PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 9, September 2008, Pages 3041–3044
S 0002-9939(08)09326-X
Article electronically published on April 17, 2008

HERMITIAN LATTICES WITHOUT A BASIS OF MINIMAL VECTORS

BYEONG MOON KIM AND POO-SUNG PARK

(Communicated by Wen-Ching Winnie Li)

Abstract. It is shown that over infinitely many imaginary quadratic fields there exists a Hermitian lattice in all even ranks $n \geq 2$ which is generated by its $4n$ minimal vectors but which is not generated by $2n-1$ minimal vectors.

In general, it is not true that a quadratic lattice always has a basis of minimal vectors, even though it is generated by its minimal vectors. This question was asked by Louis Michel and answered by Conway and Sloane [1]. Their explicit answer was the construction of a lattice of rank 11 with this property. We found a Hermitian lattice with a similar property over an imaginary quadratic field. That is, a free Hermitian lattice is generated by its minimal vectors, but has no basis of minimal vectors. Furthermore, the Hermitian lattice is not generated by $2n-1$ minimal vectors if it is of even rank n. This is trivially constructed from the binary Hermitian lattice in the following theorems.

Theorem 1. *Let $m = 4a^2 - 1$ be a squarefree positive integer with $a \geq 2$. Then the binary Hermitian lattice L with Gram matrix*

$$\begin{pmatrix} 2a & \sqrt{-m} \\ -\sqrt{-m} & 2a \end{pmatrix}$$

over $\mathbb{Q}(\sqrt{-m})$ has minimal norm a, is generated by its 8 minimal vectors, but is not generated by any 3 minimal vectors. In addition, these minimal vectors are not primitive.

Proof. Since $m \equiv 3 \pmod 4$, the ring $\mathcal{O}$ of integers of $\mathbb{Q}(\sqrt{-m})$ is generated by 1 and ω, where $\omega = \frac{1+\sqrt{-m}}{2}$. Let v_1 and v_2 be the basis of the Hermitian lattice. Then $v_1 \cdot v_1 = 2a$, $v_1 \cdot v_2 = -1 + 2\omega$, $v_2 \cdot v_1 = -1 + 2\overline{\omega}$, $v_2 \cdot v_2 = 2a$. Suppose that a vector $xv_1 + yv_2$ with $x, y \in \mathcal{O}$ has norm smaller than a. That is,

$$\begin{aligned}(xv_1 + yv_2) \cdot (xv_1 + yv_2) &= x\overline{x}\, v_1 \cdot v_1 + x\overline{y}\, v_1 \cdot v_2 + \overline{x}y\, v_1 \cdot v_2 + y\overline{y}\, v_2 \cdot v_2 \\ &= \frac{1}{2a}[2ax + (-1+2\overline{\omega})y]\overline{[2ax + (-1+2\overline{\omega})y]} + \frac{1}{2a}y\overline{y} \\ &< a\end{aligned}$$

Received by the editors July 6, 2007.
2000 *Mathematics Subject Classification.* Primary 11E39; Secondary 11H50.
Key words and phrases. Hermitian lattice, minimal vector.
The second author was partially supported by KRF(2003-070-c00001).

or

$$z\overline{z} + y\overline{y} < 2a^2$$

if we set $z = 2ax + (-1 + 2\overline{\omega})y$.

Let $x = x_1 + x_2\omega$ and $y = y_1 + y_2\omega$ with $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. If $y_2 \geq 2$ or $y_2 \leq -2$, then $y\overline{y} \geq 4a^2$. Thus $y_2 = 0$ or ± 1. Note that

$$z = 2ax + (-1 + 2\overline{\omega})y = 2ax_1 + y_1 + 2a^2y_2 + (2ax_2 - 2y_1 - y_2)\omega.$$

If $y_2 = \pm 1$, then $y\overline{y} \geq a^2$. Thus $z\overline{z}$ can be smaller than a^2 only when $2ax_2 - 2y_1 - y_2 = 0$, which is impossible by checking the parity. So $y_2 = 0$, and the same argument shows that $x_2 = 0$.

