SCIENCE CHINA
Mathematics

• ARTICLES •

July 2015 Vol. 58 No. 7: 1433–1444
doi: 10.1007/s11425-014-4898-8

8-rank of the class group and isotropy index

LU Qing[1,2]

[1]*Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190, *China;*
[2]*School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing* 100049, *China*

Email: qlu@ucas.ac.cn

Received December 5, 2013; accepted March 1, 2014; published online September 17, 2014

Abstract Suppose $F=\mathbb{Q}(\sqrt{-p_1\cdots p_t})$ is an imaginary quadratic number field with distinct primes $p_1,\ldots,p_t$, where $p_i\equiv 1 \pmod 4$ $(i=1,\ldots,t-1)$ and $p_t\equiv 3 \pmod 4$. We express the possible values of the 8-rank r_8 of the class group of F in terms of a quadratic form Q over $\mathbb{F}_2$ which is defined by quartic symbols. In particular, we show that r_8 is bounded by the isotropy index of Q.

Keywords imaginary quadratic field, class group, 8-rank, isotropy index, Rédei matrix

MSC(2010) 11R29, 11D09, 11R11, 15A63

Citation: Lu Q. 8-rank of the class group and isotropy index. Sci China Math, 2015, 58: 1433–1444, doi: 10.1007/s11425-014-4898-8

1 Introduction

Let t be a fixed positive integer. Suppose $F=\mathbb{Q}(\sqrt{-p_1\cdots p_t})$ is an imaginary quadratic number field with distinct primes $p_1,\ldots,p_t$, where $p_i\equiv 1 \pmod 4$ $(i=1,\ldots,t-1)$ and $p_t\equiv 3 \pmod 4$. We will study the 8-rank of the class group $\mathscr{C}$ of F. Recall that the 2^k-rank of $\mathscr{C}$ is defined to be

$$r_{2^k}=\dim_{\mathbb{F}_2} 2^{k-1}\mathscr{C}/2^k\mathscr{C}$$

for $k\geqslant 1$.

The study of the 2-primary part of class groups or narrow class groups of quadratic number fields can be traced back to Gauss, who proved that $r_2=t-1$. In a series of papers Rédei and Reichardt investigated r_{2^k} $(k\geqslant 2)$ and provided an algorithm for r_4 by the so-called *Rédei matrix* [9–13]. Waterhouse [17] found a method to compute r_8, which was further generalized to higher Rédei matrices by Kolster [6]. However, their algorithms required to determine Hilbert symbols of solutions of Diophantine equations. Yue [18] gave more explicit solutions to the 8-rank problem for the special case $t=2$.

In this paper we study the possible values of r_8 for $F=\mathbb{Q}(\sqrt{-p_1\cdots p_t})$ for an arbitrary t. We first compute the Hilbert symbols explicitly (see Theorem 3.4). Generalizing a result of Morton [7], our main result (see Theorem 4.2) describes the possible values of the 8-rank of $\mathscr{C}$ in terms of a quadratic form over $\mathbb{F}_2$ which is defined by quartic symbols. Consequently, the 8-rank is bounded by the *isotropy index* (see Definition 4.1) of the quadratic form. The proof of the main theorem is given in Section 6.

This paper is motivated by Tian's recent work [15,16] on the Birch and Swinnerton-Dyer conjecture, in which the 2-primary parts of class groups of quadratic number fields are related to the 2-descent method of elliptic curves.

2 Rédei matrices revisited

Rédei matrices are tools to study the 2-primary part of class groups of quadratic number fields. Here, we include a review for the case $F = \mathbb{Q}(\sqrt{-p_1 \cdots p_t})$, where $p_i \equiv 1 \pmod 4$ $(i = 1, \ldots, t-1)$ and $p_t \equiv 3 \pmod 4$. Instead of the matrix form found in the literature, here we express the Rédei matrix for the 8-rank as a bilinear form. In the next section, we will show that the quadratic form induced from this bilinear form can be computed from quartic symbols.

For more details about Rédei matrices, one may refer to the survey by Stevenhagen [14], which also includes some results for ℓ-primary parts, where ℓ is an odd prime.

In the following, let Δ be the discriminant of F. Then $\Delta = -p_1 \cdots p_t$.

2.1 The 2-rank of $\mathscr{C}$

Let $V = \mathscr{C}[2]$ be the group of elements of order 2 in $\mathscr{C}$.

For $i = 1, \ldots, t$, let $\mathfrak{p}_i$ be the prime ideal of F such that $\mathfrak{p}_i^2 = (p_i)$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ generate V. The only nontrivial relation in $\mathscr{C}$ among these elements is

$$\mathfrak{p}_1 \cdots \mathfrak{p}_t = 1. \tag{2.1}$$

We view V as a vector space over $\mathbb{F}_2$, the vector addition being the multiplication of ideal classes. It has a basis $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{t-1}\}$. Then

$$r_2(\mathscr{C}) = \dim_{\mathbb{F}_2} V = t - 1.$$

For later use we introduce another vector space V' over $\mathbb{F}_2$, which consists of all positive divisors of $p_1 \cdots p_{t-1}$. The vector addition is defined to be

$$q_1 \cdot q_2 = q_1 q_2 / (\gcd(q_1, q_2))^2.$$

Then

$$V' \to V, \quad p_i \mapsto \mathfrak{p}_i \tag{2.2}$$

is an isomorphism of vector spaces. We will identify V' with V.

2.2 The 4-rank of $\mathscr{C}$

We will use the quadratic characters to study the 4-rank of $\mathscr{C}$. Note that $r_4(\mathscr{C}) = \dim_{\mathbb{F}_2} \mathscr{C}[2] \cap 2\mathscr{C}$. The elements in $\mathscr{C}[2] \cap 2\mathscr{C}$ are exactly the elements in $\mathscr{C}[2]$ which are killed by all quadratic characters of $\mathscr{C}$.

