On Nearly Orthogonal Lattice Bases

Ramesh Neelamani, Sanjeeb Dash, and Richard G. Baraniuk *

July 14, 2005

Abstract

We study ”nearly orthogonal” lattice bases, or bases where the angle between any basis vector and the linear subspace spanned by the other basis vectors is greater than $\frac{\pi}{3}$ radians. We show that a nearly orthogonal lattice basis always contains a shortest lattice vector. Moreover, if the lengths of the basis vectors are “nearly equal”, then the basis is the unique nearly orthogonal lattice basis, up to multiplication of basis vectors by ± 1. These results are motivated by an application involving JPEG image compression.

Keywords

lattices, shortest lattice vector, orthogonality defect, JPEG, compression.

1 Introduction

Lattices are regular arrangements of points in space, and are studied in numerous fields, including coding theory, number theory, and crystallography [1, 6, 7, 10]. Formally, a lattice is the set of all linear integer combinations of a finite set of vectors. A lattice basis is a linearly independent set of vectors whose linear integer combinations span the lattice points. In this paper we study the properties of lattice bases whose vectors are “nearly orthogonal” to one another.

*R. Neelamani is with the ExxonMobil Upstream Research Company, 3319 Mercer, Houston, TX 77027; Email: neelsh@rice.edu; Fax: 713 431 6161. Sanjeeb Dash is with the IBM T. J. Watson Research Center, Yorktown Heights, NY 10598; Email: sanjeebd@us.ibm.com. R. G. Baraniuk is with the Department of Electrical and Computer Engineering, Rice University, 6100 South Main Street, Houston, TX 77005; Email: richb@rice.edu; Fax: 713 348 6196. R. Neelamani and R. G. Baraniuk were supported by grants from the NSF, AFOSR, ONR, DARPA, and Texas Instruments.

We quantify the closeness to orthogonality of a lattice basis in terms of angles between the basis vectors. We define a basis to be θ-orthogonal if the angle between a 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 greater than $\frac{\pi}{3}$ radians.

Our interest in nearly orthogonal lattices stems from an interesting digital image processing problem. Digital color images are routinely subjected to compression schemes such as JPEG [11]. 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 refer to this problem as JPEG compression history estimation (JPEG CHEst). In [9], we show that the JPEG compression step maps color images into a set of points contained by a collection of related lattices. Further, we show that the JPEG CHEst problem can be solved by estimating the nearly orthogonal bases spanning these lattices. We use some of the results in this paper in a heuristic to solve the JPEG CHEst problem [9].

In this paper, we derive two simple but appealing properties of nearly orthogonal lattice bases.

1. *A $\frac{\pi}{3}$-orthogonal basis always contains a shortest non-zero lattice vector.*

2. *If all the vectors of a θ-orthogonal ($\theta > \frac{\pi}{3}$) basis have lengths no more than $\frac{\sqrt{3}}{\sin\theta+\sqrt{3}\cos\theta}$ times the length of a 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).*

Thus, a nearly orthogonal basis is unique if its vectors are nearly equal in length. Gauss [5] proved the first property for lattices in $\mathbb{R}^2$. We prove (slight generalizations of) both properties for lattices in $\mathbb{R}^n$ for arbitrary n.

The paper is organized as follows. Section 2 provides some basic definitions and well-known results about lattices We formally state our contributions in Section 3 and furnish their proofs in Section 4. Section 5 describes the JPEG CHEst problem, and how our results can be used in a heuristic to solve the problem. We conclude with some discussions of the limitations of our results in Section 6.

2 Lattices

A lattice $\mathcal{L}$ in $\mathbb{R}^n$ is the set of all linear integer combinations of a finite set of vectors, which we assume to be rational; 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 $\mathcal{L}$. A linearly independent set of vectors spanning $\mathcal{L}$ is a *basis* of $\mathcal{L}$.

A lattice has many bases. Any two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ of a lattice $\mathcal{L}$ have the same number of vectors; this common number is denoted by $\dim(\mathcal{L})$. Further, $\mathcal{B}_1$ and $\mathcal{B}_2$ are related (when treated as matrices) as $\mathcal{B}_1 = \mathcal{B}_2\mathcal{U}$, where $\mathcal{U}$ is a *unimodular matrix*; that is, an integer matrix with determinant equal to ± 1. A lattice $\mathcal{L}$ in $\mathbb{R}^n$ is full-dimensional if $\dim(\mathcal{L}) = n$. We consider only full-dimensional lattices in this paper.

