A LOWER BOUND FOR THE NUMBER OF SQUARES WHOSE SUM REPRESENTS INTEGRAL QUADRATIC FORMS

Myung-Hwan Kim and Byeong-Kweon Oh

Department of Mathematics, Seoul National University, Seoul 151-742, Korea

Abstract. As a generalization of the famous four square theorem of Lagrange, Mordell and Ko proved that every positive definite integral quadratic form of n variables is represented by the sum of $n+3$ squares for $1 \leq n \leq 5$. And then for $n = 6$, Ko conjectured that every positive definite integral quadratic form of six variables that can be represented by a sum of squares is represented by the sum of nine squares. In this article, we prove that the conjecture is not valid. We also give, for every n, a lower bound for the number of squares whose sum represents all such forms of n variables.

Introduction

Lagrange's famous Four Square Theorem [L] says that every positive integer can be represented by the sum of four squares. This marvelous theorem was generalized by Mordell [M1] and Ko [K1] as follows : every positive definite integral quadratic form of two, three, four, and five variables is represented by the sum of five, six, seven, and eight squares, respectively. And they tried to extend this to positive definite integral quadratic forms of six or more variables. Mordell found [M2], however, that the positive definite integral quadratic form (of six variables) associated to the Dynkin diagram E_6 cannot be represented by a sum of squares. After Mordell found the example, Ko [K2] conjectured the following :

Every positive definite integral quadratic form of six variables, which is represented by a sum of squares, can be represented by the sum of nine squares.

In this short article, we'll show that the conjecture is not valid. More precisely, we'll find, for every positive integer n, a lower bound for the number of squares whose sum represents all those positive definite integral quadratic forms of n variables that can be

1991 *Mathematics Subject Classification.* 11E20, 11E25.

Key words and phrases. sums of squares, positive definite $\mathbb{Z}$-lattices, representations.

This work was partially supported by Korean Ministry of Education (BSRI-95-1414) and GARC-KOSEF at SNU.

Typeset by $\mathcal{AMS}$-TEX

represented by a sum of squares. The lower bound turns out to be bigger than 9 when $n = 6$.

We adopt terminologies and notations from [O1]. Let L be a positive definite $\mathbb{Z}$-lattice of rank n equipped with a symmetric bilinear form B and the corresponding quadratic form Q. Here, a $\mathbb{Z}$-lattice is a free $\mathbb{Z}$-module with $\mathfrak{s}(L) \subseteq \mathbb{Z}$, where $\mathfrak{s}(L)$ is the scale of L. Let $I_N = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_N$, where $\{e_1, e_2, \cdots, e_N\}$ is the standard basis of $\mathbb{Z}^N$ with $e_i \cdot e_j = \delta_{ij}$ for all $i, j = 1, 2, \cdots, N$. So, I_N corresponds to the sum of N squares and we may write $I_N = \mathbb{Z}e_1 \perp \mathbb{Z}e_2 \perp \cdots \perp \mathbb{Z}e_N$. We now define $g[n]$ to be the smallest positive integer g (if exists) for which $L \to I_g$ (meaning that L is represented by I_g) for every positive definite $\mathbb{Z}$-lattice L of rank n such that

$$L \to I_N \text{ for some } N = N(L). \tag{1}$$

Remark. It is known (see [I]) that $g[n]$ exists for all n.

Before we compute a lower bound for $g[n]$, we introduce a very short proof of the above results of Lagrange, Mordell, and Ko, in lattice theoretic language (see [I], for instance).

Theorem 1. *Every positive definite $\mathbb{Z}$-lattice L of rank n is represented by the genus of I_{n+3}, i.e., $L \to K$ for some $K \in gen(I_{n+3})$.*

Proof. Applying Theorems 1 and 2 in [O2], one can easily obtain that $L_p \to (I_{n+3})_p$ for any finite prime p. Since L is positive definite, $L_\infty \to (I_{n+3})_\infty$, which completes the proof. □

Since $\mathrm{gen}(I_n) = \mathrm{cls}(I_n)$ for $n \leq 8$, one can recapture the results of Lagrange, Mordell, and Ko all at once in the following theorem :

Theorem 2. *Every positive definite $\mathbb{Z}$-lattice L of rank n is represented by I_{n+3} for $1 \leq n \leq 5$.*

It is easy to check that $n + 3$ is the minimum number of squares necessary for I_{n+3} to represent all such L, and thereby we obtain

$$g[n] = n + 3 \quad \text{for } 1 \leq n \leq 5. \tag{2}$$

Observe that the condition (1) is not necessary for (2).

A Lower Bound for $g[n]$

By $A(\alpha_1, \alpha_2)$ we denote the positive definite $\mathbb{Z}$-lattice whose corresponding matrix is $\begin{pmatrix} \alpha_1 & 1 \\ 1 & \alpha_2 \end{pmatrix}$, i.e., $A(\alpha_1, \alpha_2) = \mathbb{Z}v_1 + \mathbb{Z}v_2$ such that $Q(v_i) = \alpha_i$ for $i = 1, 2$, and $B(v_1, v_2) = 1$. And let $A^m(\alpha_1, \alpha_2)$ denote the orthogonal sum of m copies of $A(\alpha_1, \alpha_2)$.

