EasyChair Preprint

№ 8862

On the Bases of Z^n Lattice

Shashank Mehta and Mahesh Rajasree

September 22, 2022

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

Shashank K Mehta
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
Kanpur, India
skmehta@cse.iitk.ac.in

Mahesh Sreekumar Rajasree
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
Kanpur, India
mahesr@cse.iitk.ac.in

***Abstract*—The $\mathbb{Z}^n$ lattice is the lattice generated by the set of all orthogonal unit integer vectors. Since it has an orthonormal basis, the shortest vector problem and the closest vector problem are easy to solve in this particular lattice. But, these problems are hard to solve when we consider a rotation of $\mathbb{Z}^n$ lattice. In-fact, even though it is known that the $\mathbb{Z}^n$-isomorphism problem is in NP $\cap$ Co-NP, we still don't have an efficient algorithm to solve it. Motivated by the above, in this paper we investigate the properties of the bases of $\mathbb{Z}^n$ lattice which are the sets of column/row vectors of unimodular matrices. We show that an integer primitive vector of norm strictly greater than 1 can be extended to a unimodular matrix U such that the remaining vectors have norm strictly smaller than the initial primitive vector. We also show a reduction from SVP in any lattice isomorphic to $\mathbb{Z}^n$ to SVP in $n-1$ dimensional sublattice of $\mathbb{Z}^n$. We define two new classes of lattice bases and show certain results related to $\mathbb{Z}^n$ bases. Finally, we study the relation between any solution to Successive Minima Problem and the set of Voronoi relevant vectors and present some bounds related to the compact bases of $\mathbb{Z}^n$.**

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

I. 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 $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_m\}$, i.e., $\mathcal{L}(\mathbf{B}) = \{\sum_i \alpha_i \vec{b}_i \mid \forall(\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}^m\}$. Set $\mathbf{B}$ is called a basis of this lattice. The lattice $\mathbb{Z}^n$ is $\mathcal{L}(\{\vec{e}_1, \ldots, \vec{e}_n\})$, where $\vec{e}_i$'s are orthogonal unit integer 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 (SVP) 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 $\mathbb{Z}^n$. In other words, does there exist an orthonormal transformation which will transform the vectors of the given lattice 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 $\mathbb{Z}^n$.

Mahesh Sreekumar Rajasree acknowledges the support of Prime Minister's Research Fellowship and Center for Cyber Security and Cyber Defense of Critical Infrastructures (C3i).

Prior works

There have been numerous works on the study of bases for general lattices. The Korkin-Zolotarev bases have 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.

A basis $\mathbf{B}$ generates $\mathbb{Z}^n$ if and only if it is the set of column (equivalently, row) vectors of a unimodular matrix. So $\mathbb{Z}^n$ isomorphism problem is closely related to the study of unimodular matrices. 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 [4] gave an exponential time algorithm to solve this problem. Hunkenschroder [5] shows that $\mathbb{Z}^n$ isomorhpism is in NP $\cap$ Co-NP. Lenstra and Silverberg [6] showed that when the lattice is given with enough symmetry, they can construct a deterministic polynomial-time algorithm to solve $\mathbb{Z}^n$ isomorphism. Very recently, Bennett et al. [7] showed that finding the shortest vector in a lattice isomorphic to $\mathbb{Z}^n$ is strictly easier than SVP in general lattices. They also constructed a simple public key encryption scheme that is secure if finding a shortest vector in a lattice, isomorphic to $\mathbb{Z}^n$, is hard.

In [8], the author showed that a partially filled $n \times n$ integer matrix with n entries such that these n entries do not form a row or column, can be completed into a unimodular matrix. This was further improved in [9] where a partially filled $n \times n$ matrix having $2n-3$ entries, such that no n entries form a column or row, can be completed to form a unimodular matrix. In [10], the authors showed that given a set of linearly independent primitive vectors $\vec{a}_1, \ldots, \vec{a}_m \in \mathbb{Z}^n$ with $m < n-1$, the number of primitive vectors $\vec{b} \in \mathbb{Z}^n$ with $||\vec{b}|| \leq T$, such that $\vec{a}_1, \ldots, \vec{a}_m, \vec{b}$ is again linearly independent, is $\Theta(T^n)$ as $T \to \infty$. The bound reduces to $\Theta(T^{n-1})$ when $m = n-1$. The above bound is useful only for large T.

Our contributions

The following are the major results presented in this paper.

1) We show that a primitive vector can be extended to a unimodular matrix (in which the initial vector is a column)

such that each new column vector has strictly lesser ℓ_2-norm than the ℓ_2-norm of the initial primitive vector. Here $||\vec{v}||$ denotes ℓ_2-norm of $\vec{v}$. We give a constructive proof hence it can be turned into an algorithm.

Theorem 1. *Let $\vec{v} \in \mathbb{Z}^n$ be a primitive vector such that $||\vec{v}||^2 > 1$. Then, there exists a $\mathbb{Z}^n$-basis $\mathbf{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ such that $\vec{b}_n = \vec{v}$ and $||\vec{b}_n||^2 > ||\vec{b}_i||^2, \forall i \in [n-1]$.*

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 $\{\vec{e}_1, \ldots, \vec{e}_n\}$.
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 $\mathbb{Z}^n$.

II. Preliminaries and Notations

In this paper $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{Q}$ will denote the sets of integers, reals and rationals respectively. Vectors will be denoted in small case with with arrow as in $\vec{v}$ whereas matrices and basis sets will be denoted in capital letters. Let $\mathbf{B} = \{\vec{b_1}, \ldots, \vec{b_k}\}$ 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 $\vec{v} = (v_1, \ldots, v_n)$ is the normal Euclidean norm, i.e, $||\vec{v}|| = \sqrt{\sum_i v_i^2}$. The norm of $\mathbf{B}$ is defined as $||\mathbf{B}|| = \max_i ||\vec{b}_i||$. For any two sets of vectors U and V, the notation $U + V$ denotes the set $\{\vec{u} + \vec{v} \mid \vec{u} \in U, \vec{v} \in V\}$

Definition 2 (Lattice)**.** *Given a set of linearly independent vectors $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_m\}$ 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., $\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^m \alpha_i \cdot \vec{b}_i \mid \forall \alpha_i \in \mathbb{Z}\}$. By $\mathbf{B}$ we also denote a matrix in which $\vec{b}_i$ are column vectors. In the matrix notation for $\mathbf{B}$ $\mathcal{L}(\mathbf{B}) = \{\mathbf{B} \cdot \vec{z} \mid \forall \vec{z} \in \mathbb{Z}^n\}$. $\mathbf{B}$ 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 $\vec{v}$ in a lattice is called *primitive* if $(1/k) \cdot \vec{v}$ 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 $\vec{u}, \vec{v}_1, \ldots, \vec{v}_k$ be vectors in $\mathbb{R}^n$. If the norm of $\vec{u}' = \vec{u} + \sum_{i=1}^k \alpha_i . \vec{v}_i$ is less than $||\vec{u}||$, where $\alpha_i \in \mathbb{Z}$, then $\vec{u}'$ is called a *reduction* of $\vec{u}$ by $\{\vec{v}_1, \ldots, \vec{v}_k\}$. Vector $\vec{u}$ is said to be irreducible by a set of vectors $\mathbf{V}$ if the vectors in $\mathbf{V}$ cannot reduce it.

