Bounds for Quadratic Waring's Problem

Myung-Hwan Kim* and Byeong-Kweon Oh†

*School of Mathematics, Seoul National University
Seoul 151-742, Korea. E-mail: mhkim@math.snu.ac.kr
†School of Mathematics, Korea Institute for Advanced Study
Seoul 130-012, Korea. E-mail: bkoh@math.kias.re.kr

Abstract

Let $g[n]$ be the minimum number of squares whose sum represents all positive definite integral quadratic forms of rank n that are representable by sums of squares. Mordell called the problem of determining the values of $g[n]$ for all n the *new Waring's Problem*. The values of $g[n]$ are known for $1 \leq n \leq 6$. In this article, we provide upper and lower bounds of $g[n]$ for $7 \leq n \leq 20$.

1 Introduction

In 1770, Lagrange [L] proved the famous four square theorem, i.e., for every positive integer n, there exists an integer solution of the equation

$$x^2 + y^2 + z^2 + w^2 = n.$$

After Lagrange, this theorem was generalized in many directions. One interesting generalization is so called the *new* (or *quadratic*) *Waring's problem*

*The first author was supported in part by KOSEF Research Fund(99-0701-01-5-2). AMS Subject Classification (2000): 11E12, 11E06. Keywords: quadratic Waring's problem, representations by sums of squares.

due to L. J. Mordell [M1], which is about sums of squares that represent all positive integral quadratic forms of given rank. In particular, Mordell proved that every binary positive integral quadratic form can be represented by the sum of five squares. Later, C. Ko [K1] proved that every ternary (quaternary or quinary) positive integral quadratic form can be represented by a sum of six (seven or eight, respectively) squares. So, they naturally expected that every positive n-ary integral quadratic form can be represented by a sum of $(n+3)$ squares. This, however, turned out to be false. The quadratic form defined by the root lattice E_6 cannot be represented by sums of squares (see [M2], [CS2] and [Pl]). After Mordell found this, they tried to determine the minimum number $g[n]$ of squares whose sum represents all positive integral quadratic forms of rank n that are representable by sums of squares.

We adopt lattice theoretic language. A $\mathbb{Z}$-*lattice* L is a finitely generated free $\mathbb{Z}$-module in $\mathbb{R}^n$ equipped with a non-degenerate symmetric bilinear form B such that $B(L,L) \subset \mathbb{Z}$. The corresponding quadratic map is denoted by Q, i.e., $Q(\mathbf{e}) = B(\mathbf{e},\mathbf{e})$ for every $\mathbf{e} \in L$. The ideal of $\mathbb{Z}$ generated by $B(\mathbf{e}_i,\mathbf{e}_j)$'s is called the *scale* of L, denoted by $\mathfrak{s}(L)$. For a $\mathbb{Z}$-lattice

$$L = \mathbb{Z}\mathbf{e}_1 + \mathbb{Z}\mathbf{e}_2 + \cdots + \mathbb{Z}\mathbf{e}_m$$

with basis $\{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_m\}$, we define its corresponding matrix

$$M_L := (B(\mathbf{e}_i,\mathbf{e}_j)),$$

which is an $m \times m$ symmetric integer matrix. We often identify a $\mathbb{Z}$-*lattice* L with its corresponding matrix M_L. If M_L is diagonal, we often write

$$L = \langle Q(\mathbf{e}_1), Q(\mathbf{e}_2), \cdots, Q(\mathbf{e}_n)\rangle = \langle Q(\mathbf{e}_1)\rangle \perp \langle Q(\mathbf{e}_2)\rangle \perp \cdots \perp \langle Q(\mathbf{e}_n)\rangle.$$

For $a \in \mathbb{R}^\times$, we let

$$aL := \mathbb{Z}(a\mathbf{e}_1) + \mathbb{Z}(a\mathbf{e}_2) + \cdots + \mathbb{Z}(a\mathbf{e}_n).$$

