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 $X \in \mathbb{R}^n$ in a given lattice. We show that the protocol is optimal in the sense that it minimizes the sum rate when the components of $X$ 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. In dimensions two and three, this probability is seen to grow with the packing density. For higher dimensions, we use a bound from probability theory to estimate the error probability for some well-known lattices. Our investigations suggest that for uniform distributions, the error probability becomes large with the dimension of the lattice, for lattices with good packing densities.

We also consider the case where $X$ is obtained by adding Gaussian noise to a randomly chosen lattice point. In this case, the error probability goes to zero with the lattice dimension when the noise variance is sufficiently small. In such cases, a distributed algorithm for finding the approximate nearest lattice point is sufficient for finding the nearest lattice point.

Index terms—Lattices, distributed function computation, approximate nearest lattice point, communication complexity.

I. INTRODUCTION

We are given a lattice $\Lambda \subset \mathbb{R}^n$ and a random vector of observations, $X = (X_1, X_2, \ldots, X_n) \in \mathbb{R}^n$. 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 $X$ \cite{3}. Towards this end, the $i$th 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.

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 \cite{23}. In our case, $f$ is the function which computes an approximate nearest lattice point based on the nearest plane algorithm \cite{3} and $f(X)$ is the Babai point.

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).

Interest in communication issues for the distributed computation of the Babai point, and more generally for the nearest lattice point \cite{27}, 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 \[25\]. More generally, communication
issues for channel decoding and demodulation have been studied in the context of cooperative
communications \[11\], \[26\]. For a comprehensive review of lattice methods in communication,
see \[29\].

In recent years, interest has grown in communication issues related to distributed machine
learning \[17\]. 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 of interest in cryptography. In fact
the nearest lattice point problem has been proposed as a basis for lattice cryptography \[2\], \[13\],
\[15\], \[20\], \[24\], due to its hardness \[12\], examples being the GGH and LWE cryptosystems.
The security of such cryptosystems rely on the solution of this problem and the nearest plane
algorithm 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 paper is organized as follows. Mathematical preliminaries 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, for a
uniform conditional distribution on \(X\). This requires a special basis for a lattice as described in
Sec IV-A. This section also examines the relation between the error probability and the packing
density of the lattice being considered. Since these calculations are difficult to generalize to
higher dimensions, we use probabilistic tools to understand the behavior of the error probability
and its relation to the ‘sphericity’ of a Voronoi cell of the lattice in Sec. V in terms of its
covering and packing radii. In this section we also discuss and compare results about error
probability and packing density when \(X\) 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 and error probability simplifications are described 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 in-
dependent vectors \(\{v_1, v_2, \ldots, v_n\} \subset \mathbb{R}^n\), called lattice basis. We can also write \(\Lambda = \{V u, u \in \mathbb{Z}^n\}\),
where the columns of the generator matrix $V$ are the basis vectors $v_1, \ldots, v_n$. The matrix $A = V^T V$ is the associated Gram matrix and the $(i, j)$ entry of $A$ is the Euclidean inner product of $v_i$ and $v_j$, which here will be denoted by $v_i \cdot v_j$.

A set $\mathcal{F}$ is called a fundamental region of a lattice $\Lambda$ if all its translations by elements of $\Lambda$ cover $\mathbb{R}^n$, i.e., $\bigcup_{\lambda \in \Lambda} \mathcal{F} + \lambda = \mathbb{R}^n$ and the interior 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

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

where $||.||$ denotes the Euclidean norm. Note that $\mathcal{V}(\lambda)$ is congruent to $\mathcal{V}(0)$. The volume of a lattice $\Lambda$ is the volume of any of its fundamental regions and it is given by $\text{vol}(\Lambda) = |\det(V)|$, where $V$ is a generator matrix of $\Lambda$. We refer to $\mathcal{V}(\lambda)$ as a Voronoi cell.

A vector $v$ is called a Voronoi vector if the hyperplane $\{x \in \mathbb{R}^n : x \cdot v = \frac{1}{2} v \cdot v\}$ has a non-empty intersection with $\mathcal{V}(0)$. A Voronoi vector is said to be relevant if this intersection is an $(n-1)$-dimensional face of $\mathcal{V}(0)$.

The packing radius $r_{\text{pack}}$ of a lattice $\Lambda$ is half of the minimum distance between lattice points and the packing density $\Delta(\Lambda)$ is the fraction of space that is covered by balls $S(\lambda, r_{\text{pack}})$ of radius $r_{\text{pack}}$ in $\mathbb{R}^n$ centered at lattice points $\lambda \in \Lambda$, i.e., $\Delta(\Lambda) = \frac{\text{vol } S(0, r_{\text{pack}})}{\text{vol}(\Lambda)}$.

The objective of the nearest lattice point problem is to find

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

where the norm considered is the standard Euclidean norm. The nearest lattice point to $x$ is then given by $x_{\text{nl}} = Vu$.

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 $\lfloor x \rfloor = \lfloor x + 1/2 \rfloor$.

For a triangular generator matrix, the nearest plane (np) algorithm [3] computes $x_{\text{np}}$, an approximation to $x_{\text{nl}}$, given by $x_{\text{np}} = V u = u_1 v_1 + u_2 v_2 + \ldots + u_n v_n$, where $u_i \in \mathbb{Z}$ is given by

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

in the order $i = n, n-1, \ldots, 1$. We refer to $x_{\text{np}}$ as the Babai point for $x$ and the closure of the set of $x$ mapped to $y \in \Lambda$ as the Babai cell $\mathcal{B}(y)$. A method for finding $x_{\text{np}}$ for general $V$ is in [3].
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 point problem.

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

In case the generator matrix $V$ is upper triangular with $(i,j)$ entry $v_{ij}$, each rectangular cell is axis-aligned and has sides of length $|v_{11}|, |v_{22}|, \ldots, |v_{nn}|$. We remark that given a lattice $\Lambda$ 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 $R$ will then generate a rotated (and equivalent) version of the original lattice $\Lambda$.

