Nihonkai Math. J.
Vol.2(1991),155-167

Quinary code construction of the Leech lattice

Michio Ozeki

1 Introduction

Let Γ_{24} be the genus consisiting of all the equivalence classes of positive definite even unimodular lattices of rank 24. Let $\mathbf{L}$ be an element of Γ_{24}. An element $\mathbf{x}$ in $\mathbf{L}$ is called a 2m-vector if $\mathbf{x}$ satisfies $(\mathbf{x},\mathbf{x}) = 2m$ for some positive integer m. In Γ_{24} , there is a unique class $\{ \mathbf{L} \}$, in which there is no 2-vector. Such a lattice is first given by Leech [3], and it is called the Leech lattice. Leech's construction is based on the binary Golay code of length 24. Later on Leech and Sloane [4] gave another construction for the Leech lattice based on the self-dual ternary codes of length 24. After that various constructions for the Leech lattice have been given (e.g. [6], [16]) because of the plentiful structures and properties which the Leech lattice has.
In [10], [11] and [12] we have investigated the notion of the c-sublattice $\mathbf{M}$ of an even unimodular lattice $\mathbf{L}$. As a byproduct we give a construction of the Leech lattice by using a self-dual code $\mathbf{C}$ over GF(5) of length 24.

Remark 1 *We expect that the present method may serve to search positive definite even unimodular extremal lattices of ranks 72, 80 or 88. However it would take much labors, such as giving codes over GF(5) with large minimum distances or computing Lee weight enumerators of such codes, to attack the problem.*

Remark 2 *It seems to us that there would be another constructions of the Leech lattice using (special) self-dual codes of length 24 over GF(p), the field* *of p (a prime) elements along our idea. It would require a closer study of such codes, as the present work or the papers [3],[4],[11] show.*

2 Preliminary notions and results

Let $\mathbb{Z}$ be the ring of rational integers and $\mathbb{R}$ the field of real numbers. Let $\mathbf{F}_5 = GF(5)$ be the field of 5 elements. Elements in $\mathbf{F}_5$ are denoted by $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ and $\overline{4}$ respectively. We adopt many notations from [5]. We use a special code $\mathbf{Q}_{24}$ given in [5], page 186. The code $\mathbf{Q}_{24}$ has the generator matrix

$$(\star) \qquad\qquad (\overline{2}\mathbf{I}_{12}, \mathbf{B}_{12}),$$

where $\mathbf{B}_{12} = (b_{\lambda\mu})$ is the Paley matrix of order 12 and $\mathbf{I}_{12}$ the unit matrix. The matrix $\mathbf{B}_{12}$ is given by :

$$\mathbf{B}_{12} = \begin{pmatrix} \overline{0} & \mathbf{e} \\ \overline{4}\mathbf{e}^T & \mathbf{W} \end{pmatrix},$$

where $\mathbf{e}$ is the all $\overline{1}$ row vector of length 11, $\mathbf{e}^T$ is the transpose of e, and $\mathbf{W}$ is the circulant matrix of order 11 whose first row vector is

$$(\overline{0}, \overline{1}, \overline{4}, \overline{1}, \overline{1}, \overline{1}, \overline{4}, \overline{4}, \overline{4}, \overline{1}, \overline{4}).$$

The rows of the above matrix $(\star)$ generate the code $\mathbf{Q}_{24}$. Usually the number of non-zero coordinates in a codeword is called the weight of the codeword. The first clue to our present work is the fact stated in [5], page 186 :

Lemma 1 *The minimal weight of the code $\mathbf{Q}_{24}$ is 9.*

Next lemma is a further information on $\mathbf{Q}_{24}$ not given in [5].