The lattice $\mathbb{Z}^n$ equipped with the standard inner product is denoted by I_n. A $\mathbb{Z}$-lattice L is said to be *positive definite* or simply *positive* if $Q(\mathbf{e}) > 0$ for every $\mathbf{e} \in L, \mathbf{e} \neq \mathbf{0}$. In this paper, we always assume the following unless stated otherwise:

$$\textit{Every } \mathbb{Z}\textit{-lattice is positive definite.} \tag{1}$$

A $\mathbb{Z}$-*lattice* L is said to be *even* when $Q(L) \subset 2\mathbb{Z}$, and *odd*, otherwise. As usual,

$$\det L := \det(B(\mathbf{e}_i, \mathbf{e}_j))$$

is called the *discriminant* of L. A $\mathbb{Z}$-lattice L is said to be *unimodular* if $\det L = 1$. For a $\mathbb{Z}$-lattice L and a prime p,

$$L_p := \mathbb{Z}_p L = \mathbb{Z}_p \otimes_{\mathbb{Z}} L$$

is a $\mathbb{Z}_p$-lattice called the *localization* of L at p, where $\mathbb{Z}_p$ is the p-adic integer ring.

Let ℓ, L be $\mathbb{Z}$-lattices. We say that L *represents* ℓ if there is an injective $\mathbb{Z}$-linear map from ℓ into L that preserves the bilinear forms, and write $\ell \to L$. Such a map is called a *representation*. A representation is called an *isometry* if it is surjective. We say that ℓ and L are *isometric* and write $\ell \cong L$ if there exists an isometry between them. For a $\mathbb{Z}$-lattice L, we define the *class* and *genus* of L by

$$\begin{aligned} \operatorname{cls}(L) &:= \{\, K : \mathbb{Z}\text{-lattice} \,|\, K \simeq L \text{ over } \mathbb{Z} \,\}, \\ \operatorname{gen}(L) &:= \{\, K : \mathbb{Z}\text{-lattice} \,|\, K_p \simeq L_p \text{ over } \mathbb{Z}_p \ \text{ for all } p \,\}. \end{aligned}$$

It is well known that $\operatorname{gen}(L)$ contains a finite number of distinct classes. This number is called the *class number* of L, denoted by $h(L)$. If $\ell_p \to L_p$ for all p, or equivalently $\ell \to \operatorname{gen}(L)$, then it is known that $\ell \to K$ for some $K \in \operatorname{gen}(L)$.

Let

$$\mathfrak{S}_n := \{\, \ell : \mathbb{Z}\text{-lattices} \mid \ell \to I_g \ \text{ for some } g,\, \operatorname{rank}(\ell) = n \,\},$$

and

$$g[n] := \min\{\, g \mid \ell \to I_g \ \text{ for every } \ell \in \mathfrak{S}_n \,\}. \tag{2}$$

Applying the results in [HKK], one can easily prove that $g[n]$ exists for all n. The four square theorem of Lagrange, and the results of Mordell's and Ko's mentioned above can be summarized as the following:

$$g[n] = n + 3 \ \text{ for } 1 \le n \le 5. \tag{3}$$

In fact, this is an immediate consequence of the fact that the class number of I_n is 1 for $1 \le n \le 8$ and the local representation theory. The following question arises quite naturally:

$$g[n] = n + 3 \ \ \textit{for all} \ \ n \geq 1 \ ?$$

Concerning this question, Ko conjectured in [K2] that $g_{\mathbb{Z}}[6] = 9$. However, the authors proved recently [KO1,2] that

$$g[n] \geq \lfloor 3n/2 \rfloor + 1 > n + 3 \ \text{ for all } n \geq 6, \quad \text{and} \quad g[6] = 10. \tag{4}$$

The first explicit upper bound for $g[n]$ was given by Icaza [Ic]. She obtained her bound by computing the so called HKK-constant. But her bound is huge containing a factor

$$n^{n+1} 2^{\,4h(I_{n+3})},$$

where $h(I_n) = n^{\Theta(n^2)}$. Recently, the authors improved the bounds of $g[n]$ for $n \geq 14$:

$$2n - \lceil \log_2 n \rceil - 2 \leq g[n] \leq 3 \cdot 3^{n/2}\, \tau_{n+3} + n + 4, \tag{5}$$

where

$$\tau_k := \sum_{i=17}^{k} \lfloor 2 \log_2 i \rfloor - k + 18 = O(k \log k)$$

for $k \geq 17$ (see [KO3]). As for small n's, Oh [Oh] proved

$$g[n] \leq n(n+1)/2 + n + 3 \tag{6}$$

for $7 \leq n \leq 11$, and Sasaki [Sa] recently proved:

$$g[n] \leq \begin{cases} 2 \cdot 3^n + n + 6 & \text{for } 12 \leq n \leq 13, \\ 3 \cdot 4^n + n + 3 & \text{for } 14 \leq n \leq 20, \end{cases} \quad \text{and} \quad g[7] \leq 25. \tag{7}$$