The *shortest vector problem* (SVP) consists of finding a vector in a lattice $\mathcal{L}$ with the shortest non-zero length $\lambda(\mathcal{L})$. Here we refer to the Euclidean norm of a vector v in $\mathbb{R}^n$ as its length and denote it by $\|v\|$. SVP is NP-hard under randomized reductions [2], but the decision version of SVP is not known to be NP-complete in the traditional sense.

Orthogonal bases always contain a shortest non-zero lattice vector. Hence, one approach to finding short vectors in lattices is to obtain a basis that is close (in some sense) to orthogonal, and then 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* [7],

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

with det denoting determinant. The Lovász basis reduction algorithm [7], often called the LLL algorithm, obtains an *LLL-reduced* lattice basis in polynomial time. Such a basis has a small orthogonality defect. There are other notions of reduced bases due to Minkowski, and Korkin and Zolotarev (KZ) [6]. Minkowski-reduced and KZ-reduced bases contain the shortest lattice vector, but it is NP-hard to obtain such bases.

We use the following definitions to quantify the closeness to orthogonality of a basis. By an *ordered basis*, 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 $u^T v$ and $\langle u, v\rangle$ to denote the inner product of u and v.

- *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 $[\theta, \frac{\pi}{2}]$. That is,

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

- *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. Thus, a weakly θ-orthogonal basis is assumed to be ordered, whereas a θ-orthogonal basis is not.

In the JPEG CHEst application we describe in Section 5, we will encounter weakly θ-orthogonal bases with $\theta \geq \frac{\pi}{3}$. In $\mathbb{R}^n$, Babai [3] proved that an LLL-reduced basis is θ-orthogonal where $\sin\theta = \left(\frac{\sqrt{2}}{3}\right)^n$; 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.

3 Main Results

It is trivial to show that one of the basis vectors in an orthogonal lattice basis 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

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

Therefore a weakly 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 two dimensions (2-D) every $\frac{\pi}{3}$-orthogonal lattice basis indeed contains a shortest lattice vector and provided a polynomial time algorithm to determine such a basis; see [14] for a nice description. We first show that Gauss's result can be extended to higher-dimensional lattices with an appropriate measure of closeness to orthogonality.

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 non-zero vector in $\mathcal{L}$. More generally,*

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

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 ($\frac{\pi}{3} + \epsilon$)-orthogonal basis contains every shortest non-zero lattice vector (up to multiplication by ± 1).*

Corollary 2 *A $\frac{\pi}{3}$-orthogonal basis contains a shortest non-zero lattice vector.*

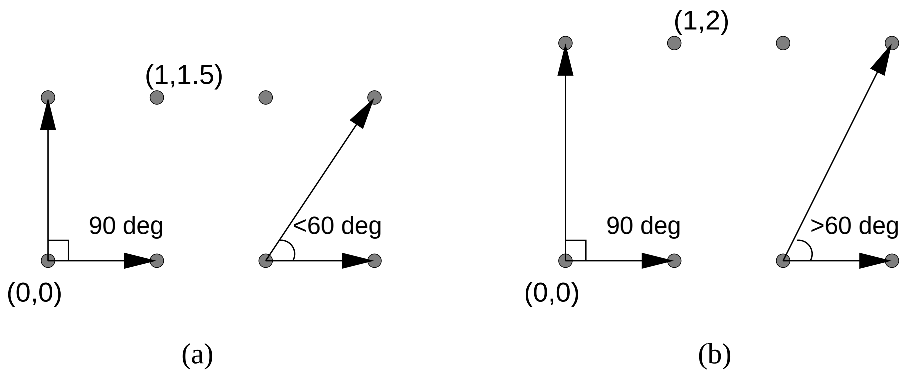

Figure 1: *(a) The vectors comprising the lattice are denoted by circles. One of the lattice bases comprises two orthogonal vectors of lengths* 1 *and* 1.5*. Since* $1.5 < \eta\left(\frac{\pi}{2}\right) = \sqrt{3}$*, the lattice possesses no other basis such that the angle between its vectors is greater than* $\frac{\pi}{3}$ *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* $2 > \eta\left(\frac{\pi}{2}\right)$*, and so this basis is not the only* $\frac{\pi}{3}$*-orthogonal basis.*

