_1$, of $\mathcal{L}$ perpendicular to b. Compute a shortest vector b_1 in $\mathcal{L}_1$. Then either b_1 is a unit vector (which is the desired result) or $||b_1|| \leq ||b||/\sqrt{2}$. Thus b_1 is the new b and we repeat this step. This algorithm requires at most $2. \log_2 ||b||$ iterations. Hence we have the following result.

Theorem 3. *SVP on any lattice isomorphic to $\mathbb{Z}^n$ can be solved using polynomially many calls to an oracle that solves SVP on a hyperplane sublattice of $\mathcal{L}$.*

One way to solve $\mathbb{Z}^n$ isomorphism is to solve SVP. If the shortest vector is a unit vector s_1, then compute the subspace perpendicular to s_1, determine a basis of the corresponding hyperplane sublattice and recursively prove that this sublattice is isomorphic to $\mathbb{Z}^{n-1}$. If the shortest vector is not a unit vector, then the given lattice cannot be isomorphic to $\mathbb{Z}^n$.

Corollary 3. *$\mathbb{Z}^n$ isomorphism problem can be reduced to SVP on hyperplane sublattice of a $\mathbb{Z}^n$-isomorphic lattice.*

5 Min distance vector and Max distance subspace

Definition 9 (Minimum Distance Vector (MDV)). *Let $\mathcal{L}$ be a lattice and S_0 be a pseudo-rational subspace of $\mathcal{L}$. A shortest lattice vector compatible with S_0 is called MDV of S_0.*

Definition 10 (Maximum Distance Subspace (MDS)). *Let b_1 be any primitive vector of a lattice. Then that b_1-compatible subspace is the MDS of b_1, to which the perpendicular drop from the point b_1 to the subspace is longest (equivalently the projection of b_1 on the subspace is the shortest).*

Lemma 6. *Let S be a pseudo-rational subspace of some lattice. That lattice vector b, compatible with S, is its MDV for which $||d||.\sin\theta$ is minimum where d is a normal to S and θ is the angle between d and b.*

Lemma 7. *Let b be a primitive vector of a lattice. Then that b-compatible subspace S is its MDS for which $||b||.\cos\theta$ is maximum, where θ is the angle between b and the normal of S.*

Corollary 4. *Let $\mathbf{B} = [b_1, b_2, \ldots, b_n]$ be a lattice basis and $\mathbf{D} = [d_1, \ldots, d_n]$ be its dual basis. Then, b_1 is MDV of $[b_2, \ldots, b_n]$ if and only if $[d_2, \ldots, d_n]$ is MDS of d_1.*

Proof. Recall that b_1 is normal to $Span(d_2, \ldots, d_n)$ and d_1 is normal to $span(b_2, \ldots, b_n)$. Then b_1 is MDV of $[b_2, \ldots, b_n]$ if and only if $b_1.\sin\theta$ is minimum if and only if $d_1.\cos\theta$ is maximum if and only if $[d_2, d_3, \ldots, d_n]$ is MDS of d_1. □

One of the consequences of Lemma 2 is the following result.

Lemma 8. *Let $\{b_1, b_2, \ldots, b_n\}$ be a basis of a lattice. Then the MDV of $[b_2, \ldots, b_n]$ is $b_1 + \sum_{i=2}^{n} \alpha_i.b_i$ for some integers α_i.*
Similarly the MDS of b_1 has a sublattice basis given by $[b_2 - \alpha_2.b_1, \ldots, b_n - \alpha_n.b_1]$, where α_i are integers.

Following results shows that MDV and MDS properties together impose a strong condition.

Lemma 9. *Let $\mathbf{B} = \{b_1, \ldots, b_n\}$ be a basis of a lattice isomorphic to $\mathbb{Z}^n$. Let $\mathbf{D} = \{d_1, \ldots, d_n\}$ be its dual basis. If $||d_1|| \leq ||b_1||$ and $||b_1|| > 1$, then b_1 is not an MDV.*

Proof. First consider the case that $d_1 = e_1$. In this case $span(b_2, \ldots, b_n) = span(e_2, \ldots, e_n)$ which is isomorphic to $\mathbb{Z}^{n-1}$. If b_1 were MDV, then $b_1 = e_1$. This contradicts the given fact that $||b_1|| > 1$. Hence b_1 cannot be an MDV.
Now consider the case that $||d_1|| > 1$. Then $1 < ||d_1|| \leq ||b_1||$. From Corollary 2, there exists a primitive vector b_1' such that $d_1^T \cdot b_1' = 1$ and $||b_1'|| \leq \max\{1, ||d_1||/2\}$. So $||b_1'|| \leq \max\{1, ||b_1||/2\}$.
$d_1^T \cdot b_1 = d_1^T \cdot b_1'$ implies that the length of the projection of b_1' on d_1 is equal to that of b_1, namely, $1/||d_1||$. Hence b_1' is also compatible with $[b_2, \ldots, b_n]$, i.e., $[b_1', b_2, \ldots, b_n]$ is also a lattice basis. Since $||b_1'|| < ||b_1||$, b_1 cannot be an MDV. □