Lemma 2 *There is no codeword of weight 10 with all $\pm\overline{1}$'s or all $\pm\overline{2}$'s as the non-zero coordinates.*

This is verified by using an electronic computer, and more precisely we have determined the Lee weight enumerator L(x,y,z) of the code $\mathbf{Q}_{24}$. Here we give L(x,y,z) explicitly :

$$
\begin{aligned}
&L(x,y,z) = \\
&\quad x^{24} + 528x^{15}(y^7z^2 + y^2z^7) + 11088x^{14}y^5z^5 \\
&\quad +18480x^{13}(y^8z^3 + y^3z^8) + 206976x^{12}y^6z^6 + \\
&\quad 2688x^{12}(y^{11}z + yz^{11}) + 295680x^{11}(y^9z^4 + y^4z^9) + \\
&\quad 59136x^{10}(y^{12}z^2 + y^2z^{12}) + 2264064x^{10}y^7z^7 + \\
&\quad 880x^9(y^{15} + z^{15}) + 2642640x^9(y^{10}z^5 + y^5z^{10}) + \\
&\quad 554400x^8(y^{13}z^3 + y^3z^{13}) + 12687840x^8y^8z^8 + \\
&\quad 16896x^7(y^{16}z + yz^{16}) + 11501952x^7(y^{11}z^6 + y^6z^{11}) + \\
&\quad 35130480x^6y^9z^9 + 2199120x^6(y^{14}z^4 + y^4z^{14}) + \\
&\quad 77616x^5(y^{17}z^2 + y^2z^{17}) + 23003904x^5(y^{12}z^7 + y^7z^{12}) \\
&\quad +3548160x^4(y^{15}z^5 + y^5z^{15}) + 42156576x^4y^{10}z^{10} + \\
&\quad 117040x^3(y^{18}z^3 + y^3z^{18}) + 17685360x^3(y^{13}z^8 + y^8z^{13}) \\
&\quad +16720704x^2y^{11}z^{11} + 1759296x^2(y^{16}z^6 + y^6z^{16}) + \\
&\quad 528x^2(y^{21}z + yz^{21}) + 36960x(y^{19}z^4 + y^4z^{19}) + \\
&\quad 3379200x(y^{14}z^9 + y^9z^{14}) + 923216y^{12}z^{12} + \\
&\quad 119328(y^{17}z^7 + y^7z^{17}) + 48(y^{22}z^2 + y^2z^{22}).
\end{aligned}
$$

Now we describe the method of construction of the lattice.
Let $\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_{24}$ be vectors in $\mathbb{R}^{24}$ satisfying

$$(\mathbf{f}_\lambda, \mathbf{f}_\mu) = 5\delta_{\lambda\mu} \quad for \quad 1 \le \lambda, \mu \le 24,$$

where (,) is the usual inner product on $\mathbb{R}^{24}$ and $\delta_{\lambda\mu}$ is Kronecker's delta. Let M be the lattice generated by the vectors $\pm\mathbf{f}_\lambda \pm \mathbf{f}_\mu$ $(1 \le \lambda,\ \mu \le 24)$. It can be seen that the lattice M is similar to the root lattice $\mathbf{D}_{24}$ with the similitude $\sqrt{5}$ (Conf. [10], [12]). If we let $\mathrm{M}^\prime$ denote the dual lattice of M, then we have

$$
\begin{aligned}
[\mathrm{M}^\prime : \mathrm{M}] &= d(\mathrm{M}) \\
&= 2^2 \cdot 5^{24} ,
\end{aligned}
$$

where d(M) is the determinant of the lattice M.

3 Quinary Code construction of the Leech lattice

Let $\mathbf{B}_{12} = (b_{\lambda\mu})$ be the Paley matrix as in §2. Its entries are in $\mathbf{F}_5$. The original Paley matrix $\mathbf{A}_{12} = (a_{\lambda\mu})$ of order 12, whose entries lie in $\mathbb{Z}$, can be obtained from the above matrix $\mathbf{B}_{12}$ by replacing $\overline{1}$'s (resp. $\overline{0}$'s or $\overline{4}$'s) in $\mathbf{B}_{12}$ by 1's (resp. 0's or -1's). We put

$$\mathbf{x}_\lambda = \frac{1}{5}(-3\mathbf{f}_\lambda + \sum_{\mu=1}^{12} a_{\lambda\mu}\mathbf{f}_{\mu+12}) \quad (1 \leq \lambda \leq 12)\,.$$

