GENERATION OF ISOMETRIES OF CERTAIN $\mathbb{Z}$-LATTICES BY SYMMETRIES

Myung-Hwan Kim[1] and Byeong-Kweon Oh[2]

[1] Dept. of Math., Seoul Nat'l Univ., Seoul 151-742, Korea
[2] Korea Institute for Advanced Study, Seoul 130-012, Korea
E-mails: mhkim@math.snu.ac.kr and bkoh@math.kias.re.kr

Abstract. It is well known that every isometry of a quadratic space is generated by symmetries. Although this is not true in general for isometries of lattices, there are certain $\mathbb{Z}$-lattices whose isometries are generated by -1 and symmetries. In this paper, we prove that positive $\mathbb{Z}$-lattices with determinant an odd prime p (or $2p$ if p is not possible), which we call primal lattices, have this property if the rank is not too big. More precisely, we prove that every isometry is generated by -1 and symmetries with respect to minimal vectors of length 2 for primal even (or odd) $\mathbb{Z}$-lattices of rank less than 16 (or 13, repectively) provided that the minimal length is at least 2, and that the bound of rank in each case is extremal. The most important ingredient in this work is the behavior of the maximal root sublattice which, we found, plays an essential role in shaping the isometry group of a given lattice.

§1. Introduction

Let L be a regular quadratic $\mathbb{Z}$-*lattice* or a *lattice* in short, by which we mean a free $\mathbb{Z}$-module equipped with a non-degenerate bilinear form B satisfying $B(L,L) \subset \mathbb{Z}$. The *isometry group* $O(L)$ of L is the group of $\mathbb{Z}$-module isomorphisms of L which preserve the bilinear form B. The group $O(L)$ is known to be finitely generated, and in particular, $O(L)$ is finite if L is positive definite.

It is well known that every isometry of a quadratic space is generated by symmetries. this, however, is not true in general for isometries of lattices. For example,

---

1991 *Mathematics Subject Classification.* 11E12, 11H06.
Key words and phrases. isometries of lattices, symmetries of lattices, root sublattices.
This work was partially supported by KOSEF (98-0701-01-5-2) and KRF (98-015-D00024).

if we let $L = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 + \mathbb{Z}x_4$ such that

$$(B(x_i, x_j)) = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

then the isometry $\sigma \in O(L)$ such that $\sigma(x_1) = x_3, \sigma(x_2) = x_4$ and $\sigma(x_3) = x_1, \sigma(x_4) = x_2$ can not be represented by a product of symmetries.

In connection with this problem, Kitaoka's result [16] is notable. He proved that every isometry is generated by -1 and symmetries for positive even quaternary lattices of odd prime determinant (see also [17]). His result played an important role in finding class number formula for such lattices and in determining linear independence of certain theta series as well (see [13],[14]). In this vein, the following interesting question arises naturally: For a $\mathbb{Z}$-lattice L, let $S'(L)$ be the subgroup of $O(L)$ generated by -1 and symmetries in $O(L)$.

$(*)$ *"When is $S'(L)$ equals to $O(L)$?"*

In this paper, we extend Kitaoka's result to higher rank lattices with no parity restriction. In dong so, it is necessary for us to develop a different method because Kitaoka's method, which depends heavily on the structure of binary sublattices contained in quaternary lattices, was not applicable to higher rank case. Let $S(L)$ be the subgroup of $S'(L)$ generated by -1 and symmetries with respect to the minimal vectors of rank 2 in L. In our case, to deal with the following question is easier than the question $(*)$.

$(**)$ *"When is $S(L)$ equal to $O(L)$?"*

We always assume that L is a positive $\mathbb{Z}$-lattice such that $1 \notin Q(L)$, where Q is the quadratic map corresponding to the bilinear form B, because otherwise the sublattice I_k generated by the vectors of length 1 splits L, i.e., $L = I_k \perp L'$ with $1 \notin Q(L')$, so that $O(L) = O(I_k) \oplus O(L')$. In this paper, we prove that $S(L) = O(L)$ if L is even with even rank ≤ 14 and $dL = p$, or if L is even with odd rank ≤ 15 and $dL = 2p$, or if L is odd with rank ≤ 12 and $dL = p$, and that the bound of rank in each case is extremal.

For various interesting results on isometry groups of positive definite lattices, see, for example, [3], [5], [6], [12], [21], [22], [23], [27] and [28]. We adopt standard terminologies and notations from [26].

§2. Isometry groups of lattices

In this section, we prove some properties of isometry groups of $\mathbb{Z}$-lattices, which are useful in the sequel. A positive $\mathbb{Z}$-lattice L with $dL = \delta p$ is called a *primal lattice*, where p is an odd prime, $\delta = 1$ if either L is odd or L is even of even rank, and $\delta = 2$ if L is even of odd rank (see [16], where such lattices are called *nice lattices*). Note that dL cannot be an odd prime in the latter case. If L is primal even of even rank n, then $n \equiv dL - 1 \pmod 4$. A vector $x \in L$ is called a *minimal vector* if $Q(x) = 2$.

