On Communication for Distributed Babai Point Computation

Maiara F. Bollauf, Vinay A. Vaishampayan, and Sueli I. R. Costa.

Abstract

We present a communication-efficient distributed protocol for computing the Babai point, an approximate nearest point for a random vector $\mathbf{X} \in \mathbb{R}^n$ in a given lattice. We show that the protocol is optimal in the sense that it minimizes the sum rate when the components of $\mathbf{X}$ are mutually independent. We then investigate the error probability, i.e. the probability that the Babai point does not coincide with the nearest lattice point, motivated by the fact that for some cases, a distributed algorithm for finding the Babai point is sufficient for finding the nearest lattice point itself. Two different probability models for $\mathbf{X}$ are considered—uniform and Gaussian. For the uniform model, in dimensions two and three, the error probability is seen to grow with the packing density, and we demonstrate that the densest lattice in dimension two presents the worst error probability. For higher dimensions, we develop probabilistic concentration bounds as well as bounds based on geometric arguments for the error probability. The probabilistic bounds lead to the conclusion that for lattices which generate suitably thin coverings of $\mathbb{R}^n$ (which includes lattices that meet Rogers' bound on the covering radius), the error probability goes to unity as n grows. Probabilistic and geometric bounds are also used to estimate the error probability under the uniform model for various lattices including the A_n family and the Leech lattice, Λ_{24}. On the other hand, for the Gaussian model, the error probability goes to zero as the lattice dimension tends to infinity, provided the noise variance is sufficiently small.

***Index terms*—Lattices, data compression, distributed function computation, Babai point, nearest lattice point, communication complexity, error probability.**

M. F. Bollauf was with the Institute of Mathematics, Statistics and Computer Science, University of Campinas and is now with Simula UiB, Norway (e-mail: maiara@simula.no).

V. A. Vaishampayan is with Department of Engineering Science and Physics, City University of New York (CUNY) (e-mail: Vinay.Vaishampayan@csi.cuny.edu).

S. I. R. Costa is with the Institute of Mathematics, Statistics and Computer Science, University of Campinas (e-mail: sueli@unicamp.br).

This work was initiated during a visit by M. F. B. to CUNY in 2016, and was presented in part at the IEEE International Symposium on Information Theory, Aachen, Germany, 2017 [4].

I. Introduction

We are given a lattice $\Lambda \subset \mathbb{R}^n$ and a random vector of observations, $\mathbf{X} = (X_1, X_2, \ldots, X_n) \in \mathbb{R}^n$. Each X_i is available at a distinct sensor-processor node (SN), which is connected by a communication link to a central computing node (CN). The objective is to compute at the CN, the Babai point, a well-known approximation to the nearest lattice point of $\mathbf{X}$ [3]. Towards this end, the ith SN sends an approximation of X_i to the CN at a communication rate of R_i bits/sample. In this work, we present a communication protocol for this computation and show that it is optimal in the sense of minimizing the communication rate. We then investigate the connection between the structure of the lattice, as determined by its generator matrix, and the communication cost, the error probability (the probability that the Babai point does not coincide with the nearest lattice point), and the packing density. While this connection is of independent interest, it also allows a designer to understand situations under which any further communication for determining the true nearest lattice point is unnecessary. Our model for distributed computation is referred to as the centralized model and is illustrated in Fig. 1.

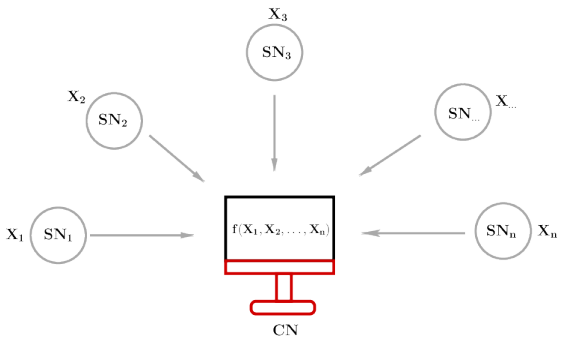

Fig. 1. Centralized model for distributed computation. Each sensor node (SN) encodes its observation at a finite rate and sends it to the central compute node (CN), where the function f is to be computed. The problem is to determine the tradeoff between communication rate and the accuracy with which the function is computed. In this work, the function is the approximate nearest lattice point (Babai point).

We note that our problem is a special case of the general distributed function computation problem, where the objective is to compute a given function $f(X_1, X_2, \ldots, X_n)$ at the CN based on information communicated from each of the n SN's [26]. In our case, f is the function which computes an approximate nearest lattice point based on the nearest plane algorithm [3] and $f(\mathbf{X})$ is the Babai point.

Interest in communication issues for the distributed computation of the Babai point, and more generally for the nearest lattice point [32], arise in many contexts: wireless communication, machine learning and cryptography. We briefly describe the applications next.

In MIMO wireless systems, the decoding problem is equivalent to finding a nearest lattice point. Well-known systems such as V-BLAST prefer to find the Babai point because of the high computational complexity of finding the nearest lattice point. Thus, distributed computation of the Babai point is useful in distributed MIMO receivers [30]. More generally, communication issues for channel decoding and demodulation have been studied in the context of cooperative communications [11], [31]. For a comprehensive review of lattices in communication, see [34].

In recent years, interest has grown in communication issues related to distributed machine learning [20]. Such problems also fit into the distributed function computation framework, and we expect that lattice methods will eventually play an important role here.

The study of the approximate nearest lattice point is also relevant in cryptography. In fact the nearest lattice point problem has been proposed as a basis for lattice cryptography [2], [15], [18], [23], [28], due to its hardness [12], examples being the Goldreich-Goldwasser-Halevi (GGH) and learning with errors (LWE) cryptosystems. Their security relies on the solution of this problem and the nearest plane algorithm [3] is used to estimate the resistance to attack when the received message is relatively close to the lattice point to be decoded. Our work is of interest in understanding the communication required in a distributed lattice-based cryptosystem.

This paper is based on preliminary work presented in [4].

The following are the contributions of this paper.

- The problem of determining the communication cost for computing the Babai point in a distributed setting is formulated as a distributed function computation problem.
- A communication efficient distributed protocol for computing the Babai point is presented.
- Optimality of the protocol is shown by evaluating the conditional graph entropy for the problem.
- Since the Babai point is not identical to the true nearest lattice point, we evaluate the probability that the two points differ. This probability is referred to as the error probability.
- In dimensions two and three a complete calculation of the error probability is provided. This calculation is based on special bases for a lattice, namely Minkowski-reduced and obtuse superbase.

- In dimensions two and three a relation between the error probability and the packing density of the lattice is investigated and lattices that achieve the optimum tradeoff are characterized.
- For higher dimensions, a combination of probabilistic and geometric tools are used to understand the behavior of the error probability and its relation to the 'sphericity' of a Voronoi cell of the lattice. These approaches allow us to bound the error probability for A_n, Λ_{24}, and further, to show that for lattices that result in thin coverings, in the sense that they meet Rogers' bound on the covering radius, the error probability goes to one as the dimension goes to infinity for a uniform probability model.
- For the families of lattices that we have considered, our results suggest that lattices with higher packing densities have a higher error probability. However, there is not a monotone relationship between the communication cost and the lattice packing density.

The paper is organized as follows. Mathematical foundations, a preliminary analysis, and a more precise problem formulation, are in Sec. II. A communication protocol and its associated communication cost are presented in Sec. III, along with a proof of optimality. The error probability is analyzed in Sec. IV for dimensions two and three, assuming a uniform conditional distribution on $\mathbf{X}$. An analysis of the error probability for higher dimensions and its relation to the 'sphericity' of a Voronoi cell of the lattice (in terms of its covering and packing radii), is presented in Sec. V. This analysis differs from prior sections in that it uses probabilistic tools to overcome difficulties with multi-dimensional integration. In this section we also discuss results about error probability when $\mathbf{X}$ is obtained by adding Gaussian noise to a randomly chosen lattice point. Conclusions and future work are in Sec. VI.

II. Lattice Basics and Preliminary Calculations

Notations, lattice basics, error probability simplifications and a more precise problem formulation are presented in this section.

A (full rank) lattice $\Lambda \subset \mathbb{R}^n$ is the set of all integer linear combinations of a set of linearly independent vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\} \subset \mathbb{R}^n$, called *lattice basis*. We can also write $\Lambda = \{V\mathbf{u},\ \mathbf{u} \in \mathbb{Z}^n\}$, where the columns of the *generator matrix* V are the basis vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$. The matrix $A = V^T V$ is the associated *Gram matrix* and the (i, j) entry of A is the Euclidean inner product of $\mathbf{v}_i$ and $\mathbf{v}_j$, which here will be denoted by $\mathbf{v}_i \cdot \mathbf{v}_j$. Two matrices V_1 and V_2 generate the same lattice if and only if $V_1 = V_2 U$, where U is an unimodular matrix, i.e., it has integer entries and $|\det(U)| = 1$.

A set $\mathcal{F}$ is called a *fundamental region* of a lattice Λ if all its translations by elements of Λ cover $\mathbb{R}^n$, i.e., $\bigcup_{\lambda\in\Lambda} \mathcal{F}+\lambda = \mathbb{R}^n$, and the interiors of $\lambda_1+\mathcal{F}$ and $\lambda_2+\mathcal{F}$ do not intersect for $\lambda_1 \neq \lambda_2$. The *Voronoi region* or *Voronoi cell* $\mathcal{V}(\lambda)$ is an example of fundamental region and it is defined as

$$\mathcal{V}(\lambda) = \{\mathbf{x}\in\mathbb{R}^n : \|\mathbf{x}-\lambda\| \leq \|\mathbf{x}-\tilde{\lambda}\|, \text{ for all } \tilde{\lambda}\in\Lambda\},$$

where $\|.\|$ denotes the Euclidean norm. Note that $\mathcal{V}(\lambda) = \lambda + \mathcal{V}(0)$. The *volume* of a lattice Λ is the volume of any of its fundamental regions and is given by $\text{vol}\,(\Lambda) = |\det(V)|$, where V is a generator matrix of Λ.

A vector $\mathbf{v}\in\Lambda$ is called a *Voronoi vector* if the hyperplane $\{\mathbf{x}\in\mathbb{R}^n : \mathbf{x}\cdot\mathbf{v} = \frac{1}{2}\mathbf{v}\cdot\mathbf{v}\}$ has a non-empty intersection with $\mathcal{V}(0)$. A Voronoi vector is said to be *relevant* (or face-determining) if this intersection is an $(n-1)-$dimensional face of $\mathcal{V}(0)$, here we are adopting the notation of [8]. Observe that the hyperplane above defines a halfspace

$$\mathcal{H}_{\mathbf{v}} = \left\{\mathbf{x}\in\mathbb{R}^n : \mathbf{x}\cdot\mathbf{v} \leq \frac{1}{2}\mathbf{v}\cdot\mathbf{v}\right\},$$

and the Voronoi region is the intersection of $\mathcal{H}_{\mathbf{v}}$ over all relevant Voronoi vectors $\mathbf{v}\in\Lambda$.

Let $\mathcal{S}_n(r)$ denote the n-dimensional sphere (ball) in $\mathbb{R}^n$, centered at the origin. The packing radius r_{pack} of a lattice Λ is half of the minimum distance between lattice points and the packing density $\Delta(\Lambda) = \text{vol}\,(\mathcal{S}_n(r_{\text{pack}}))\,/\text{vol}\,(\Lambda)$ is the fraction of space that is covered by balls of radius r_{pack} in $\mathbb{R}^n$ centered at lattice points. The covering radius r_{cov} of lattice Λ is the smallest r for which the union of spheres of radius r, centered at the lattice points, covers $\mathbb{R}^n$. The thickness of a covering is $\Theta = \text{vol}\,(\mathcal{S}_n(r_{\text{cov}}))/\text{vol}\,(\Lambda)$. A lattice with smaller Θ than another is said to provide a *thinner* covering of $\mathbb{R}^n$. The relation $\mathcal{S}_n(r_{\text{pack}}) \subset \mathcal{V}(0) \subset \mathcal{S}_n(r_{\text{cov}})$ always holds.

The objective of the *nearest lattice point problem* is to find

$$\mathbf{u} = \arg\min_{\overline{\mathbf{u}}\in\mathbb{Z}^n} \|\mathbf{x} - V\overline{\mathbf{u}}\|^2,$$

for a given $\mathbf{x}\in\mathbb{R}^n$, where the norm considered is the standard Euclidean norm. The nearest lattice point to $\mathbf{x}$ is then given by $\mathbf{x}_{nl} = V\mathbf{u}$. We refer to $\mathbf{x}_{nl}$ as the Voronoi point corresponding to $\mathbf{x}$.

We denote the integer and fractional parts of $x\in\mathbb{R}$ by $\lfloor x\rfloor$ and $\{x\}$, respectively. Thus $x = \lfloor x\rfloor + \{x\}$ and $0\leq\{x\}<1$. The nearest integer function is $[x] = \lfloor x+1/2\rfloor$.

The nearest plane (np) algorithm [3], an approach for approximating the nearest lattice point, computes $\mathbf{x}_{np}$, an approximation to $\mathbf{x}_{nl}$, given by $\mathbf{x}_{np} = u_1\mathbf{v}_1 + u_2\mathbf{v}_2 + \ldots + u_n\mathbf{v}_n$, where

the computation of $u_i \in \mathbb{Z}$ is described next. Note that we refer to $\mathbf{x}_{np}$ as the Babai point corresponding to $\mathbf{x}$ and to the closure of the set of $\mathbf{x}$ mapped to $\mathbf{y} \in \Lambda$ by the nearest plane algorithm as the Babai cell $\mathcal{B}(\mathbf{y})$. Babai cells are also fundamental regions for the lattice Λ, and hence have volume $|\det V|$. Further, Babai cells are congruent hyperrectangles in $\mathbb{R}^n$.

The method for obtaining the Babai point for general lattice generators [3] is described as follows. Let $\mathcal{S}_i$ denote the subspace spanned by the vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_i\}$, $i = 1, 2, \ldots, n$. Let $\mathcal{P}_i(\mathbf{z})$ be the orthogonal projection of $\mathbf{z}$ onto $\mathcal{S}_i$ and let $\mathbf{v}_{i,i-1} = \mathcal{P}_{i-1}(\mathbf{v}_i)$ be the closest vector to $\mathbf{v}_i$ in $\mathcal{S}_{i-1}$. Consider the decomposition $\mathbf{v}_i = \mathbf{v}_{i,i-1} + \mathbf{v}_{i,i-1}^{\perp}$, and let $\mathbf{z}_i^{\perp} = \mathbf{z}_i - \mathcal{P}_i(\mathbf{z}_i)$. Start with $\mathbf{z}_n = \mathbf{x}$ and $i = n$ and compute $u_i = \left\lceil \frac{\mathbf{z}_i \cdot \mathbf{v}_{i,i-1}^{\perp}}{\|\mathbf{v}_{i,i-1}^{\perp}\|^2} \right\rfloor$, $\mathbf{z}_{i-1} = \mathcal{P}_{i-1}(\mathbf{z}_i) - u_i \mathbf{v}_{i,i-1}$, for $i = n, n-1, \ldots, 1$. Here "$\cdot$" stands for the usual inner product.