For a lattice defined by some basis $\mathcal{B}_1$, a weakly $\frac{\pi}{3}$-orthogonal basis $\mathcal{B}_2 = \mathcal{B}_1\mathcal{U}$ with $\mathcal{U}$ having polynomially bounded size provides a polynomial-size certificate for $\lambda(\mathcal{L})$. However, we do not expect all lattices to have such bases because this would imply that NP=co-NP, assuming SVP is NP-complete. We show in Section 6 that even in $\mathbb{R}^3$, there exist lattices that do not have any 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*

$$\|b_i\| < \eta(\theta) \min_{j\in\{1,2,\ldots,m\}} \|b_j\|, \tag{3}$$

$$\text{with } \eta(\theta) = \frac{\sqrt{3}}{|\sin\theta| + \sqrt{3}|\cos\theta|}, \tag{4}$$

then any $\frac{\pi}{3}$*-orthogonal basis consists of 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 Fig. 1(a) and (b) illustrate 2-D lattices that can be spanned by orthogonal basis vectors. For the lattice in Fig. 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 Fig. 1(b) contains many distinct $\frac{\pi}{3}$-orthogonal bases.

In the JPEG CHEst application [9], the target 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 in $\mathbb{R}^3$ 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 $\mathcal{L}$ in $\mathbb{R}^m$, where $\theta > \frac{\pi}{3}$. Let $\mathcal{U} = (u_{ij})$ be a unimodular matrix such that $\widetilde{\mathcal{B}}\mathcal{U} = \mathcal{B}$. Define*

$$\kappa(\mathcal{B}) = \left(\frac{2}{\sqrt{3}}\right)^{m-1} \times \frac{\max_{i\in\{1,2,\ldots,m\}} \|b_i\|}{\min_{i\in\{1,2,\ldots,m\}} \|b_i\|}. \tag{5}$$

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 lattice in $\mathbb{R}^3$ with $\frac{\max_{m\in\{1,2,3\}}\|b_m\|}{\min_{m\in\{1,2,3\}}\|b_m\|} < 1.5$, 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 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. By rotating the lattice, the basis vectors b_1 and b_2 can be expressed as the columns of

$$\begin{bmatrix} \|b_1\| & \|b_2\|\cos\theta \\ 0 & \|b_2\|\sin\theta \end{bmatrix},$$

with θ the angle between b_1 and b_2. By definition, $\frac{\pi}{3} \le \theta \le \frac{2\pi}{3}$. Any non-zero vector v in the lattice can be expressed as

$$v = \begin{bmatrix} \|b_1\| & \|b_2\|\cos\theta \\ 0 & \|b_2\|\sin\theta \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} u_1\|b_1\| + u_2\|b_2\|\cos\theta \\ u_2\|b_2\|\sin\theta \end{bmatrix}$$

where $u_1, u_2 \in \mathbb{Z}$ and $|u_1| + |u_2| > 0$. The squared-length of v equals

$$\begin{aligned}
\|v\|^2 &= (u_1\|b_1\| + u_2\|b_2\|\cos\theta)^2 + (u_2\|b_2\|\sin\theta)^2 \\
&= |u_1|^2\|b_1\|^2 + |u_2|^2\|b_2\|^2 + 2u_1u_2\|b_1\|\|b_2\|\cos\theta \\
&\geq |u_1|^2\|b_1\|^2 + |u_2|^2\|b_2\|^2 - 2|u_1||u_2|\|b_1\|\|b_2\|\cos\frac{\pi}{3} \\
&= (|u_1|\|b_1\| - |u_2|\|b_2\|)^2 + |u_1||u_2|\|b_1\|\|b_2\| \qquad (6) \\
&\geq \min\left(\|b_1\|^2,\ \|b_2\|^2\right),
\end{aligned}$$

with equality possible only if either $|u_1| + |u_2| = 1$ or $\theta \in \{\frac{\pi}{3}, \frac{2\pi}{3}\}$. 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 $(k-1)$-dimensional lattice. Consider a k-dimensional 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 non-zero 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 $(k-1)$-dimensional 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 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 equality to hold above.