A. Error Probability

We now define and simplify the error probability, $P_e$ and its complement, $P_c$, the success probability, for use in Secs. IV and V. The error probability and its complement are defined by $P_e = 1 - P_c = \text{Prob} \{ X_{nl} \neq X_{np} \}$. Clearly $P_c = \sum_{y \in \Lambda} \text{Prob} \{ X_{nl} = y, X_{np} = y \}$. Two situations of interest are (i) $X$ is uniformly distributed over a union of Babai cells, which we refer to hereafter as the uniform distribution case, and (ii) $x = y + z$, where $y \in \Lambda$ is the transmitted lattice vector, and $z \in \mathbb{R}^n$ is Gaussian noise, $\mathcal{N}(0, \sigma^2 \mathbf{I})$. We refer to this as the Gaussian case.

In the uniform case

$$P_c = \frac{\text{vol} \{ V(0) \cap B(0) \}}{\text{vol} \{ B(0) \}}.$$  

In the Gaussian case,
\[ P_c = \sum_{y \in \Lambda} \sum_{y' \in \Lambda} \text{Prob} [X_{nl} = y', X_{np} = y', Y = y] \]

\[ \geq (a) \sum_{y \in \Lambda} \text{Prob} [Y = y] \sum_{y' \in \Lambda} \text{Prob} [Z \in B(y' - y) \cap V(y' - y)] \]

\[ = \sum_{y \in \Lambda} \text{Prob} [Y = y] \sum_{y' \in \Lambda} \text{Prob} [Z \in B(y') \cap V(y')] \]

\[ = \sum_{y' \in \Lambda} \text{Prob} [Z \in B(y') \cap V(y')] \]

\[ = \text{Prob} [Z \in B(0) \cap V(0)] + \sum_{y' \in \Lambda, y' \neq 0} \text{Prob} [Z \in B(y') \cap V(y')], \quad (2) \]

where in (a) we have asserted the independence of \( Z \) and \( Y \). For small noise variance, the dominant term in the above sum is \( T = \text{Prob} [Z \in V(0) \cap B(0)] \). Note also that \( P_c = 1 \) when the basis vectors are mutually orthogonal.

It is an important fact that the Babai cell \( B(0) \) is dependent on the choice of the lattice basis, whereas the Voronoi cell is invariant to the choice of lattice basis. Thus, the error probability depends on the choice of basis, and in particular, the order in which the basis vectors are listed. Thus, in future sections, 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.

III. THE DISTRIBUTED BABAI PROTOCOL (DBP) AND ITS COMMUNICATION COST

We now describe the protocol DBP, by which the Babai point \( x_{np} = V u \) can be determined exactly at the computing node with a finite rate of transmission. We assume that

1) the lattice \( \Lambda \) 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, by canceling out common factors in \( v_{ml}/v_{mm} \), i.e. let \( p_{ml}/q_{ml} = v_{ml}/v_{mm} \). Let \( q_m = \text{lcm} \{ q_{ml}, l > m \} \), where \( \text{lcm} \) denotes the least common multiple of its arguments. By definition \( q_m = 1 \). The ‘interference’ term \( \nu_m \) is given by \( \nu_m = \sum_{l=m+1}^n wlv_{ml}/v_{mm} \). In terms of integer and fractional parts, \( \nu_m = [\nu_m] + \{\nu_m\} \), \( 0 \leq \{\nu_m\} < 1 \) and further, \( \{\nu_m\} \) is of the form \( s/q_m, 0 \leq s < q_m \). Let \( S_m \subset \{0, 1, \ldots, q_m - 1\} \) be the set of values taken by \( \{\nu_m\}q_m \) with positive probability. For most source probability
distributions $S_m = \{0, 1, \ldots, q_m - 1\}$. 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-C.

**Action of the Encoder in the $m$th SN:**
Define $s_m$ to be the largest integer $s \in S_m$ for which

$$[x_m/v_{mm} - s/q_m] = [x_m/v_{mm}]$$

Then the $m$th SN sends

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

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 $u = (u_1, u_2, \ldots, u_n)$ where,

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

where $\tilde{u}_m$ is given by (4),

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

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 $u$ given in (1).

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

$$u_m = \left[ \frac{x_m}{v_{mm}} - \left\{ \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right\} \right] - \left[ \frac{\sum_{l=m+1}^{n} u_l v_{ml}}{v_{mm}} \right], \quad m = n, n - 1, \ldots, 1.$$  \hspace{1cm} (6)

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

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

where $\tilde{u}_m$ is given by (4), and the computation of $u_m$ is performed at the CN in the order $m = n, n - 1, \ldots, 1$. \hfill $\square$
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 \(R_{\text{sum}}\) of protocol DBP is

\[
R_{\text{sum}} = \sum_{i=1}^{n} R_i = \sum_{i=1}^{n} H(\tilde{U}_i, S_i). \tag{8}
\]

As an example, suppose that \(X\) is uniformly distributed over a rectangular region \([-A/2, A/2]^n\), for \(A\) large. The total rate is

\[
R_{\text{sum}} = n \log_2(A) - \log_2 |\det V| + \sum_{i=1}^{n-1} H(S_i|\tilde{U}_i) \leq n \log_2(A) - \log_2 |\det V| + \sum_{i=1}^{n-1} \log_2(q_i). \tag{9}
\]

The first two terms in (9) can be interpreted as the rate required to compute the Babai point for a lattice \(\Lambda' \subset \mathbb{R}^n\) generated by orthogonal vectors \(\{(v_{11}, 0, \ldots, 0), \ldots, (0, 0, \ldots, v_{nn})\}\), where \(v_{ii}, 1 \leq i \leq n\) are the diagonal elements from the upper triangular generator matrix \(V\) of the lattice \(\Lambda\). Observe that the Babai cells of \(\Lambda\) are congruent to those of \(\Lambda'\), but are not aligned as they are in \(\Lambda'\). The last term in (9) is the additional communication cost because of the misalignment of the Babai cells of \(\Lambda\).

