Voronoï’s reduction theory of $GL_n$
over a totally real number field

Takao Watanabe, Syouji Yano and Takuma Hayashi

Abstract. Let $k$ be a totally real algebraic number field of degree $r$ and $\mathcal{O}_k$ the ring of integers of $k$. In this paper, we study Voronoï’s reduction theory and algorithm for $GL_n(k \otimes_\mathbb{Q} \mathbb{R})$ with respect to an action of $GL(\Lambda_0)$, where $GL(\Lambda_0)$ is the stabilizer in $GL_n(k)$ of a projective $\mathcal{O}_k$-module $\Lambda_0$ in $k^n$ of rank $n$.

Introduction

Let $k$ be a totally real algebraic number field of degree $r$ and $\mathcal{O}_k$ the ring of integers of $k$. We write $k \otimes_\mathbb{Q} \mathbb{R}$ for $k \otimes_\mathbb{Q} \mathbb{R}$. In this paper, we study Voronoï’s reduction theory and algorithm for $GL_n(k \otimes_\mathbb{Q} \mathbb{R})$ with respect to an action of $GL(\Lambda_0)$, where $GL(\Lambda_0)$ is the stabilizer in $GL_n(k)$ of a projective $\mathcal{O}_k$-module $\Lambda_0$ in $k^n$ of rank $n$.

Voronoï’s reduction theory was originally investigated by Voronoï [16] and was extended by Köcher [5] to self-dual homogeneous cones. Gunnells [2], Sikirić, Schürmann and Vallentin [13] also studied Voronoï’s reduction theory. To construct a fundamental domain via Voronoï’s reduction theory, we need to compute perfect forms. This is made by Voronoï algorithm. Ong [10], Gunnells [2], Opgenorth [11] and Martinet [7, §13] studied some generalizations of Voronoï algorithm. Explicit computations of perfect forms over real quadratic fields were made by Ong [10], Leibak [6], Gunnells and Yasaki [3]. Most of these previous works restrict us to the case that $\Lambda_0$ is a free $\mathcal{O}_k$-module. We systematically study $\Lambda_0$-perfect forms and Voronoï algorithm for any projective $\mathcal{O}_k$-module $\Lambda_0$ by using Ryshkov polyhedra. Some results in this paper give refinements of Köcher’s theory for the case of $GL_n(k \otimes_\mathbb{Q} \mathbb{R})/GL_n(\mathcal{O}_k)$. Moreover, as we will see in §5, observations of Ryshkov polyhedra for real quadratic fields suggest some interesting problems.

To explain results in this paper, let $H_n(k \otimes_\mathbb{Q} \mathbb{R})$ be the space of all $n \times n$ symmetric matrices with entries in $k \otimes_\mathbb{Q} \mathbb{R}$. $P_n(k \otimes_\mathbb{Q} \mathbb{R}) = \{gg \mid g \in GL_n(k \otimes_\mathbb{Q} \mathbb{R})\}$ an open cone in $H_n(k \otimes_\mathbb{Q} \mathbb{R})$ and $P_n^-(k \otimes_\mathbb{Q} \mathbb{R})$ a closure of $P_n(k \otimes_\mathbb{Q} \mathbb{R})$ in $H_n(k \otimes_\mathbb{Q} \mathbb{R})$. The group $GL_n(k \otimes_\mathbb{Q} \mathbb{R})$ acts on both $P_n^-(k \otimes_\mathbb{Q} \mathbb{R})$ and $P_n(k \otimes_\mathbb{Q} \mathbb{R})$ by $(a, g) \mapsto a \cdot g = t g a t$, where $a \in P_n^-(k \otimes_\mathbb{Q} \mathbb{R})$ or $a \in P_n(k \otimes_\mathbb{Q} \mathbb{R})$ and $g \in GL_n(k \otimes_\mathbb{Q} \mathbb{R})$. The rational closure $\Omega_4$ of $P_n(k \otimes_\mathbb{Q} \mathbb{R})$ is given by the cone generated

©0000 (copyright holder)

2010 Mathematics Subject Classification. 11H55.

Key words and phrases. Hermite constant, Polyhedral reduction, Ryshkov polyhedron, Shintani’s unit theorem, Voronoi algorithm.
by \( \{ x'x \mid x \in \Lambda_0 \setminus \{ 0 \} \} \) in \( H_n(k_\mathbb{R}) \). We have \( P_n(k_\mathbb{R}) \subseteq \Omega_k \subseteq P_n^-(k_\mathbb{R}) \) and \( \Omega_k \) is stabilized by the action of the discrete subgroup \( GL(\Lambda_0)^* = \{ t \gamma \mid \gamma \in GL(\Lambda_0) \} \).

What we want to do is to construct a fundamental domain of \( \Omega_0/\text{GL}(\Lambda_0)^* \) from perfect domains. To do this, we need a precise study of \( \Lambda_0 \)-perfect forms in \( P_n(k_\mathbb{R}) \).

As an \( \mathbb{R} \) vector space, \( H_n(k_\mathbb{R}) \) is equipped with an inner product defined by

\[
(a, b) = \text{Tr}_{k_\mathbb{R}/\mathbb{R}}(\text{Tr}(ab))
\]

for \( a, b \in H_n(k_\mathbb{R}) \). We define \( \Lambda_0 \)-minimum function \( m_{\Lambda_0} : P_n^-(k_\mathbb{R}) \rightarrow \mathbb{R}_{\geq 0} \) by

\[
m_{\Lambda_0}(a) = \inf_{0 \neq x \in \Lambda_0} (a, x^tx).
\]

If \( a \in P_n(k_\mathbb{R}) \), then the set of shortest vectors

\[
S_{\Lambda_0}(a) = \{ x \in \Lambda_0 \mid m_{\Lambda_0}(a) = (a, x^tx) \}
\]

is a finite set. We call an element \( a \in P_n(k_\mathbb{R}) \) is \( \Lambda_0 \)-perfect if \( \{ x'x \mid x \in S_{\Lambda_0}(a) \} \) spans \( H_n(k_\mathbb{R}) \) as an \( \mathbb{R} \) vector space. Okuda and Yano \cite{9} proved that \( \Lambda_0 \)-perfect forms are \( k \)-rational, i.e., if \( a \in P_n(k_\mathbb{R}) \) is \( \Lambda_0 \)-perfect with \( m_{\Lambda_0}(a) = 1 \), then \( a \in GL_n(k) \), and that the number of similar equivalent classes of \( \Lambda_0 \)-perfect forms is finite. For further study of \( \Lambda_0 \)-perfect forms, we introduce an analog of Ryshkov polyhedron, which is defined by

\[
K_1(m_{\Lambda_0}) = \{ a \in P_n^-(k_\mathbb{R}) \mid m_{\Lambda_0}(a) \geq 1 \}.
\]

The domain \( K_1(m_{\Lambda_0}) \) is a closed convex set in \( P_n(k_\mathbb{R}) \). In §2 and §3, we will prove the following:

**Theorem.** The domain \( K_1(m_{\Lambda_0}) \) is a locally finite polyhedron. If we denote by \( \partial^0 K_1(m_{\Lambda_0}) \) the set of all vertices of \( K_1(m_{\Lambda_0}) \), then \( \partial^0 K_1(m_{\Lambda_0}) \) coincides with the set of all \( \Lambda_0 \)-perfect forms \( a \) with \( m_{\Lambda_0}(a) = 1 \). Furthermore, for any two vertices \( a, a' \in \partial^0 K_1(m_{\Lambda_0}) \), there exists a finite sequence of vertices \( \{ a_i \}_{i=0}^k \subseteq \partial^0 K_1(m_{\Lambda_0}) \) such that \( a_0 = a, a_k = a' \) and the line segment between \( a_i \) and \( a_{i+1} \) is a one-dimensional face of \( \partial^0 K_1(m_{\Lambda_0}) \) for \( i = 0, \ldots, k-1 \).

This result gives Voronoi algorithm for \( \partial^0 K_1(m_{\Lambda_0}) \), i.e., the algorithm to determine a complete system \( \{ b_1, \ldots, b_t \} \) of representatives of \( \partial^0 K_1(m_{\Lambda_0})/GL(\Lambda_0) \).

For each \( a \in \partial^0 K_1(m_{\Lambda_0}) \), the closed cone \( D_a \) in \( P_n^-(k_\mathbb{R}) \) generated by \( \{ x'x \mid x \in S_{\Lambda_0}(a) \} \) is called a perfect domain. We will prove in §4 the following polyhedral subdivision of \( \Omega_k \):

\[
\Omega_k = \bigcup_{a \in \partial^0 K_1(m_{\Lambda_0})} D_a.
\]

If \( a \) and \( a' \) are distinct elements of \( \partial^0 K_1(m_{\Lambda_0}) \), then the intersection of \( D_a \) and the interior of \( D_{a'} \) is empty. Since \( D_{a \gamma} = D_a \cdot t\gamma \) holds for any \( a \in \partial^0 K_1(m_{\Lambda_0}) \) and \( \gamma \in GL(\Lambda_0) \), this subdivision yields the following:

**Theorem.** Let \( \{ b_1, \ldots, b_t \} \) be the same as above and \( \Gamma_i \) the stabilizer of \( b_i \) in \( GL(\Lambda_0) \) for \( i = 1, \ldots, t \). Then the domain

\[
\bigcup_{i=1}^t D_{b_i}/\Gamma_i^*
\]

is a fundamental domain of \( \Omega_k/GL(\Lambda_0)^* \), where \( \Gamma_i^* = \{ t\gamma \mid \gamma \in \Gamma_i \} \).
If the dimension \( n \) is equal to one and \( \Lambda_0 = \alpha_k \), then this theorem may be regarded as a precise form of Shintani’s unit theorem ([8, (9.2)], [15, Proposition 4]) for the square \( E_k^2 \) of the unit group \( E_k = GL(\alpha_k) \). In this case, \( \Omega_k \setminus \{ 0 \} \) equals the quadrant \( k_R^+ = R_{\geq 0} \) and \( E_k^2 \) acts on \( k_R^+ \) by scalar multiplications. Since \( \Gamma_1 = \{ \pm 1 \} \) (and hence \( \Gamma_2 = \{ 1 \} \)), we obtain a cone decomposition of \( E_k^2 \setminus k_R^+ \) as

\[ E_k^2 \setminus k_R^+ = \bigcup_{i=1}^t D_{b_i}^+ , \]

where \( D_{b_i}^+ = D_{b_i} \setminus \{ 0 \} \). If \( k \) is a real quadratic field, then \( K_1(\alpha_k) \) is a domain in \( \mathbb{R}^2_{\geq 0} \) with infinite vertices. In §5, several examples of \( K_1(\alpha_k) \) are given. We will see that there are many real quadratic fields such that the number \( t \) of elements of \( E_k^2 \setminus \partial K_1(\alpha_k) \) is equal to one.