Theorem 4. *Let $\mathbf{B}$ be a basis of a lattice isomorphic to $\mathbb{Z}^n$. If b_1 is MDV of $[b_2, \ldots, b_n]$ and $[b_2, \ldots, b_n]$ is MDS of b_1, then $||b_1|| = 1$.*

Proof. Let $\mathbf{B} = [b_1, \ldots, b_n]$ be a basis and $\mathbf{D} = [d_1, \ldots, d_n]$ be its dual. Suppose b_1 is the MDV $[b_2, \ldots, b_n]$ and $[b_2, \ldots, b_n]$ be the MDS of b_1. From Corollary 4 d_1 is MDV of $[d_2, \ldots, d_n]$.
Suppose $||d_1|| \leq ||b_1||$. Since b_1 is MDV, from Lemma 9, $||b_1|| = 1$. Hence $||d_1|| = 1$. Same argument applies to the case $||b_1|| \leq ||d_1||$. Hence in either case b_1 and d_1 are both unit vectors. □

Corollary 5. *If* $\mathbf{B}$ *is a basis of a lattice isomorphic to* $\mathbb{Z}^n$ *such that for all* $i \in [n]$, b_i *is MDV of* $\mathbf{B} \setminus \{b_i\}$ *and* $\mathbf{B} \setminus \{b_i\}$ *is MDS of* b_i, *then* $\mathbf{B}$ *is orthonormal.*

6 On AMDV bases

In this section we investigate the bases, $\mathbf{B} = \{b_1, \ldots, b_n\}$, in which b_i is the MDV of $\mathbf{B} \setminus \{b_i\}$ for each i. Such a basis will be called an AMDV (all MDV) basis. It is easy to see that if D is the dual of an AMDV basis, then D is an AMDS (all MDS) basis of the dual lattice.

Corollary 6. *Let* $\mathcal{L}$ *be a lattice isomorphic to* $\mathbb{Z}^n$. *Let* $\mathbf{B} = [b_1, \ldots, b_n]$ *be an AMDV basis of* $\mathcal{L}$ *and* $[d_1, \ldots, d_n]$ *be its dual. Then for each* i, *either* $||b_i|| = 1$ *or* $||b_i|| < ||d_i||$.

Lemma 10. $\{e_1, \ldots, e_n\}$ *is the only* $\mathbb{Z}^n$ *basis which is AMDV and totally unimodular.*

Proof. Let $\mathbf{B} = [b_1, \ldots, b_n]$ be an AMDV basis of $\mathbb{Z}^n$ which is also totally unimodular. If any b_i is a unit vector, then $\mathbf{B} \setminus \{b_i\}$ must span $\mathbb{Z}^{n-1}$. In this case we can reduce the problem to $(n-1)$ dimensions.
So to assume the contrary we assume that $||b_i|| > 1, \forall i \in [n]$. The inverse matrix $\mathbf{B}^{-1} = [c_1, \ldots, c_n]$ is also a totally unimodular matrix, i.e., $\mathbf{B}^{-1} \in \{-1, 0, 1\}^{n \times n}$. Without loss of generality, we can assume that $(\mathbf{B}^{-1})_{1,1} = 1$. This implies that $\mathbf{B}c_1 = e_1$, i.e., $||b_1|| > 1 = ||\mathbf{B}c_1|| = ||b_1 + \sum_{j=2}^{n} (c_1)_j . b_j||$. This means that b_1 is not MDV. □

Next we will investigate whether the only AMDV basis of $\mathbb{Z}^n$ is $\{e_1, \ldots, e_n\}$?

6.1 AMDV and Cascaded Minimal Basis

To study AMDV bases we first define a new class of bases called *cascaded minimal bases.*

Definition 11. *Let* $\mathcal{L}$ *be any lattice in* $\mathbb{R}^n$. *Then* $\mathbf{B} = \{b_1, \ldots, b_n\}$ *is* cascaded minimal basis or CMB *if for each* i, b_i *is a shortest vector in the sublattice spanned by* $\{b_i, b_{i+1}, \ldots, b_n\}$ *and the* b_i *is irreducible by the set* $\{b_1, b_2, \ldots, b_{i-1}\}$.

Algorithm 1, given in the Appendix, computes a CMB of an arbitrary lattice, proving the existence of CMB in every lattice. We will prove the correctness of this algorithm however will not analyse its time complexity because our objective is only to show the existence of this type of basis.

