SIAM J. DISCRETE MATH.
Vol. 21, No. 1, pp. 199–219

ON NEARLY ORTHOGONAL LATTICE BASES AND RANDOM LATTICES*

RAMESH NEELAMANI†, SANJEEB DASH‡, AND RICHARD G. BARANIUK§

Abstract. We study lattice bases where the angle between any basis vector and the linear subspace spanned by the other basis vectors is at least $\frac{\pi}{3}$ radians; we denote such bases as "nearly orthogonal." We show that a nearly orthogonal lattice basis always contains a shortest lattice vector. Moreover, we prove that if the basis vector lengths are "nearly equal," then the basis is the unique nearly orthogonal lattice basis up to multiplication of basis vectors by ± 1. We also study random lattices generated by the columns of random matrices with n rows and $m \leq n$ columns. We show that if $m \leq c\,n$, with $c \approx 0.071$, then the random matrix forms a nearly orthogonal basis for the random lattice with high probability for large n and almost surely as n tends to infinity. Consequently, the columns of such a random matrix contain the shortest vector in the random lattice. Finally, we discuss an interesting JPEG image compression application where nearly orthogonal lattice bases play an important role.

Key words. lattices, shortest lattice vector, random lattice, JPEG, compression

AMS subject classifications. 03G10, 15A52, 94A08

DOI. 10.1137/050635985

1. Introduction.

Lattices are regular arrangements of points in space that are studied in numerous fields, including coding theory, number theory, and cryptography [1, 15, 17, 21, 25]. Formally, a lattice $\mathcal{L}$ in $\mathbb{R}^n$ is the set of all linear integer combinations of a finite set of vectors; that is, $\mathcal{L} = \{u_1 b_1 + u_2 b_2 + \cdots + u_m b_m \,|\, u_i \in Z\}$ for some $b_1, b_2, \ldots, b_m$ in $\mathbb{R}^n$. The set of vectors $\mathcal{B} = \{b_1, b_2, \ldots, b_m\}$ is said to *span* the lattice $\mathcal{L}$. An independent set of vectors that spans $\mathcal{L}$ is a *basis* of $\mathcal{L}$. A lattice is said to be m-dimensional (m-D) if a basis contains m vectors.

In this paper we study the properties of lattice bases whose vectors are "nearly orthogonal" to one another. We define a basis to be θ-orthogonal if the angle between any basis vector and the linear subspace spanned by the remaining basis vectors is at least θ. A θ-orthogonal basis is deemed to be *nearly orthogonal* if θ is at least $\frac{\pi}{3}$ radians.

We derive two simple but appealing properties of nearly orthogonal lattice bases.

1. A $\frac{\pi}{3}$-orthogonal basis always contains a shortest nonzero lattice vector.
2. If all vectors of a θ-orthogonal ($\theta > \frac{\pi}{3}$) basis have lengths less than $\frac{\sqrt{3}}{\sin\theta + \sqrt{3}\cos\theta}$ times the length of the shortest basis vector, then the basis is the unique $\frac{\pi}{3}$-orthogonal basis for the lattice (up to multiplication of basis vectors by ± 1).

Gauss [13] proved the first property for two-dimensional (2-D) lattices. We prove (generalizations of) the above properties for m-D lattices for arbitrary m.

We also study lattices generated by a set of random vectors; we focus on vectors comprising Gaussian or Bernoulli ($\pm\frac{1}{\sqrt{n}}$) entries. The set of vectors and the generated

*Received by the editors July 14, 2005; accepted for publication (in revised form) October 9, 2006; published electronically March 15, 2007. A part of this work was supported by grants from NSF, AFOSR, ONR, DARPA, and the Texas Instruments Leadership Universities program.
http://www.siam.org/journals/sidma/21-1/63598.html
†ExxonMobil Upstream Research Company, Houston, TX 77027 (ramesh.neelamani@exxonmobil.com).
‡IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 (sanjeebd@us.ibm.com).
§Department of Electrical and Computer Engineering, Rice University, Houston, TX 77005 (richb@rice.edu).

lattice are henceforth referred to as a *random basis* and a *random lattice*, respectively. Random bases and lattices find applications in coding [7] and cryptography [28]. We prove an appealing property of random lattices.

> *If a random lattice $\mathcal{L}$ in $\mathbb{R}^n$ is generated by $m \leq c\,n$ ($c \approx 0.071$) random vectors, then the random vectors form a $\frac{\pi}{3}$-orthogonal basis of $\mathcal{L}$ with high probability at finite n and* almost surely *as $n \to \infty$.*

Consequently, the shortest vector in $\mathcal{L}$ is contained by the random basis with high probability.

We also exploit properties of nearly orthogonal bases to solve an interesting digital image processing problem. Digital color images are routinely subjected to compression schemes such as the JPEG standard [26]. The various settings used during JPEG compression of an image—termed as the image's JPEG compression history—are often discarded after decompression. For recompression of images which were earlier in JPEG-compressed form, it is useful to estimate the discarded compression history from their current representation. We call this problem JPEG compression history estimation (CHEst). The JPEG compression step maps a color image into a set of points contained in a collection of related lattices [23]. We show that the JPEG CHEst problem can be solved by estimating the nearly orthogonal bases spanning these lattices. Then, we invoke the derived properties of nearly orthogonal bases in a heuristic to solve the JPEG CHEst problem [23].

Lattices that contain nearly orthogonal bases are somewhat special[1] because there exist lattices without any $\frac{\pi}{3}$-orthogonal basis (see (4) for an example). Consequently, the new properties of nearly orthogonal lattice bases in this paper cannot be exploited in all lattice problems.

This paper is organized as follows. Section 2 provides some basic definitions and well-known results about lattices. Section 3 formally states our results on nearly orthogonal lattice bases, and section 4 furnishes the proofs for the results in section 3. Section 5 identifies new properties of random lattices. Section 6 describes the role of nearly orthogonal bases in solving the JPEG CHEst problem. Section 7 discusses some limitations of our results and future research directions.

2. Lattices. Consider an m-D lattice $\mathcal{L}$ in $\mathbb{R}^n$, $m \leq n$. By an *ordered basis* for $\mathcal{L}$, we mean a basis with a certain ordering of the basis vectors. We represent an ordered basis by an ordered set and also by a matrix whose columns define the basis vectors and their ordering. We use the braces $(.,.)$ for ordered sets (for example, $(b_1, b_2, \ldots, b_m)$) and $\{.,.\}$ otherwise (for example, $\{b_1, b_2, \ldots, b_m\}$). For vectors $u, v \in \mathbb{R}^n$, we use both $u^T v$ (with T denoting matrix or vector transpose) and $\langle u, v \rangle$ to denote the inner product of u and v. We denote the Euclidean norm of a vector v in $\mathbb{R}^n$ by $\|v\|$.

Any two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of $\mathcal{L}$ are related (when treated as $n \times m$ matrices) as $\mathcal{B}_1 = \mathcal{B}_2 \mathcal{U}$, where $\mathcal{U}$ is a $m \times m$ *unimodular matrix*; that is, $\mathcal{U}$ is an integer matrix with determinant equal to ± 1.

The *closest vector problem* (CVP) and the *shortest vector problem* (SVP) are two closely related fundamental lattice problems [1, 2, 10, 15]. Given a lattice $\mathcal{L}$ and an input vector (not necessarily in $\mathcal{L}$), CVP aims to find a vector in $\mathcal{L}$ that is closest (in the Euclidean sense) to the input vector. Even finding approximate CVP solutions is known to be NP-hard [10]. The SVP seeks a vector in $\mathcal{L}$ with the shortest (in the Euclidean sense) nonzero length $\lambda(\mathcal{L})$. The decision version of SVP is not known

[1] However, our random basis results suggest nearly orthogonal bases occur frequently in low-dimensional lattices.

to be NP-complete in the traditional sense, but SVP is NP-hard under randomized reductions [2]. In fact, even finding approximately shortest vectors (to within any constant factor) is NP-hard under randomized reductions [16, 20].

A shortest lattice vector is always contained by orthogonal bases. Hence, one approach to finding short vectors in lattices is to obtain a basis that is close (in some sense) to orthogonal and use the shortest vector in such a basis as an approximate solution to the SVP. A commonly used measure to quantify the "orthogonality" of a lattice basis $\{b_1, b_2, \ldots, b_m\}$ is its *orthogonality defect* [17]:

$$\frac{\prod_{i=1}^{m} \|b_i\|}{|\det([b_1, b_2, \ldots, b_m])|},$$

with det denoting the determinant. For rational lattices (lattices comprising rational vectors), the Lovász basis reduction algorithm [17], often called the LLL algorithm, obtains an *LLL-reduced* lattice basis in polynomial time. Such a basis has a small orthogonality defect. There exist other notions of reduced bases due to Minkowski and to Korkine and Zolotarev (KZ) [15]. Both Minkowski-reduced and KZ-reduced bases contain the shortest lattice vector, but it is NP-hard to obtain such bases.

We choose to quantify a basis's closeness to orthogonality in terms of the following new measures.

- *Weak θ-orthogonality:* An *ordered* set of vectors $(b_1, b_2, \ldots, b_m)$ is weakly θ-orthogonal if for $i = 2, 3, \ldots, m$, the angle between b_i and the subspace spanned by $\{b_1, b_2, \ldots, b_{i-1}\}$ lies in the range $\left[\theta, \frac{\pi}{2}\right]$. That is,

$$\cos^{-1}\left(\frac{|\langle b_i, \sum_{j=1}^{i-1} \alpha_i\, b_i\rangle|}{\|b_i\| \left\|\sum_{j=1}^{i-1} \alpha_i\, b_i\rangle\right\|}\right) \geq \theta \text{ for all } \alpha_j \in \mathbb{R} \text{ with } \sum_j |\alpha_j| > 0. \tag{1}$$

- *θ-orthogonality:* A set of vectors $\{b_1, b_2, \ldots, b_m\}$ is θ-orthogonal if every ordering of the vectors yields a weakly θ-orthogonal set.

A (weakly) θ-orthogonal basis is one whose vectors are (weakly) θ-orthogonal. Babai [4] proved that an n-D LLL-reduced basis is θ-orthogonal where $\sin\theta = (\sqrt{2}/3)^n$; for large n, this value of θ is very small. Thus the notion of an LLL-reduced basis is quite different from that of a weakly $\frac{\pi}{3}$-orthogonal basis.