Lemma 2.1. *For a positive $\mathbb{Z}$-lattice L of rank n, if the isometry group $O(L)$ contains an element σ such that $\sigma^2 = -1$, then n is even and dL is a square of some integer.*

Proof. Let $\sigma \in O(L)$ satisfying $\sigma^2 = -1$. Since $\det(-1)$ is positive, the rank n of L must be even. Since L is rationally equivalent to a diagonal form, we can find a rational matrix $T = (t_{ij})$ and a positive diagonal matrix $D = (d_i \delta_{ij})$ such that $T^t DT = D$, $T^2 = -1$, and $dL = \prod_{i=1}^n d_i$. We define a matrix $T' = (t'_{ij})$ such that $t'_{ij} = t_{ij} d_i$. Then T' is a skew-symmetric matrix with rational entries. Since $\det T' = \det T \; dL$ is a square of some rational number, dL is a square of some integer. $\square$

Lemma 2.2. *Let L be a positive $\mathbb{Z}$-lattice of rank n such that $q = n + 1$ is an odd prime. If there is an element $\sigma \in O(L)$ of order q, then $dL = q \times$ (a square).*

Proof. For a prime r ($r \neq 2, q$ and dL is not divisible by r), the quotient L/rL becomes a regular quadratic space over $\mathbb{Z}/r\mathbb{Z}$. Let's denote the orthogonal group of L/rL over $\mathbb{Z}/r\mathbb{Z}$ by $O_r(L)$. Then, there is a natural injective homomorphism (see [24], Theorem IX. 7)

$$\pi : O(L) \longmapsto O_r(L).$$

for sufficiently large r. So if q divides $|O(L)|$, then q also divides $|O_r(L)|$. It is well known that

$$|O_r(L)| = 2r^{n(n-1)/2} \prod_{i=1}^{(n/2)-1} (1 - r^{2i-n}) \times \left(1 - r^{-n/2}\left(\frac{(-1)^{n/2} d(L/rL)}{r}\right)\right),$$

where $\left(\frac{*}{r}\right)$ is the Legendre symbol (see [4],[19]). From this, choosing r a primitive root modulo q, we get

$$\left(\frac{(-1)^{n/2} dL}{r}\right) = -1.$$

From this, follows the lemma, for otherwise we may choose a prime r such that r is a primitive root modulo q and $\left(\dfrac{(-1)^{n/2}dL}{r}\right) = 1$. $\square$

For a lattice L and $\sigma \in O(L)$, we set

$$L(\sigma) = \{x \in L^{\#} \mid \sigma(x) - x \in L\},$$

where $L^{\#}$ is the dual lattice of L. Then $L(\sigma)$ is a sublattice of $L^{\#}$ containing L. We define

$$O^{\#}(L) = \{\sigma \in O(L) \mid L(\sigma) = L^{\#}\}.$$

Then $O^{\#}(L)$ is a normal subgroup of $O(L)$. Note that every symmetry with respect to a minimal vector of L is a member of $O^{\#}(L)$.

Lemma 2.3. *Let L be a primal $\mathbb{Z}$-lattice. Then $O(L)$ is isomorphic to $O^{\#}(L) \oplus \mathbb{Z}/2\mathbb{Z}$, where the generator of $\mathbb{Z}/2\mathbb{Z}$ is -1.*

Proof. By [26], 81:11, there exists a basis $\{e_1, e_2, \ldots, e_n\}$ satisfying the following:

$$L^{\#} = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1} + \mathbb{Z}\frac{1}{\delta p}e_n,$$
$$L = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1} + \mathbb{Z}e_n,$$

where $dL = \delta p$. The element $\sigma \in O(L) \setminus O^{\#}(L)$ induces a nontrivial group isomorphism

$$\sigma : L^{\#}/L \longrightarrow L^{\#}/L,$$

where $L^{\#}/L \simeq \mathbb{Z}/\delta p\mathbb{Z}$. Let $\sigma(e_n) = \delta p x + a e_n$ for $x \in \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_{n-1}$ and $a \in \mathbb{Z}$. We may assume that $(\delta p, a) = 1$ and $a \not\equiv 1 \pmod{\delta p}$. If $Q(e_n) \equiv 0 \pmod{p^2}$, then $B(e_n, L) \subseteq p\mathbb{Z}$ implies that p^2 divides dL, which is absurd. So, $Q(e_n) \not\equiv 0 \pmod{p^2}$. Similarly, $Q(e_n) \not\equiv 0 \pmod{4}$. Since $Q(e_n) \equiv 0 \pmod{\delta p}$ and $Q(e_n) = Q(\sigma(e_n)) = \delta^2p^2Q(x) + 2\delta paB(x, e_n) + a^2Q(e_n)$, we have $(1 - a^2)Q(e_n) \equiv 0 \pmod{\delta^2p^2}$ and hence $1 - a^2 \equiv 0 \pmod{\delta p}$. Therefore $a \equiv -1 \pmod{\delta p}$, which implies $-\sigma \in O^{\#}(L)$ as desired. $\square$

§3. $\mathbb{Z}[\theta]$-modules

Throughout this section, we assume that q is an odd prime such that the class number of $\mathbb{Q}(\theta)$ is 1, where θ is a primitive q-th root of unity. Let $\mathbb{Z}[\theta]$ be the group ring over $\mathbb{Z}$ of the cyclic group $\langle\theta\rangle$. Every $\mathbb{Z}[\theta]$-module is isomorphic to a direct sum of $(\mathbb{Z}[\theta], 1)$, $\mathbb{Z}[\theta]$ and $\mathbb{Z}$, whose $\mathbb{Z}[\theta]$-module structures are as described in [10]. If an element $\sigma \in O(L)$ is of order q, then L has a natural $\mathbb{Z}[\sigma]$-module structure, where $\mathbb{Z}[\sigma]$ again denotes the group ring over $\mathbb{Z}$ of the cyclic group $\langle\sigma\rangle$. Since $\mathbb{Z}[\sigma]$ is isomorphic to $\mathbb{Z}[\theta]$ as a ring, we may regard L as a $\mathbb{Z}[\theta]$-module. In this section, we investigate the structure of L via the structure of L as a $\mathbb{Z}[\sigma]$-module.