B. 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 [23]. 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 [23] 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 [23], 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 \(i\)th SN and \(f\) is to be computed at the CN. A lower bound on the communication rate from the \(i\)th 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
Let $\nu = \{1 \leq j \leq n, j \neq i\}$ and $x_i^c$ for the vector $(x_j, j \neq i)$. From [23], 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 $f(x) = f(x_i|x_i^c)$, when studying the communication rate from the $i$th SN to the CN, to emphasize the fact that $x_i^c$ is side information at the CN.

The characteristic graph, $G_i$, of the function $f(x_i|x_i^c)$, 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 $x_i^c$ for which $f(x_i|x_i^c) \neq f(x_i'|x_i^c)$. 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 $f(x_i|x_i^c)$ with $x_i^c$ known at the CN is given by the conditional graph entropy $H_{G_i}(X_i|X_i^c)$ [23], described next. Let $\Gamma_i$ be the collection of maximal independent sets of $G_i$ 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 $p(w|x_i, x_i^c)$ be a conditional probability distribution with the following properties:

1) $p(w|x_i, x_i^c) = p(w|x_i)$, for all $w \in \Gamma_i, (x_i, x_i^c) \in \mathbb{R}^n$. (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

$$H_{G_i}(X_i|X_i^c) = \min_{p \in \mathcal{P}_i} I(W; X_i|X_i^c). \quad (10)$$

We now apply this machinery for obtaining a lower bound on the rate $R_i$ for computing $u(x_i|x_i^c) = \left[ \frac{x_i - \sum_{j=i+1}^{n} u_{i,j} u_j}{u_{i,i}} \right]$, for $i = n, n - 1, \ldots, 1$. Our goal is to determine $G_i$ and its maximal independent sets, $i = 1, 2, \ldots, n$, and the probability distribution that solves (10).

First consider $G_n$. In $G_n$, $x_n$ 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 (4) that $W = \tilde{U}_n$. Hence $R_n \geq \min_{p \in \mathcal{P}_n} I(W; X_n|X_n^c) = H(\tilde{U}_n|X_n^c)$, since $H(\tilde{U}_n|X_n) = 0$.

Now consider $G_m$ for $m < n$. As before, let $\nu = \sum_{j=m+1}^{n} v_{m,j} u_j / v_{m,m}$ and write $\nu = \{\nu\} + [\nu]$. Since $\{\nu\} = s/q_m, s \in S \subset \{0, 1, \ldots, q_m - 1\}$ it follows that $x_m$ and $x_m'$ are disconnected in $G_m$ iff $[x_m/v_{m,m} - s/q_m] = [x_m'/v_{m,m} - s/q_m]$ for all $s \in S \subset \{0, 1, \ldots, q_m - 1\}$ or equivalently,
[x_m/v_{m,m}] = [x'_m/v_{m,m}] and the value of s_m evaluated using (3) is the same for x_m and x'_m.

From item 2 and (4), it follows that W = (\hat{U}_m, S_m) and hence R_m \geq \min_{p \in \mathcal{P}_m} I(W; X_m|X_m^c) = H(\hat{U}_m, S_m|X_m^c).

Thus (recall that S_n = 0)

\[ R_{\text{sum}} = \sum_{i=1}^{n} R_i \geq \sum_{i=1}^{n} H(\hat{U}_i, S_i|X_i^c). \] (11)

Since the lower bound coincides with the sum rate of the protocol DBP given by (8) when the X_i are mutually independent, DBP is optimal.

C. Examples

![Graph](image)

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 Th. 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), (-1/3, 2\sqrt{2}/3, 0), (-1/3, -\sqrt{2}/3, \sqrt{2}/3)\}. The Babai point given by \(u = (u_1, u_2, u_3)\), is given by

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

\[ \text{and} \quad u_1 = \left[ x_1 + \left\{ \frac{1}{3} u_2 + \frac{1}{3} u_3 \right\} \right] + \left\lfloor \frac{1}{3} u_2 + \frac{1}{3} u_3 \right\rfloor. \]
In order for the Babai point $u$ to be correctly calculated at the CN, nodes 2 and 1 send the following extra information, according to the protocol DBP:

node 2: \[ \left\{ \frac{1}{2}u_3 \right\} = \frac{s_2}{q_2}, \quad q_2 = 2 \text{ then } s_2 = 0 \text{ or } 1 \]

node 1: \[ \left\{ \frac{1}{3}u_2 + \frac{1}{3}u_3 \right\} = \frac{s_1}{q_1}, \quad q_1 = 3 \text{ then } s_1 = 0, 1 \text{ or } 2. \]

Observe that the values of $s_1$ and $s_2$ are calculated for a general received vector $x = (x_1, x_2)$. 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

\[
 u_2 = \left[ \frac{x_2}{v_{22}} \right] = \left[ \frac{100}{101} x_2 \right]
\]

and

\[
 u_1 = \left[ \frac{x_1 - \left\{ \frac{u_2v_{21}}{v_{11}} \right\}}{v_{11}} - \left\{ \frac{u_2v_{21}}{v_{11}} \right\} \right] = \left[ \frac{100}{101} x_2 \right] - \left[ \frac{100}{101} \frac{311}{1000} \right].
\]

Consider, for example, $x = (1, 1)$, then \( \left\{ \left[ \frac{100}{101} x_2 \right] \frac{311}{1000} \right\} = \frac{311}{1000} = \frac{s}{q} \). In this case, node 1 must send the largest integer $s_1$ in the range \{0, 1, \ldots, 999\} for which \( x_1 - \frac{s_1}{q_1} = [x_1] \) 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 \((a, b), a^2 + b^2 = 1, \text{ with } a = 1/m, \text{ and integer } m \geq 2\). The sum rate is seen to peak at $a = 1/6$. Consider the case where $m = 991$. Note that $u_2 = \left\lfloor \frac{x_2}{b} \right\rfloor$ and $u_1 = \left\lfloor x_1 - au_2 \right\rfloor$. The scaled fractional interference term $m\{au_2\}$ takes values in $S = \{0, 1, 2, 3, 988, 989, 990\}$ 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 analyze $P_e$ for the uniform case. The Gaussian case is presented
in a later section. 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 [27].