For an upper triangular generator matrix V, which is the case considered in this paper, the Babai point is obtained by computing

$$u_i = \left\lceil \frac{x_i - \sum_{j=i+1}^{n} v_{i,j} u_j}{v_{i,i}} \right\rfloor \tag{1}$$

in the order $i = n, n-1, \ldots, 1$. For a triangular generator matrix, each Babai cell $\mathcal{B}(\mathbf{y})$ is an axis-aligned rectangle and has vertices $\mathbf{y} \pm |v_{11}|/2, \mathbf{y} \pm |v_{22}|/2, \ldots, \mathbf{y} \pm |v_{nn}|/2$. We remark that given a lattice Λ with an arbitrary generator matrix $V \in \mathbb{R}^{n \times n}$ we can always apply the QR decomposition $V = QR$, where $Q \in \mathbb{R}^{n \times n}$ is an orthogonal matrix and $R \in \mathbb{R}^{n \times n}$ is an upper triangular matrix. The matrix R, whose column vectors are a rotation of the original basis vectors of Λ, will generate a congruent version of this lattice.

Example 1. *Fig. 2 represents the Babai cells and the Voronoi cells (hexagons) for the hexagonal lattice A_2 generated by $\{(1,0), (1/2, \sqrt{3}/2)\}$ and illustrates how the np algorithm approximates the nearest lattice point problem.*

It is an important fact that the Babai cell $\mathcal{B}(0)$ is dependent on the choice of the lattice basis, whereas the Voronoi cell is invariant to the choice of lattice basis. In particular, the Babai cell even depends on the order in which the basis vectors are listed. There are previous works in the literature, here we particularly address [15, Ch. 18], where the Babai point is obtained after LLL basis reduction. Under the LLL assumption, the author presents upper bounds for the magnitude of the error between the Babai point and the Voronoi point. This approach differs from what we are presenting here, as we discuss the error in a probabilistic fashion.

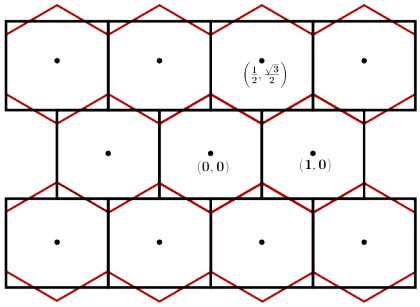

Fig. 2. Babai and Voronoi cells for the hexagonal lattice A_2

A. Error Probability

In this section we define and simplify the error probability, P_e and its complement, P_c, the success probability. This is needed for the second of the two problems described in Sec. II-B and for the analysis in Secs. IV and V. The error probability and its complement are defined by $P_e = 1 - P_c = \text{Prob}\left(\mathbf{X}_{nl} \neq \mathbf{X}_{np}\right)$. Clearly $P_c = \sum_{\mathbf{y}\in\Lambda} \text{Prob}\left(\mathbf{X}_{nl} = \mathbf{y}, \mathbf{X}_{np} = \mathbf{y}\right)$. We consider two probability models.

1) **Conditional Distribution Model**. Given that $\mathbf{X} \in \mathcal{B}(\mathbf{y})$, we assume the conditional distribution of $\mathbf{X} - \mathbf{y}$ is independent of $\mathbf{y}$ and that the components of $\mathbf{X}$ are conditionally independent. For this model the probability that the Babai and Voronoi points coincide is given by

$$\begin{aligned} P_c &= \sum_{\mathbf{y}\in\Lambda} \text{Prob}\left(\mathbf{X}_{nl} = \mathbf{y}, \mathbf{X}_{np} = \mathbf{y} | \mathbf{X}_{np} = \mathbf{y}\right) \text{Prob}\left(\mathbf{X}_{np} = \mathbf{y}\right) \\ &= \sum_{\mathbf{y}\in\Lambda} \text{Prob}\left(\mathbf{X} \in \mathcal{V}(\mathbf{y}) \bigcap \mathcal{B}(\mathbf{y}) | \mathbf{X} \in \mathcal{B}(\mathbf{y})\right) \text{Prob}\left(\mathbf{X} \in \mathcal{B}(\mathbf{y})\right) \\ &= \frac{\text{Prob}\left(\mathbf{X} \in \mathcal{V}(0) \bigcap \mathcal{B}(0)\right)}{\text{Prob}\left(\mathbf{X} \in \mathcal{B}(0)\right)}. \end{aligned} \tag{2}$$

A special case is when $\mathbf{X}$ is uniformly distributed over a Babai cell, which we refer to hereafter as the **Uniform Distribution Model**. Specialized to the uniform distribution this simplifies to

$$P_c = \frac{\text{vol}\left(\mathcal{V}(0) \bigcap \mathcal{B}(0)\right)}{\text{vol}\left(\mathcal{B}(0)\right)}. \tag{3}$$

2) **Gaussian Generative Model**: Here $\mathbf{X}$ is assumed to be obtained through the addition of noise to a transmitted signal vector, $\mathbf{X} = \mathbf{Y} + \mathbf{Z}$, where $\mathbf{Y} \in \Lambda$ is the transmitted lattice

vector, and $\mathbf{Z} \in \mathbb{R}^n$ is the white Gaussian noise, $\mathcal{N}(0, \sigma^2\mathbf{I})$. Here, P_c is the probability that a Babai decoder and a Voronoi decoder compute the same lattice point.

$$\begin{aligned}
P_c &= \sum_{\mathbf{y}\in\Lambda}\sum_{\mathbf{y}'\in\Lambda} \text{Prob}\left(\mathbf{X}_{nl} = \mathbf{y}', \mathbf{X}_{np} = \mathbf{y}', \mathbf{Y} = \mathbf{y}\right) \\
&\overset{(a)}{=} \sum_{\mathbf{y}\in\Lambda} \text{Prob}\left(\mathbf{Y} = \mathbf{y}\right) \sum_{\mathbf{y}'\in\Lambda} \text{Prob}\left(\mathbf{Z} \in \mathcal{B}(\mathbf{y}' - \mathbf{y}) \bigcap \mathcal{V}(\mathbf{y}' - \mathbf{y})\right) \\
&= \sum_{\mathbf{y}\in\Lambda} \text{Prob}\left(\mathbf{Y} = \mathbf{y}\right) \sum_{\mathbf{y}'\in\Lambda} \text{Prob}\left(\mathbf{Z} \in \mathcal{B}(\mathbf{y}') \bigcap \mathcal{V}(\mathbf{y}')\right) \\
&= \sum_{\mathbf{y}'\in\Lambda} \text{Prob}\left(\mathbf{Z} \in \mathcal{B}(\mathbf{y}') \bigcap \mathcal{V}(\mathbf{y}')\right) \\
&= \underbrace{\text{Prob}\left(\mathbf{Z} \in \mathcal{B}(0) \bigcap \mathcal{V}(0)\right)}_{T} + \sum_{\mathbf{y}'\in\Lambda, \mathbf{y}'\neq 0} \text{Prob}\left(\mathbf{Z} \in \mathcal{B}(\mathbf{y}') \bigcap \mathcal{V}(\mathbf{y}')\right), \qquad (4)
\end{aligned}$$

where in (a) we have asserted the independence of $\mathbf{Z}$ and $\mathbf{Y}$. The second term on the right hand side of the above equation is the probability that the Babai and Voronoi points coincide but are incorrect. For small noise variance, the dominant term in the above sum is $T = \text{Prob}\left(\mathbf{Z} \in \mathcal{V}(0) \bigcap \mathcal{B}(0)\right)$.

Note also that $P_c = 1$ when the basis vectors are mutually orthogonal.

As already noted, the Babai cell $\mathcal{B}(0)$ is dependent on the choice of the lattice basis, whereas the Voronoi cell is invariant to the choice of lattice basis. In particular, the Babai cell depends on the order in which the basis vectors are listed. Thus, in Sec. IV, where we evaluate the error probability for a given generator matrix V, we determine the Babai cell for all $n!$ column permutations of V by applying the QR decomposition to each permutation. The error probability is then the minimum that is obtained over all column permutations.

B. Problem Formulations

Let $\mathbf{X} \in \mathbb{R}^n$ be a random vector with a known probability distribution and let Λ be a lattice with a known generator matrix, V, which is upper triangular. X_i, the ith component of $\mathbf{X}$ is observed at the ith SN, $i = 1, 2, \ldots, n$. The objective is to compute the Babai point $\mathbf{X}_{nl}$ at the CN. Towards this end, the encoder in the ith SN maps X_i to the index j_i of a codeword in a codebook $\mathcal{C}_i$ of size 2^{R_i} and sends j_i to the CN using R_i bits. The CN computes the Babai point based on all the received codebook indices $(j_1, j_2, \ldots, j_n)$. Two problems are considered.

1) Determine the minimum communication cost $\sum_{i=1}^{n} R_i$ and an optimal protocol for computing the Babai point at the CN and study the dependence on the geometric structure of

the lattice. This requires that we construct the codebooks $\mathcal{C}_i$, describe the action of the encoder at each SN and the action of the decoder at the CN.

2) Determine the error probability P_e for various lattices under the Conditional Distribution and Gaussian Generative models and study its dependence on the packing and covering properties of the lattice.

III. The Distributed Babai Protocol (DBP) and its Communication Cost

We now describe the protocol DBP, by which the Babai point $\mathbf{x}_{np} = V\mathbf{u}$ can be determined exactly at the CN with a finite rate of transmission from SN to CN. We assume that

1) the lattice Λ has upper triangular generator matrix V, and
2) the ratio of any two non-zero entries in any row of V are rational numbers.

Define integers p_{ml}, $q_{ml} > 0$ and relatively prime to each other, by canceling out common factors in v_{ml} and v_{mm}, i.e. let $p_{ml}/q_{ml} = v_{ml}/v_{mm}$. Let $q_m = \text{lcm}\ \{q_{ml}, l > m\}$, where lcm denotes the least common multiple of its arguments. By definition let $q_m = 1$ if $m = n$ or $v_{ml} = 0$ for all $l > m$. The 'interference' term ν_m is given by $\nu_m = \sum_{l=m+1}^{n} u_l v_{ml}/v_{mm}$. In terms of integer and fractional parts, $\nu_m = \lfloor \nu_m \rfloor + \{\nu_m\}$, $0 \leq \{\nu_m\} < 1$ and further, $\{\nu_m\}$ is of the form s/q_m, $0 \leq s < q_m$. Let $\mathcal{S}_m \subset \{0, 1, \ldots, q_m - 1\}$ be the set of values taken by $\{\nu_m\}q_m$ with positive probability. For most source probability distributions $\mathcal{S}_m = \{0, 1, \ldots, q_m - 1\}$. However, in some cases, when q_m is large this may not be the case. One such situation is described at the end of Sec. III-D.

Action of the Encoder in the mth SN:

Define s_m to be the largest integer $s \in \mathcal{S}_m$ for which

$$[x_m/v_{mm} - s/q_m] = [x_m/v_{mm}]. \tag{5}$$

Then the mth SN sends

$$\tilde{u}_m = [x_m/v_{mm}] \tag{6}$$

and s_m to the CN in the order $m = n, n-1, \ldots, 2, 1$ (by definition $s(n) = 0$).

Action of the Decoder in the CN:

The decoder computes $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ where,

$$u_m = \begin{cases} \tilde{u}_m - \left\lfloor \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\rfloor, & f_m \leq s_m, \\ \tilde{u}_m - \left\lfloor \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\rfloor - 1, & f_m > s_m, \end{cases} \tag{7}$$

where $\tilde{u}_m$ is given by (6),

$$f_m = \left\{ \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\} q_m,$$

and computation proceeds in the order $m = n, n-1, \ldots, 1$.

Theorem 1. *(Decoder output is the Babai point) The output of the decoder coincides with the solution* $\mathbf{u}$ *given in* (1).

Proof. Rewrite (1) in terms of fractional and integer parts to get

$$u_m = \left[\frac{x_m}{v_{mm}} - \left\{ \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\} \right] - \left\lfloor \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\rfloor, \quad m = n, n-1, \ldots, 1. \tag{8}$$

The fractional part in the above equation is of the form s/q_m, $s \in \mathbb{Z}$ and further, $0 \le s < q_m$. Thus

$$u_m = \begin{cases} \tilde{u}_m - \left\lfloor \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\rfloor, & s \le s_m, \\ \tilde{u}_m - \left\lfloor \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\rfloor - 1, & s > s_m, \end{cases} \tag{9}$$

where $\tilde{u}_m$ is given by (6), and the computation of u_m is performed at the CN in the order $m = n, n-1, \ldots, 1$. □

A. Communication Cost of Protocol DBP

Theorem 2. *(Sum rate of the protocol DBP) Assume that* X_i, $i = 1, 2, \ldots, n$ *are mutually independent and identically distributed with known marginal probability distribution. The sum rate* R_{sum} *of protocol DBP is*

$$R_{sum} = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} H(\tilde{U}_i, S_i). \tag{10}$$

As an example, suppose that $\mathbf{X}$ is uniformly distributed over a rectangular region $[-A/2, A/2]^n$. The total rate satisfies

$$\left| R_{sum} - \left(n \log_2(A) - \log_2 |\det V| + \sum_{i=1}^{n-1} H(S_i|\tilde{U}_i) \right) \right| \le \frac{2}{A} \sum_{i=1}^{n} |v_{ii}|.$$

Further, since $\lim_{A\to\infty} H(S_i|\tilde{U}_i) = \log_2 q_i$ for $i = 1, 2, \ldots, n$ it follows that

$$\lim_{A\to\infty} (R_{sum} - n \log_2 A) = \log_2 |\det V| + \sum_{i=1}^{n-1} \log_2 q_i. \tag{11}$$

The term $n \log_2 A - \log_2 |\det V|$ can be interpreted as the rate required to compute the Babai point for a lattice $\Lambda' \subset \mathbb{R}^n$ generated by orthogonal vectors $\{v_{11}\mathbf{e}_1, \ldots, v_{nn}\mathbf{e}_n\}$, where v_{ii} is the ith element on the main diagonal of the upper triangular generator matrix V of the lattice Λ and $\mathbf{e}_i$ is the ith basis vector in the standard basis, i.e. the vector with 1 in the ith position and 0's elsewhere. Observe that the Babai cells of Λ are congruent to those of Λ', but are not aligned as they are in Λ'. The term $\sum_{i=1}^{n-1} \log_2 q_i$ in (11) is the additional communication cost because of the misalignment of the Babai cells of Λ.

B. Communication Cost for Some Other Communication Models

In order to benchmark the communication cost of protocol DBP, we consider two other communication models. The first is a simple model, in which all the SNs are co-located but are separate from the CN. The second is a matched model, which allows one-time, one-way communication from the ith SN to the lth SN with lower index, $l < m$, $m = 2, 3, \ldots, n$ (this model is a natural choice because it is matched to the triangular structure of the lattice generator). We assume a noiseless broadcast model so that a single transmission by an SN can be seen by all the other SNs and the CN.