We will encounter θ-orthogonal bases in random lattices in section 5 and weakly θ-orthogonal bases (with $\theta \geq \frac{\pi}{3}$) in the JPEG CHEst application in section 6.

3. Nearly orthogonal bases: Results. This section formally states the two properties of nearly orthogonal lattice bases that were identified in the introduction. We also identify an additional property characterizing unimodular matrices that relate two nearly orthogonal bases; this property is particularly useful for the JPEG CHEst application.

Obviously, in an orthogonal lattice basis, the shortest basis vector is a shortest lattice vector. More generally, given a lattice basis $\{b_1, b_2, \ldots, b_m\}$, let θ_i be the angle between b_i and the subspace spanned by the other basis vectors. Then

$$\lambda(\mathcal{L}) \geq \min_{i \in \{1,2,\ldots,m\}} \|b_i\| \sin\theta_i. \tag{2}$$

Therefore, a θ-orthogonal basis has a basis vector whose length is no more than $\lambda(\mathcal{L}) / \sin\theta$; if $\theta = \frac{\pi}{3}$, this bound becomes $\frac{2\,\lambda(\mathcal{L})}{\sqrt{3}}$. This shows that nearly orthogonal lattice bases contain short vectors.

Gauss proved that in $\mathbb{R}^2$ every $\frac{\pi}{3}$-orthogonal lattice basis indeed contains a shortest lattice vector and provided a polynomial time algorithm to determine such a basis in a rational lattice; see [32] for a nice description. We first show that Gauss's shortest lattice vector result can be extended to higher-dimensional lattices.

THEOREM 1. *Let $\mathcal{B} = (b_1, b_2, \ldots, b_m)$ be an ordered basis of a lattice $\mathcal{L}$. If $\mathcal{B}$ is weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal for $0 \leq \epsilon \leq \frac{\pi}{6}$, then a shortest vector in $\mathcal{B}$ is a shortest nonzero vector in $\mathcal{L}$. More generally,*

$$\min_{j \in \{1,2,\ldots,m\}} \|b_j\| \leq \left\| \sum_{i=1}^{m} u_i b_i \right\| \qquad \text{for all } u_i \in \mathbb{Z} \text{ with } \sum_{i=1}^{m} |u_i| \geq 1, \tag{3}$$

with equality possible only if $\epsilon = 0$ or $\sum_{i=1}^{m} |u_i| = 1$.

COROLLARY 1. *If $0 < \epsilon \leq \frac{\pi}{6}$, then a weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis contains every shortest nonzero lattice vector (up to multiplication by ± 1).*

Theorem 1 asserts that a θ-orthogonal lattice basis is guaranteed to contain a shortest lattice vector if $\theta \geq \frac{\pi}{3}$. In fact, the bound $\frac{\pi}{3}$ is tight because, for any $\epsilon > 0$, there exist lattices where some θ-orthogonal basis, with $\theta = \frac{\pi}{3} - \epsilon$, does not contain the shortest lattice vector. For example, consider a lattice in $\mathbb{R}^2$ defined by the basis $\{b_1, b_2\}$, with $\|b_1\| = \|b_2\| = 1$, and the angle between them equal to $\frac{\pi}{3} - \epsilon$. Obviously $b_2 - b_1$ has length less than 1.

For a rational lattice defined by some basis $\mathcal{B}_1$, a weakly $\frac{\pi}{3}$-orthogonal basis $\mathcal{B}_2 = \mathcal{B}_1 \mathcal{U}$, with $\mathcal{U}$ polynomially bounded in size, provides a polynomial-size certificate for $\lambda(\mathcal{L})$. However, we do not expect all rational lattices to have such bases because this would imply that NP=co-NP, assuming SVP is NP-complete. For example, the lattice $\mathcal{L}$ spanned by the basis

$$\mathcal{B} = \begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{4}$$

does not have any weakly $\frac{\pi}{3}$-orthogonal basis. It is not difficult to verify that $[1\ 0\ 0]^T$ is a shortest lattice vector. Thus, $\lambda(\mathcal{L}) = 1$. Now, assume that $\mathcal{L}$ possesses a weakly $\frac{\pi}{3}$-orthogonal basis $\widetilde{\mathcal{B}} = (b_1, b_2, b_3)$. Let θ_1 be the angle between b_2 and b_1, and let θ_2 be the angle between b_3 and the subspace spanned by b_1 and b_2. Since b_1, b_2, and b_3 have length at least 1,

$$\det(\widetilde{\mathcal{B}}) = \|b_1\| \, \|b_2\| \, \|b_3\| \, |\sin\theta_1| \, |\sin\theta_2| \geq \sin^2 \frac{\pi}{3} = \frac{3}{4}. \tag{5}$$

But $\det(\mathcal{B}) = \frac{1}{\sqrt{2}} < \det(\widetilde{\mathcal{B}})$, which shows that the lattice $\mathcal{L}$ with basis $\mathcal{B}$ in (4) has no weakly $\frac{\pi}{3}$-orthogonal basis.

Our second observation describes the conditions under which a lattice contains the unique (modulo permutations and sign changes) set of nearly orthogonal lattice basis vectors.

THEOREM 2. *Let $\mathcal{B} = (b_1, b_2, \ldots, b_m)$ be a weakly θ-orthogonal basis for a lattice $\mathcal{L}$ with $\theta > \frac{\pi}{3}$. For all $i \in \{1, 2, \ldots, m\}$, if*

$$\|b_i\| < \eta(\theta) \min_{j \in \{1,2,\ldots,m\}} \|b_j\|, \tag{6}$$

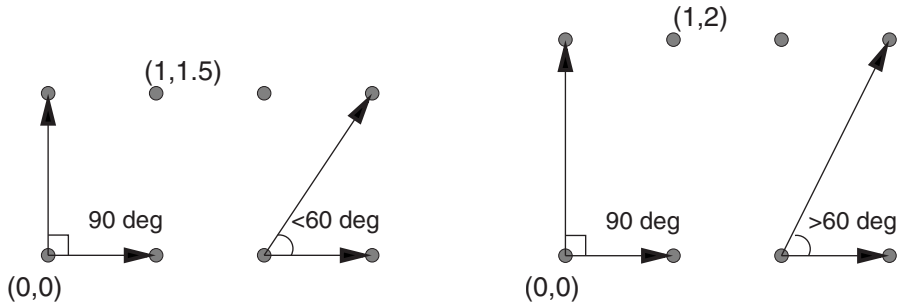


FIG. 1. (a) *The vectors comprising the lattice are denoted by circles. One of the lattice bases comprises two orthogonal vectors of lengths* 1 *and* 1.5. *Since* $1.5 < \eta(\frac{\pi}{2}) = \sqrt{3}$, *the lattice possesses no other basis such that the angle between its vectors is at least* $\frac{\pi}{3}$ *radians.* (b) *This lattice contains at least two* $\frac{\pi}{3}$*-orthogonal bases. One of the lattice bases comprises two orthogonal vectors of lengths* 1 *and* 2. *Here* $2 > \eta(\frac{\pi}{2})$, *and this basis is not the only* $\frac{\pi}{3}$*-orthogonal basis.*

$$\text{with } \eta(\theta) = \frac{\sqrt{3}}{\sin\theta + \sqrt{3}\cos\theta}, \tag{7}$$

then any $\frac{\pi}{3}$*-orthogonal basis comprises the vectors in* $\mathcal{B}$ *multiplied by* ± 1.

In other words, a nearly orthogonal basis is essentially unique when the lengths of its basis vectors are nearly equal. For example, both Figures 1(a) and 1(b) illustrate 2-D lattices that can be spanned by orthogonal basis vectors. For the lattice in Figure 1(a), the ratio of the lengths of the basis vectors is less than $\eta\left(\frac{\pi}{2}\right) = \sqrt{3}$. Hence, there exists only one (modulo sign changes) basis such that the angle between the vectors is greater than $\frac{\pi}{3}$. In contrast, the lattice in Figure 1(b) contains many distinct $\frac{\pi}{3}$-orthogonal bases.

In the JPEG CHEst application [23], the target three-dimensional (3-D) lattice bases in $\mathbb{R}^3$ are known to be weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal but not $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal. Theorem 2 addresses the uniqueness of $\frac{\pi}{3}$-orthogonal bases but not weakly $\frac{\pi}{3}$-orthogonal bases. To estimate the target lattice basis, we need to understand how different weakly orthogonal bases are related. The following theorem guarantees that for 3-D lattices a weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis with nearly equal-length basis vectors is related to every weakly orthogonal basis by a unimodular matrix with small entries.

THEOREM 3. *Let* $\mathcal{B} = (b_1, b_2, \ldots, b_m)$ *and* $\widetilde{\mathcal{B}}$ *be two weakly* θ*-orthogonal bases for a lattice* $\mathcal{L}$, *where* $\theta > \frac{\pi}{3}$. *Let* $\mathcal{U} = (u_{ij})$ *be a unimodular matrix such that* $\mathcal{B} = \widetilde{\mathcal{B}}\mathcal{U}$. *Define*

$$\kappa(\mathcal{B}) = \left(\frac{2}{\sqrt{3}}\right)^{m-1} \times \frac{\max_{i\in\{1,2,\ldots,m\}} \|b_i\|}{\min_{i\in\{1,2,\ldots,m\}} \|b_i\|}. \tag{8}$$

Then, $|u_{ij}| \le \kappa(\mathcal{B})$ *for all* i *and* j.

For example, if $\mathcal{B}$ is a weakly θ-orthogonal basis of a 3-D lattice with $\frac{\max_{i\in\{1,2,3\}}\|b_i\|}{\min_{i\in\{1,2,3\}}\|b_i\|} < 1.5$, then the entries of the unimodular matrix relating another weakly θ-orthogonal basis $\widetilde{\mathcal{B}}$ to $\mathcal{B}$ are either 0 or ± 1.

4. Nearly orthogonal bases: Proofs.

4.1. Proof of Theorem 1. We first prove Theorem 1 for 2-D lattices (Gauss's result) and then tackle the proof for higher-dimensional lattices via induction.