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 becomes 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.

A. Special Bases: Minkowski and Obtuse Superbase

A basis $\{v_1, v_2, \ldots, v_n\}$ of a lattice $\Lambda \subset \mathbb{R}^n$ is said to be Minkowski-reduced if $v_j$, $j = 1, \ldots, n$, is such that $\|v_j\| \leq \|v\|$, for any $v$ such that $\{v_1, \ldots, v_{j-1}, v\}$ can be extended to a basis of $\Lambda$.

Theorem 3. [7] (Minkowski-reduced basis from Gram matrix) Consider the Gram matrix $A$ of a lattice $\Lambda$. The inequalities from Eq. (13), Eqs. (13)–(14) and Eqs. (13)–(15) below define a Minkowski-reduced basis for dimensions 1, 2 and 3, respectively.

\begin{align}
0 < a_{11} & \leq a_{22} \leq a_{33} \\
2|a_{st}| & \leq a_{ss} \quad (s < t) \\
2|a_{rs} \pm a_{rt} \pm a_{st}| & \leq a_{rr} + a_{ss} \quad (r < s < t).
\end{align}

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 $\theta$ be the angle between $(1, 0)$ and $(a, b)$. Then
besides the basis vectors, a third relevant vector is
\[
\begin{cases}
(-1 + a, b), & \text{if } \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2} \\
(1 + a, b), & \text{if } \frac{\pi}{2} < \theta \leq \frac{2\pi}{3}.
\end{cases}
\]

(16)

In dimension two, the characterization \cite{7} for a Minkowski-reduced basis is the following: a lattice basis \( \{v_1, v_2\} \) is Minkowski-reduced if only if \( \|v_1\| \leq \|v_2\| \) and \[2|v_1 \cdot v_2| \leq \|v_1\|^2\]. Consequently, the angle \( \theta \) between \( v_1 \) and \( v_2 \) is such that \( \frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3} \).

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

Let \( \{v_1, v_2, \ldots, v_n\} \) be a basis for a lattice \( \Lambda \subset \mathbb{R}^n \). A superbasis \( \{v_0, v_1, \ldots, v_n\} \) with \( v_0 = -\sum_{i=1}^{n} v_i \), is said to be obtuse if \( p_{ij} = v_i \cdot v_j \leq 0 \), for \( i, j = 0, \ldots, n, \ i \neq j \). A lattice \( \Lambda \) is said to be of Voronoi’s first kind if it has an obtuse superbasis. The existence of an obtuse superbasis allows a characterization of the relevant Voronoi vectors of a lattice \cite{8, Th.3, Sec. 2}, which are of the form \( \sum_{i \in S} v_i \), where \( S \) is a strict non-empty subset of \( \{0, 1, \ldots, n\} \).

It was demonstrated \cite{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 superbasis, since \( v_0 = -v_1 - v_2 - v_3 \), all Voronoi vectors can be written as one of the following seven vectors or their negatives:

\[ v_1, v_2, v_3, v_{12} = v_1 + v_2, v_{13} = v_1 + v_3, v_{23} = v_2 + v_3, v_{123} = v_1 + v_2 + v_3. \]

The Euclidean norm of such vectors \( N(v_1), N(v_2), N(v_3), N(v_{12}), N(v_{13}), N(v_{23}), N(v_{123}) \) are called vonorms and \( p_{ij} = -v_i \cdot v_j \) \((0 \leq i < j \leq 3)\) are denoted as conorms.

**Remark 1.** The Voronoi region of a lattice \( \Lambda \subset \mathbb{R}^n \) with obtuse superbasis \( \{v_0, v_1, v_2, v_3\} \) can be classified \cite{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 only one \( p_{12}, p_{13} \) or \( p_{23} \) is zero and \( p_{0j} \) are nonzero for all \( j = 1, 2, 3 \).
- **hexa-rhombic dodecahedron**, if only one \( p_{12}, p_{13} \) or \( p_{23} = 0 \) and \( p_{0j} = 0 \), for \( j = 1, 2, 3 \).
- **truncated octahedron**, if all \( p_{ij} \) \((0 \leq i < j \leq 3)\) are nonzero.
Indeed, \( \alpha \) (Proof. The case superbase, then a Minkowski-reduced basis can be constructed from it. \{the superbase to guarantee that \{the\} \}

With analogous arguments, we show that \( \alpha \) \( \beta \) \( \gamma \) \( \delta \) \( \epsilon \) \( \zeta \) \( \eta \) \( \theta \) \( \iota \) \( \kappa \) \( \lambda \) \( \mu \) \( \nu \) \( \xi \) \( \omicron \) \( \rho \) \( \sigma \) \( \tau \) \( \upmu \) \( \phi \) \( \chi \) \( \psi \) \( \omega \) \( \Gamma \) \( \Delta \) \( \Theta \) \( \Lambda \) \( \Xi \) \( \Pi \) \( \Sigma \) \( \Upsilon \) \( \Phi \) \( \Psi \) \( \Omega \)

Consider a Minkowski-reduced basis \( \{v_0, v_1, \ldots, v_n\} \) is an obtuse superbase, any permutation of it is also an obtuse superbase. So, we may consider one such that \( p_{01} \leq 0 \) and \( p_{02} \leq 0 \). Indeed, \( p_{01} = v_0 \cdot v_1 = (-v_1 - v_2) \cdot v_1 = -v_1 \cdot v_1 - v_1 \cdot v_2 \leq -2|v_1 \cdot v_2| + |v_1 \cdot v_2| \leq 0 \).

Similarly we have that \( p_{02} \leq 0 \).