For the co-located model, u_i is computed using (1) and $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ is sent to the CN. The CN is thus able to recover $\mathbf{x}_{np}$. For the matched model, the i-th SN computes u_i as in the centralized model, and broadcasts u_i to lower indexed SN j and to the CN.

Under the same assumptions on the probability distribution of $\mathbf{X}$ as in Theorem 2, the sum rate is $H(U_1, U_2, \ldots, U_n) = \sum_{k=1}^{n} H(U_k | U_l, l > k)$ for both models. For the case where $\mathbf{X}$ is uniformly distributed over $[-A/2, A/2]^n$, the sum rate for both models satisfies $\lim_{A\to\infty} R_{sum} - n \log_2 A = \log_2 |\det V|$. Thus the excess communication cost for the centralized model, which is the model that we study in this paper, as illustrated in Fig. 1, is $\sum_{i=1}^{n} \log_2 q_i$.

C. Optimality of Protocol DBP

We prove optimality of the protocol DBP based on a bound on the sum rate for the distributed function computation problem from [26]. In order to make the derivation self-contained, we first summarize the salient facts about characteristic graphs and graph entropy which play a fundamental role in the bound derived in [26] before proceeding to derive a lower bound for protocol DBP. Note that our bound is for continuous alphabets, and is based on a limiting form

of the result stated in [26], for discrete alphabets. The limiting argument is self-evident and is not presented.

Consider a function $f(x_1, x_2, \ldots, x_n) \ : \ \mathbb{R}^n \to \mathbb{Z}^n$, and our distributed computation setup where x_i is available at the ith SN and f is to be computed at the CN. A lower bound on the communication rate from the ith SN to the CN is given by the minimum rate required to compute f, assuming that $x_j, \ j \neq i$ is known at the receiver. We will use the notation $i^c = \{1 \leq j \leq n, \ j \neq i\}$ and $\mathbf{x}_{i^c}$ for the vector $(x_j, \ j \neq i)$. From [26], the minimum communication rate is given in terms of the conditional graph entropy of a specific graph. We now describe computation of the conditional graph entropy. For convenience we will write $f(\mathbf{x}) = f(x_i|\mathbf{x}_{i^c})$, when studying the communication rate from the ith SN to the CN, to emphasize the fact that $\mathbf{x}_{i^c}$ is side information at the CN.

The characteristic graph, $\mathcal{G}_i$, of the function $f(x_i|\mathbf{x}_{i^c})$, has as its nodes the support of x_i, which in this case is $\mathbb{R}$. Two distinct nodes x_i and x_i' are connected by an edge if and only if (iff) there is an $\mathbf{x}_{i^c}$ for which $f(x_i|\mathbf{x}_{i^c}) \neq f(x_i'|\mathbf{x}_{i^c})$. An independent set is a collection of nodes, no two of which are connected by an edge. A maximal independent set is an independent set which is not contained in any other independent set. The minimum rate required to compute $f_i(x_i|\mathbf{x}_{i^c})$ with $\mathbf{x}_{i^c}$ known at the CN is given by the conditional graph entropy $H_{\mathcal{G}_i}(X_i|\mathbf{X}_{i^c})$ [26], described next. Let Γ_i be the collection of maximal independent sets of $\mathcal{G}_i$ and let W be a random variable which takes the values $w \in \Gamma_i$—thus the realizations of W are maximally independent sets. Let $p(w|x_i, \mathbf{x}_{i^c})$ be a conditional probability distribution with the following properties:

1) $p(w|x_i, \mathbf{x}_{i^c}) = p(w|x_i)$, for all $w \in \Gamma_i$,$(x_i, \mathbf{x}_{i^c}) \in \mathbb{R}^n$ (Markov condition).
2) $p(w|x_i) = 0$ if $x_i \notin w$.
3) $\sum_{w \in \Gamma_i} p(w|x_i) = 1$.

Let $\mathcal{P}_i$ be the collection of all such probability distributions. Then by definition

$$H_{\mathcal{G}_i}(X_i|\mathbf{X}_{i^c}) = \inf_{p \in \mathcal{P}_i} I(W; X_i|\mathbf{X}_{i^c}). \tag{12}$$

We now apply this machinery for obtaining a lower bound on the rate R_i for computing

$$\mathbf{u}(x_i|\mathbf{x}_{i^c}) = \left\lceil \frac{x_i - \sum_{j=i+1}^{n} v_{i,j} u_j}{v_{i,i}} \right\rceil,$$

for $i = n, n-1, \ldots, 1$. Our goal is to determine $\mathcal{G}_i$ and its maximal independent sets, $i = 1, 2, \ldots, n$, and the probability distribution that solves (12).

First consider $\mathcal{G}_n$. In $\mathcal{G}_n$, x_n is *disconnected* from x'_n iff $[x_n/v_{n,n}] = [x'_n/v_{n,n}]$ or equivalently the maximal independent sets are the level sets of $[x_n/v_{n,n}]$. Since x_n lies in exactly one of these sets, it follows from item 2 and (6) that $W = \tilde{U}_n$. Hence $R_n \geq \inf_{p\in\mathcal{P}_n} I(W; X_n|\mathbf{X}_{n^c}) = H(\tilde{U}_n|\mathbf{X}_{n^c})$, since $H(\tilde{U}_n|X_n) = 0$.

Now consider $\mathcal{G}_m$ for $m < n$. As before, let $\nu = \sum_{j=m+1}^{n} v_{m,j}u_j/v_{m,m}$ and write $\nu = \{\nu\}+\lfloor\nu\rfloor$. Since $\{\nu\} = s/q_m$, $s \in \mathcal{S} \subset \{0, 1, \ldots, q_m - 1\}$ it follows that x_m and x'_m are disconnected in $\mathcal{G}_m$ iff $[x_m/v_{m,m} - s/q_m] = [x'_m/v_{m,m} - s/q_m]$ for all $s \in \mathcal{S} \subset \{0, 1, \ldots, q_m - 1\}$ or equivalently, $[x_m/v_{m,m}] = [x'_m/v_{m,m}]$ and the value of s_m evaluated using (5) is the same for x_m and x'_m. From item 2 and (6), it follows that $W = (\tilde{U}_m, S_m)$ and hence $R_m \geq \inf_{p\in\mathcal{P}_m} I(W; X_m|\mathbf{X}_{m^c}) = H(\tilde{U}_m, S_m|\mathbf{X}_{m^c})$.

Thus (recall that $S_n = 0$)

$$R_{sum} = \sum_{i=1}^{n} R_i \geq \sum_{i=1}^{n} H(\tilde{U}_i, S_i|\mathbf{X}_{i^c}). \tag{13}$$

Since the lower bound coincides with the sum rate of the protocol DBP given by (10) when the X_i are mutually independent, DBP is optimal.

D. Examples

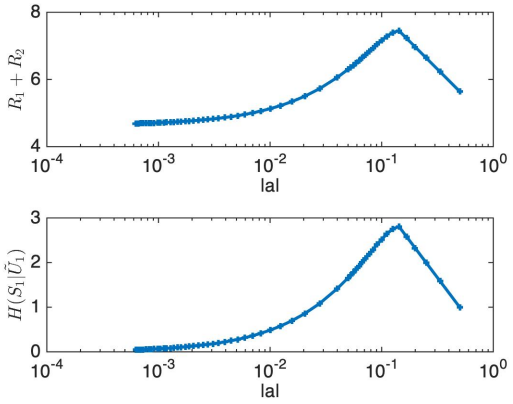

Fig. 3. Communication rates for 2 dimensional lattices and a uniform source distribution over the square $[-5/2, 5/2) \times [-5/2, 5/2)$. The basis vectors are $(1, 0)$ and $(a, b) = (1/m, \sqrt{1 - 1/m^2})$, with integer $m \geq 2$.

In the following examples, we illustrate how the method proposed in Theorem 1 works, present a case where the communication cost is large, and compute communication rates for a family of two-dimensional lattices, for a uniformly distributed source.

Example 2. *Consider the three dimensional body-centered cubic (BCC) lattice with basis* $\{(1,0,0), (-\frac{1}{3}, \frac{2\sqrt{2}}{3}, 0), (-\frac{1}{3}, -\frac{\sqrt{2}}{3}, \sqrt{\frac{2}{3}})\}$. *The Babai point* $\mathbf{u} = (u_1, u_2, u_3)$ *is given by*

$$u_3 = \left\lceil \sqrt{\frac{3}{2}} x_3 \right\rceil, \quad u_2 = \left\lceil \frac{3}{2\sqrt{2}} x_2 + \left\{ \frac{1}{2} u_3 \right\} \right\rceil + \left\lfloor \frac{1}{2} u_3 \right\rfloor,$$

$$\textit{and} \quad u_1 = \left\lceil x_1 + \left\{ \frac{1}{3} u_2 + \frac{1}{3} u_3 \right\} \right\rceil + \left\lfloor \frac{1}{3} u_2 + \frac{1}{3} u_3 \right\rfloor.$$

In order for the Babai point $\mathbf{u}$ *to be correctly calculated at the CN, nodes* 2 *and* 1 *send the following extra information, according to the protocol DBP:*

$$\textit{node 2:} \ \left\{ \frac{1}{2} u_3 \right\} = \frac{s_2}{q_2}, \ q_2 = 2 \ \textit{then} \ s_2 = 0 \ \textit{or} \ 1$$

$$\textit{node 1:} \ \left\{ \frac{1}{3} u_2 + \frac{1}{3} u_3 \right\} = \frac{s_1}{q_1}, \ q_1 = 3 \ \textit{then} \ s_1 = 0, 1 \ \textit{or} \ 2.$$

Observe that the values of s_1 *and* s_2 *are calculated for a general received vector* $\mathbf{x} = (x_1, x_2)$. *Therefore, the sum rate to send* s_1 *and* s_2 *to the CN is* $\log_2 2 + \log_2 3 \approx 2.5859 \approx 3$ *bits*.

Example 3. *Consider a two-dimensional lattice with basis* $\{(1,0), (\frac{311}{1000}, \frac{101}{100})\}$. *We have that*

$$u_2 = \left\lceil \frac{x_2}{v_{22}} \right\rceil = \left\lceil \frac{100}{101} x_2 \right\rceil \tag{14}$$

and

$$u_1 = \left\lceil \frac{x_1}{v_{11}} - \left\{ \frac{u_2 v_{21}}{v_{11}} \right\} \right\rceil - \left\lfloor \frac{u_2 v_{21}}{v_{11}} \right\rfloor = \left\lceil x_1 - \left\{ \left\lceil \frac{100}{101} x_2 \right\rceil \frac{311}{1000} \right\} \right\rceil - \left\lfloor \left\lceil \frac{100}{101} x_2 \right\rceil \frac{311}{1000} \right\rfloor.$$

Consider, for example, $\mathbf{x} = (1,1)$, *then* $\left\{ \left\lceil \frac{100}{101} x_2 \right\rceil \frac{311}{1000} \right\} = \frac{311}{1000} = \frac{s}{q}$. *In this case, node* 1 *must send the largest integer* s_1 *in the range* $\{0, 1, \ldots, 999\}$ *for which* $\left\lceil x_1 - \frac{s_1}{q_1} \right\rceil = \lceil x_1 \rceil$ *and we get* $s_1 = 500$. *This procedure will cost no larger than* $\log_2 q_1 = \log_2 1000 \approx 9.96$ *and in the worst case, we need to send almost* 10 *bits to recover the Babai point at the CN.*

Communication rates for various two-dimensional lattices are presented in Fig. 3 for a source uniformly distributed over the square $[-5/2, 5/2) \times [-5/2, 5/2)$. The basis vectors are $(1,0)$ and (a,b), $a^2 + b^2 = 1$, with $a = 1/m$, and integer $m \geq 2$. The sum rate is seen to peak at $a = 1/6$. Consider the case where $m = 991$. Note that $u_2 = \lceil x_2/b \rceil$ and $u_1 = \lceil x_1 - a u_2 \rceil$. The scaled fractional interference term $m\{a u_2\}$ takes values in $\mathcal{S} = \{0, 1, 2, 3, 988, 989, 990\}$ which is a much smaller set than $\{0, 1, \ldots, 990\}$. This observation is essential for ensuring that the conditional entropy $H(S_1 | \tilde{U}_1)$ eventually decreases as $a \to 0$.

IV. Error Probability Calculations for Dimensions $n = 2,\ 3$:

We have presented a protocol for computing the Babai point in a distributed network and evaluated its communication cost. We now explore several issues related to the Babai point.

First, since the Babai point is an approximation for the nearest lattice point, it is of interest to evaluate the probability that the two points are unequal, i.e., the error probability P_e as defined in Sec. II-A. In this section we provide a precise analysis of P_e for the Conditional Distribution model, specifically the Uniform Distribution model, for dimensions 2 and 3. Since the probability that the Babai and nearest lattice point coincides is basis dependent, we will work in this section with Minkowski-reduced basis for all lattices.

A less precise but more general analysis of P_e for general dimensions, and under both the Conditional Distribution and Gaussian Generative model, is considered in Sec. V. Efficient numerical computation of P_e requires that we work with special bases as defined in Sec. IV-A. Analytic and numerical computation of P_e for $n = 2, 3$ is then addressed in Secs. IV-B and IV-C. Knowledge of the error probability is useful because in some situations it might be sufficient to compute the Babai point, and not incur the extra communication cost of finding the nearest lattice point. We mention here that the additional cost of finding the true nearest lattice point has been addressed in dimension two in [32].

Second, we study the variation of the error probability P_e with the packing density of the lattice. The intuition driving this study is that as the packing density increases, the Voronoi cell become increasingly spherical, and we should expect the error probability to increase. We see that some well-known regular polyhedra lie on the optimal tradeoff curve between the packing density and the error probability. Numerical evidence about the nature of polyhedra that lie on this optimal tradeoff curve is also presented (Figs. 7 and 8).

A. Special Bases: Minkowski and Obtuse Superbase

A basis $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n\}$ of a lattice $\Lambda \subset \mathbb{R}^n$ is said to be *Minkowski-reduced* if $\mathbf{v}_j$, $j = 1, \ldots, n$, is such that $\|\mathbf{v}_j\| \leq \|\mathbf{v}\|$, for any $\mathbf{v}$ such that $\{\mathbf{v}_1, ..., \mathbf{v}_{j-1}, \mathbf{v}\}$ can be extended to a basis of Λ.

Theorem 3. *[7] (Minkowski-reduced basis from Gram matrix) Consider the Gram matrix A of a lattice Λ. The inequalities (15), (15)–(16), and (15)–(17) below define a Minkowski-reduced*

basis for dimensions 1,2 and 3, respectively.

$$0 < a_{11} \leq a_{22} \leq a_{33} \tag{15}$$

$$2|a_{st}| \leq a_{ss} \quad (s < t) \tag{16}$$

$$2|a_{rs} \pm a_{rt} \pm a_{st}| \leq a_{rr} + a_{ss} \quad (r < s < t). \tag{17}$$

All lattices in $\mathbb{R}^n$ have a Minkowski-reduced basis, which roughly speaking, consists of short vectors that are as perpendicular as possible [7]. In dimension two, relevant vectors can be determined from a Minkowski-reduced basis as follows.

