ON REDUCED ARAKELOV DIVISORS OF REAL QUADRATIC FIELDS

TRAN NGUYEN THANH HA

Abstract. We generalize the concept of reduced Arakelov divisors and define C-reduced divisors for a given number $C \geq 1$. These C-reduced divisors have very nice properties which are similar to the properties of reduced ones. In this paper, we describe an algorithm to test whether an Arakelov divisor of a real quadratic field $F$ is $C$-reduced in polynomial time in $\log|\Delta_F|$ with $\Delta_F$ the discriminant of $F$. Moreover, we give an example of a cubic field for which our algorithm does not work.

1. Introduction

The idea of infrastructure of real quadratic fields of D. Shanks in [11] was modified and extended by H. Lenstra [5], R. Schoof [9] and J. Buchmann and H. Williams [2] to certain number fields. Finally, it was generalized to arbitrary number field by J. Buchmann [1]. In 2008, Schoof [10] gave the first description of infrastructure in terms of reduced Arakelov divisors and the Arakelov class group $Pic_F^0$ of a general number field $F$. Reduced Arakelov divisors can be used for computing $Pic_F^0$. They form a finite and regularly distributed set in this topological group (cf.[10, Proposition 7.2, Theorem 7.4 and Theorem 7.7]). Computing $Pic_F^0$ is of interest because knowing this group is equivalent to knowing the class group and the unit group of $F$ (see [6] and [10]).

In [10], Schoof proposed two algorithms which run in polynomial time in $\log|\Delta_F|$ with $\Delta_F$ the discriminant of $F$ (cf.[10, Algorithm 10.3]). Namely, the testing algorithm to check whether a given Arakelov divisor $D$ is reduced and the reduction algorithm to compute a reduced Arakelov divisor that is close to a given divisor $D$ in $Pic_F^0$. However, the reduction algorithm requires finding a shortest vector of the lattice associated to the Arakelov divisor while finding a reasonably short vector using the LLL algorithm is much faster and easier than finding a shortest vector. This leads to a modification and generalization of the definition of reduced Arakelov divisors.

One of the generalizaton comes from the reduction algorithm of Schoof (cf.[10, Algorithm 10.3]) that we call $C$-reduced Arakelov divisors. With this definition, $C$-reduced Arakelov divisors are reduced in the usual sense when $C = 1$ and Arakelov divisors that are reduced in the usual sense are $C$-reduced with $C = \sqrt{n}$ (see [10]). $C$-reduced divisors still form a finite and regularly distributed set in $Pic_F^0$ as the reduced divisors.

However, the modification has a drawback. Because for general number fields, we do not know how to test whether a given divisor is $C$-reduced. Currently, we have a testing

\[Key words and phrases.\] Arakelov, divisor, reduced.

1
algorithm to do this only for real quadratic fields in polynomial time in log (|Δ_F|). It is
the main result of this paper and is presented in Section 4.

In Section 2, we discuss C-reduced Arakelov divisors in an arbitrary number field. Section 3 is devoted to showing the properties of C-reduced fractional ideals of real quadratic fields. An example of real cubic fields in which the testing algorithm is no longer efficient is given in Section 5.

2. C-reduced Arakelov divisors

In this section, we introduce C-reduced Arakelov divisors of number fields.

Let F be a number field of degree n and r_1, r_2 the number of real and complex infinite primes of F. Let F_R := F ⊗ Q R ≃ \prod_{σ_{\text{real}}} R \times \prod_{σ_{\text{complex}}} C. Here σ’s are the infinite primes of F.

Definition 2.1. An Arakelov divisor is a formal finite sum D = \sum p n_p p + \sum σ x_σ σ where p runs over the nonzero prime ideals of \(O_F\) and σ runs over the infinite primes of \(F\), \(n_p \in \mathbb{Z}\) but \(x_σ \in \mathbb{R}\).

For each divisor D, we associate to it the pair of Hermitian line bundle \((I, u)\) where \(I = \prod_p p^{-n_p}\) is a fractional ideal of \(F\) and \(u = (e^{-x_{σ}})_σ\) is a vector in \(\prod_σ \mathbb{R}_{>0} \subset F_R\).

There is a natural way to associate an ideal lattice to \(D\). Indeed, \(I\) is embedded into \(F_R\) by the infinite primes \(σ\). Each element \(g\) of \(I\) is mapped to the vector \((σ(g))_σ\) in \(F_R\). Since the vector \(ug := (u_σ σ(g))_σ\in F_R\), we can define \(\|g\|_D := \|ug\|\).

In term of coordinate, we have
\[
\|g\|_D^2 = \sum_{σ_{\text{real}}} u_σ^2 |σ(g)|^2 + 2 \sum_{σ_{\text{complex}}} |u_σ|^2 |σ(g)|^2.
\]

With this scalar product, \(I\) becomes an ideal lattice in \(F_R\). We call \(I\) the ideal lattice associated to \(D\). The vector \(u\) has a role as a metric for \(I\). So we define as follows.

Definition 2.2. Let \(I\) be a fractional ideal of \(F\) and let \(u\) in \(F_R^*\). The length of an element \(g\) of \(I\) with respect to the metric \(u\) is defined by \(\|g\|_u := \|ug\|\).

Definition 2.3. Let \(I\) be a fractional ideal. Then 1 is called primitive in \(I\) if 1 belongs to \(I\) and it is not divisible by any integer at least 2.

Definition 2.4. Let \(C \geq 1\). A fractional ideal \(I\) is called C-reduced if the following hold:

- 1 is primitive in \(I\).
- There exists a metric \(u \in \prod_σ \mathbb{R}_{>0}\) such that for all \(g \in I \setminus \{0\}\), we have \(\|1\|_u \leq C\|g\|_u\).

The second condition is equivalent to saying that there exists a metric \(u\) such that with respect to this metric, the vector 1 scaled by the scalar \(C\) is the shortest vector in the lattice \(I\).
Lemma 2.1. Let $I$ be a fractional ideal of $F$. We define $d(I) := (I, N(I)^{-\frac{1}{2}})$ the Arakelov divisor with the Hermitian line bundle $(I, u)$ where $u = (u_\sigma)_\sigma$ and $u_\sigma = N(I)^{-\frac{1}{2}}$ for all $\sigma$.

Definition 2.5. Let $I$ be an integral ideal and its norm is at most $C$.

An Arakelov divisor $D$ is called $C$-reduced if $D$ has the form $D = d(I)$ for some $C$-reduced fractional ideal $I$.

Now we prove the following lemma.

Lemma 2.1. Let $I$ be a fractional ideal. If $I$ is $C$-reduced then the inverse $I^{-1}$ of $I$ is an integral ideal and its norm is at most $C^n \partial_F$ where $\partial_F = (2/\pi)^2 \sqrt{|\Delta_F|}$.

