Lattice Packing from Quaternion Algebras

By

Fang-Ting Tu* and Yifan YANG**

Abstract

In this paper, we will discuss ideal lattices from a definite quaternion algebra, which is an analogue of the ideal lattices from number fields. In particular, we will construct the root lattices $D_4, E_8$, the Coxeter-Todd lattice $K_{12}$, the laminated lattice $\Lambda_{16}$, the Leech lattice $\Lambda_{24}$, and a lattice of rank 32 with center density $3^{16}/2^2$. All of them have the highest densities known in their own dimensions 4, 8, 16, 24, and 32.

§1. Introduction

A lattice in the Euclidean space $\mathbb{R}^n$ is a pair $(\Lambda, B)$ of a free $\mathbb{Z}$-module $\Lambda$ of finite rank, and a positive definite symmetric $\mathbb{Z}$-bilinear form $B$. The center density of this lattice is defined by

$$\delta_\Lambda := \frac{||v||^n}{2^n \sqrt{\det \Lambda}},$$

where $v$ is a nonzero vector in $\Lambda$ with the smallest norm (see [10]). Lattices are closely related to the sphere packing problem. In mathematics, there are many applications of lattice packing, such as in number theory and coding theory.

There are many ways to construct lattices, and one of them is using ideals from number fields([3, 4, 5, 6, 7]). We call such lattices ideal lattices, which is obtained by a scaled trace construction. To be more precise, we let $I$ be an ideal in a totally real...
number field or a CM field $K$, and $\alpha$ be a totally positive element in $K$. Then we have a positive definite quadratic form given by

$$Q_\alpha(x) = \text{tr}_F^\mathbb{Q}(\alpha xx^\sigma),$$

where $\sigma : K \rightarrow K$ is a $\mathbb{Q}$-linear involution and $F$ is the subfield of $K$ fixed by $\sigma$. In this case, we let the pair $(I, \alpha)$ denote the ideal lattice associated to the quadratic form $Q_\alpha$. Bayer-Fluckiger used this to construct the root lattice $E_8$, the Coxeter-Todd lattice $K_{12}$, and the Leech lattice $\Lambda_{24}$ ([5]). Besides, she gave a criterion to determine whether a number field of class number one is Euclidean ([5]), and discussed upper bounds of Euclidean minima of some special number fields ([8]).

As the ideal lattices from a number field, we can also construct lattices from the ideals of a definite quaternion algebra over a totally real number field [1, 2, 11, 14, 15, 16, 17]. By a suitable scaled trace construction, the reduced trace of such kind quaternion algebra gives rise a non-degenerate symmetric bilinear form. The aim of this paper is to use this construction of ideal lattices from definite quaternion algebras to construct the densest known lattices in dimension 4, 8, 16, 24, and 32. In particular, they are the root lattices $D_4$, $E_8$, the Coxeter-Todd lattice $K_{12}$, laminated lattice $\Lambda_{16}$, the Leech lattice $\Lambda_{24}$, and a lattice of rank 32 with center density $3^{16}/2^{24}$, which has the best known density in dimension 32.

In this paper, we will first discuss quadratic forms on quaternion algebras in section 2. In section 3, we will introduce lattice construction from quaternion algebras, then we establish a determinant formula, and finally give some examples for construction of lattices.

\section{2. Quaternion Algebras}

In this section, we will briefly recall some basic definitions and properties of quaternion algebras, especially quaternion algebras over a local field or number field. Most of the materials are referred to [18]. From now on, we let $K$ be a field and its characteristic is not 2.

\subsection{2.1. Quaternion algebras and quadratic forms}

A \textit{quaternion algebra} $A$ over a field $K$ is a central simple algebra of dimension 4 over $K$, or equivalently, there exist $i, j \in A$ and $a, b \in K^*$ so that

$$A = K + Ki + Kj + Kij, \quad i^2 = a, \quad j^2 = b, \quad ij = -ji.$$  

In such case, we denote by $(\frac{a, b}{K})$ the quaternion algebra $A$, which has canonical $K$-basis $\{1, i, j, k = ij\}$. 

230 FANG-TING Tu, YIFAN YANG
Notice that an element $h$ in a quaternion algebra satisfies a monic polynomial equation over $K$ of degree at most 2. Therefore, any quaternion algebra $A = \left( \begin{array}{c} a \\ h \\ K \end{array} \right)$ is provided with a unique $K$-linear anti-involution $\cdot : A \rightarrow A$, which is called conjugation. The reduced trace on $A$ is defined by $\text{tr}(h) = h + \overline{h}$; the reduced norm is defined to be $N(h) = h\overline{h}$. We remark that $\text{tr}(h) = 2h$ and $N(h) = h^2$, while $h$ lies in the center $K$. Then these maps lead to a nondegenerate symmetric $K$-bilinear form on $A$, which is given by $B(x, y) = \text{tr}(xy)$.