Then, $z = 2ax_1 + y_1 - 2y_1\omega$. Since $z\overline{z} < 2a^2$, $y_1 = 0$ and $x_1 = 0$ subsequently. That is, if $z\overline{z} + y\overline{y} < 2a^2$, then $x = y = 0$.

A similar argument shows that L has exactly 8 minimal vectors:

$$\pm(av_1 - \omega v_2), \pm(av_1 + \overline{\omega}v_2), \pm(\omega v_1 + av_2), \pm(\overline{\omega}v_1 - av_2),$$

and their norms are all a. It is clear that these vectors are not primitive since $1 \notin a\mathcal{O} + \omega\mathcal{O}$. Since $v_1 = (\omega v_1 + av_2) + (\overline{\omega}v_1 - av_2)$ and $v_2 = -(av_1 - \omega v_2) + (av_1 + \overline{\omega}v_2)$, these minimal vectors generate L.

Now we will show that no set of three minimal vectors generates L. Suppose that $av_1 - \omega v_2$, $av_1 + \overline{\omega}v_2$, and $\omega v_1 + av_2$ generate $\overline{\omega}v_1 - av_2$. That is,

$$(xa + ya + z\omega)v_1 + (-x\omega + y\overline{\omega} + za)v_2 = \overline{\omega}v_1 - av_2$$

for some $x, y, z \in \mathcal{O}$. This means that $\overline{\omega} \in (a, \omega)\mathcal{O}$ and $a \in (\omega, \overline{\omega}, a)\mathcal{O}$ simultaneously. But this is impossible since $1 = \omega + \overline{\omega} \notin (a, \omega)\mathcal{O}$. Similarly we can verify that any 3 minimal vectors never generate all minimal vectors. □

Theorem 2. *Let $m = (2a+1)^2 - 2$ be a squarefree positive integer with $a \geq 2$. Then the binary Hermitian lattice L with Gram matrix*

$$\begin{pmatrix} 2a+1 & \sqrt{-m} \\ -\sqrt{-m} & 2a+1 \end{pmatrix}$$

over $\mathbb{Q}(\sqrt{-m})$ has minimal norm $2a$, is generated by its 8 minimal vectors, but is not generated by any 3 minimal vectors. In addition, these minimal vectors are not primitive.

Proof. The ring $\mathcal{O}$ of integers of $\mathbb{Q}(\sqrt{-m})$ is also $\mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-m}}{2}$. Let v_1 and v_2 be the basis of the Hermitian lattice. Then $v_1 \cdot v_1 = 2a+1$, $v_1 \cdot v_2 = -1+2\omega$, $v_2 \cdot v_1 = -1 + 2\overline{\omega}$, $v_2 \cdot v_2 = 2a+1$. Suppose that a vector $xv_1 + yv_2$ with $x, y \in \mathcal{O}$ has norm smaller than $2a$. That is,

$$\begin{aligned}
&(xv_1 + yv_2) \cdot (xv_1 + yv_2) \\
&= x\overline{x}\, v_1 \cdot v_1 + x\overline{y}\, v_1 \cdot v_2 + \overline{x}y\, v_1 \cdot v_2 + y\overline{y}\, v_2 \cdot v_2 \\
&= \frac{1}{2a+1}[(2a+1)x + (-1+2\overline{\omega})y][\overline{(2a+1)x + (-1+2\overline{\omega})y}] + \frac{2}{2a+1}y\overline{y} \\
&< 2a
\end{aligned}$$

or

$$z\overline{z} + 2y\overline{y} < 2a(2a+1) \tag{1}$$

if we set

$$\begin{aligned} z &= (2a+1)x + (-1+2\overline{\omega})y \\ &= (2a+1)x_1 + y_1 + 2a(a+1)y_2 + ((2a+1)x_2 - 2y_1 - y_2)\omega. \end{aligned}$$

If $y_2 \geq 2$ or $y_2 \leq -2$, then $y\overline{y} \geq 4a(a+1) > 2a(2a+1)$. So $y_2 = 0$ or ± 1. The same argument shows that $x_2 = 0$ or $x_2 = \pm 1$.

