On even lattices of 2-square type and self-dual codes

By Takashi TASAKA

To the memory of Takuro Shintani

Introduction.

The theory of integral quadratic forms has a long history. Here we restrict ourselves to the theory of definite even unimodular quadratic forms. If the quadratic form is definite, the theory can be translated to the theory of lattices in Euclidean space.

Let E_Ω $(=\boldsymbol{R}^N)$ be a Euclidean vector space of dimension N with an orthonormal basis $\{v_\alpha : \alpha\in\Omega\}$, where Ω is a finite set with N elements. As usual, we denote by $|\Omega|$ the cardinality of finite set Ω, thus $N=|\Omega|$. The canonical inner product in E_Ω is denoted by $l(x, y)$ for $x, y\in E_\Omega$, and $l(x)=l(x, x)$ is the squared length of the vector x in E_Ω. We call a vector x as m-vector, if $l(x)=m$. In this notation, we have

$$l(v_\alpha, v_\beta)=0 \quad (\alpha\neq\beta), \qquad l(v_\alpha)=1.$$

A lattice L in E_Ω is a free abelian subgroup of rank N in E_Ω. If $\{a_\alpha : \alpha\in\Omega\}$ is a basis of the lattice L $(a_\alpha=\sum a_{\beta\alpha}v_\beta,\ A=(a_{\alpha\beta}))$, we put

$$\omega(L)=|\det A|, \qquad d(L)=\det {}^tAA=\omega(L)^2.$$

($\omega(L)$ means the volume of the fundamental domain of the lattice L, and ${}^tAA=(l(a_\alpha, a_\beta))$ is the positive definite symmetric matrix representing the quadratic form which corresponds to the lattice L, and $d(L)$ is its discriminant.) Clearly these are independent on the choice of basis. Two lattices are called equivalent, if an orthogonal transformation transforms one to another. For a while, we call a lattice L as rational, if the corresponding matrix A is a rational matrix. Putting

$$L^0=\{y\in E_\Omega : l(y, x)\in\boldsymbol{Z} \text{ for all } x\in L\},$$

we call this L^0 the (integrally) dual lattice of L. It is easy to see that $[L^0 : L]=d(L)$ for a rational lattice L, where $[L^0 : L]$ means the generalised index.

By definition, if L is contained in L^0, we call L an integral lattice, and if $L=L^0$, we call L a unimodular lattice. If $l(x)\in 2\boldsymbol{Z}$ for all x in an integral lattice L, we call L an even lattice. An even unimodular lattice is a lattice

which is even and unimodular.

It is known that even unimodular lattices exist if and only if $N\equiv 0 \pmod 8$, and equivalence classes of these lattices in dimension N form only one genus C_N. The mass-formula of Minkowski-Siegel states that

$$\sum_{L\in C_N} |\mathrm{Aut}(L)|^{-1}=M_N,$$

where M_N is a rational number described explicitly by Bernoulli numbers and N [3], [5]. The class numbers h_N (that is the cardinality of C_N) are known for first three N's, that is, $h_8=1$ (L.-J. Mordell), $h_{16}=2$ (E. Witt [18]), and $h_{24}=24$ (H.-V. Niemeier [16]). But from the mass-formula, it follows that $h_{32}\geqq 8.10^7$ for example.

In this paper, we study the theory from different point of view, that is, from code-theoretic view point. The code-theoretic methods are known to be very powerful to the theory [7], [9], [22]. We follow that methods, and consider the relations between the even unimodular lattices and the even self-dual codes, and the relations [between the (binary) super codes and the self-dual $\boldsymbol{F}_4$-codes.

We begin our studies by preparing some elementary lemmas.

LEMMA A. *Every lattice is uniquely decomposed into a direct orthogonal sum* [12].

LEMMA B. *Let L be an even unimodular lattice, and $x\in\frac{1}{2}L$ be a vector such that $l(x)$ is (even) integer. Put $K_x=\{y\in L : l(x, y)\in \boldsymbol{Z}\}$. Then*

$$L_0=K_x+\boldsymbol{Z}\cdot x=K_x\cup\{x+K_x\}$$

is an (even) unimodular lattice [13], [16].

LEMMA C. *Let Λ be an even lattice. For subgroup $\Theta\subset\Lambda^0/\Lambda$, put*

$$\Lambda(\Theta)=\bigcup_{b\in\Theta}\{b+\Lambda\},$$

then $\Lambda(\Theta)$ is an even unimodular lattice if and only if $|\Theta|^2=[\Lambda^0:\Lambda]$ and for every $b\in\Theta$, $l(b)$ is even [16].

REMARK 1. For any $b\in\Theta$, we assume that b is contained in Λ^0, and that $l(b)$ is the minimum value in $b+\Lambda$, if it is possible and easy to choose.