**Notation.** For a given ring \( R \), the set of all \( m \times n \) matrices with entries in \( R \) is denoted by \( M_{m,n}(R) \). We write \( M_n(R) \) for \( M_{n,n}(R) \) and \( R^n \) for \( M_{n,1}(R) \). The transpose of a given matrix \( \alpha \in M_{m,n}(R) \) is denoted by \( \alpha^t \). If \( R = \mathbb{R} \) (resp. \( R = \mathbb{C} \)), then the set of symmetric matrices in \( M_n(\mathbb{R}) \) (resp. Hermitian matrices in \( M_n(\mathbb{C}) \)) is denoted by \( H_n(\mathbb{R}) \) (resp. \( H_n(\mathbb{C}) \)). For a constant \( c \in \mathbb{R} \), \( \mathbb{R}_{>c} \) and \( \mathbb{R}_{\geq c} \) stand for the open interval \((c, +\infty)\) and the closed interval \([c, +\infty)\).

In this paper, \( k \) denotes an algebraic number field of degree \( r \) and \( \alpha_k \) the ring of integers of \( k \). Up to §3, \( k \) is an arbitrary number field. From §4, \( k \) is restricted to a totally real number field. The set of all infinite (resp. real and imaginary) places of \( k \) is denoted by \( \mathbb{P}_\infty \) (resp. \( \mathbb{P}_1 \) and \( \mathbb{P}_2 \)). Let \( k_\sigma \) be the completion of \( k \) at \( \sigma \in \mathbb{P}_\infty \), i.e., \( k_\sigma = \mathbb{R} \) if \( \sigma \in \mathbb{P}_1 \) and \( k_\sigma = \mathbb{C} \) if \( \sigma \in \mathbb{P}_2 \). We use the étale \( \mathbb{R} \)-algebra \( k_R = k \otimes_{\mathbb{Q}} \mathbb{R} \), which is identified with \( \prod_{\mathbb{P}_\infty} k_\sigma \). As usual, \( k \) is embedded in \( k_R \) by \( \lambda \mapsto (\sigma(\lambda))_{\sigma \in \mathbb{P}_\infty} \). For \( \alpha = (\alpha_\sigma) \in k_R \), the conjugate \( \overline{\alpha} \) of \( \alpha \) stands for \( (\overline{\alpha_\sigma}) \), where \( \overline{\alpha_\sigma} \) denotes the complex conjugate of \( \alpha_\sigma \in k_\sigma \). The trace of \( k_R \) over \( R \) defined by

\[ \text{Tr}_{k_R}(\alpha) = \sum_{\sigma \in \mathbb{P}_\infty} \text{Tr}_{k_\sigma/R}(\alpha_\sigma) \]

for \( \alpha \in k_R \).

1. Preliminaries

We recall results of [9]. Let \( k_R^n = k^n \otimes_{\mathbb{Q}} \mathbb{R} \). An element of \( k_R^n \) is denoted as a column vector with entries in \( k_R \). For \( x = (x_1, \cdots, x_n) \in k_R^n \) with components \( x_\sigma \in k_R \), \( x^* \) and \( x^* \) stand for \( (\overline{x_\sigma}) \) and \( x_\sigma \), respectively. As an \( \mathbb{R} \) vector space, \( k_R^n \) is equipped with an inner product \( \langle \ , \ \rangle \) defined by

\[ \langle x, y \rangle = \text{Tr}_{k_R}(x^* y) \]

for \( x, y \in k_R^n \). We set \( Q(x) = \langle x, x \rangle \). For every \( a \in M_n(k_R) \), \( a^* \) stands for the adjoint matrix with respect to the inner product \( \langle \ , \ \rangle \).

The group of \( k_R \)-linear automorphisms of \( k_R^n \) is denoted by \( GL_n(k_R) \). The group of isometries with respect to \( \langle \ , \ \rangle \) is denoted by \( O_n(k_R) \), i.e.,

\[ O_n(k_R) = \{ g \in GL_n(k_R) \mid \langle gx, gy \rangle = \langle x, y \rangle \text{ for all } x, y \in k_R^n \} , \]

and the set of self-adjoint matrices in \( M_n(k_R) \) is denoted by \( H_n(k_R) \), i.e.,

\[ H_n(k_R) = \{ a \in M_n(k_R) \mid \langle ax, y \rangle = \langle x, ay \rangle \text{ for all } x, y \in k_R^n \} . \]
According to the identification $k_R \simeq \prod_{r \in p_\infty} k_r$, the group $GL_n(k_R)$ and the space $H_n(k_R)$ are identified with $\prod_{r \in p_\infty} GL_n(k_r)$ and $\prod_{r \in p_\infty} H_n(k_r)$, respectively.

A self-adjoint matrix $a \in H_n(k_R)$ is said to be positive definite (resp. semi-positive definite) if $\langle ax, x \rangle > 0$ (resp. $\langle ax, x \rangle \geq 0$) for all $x \in k_R^n \setminus \{0\}$. We denote the set of positive definite (resp. semi-positive definite) self-adjoint matrices in $H_n(k_R)$ by $P_n(k_R)$ (resp. $P^\dagger_n(k_R)$). The trace $TR$ on $H_n(k_R)$ is defined to be

$$TR(a) = Tr_{k_R}(\langle Tr(a_x) \rangle_{\sigma \in p_\infty})$$

for $a \in H_n(k_R)$. This defines an inner product $(\ , \ )$ on $H_n(k_R)$ by $(a, b) = TR(ab)$.

An $\mathfrak{o}_k$-submodule $\Lambda$ in $k_R^n$ is called an $\mathfrak{o}_k$-lattice if $\Lambda$ is discrete and $\Lambda \otimes \mathbb{Z} R = k_R^n$. The set of all $\mathfrak{o}_k$-lattices in $k_R^n$ is denoted by $\mathcal{L}$. For any $\mathfrak{o}_k$-lattice $\Lambda$, there exists $g \in GL_n(k_R)$ such that $g^{-1} \Lambda$ is a projective $\mathfrak{o}_k$-module in $k^n$. By Steinitz’s theorem, any projective $\mathfrak{o}_k$-module in $k^n$ is isomorphic to $\mathfrak{o}_k^{n-1} \oplus q$ for some integral ideal $q$ in $\mathfrak{o}_k$. We choose a complete system $\{q_1 = \mathfrak{o}_k, q_2, \cdots, q_h\}$ of representatives of the ideal class group of $k$. Let $\Lambda_i = \mathfrak{o}_k^{n-1} \oplus q_i$, for $1 \leq i \leq h$. Then the set of all $\mathfrak{o}_k$-lattices of $k_R^n$ is given by the disjoint union

$$\mathcal{L} = \bigoplus_{i=1}^h \mathcal{L}_i,$$

where $\mathcal{L}_i$ is the $GL_n(k_R)$-orbit of $\Lambda_i$. Each $\mathcal{L}_i$ is identified with $GL_n(k_R)/GL_\sigma(\Lambda_i)$, where $GL_\sigma(\Lambda_i)$ denotes the stabilizer of $\Lambda_i$ in $GL_n(k_R)$. Two $\mathfrak{o}_k$-lattices $\Lambda$ and $\Lambda'$ are said to be isometric if there exists $T \in O_n(k_R)$ such that $\Lambda = T \Lambda'$. For every $\Lambda \in \mathcal{L}$, the minimum $Q(\Lambda)$, the set of shortest vectors $S(\Lambda)$ and the determinant $\det(\Lambda)$ are defined as follows:

$$Q(\Lambda) = \min_{x \in \Lambda \setminus \{0\}} \langle x, x \rangle, \quad S(\Lambda) = \{ x \in \Lambda \mid Q(x) = Q(\Lambda) \}$$

and

$$\det(\Lambda) = \left( \frac{\omega(k_R^n/\Lambda)}{\omega(k_R^n/\mathfrak{o}_k^n)} \right)^2,$$

where $\omega$ denotes an invariant measure on $k_R^n$.

Let $H_n(k_R)^*$ denote the dual vector space of $H_n(k_R)$ as an $R$ vector space. Then we define $\varphi_x \in H_n(k_R)^*$ for each $x \in k_R^n$ as

$$\varphi_x(a) = \langle ax, x \rangle \text{ for } a \in H_n(k_R).$$

**DEFINITION.** Let $\Lambda \subset k_R^n$ be an $\mathfrak{o}_k$-lattice.

(1) $\Lambda$ is said to be perfect if $\{ \varphi_x \mid x \in S(\Lambda) \}$ generates $H_n(k_R)^*$.

(2) $\Lambda$ is said to be eutactic if there exist $\rho_x \in R_{>0}$ for all $x \in S(\Lambda)$ such that

$$TR = \sum_{x \in S(\Lambda)} \rho_x \varphi_x.$$
Since $\gamma_k^1$ is invariant by isometry and similarity, we may regard $\gamma_k^1$ as a function defined on $\mathbb{R}^\times \text{O}_n(k_R) \setminus \mathcal{L}$. If $\gamma_k^0$ attains a local maximum on $\Lambda \in \mathcal{L}$, then $\Lambda$ is said to be extreme. The following theorem was proved by Okuda and Yano.

**Theorem 1.1 ([9]).** Let $\Lambda \in \mathcal{L}$ be an $\mathfrak{o}_k$-lattice. Then $\Lambda$ is extreme if and only if $\Lambda$ is perfect and eutactic.

If $k$ is a totally real or a CM-field (i.e. a totally imaginary quadratic extension over a totally real algebraic number field), then we have the following rationality theorem of perfect forms.

**Theorem 1.2 ([9]).** Let $k$ be a totally real or a CM-field. If $g \in \text{GL}_n(k_R)$ is a perfect $\mathfrak{o}_k$-lattice with $Q(\Lambda) = 1$, then $g^*g \in M_n(k)$.