For $i = 1, \ldots, t$, the characters χ_{p_i} defined by

$$\chi_{p_i}(\mathfrak{a}) = \left(\frac{N\mathfrak{a}, \Delta}{p_i}\right)$$

generate $(\mathscr{C}/2\mathscr{C})^\vee$, the group of quadratic characters on $\mathscr{C}$. Here $\mathfrak{a}$ is any (fractional) ideal of F, and $(\frac{a,b}{p_i})$ is the Hilbert symbol. The only nontrivial relation among these generators is

$$\chi_{p_1} \cdots \chi_{p_t} = 1. \tag{2.3}$$

We view $(\mathscr{C}/2\mathscr{C})^\vee$ as a vector space over $\mathbb{F}_2$, the vector addition being the multiplication of quadratic characters. It has a basis $\{\chi_{p_1}, \ldots, \chi_{p_{t-1}}\}$ and there is an isomorphism of vector spaces over $\mathbb{F}_2$:

$$V = \mathscr{C}[2] \xrightarrow{\cong} (\mathscr{C}/2\mathscr{C})^\vee, \quad \mathfrak{p}_i \mapsto \chi_{p_i}.$$

We restrict the quotient map $\mathscr{C} \to \mathscr{C}/2\mathscr{C}$ to $\mathscr{C}[2]$ and get

$$f_{\mathcal{A}} \colon V = \mathscr{C}[2] \to \mathscr{C}/2\mathscr{C} \cong V^\vee.$$

This induces a bilinear form on V:

$$\mathcal{A} \colon V \times V \to \mathbb{F}_2.$$

Under the basis $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{t-1}\}$, we may write $\mathcal{A}$ in the matrix form as follows:

Definition 2.1 (Rédei matrix)**.** Let $\xi\colon \{\pm 1\} \to \mathbb{F}_2$ be the group isomorphism defined by $\xi(1) = 0$ and $\xi(-1) = 1$. The Rédei matrix (for the 4-rank) is defined to be

$$M_4 = \left(\xi\left(\frac{p_i, \Delta}{p_j}\right)\right)_{1\leqslant i\leqslant t-1,\, 1\leqslant j\leqslant t-1} \quad (\text{over } \mathbb{F}_2).$$

We need the following result to compute the Hilbert symbol:

Lemma 2.2 (See [8, Chapter V, Theorem 3.6])**.** *Let $p \neq 2$ be a prime number. For $a,\, b \in \mathbb{Q}_p^*$, we write*

$$a = p^\alpha a', \quad b = p^\beta b',$$

where a' and b' are units in $\mathbb{Q}_p$. Then

$$\left(\frac{a, b}{p}\right) = (-1)^{\frac{p-1}{2}\alpha\beta}\left(\frac{a'}{p}\right)^\beta \left(\frac{b'}{p}\right)^\alpha.$$

Here (-) *is the Jacobi symbol.*

Proposition 2.3. *Under our assumption, M_4 is a symmetric matrix. In other words, $\mathcal{A}$ is a symmetric bilinear form.*

Proof. If $p_i \neq p_j$, we have

$$\left(\frac{p_i, \Delta}{p_j}\right) = \left(\frac{p_i}{p_j}\right)$$

by Lemma 2.2.

Since $p_i \equiv 1 \pmod 4$ for $i = 1, \ldots, t-1$, we see that

$$\left(\frac{p_j}{p_i}\right) = \left(\frac{p_i}{p_j}\right)(-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}} = \left(\frac{p_i}{p_j}\right) \quad \text{for all } i \neq j. \qquad \square$$

Note that $\ker f_{\mathcal{A}} = \mathscr{C}[2] \cap 2\mathscr{C}$. Therefore we have the following result:

Proposition 2.4 (Rédei)**.** *The 4-rank of $\mathscr{C}$ is*

$$r_4 = \dim_{\mathbb{F}_2} V - \dim_{\mathbb{F}_2} f_{\mathcal{A}}(V) = t - 1 - \operatorname{rank}_{\mathbb{F}_2} M_4.$$

2.3 The 8-rank of $\mathscr{C}$

We write $V_0 = \ker f_{\mathcal{A}} = \mathscr{C}[2] \cap 2\mathscr{C}$, where $\mathcal{A}$ is the bilinear form defined in Subsection 2.2.

In Subsection 2.2, we have seen that $\mathcal{A}$ is a symmetric bilinear form. Therefore, there is a natural isomorphism of vector spaces over $\mathbb{F}_2$:

$$\mathscr{C}/(\mathscr{C}[2] + 2\mathscr{C}) = \operatorname{coker} f_{\mathcal{A}} \cong V_0^\vee.$$

We have the following homomorphism of vector spaces over $\mathbb{F}_2$:

$$f_{\mathfrak{B}} : V_0 = \mathscr{C}[2] \cap 2\mathscr{C} \xrightarrow{\div 2} \mathscr{C}/\mathscr{C}[2] \to \mathscr{C}/(\mathscr{C}[2] + 2\mathscr{C}) \cong V_0^\vee.$$

The first map "division-by-2" in $2\mathscr{C}$ means taking square roots of the ideal classes. The second map is the natural quotient homomorphism. Since $\ker f_{\mathfrak{B}} = \mathscr{C}[2] \cap 4\mathscr{C}$, we have

$$r_8 = \dim_{\mathbb{F}_2} V_0 - \dim_{\mathbb{F}_2} f_{\mathfrak{B}}(V_0).$$

We are going to describe $f_{\mathfrak{B}}$ more explicitly. Let us identify $\mathscr{C}[2] \cap 2\mathscr{C}$ and its preimage V_0' in V' under the isomorphism in (2.2), and write both of them as V_0. Consider $\mathfrak{a} \in V_0 = \ker \mathcal{A} = \mathscr{C}[2] \cap 2\mathscr{C}$. We will take the square root of $\mathfrak{a}$ as follows:

Lemma 2.5 (See [7, Lemma 5]). *Assume $\mathfrak{a}$ is a proper ideal of the ring of integers of $F = \mathbb{Q}(\sqrt{\Delta})$ such that $N\mathfrak{a} \mid \Delta$, and that the class of $\mathfrak{a}$ in $\mathscr{C}$ belongs to $2\mathscr{C}$. For any positive primitive solution (x, y, z) of $x^2 = \Delta y^2 + 4az^2$ where $a = N\mathfrak{a}$, there exists an ideal $\mathfrak{b}$ for which the class of $\mathfrak{b}^2$ in $\mathscr{C}$ coincides with the class of $\mathfrak{a}$ in $\mathscr{C}$ and $N\mathfrak{b} = z$.*

The existence of (x, y, z) is ensured by the assumption that the class of $\mathfrak{a}$ in $\mathscr{C}$ belongs to $2\mathscr{C}$.

Let $\mathfrak{B}\colon V_0 \times V_0 \to \mathbb{F}_2$ be the bilinear form induced from $f_{\mathfrak{B}}$, i.e., if $\mathfrak{a} \in V_0$, $D \in V_0' \cong V_0$, and $\mathfrak{b}$ is the square root of $\mathfrak{a}$ as in Lemma 2.5, then

$$\mathfrak{B}(\mathfrak{a}, D) = \xi(\chi_D(\mathfrak{b})) = \xi\left(\left(\frac{N\mathfrak{b}, \Delta}{D}\right)\right).$$

Summarizing the above discussions, we obtain the following two propositions:

Proposition 2.6. *With the above notation,*

$$\mathfrak{B}(\mathfrak{a}, D) = \xi\left(\left(\frac{N\mathfrak{b}, \Delta}{D}\right)\right) = \xi\left(\left(\frac{z, \Delta}{D}\right)\right).$$

Proposition 2.7. *The 8-rank* $r_8 = \dim_{\mathbb{F}_2} V_0 - \dim_{\mathbb{F}_2} f_{\mathfrak{B}}(V_0) = r_4 - \operatorname{rank}_{\mathbb{F}_2} \mathfrak{B}$.

3 The quadratic form $Q_{\mathfrak{B}}$

Definition 3.1. Let W be a vector space over a field k. Then a map $Q\colon W \to k$ is called a *quadratic form* if there exists a bilinear form B such that $Q(x) = Q_B(x) := B(x, x)$.

Remark 3.2. (1) Note that if $\operatorname{char} k \neq 2$, there is always a symmetric bilinear form B satisfying the condition above. When $\operatorname{char} k = 2$, this is no longer true.

(2) By [2, Paragraphe 3, No. 4, Proposition 2], Definition 3.1 is equivalent to [2, Paragraphe 3, No. 4, Définition 2]: A quadratic form on W is a map $Q\colon W \to k$ such that

(i) $Q(ax) = a^2 Q(x)$ for all $a \in k$ and $x \in W$, and

(ii) the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.

Definition 3.3 (Quartic symbol). Let $p \equiv 1 \pmod 4$ be a prime number. If $a \in \mathbb{Z}$ is a quadratic residue $(\bmod p)$ and $(a, p) = 1$, we define the (*rational*) *quartic residue symbol* as

$$\left(\frac{a}{p}\right)_4 = \pm 1 \equiv a^{\frac{p-1}{4}} \pmod p.$$

For $D = p_1 \cdots p_s$ where $p_i \equiv 1 \pmod 4$ $(i = 1, \ldots, s)$ are distinct primes, and $a \in \mathbb{Z}$ satisfying $(a, D) = 1$ and $(\frac{a}{p_i}) = 1$, we define

$$\left(\frac{a}{D}\right)_4 = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)_4.$$

Then $(\frac{a}{D})_4 = 1$ if a is congruent to the fourth power of an integer $(\bmod D)$.

Theorem 3.4. *Let $Q_{\mathfrak{B}}$ be the quadratic form on V_0 defined by $Q_{\mathfrak{B}}(D) = \mathfrak{B}(D, D)$ (see Subsection 2.3). Then*

$$Q_{\mathfrak{B}}(D) = \xi\left(\left(\frac{\Delta/D}{D}\right)_4\right).$$

Remark 3.5. This generalizes [7, Lemma 7]. Note that unlike [7], we do not assume $(\frac{p_i}{p_j}) = 1$ for $1 \leqslant i \neq j < t$.

Proof. When $D = 1$, this is trivial. So we may assume $D \neq 1$.

If $N\mathfrak{a} = D$, let (x, y, z) be a primitive solution of the equation

$$x^2 = \Delta y^2 + 4Dz^2.$$

Then $z = N\mathfrak{b}$ by Lemma 2.5. We also have $D \mid x$. Suppose $\Delta = D \cdot D'$, $x = Dx'$. Then

$$Dx'^2 = D'y^2 + 4z^2. \tag{3.1}$$

If $p \mid D$, then $p \nmid D'$ and hence $p \nmid z$. We have

$$\chi_D(\mathfrak{a}) = \left(\frac{N\mathfrak{b}, \Delta}{D}\right) = \prod_{p|D}\left(\frac{N\mathfrak{b}, \Delta}{p}\right) = \prod_{p|D}\left(\frac{z}{p}\right) = \left(\frac{z}{D}\right), \tag{3.2}$$

by Lemma 2.2.