Assume that $u_k \neq 0$ and $u_i \neq 0$ for some $i = 1, 2, \ldots, k-1$. 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 non-zero vectors $\sum_{i=1}^{k-1} u_i\, b_i$ and $u_k b_k$ lies in the interval $\left[\frac{\pi}{3} + \epsilon, \frac{2\pi}{3} - \epsilon\right]$. Invoking Theorem 1 for 2-D lattices, we have

$$\begin{aligned}
\left\|\sum_{i=1}^{k} u_i\, b_i\right\| &\geq \min\left(\left\|\sum_{i=1}^{k-1} u_i\, b_i\right\|,\ \|u_k b_k\|\right) \\
&\geq \min\left(\min_{j\in\{1,2,\ldots,k-1\}} \|b_j\|,\ \|u_k b_k\|\right) \\
&\geq \min_{j\in\{1,2,\ldots,k\}} \|b_j\|. \qquad (7)
\end{aligned}$$

Thus, the set of basis vectors $\{b_1, b_2, \ldots, b_k\}$ contains a shortest non-zero vector in the k-dimensional lattice. Also, if $\epsilon > 0$, then equality is not possible in (7), and the second part of the theorem follows. $\square$

4.2 Proof of Theorem 2

Similar to Theorem 1's proof, 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 lattice 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 in $\mathbb{R}^2$, weak θ-orthogonality is the same as θ-orthogonality. Without loss of generality (w.l.o.g.), we can assume that $1 = \|b_1\| \leq \|b_2\|$. Further, by rotating the 2-D lattice, the basis vectors can be expressed as the columns of

$$\begin{bmatrix} 1 & \|b_2\| \cos \widetilde{\theta} \\ 0 & \|b_2\| \sin \widetilde{\theta} \end{bmatrix},$$

with $\widetilde{\theta} \in [\theta, 2\pi - \theta]$ the angle between b_1 and b_2. Let $\left\{\widetilde{b}_1, \widetilde{b}_2\right\}$ denote another $\frac{\pi}{3}$-orthogonal basis for the same 2-D lattice. Using Theorem 1 and its 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

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

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

The angle between $\widetilde{b}_1$ and $\pm\widetilde{b}_2$, denoted by $\angle\left(\widetilde{b}_1, \pm\widetilde{b}_2\right)$, is given by

$$\angle\left(\widetilde{b}_1, \pm\widetilde{b}_2\right) = \tan^{-1}\left(\left|\frac{\|b_2\| \sin \widetilde{\theta}}{\|b_2\| \cos \widetilde{\theta} \pm u}\right|\right).$$

Since $\angle\left(\widetilde{b}_1, \pm\widetilde{b}_2\right)$ lies in the interval $\left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$ by construction, we have

$$\begin{aligned} \tan^2\left(\frac{\pi}{3}\right) = 3 &\leq \tan^2\left(\angle\left(\widetilde{b}_1, \pm\widetilde{b}_2\right)\right) \\ \Leftrightarrow 3\left(\|b_2\|^2 \cos^2 \widetilde{\theta} + u^2 \pm 2u\|b_2\| \cos^2 \widetilde{\theta}\right) &\leq \|b_2\|^2 \sin^2 \widetilde{\theta} \\ \Leftrightarrow 3u^2 \pm 6u\|b_2\| \cos^2 \widetilde{\theta} + 3\|b_2\|^2 \cos^2 \widetilde{\theta} - \|b_2\|^2 \sin^2 \widetilde{\theta} &\leq 0. \qquad (8) \end{aligned}$$

The left-hand side of (8) is a quadratic expression in u, say $Q(u)$. The roots of $Q(u) = 0$ are given by

$$\frac{1}{6}\left(\pm 6\|b_2\|\cos\widetilde{\theta} \pm \sqrt{\left(6\|b_2\|\cos\widetilde{\theta}\right)^2 - 12\left(3\|b_2\|^2\cos^2\widetilde{\theta} - \|b_2\|^2\sin^2\widetilde{\theta}\right)}\right).$$