### 2. Geometric characterizations of perfect forms

In this section, we fix a projective $\mathfrak{o}_k$-module $\Lambda_0 \subset k^n$ of rank $n$. For $a \in P_n^+(k_R)$, we define the minimum $m_{\Lambda_0}(a)$ and the set of shortest vectors $S_{\Lambda_0}(a)$ by:

$$m_{\Lambda_0}(a) = \inf_{x \in \Lambda_0 \setminus \{0\}} \langle ax, x \rangle \quad \text{and} \quad S_{\Lambda_0}(a) = \{ x \in \Lambda_0 \mid m_{\Lambda_0}(a) = \langle ax, x \rangle \}$$

We write simply $m$ and $S(a)$ for $m_{\Lambda_0}$ and $S_{\Lambda_0}(a)$, respectively, if no confusions arise. If $a = g^*g$ is positive definite with $g \in \text{GL}_n(k_R)$, then we have:

$$m(a) = \min_{x \in \Lambda_0 \setminus \{0\}} \langle gx, gx \rangle = Q(g\Lambda_0)$$

and $S(a) = S(g\Lambda_0)$. A positive definite $a \in P_n(k_R)$ is said to be $\Lambda_0$-perfect if $\{ x \mid x \in S(a) \}$ generates $H_n(k_R)^*$ as an $\mathbb{R}$ vector space. It is clear that $a = g^*g$ is $\Lambda_0$-perfect if and only if $g\Lambda_0$ is perfect. From $\phi_x(a) = (a, xx^*)$ for $x \in S(a)$, it follows that $a$ is $\Lambda_0$-perfect if and only if $\{ xx^* \mid x \in S(a) \}$ generates $H_n(k_R)$ as an $\mathbb{R}$ vector space.

We define an analog of Rychkov polyhedron (cf. [12], [14]) for $m$ by:

$$K_1(m) = \{ a \in P_n^-(k_R) \mid m(a) \geq 1 \}$$

The boundary of $K_1(m)$ is denoted by $\partial K_1(m)$, i.e.,

$$\partial K_1(m) = \{ a \in P_n^-(k_R) \mid m(a) = 1 \}$$

For $x \in k_R^n \setminus \{0\}$, define the half-space $H_x^+$ in $H_n(k_R)$ by:

$$H_x^+ = \{ a \in H_n(k_R) \mid \langle ax, x \rangle \geq 1 \}$$

Then $K_1(m)$ is the intersection of half-spaces $H_x^+$, $x \in \Lambda_0 \setminus \{0\}$. In particular, $K_1(m)$ is a closed convex domain in $H_n(k_R)$.

**Lemma 2.1.** $K_1(m)$ is contained in $P_n(k_R)$.

**Proof.** It is enough to show that $m(a) = 0$ for any $a \in P_n^-(k_R) \setminus P_n(k_R)$. For $a \in P_n^-(k_R) \setminus P_n(k_R)$ and any $\epsilon > 0$, the set $B_{a,\epsilon} = \{ x \in k_R^n \mid \langle ax, x \rangle \leq \epsilon \}$ is a symmetric convex set of infinite volume. By Minkowski’s theorem on convex bodies, $B_{a,\epsilon}$ contains a non-zero element in $\Lambda_0$. Then we have $m(a) \leq \epsilon$, and hence $m(a) = 0$. 

**Proposition 2.2.** $K_1(m)$ is a locally finite polyhedron, i.e. the intersection of $K_1(m)$ and any polytope is a polytope.
We suppose that there exists a \( K \) and hence \( \lambda \). It is obvious by the definition of \( A \), and \( \lambda \) is bounded for all \( i \). One can take an orthogonal matrix \( T = (t_{ij}) \) such that \( T \lambda i \). Then we have \( \lambda i \leq nr \theta \).

Step 2 : Let \( W \) be a subset consisting of all \( x \in \Lambda \) such that \( \langle ax, x \rangle = 1 \) for some \( a \in K_1(m) \cap X_\theta \). We prove

\[
K_1(m) \cap X_\theta = \bigcap_{x \in W} (H^+ x \cap X_\theta).
\]

It is obvious by the definition of \( K_1(m) \) that

\[
K_1(m) \cap X_\theta \subset \bigcap_{x \in W} (H^+ x \cap X_\theta).
\]

We suppose that there exists \( a \in \bigcap_{x \in W} (H^+ x \cap X_\theta) \) such that \( a \not\in K_1(m) \cap X_\theta \). Fix an interior point \( b \) in \( K_1(m) \cap X_\theta \). Since \( a \not\in K_1(m) \) and \( b \in K_1(m) \), the line segment between \( a \) and \( b \) crosses the boundary of \( K_1(m) \), namely, \( c = \lambda a + (1-\lambda)b \in \partial K_1(m) \) for some \( \lambda \in (0,1) \). Then there is an \( x_0 \in \Lambda \) such that \( \langle ax_0, x_0 \rangle = 1 \). Since \( X_\theta \) is convex, we have \( c \in \partial K_1(m) \cap X_\theta \). This implies \( x_0 \in W \). On the other hand, we have

\[
\langle ax_0, x_0 \rangle = \lambda (ax_0, x_0) + (1-\lambda)(bx_0, x_0) > 1
\]

since \( b \in H^+ x \) for all \( x \in W \) and \( b \) is an interior point in \( K_1(m) \). This is a contradiction.

Step 3 : We prove that \( W \) is a finite set. For \( a \in K_1(m) \cap X_\theta \), put \( B_a = \{ x \in k^n_R \mid \langle ax, x \rangle \leq 1 \} \). Since the interior of \( B_a \) does not contain any non-zero lattice point of \( \Lambda_0 \), we have

\[
\omega(B_a) \leq 2^{nr} \omega(k^n_R / \Lambda_0).
\]

Since \( \{ v_k \}_k \) is a basis of \( k^n_R \) as an \( R \) vector space, each \( x \in B_a \) is represented by a linear combination of \( \{ v_k \}_k \) as

\[
x = \sum_{k=1}^{nr} \lambda_k v_k.
\]
Fix $x \in B_{a}$ and $k_{0}$ such that $|\lambda_{k_{0}}| = \max_{1 \leq k \leq nr} |\lambda_{k}|$. For $1 \leq i \leq nr$, we define the parallelepiped $D_{i}$ of dimension $nr - 1$ in $k_{R}^{n}$ as

$$D_{i} = \{ \sum_{k \neq i} (\mu_{k} - \mu'_{k})v_{k} \mid \mu_{k}, \mu'_{k} \in \mathbb{R}_{\geq 0}, \sum_{k \neq i} (\mu_{k} + \mu'_{k}) \leq \theta^{-1/2} \}.$$ 

In other words, $D_{i}$ is the closed convex hull of $\{ \pm \theta^{-1/2}v_{k} \mid k = 1, \cdots, nr, k \neq i \}$ in $k_{R}^{n}$. Let $V_{x}$ be a pyramid in $k_{R}^{n}$ of the base $D_{k_{0}}$ and the apex $x$, i.e.,

$$V_{x} = \{ \lambda x + \mu y \mid y \in D_{k_{0}}, \lambda, \mu \in \mathbb{R}_{\geq 0}, \lambda + \mu \leq 1 \}.$$ 

Since $\theta^{-1/2}v_{k} \in B_{a}$ for all $k$ and $B_{a}$ is convex, $D_{k_{0}}$ is contained in $B_{a}$. This implies $V_{x} \subset B_{a}$. We take another basis $\{ u_{k} \}_{k=1}^{nr}$ of $k_{R}^{n}$ such that $\langle u_{k}, v_{j} \rangle = 0$ for any $k \neq j$ and $\langle u_{k}, u_{j} \rangle = 1$ for all $k$. Then the volume $\omega(V_{x})$ of $V_{x}$ equals

$$\frac{|\langle x, u_{k_{0}} \rangle| \text{vol}(D_{k_{0}})}{nr}.$$ 

If we put $\nu = (\min_{1 \leq k \leq nr} |\langle u_{k}, v_{k} \rangle|) \cdot (\min_{1 \leq i \leq nr} \text{vol}(D_{i}))$, then we obtain

$$\max_{1 \leq k \leq nr} |\lambda_{k}| \leq \frac{\nu n \nu r \omega(k_{R}^{n}/\Lambda_{0})}{\nu}.$$ 

This estimate holds for all $x \in B_{a}$. Since the upper bound does not depend on $a \in K_{1}(m) \cap X_{\theta}$, the union of all $B_{a}$, $a \in K_{1}(m) \cap X_{\theta}$, is a bounded set in $k_{R}^{n}$. Since $W$ is a subset of $\Lambda_{0} \cap \bigcup_{a \in K_{1}(m) \cap X_{\theta}} B_{a}$, $W$ must be a finite set.

By Step 1, $K_{1}(m) \cap X_{\theta}$ is bounded, and by Step 2 and Step 3, it is an intersection of finite number of half-spaces. Thus $K_{1}(m) \cap X_{\theta}$ is a polytope. Since $K_{1}(m) \cap T_{\theta} \subset K_{1}(m) \cap X_{\theta}$ by the proof of Step 1, $K_{1}(m) \cap T_{\theta}$ is also polytope. \hfill $\Box$

Faces of $K_{1}(m)$ are described by using shortest vectors.

**Lemma 2.3.** Let $a_{1}, \cdots, a_{k} \in \partial K_{1}(m)$ and $S$ be a non-empty finite subset of $\Lambda_{0}$ such that $S \subset S(a_{i})$ for all $1 \leq i \leq k$. Then, for any $\lambda_{1}, \cdots, \lambda_{k} \in \mathbb{R}_{\geq 0}$ with $\sum_{i=1}^{k} \lambda_{i} = 1$, one has

$$\lambda_{1}a_{1} + \cdots + \lambda_{k}a_{k} \in \partial K_{1}(m)$$

and $S \subset S(\lambda_{1}a_{1} + \cdots + \lambda_{k}a_{k})$.

The proof is easy.

For a non-empty finite subset $S \subset \Lambda_{0} \setminus \{0\}$, we define the subset $F_{S} \subset \partial K_{1}(m)$ by

$$F_{S} = \{ a \in \partial K_{1}(m) \mid S \subset S(a) \}.$$ 

By Lemma 2.3, $F_{S}$ is a convex set. Let $H_{S}$ be the affine subspace of $H_{n}(k_{R})$ generated by $F_{S}$, i.e.

$$H_{S} = \left\{ \sum_{i=1}^{k} \lambda_{i}a_{i} \mid 1 \leq k \in \mathbb{Z}, \lambda_{i} \in \mathbb{R}, \sum_{i=1}^{k} \lambda_{i} = 1 \right\}.$$ 

if $F_{S}$ is non-empty. Since $S$ is non-empty, $H_{S}$ is a proper affine subspace of $H_{n}(k_{R})$. Then the following is proved by the same argument as in [17, Lemmas 1.5 and 1.6].

**Proposition 2.4.** One has $F_{S} = \partial K_{1}(m) \cap H_{S}$. In particular, $F_{S}$ is a face of $K_{1}(m)$ if $F_{S} \neq \emptyset$. Conversely, any face of $K_{1}(m)$ is of the form $F_{S}$ for some non-empty finite subset $S \subset \Lambda_{0}$.
We denote by $\partial^0 K_1(m)$ the set of all 0-dimensional faces of $K_1(m)$. By the same argument as in [17, Theorem 1.4], we obtain the following:

**Theorem 2.5.** For $a \in \partial K_1(m)$, the following three conditions are equivalent each other.

1. $a$ is $\Lambda_0$-perfect.
2. $a \in \partial^0 K_1(m)$.
3. There exists a neighborhood $N$ of $a$ in $P_\infty(kR)$ such that $S(b) \subseteq S(a)$ for any $b \in N \setminus (R_{\geq 0}a)$.