Given a basis $b_1, b_2, \ldots, b_n$ of a lattice, we say that b_i satisfies property P_1 if b_i is a shortest vector in $\mathcal{L}(b_i, b_{i+1}, \ldots, b_n\})$. Further we say that it satisfies property P_2 if b_i is irreducible by $\{b_1, \ldots, b_{i-1}\}$.
From Lemma 1 we know that after each iteration the set $\{b_1, \ldots, b_n\}$ remains a basis of $\mathcal{L}$. Also replacing $b_i, \ldots, b_n$ by $b'_i, \ldots, b'_n$ in the basis results into another basis if $\mathcal{L}(b_i, \ldots, b_n) = \mathcal{L}(b'_i, \ldots, b'_n)$.
Now to argue that the process will terminate, let us define a lexicographic partial order on the ordered bases as follows. Given two ordered bases $\mathbf{B}' : b'_1, \ldots, b'_n$ and $\mathbf{B}'' : b''_1, \ldots, b''_n$ with non-decreasing norms, we say $\mathbf{B}' < \mathbf{B}''$ if there exists an index i such that $||b'_j|| = ||b''_j||$ for all $j < i$ and $||b'_i|| < ||b''_i||$. Observe that in each iteration of the algorithm the basis strictly reduces with respect to this partial ordering. Since this ordering is bounded below, the algorithm must terminate.
Above algorithm establishes that cascaded minimal basis exists for every lattice. Set $\{e_1, \ldots, e_n\}$ is a cascading minimal basis of $\mathbb{Z}^n$. We will now show that this is the only such basis in $\mathbb{Z}^n$. Let $\{b_1, \ldots, b_n\}$ be a CMB of $\mathbb{Z}^n$. Since the shortest vector in this lattice is a unit vector, b_1 must be a unit vector. Without loss of generality assume that $b_1 = e_1$. Since each b_j is irreducible by e_1 for any $j > 1$, $\mathcal{L}(b_2, \ldots, b_n)$ must be $\mathbb{Z}^{n-1}$, spanned by $\{e_2, \ldots, e_n\}$. By the definition $b_2, \ldots, b_n$ is itself a CMB, therefore by induction $b_i = e_i$ for all i.

Lemma 11. *The unique cascaded minimal basis of $\mathbb{Z}^n$ is $\{e_1, \ldots, e_n\}$.*

Following is the main result of this section.

Theorem 5. *Let $\mathbf{B} = \{b_1, \ldots, b_n\}$ be an AMDV basis of a lattice $\mathcal{L}$ in $\mathbb{R}^n$ and let $\{d_1, \ldots, d_n\}$ be its dual. Also given that the angle between b_i and d_i is less than or equal to 60-degrees for all i. For any subset $\mathbf{B}' \subseteq \mathbf{B}$ and $v \in \mathcal{L}(\mathbf{B}')$, there exists $b \in \mathbf{B}'$ such that $||b|| \leq ||v||$.*

The proof is in the Appendix.

Corollary 7. *Let $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$ be an AMDV basis of a lattice $\mathcal{L}$ and let $\mathbf{D} = \{d_1, d_2, \ldots, d_n\}$ be its dual basis. If for each i, the angle between b_i and d_i is at most 60-degrees, then $\mathbf{B}$ is a cascaded minimal basis.*

Proof. Suppose $||b_1|| \leq ||b_2|| \leq ||b_3|| \leq \ldots$. Due to MDV property no b_i can reduce any b_j. Now consider the sublattice $\mathcal{L}_i$ spanned by $\{b_i, b_{i+1}, b_{i+2}, \ldots, b_n\}$. Let $v \in \mathcal{L}_i$. So there exist α_j such that $v = \sum_{j=i}^{n} \alpha_j . b_j$. Let j_0 be the smallest index such that $\alpha_{j_0} \neq 0$. From the previous theorem $||b_{j_0}|| \leq ||v||$. Hence $||b_i|| \leq ||v||$. Thus b_i is a shortest vector in the sublattice $\mathcal{L}_i$. This proves that $\mathbf{B}$ is a cascaded minimal basis.

Corollary 8. *Let $\mathcal{L}$ denote $\mathbb{Z}^n$ or any of its isomorphic lattice. Let $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$ be an AMDV basis of $\mathcal{L}$ and $\mathbf{D} = \{d_1, d_2, \ldots, d_n\}$ be its dual basis. If the angle between b_i and d_i is no more than 60-degrees for each i, then $\mathbf{B} = \{e_1, e_2, \ldots, e_n\}$.*

7 Short Vectors that are Voronoi Relevant

Definition 12 (Voronoi Cell). *Let $\mathcal{L}$ be a lattice. The Voronoi cell of the lattice is*

$$\mathcal{C}(\mathcal{L}) = \{x \in \mathbb{R}^n \mid \forall v \in \mathcal{L}, ||x|| \leq ||x - v||\}$$

The half space for a lattice vector v is defined as

$$H(v) = \{x \in \mathbb{R}^n \mid ||x|| \leq ||x - v||\}$$

Observe that $\mathcal{C}(\mathcal{L}) = \bigcap_{v \in \mathcal{L} \setminus \{\vec{0}\}} H(v)$. The minimal set of lattice vectors $V(\mathcal{L})$, such that $\mathcal{C}(\mathcal{L}) = \bigcap_{v \in V(\mathcal{L})} H(v)$, is called the set of Voronoi relevant vectors.

Theorem 6 (Voronoi, [11]). *Let $\mathcal{L}$ be a lattice and $v \in \mathcal{L}$ be any lattice vector. Then v is a Voronoi relevant vector if and only if $\pm v$ are the only shortest vectors in the coset $2\mathcal{L} + v$.*

We first prove the following claim that will be used later in the proof of the main result.

Claim. Let $\mathbf{S} = \{\vec{s}_1, \ldots, \vec{s}_n\}$ be a solution to SMP of a lattice $\mathcal{L}$, i.e. it is a set of n linearly independent lattice vectors such that $||\vec{s}_i|| = \lambda_i(\mathcal{L})$. If $\vec{w} \in \mathcal{L}$ and $||\vec{w}|| < \lambda_j$, then $\vec{w} \in span(\vec{s}_1, \ldots, \vec{s}_{j-1})$.