4.1.1. Proof for 2-D lattices. Consider a 2-D lattice with a basis $\mathcal{B} = \{b_1, b_2\}$ satisfying the conditions of Theorem 1. Let θ' denote the angle between b_1 and b_2. Since $\frac{\pi}{3} \leq \theta' \leq \frac{\pi}{2}$ by assumption,

$$|\langle b_1, b_2 \rangle| = \|b_1\| \, \|b_2\| \cos\theta' \leq \frac{\|b_1\| \, \|b_2\|}{2}. \tag{9}$$

The squared-length of any nonzero lattice vector $v = u_1 b_1 + u_2 b_2$, with $u_1, u_2 \in \mathbb{Z}$ and $|u_1| + |u_2| > 0$, equals

$$\begin{aligned}
\|v\|^2 &= |u_1|^2 \|b_1\|^2 + |u_2|^2 \|b_2\|^2 + 2u_1 u_2 \langle b_1, b_2 \rangle \\
&\geq |u_1|^2 \|b_1\|^2 + |u_2|^2 \|b_2\|^2 - 2|u_1||u_2||\langle b_1, b_2 \rangle| \\
&\geq |u_1|^2 \|b_1\|^2 + |u_2|^2 \|b_2\|^2 - |u_1||u_2| \|b_1\| \, \|b_2\| \qquad \text{(using (9))} \\
&= \left(|u_1| \|b_1\| - |u_2| \|b_2\|\right)^2 + |u_1||u_2| \|b_1\| \, \|b_2\| \qquad (10) \\
&\geq \min\left(\|b_1\|^2, \, \|b_2\|^2\right),
\end{aligned}$$

with equality possible only if either $|u_1| + |u_2| = 1$ or $\theta' = \frac{\pi}{3}$. This proves Theorem 1 for 2-D lattices.

4.1.2. Proof for higher-dimensional lattices. Let $k > 2$ be an integer, and assume that Theorem 1 is true for every $(k-1)$-D lattice. Consider a k-D lattice $\mathcal{L}$ spanned by a weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis $(b_1, b_2, \ldots, b_k)$, with $\epsilon \geq 0$. Any nonzero vector in $\mathcal{L}$ can be written as $\sum_{i=1}^{k} u_i \, b_i$ for integers u_i, where $u_i \neq 0$ for some $i \in \{1, 2, \ldots, k\}$. If $u_k = 0$, then $\sum_{i=1}^{k} u_i \, b_i$ is contained in the $(k-1)$-D lattice spanned by the weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis $(b_1, b_2, \ldots, b_{k-1})$. For $u_k = 0$, by the induction hypothesis, we have

$$\left\| \sum_{i=1}^{k} u_i \, b_i \right\| = \left\| \sum_{i=1}^{k-1} u_i \, b_i \right\| \geq \min_{j \in \{1,2,\ldots,k-1\}} \|b_j\| \geq \min_{j \in \{1,2,\ldots,k\}} \|b_j\| .$$

If $\epsilon > 0$, then the first inequality in the above expression can hold as an equality only if $\sum_{i=1}^{k-1} |u_i| = 1$. If $u_k \neq 0$ and $u_i = 0$ for $i = 1, 2, \ldots, k-1$, then again

$$\left\| \sum_{i=1}^{k} u_i \, b_i \right\| \geq \|b_k\| \geq \min_{j \in \{1,2,\ldots,k\}} \|b_j\| .$$

Again, it is necessary that $|u_k| = 1$ for the equality to hold above.

Assume that $u_k \neq 0$ and $u_i \neq 0$ for some $i \in \{1, 2, \ldots, k-1\}$. Now $\sum_{i=1}^{k} u_i \, b_i$ is contained in the 2-D lattice spanned by the vectors $\sum_{i=1}^{k-1} u_i \, b_i$ and $u_k b_k$. Since the ordered set $(b_1, b_2, \ldots, b_k)$ is weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal, the angle between the nonzero vectors $\sum_{i=1}^{k-1} u_i \, b_i$ and $u_k b_k$ lies in the interval $\left[\frac{\pi}{3} + \epsilon, \frac{\pi}{2}\right]$. Invoking Theorem 1 for 2-D lattices, we have

$$\begin{aligned}
\left\| \sum_{i=1}^{k} u_i \, b_i \right\| &\geq \min\left(\left\| \sum_{i=1}^{k-1} u_i \, b_i \right\|, \; \|u_k b_k\| \right) \\
&\geq \min\left(\min_{j \in \{1,2,\ldots,k-1\}} \|b_j\| , \; \|u_k b_k\| \right) \\
&\geq \min_{j \in \{1,2,\ldots,k\}} \|b_j\| . \qquad (11)
\end{aligned}$$

Thus, the set of basis vectors $\{b_1, b_2, \ldots, b_k\}$ contains a shortest nonzero vector in the k-D lattice. Also, if $\epsilon > 0$, then equality is not possible in (11), and the second part of the theorem follows. □

4.2. Proof of Theorem 2. Similar to the proof of Theorem 1, we first prove Theorem 2 for 2-D lattices and then prove the general case by induction.

4.2.1. Proof for 2-D lattices. Consider a 2-D lattice in $\mathbb{R}^n$ with basis vectors b_1 and b_2 such that the basis $\{b_1, b_2\}$ is weakly θ-orthogonal with $\theta > \frac{\pi}{3}$. Note that for 2-D lattices, weak θ-orthogonality is the same as θ-orthogonality. Without loss of generality (w.l.o.g.), we can assume that $1 = \|b_1\| \le \|b_2\|$. Further, by rotating the 2-D lattice, the basis vectors can be expressed as the columns of the $n \times 2$ matrix

$$\begin{bmatrix} 1 & b_{21} \\ 0 & b_{22} \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix}.$$

Let $\theta' \in \left[\theta, \frac{\pi}{2}\right]$ denote the angle between b_1 and b_2. Clearly,

$$\cos\theta' = \frac{|b_{21}|}{\|b_2\|} \text{ and } \sin\theta' = \frac{|b_{22}|}{\|b_2\|}.$$

Since (6) holds by assumption,

$$\|b_2\| < \frac{\sqrt{3}\|b_1\|}{\sin\theta + \sqrt{3}\cos\theta} \le \frac{\sqrt{3}\|b_1\|}{\sin\theta' + \sqrt{3}\cos\theta'} = \frac{\sqrt{3}}{\frac{|b_{22}|}{\|b_2\|} + \sqrt{3}\frac{|b_{21}|}{\|b_2\|}},$$

where we have used the fact that $\eta(\theta)$ is a nondecreasing function of θ for $\theta \in \left[\frac{\pi}{3}, \frac{\pi}{2}\right]$. Therefore,

$$|b_{22}| < \sqrt{3}(1 - |b_{21}|). \tag{12}$$

Let $\{\widetilde{b}_1, \widetilde{b}_2\}$ denote another $\frac{\pi}{3}$-orthogonal basis for the same 2-D lattice. Using Theorem 1 and Corollary 1, we infer that $\{b_1, b_2\}$ contains every shortest lattice vector (multiplied by ± 1) and $\{b_1, b_2\}$ and $\left\{\widetilde{b}_1, \widetilde{b}_2\right\}$ contain a common shortest lattice vector. Assume w.l.o.g. that $\widetilde{b}_1 = \pm b_1$ is a shortest lattice vector. Then, we can write

$$\begin{bmatrix} \widetilde{b}_1 & \widetilde{b}_2 \end{bmatrix} = \begin{bmatrix} b_1 & b_2 \end{bmatrix} \begin{bmatrix} \pm 1 & u \\ 0 & \pm 1 \end{bmatrix} \quad \text{with } u \in \mathbb{Z}.$$

To prove Theorem 2, we need to show that $u = 0$.

Let $\widetilde{\theta}$ denote the angle between $\widetilde{b}_1$ and $\pm\widetilde{b}_2$. Then,

$$\begin{aligned}\cos^2\widetilde{\theta} &= \frac{\left|\langle\widetilde{b}_1,\widetilde{b}_2\rangle\right|^2}{\left\|\widetilde{b}_1\right\|^2\left\|\widetilde{b}_2\right\|^2}\\ &= \frac{(u\pm b_{21})^2}{(u\pm b_{21})^2+b_{22}^2}\\ &> \frac{(u\pm b_{21})^2}{(u\pm b_{21})^2+3(1-|b_{21}|)^2} \qquad \text{(using (12))}\\ &= \frac{1}{1+\frac{3(1-|b_{21}|)^2}{(u\pm b_{21})^2}}. \qquad (13)\end{aligned}$$

If $u \neq 0$, then

$$|u\pm b_{21}| \geq |u| - |b_{21}| \geq 1 - |b_{21}| \geq 0 \quad \text{(from (12))}.$$

Hence,

$$|u\pm b_{21}|^2 \geq (1-|b_{21}|)^2.$$

Therefore, from (13) we have

$$\cos^2\widetilde{\theta} > \frac{1}{4}, \qquad (14)$$

which holds if and only if $\widetilde{\theta} < \frac{\pi}{3}$. Thus, $\{\widetilde{b}_1,\widetilde{b}_2\}$ can be $\frac{\pi}{3}$-orthogonal only if $u=0$. This proves Theorem 2 for 2-D lattices.

4.2.2. Proof for higher-dimensional lattices. Let $\mathcal{B}$ and $\widetilde{\mathcal{B}}$ be two $n\times k$ matrices defining bases of the same k-D lattice in $\mathbb{R}^n$. We can write $\mathcal{B}=\widetilde{\mathcal{B}}\mathcal{U}$ for some integer unimodular matrix $\mathcal{U}=(u_{ij})$. Using induction on k, we will show that if $\mathcal{B}$ is weakly θ-orthogonal with $\frac{\pi}{3} < \theta \leq \frac{\pi}{2}$, if the columns of $\mathcal{B}$ satisfy (6), and if $\widetilde{\mathcal{B}}$ is $\frac{\pi}{3}$-orthogonal, then $\widetilde{\mathcal{B}}$ can be obtained by permuting the columns of $\mathcal{B}$ and multiplying them by ±1. Equivalently, we will show every column of $\mathcal{U}$ has exactly one component equal to ±1 and all others equal to 0 (we call such a matrix a *signed permutation matrix*).