In this article, we provide sharper bounds of $g[n]$ for $12 \leq n \leq 20$. More precisely, we prove

$$g[n] \leq 5n^3/2 \tag{8}$$

for $12 \leq n \leq 20$. We also prove

$$11 \leq g[7] \leq 24 \ \text{ and } \ 13 \leq g[8] \leq 37. \tag{9}$$

For unexplained terminology, notation, and basic facts about $\mathbb{Z}$-lattices, we refer the readers to O'Meara [O'M1], Conway and Sloane [CS1].

2 Lemmas

Let $\ell = \mathbb{Z}\mathbf{x}_1 + \mathbb{Z}\mathbf{x}_2 + \cdots + \mathbb{Z}\mathbf{x}_n \subset I_g$ be a $\mathbb{Z}$-lattice, where $\mathbf{x}_i = (a_{i1}, a_{i2}, \cdots, a_{ig})$ for $1 \leq i \leq n$. For $1 \leq j \leq g$, define

$$\mathbf{v}_j := {}^t(a_{1j}, a_{2j}, \cdots, a_{nj}),$$

where ${}^tA$ is the transpose of a matrix or a vector A. Since these $\mathbf{v}_j$'s also characterize ℓ, we may write

$$\ell = S_n(\mathbf{v}_1, \mathbf{v}_2, \cdots \mathbf{v}_g) \subset I_g. \tag{10}$$

Note that for positive integers $s_1, s_2, \cdots, s_g$,

$$\tilde{\ell} = S_n(\overbrace{\mathbf{v}_1, \cdots \mathbf{v}_1}^{s_1 \text{ times}}, \overbrace{\mathbf{v}_2, \cdots \mathbf{v}_2}^{s_2 \text{ times}}, \cdots, \overbrace{\mathbf{v}_g, \cdots \mathbf{v}_g}^{s_g \text{ times}}) \subset I_{s_1+s_2+\cdots+s_g}$$

of rank n is represented by the $\mathbb{Z}$-lattice $\langle s_1 \rangle \perp \langle s_2 \rangle \perp \cdots \perp \langle s_g \rangle$ of rank g.

A $\mathbb{Z}$-lattice ℓ of rank n is said to be *s-integrable* if $\sqrt{s}\ell$ can be represented by a sum of squares, i.e., $\sqrt{s}\ell \in \mathfrak{S}_n$, where s is a positive integer. Define

$$\phi(s) := \min\{\, n \mid \exists \text{ a } \mathbb{Z}\text{-lattice } \ell \text{ of rank } n \text{ such that } \sqrt{s}\ell \notin \mathfrak{S}_n \,\}. \tag{11}$$

It is known [CS2], [KO3] that

$$\phi(1) = 6,\ \phi(2) = 12,\ \phi(3) = 14,\ \cdots \tag{12}$$

and that for large enough s,

$$\phi(s) > \frac{\ln s}{8 \ln \ln s}. \tag{13}$$

Let $\mathbb{F}_2 = \{0, 1\}$ be the field of 2 elements and $Sym_n(\mathbb{F}_2)$ be the set of all $n \times n$ symmetric matrices over $\mathbb{F}_2$. For a vector $\mathbf{a} = (a_1, a_2, \cdots, a_g) \in \mathbb{F}_2^g$, we define $wt(\mathbf{a})$, the *weight* of $\mathbf{a}$, to be the number of indices i such that $a_i = 1$.

Lemma 2.1 *Let V be an m-dimensional subspace of $\mathbb{F}_2^g$. Then there exist $\mathbf{x} \in V$ such that $wt(\mathbf{x}) \geq m$.*
Proof. Trivial.

Let $\ell = S_n(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_g) \subset I_g$ be a $\mathbb{Z}$-sublattice of rank n. Let $H = \{ i_1, i_2, \cdots, i_h \} \subset G = \{1, 2, \cdots, g\}$. We define

$$\ell_H := S_n(\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \cdots, \mathbf{v}_{i_h}) \subset I_h. \tag{14}$$

Note that the rank of ℓ_H is obviously less than or equal to $\min\{n, h\}$ and that ℓ_H is not necessarily a sublattice of ℓ.