Lemma 1. *[8] (Relevant vectors given a Minkowski-reduced basis) Consider a Minkowski-reduced basis of the form* $\{(1,0),(a,b)\}$ *and let* θ *be the angle between* $(1,0)$ *and* (a,b)*. Then besides the basis vectors, a third relevant vector is*

$$\begin{cases} (-1+a,b), & \text{if } \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2} \\ (1+a,b), & \text{if } \frac{\pi}{2} < \theta \leq \frac{2\pi}{3}. \end{cases} \tag{18}$$

In dimension two, the characterization [7] for a Minkowski-reduced basis is the following: a lattice basis $\{\mathbf{v}_1, \mathbf{v}_2\}$ is Minkowski-reduced if only if $\|\mathbf{v}_1\| \leq \|\mathbf{v}_2\|$ and $2|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \|\mathbf{v}_1\|^2$. Consequently, the angle θ between $\mathbf{v}_1$ and $\mathbf{v}_2$ is such that $\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$.

We describe next the concept of an obtuse superbase that will be applied in the three-dimensional approach.

Let $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be a basis for a lattice $\Lambda \subset \mathbb{R}^n$. A *superbase* $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n\}$ with $\mathbf{v}_0 = -\sum_{i=1}^n \mathbf{v}_i$, is said to be *obtuse* if $p_{ij} = \mathbf{v}_i \cdot \mathbf{v}_j \leq 0$, for $i, j = 0, \ldots, n, \quad i \neq j$. A lattice Λ is said to be of *V*oronoi's first kind if it has an *obtuse superbase*. The existence of an obtuse superbase allows a characterization of the relevant Voronoi vectors of a lattice [8, Theorem 3, Sec. 2], which are of the form $\sum_{i \in S} \mathbf{v}_i$, where $S \subset \{0, 1, \ldots, n\}$ and $S \neq \varnothing$.

It was demonstrated [8] that all lattices with dimension less or equal than three are of Voronoi's first kind and given the existence of obtuse superbases for three dimensional lattices, their Voronoi regions can be classified into five possible parallelohedra which we present in the sequel.

Given an obtuse superbase, since $\mathbf{v}_0 = -\mathbf{v}_1 - \mathbf{v}_2 - \mathbf{v}_3$, all relevant Voronoi vectors can be written as one of the following seven vectors or their negatives:

$$\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_{12} = \mathbf{v}_1 + \mathbf{v}_2, \mathbf{v}_{13} = \mathbf{v}_1 + \mathbf{v}_3, \mathbf{v}_{23} = \mathbf{v}_2 + \mathbf{v}_3, \mathbf{v}_{123} = \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3.$$

The Euclidean norm of such vectors $N(\mathbf{v}_1), N(\mathbf{v}_2), N(\mathbf{v}_3), N(\mathbf{v}_{12}), N(\mathbf{v}_{13}),\ N(\mathbf{v}_{23}), N(\mathbf{v}_{123})$ are called *vonorms* and $p_{ij} = -\mathbf{v}_i \cdot \mathbf{v}_j\ (0 \leq i < j \leq 3)$ are denoted as *conorms*.

Remark 1. *The Voronoi region of a lattice $\Lambda \subset \mathbb{R}^n$ with obtuse superbase $\{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ can be classified [8] according to the five choices of zeros for their conorms, which leads to five possible parallelohedra, as presented in Fig. 4. The characterization is based on the conorms as follows:*

- *cuboid, if $p_{12} = p_{13} = p_{23} = 0$.*
- *hexagonal prism, if only two conorms among p_{12}, p_{13} and p_{23} are zero.*
- *rhombic dodecahedron, if $p_{01} = p_{23} = 0$, or $p_{02} = p_{13} = 0$, or $p_{03} = p_{12} = 0$.*
- *hexa-rhombic dodecahedron, if only one conorm among p_{12}, p_{13} or p_{23} is zero, and p_{0j} are nonzero for all $j = 1, 2, 3$.*
- *truncated octahedron, if all $p_{ij}\ (0 \leq i < j \leq 3)$ are nonzero.*

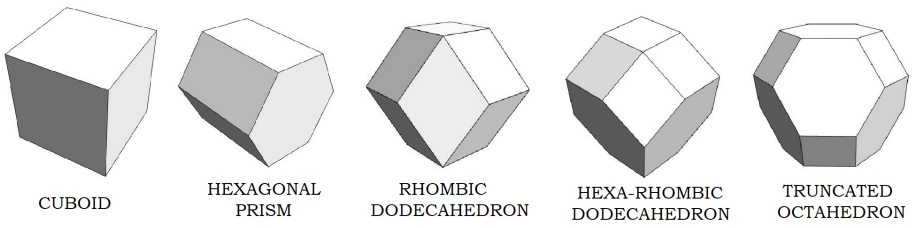

Fig. 4. The five possible shapes for a Voronoi cell of a three-dimensional lattice

Now that the Minkowski-reduced basis and obtuse superbase have been defined, we present a relation between them.

Theorem 4. *(Minkowski-reduced basis and obtuse superbase) In dimensions $n = 1, 2, 3$, if a lattice $\Lambda \subset \mathbb{R}^n$ has a Minkowski-reduced basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, where $\mathbf{v}_i.\mathbf{v}_j \leq 0$, $i \neq j$, then the superbase $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is an obtuse superbase for Λ. Conversely, if Λ has an obtuse superbase, then a Minkowski-reduced basis can be constructed from it.*

Proof. The case $n = 1$ is trivial, hence we will start with $n = 2$.
($\Rightarrow$) Suppose that $\{\mathbf{v}_1, \mathbf{v}_2\}$ is a Minkowski-reduced basis, then, according to Theorem 3, $0 < \mathbf{v}_1 \cdot \mathbf{v}_1 \leq \mathbf{v}_2 \cdot \mathbf{v}_2$ and $2|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \mathbf{v}_1 \cdot \mathbf{v}_1$. Moreover, by hypothesis, $\mathbf{v}_1 \cdot \mathbf{v}_2 \leq 0$. Define $\mathbf{v}_0 = -\mathbf{v}_1 - \mathbf{v}_2$ and to guarantee that $\{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2\}$ is an obtuse superbase, we need to check that $p_{01} \leq 0$ and

$p_{02} \leq 0$. Indeed, $p_{01} = \mathbf{v}_0 \cdot \mathbf{v}_1 = (-\mathbf{v}_1 - \mathbf{v}_2) \cdot \mathbf{v}_1 = -\mathbf{v}_1 \cdot \mathbf{v}_1 \underbrace{-\mathbf{v}_1 \cdot \mathbf{v}_2}_{|\mathbf{v}_1 \cdot \mathbf{v}_2|} \leq -2|\mathbf{v}_1 \cdot \mathbf{v}_2| + |\mathbf{v}_1 \cdot \mathbf{v}_2| \leq 0$. Similarly we have that $p_{02} \leq 0$.

($\Leftarrow$) If $\{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2\}$ is an obtuse superbase, any permutation of it is also an obtuse superbase. So, we may consider one such that $|\mathbf{v}_1| \leq |\mathbf{v}_2| \leq |\mathbf{v}_0|$. Then we have that $0 < \mathbf{v}_1 \cdot \mathbf{v}_1 \leq \mathbf{v}_2 \cdot \mathbf{v}_2 \leq (\mathbf{v}_1 + \mathbf{v}_2) \cdot (\mathbf{v}_1 + \mathbf{v}_2)$ and $\mathbf{v}_1 \neq 0$. From the last inequality, we have that $-2\mathbf{v}_1 \cdot \mathbf{v}_2 \leq \mathbf{v}_1 \cdot \mathbf{v}_1 \Rightarrow 2|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \mathbf{v}_1 \cdot \mathbf{v}_1$.

For n=3: ($\Rightarrow$) Consider a Minkowski-reduced basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ such that $\mathbf{v}_1 \cdot \mathbf{v}_2 \leq 0, \mathbf{v}_1 \cdot \mathbf{v}_3 \leq 0$ and $\mathbf{v}_2 \cdot \mathbf{v}_3 \leq 0$. To check if $\{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ is an obtuse superbase, we need to verify that $p_{01} \leq 0, p_{02} \leq 0$ and $p_{03} \leq 0$. One can observe that

$$p_{01} = \mathbf{v}_0 \cdot \mathbf{v}_1 = -\mathbf{v}_1 \cdot \mathbf{v}_1 \underbrace{-\mathbf{v}_1 \cdot \mathbf{v}_2}_{|\mathbf{v}_1 \cdot \mathbf{v}_2|} \underbrace{-\mathbf{v}_1 \cdot \mathbf{v}_3}_{|\mathbf{v}_1 \cdot \mathbf{v}_3|} \leq -\mathbf{v}_1 \cdot \mathbf{v}_1 + \frac{\mathbf{v}_1 \cdot \mathbf{v}_1}{2} + \frac{\mathbf{v}_1 \cdot \mathbf{v}_1}{2} \leq 0.$$

With analogous arguments, we show that $p_{02} \leq 0$ and $p_{03} \leq 0$.

($\Leftarrow$) To prove the converse, up to a permutation, we may consider an obtuse superbase such that $|\mathbf{v}_1| \leq |\mathbf{v}_2| \leq |\mathbf{v}_3| \leq |\mathbf{v}_0|$. This basis will be Minkowski-reduced if we prove conditions (16) and (17) from Th. 3, i.e.,

$$2|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \mathbf{v}_1 \cdot \mathbf{v}_1; \quad 2|\mathbf{v}_1 \cdot \mathbf{v}_3| \leq \mathbf{v}_1 \cdot \mathbf{v}_1; \quad 2|\mathbf{v}_2 \cdot \mathbf{v}_3| \leq \mathbf{v}_2 \cdot \mathbf{v}_2, \tag{19}$$

$$2|\pm(\mathbf{v}_1 \cdot \mathbf{v}_2) \pm (\mathbf{v}_1 \cdot \mathbf{v}_3) \pm (\mathbf{v}_2 \cdot \mathbf{v}_3)| \leq (\mathbf{v}_1 \cdot \mathbf{v}_1) + (\mathbf{v}_2 \cdot \mathbf{v}_2). \tag{20}$$

The inequalities in (19) are shown similarly to the two dimensional case starting from $\mathbf{v}_2 \cdot \mathbf{v}_2 \leq (\mathbf{v}_1 + \mathbf{v}_2) \cdot (\mathbf{v}_1 + \mathbf{v}_2)$, $\mathbf{v}_3 \cdot \mathbf{v}_3 \leq (\mathbf{v}_1 + \mathbf{v}_3) \cdot (\mathbf{v}_1 + \mathbf{v}_3)$ and $\mathbf{v}_3 \cdot \mathbf{v}_3 \leq (\mathbf{v}_2 + \mathbf{v}_3) \cdot (\mathbf{v}_2 + \mathbf{v}_3)$. Starting from $\mathbf{v}_3 \cdot \mathbf{v}_3 \leq (\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3) \cdot (\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3)$, the inequality in (20) follows, concluding the proof. □

Characteristics of relevant Voronoi vectors of low-dimensional lattices can be found in [22]. For our application, the obtuse superbase ([8, Th.3, Sec. 2]) leads to considerable simplification in identifying all the relevant vectors for a Voronoi cell. For more details about low dimensional reduced bases, see [25]. Computation of a Minkowski-reduced basis in high dimensions is a hard problem and the basis commonly used in practice is an approximation, obtained using the the LLL algorithm [21].

B. Error Probability and Packing Density: Two-dimensional lattices, Uniform Distribution Model

We consider that a Minkowski-reduced lattice basis, which is also obtuse (Theorem 4) can be chosen by the designer of the lattice code and it can be transformed into an equivalent basis $\{(1,0),(a,b)\}$, by applying QR decomposition to the lattice generator matrix.

From the Minkowski-reduced basis $\{(1,0),(a,b)\}$, where $a^2+b^2 \geq 1$ and $-\frac{1}{2} \leq a \leq 0$, it is possible to use Lemma 1 to describe the Voronoi region of Λ and determine its intersection with the associated Babai cell. Observe that the area of both regions must be the same and in this specific case, equal to $|b|$.

In addition $\{(-1-a,-b),(1,0),(a,b)\}$ is an obtuse superbase for Λ, so the relevant vectors that define the Voronoi region are $\pm(1,0), \pm(a,b)$ and $\pm(-1-a,-b)$. We will choose for the analysis proposed in Theorem 5 only the vectors in the first quadrant, i.e., $(1,0),(1+a,b),(a,b)$, due to the symmetry of the Voronoi cell. Hence, the following result states a closed formula for the error probability $P_e := \text{Prob}\left(\mathbf{X}_{np} \neq \mathbf{X}_{nl}\right)$ of any two-dimensional lattice.

Theorem 5. *[4] (Error probability for two-dimensional lattices) Consider a lattice $\Lambda \subset \mathbb{R}^2$ with a Minkowski-reduced basis $\{\mathbf{v_1},\mathbf{v_2}\} = \{(1,0),(a,b)\}$, such that the angle θ between $\mathbf{v_1}$ and $\mathbf{v_2}$ satisfies $\frac{\pi}{2} \leq \theta \leq \frac{2\pi}{3}$. The error probability P_e, when the received vector $\mathbf{x} = (x_1,x_2) \in \mathbb{R}^2$ is uniformly distributed over the Babai cell, is*

$$P_e = F(a,b) = \frac{-a-a^2}{4b^2} = \frac{1-(1+2a)^2}{16b^2}. \tag{21}$$

Proof. To calculate P_e for Λ, we first obtain the vertices of the Voronoi region. This is done by calculating the points of the intersection of the perpendicular bisectors of the three relevant vectors $(1,0),(a,b)$ and $(1+a,b)$, according to Lemma 1, Fig. 5. The vertices that define the Voronoi region are $\pm(\frac{1}{2},\frac{a^2+b^2+a}{2b})$, $\pm(-\frac{1}{2},\frac{a^2+b^2+a}{2b})$ and $\pm(\frac{2a+1}{2},\frac{-a^2+b^2-a}{2})$, while the Babai cell $\mathcal{B}(0)$ has vertices $(\pm\frac{1}{2},\pm\frac{b}{2})$.

P_e is then computed as the ratio between the area of the Babai region which is not overlapped by the Voronoi region $\mathcal{V}(0)$ and the area $|b|$ of the Babai region. From Fig. 5, the error can be written as the sum of the areas of four triangles. Two of them are defined respectively by the points $\left(\frac{1}{2},\frac{b}{2}\right), \left(\frac{1}{2},\frac{a^2+a+b^2}{2b}\right), \left(\frac{a+1}{2},\frac{b}{2}\right)$ and $\left(-\frac{1}{2},\frac{b}{2}\right), \left(-\frac{1}{2},\frac{a^2+a+b^2}{2b}\right), \left(\frac{a}{2},\frac{b}{2}\right)$, while the remaining two are symmetric to these ones. Therefore, the error probability is the sum of the four areas, normalized by the area of the Voronoi region $|\det(V)| = |b|$. The explicit formula for it is given by $F(a,b) = \dfrac{-a-a^2}{4b^2}$.