Proof. Since $1 \in I$, we have $I^{-1} \subset O_F$. Then $L = N(I)^{-1/n}I$ is a lattice of covolume $\sqrt{|\Delta_F|}$ (cf.[10] Section 4]). Consider the symmetric, convex and bounded subset of $F_\mathbb{R}$

$$S = \{(x_\sigma)_\sigma : |x_\sigma| < \partial_F^{1/n} \text{ for all } \sigma\}.$$ 

We have

$$\text{vol}(S) = 2^n (2\pi)^2 \partial_F = 2^n \text{covol}(L).$$

By Minkowski’s theorem, there is a nonzero element $f \in I$ such that

$$N(I)^{-1/n} |\sigma(f)| \leq \partial_F^{1/n} \text{ for all } \sigma.$$ 

Since $I$ is $C$-reduced, there exists a matrix $u$ such that $\|1\|_u \leq C \|f\|_u$. This implies that $\|u\| \leq C \|u\| \max_\sigma |\sigma(f)| \leq C \|u\| \partial_F^{1/n} N(I)^{1/n}$. So, we have $N(I^{-1}) \leq C^n \partial_F$.

Remark 2.1. In this paper, given a fractional ideal $I$, we assume that it is represented by a matrix with rational entries as in (cf.[7] Section 4) and (cf.[6] Section 2). Without loss of generality, we can also assume that the length of the input is polynomial in $\log |\Delta_F|$.

By Lemma (2.1), to test whether $I$ is $C$-reduced, first we can check that $N(I)^{-1} \leq C^n \partial_F$. We have the following.

Lemma 2.2. Testing $N(I)^{-1} \leq C^n \partial_F$ can be done in polynomial time in $\log |\Delta_F|$.

Proof. Since we know that $N(I)^{-1} = \sqrt{|\Delta_F|/\text{covol}(I)}$, it is sufficient to check that $|\det(M)| = \text{covol}(I) > \left(\frac{2}{\pi}\right)^2 C^n$. Recall that the determinant of the matrix $M$ can be computed in polynomial time (cf.[3] Section 1]). This reason and Remark (2.1) imply that testing $N(I)^{-1} \leq C^n \partial_F$ can be done in polynomial time in $\log |\Delta_F|$.

Regarding the primitiveness of 1 in $I$, we have the result below.

Lemma 2.3. Let $C \geq 1$ and let $I$ be a fractional ideal containing 1 and $N(I)^{-1} \leq C^n \partial_F$. Then testing whether or not 1 is primitive can be done in time polynomial in $\log |\Delta_F|$.

Proof. Let $\{c_1, ..., c_n\}$ be an LLL-reduced basis of $O_F$ and $\{b_1, ..., b_n\}$ be an LLL-reduced basis of $I^{-1}$. Since $1 \in I$, we get $I^{-1} \subset O_F$ and so $b_i \in O_F$ for all $i$. Then for each $i = 1, ..., n$, there exist the integers $k_{ij}$ with $j = 1, ..., n$ for which $b_i = \sum_j k_{ij}c_j$. Thus,
there is an integer \( d \) such that \( \frac{1}{d} \in I \) if and only if \( I^{-1} \subseteq dO_F \). This is equivalent to \( d | gcd(k_{ij}) \) for all \( i, j \). In conclusion, 1 is primitive in \( I \) if and only if \( I^{-1} \subseteq dO_F \). This is equivalent to \( d | k_{ij} \) for all \( i, j \). In other words, testing the primitiveness of 1 is in polynomial time in \( \log |\Delta_F| \).

By Lemma (2.3), we know how to test the first condition of Definition (2.4). From now on, we only consider the second condition of this definition.

**Remark 2.2.** Note that if \( u \in \prod_{\sigma} \mathbb{R}_{>0} \) satisfies the second condition of Definition (2.4) then \( u' = \left( \frac{u_{\sigma} |u_{\sigma}|}{N(u)^{r_2/n}} \right)_{\sigma} \in \prod_{\sigma} \mathbb{R}_{>0} \) still satisfies the second condition of Definition (2.4) and \( N(u') = 1 \). Therefore, we can always assume that \( u \) has the property that \( N(u) = 1 \) from now on.

**Proposition 2.1.** Let \( I \) be a fractional ideal and \( u \) be a vector satisfying the second condition of Definition (2.4) with \( \prod_{\sigma} u_{\sigma} = 1 \). Then
\[
\|u\| \leq C \sqrt{n} (2/\pi)^{r_2/n} \text{covol}(I)^{1/n}.
\]

**Proof.** Let \( L = uI \). Since \( N(u) = 1 \), \( L \) is a lattice of covolume equal to \( \text{covol}(I) \). Consider the symmetric, convex and bounded subset \( S \) of \( F_\mathbb{R} \)
\[
S = \{ (x_\sigma) : |x_\sigma| < (2/\pi)^{r_2/n} \text{covol}(I)^{1/n} \text{ for all } \sigma \}.
\]

We have \( \text{vol}(S) = 2^\pi (2/\pi)^{r_2} (2/\pi)^{r_2} \text{covol}(I) = 2^n \text{covol}(I) \). By Minkowski's theorem, there is a nonzero element \( f \in I \) such that
\[
u_\sigma |\sigma(f)| \leq (2/\pi)^{r_2/n} \text{covol}(I)^{1/n} \text{ for all } \sigma.
\]

So
\[
\|uf\| \leq \sqrt{n} (2/\pi)^{r_2/n} \text{covol}(I)^{1/n}.
\]
Because \( u \) satisfies the second condition of Definition (2.4), we have \( \|u\| \leq C\|uf\| \). So, the proposition is proved.

3. **C-reduced Arakelov divisors in real quadratic fields**

In this part, fix \( C \geq 1 \) and fix a real quadratic field \( F \) with the discriminant \( \Delta_F \), we describe what \( C \)-reduced ideals look like and their properties. The most important results are given in Proposition (3.3), Proposition (3.8) and Proposition (3.9).

3.1. **A geometrical view of reduced reduced ideals in real quadratic cases.** We have \( F_\mathbb{R} \cong \mathbb{R}^2 \). Let \( I \) be a fractional ideal of \( F \) and \( S_1 \) be the square centered at the origin of \( F_\mathbb{R} \) which has a vertex \((1/C, 1/C)\). We have the below result.

**Proposition 3.1.** The second condition in Definition (2.4) can be restated as follows. There exists an ellipse \( E_4 \) which has its center at the origin, passes through the vertices of \( S_1 \) and of which interior does not contain any nonzero points of the lattice \( I \).
Proof. It is easy to see by writing down the condition \( \|u\| \leq C \|uf\| \) in term of coordinates of \( u \) and \( f \).

\[ \square \]

**Proposition 3.2.** If \( I \) has some nonzero element in the square \( S_1 \) then the ellipse \( E_4 \) described in Proposition (3.1) does not exist. On the other hand, such \( E_4 \) exists when the shortest vector of \( I \) has length at least \( \sqrt{2}/C \).

\[ \text{Figure 1. The shortest vector of } I \text{ is inside square } S_1 \]

\[ \text{Figure 2. The shortest vector of } I \text{ is outside circle } E_1. \]

Proof. For the first case, we assume that there is a nonzero element \( g \) of \( I \) in the square \( S_1 \). Since the square \( S_1 \) is inside \( E_4 \), the element \( g \) is so (see Figure (1)). In the second case, we can take for \( E_4 \) the circle \( E_1 \) centered at the origin and radius \( \sqrt{2}/C \). Because the shortest vector of \( I \) is out side \( E_1 \), all of nonzero elements of \( I \) are out of \( E_4 \). (see Figure (2)) \( \square \)

**Remark 3.1.** By Proposition (3.2), if the shortest vector \( f \) of \( I \) is inside the circle \( E_1 \) and \( I \) does not have any nonzero element in the square \( S_1 \) (see Figure (3)), it is not clear whether the ellipse \( E_4 \) exists or not.