§ 2.2. Classification of Quaternion algebras

For a local field $K$, there are at most 2 structures of quaternion algebras over $K$, up to isomorphism. If $K = \mathbb{C}$, there is only one structure for $\mathbb{C}$-quaternion algebra, the matrix algebra $M_2(\mathbb{C})$. For the Archimedean local field $\mathbb{R}$, a quaternion algebra over $\mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$ or the quaternions of Hamilton, $\mathbb{H}$. If $K$ is non-Archimedean, then a quaternion algebra over $K$ is either isomorphic to $M_2(K)$ or the unique division quaternion algebra over $K$.

We now recall the classification of quaternion algebras over a number field. Let $K$ be a number field, $v$ be a place of $K$, and $K_v$ be the local field respect to $v$. A quaternion algebra $A$ over a number field $K$ is said to be ramified at $v$ if $A_v = A \otimes_K K_v$ is a division algebra.

Let $\text{Ram}(A)$ denote the set of ramified places of $A$. Then the set $\text{Ram}(A)$ is even. Moreover, if $S$ is a finite set of noncomplex places of $K$ such that $|S|$ is even, then there exists a quaternion algebra $A$ over $K$ such that $\text{Ram}(A) = S$. Therefore, if an even number of noncomplex places of $K$ is given, then there exists one and only one $K$-quaternion algebra that ramifies exactly at these places.

In the case of a totally real number field $K$, if a quaternion algebra over $K$ is ramified at all the real infinite places, we say that the quaternion algebra is definite; otherwise, we call it indefinite. We remark that a quaternion algebra $A$ is definite if and only if the quadratic form given by $B(x, y) = \text{tr}(xy)$ on $A$ is positive definite.

§ 2.3. Ideals in Quaternion Algebras

As the fractional ideals in a number field, there is a similar theory for ideals in a quaternion algebra. Let $R$ be a Dedekind domain and $K$ be its field of fractions. Let $A$ be a quaternion algebra over $K$. An ideal of $A$ is a complete $R$-lattice in $A$. If an ideal of $A$ is also a ring with unity, it is called an order. A maximal order of $A$ is an order that is not properly contained in another order of $A$.

If $I$ is an ideal and $O$ is an order of $A$. We say that $I$ is a left ideal of $O$ if $OI \subseteq I$; $I$ is a right ideal of $O$ if $IO \subseteq I$. The inverse of $I$ is defined to be $I^{-1} = \{h \in A : IhI \subseteq I\}$, which is also an ideal. The norm of $I$ is the $R$-fractional
ideal generated by \( \{N(x) : x \in I \} \). We denote \( N(I) \) the norm of \( I \). The dual \( I^* \) of \( I \) is \( I^* = \{ h \in A : \mathrm{tr}(h \overline{I}) \subset R \} \). The discriminant of an order \( \mathcal{O} \) is \( \text{disc}(\mathcal{O}) = N(\mathcal{O}^*)^{-1} \). It is known that the discriminant of \( \mathcal{O} \) is an \( R \)-ideal generated by the set

\[
\{ \det(\mathrm{tr}(h_i \overline{h_j})) : 1 \leq i, j \leq 4, h_i \in \mathcal{O} \}.
\]

Moreover, if \( \mathcal{O} \) has a free \( R \)-basis \( \{ h_1, h_2, h_3, h_4 \} \), then \( \text{disc}(\mathcal{O}) \) is the principal \( R \)-ideal \( \det(\mathrm{tr}(h_i \overline{h_j}))R \).

\section{Lattice from Quaternion Algebras}

In this section, we will discuss lattices from a definite quaternion algebra, and then construct lattices have the highest densities known in their own dimensions 4, 8, 16, 24, and 32.

\subsection{From quaternion algebra to ideal lattices}

Let \( K \) be a totally real number field and \( A \) be a definite quaternion algebra over \( K \). The ring of integers of \( K \) and the discriminant of \( K \) are denoted \( \mathcal{O}_K \) and \( d_K \), respectively. Also, the maps \( \mathrm{tr}_K \), \( N_K \) mean the trace map and the norm map defined on \( K \).

