A Construction of Unimodular Lattices Without Non-Trivial Automorphisms
(A survey)

神戸薬科大学　味村 良雄 (Yoshio Mimura)
Kobe Pharmaceutical University

1. Introduction

2. Results of Etsuko Bannai (1988)

3. Examples of Yoshio Mimura (1990)

4. Examples of Roland Bacher (1993)

1. Introduction

Let V be a positive definite quadratic space over $\mathbb{Q}$ with its bilinear symmetric form B and associated quadratic form Q : $Q(x) = B(x,x)$, $2\,B(x,y) = Q(x+y) - Q(x) - Q(y)$. Let L be a lattice in V, that is, a finitely generated $\mathbb{Z}$-module in V. The orthogonal group of V is defined as follows:

$$O(V) = \{\sigma \in GL(V) \mid Q(\sigma x) = Q(x) \text{ for } \forall x \in V\}$$

The automorphism group (unit group) of L is:

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

Note that $O(L)$ is a finite group and $\pm 1_V \in O(L)$.

Problem:

Can the group $O(L)$ be trivial (i.e., $O(L) = \{\pm 1_V\}$) ?

In 1975 O .T .O'Meara gives a method to construct such a lattice starting from any given lattice. But the discriminant is big!

In 1981 J. Biermann proved that there is such a lattice of any rank with sufficiently big discriminant.

A lattice L is a free $\mathbb{Z}$-module, hence it can be written as

$$L = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_n$$

with a suitable basis $x_1, x_2, \ldots, x_n$. For this basis we consider the matrix

$$A = \begin{bmatrix} B(x_1,x_1) & B(x_1,x_2) & \cdots & B(x_1,x_n) \\ B(x_2,x_1) & B(x_2,x_2) & \cdots & B(x_2,x_n) \\ \vdots & \vdots & \ddots & \vdots \\ B(x_n,x_1) & B(x_n,x_2) & \cdots & B(x_n,x_n) \end{bmatrix}$$

and we represent L by using the matrix A. The discriminant $d(L)$ of L is defined by $d(L) = \det A$. It is independent of the choice of basis, and note that $d(L) > 0$. The scale $s(L)$ and the norm $n(L)$ of L are defined as follows:

$s(L)$ is the ideal generated by $\{B(x,y) \mid x, y \in L\}$,

$n(L)$ is the ideal generated by $\{Q(x) \mid x \in L\}$.

In the following we assume that $s(L) = \mathbb{Z}$, hence $n(L) = \mathbb{Z}$ or $n(L) = 2\mathbb{Z}$. L is said to be odd when $n(L) = \mathbb{Z}$, and L is said to be even when $n(L) = 2\mathbb{Z}$. And we say that L is unimodular if $s(L) = \mathbb{Z}$ and $d(L) = 1$.

Consider the lattice M_n of rank n:

$$M_n \cong \begin{bmatrix} 3 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 3 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 3 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 4 \end{bmatrix}.$$

Then it is clear that $O(L)$ is trivial, but the discriminant is big as n is big.

We list up all binary lattices $L \cong \begin{bmatrix} a & c \\ c & b \end{bmatrix}$ $(0 < a \leqq b, 0 \leqq c \leqq a/2)$.

$L \cong \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, $\#O(L) = 12$, $d(L) = 3$. $L \cong \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\#O(L) = 8$, $d(L) = 1$.

$L \cong \begin{bmatrix} a & c \\ c & a \end{bmatrix}$, $\#O(L) = 4$ $(0 < c < a/2)$. $L \cong \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $\#O(L) = 4$ $(0 < a < b)$.

$L \cong \begin{bmatrix} a & c \\ c & b \end{bmatrix}$, $\#O(L) = 4$ $(0 < a < b, a = 2c)$.

$L \cong \begin{bmatrix} a & c \\ c & b \end{bmatrix}$, $\#O(L) = 2$ $(0 < a < b, 0 < c < a/2)$.

We may say "$\#O(L) = 2$ for almost all binary lattices L !!"

From now on we assume that L is an odd or even unimodular lattice. It is known that there is at least an odd unimodular lattice of any rank. We know that there is an even unimodular lattice if and only if the rank is divisible by 8. We list up the orders of $O(L)$ for unimodular lattices L of low rank.