(3.1) implies

$$D'y^2 + 4z^2 \equiv 0 \pmod{p}.$$

Therefore,

$$\left(\frac{D'}{p}\right)_4\left(\frac{y}{p}\right) = \left(\frac{z}{p}\right)\left(\frac{-4}{p}\right)_4.$$

We are going to compute $(\frac{y}{D})$ and $(\frac{-4}{p})_4$.

Write $y = 2^k y'$ where $2 \nmid y'$. Then

$$\left(\frac{y'}{D}\right) = \prod_{q|y'}\left(\frac{q}{D}\right) = \prod_{q|y'}\prod_{p|D}\left(\frac{q}{p}\right) = \prod_{q|y'}\prod_{p|D}\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \prod_{q|y'}\left(\frac{D}{q}\right).$$

(3.1) implies $Dx'^2 \equiv 4z^2 \pmod{q}$ for all prime factors q of y'. Hence, $(\frac{D}{q}) = 1$ and $(\frac{y'}{D}) = 1$.

Now let us consider the possible values of k.

(i) If $k = 0$, we have

$$\left(\frac{y}{D}\right) = \left(\frac{y'}{D}\right) = 1.$$

(ii) Now assume $k > 0$. We have $D \equiv 1 \pmod 4$ and $D' \equiv 1 \pmod 4$. From $Dx'^2 = D'2^{2k}y'^2 + 4z^2$, we see that if $k > 0$, then $2 \mid x'$. Since $\gcd(x, y, z) = 1$, we know $2 \nmid z$. Hence $z^2 \equiv 1 \pmod 8$. Write $y = 2\tilde{y}$ and $x' = 2\tilde{x}$. Then

$$D\tilde{x}^2 = D'\tilde{y}^2 + z^2. \tag{3.3}$$

(a) If $k = 1$, i.e., $2 \nmid \tilde{y}$, then (3.3) implies

$$\tilde{x}^2 \equiv 1 + 1 \pmod 4,$$

which is impossible.

(b) If $k = 2$, we have

$$\left(\frac{y}{D}\right) = \left(\frac{2}{D}\right)^2\left(\frac{y'}{D}\right) = \left(\frac{y'}{D}\right) = 1.$$

(c) If $k \geqslant 3$, then $4 \mid \tilde{y}$. It follows from (3.3) that $2 \nmid \tilde{x}$ and hence $\tilde{x}^2 \equiv 1 \pmod 8$. Then (3.3) implies $D \equiv 1 \pmod 8$. In other words, D has an even number of prime factors p with $p \equiv 5 \pmod 8$. Note that $(\frac{2}{p})$ is 1 if $p \equiv 1 \pmod 8$ and is -1 if $p \equiv 5 \pmod 8$. Therefore,

$$\left(\frac{y}{D}\right) = \left(\frac{y}{D'}\right)\cdot\prod_{p|D}\left(\frac{2}{p}\right) = \left(\frac{y'}{D}\right) = 1.$$

To summarize, $(\frac{y}{D}) = 1$ in all cases.

Note that

$$\left(\frac{-4}{p}\right)_4 = \left(\frac{-1}{p}\right)_4\left(\frac{2}{p}\right).$$

We have $(\frac{-1}{p})_4 \equiv (-1)^{\frac{p-1}{4}} \pmod p$ and $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. No matter whether $p \equiv 1$ or $5 \pmod 8$, we always have $(\frac{-4}{p})_4 = 1$.

By (3.2), we have $(\frac{z}{D}) = (\frac{D'}{D})_4$. □

4 Statement of the main theorem

Definition 4.1. The *isotropy index* of a quadratic form Q on a vector space W is defined to be the maximal dimension of W', where W' is a subspace of W and $Q|_{W'} = 0$. We denote the isotropy index of Q by $\rho(Q)$.

For a quadratic form Q, we write

$$\mathscr{N}(Q) = \{\text{null}(B) \mid B\colon W \times W \to k \text{ is a bilinear form such that } Q_B = Q\}.$$

Here $\text{null}(B) = \dim W - \text{rank}(B)$ is the *nullity* of B.

Theorem 4.2. (1) *Let $Q_{\mathfrak{B}}$ be the quadratic form on V_0 defined by*

$$Q_{\mathfrak{B}}(D) = \xi\left(\left(\frac{\Delta/D}{D}\right)_4\right)$$

as in Section 3. *Let r_8 be the* 8*-rank of the class group of $F = \mathbb{Q}(\sqrt{\Delta})$. Then*

$$r_8 \in \mathscr{N}(Q_{\mathfrak{B}}).$$

(2) *Let Q be a quadratic form on an r-dimensional vector space over $\mathbb{F}_2$ with isotropy index ρ. Then*

$$\mathscr{N}(Q) = S(\rho, r) := \left\{ a \;\middle|\; \begin{array}{l} 0 \leqslant a \leqslant \rho, \\ a \equiv r \pmod 2 \text{ if } \rho = r, \\ a = 1 \text{ if } r = 2 \text{ and } Q \cong X \end{array} \right\}, \tag{1}$$

where X is the quadratic form on $\mathbb{F}_2^2$ defined by $X(x_1e_1 + x_2e_2) = x_1x_2$ for the standard basis $\{e_1, e_2\}$ of $\mathbb{F}_2^2$.

In particular, for the quadratic form $Q_{\mathfrak{B}}$ in (1)*, we have $\mathscr{N}(Q_{\mathfrak{B}}) = S(\rho, r_4)$, where $r_4 = \dim_{\mathbb{F}_2} V_0$ is the* 4*-rank of the class group of $F = \mathbb{Q}(\sqrt{\Delta})$.*

The proof will be given in Section 6.

