Relations Between Minkowski-Reduced Basis and θ-orthogonal Basis of Lattice

Yuyun Chen[1(✉)], Gengran Hu[2], Renzhang Liu[2], Yanbin Pan[2], and Shikui Shang[3]

[1] College of Science, National University of Defense Technology, Changsha 410073, China
kasineya@sina.com
[2] Key Laboratory of Mathematics Mechanization, NCMIS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[3] Department of Mathematics, University of Science and Technology of China, Hefei 230026, China

Abstract. We prove that the angle between any two Minkowski-reduced basis vectors is more than $\pi/3$; if the orthogonal defect of 3-dimension lattice is less than $2/\sqrt{3}$, the Minkowski-reduced basis of the lattice is $\pi/3$-orthogonal; if a weakly θ-orthogonal basis for a lattice with $\theta \geqslant \pi/3$ has been ordered by the Euclidean norm of the vectors, and the minimum length ratio maximum length is more than $2\cos\theta$, the basis is Minkowski reduced. We improve an algorithm used in JPEG CHEst by changing it from heuristic one to deterministic one, furthermore we add a constraint to reduce the number of unimodular matrix that need to determine. *abstract* environment.

Keywords: Lattice · Minkowski-reduced basis · Orthogonal defect · Greedy algorithm · θ-orthogonal

1 Introduction

The theory of reduction of positive definite quadratic forms was introduced by Hermann Minkowski in 1905 [1]. This theory is one of the essential foundations of the geometry of numbers, while another is the lattice theory. The structure of lattice is widely studied. In [2], the authors study the lattices of A and E styles. In [3], the authors study the covering dimension for the class of the finite lattices. A lattice is a discrete additive subgroup of $\mathbb{R}^n$. Any lattice has a lattice basis, i.e., a set $\{b_1, \cdots, b_m\}$ of linearly independent vectors such that the lattice is the set of all integer linear combinations of the b_i's:

$$\mathcal{L}(b_1, \cdots, b_m) = \{\sum_{i=1}^{m} x_i b_i | x_i \in \mathbb{Z}, 1 \leq i \leq m\}.$$

Y.-J. Zhang (Ed.): ICIG 2015, Part III, LNCS 9219, pp. 169–179, 2015.
DOI: 10.1007/978-3-319-21969-1_15

In lattice theory, an important thing is lattice basis reduction. Roughly speaking, a reduced basis is a basis made of almost orthogonal vectors which are reasonably short. This problem is known as lattice reduction and can intuitively be viewed as a vectorial generalization of gcd computation [4]. There exist many different notions of reduction, such as those of Hermite, Minkowski, Hermite-Korkine-Zolotarev, Lenstra-Lenstra-Lovsz. Among these, the most intuitive one is perhaps Minkowskis, and up to dimension four it is arguably optimal compared to all other known reductions, because it reaches all the so-called successive minima of a lattice [4]. Finding good reduced bases has been proved to be important in many fields of computer science and mathematics.

In [5], Neelamani, Dash and Baraniuk define a lattice 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, and if θ is at least $\frac{\pi}{3}$-radians, they call the θ-orthogonal basis "nearly orthogonal" [6]. Because they have proved that a shortest non-zero lattice vector is always contained in a $\frac{\pi}{3}$-orthogonal basis, then SVP for a given $\pi/3$-orthogonal basis is trivial. In [6], Dash, Neelamani, and Sorkin prove additional properties of $\frac{\pi}{3}$-orthogonal bases. They show that the basis is Minkowski reduced for some ordering of the vectors, if all vectors of a θ-orthogonal $\left(\theta > \frac{\pi}{3}\right)$ basis have lengths no more than $\frac{2}{\cos\theta}$ times the length of the shortest basis vector. In this point, we find that if the weakly θ-orthogonal basis vectors rather than θ-orthogonal basis for a lattice $\mathcal{L}$ with $\theta \geqslant \frac{\pi}{3}$ are ordered by their lengths, the shortest vector length ratios the maximum vector length is more than $2\cos\theta$, then the basis is Minkowski reduced. We also find that the angle between any two Minkowski-reduced basis vectors is more than $\frac{\pi}{3}$. In 3-dimension lattice, we find that if the orthogonal defect is less than $\frac{2}{\sqrt{3}}$, the Minkowski-reduced basis is $\frac{\pi}{3}$-orthogonal. We also find some intuitive relations between Minkowski-reduced basis and orthogonal defect of lattice.