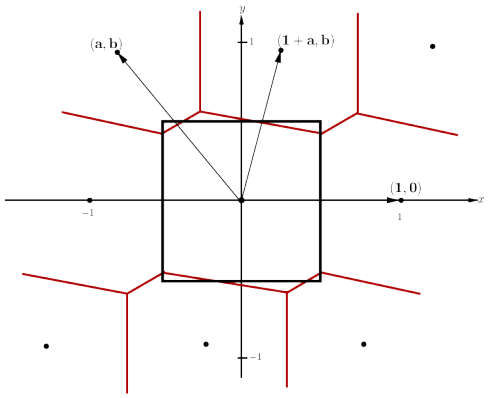

Fig. 5. Voronoi cell, Babai cell and three relevant vectors

□

Corollary 1. *(Error probability analysis for two dimensional lattices) For any two dimensional lattice with a Minkowski-reduced basis satisfying the conditions of Theorem 5, we have*

$$0 \leq P_e \leq \frac{1}{12}, \tag{22}$$

and

i) $P_e = 0 \iff a = 0$, *i.e., the lattice is orthogonal.*

ii) $P_e = \frac{1}{12} \iff (a,b) = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, *i.e., the lattice is equivalent to the hexagonal lattice.*

iii) *the level curves of* P_e *are described as ellipsoidal arcs (Fig. 6) in the region* $a^2 + b^2 \geq 1$ *and* $-\frac{1}{2} \leq a \leq 0$ *(condition required for the basis to be Minkowski-reduced).*

Remark 2. *From Corollary 1, one can notice a straightforward relation between the packing density of the lattice and its error probability. The packing density of a lattice with basis* $\{(1,0),(a,b)\}$ *is given by* $\Delta_2(a,b) = \frac{\pi}{4b}$ *and* $F(a,\Delta_2) = \frac{\Delta_2^2[1-(1+2a)^2]}{\pi^2}$, *following the notation from Theorem 5. For a fixed* a, *the error probability increases with* Δ_2, *and for a fixed density* Δ_2 *and fixed* b, *the error probability is decreasing with* a, *where* $-\frac{1}{2} \leq a \leq \min\left\{-\sqrt{1-\left(\frac{\pi}{4\Delta_2}\right)^2}, 0\right\}$.

Indeed, if we consider the error probability for a given density Δ_2, *we have that* $F(a,\Delta_2)$ *is minimized by* $a = a^*$, *where*

$$a^* = \begin{cases} 0, & \Delta_2 \leq \frac{\pi}{4} \quad (b^2 \geq 1) \\ -\sqrt{1-\left(\frac{\pi}{4\Delta_2}\right)^2}, & \frac{\pi}{4} < \Delta_2 \leq \frac{\pi}{2\sqrt{3}} \quad (3/4 \leq b^2 < 1). \end{cases}$$

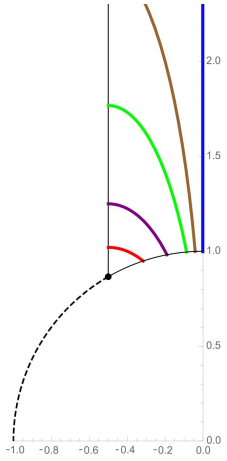

Fig. 6. Level curves of $P_e = k$, in right-left ordering, for $k = 0, k = 0.01, k = 0.02, k = 0.04, k = 0.06$ and $k = 1/12 \approx 0.0833$. Notice that a is represented in the horizontal axis and b in vertical axis.

and maximized by $a = -\frac{1}{2}$*, for any* Δ_2*. Fig. 7 represents the minimum error probability function* $F(a, \Delta_2)$ *for* $\frac{\pi}{4} \leq \Delta_2 \leq \frac{\pi}{2\sqrt{3}}$ *and expresses how the error probability varies with the packing density* Δ_2*.*

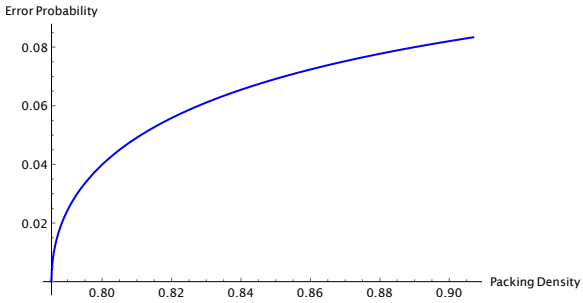

Fig. 7. Minimum error probability for given packing density assuming $\frac{\pi}{4} < \Delta_2 \leq \frac{\pi}{2\sqrt{3}}$, considering a uniform distribution

C. Error Probability and Packing Density: Three-dimensional lattices, Uniform Distribution Model

For the three dimensional case, we developed and implemented an algorithm in the software *Wolfram Mathematica, version* 12.1 [33] which calculates the error probability of any three dimensional lattice, given an obtuse superbase, by following the characterization given in [8].

We assume an initial upper triangular lattice basis given by $\{(1,0,0),(a,b,0),(c,d,e)\}$, where $a,b,c,d,e \in \mathbb{R}$.

It is important to remark that in dimensions greater than two, the error probability is dependent on the basis ordering. Hence, in order to analyze the smallest error probability for a given lattice, we relax the ordering imposed for the Minkowski-reduced basis and allow any permutation of a basis from now on. Our algorithm searches over all orderings and determines the best one. As an example, the performance of the BCC lattice is invariant over basis ordering, due to its symmetries. On the other hand, for the FCC lattice, depending on how the basis is ordered, we can find two different error probabilities, 0.1505 and 0.1667, but we choose to tabulate the smallest one. A detailed description of the algorithm is presented in Algorithm 1.

Algorithm 1 Error probability and packing density computation, $n = 3$, for basis $\{(1,0,0),(a,b,0),(c,d,e)\}$.

Voronoi cell: Given an obtuse superbase, determine the vertices of the Voronoi cell $\mathcal{V}(0)$ of Λ using the relevant Voronoi vectors (Sec. IV-A). Use *ConvexHullMesh[]* available in Mathematica [33] to obtain the convex hull of the vertices of $\mathcal{V}(0)$.

Babai cell: Determine the vertices of the Babai cell $\mathcal{B}(0)$. Apply function *ConvexHullMesh[]* to compute the convex hull of these vertices.

Intersection: Apply *RegionIntersection[]* in Mathematica [33], to compute $\mathcal{B}(0) \bigcap \mathcal{V}(0)$ and its volume normalized by the volume of the lattice.

Packing density: Calculate the packing density $\Delta_3 = \frac{\pi}{6}\frac{d^3_{\min}(\Lambda)}{\mathrm{vol}(\Lambda)}$.

For lattices with a randomly chosen basis, we start by considering a basis, with the format $\{(1,0,0),(a,b,0),(c,d,e)\}$, where $a,c \in [-1/2,0]$ and $b,d,e \in [-2,2]$ are chosen independently and uniformly at random (the choice of the range is justified because we are only interested in lattices whose packing density is greater than 0.4). Then, the program tests if this basis is an obtuse superbase. If this condition is false, another random basis is generated until a suitable one is found. At the end of this stage, we will have a randomly chosen obtuse and Minkowski-reduced superbase for the lattice Λ.

Fig. 8 has points given by known lattices, together with random points (orange) that are associated with lattices having a packing density greater than 0.4. Note that with overwhelming probability, all orange points with a randomly chosen basis have a truncated octahedron as

Voronoi region, which is the most general Voronoi region in three dimensions. Indeed, the existence of a Voronoi region which is not a truncated octahedron is conditioned to at least one $p_{ij} = 0$, where

$$p_{01} = 1 + a + c, \;\; p_{02} = a(1 + a + c) + b(b + d)$$

$$p_{03} = c(1 + a + c) + d(b + d) + e^2,$$

$$p_{12} = a, \;\; p_{13} = c, \;\; p_{23} = -ac - bd,$$

for the selected parameters a, b, c, d and e. Since these equations correspond to a set of measure zero in the 5D parameter hyperbox $[-1/2, 0] \times [-2, 2] \times [-1/2, 0] \times [-2, 2] \times [-2, 2]$, this probability is negligible.

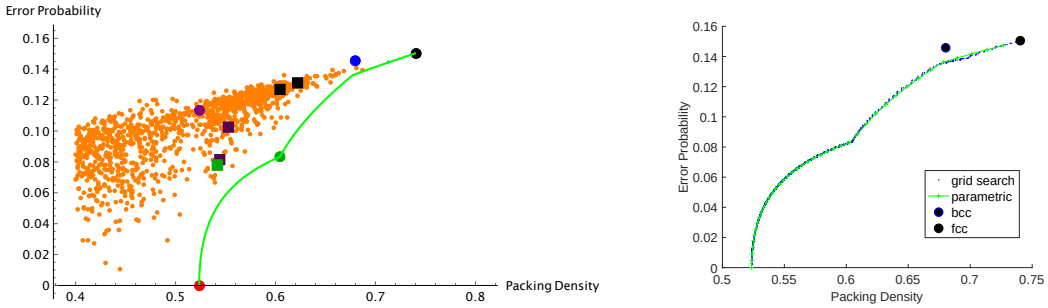

Fig. 8. Plot of error probability and packing density for $n = 3$, (left) known and randomly chosen (orange points) lattices, (right) best points obtained from a grid search and the parametric representation.

The circular points in Fig. 8 are respectively described as: in **red**, the cubic lattice $\mathbb{Z}^3$ with basis $\{(1,0,0),(0,1,0),(0,0,1)\}$; in **green**, the lattice Λ_{hp} with basis $\{(1,0,0),(-\frac{1}{2},-\frac{\sqrt{3}}{2},0),(0,0,1)\}$, whose Voronoi region is a regular hexagonal prism; in **blue**, the body-centered cubic lattice with basis $\{(1,0,0),(-\frac{1}{3},\frac{2\sqrt{2}}{3},0),\ (-\frac{1}{3},-\frac{\sqrt{2}}{3},\sqrt{\frac{2}{3}})\}$, whose Voronoi region is a truncated octahedron; in **black**, the face-centered cubic lattice with basis $\{(1,0,0),(-\frac{1}{2},-\frac{1}{2},\frac{1}{\sqrt{2}}),\ (0,1,0)\}$, whose Voronoi region is a rhombic dodecahedron; in **purple**, the lattice Λ_{hrd} with basis $\{(1,0,0),\ (-\frac{1}{\sqrt{5}},\frac{2}{\sqrt{5}},0),(0,-\frac{1}{2},\frac{\sqrt{5}}{2})\}$, whose Voronoi region is a hexa-rhombic dodecahedron. Table I summarizes their performances when we run Alg. 1.

Fig. 8 also presents some particular cases (square points), where the numerical random search led to a Voronoi region different than the general truncated octahedron. The color corresponds

TABLE I

PERFORMANCE IN ALGORITHM 1 FOR KNOWN LATTICES

Lattice/Voronoi cell	Notation 15.6 [7]	Δ_3	P_e
$\mathbb{Z}^3$/ Cuboid	111	0.5235	0
Λ_{hp}/ Hexagonal prism	$2_{-1}22$	0.6046	0.0833
FCC/ Rhombic dodecahedron	2_12_12	0.7404	0.1505
Λ_{hrd}/ Hexa-rhombic dodecahedron	2_13_12	0.5235	0.1134
BCC/ Truncated octahedron	$3_13_13_{-1}$	0.6802	0.1458

to the cell type, i.e., **green** is an hexagonal prism, **purple** are hexa-rhombic dodecahedrons, and **black** represents rhombic dodecahedrons.

D. Analysis of the Data and Observations

Let P_e and Δ_3 be the error probability and packing density for a lattice Λ. Consider the curve $P_e^*(\Delta)$, the lower boundary of the set of points (Δ_3, P_e) obtained by minimizing P_e subject to the constraint $\Delta_3 \geq \Delta$. Our interest is in finding a parametric form for the three-dimensional lattices that achieve points on this boundary. Observe that $P_e^*(\Delta) = 0$, for $\Delta \leq \pi/6$, where $\pi/6$ is the packing density for the cubic lattice in three dimensions. In fact lattices with densities strictly smaller than $\pi/6$ and error probability equal to zero can be obtained by rectangular (i.e. cuboidal) lattices. However, since $P_e = 0$ is already achieved at the packing density $\pi/6$, we need only consider Δ in the range $\left[\pi/6, \pi/(3\sqrt{2})\right]$, where $\pi/(3\sqrt{2})$ is the packing density of the FCC lattice, the lattice with the highest packing density in three dimensions. It turns out that a parametric form can be given, which closely approximates $P_e^*(\Delta)$, and coincides with it over a range of packing densities. This parametric form was first discovered by analyzing the data. Later it was realized that these lattices could be obtained by placing some constraints on the parameters in the family of well-rounded lattices (defined in the sequel).

Strongly well-rounded lattices, are defined as lattices having a basis consisting of vectors of minimum norm, which in our context is equal to 1. Well-rounded lattices have been studied generally [9], [24], and also for applications such as coding for wiretap Gaussian and fading channels [10], [16].

The bases for the family of well-rounded lattices can be written as $\{(1,0,0), (-\cos\alpha, \sin\alpha, 0), (-\sin\beta\cos\gamma, -\sin\beta\sin\gamma, \cos\beta)\}$, with $-1/2 \leq -\cos\alpha \leq 0$, $-1/2 \leq -\sin\beta\cos\gamma \leq 0$ and

$-1/2 \leq \sin\beta\cos(\alpha+\gamma) \leq 0$. These bases are in Minkowski reduced form, and satisfy the superbase constraint. It turns out that $\Lambda(\beta)$, the well-rounded lattice parameterized by β with $\alpha = \pi/2$ and

$$\sin\gamma = \begin{cases} 0, & 0 \leq \beta < \pi/6, \\ \frac{1}{2\sin\beta}, & \pi/6 \leq \beta \leq \pi/4, \end{cases} \tag{23}$$

leads to a curve which closely approximates $P_e^*(\Delta)$.

Error probability – packing density curves, obtained using the above parameterization, as well as a grid search, are plotted in the right hand panel in Fig. 8. We have the following observations.

For $0 \leq \beta \leq \pi/6$, $\Lambda(\beta)$ has basis $\{(1,0,0),(0,1,0),(-\sin\beta,0,\cos\beta)\}$. The packing density $\Delta(\beta) = \pi/(6\cos\beta)$, varies between $\pi/6$ (cubic lattice) and $\pi/(3\sqrt{3})$ (hexagonal lattice). The error probability is the same as for the two dimensional case and is given by $P_e = (1-(1-2\sin\beta)^2)/(16\cos^2\beta)$, which is an increasing function of β and lies in the range $[0, 1/12]$. The Voronoi cell is a cube for $\beta = 0$, a regular hexagonal prism for $\beta = \pi/6$ and an irregular hexagonal prism for $0 < \beta < \pi/6$. From Fig. 8 it is evident that the parameterization is optimal for this range of β values. It is interesting that there is no truly 3 dimensional Voronoi cell that is is able to do better in this range.