Definition 3. *$Red(\vec{u}, \mathbf{V})$ denotes any vector $\vec{u}'$ which is a reduction of $\vec{u}$ by $\mathbf{V}$ and it is not further reducible by it. Observe that $Red(\vec{u}, \mathbf{V})$ is not unique.*

Following is a trivial result.

Lemma 4. *Let $\mathbf{B} = \{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ be a basis of $\mathcal{L}$ and $\vec{b}'_i = Red(\vec{b}_i, \mathbf{B} \setminus \{\vec{b}_i\})$. Then $\{\vec{b}_1, \ldots, \vec{b}_{i-1}, \vec{b}'_i, \vec{b}_{i+1}, \ldots, \vec{b}_n\}$ is also a basis of $\mathcal{L}$.*

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

Definition 5. *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. Observe that the lattice denoted by $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ which is $\{\sum_{i=1}^n 2z_i\vec{b}_i \mid \forall z_i \in \mathbb{Z}\}$ is a sublattice of $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. It is easy to verify that $B' = \{2\vec{b}_1, \ldots, 2\vec{b}_n\}$ is a basis of $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. Further, the shifted lattice $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n) + \vec{v}$ is a subset of $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ for any $\vec{v} \in \mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. For each $\vec{v} \in \mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$, $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n) + \vec{v}$ is called a coset of $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$. Each vector of $\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ belongs to either $2\mathcal{L}(\vec{b}_1, \ldots, \vec{b}_n)$ or to one of its cosets. Hence they partition the entire lattice.

Claim 6. *Let $n \times n$ matrix $\mathbf{B}$ be a basis matrix of a lattice. Then there are 2^n distinct cosets of $2\mathcal{L}(\mathbf{B})$, given by $2\mathcal{L}(\mathbf{B}) + \mathbf{B} \cdot \vec{z}$ for all $\vec{z} \in \{0,1\}^n$.*

A. Lattice Related Problems

We now define some interesting problems related to lattices.

Definition 7 (Shortest Vector Problem (SVP))**.** *Given a basis $\mathbf{B}$, find a shortest non-zero vector $\vec{v}$ in the lattice $\mathcal{L}(B)$, i.e., $||\vec{v}|| \leq ||\vec{u}||$ for all $\vec{u} \in \mathcal{L}(\mathbf{B}) \setminus \{\vec{0}\}$.*

Definition 8 (Closest Vector Problem (CVP))**.** *Given a basis $\mathbf{B}$ and a vector $\vec{t}$ in the ambient space, find the vector $\vec{v}$ in the lattice $\mathcal{L}(\mathbf{B})$ which is closest from $\vec{t}$, i.e., $||\vec{v} - \vec{t}|| \leq ||\vec{u} - \vec{t}||$ for all $\vec{u} \in \mathcal{L}(\mathbf{B})$.*

Definition 9 (Shortest Basis Problem (SBP))**.** *Given a basis of a lattice $\mathcal{L}$, find a basis $\mathbf{C}$ of $\mathcal{L}$ such that $||\mathbf{C}|| \leq ||\mathbf{D}||$ for all bases $\mathbf{D}$ of $\mathcal{L}$.*

Definition 10 (Successive Minima)**.** *The i^{th} successive minimum $\lambda_i(\mathcal{L})$ for a lattice $\mathcal{L}$ of rank n is the radius of the smallest sphere centered at the origin containing at least i independent lattice vectors.*

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

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

A direct consequence of this definition is as follows.

Lemma 11. *Let $S = \{\vec{v}_1, \ldots, \vec{v}_k\}$ be a linearly independent set of vectors of a $\mathcal{L}$. Then there exists a $\vec{v} \in S$ such that $||\vec{v}|| \geq \lambda_k$.*

A non-trivial relation between the norm of a shortest basis of a lattice and the λ_n of the lattice is given in Lemma 12.

Lemma 12 (Corollary 7.2, [11])**.** *For any lattice $\mathcal{L}$, there exists a basis $\mathbf{B}$ such that $||\mathbf{B}|| \leq \sqrt{n}\lambda_n/2$.*

Definition 13 (Successive Minima Problem (SMP))**.** *Given a basis $\mathbf{B}$ of a lattice, find linearly independent vectors $\vec{s}_1, \vec{s}_2, \ldots, \vec{s}_n$ such that $||\vec{s}_i|| = \lambda_i \ \forall i$.*

Definition 14 (Shortest Independent Vector Problem (SIVP))**.** *Given a basis $\mathbf{B}$ of a lattice, find n linearly independent vectors $\vec{s}_1, \ldots, \vec{s}_n$ such that $||\vec{s}_i|| \leq ||\vec{s}_{i+1}|| \ \forall i$ and $||\vec{s}_n|| = \lambda_n$.*

Observe that a solution to SMP is also a solution to SIVP.

Theorem 15 (Corollary 4, [12])**.** *There is a dimension and rank preserving reduction from SMP and SIVP to CVP. The reduction calls the CVP oracle $poly(n, b)$ times where b is the number of input bits.*

Many interesting lattice problems are reducible to 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, $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$ 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. Another desirable property is that for any lattice vector $\vec{v}$ its nearest neighbour lattice vectors are given by $\{\vec{v} + \mathbf{B} \cdot \vec{z} \mid \vec{z} \in \{-1, 0, 1\}^n\}$. 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.