Simplifying further, we obtain the roots of $Q(u) = 0$ to be

$$\|b_2\|\left(\pm\cos\widetilde{\theta} \pm \frac{\sin\widetilde{\theta}}{\sqrt{3}}\right).$$

To satisfy $Q(u) \le 0$, u must lie between the roots of $Q(u) = 0$. Hence,

$$\begin{aligned} |u| &\le \|b_2\|\left|\left(\pm\cos\widetilde{\theta} \pm \frac{\sin\widetilde{\theta}}{\sqrt{3}}\right)\right| \\ &\le \|b_2\|\frac{|\sin\widetilde{\theta}| + \sqrt{3}|\cos\widetilde{\theta}|}{\sqrt{3}} \\ &= \frac{\|b_2\|}{\eta\left(\widetilde{\theta}\right)}. \end{aligned}$$

Note that $\eta(\theta)$ is an increasing function of θ for $\frac{\pi}{3} \le \theta \le \frac{\pi}{2}$. Hence we have

$$|u| \le \frac{\|b_2\|}{\eta\left(\widetilde{\theta}\right)} \le \frac{\|b_2\|}{\eta(\theta)} < \|b_1\| = 1.$$

Since $u \in \mathbb{Z}$ and $|u| < 1$, $u = 0$. 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 $n \times n$ matrices defining bases of the same n-dimensional lattice. We can write $\mathcal{B} = \widetilde{\mathcal{B}}U$ for some integer unimodular matrix $U = (u_{ij})$. Using induction on n, we will show that if $\mathcal{B}$ is weakly θ-orthogonal with $\frac{\pi}{3} < \theta \le \frac{\pi}{2}$, if the columns of $\mathcal{B}$ satisfy (3), 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 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 $(n-1)$-dimensional lattices with $n > 2$. Let $b_1, b_2, \ldots, b_n$ denote the columns of $\mathcal{B}$ and let $\widetilde{b}_1, \widetilde{b}_2, \ldots, \widetilde{b}_n$ 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 $b_k = \pm\widetilde{b}_1$ for some

$k \in \{1, 2, \ldots, n\}$. Then

$$\mathcal{B} = \widetilde{\mathcal{B}} \begin{bmatrix} u_{11} & \ldots & u_{1k-1} & \pm 1 & u_{1k+1} & \ldots & u_{1n} \\ & & & \vdots & & & \\ & U_1' & & 0 & & U_2' & \\ & & & \vdots & & & \end{bmatrix} \tag{9}$$

Above, U_1' is a $(n-1) \times (k-1)$ sub-matrix, where as U_2' is a $(n-1) \times (n-k)$ sub-matrix. We will show that $u_{1j} = 0$, for all $j \in \{1, 2, \ldots, n\}$ with $j \neq k$. Define

$$\mathcal{B}_r = \left[\begin{array}{cc} b_k & b_j \end{array} \right], \qquad \widetilde{\mathcal{B}}_r = \left[\begin{array}{cc} \widetilde{b}_1 & \sum_{i=2}^{n} u_{ij} \widetilde{b}_i \end{array} \right]. \tag{10}$$

Then, from (9) and (10),

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

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 $||b_j|| < \eta(\theta) ||b_k||$, 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 $U' = [U_1' \; U_2']$ is also a signed permutation matrix, where

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

with $\mathcal{B}' = [b_1, b_2, \ldots, b_{k-1}, \; b_{k+1}, \ldots, b_n]$ and $\widetilde{\mathcal{B}}' = \left[\widetilde{b}_2, \widetilde{b}_3, \ldots, \widetilde{b}_n\right]$. Observe that $\det(U') = \det(U) = \pm 1$. Both $\mathcal{B}'$ and $\widetilde{\mathcal{B}}'$ are bases of the same $(n-1)$-dimensional lattice as U' is unimodular. $\widetilde{\mathcal{B}}'$ is $\frac{\pi}{3}$-orthogonal, whereas $\mathcal{B}'$ is weakly θ-orthogonal and its columns satisfy (3). By the induction hypothesis, U' is a signed permutation matrix. Therefore, U is also a signed permutation matrix. $\square$