3.2. Some properties of \( C \)-reduced ideals in real quadratic fields. We identity each element \( g \in I \) with its image in \( F_\mathbb{R} \) as the vector \( (g_1, g_2) \). In this section, by Remark (3.1), we always assume that \( I \) satisfies the contions \((*)\) as follows.

\[ (*) \begin{align*}
1) & \ 1 \text{ is primitive in } I. \\
2) & \ I \text{ does not have any nonzero element in the square } \{ (x_1, x_2) \in \mathbb{R}^2 : |x_1| \leq \frac{1}{C} \text{ and } |x_2| \leq \frac{1}{C} \text{ and } x_1^2 + x_2^2 < \frac{2}{C^2} \}.
3) & \text{ The shortest vector } f \text{ of } I \text{ has length } \frac{1}{C} < \|f\| < \frac{\sqrt{2}}{C}. \end{align*} \]

Moreover, by Remark (2.2), we can assume that the vector \( u \) in Definition (2.4) has the form \( u = (\alpha^{-1}, \alpha) \in (\mathbb{R}_{>0})^2 \subset F_\mathbb{R} \) for some \( \alpha \in \mathbb{R}_{>0} \).
Figure 3. The shortest vector of $I$ is inside $E_1$ and $I$ does not have any nonzero element in $S_1$.

Let $\{b_1, b_2\}$ be an LLL-basis of $I$ then $\|b_1\| = \|f\| < \frac{\sqrt{C}}{C}$. We denote by $\{b'_1, b'_2\}$ the Gram-Schmidt orthogonalization of the basis $\{b_1, b_2\}$.

Let $G = \{g \in I : (g_1^2 - \frac{1}{C^2})(g_2^2 - \frac{1}{C^2}) < 0 \text{ and } \|g\| < \frac{4}{\pi}C\text{covol}(I)\}$. We also put $G_1 = \{g \in G : g_1^2 - \frac{1}{C^2} < 0\}$ and $G_2 = \{g \in G : g_2^2 - \frac{1}{C^2} < 0\}$. So, we get $G = G_1 \cup G_2$.

For each $g \in G$, we define $B(g) := \left(\frac{-C^2g_1^2 - 1}{C^2g_2^2 - 1}\right)^{1/4}$. Then denote by

$$B_{\text{min}} = \begin{cases} \frac{1}{2\sqrt{C}} & \text{if } G_1 = \emptyset \\ \max \{B(g) : g \in G_1\} & \text{if } G_1 \neq \emptyset \end{cases}$$

and

$$B_{\text{max}} = \begin{cases} 2\sqrt{C} & \text{if } G_2 = \emptyset \\ \min \{B(g) : g \in G_2\} & \text{if } G_2 \neq \emptyset \end{cases}$$

Let $G' = \{g \in G : B(g) = B_{\text{max}} \text{ or } B(g) = B_{\text{min}}\}$. Then because of assumption $(\ast)$, vector $b_1$ is in $G$. So, $G'$ is nonempty.

We have the most important proposition as follows.

**Proposition 3.3.** The ideal $I$ is $C$-reduced if and only if $B_{\text{min}} \leq B_{\text{max}}$.

We prove this proposition after proving some results below. First, we show one of the properties of the ellipses $E_1$ described in Section (3.1).

**Proposition 3.4.** Assume that $E_4 : \frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} = 1$ with $a_1 > 0$ and $a_2 > 0$ is an ellipse satisfying Proposition (3.1). In other words, $E_4$ has its center at the origin, passes through the vertices of $S_1$, and the interior does not contain any nonzero points of the lattice $I$. Then we have the following.

i) The coefficients $a_1$ and $a_2$ are bounded by $\frac{4}{\pi}C\text{covol}(I)$. 
ii) \( E_4 \) is inside the circle \( E_5 \) centered at the origin of radius \( \frac{4}{\pi} \text{covol}(I) \).

**Proof.** Since \( E_4 \) passes through the vertex \((1/C, 1/C)\) of \( S_1 \), its coefficients satisfy \( a_1 > \frac{1}{C} \) and \( a_2 > \frac{1}{C} \). We also know that \( \text{vol}(E_4) = \pi a_1 a_2 \). So then
\[
a_1 = \frac{\text{vol}(E_4)}{\pi a_2} < \frac{1}{\pi} \text{covol}(E_4).
\]
In addition, by Minkowski’s theorem, the ellipse \( E_4 \), which is a symmetric, convex and bounded set and its interior does not contain any nonzero points of the lattice \( I \) must have volume less than \( 2^4 \text{covol}(I) \). Therefore
\[
a_1 < \frac{4}{\pi} \text{covol}(I).
\]
By symmetry, we also have this bound for \( a_2 \). Therefore, the first statement of the proposition is obtained. The second one follows from the first. □

We have another equivalent condition to Definition (2.4) as follows.

**Proposition 3.5.** The second condition in Definition (2.4) is equivalent to the following. There exists a metric \( u \in (\mathbb{R}_>0)^2 \) such that for all \( g \in G \), we have \( \|1\|_u \leq C\|g\|_u \).

**Proof.** Let \( g = (g_1, g_2) \) be an arbitrary nonzero element of \( I \). If \( \|g\| \geq \frac{2}{\pi} \text{covol}(I) \) then \( g \) is outside the circle \( E_5 \). By Proposition (3.4), \( g \) is also outside ellipses \( E_4 \) (see Figure (4)). Using this and the equivalent condition of Proposition (3.1), we obtain the following: a vector \( u \) satisfies Definition (2.4) if and only if for all \( g \) of \( I \setminus \{0\} \) and \( \|g\| < \frac{4}{\pi} \text{covol}(I) \), we have \( \|u\| \leq C\|ug\| \).

On the other hand, if \( |g_1| \geq 1/C \) and \( |g_2| \geq 1/C \), then \( g \) satisfies \( \|u\| \leq C\|ug\| \) for any \( u \in (\mathbb{R}_>0)^2 \). Therefore, it is sufficient to consider the elements \( g \) such that \( |g_1| < \frac{1}{C} \) or \( |g_2| < \frac{1}{C} \) to show the existence of \( u \).
Moreover, $I$ does not have any nonzero elements in $S_1$, so $g \notin \{(x_1, x_2) \in \mathbb{R}^2 : |x_1| \leq \frac{1}{2}, |x_2| \leq \frac{1}{2}, x_1^2 + x_2^2 < \frac{3}{2}\}$.