Proof. We are given that $||w|| < \lambda_j$ so $w \in \mathcal{B}(0, \lambda_j - \epsilon)$ where $\epsilon = (\lambda_j - ||w||)/2 > 0$. Since $\mathcal{B}(0, \lambda_j - \epsilon)$ has at most $j-1$ linearly independent vectors and $s_1, \ldots, s_{j-1}$ is one such set, $w \in span(s_1, \ldots, s_{j-1})$.

An obvious corollary of Claim 7 is as follows.

Corollary 9. *Let $\mathbf{S} = \{\vec{s}_1, \ldots, \vec{s}_n\}$ and $\mathbf{S}' = \{\vec{s}'_1, \ldots, \vec{s}'_n\}$ be any two solutions of SMP. If $\lambda_i < \lambda_{i+1}$, then $span(\vec{s}_1, \ldots, \vec{s}_i) = span(\vec{s'}_1, \ldots, \vec{s'}_i)$.*

In [12], it is proved that for any $\vec{s} \in \mathcal{L}$ and $||\vec{s}|| = \lambda_1$, $\vec{s}$ belongs to the set of Voronoi relevant vectors. We will show in the main result of this section that if $\vec{s} \in \mathcal{L}$ and $||\vec{s}|| \leq \lambda_n$, then $\vec{s}$ is a Voronoi relevant vector.

Theorem 7. *If $S = \{\vec{s}_i, \ldots, \vec{s}_n\}$ is a solution to SMP for a lattice $\mathcal{L}$, then $S \subseteq V(\mathcal{L})$.*

The proof is in the Appendix.

Corollary 10. *For any lattice $\mathcal{L}$, $\lambda_n(\mathcal{L}) \leq ||V(\mathcal{L})||$.*

The algorithm given by Micciancio et al. [13] computes all the Voronoi relevant vectors, then Algorithm 2, given in the appendix, computes a solution of SMP.
In [14], the authors defined a new concept of *c-compact basis* as follows. For any $c > 0$, a basis $\mathbf{B}$ of a lattice $\mathcal{L}$ is c-compact if

$$V(\mathcal{L}) \subseteq \{\mathbf{B}z : z \in \mathbb{Z}^n \text{ and } ||z||_\infty \leq c\}$$

A 1-compact basis is simply called a *compact basis*.
Since, a compact basis $\mathbf{B}$ generates $V(\mathcal{L})$ with coefficients from $\{-1, 0, 1\}$, one would expect $\mathbf{B}$ to consist of short vectors. But, consider the lattice $\mathbb{Z}^n$ with the following basis

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 2^1 & \dots & 2^{n-3} & 2^{n-2} \\ 0 & 1 & 1 & \dots & 2^{n-4} & 2^{n-3} \\ 0 & 0 & 1 & \dots & 2^{n-5} & 2^{n-4} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}$$

This basis is compact whereas $\mathbf{B} \subset \left(2^{n-1}\mathcal{C}(\mathbb{Z}^n)\right) \cap \mathbb{Z}^n$ which contains vectors with exponentially large norms.

Claim. For any compact basis $\mathbf{B}$ of $\mathcal{L}$, $\mathbf{B} \subseteq \left(n.n! \times 2\mathcal{C}(\mathcal{L})\right) \cap \mathcal{L}$. Also, $||\mathbf{B}|| \leq n.n!\lambda_n$.

Proof. Since $\mathbf{B}$ is a compact basis and using theorem 6, we have $\mathbf{S} = \mathbf{B}Y$ where $\mathbf{S}$ is any solution to SMP and $\mathbf{Y} \in \{0, \pm 1\}^{n \times n}$. This implies that $\mathbf{B} = \mathbf{S}\mathbf{Y}^{-1}$. The entries of $\mathbf{Y}^{-1}$ are bounded by $n!$, therefore each b_i is sum of vectors in $n! \times 2\mathcal{C}(\mathcal{L})$. Therefore, $||\mathbf{B}|| \leq n.n!.\lambda_n$.

8 Conclusion

We have presented several results related to the bases of $\mathbb{Z}^n$ such as extending a primitive vector v to a unimodular matrix by ensuring that v remains the longest. We give a reduction from SVP in $\mathbb{Z}^n$ to SVP and CVP in $n-1$ dimensional sublattice of $\mathbb{Z}^n$. We also describes some good bases of $\mathbb{Z}^n$ and gave results related to those. Finally, we showed that the solution to SMP is a subset of the set of Voronoi relavant vector.
In future works, we would like to see whether the extension lemma can be generalised where more than one vector is given and one of these vectors remains the largest in the computed basis.If it holds than we can deduce that $\mathbb{Z}^n$ has a unique AMDV basis, namely, $\{e_1, \dots, e_n\}$.
It would be interesting to know if the angle condition from Theorem 5 can be dropped. This would give an alternative proof of uniqueness of AMDV basis in $\mathbb{Z}^n$. Finally, it is still an open question whether in the lattices having compact bases, SMP solution forms a basis.

References

1. Jeffrey C Lagarias, Hendrik W Lenstra, and Claus-Peter Schnorr. Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.
2. Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of operations research*, 12(3):415–440, 1987.

3. Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261(ARTICLE):515–534, 1982.
4. Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical computer science*, 53(2-3):201–224, 1987.
5. Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, pages 391–404. SIAM, 2014.
6. Christoph Hunkenschröder. Deciding whether a lattice has an orthonormal basis is in co-np. *arXiv preprint arXiv:1910.03838*, 2019.
7. Hendrik W Lenstra and Alice Silverberg. Lattices with symmetry. *Journal of Cryptology*, 30(3):760–804, 2017.
8. Daniele Micciancio. Efficient reductions among lattice problems. In *Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms*, pages 84–93. Society for Industrial and Applied Mathematics, 2008.
9. David Ford and George Havas. A new algorithm and refined bounds for extended gcd computation. In *International Algorithmic Number Theory Symposium*, pages 145–150. Springer, 1996.
10. Peter van Emde Boas. Another np-complete problem and the complexity of computing short vectors in a lattice. *Tecnical Report, Department of Mathmatics, University of Amsterdam*, 1981.
11. John Horton Conway and Neil James Alexander Sloane. *Sphere packings, lattices and groups*, volume 290. Springer Science & Business Media, 2013.
12. Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Algorithms for the shortest and closest lattice vector problems. In *International Conference on Coding and Cryptology*, pages 159–190. Springer, 2011.
13. Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations. *SIAM Journal on Computing*, 42(3):1364–1391, 2013.
14. Christoph Hunkenschröder, Gina Reuland, and Matthias Schymura. On compact representations of voronoi cells of lattices. *Mathematical Programming*, pages 1–22, 2020.

Appendix

8.1 Proofs of Main Theorems

Theorem 2. Let $v \in \mathbb{Z}^n$ be primitive vector such that $||v||^2 > 1$. Then, there exists a $\mathbb{Z}^n$-basis $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$ such that $b_n = v$ and $||b_n||^2 > ||b_i||^2, \forall i \in [n-1]$.

Proof. We will construct an $n \times n$ integer matrix $\mathbf{B}$ with determinant 1 which contains v as a column and the norm of all other columns being less than $||v||$. We prove this theorem using induction on the dimension n.

(1) Base case is $n = 2$. Let $b_2 = (a, b)$. So there exists c, d such that $c.a + d.b = 1$ where $|c| < |b|$ and $|d| < |a|$. Let $b_1 = (-d, c)$. Then $\mathbf{B} = \{b_2, b_1\}$ spans $\mathbb{Z}^2$ because the determinant of $\mathbf{B}$ is $a.c + b.d = 1$. Further $||b_2||^2 = a^2 + b^2 > d^2 + c^2 = ||b_1||^2$. Hence the claim holds for this case.
Next steps will address the cases with $n > 3$.
(2) Let $v = (v_1, \ldots, v_n)^T$. First consider the case where at least one component of v is zero. Without loss of generality assume that $v_n = 0$. We will reduce the problem to $n - 1$ dimensional case. Let $b'_n = (v_1, \ldots, v_{n-1})$. From induction hypothesis we have a basis $\mathbf{B}' = [b'_2, \ldots, b'_n]$ which spans $\mathbb{Z}^{n-1}$ and $||b'_i|| < ||b'_n||$ for all $2 \leq i \leq n-1$. Define the basis matrix $\mathbf{B}$ for $\mathbb{Z}^n$ as follows. Here $\vec{0}$ denotes an $(n-1)$-dimensional zero vector.

$$\mathbf{B} = \begin{bmatrix} \vec{0} & \mathbf{B}' \\ 1 & \vec{0}^T \end{bmatrix}$$

Observe that the rightmost column is v.
(3) Next we consider the case when at least one component of v is 1. Case in which one component is -1 can be handled similarly. Without loss of generality assume that $v_n = 1$. Since $v_n = 1$, we have a trivial solution $\mathbf{B} = [e_1, e_2, \ldots, e_{n-1}, v]$.
Observe that $Det(\mathbf{B})$ and all columns, other than v are unit vector.
(4) Finally we consider the case where $v_i \notin [-1, 0, 1], \forall i$. For convenience we will denote v by $(v_n, v_{n-1}, \ldots, v_1)^T$. Define $d_1 = v_1$ and for all $i > 1$, we define $d_i = GCD(v_1, \ldots, v_i)$ and $r_i, s_i \in \mathbb{Z}$ such that $r_i v_i + s_i d_{i-1} = d_i$. Observe that $d_n = 1$. Define matrix $\mathbf{T}_i$ for $i > 1$ as follows. The inverse is also given below.