The discrete group $GL(\Lambda_0)$ acts on $P_\infty^-(kR)$ by $a \cdot \gamma = \gamma^* a \gamma$ for $(a, \gamma) \in P_\infty^-(kR) \times GL(\Lambda_0)$. The set $\partial^0 K_1(m)$ is stable by this action of $GL(\Lambda_0)$. By [9, Theorem 5.1], the orbit space $\partial^0 K_1(m)/GL(\Lambda_0)$ is a finite set.

For each $a \in \partial^0 K_1(m)$, we set

$$C_a = \{ b \in H_n(kR) \mid \langle bx, x \rangle \geq 0 \text{ for any } x \in S(a) \}.$$ 

The half-line $R_{\geq 0}b$ generated by $b \in C_a \setminus \{0\}$ is said to be an extreme ray of $C_a$ if for any $b_1, b_2 \in C_a$, whenever $b = (b_1 + b_2)/2$, we must have $b_1, b_2 \in R_{\geq 0}b$. By the same argument as in [17, Lemma 1.7, Proposition 1.3], one can prove the following:

- If $R_{\geq 0}b$ is an extreme ray of $C_a$, then $b \notin P_\infty^-(kR)$.
- For any 1-dimensional face $L$ of $\partial K_1(m)$, there exist two vertices $a_1, a_2 \in \partial^0 K_1(m)$ such that $L = \{ \lambda a_1 + (1 - \lambda) a_2 \mid 0 \leq \lambda \leq 1 \}$.

By these properties and Proposition 2.2, we obtain the following theorem (cf. [17, Corollary 1.2]).

**Theorem 2.6.** $K_1(m)$ is the convex hull of $\partial^0 K_1(m)$.

3. **Voronoï algorithm for $\partial K_1(m)$**

In this section, we show that Voronoï algorithm is effective for $\partial K_1(m)$, which is an algorithm to compute adjacent vertices of a given vertex in $\partial K_1(m)$. Here, two vertices $a_1, a_2 \in \partial^0 K_1(m)$ are said to be adjacent if $L = \{ \lambda a_1 + (1 - \lambda) a_2 \mid 0 \leq \lambda \leq 1 \}$ is an edge (= 1-dimensional face) of $\partial K_1(m)$. Our purpose is to show the connectedness of vertices of $\partial K_1(m)$, i.e. any two vertices of $\partial K_1(m)$ are linked with finite edges. We follow the argument of [4].

For $a \in \partial^0 K_1(m)$, the perfect domain $D_a \subset H_n(kR)$ of $a$ is defined by

$$D_a = \left\{ \sum_{x \in S(a)} \lambda_x x^* \mid 0 \leq \lambda_x \in R \right\}.$$ 

Let $R_{\geq 0}c_1, \cdots, R_{\geq 0}c_k$ be all of extreme rays of $C_a$. The hyperplane in $H_n(kR)$ orthogonal to $c_i$ is a supporting hyperplane of $D_a$, and $D_a$ is the intersection of closed half-spaces $H_{\alpha_i} = \{ b \in H_n(kR) \mid \langle b, c_i \rangle \geq 0 \}$, $i = 1, \cdots, k$.

**Lemma 3.1.** Let $D_a^\circ$ be the interior of a perfect domain $D_a$. Then $D_a^\circ \subset P_\infty(kR)$. If $D_a^\circ \cap D_{a'} \neq \emptyset$ for $a, a' \in \partial^0 K_1(m)$, then $a = a'$.

**Proof.** Let $D'_a$ be a subset of $D_a$ consisting of all elements of the form $\sum \lambda_x x^*$ with $\lambda_x > 0$ for all $x \in S(a)$. Since $a$ is $\Lambda_0$-perfect, $D'_a$ is an open
convex cone in $H_{R}(k_{R})$ and the closure of $D'_{a}$ coincides with $D_{a}$. Then $D'_{a}$ must be equal to $D_{a}^{\circ}$ (cf. [1, Theorem 5.23]). Therefore, each $b \in D_{a}^{\circ}$ is represented by

$$b = \sum_{x \in S(a)} \lambda_{x}xx^{*}$$

with $\lambda_{x} > 0$. One has

$$\langle by, y \rangle = \sum_{x \in S(a)} \lambda_{x}\langle xx^{*}y, y \rangle = \sum_{x \in S(a)} \lambda_{x}\text{Tr}_{k_{R}}(y^{*}xx^{*}y) = \sum_{x \in S(a)} \lambda_{x}\text{Tr}_{k_{R}}((x^{*}y)^{*}x^{*}y)$$

for any $y \in k_{R}^{n} \setminus \{0\}$. In the right-hand side, $\text{Tr}_{k_{R}}((x^{*}y)x^{*}y) \geq 0$ for every $x \in S(a)$. From the perfection of $a$, it follows $\text{Tr}_{k_{R}}((x^{*}y)x^{*}y) > 0$ for at least one $x \in S(a)$. Therefore we have $b \in P_{n}(k_{R})$.

Next, let $b \in D_{a}^{\circ} \cap D_{a}$. Then we have

$$(b, a) = \sum_{x \in S(a)} \lambda_{x}\langle xx^{*}, a \rangle = \sum_{x \in S(a)} \lambda_{x}\langle ax, x \rangle = \sum_{x \in S(a)} \lambda_{x}$$

and

$$(b, a') = \sum_{x \in S(a)} \lambda_{x}\langle xx^{*}, a' \rangle = \sum_{x \in S(a)} \lambda_{x}\langle a'x, x \rangle \geq \sum_{x \in S(a)} \lambda_{x} = (b, a)$$

because of $\langle a'x, x \rangle \geq m(a') = 1$. On the other hand, $b$ is represented as

$$b = \sum_{x \in S(a')} \mu_{x}xx^{*}$$

with $\mu_{x} \geq 0$. The same argument yields $(b, a) \geq (b, a')$, and hence $(b, a) = (b, a')$. Since

$$\sum_{x \in S(a)} \lambda_{x}\langle xx^{*}, a' - a \rangle = 0, \quad (xx^{*}, a') \geq (xx^{*}, a)$$

and $\lambda_{x} > 0$, we obtain $(xx^{*}, a - a') = 0$ for any $x \in S(a)$. This concludes $a = a'$. \qed

**Lemma 3.2.** Let $b \in P_{n}(k_{R})$ and $\theta$ be a positive constant. Then the number of elements in $\{a \in \partial^{\theta}K_{1}(m) \mid (a, b) \leq \theta\}$ is finite.

**Proof.** Assume that $a = gg^{*} \in \partial^{\theta}K_{1}(m)$ with $g \in GL_{n}(k_{R})$ satisfies $(a, b) \leq \theta$. Let $g_{k} \in k_{R}^{n}$ be the $k$-th column vector of $g$. Then we have

$$(a, b) = \text{TR}(gg^{*}b) = \text{TR}(g^{*}by) = \text{Tr}_{k_{R}}(\sum_{k=1}^{n} g_{k}^{*}bg_{k}) = \sum_{k=1}^{n} \langle bg_{k}, g_{k} \rangle.$$ 

Put

$$\lambda_{b} = \min_{x \in k_{R}^{n} \setminus \{0\}} \frac{\langle bx, x \rangle}{\langle x, x \rangle}$$

Then $\lambda_{b} > 0$ because of $b \in P_{n}(k_{R})$ and

$$\text{TR}(a) = \sum_{k=1}^{n} \langle g_{k}, g_{k} \rangle \leq \sum_{k=1}^{n} \frac{\langle bg_{k}, g_{k} \rangle}{\lambda_{b}} \leq \frac{(a, b)}{\lambda_{b}} \leq \frac{\theta}{\lambda_{b}}.$$ 

By Proposition 2.2, $a$ is a vertex of the polytope $K_{1}(m) \cap T_{\theta/\lambda_{b}}$. \qed

**Proposition 3.3.** For $a, a' \in \partial^{\theta}K_{1}(m)$, there exists a finite sequence of vertices $\{a_{i}\}_{i=0}^{k-1} \subset \partial^{\theta}K_{1}(m)$ such that $a_{0} = a, a_{k} = a'$ and $a_{i+1}$ are adjacent to $a_{i}$ for $i = 0, \cdots, k - 1$. 


3.1. Assume $b \not\in D_{a_0}$. If $b \in D_{a_0}$, then we have $a' = a_0$ by Lemma 3.1. Assume $b \not\in D_{a_0}$. We choose a $c \in C_{a_0}$ such that $R_{\geq 0}c$ is an extreme ray of $C_{a_0}$ and $b \not\in H_c$. Let $a_1 = a_0 + pc$ be the adjacent vertex to $a_0$ which is lying on the ray $a_0 + R_{\geq 0}c$. Since $b \not\in H_c$, we have 

$$(a_1, b) = (a_0, b) + (pc, b) < (a_0, b).$$

If $b \in D_{a_1}$, then $a' = a_1$ by Lemma 3.1. Otherwise, by the same argument, we can take a vertex $a_2$ which is adjacent to $a_1$ and satisfies $(a_2, b) < (a_1, b) < (a_0, b)$. By Lemma 3.2, this process terminates at finite times. 

Voronoi algorithm for $\partial K_1(m)$ is summarized as follows.

1. Fix an initial point $a_0 = a \in \partial^0 K_1(m)$.
2. Calculate the set of shortest vectors $S(a)$ of $a$.
3. Enumerate the extreme rays $R_{\geq 0}c_1, \cdots, R_{\geq 0}c_k$ of $C_a$.
4. Determine the adjacent vertex of the form $a_i = a + \rho c_i$ for each $i = 1, \cdots, k$.
5. Check whether $a_i$ is equivalent with the vertex which has already been found.
6. Repeat the operations (2) – (5) for new inequivalent vertices.

4. Polyhedral reduction of $P_n(k_R)/GL(\Lambda_0)$

In the rest of this paper, we assume that $k$ is totally real, i.e., $p_\infty = p_1$.

We identify $R$ with its diagonally embedding in $k_R = R^\sigma$. Let

$$k_R^+ = \{ (\alpha_\sigma)_{\sigma \in p_\infty} \in k_R \mid \alpha_\sigma > 0 \text{ for all } \sigma \in p_\infty \}.$$ 

We put

$$H_n(k) = H_n(k_R) \cap M_n(k) \text{ and } P_n(k) = P_n(k_R) \cap H_n(k).$$

For $a \in P_n^+(k_R)$, the radical of $a$ is defined to be

$$\text{rad}(a) = \{ x \in k_R^0 \mid (ax, x) = 0 \}.$$ 

We call that $\text{rad}(a)$ is defined over $k$ if $(\text{rad}(a) \cap k^n) \otimes Q = \text{rad}(a)$ holds. By $\Omega_k$, we denote the set of all $a \in P_n^+(k_R)$ such that $\text{rad}(a)$ is defined over $k$. Since $\text{rad}(a) = \{ 0 \}$ if $a \in P_n^+(k_R)$, $\Omega_k$ contains $P_n^+(k_R)$.