Combining these conditions, we obtain the statement of the proposition.  

The ideal $I$ with the properties $(\star)$ mentioned at the beginning of this section has bounded covolume. Explicitly, we have the following.

**Proposition 3.6.** The covolume of $I$ is bounded by $\frac{2}{C}$.

**Proof.** Since 1 is in $I$, there exist some integers $m_1$ and $m_2$ such that $1 = m_1b_1 + m_2b_2$. If $m_2 = 0$ then $1 = m_1b_1$ so $\frac{1}{m_1} = b_1 \in I$. Because 1 is primitive in $I$, we must have $m_1 = \pm 1$. So, $\|b_1\| = \|1\| = \sqrt{2} \geq \frac{\sqrt{2}}{C}$ for any $C \geq 1$. This contradicts the fact that the length of the shortest vector of $I$ is strictly less than $\frac{\sqrt{2}}{2}$. So $m_2 \neq 0$.

We have $\|b_1^*\| \leq \frac{1}{|m_2|}\|b_1\| \leq \sqrt{2}$. Thus, $covol(I) = \|b_1\|\|b_1^*\| < \sqrt{2^2 \times \sqrt{2} = \frac{2}{C}}$.  

By this proposition and Proposition (3.4), we obtain the corollary below.

**Corollary 3.1.** The coefficients $a_1$ and $a_2$ and the radius of the circle $E_5$ in Proposition (3.4) are bounded by $\frac{8}{\pi}$. In addition, the set $G$ is contained in the finite set $\{g \in I : (g_1^2 - \frac{1}{4})(g_2^2 - \frac{1}{4}) < 0 \text{ and } \|g\| < \frac{8}{\pi}\}$.

For a real quadratic field, the Proposition (2.1) can be restated as below.

**Proposition 3.7.** Assume that $u = (\alpha^{-1}, \alpha) \in (\mathbb{R}_{>0})^2$ satisfies the second condition of Definition (2.4). Then $\|u\| \leq 2\sqrt{C}$ and so $\frac{1}{2\sqrt{C}} \leq \alpha < 2\sqrt{C}$.

**Proof.** By Proposition (2.1), vector $u$ has the bounded length $\|u\| \leq C\sqrt{2}covol(I)^{1/2}$. By Proposition (3.6), we have $covol(I) < \frac{2}{C}$, so $\|u\| \leq 2\sqrt{C}$. Since $\alpha^{-1} < \|u\|$ and $\alpha < \|u\|$, the conclusion follows.  

Now, we prove Proposition (3.3).

**Proof.** Let $u = (\alpha^{-1}, \alpha) \in (\mathbb{R}_{>0})^2$. Then from $\|1\|_a \leq C\|g\|_u$, we get $\alpha^4(C^2g_2^2 - 1) \geq -(C^2g_1^2 - 1)$. Then $\alpha \geq B(g)$ if $g \in G_1$ and $\alpha \leq B(g)$ if $g \in G_2$. Because of the assumption that 1 is primitive in $I$, by Proposition (3.5), the ideal $I$ is $C$-reduced if and only if it satisfies the below condition:

There exists $u \in (\mathbb{R}_{>0})^2$ such that for all $g \in G$, we have $\|1\|_u \leq C\|g\|_u$.

$$\iff \text{ There exist } \alpha \in \mathbb{R}_{>0} \text{ such that } \begin{cases} g \in G_1 \text{ we have } \alpha \geq B(g) \\ g \in G_2 \text{ we have } \alpha \leq B(g). \end{cases}$$

$$\iff \text{ There exists } \alpha \in \mathbb{R}_{>0} \text{ such that } \begin{cases} \alpha \geq B_{\min} \\ \alpha \leq B_{\max}. \end{cases} \iff B_{\max} \geq B_{\min}.$$  

The second equivalence is because of Proposition (3.7) and the definition of $B_{\min}$ and $B_{\max}$. So, the proof is complete.
By Proposition (3.5) and Proposition (3.3), it is useful to know about the set \( G \) and \( G' \). We first show a special property of the elements in \( G \).

**Proposition 3.8.** If \( g = s_1b_1 + s_2b_2 \in G \) then \( |s_2| \leq 1 \).

**Proof.** Let \( g = s_1b_1 + s_2b_2 \in G \). As in the proof of Proposition (3.6), we get \( \|b_1\| < \frac{\sqrt{2}}{\pi} \) and \( \|b_2^*\| \leq \sqrt{2} \). By the property of LLL-reduced basis, \( \|b_2\| \leq \sqrt{2}\|b_2^*\| \leq 2 \). Therefore, 

\[
\frac{4C\text{covol}(I)}{\pi} = \frac{4C\|b_1\|\|b_2^*\|}{\pi} < \frac{4\sqrt{2}\|b_2^*\|}{\pi}.
\]

Now let \( g^* \) be the vector of which length is the distance from \( g \) to the 1-dimensional vector space \( \mathbb{R}b_1 \), i.e., we have \( \|g^*\| = d(g, \mathbb{R}b_1) = \|s_2\|\|b_2^*\| \). So if \( |s_2| \geq 2 \) then 

\[
\|g\| \geq d(g, \mathbb{R}b_1) = \|g^*\| \geq 2\|b_2^*\| > \frac{4\sqrt{2}\|b_2^*\|}{\pi} > \frac{4}{\pi}C\text{covol}(I).
\]

Therefore, \( |s_2| \leq 1 \). \( \square \)

In next proposition, we prove that the cardinality of \( G \) is bounded by a number that depends only on \( C \) but not \( I \) and the number field \( F \).

**Lemma 3.1.** The number of the vectors (up to sign) in \( G \) is less than \( 17C + 3 \).

**Proof.** Let \( g \in G \). Then \( g = s_1b_1 + s_2b_2 \) for some integers \( s_1, s_2 \). We have \( \|b_1\| \geq \frac{1}{C} \) and \( \|g\| < \frac{3}{2} \) (by Corollary (3.1)). This implies that 

\[
|s_1| \leq \sqrt{2} \left( \frac{3}{2} \right) \frac{\|g\|}{\|b_1\|} < \frac{12\sqrt{2}C}{\pi}
\]

(see cf. [7] Section 12). By Proposition (3.8), we get \( |s_2| \leq 1 \).

Therefore, the number the elements (up to sign) in \( G \) is at most \( 3 \times (\frac{12\sqrt{2}C}{\pi} + 1) \) that is less than \( 17C + 3 \). \( \square \)

The proposition below gives a property of the elements in \( G' \).

**Proposition 3.9.** Let \( g = s_1b_1 + b_2 \in G' \). Then:

- \( |s_1| \leq 2 \) or 
- \( s_1 \in \{t_1, t_2\} \) for some integers \( t_1 \leq t_2 \) in the interval \((-1 - 2C, 1 + 2C)\).