Now, if \( I \) is an ideal in \( A \) and \( \alpha \) is a totally positive element in \( K \), then we have a positive definite quadratic form \( Q_\alpha : I \to \mathbb{Q} \) given by

\[
Q_\alpha(x) = \mathrm{tr}_K(\alpha x \overline{x}),
\]

where \( \overline{x} \) is the conjugate of \( x \) in \( A \). In this case, we let \( (I, \alpha) \) denote the lattice associated to the quadratic form \( Q_\alpha \). Moreover, the associated symmetric bilinear form is given by

\[
B(x, y) = \mathrm{tr}_K(\alpha \mathrm{tr}(x \overline{y})).
\]

For example, the maximal order \( \mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z} \frac{1+i+j+ij}{2} \) in the Hamilton quaternions over \( \mathbb{Q} \), \( A = \left( \frac{-1}{\mathbb{Q}} \right) \), and the number 1 forms a lattice \( (\mathcal{O}, 1) \) with density 1/8. In particular, this lattice is isomorphic to \( D_4 \).

\subsection{Determinant formula}

As the determinant formula in the case of ideal lattice \( (I, \alpha) \) from number field, \( \det I = |d_K|N_K(I)^2N_K(\alpha) \), we have a similar result for the lattices obtained by quaternion algebra.

\textbf{Proposition 3.1.} Let \( K \) be a totally real algebraic number field with discriminant \( d_K \). Let \( A \) be a quaternion algebra over \( K \) and \( \mathcal{O} \) be a maximal order of \( A \). If \( I \)
is a right ideal of $\mathcal{O}$ and $\alpha$ is a totally positive element in $K$ so that $(I, \alpha)$ is a lattice. Then we have the following identity

$$\det M = N(\text{disc} \mathcal{O})^2 d_K^4 N_K \alpha N_K(N(I))^4,$$

where $M$ is the Gram matrix of $I$ associated to the element $\alpha$, $N(I)$ is norm of the ideal $I$, $N_K$ is the norm map defined on $K$ over $\mathbb{Q}$, and disc($\mathcal{O}$) is the discriminant of $\mathcal{O}$.

**Proof.** First, we need to determine a $\mathbb{Z}$-basis for $I$. Suppose $K$ is of degree $n$. A $\mathbb{Z}$-basis for $I$ is $\beta = \{\beta_i v_j\}$, where $\{\beta_i\}_{1 \leq i \leq n}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and $\{v_j\}_{1 \leq j \leq 4}$ is an $\mathcal{O}_K$-basis for $I$. Then the Gram matrix associated to $I$ with respect to $\beta$ can be written as $M = (A_{ij})$, where $A_{ij} = (a_{\ell m})$ is an $n \times n$ matrix with entries

$$a_{\ell m} = \text{tr}_K(\alpha \text{tr}(\beta_i v_i \overline{\beta_m v_j})).$$

Consequently, one can expand $a_{\ell m}$ as

$$a_{\ell m} = \sum_{k=1}^{n} \sigma_k(\alpha \beta_i \text{tr}(v_i \overline{v_j})) \sigma_k(\beta_m),$$

where $\{\sigma_k\}$ are embeddings of $K$ in $\mathbb{C}$ which fix $\mathbb{Q}$ pointwise. Therefore, this Gram matrix is a product of these three matrices

$$M = \left(\begin{array}{cccc}
B & 0 & 0 & 0 \\
0 & B & 0 & 0 \\
0 & 0 & B & 0 \\
0 & 0 & 0 & B
\end{array}\right) \left(\begin{array}{cccc}
D_{11} & \cdots & \cdots & D_{14} \\
\vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots \\
D_{41} & \cdots & \cdots & D_{44}
\end{array}\right) \left(\begin{array}{cccc}
B^t & 0 & 0 & 0 \\
0 & B^t & 0 & 0 \\
0 & 0 & B^t & 0 \\
0 & 0 & 0 & B^t
\end{array}\right),$$

where $B = (\sigma_k(\beta_i))$, $B^t$ is the transpose of $B$, and

$$D_{ij} = \left(\begin{array}{c}
\sigma_1(\alpha \text{tr}(v_i \overline{v_j})) \\
\vdots \\
\sigma_n(\alpha \text{tr}(v_i \overline{v_j}))
\end{array}\right)$$

is an $n \times n$ diagonal matrix. Thus, the determinant of $M$ is equal to $(\det BB^t)^4 \det D$ with $D = (D_{ij})$. In order to consider the determinant of $D$, we exchange the rows and columns of the matrix $D$ so that