Theorem 3. *Let $L = A^m(2,2) \perp A(2,3)$. Then*

$$L \to I_{3m+4} \quad \textit{but} \quad L \not\to I_{3m+3}. \tag{3}$$

Proof. Consider the following sublattice K of I_{3m+4} :

$$\begin{aligned} K = \ & \Big(\mathbb{Z}(e_1+e_2)+\mathbb{Z}(e_2+e_3)\Big) \perp \Big(\mathbb{Z}(e_4+e_5)+\mathbb{Z}(e_5+e_6)\Big) \perp \cdots \\ & \perp \Big(\mathbb{Z}(e_{3m-2}+e_{3m-1})+\mathbb{Z}(e_{3m-1}+e_{3m})\Big) \\ & \perp \Big(\mathbb{Z}(e_{3m+1}+e_{3m+2})+\mathbb{Z}(e_{3m+2}+e_{3m+3}+e_{3m+4})\Big). \end{aligned}$$

Obviously, $L \simeq K$ and hence $L \to I_{3m+4}$. Now suppose that there exists a representation $\sigma : L \to I_{m+3}$. Then $\sigma(A(2,2)) = \mathbb{Z}(e_i \pm e_j) + \mathbb{Z}(e_k \pm e_j)$ for some distinct $i,j,k \in \{1,2,\cdots,3m+3\}$. By applying $\tau \in O(I_{3m+3})$ to $\sigma(A^m(2,2))$ if necessary, we may assume that

$$\begin{aligned} \sigma(A^m(2,2)) = \ & \Big(\mathbb{Z}(e_1+e_2)+\mathbb{Z}(e_2+e_3)\Big) \perp \Big(\mathbb{Z}(e_4+e_5)+\mathbb{Z}(e_5+e_6)\Big) \perp \cdots \\ & \perp \Big(\mathbb{Z}(e_{3m-2}+e_{3m-1})+\mathbb{Z}(e_{3m-1}+e_{3m})\Big) \subset I_{3m+3}. \end{aligned}$$

The image of $A(2,3)$ under σ is contained in the orthogonal complement $\sigma(A^m(2,2))^\perp$ of $\sigma(A^m(2,2))$ in I_{3m+3}. And one can easily verify that

$$\begin{aligned} \sigma(A^m(2,2))^\perp = \ & \mathbb{Z}(e_1-e_2+e_3) \perp \mathbb{Z}(e_4-e_5+e_6) \perp \cdots \perp \mathbb{Z}(e_{3m-2}-e_{3m-1}+e_{3m}) \\ & \perp \mathbb{Z}e_{3m+1} \perp \mathbb{Z}e_{3m+2} \perp \mathbb{Z}e_{3m+3}. \end{aligned}$$

Let $\sigma(A(2,3)) = \mathbb{Z}v_1 + \mathbb{Z}v_2$. Without loss of generality, we may assume that $v_1 = e_{3m+1} + e_{3m+2}$. Then

$$v_2 = \Big(\sum_{1\le j\le m} a_j(e_{3j-2}-e_{3j-1}+e_{3j})\Big) + b_1 e_{3m+1} + b_2 e_{3m+2} + b_3 e_{3m+3}$$

should satisfy

$$b_1 + b_2 = 1, \quad 3\Big(\sum_{1\le j\le m} a_j^2\Big) + b_1^2 + b_2^2 + b_3^2 = 3,$$

which is impossible because all a's and b's are integers. $\square$

Corollary 4. *For every positive integer n,*

$$g[n] \geq \left[\frac{3n+2}{2}\right],$$

where $[\ \ ]$ is the largest integer function. In particular, $g_{\mathbb{Z}}(6) \gneqq 9$.

Proof. For $1 \leq n \leq 5$, we already know the exact value of $g[n]$ in (2). So, let us assume $n \geq 6$. By using Theorem 3, one can easily prove that

$$L \perp \langle 1 \rangle \to I_{3m+5} \quad \text{but} \quad L \perp \langle 1 \rangle \nrightarrow I_{3m+4}, \tag{4}$$

where L is $\mathbb{Z}$-lattice in Theorem 3. The corollary then follows immediately from (3) and (4). $\square$

References

[I] M.I. Icaza, *Effectiveness in representations of positive definite quadratic forms*, Ph.D. Dissertation, Ohio State University, 1992.

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

[L] J.L. Lagrange, *Oeuvres Vol. 3*, 1869, pp. 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] ______, *The representation of a definite quadratic form as a sum of two others*, Ann. Math. 38, No.4 (1937), 751-757.

[O1] O.T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, 1973.

[O2] ______, *The integral representation of quadratic forms over local fields*, Amer. J. Math. 80 (1958), 843-878.