We define other two subsets $\Omega_1$ and $\Omega_2$ of $P_n^+(k_R)$ as follows. For $x \in k^n$, $xx^* = x^*x$ is an element of $M_n(k)$. We consider $M_n(k)$ as a subset of $M_n(k_R)$ by usual way. Then we put

$$\Omega_1 = \left\{ \sum_{i=1}^k \alpha_i x_i x_i^* \mid 1 \leq k \in Z, \alpha_i \in k_R^+ \cup \{ 0 \}, x_i \in k^n \right\},$$

$$\Omega_2 = \left\{ \sum_{i=1}^k \lambda_i x_i x_i^* \mid 1 \leq k \in Z, \lambda_i \in R_{\geq 0}, x_i \in k^n \right\}.$$ 

Since $R_{\geq 0} \subset k_R^+ \cup \{ 0 \}$, $\Omega_2$ is a subset of $\Omega_1$. In the following, we show $\Omega_k = \Omega_1 = \Omega_2$.

**Lemma 4.1.** The set $(k^+)^2 = \{ \alpha^2 \mid \alpha \in k^+ \}$ is dense in $k_R^+$.

**Proof.** We define the norm $\| \cdot \|_{k_R}$ on $k_R$ by

$$\| a \|_{k_R} = \max_{\sigma \in p_\infty} |a_\sigma|_\sigma$$
for $\alpha = (\alpha_\sigma) \in k_R$, where $\cdot$ denotes the absolute value of $k$. Since $k$ is dense in $k^+_R$, $k^+_R \cap k$ is also dense in $k^+_R$. For a given $\alpha = (\alpha_\sigma) \in k^+_R$, there is a square root $\sqrt{\alpha} = \sqrt{\alpha_\sigma} \in k^+_R$ of $\alpha$. Then, for any $\epsilon \in (0, 1)$, there exists $\beta \in k^+_R \cap k$ such that

$$||\sqrt{\alpha} - \beta||_{k_R} < \frac{\epsilon}{2||\sqrt{\alpha}||_{k_R} + 1}.$$ 

From $||\beta||_{k_R} < ||\sqrt{\alpha}||_{k_R} + 1$, it follows that

$$||\sqrt{\alpha} + \beta||_{k_R} < 2||\sqrt{\alpha}||_{k_R} + 1.$$ 

Therefore, we have

$$||\alpha - \beta^2||_{k_R} \leq ||\sqrt{\alpha} - \beta||_{k_R} \cdot ||\sqrt{\alpha} + \beta||_{k_R} < \epsilon.$$ 

□

Let $\text{Cone}((k^\times)^2)$ be the cone in $k_R$ generated by $(k^\times)^2$, i.e.,

$$\text{Cone}((k^\times)^2) = \{ \sum_{i=1}^k \lambda_i \alpha_i^2 \mid 0 < k \in \mathbb{Z}, \lambda_i \in \mathbb{R}_{\geq 0}, \alpha_i \in k^\times \}.$$ 

**Lemma 4.2.** $k^+_R \cup \{0\} = \text{Cone}((k^\times)^2)$.

**Proof.** For a given $\alpha = (\alpha_\sigma) \in k^+_R$, we choose $\epsilon > 0$ so that the neighborhood

$$U = \{ \beta \in k_R \mid ||\alpha - \beta||_{k_R} < \epsilon \}$$

of $\alpha$ is contained in $k^+_R$. For $\kappa = (\kappa_\sigma) \in \{\pm 1\}^r$, we put

$$U_\kappa = \{ \beta \in U \mid \kappa_\sigma(\alpha_\sigma - \beta_\sigma) > 0 \text{ for all } \sigma \in p_\infty \}.$$ 

By Lemma 4.1, there is a $\beta_\kappa \in U_\kappa \cap (k^\times)^2$. Then $\alpha$ is contained in the convex hull of $\{ \beta_\kappa^2 \mid \kappa \in \{\pm 1\}^r \}$. This implies $\alpha \in \text{Cone}((k^\times)^2)$. □

**Proposition 4.3.** $\Omega_1 = \Omega_2$.

**Proof.** For any $\alpha \in k^+_R$ and $x \in k^n$, we must prove $\alpha x x^* \in \Omega_2$. By Lemma 4.2, $\alpha$ is represented as

$$\alpha = \sum_i \lambda_i \alpha_i^2$$

with $\lambda_i \in \mathbb{R}_{\geq 0}$ and $\alpha_i \in k^\times$. Then we have

$$\alpha x x^* = \sum_i \lambda_i (\alpha_i x) (\alpha_i x)^* \in \Omega_2.$$ 

□

Next, we prove $\Omega_k = \Omega_1$.

**Lemma 4.4.** $P_n(k) \subset \Omega_1$.

**Proof.** For $a \in P_n(k)$, there exists $g \in GL_n(k)$ such that

$$a = g \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} g^*.$$
where $\lambda_1, \ldots, \lambda_n \in k^\times$. Since $a$ is positive definite, every $\lambda_i$ must be totally positive, i.e., $\lambda_i \in k_R^+ \cap k$. If $e_1, \ldots, e_n$ denote the standard basis of the column vector space $k^n$, then

$$
\begin{pmatrix}
\lambda_1 & 0 \\
\ddots & \ddots \\
0 & \lambda_n
\end{pmatrix} = \lambda_1 e_1^* + \cdots + \lambda_n e_n^*.
$$

By putting $x_i = ge_i \in k^n$, we obtain

$$a = \lambda_1 x_1 x_1^* + \cdots + \lambda_n x_n x_n^* \in \Omega_1.$$

□

**Lemma 4.5.** $P_n(k_R) \subset \Omega_1$.

**Proof.** We fix an $a \in P_n(k_R)$ and a sufficiently small rational number $\mu > 0$ such that $a - \mu I \in P_n(k_R)$, where $I$ denotes the identity matrix. Since $P_n(k)$ is dense in $P_n(k_R)$, for any $\epsilon \in Q$, $0 < \epsilon < \mu$, there exists $a' \in P_n(k)$ such that

$$b = (a - \mu I) - a' \in P_n(k_R),$$

and the $(i, j)$-component $b_{ij} \in k_R$ of $b$ satisfies

$$||b_{ij}||_{k_R} < \epsilon$$

for all $i, j$. We put $c = b + \mu I \in P_n(k_R)$ and

$$d = c - \sum_{i<j} \epsilon E_{ij} \in H_n(k_R),$$

where $E_{ij} = (e_i + e_j)(e_i + e_j)^* \in H_n(k)$. Let $c_{ij} = ((c_{ij})_{\sigma})_{\sigma \in p_{\infty}}$ and $d_{ij} = ((d_{ij})_{\sigma})_{\sigma \in p_{\infty}}$ be the $(i, j)$ components of $c$ and $d$, respectively. Then, we have

$$(d_{ij})_{\sigma} = \begin{cases} (c_{ii})_{\sigma} - (n-1)\epsilon = (b_{ii})_{\sigma} + \mu - (n-1)\epsilon & (i = j) \\ (c_{ij})_{\sigma} - \epsilon = (b_{ij})_{\sigma} - \epsilon < 0 & (i \neq j) \end{cases}$$

for all $\sigma \in p_{\infty}$. Here we note that both $\mu$ and $\epsilon$ are rational numbers. If we fix $i$ and $\sigma$, then

$$\sum_{j \neq i} |(d_{ij})_{\sigma}| = \sum_{j \neq i} |(b_{ij})_{\sigma} - \epsilon_{\sigma}| < 2(n-1)\epsilon.$$

We may assume that $0 < \epsilon \in Q$ is sufficiently small as

$$3(n-1) + 1)\epsilon < \mu.$$

Then, by $3(n-1)\epsilon < \mu - \epsilon \leq \mu + (b_{ii})_{\sigma}$, we have $2(n-1)\epsilon < (d_{ii})_{\sigma}$, and hence

$$\sum_{j \neq i} |(d_{ij})_{\sigma}| < (d_{ii})_{\sigma}.$$

Therefore, the matrix $d_{\sigma} = ((d_{ij})_{\sigma})_{ij} \in M_n(k_{\sigma})$ is near-diagonal and its all non-diagonal elements are negative. This leads us to the following representation of $d_{\sigma}$:

$$d_{\sigma} = \sum_{i<j} \{- (d_{ij})_{\sigma}\}(e_i - e_j)(e_i - e_j)^* + \sum_i (d_{ii})_{\sigma} + \sum_{j \neq i} (d_{ij})_{\sigma} e_i e_i^*.$$
We define \( \alpha_{ij} \in k_\mathbb{R}^+ + \mathbb{R} \) by
\[
(\alpha_{ij})_\sigma = \begin{cases} 
(d_{ii})_\sigma + \sum_{k \neq i} (d_{ik})_\sigma & (i = j) \\
-(d_{ij})_\sigma & (i \neq j)
\end{cases}
\]
for \( \sigma \in \mathbb{P}_\infty \). Then we have
\[
d = \sum_{i<j} \alpha_{ij} (e_i - e_j)(e_i - e_j)^* + \sum_i \alpha_{ii} e_i e_i^* \in \Omega_1,
\]
and hence
\[
c = d + \sum_{i<j} eE_{ij} \in \Omega_1.
\]
Since \( \Omega_1 \) is a convex cone and \( a' \in \Omega_1 \) by Lemma 4.4, \( a = c + a' \) is contained in \( \Omega_1 \). This completes the proof.

**Proposition 4.6.** \( \Omega_k = \Omega_1 \).

**Proof.** We fix a non-zero \( a \in \Omega_1 \). Then \( a \) is represented as
\[
a = \sum_i \alpha_i x_i x_i^*, \quad (\alpha_i \in k_\mathbb{R}^+, \ x_i \in k^n \setminus \{0\}).
\]
An element \( x = (x_\sigma) \in k_\mathbb{R}^n \) is contained in \( \text{rad}(a) \) if and only if
\[
\sum_\sigma \sum_i (\alpha_i)_\sigma (x_\sigma^* \cdot \sigma(x_i))^2 = 0.
\]
Since \( (\alpha_i)_\sigma > 0 \), we have
\[
\text{rad}(a) = \{ x = (x_\sigma) \in k_\mathbb{R}^n \mid x_\sigma^* \cdot \sigma(x_i) = 0 \text{ for all } \sigma, i \}.
\]
If we take a \( k \)-linear subspace
\[
W = \{ x \in k^n \mid x^* \cdot x_i = 0 \},
\]
then
\[
W \otimes \mathbb{Q} \mathbb{R} = \prod_\sigma \sigma(W) \otimes_k k_\sigma = \text{rad}(a).
\]
Thus \( a \) is contained in \( \Omega_k \).