If $\mathrm{rank}(L) = n \leqq 7$ then L is odd and

$L = I_n \cong [1] \perp [1] \perp \cdots \perp [1]. \ \#O(L) = 2^n \times n!$

If $\text{rank}(L) = 8$ then L is I_8 (odd) or E_8 (even):

$L = I_8 \cong [1] \perp [1] \perp \cdots \perp [1]. \ \#O(L) = 2^8 \times 8!$

$$L = E_8 \cong \begin{bmatrix} 2 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}$$

$\#O(L) = 2^{14} \times 3^5 \times 5^2 \times 7 = 696729600.$

If $\text{rank}(L) = n \ (n = 9, 10, 11)$, then we have:

$L = I_n.$ $\qquad\qquad \#O(L) = 2^n \times n!$

$L = I_{n-8} \perp E_8.$ $\quad \#O(L) = 2^{n-8}(n-8)! \times \#O(E_8)$

Cf. J. H. Conway & N. J. A. Sloane's book : Sphere Packings, Lattices and Groups.

In the above book you can see all quadratic lattices of rank$\leq$ 24, and they have non-trivial automorphism group except the trivial case I_1.

Remark. It is known that if the automorphism group of a unimodular lattice is trivial, then the rank$\geq$ 28 (odd case) and the rank$\geq$ 32 (even case). Recently it was proved that the rank$\geq$ 29 in odd case.

2. Results of Etsuko Bannai (1988)

She proved :

There is an odd unimodular lattice with the trivial automorphism group of any rank$\geq$ 43, and there is an even unimodular lattice with the trivial automorphism group of any rank$\geq$ 144

in her paper *Positive definite unimodular lattices with the trivial automorphism groups* (Diss, The Ohio State Univ). But any explicit examples of such a lattice was not known.

3. Examples of Y. Mimura (1990)

Among the unimodular lattices with the trivial automorphism groups, Mimura gives

two examples of odd unimodular lattices of rank 36, 40,

one example of even unimodular lattices of rank 64.

Cf. Explicit examples of unimodular lattices with the trivial automorphism groups, Proceedings of KAIST Mathematics Workshop, vol 5, 1990, 91-95.

3-1. Construction of unimodular lattices (by using Kneser's neighbouring).

Kneser's neighbouring is a simple way of constructing many lattices in the given genus of lattices.

1. Initial lattice : $I = I_n = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n \cong [1] \perp \cdots \perp [1]$

2. Take a positive integer q and a vector $v \in q^{-1}I$ such that $Q(x) \in \mathbb{Z}$.

3. Neighbouring : $L = I[v] = \mathbb{Z}v + \{u \in I \mid B(u, v) \in \mathbb{Z}\}$.

(detail)

a) L is unimodular. Especially, L is odd if q is odd.

b) Let $v = q^{-1} \sum_{i=1}^{n} c_i e_i, \quad c_i \in \mathbb{Z}$.

Then a vector $x \in L$ is written as

$$x = \pm \left(cv + \sum_{i=1}^{n} a_i e_i \right), \quad c \in \mathbb{Z}, \quad a_i \in \mathbb{Z}, \quad 0 \leq c \leq q/2, \quad \sum_{i=1}^{n} c_i a_i \equiv 0 \pmod{q}$$

c) $Q(x) = q^{-2} \sum_{i=1}^{n} (cc_i + qa_i)^2$

Remark.

i) If $L = J \perp K$ ($J, K \neq \{0\}$), then $\pm 1_L \neq 1_J \perp (-1_K) \in O(L)$, i.e., $O(L)$ is not trivial.

ii) If there is a vector $x \in L$ with $Q(x) = 1$, then $L = [1] \perp L'$.

iii) If there is a vector $x \in L$ with $Q(x) = 2$, then $\pm 1_L \neq \tau_x \in O(L)$, i.e., $O(L)$ is not trivial. Here the symmetry τ_x w.r.t. x is defined by

$$\tau_x(y) = y - \frac{2B(x, y)}{Q(x)} x \text{ for } y \in L.$$

iv) Hence we must choose a vector v so that

  a) $c_i \not\equiv 0 \pmod{q}$ $(1 \leq i \leq n)$ by (i) and (ii)

  b) $c_i \not\equiv c_j \pmod{q}$ $(1 \leq i < j \leq n)$ by (iii)

  c) $\sum_{i=1}^{n} R(cc_i)^2 > 2q^2$ $(1 \leq c \leq q/2)$ by (iii)

   where $R(a)$ is defined by $R(a) \equiv a \pmod{q}$ and $|R(a)| \leq q/2$

3-2. Proof of the triviality of $O(L)$

Let m be a positive integer. Put

$$X = \{x \in L \mid Q(x) = m\}, \quad \overline{X} = X/\pm 1.$$

We consider a graph G with the vertex set $\overline{X}$,

where $\pm x$ and $\pm y$ are adjacent $\Longleftrightarrow B(x,y) \neq 0$

Then the group $O(L)$ induces a subgroup H of the automorphism group of G.

Proposition. The automorphism group $O(L)$ is trivial if

(P1) $H = \{1\}$,

(P2) G is connected,

(P3) V is generated by X over $\mathbb{Q}$.