Proposition 3.1. *Let $\sigma \in O(L)$ be of order q. If L is isomorphic to $\bigoplus_{i=1}^{b} \mathbb{Z}[\theta]$ as a $\mathbb{Z}[\theta] \simeq \mathbb{Z}[\sigma]$ module, then $dL = q^{\epsilon(b)} \times$ (a square), where $\epsilon(b) = 0$ or 1 according to b even or odd, respectively. Furthermore, if $2 \in Q(L)$, then L represents the root lattice A_{q-1}.*

Proof. Lemma 2.2 tells the first assertion is true for $b = 1$. We use induction on b. Assume that the submodule $K = \bigoplus_{i=1}^{b-1} \mathbb{Z}[\theta]$ of L satisfies the assertion. Since we may regard the isometry σ as an element of $O(K^{\perp})$, we have $dK^{\perp} = q \times$ (a square) and hence $d(K \perp K^{\perp}) = q^{\epsilon(b)} \times$ (a square), which proves the first assertion.

We now assume that $Q(e) = 2$ for some $e \in L$. Then the sublattice $R = \mathbb{Z}e + \mathbb{Z}\sigma(e) + \mathbb{Z}\sigma^2(e) \cdots + \mathbb{Z}\sigma^{q-2}(e)$ of L is a root lattice. Since $\sum_{i=0}^{q-1} \sigma^i = 0$, we may regard σ as an isometry of R of order q. Therefore from Lemma 2.2 can be deduced that R is isometric to A_{q-1}. $\square$

Let $\sigma \in O(L)$ be of order q. If

$$L \simeq \left[\bigoplus_{i=1}^{a} (\mathbb{Z}[\theta], 1)\right] \bigoplus \left[\bigoplus_{j=1}^{b} \mathbb{Z}[\theta]\right] \bigoplus \left[\bigoplus_{k=1}^{c} \mathbb{Z}\right],$$

as $\mathbb{Z}[\theta] \simeq \mathbb{Z}[\sigma]$-modules, then the pair (L, σ) is said to be of *type* $(q; a, b, c)$.

Proposition 3.2. *Let L be a primal lattice and Let $\sigma \in O(L)$ such that (L, σ) is of type $(q; a, b, c)$. Then L has a sublattice K with rank $(a+b)(q-1)$ and $dK = q^s$, where $\epsilon(s) = \epsilon(a+b)$, $s \leq a$ (or $s \leq a+1$) if $q \nmid dL$ (or $q \mid dL$, respectively).*

Proof. By taking a suitable basis of L, we may write L in the following form:

$$L = \left[\bigoplus_{i=1}^{a} (\mathbb{Z}e_{i1} + \cdots + \mathbb{Z}e_{iq})\right] \bigoplus \left[\bigoplus_{j=1}^{b} (\mathbb{Z}f_{j1} + \cdots + \mathbb{Z}f_{j,q-1})\right] \bigoplus \left[\bigoplus_{k=1}^{c} \mathbb{Z}x_k\right],$$

where $\sigma(e_{it}) = e_{i,t+1}$, $\sigma(f_{jt}) = f_{j,t+1}$ for $1 \leqq t \leqq q-2$; $\sigma(e_{i,q-1}) = -\sum_{t=1}^{q-1} e_{it}$, $\sigma(f_{j,q-1}) = -\sum_{t=1}^{q-1} f_{jt}$; $\sigma(e_{iq}) = e_{i1} + e_{iq}$; and $\sigma(x_k) = x_k$ for all $1 \leq i \leq a$, $1 \leq j \leq b$, and $1 \leq k \leq c$.

Let K be the sublattice of L generated by the vectors e_{it}, f_{jt}, for $1 \leq i \leq a$, $1 \leq j \leq b$, and $1 \leq t \leq q-1$. Since $\sigma(K) = K$, we get $dK = q^{\epsilon(a+b)} \times$ (a square) from Proposition 3.1. For a vector $z \in L$, if $\sigma(z) = z$, then $B(z, K) = 0$, i.e., $z \in K^{\perp}$. Let $z_i = \sum_{t=1}^{q-1} (q-t)e_{it} + qe_{iq} \in L$ for $1 \leq i \leq a$. Then $\sigma(z_i) = z_i$ for all i, and hence

$$K^{\perp} = (\mathbb{Z}z_1 + \mathbb{Z}z_2 + \cdots + \mathbb{Z}z_a) + (\mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_c).$$

Since the index $[L : K \perp K^{\perp}] = q^a$, we have $d(K \perp K^{\perp}) = \delta p q^{2a}$. The fact that $B(z_i, K^{\perp}) \in q\mathbb{Z}$ for all i $(1 \leq i \leq a)$ implies that $dK^{\perp}$ is divisible by q^a. So the proposition follows immediately. $\square$

Observe that $dK = q^{a+1}$ may occur only when b is odd and $q \mid dL$. If $a = 0$ and $b, c \neq 0$, then $L = K \perp K^{\perp}$, where $K = \bigoplus_{j=1}^{b}(\mathbb{Z}f_{j1} + \cdots + \mathbb{Z}f_{j,q-1})$ and $K^{\perp} = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_c$.

For $\sigma \in O(L)$, we set

$$L^{\sigma} = \{x \in L \mid \sigma(x) = x\}.$$

Then L^{σ} is a sublattice, called *the σ-fixed sublattice*, of L. The orthogonal complement of L^{σ} in L is called *the σ-variant sublattice* of L and is denoted by L_{σ}. And for a pair (L, σ) of type $(q; a, b, c)$, the triplet $(q; a, b)$ is called *the signature* of L_{σ}. So, the sublattice K of L in Proposition 3.2 is the σ-variant sublattice L_{σ} with the signature $(q; a, b)$.