Definition 16 (Voronoi Cell)**.** *Let $\mathcal{L}$ be a lattice. The Voronoi cell of the lattice is*

$$\mathcal{C}(\mathcal{L}) = \{\vec{x} \in \mathbb{R}^n \mid \forall \vec{v} \in \mathcal{L} \setminus \{\vec{0}\}, ||\vec{x}|| \leq ||\vec{x} - \vec{v}||\}$$

The half space for a lattice vector $\vec{v}$ is defined as

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

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

Theorem 17 (Voronoi, [13])**.** *Let $\mathcal{L}$ be a lattice and $\vec{v} \in \mathcal{L}$ be any lattice vector. Then $\vec{v}$ is a Voronoi relevant vector if and only if $\pm\vec{v}$ are the only shortest vectors in the coset $2\mathcal{L} + \vec{v}$.*

Corollary 18. *The number of Voronoi relevant vectors is upper bounded by $2(2^n - 1)$.*

Proof. According to Theorem 17, if coset has a unique (along with its negative) minimum vector, then that vector and its negative are Voronoi relevant vectors. Therefore the total number of Voronoi relevant vectors is bounded by the number of cosets of $2\mathcal{L}$, not including $2\mathcal{L}$ itself, because $\vec{0}$ is not a Voronoi relevant vector. So the number of Voronoi relevant vectors is at most $2(2^n - 1)$. See Claim 6. □

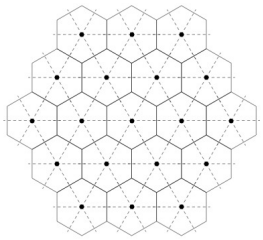

Fig. 1. Voronoi cells

B. Hyperplane Sublattice and Basis

We define a *rational subspace* as the $(n-1)$-dimensional subspace perpendicular to an integer vector in $\mathbb{R}^n$. An $(n-1)$-dimensional subspace S of $\mathbb{R}^n$ contains an $(n-1)$-dimensional sublattice of $\mathbb{Z}^n$ if and only if S 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 subspaces.

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 hyperplane 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 $\mathbf{B}_1 = \{\vec{b}_2, \ldots, \vec{b}_n\}$ is a basis of the hyperplane sublattice of S_0 and $\vec{b}_1 \in S_1 \cap \mathcal{L}$, then $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ is a basis of $\mathcal{L}$. Conversely if $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ is a basis of $\mathcal{L}$ and $\{\vec{b}_2, \ldots, \vec{b}_n\}$ spans S_0, then $\vec{b}_1$ belongs to the hyperplane S_1. Such pairs of $\vec{b}_1$ and S_0 will be called mutually *compatible*. Some times we may say $\vec{b}_1$ is compatible to $\{\vec{b}_2, \ldots, \vec{b}_n\}$ or the other way around, where the concerned pseudo-rational subspace is $span(\vec{b}_2, \ldots, \vec{b}_n)$ and the vectors, $\vec{b}_2, \ldots, \vec{b}_n$, 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 19. *Let S_0 be a pseudo rational subspace of a lattice with a sublattice basis $\mathbf{B}_1 = [\vec{b}_2, \vec{b}_3, \ldots, \vec{b}_n]$ and $\vec{b}_1$ be a lattice*

vector which are mutually compatible. Then (i) any compatible vector to S_0 is given by $\vec{b}_1 + \sum_{i=2}^{n} \alpha_i.\vec{b}_i$ for some integer coefficients α_i. (ii) Every pseudo-rational subspace compatible with $\vec{b}_1$ has a sublattice basis given by $[\vec{b}_2 - \alpha_2 \cdot \vec{b}_1, \vec{b}_3 - \alpha_3 \cdot \vec{b}_1, \ldots, \vec{b}_n - \alpha_n \cdot \vec{b}_1]$ where α_i are some integer coefficients.

Proof. (i) Suppose $\mathbf{B}' = [\vec{b'}_1, \vec{b}_2, \ldots, \vec{b}_n]$ is also a basis of the whole lattice, then $\vec{b'}_1$ must also belong to S_1, the next parallel hyperplane with lattice points. Then $\vec{b'}_1 = \vec{b}_1 + v$ where $v \in \mathcal{L}(\mathbf{B}_1)$. So $\vec{b'}_1 = \vec{b}_1 + \sum_{i=2}^{n} \alpha_i.\vec{b}_i$ for some $\alpha_i \in \mathbb{Z}$.

(ii) Let $[\vec{b}_2, \ldots, \vec{b}_n]$ be compatible with $\vec{b}_1$ so $\mathbf{B} = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n]$ is a lattice basis. Its dual is $\mathbf{D} = (\mathbf{B}^T)^{-1} = [\vec{d}_1, \vec{d}_2, \ldots, \vec{d}_n]$. So $\vec{d}_1$ is perpendicular to S_0 and $\vec{b}_1$ is perpendicular to the subspace of $[\vec{d}_2, \vec{d}_3, \ldots, \vec{d}_n]$. By definition $\vec{d}_1$ and the subspace of $[\vec{d}_2, \ldots, \vec{d}_n]$ are compatible w.r.t. the dual lattice.

Suppose $\mathbf{B}'_1 = \{\vec{b'}_2, \ldots, \vec{b'}_n\}$ is a basis of the hyperplane sublattice of another subspace compatible with $\vec{b}_1$. Let $\vec{d'}_1$ be the normal to this subspace such that $\vec{b}_1^T \cdot \vec{d'}_1 = 1$ So the dual of $\mathbf{B}' = [\vec{b}_1, \vec{b'}_2, \ldots, \vec{b'}_n]$ is of the form $[\vec{d'}_1, \vec{d}_2, \ldots, \vec{d}_n]$. Hence $[\vec{d'}_1, \vec{d}_2, \ldots, \vec{d}_n]$ is also a basis of the dual lattice $\mathcal{L}^*$. Hence $\vec{d'}_1$ is another compatible vector for $[\vec{d}_2, \ldots, \vec{d}_n]$. From the first part, there exist integers α_i such that $\vec{d'}_1 = \vec{d}_1 + \sum_{i=2}^{n} \alpha_i \cdot \vec{d}_i$. The dual of $[\vec{d}_1 + \sum_{i=2}^{n} \alpha_i \cdot \vec{d}_i, \vec{d}_2, \ldots, \vec{d}_n]$ is $[\vec{b}_1, \vec{b}_2 - \alpha_2 \cdot \vec{b}_1, \ldots, \vec{b}_n - \alpha_n \cdot \vec{b}_1]$. Then $[\vec{b'}_2, \ldots, \vec{b'}_n]$ and $[\vec{b}_2 - \alpha_2 \cdot \vec{b}_1, \ldots, \vec{b}_n - \alpha_n \cdot \vec{b}_1]$ are bases of the same hyperplane sublattice, perpendicular to $\vec{d'}_1$. □

C. 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., $\mathbf{B}$ 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 $\{\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n\}$. Suppose $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ is a basis of a lattice resulting from rotating/refelcting $\mathbb{Z}^n$. So there exists an orthonormal matrix $\mathbf{R}$ such that $\{\mathbf{R} \cdot \vec{b}_1, \ldots, \mathbf{R} \cdot \vec{b}_n\}$ is a basis of $\mathbb{Z}^n$.