Assume that Theorem 2 holds for all $(k-1)$-D lattices with $k>2$. Let $b_1,b_2,\ldots,b_k$ denote the columns of $\mathcal{B}$, and let $\widetilde{b}_1,\widetilde{b}_2,\ldots,\widetilde{b}_k$ denote the columns of $\widetilde{\mathcal{B}}$. Since permuting the columns of $\widetilde{\mathcal{B}}$ does not destroy $\frac{\pi}{3}$-orthogonality, we can assume w.l.o.g. that $\widetilde{b}_1$ is $\widetilde{\mathcal{B}}$'s shortest vector. From Theorem 1, $\widetilde{b}_1$ is also a shortest lattice vector. Further, using Corollary 1, $\pm\widetilde{b}_1$ is contained in $\mathcal{B}$. Assume that $b_\ell = \pm\widetilde{b}_1$ for some $\ell\in\{1,2,\ldots,k\}$. Then

$$\mathcal{B} = \widetilde{\mathcal{B}}\begin{bmatrix} u_{11} & \ldots & u_{1\ell-1} & \pm1 & u_{1\ell+1} & \ldots & u_{1k}\\ & & & \vdots & & & \\ & \mathcal{U}_1' & & 0 & & \mathcal{U}_2' & \\ & & & \vdots & & & \end{bmatrix}. \qquad (15)$$

Above, $\mathcal{U}_1'$ is a $(k-1)\times(\ell-1)$ submatrix, where as $\mathcal{U}_2'$ is a $(k-1)\times(k-\ell)$ submatrix.

We will show that $u_{1j} = 0$ for all $j \in \{1, 2, \ldots, k\}$ with $j \neq \ell$. Define

$$\mathcal{B}_r = \begin{bmatrix} b_\ell & b_j \end{bmatrix}, \qquad \widetilde{\mathcal{B}}_r = \begin{bmatrix} \widetilde{b}_1 & \sum_{i=2}^{k} u_{ij} \widetilde{b}_i \end{bmatrix}. \tag{16}$$

Then, from (15) and (16),

$$\mathcal{B}_r = \widetilde{\mathcal{B}}_r \begin{bmatrix} \pm 1 & u_{1j} \\ 0 & 1 \end{bmatrix}.$$

Since $\mathcal{B}_r$ and $\widetilde{\mathcal{B}}_r$ are related by a unimodular matrix, they both define bases of the same 2-D lattice. Further, $\mathcal{B}_r$ is weakly θ-orthogonal with $||b_j|| < \eta(\theta)||b_\ell||$, and $\widetilde{\mathcal{B}}_r$ is $\frac{\pi}{3}$-orthogonal. Invoking Theorem 2 for 2-D lattices, we can infer that $u_{1j} = 0$. It remains to be shown that $\mathcal{U}' = [\mathcal{U}'_1\ \mathcal{U}'_2]$ is also a signed permutation matrix, where

$$\mathcal{B}' = \widetilde{\mathcal{B}}' \mathcal{U}',$$

with $\mathcal{B}' = [b_1, b_2, \ldots, b_{\ell-1},\ b_{\ell+1}, \ldots, b_k]$ and $\widetilde{\mathcal{B}}' = \begin{bmatrix} \widetilde{b}_2, \widetilde{b}_3, \ldots, \widetilde{b}_k \end{bmatrix}$. Observe that $\det(\mathcal{U}') = \det(\mathcal{U}) = \pm 1$. Both $\mathcal{B}'$ and $\widetilde{\mathcal{B}}'$ are bases of the same $(k-1)$-D lattice as $\mathcal{U}'$ is unimodular. $\widetilde{\mathcal{B}}'$ is $\frac{\pi}{3}$-orthogonal, whereas $\mathcal{B}'$ is weakly θ-orthogonal, and its columns satisfy (6). By the induction hypothesis, $\mathcal{U}'$ is a signed permutation matrix. Therefore, $\mathcal{U}$ is also a signed permutation matrix. □

4.3. Proof of Theorem 3. Theorem 3 is a direct consequence of the following lemma.

LEMMA 1. *Let $\mathcal{B} = (b_1, b_2, \ldots, b_m)$ be a weakly θ-orthogonal basis of a lattice, where $\theta > \frac{\pi}{3}$. Then, for any integers $u_1, u_2, \ldots, u_m$,*

$$\left\| \sum_{i=1}^{m} u_i b_i \right\| \geq \left(\frac{\sqrt{3}}{2} \right)^{m-1} \times \max_{i \in \{1,2,\ldots,m\}} \|u_i b_i\|. \tag{17}$$

Lemma 1 can be proved as follows. Consider the vectors b_1 and b_2; the angle θ between them lies in the interval $\left(\frac{\pi}{3}, \frac{\pi}{2}\right)$. Recall from (10) that

$$\|u_1 b_1 + u_2 b_2\|^2 \geq \left(|u_1|\,\|b_1\| - |u_2|\,\|b_2\|\right)^2 + |u_1||u_2|\|b_1\|\|b_2\|.$$

Consider the expression $(y-x)^2 + yx$ with $0 \leq x \leq y$. For fixed y this expression attains its minimum value of $\left(\frac{3}{4}\right) y^2$ when $x = \frac{y}{2}$. By setting $y = |u_1|\,\|b_1\|$ and $x = |u_2|\,\|b_2\|$ w.l.o.g, we can infer that

$$\|u_1 b_1 + u_2 b_2\| \geq \frac{\sqrt{3}}{2} \max_{i \in \{1,2\}} \|u_i b_i\|.$$

Since $\mathcal{B}$ is weakly θ-orthogonal, the angle between $u_k b_k$ and $\sum_{i=1}^{k-1} u_i b_i$ lies in the interval $\left(\frac{\pi}{3}, \frac{\pi}{2}\right)$ for $k = 2, 3, \ldots, m$. Hence (17) follows by induction. □

We now proceed to prove Theorem 3 by invoking Lemma 1. First, we define $\Delta = (\sqrt{3}/2)^{m-1}$. For any $j \in \{1, 2, \ldots, m\}$, we have

$$\|b_j\| = \left\| \sum_{i=1}^{m} u_{ij} \widetilde{b}_i \right\| \geq \Delta \max_{i \in \{1,2,\ldots,m\}} \left\| u_{ij} \widetilde{b}_i \right\| \geq \Delta \min_{i \in \{1,2,\ldots,m\}} \|\widetilde{b}_i\| \max_{i \in \{1,2,\ldots,m\}} |u_{ij}|.$$

Since $\mathcal{B}$ and $\widetilde{\mathcal{B}}$ are both weakly θ-orthogonal with $\theta > \frac{\pi}{3}$, $\min_{i\in\{1,2,\ldots,m\}} \|\widetilde{b}_i\| = \min_{i\in\{1,2,\ldots,m\}} \|b_i\|$. Therefore,

$$\Delta \max_{i\in\{1,2,\ldots,m\}} |u_{ij}| \leq \frac{\|b_j\|}{\min_{i\in\{1,2,\ldots,m\}} \|\widetilde{b}_i\|} \leq \frac{\max_{i\in\{1,2,\ldots,m\}} \|b_i\|}{\min_{i\in\{1,2,\ldots,m\}} \|b_i\|} = \Delta\kappa(\mathcal{B}).$$

Thus, $|u_{ij}| \leq \kappa(\mathcal{B})$ for all i and j. □

5. Random lattices and SVP. In several applications, the orthogonality of random lattice bases and the length of the shortest vector $\lambda(\mathcal{L})$ in a random lattice $\mathcal{L}$ play an important role. For example, in certain wireless communications applications involving multiple transmitters and receivers, the received message ideally lies on a lattice spanned by a random basis [7]. The random basis models the fluctuations in the communication channel between each transmitter-receiver pair. Due to the presence of noise, the ideal received message is retrieved by solving a CVP. The complexity of this problem is controlled by the orthogonality of the random basis [1]. Random bases are also employed to perform error correction coding [28] and in cryptography [28]. The level of achievable error correction is controlled by the shortest vector in the lattice.

In this section, we determine the θ-orthogonality of random bases. This result immediately lets us identify conditions under which a random basis contains (with high probability) the shortest lattice vector.

Before describing our results on random lattices and bases, we first review some known properties of random lattices and then list some powerful results from random matrix theory.

5.1. Known properties of random lattices. Consider an m-D lattice generated by a random basis with each of the m basis vectors chosen independently and uniformly from the unit ball in $\mathbb{R}^n$ $(n \geq m)$.[2] With m fixed and with $n \to \infty$, the probability that the random basis is Minkowski-reduced tends to 1 [11]. Thus, as $n \to \infty$, the random basis contains a shortest vector in the lattice almost surely. Recently, [3] proved that, as $n - m \to \infty$, the probability that a random basis is LLL-reduced $\to 1$. Further, [3] also showed that a random basis is LLL-reduced with nonzero probability when $n - m$ is fixed with $n \to \infty$.

5.2. Known properties of random matrices. Random matrix theory, a rich field with many applications [6, 12], has witnessed several significant developments over the past few decades [12, 18, 19, 30]. We will invoke some of these results to derive some new properties of random bases and lattices; the paper [6] provides an excellent summary of the results we mention below.

Consider an $n \times m$ matrix $\mathcal{B}$ with each element of $\mathcal{B}$ an independent identically distributed random variable. If the variables are zero-mean Gaussian distributed with variance $\frac{1}{n}$, then we refer to such a $\mathcal{B}$ as a *Gaussian* random basis. If the variables take on values in $\{-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}\}$ with equal probability, then we term $\mathcal{B}$ to be a *Bernoulli* random basis. We say that $\mathcal{B}$ is a *scaled* Gaussian (Bernoulli) basis if it is obtained by scaling the columns of a Gaussian (Bernoulli) basis arbitrarily.

Gaussian and Bernoulli random bases enjoy the following properties. Below, ψ_i^2, $i = 1, 2, \ldots, m$, denote the eigenvalues of $\mathcal{B}^T\mathcal{B}$.

[2] The m vectors form a basis because they are linearly independent almost surely.