\( \Leftarrow \) If \( \{v_0, v_1, v_2\} \) is an obtuse superbase, any permutation of it is also an obtuse superbase. So, we may consider one such that \( |v_1| \leq |v_2| \leq |v_0| \). Then we have that \( 0 < v_1 \cdot v_1 \leq v_2 \cdot v_2 \leq (v_1 + v_2) \cdot (v_1 + v_2) \) and \( v_1 \neq 0 \). From the last inequality, we have that \( -2v_1 \cdot v_2 \leq v_1 \cdot v_1 \Rightarrow 2|v_1 \cdot v_2| \leq v_1 \cdot v_1 \).

For \( n=3 \): \( \Rightarrow \) Consider a Minkowski-reduced basis \( \{v_1, v_2, v_3\} \) such that \( v_1 \cdot v_2 \leq 0, v_1 \cdot v_3 \leq 0 \) and \( v_2 \cdot v_3 \leq 0 \). To check if \( \{v_0, v_1, v_2, v_3\} \) 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

\[
p_{01} = v_0 \cdot v_1 = -v_1 \cdot v_1 - v_1 \cdot v_2 - v_1 \cdot v_3 \leq -v_1 \cdot v_1 + \frac{v_1 \cdot v_1}{2} + \frac{v_1 \cdot v_1}{2} \leq 0.
\]

With analogous arguments, we show that \( p_{02} \leq 0 \) and \( p_{03} \leq 0 \).
To prove the converse, up to a permutation, we may consider an obtuse superbase such that $|v_1| \leq |v_2| \leq |v_3| \leq |v_0|$. This basis will be Minkowski-reduced if we prove conditions (14) and (15) from Th. 3, i.e.,

$$2|v_1 \cdot v_2| \leq v_1 \cdot v_1; \quad 2|v_1 \cdot v_3| \leq v_1 \cdot v_1; \quad 2|v_2 \cdot v_3| \leq v_2 \cdot v_2;$$

$$2|\pm v_1 \cdot v_2 \pm v_1 \cdot v_3 \pm v_2 \cdot v_3| \leq v_1 \cdot v_1 + v_2 \cdot v_2. \quad (17)$$

The inequalities in Eq. (17) are shown similarly to the two dimensional case starting from $v_2 \cdot v_2 \leq (v_1 + v_2) \cdot (v_1 + v_2)$, $v_3 \cdot v_3 \leq (v_1 + v_3) \cdot (v_1 + v_3)$ and $v_3 \cdot v_3 \leq (v_2 + v_3) \cdot (v_2 + v_3)$. Starting from $v_3 \cdot v_3 \leq (v_1 + v_2 + v_3) \cdot (v_1 + v_2 + v_3)$, the inequality in Eq. (18) follows, concluding the proof.

The characteristics of Voronoi vectors of low-dimensional lattices can be found in [19]. 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 [22]. 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 LLL algorithm [18].

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

We consider that a Minkowski-reduced lattice basis, which is also obtuse (Th. 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 Lem. 1 to describe the Voronoi region of $\Lambda$ 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 $\Lambda$, so the relevant vectors that defines the Voronoi region are $\pm (1,0), \pm (a,b)$ and $\pm (-1 - a, -b)$. We will choose for the analysis proposed in Thm. 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 $P_e := \text{Prob} [X_{np} \neq X_{nI}]$ 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 \( \{v_1, v_2\} = \{(1, 0), (a, b)\} \), such that the angle \( \theta \) between \( v_1 \) and \( v_2 \) satisfies \( \frac{\pi}{2} \leq \theta \leq \frac{2\pi}{3} \). The error probability \( P_e \), when the received vector \( x = (x_1, x_2) \in \mathbb{R}^2 \) is uniformly distributed over the Babai cell, is

\[
P_e = F(a, b) = \frac{-a - a^2}{4b^2} = \frac{1 - (1 + 2a)^2}{16b^2}. \tag{19}
\]

**Proof.** We are going to present just the main idea of the proof. A detailed version is available in [4, Thm. 1]. According to Lemma 1, we can find the vertices of the Voronoi cell \( V(0) \), which are: \( \pm \left( \frac{1}{2}, \frac{a^2 + b^2 + a}{2b} \right) \), \( \pm \left( -\frac{1}{2}, \frac{a^2 + b^2 + a}{2b} \right) \) and \( \pm \left( \frac{2a+1}{2}, \frac{-a^2 + b^2 - a}{2} \right) \), while the Babai cell \( B(0) \) has vertices \( (\pm \frac{1}{2}, \pm \frac{b}{2}) \).

![Voronoi cell, Babai cell and three relevant vectors](image)

From Fig. 5, the error probability is calculated as the sum of the areas of four ‘error’ triangles normalized by the area of a Babai cell. The explicit formula for it is \( F(a, b) = \frac{1 - a - a^2}{4b^2} \).

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

\[
0 \leq P_e \leq \frac{1}{12}, \tag{20}
\]

and

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

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

c) 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 7 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 Th. 5. For a fixed \(a\), the error probability increases with \(\Delta_2\), and for a fixed density \(\Delta_2\) 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 \(\Delta_2\), we have that \(F(a, \Delta_2)\) is minimized by \(a = a^*\), where

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

and maximized by \(a = -\frac{1}{2}\), for any \(\Delta_2\). 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 \(\Delta_2\).

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

For the three dimensional case, we developed and implemented an algorithm in the software Wolfram Mathematica, version 12.1 [28] 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 Alg. 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 \( \Lambda \) using the Voronoi vectors (Sec. IV-A). Use \textit{ConvexHullMesh[]} available in Mathematica [28] 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 \textit{ConvexHullMesh[]} to compute the convex hull of these vertices.

**Intersection:** Apply \textit{RegionIntersection[]} in Mathematica [28], to compute \( \mathcal{B}(0) \cap \mathcal{V}(0) \) and its volume normalized by the volume of the lattice.

**Packing density:** Calculate the packing density \( \Delta_3 = \frac{\pi d_{\min}^3(\Lambda)}{6 \cdot \text{vol}(\Lambda)} \).