The settings used during the previous JPEG compression and decompression, such as the color transformation matrix, and the quantization table will be stored in the JPEG compressed file format and be discarded after decompression. We refer to such previous JPEG compression settings as the images JPEG compression history [5]. The compression history is lost during operations such as conversion from JPEG format to BMP or TIFF format, while it can be used for JPEG recompression, for covert message passing, or to uncover the compression settings used inside digital cameras [7]. In [5], Neelamani, Dash, and Baraniuk give a heuristic algorithm which solved the JPEG CHEst. We find that all the color-transform matrices orthogonal defect which were tested in [5] are less than $\frac{2}{\sqrt{3}}$, and the Minkowski-reduced bases of the lattices spanned by them are $\frac{\pi}{3}$-orthogonal. We use the greedy algorithm [4] to find the Minkowski-reduced bases, and add a constraint when enumerating the unimodular matrix. The improved algorithm is deterministic algorithm.

The paper is organized as follows. Section 2 provides some basic definitions and well-known results about nearly orthogonal basis, formally states our result on Minkowski-reduced basis and orthogonal defect. Section 3 describe the improvement of algorithm. Section 4 is the conclusion.

2 The Relations Between Minkowski-Reduced Basis and Nearly Orthogonal Basis

2.1 Some Definitions

Consider an m-dimensional lattice in $\mathbb{R}^n$, $m \leqslant n$. By an ordered basis of $\mathcal{L}$, we mean a basis with a certain ordering of the basis vector, we use the brace (.,.) for ordered sets and $\{.,.\}$ otherwise, just like Neelamani, Dash and Baraniuk have done in [5]. For vectors $u, v \in \mathbb{R}^n$, we use $\langle u, v\rangle$ to denote the inner product and $\|v\|$ to denote the Euclidean norm of a vector v. Let B_1 and B_2 (when treated as $n \times m$ matrices) be any two bases of $\mathcal{L}$, there exists a unimodular matrix U (i.e., a $m \times m$ matrix with integer entries and determinant ± 1) such that $B_1 = B_2 U$.

The shortest vector problem (SVP) and the closest vector problem (CVP) [8] are most important computational problems of lattice problems. An appealing class of problems involves finding closest and shortest vectors in lattices. The shortest vector problem (SVP) is to find a shortest nonzero vector in $\mathcal{L}$ and the closet vector problem(CVP) is that given a vector $t \in \mathbb{R}^n$ not in $\mathcal{L}$, find a vector in $\mathcal{L}$ that is closest to t. The general CVP is known to be NP-hard and the SVP is NP-hard under a randomized reduction hypothesis.

Neelamani et al. define a lattice basis to be weakly θ-orthogonal, θ-orthogonal and nearly orthogonal [5]. Minkowski gave the notion of Minkowski reduction in 1896. Minkowski reduction is the most intuitive one among all known reduction, and up to dimension four it is arguably optimal, because it reaches all the so-called successive minima of a lattice [4]. We revisit the definitions and give the relations between them.

Definition 1. *(Weak θ-orthogonality) [5]. An ordered set of vectors $(b_1, b_2, \cdots, b_m)$ is weakly θ-orthogonal if for $i = 2, 3, \cdots, m$, the angle between b_i and the subspace spanned by $\{b_1, b_2, \cdots, b_{i-1}\}$ lies in the range $\left[\theta, \frac{\pi}{2}\right]$. That is,*

$$\cos^{-1}\left(\frac{|\langle b_i, \sum_{j=1}^{i-1} \alpha_i b_i\rangle|}{\|b_i\| \cdot \|\sum_{j=1}^{i-1} \alpha_i b_i\|}\right) \geq \theta,$$

for all $\alpha_j \in \mathbb{R}$ with $\sum_j |\alpha_j| > 0$.