By definition we see that

$$(2) \qquad (\mathbf{x}_\lambda, \mathbf{x}_\lambda) = 4 \qquad \text{and}$$
$$(3) \qquad (\mathbf{x}_\lambda, \mathbf{x}_\mu) = 0 \qquad \text{for } \lambda \neq \mu.$$

The property (3) is a direct consequence of the orthogonality of the Paley matrix $\mathbf{A}_{12}$.
The lattice generated by $\mathbf{x}_1, \cdots, \mathbf{x}_{12}$ and the lattice $\mathbf{M}$ over $\mathbb{Z}$ is denoted by $\mathbf{J}$. Clearly the lattice $\mathbf{J}$ is even integral. Any element $\mathbf{x}$ of $\mathbf{J}$ can be expressed as

$$(4) \qquad \mathbf{x} = \frac{1}{5}\sum_{\lambda=1}^{24} c_\lambda \mathbf{f}_\lambda \quad \text{with suitable } c_\lambda \in \mathbb{Z}\,.$$

We now define a map ϕ from the lattice $\mathbf{J}$ to the code $\mathbf{Q}_{24}$. For $\mathbf{x} \in \mathbf{J}$, we put

$$supp\, \mathbf{x} = \phi(\mathbf{x}) = (\xi_1, \xi_2, \cdots, \xi_{24}) \in \mathbf{F}_5^{24}\,,$$

where ξ_λ is the residue class modulo $5\mathbb{Z}$ to which c_λ belongs. We remark that ϕ satisfies the properties :

$$(5) \quad \phi(\mathbf{x}+\mathbf{y}) = \phi(\mathbf{x}) + \phi(\mathbf{y}) \quad \text{for any } \mathbf{x}, \mathbf{y} \in \mathbf{J}\,,$$
$$(6) \quad \phi(t\mathbf{x}) = \bar{t}\phi(\mathbf{x}) \quad \text{for any } \mathbf{x} \in \mathbf{J} \text{ and any } t \in \mathbb{Z}\,,$$

where $\bar{t}$ is the residue class of t modulo $5\mathbb{Z}$. We prove

Lemma 3 *Let the notations be as above. then the kernel* $\ker\phi$ *of* ϕ *is* $\mathbf{M}$.

Proof. It is obvious that $\ker\phi \supset \mathbf{M}$. By the definition of the vectors $\mathbf{x}_\lambda$ $(1 \le \lambda \le 12)$, we see that

$$-3 + \sum_{\mu=1}^{12} a_{\lambda\mu} \equiv 0 \pmod 2 \quad \text{for } (1 \le \lambda \le 12)\ .$$

If we rewrite each element $\mathbf{x}$ in $\mathbf{J}$ of the form (4), then the coefficients c_λ of $\mathbf{x}$ also satisfy

$$(7) \qquad \sum_{\lambda=1}^{24} c_\lambda \equiv 0 \pmod 2.$$

Thus, any element $\mathbf{x}$ in $\mathbf{J}$ of the form (4) should satisfy the congruence (7). Let $\mathbf{x}$ be an element of $\ker\phi$ of the form (4), then

$$c_\lambda \equiv 0 \pmod 5 \qquad \text{for } \lambda \text{ with } 1 \le \lambda \le 24\ .$$

By putting $c_\lambda = 5c'_\lambda$ with $c'_\lambda \in \mathbb{Z}$, then we substitute these into (7), so that we have

$$(8) \qquad \sum_{\lambda=1}^{24} c'_\lambda \equiv 0 \pmod 2.$$

Therefore the vector $\mathbf{x} \in \ker\phi$ can be written as

$$\mathbf{x} = \sum_{\lambda=1}^{24} c'_\lambda \mathbf{f}_\lambda \ \text{ with the condition } \ (8)\ .$$

It is easy to check that the above $\mathbf{x}$ belongs to the lattice $\mathbf{M}$, implying $\ker\phi = \mathbf{M}$.