Corollary 4.3. $r_8 \leqslant \rho(Q_{\mathfrak{B}})$.

An immediate consequence of Corollary 4.3 is

$$r_8 \leqslant \log_2 \#Q_{\mathfrak{B}}^{-1}(0). \tag{4.1}$$

For an analogue of (4.1) for certain real quadratic fields, see Fouvry and Klüners [5, Theorem 3(ii)].

Corollary 4.4. *If $Q_{\mathfrak{B}} = 0$, then $r_8 \equiv r_4 \pmod 2$.*

Indeed, Corollaries 4.3 and 4.4 follow from Theorem 4.2(1) and the easy part of (2), i.e.,

$$\mathscr{N}(Q) \subset S(\rho, r).$$

5 Interlude: Quadratic forms over $\mathbb{F}_2$

In this section, we will review the classification of quadratic forms over $\mathbb{F}_2$ which will be used in the proof of Theorem 4.2, and calculate the isotropy index (Definition 4.1) in each case. Some of the material (in more general form) can be found in [4, Chapitre 1, Paragraphe 16].

In this section, Q is a quadratic form on a finite-dimensional vector space W over $\mathbb{F}_2$. It induces an alternating bilinear form

$$\nabla_Q(x, y) := Q(x + y) - Q(x) - Q(y).$$

If W' is a subspace of W, we define

$$W'^{\perp} = \{x \in W \mid \nabla_Q(x, y) = 0 \text{ for all } y \in W'\}.$$

∇_Q induces a nondegenerate alternating bilinear form $\overline{\nabla}_Q$ on $W/W^\perp$. Therefore, there exists a basis $\{e_1,\dots,e_k,e_{k+1},\dots,e_{2k}\}$ of $W/W^\perp$ so that $\overline{\nabla}_Q$ can be written as

$$\begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

The restriction of Q to $W^\perp$ is linear.

Definition 5.1. The *defect* of Q is defined to be $d = \dim_{\mathbb{F}_2} Q(W^\perp)$.

By definition, d equals 0 or 1.

Definition 5.2. The *rank* of Q is defined to be $\mathrm{rk}(Q) = 2k + d$, where $2k = \dim W/W^\perp$ as before.

It follows that the isotropy index $\rho(Q) = \rho(Q_0) + (n - \mathrm{rk}(Q))$, where Q_0 is the (nondegenerate) quadratic form on $W_0 := W/\ker(Q|_{W^\perp})$ induced from Q.

Classification of quadratic forms over $\mathbb{F}_2$. Let $\{e_1,\dots,e_n\}$ be a basis of $\mathbb{F}_2^n$. As a shorthand, we introduce the following quadratic forms:

- On $\mathbb{F}_2^1$, let $I(x_1e_1) = x_1^2$.
- On $\mathbb{F}_2^2$, let $X(x_1e_1 + x_2e_2) = x_1x_2$ and $Y(x_1e_1 + x_2e_2) = x_1^2 + x_1x_2 + x_2^2$.
- On $\mathbb{F}_2^n$, let $O_n(\sum_{i=1}^n x_ie_i) = 0$.

Type 1. The rank of Q is odd ($\mathrm{rk}(Q) = 2k+1$).

There exists a basis $\{e_1,\dots,e_{2k+1},\dots,e_n\}$ such that

$$Q\Big(\sum_{i=1}^n x_ie_i\Big) = \sum_{i=1}^k x_ix_{k+i} + x_{2k+1}^2. \quad (Q \cong X^{\oplus k} \oplus I \oplus O_{n-2k-1}.) \tag{2}$$

Then

$$\rho(Q_0) = k \quad \text{and} \quad \rho(Q) = k + (n - \mathrm{rk}(Q)).$$

Type 2. The rank of Q is even ($\mathrm{rk}(Q) = 2k$).

There exists a basis $\{e_1,\dots,e_{2k},\dots,e_n\}$ such that either

$$\text{(Type 2.1)} \quad Q\Big(\sum_{i=1}^n x_ie_i\Big) = \sum_{i=1}^k x_ix_{k+i} \quad (Q \cong X^{\oplus k} \oplus O_{n-2k}) \tag{3}$$

or

$$\text{(Type 2.2)} \quad Q\Big(\sum_{i=1}^n x_ie_i\Big) = \sum_{i=1}^{k-1} x_ix_{k+i} + x_k^2 + x_kx_{2k} + x_{2k}^2. \quad (Q \cong X^{\oplus(k-1)} \oplus Y \oplus O_{n-2k}.) \tag{4}$$

Then

$$\rho(Q_0) = \begin{cases} k & \text{(Type 2.1)} \\ k-1 & \text{(Type 2.2)} \end{cases} \quad \text{and} \quad \rho(Q) = \rho(Q_0) + (n - \mathrm{rk}(Q)).$$

For the proof of the classification (and generalization to finite fields of characteristic 2), one may refer to [3, Chapter VIII, Section 199].

In both Types 1 and 2, we have $2\rho(Q) \geqslant n - 2$.

How to determine the type of Q? There is an easy way to determine the type of Q. It can be checked that the cardinality of the preimage of 0 is

$$\#Q^{-1}(0) = \begin{cases} 2^{n-1} & \text{(Type 1)}, \\ 2^{n-1} + 2^{\rho-1} & \text{(Type 2.1)}, \\ 2^{n-1} - 2^{\rho} & \text{(Type 2.2)}. \end{cases}$$

Therefore, the type of Q can be determined by "vote":

$$Q \text{ is of } \begin{cases} \text{Type 1}, & \text{if } \#Q^{-1}(0) = \#Q^{-1}(1), \\ \text{Type 2.1}, & \text{if } \#Q^{-1}(0) > \#Q^{-1}(1), \\ \text{Type 2.2}, & \text{if } \#Q^{-1}(0) < \#Q^{-1}(1). \end{cases}$$

The *Arf invariant* of Q is 0 if Q is of Type 2.1 and is 1 if Q is of Type 2.2 (see [1]).