If a basis is a weakly θ-orthogonal basis, at first, it is ordered, secondly, the angle between any two basis vectors is more than θ.

Definition 2. *(θ-orthogonality) [5]. A set of vectors $\{b_1, b_2, \cdots, b_m\}$ is θ-orthogonal if every ordering of the vectors yields a weakly θ-orthogonal set.*

Definition 3. *(Nearly orthogonal) [5]. A θ-orthogonal basis is deemed to be nearly orthogonal if θ is at least $\frac{\pi}{3}$ radians.*

We do not expect all rational lattices to have such bases because this would imply that NP=co-NP [5]. For example, the basis:

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

span the lattice $\mathcal{L}$, but $\mathcal{L}$ does not have any weakly $\frac{\pi}{3}$-orthogonal basis.

Definition 4. *(Successive minimum) [9]. Let $\mathcal{L}$ be a lattice of rank m. For $i \in \{1, \cdots, m\}$, we define the ith successive minimum as:*

$$\lambda_i(\mathcal{L}) = inf\left\{r \middle| dim(span(\mathcal{L} \cap \overline{B}(0,r))) \geq i\right\},$$

where

$$\overline{B}(0,r) = \left\{x \in \mathbb{R}^n \middle| \|x\| \leqslant r\right\}$$

is the closed ball of radius r around 0.

Definition 5. *(Orthogonal Defect) [10]. The orthogonal defect of a latticxe basis $\{b_1, b_2, \cdots, b_m\}$ is*

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

with det denoting determinant.

Definition 6. *(OD-r-orthogonality). Let $r \in \mathbb{R}$, a set of vectors $\{b_1, b_2, \cdots, b_m\}$ is OD-r-orthogonal if the orthogonal defect is at most r.*

Definition 7. *(Minkowski reduced) [6]. An ordered basis $(b_1, b_2, \cdots, b_m)$ is Minkowski reduced if b_1 is a shortest lattice vector, and for $i \in \{2, 3, \cdots, m\}$, b_i is a shortest vector among all the lattice vectors $\tilde{b_i}$ s.t. $\{b_1, b_2, \cdots, b_{i-1}, \tilde{b_i}\}$ can be extended to a complete lattice basis.*

A basis of a m-dimensional lattice that reaches the m minima must be Minkowski reduced, but a Minkowski-reduced basis may not reach all the minima, except the first four ones: if $(b_1, b_2, \cdots, b_m)$ is a Minkowski-reduced basis, then we have

$$\|b_i\| = \lambda_i(\mathcal{L}), 1 \leqslant i \leqslant min(d, 4),$$

but the best theoretical upper bound known for $\|b_d\|/\lambda_d(\mathcal{L})$ grows exponentially in d. Therefore, a Minkowski-reduced basis is optimal in a natural sense up to dimension four. There is a classical result states that the orthogonal defect of a Minkowski-reduced basis can be upper-bounded by a constant that only depends on the lattice dimension.

2.2 Some Results

Theorem 1. *[5] Let $B = (b_1, b_2, \cdots, b_m)$ be an ordered basis of a lattice $\mathcal{L}$. If B is weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal, for $0 \leqslant \epsilon \leqslant \frac{\pi}{6}$, then a shortest vector in B is a shortest non-zero vector in $\mathcal{L}$. More generally,*

$$min_{j \in \{1,2,\cdots,m\}} \|b_j\| \leqslant \|\sum_{i=1}^{m} u_i b_i\|,$$

for all $u_i \in \mathbb{Z}$ with $\sum_{i=1}^{m} |u_i| \geqslant 1$, with equality possible only if $\epsilon = 0$ or $\sum_{i=1}^{m} |u_i| = 1$.

From Theorem 1, we conclude that if $\theta \geqslant \frac{\pi}{3}$, the weakly θ-orthogonal lattice basis contain a shortest lattice vector, so, it is not easier to find a weakly θ-orthogonal lattice basis $\left(\theta \geqslant \frac{\pi}{3}\right)$ than to find the shortest vector.