Q.E.D.

By the equations (5),(6), the image $\phi(J)$ forms a vector subspace of $\mathbf{F}_5^{24}$. Since $\phi(\mathbf{M}) = \{0\}$ and $\phi(\mathbf{x}_\lambda)$ $(1 \le \lambda \le 12)$ are a basis of the self-dual code $\mathbf{Q}_{24}$ of length 24. $\phi(J)$ is self-orthogonal vector subspace of $\mathbf{F}_5^{24}$, of dimension 12 over $\mathbf{F}_5$, and therefore coincides with the code $\mathbf{Q}_{24}$. By the Lemma 3, ϕ defines a bijective map $\overline{\phi}$ between $\mathbf{J}/\mathbf{M}$ and $\mathbf{Q}_{24}$. We summarize this fact as a proposition :

Proposition 1 *Let the notations be as above, then* $\mathbf{J}/\mathbf{M}$ *is isomorphic to the code* $\mathbf{Q}_{24}$.

As a consequence of this proposition, we have

$$(9) \qquad [\mathbf{J}:\mathbf{M}] = 5^{12} \quad .$$

We introduce a new vector $\mathbf{x}_0$:

$$\begin{aligned}\mathbf{x}_0 &= \frac{1}{2}\mathbf{x}_1 - \sum_{\lambda=2}^{12}\mathbf{x}_\lambda - \frac{1}{2}(\mathbf{f}_2 + \mathbf{f}_3 + \cdots + \mathbf{f}_{12} + 5\mathbf{f}_{13}) + \mathbf{f}_1 \\ &= \frac{1}{10}(7\mathbf{f}_1 + \sum_{\lambda=2}^{12}\mathbf{f}_\lambda - 3\mathbf{f}_{13} + \sum_{\lambda=14}^{24}\mathbf{f}_\lambda) \, .\end{aligned}$$

The vector $\mathbf{x}_0$ does not belong to $\mathbf{J}$, but $2\mathbf{x}_0 \in \mathbf{J}$. We observe that

$$\begin{aligned}&(\mathbf{x}_0, \mathbf{x}_0) = 4, \\ &(\mathbf{x}_0, \mathbf{x}_1) = -1, \\ &(\mathbf{x}_0, \mathbf{x}_\lambda) = 0 \ \text{ for } \ 2 \le \lambda \le 12,\end{aligned}$$

and

$$(\mathbf{x}_0, \mathbf{y}) \in \mathbb{Z} \ \text{ for any } \mathbf{y} \in \mathbf{M}.$$

Thus the lattice $\mathbf{L}$ generated by $\mathbf{x}_0$ and $\mathbf{J}$ over $\mathbb{Z}$ is an even integral lattice. We prove

Theorem 1 *The lattice* $\mathbf{L}$ *is an even unimodular lattice of rank 24, and* $\mathbf{L}$ *has no 2-vector.*

Proof. We have already shown that $\mathbf{L}$ is an even integral lattice. Let $\mathbf{L}'$ (resp.$\mathbf{J}'$) be the dual lattice of $\mathbf{L}$ (resp. $\mathbf{J}$). By the definition of $\mathbf{L}$, it holds that

$$(10) \qquad [\mathbf{L}:\mathbf{J}] \ = 2 \, .$$

It is known that

$$\begin{aligned}&(11) \quad [\mathbf{M}':\mathbf{M}] &&= [\mathbf{M}':\mathbf{J}'][\mathbf{J}':\mathbf{L}'][\mathbf{L}':\mathbf{L}][\mathbf{L}:\mathbf{J}][\mathbf{J}:\mathbf{M}] \, , \\ &(12) \quad [\mathbf{J}':\mathbf{L}'] &&= [\mathbf{L}:\mathbf{J}] \, , \\ &(13) \quad [\mathbf{M}':\mathbf{J}'] &&= [\mathbf{J}:\mathbf{M}] \, .\end{aligned}$$

By the conditions (1), (9), (10), (11), (12) and (13), we must have $[\mathbf{L}^\sharp : \mathbf{L}] = 1$. Thus $\mathbf{L}$ is unimodular.