§4. Primal lattices of lower rank

In this section, we assume that every positive $\mathbb{Z}$-lattice L is an indecomposable primal even (or odd) lattice of rank less than 16 (or 13, respectively) unless stated otherwise. Then every odd prime q dividing $|O(L)|$ is less than or equal to 13, (see, for example, [5] Ch. 13, Example 13) and hence the class number of $\mathbb{Q}(\theta)$ is 1, where θ is a primitive q-th root of unity [31]. The results in the previous section, therefore, are applicable.

The sublattice of L generated by the minimal vectors (of length 2) of L is called *the root sublattice* of L and is denoted by R_L. For a $\mathbb{Z}$-lattice L, its root sublattice R_L is isometric to an orthogonal sum of the followings:

$$A_k \ \ (k \geq 1), \quad D_k \ \ (k \geq 4), \quad E_k \ \ (6 \leq k \leq 8),$$

where A_k, D_k, E_k are root lattices (see [7]). If R is an indecomposable root lattice, then $S(R) = O(R)$ unless $R \simeq D_{2k}$ (see [7],[15]). A root lattice R is said to be *mild* if the isometry -1 is generated by symmetries with respect to the minimal vectors. Otherwise R is said to be *wild*. If R is mild, then R is isometric to a direct sum of the indecomposable root lattices A_1, D_{2k}, E_7 and E_8.

Theorem 4.1. *If an element $\sigma \in O(L)$ is of prime order, then $\sigma \in S(L)$.*

To prove the theorem, we need the following lemma:

Lemma 4.2. *Let $\sigma \in O(L)$ be of order q, where q is a prime. If $\sigma \in O^{\#}(L)$, then $2 \in Q(L_\sigma)$.*

Proof. Notice that q is not necessarily an odd prime here. First, let q be an odd prime. Then from Proposition 3.2 follows that the σ-variant sublattice L_σ is always even. If (L, σ) is of type $(q; a, b, c)$, then $qa + (q-1)b + c \leq 15$. All the possible signature $(q; a, b)$'s of L_σ's, where $a \neq 0$, are listed in (Table 1) below.

$m =$ rank (L_σ)	possible $(q; a, b)$	max (dL_σ)	γ_m
14	$(\mathbf{3}; \mathbf{1}, \mathbf{6})$	3	$2.8020\cdots$
12	$(13; 1, 0), (7; 1, 1), (7; 2, 0)$ $(5; 1, 2), (\mathbf{5}; \mathbf{2}, \mathbf{1}), (5; 3, 0)$ $(3; 1, 5), (3, 2, 4), (3; 3, 3)$	125	$2.5401\cdots$
10	$(11; 1, 0), (3; 1, 4), (3; 2, 3)$ $(3; 3, 2), (\mathbf{3}; \mathbf{4}, \mathbf{1}), (3; 5, 0)$	243	$2.2751\cdots$
8	$(5; 1, 1), (5; 2, 0), (3; 1, 3)$ $(3; 2, 2), (\mathbf{3}; \mathbf{3}, \mathbf{1}), (3; 4, 0)$	81	2
6	$(7; 1, 0), (3; 1, 2), (\mathbf{3}; \mathbf{2}, \mathbf{1})$ $(3; 3, 0)$	27	$\sqrt[6]{64/3}$
4	$(5; 1, 0), (\mathbf{3}; \mathbf{1}, \mathbf{1}), (3; 2, 0)$	9	$\sqrt{2}$
2	$(\mathbf{3}; \mathbf{1}, \mathbf{0})$	3	$2/\sqrt{3}$

(Table 1)

In the table, m is the rank of L_σ, and $\max(dL_\sigma)$ is the possible maximum determinant that can be attained by L_σ's of rank m. Note that for L_σ of signature $(q; a, b)$, the rank is $(a+b)(q-1)$ and the possible maximum determinant is q^a or q^{a+1} according to b even or odd, respectively, by Proposition 3.2. The signature listed in bold face in each row is the one attaining the possible maximum determinant for a given rank m. Suppose $a = 0$. Then $b \neq 0$. Since L is indecomposable, we have $c = 0$. But then $L_\sigma = L$ with $dL_\sigma = q$ and b must be odd by Proposition 3.1. Such lattices, however, cannot provide the possible maximum dL_σ unless $\mathrm{rank}(L) = 2$, in which case another lattice with $a \neq 0$ that attains the possible maximum dL_σ exists. So, we excluded the signature $(q; a, b)$'s with $a = 0$ from the table. Finally, γ_m is the Hermite's constant for $m = 2, 4, 6, 8$ and the Roger's bound for the Hermite's constant for $m = 10, 12, 14$ (see [20],[29]). In all cases, $\gamma_m(\max dL_\sigma)^{1/m} < 4$ and hence we may conclude $2 \in Q(L_\sigma)$.

Now let $q = 2$. Then L may be both even and odd. Since both cases can be proved in a similar manner, we provide a proof only for the case when L is even. If L is odd, then the proof for $2 \in Q(L_\sigma)$ is indeed easier than the even case but requires tedious computation of the determinants of possible L_σ's and Hermite's constants. By a suitable base change, we may write L in the following form:

$$L = (\mathbb{Z}e_1 + \mathbb{Z}f_1) + \cdots + (\mathbb{Z}e_a + \mathbb{Z}f_a) + \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_b + \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_c,$$

where $\sigma(e_i) = f_i$, $\sigma(f_i) = e_i$; $\sigma(y_j) = -y_j$; and $\sigma(x_k) = x_k$ for $1 \le i \le a$, $1 \le j \le b$, and $1 \le k \le c$. Then we get the followings:

$$\begin{aligned} L_\sigma &= \mathbb{Z}(e_1 - f_1) + \cdots + \mathbb{Z}(e_a - f_a) + \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_b, \\ L^\sigma &= \mathbb{Z}(e_1 + f_1) + \cdots + \mathbb{Z}(e_a + f_a) + \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_c. \end{aligned}$$