Moreover, the isotropy index ρ of Q can be determined from $\#Q^{-1}(0)$ if Q is of Type 2.

6 Proof of the main theorem

For Part (1) of Theorem 4.2: From Subsection 2.3 and the definition of Q we see $r_8 \in \mathscr{N}(Q_{\mathfrak{B}})$.

For Part (2) of Theorem 4.2: We first show $\mathscr{N}(Q) \subset S(\rho, r)$. Suppose B is a bilinear form which induces the quadratic form $Q_B = Q$. Then $\text{null}(B) \leqslant \rho(Q)$ by definition.

If $\rho = r$, i.e., $Q = 0$, then B is an alternating bilinear form. Therefore $\text{rank}(B) \equiv 0 \pmod 2$ and $\text{null}(B) \equiv r \pmod 2$.

If $r = 2$ and $Q \cong X$, we have $\text{null}(B) = 1$.

Now we show $\mathscr{N} \supset S(\rho, r)$. Suppose $a \in S(\rho, r)$. We are going to show that there is a bilinear form B such that $Q_B = Q$ and $\text{null}(B) = a$.

We will adopt the following notation: If S_1, $S_2 \subset \mathbb{Z}$, we write

$$S_1 + S_2 = \{s_1 + s_2 \mid s_1 \in S_1, s_2 \in S_2\}.$$

We define

$$\mathscr{B}(Q) = \{B \mid B \text{ is a bilinear form such that } Q_B = Q\}.$$

Lemma 6.1. *Let Q_1 and Q_2 be two quadratic forms. Then*

$$\mathscr{N}(Q_1) + \mathscr{N}(Q_2) \subset \mathscr{N}(Q_1 \oplus Q_2).$$

According to the classification of quadratic forms over $\mathbb{F}_2$, it suffices to prove that $\mathscr{N} \supset S(\rho, r)$ for the following cases:

(I) $X^{\oplus k} \oplus O_m$ for $k \geqslant 0$, $m \geqslant 0$.

(II) $X^{\oplus k} \oplus O_m \oplus Y$ for $k \geqslant 0$, $m \geqslant 0$.

(III) $X^{\oplus k} \oplus O_m \oplus I$ for $k \geqslant 0$, $m \geqslant 0$.

In all cases, the isotropy index ρ is equal to $k + m$.

Now we will check the theorem by exhausting all the cases.

(i) $\rho(O_1) = 1$. We have $\mathscr{N}(O_1) = \{1\}$.

(ii) $\rho(O_2) = 2$. Since

$$\mathscr{B}(O_2) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

we get $\mathscr{N}(O_2) = \{0, 2\}$.

(iii) We will show that

$$\mathscr{N}(O_m) = \{a \mid 0 \leqslant a \leqslant m,\ a \equiv m \pmod 2\}$$

for $m > 2$ by induction. In fact,

$$\begin{aligned} \mathscr{N}(O_m) &\supset \mathscr{N}(O_{m-2}) + \mathscr{N}(O_2) \\ &= \{a \mid 0 \leqslant a \leqslant m-2,\ a \equiv m \pmod 2\} + \{0, 2\} \\ &= \{a \mid 0 \leqslant a \leqslant m,\ a \equiv m \pmod 2\}. \end{aligned}$$

(iv) $\rho(X)=1$. We have

$$\mathscr{B}(X)=\left\{\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix}\right\}.$$

Therefore, $\mathscr{N}(X)=\{1\}$.

(v) $\rho(X\oplus O_1)=2$. We have

$$\mathscr{N}(X\oplus O_1)\supset\mathscr{N}(X)+\mathscr{N}(O_1)=\{2\}.$$

Since

$$\begin{pmatrix}0&1&1\\0&0&1\\1&1&0\end{pmatrix},\ \begin{pmatrix}0&1&1\\0&0&0\\1&0&0\end{pmatrix}\in\mathscr{B}(X\oplus O_1)$$

and they have nullity 0 and 1 respectively, we have $\mathscr{N}(X\oplus O_1)=\{0,1,2\}$.

(vi) $\rho(X\oplus O_2)=3$. On the other hand,

$$\begin{aligned}\mathscr{N}(X\oplus O_2)&=\mathscr{N}((X\oplus O_1)\oplus O_1)\\&\supset\mathscr{N}(X\oplus O_1)+\mathscr{N}(O_1)\\&=\{0,1,2\}+\{1\}=\{1,2,3\}.\end{aligned}$$

It can be checked that

$$\begin{pmatrix}0&1&1&1\\0&0&0&1\\1&0&0&0\\1&1&0&0\end{pmatrix}\in\mathscr{B}(X\oplus O_2)$$

and has nullity 0. Therefore, $\mathscr{N}(X\oplus O_2)=\{0,1,2,3\}$.