It remains to prove that $\mathbf{L}$ does not contain any 2-vector. We divide the arguments into three cases, namely, (a) for the elements in $\mathbf{M}$, (b) for the elements in $\mathbf{J} - \mathbf{M}$, and (c) for the elements in $\mathbf{L}-\mathbf{J}$. In each case,we show that the vecors $\mathbf{x}$ in the subset in question satisfy $(\mathbf{x},\mathbf{x}) \geq 4$.

Case (a). First we remark that any non-zero element $\mathbf{y}$ of $\mathbf{M}$ satisfies

$$(\mathbf{y},\mathbf{y}) \geq 10.$$

This comes from fact that the lattice $\mathbf{M}$ is a scaled lattice of the root lattice of type D_{24} with scaling factor $\sqrt{5}$, whereas the minimal vectors of the lattice D_{24} are 2-vectors.

Case (b). Let $\mathbf{x}$ be an elemnt of $\mathbf{J} - \mathbf{M}$ of the form (4), then it holds that

$$(\mathbf{x},\mathbf{x}) = \frac{1}{5}\sum_{\lambda=1}^{24} c_\lambda^2.$$

Since supp $\mathbf{x}$ is a non-zero codeword in $\mathbf{Q}_{24}$ and the minimal weight of $\mathbf{Q}_{24}$ is 9 (Lemma 1), we may say that at least 9 of c_λ's are non-zero. If the weight of *supp* $\mathbf{x} = (\xi_1, \cdots, \xi_{24})$ is 9, then after [5] we take that there are j $\pm\overline{1}$'s and k $\pm\overline{2}$'s among ξ_λ's with $j + k = 9$. By the restriction (1) in [5], we must have either $j = 2,\ k = 7$ or $j = 7,\ k = 2$. At any rate, we get

$$| c_\lambda | \geq 2 \text{ for at least two } \lambda's ,$$

and

$$(\mathbf{x},\mathbf{x}) = \frac{1}{5}\sum_{\lambda=1}^{24} c_\lambda^2 \geq \frac{1}{5}(4+4+7) > 2 .$$

Since $(\mathbf{x},\mathbf{x})$ is an even integer, we have $(\mathbf{x},\mathbf{x}) \geq 4$. If the weight of supp $\mathbf{x}$ is 10, then by (1) in [5] we also have either (i) $j = 10,\ k = 0$ or (ii) $j = 0,\ k = 10$ or (iii) $j = k = 5$. However, by Lemma 2 the cases (i) and (ii) do not give rise, so that we get

$$| c_\lambda | \geq 2 \ \text{ for at least five } \ \lambda's ,$$

and

$$(\mathbf{x},\mathbf{x}) = \frac{1}{5}\sum_{\lambda=1}^{24} c_\lambda^2 \geq \frac{1}{5}(5+4*5) \geq 5\ ,$$

implying $(\mathbf{x},\mathbf{x}) \geq 6$.
If the weight of supp $\mathbf{x}$ exceeds 10, then we can easily show that $(\mathbf{x},\mathbf{x}) \geq 4$.
Thus for each $\mathbf{x} \in \mathbf{J} - \mathbf{M}$, we have $(\mathbf{x},\mathbf{x}) \geq 4$.