2. From $2l(b, c)=l(b+c)-l(b)-l(c)$, we have $l(b, c)\in\boldsymbol{Z}$ for all $b, c\in\Theta$.

3. Clearly Lemma B is a special case of Lemma C, but we state them separately for the later convenience.

§ 1. Even lattices of 2-square type and even codes.

Let $\mathcal{H}$ be an even self-dual code on Ω. That is, $\mathcal{H}$ is a subgroup of $\mathcal{P}(\Omega)$ (the set of all subsets of Ω which is a vector space of dimension $N=|\Omega|$ over the two elements field $\boldsymbol{F}_2$ under the symmetric difference), such that $\mathcal{H}^0=\mathcal{H}$ and $|X|\equiv 0 \pmod 4$ for all $X\in\mathcal{H}$. Note that $\mathcal{P}(\Omega)$ has a symmetric bilinear form φ defined in the following way;

$$\varphi(X, Y)=|X\cap Y| \pmod 2 \in \boldsymbol{F}_2 \qquad \text{for any} \quad X, Y\in\mathcal{P}(\Omega),$$

to which the annihilator $\mathcal{H}^0$ of $\mathcal{H}$ is defined. (The theory of binary linear code will be discussed in some details in the subsequent sections.)

We take an orthogonal frame $F=\{\pm e_\alpha : \alpha\in\Omega\}$ of 2-vectors in the Euclidean space E_Ω. That is, $l(e_\alpha)=2$ and $l(e_\alpha, e_\beta)=0$ $(\alpha\neq\beta)$. By abuse of language, we call this frame F an orthogonal 2-frame. Then $\Lambda=\sum_{\alpha\in\Omega} \boldsymbol{Z} e_\alpha$ is an even lattice such that $\Lambda^0=\frac{1}{2}\Lambda$. For a subset X of Ω, we define e_X by

$$e_X=\sum_{\alpha\in X} e_\alpha . \tag{1}$$

From the above-mentioned code $\mathcal{H}$, we make the following lattice;

$$L(\mathcal{H})=\left\langle e_\alpha, \frac{1}{2}e_X : \alpha\in\Omega, X\in\mathcal{H}\right\rangle=\bigcup_{X\in\mathcal{H}}\left\{\frac{1}{2}e_X+\Lambda\right\}. \tag{2}$$

PROPOSITION 1. *For even self-dual code $\mathcal{H}$, the lattice $L(\mathcal{H})$ defined by* (2) *is even unimodular. (Thus even self-dual codes exist only if N is a multiple of* 8.)

PROOF. Noting that $X+Y=X\cup Y\setminus X\cap Y$ (the symmetric difference), we have

$$\frac{1}{2}e_X+\frac{1}{2}e_Y=\frac{1}{2}e_{X+Y}+e_{X\cap Y}, \tag{3}$$

$$l\left(\frac{1}{2}e_X\right)=\frac{1}{2}|X|, \tag{4}$$

$$l\left(\frac{1}{2}e_X+\sum_{\alpha\in\Omega} x_\alpha e_\alpha\right)=\frac{1}{2}|X|+2\sum_{\alpha\in X} x_\alpha(x_\alpha+1)+2\sum_{\alpha\notin X} x_\alpha^2 . \tag{5}$$

As $\Lambda^0/\Lambda=\mathcal{P}(\Omega)$ canonically, this proposition follows from Lemma C.

Especially in (5), $l\left(\frac{1}{2}e_X+\sum x_\alpha e_\alpha\right)=\frac{1}{2}|X|$, if and only if $x_\alpha=0$ or -1 $(\alpha\in X)$ and $x_\alpha=0$ $(\alpha\notin X)$. Thus the number of 2-vectors in $L(\mathcal{H})$ is

$$2N+2^4\omega_4 ,$$

where ω_4 is the number of tetrads in $\mathcal{H}$, that is, the cardinality of $\mathcal{H}_4=\{X\in\mathcal{H}: |X|=4\}$.

The automorphism group of a lattice L will be denoted by $G(L)$. For any $X\in\mathcal{P}(\Omega)$, we put $\varepsilon_X(e_\alpha)=-e_\alpha$ $(\alpha\in X)$ or e_α $(\alpha\notin X)$. Thus we have an isomorphism ε of $\mathcal{P}(\Omega)$ into $G(\Lambda)$, and we identify $\mathcal{P}(\Omega)$ as a subgroup of $G(\Lambda)$, sometimes. Clearly

$$G(\Lambda)=\mathcal{P}(\Omega)\rtimes S(\Omega), \quad \text{(semi-direct product)}$$

where $S(\Omega)$ is the symmetric group on the set Ω. The subgroup H of $G(L(\mathcal{H}))$ consisting the automorphisms which fix the orthogonal 2-frame F is also a subgroup of $G(\Lambda)$, and we have

$$H=\mathcal{P}(\Omega)\rtimes \operatorname{Aut}\mathcal{H}, \tag{6}$$

where $\operatorname{Aut}\mathcal{H}$ is the automorphism group of the code $\mathcal{H}$ which is the subgroup of $S(\Omega)$ stabilising the code $\mathcal{H}$.