1. For both Gaussian and Bernoulli $\mathcal{B}$, $\mathcal{B}^T\mathcal{B}$'s smallest and largest eigenvalues, $\psi^2_{\min}$ and $\psi^2_{\max}$, converge almost surely to $(1-\sqrt{c})^2$ and $(1+\sqrt{c})^2$, respectively, as $n, m \to \infty$ and $\frac{m}{n} \to c < 1$ [6, 12, 30].
2. Let $\epsilon > 0$ be given. Then, there exists an N_ϵ such that, for every $n > N_\epsilon$ and $r > 0$,

$$P\left(|\psi_{\min}| \leq \left(1 - \sqrt{\frac{m}{n}}\right) - (r+\epsilon)\right) \leq e^{-\frac{nr^2}{\rho}}, \tag{18}$$

$$P\left(|\psi_{\max}| \geq \left(1 + \sqrt{\frac{m}{n}}\right) + (r+\epsilon)\right) \leq e^{-\frac{nr^2}{\rho}}, \tag{19}$$

with $\rho = 2$ for Gaussian $\mathcal{B}$ and $\rho = 16$ for Bernoulli $\mathcal{B}$ [6, 18].

In essence, a random matrix's largest and smallest singular values converge, respectively, to $1 \pm \sqrt{\frac{m}{n}}$ almost surely as $n, m \to \infty$ and lie close to $1 \pm \sqrt{\frac{m}{n}}$ with very high probability at finite (but sufficiently large) n.

5.3. New results on random lattices. We now formally state the new properties of random lattices mentioned in the introduction plus several additional corollaries. Our proofs assume that the lattices are generated by Gaussian or Bernoulli random bases (whose column vectors are essentially unit-length). However, our results easily extend to lattices generated by Gaussian or Bernoulli random bases because the θ-orthogonality of a basis does not change upon scaling the basis vectors.

The key step in proving our results is to relate the condition number of a random basis to its θ-orthogonality (see Lemma 2). A matrix's condition number is defined as the ratio of the largest to the smallest singular value. Then we invoke the results in section 5.2 to quantify the θ-orthogonality of random bases. Finally we invoke previously deduced properties of nearly orthogonal lattice bases.

We wish to emphasize that we prove our statements only for lattices which are not full-dimensional. Our computational results suggest these statements are not true for full-dimensional lattices. Further, Sorkin [31] proves that, with high probability, Gaussian random matrices are not nearly orthogonal when $m > n/4$. See the paragraph after Corollary 3 for more details.

LEMMA 2. *Consider an arbitrary $n \times m$ real-valued matrix $\mathcal{B}$, with $m \leq n$, whose largest and smallest singular values are denoted by $\psi_{\max}$ and $\psi_{\min}$, respectively. Then the columns of $\mathcal{B}$ are θ-orthogonal with*

$$\theta = \sin^{-1}\left(\frac{2\,\psi_{\max}\,\psi_{\min}}{\psi^2_{\min} + \psi^2_{\max}}\right). \tag{20}$$

The proof is given in section 5.4. The value of θ in (20) is the best possible in the sense that there is a 2×2 matrix $\mathcal{B}$ with singular values $\psi_{\min}$ and $\psi_{\max}$ such that the angle between the two columns of $\mathcal{B}$ is given by (20). Note that for large $\frac{\psi_{\min}}{\psi_{\max}}$ (that is, for a small condition number), the θ in (20) is close to $\frac{\pi}{2}$. Thus, Lemma 2 quantifies our intuition that a matrix with a small condition number should be nearly orthogonal.

By combining Lemma 2 with the properties of random matrices listed in section 5.2, we can immediately deduce the θ-orthogonality of an $n \times m$ random basis. See section 5.4.2 for the proof.

THEOREM 4. *Let $\mathcal{B}$ denote an $n \times m$ Gaussian or Bernoulli random basis. If $m \leq cn$, $0 \leq c < 1$, then as $n \to \infty$, $\mathcal{B}$ is θ-orthogonal almost surely with*

$$\theta = \sin^{-1}\left(\frac{1-c}{1+c}\right). \tag{21}$$

Further, given an $\epsilon > 0$, there exists an N_ϵ such that, for every $n > N_\epsilon$ and $r > 0$, $\mathcal{B}$ is θ-orthogonal,

$$\theta = \sin^{-1}\left(\frac{1-c}{1+c} - \frac{3\sqrt{3}}{4}(r+\epsilon)\right), \tag{22}$$

with probability greater than $1 - 2e^{-\frac{nr^2}{\rho}}$, where $\rho = 2$ for Gaussian $\mathcal{B}$ and $\rho = 16$ for Bernoulli $\mathcal{B}$.

The value of θ in (21) is not the best possible in the sense that, for a given value of c, a random $n \times m$ Gaussian matrix with $m \leq cn$ would be θ'-orthogonal (with high probability) for some $\theta' > \theta$ (see Figure 2). The reason is that the θ predicted by Lemma 2 is satisfied by *all* matrices. However, Theorem 4 is restricted to random matrices.

Theorem 4 allows us to bound the length of the shortest nonzero vector in a random lattice.

COROLLARY 2. *Let the $n \times m$ matrix $\mathcal{B} = (b_1, b_2, \ldots, b_m)$, with $m \leq cn$ and $0 \leq c < 1$, denote a Gaussian or Bernoulli random basis for a lattice $\mathcal{L}$. Then the shortest vector's length $\lambda(\mathcal{L})$ satisfies*

$$\lambda(\mathcal{L}) \geq \frac{1-c}{1+c}$$

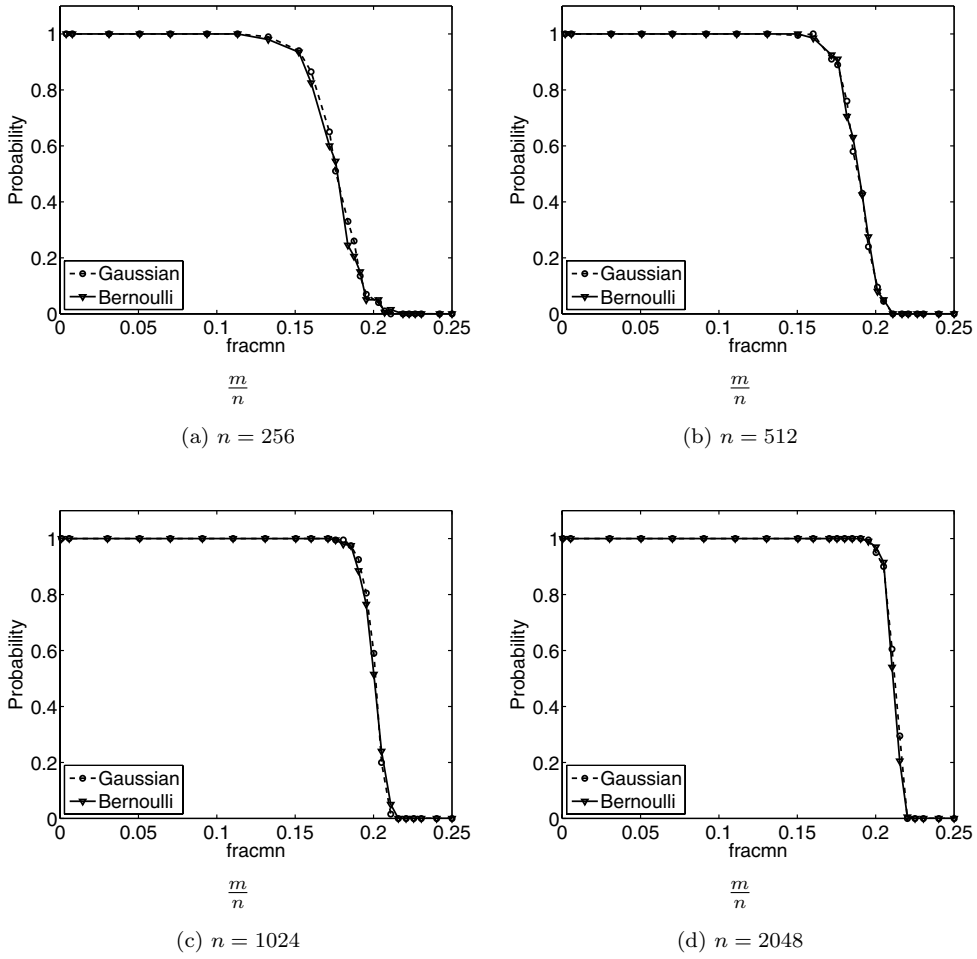
almost surely as $n \to \infty$.

Each column of a Bernoulli $\mathcal{B}$ is unit-length by construction. For Gaussian $\mathcal{B}$, it is not difficult to show that all columns have length 1 almost surely as $n \to \infty$. Hence Corollary 2 is an immediate consequence of Theorem 4 and (2). Corollary 2 implies that, in random lattices that are not full-dimensional, it is easy to obtain approximate solutions to the SVP (within a constant factor). This is because for random lattices in $\mathbb{R}^n$ with dimension $n(1-\epsilon)$, $\lambda(\mathcal{L})$ is greater than ϵ times the length of the shortest basis vector (approximately). Compare this with Daudé's and Vallée's [9] result that in random full-dimensional lattices in $\mathbb{R}^n$, $\lambda(\mathcal{L})$ is at least $O(1/\sqrt{n})$ times the length of the shortest basis vector with high probability.

By substituting $\theta = \frac{\pi}{3}$ into Theorem 4 and then invoking Corollary 1, we can deduce sufficient conditions for a random basis to be $\frac{\pi}{3}$-orthogonal.