Case (c). Any element $\mathbf{z}$ in $\mathbf{L} - \mathbf{J}$ can be written as

$$\mathbf{z} = \mathbf{x}_0 + \mathbf{x} \quad \text{with} \quad \mathbf{x} \in \mathbf{J}.$$

If we express $\mathbf{x}$ in the form (4), then $\mathbf{z}$ takes the form :

$$\begin{aligned} \text{(14)} \qquad \mathbf{z} &= \frac{1}{10}[(7+2c_1)\mathbf{f}_1 + \sum_{\lambda=2}^{12}(1+2c_\lambda)\mathbf{f}_\lambda \\ &\quad +(2c_{13}-3)\mathbf{f}_{13} + \sum_{\lambda=14}^{24}(1+2c_\lambda)\mathbf{f}_\lambda] \\ &= \frac{1}{10}\sum_{\lambda=1}^{24} t_\lambda \mathbf{f}_\lambda. \end{aligned}$$

Note that t_λ $(1 \leq \lambda \leq 24)$ are all odd integers and $2\mathbf{z} \in \mathbf{J}$. If the weight of supp $2\mathbf{z}$ is less than 24, then there exists at least one t_λ with $t \equiv 0 \pmod 5$.
In this case we have

$$(\mathbf{z},\mathbf{z}) \geq \frac{5}{100}(23+25) > 2,$$

implying that $(\mathbf{z},\mathbf{z}) \geq 4$.
The remaining case is that when the weight of supp $2\mathbf{z}$ is 24. We put

$$supp\ 2\mathbf{z} = (\zeta_1, \zeta_2, \cdots, \zeta_{24}),$$

where ζ_λ is the residue of t_λ mod 5. Let S_1 (resp. S_2) be the set of the indeces λ with $\zeta_\lambda = \overline{1}$ or $\overline{4}$ (resp. $\zeta_\lambda = \overline{2}$ or $\overline{3}$). Note that $\mid t_\lambda \mid \geq 3$ holds for $\lambda \in S_2$, because this t_λ is odd and $\equiv 2$ or $3 \pmod 5$. Let j (resp. k) be the cardinality of S_1 (resp. S_2). By the condition (1) in [5], we know that $j \equiv k \pmod 5$. Since $j + k = 24$, there are five possibilities for the pair (j,k), namely, (i) (22,2), (ii) (17,7), (iii) (12,12), (iv) (7,17) and (v) (2,22)

In the cases (ii)-(v), we can easily prove that $(\mathbf{z}, \mathbf{z}) \geq 4$. For instance, let j=17 and k=7, then we have

$$\begin{aligned}(\mathbf{z}, \mathbf{z}) &= \frac{1}{20} \sum_{\lambda=1}^{24} t_\lambda^2 \\ &\geq \frac{1}{20}(17 + 9 * 7) = 4,\end{aligned}$$

because we know $| t_\lambda | \geq 3$ for $\lambda \in S_2$. To treat the case (i), we need a lemma:

Lemma 4 *Let the notations be as above. Let* $\mathbf{z}$ *be an element of* **L-J** *of the form (14) with the weight of supp* $(2\mathbf{z}) = 24$. *Suppose* $j = 22$ *and* $k = 2$ *holds for this vector* $\mathbf{z}$. *Then it is impossssible to set simultaneously that*

(15) $\quad | t_\lambda | = 1$ for all $\lambda \in S_1$ and $| t_\lambda | = 3$ for all $\lambda \in S_2$.

Proof of lemma. By using an electronic computer, we have enumerated all the codewords of weight 24 with $j = 22$ and $k = 2$, and they are described in the **Appendix**. Suppose that

$$(\zeta_1, \zeta_2, \cdots, \zeta_{24}) \qquad (\zeta_\lambda = t_\lambda \bmod 5)$$

is any one of 48 codewords in the **Appendix**, and further $| t_\lambda | = 1$ for all $\lambda \in S_1$ and $| t_\lambda | = 3$ for all $\lambda \in S_2$. Then we verify that

$$(\mathbf{x}_0, \mathbf{z}) \notin \mathbb{Z} \quad \text{for} \quad \mathbf{z} = \tfrac{1}{10} \textstyle\sum_{\lambda=1}^{24} t_\lambda \mathbf{f}_\lambda \,.$$

To illustrate this, we give two examples of computation.