Next we show \( \Omega_k \subset \Omega_1 \) by induction of \( n \). When \( n = 1 \), then \( \Omega_1 = k_\mathbb{R}^+ \cup \{0\} \). For \( a \in \Omega_1 \), its radical is either the whole \( k_\mathbb{R} \) or \( \{0\} \). This means \( a \in k_\mathbb{R}^+ \) or \( a = 0 \).

We consider the case of \( n > 1 \). Let \( a \in \Omega_k \). If \( \text{rad}(a) = \{0\} \), then \( a \in P_{n-1}(k_\mathbb{R}) \), and hence \( a \in \Omega_1 \) by Lemma 4.5. Thus we assume \( \text{rad}(a) \neq \{0\} \). In this case, there is a non-zero \( x \in \text{rad}(a) \cap k^n \). If we take \( g \in GL_n(k) \) whose first column equals \( x \), then \( g^*ag \) is of the form
\[
\begin{pmatrix}
0 & 0 \\
0 & a'
\end{pmatrix}, \quad (a' \in P_{n-1}(k_\mathbb{R})).
\]
We note that
\[
\text{rad}(\begin{pmatrix}
0 & 0 \\
0 & a'
\end{pmatrix}) = g^{-1}\text{rad}(a).
\]
Let $\varphi : k^n \to k^{n-1}$ be a linear map defined by $\varphi((\lambda_1, \ldots, \lambda_n)^*) = (\lambda_2, \ldots, \lambda_n)^*$. Since $\text{rad}(a') = \varphi(g^{-1}\text{rad}(a))$, $a'$ is defined over $k$. By the assumption of induction, $a'$ is represented as
\[
a' = \sum_{i} a_i y_i y_i^* \quad (a_i \in k_R^+, y_i \in k^{n-1}).\]
Then, we obtain
\[
g^*ag = \sum_{i} a_i \begin{pmatrix} 0 \\ y_i \end{pmatrix} \begin{pmatrix} 0 \\ y_i^* \end{pmatrix}^* \in \Omega_1,\]
and hence $a \in (g^*)^{-1}\Omega_1g^{-1} = \Omega_1$. $\square$

In the following, we fix a projective $\mathbb{A}_k$-module $\Lambda_0 \subset k^n$ of rank $n$ and use the same notations as in $\S 2$ and $\S 3$. We note that, since $\Lambda_0 \otimes \mathbb{Q} = k^n$, $\Omega_2$ (and hence $\Omega_k$) is defined as
\[
\Omega_2 = \left\{ \sum_{i=1}^{k} \lambda_i x_i x_i^* \mid 1 \leq k \in \mathbb{Z}, \lambda_i \in \mathbb{R}_{\geq 0}, x_i \in \Lambda_0 \right\}.
\]
Then, it is obvious that $\Omega_k$ is stabilized by the action of $GL(\Lambda_0)$ on $P_{n}^{-}(k_R)$. For $a \in \Omega_k$, define the subgroup $\Gamma_a$ of $GL(\Lambda_0)$ by
\[
\Gamma_a = \{ \gamma \in GL(\Lambda_0) \mid a \cdot \gamma^* = \gamma a \gamma^* = a \}.
\]

**Lemma 4.7.** For a given non-zero $a \in \Omega_k$ and a constant $\theta > 0$, the set
\[
[a]_{\theta} = \{ b \in \partial^0 K_1(m) \mid (a, b) \leq \theta \}
\]
is $\Gamma_a$-invariant, and the number of $\Gamma_a$-orbits in $[a]_{\theta}$ is finite.

**Proof.** Since
\[
(a, b \cdot \gamma) = (a \cdot \gamma^*, b) = (a, b)
\]
holds for any $b \in [a]_{\theta}$ and $\gamma \in \Gamma_a$, $[a]_{\theta}$ is $\Gamma_a$-invariant. By the remark mentioned above, $a$ is represented as
\[
a = \sum_{i=1}^{k} \lambda_i x_i x_i^*, \quad (\lambda_i \in \mathbb{R}_{\geq 0}, x_i \in \Lambda_0 \setminus \{0\}).
\]
Since $\partial^0 K_1(m)/GL(\Lambda_0)$ is a finite set, we choose a complete system $b_1, \ldots, b_t$ of representatives of $\partial^0 K_1(m)/GL(\Lambda_0)$. We define the subgroup $\Gamma$ of $GL(\Lambda_0)$ as
\[
\Gamma = \{ \gamma \in GL(\Lambda_0) \mid \gamma x_i = x_i \text{ for all } i = 1, \ldots, k \}.
\]
Since $\Gamma \subset \Gamma_a$ and
\[
[a]_{\theta} = \bigcup_{i=1}^{t} [a]_{\theta} \cap (b_i \cdot GL(\Lambda_0))
\]
it is sufficient to prove the finiteness of $\Gamma$-orbits in $[a]_{\theta} \cap (b_i \cdot GL(\Lambda_0))$ for all $i = 1, \ldots, t$. We fix $b \in [a]_{\theta} \cap (b_i \cdot GL(\Lambda_0))$. By replacing $b_i$ with $b$ if necessary, we may assume $b = b_i$. We choose a complete system $\{ \gamma_j \}$ of representatives of $GL(\Lambda_0)/\Gamma$, which is an infinite set. We put
\[
\tilde{x} = t(x_1, x_2, \ldots, x_k) \in \Lambda_0^{\oplus k}
\]
and
\[
\tilde{x}_j = t(\gamma_j x_1, \gamma_j x_2, \ldots, \gamma_j x_k) \in \Lambda_0^{\oplus k}.
\]
If \( j \neq j' \), then \( \tilde{x}_j \neq \tilde{x}_{j'} \). For \( b \in P_n(k_{\mathbb{R}}) \), define
\[
\tilde{b} = \begin{pmatrix} \lambda_1 b & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_k b \end{pmatrix} \in P_{kn}(k_{\mathbb{R}}).
\]
Then we have
\[
(a, b \cdot \gamma_j) = \text{Tr}_{k_{\mathbb{R}}}((\tilde{x}_j \tilde{b}_i \tilde{x}_j^*)).
\]
Since \( \Lambda_0^{\oplus k} \subset k_{\mathbb{R}}^{kn} \) is a lattice and \( \tilde{b}_i \) is positive definite, the cardinality of the set
\[
\{ \tilde{x} \in \Lambda_0^{\oplus k} \mid \text{Tr}_{k_{\mathbb{R}}}((\tilde{x} \tilde{b}_i \tilde{x})^*) \leq \theta \}
\]
is finite. In particular, the number of \( \Gamma \)-orbits in \([a]_\theta \) is finite. This shows that the number of \( \Gamma \)-orbits in \([a]_\theta \cap (b \cdot GL(\Lambda_0)) \) is finite. \( \square \)

Since \( \Gamma_a \) is a finite group, Lemma 4.7 gives another proof of Lemma 3.2.

**Lemma 4.8.** For \( a \in \Omega_k \setminus \{0\} \), there exists \( b_0 \in \partial^0 K_1(m) \) such that
\[
\inf_{b \in K_1(m)} (a, b) = (a, b_0),
\]
and then \( a \in D_{b_0} \).

**Proof.** We choose a sufficiently large \( \theta > 0 \) so that \([a]_\theta \neq \emptyset \). Since \( K_1(m) \) is the convex hull of \( \partial^0 K_1(m) \), we have
\[
\inf_{b \in K_1(m)} (a, b) = \inf_{b \in \partial^0 K_1(m)} (a, b) = \inf_{b \in [a]_\theta} (a, b) = \inf_{b \Gamma_a \in [a]_\theta / \Gamma_a} (a, b).
\]
The existence of \( b_0 \) follows from Lemma 4.7.

By [9, Lemma 4.3] (or Theorem 2.5), there is a neighborhood \( N \) of \( b_0 \) in \( P_n(k_{\mathbb{R}}) \) such that \( S(b) \subset S(b_0) \) for any \( b \in N \). Let \( R_{\geq 0}c_1, \cdots, R_{\geq 0}c_k \) be all extreme rays of \( C_{b_0} \). We choose a sufficiently small \( \epsilon > 0 \) so that \( b_0 + \epsilon c_i \in N \) for all \( i = 1, \cdots, k \).

Since \( m(b_0 + \epsilon c_i)^{-1}(b_0 + \epsilon c_i) \in K_1(m) \), we have
\[
(a, b_0)m(b_0 + \epsilon c_i) \leq (a, b_0 + \epsilon c_i).
\]
Then, for \( x \in S(b_0 + \epsilon c_i) \subset S(b_0) \),
\[
(a, b_0)(b_0 + \epsilon c_i, xx^*) \leq (a, b_0 + \epsilon c_i)
\]
holds. From \( c_i \in C_{b_0} \), it follows
\[
0 \leq \epsilon(a, b_0)(c_i, xx^*) \leq \epsilon(a, c_i),
\]
namely,
\[
a \in \bigcap_{i=1}^{k} H_{c_i} = D_{b_0}.
\]
\( \square \)

By this Lemma, we have
\[
\Omega_k = \bigcup_{b \in \partial^0 K_1(m)} D_b.
\]
Let \( b_1, \cdots, b_l \) be a complete system of representatives of \( \partial^0 K_1(m)/GL(\Lambda_0) \). For each \( i \), \( \Gamma_i \) denotes the stabilizer of \( b_i \) in \( GL(\Lambda_0) \), i.e.,
\[
\Gamma_i = \{ \gamma \in GL(\Lambda_0) \mid b_i \cdot \gamma = b_i \},
\]
which is a finite subgroup. We put $GL(\Lambda_0)^* = \{ \gamma^* \mid \gamma \in GL(\Lambda_0) \}$ and $
abla^* = \{ \gamma^* \mid \gamma \in \Gamma_i \}$. It is easy to check that $S(a \cdot \gamma) = \gamma^{-1} S(a)$ and $D_a \cdot \gamma = D_a \cdot \gamma^*$ hold for all $a \in \partial^0 K_1(m)$ and $\gamma \in GL(\Lambda_0)$. In particular, the finite group $\nabla^*$ stabilizes $D_b_0$. Now the following theorem is obvious.