For lattices with randomly chosen basis, we start by considering a basis at random, with the
format \( \{(1, 0, 0), (a, b, 0), (c, d, e)\} \), where \( a, c \in [-1/2, 0] \) and \( b, d, e \in [-2, 2] \) (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 \( \Lambda \).

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.

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 \( \Lambda_{hp} \) 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 \( \{(1, 0, 0), (-\frac{1}{2}, \frac{2\sqrt{2}}{3}, 0), (-\frac{1}{2}, -\frac{\sqrt{2}}{3}, \sqrt{\frac{2}{3}})\} \), 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 \( \Lambda_{hrd} \) with basis \( \{(1, 0, 0), (-\frac{1}{\sqrt{3}}, \frac{2}{\sqrt{3}}, 0), (0, -\frac{1}{2}, \frac{\sqrt{2}}{2})\} \), 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 to the cell type, i.e., green is an hexagonal prism, purple are hexa-rhombic dodecahedrons, and black represents rhombic dodecahedrons.
TABLE I

PERFORMANCE IN ALGORITHM 1 FOR KNOWN LATTICES

| Lattice/Vorono cell          | Notation 15.6 [7] | $\Delta_3$ | $P_e$  |
|------------------------------|------------------|------------|--------|
| $\mathbb{Z}^3$/ Cuboid       | 111              | 0.5235     | 0      |
| $\Lambda_{hp}$/ Hexagonal prism | 2_{-1}22        | 0.6046     | 0.0833 |
| FCC/ Rhombic dodecahedron    | 2;2;2            | 0.7404     | 0.1505 |
| $\Lambda_{hrd}$/ Hexa-rhombic dodecahedron | 2;3;2          | 0.5235     | 0.1134 |
| BCC/ Truncated octahedron    | 3;3;3;3_{-1}     | 0.6802     | 0.1458 |

D. Some Observations and Analysis of the Data

Let $P_e$ and $\Delta_3$ be the error probability and packing density for a lattice $\Lambda$. Consider the curve $P_e^*(\Delta)$, the lower boundary of the set of points $(\Delta_3, P_e)$ 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 $\Delta$ in the range $[\pi/6, \pi/(3\sqrt{2})]$, 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 is 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], [21], and also for applications such as coding for wiretap Gaussian and fading channels [10], [14].

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 $\beta$ with
\[ \alpha = \pi/2 \] and
\[ \sin \gamma = \begin{cases} 
0, & 0 \leq \beta < \pi/6, \\
\frac{1}{2 \sin \beta}, & \pi/6 \leq \beta \leq \pi/4, 
\end{cases} \tag{21} \]
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.

1) 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 \( \beta \) 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 \( \beta \) values. It is interesting that there is no truly 3 dimensional Voronoi cell that is is able to do better in this range.

2) For \( \pi/6 \leq \beta \leq \pi/4 \), \( \Lambda(\beta) \) has basis \( \{(1, 0, 0), (0, 1, 0), (-\sqrt{17/108}, -1/2, \sqrt{16/27})\} \). 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 \( \beta \) 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 \( \beta \) 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 Tab. 8. Specifically, the lattice with basis \( \{(1, 0, 0), (0, 1, 0), (-\sqrt{17/108}, -1/2, \sqrt{16/27})\} \) has the same volume and consequently 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. An 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 \( \Delta \) 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. Further, no parameterizations of lattices in very large dimensions are known, which makes it difficult to examine the tradeoff between the packing density and the error probability $P_e$. Thus it is more fruitful to obtain bounds using tools from probability theory, when $n$ becomes large.

We first study the error probability under uniform probability distributions in Sec. V-A and under Gaussian distributions in Sec. V-B.

A. Uniform Distributions

We need a few definitions. Let $S(r)$ 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 hyperrectangle with sides of length $a_i > 0$, $i = 1, 2, \ldots, n$ and we say that the Babai cell has size $a = (a_1, a_2, \ldots, a_n) = (|v_{11}|, |v_{22}|, \ldots, |v_{nn}|)$, where $V$ is the upper triangular generator matrix of $\Lambda$.

Note that in this section we primarily work with $P_c = 1 - P_e$.

**Theorem 6.** (A Chebyshev Bound) Suppose lattice $\Lambda \subset \mathbb{R}^n$ has covering radius $r_{\text{cov}}$, a Babai cell of size $a = (a_1, a_2, \ldots, a_n)$, and satisfies

$$\frac{1}{12} \sum_{i=1}^{n} a_i^2 > r_{\text{cov}}^2. \quad (22)$$

Then, for the uniformly distributed case,

$$P_e = \text{Prob}(X \in \mathcal{V}(0) ) \cap \mathcal{B}(0)|X \in \mathcal{V}(0) ) \leq \frac{1}{180n^2} \sum_{i=1}^{n} a_i^4 \delta^2 \quad (23)$$

where $\delta = \frac{1}{n} \left( \frac{1}{12} \sum_{i=1}^{n} a_i^2 - r_{\text{cov}}^2 \right)$.

**Proof.** Note that $\text{Var} X_i = a_i^2/12$ and the $X_i$ are mutually independent. Let $\mu = (1/12n) \sum_{i=1}^{n} a_i^2$. It follows that the event

$$\{X \in S(r_{\text{cov}})\} = \left\{ \frac{1}{n} \sum_{i=1}^{n} X_i^2 \leq \frac{r_{\text{cov}}^2}{n} \right\} \subset \left\{ \left| \frac{1}{n} \sum_{i=1}^{n} X_i^2 - \mu \right| > \mu - \frac{r_{\text{cov}}^2}{n\delta} \right\}. \quad (24)$$