Corollary 1. *[5] If $0 < \epsilon \leqslant \frac{\pi}{6}$, then a weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal basis contains every shortest non-zero lattice vector(up to multiplication by ± 1).*

Theorem 2. *[5] Let $B = (b_1, b_2, \cdots, b_m)$ be a weakly θ-orthogonal basis for a lattice $\mathcal{L}$ with $\theta > \frac{\pi}{3}$. For all $i \in \{1, 2, \cdots, m\}$, if*

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

with

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

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

This means that when the lengths of its basis vectors are almost equal, a nearly orthogonal basis is essentially unique.

Theorem 3. *[5] Let $B = (b_1, b_2, \cdots, b_m)$ and $\widetilde{B}$ be two weakly θ-orthogonal bases for a lattice $\mathcal{L}$, where $\theta > \frac{\pi}{3}$. Let $U = (u_{ij})$ be a unimodular matrix such that $B = \widetilde{B}U$.*

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

then $|u_{ij}| \leqslant \kappa(B)$, for all i and j.

From Theorem 3, we know that if a weakly $\frac{\pi}{3}$-orthogonal basis vectors transform into another weakly orthogonal basis by a unimodular matrix, the coefficient of unimodular matrix will be small.

Theorem 4. *[6] Let $B = b_1, b_2, \cdots, b_m$ be a θ-orthogonal basis for a lattice $\mathcal{L}$ with $\theta \geqslant \frac{\pi}{3}$. Further, suppose that*

$$\frac{min_i \|b_i\|}{max_i \|b_i\|} \geqslant 2\cos\theta.$$

Then some ordering of the basis is Minkowski reduced.

The proof of Theorem 4 is omitted, the detail can be found in [6]. From Theorem 4, we can quickly get the Theorem 5 whose conditions are not harder than Theorem 4.

Theorem 5. *Let $B = (b_1, b_2, \cdots, b_m)$ be a weakly θ-orthogonal basis for a lattice $\mathcal{L}$ with $\theta \geqslant \frac{\pi}{3}$, and it has been ordered by the Euclidean norm of the vectors, if*

$$\frac{min_i \|b_i\|}{max_i \|b_i\|} \geqslant 2\cos\theta,$$

then $B = (b_1, b_2, \cdots, b_m)$ is Minkowski reduced.

Theorem 6. *Let $B = (b_1, b_2, \cdots, b_m)$ be a Minkowski-reduced basis for a lattice $\mathcal{L}$, the angle between b_i and b_j is θ_{ij}, for all $i, j \in \{1, 2, \cdots, m\}$, $i \neq j$, then $|cos\theta_{ij}| \leqslant \frac{1}{2}$.*

Proof. By the definition of Minkowski-reduced basis, we have

$$\|b_1\| \leqslant \|b_2\| \leqslant \cdots \leqslant \|b_m\|.$$

For any $i < j$, we have

$$\|b_j\| \leqslant \|b_i + b_j\|,$$

$$\|b_j\|^2 \leqslant \|b_i + b_j\|^2 = \|b_i\|^2 + \|b_j\|^2 + 2\langle b_i, b_j\rangle.$$

Delete the $\|b_j\|^2$ from two sides of inequality, we have

$$\|b_i\|^2 + 2\langle b_i, b_j\rangle \geqslant 0,$$

then

$$\left|\frac{\langle b_i, b_j\rangle}{\|b_i\| \cdot \|b_j\|}\right| \leqslant \left|\frac{\langle b_i, b_j\rangle}{\|b_i\|^2}\right| \leqslant \frac{1}{2}.$$

Theorem 7. *If the orthogonal defect of 3-dimension lattice $\mathcal{L}$ is less than $\frac{2}{\sqrt{3}}$, then there exits $\epsilon > 0$ such that the Minkowski-reduced basis of the lattice is $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal.*

Proof. Let $B = \{b_1, b_2, b_3\}$ be the basis whose orthogonal defect is smaller than $\frac{2}{\sqrt{3}}$. Let us define the angle between b_1 and b_2 is θ_{12}, the angle between b_3 and the subspace spanned by $\{b_1, b_2\}$ is θ_{3-12}. Because

$$det(\mathcal{L}) = \|b_1\| \cdot \|b_2\| \cdot \|b_3\| \cdot \sin\theta_{12} \cdot \sin\theta_{3-12},$$

we can get that

$$\frac{\|b_1\| \cdot \|b_2\| \cdot \|b_3\|}{det(\mathcal{L})} = \frac{1}{\sin\theta_{12} \cdot \sin\theta_{3-12}} < \frac{2}{\sqrt{3}},$$

i.e.