**Theorem 4.9.** Notations being as above, one has

$$\Omega_k/GL(\Lambda_0)^* = \bigcup_{i=1}^t D_{b_i}/\nabla_i^*.$$

As an example, we consider the case of $n = 1$. In this case, $\Omega_k \setminus \{0\}$ equals $k^+_R$. If $\Lambda_0 = \omega_k$, then $GL(\Lambda_0)$ equals the unit group $E_k$ of $\omega_k$. The action of $E_k$ on $k^+_R$ is given by $x \cdot \epsilon = \epsilon^2 x$ for $\epsilon \in E_k$ and $x \in k_R$. Since $\Gamma_i = \{ \pm 1 \}$ trivially acts on $D_{b_i}$, Theorem 4.9 yields

$$k^+_R/E_k = E_k^2 \setminus k^+_R = \bigcup_{i=1}^t D_{b_i}^*,$$

where $D_{b_i}^* = D_{b_i} \setminus \{0\}$. In other words, a fundamental domain of $E_k^2 \setminus k^+_R$ decomposes into a union of cones.

5. **Ryshkov polyhedra of real quadratic fields**

In this section, we consider the simplest case, i.e., $n = 1$ and $k$ is a real quadratic field $Q(\sqrt{d})$, where $d$ is a square free positive integer. In this case, we have $\Omega_k \setminus \{0\} = P_2(k_R) = k^+_R = R^2_\omega$ by identifying $k_R$ with $R^2$. We denote by $\tau$ the Galois involution of $k$, which acts on $k^+_R$ by the reflection with respect to the line $R1 = R(1, 1)$ of the direction $(1, 1)$. Let $\Lambda_0 = \omega_k = Z[\omega]$, where $\omega = \sqrt{d}$ if $d \equiv 2, 3 \mod 4$ or $\omega = (1 + \sqrt{d})/2$ if $d \equiv 1 \mod 4$. The $\Lambda_0$-minimum function $m = m_{\Lambda_0}$ is given by

$$m(a) = \min_{0 \neq x \in \omega_k} (\alpha_1 x^2 + \alpha_2 \tau(x^2))$$

for $a = (\alpha_1, \alpha_2) \in k_R^2$. The Ryshkov polyhedron $K_1(m)$ is a convex domain in $k_R^2$ with infinite vertices.

**Lemma 5.1.** The Ryshkov polyhedron $K_1(m)$ is invariant by $\tau$, i.e., $K_1(m)$ is symmetric with respect to $R1$. If $a \in \partial^0 K_1(m)$, then $a \in k_R^2 \cap k$ and $\tau(a) \in \partial^0 K_1(m)$.

This is clear from $\tau(\omega_k) = \omega_k$ and Theorem 1.2.

Every $\omega_k$-perfect form $a \in \partial^0 K_1(m)$ is of the form $(\alpha, \tau(\alpha))$ with a totally positive $\alpha \in k$. It is easy to prove that there is no $\omega_k$-perfect form on the half-line $R_{>0}1$. Thus there is a unique $\omega_k$-perfect form $a = (\alpha, \tau(\alpha)) \in \partial^0 K_1(m)$ such that $\tau(\alpha)$ is minimal among $\omega_k$-perfect forms in $K_1(m) \cap \{ (\alpha_1, \alpha_2) \in k_R^2 \mid \alpha_1 < \alpha_2 \}$. We call this $\omega_k$-perfect form the minimal $\omega_k$-perfect form.

Let $E_k$ be the unit group of $\omega_k$. The action of $GL(\Lambda_0) = E_k$ on $K_1(m)$ is given by $(a, u) \mapsto a \cdot u = u^2 a$ for $(a, u) \in K_1(m) \times E_k$. We fix a fundamental unit $\epsilon \in E_k$ such that $\epsilon^2 < 1$. Then $\{ \epsilon^2 a \mid k \in Z \}$ is the set of elements that are equivalent with $a$. Let $t_k$ be the number of equivalent classes in $\partial^0 K_1(m)$, i.e., the cardinal number of $\partial^0 K_1(m)/GL(\Lambda_0) = E_k^2/\partial^0 K_1(m)$.

**Lemma 5.2.** Let $a$ be the minimal $\omega_k$-perfect form. Then $t_k = 1$ if and only if $\epsilon^{-2} a = \tau(a)$. 
**Proof.** By Lemma 5.1, $a$ and $\tau(a)$ are symmetric each other with respect to $R$. Obviously, $a$ and $\tau(a)$ are equivalent if and only if $t_k = 1$. Assume $a$ and $\tau(a)$ are equivalent. Then $\tau(a)$ is equal to $\epsilon^{2k}a$ for some $k$. By the minimal condition of $a$, $k$ must be equal to $-1$. □

**Lemma 5.3.** Let $\beta_0 = (\tau(\epsilon^2) - 1)^{-1}\sqrt{d}$ and $b_0 = (\beta_0, \tau(\beta_0)) \in k^+_R \cap k$. If $b = (\beta, \tau(\beta)) \in k^+_R \cap k$ satisfies $\beta < \tau(\beta)$ and $\tau(b) = \epsilon^{-2}b$, then $b$ is a scalar multiple of $b_0$.

**Proof.** Since the slope of the line segment between $b$ and $\tau(b) = \epsilon^{-2}b$ equals $-1$, we have

$$\frac{\epsilon^2\tau(\beta) - \tau(\beta)}{\tau(\epsilon^2)\beta - \beta} = -1.$$  

If we put $\delta = (\tau(\epsilon^2) - 1)\beta$, then $\tau(\delta) = -\delta$. Thus $\delta$ is of the form $\xi\sqrt{d}$ with $\xi \in \mathbb{Q}$, and hence $b = \xi b_0$. □

**Proposition 5.4.** Let $b_0$ be the same as above. Then $b_0$ is $\mathfrak{o}_k$-perfect if and only if $t_k$ is odd.

**Proof.** Let $a_0$ be the minimal $\mathfrak{o}_k$-perfect form. We assume that $b_0 = \mathfrak{o}_k$-perfect. Let $\{a_0, \cdots, a_k = m(b_0)^{-1}b_0\}$ be a sequence of $\mathfrak{o}_k$-perfect forms in $\mathfrak{O}^K_1(m)$ such that $a_i$ and $a_{i+1}$ are adjacent each other for $i = 0, \cdots, k - 1$ and the first component of $a_i$ is larger than that of $a_{i+1}$ for all $i$. From $\tau(a_k) = \epsilon^{-2}a_k$, it follows that any two elements of $\{a_0, \cdots, a_k, \tau(a_0), \cdots, \tau(a_{k-1})\}$ can not be equivalent. This yields $t_k = 2k + 1$. Conversely, we assume that $t_k$ is odd, say $t_k = 2k + 1$. We can take a complete set $\{a_0, \cdots, a_{2k}\}$ of representatives of $E^\infty_k(\mathfrak{O}^K_1(m))$ contained in $\{\{a_0, a_2\} \in k^+_R \mid \alpha_1 < \alpha_2\}$ so that $a_i$ and $a_{i+1}$ are adjacent each other for $i = 0, \cdots, 2k - 1$. By comparing size of first components of $a_0, \cdots, a_{2k}, \epsilon^{-2}a_0, \cdots, \epsilon^{-2}a_{2k}$, we obtain $\tau(a_i) = \epsilon^{-2}a_{2k-i}$ for $i = 0, \cdots, 2k$, in particular, $\tau(a_k) = \epsilon^{-2}a_k$. By Lemma 5.3, $a_k$ must be a scalar multiple of $b_0$. □

Let $\eta = (1 + \epsilon^2)/(1 - \epsilon^2)$. Since $\tau(\eta) = -\eta$, $\eta$ is of the form $\theta\sqrt{d}$ with $\theta \in \mathbb{Q}$. Define the rational binary quadratic form $q$ as

$$q(x_1, x_2) = \begin{cases} 
\theta x_1^2 - 2x_1x_2 + \theta x_2^2 & (d \equiv 2, 3 \mod 4) \\
\theta x_1^2 + (\theta - 1)x_1x_2 + 4^{-1}(1 + d)(\theta - 1)x_2^2 & (d \equiv 1 \mod 4) 
\end{cases}$$

Then, $(b_0, xx^*) = d \cdot q(x_1, x_2)$ holds for $x = x_1 + x_2\omega \in \mathfrak{o}_k$. Therefore, $b_0$ is $\mathfrak{o}_k$-perfect if and only if the perfection rank of $q$ is greater than 1. See [7, Definition 13.1.2] for perfection rank.

**Example.** When $d \leq 10000$ and $d \equiv 2, 3 \mod 4$, there are 486 $d$ such that $b_0$ is $\mathfrak{o}_k$-perfect, for example,

$$2, 3, 10, 15, 26, 35, 58, 74, 82, 91, 106, 122, 130, 143, 170, 195, 202, 218, 226, 247, \ldots, 9699, 9722, 9754, 9770, 9778, 9818, 9831, 9866, 9879, 9919, 9993, 9946, 9970.$$

**Example.** When $d \leq 10000$ and $d \equiv 1 \mod 4$, there are 1061 $d$ such that $b_0$ is $\mathfrak{o}_k$-perfect, for example,

$$5, 13, 17, 21, 29, 37, 41, 53, 61, 65, 73, 77, 85, 89, 97, 101, 109, 113, 133, 137, \ldots, 9865, 9869, 9877, 9881, 9939, 9901, 9929, 9941, 9949, 9953, 9965, 9973, 9985, 9997.$$

**Proposition 5.5.** If $\epsilon \cdot \tau(\epsilon) = -1$, then $t_k$ is odd.
Let $a_0$ be the minimal $o_k$-perfect form. We choose a sequence $a_0, a_1, \ldots, a_t = (\alpha_i, \tau(\alpha_i))$ of $\partial^0 K_1(m)$ such that $a_{t-1}$ and $a_t$ are adjacent, $\alpha_i < \tau(\alpha_i)$ and $\alpha_i < \alpha_{i-1}$ for all $i$. Since $a_{tk} = c^2 \tau(a_0)$, we have:

$$a_k = \begin{cases} c^2 \tau(a_k) & \text{if } t_k = 2k + 1 \\ c^2 \tau(a_{k-1}) & \text{if } t_k = 2k \\ \end{cases}.$$

Since $a_{k-1}$ and $a_k$ are adjacent each other, there exists an $x \in S(a_{k-1}) \cap S(a_k)$. If $t_k = 2k$, then $\tau(\epsilon x) \in S(a_{k-1}) \cap S(a_k)$. Therefore, we have $x = \pm \tau(\epsilon x)$, and hence $\epsilon \cdot \tau(\epsilon) = 1$. This is a contradiction. □

If $b_0$ is not $o_k$-perfect, we need to construct an initial $o_k$-perfect form of Voronoï algorithm. The following proposition gives this. This initial $o_k$-perfect form was also found by Gunnells and Yasaki [3, Proposition 6.1] by other method.