Since $\text{Var}(X_i^2) = E[X_i^4] - E[X_i^2]^2 = a_i^4/180$, it follows by an application of the Chebyshev inequality that

$$\text{Prob}(X \in \mathcal{V}(0) ) \leq \text{Prob} \{X \in S(r_{\text{cov}})\} \leq \frac{\text{Var}((1/n) \sum_{i=1}^{n} X_i^2)}{\delta^2} = \frac{\sum_{i=1}^{n} a_i^4}{180n^2\delta^2}. \quad (25)$$
As an application of the theorem, consider the Barnes-Wall lattice $\Lambda_{16} \subset \mathbb{R}^{16}$ whose generator matrix is given in Fig. 4.10 [7]. From the generator matrix which is in lower triangular form, the Babai cell has size $\left(4, 2^{(10)}, 1^{(5)}\right)$ and the covering radius is known to be $\sqrt{3}$ [7]. An application of the above theorem gives $\text{Prob}(X \in \mathcal{V}(0)) \leq 0.539$. For the Leech lattice $\Lambda_{24}$, the size of the Babai cell is $\left(8, 4^{(11)}, 2^{(11)}, 1\right)$ and the covering radius is $\sqrt{2}$ which gives $\text{Prob}(X \in \mathcal{V}(0)) \leq 0.0833$.

We also note that the theorem cannot be used for the lattice $E_8$, using the generator matrix given in [7], since the condition (22) is not satisfied.

Unfortunately, the method does not apply to the family of lattices $A_n$, $A_n$ 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 [16]. From this fact, we can determine the size of the Babai cell, i.e., the numbers $a_1, \ldots, a_n$, 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, we get that the $k$-th side of the Babai cell is

$$a_{k} = \sqrt{\frac{k+1}{k}},$$

for any $k = 1, \ldots, n$. Observe that the condition from Eq. (22) is not satisfied for this lattice. Indeed,

$$\frac{1}{12} \sum_{i=1}^{n} a_i^2 = \frac{1}{12} \sum_{i=1}^{n} \left(1 + \frac{1}{i}\right), \quad (26)$$

and $r_{\text{cov}} = \frac{1}{\sqrt{2}} \left(\frac{2 \cdot \left\lfloor \frac{n+1}{2} \right\rfloor}{n+1} \left(n+1-\left\lfloor \frac{n+1}{2} \right\rfloor\right)\right)^{1/2}$ [7, p. 109]. By considering the approximation for partial finite sum of the harmonic series together with Eq. (26), it is valid that

$$\frac{1}{12} \sum_{i=1}^{n} \left(1 + \frac{1}{i}\right) \approx \frac{1}{12} (n + \log(n) + 1) < r_{\text{cov}}^2, \quad \text{for all } n. \quad (27)$$

**Theorem 7. (Exclusion Bound)** For a lattice $\Lambda$ with covering radius is $r_{\text{cov}}$, suppose that a Babai cell has size $a = (a_1, a_2, \ldots, a_n)$ which satisfies $a_1 \geq a_2 \geq \ldots \geq a_m > 2r_{\text{cov}} \geq a_{m+1} \geq \ldots a_n$. Then

$$P_c = \text{Prob}(X \in \mathcal{V}(0) \cap \mathcal{B}(0) | X \in \mathcal{V}(0)) \leq \frac{(2r_{\text{cov}})^m}{\prod_{i=1}^{m} a_i}. \quad (28)$$

When $m = 0$, the bound is unity.

**Proof.** Without loss of generality assume that $\det \Lambda = 1$. The idea is to cut off parts of the Babai rectangle which are outside the sphere $S(r_{\text{cov}})$, starting with cutting planes $\pm r_{\text{cov}} e_1 \in \mathbb{R}^n$,
where \( e_1 = (1, 0, \ldots, 0) \). After the \( i \)th pair of cuts \( \pm r_{\text{cov}} e_i \), we are left with a smaller rectangle of size \( (r_{\text{cov}}, \ldots, r_{\text{cov}}, a_{i+1}, \ldots, a_n) \) which intersects \( S(r_{\text{cov}}) \). We stop after the \( m \)th pair of cuts, for then every face of the remaining rectangle intersects the interior of \( S(r_{\text{cov}}) \). The volume of the remaining rectangle is the desired upper bound on the probability. Thus

\[
P_e \leq (2r_{\text{cov}})^m a_{m+1} \ldots a_n = \frac{(2r_{\text{cov}})^m}{a_1 a_2 \ldots a_m},
\]

where in the last step we have used \( a_1 a_2 \ldots a_n = \det \Lambda = 1 \).

For the Barnes-Wall \( \Lambda_{16} \) and Leech \( \Lambda_{24} \) lattices, the corresponding values of \( P_e \) are 0.866 and 0.0078 respectively. Similar to the Chebyshev bound, the Exclusion bound gives only a trivial result for the lattice \( E_8 \).

In fact the two bounds can sometimes be combined.

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

\[
P_e \leq \frac{(2r_{\text{cov}})^m}{\prod_{i=1}^{m} a_i} \left( \frac{m(2r_{\text{cov}})^4 + \sum_{i=m+1}^{n} a_i^4}{180 n^2 \delta_1^2} \right).
\]

**Proof.** Direct application of the Exclusion bound followed by the Chebyshev bound.

For the Barnes-Wall lattice and the Leech lattice this gives \( \text{Prob}(X \in V(0)) \leq 0.4854 \) and \( \text{Prob}(X \in V(0)) \leq 4.314 \times 10^{-4} \), respectively.

**B. Gaussian Distribution**

We now analyze the Gaussian case, as described in Sec. II-A for which \( P_e \) is given by (2). 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 \( \sigma^2 \) is presented in Fig. 9 (this is the counterpart of Fig. 7 for the Gaussian case). For a two dimensional lattice \( \Lambda \) with basis \( \{(1, 0), (a, b)\} \), we have calculated the term \( T \) in (2), 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 \( \sigma^2 \) and fixed \( b \), \( P_e(\sigma^2, a, b) \) is decreasing with \( a \). Thus, the same minimization for the parameter \( a \) done in Remark 2 applies here. It is straightforward to conclude that smaller variance provides smaller error probability.
Now, consider a lattice $\Lambda \subset \mathbb{R}^n$, with $n$ large and its Voronoi cell $\mathcal{V}$. The largest radius among the radii of inscribed spheres in the Voronoi region $\mathcal{V}$ is the packing radius $r_{\text{pack}}$. Given that $Z \sim \mathcal{N}(0, \sigma^2 I)$, we are interested in calculating $\text{Prob} \left[ Z \in \mathcal{V}(0) \cap B(0) \right]$. Thus

$$\text{Prob} \left[ Z \in \mathcal{V}(0) \cap B(0) \right] \geq \text{Prob} \left[ Z \in S(r_{\text{pack}}) \cap B(0) \right],$$

where recall that $S(r)$ denotes the $n-$dimensional ball centered at zero with radius $r$.