Lemma 2.2 *For a sublattice $\ell \subset I_g$ of rank n with $g > n(n+1)/2$, there exists an $H \subset G$ such that*

$$|H| \leq \frac{n(n+1)}{2} \quad \textit{and} \quad \mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z},$$

where H' is the complement of H in G.

Proof. Put $\ell = S_n(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_g)$, where $\mathbf{v}_j = {}^t(a_{1j}, a_{2j}, \cdots, a_{nj})$. We define a group homomorphism

$$\Phi(\ell) : \ \mathbb{F}_2^g \longrightarrow Sym_n(\mathbb{F}_2) \tag{15}$$

such that the (i,j)-entry of $\Phi(\ell)(s_1, s_2, \cdots, s_g)$ is $\sum_{k=1}^{g} s_k a_{ik} a_{jk}$ (mod 2) for all $1 \leq i, j \leq n$. Note that if we let

$$V_\ell = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1g} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{ng} \end{pmatrix},$$

then

$$\Phi(\ell)(s_1, s_2, \cdots, s_g) \equiv V_\ell \begin{pmatrix} s_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & s_g \end{pmatrix} {}^tV_\ell \pmod 2.$$

Since $\dim(Sym_n(\mathbb{F}_2)) = n(n+1)/2$, we get

$$\dim(\ker(\Phi(\ell))) \geq g - (n(n+1)/2).$$

Hence there exists an $\mathbf{x} \in \ker(\Phi(\ell))$ such that

$$wt(\mathbf{x}) \geq g - (n(n+1)/2)$$

by Lemma 2.1. Let H be the set of all indices i for which the i-th component of $\mathbf{x}$ is zero. Then $|H| \le n(n+1)/2$ and $\mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z}$ as desired.

Any sublattice ℓ of $L \perp M$ is of the form

$$\ell = \mathbb{Z}(\mathbf{x}_1 + \mathbf{y}_1) + \mathbb{Z}(\mathbf{x}_2 + \mathbf{y}_2) + \cdots + \mathbb{Z}(\mathbf{x}_n + \mathbf{y}_n)$$

for $\mathbf{x}_i \in L$ and $\mathbf{y}_i \in M$. We define sublattices

$$\begin{aligned} \ell(L) \quad &:= \mathbb{Z}\mathbf{x}_1 + \mathbb{Z}\mathbf{x}_2 + \cdots + \mathbb{Z}\mathbf{x}_n \quad \subset L \\ \ell(M) \quad &:= \mathbb{Z}\mathbf{y}_1 + \mathbb{Z}\mathbf{y}_2 + \cdots + \mathbb{Z}\mathbf{y}_n \quad \subset M. \end{aligned} \tag{16}$$

Even when $\sigma : \ell \to L \perp M$, we use $\ell(L)$ and $\ell(M)$ instead of $\sigma(\ell)(L)$ and $\sigma(\ell)(M)$, respectively, by abuse of notation.

Lemma 2.3 *For $n = 7, 8$, let ℓ be the $\mathbb{Z}$-lattice of rank n such that the rank of the unimodular component of ℓ_2 in 2-adic Jordan decomposition is less than or equal to $11 - n$. Then $\ell \to I_{n+3}$.*

Proof. We prove only for the case when $n = 7$. The other case can be proved in a similar manner. Let $(\ell_2)_0$ be the unimodular component of ℓ_2 in 2-adic Jordan decomposition. If the rank of $(\ell_2)_0 \le 5$ and $\ell \to E_8$, then $\ell \to I_8$ by Theorem 2 of [O'M2]. Recall the following fact:

$$gen(I_{10}) = \{I_{10}, E_8 \perp I_2\}.$$

Since ℓ_p is represented by $(I_{10})_p$ for every p, ℓ is represented by $gen(I_{10})$, which means ℓ is represented by either I_{10} or by $E_8 \perp I_2$. Suppose $\ell \to E_8 \perp I_2$. We may further assume that $\ell = \mathbb{Z}\mathbf{z}_1 + \mathbb{Z}\mathbf{z}_2 + \cdots + \mathbb{Z}\mathbf{z}_7 \subset E_8 \perp I_2$, where $\mathbf{z}_i = \mathbf{x}_i + (a_{i1}\mathbf{e}_1 + a_{i2}\mathbf{e}_2)$ with $\mathbf{x}_i \in E_8, a_{i1}\mathbf{e}_1 + a_{i2}\mathbf{e}_2 \in I_2$ for all i, and that $B(\mathbf{z}_i, \ell) \equiv 0 \pmod 2$ for $1 \le i \le 3$. So, the rank of $(\ell(E_8)_2)_0 \le 5$ and hence $\ell(E_8) \to I_8$. This implies $\ell \to I_{10}$.