**Proposition 5.6.** (1) Let $d \equiv 2, 3 \pmod{4}$ and $n$ be the integer such that

$$n - 1 \leq \frac{-1 + \sqrt{4d - 3}}{2} < n.$$

Then $a_0 = (\alpha, \tau(\alpha))$ defined by

$$\alpha = \frac{1}{2} + \frac{n^2 + d - 1}{4dn} \sqrt{d}$$

is $o_k$-perfect and

$$S(a_0) = \begin{cases} \{\pm 1, \pm (n - \omega)\} & (d > n^2 - n + 1) \\ \{\pm 1, \pm (n - \omega), \pm (n - 1 - \omega)\} & (d = n^2 - n + 1) \\ \end{cases}.$$

Moreover, $\tau(a_0) = (\tau(\alpha), \alpha)$ is the minimal $o_k$-perfect form.

(2) Let $d \equiv 1 \pmod{4}$ and $n$ be the integer such that

$$n - 1 < \frac{\sqrt{d - 3}}{2} < n.$$

Then $a_0 = (\alpha, \tau(\alpha))$ defined by

$$\alpha = \frac{1}{2} + \frac{(2n - 1)^2 + d - 4}{4d(2n - 1)} \sqrt{d}$$

is $o_k$-perfect and $S(a_0) = \{\pm 1, \pm (n - \omega)\}$. Moreover, $\tau(a_0) = (\tau(\alpha), \alpha)$ is the minimal $o_k$-perfect form.

**Proof.** (1) From the definition of $n$, it follows $n^2 - n + 1 \leq d < n^2 + n + 1$. For $x = x_1 + x_2 \omega \in o_k$, $(a_0, xx^*)$ equals

$$\frac{1}{4n^2} \{2n x_1 + (n^2 + d - 1)x_2 \}^2 + \frac{1}{4n^2} \{4dn^2 - (n^2 + d - 1)^2 \} x_2^2.$$

If $x_2 = 0$, then $(a_0, xx^*) \geq 1$ and the equality holds for $x = \pm 1$. If $|x_2| = 1$, then we may assume $x_2 = -1$. We have $(a_0, xx^*) \geq 1$ since

$$\langle a_0, (x_1 - \sqrt{d})(x_1 - \sqrt{d})^* \rangle - 1 = \langle x_1 - n \rangle \{nx_1 - (d - 1) \} / n$$

and $n - 1 \leq (d - 1)/n < n + 1$. The equality holds for $x = \pm (n - \omega)$ and in addition $x = \pm (n - 1 - \omega)$ if $d = n^2 - n + 1$. If $|x_2| \geq 2$, then we have

$\{4dn^2 - (n^2 + d - 1)^2 \} x_2^2 - 4n^2 \geq 4 \{4dn^2 - (n^2 + d - 1)^2 \} - 4n^2$

$$= -4 \{d^2 - 2d(n^2 + 1) + (n^2 - 1)^2 + n^2 \}.$$
This polynomial is positive if \( n^2 - \sqrt{3}n + 1 < d < n^2 + \sqrt{3}n + 1 \) and this is the case. Hence \( x = \pm 1 \) and \( y = \pm (n - \omega) \) are shortest vectors of \( a_0 \). Since \( xx^* = (1, 1) \) and \( yy^* = ((n - \omega)^2, (n + \omega)^2) \in k_R^+ \) are linearly independent, \( a_0 \) is \( \omega_k \)-perfect. From \( S(a_0) \cap S(\tau(a_0)) = \{ \pm 1 \} \) and Lemma 2.3, it follows that \( a_0 \) and \( \tau(a_0) \) are adjacent each other. Such an \( \omega_k \)-perfect form must be minimal.

(2) The integer \( d \) is bounded as \( 4n^2 - 8n + 7 < d < 4n^2 + 3 \). For \( x = x_1 + x_2\omega \in \omega_k \), \((a_0, xx^*)\) equals

\[
\frac{1}{16(2n-1)^2} \{ 4(2n-1)x_1 + (4n^2 + d - 5)x_2 \}^2
+ \frac{1}{16(2n-1)^2} \{ 8(2n-1)(2n^2 + dn - n - 2) - (4n^2 + d - 5)^2 \} x_2^2.
\]

If \( x_2 = 0 \), then \((a_0, xx^*) \geq 1\) and the equality holds for \( x = \pm 1 \). If \( |x_2| = 1 \), then we may assume \( x_2 = -1 \). Then we have \((a_0, xx^*) \geq 1\) since

\[
(a_0, (x_1 - \omega)(x_1 - \omega)^*) - 1 = (x_1 - n) \{ 2(2n-1)x_1 - (2n + d - 5) \}/2(2n-1)
\]

and \( n - 1 < (2n + d - 5)/2(2n-1) < n + 1 \). The equality holds for \( x = \pm(n - \omega) \). If \( |x_2| \geq 2 \), then we have

\[
\{8(2n-1)(2n^2 + dn - n - 2) - (4n^2 + d - 5)^2 \} x_2^2 - 16(2n-1)^2
\]

\[
\geq 4 \{ 8(2n-1)(2n^2 + dn - n - 2) - (4n^2 + d - 5)^2 \} - 16(2n-1)^2
= -4(d^2 - 2(4n^2 - 4n + 5)d + 16n^4 - 32n^3 + 8n^2 + 8n + 13).
\]

This polynomial is positive if \( 4n^2 - 4n + 5 - 2(2n - 1) \sqrt{3} < d < 4n^2 + 4n + 5 + 2(2n - 1) \sqrt{3} \) and this is the case. Hence \( x = \pm 1 \) and \( y = \pm(n - \omega) \) are shortest vectors of \( a_0 \). This implies that \( a_0 \) is \( \omega_k \)-perfect and \( \tau(a_0) \) is the minimal \( \omega_k \)-perfect form.

By Proposition 5.6 and Lemma 5.2, we can easily determine whether \( t_k = 1 \) or not for a given \( k \).

**Example.** When \( d \leq 10000 \) and \( d \equiv 2, 3 \mod 4 \), there are 77 \( d \) such that \( t_k = 1 \). These are given by

\[
\begin{align*}
2, 3, 10, 15, 26, 35, 82, 122, 143, 170, 195, 226, 255, 290, 323, 362, 399, 442, 483, 530, 620, 730, 842, 899, 962, 1023, 1090, 1155, 1226, 1295, 1370, 1443, 1522, 1599, 1763, 2026, 2210, 2402, 2602, 2703, 2810, 2915, 3026, 3135, 3363, 3482, 3599, 3722, 3970, 4226, 4355, 4490, 4623, 4762, 4899, 5042, 5183, 5330, 5626, 5930, 6083, 6242, 6562, 6890, 7055, 7226, 7395, 7570, 7743, 7922, 8099, 8282, 8463, 8835, 9026, 9215, 9410.
\end{align*}
\]

**Example.** When \( d \leq 10000 \) and \( d \equiv 1 \mod 4 \), there are 77 \( d \) such that \( t_k = 1 \). These are given by

\[
\begin{align*}
\end{align*}
\]

These examples lead us to the following question.

**Question.** Are there infinitely many real quadratic fields \( k \) such that \( t_k = 1 \)?

If \( t_k = 1 \), we have a simple description of the fundamental unit \( \epsilon^{-1} \).
Proposition 5.7. Let \( n \) be the same as above. Then \( t_k = 1 \) if and only if \( \epsilon^{-1} = n - \tau(\omega) \).

Proof. Let \( a_0 \) be the same as in Proposition 5.6. Assume \( t_k = 1 \). From \( \epsilon^2 a_0 = \tau(a_0) \), it follows \( \epsilon^{-1} S(a_0) = S(\tau(a)) \). Therefore, \( \epsilon^{-1} \) must be equal to \( n - \tau(\omega) \) since \( \epsilon^{-1} > 1 \) and \( n - \tau(\omega) > 1 \). Conversely, assume \( \epsilon^{-1} = n - \tau(\omega) \). Then one has \( S(\epsilon^2 a_0) = \epsilon^{-1} S(a_0) = S(\tau(a_0)) \). Since any perfect form \( a \) is uniquely determined by \( m(a) \) and \( S(a) \), we get \( \epsilon^2 a_0 = \tau(a_0) \).

We give some examples of \( K_1(m) \).

Example. The case of \( d = 5 \). In this case, \( t_k = 1 \) and the minimal \( \alpha_k \)-perfect form is

\[
a = \left( \frac{1}{2} - \frac{\sqrt{5}}{10}, \frac{1}{2} + \frac{\sqrt{5}}{10} \right).
\]

The Ryshkov domain \( K_1(m) \) is of the following form.

![Graph for d=5](image)

Example. The case of \( d = 6 \). In this case, \( t_k = 2 \) and the minimal \( \alpha_k \)-perfect form is

\[
a = \left( \frac{1}{2} - \frac{3\sqrt{6}}{16}, \frac{1}{2} + \frac{3\sqrt{6}}{16} \right).
\]

An inequivalent \( \alpha_k \)-perfect form is \( \tau(a) \). The Ryshkov domain \( K_1(m) \) is of the following form.

![Graph for d=6](image)
Example. The case of \( d = 17 \). In this case, \( t_k = 3 \) and the minimal \( \sigma_k \)-perfect form is
\[
a = \left( \frac{1}{2} \frac{11\sqrt{17}}{102} \frac{1}{2} + \frac{11\sqrt{17}}{102} \right).
\]
Vertices adjacent to \( a \) are \( \tau(a) \) and
\[
b = \left( 1 - \frac{4\sqrt{17}}{17}, 1 + \frac{4\sqrt{17}}{17} \right).
\]
Representatives of \( E_k^2 \setminus \partial^0 K_1(m) \) is given by \( \{a, \tau(a), b\} \).

Example. The case of \( d = 19 \). In this case, \( t_k = 4 \) and the minimal \( \sigma_k \)-perfect form is
\[
a = \left( \frac{1}{2} \frac{17\sqrt{19}}{152} \frac{1}{2} + \frac{17\sqrt{19}}{152} \right).
\]
Vertices adjacent to \( a \) are \( \tau(a) \) and
\[
b = \left( \frac{7}{2} \frac{61\sqrt{19}}{76} \frac{7}{2} + \frac{61\sqrt{19}}{76} \right).
\]
Representatives of \( E_k^2 \setminus \partial^0 K_1(m) \) is given by \( \{a, \tau(a), b, \tau(b)\} \).

We do not know whether \( t_k \) has a bound or not when \( k \) runs over all real quadratic fields.
References


Graduate School of Science, Osaka University, Toyonaka, Osaka 560-0043, Japan
E-mail address: twatanabe@math.sci.osaka-u.ac.jp; yn.showg@gmail.com