COROLLARY 3. *Let the $n \times m$ matrix $\mathcal{B}$ denote a Gaussian or Bernoulli random basis for lattice $\mathcal{L}$. If $\frac{m}{n} \leq c < \left(7 - \sqrt{48}\right)$ (≈ 0.071), then $\mathcal{B}$ is $\frac{\pi}{3}$-orthogonal almost surely as $n \to \infty$. Further, given an $\epsilon > 0$, there exists an N_ϵ such that, for every $n > N_\epsilon$ and $\frac{4(1-c)}{3\sqrt{3}(1+c)} - \epsilon - \frac{2}{3} > r > 0$, $\mathcal{B}$ is $\frac{\pi}{3}$-orthogonal with probability greater than $1 - 2e^{-nr^2/\rho}$, where $\rho = 2$ for Gaussian $\mathcal{B}$ and $\rho = 16$ for Bernoulli $\mathcal{B}$.*

Figure 2 illustrates that, in practice, an $n \times m$ Gaussian and Bernoulli random matrix is nearly orthogonal for much larger values of $\frac{m}{n}$ than our results claim. Our plots suggest that the probability for a random basis to be nearly orthogonal sharply transitions from 1 to 0 for $\frac{m}{n}$ values in the interval $[0.2, 0.25]$. Sorkin [31] has shown us that if the columns of $\mathcal{B}$ represent points chosen uniformly from the unit sphere in



(a) $n = 256$ (b) $n = 512$

(c) $n = 1024$ (d) $n = 2048$

FIG. 2. *Empirical probability that a $n \times m$ Gaussian or Bernoulli random matrix is $\frac{\pi}{3}$-orthogonal. At $n = 256$, 512, 1024, and 2048 and at m indicated by circles (for Gaussian) and triangles (for Bernoulli), we tested 200 randomly generated matrices. The empirical probability is the fraction of random matrices that were $\frac{\pi}{3}$-orthogonal.*

$\mathbb{R}^n$ (one can obtain such points by dividing the columns of a Gaussian matrix by their norms), then the best possible $\frac{m}{n}$ value for random $n \times m$ matrices to be $\frac{\pi}{3}$-orthogonal is $\frac{m}{n} = 0.25$. Further, if $m/n > 0.25$, $\mathcal{B}$ is almost surely not $\frac{\pi}{3}$-orthogonal as $n \to \infty$. For large n, the columns of a Gaussian matrix almost surely have length 1 and thus behave like points chosen uniformly from the unit sphere in $\mathbb{R}^n$. Therefore, as $n \to \infty$, random $n \times n/4$ Gaussian matrices are almost surely $\frac{\pi}{3}$-orthogonal.

5.4. Proof of results on random lattices. This section provides the proofs for Lemma 2 and Theorem 4.

5.4.1. Proof of Lemma 2. Our goal is to construct a lower-bound for the angle between any column of $\mathcal{B}$ and the subspace spanned by all the other columns in terms of the singular values of $\mathcal{B}$. Clearly, if $\psi_{\min} = 0$, then the columns of $\mathcal{B}$ are linearly dependent. Hence, (20) holds as $\mathcal{B}$'s columns are θ-orthogonal with $\theta = 0$. For the rest of the proof, we will assume that $\psi_{\min} \neq 0$.

Consider the SVD of $\mathcal{B}$:

$$\mathcal{B} = \mathcal{X}\Psi\mathcal{Y}, \tag{23}$$

where $\mathcal{X}$ and $\mathcal{Y}$ are $n \times m$ and $m \times m$ real-valued matrices, respectively, with orthonormal columns and Ψ is a $m \times m$ real-valued diagonal matrix. Let b_i and x_i denote the ith column of $\mathcal{B}$ and $\mathcal{X}$, respectively, let y_{ij} denote the element from the ith row and jth column of $\mathcal{Y}$, and let ψ_i denote the ith diagonal element of Ψ. Then, (23) can be rewritten as

$$\begin{bmatrix} b_1 & b_2 & \dots & b_m \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \dots & x_m \end{bmatrix} \begin{bmatrix} \psi_1 & 0 & \dots & 0 \\ 0 & \psi_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & \psi_m \end{bmatrix} \begin{bmatrix} y_{11} & y_{12} & \dots & y_{1m} \\ y_{21} & y_{22} & \dots & y_{2m} \\ \vdots & & \ddots & \vdots \\ y_{m1} & \dots & \dots & y_{mm} \end{bmatrix}.$$

We now analyze the angle between b_1 (w.l.o.g) and the subspace spanned by $\{b_2, b_3, \dots, b_m\}$. Note that

$$b_1 = \sum_{i=1}^{m} \psi_i \, y_{i1} \, x_i.$$

Let $\widetilde{b}_1$ denote an arbitrary nonzero vector in the subspace spanned by $\{b_2, b_3, \dots, b_m\}$. Then,

$$\widetilde{b}_1 = \sum_{k=2}^{m} \alpha_k \, b_k = \sum_{k=2}^{m} \alpha_k \sum_{i=1}^{m} \psi_i \, y_{ik} \, x_i = \sum_{i=1}^{m} x_i \, \psi_i \sum_{k=2}^{m} \alpha_k \, y_{ik}$$

for some $\alpha_k \in \mathbb{R}$ with $\sum_k |\alpha_k| > 0$. Let $\widetilde{y}_{i1} = \sum_{k=2}^{m} \alpha_k \, y_{ik}$. Then,

$$\widetilde{b}_1 = \sum_{i=1}^{m} \psi_i \widetilde{y}_{i1} x_i.$$

Let $\widetilde{\theta} \geq \theta$ denote the angle between b_1 and $\widetilde{b}_1$. Then,

$$\cos\widetilde{\theta} = \frac{\left|\left\langle b_1, \widetilde{b}_1 \right\rangle\right|}{\|b_1\| \, \left\|\widetilde{b}_1\right\|} = \frac{|\langle \sum_{i=1}^{m} \psi_i \, y_{i1} \, x_i, \sum_{i=1}^{m} \psi_i \, \widetilde{y}_{i1} \, x_i \rangle|}{\|\sum_{i=1}^{m} \psi_i \, y_{i1} \, x_i\| \; \|\sum_{i=1}^{m} \psi_i \, \widetilde{y}_{i1} \, x_i\|} \tag{24}$$

$$= \frac{\left|\sum_{i=1}^{m} \psi_i^2 \, y_{i1} \, \widetilde{y}_{i1}\right|}{\sqrt{\sum_{i=1}^{m} \psi_i^2 \, y_{i1}^2} \, \sqrt{\sum_{i=1}^{m} \psi_i^2 \, \widetilde{y}_{i1}^2}}, \tag{25}$$

where the orthonormality of the $\mathcal{X}$ columns is used to obtain (25) from (24). Let y_i, $i = 1, 2, \dots, m$, and $\widetilde{y}_1$ denote column vectors

$$y_i := \begin{bmatrix} y_{1i} \\ y_{2i} \\ \vdots \\ y_{mi} \end{bmatrix} \text{ and } \widetilde{y}_1 := \begin{bmatrix} \widetilde{y}_{11} \\ \widetilde{y}_{21} \\ \vdots \\ \widetilde{y}_{m1} \end{bmatrix}.$$

Since $\widetilde{y}_1 = \sum_{k=2}^{m} \alpha_k \, y_k$,

$$\widetilde{y}_1^T y_1 = 0.$$

Then (25) can be rewritten using matrix notation as

$$\cos\widetilde{\theta} = \frac{\left|y_1^T\,\Psi^2\,\widetilde{y}_1\right|}{\sqrt{y_1^T\Psi^2\,y_1}\,\sqrt{\widetilde{y}_1^T\Psi^2\,\widetilde{y}_1}}, \tag{26}$$

with $\Psi^2 := \Psi^T\Psi$. The angle $\widetilde{\theta}$ is minimized when the right-hand side of (26) is maximized.

For arbitrary $\mathcal{B}$ with only the singular values known (that is, Ψ is known), the θ-orthogonality of $\mathcal{B}$ is given by solving the following constrained optimization problem:

$$\cos\theta = \max_{y_1,\widetilde{y}_1} \frac{\left|y_1^T\Psi^2\widetilde{y}_1\right|}{\sqrt{y_1^T\Psi^2\,y_1}\,\sqrt{\widetilde{y}_1^T\Psi^2\widetilde{y}_1}} \text{ such that } \widetilde{y}_1^T y_1 = 0. \tag{27}$$

Wielandt's inequality [14, Thm. 7.4.34] states that if A is a positive definite matrix, with $\gamma_{\min}$ and $\gamma_{\max}$ denoting its minimum and maximum eigenvalues (both are positive), then

$$|x^TAy|^2 \le \left(\frac{\gamma_{\max}-\gamma_{\min}}{\gamma_{\max}+\gamma_{\min}}\right)^2 (x^TAx)(y^TAy)$$

for every pair of orthogonal vectors x and y (equality holds for some pair of orthogonal vectors). In our problem, $A = \Psi^2$, $x = \widetilde{y}_1$, $y = y_1$, $\gamma_{\max} = \psi_{\max}^2$, and $\gamma_{\min} = \psi_{\min}^2$. Therefore, using Wielandt's inequality and (27), we have

$$\cos\theta = \frac{\psi_{\max}^2 - \psi_{\min}^2}{\psi_{\max}^2 + \psi_{\min}^2}.$$

Hence

$$\sin\theta = \frac{2\psi_{\max}\psi_{\min}}{\psi_{\max}^2 + \psi_{\min}^2}, \tag{28}$$

which proves (20). □

5.4.2. Proof of Theorem 4. The first part of Theorem 4 follows easily. From section 5.2, we can infer that with $m \le cn$, $0 \le c < 1$, both $\psi_{\min} \ge 1-\sqrt{c}$ and $\psi_{\max} \le 1+\sqrt{c}$ almost surely as $n \to \infty$. Invoking Lemma 2 and substituting $\psi_{\min} = 1-\sqrt{c}$ and $\psi_{\max} = 1+\sqrt{c}$ into (20), it follows that, as $n \to \infty$, $\mathcal{B}$ is θ-orthogonal almost surely with θ given by (21).

We now focus on proving the second part of Theorem 4. Let $d = \sqrt{c}$, and define

$$G(d) := \frac{1-d^2}{1+d^2}.$$

We first show that, for $\delta \ge 0$,

$$G(d+\delta) \ge G(d) - \frac{3\sqrt{3}}{4}\delta. \tag{29}$$

Using the mean value theorem,

$$G(d+\delta) = G(d) + G'\left(d+\widetilde{\delta}\right)\delta \text{ for some } \widetilde{\delta} \in (0,\delta), \tag{30}$$

with G' denoting the derivative of G with respect to d. Further,

$$G'(d) = \frac{-4d}{(1+d^2)^2} \geq -\frac{3\sqrt{3}}{4} \qquad \text{for } d > 0. \tag{31}$$

One can verify the inequality above by differentiating $G'(d)$ and observing that $G'(d)$ is minimized when $3d^4+2d^2-1=0$. The only positive root of this quadratic equation is $d^2 = 1/3$ or $d = 1/\sqrt{3}$. Combining (30) and (31), we obtain (29).