Definition 20 ($\mathbb{Z}^n$ Isomorphism Problem)**.** *Given a linearly independent set of n-dimensional real vectors $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$, the lattice $\mathcal{L}(\mathbf{B})$ is called* isomorphic to $\mathbb{Z}^n$ *if there exists an orthonormal transformation matrix $\mathbf{R}$ such that $\mathbf{B}' = \{\mathbf{R} \cdot \vec{b}_1, \ldots, \mathbf{R} \cdot \vec{b}_n\}$ 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 $\mathbf{U}$ 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 $\mathbf{B}$ is a basis of a lattice isomorphic to $\mathbb{Z}^n$ and $\mathbf{D}$ is its dual, then self duality implies that $\mathbf{D} \subseteq \mathcal{L}(\mathbf{B})$. We have the following result.

Lemma 21. *Let $\mathbf{B}$ be a basis of a full rank lattice in $\mathbb{R}^n$. Then if $Det(\mathbf{B}) \neq 1$ or $\mathbf{D} \not\subseteq \mathcal{L}(\mathbf{B})$ where $\mathbf{D}$ is dual of $\mathbf{B}$, then $\mathcal{L}(\mathbf{B})$ is not isomorphic to $\mathbb{Z}^n$. Both these conditions can be decided in polynomial time.*

III. Proof of the Theorem 1

The proof of the main theorem heavily depends on a result from [14].

Theorem 22 (Theorem 2, [14])**.** *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 $|x_n| \leq max(\frac{m}{2g_1}, 1)$.*

An immediate corollary of the above lemma is as follows.

Corollary 23. *Let $gcd(a_1, a_2) = g$. Then, there exists integers x_1, x_2 such that $x_1a_1 + x_2a_2 = g$ and*

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

Another useful corollary is as follows.

Corollary 24. *Let $\vec{a} = (a_1, a_2, \ldots, a_n)$ be a primitive vector in $\mathbb{Z}^n$. Then there exists a vector $\vec{x} = (x_1, \ldots, x_n)$ in the lattice such that $\vec{a}^T \cdot \vec{x} = 1$ and either $||\vec{x}|| = 1$ or $||\vec{x}|| \leq ||\vec{a}||/2$.*

Proof. The bound to be proven for $||\vec{x}||$ is only dependent on the norm of $\vec{a}$ so w.l.g. assume that a_n is the largest component.

Let $g_k = gcd\{a_k, a_{k+1}, \ldots, a_n\}$. Since $\vec{a}$ is a primitive vector so $1 = g_1 = gcd\{a_1, a_2, \ldots, a_n\}$. From the above theorem there exist $x_1, \ldots, x_n$ such that $a_1x_1 + \cdots + a_nx_n = g_1 = 1$ such that $x_j^2 \leq (g_{j+1}/2g_j)^2$ for $1 \leq j \leq n-1$ and $x_n^2 \leq (\max\{a_n/(2g_1), 1\}^2$.

Observe that $g_{j+1} \leq a_j.g_j$. So $\sum_{j=1}^{n-1}(g_{j+1}/2g_j)^2 \leq (1/4).\sum_{j=1}^{n-1} a_j^2$. So $\sum_{j=1}^{n-1} x_j^2 \leq (1/4).\sum_{j=1}^{n-1} a_j^2$.

Now consider two cases: $a_n > 1$ and $a_n = 1$. In the first case $x_n^2 \leq a_n^2/4$. In this case $||\vec{x}||^2 \leq (1/4)||\vec{a}||^2$, where $\vec{x} = (x_1, x_2, \ldots, x_n)$.

Next consider the case $a_n = 1$. In this case define $\vec{x} = (0, 0 \ldots, 0, 1)$. □

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

(1) Base case is $n = 2$. Let $\vec{b}_2 = (a, b)$. So there exists c, d such that $c.a + d.b = 1$ where $|c| < |b|$ and $|d| < |a|$. Let $\vec{b}_1 = (-d, c)$. Then $\mathbf{B} = \{\vec{b}_2, \vec{b}_1\}$ spans $\mathbb{Z}^2$ because the determinant of $\mathbf{B}$ is $a.c + b.d = 1$. Further $||\vec{b}_2||^2 = a^2 + b^2 > d^2 + c^2 = ||\vec{b}_1||^2$. Hence the claim holds for this case.

Next steps will address the cases with $n > 2$.

(2) Let $\vec{v} = (v_1, \ldots, v_n)^T$. First consider the case where at least one component of $\vec{v}$ is zero. Without loss of generality assume that $v_n = 0$. We will reduce the problem to $n-1$ dimensional case. Let $\vec{b'}_n = (v_1, \ldots, v_{n-1})$. From induction hypothesis we have a basis $\mathbf{B'} = [\vec{b'}_2, \ldots, \vec{b'}_n]$ which spans $\mathbb{Z}^{n-1}$ and $||\vec{b'}_i|| < ||\vec{b'}_n||$ 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 $\vec{v}$.

(3) Next we consider the case when at least one component of $\vec{v}$ 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 $\mathbf{B} = [\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_{n-1}, \vec{v}]$.

Observe that $Det(\mathbf{B}) = 1$ 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 $\vec{v}$ 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.

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

where $(n + 1 - i)$-th column is $(0, \ldots, 0, r_i, -d_{i-1}/d_i, 0, \ldots, 0)^T$ in which r_i is the $(n + 1 - i)$-th entry and the $(n + 2 - i)$-th column is $(0, \ldots, 0, s_i, v_i/d_i, 0, \ldots, 0)^T$ in which v_i/d_i is the $n+1-i$-th entry.

Observe that d_i divides v_i and d_{i-1}. Therefore each entry of $\mathbf{T}_i$ is an integer. Further, $Det(\mathbf{T}_i) = (r_i v_i + s_i d_{i-1})/d_i = 1$. So $\mathbf{T}_i$ is a unimodular matrix. The inverse of $\mathbf{T}_i$, given below, is also unimodular.