**Proof.** It is easy to show that \( b_1 \) belongs to \( G = G_1 \cup G_2 \) since \( \|b_1\| \leq \frac{1}{\pi}C\text{covol}(I) \).

Here, we only prove the proposition in the case in which \( b_1 \in G_1 \), so \( 0 < b_{11} < \frac{1}{C} \) and \( \frac{1}{C} < |b_{12}| < \frac{\sqrt{2}}{C} \). For the case \( b_1 \in G_2 \) , it is sufficient to switch \( b_{11} \) and \( b_{12} \). In the first case, by definition of \( B_{\min} \), we get \( B(b_1) \leq B_{\min} \). The element \( g \) is in \( G' \) and so it belongs to \( G_1 \) or \( G_2 \).

If \( g \) is in \( G_1 \) then we have \( 0 < |g_1| < \frac{1}{C} \) and \( |g_2| > \frac{1}{C} \). Since \( g \in G' \) and \( B(b_1) \leq B_{\min} \), we also have \( B(b_1) \leq B(g) \). If \( |g_1| > \frac{\sqrt{2}}{C} \) then \( B(b_1) > B(g) \) contradicting the previous
\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure5.png}
\caption{\textit{b}_1 is in the red shaded area and \textit{g} is in the black shaded area.}
\end{figure}

inequality. So, we have $\|g\| \leq \sqrt{2}/C$. With this in mind and the properties of LLL-reduced bases (cf.\[7\] Section 12), we get the following.

\begin{equation}
|s_1| \leq \sqrt{2} \left( \frac{3}{2} \right) \left( \frac{\sqrt{2}}{C} \right) = \frac{3}{2}C 
\end{equation}

If \textit{g} is in \textit{G}_2 then $|g_1| > \frac{1}{C}$ and $|g_2| < \frac{1}{C}$. Since $g = s_1b_1 + b_2$ and $|g_2| < \frac{1}{C}$, the value of $s_1$ is between $-\frac{1/C - b_{22}}{b_{12}}$ and $\frac{1/C - b_{22}}{b_{12}}$. The fact that $0 < |b_{12}| < \frac{\sqrt{2}}{C}$ implies that the distance between these numbers

\begin{equation}
\left| \frac{-1/C - b_{22}}{b_{12}} - \frac{1/C - b_{22}}{b_{12}} \right| = \frac{2}{C|b_{12}|}
\end{equation}

is in the interval $(\sqrt{2}, 2)$. So, there exit two integers $t_1 \leq t_2$ between these numbers. Moreover, since $\frac{1}{C} < |b_{12}| < \frac{\sqrt{2}}{C}$ and since $|b_{22}| < \|b_2\| \leq 2$ (see the proof of Proposition (3.8)), one can easily see that

\begin{equation}
\left| \frac{\pm 1/C - b_{22}}{b_{12}} \right| < 1 + 2C.
\end{equation}

Thus, we get the the bounds for $s_1$ in this case. This also completes the proof. \qed
4. Test Algorithm for real quadratic fields

In this part, given $C \geq 1$, we explain an algorithm to test whether a given fractional ideal $I$ is $C$-reduced for a real quadratic field $F$ in time polynomial in $\log |\Delta_F|$ with $\Delta_F$ the discriminant of $F$.

By Proposition (3.3), if we know $B_{\min}$ and $B_{\max}$ then we can show the existence of a metric $u = (\alpha^{-1}, \alpha)$ in Definition (2.4). In this algorithm, we first find all the possible elements of $G' = \{ g \in G : B(g) = B_{max} \text{ or } B(g) = B_{min} \}$ then compute $B_{min}$ and $B_{max}$. Let $\{b_1, b_2\}$ be an LLL-basis of $I$ and $g = s_1 b_1 + s_2 b_2 \in G'$. Then Proposition (3.8) says that $s_2 = 0$ or $s_2 = \pm 1$. By symmetry, it is sufficient to consider only the case $s_2 \in \{0, 1\}$.

- If $s_2 = 0$ then $g = b_1$.
- If $s_2 = 1$ then $g = s_1 b_1 + b_2$. By Proposition (3.9), there are five possible values for $s_1$ in the interval $[-2, 2]$ and 2 possible values $t_1, t_2$ (with $t_1 \leq t_2$) of $s_1$ either between $-1/C - b_{22}$ and $1/C - b_{22}$ or between $-1/C - b_{22}$ and $1/C - b_{22}$. This proposition also shows that the coefficients $s_1$ have absolute values less than $1 + 2C$.

Furthermore, by Proposition (3.7), we have $\frac{1}{2C^2} < \alpha < 2\sqrt{C}$ and so $\frac{1}{16C^2} < B(g)^4 < 16C^2$ for all $g \in G$. In other words, we have the following.

\[
\begin{cases}
\text{If } |g_2| < 1/C & \text{then } |g_1|^2 + 16C^2|g_2|^2 < 16 + \frac{1}{C^2} \text{ and } |g_2|^2 + 16C^2|g_1|^2 > 16 + \frac{1}{C^2}.
\end{cases}
\]

Using (**) we can eliminate some elements $g$ which are not in $G'$ without having to compute $B(g)$.

Let $C \geq 1$ and let $I$ be a fractional ideal of a real quadratic field $F$. Assume that an LLL-reduced basis $\{b_1, b_2\}$ of $I$ also given and change the sign if necessary to have the first component of $b_1 = (b_{11}, b_{12}) \in F_\mathbb{R}$ is positive. In Remark (2.1), we assume that the coordinates of $b_1$ and $b_2$ have at most $O(\log |\Delta_F|^a)$ digits for some integer $a > 0$.

The step 3 of the algorithm below is done in a similar way as testing the minimality of 1 was done (cf.[10, Algorithm 10.3]) but here 1 is replaced by $\frac{1}{C}$. In fact, we have the lemma below.

**Lemma 4.1.** Testing if there is no nonzero element of $I$ in the square $S_1$ in the step 4) of the algorithm can be done by checking at most six short vectors of the lattice $I$.

**Proof.** If $b_1$ is in $S_1$ then $I$ is not $C$-reduced. Otherwise, we get $\|b_1\| > \frac{1}{C}$. Assume that $g = s_1 b_1 + s_2 b_2$ is in $S_1$. Then $g$ has length $\|g\| < \sqrt{\frac{2}{C}}$.

Since $\{b_1, b_2\}$ is an LLL-reduced basis of $I$, the coefficients $s_1$ and $s_2$ are bounded as

\[|s_1| \leq \sqrt{2} \left(\frac{3}{2} \right) \frac{\|g\|}{\|b_1\|} < \sqrt{2} \left(\frac{3}{2} \right) \left(\frac{\sqrt{\frac{2}{C}}}{\frac{1}{C}} \right) = 3\]

and

\[|s_2| \leq \sqrt{2} \frac{\|g\|}{\|b_1\|} < \sqrt{2} \left(\frac{\frac{\sqrt{2}}{C}}{\frac{1}{C}} \right) = 2\]
Therefore, the elements of $I$ which are in $S_1$ have the form $g = s_1b_1 + s_2b_2$ with $|s_1| \leq 2$ and $|s_2| \leq 1$. By symmetry, it is sufficient to test at most six short elements of $I$.