$$\det D = \det \left(\begin{array}{cccc}
D_1 & \cdots & \cdots & D_n \\
\sigma_{\ell}(\alpha \text{tr}(v_i \overline{v_j}))_{i,j} & \cdots & \cdots & \sigma_{\ell}(\alpha \text{tr}(v_i \overline{v_j}))_{i,j}
\end{array}\right),$$

$$= \prod_{\ell=1}^{n} \sigma_{\ell}(\det(\alpha \text{tr}(v_i \overline{v_j}))) = N_K(\alpha)^4 N_K(\det(\text{tr}(v_i \overline{v_j}))).$$
Notice that $\det BB^t = d_K$ and $\det(\text{tr}(v_iv_j^*))$ is equal to $N_K(N(I)^4\text{disc}(\mathcal{O})^2)$. Hence,

$$\det M = d_K^4 N_K(\alpha)^4 N_K(N(I))^4 N_K(\text{disc}(\mathcal{O})^2).$$

This formula provides us some information and conditions for $I$ and $\alpha$. In the next subsection, we will introduce how we use it to find the lattice which has the best known center density.

§3.3. Examples

Notice that if the field $K$ over $\mathbb{Q}$ is of degree $n$ then the lattice has rank $4n$. So, for example, if we wish to find $E_8$ lattice, we must find a real quadratic extension over $\mathbb{Q}$. Here, we construct $E_8$ lattice using the ideal lattice via the quaternion algebra $A = \left( \frac{-1,-1}{\mathbb{Q}(\sqrt{2})} \right)$.

**Example 3.2.** The $E_8$ lattice. Let $I$ be the ideal

$$I = \mathcal{O}_K + \mathcal{O}_K \frac{1+i}{\sqrt{2}} + \mathcal{O}_K \frac{1+j}{\sqrt{2}} + \mathcal{O}_K \frac{1+i+j+ij}{2},$$

of the quaternion algebra $A = \left( \frac{-1,-1}{\mathbb{Q}(\sqrt{2})} \right)$ and choose $\alpha = \frac{2+\sqrt{2}}{4}$. Then $(I, \alpha)$ forms a lattice with a free $\mathbb{Z}$-basis

$$\left\{ 1, \sqrt{2}, \frac{1+i}{\sqrt{2}}, 1+i, \frac{1+j}{\sqrt{2}}, 1+j, \frac{1+i+j+ij}{2}, \frac{1+i+j+ij}{\sqrt{2}} \right\}.$$ 

Observe that the norm of the elements $1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+ij}{2}$ are integers, and the trace of $\frac{2+\sqrt{2}}{4}$ is 1. Hence, the value of $B(x, x) = 2\text{tr}_K(\alpha N(x))$ is even for any $x \in I$. It is known that an even definite unimodular lattice having rank 8 is isomorphic to $E_8$ lattice. Therefore, the lattice $(I, \frac{2+\sqrt{2}}{4})$ is isomorphic to $E_8$ and its center density is $1/16$.

The following constructions are concerned with totally real subfields of cyclotomic fields. Here, we let $\zeta_m$ denote a primitive $m$th root of unity, $\eta_m = \zeta_m + \zeta_m^{-1}$, for $m > 1$, and $\mathbb{Q}(\zeta_m)^+$ the maximal real subfield of $\mathbb{Q}(\zeta_m)$. We also use Magma to find ideal lattices.

**Example 3.3.** The Coxeter-Todd lattice $K_{12}$. In order to find a lattice isomorphic to $K_{12}$, we choose a quaternion algebra over the totally real field $\mathbb{Q}(\zeta_7)^+$, which has three real infinity places and $d_K = 49$. According to the determinant formula and the center density for $K_{12}$, we have

$$\frac{1}{36} = \delta^2 = \text{minimal norm}^{12} 2^{24} \cdot 7^8 \cdot N_K(\alpha)^4 N_K(N(I))^4 N_K(\text{disc}(\mathcal{O})^2).$$
Since the minimal norm is an integer, comparing the RHS and LHS, we shall choose the quaternion algebra to be \((-\frac{1}{K}, -3)\), which is ramified at all of 3 real infinity places and the finite place 3. Hence, we have the equality

$$\frac{1}{3^6} = \frac{\text{minimal norm}^{12}}{2^{24} \cdot 7^8 \cdot 3^6 \cdot N_K(\alpha)^4 N_K(N(I))^4}.$$ 