3 Bounds of $g[n]$ for $7 \le n \le 20$

In this section, we provide bounds of $g[n]$ for small n's, which improves Sasaki's.

Theorem 3.1 *For* $7 \leq n \leq 11$,

$$g[n] \leq \frac{n(n+1)}{2} + n + 3.$$

Proof. Let $\ell \subset I_g$ be a $\mathbb{Z}$-sublattice of rank n, where $g > n(n+1)/2$. Let H, H' be the subsets of G satisfying the conditions in Lemma 2.2. Since $\phi(2) = 12$, every $\mathbb{Z}$-lattice of rank n is represented by $(1/\sqrt{2})I_{n+3}$. So, $\mathfrak{s}(\ell_{H'}) \subset 2\mathbb{Z}$ implies $\ell_{H'} \to I_{n+3}$. The theorem follows immediately. (See [Oh].)

Note that the above proof cannot be applied to higher ranks because $\phi(2) = 12$. For $12 \leq n \leq 20$, let $\alpha(n), \beta(n)$ be integers satisfying

$$\begin{pmatrix} \alpha(n) \\ 1 \end{pmatrix} + \begin{pmatrix} \alpha(n) \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} \alpha(n) \\ \beta(n) \end{pmatrix} \geq 2^{n(n+1)/2}. \qquad (17)$$

Theorem 3.2 *For* $12 \leq n \leq 20$,

$$g[n] \leq n(n+1)\beta(n) + \alpha(n) + n + 2$$

where $\alpha(n), \beta(n)$ *be any integers satisfying inequality (17).*

Proof. Let $\ell \in \mathfrak{S}_n$ such that $\ell \subset I_g$. Then we may write ℓ as in (10). By (17) and the pigeon hole principle applied to $Sym_n(\mathbb{F}_2)$ via the map $\Phi(\ell)$ of (15), we may assume that

$$\ell = S_n(\mathbf{u}_1, \cdots \mathbf{u}_t, \mathbf{v}_{11}, \cdots, \mathbf{v}_{1j_1}, \cdots, \mathbf{v}_{s1}, \cdots, \mathbf{v}_{sj_s}),$$

where $\mathfrak{s}(S_n(\mathbf{v}_{k1}, \mathbf{v}_{k2}, \cdots, \mathbf{v}_{kj_k})) \subset 2\mathbb{Z}$, $1 \leq j_k \leq 2\beta(n)$ for all $k = 1, \cdots, s$, and $0 \leq t \leq \alpha(n) - 1$. Note that $t + j_1 + \cdots + j_s = g$. Here, s may be 0, which makes $t = g \leq \alpha(n) - 1$. So, we may assume that $s \neq 0$. For each $\ell_k = S_n(\mathbf{v}_{k1}, \mathbf{v}_{k2}, \cdots, \mathbf{v}_{kj_k})$, $1 \leq k \leq s$, we let $2M_k$ be the corresponding symmetric matrix. Define

$$\Phi : \mathbb{F}_2^s \longrightarrow Sym_n(\mathbb{F}_2) \ \text{ by } \ \Phi((\alpha_1, \alpha_2, \cdots, \alpha_s)) = \sum_{k=1}^{s} \alpha_k M_k.$$

Then by a similar reasoning to Lemma 2.2, we may conclude that there exists a subset $K \subset \{(1,1), \cdots, (1, j_1), (2,1), \cdots, (2, j_2), \cdots, (s,1), \cdots, (s, j_s)\}$ such that

$$|K| \leq n(n+1)\beta(n) \ \text{ and } \ \mathfrak{s}((\ell_1 \perp \ell_2 \perp \cdots \perp \ell_s)_{K'}) \subset 4\mathbb{Z},$$

where $\ell_1 \perp \ell_2 \perp \cdots \perp \ell_s = S_n(\mathbf{v}_{11}, \cdots, \mathbf{v}_{1j_1}, \mathbf{v}_{21}, \cdots, \mathbf{v}_{2j_2}, \cdots, \mathbf{v}_{s1}, \cdots, \mathbf{v}_{sj_s})$. Therefore the desired inequality follows from Theorem 18 of [CS2].