We have the following algorithm to test whether $I$ is $C$-reduced in time polynomial in $\log |\Delta_F|$.

**Algorithm**

1. Check if $1 \in I$ and $N(I)^{-1} < C^2/\sqrt{|\Delta_F|}$ or not.
2. Test whether or not $1 \in I$ is primitive.
3. Check whether there is no nonzero element of $I$ in the square
   $S_1 = \{(x_1, x_2) \in \mathbb{R}^2 : |x_1| \leq \frac{1}{C} \text{ and } |x_2| \leq \frac{1}{\sqrt{C}} \text{ and } x_1^2 + x_2^2 < \frac{2}{C^2}\}$.
4. If $\|b_1\| \geq \frac{\sqrt{2}}{C}$ then $I$ is $C$-reduced.
   If not, then find all possible elements of $G'$.
   - If $0 < b_{11} < \frac{1}{C}$ and $\frac{1}{\sqrt{C}} < |b_{12}| < \frac{\sqrt{2}}{C}$ then compute the integers $t_1 \leq t_2$
     which are between $\frac{-1/C-b_{22}}{b_{12}}$ and $\frac{1/C-b_{22}}{b_{12}}$.
   - If $\frac{1}{\sqrt{C}} < b_{11} < \frac{\sqrt{2}}{C}$ and $0 < |b_{12}| < \frac{1}{\sqrt{C}}$ then compute the integers $t_1 \leq t_2$
     which are between $\frac{-1/C-b_{22}}{b_{12}}$ and $\frac{1/C-b_{22}}{b_{12}}$.
   Let $G_3 = \{b_1, t_1b_1 + b_2, t_2b_1 + b_2, s_1b_1 + b_2 \text{ with } |s_1| \leq 2\}$.
5. Eliminate the elements which do not satisfy the condition (\(\star\)) from $G_3$.
6. Compute $B(g)$ for all $g \in G_3$ then $B_{\text{max}}$ and $B_{\text{min}}$.
   If $B_{\text{min}} \leq B_{\text{max}}$ then $I$ is $C$-reduced. If not, then $I$ is not $C$-reduced.

The first step can be done in polynomial time in $\log |\Delta_F|$ by Lemma (2.2). An LLL-reduced basis of $I$ can be computed in time polynomial in $\log |\Delta_F|$ and Step 2 can be done in time polynomial in $\log |\Delta_F|$ (see Lemma (2.3) in Section 2). In Step 3, we only check a few short vectors of $I$ which has length bounded by $\sqrt{2}$. Step 4 can be done by finding 2 integer numbers $t_1, t_2$ which are in the interval $[-1 - 2C, 1 + 2C]$. In Step 6, the bounds $B(g)$ are between $\frac{1}{2\sqrt{C}}$ and $2\sqrt{C}$. Overall, this algorithm runs in time polynomial in $\log |\Delta_F|$.

5. A COUNTEREXAMPLE

For a real quadratic field, the algorithm to test whether a given ideal $I$ is $C$-reduced in Section 4 only requires us to check the elements of $I$ in a certain subset $G$ (see Proposition (3.5)). Since we can bound the covolume of $I$ by $\frac{2}{C}$, the elements of $G$ have length bounded by $\frac{1}{2}C\text{covol}(I)$ which is less than $\frac{2}{\pi}$. So, $G$ has only a few elements and the test algorithm works well.

However, for a number field of degree at least 3, that does not hold. In other words, in this case, the set $G$ may have many elements. In this section, we provide an example of a real cubic field $F$ with large discriminant $\Delta_F$ and shows that $G$ has at least $|\Delta_F|^{1/4}$
We briefly denote by $\delta(I, C) = \frac{6}{2} C^2 \text{covol}(I)$ and let
\[
S_1 = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : |x_i| \leq \frac{1}{C}, 1 \leq i \leq 3 \text{ and } x_1^2 + x_2^2 + x_3^2 < \frac{3}{C^2}\},
\]
\[
G = \{g = (g_1, g_2, g_3) \in I : \|g\| < \delta(I, C) \text{ and there exists } i \text{ such that } |g_i| < \frac{1}{C}\}.
\]

Let $E_1$ be the sphere centered at the origin of radius $\frac{\sqrt{3}}{C}$. As condition $(\ast)$ for quadratic case (see Remark (3.1)), we assume that 1 is primitive in $I$ and $I$ does not have any element in $S_1$ but the shortest vector of $I$ is inside $E_1$.

Proposition (3.1) and Proposition (3.4) for quadratic case can be naturally generalized to a real cubic field. Similar to Proposition (3.5), we have the following result.

**Lemma 5.1.** The second condition in Definition (2.4) is equivalent to the following statement. There exists $u \in (\mathbb{R}_{>0})^3$ such that for all $g \in G$, we have $\|1\|_u \leq C\|g\|_u$.

Let $\{b_1, b_2, b_3\}$ be an LLL-basis of $I$. We show an example with $C = 1$.

5.1. **An example.** Let $P = 1000000019X^3 + 1021840019X^2 - 8813199073X - 4923977196$ be an irreducible polynomial with a root $\beta$ and $F = \mathbb{Q}(\beta)$. Then $F$ is a real cubic field with the discriminant $\Delta_F = 7086249922322398531211367826392679055149 > 7 \times 10^{40}$. Denote by $O_F$ the ring of integers of $F$. Let $I = O_F + O_F\beta$. Then the fractional ideal $I$ has the properties that:

- $1$ is primitive in $I$.
- $I$ does not have any nonzero element in the cuboid $S_1$.
- $b_1$ is inside $E_1$ so the shortest vector of $I$.
- The covolumn of $I$ is greater than $1.6 \times |\Delta_F|^{1/4}$.

The cardinality of $G$ is at least $1.7 \times 10^{40} > |\Delta_F|^{1/4}$.

5.2. **Idea to find the above example.** We construct a real cubic field $F$ with a fractional ideal $I$ satisfying the conditions in Example (5.1).

Let $C \geq 1$. Assume that $F = \mathbb{Q}(\beta)$ for some $\beta$ of length $\|\beta\| < \frac{\sqrt{3}}{C}$ and outside the cuboid $S_1$. Let $O_F$ be the ring of integers of $F$. Suppose that $I = O_F + O_F\beta$. Then the shortest vector of $I$ has length at most $\|\beta\| < \frac{\sqrt{3}}{C}$.

Denote by $P = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$ with $\gcd(a, b, c, d) = 1$ and $a > 0$ an irreducible polynomial that has a root $\beta$. Let $R = \mathbb{Z} \oplus \mathbb{Z}(a\beta) \oplus \mathbb{Z}(a\beta^2 + b\beta)$. Then $R$ is a multiplier ring and so it is an order of $F$ (cf.[4, Section 12.6]).