The following theorem provides a condition on $\sigma$ under which $P_c \to 1$ as $n \to \infty$.

**Theorem 8.** *(Condition on $\sigma^2$ for success probability)* $\text{Prob} \left[ Z \in \mathcal{V}(0) \cap B(0) \right] \to 1$ as $n \to \infty$ for all $\sigma^2 < \frac{\text{vol}(\Lambda)^2/n}{4}$, if $r_{\text{pack}} \leq \frac{|a_i|}{2}$, for all $i = 1, \ldots, n$, where $a_i$ are the sizes of the Babai cell.

**Proof.** This follows from

$$\text{Prob}(||Z|| < r_{\text{pack}}) = \chi^2_{CDF} \left( \frac{r_{\text{pack}}^2}{\sigma^2}; n \right),$$

where $\chi^2_{CDF}(x; k)$ stands for the cumulative chi-squared distribution function with $k$ degrees of freedom. For $\chi^2_{CDF}(zn; n)$, if we take $z = \frac{r_{\text{pack}}^2}{\sigma^2 n}$, it is valid for large $n$, according to Corollary 7.2.2 [29, p. 145] that

$$\chi^2_{CDF}(zn; n) \approx \begin{cases} 1, & z > 1 \\ 0, & z < 1 \end{cases}.$$
Since we want $\Pr[Z \in S(r_{\text{pack}})] \to 1$ we must have that $z > 1 \Rightarrow z = \frac{r_{\text{pack}}^2}{\sigma^2 n} > 1 \Rightarrow \sigma^2 < \frac{r_{\text{pack}}^2}{n} = \frac{d_{\min}^2(\Lambda)}{4n} = \frac{||\Lambda||^2_2}{4n},$

where $d_{\min}(\Lambda)$ is the minimum distance among all lattice points and $\lambda = \inf\{||x||_2 : x \in \Lambda \setminus \{0\}\}.$

Recall that from Minkowski theorem [5], one can upper bound the Euclidean norm of the shortest vector in a given lattice $\Lambda$ by $\sqrt{n} \text{vol}(\Lambda)^{1/n}$. Thus,

$$\sigma^2 < \frac{||\lambda||^2_2}{4n} \leq \frac{\left(\sqrt{n} \text{vol}(\Lambda)^{1/n}\right)^2}{4n} = \frac{\text{vol}(\Lambda)^{2/n}}{4}.$$

Therefore, due to the fact that $r_{\text{pack}} \leq \frac{|a_i|}{2},$ for all $i$, where $a_i$ denotes the sizes of the Babai cell, then for values of $\sigma^2 < \frac{\text{vol}(\Lambda)^{2/n}}{4},$ we can guarantee that $\Pr[Z \in \mathcal{V}(0) \cap \mathcal{B}(0)] \geq \Pr[Z \in S(r_{\text{pack}})] \to 1$ as $n \to \infty$.

Thm. 8 states that if the variance $\sigma^2$ satisfies the proposed condition, then estimating the Babai point is enough to guarantee the correct solution for the nearest lattice point problem. In particular, examples where the hypothesis of Thm. 8 are satisfied includes the cubic lattice $\mathbb{Z}^n$ or rectangular lattices and we reach an analogous conclusion to the uniform case, i.e., that the error probability is vanishing for cubic (and rectangular) lattices.

VI. CONCLUSIONS AND FUTURE WORK

We have considered the problem of finding an approximate nearest point in a given lattice $\Lambda$ to $x \in \mathbb{R}^n$ in a distributed network. We assumed that each component of the vector $x$ 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 is presented, its communication rate is determined, and is shown to be optimal when the components of $X$ are mutually independent. We then consider the problem of evaluating the error probability, namely, the probability that the approximate nearest lattice point does not coincide with the nearest lattice point. Closed form expressions for the error probability are derived in two dimensions. For the three dimensional case, using an obtuse superbase, we have estimated computationally for random lattices the worst error probability. For dimensions greater than 3, we have obtained bounds for the error probability. Our results show that the error probability becomes larger as the packing density of the lattice becomes larger. When the vector $x$ is uniformly distributed
over a certain region, it will be necessary to send extra bits to compute the nearest lattice point. However, when \( x \) is obtained by the addition of Gaussian noise of sufficiently small variance to a lattice point, no further communication will be necessary.

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 reviewers of a previous draft 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] S.D. Galbraith, *Mathematics of Public Key Cryptography*. New York, NY: Cambridge University Press, 2012.

[14] O. W. Gnifeke, 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.

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

[16] M. Kim and J. Peters, “Symmetric Box-splines on the \( \mathbb{A}^n \) Lattice”, *J. of Approx. Th.*, vol. 162, no. 9, pp. 1607-1630, Sep. 1997.
[17] 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.

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

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

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

[21] C. T. McMullen, “Minkowski’s Conjecture, Well-Rounded Lattices and Topological Dimension”, *J. Amer. Math. Soc.*, vol. 18, no. 3, pp. 711-735, Mar. 2005.

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

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

[24] C. Peikert. “A Decade of Lattice Cryptography”, 2016.

[25] V. A. Vaishampayan, “Precoder Design for Distributed MIMO Receivers with Controlled Peak-Average Power Ratio,” submitted.

[26] 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.

[27] 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.

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

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