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

Define $\mathbf{B} = \mathbf{T}_2^{-1}\mathbf{T}_3^{-1}\ldots\mathbf{T}_n^{-1}$ which is a unimodular matrix. Our next objective is to show that the first column of $\mathbf{B}$ is $\vec{v}$. To do this we determine the structure of $\mathbf{B}$. To begin with, the product of the rightmost two matrices is

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

and the product of $\mathbf{T}_{n-2}^{-1}$ with the above matrix is

$$\mathbf{T}_{n-2}^{-1}\mathbf{T}_{n-1}^{-1}\mathbf{T}_n^{-1} =$$

$$\begin{bmatrix} v_n & -s_n & 0 & 0 & \ldots \\ v_{n-1} & v_{n-1}r_n/d_{n-1} & -s_{n-1} & 0 & \ldots \\ v_{n-2} & v_{n-2}r_n/d_{n-1} & v_{n-2}r_{n-1}/d_{n-2} & -s_{n-2} & \ldots \\ d_{n-3} & d_{n-3}r_n/d_{n-1} & d_{n-3}r_{n-1}/d_{n-2} & r_{n-2} & \ldots \\ \vdots & & & & \end{bmatrix}$$

So, finally we will get

$$\mathbf{B} =$$

$$\begin{bmatrix} v_n & -s_n & 0 & 0 & \ldots & 0 & 0 \\ v_{n-1} & \frac{v_{n-1}r_n}{d_{n-1}} & -s_{n-1} & 0 & \ldots & 0 & 0 \\ v_{n-2} & \frac{v_{n-2}r_n}{d_{n-1}} & \frac{v_{n-2}r_{n-1}}{d_{n-2}} & -s_{n-2} & \ldots & 0 & 0 \\ v_{n-3} & \frac{v_{n-3}r_n}{d_{n-1}} & \frac{v_{n-3}r_{n-1}}{d_{n-2}} & \frac{v_{n-3}r_{n-2}}{d_{n-3}} & \ldots & 0 & 0 \\ \vdots & & & & & & \\ v_2 & \frac{v_2 r_n}{d_{n-1}} & \frac{v_2 r_{n-1}}{d_{n-2}} & \frac{v_2 r_{n-2}}{d_{n-3}} & \ldots & \frac{v_2 r_3}{d_2} & -s_2 \\ v_1 & \frac{v_1 r_n}{d_{n-1}} & \frac{v_1 r_{n-1}}{d_{n-2}} & \frac{v_1 r_{n-2}}{d_{n-3}} & \ldots & \frac{v_1 r_3}{d_2} & r_2 \end{bmatrix}$$

Observe that the first column of $\mathbf{B}$ is $\vec{v}$, as desired. In the last step we will show that the norm of all columns other than $\vec{v}$ is strictly less than $||\vec{v}||$. Label the columns of $\mathbf{B}$, from left to right, by $\vec{b}_n, \vec{b}_{n-1}, \ldots, \vec{b}_1$ respectively.

Square of the norm of vector $\vec{b}_k$ is

$$||\vec{b}_k||^2 = s_{k+1}^2 + (r_{k+1}^2/d_k^2)[v_k^2 + v_{k-1}^2 + \cdots + v_1^2]$$

Since $r_i.v_i + s_i.d_{i-1} = d_i$, from Corollary 23, $|r_i| \leq |d_{i-1}|/(2.|d_i|)$ 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 $||\vec{b}_k||^2$.

First, the case of $|d_k| = 1$. In this case

$$\begin{aligned} ||\vec{b}_k||^2 &\leq 1 + \frac{1}{4d_{k+1}^2} \cdot (v_k^2 + v_{k-1}^2 + \cdots + v_1^2) \\ &\leq 1 + (v_k^2 + v_{k-1}^2 + \cdots + v_1^2)/4 \\ &\leq v_{k+1}^2/4 + (v_k^2 + v_{k-1}^2 + \cdots + v_1^2)/4 \\ &< ||\vec{b}_n||^2 = ||\vec{v}||^2 \end{aligned}$$

In case $|d_k| > 1$,

$$\begin{aligned} ||\vec{b}_k||^2 &\leq \frac{v_{k+1}^2}{4.d_{k+1}^2} + \frac{1}{4.d_{k+1}^2} \cdot (v_k^2 + v_{k-1}^2 + \cdots + v_1^2) \\ &\leq (1/4)(v_{k+1}^2 + v_k^2 + \cdots + v_1^2) \\ &< ||\vec{b}_n||^2 = ||v||^2 \end{aligned}$$

In [14], the authors also show that the x_i's in Theorem 22 can be computed in polynomial time. Therefore, the basis $\mathbf{B}$ in Theorem 1 can also be computed in polynomial time.

IV. Min distance vector and Max distance subspace

Definition 25 (Minimum Distance Vector (MDV))**.** *Let $\mathcal{L}$ be a lattice and S be a pseudo-rational subspace of $\mathcal{L}$. A shortest lattice vector compatible with S is called MDV of S.*

Lemma 26. *Let S be a pseudo-rational subspace of some lattice. That S-compatible lattice vector is MDV of S which make the least angle with the normal to S.*

Definition 27 (Maximum Distance Subspace (MDS))**.** *Let $\vec{b}$ be any primitive vector of a lattice. Then that $\vec{b}$-compatible subspace S is the MDS of $\vec{b}$ whose normal makes the least angle with $\vec{b}$. Equivalently, that compatible S on which the projection of $\vec{b}$ is smallest.*

Lemma 28. *Let $\mathbf{B} = [\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n]$ be a lattice basis and $\mathbf{D} = [\vec{d}_1, \ldots, \vec{d}_n]$ be its dual basis. Then, $\vec{b}_1$ is the MDV of $[\vec{b}_2, \ldots, \vec{b}_n]$ if and only if $[\vec{d}_2, \ldots, \vec{d}_n]$ is MDS of $\vec{d}_1$.*

Proof. Recall that $\vec{b}_1$ is normal to $Span(\vec{d}_2, \ldots, \vec{d}_n)$ and $\vec{d}_1$ is normal to $span(\vec{b}_2, \ldots, \vec{b}_n)$. Let θ denotes the angle between $\vec{b}_1$ and $\vec{d}_1$. Then $\vec{b}_1$ is MDV of $[\vec{b}_2, \ldots, \vec{b}_n]$ if and only if θ is minimum if and only if $[\vec{d}_2, \vec{d}_3, \ldots, \vec{d}_n]$ is MDS of $\vec{d}_1$. □

One of the consequences of Lemma 19 is the following result.

Lemma 29. *Let $\{\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n\}$ be a basis of a lattice. Then the MDV of $[\vec{b}_2, \ldots, \vec{b}_n]$ is $\vec{b}_1 + \sum_{i=2}^{n} \alpha_i . \vec{b}_i$ for some integers α_i.*

Similarly the MDS of $\vec{b}_1$ has a sublattice basis given by $[\vec{b}_2 - \beta_2 . \vec{b}_1, \ldots, \vec{b}_n - \beta_n . \vec{b}_1]$, where β_i are integers.