For $\pi/6 \leq \beta \leq \pi/4$, $\Lambda(\beta)$ has basis $\{(1,0,0),(0,1,0),(-\sqrt{\sin^2\beta - 1/4},-1/2,\cos\beta)\}$. The packing density $\Delta(\beta) = \pi/(6\cos\beta)$, varies between $\pi/(3\sqrt{3})$ and $\pi/(3\sqrt{2})$ (FCC). The error probability is an increasing function of β and lies in the range $[1/12, 0.1505]$. The Voronoi cell is a hexarhombic dodecahedron for $\pi/6 < \beta < \pi/4$ and a rhombic dodecahedron for $\beta = \pi/4$. The parameterization coincides with $P_e^*(\beta)$ for only part of this range of β values, but is a close approximation to $P_e^*(\Delta)$ over this entire range.

We also present an interesting comparison to a value listed in Table I. Specifically, the lattice with basis $\{(1,0,0),(0,1,0),(-\sqrt{17/108},-1/2,\sqrt{16/27})\}$ has the same volume and therefore the same packing density as the BCC lattice (whose Voronoi region is a truncated octahedron), but has error probability 0.1368 which is smaller than 0.1458 achieved by the BCC lattice.

At least in dimension $n = 3$, we have numerical evidence that when the packing density is small enough to be obtained by a prism, a prism is optimal. A natural question is whether this observation holds for dimensions greater than 3, i.e. do prisms achieve points on $P_e^*(\Delta)$ in higher dimensions, when Δ is small enough. The resolution of this is left as future work, since it will require the development of alternative analytic methods.

V. Error Probability Estimation for Higher Dimensions

Direct error probability calculations become increasingly difficult as the lattice dimension grows—we have already seen an example of this in going from $n = 2$ to $n = 3$ dimensions. The main focus of this section is to use tools from probability theory to bound the error probability. These bounds are particularly effective when the dimension becomes large. We also complement these bounds with those of a more geometric nature.

More specifically, under the Conditional Distribution model for $\mathbf{X}$, probabilistic concentration bounds are developed in Theorems 6 and 7. These bounds allow us to show in Theorem 8 that for lattices that generate suitably thin coverings of $\mathbb{R}^n$, $P_c \to 0$ as $n \to \infty$ under the Uniform Distribution Model. The proof of Theorem 8 requires an extremal result on the volume of intersection of a sphere and rectangle in $\mathbb{R}^n$, Theorem 9. While the probabilistic bounds are useful when the dimension is large, a bound based on estimating the volume of spherical caps, Theorem 11, can provide useful results when the dimension is small. Calculations for various lattices are provided in Sec. V-C. Error probability under the Gaussian Generative model is derived in Sec. V-D where it is shown that $P_c \to 1$ as $n \to \infty$ provided the noise variance is sufficiently small.

We have already noted that unlike the Voronoi cell, the Babai cell is *basis-dependent*. Hence most of the bounds developed here are basis dependent. One important exception is the result for thin coverings, which holds for *any* basis for the lattice.

A. Probabilistic Concentration Bounds: Conditional Distribution Model

We need to recall a few definitions. Let $\mathcal{S}_n(r)$ be the Euclidean ball (sphere) of radius r in $\mathbb{R}^n$ centered at the origin. The Babai cell of a lattice with a given basis is a hyper-rectangle with sides of length $a_i > 0$, $i = 1, 2, \ldots, n$ and we say that the Babai cell has size $\mathbf{a} = (a_1, a_2, \ldots, a_n) = (|v_{11}|, |v_{22}|, \ldots, |v_{nn}|)$, where V is the upper triangular generator matrix of Λ.

The error probability is $P_e = 1 - P_c$, where P_c, the success probability, is given by

$$P_c = \text{Prob}(\mathbf{X} \in \mathcal{V}(0) \bigcap \mathcal{B}(0) | \mathbf{X} \in \mathcal{B}(0)). \tag{24}$$

Theorem 6. *(Chebyshev bound) Suppose lattice $\Lambda \subset \mathbb{R}^n$ has covering radius r_{cov}, and for a given basis has a Babai cell of size $\mathbf{a} = (a_1, a_2, \ldots, a_n)$. Further, suppose that conditioned on*

event $\{\mathbf{X} \in \mathcal{B}(0)\}$*, (i)* X_i*,* $i = 1, 2, \ldots, n$ *are independent, and (ii)* $\mu := \frac{1}{n}\sum_{i=1}^{n} E[X_i^2] > \frac{r_{cov}^2}{n}$*. Then*

$$P_c \leq P_{cheb}(\mathbf{a}) := \frac{Var[\frac{1}{n}\sum_{i=1}^{n} X_i^2]}{(\mu - r_{cov}^2/n)^2}. \tag{25}$$

In particular, if conditioned on the event $\{\mathbf{X} \in \mathcal{B}(0)\}$*,* $\mathbf{X}$ *is uniformly distributed on* $\mathcal{B}(0)$ *and*

$$\frac{1}{12}\sum_{i=1}^{n} a_i^2 > r_{cov}^2. \tag{26}$$

then

$$P_c \leq \frac{4}{5}\frac{\sum_{i=1}^{n} a_i^4}{(\sum_{i=1}^{n} a_i^2 - 12r_{cov}^2)^2}. \tag{27}$$

Proof. From the conditions of the theorem

$$\{\mathbf{X} \in \mathcal{S}_n(r_{\text{cov}})\} = \left\{\frac{1}{n}\sum_{i=1}^{n} X_i^2 \leq \frac{r_{\text{cov}}^2}{n}\right\} \subset \left\{\left|\frac{1}{n}\sum_{i=1}^{n} X_i^2 - \mu\right| > \mu - \frac{r_{\text{cov}}^2}{n}\right\}. \tag{28}$$

Thus

$$P_c \leq \text{Prob}\left(\mathbf{X} \in \mathcal{S}_n(r_{\text{cov}})\right) \leq \text{Prob}\left(\left|\frac{1}{n}\sum_{i=1}^{n} X_i^2 - \mu\right| > \mu - \frac{r_{\text{cov}}^2}{n}\right) \leq \frac{\text{Var}[\frac{1}{n}\sum_{i=1}^{n} X_i^2]}{(\mu - r_{\text{cov}}^2/n)^2}$$

where the last step follows from Chebyshev's inequality [27].

When $\mathbf{X}$ is uniformly distributed on $\mathcal{B}(0)$, $\text{Var}[X_i] = a_i^2/12$, $\text{Var}[X_i^2] = E[X_i^4] - E[X_i^2]^2 = a_i^4/180$, and the X_i are mutually independent. Thus (27) follows by direct substitution in (25). □

The Chernoff bound [27] sometimes gives tighter bounds on P_c.

Theorem 7. *(Chernoff bound) Suppose lattice* $\Lambda \subset \mathbb{R}^n$ *has covering radius* r_{cov}*, and for a given basis has a Babai cell of size* $\mathbf{a} = (a_1, a_2, \ldots, a_n)$*. Further, suppose that conditioned on the event* $\{\mathbf{X} \in \mathcal{B}(0)\}$*, (i)* X_i*,* $i = 1, 2, \ldots, n$ *are independent, and (ii)* $\mu := \frac{1}{n}\sum_{i=1}^{n} E[X_i^2] > \frac{r_{cov}^2}{n}$*. Then*

$$P_c \leq P_{cher}(\mathbf{a}) := e^{\beta r_{cov}^2/n} E[e^{-(\beta/n)\sum_{i=1}^{n} X_i^2}], \tag{29}$$

for any $\beta > 0$*. In particular, if conditioned on the event* $\{\mathbf{X} \in \mathcal{B}(0)\}$*,* $\mathbf{X}$ *is uniformly distributed on* $\mathcal{B}(0)$ *and*

$$\frac{1}{12}\sum_{i=1}^{n} a_i^2 > r_{cov}^2, \tag{30}$$

then

$$P_c \leq \frac{e^{\beta r_{cov}^2/n}}{vol\,(\Lambda)}\prod_{i=1}^{n}\int_{-a_i/2}^{a_i/2} e^{-\beta x^2/n} dx \tag{31}$$

for any $\beta > 0$*.*

Proof. The proof is a direct application of the Markov inequality [27] and proceeds as follows. For any $\beta > 0$

$$\begin{aligned} P_c &\leq \text{Prob}\left(\frac{1}{n}\sum_{i=1}^{n} X_i^2 \leq \frac{r_{\text{cov}}^2}{n}\right) = \text{Prob}\left(e^{-\beta\sum_{i=1}^{n} X_i^2/n} \geq e^{-\beta r_{\text{cov}}^2/n}\right) \\ &\leq \frac{E[e^{-\beta\sum_{i=1}^{n} X_i^2/n}]}{e^{-\beta r_{\text{cov}}^2/n}} = e^{\beta r_{\text{cov}}^2/n}\prod_{i=1}^{n} E[e^{-\beta X_i^2/n}] = \frac{e^{\beta r_{\text{cov}}^2/n}}{\text{vol}\,(\Lambda)}\prod_{i=1}^{n}\int_{-a_i/2}^{a_i/2} e^{-\beta x^2/n}dx. \end{aligned}$$

□

Lattices that result in thin coverings: Under the Uniform Distribution Model, we derive a sufficient condition on the thickness of the lattice covering and hence its covering radius, such that $P_c \to 0$ as $n \to \infty$ (for such lattices, the Babai point is asymptotically bad). We describe our method first, and then provide theorems and proofs.

Let $\mathcal{K}$ be an n-dimensional centrally symmetric cube whose volume is the same as that of a Babai cell, i.e. $\text{vol}\,(\mathcal{K}) = \text{vol}\,(\mathcal{B}(0)) = \text{vol}\,(\Lambda)$.

1) We will show that $\text{vol}\,(\mathcal{B}(0)\bigcap\mathcal{S}_n(r_{cov})) \leq \text{vol}\,(\mathcal{K}\bigcap\mathcal{S}_n(r_{cov}))$. This is based on an extremal result, whose proof will be provided next, regarding the volume of intersection of a sphere and a rectangle of given volume, namely, that the volume is maximized when the rectangle is a cube. This together with (3) will lead to
$$P_c = \frac{\text{vol}\,(\mathcal{B}(0)\bigcap\mathcal{V}(0))}{\text{vol}\,(\mathcal{B}(0))} \leq \frac{\text{vol}\,(\mathcal{B}(0)\bigcap\mathcal{S}_n(r_{\text{rcov}}))}{\text{vol}\,(\mathcal{B}(0))} \leq \frac{\text{vol}\,(\mathcal{K}\bigcap\mathcal{S}_n(r_{\text{cov}}))}{\text{vol}\,(\mathcal{K})}.$$
2) For a lattice that results in a sufficiently thin covering, we will show that the Chebyshev condition, $\mu > r_{\text{cov}}^2/n$ of Theorem 6, will hold when $\mathbf{X}$ is uniformly distributed over $\mathcal{K}$, by using the result of Item 1. The result $P_c \to 0$ as $n \to \infty$ will then follow by application of Theorem 6.

We address Item 2 first in the following theorem, assuming that Item 1 holds.

Theorem 8. *(Success probability of thin coverings) Suppose there is an $\epsilon > 0$ and an $n_0 > 0$ such that for all $n > n_0$ the covering radius of a lattice $\Lambda_n \subset \mathbb{R}^n$ satisfies*
$$\frac{vol\,(\Lambda_n)^{2/n}}{12} - \frac{r_{cov}^2}{n} \geq \epsilon\, vol\,(\Lambda_n)^{2/n}.$$
Then $P_c \to 0$ as $n \to \infty$.

Proof. The theorem states that P_c becomes small for lattices that generate a suitably thin covering of $\mathbb{R}^n$. Apply Theorem 6 with $\mathbf{X}$ uniformly distributed over $\mathcal{K}$, a centrally symmetric cube whose

volume is equal to that of $\mathcal{B}(0)$, in order to obtain an upper bound on vol $(\mathcal{K} \bigcap \mathcal{S}_n(r_{cov}))$. Denote the length of each side of $\mathcal{K}$ by b; thus $b^n = \text{vol}\,(\mathcal{B}(0)) = \text{vol}\,(\Lambda_n)$. From the condition of this theorem (26) is satisfied and from (27) it follows that

$$P_c \leq \frac{4}{720} \frac{nb^4}{n^2\epsilon^2 b^4} \to 0,$$

as $n \to \infty$. □

Before we state and prove the theorem for Item 1, we introduce some definitions, for convenience. Given $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha_i > 0,\ i = 1, 2, \ldots, n$, let $\alpha_{\sim i}$ to be the $(n-1)$-dimensional vector obtained by deleting the ith component α_i from α, so with $\alpha = (3, 19, 7, 6)$, $\alpha_{\sim 2} = (3, 7, 6)$. Let

$$R(\alpha) = \{\mathbf{x} \in \mathbb{R}^n : |x_i| \leq \alpha_i,\ i = 1, 2, \ldots, n\}$$

be the n-dimensional centered rectangle with vertices $(\pm\alpha_1, \pm\alpha_2, \ldots, \pm\alpha_n)$. Let

$$V(r, \alpha, n) = \text{vol}\left(\mathcal{S}_n(r) \bigcap R(\alpha)\right).$$

For any n-dimensional vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, let $f(\alpha) = (\beta, \beta, \ldots, \beta)$, where $\beta = (\alpha_1\alpha_2 \ldots \alpha_n)^{1/n}$, i.e. $f(\alpha)$ is the n-dimensional vector with each component equal to geometric mean of the components of α. Thus $R(f(\alpha))$ is a centrally symmetric cube, with volume equal to that of $R(\alpha)$. Our objective is to show that $V(r, \alpha, n) \leq V(r, f(\alpha), n)$ for every n.

Also for convenience we introduce the operator, g_i defined by

$$g_i(\alpha) = g_i(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\beta, \beta, ..., \beta, \alpha_i, \beta, \ldots, \beta),$$

where

$$\beta = \left(\prod_{j=1}^{n} \alpha_j/\alpha_i\right)^{\frac{1}{(n-1)}}.$$

Thus g_i fixes the ith component of α and replaces every other component by β, while preserving the product. Further let $g^{(m)}(\alpha)$ denote the m-fold circular composition of the g_i's, where we apply to α, the operators g_1, g_2,...,g_n, g_1, g_2, ... sequentially in circular fashion, m times. The proof relies on the following lemma, which states that when g_i is applied to α many times, circularly, the result converges to the constant vector $f(\alpha)$.

Lemma 2. *(Convergence of the composition) For fixed $n > 2$ and any $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ with strictly positive and finite components*

$$\lim_{m\to\infty} g^{(m)}(\alpha) = f(\alpha).$$

Proof. After m iterations of g, $m \geq 1$, the resulting vector $g^{(m)}(\alpha)$ has at most two distinct entries, u_m which appears once and v_m which is repeated $(n-1)$ times. Both entries are finite and strictly positive. The ratio satisfies the recursion $(u_{m+1}/v_{m+1}) = (v_m/u_m)^{1/(n-1)}$ which converges to 1 as $m \to \infty$. □

Theorem 9. *(Extremal intersection) Over the class of all centrally symmetric rectangles in $\mathbb{R}^n$ with given volume, the volume of intersection with a centrally symmetric sphere is maximized by the n-dimensional cube. Specifically,*

$$V(r, \alpha, n) \leq V(r, f(\alpha), n)$$

for every $r > 0$, every rectangle $R(\alpha)$ and every $n \geq 2$.