$$\sin\theta_{12} \cdot \sin\theta_{3-12} > \frac{\sqrt{3}}{2}.$$

Let $\{m_1, m_2, m_3\}$ be the Minkowski-reduced basis of the lattice $\mathcal{L}$, from the definition of Minkwoski-reduced basis, we have that

$$\|m_1\| = \lambda_1(\mathcal{L}), \|m_2\| = \lambda_2(\mathcal{L}), \|m_3\| = \lambda_3(\mathcal{L}).$$

Let the angle between m_1 and m_2 be φ_{12}, and the angle between m_3 and the subspace spanned by $\{m_1, m_2\}$ be φ_{3-12}. The same as above,

$$\|m_1\| \cdot \|m_2\| \cdot \|m_3\| \cdot \sin\varphi_{12} \cdot \sin\varphi_{3-12} = det(\mathcal{L}).$$

Because

$$\|m_1\| \cdot \|m_2\| \cdot \|m_3\| \leqslant \|b_1\| \cdot \|b_2\| \cdot \|b_3\|,$$

then

$$\sin\varphi_{12}\cdot\sin\varphi_{3-12}\geqslant\sin\theta_{12}\cdot\sin\theta_{3-12}>\frac{\sqrt{3}}{2}.$$

Obviously,

$$\sin\varphi_{12}\neq\frac{\sqrt{3}}{2},$$

otherwise,

$$\sin\varphi_{3-12}>1,$$

thus

$$\sin\varphi_{12}>\frac{\sqrt{3}}{2}.$$

At the same time, $\sin\varphi_{12}\leqslant 1$, we have

$$\sin\varphi_{3-12}>\frac{\sqrt{3}}{2},$$

i.e.

$$\varphi_{3-12}>\frac{\pi}{3}.$$

Thus the Minkowski-reduced basis is weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal. Because during the period of comparing the size of $\|m_1\|\cdot\|m_2\|\cdot\|m_3\|$ and $\|b_1\|\cdot\|b_2\|\cdot\|b_3\|$, we need not consider the order of the basis, thus we can conclude that the Minkowski-reduced basis is $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal.

We have known of some properties of the weakly θ-orthogonality, θ-orthogonality, nearly orthogonality, orthogonal defect and the Minkowski-reduced basis. It is easy to induce the relations between them:

(i) Let $B=(b_1,b_2,\cdots,b_m)$ be a weakly θ-orthogonal basis for a lattice $\mathcal{L}$, then B is $(\sin\theta)^{1-n}$-orthogonal basis.
(ii) Changing the ordering of the basis vectors will change the weakly θ-orthogonality , but will not change the OD-r-orthogonality.
(iii) Let $B=(b_1,b_2,\cdots,b_m)$ be a OD-r-orthogonal basis for a lattice $\mathcal{L}$, then B is $\arcsin\frac{1}{r}$-orthogonal basis.

3 JPEG Compression History Estimation (CHEst)

In this section, we briefly describe the JPEG CHEst problem firstly; secondly, we describe the algorithm that Neelamani et al. gives in [5]; thirdly, we apply the properties of orthogonal defect of color-transform matrix and give a Deterministic algorithm.

3.1 JPEG CHEst Problem Statement

In [5,11], the authors discussed the JPEG CHEst problem as follows:

Given a decompressed image

$$P_d = \{CQ_1P_{c,1}, CQ_2P_{c,2}, \cdots, CQ_kP_{c,k}\}, C \in \mathbb{R}^{3\times 3}$$

which is a color-transform matrix, the columns of C form a different basis for the color space spanned by the R, G and B vectors. P is the image and is mapped to $C^{-1}P$. Choose a diagonal, positive and integer quantization matrix Q, then compute the quantized compressed image as

$$p_c = \lceil Q^{-1}C^{-1}P \rfloor$$

where $\lceil \cdot \rfloor$ means rounding to the nearest integer. JPEG decompression constructs

$$P_d = CQP_c = CQ\lceil Q^{-1}C^{-1}P \rfloor.$$

In fact, during compression, the image matrix P is decomposed into different frequency components $P = \{P_1, P_2, \cdots, P_k\}$, $k > 1$. Then the same C and different quantization matrix Q_i are applied to the sub-matrices P_i, $i = 1, \cdots, k$. The compressed image is

$$P_c = \{P_{c,1}, P_{c,2}, \cdots, P_{c,k}\} = \{\lceil Q_1^{-1}C^{-1}P_1 \rfloor \lceil Q_2^{-1}C^{-1}P_2 \rfloor, \cdots, \lceil Q_kC^{-1}P_k \rfloor\},$$

and the decompressed image is

$$P_d = \{CQ_1P_{c,1}, CQ_2P_{c,2}, \cdots, CQ_kP_{c,k}\}.$$

The JPEG compressed file format stores the C and the matrices Q_i with P_c. When decompressing the JPEG image, we will use the stored matrices and discarded them afterward. We call the set $\{C, Q_1, Q_2, \cdots, Q_k\}$ the compression history of the image.

3.2 Neelamani, Dash and Baraniuk's Contributions [5] Revisited

Neelamani, Dash and Baraniuk's contributions [5] are a heuristic algorithm to solve the following question: given a decompressed image

$$P_d = \{CQ_1P_{c,1}, \cdots, CQ_kP_{c,k}\}$$

and some information about the structure of C and the Q_i's, how can we find the color transform C and the quantization matrices Q_i's.

We can see the columns of $CQ_iP_{c,i}$ lie on a 3-D lattice basis with basis CQ_i, because $P_{c,i}$ are integer matrices. The estimation of CQ_is comprise the main step in JPEG CHEst. What Neelamani et al. have done is exploiting the near-orthogonality of C to estimate the products CQ_i. Neelamani et al. use the LLL algorithm to compute LLL-reduced bases B_i for each $\mathcal{L}$ spanned by CQ_i, but such B_i are not guaranteed to be weakly $\left(\frac{\pi}{3} + \epsilon\right)$-orthogonal. Because B_i and

CQ_i are the bases of the same lattice $\mathcal{L}_i$, there exist some unimodular matrix U_i, such that

$$B_i = CQ_iU_i,$$

then estimating CQ_i is equivalent to estimating the respective U_i. Using the theorems above, Neelamani et al. list the constraints that the correct U_is must satisfied at first, secondly, they enumerate a lot of U_i satisfying Theorems 1 and 3, then test constraints that Neelamani et al. list in [5]. At last, by a four-step heuristic algorithm, they can find the solution. Neelamani et al. believe that the solution can be non-unique only if the Q_is are chosen carefully, but JPEG employ Q_is that are not related in any special way. Therefore, they believe that for most practical cases JPEG CHEst has a unique solution. For clarity, the correct U_is should satisfy some constraints as follows [5]:

1. The U_i's are such that $B_iU_i^{-1}$ is weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal.
2. The product $U_iB_i^{-1}B_jU_j^{-1}$ is diagonal with positive entries for any $i, j \in \{1, 2, \cdots, k\}$.
3. The columns of U_i corresponding to the shortest columns of B_i are the standard unit vectors times ± 1.
4. All entries of U_i are $\leqslant \kappa(B_i)$ in magnitude.

Neelamani, Dash and Baraniuks heuristic algorithm [5] is as follows:

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

3.3 Our Improvement

What we want to do is to improve the algorithm that Neelamani, Dash and Baraniuk [5] solved the JPEG CHEst problem. The algorithm used in [5] is heuristic, because in the step (i), constructing a weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal basis B_i for at least one lattice $\mathcal{L}_i$, $i \in \{1, 2, \cdots, k\}$ is uncertain. Using the property of orthogonal defect of the color-transform matrix C, we can exactly construct a $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal basis B_i for every lattice $\mathcal{L}_i$, $i \in \{1, 2, \cdots, k\}$.