Proof. Take any $\sigma \in O(L)$. By (P1) we see that $\sigma x \in \{x, -x\}$ for all $x \in X$. Take a vector $x_0 \in X$. We may suppose that $\sigma x_0 = x_0$ (Replace σ by $-\sigma$ if neccesary.) Thus we have $\sigma y = y$ for any $y \in X$ with $B(x_0, y) \neq 0$. Hence, by (P2), we have $\sigma x = x$ for any $x \in X$. Finally, by (P3), we have $\sigma = 1_V$. $\square$

3-3. Explicit Examples

(1) Odd unimodular lattice of rank 40.

$$n = 48, \quad q = 97, \quad 97v = \sum_{j \in J} j\, e_j, \quad Q(v) = 4,$$

where $J = \{j \in \mathbb{Z} \mid 6 \leq j \leq 48, j \neq 8, 10, 13\}$.

$$I_{48}[v] = I_8 \perp L, \quad X = \{x \in L \mid Q(x) = 3\}.$$

The elements of $\overline{X}$ are

$\pm(e_i + e_j + e_k)$, with $i, j, k \in J$, $i < j < k$, $i + j + k = 97$,

$\pm(e_i + e_j - e_k)$, with $i, j, k \in J$, $i < j < k$, $i + j = k$.

We see $\#\overline{X} = 163 + 249 = 412$.

The degree of a vertex of G is one of $81, 82, \ldots, 94$.

Hence $\overline{X} = \overline{X}_{81} \cup \cdots \cup \overline{X}_{94}$ (disjoint), where $\overline{X}_t = \{\pm x \in \overline{X} \mid \deg(\pm x) = t\}$

Each set $\overline{X}_t$ is invariant under $O(L)$. Consider the function δ_t of $\overline{X}$:

$\delta_t(\pm x) = \#\{\pm y \in \overline{X}_t \mid \pm x \text{ and } \pm y \text{ are adjacent}\}$.

We can prove: $\pm x = \pm y \Longleftrightarrow \delta_t(\pm x) = \delta_t(\pm y)$ for all t.

(P1) is satisfied since $\delta_t(\pm x) = \delta_t(\sigma(\pm x))$ for all $\sigma \in O(L)$. By a direct computation, we can see that (P2) and (P3) are valid. $\square$

(2) Odd unimodular lattice of rank 36.

$$n = 38, \quad q = 79, \quad 79v = \sum_{j \in J} j\, e_j, \quad Q(v) = 3,$$

where $J = \{j \in \mathbb{Z} \mid 1 \le j \le 38,\ j \ne 10, 14\}$.

$I_{38}[v] = I_2 \perp L$, $X = \{x \in L \mid Q(x) = 3\}$.

In this case we have $\overline{X} = \overline{X}_{91} \cup \overline{X}_{93} \cup \overline{X}_{95}$ (disjoint). This is a disjoint sum of 400 subsets which are $O(L)$-invariant.

(3) Even unimodular lattice of rank 64.

$$n = 129, \quad q = 270, \quad 270v = \sum_{j \in J} j'\, e_j, \quad Q(v) = 6,$$

where $J = \{j \in \mathbb{Z} \mid 1 \le j \le 129,\ j \ne 5,\ j : \text{odd}\}$, $j' = j$ if $j \ne 3$, and $3' = -267$.

$I_{129}[v] = I_{65} \perp L$, $X = \{x \in L \mid Q(x) = 4\}$.

4. Results of Roland Bacher (1993)

Using the same method of Mimura, R. Bacher presented:

an odd unimodular lattice of rank 29 and

an even unimodular lattice of rank 32

among the unimodular lattices with the trivial automorphism groups.

Cf. Réseaux unimodulaires sans automorphismes, 18-ièmes Jounées arithmétiques, Bordeaux, 1993.

(1) Odd unimodular lattice of rank 29 : $I_{29}[v]$

$$n = 29, \quad q = 71, \quad 71v = \sum_{j=1}^{29} c_j\, e_j, \quad Q(v) = 14,$$

where c_i' are $5, 7, \ldots, 16, 18, \ldots, 24, 238, 26, \ldots, 35$

(2) Even unimodular lattice of rank 32 : $I_{32}[v]$

$$n = 32, \quad q = 142, \quad 142v = \sum_{j=1}^{32} c_j\, e_j, \quad Q(v) = 4,$$

where c_i's are $3, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, -105, 39,$

$41, 43, 45, -95, 49, 53, 55, -85, 59, -81, -79, 65, 67, -73$

There was an open problem : Is there a unimodular lattice (of rank 28) with the trivial automorphism group ? This was solved : No. So his explicit examples are ones of the smallest rank.