$$\mathbf{T}_i = \begin{bmatrix} 1\,0\ldots & 0 & 0 & 0\,0\ldots \\ 0\,1\ldots & 0 & 0 & 0\,0\ldots \\ \vdots & & & \\ 0\,0\ldots & r_i & s_i & 0\,0\ldots \\ 0\,0\ldots & -d_{i-1}/d_i & v_i/d_i & 0\,0\ldots \\ 0\,0\ldots & 0 & 0 & 1\,0\ldots \\ \vdots & & & \end{bmatrix}, \mathbf{T}_i^{-1} = \begin{bmatrix} 1\,0\ldots & 0 & 0 & \ldots \\ 0\,1\ldots & 0 & 0 & \ldots \\ \vdots & & & \\ 0\,0\ldots & v_i/d_i & -s_i & \ldots \\ 0\,0\ldots & d_{i-1}/d_i & r_i & \ldots \\ \vdots & & & \end{bmatrix}$$

where $(i-1)$-st column is $(0, \ldots, 0, r_i, -d_i/d_{i-1}, 0, \ldots, 0)^T$ in which r_i is the $(i-1)$-st entry and the i-th column is $(0, \ldots, 0, s_i, v_i/d_{i-1}, 0, \ldots, 0)^T$ in which v_i/d_i is the i-th entry. The determinant of $\mathbf{T}_i$ is $(r_i.v_i + s_i.d_{i-1})/d_i = 1$. Define $\mathbf{B} = \mathbf{T}_n^{-1}\mathbf{T}_{n-1}^{-1}\ldots\mathbf{T}_2^{-1}$ which is a unimodular matrix. Our next objective is to show that the first column of $\mathbf{B}$ is v. To do this we determine the structure of $\mathbf{B}$. To begin with the product of the rightmost two matrices is

$$\mathbf{T}_3^{-1}.\mathbf{T}_2^{-1} = \begin{bmatrix} v_n & -s_n & 0 & \ldots \\ v_{n-1} & v_{n-1}r_n/d_{n-1} & -s_{n-1} & \ldots \\ d_{n-2} & d_{n-2}r_n/d_{n-1} & r_{n-1} & \ldots \\ \vdots & & & \end{bmatrix}$$

and the product of $\mathbf{T}_4^{-1}$ with the above matrix is

$$\mathbf{T}_4^{-1}\mathbf{T}_3^{-1}\mathbf{T}_2^{-1} = \begin{bmatrix} v_n & -s_n & 0 & 0 & \dots \\ v_{n-1} & v_{n-1}r_n/d_{n-1} & -s_{n-1} & 0 & \dots \\ v_{n-2} & v_{n-2}r_n/d_{n-1} & v_{n-2}r_{n-1}/d_{n-2} & -s_{n-2} & \dots \\ d_{n-3} & d_{n-3}r_n/d_{n-1} & d_{n-3}r_{n-1}/d_{n-2} & r_{n-2} & \dots \\ \vdots & & & & \end{bmatrix}$$

So, finally we will get

$$\mathbf{B} = \begin{bmatrix} v_n & -s_n & 0 & 0 & \dots & 0 & 0 \\ v_{n-1} & v_{n-1}r_n/d_{n-1} & -s_{n-1} & 0 & \dots & 0 & 0 \\ v_{n-2} & v_{n-2}r_n/d_{n-1} & v_{n-2}r_{n-1}/d_{n-2} & -s_{n-2} & \dots & 0 & 0 \\ v_{n-3} & v_{n-3}r_n/d_{n-1} & v_{n-3}r_{n-1}/d_{n-2} & v_{n-3}r_{n-1}/d_{n-3} & \dots & 0 & 0 \\ \vdots & & & & & & \\ v_2 & v_2r_n/d_{n-1} & v_2r_{n-1}/d_{n-2} & v_2r_{n-1}/d_{n-3} & \dots & v_2r_3/d_2 & -s_2 \\ v_1 & v_1r_n/d_{n-1} & v_1r_{n-1}/d_{n-2} & v_1r_{n-1}/d_{n-3} & \dots & v_1r_3/d_2 & r_2 \end{bmatrix}$$

Since $Det(\mathbf{T}_i^{-1}) = 1$, $Det(\mathbf{B}) = 1$. Observe that the first column of $\mathbf{B}$ is v, as expected. In the last step we will show that the norm of all columns other than v is strictly less than $||v||$. Label the columns of $\mathbf{B}$, from left to right, by $b_n, b_{n-1}, \dots, b_1$ respectively.
Square of the norm of vector b_k is $b_k^2 = s_{k+1}^2 + (r_{k+1}^2/d_k^2)[v_k^2 + v_{k-1}^2 + \cdots + v_1^2]$. Since $r_i.v_i + s_i.d_{i-1} = d_i$, from Corollary 1, $|r_i| \leq |d_{i-1}|/(2.|d_i|)$ because $|v_i| > 1$. Also, $|s_i| = 1$ if $|d_{i-1}| = 1$. Otherwise $|s_i| \leq |v_i|/(2.|d_i|)$. We will plug these values into the expression for b_k.
First, the case of $|d_k| = 1$. In this case $b_k^2 \leq 1 + (1/(4d_{k+1}^2)).(v_k^2 + v_{k-1}^2 + \cdots + v_1^2) \leq 1 + (v_k^2 + v_{k-1}^2 + \cdots + v_1^2)/4 \leq v_{k+1}^2/4 + (v_k^2 + v_{k-1}^2 + \cdots + v_1^2)/4 < b_n^2 = v^2$.
In case $|d_k| > 1$, $b_k^2 \leq v_{k+1}^2/(4.d_{k+1}^2) + 1/(4.d_{k+1}^2).(v_k^2 + v_{k-1}^2 + \cdots + v_1^2) \leq (1/4)(v_{k+1}^2 + v_k^2 + \cdots + v_1^2) < b_n^2 = v^2$. □

Theorem 5 Let $\mathbf{B} = \{b_1, \dots, b_n\}$ be an AMDV basis of a lattice $\mathcal{L}$ in $\mathbb{R}^n$ and let $\{d_1, \dots, d_n\}$ be its dual. Also given that the angle between b_i and d_i is less than or equal to 60-degrees for all i. For any subset $\mathbf{B'} \subseteq \mathbf{B}$, if $v \in \mathcal{L}(\mathbf{B'})$, then there exists a $b \in \mathbf{B'}$ such that $||b|| \leq ||v||$.