(vii) We will show that

$$\mathscr{N}(X\oplus O_m)=\{0,1,2,\ldots,m+1\}$$

for $m\geqslant 3$ by induction. In fact,

$$\begin{aligned}\mathscr{N}(X\oplus O_m)&=\mathscr{N}((X\oplus O_{m-2})\oplus O_2)\\&\supset\mathscr{N}(X\oplus O_{m-2})+\mathscr{N}(O_2)\\&=\{0,1,\ldots,m-1\}+\{0,2\}\\&=\{0,1,\ldots,m+1\}.\end{aligned}$$

(viii) $\rho(X\oplus X)=2$. We have

$$\mathscr{N}(X\oplus X)\supset\mathscr{N}(X)+\mathscr{N}(X)=\{2\}.$$

Since

$$\begin{pmatrix}0&1&1&1\\0&0&0&1\\1&0&0&1\\1&1&0&0\end{pmatrix},\ \begin{pmatrix}0&1&0&1\\0&0&0&0\\0&0&0&1\\1&0&0&0\end{pmatrix}\in\mathscr{B}(X\oplus X)$$

and they have nullity 0 and 1, respectively, we have

$$\mathscr{N}(X\oplus X)=\{0,1,2\}.$$

(ix) $\rho(X\oplus X\oplus O_1)=3$. On the other hand,

$$\mathscr{N}(X\oplus X\oplus O_1)\supset\mathscr{N}(X\oplus X)+\mathscr{N}(O_1)=\{0,1,2\}+\{1\}=\{1,2,3\}.$$

Note that

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix} \in \mathscr{B}(X \oplus X \oplus O_1)$$

and it has nullity 0. It follows that

$$\mathscr{N}(X \oplus X \oplus O_1) = \{0, 1, 2, 3\}.$$

(x) We will show that the theorem holds for all $X \oplus X \oplus O_m$ for $m \geqslant 2$ by induction. In fact, we have

$$\mathscr{N}(X \oplus X \oplus O_m) \supset \mathscr{N}(X \oplus X \oplus O_{m-2}) + \mathscr{N}(O_2) = \{0, 1, 2, \ldots, m\} + \{0, 2\} = \{0, 1, 2, \ldots, m+2\},$$

for $m > 2$.

(xi) $\rho(X \oplus X \oplus X) = 3$. We have

$$\mathscr{N}(X \oplus X \oplus X) \supset \mathscr{N}(X \oplus X) + \mathscr{N}(X) = \{0, 1, 2\} + \{1\} = \{1, 2, 3\}.$$

Besides,

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \in \mathscr{B}(X \oplus X \oplus X)$$

and it has nullity 0. Therefore,

$$\mathscr{N}(X \oplus X \oplus X) = \{0, 1, 2, 3\}.$$

(xii) The theorem holds for all $X^{\oplus k} \oplus O_m$ by induction for $k \geqslant 3$ and $k + m \geqslant 4$, because

$$\begin{aligned} \mathscr{N}(X^{\oplus k} \oplus O_m) &\supset \mathscr{N}(X^{\oplus(k-2)} \oplus O_m) + \mathscr{N}(X \oplus X) \\ &= \{0, 1, 2, \ldots, k-2+m\} + \{0, 1, 2\} \\ &= \{0, 1, 2, \ldots, k+m\}. \end{aligned}$$

(xiii) $\rho(Y) = 0$. On the other hand,

$$\mathscr{B}(Y) = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\},$$

and $\mathscr{N}(Y) = \{0\}$.

(xiv) $\rho(Y \oplus O_1) = 1$. Since

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathscr{B}(Y \oplus O_1)$$

and they have nullity 1 and 0 respectively, we get $\mathscr{N}(Y \oplus O_1) = \{0, 1\}$.

(xv) $\rho(Y \oplus O_2) = 2$. On the other hand,

$$\mathscr{N}(Y \oplus O_2) \supset \mathscr{N}(Y) + \mathscr{N}(O_2) = \{0\} + \{0, 2\} = \{0, 2\}$$

and

$$\mathscr{N}(Y \oplus O_2) \supset \mathscr{N}(Y \oplus O_1) + \mathscr{N}(O_1) = \{0,1\} + \{1\} = \{1,2\}.$$

Therefore, $\mathscr{N}(Y \oplus O_2) = \{0,1,2\}$.

(xvi) We prove for all $Y \oplus O_m$ $(m \geqslant 3)$ by induction

$$\begin{aligned}\mathscr{N}(Y \oplus O_m) &\supset \mathscr{N}(Y \oplus O_{m-2}) + \mathscr{N}(O_2)\\ &= \{0,1,\ldots,m-2\} + \{0,2\} = \{0,1,\ldots,m\}.\end{aligned}$$

(xvii) $\rho(X \oplus Y) = 1$. Since

$$\begin{pmatrix}0&1&0&0\\0&0&0&0\\0&0&1&1\\0&0&0&1\end{pmatrix}, \begin{pmatrix}0&1&1&1\\0&0&1&0\\1&1&1&1\\1&0&0&1\end{pmatrix} \in \mathscr{B}(X \oplus Y)$$

and they have nullity 0 and 1, respectively, we know that $\mathscr{N}(X \oplus Y) = \{0,1\}$.

(xviii) $\rho(X^{\oplus k} \oplus Y \oplus O_m) = k + m$. For $k \geqslant 1$ and $k + m \geqslant 2$, we have

$$\mathscr{N}(X^{\oplus k} \oplus Y \oplus O_m) \supset \mathscr{N}(X^{\oplus k} \oplus O_m) + \mathscr{N}(Y) = \{0,1,\ldots,k+m\}.$$

(xix) $\rho(I) = 0$. We also have $\mathscr{B}(I) = \{(1)\}$ and hence $\mathscr{N}(I) = \{0\}$.

(xx) $\rho(I \oplus O_1) = 1$. In this case, $r_4 = 2$. We see that

$$\mathscr{B}(I \oplus O_1) = \left\{\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}\right\}.$$

Therefore, $\mathscr{N}(I \oplus O_1) = \{0,1\}$.