Neelamani, Dash and Baraniuk [5] have verified that all C's used in practice are weakly $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal, with $0 < \epsilon \leqslant \frac{\pi}{6}$, while we have verified that all C's used in practice whose orthogonal defect is less than $\frac{2}{\sqrt{3}}$. By Theorem 6, we find that the Minkowski-reduced basis of lattice spanned by all C's used in practice is $\left(\frac{\pi}{3}+\epsilon\right)$-orthogonal. We can use the greedy algorithm to find the Minkowski-reduced basis of the lattice. From now on, the algorithm becomes a deterministic algorithm. And because C's used in practice whose orthogonal

defect is less than $\frac{2}{\sqrt{3}}$, we can change constraint 1 as follows: the U_i's are such that $B_i U_i^{-1}$'s orthogonal defect is less than $\frac{2}{\sqrt{3}}$. In step (iii) of the algorithm in [5], besides satisfy the constraint 3 and constraint 4 at first, every unimodular matrix U_{ij} should satisfy the following constraint: every unimodular matrix U_{ij} by B_i is some basis M_i of lattice $\mathcal{L}_i$, if M_is orthogonal defect is less than $\frac{2}{\sqrt{3}}$, then go on to test the other constraints, otherwise discard the U_{ij}. Add the constraint, we will greatly reduce the number of the unimodular matrix tested.

4 Conclusion

In this paper, we derived some interesting relations among Minkowski-reduced basis, orthogonal defect and nearly orthogonal lattice basis. We prove that the angle between Minkowski-reduced basis vectors is in $\left[\frac{\pi}{3}, \frac{2\pi}{3}\right]$, and if the orthogonal defect of 3-dimension lattice $\mathcal{L}$ is less than $\frac{2}{\sqrt{3}}$, the Minkowski-reduced basis of the lattice is $\frac{\pi}{3}$-orthogonal. We use the property of the Minkowski-reduced basis to improve the algorithm in [5] by removing the heuristic hypothesis, thus our algorithm is deterministic. We also use the orthogonal defect to constraint the unimodular matrix to greatly reduce the number of the unimodular matrix that should be tested next.

Acknowledgment. This work was supported by the grants from the Student Research Innovation Scholarship of Hunan Province (Grant No. CX2014B010) and the National Natural Science Foundation of China (Grant No. 61304119).

References

1. Donaldson, J.L.: Minkowski reduction of integral matrices. Math. Comput. **33**(145), 201–216 (1979)
2. Dube, T., Georgiou, D.N., Megaritis, A.C., Moshokoa, S.P.: A study of covering dimension for the class of finite lattices. Discrete Math. **338**(7), 1096–1110 (2015)
3. Jorge, G.C., de Andrade, A.A., Costa, S.I., Strapasson, J.E.: Algebraic constructions of densest lattices. J. Algebra **429**, 218–235 (2015)
4. Nguyên, P.Q., Stehlé, D.: Low-dimensional lattice basis reduction revisited. In: Buell, D.A. (ed.) ANTS 2004. LNCS, vol. 3076, pp. 338–357. Springer, Heidelberg (2004)
5. Neelamani, R., Dash, S., Baraniuk, R.G.: On nearly orthogonal lattice bases and random lattices. SIAM J. Discrete Math. **21**(1), 199–219 (2007)
6. Dash, R.S., Sorkin, G.: On nearly orthogonal lattice bases and minkowski reduction, IBM Research Report RC (24696)
7. Neelamani, R.: Inverse Problems in Image Processing. Rice University, Houston, Texas (2003)
8. Agrell, E., Eriksson, T., Vardy, A., Zeger, K.: Closest point search in lattices. IEEE Trans. Inf. Theory **48**(8), 2201–2214 (2002)
9. Wang, Y., Shang, S., Gao, F., Huang, M.: Some sufficient conditions of the equivalence between successive minimal independent vectors and minkowski-reduced basis in lattices. Sci. Sinica (Math.) **8**, 001 (2010)

10. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
11. Bauschke, H.H., Hamilton, C.H., Macklem, M.S., McMichael, J.S., Swart, N.R.: Recompression of JPEG images by requantization. IEEE Trans. Image Process. **12**(7), 843–849 (2003)