Proof. To avoid notational complexity suppose $v = \alpha_1.b_1 + \alpha_2.b_2 + \cdots + \alpha_k.b_k$ where each α_i is non-zero. Also assume that $\alpha_1 \geq 0$. If not, then replace v by $-v$. This does not affect the argument since $||v|| = ||-v||$.
First consider the case of $\alpha_1 = 1$. In this case $v = b_1 + \alpha_2.b_2 + \cdots + \alpha_k.b_k$. Since b_1 is MDV, $||v|| \geq ||b_1||$.
Now consider the remaining case, i.e., $\alpha_1 \geq 2$. Let $v_1 = \alpha_2.b_2 + \cdots + \alpha_k.b_k$. Let P denote the 2-D plane spanned by v_1 and b_1. Observe that vectors $v_2 = b_1 + v_1$ and $v = \alpha_1.b_1 + v_1$ belong to P. In this 2-Dim space let $b_1 = (b, 0)$ and $v_1 = (p, q)$. So $v = (\alpha_1.b + p, q)$. Let θ be the angle between b_1 and v_1. So $\tan\theta = q/p$.
The condition $v^2 \geq b_1^2$ can be written as $(q/p)^2 \geq -1 - 2\alpha_1.(b/p) - (\alpha_1^2 - 1)(b/p)^2$. Let x denote b/p. We need to find the maximum value

of $\phi = -1 - 2\alpha_1.x - (\alpha_1^2 - 1)x^2$. We have $d\phi/dx = -2(\alpha_1^2 - 1)x - 2\alpha_1$ and $d^2\phi/dx^2 = -2(\alpha_1^2 - 1)$. Since $\alpha_1 \geq 2$, the maximum of ϕ will occur at $d\phi/dx = -2(\alpha_1^2 - 1)x - 2\alpha_1 = 0$ or $x = -\alpha_1/(\alpha_1^2 - 1)$. Plugging this value in ϕ gives maximum value of ϕ to be $-1 - (\alpha_1^2 - 1).\alpha_1^2/(\alpha_1^2 - 1)^2 + 2\alpha_1^2/(\alpha_1^2 - 1) = \alpha_1^2/(\alpha_1^2 - 1) - 1 = 1/(\alpha_1^2 - 1)$. So ϕ is maximum at $\alpha_1 = 2$ and it is equal to $1/3$.
We have shown that a sufficient condition for $||v|| \geq ||b_1||$ is that $\tan^2\theta \geq 1/3$ or $\theta \geq 30$. This condition is satisfied when the angle between b_1 and the subspace, spanned by $\mathbf{B} \setminus \{b_1\}$, is at least 30-degrees because v_1 belongs to this subspace. This condition is the same as the condition that the angle between b_1 and d_1 (the normal to the subspace) is at most 60-degrees. □

Theorem 6 If $\mathbf{S} = \{\vec{s}_i, \ldots, \vec{s}_n\}$ is a solution to SMP for a lattice $\mathcal{L}$, then $\mathbf{S} \subseteq V(\mathcal{L})$.

Proof. From theorem 6, if $v \in \mathcal{L}$ is not a Voronoi relevant vector, then there exist $\vec{w} \in \mathcal{L} \setminus \{0, v\}$ such that $||\frac{v}{2} - \vec{w}|| \leq ||\frac{v}{2}||$. We will use this criterion to prove the claim.
We first show that $\vec{s}_1$ is Voronoi relevant. If $\vec{s}_1$ is not Voronoi relevant, then from the above criterion we consider two cases.

$||\frac{\vec{s}_1}{2} - \vec{w}|| < ||\frac{\vec{s}_1}{2}||$ **:** In this case $||\vec{s}_1 - 2\vec{w}|| < ||\vec{s}_1||$ which is a contradiction because $\vec{s}_1$ is the shortest vector in $\mathcal{L}$.

$||\frac{\vec{s}_1}{2} - \vec{w}|| = ||\frac{\vec{s}_1}{2}||$ **:** It implies that $cos\theta = \frac{||\vec{w}||}{||\vec{s}_1||}$ where θ is the angle between $\vec{s}_1$ and $\vec{w}$. Since $||\vec{w}|| \geq ||\vec{s}_1||$, we have $cos(\theta) \geq 1$. Therefore $\theta = 0$ and $\vec{w} = \vec{s}_1$, which is absurd.

This implies that $\vec{s}_1 \in V(\mathcal{L})$. Now to argue using induction assume that $\vec{s}_1, \ldots, \vec{s}_{i-1}$ belong to $V(\mathcal{L})$ and $\vec{s}_i \notin V(\mathcal{L})$, for some i. Again we consider two cases based on the criterion.