Example 1. When

$$(\zeta_1, \zeta_2, \cdots, \zeta_{24}) = (\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4})$$

then the precise shape of $\mathbf{z} = \frac{1}{10} \sum_{\lambda=1}^{24} t_\lambda \mathbf{f}_\lambda$ is

$$\begin{aligned}\mathbf{z} \;=\; & \frac{1}{10}(-\mathbf{f}_1 - 3\mathbf{f}_2 + \mathbf{f}_3 - \mathbf{f}_4 + \mathbf{f}_5 + \mathbf{f}_6 + \mathbf{f}_7 - \mathbf{f}_8 - \mathbf{f}_9 - \mathbf{f}_{10} + \mathbf{f}_{11} - \mathbf{f}_{12} \\ & -\mathbf{f}_{13} - 3\mathbf{f}_{14} + \mathbf{f}_{15} - \mathbf{f}_{16} + \mathbf{f}_{17} + \mathbf{f}_{18} + \mathbf{f}_{19} - \mathbf{f}_{20} - \mathbf{f}_{21} - \mathbf{f}_{22} + \mathbf{f}_{23} - \mathbf{f}_{24}) \,.\end{aligned}$$

And we get

$$(\mathbf{x}_0, \mathbf{z}) = -\frac{1}{2} \notin \mathbb{Z} .$$

Example 2. When

$$(\zeta_1, \zeta_2, \cdots, \zeta_{24}) = (\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{2}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4})$$

then the shape of $\mathbf{z}$ is

$$\begin{aligned} \mathbf{z} \;=\; & \frac{1}{10}(-\mathbf{f}_1 - \mathbf{f}_2 - \mathbf{f}_3 - \mathbf{f}_4 + \mathbf{f}_5 - \mathbf{f}_6 + 3\mathbf{f}_7 + \mathbf{f}_8 - \mathbf{f}_9 + \mathbf{f}_{10} + \mathbf{f}_{11} + \mathbf{f}_{12} \\ & + \mathbf{f}_{13} + \mathbf{f}_{14} + \mathbf{f}_{15} + \mathbf{f}_{16} - \mathbf{f}_{17} + \mathbf{f}_{18} - 3\mathbf{f}_{19} - \mathbf{f}_{20} + \mathbf{f}_{21} - \mathbf{f}_{22} - \mathbf{f}_{23} - \mathbf{f}_{24}) . \end{aligned}$$

And we also get

$$(\mathbf{x}_0, \mathbf{z}) = -\frac{1}{2} \notin \mathbb{Z} .$$

Remaining 46 cases are treated similarly. Since $\mathbf{L}$ is integral, the vectors satisfying (15) can not belong to $\mathbf{L}$. Q.E.D.

We now return to the proof of the Theorem. By the above lemma, for the case (i) we have either $| t_\lambda | \geq 9$ for some $\lambda \in S_1$ or $| t_\lambda | \geq 7$ for some $\lambda \in S_2$. In the former case we get

$$(\mathbf{z}, \mathbf{z}) \geq \frac{1}{20}(21 + 81 + 9 * 2) > 5.$$

In the latter case we get

$$(\mathbf{z}, \mathbf{z}) \geq \frac{1}{20}(22 + 49 + 9) \geq 4.$$

Thus we have proved that $(\mathbf{z}, \mathbf{z}) \geq 4$ for any $\mathbf{z} \in \mathbf{L} - \mathbf{J}$. This completes the proof of the Theorem.

Q.E.D.

By a characterization of the Leech lattice ([1] , Theorem 7), the lattice $\mathbf{L}$ is the Leech lattice.