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

Lemma 30. *Let $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ be a basis of a lattice isomorphic to $\mathbb{Z}^n$. Let $\mathbf{D} = \{\vec{d}_1, \ldots, \vec{d}_n\}$ be its dual basis. If $||\vec{d}_1|| \leq ||\vec{b}_1||$ and $||\vec{b}_1|| > 1$, then $\vec{b}_1$ is not an MDV.*

Proof. First consider the case that $\vec{d}_1 = \vec{e}_1$. In this case $span(\vec{b}_2, \ldots, \vec{b}_n) = span(\vec{e}_2, \ldots, \vec{e}_n)$ which is isomorphic to $\mathbb{Z}^{n-1}$. If $\vec{b}_1$ was MDV, then $\vec{b}_1 = \vec{e}_1$. This contradicts the given fact that $||\vec{b}_1|| > 1$. Hence $\vec{b}_1$ cannot be an MDV.

Now consider the case that $||\vec{d}_1|| > 1$. Then $1 < ||\vec{d}_1|| \leq ||\vec{b}_1||$. From Corollary 24, there exists a primitive vector $\vec{b'}_1$ such that $\vec{d}_1^T \cdot \vec{b'}_1 = 1$ and $||\vec{b'}_1|| \leq \max\{1, ||\vec{d}_1||/2\}$. So $||\vec{b'}_1|| \leq \max\{1, ||\vec{b}_1||/2\}$.

$\vec{d}_1^T \cdot \vec{b}_1 = 1 = \vec{d}_1^T \cdot \vec{b'}_1$ implies that the length of the projection of $\vec{b'}_1$ on $\vec{d}_1$ is equal to that of $\vec{b}_1$, namely, $1/||\vec{d}_1||$. Hence $\vec{b'}_1$ is also compatible with $[\vec{b}_2, \ldots, \vec{b}_n]$, i.e., $[\vec{b'}_1, \vec{b}_2, \ldots, \vec{b}_n]$ is also a lattice basis. Since $||\vec{b'}_1|| < ||\vec{b}_1||$, $\vec{b}_1$ cannot be an MDV. □

Theorem 31. *Let $\mathbf{B}$ be a basis of a lattice isomorphic to $\mathbb{Z}^n$. If $\vec{b}_1$ is MDV of $[\vec{b}_2, \ldots, \vec{b}_n]$ and $[\vec{b}_2, \ldots, \vec{b}_n]$ is MDS of $\vec{b}_1$, then $||\vec{b}_1|| = 1$.*

Proof. Let $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$ be a basis and $\mathbf{D} = [\vec{d}_1, \ldots, \vec{d}_n]$ be its dual. Suppose $\vec{b}_1$ is the MDV of $[\vec{b}_2, \ldots, \vec{b}_n]$ and $[\vec{b}_2, \ldots, \vec{b}_n]$ be the MDS of $\vec{b}_1$.

If $\vec{d}_1$ is not the MDV of $[\vec{d}_2, \ldots, \vec{d}_n]$, then some $\vec{d'}_1$ is its MDV. So $\mathbf{D'} = [\vec{d'}_1, \vec{d}_2, \vec{d}_3, \ldots, \vec{d}_n]$ is a basis of the lattice and $angle(\vec{b}_1, \vec{d'}_1) < angle(\vec{b}_1, \vec{d}_1)$. Let $\mathbf{B'} = [\vec{b'}_1, \vec{b'}_2, \ldots, \vec{b'}_n]$ be the dual of $\mathbf{D'}$. Since $\vec{b'}_1$ is the primitive vector perpendicular to $[\vec{d}_2, \ldots, \vec{d}_n]$, $\vec{b'}_1 = \vec{b}_1$. So $[\vec{b'}_2, \ldots, \vec{b'}_n]$ is also compatible to $\vec{b}_1$. Since $\vec{d'}_1$ is perpendicular to $[\vec{b'}_2, \ldots, \vec{b'}_n]$ and $angle(\vec{b}_1, \vec{d'}_1) < angle(\vec{b}_1, \vec{d}_1)$ so $[\vec{b}_2, \ldots, \vec{b}_n]$ cannot be the MDS of $\vec{b}_1$. That is absurd. So $\vec{d}_1$ must be the MDV of $[\vec{d}_2, \ldots, \vec{d}_n]$.

Suppose $||\vec{d}_1|| \leq ||\vec{b}_1||$. Since $\vec{b}_1$ is MDV, from Lemma 30, $||\vec{b}_1|| = 1$. Hence $||\vec{d}_1|| = 1$. Reversing the roles of primal and dual bases apply the same argument to again conclude that $\vec{b}_1$ and $\vec{d}_1$ are both unit vectors. □

Corollary 32. *If $\mathbf{B}$ is a basis of a lattice isomorphic to $\mathbb{Z}^n$ such that for all $i \in [n]$, $\vec{b}_i$ is MDV of $\mathbf{B} \setminus \{\vec{b}_i\}$ and $\mathbf{B} \setminus \{\vec{b}_i\}$ is MDS of $\vec{b}_i$, then $\mathbf{B}$ is the orthonormal basis.*

V. On AMDV bases

In this section we investigate the bases, $\mathbf{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$, in which $\vec{b}_i$ is the MDV of $\mathbf{B} \setminus \{\vec{b}_i\}$ for each i. Such a basis will be called an AMDV (all MDV) basis. It is easy to see that if $\mathbf{D}$ is the dual of an AMDV basis, then $\mathbf{D}$ is an AMDS (all MDS) basis of the dual lattice.

Corollary 33. *Let $\mathcal{L}$ be a lattice isomorphic to $\mathbb{Z}^n$. Let $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$ be an AMDV basis of $\mathcal{L}$ and $[\vec{d}_1, \ldots, \vec{d}_n]$ be its dual. Then for each i, either $||\vec{b}_i|| = 1$ or $||\vec{b}_i|| < ||\vec{d}_i||$.*

Lemma 34. *$\{\vec{e}_1, \ldots, \vec{e}_n\}$ is the only $\mathbb{Z}^n$ basis which is AMDV and totally unimodular.*