$||\vec{s}_i - 2\vec{w}|| < ||\vec{s}_i||$ **:** From the Claim 7, $\vec{s}_i - 2\vec{w}$ belongs to $X = span(\vec{s}_1, \ldots, \vec{s}_{i-1})$. Due to triangular inequality, we have $||\vec{w}|| = ||\vec{w} - \vec{s}_i/2 + \vec{s}_i/2|| < ||\vec{s}_i||$. So $\vec{w} \in X$. Combining with the fact that $\vec{s}_i - 2\vec{w} \in X$, we get that $\vec{s}_i$ also belongs to X. But that is impossible because $\vec{s}_i$ is linearly independent from $\vec{s}_1, \ldots, \vec{s}_{i-1}$.

$||\vec{s}_i - 2\vec{w}|| = ||\vec{s}_i||$ **:** This implies that $||\vec{w}||^2 = \vec{s}_i.\vec{w} \implies cos(\theta) = \frac{||\vec{w}||}{||\vec{s}_i||}$. If $\theta = 0$, then $\vec{w} = \vec{s}_i$ which contradicts the choice of $\vec{w}$. So, we consider the case when $||\vec{s}_i|| > ||\vec{w}||$. In this case $\vec{w} \in X = span(\vec{s}_1, \ldots, \vec{s}_{i-1})$. We get an inequality as follows.

$$\begin{aligned} ||\vec{s}_i - \vec{w}||^2 &= ||\vec{s}_i||^2 + ||\vec{w}||^2 - 2\vec{s}_i.\vec{w} \\ &= ||\vec{s}_i||^2 + ||\vec{w}||^2 - 2||\vec{w}||^2 \\ &= ||\vec{s}_i||^2 - ||\vec{w}||^2 \\ &< ||\vec{s}_i||^2 \end{aligned}$$

This implies that $\vec{s}_i - \vec{w}$ also belongs to X. Thus we deduce that $\vec{s}_i$ must also belong to X, which is absurd because $\vec{s}_i$ is linearly independent from $\vec{s}_1, \ldots, \vec{s}_{i-1}$.

□

8.2 Counterexamples

The following basis of $\mathbb{Z}^n$ has the property that for all $i \neq j$, b_i is irreducible with respect to b_j but it is not AMDV.

$$\mathbf{B}_1 = \begin{bmatrix} 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & -1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

The following basis of $\mathbb{Z}^n$ has the property that it is $+1, 0, -1$ matrix but its dual does not contain any entry with value $+1$ or -1.

$$\mathbf{B}_2 = \begin{bmatrix} -1 & 0 & -1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0 \\ -1 & -1 & 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & -1 & 0 & -1 & 0 & 0 \\ 1 & 0 & -1 & -1 & 1 & 1 & 0 & 1 \\ -1 & 1 & -1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 & -1 & -1 \end{bmatrix}, \mathbf{B}_2^{-T} = \begin{bmatrix} -6 & -5 & -6 & -2 & -7 & 3 & -2 & 2 \\ -14 & -11 & -13 & -5 & -17 & 7 & -5 & 6 \\ 8 & 6 & 7 & 3 & 9 & -4 & 3 & -3 \\ 13 & 10 & 12 & 5 & 16 & -7 & 4 & -5 \\ -5 & -4 & -5 & -2 & -6 & 2 & -2 & 2 \\ 16 & 12 & 14 & 6 & 19 & -8 & 5 & -6 \\ 8 & 7 & 8 & 3 & 10 & -4 & 3 & -3 \\ 10 & 8 & 9 & 4 & 12 & -5 & 3 & -4 \end{bmatrix}$$

8.3 Algorithms

Algorithm 1 finds a solution to SMP from the set of all Voronoi relevant vectors.

Input: A basis $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$ of a lattice $\mathcal{L}$ with $||b_i|| \leq ||b_{i+1}|| \forall i$.
Output: A cascaded minimal basis of $\mathcal{L}$.
while $\exists b_i$ *that does not satisfy* P_1 *or* P_2 **do**
  Select the minimum index i such that b_i does not satisfy P_1 or P_2;
  if b_i *does not satisfy* P_1 **then**
    Compute a basis $c_i, \ldots, c_n$ for $\mathcal{L}(b_i, \ldots, b_n)$ where c_i is a shortest vector in $\mathcal{L}(b_i, \ldots, b_n)$ and $||c_j|| \leq ||c_{j+1}|| \forall j$;
    for $j := i$ *to* n **do**
      $b_j := c_j$;
    end
  else
    $b_i := Red(b_i, \{b_1, \ldots, b_{i-1}\})$;
  end
end
return $\{b_1, \ldots, b_n\}$

Algorithm 1: Every lattice has at least one Cascading Minimal Basis

Input: A basis $\mathbf{B} = [b_1, \ldots, b_n]$ for $\mathcal{L}$.
Run the algorithm given by Micciancio et al. to compute the set of all Voronoi relevant vector V;
Sort V in the order of non-decreasing norm;
$\mathbf{S} := \{\}$;
$i = 1$;
while $|\mathbf{S}| < n$ **do**
  if $V[i] \notin Span(\mathbf{S})$ **then**
    $\mathbf{S} = \mathbf{S} \cup \{V[i]\}$;
  end
end
Return $\mathbf{S}$.

Algorithm 2: Algorithm for solving SMP