Appendix

We give a description of all codewords of weight 24 in $\mathbf{Q}_{24}$ with $j = 22$ and $k = 2$ (j and k are explained in the proof of **Theorem 1**). By observing the Lee weight enumerator of the code $\mathbf{Q}_{24}$, which is given in the second section, we see that there are 48 such codewords.
The codewords are divided into two different types. The repeat type is expressed as $(\mathbf{u}\ \mathbf{u})$, where $\mathbf{u}$ is a vector in $GF(5)^{12}$. The converse type is expressed as $(\mathbf{u}\ \mathbf{v})$, where $\mathbf{u}$ and $\mathbf{v}$ are vectors in $GF(5)^{12}$ such that $\mathbf{u}+\mathbf{v} = \mathbf{0}$, and $\mathbf{0}$ is the all $\overline{0}$ vector. In both types it is sufficient to give the first half vector $\mathbf{u}$. We give only 24 first codewords, because the rest codewords are obtained as scaler multiples by $\overline{4}$ of the codewords given above.

repeat type :

$(\overline{2}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{1})$, $(\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4})$

$(\overline{4}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1})$, $(\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1})$

$(\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4})$, $(\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4})$

$(\overline{4}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1})$, $(\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4})$

$(\overline{4}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1})$, $(\overline{4}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2})$

$(\overline{4}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4}\,\overline{1})$, $(\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{2}\,\overline{1}\,\overline{4})$

converse type :

$(\overline{2}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{4})$, $(\overline{4}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1})$

$(\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4})$, $(\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4})$

$(\overline{4}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1})$, $(\overline{4}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1})$

$(\overline{4}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1})$, $(\overline{4}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3})$

$(\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4})$, $(\overline{4}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1})$

$(\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4}\,\overline{3}\,\overline{1}\,\overline{4})$, $(\overline{4}\,\overline{3}\,\overline{1}\,\overline{4}\,\overline{1}\,\overline{1}\,\overline{1}\,\overline{4}\,\overline{4}\,\overline{4}\,\overline{1}\,\overline{4})$

References

[1] J.H.Conway, A characterization of Leech's lattice, Invent. Math. 7 (1969) 137-142.

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

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

[4] J.Leech and N.J.A.Sloane, Sphere packings and error-correcting codes, Can. J. Math., 23(1971) 718-745.

[5] J.S.Leon, V.Pless and N.J.A.Sloane, Self-dual codes over GF(5), J.Comb. Theory, Ser.A 32 (1982) 178-194.

[6] J.Lepowsky and A.Meurman, An E_8-approach to the Leech lattice and the Conway group, J. Alg. 77(1982) 484-504.

[7] F.J.MacWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes",North-Holland, Amsterdam, 1977.

[8] D.P.Maher, Modular forms from codes, Can. J. Math., 32(1980) 40-58.

[9] O.T.O'Meara, Introduction to quadratic forms, Springer-Verlag, 1963.

[10] M.Ozeki, On the structure of even unimodular extremal lattices of rank 40, Rocky Mountain J. Math. 19 (1989) 847-862

[11] M.Ozeki, Ternary code construction of even unimodular lattices, in the Proceedings of International Conference held at Quebec in 1987. ed.J.-M. De Koninck and C. Levesque, Walter de Gruyter, Berlin-New York (1989) 773-784

[12] M.Ozeki, On the extent of the usefulness of the linear codes to construct (extremal) even unimodular lattices , a talk at "Conference internationale de theorie des nombres , held at Laval University (1987).

[13] V.Pless, An Introduction to the Theory of Error-Correcting Codes, Wiley Interscience, New York, 1982.

[14] N.J.A.Sloane, Binary Codes, lattices, and sphere-packings in "Combinatorial Surveys, Proc. 6th British Comb. Conf." ed. by P.J.Cameron, Academic Press (1977) 117-164.

[15] N.J.A.Sloane, Self-dual codes and lattices, in "Relations between Combinatorics and Other Parts of Mathematics", Proc. Symp. in Pure Math., no.34 (1979) 273-308.

[16] J.Tits, Four presentations of Leech's lattice, in "Finite Simple Groups II", Proc. of a London Math. Soc. research Symposium,Durham, ed. M.J.Collins, Academic Press, 1980.

Department of Information Science
Faculty of Science
Hirosaki University
Bunkyo-cho 3, Hirosaki
036 Japan

Received August 20, 1991