This gives us the condition for \((I, \alpha)\). Finally, we find that we can choose \(I\) to be

$$I = O_K \langle \eta^2 - \eta - 2, (\eta^2 - \eta - 2)i, \frac{-3 + 4i + j}{2}, \frac{4 + 3i + k}{2} \rangle$$

with \(N_K(N(I)) = 7\), \(\eta = \eta_7\), and \(\alpha = 1/7\). Essentially, the ideal \(I\) is a right unimodular \(\mathbb{Z} \langle \frac{1+j}{2} \rangle\)-lattice of rank 6 and the theta series associated to \(I\) is

$$\theta_I(\tau) = 1 + 756q^2 + 4032q^3 + 20412q^4 + \cdots, \quad q = e^{2\pi i \tau}.$$ 

According to the results in [9], we conclude that the Coxeter-Todd lattice \(K_{12}\) can be realized as the ideal lattice \((I, 1/7)\).

**Example 3.4.** The \(\Lambda_{16}\) lattice. Let \(K\) be the totally real subfield of \(\mathbb{Q}(\zeta_{17})\) of degree 4 over \(\mathbb{Q}\) and the quaternion algebra is \(A = (-\frac{1}{K}, -1)\). Set \(K = \mathbb{Q}(\omega)\), where the minimal polynomial of \(\omega\) is \(x^4 + x^3 - 6x^2 - x + 1\). A \(\mathbb{Z}\)-basis for \(O_K\) is \(\{1, \omega, \omega^2, \frac{1+\omega^3}{2}\}\). The ideal we chosen is

$$I = O_K \langle 1 + \omega, (1 + \omega)j, \frac{\omega^3 + 4 + i}{2}, \frac{(3\omega^3 - 42\omega + 78) - 17i + (3\omega^3 + 6)j + k}{6} \rangle$$

with \(N_K(N(I)) = 4\); the totally positive element we picked is \(\alpha = 3 + \omega - \frac{1+\omega^3}{2}\) with minimal polynomial \(x^4 - 17x^3 + 68x^2 - 85x + 17\). Then the minimal norm of this ideal lattice \((I, \alpha/17)\) is 4, and the lattice is a 2-elementary totally even lattice. Hence, we can conclude that it is just the \(\Lambda_{16}\)-lattice from [12, 13].

**Example 3.5.** The Leech lattice \(\Lambda_{24}\). Here, we let \(K = \mathbb{Q}(\zeta_{13})^+, A = (-\frac{1}{K}, -1)\), and \(I\) be the ideal of \(A\) with the free \(O_K\)-basis

$$\eta^2 - \eta - 2, (\eta^2 - \eta - 2)i, (\eta^4 + \eta^3 + 2) + (\eta^4 + \eta^3 + 7)i + j,$$

$$\frac{(\eta^4 + \eta^3 + 7) + (\eta^4 + \eta^3 + 2)i + k}{2},$$

with \(N_K(N(I)) = 13\). We find that the ideal lattice \((I, 1/13)\) is an even unimodular lattice and has no vector with norm 2. Up to isomorphism, the Leech lattice is the unique even, unimodular definite lattice of rank 24 and has no vectors with norm 2. That is, the lattice \((I, 1/13)\) is the Leech lattice.
Example 3.6. For a rank 32 lattice. We choose the quaternion algebra $A = \left(\frac{-1,-1}{K}\right)$ with $K = \mathbb{Q}(\zeta_{17})^{+}$, and $I$ the $\mathcal{O}_{K}$-module generated by

$$
\begin{align*}
&\left(2\eta^5 - 8\eta^3 + 2\eta^2 + 6\eta - 4\right), \\
&(\eta^5 - 4\eta^3 + \eta^2 + 3\eta - 2)(1 + i), \\
&(\eta^6 + \eta^4 - 32\eta^3 + 64\eta^2 + 74\eta - 7) + (\eta^6 + \eta^4 + 2\eta^3 - 4\eta^2 + 6\eta + 27)i + j, \\
&\frac{3\eta^6 + 3\eta^4 + 23\eta^3 + 56\eta^2 - 50\eta + 64}{2} + \frac{(3\eta^6 + 3\eta^4 + 57\eta^3 - 12\eta^2 + 18\eta + 98)i + 3j + k}{6},
\end{align*}
$$

with $N_{K}(N(I)) = 4096$, and $\alpha$ be an element with minimal polynomial $x^8 - 68x^7 + 1190x^6 - 5202x^5 + 5406x^4 + 1819x^2 - 289x + 17$. Then the lattice $(I, \alpha)$ has the highest known center density in dimension 32.

Acknowledgment

The authors would like to thank the anonymous referee for his careful reading of the manuscript. His suggestions make the article more complete and clearer.

References