From the results in section 5.2, it follows that the probability that both minimum and maximum singular values of $\mathcal{B}$ satisfy

$$|\psi_{\min}| \geq 1 - \left(\sqrt{c} + r + \epsilon\right) \quad \text{and} \quad |\psi_{\max}| \leq 1 + \left(\sqrt{c} + r + \epsilon\right) \tag{32}$$

is greater than $1 - 2e^{-\frac{nr^2}{\rho}}$. When (32) holds, $\mathcal{B}$ is at least $\sin^{-1}\left(G\left(\sqrt{c}+r+\epsilon\right)\right)$-orthogonal. This follows from (20). Invoking (29), we can infer that $\mathcal{B}$ is θ-orthogonal with θ as in (22). □

6. JPEG CHEst. In this section, we review the JPEG CHEst problem that motivates our study of nearly orthogonal lattices and describe how we use this paper's results to solve this problem. We first touch on the topic of digital color image representation and briefly describe the essential components of JPEG image compression.

6.1. Digital color image representation. Traditionally, digital color images are represented by specifying the color of each pixel, the smallest unit of image representation. According to the trichromatic theory [29], three parameters are sufficient to specify any color perceived by humans.[3] For example, a pixel's color can be conveyed by a vector $w_{RGB} = (w_R, w_G, w_B) \in \mathbb{R}^3$, where w_R, w_G, and w_B specify the intensity of the color's red (R), green (G), and blue (B) components, respectively. Call w_{RGB} the RGB encoding of a color. RGB encodings are vectors in the vector space where the R, G, and B colors form the standard unit basis vectors; this coordinate system is called the RGB *color space*. A color image with M pixels can be specified using RGB encodings by a matrix $P \in \mathbb{R}^{3\times M}$.

6.2. JPEG compression and decompression. To achieve color image compression, schemes such as JPEG first transform the image to a color encoding other than the RGB encoding and then perform *quantization*. Such color encodings can be related to the RGB encoding by a *color-transform* matrix $C \in \mathbb{R}^{3\times 3}$. The columns of C form a different basis for the color space spanned by the R, G, and B vectors. Hence an RGB encoding w_{RGB} can be transformed to the C encoding vector as $C^{-1}w_{RGB}$; the image P is mapped to $C^{-1}P$. For example, the matrix relating the RGB color space to the ITU.BT-601 $YCbCr$ color space is given by [27]

$$\begin{bmatrix} w_Y \\ w_{Cb} \\ w_{Cr} \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.5 \\ 0.5 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} w_R \\ w_G \\ w_B \end{bmatrix}. \tag{33}$$

The quantization step is performed by first choosing a diagonal positive (nonzero entries are positive) integer *quantization* matrix Q and then computing the quantized (compressed) image from $C^{-1}P$ as $P_c = \lceil Q^{-1}C^{-1}P \rfloor$, where $\lceil . \rfloor$ stands for

[3] The underlying reason is that the human retina has only three types of receptors that influence color perception.

the operation of rounding to the nearest integer. JPEG decompression constructs $P_d = CQP_c = CQ\left\lceil Q^{-1}C^{-1}P\right\rfloor$. Larger Q's achieve more compression but at the cost of greater distortion between the decompressed image P_d and the original image P.

In practice, the image matrix P is first decomposed into different frequency components $P = \{P_1, P_2, \ldots, P_k\}$ for some $k > 1$ (usually $k = 64$) during compression. Then, a common color transform C is applied to all the submatrices $P_1, P_2, \ldots, P_k$, but each submatrix P_i is quantized with a different quantization matrix Q_i. The compressed image is $P_c = \{P_{c,1}, P_{c,2}, \ldots, P_{c,k}\} = \left\{\left\lceil Q_1^{-1}C^{-1}P_1\right\rfloor, \left\lceil Q_2^{-1}C^{-1}P_2\right\rfloor, \ldots, \left\lceil Q_k^{-1}C^{-1}P_k\right\rfloor\right\}$, and the decompressed image is $P_d = \{CQ_1P_{c,1}, CQ_2P_{c,2}, \ldots, CQ_kP_{c,k}\}$.

During compression, the JPEG-compressed file format stores the matrix C and the matrices Q_i along with P_c. These stored matrices are utilized to decompress the JPEG image but are discarded afterward. Hence we refer to the set $\{C, Q_1, Q_2, \ldots, Q_k\}$ as the *compression history* of the image.

6.3. JPEG CHEst problem statement. This paper's contributions are motivated by the following question: *Given a decompressed image* $P_d = \left\{CQ_1P_{c,1}, CQ_2P_{c,2}, \ldots, CQ_kP_{c,k}\right\}$ *and some information about the structure of* C *and the* Q_i*'s, can we estimate the color transform* C *and the quantization matrices* Q_i*?* As $\{C, Q_1, Q_2, \ldots, Q_k\}$ comprises the compression history of the image, we refer to this problem as JPEG CHEst. An image's compression history is useful for applications such as JPEG recompression [5, 22, 23].

6.4. Near-orthogonality and JPEG CHEst. The columns of $CQ_iP_{c,i}$ lie on a 3-D lattice with basis CQ_i because $P_{c,i}$ is an integer matrix. The estimation of CQ_i's comprises the main step in JPEG CHEst. Since a lattice can have multiple bases, we must exploit some additional information about practical color transforms to correctly deduce the CQ_i's from the $CQ_iP_{c,i}$'s. Most practical color transforms aim to represent a color using an approximately rotated reference coordinate system. Consequently, most practical color transform matrices C (and, thus, CQ_i) can be expected to be almost orthogonal. We have verified that all C's used in practice are weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal, with $0 < \epsilon \leq \frac{\pi}{6}$.[4] Thus, nearly orthogonal lattice bases are central to JPEG CHEst.

6.5. Our approach. Our approach is to first estimate the products CQ_i by exploiting the near-orthogonality of C and to then decompose CQ_i into C and Q_i. We will assume that C is weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal, $0 < \epsilon \leq \frac{\pi}{6}$.

6.5.1. Estimating the CQ_i's. Let $\mathcal{B}_i$ be a basis of the lattice $\mathcal{L}_i$ spanned by CQ_i. Then, for some unimodular matrix $\mathcal{U}_i$, we have

$$\mathcal{B}_i = CQ_i\mathcal{U}_i. \tag{34}$$

If $\mathcal{B}_i$ is given, then estimating CQ_i is equivalent to estimating the respective $\mathcal{U}_i$.

Thanks to our problem structure, the correct $\mathcal{U}_i$'s satisfy the following constraints. Note that these constraints become increasingly restrictive as the number of frequency components k increases.

1. The $\mathcal{U}_i$'s are such that $\mathcal{B}_i\mathcal{U}_i^{-1}$ is weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal.
2. The product $\mathcal{U}_i\mathcal{B}_i^{-1}\mathcal{B}_j\mathcal{U}_j^{-1}$ is diagonal with positive entries for any $i, j \in \{1, 2, \ldots, k\}$. This is an immediate consequence of (34).

[4] In general, the stronger assumption of $\frac{\pi}{3}$-orthogonality does not hold for some practical color transform matrices.

TABLE 6.1
Number of unimodular matrices satisfying constraints 3 *and* 4 *for small* κ.

κ	Constraint 4	Constraints 3 and 4
1	6960	5232
2	135408	43248
3	1281648	197616
4	5194416	513264
5	20852976	1324272

If, in addition, $\mathcal{B}_i$ is weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal, then the following hold.

3. The columns of $\mathcal{U}_i$ corresponding to the shortest columns of $\mathcal{B}_i$ are the standard unit vectors times ± 1. This follows from Corollary 1 because the columns of both $\mathcal{B}_i$ and CQ_i indeed contain all shortest vectors in $\mathcal{L}_i$ up to multiplication by ± 1.
4. All entries of $\mathcal{U}_i$ are $\leq \kappa(\mathcal{B}_i)$ in magnitude. This follows from Theorem 3.

We now outline our heuristic.

(i) Obtain bases $\mathcal{B}_i$ for the lattices $\mathcal{L}_i$, $i = 1, 2, \ldots, k$. Construct a weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal basis $\mathcal{B}_\ell$ for at least one lattice $\mathcal{L}_\ell$, $\ell \in \{1, 2, \ldots, k\}$.
(ii) Compute $\kappa(\mathcal{B}_\ell)$.
(iii) For every unimodular matrix $\mathcal{U}_\ell$ satisfying constraints 1, 3, and 4, go to step (iv).
(iv) For $\mathcal{U}_\ell$ chosen in step (iii), test if there exist unimodular matrices $\mathcal{U}_j$ for each $j = 1, 2, \ldots, k, j \neq \ell$, that satisfies constraint 2. If such a collection of matrices exists, then return this collection; otherwise, go to step (iii).

For step (i), we simply use the LLL algorithm to compute LLL-reduced bases for each $\mathcal{L}_i$. Such bases are not guaranteed to be weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal, but in practice, this is usually the case for a number of the $\mathcal{L}_i$'s. Instead of LLL, the method proposed in [24] could be also employed (as suggested by the referees). In contrast to the LLL, [24] always finds a basis that contains the shortest lattice vector in low-dimensional lattices (up to four dimensions) such as the $\mathcal{L}_i$'s in our problem. In step (iv), for each frequency component $j \neq \ell$, we compute the diagonal matrix D_j with smallest positive entries such that $\widetilde{\mathcal{U}}_j = \mathcal{B}_j^{-1}\mathcal{B}_\ell\mathcal{U}_\ell^{-1}D_j$ is integral, and then we test whether $\widetilde{\mathcal{U}}_j$ is unimodular. If not, then for the given $\mathcal{U}_\ell$ no appropriate unimodular matrix $\mathcal{U}_j$ exists.

The overall complexity of the heuristic is determined mainly by the number of times we repeat step (iv), which equals the number of distinct choices for $\mathcal{U}_\ell$ in step (iii). This number is typically not very large because in step (i) we are usually able to find some weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal basis $\mathcal{B}_l$ with $\kappa < 2$. In fact, we enumerate all unimodular matrices satisfying constraints 3 and 4 and then test constraint 1. (In practice, one can avoid enumerating the various column permutations of a unimodular matrix). Table 6.1 provides the number of unimodular matrices satisfying constraint 4 alone and also constraints 3 and 4. Clearly, constraints 3 and 4 help us to significantly limit the number of unimodular matrices we need to test, thereby speeding up our search.