Proof. Proof is by induction. From the result due to L. Fejes Tóth, [13], reproved in a more specific manner by G. Hajós, [17], as described by Florian [14], the result is valid for $n = 2$. Assume that the theorem is true for $n = k-1$, which is our induction hypothesis. We now show it is true for $n = k$.

For any i, $1 \leq i \leq k$, we can write

$$V(r, \alpha, k) = \int_{-\alpha_i}^{\alpha_i} V(\sqrt{(r^2 - x^2)^+}, \alpha_{\sim i}, k-1)dx, \tag{32}$$

where $(x)^+ = \max(x, 0)$. From the induction hypothesis

$$V(\sqrt{(r^2 - x^2)^+}, \alpha_{\sim i}, k-1) \leq V(\sqrt{(r^2 - x^2)^+}, f(\alpha_{\sim i}), k-1).$$

Thus, it follows that

$$V(r, \alpha, k) \leq \int_{-\alpha_i}^{\alpha_i} V(\sqrt{(r^2 - x^2)^+}, f(\alpha_{\sim i}), k-1)dx = V(r, g_i(\alpha), k). \tag{33}$$

Repeating this step circularly, we get

$$V(r, \alpha, k) \leq \lim_{m \to \infty} V(r, g^{(m)}(\alpha), k) = V(r, f(\alpha), k), \tag{34}$$

proving our assertion. □

Corollary 2. *(Success probability of Rogers' lattices) The success probability $P_c \to 0$ as $n \to \infty$ for lattices which satisfy Rogers' bound [29] on the thickness, Θ_n, namely,*

$$\Theta_n \leq cn(\log_e n)^\kappa,$$

$\kappa = \log_2 \sqrt{2\pi e}$.

Proof. Rogers' bound implies that for any $\delta > 0$ and n sufficiently large

$$\frac{r_{\text{cov}}^2}{n} \leq \frac{(1+\delta)\text{vol}\,(\Lambda_n)^{2/n}}{2\pi e}.$$

Choose δ such that $\frac{(1+\delta)}{2\pi e} < \frac{1}{12}$ and let $\epsilon = \frac{1}{12} - \frac{(1+\delta)}{2\pi e}$. Thus there is an $\epsilon > 0$ and an n_0 such that for all $n > n_0$, $\frac{\text{vol}(\Lambda_n)^{2/n}}{12} - \frac{r_{\text{cov}}^2}{n} \geq \epsilon\,\text{vol}\,(\Lambda_n)^{2/n}$ and the condition of Theorem 8 is satisfied. □

Remark 3. *Unlike the bounds derived earlier which depend on the basis, the results of Theorem 8 and Corollary 2 hold for* **any basis** *for the lattice.*

B. Geometric Bounds

We consider next some bounds of more geometric nature.

Theorem 10. *(Exclusion bound) For a lattice Λ with covering radius r_{cov} and a given basis, suppose that a Babai cell has size $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ which satisfies $a_1 \geq a_2 \geq \ldots \geq a_m > 2r_{cov} \geq a_{m+1} \geq \ldots a_n$. Then*

$$P_c = \textit{Prob}(\mathbf{X} \in \mathcal{V}(0) \bigcap \mathcal{B}(0) | \mathbf{X} \in \mathcal{B}(0)) \leq \frac{(2r_{cov})^m}{\prod_{i=1}^m a_i}. \tag{35}$$

When $2r_{cov} \geq a_1$, the bound is unity.

Proof. The idea is to cut off parts of the Babai rectangle which are outside the sphere $\mathcal{S}_n(r_{\text{cov}})$, starting with cutting planes $\pm r_{\text{cov}}\mathbf{e}_1 \in \mathbb{R}^n$, where $\mathbf{e}_i$ is the ith standard basis vector. After the ith pair of cuts $\pm r_{\text{cov}}\mathbf{e}_i$, we are left with a smaller rectangle of size $(2r_{\text{cov}}, \ldots, 2r_{\text{cov}}, a_{m+1}, \ldots, a_n)$ which intersects $\mathcal{S}_n(r_{\text{cov}})$. We stop after the mth pair of cuts, for then every face of the remaining rectangle intersects the interior of $\mathcal{S}_n(r_{\text{cov}})$. The ratio of the volume of the remaining rectangle to the volume of $\mathcal{B}(0)$ is the desired upper bound on the probability. Thus

$$P_c \leq \frac{(2r_{\text{cov}})^m a_{m+1} \ldots a_n}{\text{vol}\,(\Lambda)} = \frac{(2r_{\text{cov}})^m}{a_1 a_2 \ldots a_m}, \tag{36}$$

where in the last step we have used $a_1 a_2 \ldots a_n = \text{vol}\,(\Lambda)$. □

Remark 4. *We refer to the rectangular cell obtained by cutting the Babai cell $\mathcal{B}(0)$ in Theorem 10 as the excluded Babai cell $\mathcal{B}_{ex}(0)$.*

By applying the Chebyshev or Chernoff bound to $\mathcal{B}_{\text{ex}}(0)$ we obtain the following bound.

Corollary 3. *(Exclusion-concentration bound) Suppose m is defined as in the Exclusion bound (Theorem 10) and that $\delta_1 = \frac{1}{12}\sum_{i=m+1}^{n} a_i^2 - r_{cov}^2(1-m/3) > 0$. Then*

$$P_c \leq \frac{(2r_{cov})^m}{\prod_{i=1}^{m} a_i} P_{conc}(\tilde{\mathbf{a}})$$

where $P_{conc}(\tilde{\mathbf{a}})$ is either of $\min\left[P_{cheb}(\tilde{\mathbf{a}}), 1\right]$ or $\min\left[P_{cher}(\tilde{\mathbf{a}}), 1\right]$ with

$$\tilde{\mathbf{a}} = (\underbrace{2r_{cov}, \ldots, 2r_{cov}}_{m \text{ times}}, a_{m+1}, \ldots, a_n).$$

Proof. Direct application of the Exclusion bound followed by the one of the concentration bounds, Theorems 6 or 7. □

As a dual of the Theorem 10, lower bounds for the error probability can also be derived, given a Babai cell size $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ of a lattice Λ, if $a_i < 2r_{\text{pack}}$ for some $i = 1, \ldots, n$. When this condition is satisfied, the region of two spherical caps which are cut from the packing sphere $\mathcal{S}_n(r_{\text{pack}})$ by the hyperplanes $x_i = \pm\frac{a_i}{2}$ will be out of the Babai region $\mathcal{B}(0)$, but inside the Voronoi region $\mathcal{V}(0)$, and their volumes will contribute to the error probability. Note that here we are assuming that $\mathbf{X}$ is uniformly distributed over $\mathcal{V}(0)$, rather than $\mathcal{B}(0)$. This is justified since for the Uniform Distribution Model, $\text{vol}\left(\mathcal{B}(0)\bigcap\mathcal{V}(0)\right)/\text{vol}\left(\mathcal{B}(0)\right) = \text{vol}\left(\mathcal{B}(0)\bigcap\mathcal{V}(0)\right)/\text{vol}\left(\mathcal{V}(0)\right)$.

When the condition $a_i < 2r_{\text{pack}}$ is satisfied for more than one i, let us say, a_j and a_k for example, we may consider other caps to be cut, but in order to have no overlapping of volumes between caps, we must have $\frac{a_j^2}{4} + \frac{a_k^2}{4} \geq r_{\text{pack}}^2$. We consider here the reordered set such that $a_1 \leq \cdots \leq a_m < 2r_{\text{pack}}$. For the purpose of this proof we use the following notation. Let V_n be the volume of the unit radius n-dimensional sphere given by $V_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)}$, $\Gamma(n)$ is the Euler's gamma function.

Using this geometric approach, we can state the following result.

Theorem 11. *(Spherical cap bounds) For a lattice Λ with packing radius r_{pack}, suppose the Babai cell sizes $\mathbf{a} = (a_1, \ldots, a_n)$ are ordered in a way such that $a_1 \leq a_2 \leq \cdots \leq a_n$. If $a_i \leq 2r_{pack}$, for $i = 1, \ldots, m$, two lower bounds for the error probability are*

i) $P_e \geq 2V_{n-1}\frac{r_{pack}^n}{a_1 \ldots a_n}\Big(\int_0^{\arccos\left(\frac{a_1}{2r_{pack}}\right)} \sin^n(t)\ dt + \sum_{i=2}^{m}\int_0^{\arccos\left(\frac{\ell_i}{2r_{pack}}\right)} \sin^n(t)\ dt\Big)$, *where* $\ell_i = \max\left\{\frac{a_i}{2}, \sqrt{r_{pack}^2 - \frac{a_1^2}{4}}\right\}$.

ii) $P_e \geq 2V_{n-1}\frac{r_{pack}^n}{a_1 \ldots a_n}\Big(\sum_{i=1}^{m}\int_0^{\arccos\left(\frac{b_i}{2r_{pack}}\right)} \sin^n(t)\ dt\Big)$, *where* $b_i = \max\{\frac{a_i}{2}, \frac{r_{pack}}{\sqrt{2}}\}$.

Proof. For $i = 1$, we consider the volume of two spherical caps of a sphere with radius r_{pack} cut by the hyperplanes $x_1 = \pm\frac{a_1}{2}$. For $i = 2, \ldots, m$ we consider the volume of the caps cut by the hyperplanes $x_i = \pm\ell_i = \pm\max\left\{\frac{a_i}{2}, \sqrt{r_{\text{pack}}^2 - \frac{a_1^2}{4}}\right\}$. Since we have no overlapping of volumes, we can assert that

$$P_e \geq \frac{2}{a_1 \ldots a_n}\Big[\text{vol}\left(Cap(r_{\text{pack}}, \tfrac{a_1}{2})\right) + \sum_{i=2}^{m}\text{vol}\left(Cap(r_{\text{pack}}, \ell_i)\right)\Big], \tag{37}$$

where $\text{vol}\left(Cap(r, b)\right) = V_{n-1}\int_0^{\arccos\left(\frac{b}{r}\right)} \sin^n(t)\ dt$ is the volume of a spherical cap in a sphere of radius r in $\mathbb{R}^n$ cut by parallel hyperplanes at distance b from the equator. From (37), the result stated in item (i) follows.

Regarding item (ii), for $i = 1, \ldots, m$, let $b_i = \max\{\frac{a_i}{2}, \frac{r_{\text{pack}}}{\sqrt{2}}\}$. Again, there is no common volume between the spherical caps cut by the hyperplanes $x_i = \pm b_i$ and it follows that

$$P_e \geq \frac{2}{a_1 \ldots a_n}\Big[\sum_{i=1}^{m}\text{vol}\left(Cap(r_{\text{pack}}, \tfrac{b_i}{2})\right)\Big]. \tag{38}$$

Upon expanding the formula for the volume of the spherical cap, the result of item (ii) arises. □

One can observe that the bounds stated in Theorem 11 are directly related to the lattice center density, defined as $\frac{r_{\text{pack}}^n}{a_1 \ldots a_n}$.

C. Applications of the Bounds for the Uniform Distribution Model

Examples of the bounds discussed in Secs. V-A and V-B are presented for some lattices lattices.

$\mathbb{Z}^2$ *lattice:* Consider the $\mathbb{Z}^2$ lattice with basis $\{(5, 12), (2, 5)\}$, which is not Minkowski-reduced. After performing a QR decomposition, we get $\left\{(13, 0), \left(\frac{70}{13}, \frac{1}{13}\right)\right\}$. Since $13 > \sqrt{2} = 2r_{\text{cov}}$, Theorem 6, we gives the looser bound $P_c \leq 0.859$, while Theorem 10 provides $P_c \leq \frac{\sqrt{2}}{13} \approx 0.108$. The exact success probability here is $P_c = 0.0833$. This particular example illustrates a general observation that Theorem 10 and Corollary 3 are useful when we are working with bad bases, which results in highly elongated Babai cells and consequently, a reduced success probability.

E_8 *lattice:* Consider the generator matrix for the E_8 lattice as in [7, Eq. (99)]. Since the packing radius is $r_{\text{pack}} = \frac{1}{\sqrt{2}}$, Theorem 11 (i) gives $P_e \geq 0.0725$ and the conditions required on

Theorems 6 and 10 regarding the covering radius are not satisfied.

Barnes-Wall lattice Λ_{16}*:* Consider the Barnes-Wall lattice Λ_{16} with generator matrix as presented in [7] , Fig. 4.10 scaled by a factor of $\sqrt{2}$,, with packing radius $\sqrt{2}$. The lower bound on the error probability given by Theorem 11 (i) is $P_e \geq 0.00203$, while the conditions for the covering radius on Theorems 6 and 10 are not satisfied.

Leech lattice Λ_{24}*:* Consider the Leech lattice Λ_{24} with generator matrix as given in [7], Fig. 4.12. For this generator matrix the size of the Babai cell is $\mathbf{a} = (8, 4^{(11)}, 2^{(11)}, 1)/\sqrt{8}$ and the covering radius is $\sqrt{2}$ which gives $P_c \leq P_{cheb}(\mathbf{a}) = 0.6557$. A lower value is obtained by minimizing the Chernoff bound in Theorem 7. Specifically for $\beta = 53.96$, we obtain $P_c \leq P_{cher}(\mathbf{a}) = 0.3882$. Behavior of the Chernoff bound for different values of β is illustrated in Fig. 9. Regarding the lower bound given by Theorem 11, $P_e \geq 0.00197$.

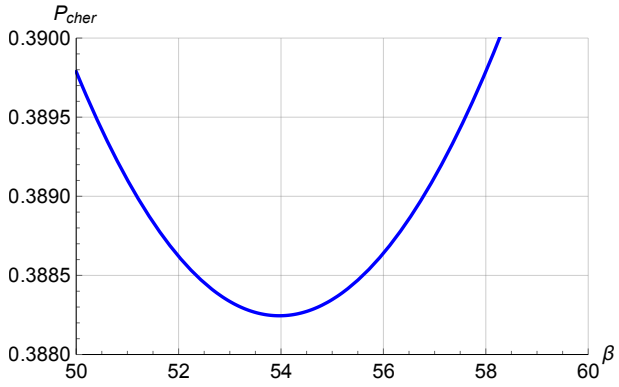

Fig. 9. Chernoff upper bound on P_c as a function of β for the Leech lattice.