Let m be a rank of L_σ, i.e., $m = a + b$. From $[L : L_\sigma \perp L^\sigma] = 2^a$ follows $dL_\sigma dL^\sigma = \delta p 4^a$, where $dL = \delta p$. Suppose p divides dL_σ. Then we can find a primitive vector $y \in L_\sigma$ such that $y/p \in L_\sigma^\#$. But then $\sigma(y/p) - y/p = -2y/p \notin L$, which is impossible because $\sigma \in O^\#(L)$. So we may conclude that p divides dL^σ. Both $B(e_i - f_i, L_\sigma)$ and $B(e_i + f_i, L^\sigma)$ are contained in $2\mathbb{Z}$ for all $1 \le i \le a$ and hence both dL_σ and dL^σ are divisible by 2^a. Furthermore, if b (or c) is odd, then dL_σ (or dL^σ, respectively) is divisible by 2^{a+1}. Therefore the possible maximum determinant of L_σ is 2^m, which can be attained when $b = 0$ or 1. If $m \le 7$, then the Minkowski's constant is less than 2 and hence we get $2 \in Q(L_\sigma)$. Let $m = 8$. The possible maximum determinant 2^8 of L_σ occurs only when $a = 7$ and $b = 1$. Suppose $2 \notin Q(L_\sigma)$. Then $L_\sigma \simeq E_8^{(2)}$, where $E_8^{(2)}$ is the lattice obtained from scaling E_8 by 2. From $Q(L_\sigma) \subset 4\mathbb{Z}$ and $Q(e_i + f_i) \equiv Q(e_i - f_i) \pmod 4$ follows that $(L^\sigma)^{(1/2)}$ is even with determinant p. But this cannot happen because $\mathrm{rank}(L^\sigma) = 7$. Therefore $2 \in Q(L_\sigma)$ as desired. Now let $m \ge 9$. From $m \le 15 - a$ follows $d(L_\sigma) \le 2^{16-m}$. Again we can easily get $2 \in Q(L_\sigma)$ by computing $\gamma_m(dL_\sigma)^{1/m}$. $\square$

Proof of Theorem 4.1. We keep the notations from the previous lemma. Note that $\sigma \in O^\#(L)$ if q is odd, and that either $\sigma \in O^\#(L)$ or $-\sigma \in O^\#(L)$ if $q = 2$ (see Lemma 2.3). So $2 \in Q(L_\sigma)$ according to Lemma 4.2. We use induction on $m = (a + b)(q - 1)$. The σ-variant sublattice L_σ contains a sublattice R which is isometric to A_{q-1} by Lemma 3.1. Then $\tau = \sigma|_R \in O(R)$ and hence τ is a product of symmetries with respect to minimal vectors in R. Since every such symmetry can be naturally extended to a symmetry of L, we may conclude that

τ, as an element of $O(L)$, is a product of symmetries of L. Since $\sigma|_R = \tau|_R$ and $\tau|_{R^\perp} = 1_{R^\perp}$, σ and τ^{-1} commute with each other on L. Hence the order of $\sigma\tau^{-1}$ is 1 or q. The rank of $L_{\sigma\tau^{-1}}$ is less than that of L_σ and hence $\sigma\tau^{-1} \in S(L)$ by induction hypothesis. The theorem follows immediately. $\square$

Observe that L_σ has a sublattice isometric to $A_{q-1} \perp A_{q-1} \perp \cdots \perp A_{q-1}$, whose rank is $(a+b)(q-1)$, and that σ is an element of $S(A_{q-1})$ when restricted to each component.

Remark. Lemmas 2.1 and 4.2 imply that $O(L) = \pm 1$ if and only if $2 \notin Q(L)$. For sufficiently large prime p, there always exists a primal lattice L with even rank less than 13 and determinant p such that $O(L) = \pm 1$ (see [1],[2], and [18]).

Every $\sigma \in O(L)$ preserves the minimal vectors. So the map

$$\phi : O(L) \longrightarrow O(R_L) \text{ defined by } \phi(\sigma) = \sigma|_{R_L}$$

is a well defined group homomorphism. The following theorem demonstrates the important role of the root sublattice R_L in shaping the isometry group of L.

Theorem 4.3. (1) *The kernel of ϕ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (or trivial) if R_L is mild (or wild, respectively). In any case, the kernel of ϕ is contained in $S(L)$.*
(2) *The image of ϕ is equal to $S(R_L)$.*

Proof. (1) Since every isometry of odd prime order acts on a suitable sublattice of R_L with no fixed points, the order of $\ker(\phi)$ ought to be of power of 2. Let $\tau \in \ker(\phi)$ with $|\tau| = 2^k$ for $k \geq 1$. If we define $\tau_0 = \tau^{2^{k-1}}$, then $\tau_0 \in \ker(\phi)$ with $|\tau_0| = 2$. By Theorem 4.1, $\tau_0 = \pm\tau_{e_1}\tau_{e_2}\cdots\tau_{e_t}$. If the sign is positive, then $\tau_0 = 1$ because $\tau_0|_{R_L^\perp} = 1_{R_L^\perp}$. Hence -1 is generated by symmetries on R_L, which implies that R_L is mild. Notice that this also implies that ϕ is injective if R_L is wild. Suppose that k is greater than 1, and define $\tau_0' = \tau^{2^{k-2}}$. If we regard τ_0' as an element of $O(R_L^\perp)$, then $(\tau_0')^2 = -1_{R_L^\perp}$, where $R_L^\perp$ is nonempty. But this contradicts Lemma 2.1. Note that $dR_L^\perp | dR_L \cdot dL$ implies that $dR_L^\perp$ is divisible by p but not p^2. So $k = 1$ and hence $\ker(\phi)$ is an elementary 2-group, i.e., $\ker(\phi)$ is isomorphic to a direct sum of d-copies of $\mathbb{Z}/2\mathbb{Z}$ for some d. But every element of order 2 in $\ker(\phi)$ is of the form $-\tau_{f_1}\tau_{f_2}\cdots\tau_{f_t}$ for some mutually orthogonal minimal vectors $f_1, f_2, \ldots, f_t$ in R_L. From this follows $d = 1$, which proves (1).