Proof. Let $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$ be an AMDV basis of $\mathbb{Z}^n$ which is also totally unimodular. If any $\vec{b}_i$ is a unit vector, then $\mathbf{B} \setminus \{\vec{b}_i\}$ 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 $||\vec{b}_i|| > 1, \forall i \in [n]$. The inverse matrix $\mathbf{B}^{-1} = [c_1, \ldots, c_n]$ is also a totally unimodular matrix, so $\mathbf{B}^{-1} \in \{-1, 0, 1\}^{n \times n}$. Without loss of generality, we can assume that $(\mathbf{B}^{-1})_{1,1} = 1$. Since $\mathbf{B}c_1 = \vec{e}_1$, $1 = ||\mathbf{B}c_1|| = ||\vec{b}_1 + \sum_{j=2}^{n} (c_1)_j . \vec{b}_j||$. But $||\vec{b}_1|| > 1$ so $||\vec{b}_1|| > ||\vec{b}_1 + \sum_{j=2}^{n} (c_1)_j . \vec{b}_j||$. This means that $\vec{b}_1$ is not MDV. □

VI. Shortest vector in hyperplane lattice

In [15], 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 35. *Let $\mathcal{L}$ be a lattice isomorphic to $\mathbb{Z}^n$ where $n \geq 4$ and $\vec{b}$ be an arbitrary vector in $\mathcal{L}$. Let $\mathcal{L}_1$ denote the hyperplane sublattice of $\mathcal{L}$ on subspace perpendicular to $\vec{b}$. Then the shortest vector $\vec{v}$ in $\mathcal{L}_1$ is either a unit vector or $||\vec{v}|| \leq ||\vec{b}||/\sqrt{2}$.*

Proof. To prove this claim we will work in the reference frame in which $\mathcal{L}$ is $\mathbb{Z}^n$. Let $\vec{b} = (a_1, a_2, \ldots, a_n)$. Consider the case where $a_i = 0$ for some i. Then $\vec{e}_i \in \mathcal{L}_1$

Now consider the case where all the components of $\vec{b}$ are non-zero. Let a_i and a_j be the two magnitude-wise smallest components of $\vec{b}$, i.e., $|a_i| \leq |a_j| \leq |a_k|$ for all $k \in [n] \setminus \{i, j\}$. Let $\vec{u} = (0, \ldots, -a_j, 0 \ldots, 0, a_i, 0, \ldots)$ where the i-th component is $-a_j$ and the j-th component is a_i. Clearly $\vec{u}$ is perpendicular to $\vec{b}$ so $\vec{u}$ belongs to $\mathcal{L}_1$. Further, $||\vec{u}||^2 = a_i^2 + a_j^2 \leq (2/n)||\vec{b}||^2 \leq (1/2)||\vec{b}||^2$. □

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, $\vec{b}$, from $\mathcal{L}$. If $\vec{b}$ is a unit vector then the task is over. Otherwise compute the hyperplane sublattice, $\mathcal{L}_1$, of $\mathcal{L}$ perpendicular to $\vec{b}$. Compute a shortest vector $\vec{b}_1$ in $\mathcal{L}_1$. Then either $\vec{b}_1$ is a unit vector (which is the desired result) or $||\vec{b}_1|| \leq ||\vec{b}||/\sqrt{2}$. Thus $\vec{b}_1$ is the new $\vec{b}$ and we repeat this step. This algorithm requires at most $2.\log_2 ||\vec{b}||$ iterations. Hence we have the following result.

Theorem 36. *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 $\vec{s}_1$, then compute the subspace perpendicular to $\vec{s}_1$, 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 37. *$\mathbb{Z}^n$ isomorphism problem can be reduced to SVP on hyperplane sublattice of a $\mathbb{Z}^n$-isomorphic lattice.*

VII. Short Vectors that are Voronoi Relevant

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

Claim 38. *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 $||\vec{w}|| < \lambda_j$ so $\vec{w} \in \mathcal{B}(0, \lambda_j - \epsilon)$ where $\epsilon = (\lambda_j - ||\vec{w}||)/2 > 0$. Since $\mathcal{B}(0, \lambda_j - \epsilon)$ has at most $j-1$ linearly independent vectors and $\vec{s}_1, \ldots, \vec{s}_{j-1}$ is one such set, $\vec{w} \in span(\vec{s}_1, \ldots, \vec{s}_{j-1})$. □

An obvious corollary of Claim 38 is as follows.

Corollary 39. *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 [16], 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 extend this result in the following theorem.

Theorem 40. *If $S = \{\vec{s}_i, \ldots, \vec{s}_n\}$ is a solution to SMP for a lattice $\mathcal{L}$, then $S \subseteq V(\mathcal{L})$.*

Proof. From theorem 17, if $\vec{v} \in \mathcal{L}$ is not a Voronoi relevant vector, then there exist $\vec{w} \in \mathcal{L} \setminus \{0, \vec{v}\}$ such that $||\frac{\vec{v}}{2} - \vec{w}|| \leq ||\frac{\vec{v}}{2}||$. 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 $\mathcal{L}$.
- $||\vec{s}_1/2 - \vec{w}|| = ||\vec{s}_1/2||$: Then $\vec{w}, \vec{s}_1$ and $\vec{0}$ occur on the circumference of the circle centered at $\vec{s}_1/2$ and radius $||\vec{s}_1||/2$. So vector $\vec{s}_1$ forms the diameter of the circle. Since $\vec{w} \neq \vec{s}_1$, vector $\vec{w}$ forms a chord other than $\vec{s}_1$, So $\vec{w}$ must be shorter than $\vec{s}_1$. This 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 38, $\vec{s}_i - 2\vec{w}$ 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 $\vec{s}_1, \ldots, \vec{s}_{i-1}$.
- $||\vec{s}_i - 2\vec{w}|| = ||\vec{s}_i||$: Using the argument in the second part of the above proof we conclude that $||\vec{w}|| < ||\vec{s}_i||$. So $\vec{w} \in X = span(\vec{s}_1, \ldots, \vec{s}_{i-1})$.
  Next consider the following. Points $\vec{0}, \vec{s}_i$ and $2\vec{w}$ form an isosceles triangle with $2\vec{w}$ being the base. Therefore $\vec{w} \cdot (\vec{s}_i - \vec{w}) = 0$. So $||\vec{s}_i||^2 = ||\vec{s}_i - 2\vec{w}||^2 = ||\vec{s}_i - \vec{w}||^2 + ||\vec{w}||^2 - 2\vec{w} \cdot (\vec{s}_i - \vec{w}) = ||\vec{s}_i - \vec{w}||^2 + ||\vec{w}||^2$. So $||\vec{s}_i - \vec{w}|| < ||\vec{s}_i||$.
  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 $\vec{s}_1, \ldots, \vec{s}_{i-1}$.