Denote by $\beta_1 = \beta, \beta_2$ and $\beta_3$ the roots of $P$. We simply choose $P$ such that $O_F = R$. This can be obtained by using the lemma below.

**Lemma 5.2.** If the discriminant of $P$ is squarefree then $O_F = R$. 
The discriminant of \( P \) is \( \text{disc}(P) = a^4 \prod_{1 < j} (\beta_i - \beta_j)^2 \) (see cf. [3, Proposition 3.3.5]).

By computing the discriminant of \( R \), we can easily see that it is equal to \( \text{disc}(P) \). Since \([O_F : R][\text{disc}(P)]\), it is obvious to imply the lemma.

We now prove the lemma below.

**Lemma 5.3.** If \( O_F = R \) then we have \( N(I^{-1}) = a \).

**Proof.** Since \( O_F = R = \mathbb{Z} \oplus \mathbb{Z}(a \beta) \oplus \mathbb{Z}(a \beta^2 + b \beta) \) and \( I = O_F + O_F \beta \), it is easy to see that \( I = \mathbb{Z} \oplus \mathbb{Z} \beta \oplus \mathbb{Z}(a \beta^2) \). Therefore, \( N(I^{-1}) = [I : O_F] = a \) and the lemma is proved. \( \Box \)

The lemma below says that \( a \) can be chosen such that 1 is primitive in \( I \).

**Lemma 5.4.** If \( a \) is a prime number then 1 is primitive in \( I \).

**Proof.** If there is some integer \( d \) at least 2 such that \( \frac{1}{d} \in I \), then \( N(d)|N(I^{-1}) = a \) this is impossible since \( a \) is a prime number. Thus, 1 is primitive in \( I \). \( \Box \)

Let \( \{b_1 = (b_{11}, b_{12}, b_{13}), b_2 = (b_{21}, b_{22}, b_{23}), b_3 = (b_{31}, b_{32}, b_{33})\} \subset \mathbb{R}^3 \subset F_I \) and \( \{b'_1, b'_2, b'_3\} \) the Gram-Schmidt orthogonalization of this basis. We have the following result that is the most important to obtain Example [5.1].

**Proposition 5.1.** Let \( C \geq 1 \). Assume that we have the following.

- 1 is primitive in \( I \).
- \( I \) does not have any nonzero elements in the cuboid \( S_1 \).
- \( b_1 \) has length strictly less than \( \sqrt[3]{C} \).
- The covolume of \( I \) is at least 10.

Then the cardinality of \( G \) is at least \( \frac{2}{3}C^2 \text{covol}(I) \).

**Proof.** Because of the assumption that \( I \) does not have any nonzero element in the cuboid \( S_1 \), there is some coordinate \( b_{ij} \) with \( 1 \leq j \leq 3 \) of \( b_1 \) such that \( |b_{ij}| \geq \frac{1}{C} \).

Let \( g = s_1 b_1 + s_2 b_2 = (g_1, g_2, g_3) \). We show that if \( |s_2| \leq \frac{1}{C^2} \text{covol}(I) \) and if \( s_1 \) is between two numbers \( \frac{b_1}{b_1}(1/C - s_2 b_{2j}) \) and \( \frac{b_1}{b_1}(-1/C - s_2 b_{2j}) \) then \( g \) is in \( G \).

We know that \( \|b_1\| < \frac{\sqrt{3}}{C} \), so then \( |b_{1j}| < \frac{1}{\sqrt{3}} \). This means that for each \( s_2 \), the distance between two numbers \( \frac{b_1}{b_1}(1/C - s_2 b_{2j}) \) and \( \frac{b_1}{b_1}(-1/C - s_2 b_{2j}) \) is greater than \( \frac{2}{\sqrt{3}} \) and so greater than 1. Therefore there is at least one integer \( s_1 \) between them.

The bound for \( s_1 \) implies that \( |g_j| < \frac{1}{C} \). To prove that \( g \in G \), it is sufficient to prove that \( \|g\| < \delta(I, C) \).

We first show that the length of \( b_2 \) is at most \( \sqrt{3} \). By the assumption, 1 is in \( I \), there exist some integers \( m_1, m_2 \) and \( m_3 \) such that \( 1 = m_1 b_1 + m_2 b_2 + m_3 b_3 \). If \( m_3 = m_2 = 0 \) then \( 1 = m_1 b_1 \) so \( \frac{1}{m_1} = b_1 \in I \). Because of the primitiveness of 1, we must have \( m_1 = \pm 1 \). So, \( \|b_1\| = \|1\| = \sqrt{3} \geq \frac{\sqrt{3}}{C} \) for any \( C \geq 1 \). This contradicts the fact \( \|b_1\| < \frac{\sqrt{3}}{C} \). So \( m_3 \neq 0 \) or \( m_2 \neq 0 \). If \( m_2 \neq 0 \), then \( \|b_2\| \leq \frac{1}{m_2} \|1\| \leq \sqrt{3} \). By the properties of LLL-reduced bases (cf. [14, Section 12]), \( \|b_2\| \leq \sqrt{2}\|b_3\| \leq \sqrt{6} \). So then \( \text{covol}(I) = \|b_1\|\|b_2\|\|b_3\| < \frac{\sqrt{3}}{C} \times \sqrt{6} \times \sqrt{3} = \frac{3\sqrt{6}}{C} \). This contradicts to the assumption...
that the covolume of $I$ is at least 10. Hence, we must have $m_3 = 0$ and $m_2 \neq 0$. So $\|b_2^*\| \leq \frac{1}{\|m_2\|} |1| \leq \sqrt{3}$.

Next, we prove that $\|b_2\| \leq \frac{\sqrt{15}}{2}$. Indeed, denoting $\mu = \frac{b_2 b_1}{b_1 b_1}$, by the properties of LLL-reduced bases, we have $|\mu| \leq \frac{1}{2}$ and $b_2 = b_2^* + \mu b_1$ (cf. [7, Section 12]). It follows that $\|b_2\|^2 = \|b_2^*\|^2 + \mu^2 \|b_1\|^2 < 3 + \frac{3}{4} \frac{\sqrt{3}}{C^2} \leq \frac{15}{4}$.

Now, since $|b_{ij}| \geq \frac{1}{\sqrt{3}}$ and $|b_{2j}| \leq \|b_2\| \leq \frac{\sqrt{15}}{2}$, two numbers $\frac{1}{b_{ij}} (1/C - s_2 b_{2j})$ and $\frac{1}{b_{ij}} (-1/C - s_2 b_{2j})$ are in the interval $[-(1 + \frac{\sqrt{15}}{2}) |s_2| C, (1 + \frac{\sqrt{15}}{2}) |s_2| C]$ and so $s_1$. Therefore, we have the following.

$$\|g\| = \|s_1 b_1 + s_2 b_2\| \leq |s_1| \|b_1\| + |s_2| \|b_2\| \leq \left(1 + \frac{\sqrt{15}}{2} |s_2| \right) C \times \frac{\sqrt{3}}{C} + |s_2| \times \frac{\sqrt{15}}{2}$$

$$= \frac{\sqrt{15}}{2} (\sqrt{3} + 1) |s_2| + \sqrt{3} < \delta(I, C)$$ since $|s_2| \leq \frac{1}{2} C^2 \text{covol}(I)$ and $\text{covol}(I) > 10$.