(2) Suppose that the assertion is false. We fix an element $\tau \in O(L)$ such that $\phi(\tau) \notin S(R_L)$. By multiplying the nontrivial element of $\ker(\phi)$ to τ, if necessary, we may assume that $|\tau| = |\phi(\tau)|$. This is possible because $dR_L^\perp$ is nonsquare and hence the nontrivial element of $\ker(\phi)$ can not be a square of an element of $O(L)$. Let

$$R_L = \perp_{i=1}^{s} (R_{i1} \perp R_{i2} \perp \cdots \perp R_{i,j(i)}),$$

where R_{ij}'s are indecomposable root lattices for $i = 1, 2, \ldots, s$, $j = 1, 2, \ldots, j(i)$ such that R_{ij} and $R_{i'j'}$ are equal if and only if $i = i'$. Then we have [9]

$$O(R_L) = \bigoplus_{i=1}^{s} (O(R_{i1}) \text{ wr } S_{j(i)}),$$

where wr denotes a wreath product and $S_{j(i)}$ is the symmetric group on $j(i)$ letters. Note that $\phi(S(L))$ is contained in $S(R_L)$, which is a normal subgroup of $O(R_L)$. So every symmetry factor of $\phi(\tau)$ can be removed by multiplying a suitable element of $S(L)$ to τ. Therefore, we may assume that $\phi(\tau)$ is a product of λ_i's and μ_{ij}'s, where λ_i is a permutation on $R_{i1}, R_{i2}, \ldots, R_{i,j(i)}$, and μ_{ij} is a graph automorphism of Dynkin-diagram corresponding to R_{ij}. Let $|\tau| = qk$, where q is a prime. Then $\phi(\tau^k) = \phi(\tau)^k$ is still a product of λ_i's and μ_{ij}'s. But this is absurd unless $\phi(\tau^k) = 1$ because $\tau^k \in S(L)$ by Theorem 4.1 and hence $\phi(\tau^k) \in S(R_L)$. However, $\phi(\tau^k) \neq 1$ because $|\tau| = |\phi(\tau)| > k$. This proves the theorem. $\square$

Corollary 4.4. *Let L be a primal lattice, which is not necessarily indecomposable. If L is even (or odd) of rank less than* 16 *(or* 13*, respectively), then $S(L) = O(L)$.*

Proof. The assertion is true for indecomposable primal lattices by Theorem 4.3. So we may assume that L is decomposable. But then,

$$L = (\text{indecomposable primal lattice}) \perp R,$$

where R is one of the following mild root lattices A_1, E_7, E_8, $A_1 \perp E_8$. The result follows immediately. $\square$

Remark. For the lattices L in Corollary 4.4, we can easily deduce from Theorem 4.3 that $|O(L)| = 2|W(R_L)|$, where $W(R_L)$ is the Weyl group of the root lattice R_L. So we can compute the order of the isometry group of a given primal lattice via the Weyl group of its root sublattice. For isometry groups of more general even lattices, see [25].

Corollary 4.5. *$S'(L) = O(L)$ for the lattices L in the previous corollary.*

Proof. Trivial because $S(L) \subset S'(L)$.

Note that Corollary 4.5 fully generalizes Kitaoka's result [16] for primal lattices (see also Theorem 5.1). Furthermore, it removes the parity restriction on primal lattices.

§5. Primal lattices of higher rank

In this section, we investigate general properties of isometry groups of primal lattices of higher rank. See [7] and [8] for notations of $\mathbb{Z}$-lattices constructed by using glue vectors. The following theorem verifies that the bounds for ranks in Theorem 4.3 are the best possible.

Proposition 5.1. *There exists a primal even (or odd) lattice L of rank n such that $S(L) \neq O(L)$ for every $n \geq 16$ (or $n \geq 13$, respectively).*

Proof. Firstly, we prove the case when L is even. Let $n \geq 17$. Consider

$$L = E_8 \perp E_8 \perp K,$$

where K is a primal even lattice of rank $n-16$. Then L is a primal even lattice of rank n and has an isometry σ which exchanges the first two E_8's and fixes K. Clearly, σ is not an element of $S(L)$. For $n = 16$, let

$$L_0 = D_7 D_7 36^{32} 36[10\frac{1}{4}0, 010\frac{1}{4}].$$

Note that $Q(10\frac{1}{4}0) = Q(010\frac{1}{4}) = 4$ and $dL_0 = 17$. So L_0 is a primal even lattice of rank 16. Clearly, the isometry σ_0, which exchanges the two D_7's and $[10\frac{1}{4}0] \mapsto [010\frac{1}{4}]$, $[010\frac{1}{4}] \mapsto [10\frac{1}{4}0]$, is not in $S(L_0)$.

Secondly, we assume that L is odd. If $n \geq 15$, then the lattice

$$L = E_7 E_7[11] \perp K,$$

where K is a primal odd lattice of rank $n-14$, is a desired primal odd lattice of rank n. For $n = 13$ and 14, the lattices

$$E_6 E_6 3[11\frac{1}{3}] \quad \text{and} \quad A_6 A_6 7^0 203[22\frac{1}{7}0, 2(-2)0\frac{1}{7}],$$

respectively, are desired ones. $\square$

Observe that Lemma 4.2 fails when $q = 2$ and the rank is 16. Indeed, for L_0 and σ_0 in the above, we have $(L_0)_{\sigma_0} \simeq E_8^{(2)}$ and hence $2 \notin Q((L_0)_{\sigma_0})$.