□

Corollary 41. *For any lattice $\mathcal{L}$*

$$\lambda_n(\mathcal{L}) \leq ||V(\mathcal{L})|| \leq \frac{n^{3/2}}{2}\lambda_n(\mathcal{L})$$

Proof. The lower bound is obvious due to Theorem 40. Let $\mathbf{B}$ be a shortest basis of $\mathcal{L}$. Using Lemma 12, we know that $||\mathbf{B}|| \leq \sqrt{n}\lambda_n(\mathcal{L})/2$. Also, the norm of the shortest vector in the coset $2\mathcal{L} + \vec{v}$, where $\vec{v} \in \mathcal{L}$, is at most $||\vec{v}||$. We know that all possible cosets are given by $2\mathcal{L} + \mathbf{B}\vec{z}$ where $\vec{z} \in \{0, 1\}^n$. Therefore, the norm of the shortest vector cannot be more than the sum of the norms of the vectors of $\mathbf{B}$, irrespective of the choice of $\vec{z}$. The latter cannot be more than $n.||\mathbf{B}||$. Thus $||V(\mathcal{L})|| \leq n^{3/2}\lambda_n(\mathcal{L})/2$. □

The algorithm given by Micciancio et al. [17] computes all the Voronoi relevant vectors, then Algorithm 1 computes a solution of SMP.

Theorem 42. *Algorithm 1 computes a solution of SMP.*

Proof. From Theorem 40 we know that the list of Voronoi relevant vectors contain all the solutions of SMP. It is obvious that the algorithm will compute n linearly independent lattice vectors. Let the sorted sequence of the vectors of $V(\mathcal{L})$ be $\{\vec{v}_1, \vec{v}_2, \dots\}$. Let $\{\vec{v}_{j_1}, \dots, \vec{v}_{j_n}\}$ be any arbitrary solution of SMP. Suppose the algorithm computes the set $S = \{\vec{v}_{i_1}, \dots, \vec{v}_{i_n}\}$ where $i_1 < i_2 < \dots i_n$. Next we will show that $i_p \leq j_p$.

Assume that $i_p > j_p$. So we have $i_q \leq j_p < i_{q+1}$ for some $q < p$. From the algorithm we know that each of the vectors $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_{j_p}$ can be spanned by $\{\vec{v}_{i_1}, \dots, \vec{v}_{i_q}\}$. So $span(\vec{v}_{j_1}, \dots, \vec{v}_{j_p}) \subseteq span(\vec{v}_{i_1}, \dots, \vec{v}_{i_q})$. Observe that $\vec{v}_{j_1}, \dots, \vec{v}_{j_p}$ is a linearly independent set. Similarly $(\vec{v}_{i_1}, \dots, \vec{v}_{i_q})$ is also linearly independent. Therefore $p \leq q$, which is a contradiction!

From Lemma 11 $||\vec{v}_{i_p}|| \geq \lambda_p$ for all p. Also from the above result $||\vec{v}_{i_p}|| \leq ||\vec{v}_{j_p}|| = \lambda_p$ for all p. Hence $||\vec{v}_{i_p}|| = \lambda_p$ for all p. □

The number of Voronoi relevant vectors is at most $2(2^n-1)$, the sorting would take time $\tilde{O}(2^n)$. The number of iterations in the while loop is $O(2^n)$ and in each iteration, the amount of time required to check whether a vector is to be included in the set S is polynomial. Therefore, the entire running time of the algorithm is $\tilde{O}(2^{2n})$ because this is the time complexity of Micciancio's algorithm to compute $V(\mathcal{L})$.

In [18], 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

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

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

Claim 43. *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 $\vec{b}_i$ is sum of vectors in $n! \times 2\mathcal{C}(\mathcal{L})$. Therefore, $||\mathbf{B}|| \leq n.n!.\lambda_n$. □

Input: A basis $\mathbf{B} = [\vec{b}_1, \dots, \vec{b}_n]$ for $\mathcal{L}$.
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
  $i = i + 1$;
end
Return $\mathbf{S}$.

Algorithm 1: Algorithm for solving SMP

References

[1] J. C. Lagarias, H. W. Lenstra, and C.-P. Schnorr, "Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice," *Combinatorica*, vol. 10, no. 4, pp. 333–348, 1990.

[2] R. Kannan, "Minkowski's convex body theorem and integer programming," *Mathematics of operations research*, vol. 12, no. 3, pp. 415–440, 1987.

[3] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische annalen*, vol. 261, no. ARTICLE, pp. 515–534, 1982.

[4] I. Haviv and O. Regev, "On the lattice isomorphism problem," in *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*. SIAM, 2014, pp. 391–404.

[5] C. Hunkenschröder, "Deciding whether a lattice has an orthonormal basis is in co-np," *arXiv preprint arXiv:1910.03838*, 2019.

[6] H. W. Lenstra and A. Silverberg, "Lattices with symmetry," *Journal of Cryptology*, vol. 30, no. 3, pp. 760–804, 2017.

[7] H. Bennett, A. Ganju, P. Peetathawatchai, and N. Stephens-Davidowitz, "Just how hard are rotations of $\mathbb{Z}^n$? algorithms and cryptography with the simplest lattice," 2022. [Online]. Available: https://eprint.iacr.org/2021/1548

[8] X. Zhan, "Completion of a partial integral matrix to a unimodular matrix," *Linear algebra and its applications*, vol. 414, no. 1, pp. 373–377, 2006.

[9] M. Fang, "On the completion of a partial integral matrix to a unimodular matrix," *Linear algebra and its applications*, vol. 422, no. 1, pp. 291–294, 2007.

[10] M. Forst and L. Fukshansky, "Counting basis extensions in a lattice," *arXiv preprint arXiv:2011.05307*, 2020.

[11] D. Micciancio and S. Goldwasser, *Complexity of lattice problems: a cryptographic perspective*. Springer Science & Business Media, 2012, vol. 671.

[12] D. Micciancio, "Efficient reductions among lattice problems," in *Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 2008, pp. 84–93.

[13] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. Springer Science & Business Media, 2013, vol. 290.

[14] D. Ford and G. Havas, "A new algorithm and refined bounds for extended gcd computation," in *International Algorithmic Number Theory Symposium*. Springer, 1996, pp. 145–150.

[15] P. 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.

[16] G. Hanrot, X. Pujol, and D. Stehlé, "Algorithms for the shortest and closest lattice vector problems," in *International Conference on Coding and Cryptology*. Springer, 2011, pp. 159–190.

[17] D. Micciancio and P. Voulgaris, "A deterministic single exponential time algorithm for most lattice problems based on voronoi cell computations," *SIAM Journal on Computing*, vol. 42, no. 3, pp. 1364–1391, 2013.

[18] C. Hunkenschröder, G. Reuland, and M. Schymura, "On compact representations of voronoi cells of lattices," *Mathematical Programming*, pp. 1–22, 2020.