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 $u_1, u_2, \ldots, u_m$,*

$$\left\| \sum_{i=1}^{m} u_i b_i \right\| \geq \left(\frac{\sqrt{3}}{2} \right)^{m-1} \times \max_{i \in \{1,2,\ldots,m\}} \|u_i b_i\|. \tag{11}$$

Lemma 1 can be proved as follows. Consider the vectors b_1 and b_2; the angle θ between them lies in the interval $\left(\frac{\pi}{3}, \frac{2\pi}{3}\right)$. Recall from (6) that

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

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 $\left(\frac{\pi}{3}, \frac{2\pi}{3}\right)$ for $k = 2, 3, \ldots, m$. Hence (11) follows by induction. □

We now proceed to prove Theorem 3 by invoking Lemma 1. Define $\Delta = \left(\frac{\sqrt{3}}{2}\right)^{m-1}$. 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,

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

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

5 JPEG Compression History Estimation (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.

5.1 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 [13], three parameters are sufficient to specify any color perceived by humans.[1] For example, a pixel's color can be conveyed by a vector

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

$w_{RGB} = (w_R, w_G, w_B) \in \mathbb{R}^3$, 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 $P \in \mathbb{R}^{3\times M}$.

5.2 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 [12]

$$\begin{bmatrix} w_Y \\ w_{Cb} \\ w_{Cr} \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.5 \\ 0.5 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} w_R \\ w_G \\ w_B \end{bmatrix}. \tag{12}$$

The quantization step is performed by first choosing a diagonal, positive (non-zero 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 the operation of rounding to the nearest integer. JPEG decompression constructs $P_d = CQP_c = CQ \lceil Q^{-1}C^{-1}P \rfloor$. 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 sub-matrices $P_1, P_2, \ldots, P_k$, but each sub-matrix P_i is quantized with a different quantization matrix Q_i. The compressed image is $P_c = \{P_{c,1}, P_{c,2}, \ldots, P_{c,k}\} = \left\{\lceil Q_1^{-1}C^{-1}P_1 \rfloor, \lceil Q_2^{-1}C^{-1}P_2 \rfloor, \ldots, \lceil Q_k^{-1}C^{-1}P_k \rfloor\right\}$, 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's along with P_c. These stored matrices are utilized to decompress the JPEG image, but are discarded afterwards. Hence we refer to the set $\{C, Q_1, Q_2, \ldots, Q_k\}$ as the *compression history* of the image.

5.3 JPEG CHEst Problem Statement

This paper's contributions are motivated by the following question: *Given a decompressed image* $P_d = \{CQ_1P_{c,1}, CQ_2P_{c,2}, \ldots, CQ_kP_{c,k}\}$ *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*'s?* 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 [4, 8, 9].

5.4 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 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 obtain CQ_i from $CQ_iP_{c,i}$. 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 $0 < \epsilon \leq \frac{\pi}{6}$.[2] Thus, nearly orthogonal lattice bases are central to JPEG CHEst.

5.5 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, $0 < \epsilon \leq \frac{\pi}{6}$.

5.5.1 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

$$\mathcal{B}_i = CQ_i\mathcal{U}_i. \tag{13}$$

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

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 (13).

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

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 satisfy 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 $\mathcal{L}_i$'s. 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 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 1 provides the number of unimodular matrices satisfying constraint 4 alone and also constraints 3 and 4. Clearly,

Table 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

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 5.5.3, we will argue (without proof) that constraints 1 and 2 are likely to have a unique solution in most practical cases.

5.5.2 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 sub-lattice of the 1-D 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's is 1, we can uniquely determine the j-th column of C; the values of Q_i follow trivially.

5.5.3 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 non-unique only if the Q_i's are chosen carefully. For example, let Q be a diagonal matrix with positive diagonal coefficients. Assume that for $i = 1, 2, \ldots, k$, $Q_i = \lambda_i Q$, with $\lambda_i \in \mathbb{R}$ and $\lambda_i > 0$. 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 $Q'_i = \lambda_i I$ 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.

5.5.4 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 [8, 9] for details on the experimental setup and results.