Consider the case of $x_2 = y_2 = 0$. Then, the inequality (1) becomes

$$[(2a+1)x_1 + y_1 - 2y_1\omega][(2a+1)x_1 + y_1 - 2y_1\overline{\omega}] + 2y_1^2 < 2a(2a+1).$$

This inequality does not hold unless $y_1 = 0$. If $y_1 = 0$, then the LHS becomes $(2a+1)^2 x_1^2$. Thus the inequality holds only when $x = y = 0$.

Consider the case of $x_2 = \pm 1$ and $y_2 = 0$. Then,

$$z = (2a+1)x_1 + y_1 + (\pm(2a+1) - 2y_1)\omega.$$

Since the modulus of $\pm(2a+1) - 2y_1$ should be smaller than 2, we can conclude that $y_1 = \pm a$ or $\pm(a+1)$ and

$$\begin{aligned} z\overline{z} + 2y\overline{y} &\geq \begin{cases} (a+1-\omega)(a+1-\overline{\omega}) + 2a^2 = 4a^2 + 2a & \text{if } y_1 = \pm a, \\ (a-\omega)(a-\overline{\omega}) + 2(a+1)^2 = 4a^2 + 4a + 2 & \text{if } y_1 = \pm a + 1 \end{cases} \\ &\geq 2a(2a+1). \end{aligned}$$

This is absurd. We can deduce the same result when $x_2 = 0$ and $y_2 = \pm 1$. So the last case is that $x_2 = \pm 1$ and $y_2 = \pm 1$. In each case, the coefficient of ω in z is one of the following:

$$2(a - y_1), \quad 2(a+1-y_1), \quad -2(a+1+y_1), \quad -2(a+y_1).$$

These coefficients should vanish and in any case $z\overline{z} + 2y\overline{y} \geq 2a(2a+1)$. Hence the minimal norm of the Hermitian lattice L cannot be smaller than $2a$.

A similar argument shows that there exist exactly 8 minimal vectors

$$\pm(av_1 - \omega v_2), \quad \pm(av_1 + \overline{\omega} v_2), \quad \pm(\omega v_1 + av_2), \quad \pm(\overline{\omega} v_1 - av_2)$$

in L. Other parts of this theorem are obvious. □

Now we prove the infinitude of squarefree integers of the form $4a^2 - 1$ and $(2a+1)^2 - 2$. These facts are deduced since the squares of the two polynomials have degree 4 and they assume infinitely many cubefree integers [2]. In general, let $f(x)$ be a polynomial of degree $\ell \geq 2$ whose coefficients are integers with highest common factor 1. If $f(x)$ has a positive leading coefficient and is not the ℓ-th power of a linear polynomial, then any ℓ-th powerfree integer of the form $f(n)$ has asymptotically positive density

$$\prod_{p:\text{prime}} \left(1 - \frac{N_p}{p^\ell}\right),$$

where $N_p = \#\{0 \leq k \leq p^\ell - 1 \mid f(k) \equiv 0 \pmod{p^\ell}\}$.

The infinitude for the form $4a^2 - 1 = (2a-1)(2a+1)$ can be proved in an easier way [3].

References

[1] J. H. Conway, N. J. A. Sloane, *A lattice without a basis of minimal vectors*. Mathematika **42** (1995), 175–177. MR1346681 (96e:11089)

[2] P. Erdös, *Arithmetical properties of polynomials*. J. London Math. Soc. **28** (1953), 416–425. MR0056635 (15:104f)

[3] B. M. Kim, *Universal octonary diagonal forms over some real quadratic fields*. Comment. Math. Helv. **75** (2000), 410–414. MR1793795 (2001m:11046)

Department of Mathematics, Kangnung National University, Kangnung, Korea
E-mail address: kbm@kangnung.ac.kr

Korea Institute for Advanced Study, Cheongnyangni 2-dong, Dongdaemun-gu, Seoul, 130-722, Korea
E-mail address: sung@kias.re.kr