Remark. The inequality (17) is satisfied by $\alpha(n) = n^3, \beta(n) = 13n/10$ for $12 \le n \le 20$. So, from Theorem 3.2 follows

$$g[n] < 5n^3/2 \tag{18}$$

for $12 \le n \le 20$.

4 Sharper bounds for $g[7]$ and $g[8]$

In this section, we restrict ourselves to the case when $n = 7$ or 8.

Theorem 4.1

$$11 \le g_{\mathbb{Z}}(7) \le 24.$$

Proof. The lower bound comes from (4). Let $\ell = \mathbb{Z}\mathbf{x}_1 + \mathbb{Z}\mathbf{x}_2 + \cdots + \mathbb{Z}\mathbf{x}_7 \subset I_g$ for sufficiently large g, where $\mathbf{x}_i = (a_{i1}, a_{i2}, \cdots, a_{ig})$ for $1 \le i \le 7$. Let $\mathbf{v}_j = {}^t(a_{1j}, a_{2j}, \cdots, a_{7j})$ for $1 \le j \le g$ so that $\ell = S_7(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_g) \subset I_g$. For a subset $T = \{t_1, t_2, \cdots, t_5\} \subset S = \{1, 2, \cdots, 7\}$, we define a sublattice

$$\ell^T := \mathbb{Z}\mathbf{x}_{t_1} + \mathbb{Z}\mathbf{x}_{t_2} + \cdots + \mathbb{Z}\mathbf{x}_{t_5}$$

of ℓ and let $\mathbf{v}_j^T := {}^t(a_{t_1 j}, a_{t_2 j}, \cdots, a_{t_5 j})$. Then by Lemma 2.2, there exists a subset H such that $|H| \le 15$ and $\mathfrak{s}(\ell^T_{H'}) \subset 2\mathbb{Z}$. Note that $\ell^T_{H'} \subset \ell_{H'}$. After the suitable base change, this implies that

$$M_{\ell_{H'}} \equiv \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & * & * \\ * & * & * & * & * & * & * \\ * & * & * & * & * & * & * \end{pmatrix} \pmod 2.$$

Therefore the rank of unimodular component of $(\ell_{H'})_2$ is less than or equal to 4. Hence by Lemma 2.3,

$$\ell \to \ell_{H'} \perp I_{15} \to I_{25}.$$

We now fix $g = 25$ so that $\ell = S_7(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_{25})$. We may assume that ℓ is the primitive sublattice of I_{25}. Suppose that ℓ is not represented by I_{24}. Then for any subset $T \subset S$ with $|T| = 5$, we have

$$\dim(\Phi(\ell^T)(\mathbb{F}_2^{25})) = 15, \ \dim(\ker(\Phi(\ell^T))) = 10,$$

and the maximal weight among the vectors in $\ker(\Phi)$ must be 10. So, we may further assume that $\Phi(\ell^T)(\mathbf{e}_j)$'s for $1 \le j \le 15$ form a basis of $Sym_5(\mathbb{F}_2)$ and

$$\sum_{k=16}^{25} \Phi(\ell^T)(\mathbf{e}_k) = 0.$$

For each $16 \le k_0 \le 25$,

$$\Phi(\ell^T)(\mathbf{e}_{k_0}) = \sum_{k \ne k_0} \Phi(\ell^T)(\mathbf{e}_k) = \sum_{j=1}^{15} a_j \Phi(\ell^T)(\mathbf{e}_j)$$

implies that $\Phi(\ell^T)(\mathbf{e}_{k_0})$ is either 0 or $\Phi(\ell^T)(\mathbf{e}_j)$ for some $1 \le j \le 15$. Consequently there are exactly 15 distinct nonzero vectors in $\{\mathbf{v}_1^T, \mathbf{v}_2^T, \cdots, \mathbf{v}_{25}^T\}$ (mod 2) and the number of the same nonzero vectors (mod 2) in the set is always odd.