6 Discussion and Conclusions

In this paper, we presented some interesting properties of nearly orthogonal lattice 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. We defined such a basis to be nearly orthogonal when $\theta > \frac{\pi}{3}$ radians. Our main result is that a nearly orthogonal lattice basis always contains a shortest lattice vector. Further, 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.

Our results were motivated by a fascinating digital color imaging application called JPEG compression history estimation (JPEG CHEst). Given a digital color image, JPEG CHEst aims to estimate the settings used during previous JPEG compression operations. These operations make the color image coefficients conform to a lattice. The settings are encoded in a nearly orthogonal basis spanning the lattice. We use some of the results in this paper to design an effective heuristic for JPEG CHEst.

Our definition of nearly orthogonal bases is probably too strong for general applications because there exist lattices with no $\frac{\pi}{3}$-orthogonal bases. Consider the lattice $\mathcal{L}$ spanned by the basis

$$\mathcal{B} = \begin{bmatrix} 1 & 0 & \frac{1}{2} \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}. \tag{14}$$

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 equal to 1,

$$\det(\widetilde{\mathcal{B}}) = \|b_1\|\,\|b_2\|\,\|b_3\|\ |\sin\theta_1|\,|\sin\theta_2| \geq \sin^2\frac{\pi}{3} = \frac{3}{4}. \tag{15}$$

But $\det(\mathcal{B}) = \frac{1}{\sqrt{2}} < \det(\widetilde{\mathcal{B}})$, which shows that the lattice $\mathcal{L}$ with basis $\mathcal{B}$ in (14) has no weakly $\frac{\pi}{3}$-orthogonal basis. Thus lattices that contain a nearly orthogonal basis are somewhat special.

We pose two questions related to our work. First, is a shortest vector of a maximally orthogonal (in terms of θ-orthogonality or other measures such as orthogonality defect) lattice basis a solution of the SVP? Second, how do lattice reduction algorithms perform when the lattice is known to contain a nearly orthogonal basis? Note that currently we understand only the "worst-case" performance of lattice reduction algorithms such as the LLL algorithm. Lattices with nearly orthogonal bases could be used to gauge the "best-case" performance of such algorithms.

Acknowledgments

We would like to thank Gabor Pataki for useful comments and for the reference to Gauss's work in Vazirani's book.

References

[1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2201–2214, Aug. 2002.

[2] M. Ajtai, "The shortest vector problem in L_2 is NP-hard for randomized reductions," in *Thirtieth Annual ACM Symposium on Theory of Computing, ACM Press*, pp. 10–19, 1998.

[3] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, pp. 1–14, 1986.

[4] 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 Processing*, vol. 12, pp. 843–849, Jul. 2003.

[5] C. F. Gauss, *Disquitiones Arithmeticae*. New York: Springer-Verlag, English edition translated by A. A. Clark, 1986.

[6] R. Kannan, "Algorithmic geometry of numbers," *Annual Review of Comp. Sci.* vol. 2, pp. 231–267, 1987.

[7] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematics Annalen*, vol. 261, pp. 515–534, 1982.

[8] R. Neelamani, *Inverse Problems in Image Processing*. Ph.D. dissertation, ECE Dept., Rice University, 2003. `www.dsp.rice.edu/~neelsh/publications/`.

[9] R. Neelamani, R. de Queiroz, Z. Fan, S. Dash, and R. G. Baraniuk, "JPEG compression history estimation for color images," *IEEE Trans. Image Processing*, 2004. To appear.

[10] P. Nguyen and J. Stern, "Lattice reduction in cryptology: An update," in *Lecture notes in Comp. Sci.*, vol. 1838, pp. 85–112, Springer Verlag, 2000.

[11] W. Pennebaker and J. Mitchell, *JPEG, Still Image Data Compression Standard*. Van Nostrand Reinhold, 1993.

[12] C. Poynton, *A Technical Introduction to Digital Video*. New York: Wiley, 1996.

[13] G. Sharma and H. Trussell, "Digital color imaging," *IEEE Trans. Image Processing*, vol. 6, pp. 901–932, July 1997.

[14] V. V. Vazirani, *Approximation Algorithms*. Berlin: Springer, 2001.