Recall that $S'(L)$ is the subgroup of $O(L)$ generated by -1 and symmetries of L. In general, $S(L)$ is not equal to $S'(L)$. The following Theorem provides a useful criterion for determining when $S(L) = S'(L)$ holds for primal lattices L.

Theorem 5.2. *For a primal lattice L, $S(L) \neq S'(L)$ if and only if there exists a sublattice K of L of corank 1 such that $dK = 1$ or 2 when L is a primal odd lattice, $dK = 2$ when L is a primal even lattice of even rank, $dK = 1$ or 4 when L is a primal even lattice of odd rank, and the root lattice R_K of K is either wild or* $\operatorname{rank}(R_K) < \operatorname{rank}(K)$.

Proof. Since the proofs for even and odd cases are quite similar, we prove only for the even case. Assume that $S(L) \neq S'(L)$. Let $\tau_e \in S'(L) \setminus S(L)$, where e is a primitive vector of L. Then we may write $L = \mathbb{Z}e + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n$. From $dL = \delta p$ and $\dfrac{2B(e,L)}{Q(e)} \subset \mathbb{Z}$ follows $B(e, e_j) \equiv 0 \pmod p$ for $j = 2, 3, \ldots, n$ and hence the only possible value of $Q(e)$ is $2p$. For $\tilde{L} = \mathbb{Z}e + \mathbb{Z}2e_2 + \cdots + \mathbb{Z}2e_n$, we have

$$\tilde{L} \subset \mathbb{Z}e \perp K \subset L,$$

where $K = (\mathbb{Z}e)^{\perp}$ in L. Therefore the index $[L : \mathbb{Z}e \perp K]$ is equal to 2^m for some integer m. So $dK = 2$ if the rank of L is even, and $dK = 1$ or 4 if the rank of L is odd. This again follows from $dK | 2p \cdot dL$. Furthermore, since $\tau_e \notin S(L)$, the root sublattice R_K of K cannot be mild with $\operatorname{rank}(R_K) = \operatorname{rank}(K)$.

Conversely, assume that K satisfies the given conditions. Let $\mathbb{Z}e = K^{\perp}$. Then from $Q(e) | dK \cdot dL$ follow that $Q(e) = 2p$ if the rank of L is even and that $Q(e) = 2p$ or $8p$ if the rank of L is odd. We may assume that K is not unimodular. Suppose $Q(e) = 8p$. Then $dK = 4$ and $[L : K \perp \mathbb{Z}e] = 4$. So there exists a primitive vector $y \in K$ and an odd integer a such that $(y + ae)/2 \in L$. Note that $Q(y) \equiv 0 \pmod 8$. Since y is still a primitive vector in L and dL is not divisible by 4, there exists a vector $e' \in L$ such that $B(y, e') \equiv 1 \pmod 2$. Hence $B(e, e') \equiv 1 \pmod 2$. Let $e' = y' + be$, where $y' \in \mathbb{Q}K$ and $b \in (1/2)\mathbb{Z}$. Then $8b \equiv 1 \pmod 2$, which is impossible. Therefore $Q(e) = 2p$ in any case and hence $\tau_e \in S'(L) \setminus S(L)$. $\square$

As a corollary of the above theorem, we obtain the following result (see also [11] and [30]).

Corollary 5.3. *Let L be a primal even lattice of rank n. If $n \equiv 4, 5, 6 \pmod 8$, then $S(L) = S'(L)$.*

Proof. Let n be even such that $n - 1 \equiv 3, 5 \pmod 8$. Suppose that K is a lattice of rank $n - 1$ with $dK = 2$. Then for all odd prime r, the r-adic Hasse symbol $S_r(K) = 1$ and hence $S_2(K) = 1$ by Hilbert's Reciprocity Law. Since K is even, we have the following decomposition:

$$K_2 = \text{ (even unmodular of rank } n-2 \text{ with determinant } q) \perp < 2q >$$

for some odd prime q, where K_2 is the 2-adic localization of K. Note that the 2-adic Hasse symbol of an even unimodular lattice of rank n with determinant q is $(-1)^{n(n+6)/8}\left(\frac{-2}{q}\right)$. So, $S_2(K) = -1$ for $n-1 \equiv 3,5 \pmod 8$, which is a contradiction. So no such K exists and hence $S(L) = S'(L)$ by Theorem 5.2.

Now let n be odd such that $n-1 \equiv 4 \pmod 8$. Since the rank of an even unimodular lattice is divisible by 8, L does not contain a unimodular sublattice of corank 1. Suppose that L contains a sublattice of corank 1 with determinant 4. Since $S_r(L) = 1$ for all prime $r \neq 2, p$ and $S_p(L) = \left(\frac{-1}{p}\right)$, we have $S_2(L) = \left(\frac{-1}{p}\right)$, where $dL = 2p$. But since L is even, we have the following decomposition:

$$L_2 = \text{ (even unimodular of rank } n-1 \text{ with determinant } q) \perp <2pq> .$$

But then $S_2(L) = -\left(\frac{-1}{p}\right)$, which is absurd. Again from Theorem 5.2 follows $S(L) = S'(L)$. $\square$

Corollary 5.4. *Let L be a primal even (or odd) lattice of rank n less than* 17 *(or* 15*, respectively). Then $S(L) = S'(L)$. Furthermore, the bounds* 17 *and* 15 *of ranks are extremal in both cases.*