We now show that there exists a set T violating the above condition. Note that $\sum_{r \in R} \mathbf{x}_r \not\equiv \mathbf{0}$ (mod 2) for any subset $R \subset \{1, 2, \cdots, 7\}$. We may choose $T = \{1, 2, \cdots, 5\}$ and assume that $\Phi(\ell^T)(\mathbf{e}_j)$'s for $1 \le j \le 15$ form a basis of $Sym_5(\mathbb{F}_2)$. By a suitable base change and rearrangement, we may assume that for $1 \le j \le 5$

$$\mathbf{v}_j \equiv \mathbf{f}_j, \quad \text{and} \quad \mathbf{v}_{24} \equiv \mathbf{f}_6, \ \mathbf{v}_{25} \equiv \mathbf{f}_7 \pmod 2,$$

where $\mathbf{f}_j$ is the transpose of the j-th standard basis vector of $\mathbb{F}_2^7$.

Figure 4.1

$$
\begin{array}{ll}
\mathbf{x}_1 \equiv 1,0,0,0,0,a_{16},\ \cdots,a_{1,15}\ ;\ a_{1,16},\ \cdots,a_{1,23},0,0 & \pmod 2 \\
\mathbf{x}_2 \equiv 0,1,0,0,0,a_{26},\ \cdots,a_{2,15}\ ;\ a_{2,16},\ \cdots,a_{2,23},0,0 & \pmod 2 \\
\mathbf{x}_3 \equiv 0,0,1,0,0,a_{36},\ \cdots,a_{3,15}\ ;\ a_{3,16},\ \cdots,a_{3,23},0,0 & \pmod 2 \\
\mathbf{x}_4 \equiv 0,0,0,1,0,a_{46},\ \cdots,a_{4,15}\ ;\ a_{4,16},\ \cdots,a_{4,23},0,0 & \pmod 2 \\
\mathbf{x}_5 \equiv 0,0,0,0,1,a_{56},\ \cdots,a_{5,15}\ ;\ a_{5,16},\ \cdots,a_{5,23},0,0 & \pmod 2 \\
\hline
\mathbf{x}_6 \equiv 0,0,0,0,0,a_{66},\ \cdots,a_{6,15}\ ;\ a_{6,16},\ \cdots,a_{6,23},1,0 & \pmod 2 \\
\mathbf{x}_7 \equiv 0,0,0,0,0,a_{76},\ \cdots,a_{7,15}\ ;\ a_{7,16},\ \cdots,a_{7,25},0,1 & \pmod 2
\end{array}
$$

Note that for every j, $6 \leq j \leq 15$, there exists an i, $1 \leq i \leq 4$, such that $a_{ij} \not\equiv 0 \pmod 2$. For each given j, $1 \leq j \leq 5$, the number of k's, $16 \leq k \leq 23$, such that $\mathbf{v}_k^T \equiv \mathbf{f}_j^T \pmod 2$ is even. Hence we may assume that

$$\text{if} \quad a_{5k} \equiv 1 \pmod 2, \quad \text{then} \quad a_{ik} \equiv 1 \pmod 2$$

for at least one i, $1 \leq i \leq 4$. Let a, b, c, d be the numbers of $\mathbf{v}_k$'s, $16 \leq k \leq 23$, such that

$$\mathbf{v}_k = \mathbf{0}, \mathbf{v}_k = \mathbf{f}_6, \mathbf{v}_k = \mathbf{f}_7, \mathbf{v}_k = \mathbf{f}_6 + \mathbf{f}_7,$$

respectively. If we replace $\mathbf{x}_5$ by $\mathbf{x}_5 + \mathbf{x}_6$ or $\mathbf{x}_5 + \mathbf{x}_7$, then the number of j's, $1 \leq j \leq 25$, such that $\mathbf{v}_j^T \equiv \mathbf{f}_5^T \pmod 2$ has to be odd. Therefore

$$a + b + c + d \equiv 0, \quad b + d + 1 \equiv 1, \quad c + d + 1 \equiv 1 \pmod 2. \tag{19}$$

Since (18) holds for any choice of T, either the number of j's such that $\mathbf{v}_j = \mathbf{f}_k$ is always even for any $k, 1 \leq k \leq 7$, or the number of j's such that $\mathbf{v}_j = \mathbf{f}_k$ is always odd for any $k, 1 \leq k \leq 7$ and there exists $\mathbf{v}$ such that $\mathbf{v} = \mathbf{f}_k + \mathbf{f}_l$ for any k, l, $1 \leq k, l \leq 7$. Note that the latter case cannot occur. In the former case, there exists an $H \subset \{1, 2, \cdots, 25\}$ such that $|H| \leq 11$ and $\mathfrak{s}(\ell_{H'})) \subset 2\mathbb{Z}$. This implies $\ell \to I_{21}$, which is not possible either.