Our heuristic returns a collection of unimodular matrices $\{\mathcal{U}_i\}$ that satisfy constraints 1 and 2; of course, they also satisfy constraints 3 and 4 if the corresponding $\mathcal{B}_i$'s are weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal. From the U_i's, we compute $CQ_i = \mathcal{B}_i\mathcal{U}^{-1}$. If constraints 1 and 2 can be satisfied by another solution $\{\mathcal{U}_i'\}$, then it is easy to see that $\mathcal{U}_i' \neq \mathcal{U}_i$ for *every* $i = 1, 2, \ldots, k$. In section 6.5.3, we will argue (without proof) that constraints 1 and 2 are likely to have a unique solution in most practical cases.

6.5.2. Splitting CQ_i into C and Q_i. Decomposing the CQ_i's into C and Q_i's is equivalent to determining the norm of each column of C because the Q_i's are diagonal matrices. Since the Q_i's are integer matrices, the norm of each column of CQ_i is an integer multiple of the corresponding column norm of C. In other words, the norms of the jth column ($j \in \{1, 2, 3\}$) of different CQ_i's form a sublattice of the one-dimensional lattice spanned by the jth column norm of C. As long as the greatest common divisor of the jth diagonal values of the matrices Q_i is 1, we can uniquely determine the jth column of C; the values of Q_i follow trivially.

6.5.3. Uniqueness. Does JPEG CHEst have a unique solution? In other words, is there a collection of matrices

$$(C', Q'_1, Q'_2, \ldots, Q'_k) \neq (C, Q_1, Q_2, \ldots, Q_k)$$

such that $C'Q'_i$ is a weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis of $\mathcal{L}_i$ for all $i \in \{1, 2, \ldots, k\}$? We believe that the solution can be nonunique only if the Q_i's are chosen carefully. For example, let Q be a diagonal matrix with positive diagonal coefficients. Assume that, for $i = 1, 2, \ldots, k$, $Q_i = \alpha_i Q$, with $\alpha_i \in \mathbb{R}$ and $\alpha_i > 0$. Further, assume that there exists a unimodular matrix $\mathcal{U}$ not equal to the identity matrix I such that $C' = CQ\mathcal{U}$ is weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal. Define $Q'_i = \alpha_i I$ for $i = 1, 2, \ldots, k$. Then $C'Q'_i$ is also a weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis for $\mathcal{L}_i$. Typically, JPEG employs Q_i's that are not related in any special way. Therefore, we believe that for most practical cases JPEG CHEst has a unique solution.

6.5.4. Experimental results. We tested the proposed approach using a wide variety of test cases. In reality, the decompressed image P_d is always corrupted with some additive noise. Consequently, to estimate the desired compression history, the approach described above was combined with some additional noise mitigation steps. Our algorithm provided accurate estimates of the image's JPEG compression history for all the test cases. We refer the reader to [22, 23] for details on the experimental setup and results.

7. Discussion and conclusions. In this paper, we derived some interesting properties of nearly orthogonal lattice bases and random bases. We chose to directly quantify the orthogonality of a basis in terms of the minimum angle θ between a basis vector and the linear subspace spanned by the remaining basis vectors. When $\theta \geq \frac{\pi}{3}$ radians, we say that the basis is nearly orthogonal. A key contribution of this paper is to show that a nearly orthogonal lattice basis always contains a shortest lattice vector. We also investigated the uniqueness of nearly orthogonal lattice bases. We proved that if the basis vectors of a nearly orthogonal basis are nearly equal in length, then the lattice essentially contains only one nearly orthogonal basis. These results enable us to solve a fascinating digital color imaging problem called JPEG CHEst.

The applicability of our results on nearly orthogonal bases is limited by the fact that every lattice does not necessarily admit a nearly orthogonal basis. In this sense, lattices that contain a nearly orthogonal basis are somewhat special.

However, in random lattices, nearly orthogonal bases occur frequently when the lattice is sufficiently low-dimensional. Our second main result is that an m-D Gaussian or Bernoulli random basis that spans a lattice in $\mathbb{R}^n$, with $m < 0.071\,n$, is nearly orthogonal almost surely as $n \to \infty$ and with high probability at finite but large n. Consequently, a random $n \times 0.071\,n$ lattice basis contains the shortest lattice vector with high probability. In fact, based on [31], the bound 0.071 can be relaxed to 0.25, at least in the Gaussian case.

We believe that analyzing random lattices using some of the techniques developed in this paper is a fruitful area for future research. For example, we have recently realized (using Corollary 3) that a random $n \times 0.071\,n$ lattice basis is Minkowski-reduced with high probability [8].

Acknowledgments. We thank Gabor Pataki for useful comments and for the reference to Gauss's work in Vazirani's book. We also thank the editor Alexander Vardy and the anonymous reviewers for their thorough and thought-provoking reviews; our work on random lattices was motivated by their comments. Finally, we thank Gregory Sorkin who gave us numerous insights into the properties of random matrices.

REFERENCES

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, *Closest point search in lattices*, IEEE Trans. Inform. Theory, 48 (2002), pp. 2201–2214.
[2] M. Ajtai, *The shortest vector problem in L_2 is NP-hard for randomized reductions*, in Proceedings of the 30th Annual ACM Symposium on Theory of Computing, 1998, pp. 10–19.
[3] A. Akhavi, J.-F. Marckert, and A. Rouault, *On the Reduction of a Random Basis*, e-print math 060433, http://arxiv.org/abs/math/06043331 (2006). (2006).
[4] L. Babai, *On lovaász' lattice reduction and the nearest lattice point problem*, Combinatorica, 6 (1986), pp. 1–14.
[5] H. H. Bauschke, C. H. Hamilton, M. S. Macklem, J. S. McMichael, and N. R. Swart, *Recompression of JPEG images by requantization*, IEEE Trans. Image Process., 12 (2003), pp. 843–849.
[6] E. Candès and T. Tao, *Near optimal signal recovery from random projections: Universal encoding strategies?*, IEEE Trans. Inform. Theory, 25 (2006), pp. 5402–5425.
[7] O. Damen, A. Chkeif, and J. Belfiore, *Lattice code decoder for space-time codes*, IEEE Commun. Lett., 4 (2000), pp. 161–163.
[8] S. Dash and R. Neelamani, *Some Properties of SVP in Random Lattices*, manuscript in preparation, 2006.
[9] H. Daudé and B. Vallée, *An upper bound on the average number of iterations of the LLL algorithm*, Theoret. Comput. Sci., 123 (1994), pp. 95–115.
[10] I. Dinur, G. Kindler, R. Raz, and S. Safra, *Approximating CVP to within almost-polynomial factors is NP-hard*, Combinatorica, 23 (2003), pp. 205–243.
[11] J. L. Donaldson, *Minkowski reduction of integral matrices*, Math. Comput., 33 (1979), pp. 201–216.
[12] N. El-Karoui, *Recent results about the largest eigenvalue of random covariance matrices and statistical applications*, Acta Phys. Polon. B, 36 (2005), pp. 2681–2697.
[13] C. F. Gauss, *Disquisitiones Arithmeticae*, A. A. Clark, ed., Springer-Verlag, New York, 1986 (in English).
[14] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985.
[15] R. Kannan, *Algorithmic geometry of numbers*, Ann. Rev. Comput. Sci., 2 (1987), pp. 231–267.
[16] S. Khot, *Hardness of approximating the shortest vector problem in lattices*, J. ACM, 52 (2005), pp. 789–808.
[17] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534.
[18] A. E. Litvak, A. Pajor, M. Rudelson, and N. Tomczak-Jaegermann, *Smallest singular value of random matrices and geometry of random polytopes*, Adv. Math., 195 (2005), pp. 491–523.
[19] V. A. Marchenko and L. A. Pastur, *Distribution of eigenvalues in certain sets of random matrices*, Mat. Sb., 72 (1967), pp. 407–535 (in Russian).
[20] D. Micciancio, *The shortest vector problem is NP-hard to approximate to within some constant*, SIAM J. Comput., 30 (2001), pp. 2008–2035.
[21] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Kluwer Academic Publishers, Boston, 2002.
[22] R. Neelamani, *Inverse Problems in Image Processing*, Ph.D. dissertation, Rice University, Houston, TX, 2003; also available online from www.dsp.rice.edu/∼neelsh/publications.

[23] R. Neelamani, R. de Queiroz, Z. Fan, S. Dash, and R. G. Baraniuk, *JPEG compression history estimation for color images*, IEEE Trans. Image Process., 15 (2006), pp. 1365–1378.
[24] P. Nguyen and D. Stehlé, *Low-dimensional lattice basis reduction revisited*, in Proceedings of the 6th International Symposium on Algorithmic Number Theory (ANTS VI), Lecture Notes in Comput. Sci. 3076, Springer-Verlag, Berlin, 2004, pp. 338–357.
[25] P. Q. Nguyen and J. Stern, *Lattice reduction in cryptology: An update*, in Proceedings of the 4th International Symposium on Algorithmic Number Theory (ANTS IV), Lecture Notes in Comput. Sci. 1838, Springer-Verlag, Berlin, 2000, pp. 85–112.
[26] W. Pennebaker and J. Mitchell, *JPEG, Still Image Data Compression Standard*, Van Nostrand Reinhold, New York, 1993.
[27] C. Poynton, *A Technical Introduction to Digital Video*, Wiley, New York, 1996.
[28] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, in Proceedings of the 37th annual ACM Symposium on Theory of Computing, New York, 2005, pp. 84–93.
[29] G. Sharma and H. Trussell, *Digital color imaging*, IEEE Trans. Image Process., 6 (1997), pp. 901–932.
[30] J. W. Silverstein, *The smallest eigenvalue of a large dimensional Wishart matrix*, Ann. Probab., 13 (1985), pp. 1364–1368.
[31] G. Sorkin, *private communication*, 2006.
[32] V. V. Vazirani, *Approximation Algorithms*, Springer-Verlag, Berlin, 2001.