Proof. By Corollary 4.4, we may assume that $n = 16$ (or 13 and 14) if L is even (or odd, respectively). The only odd lattices with rank 12 or 13 and determinant 1 or 2 are

$$D_{12}[1], \quad E_7D_6[11], \quad D_{12}[1] \perp A_1,$$

and the only even lattices with rank 15 and determinant 2 are

$$E_8 \perp E_7, \quad D_{14}A_1[11].$$

Since the root sublattice of each of these lattices is mild with full rank, we get $S(L) = S'(L)$ from Theorem 5.2. In order to show that the bounds of ranks are extremal, we define

$$L_1 = K_1 \perp \mathbb{Z}y_1 + \mathbb{Z}(\frac{x_1+y_1}{2}) \quad \text{with} \quad K_1 = A_{13}7[4\frac{1}{7}],$$
$$L_2 = K_2 \perp \mathbb{Z}y_2 + \mathbb{Z}(\frac{x_2+y_2}{2}) \quad \text{with} \quad K_2 = A_{15}16[6\frac{1}{8}],$$

where $Q(y_i) = 2p$, and $x_i/2 \in K_i^{\#}$ such that $Q(x_i) \equiv 2 \pmod 4$ for $i = 1, 2$. Note that $dK_1 = 2$ and $dK_2 = 4$. Since $Q(x_i) \equiv 2 \pmod 4$, we can take a suitable prime p such that $Q(x_i + y_i) \in 8\mathbb{Z}$. Then L_1 (or L_2) is an odd (or even, respectively) lattice of rank 15 (or 17, respectively) with determinant p (or $2p$, respectively) and $\tau_{y_i} \notin S(L)$ for $i = 1, 2$. $\square$

References

[1] Bannai, E., *Positive definite unimodular lattices with trivial automorphism groups*, Ph.D. Dissertation, Ohio State Univ., 1988.

[2] Biermann, J., *Gitter mit keiner Automorphismen Gruppe in Geschlechten von* **Z***-Gittern mit positiv-definiter quadratischer Formen*, Ph.D. Dissertation, Göttingen, 1981.

[3] Blaschke, B., Scharlau, R., *Reflective integral lattices*, J. of algebra **181** (1996), 934-961.

[4] Carlitz, L., *Representations by quadratic forms in a finite field*, Duke Math. J. **21** (1954), 123-137.

[5] Cassels, J.W.S., *Rational quadratic forms*, Academic Press, 1978.

[6] Conway, J.H., *A group of order* $8,315,553,613,086,720,000$, Bull. London Math. Soc. **1** (1969), 79-88.

[7] Conway, J.H., Sloane, N.J.A., *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[8] ———, *Low dimensional lattices. I. Quadratic forms of small determinant*, Proc. R. Soc. Lond. A **418** (1988), 17-41.

[9] ———, *Low dimensional lattices. II. Subgroups of* $GL(n, \mathbb{Z})$, Proc. R. Soc. Lond. A **419** (1988), 29-68.

[10] Curtis, C.W., Reiner, I., *Representation theory of finite groups and associative algebras*, Interscience Pub., 1962.

[11] Esselmann, F., *Über die maximale dimension von Lorentz-Gittern mit coendlich spiegelungsgruppe*, J. Number Theory **61** (1996), 103-144.

[12] Hemkemeier, B., Scharlau, R., *Classification of integral lattices with large class number*, Math. of Comp. **67** (1998), 74-144.

[13] Hsia, J.S., Hung, D.C., *Theta series of ternary and quaternary quadratic forms*, Invent. Math. **73** (1983), 167-175.

[14] ———, *Theta series of quaternary quadratic forms over* $\mathbb{Z}$ *and* $\mathbb{Z}[(1+\sqrt{p})/2]$, Acta Arith. **45** (1985), 75-91.

[15] Humphreys, J.E., *Reflection groups and Coxeter groups*, Cambridge University Press, 1992.

[16] Kitaoka, Y., *Quaternary even positive definite quadratic forms of prime discriminant*, Nagoya Math J. **52** (1973), 147-161.

[17] ———, *Class numbers of positive definite quinary quadratic forms*, Japan J. Math. **1** (1975), 85-100.

[18] ———, *Two theorems on the class number of positive definite quadratic forms*, Nagoya Math. J. **51** (1973), 79-89.

[19] ———, *Arithmetic of quadratic forms*, Cambridge University Press, 1993.

[20] Leech, J., *Notes on sphere packings*, Canad. J. Math. **19** (1967), 251-267.

[21] Mennicke, J., *On the group of units of ternary quadratic forms with rational coefficients*, Proc. Roy. Soc. Edinburgh A **67** (1967), 309-352.

[22] Nebe, G., Plesken, P., *Finite rational matrix group of degree* 16, Memoirs of the A.M.S. **116 (556)** (1995), 74-144.

[23] Plesken, P., Nebe, G., *Finite rational matrix groups*, Memoirs of the A.M.S. **116 (556)** (1995), 1-73.

[24] Newman, M., *Integral matrices*, Academic Press, 1972.

[25] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izvestija **14 No1.** (1980), 103-167.

[26] O'Meara, O.T., *Introduction to quadratic forms*, Springer-Verlag, 1973.

[27] Quebbemann, H.G., *Zur klassifikation unimodularer gitter mit isometrie von primzahlornung*, J. reine angew. Math. **326** (1981), 158-170.

[28] ———, *Unimodular lattices with isometries of large prime order II*, Math. Nachr. **156** (1992), 219-224.

[29] Rogers, C.A., *Packing and covering*, Cambridge University Press, 1964.

[30] Vinberg, E.B., *On the group of units of certian quadratic forms*, Math. USSR Sb. **16** (1972), 17-35.

[31] Washington, L., *Introduction to cyclotomic fields*, Springer-Verlag, 1982.