Theorem 4.2

$$13 \leq g_{\mathbb{Z}}(8) \leq 37.$$

Proof. The lower bound comes from (4). Let $\ell = S_8(\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_g) \subset I_g$ be of rank 8. Let

$$W := \{M = (m_{ij}) \in Sym_7(\mathbb{F}_2) \mid m_{ij} = 0 \text{ if } (i,j) \neq (7,7)\}.$$

For any subset $T \subset \{1, 2, \cdots, 8\}$ with $|T| = 7$, we can define a linear map

$$\Phi(\ell^T) : \mathbb{F}_2^g \longrightarrow Sym_7(\mathbb{F}_2)/W$$

via factoring the map defined in (15). Note that $\dim(Sym_7(\mathbb{F}_2)/W) = 27$. Then by a similar reasoning as in Lemma 2.2, one can show that there exists a subset $H \subset G = \{1, 2, \cdots, g\}$ with $|H| \leq 27$ such that the rank of unimodular component of $(\ell_{H'})_2$ is less than or equal to 3. Therefore by Lemma 2.3, $\ell_{H'} \to I_{11}$ and hence $\ell \to I_{38}$. The rest (for improving the upper bound by 1) is almost identical to the case when $n = 7$.

References

[CS1] J. H. Conway and N. J. A. Sloane, 'Sphere packings, lattices and groups', Springer-Verlag, 1999.

[CS2] J. H. Conway and N. J. A. Sloane, 'Low dimensional lattices V - Integral coordinates for integral lattices', *Proc. Royal. Soc. London Ser. A* 426 (1989), 211-232.

[HKK] J.S. Hsia, Y. Kitaoka and M. Kneser, 'Representation of positive definite quadratic forms', *J. reine angew. Math.* 301 (1978), 132-141.

[Ic] M. I. Icaza, 'Sums of squares of integral linear forms', , *Acta Arith.* 124 (1996), 231-240.

[K1] C. Ko, 'On the representation of a quadratic form as a sum of squares of linear forms', *Quart. J. Math. Oxford* 8 (1937), 81-98.

[K2] C. Ko, 'On the decomposition of quadratic forms in six variables', *Acta Arith.* 3 (1939), 64-78.

[KO1] M-H. Kim and B.-K. Oh, 'A lower bound for the number of squares whose sum represents integral quadratic forms', *J. Korean Math. Soc.* 33 (1996), 651-655.

[KO2] M-H. Kim and B.-K. Oh, 'Representation of positive definite senary integral quadraticforms by a sum of squares', *J. Number Theory* 63 (1997), 89-100.

[KO3] M-H. Kim and B.-K. Oh, 'Representation of Integral Quadratic Forms by Sums of Squares', *preprint.*

[L] J. L. Lagrange, *Oeuvres* 3 (1869), 189-201.

[M1] L.J. Mordell, 'A new Waring's problem with squares of linear forms', *Quart. J. Math. Oxford* 1 (1930), 276–288.

[M2] L.J. Mordell, 'The representation of a definite quadratic form as a sum of two others', *Ann. Math.* 38 (1937), 751–757.

[Oh] B.-K. Oh, 'On Universal Forms', Ph.D. Thesis, Seoul National Univ., 1999.

[O'M1] O. T. O'Meara, 'Introduction to quadratic forms', Springer-Verlag, 1973.

[O'M2] O. T. O'Meara, 'The integral representations of quadratic forms over local fields', *Amer. J. Math.* 80 (1958), 843-878.

[Pl] W. Plesken, 'Additively indecomposable positive integral quadratic forms', *J. Number Theory* 47 (1994), 273-283.

[Sa] H. Sasaki, 'Sums of Squares of Integral Linear Forms', *J. Austral. Math. Soc. (Series A)* 69 (2000), 298-302.