(xxi) $\rho(I \oplus O_2) = 2$. We have

$$\mathscr{N}(I \oplus O_2) \supset \mathscr{N}(I) + \mathscr{N}(O_2) = \{0\} + \{0,2\}$$

and

$$\mathscr{N}(I \oplus O_2) \supset \mathscr{N}(I \oplus O_1) + \mathscr{N}(O_1) = \{0,1\} + \{1\} = \{1,2\}.$$

Therefore, $\mathscr{N}(I \oplus O_2) = \{0,1,2\}$.

(xxii) $\rho(I \oplus O_m) = m$. We will show that $\mathscr{N}(I \oplus O_m) = \{0,1,\ldots,m\}$ for $m > 2$ by induction. In fact,

$$\begin{aligned}\mathscr{N}(I \oplus O_m) &\supset \mathscr{N}(I \oplus O_{m-2}) + \mathscr{N}(O_2)\\ &= \{0,1,\ldots,m-2\} + \{0,2\} = \{0,\ldots,m\}.\end{aligned}$$

(xxiii) $\rho(X \oplus I) = 1$. We also have $\mathscr{N}(X \oplus I) \supset \mathscr{N}(X) + \mathscr{N}(I) = \{1\}$. Since

$$\begin{pmatrix}0&1&1\\0&0&1\\1&1&1\end{pmatrix} \in \mathscr{B}(X \oplus I)$$

and it has nullity 0, we get $\mathscr{N}(X \oplus I) = \{0,1\}$.

(xxiv) $\rho(X^{\oplus k} \oplus I \oplus O_m) = k + m$. For $k \geqslant 1$ and $k + m \geqslant 2$, we have

$$\mathscr{N}(X^{\oplus k} \oplus I \oplus O_m) \supset \mathscr{N}(X^{\oplus k} \oplus O_m) + \mathscr{N}(I) = \{0,1,\ldots,k+m\}.$$

With all cases exhausted, we conclude that Theorem 4.2 is true.

Remark 6.2. Theorem 4.2 states that the 8-rank $r_8 \in \mathscr{N}(Q_{\mathfrak{B}})$. If $r_4 = 1$, we have $Q_{\mathfrak{B}} \cong O_1$ or I. Since $\mathscr{N}(O_1) = \{1\}$ and $\mathscr{N}(I) = \{0\}$, r_8 is determined by $Q_{\mathfrak{B}}$. However, in general r_8 may not be determined by $Q_{\mathfrak{B}}$. For example, if $r_4 = 2$, $Q_{\mathfrak{B}} \cong X$ or Y or O_2 or $I \oplus O_1$. We know from Theorem 4.2 that $\mathscr{N}(X) = \{1\}$, $\mathscr{N}(Y) = \{0\}$, $\mathscr{N}(O_2) = \{0, 2\}$ and $\mathscr{N}(I \oplus O_1) = \{0, 1\}$. In the latter two cases, we have $\#\mathscr{N}(Q_{\mathfrak{B}}) > 1$. In all cases, all values in $\mathscr{N}(Q_{\mathfrak{B}})$ actually appear as the 8-ranks of the class groups of infinitely many imaginary quadratic number fields (see the proof of [7, Theorem 2]).

Acknowledgements This work was supported by China Postdoctoral Science Foundation (Grant No. 2013M541064), National Natural Science Foundation of China (Grant No. 11371043) and National Basic Research Program of China (Grant No. 2013CB834202). The author thanks Ye Tian for introducing the problem of 8-rank of class groups of quadratic number fields to her. The author is very grateful to Weizhe Zheng for many helpful discussions and constant encouragement. The author also thanks the referees for many useful comments.

References

1 Arf C. Untersuchungen über quadratische Formen in Körpern der Charakteristik 2, I. J Reine Angew Math, 1941, 183: 148–167
2 Bourbaki N. Éléments de mathématique. Algèbre. Chapitre 9. Berlin: Springer-Verlag, 2007
3 Dickson L E. Linear Groups: With an Exposition of the Galois Field Theory. New York: Dover Publications, 1958
4 Dieudonné J A. La géométrie des groupes classiques. Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. Berlin: Springer-Verlag, 1971
5 Fouvry É, Klüners J. The parity of the period of the continued fraction of $\sqrt{d}$. Proc Lond Math Soc (3), 2010, 101: 337–391
6 Kolster M. The 2-part of the narrow class group of a quadratic number field. Ann Sci Math Québec, 2005, 29: 73–96
7 Morton P. Density result for the 2-classgroups of imaginary quadratic fields. J Reine Angew Math, 1982, 332: 156–187
8 Neukirch J. Class Field Theory. Heidelberg: Springer, 2013
9 Rédei L. Über einige Mittelwertfragen im quadratischen Zahlkörper. J Reine Angew Math, 1936, 174: 15–55
10 Rédei L. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. J Reine Angew Math, 1938, 180: 1–43
11 Rédei L. Die Diophantische Gleichung $mx^2 + ny^2 = z^4$. Monatshefte Math, 1939, 48: 43–60
12 Rédei L. Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung. Acta Math Acad Sci Hung, 1953, 4: 31–87
13 Rédei L, Reichardt H. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. J Reine Angew Math, 1934, 170: 69–74
14 Stevenhagen P. Rédei-matrices and applications. In: Number Theory. London Math Soc Lecture Note Ser, vol. 215. Cambridge: Cambridge University Press, 1995, 245–259
15 Tian Y. Congruent numbers and Heegner points. Cambridge J Math, 2014, 2: 117–161
16 Tian Y. Congruent numbers with many prime factors. Proc Natl Acad Sci USA, 2012, 109: 21256–21258
17 Waterhouse W C. Pieces of eight in class groups of quadratic fields. J Number Theory, 1973, 5: 95–97
18 Yue Q. 8-ranks of class groups of quadratic number fields and their densities. Acta Math Sin Engl Ser, 2011, 27: 1419–1434