We have showed that $g = s_1 B_1 + s_2 b_2 \in G$ for all $(s_1, s_2) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ where $|s_2| \leq \frac{1}{4} C^2 \text{covol}(I)$ and $s_1$ is between two numbers $\frac{1}{b_{ij}} (1/C - s_2 b_{2j})$ and $\frac{1}{b_{ij}} (-1/C - s_2 b_{2j})$. Furthermore, if $g \in G$ then $-g \in G$. Thus, $G$ has at least $2 \times \frac{1}{4} C^2 \text{covol}(I) = \frac{2}{3} C^2 \text{covol}(I)$ elements. Hence the proposition is proved. □

**Corollary 5.1.** With the assumptions in Proposition (5.1), the set $G$ contains more than $\gamma C^2 |\Delta_F|^{1/4}$ elements for some constant $\gamma$ depending on the roots $\beta_1, \beta_2, \beta_3$ of $P$.

**Proof.** By choosing $P$ such that $O_F = R$, we have $|\Delta_F| = \text{disc}(R) = \text{disc}(P) = a^4 \prod_{i<j} (\beta_i - \beta_j)^2$. So, $a = \frac{1}{2} |\Delta_F|^{1/4}$ with $\gamma = \left(\prod_{i<j} (\beta_i - \beta_j)^2\right)^{1/4}$. So then

$$\text{colvol}(I) = \frac{\sqrt{|\Delta_F|}}{N(I^{-1})} = \frac{|\Delta_F|^{1/2}}{a} = \gamma |\Delta_F|^{1/4}.$$

Then the result follows by Proposition (5.1). □

**Remark 5.1.** Almost all the lattices $I$ constructed this way have no nonzero element in the cuboid $S_1$ as we expect. Indeed, any elements in $g = s_1 b_1 + s_2 b_2 + s_3 b_3 \in I \cap S_1$ has length at most $\frac{\sqrt{3}}{C}$. So, we can bound for the coefficients $s_1 s_2, s_3$ as following (see cf. [7, Section 12]).

$$\|s_1\| \leq 2 \left(\frac{3}{2}\right)^2 \frac{\|g\|}{\|b_1\|}, \quad \|s_2\| \leq 2 \left(\frac{3}{2}\right) \frac{\|g\|}{\|b_2^*\|}, \quad \text{and} \quad \|s_3\| \leq 2 \frac{\|g\|}{\|b_3^*\|}.$$

Therefore, $I \cap S_1$ has the cardinality bounded by

$$\frac{1}{\text{covol}(I)} \times \left(\frac{\sqrt{3}}{C}\right)^3 \times (\text{a constant})$$

(cf. [7, Section 12]). Since the covolume of $I$ is very large, this number is very small. So, usually we can get $I$ without any nonzero elements in $S_1$. 

---

**ON REDUCED ARAKELOV DIVISORS OF REAL QUADRATIC FIELDS 15**

---
From the idea above, we can produce some examples as Example (5.1) as follows.

- First choose the discriminant $|\Delta_F|$ of $F$ so that $|\Delta_F| > 10^4$ (to make sure that $\text{covol}(I) > 10$).
- Choose $a \approx |\Delta_F|^{1/4}$ a prime number (so that 1 is primitive in $I$).
- Choose a real vector $(\beta_1, \beta_2, \beta_3)$ such that $\frac{1}{\sqrt{2}} < \beta_1^2 + \beta_2^2 + \beta_3^2 < \frac{5}{\sqrt{2}}$ and it is outside the cuboid $S_1$.
- Find the polynomial $P = aX^3 + bX^2 + cX + d \in \mathbb{Z}[X]$ from $a(X - \beta_1)(X - \beta_2)(X - \beta_3)$ (in pari-gp we have the function round to do this). Then check that $P$ is irreducible.
- Check if $\text{disc}(P)$ is squarefree. If not then we change $\beta_i$ until it is. Now $O_F = R$.
- Let $I = O_F + O_F\beta$. Compute an LLL-reduced basis $\{b_1, b_2, b_3\}$ of $I$ and check if $b_1$ has length strictly less than $\frac{\sqrt{3}}{\sqrt{2}}$.
- Test whether $I$ does not have any nonzero element in the cuboid $S_1$.

Acknowledgement

I would like to thank René Schoof for proposing a new definition of $C$-reduced divisors as well as very valuable comments and Hendrik W. Lenstra for helping me to find the counterexample in Section 5. I also would like to thank Duong Hoang Dung and Chloe Martindale for useful comments.

References

[1] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In Séminaire de Théorie des Nombres, Paris 1988–1989, volume 91 of Progr. Math., pages 27–41. Birkhäuser Boston, Boston, MA, 1990.

[2] Johannes Buchmann and H. C. Williams. On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. Math. Comp., 50(182):569–579, 1988.

[3] Henri Cohen. A course in computational algebraic number theory, volume 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993.

[4] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard. The number field sieve. In The development of the number field sieve, volume 1554 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1993.

[5] H. W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In Number theory days, 1980 (Exeter, 1980), volume 56 of London Math. Soc. Lecture Note Ser., pages 123–150. Cambridge Univ. Press, Cambridge, 1982.

[6] H. W. Lenstra, Jr. Algorithms in algebraic number theory. Bull. Amer. Math. Soc. (N.S.), 26(2):211–244, 1992.

[7] Hendrik W. Lenstra, Jr. Lattices. In Algorithmic number theory: lattices, number fields, curves and cryptography, volume 44 of Math. Sci. Res. Inst. Publ., pages 127–181. Cambridge Univ. Press, Cambridge, 2008.

[8] Daniele Micciancio. Basic algorithms. http://cseweb.ucsd.edu/classes/wi10/cse206a/lec2.pdf Lecture note of the course Lattices Algorithms and Applications (Winter 2010).

[9] R. J. Schoof. Quadratic fields and factorization. In Computational methods in number theory, Part II, volume 155 of Math. Centre Tracts, pages 235–286. Math. Centrum, Amsterdam, 1982.
[10] René Schoof. Computing Arakelov class groups. In Algorithmic number theory: lattices, number fields, curves and cryptography, volume 44 of Math. Sci. Res. Inst. Publ., pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[11] Daniel Shanks. The infrastructure of a real quadratic field and its applications. In Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972), pages 217–224. Univ. Colorado, Boulder, Colo., 1972.

Department of Mathematics, University of Tor Vergata, Rome, Italy.

E-mail address: tran@axp.mat.uniroma2.it, hatran1104@gmail.com