A_n *lattices:* A_n has generator matrix in square form given by $V_{A_n} = I_n + \frac{c_n}{n} J_n$, where I_n is the $n \times n$ identity matrix, $c_n = -1 \pm \sqrt{n+1}$ and J_n is $n \times n$ the matrix of ones [19]. From this fact, we can determine $a_1, \ldots, a_n$, which are the the diagonal elements of the upper triangular matrix R obtained through QR decomposition. Hence,

$$a_1 = r_{11} = \sqrt{2}, \quad a_2 = r_{22} = \sqrt{\frac{3}{2}}, \quad a_3 = r_{33} = \sqrt{\frac{4}{3}} = \frac{2}{\sqrt{3}}.$$

If we move forward with this process, $a_k = \sqrt{\frac{k+1}{k}}$, for any $k = 1, \ldots, n$. Then, is it valid that $r_{\text{pack}} = \frac{\sqrt{2}}{2}$ and $\frac{r_{\text{pack}}}{\sqrt{2}} < \frac{a_k}{2} \leq r_{\text{pack}}$, for $k = 1, \ldots, n$. Considering item (ii) of Theorem 11, it

follows that

$$P_e \geq 2^{\frac{2-n}{2}} \frac{V_{n-1}}{\sqrt{n+1}} \Big(\sum_{i=1}^{m} \int_0^{\arccos\left(\sqrt{\frac{k+1}{2k}}\right)} \sin^n(t)\ dt \Big). \tag{39}$$

For example, we have that for A_2, $P_e \geq 0.05299$. Note that the basis for the A_2 lattice considered here is equivalent to the hexagonal lattice with Minkowski-reduced basis, and as we have seen in Corollary 1, the exact error probability is $\frac{1}{12} \approx 0.0833$. For A_3, $P_e \geq 0.1303$, for A_4, $P_e \geq 0.1918$, for A_5, $P_e \geq 0.2152$, and for A_6, $P_e \geq 0.2022$. For dimensions up to 5, the lower bound on P_e increases and after that it decreases, which is explained by the contribution of V_{n-1} in such calculation.

On the other hand, observe that the condition from (26) is not satisfied for this lattice. Indeed,

$$\frac{1}{12} \sum_{i=1}^{n} a_i^2 = \frac{1}{12} \sum_{i=1}^{n} \left(1 + \frac{1}{i}\right), \tag{40}$$

and $r_{\text{cov}} = \frac{1}{\sqrt{2}} \left(\frac{2 \cdot \lfloor \frac{n+1}{2} \rfloor \left(n+1-\lfloor \frac{n+1}{2} \rfloor\right)}{n+1} \right)^{1/2}$ [7, p. 109]. Note that

$$r_{\text{cov}}^2 = \begin{cases} \frac{n+1}{4}, & \text{if } n \text{ is odd} \\ \frac{n(n+2)}{4(n+1)}, & \text{if } n \text{ is even} \end{cases} \tag{41}$$

and $r_{\text{cov}}^2 > \frac{n}{4}$, for all n. By considering the upper bound for a partial finite sum of the harmonic series together with (40), it is valid that

$$\frac{1}{12} \sum_{i=1}^{n} \left(1 + \frac{1}{i}\right) = \frac{1}{12} \left(n + 1 + \sum_{i=2}^{n} \frac{1}{i} \right) < \frac{1}{12}(n+1+\log(n)) < \frac{1}{12}(2n+1) < \frac{n}{4} < r_{\text{cov}}^2, \tag{42}$$

for all $n \geq 1$.

D. Gaussian Generative Model

We now analyze the Gaussian case, as described in Sec. II-A for which P_e is given by (4). Analytic evaluation of this probability in closed form is difficult, even in low dimensional cases.

Numerical analysis of P_e for $n = 2$ as a function of the packing density for various values of the noise variance σ^2 is presented in Fig. 10 (this is the counterpart of Fig. 7 for the Gaussian case). For a two dimensional lattice Λ with basis $\{(1,0),(a,b)\}$, we have calculated the term T in (4), which we will refer to here as $P_e(\sigma^2,a,b)$.We could observe that $\frac{\partial P_e(\sigma^2,a,b)}{\partial a} < 0$ for $-\frac{1}{2} \leq a \leq 0$ and $b \geq \frac{\sqrt{3}}{2}$, therefore for a fixed variance σ^2 and fixed b, $P_e(\sigma^2,a,b)$ is decreasing

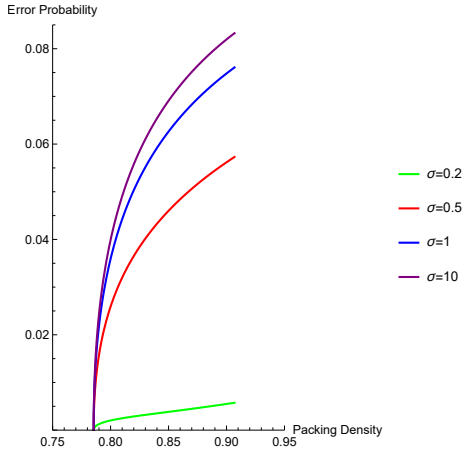

Fig. 10. Minimum error probability for given packing density assuming $\frac{\pi}{4} < \Delta_2 \leq \frac{\pi}{2\sqrt{3}}$ (or $3/4 \leq b^2 < 1$), considering a Gaussian distribution.

with a. Thus, the same minimization for the parameter a as in Remark 2 applies here. It is straightforward to conclude that smaller variance provides smaller error probability.

We now develop a sufficient condition on σ^2 for $P_c \to 1$ as $n \to \infty$, in terms of the packing radius of the lattice.

Theorem 12. *(Condition on σ^2 for success probability) Given a lattice with packing radius r_{pack} and a basis for which the Babai cell sizes are $\mathbf{a} = (a_1, a_2, \ldots, a_n)$. Let $r_b^2 = \min_{i=1,\ldots,n} \{a_i^2/4n\}$. Given that $\sigma^2 < r_0^2 := \min\{r_{pack}^2/n, r_b^2\}$, the probability that the Babai and Voronoi points coincide satisfies the lower bound*

$$P_c \geq 1 - \frac{2\sigma^4}{n(r_0^2 - \sigma^2)^2}.$$

Thus if there is an $\epsilon > 0$ such that $r_0^2 - \sigma^2 > \epsilon$, for all n larger than some n_0, then $\lim_{n\to\infty} P_c = 1$.

Proof. From (4), we have that

$$\begin{aligned}
P_c &\geq \text{Prob}\left(\mathbf{Z} \in \mathcal{V}(0) \bigcap \mathcal{B}(0)\right) \geq \text{Prob}\left(\mathbf{Z} \in \mathcal{S}_n(r_0)\right) \\
&= \text{Prob}\left(\|\mathbf{Z}\|^2/n \leq r_0^2\right) = \text{Prob}\left(\|\mathbf{Z}\|^2/n - \sigma^2 \leq r_0^2 - \sigma^2\right) \\
&= 1 - \text{Prob}\left(\|\mathbf{Z}\|^2/n - \sigma^2 > r_0^2 - \sigma^2\right) \\
&\geq 1 - \text{Prob}\left(\left|\|\mathbf{Z}\|^2/n - \sigma^2\right|^2 > (r_0^2 - \sigma^2)^2\right) \\
&\overset{(a)}{\geq} 1 - \frac{\text{Var}[\frac{1}{n}\|\mathbf{Z}\|^2]}{(r_0^2 - \sigma^2)^2} \overset{(b)}{\geq} 1 - \frac{2\sigma^4}{n(r_0^2 - \sigma^2)^2}.
\end{aligned}$$

where in (a) we have used the Markov inequality [27] and in (b) the fact that Var$[Z_i^2] = 2\sigma^4$. $\square$

Theorem 12 states that if the variance σ^2 satisfies the proposed condition, then estimating the Babai point is enough to guarantee the correct solution for the nearest lattice point problem.

VI. Summary and Conclusions

We first considered the problem of finding an approximate nearest point in a given lattice Λ to $\mathbf{x} \in \mathbb{R}^n$ in a distributed network. We assumed that each component of the vector $\mathbf{x}$ is available at a distinct sensor node and the lattice point is to be obtained at a central node. Thus each sensor node sends a quantized version of its observation to a central node. A protocol for transmitting this information to the central node was presented, its communication rate was determined, and shown to be optimal when the components of the real vector are mutually independent.

We then considered the problem of evaluating the error probability, namely, the probability that the approximate nearest lattice point (Babai point) does not coincide with the nearest lattice point (Voronoi point). Closed form expressions for the error probability were derived in two dimensions. For the three dimensional case, we have computationally estimated the worst error probability. Our results show that the error probability increases as the packing density of the lattice becomes larger. For dimensions greater than 3, we have used probabilistic and geometric methods to obtain bounds on the error probability and have shown that, when the lattice generates a suitably thin covering of $\mathbb{R}^n$, the probability that the Babai point coincides with the Voronoi point converges to 0 when the dimension n goes to infinity, under a uniform distribution assumption. Thus, when the vector $\mathbf{x}$ is uniformly distributed over a certain region, additional communication is required to compute the Voronoi point. On the other hand, when $\mathbf{x}$ is obtained by the addition of Gaussian noise of sufficiently small variance, the probability that the Babai and Voronoi points coincide converges to 1 as the dimension goes to infinity. Therefore, when $\mathbf{x}$ is obtained by the addition of Gaussian noise of sufficiently small variance to a lattice point, no further communication will be necessary in order to obtain the Voronoi point.

In the future, it would be of interest to compare the results obtained here with the ones in [15, Ch. 18], which evaluate how far the Babai point is from the Voronoi point when an LLL reduced basis is considered. It would also be interesting to check whether for high dimensions the probability that both points coincide is small for a lattices with a high packing density, even when good bases are assumed.

VII. Acknowledgment

CNPq (140797/2017-3, 312926/2013-8) and FAPESP (2013/25977-7) supported MFB and SIRC. VV was supported by CUNY-RF and CNPq (PVE 400441/2014-4). We thank the anonymous reviewers for their constructive comments which helped improve the paper.

References

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest Point Search in Lattices," *IEEE Trans. on Inf. Th.*, vol. 48, no. 8, pp. 2201-2214. Aug., 2002.

[2] M. Ajtai,"Generating Hard Instances of Lattice Problems (Extended Abstract)", in *Proc. of the Twenty-Eight Ann. ACM Symp. on the The. of Comp.*, Jul. 1996, pp. 99-108.

[3] L. Babai. "On Lovász Lattice Reduction and the Nearest Lattice Point Problem", *Combinatorica*, vol. 6, no. 1, pp. 1-13. 1986.

[4] M. F. Bollauf, V. A. Vaishampayan, and S. I. R. Costa, "On the Communication Cost of Determining an Approximate Nearest Lattice Point," in *Proc. 2017 IEEE Int. Symp. Inf. Th.*, Jul. 2017, pp. 1838-1842.

[5] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Berlin: Springer, 1997.

[6] X. Chang, J. Wen, and X. Xie, "Effects of the LLL Reduction on the Success Probability of the Babai Point on the Complexity of Sphere Decoding", *IEEE Trans. on Inf. Th.*, vol. 59, no. 8, pp. 4915-4926, Jun. 2013,

[7] J. H. Conway and N.J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, USA: Springer, 1999.

[8] J. H. Conway and N. J. A. Sloane. "Low-dimensional Lattices. VI. Voronoi Reduction of Three-dimensional Lattices," *Proc. of the Roy. Soc. of London*, vol. 436, no. 1896, pp. 55-68, Jan. 1992.

[9] M. T. Damir and L. Fukshansky, "Canonical Basis Twists of Ideal Lattices from Real Quadratic Number Fields", *H. J. of Math.*, vol. 45, n0. 4, pp. 9991019, 2019.

[10] M. T. Damir *et al.*, "Well-Rounded Lattices: Towards Optimal Coset Codes for Gaussian and Fading Wiretap Channels", arXiv: 1609:07723v4, 2020.

[11] S. C. Draper, B. J. Frey and F. R. Kschischang, Interactive decoding of a broadcast message. In Proc. Annual Allerton Conf. on Communication Control and Computing, pp. 170-180, 2003,

[12] P. van Emde Boas, "Another NP-Complete Problem and the Complexity of Computing Short Vectors in a Lattice", Amsterdam, Rep. 81-04, 1981.

[13] L. Fejes Tóth, "On the isoperimetric property of the regular hyperbolic tetrahedra," *Magyar Tud. Akad. Matematikai Kutató Intéz. Közl 8, pp. 53-57.*

[14] A. Florian, "Extremum problems for Convex Discs and Polyhedra," in Handbook of Convex Geometry, eds. P. M. Gruber and J. M. Wills, vol. A, pp. 177–221, Elsevier, Amsterdam: 1993.

[15] S. D. Galbraith, *Mathematics of Public Key Cryptography*. New York, NY: Cambridge University Press, 2012.

[16] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti, "Well-Rounded Lattices for Reliability and Security in Rayleigh Fading SISO Channels". In Proc. IEEE Inf. Th. Work., pp. 359363, 2016.

[17] G. Hajós, "Über den Durchschnitt eines Kreises und eines Polygons," *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* vol. 11, 137-144.

[18] J. Hoffstein, J. Pipher and J. H. Silverman. *An Introduction to Mathematical Cryptography*. New York, NY: Springer, 2008.

[19] M. Kim and J. Peters, "Symmetric Box-splines on the $A_n^\star$ Lattice", *J. of Approx. Th.*, vol. 162, no. 9, pp. 1607–1630, Sep. 2010.

[20] M. Li, M., D. G. Andersen, A. J. Smola and K. Yu, "Communication efficient distributed machine learning with the parameter server," In Advances in Neural Information Processing Systems, pp. 19-27, 2014.

[21] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring Polynomials with Rational Coefficients", *Mathematische Annalen*, vol. 261, no. 4, pp. 515-534, 1982.

[22] A. J. Mayer, "Low Dimensional Lattices have a Strict Voronoi Basis", *Mathematika*, vol. 42, no. 2, pp. 229-238, Dec. 1995.

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

[24] C. T. McMullen, "Minkowski's Conjecture, Well-Rounded Lattices and Topological Dimension", *J. Amer. Math. Soc.*, vol. 18, no. 3, pp. 711735, Mar. 2005.

[25] P. Q. Nguyen and D. Stehlé, "Low-Dimensional Lattice Basis Reduction Revisited", *Proc. of the Int. Alg. Num. Th. Symp.*, 2004, pp. 338-357.

[26] A. Orlitsky and J. R. Roche, "Coding for Computing", *IEEE Trans. on Inf. Th.*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[27] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. McGraw-Hill, 1991.

[28] C. Peikert. "A Decade of Lattice Cryptography", 2016.

[29] C. A. Rogers, *Packing and Covering*. Cambridge, UK: Cambridge University Press, 1964.

[30] V. A. Vaishampayan, "Precoder Design for Communication-Efficient Distributed MIMO Receivers with Controlled Peak-Average Power Ratio," IEEE Transactions on Communications, doi: 10.1109/TCOMM.2021.3070364.

[31] T. Wang, A. Cano, G. B. Giannakis and J. N. Laneman, "High-performance cooperative demodulation with decode-and-forward relays," IEEE Transactions on communications, vol 55, no. 7, pp.1427-1438, 2007.

[32] V. A. Vaishampayan and M. F. Bollauf, "Communication Cost of Transforming a Nearest Plane Partition to the Voronoi Partition", in *Proc. 2017 IEEE Int. Symp. Inform. Th.*, Jul. 2017, pp. 1843-1847.

[33] Wolfram Research, Inc., Mathematica, Version 11.2, Champaign, IL, 2017.

[34] R. Zamir, *Lattice Coding of Signals and Networks*. Cambridge University Press, 2014.