It is remarkable that the index $[G(L(\mathcal{H})): H]$ is odd for many known cases.

If an even unimodular lattice L contains an orthogonal 2-frame $F=\{\pm e_\alpha : \alpha\in\Omega\}$, we call L of *2-square type*. In this case, we have $\Lambda\subset L\subset\frac{1}{2}\Lambda=\Lambda^0$. For $x=\sum x_\alpha e_\alpha\in L$, putting

$$X=X(x)=\{\alpha\in\Omega : x_\alpha\notin\boldsymbol{Z}\}\subset\Omega,$$

we get a code $\mathcal{H}=\mathcal{H}_L=\langle X(x): x\in L\rangle$ on the set Ω.

PROPOSITION 2. *Let L be an even unimodular lattice of 2-square type. The code $\mathcal{H}_L$ defined by L is an even self-dual code.*

PROOF. From definition, we have

$$X(x+y)=X(x)+X(y), \qquad \text{for } x, y\in L,$$

$$x=\frac{1}{2}e_{X(x)}+\sum x'_\alpha e_\alpha, \qquad \text{for some } x'_\alpha\in\boldsymbol{Z}.$$

As $\frac{1}{2}e_{X(x)}\in L$ for $x\in L$, we have $|X(x)|\equiv 0 \pmod 4$. From $|X+Y|=|X|+|Y|-2|X\cap Y|$, it follows that $|X\cap Y|\equiv 0 \pmod 2$, for any $X, Y\in\mathcal{H}$, that is, $\mathcal{H}\subset\mathcal{H}^0$. As $L=L(\mathcal{H})$, we have $|\mathcal{H}|=2^{N/2}$ from Lemma C. That is, $\dim\mathcal{H}=\frac{1}{2}N$ and $\dim\mathcal{H}^0=N-\frac{1}{2}N=\frac{1}{2}N$, where $\dim\mathcal{H}$ means the dimension over $\boldsymbol{F}_2$ of the vector subspace $\mathcal{H}$, for example. This shows that $\mathcal{H}^0=\mathcal{H}$.

Thus we have a one-to-one correspondence between even self-dual codes and even unimodular lattices of 2-square type, by fixing an orthogonal 2-frame.

To decomposable lattice, it corresponds "decomposable" code, for example. Moreover we can remove the unimodularity condition, so to even lattice of 2-square type, it corresponds even code (a code C such that $C\subset C^0$ and $|X|\equiv 0 \pmod 4$ for all $X\in C$). These facts are already noticed by several authors [7], [9], [22]. In the list of Niemeier [16], nine of twenty four classes are lattices of 2-square type which can be described by the canonical decompositions of the next section. Two of them are decomposable and the others are indecomposable. There is another special class which is the class of Leech lattice [10], [14], its generalisations will be given in § 3.

§ 2. The cores of lattices and codes.

Let $\mathcal{H}$ be an even self-dual code on the set Ω, and L be the corresponding lattice of 2-square type with orthogonal 2-frame $F=\{\pm e_\alpha : \alpha\in\Omega\}$. We call a subset $X\in\mathcal{H}$ such that $|X|=4$ a tetrad in $\mathcal{H}$. Putting $\mathcal{H}_4=\{X\in\mathcal{H} : |X|=4\}$ (the set of all tetrads in $\mathcal{H}$), we consider a code C generated by $\mathcal{H}_4$. Thus $C\subset\mathcal{H}\subset\mathcal{P}(\Omega)$. We call this code C the core code of $\mathcal{H}$. If we put $h=\dim\mathcal{H}-\dim C=\frac{1}{2}N-\dim C$, there should exist linearly independent (over $\boldsymbol{F}_2$) subsets $Y_1,\cdots,Y_h$ such that C and Y_j $(1\leqq j\leqq h)$ generate the code $\mathcal{H}$. These subsets will be called the *extra subsets* for $\mathcal{H}\supset C$. For non-empty subset $Z\in\mathcal{H}$ which is not in $\mathcal{H}_4$, we must have $|Z|\geqq 8$. Especially $|Y_j|\geqq 8$ for all Y_j.

We define an equivalence relation on Ω in the following way. For $\alpha,\beta\in\Omega$, we write $\alpha\sim\beta$ if either $\alpha=\beta$ or α and β can be joined by a sequence of tetrads in $\mathcal{H}$ (that is, there exist $X_i\in\mathcal{H}_4$ $(1\leqq i\leqq m)$ such that $\alpha\in X_1$ and $\beta\in X_m$ and $X_i\cap X_{i+1}\neq\emptyset$). Decomposing into equivalence classes, we have

$$\Omega=\Delta_1\cup\Delta_2\cup\cdots\cup\Delta_\tau . \tag{7}$$

For each Δ_i, putting

$$C(\Delta_i)=\langle X\in\mathcal{H}_4 : X\subset\Delta_i\rangle ,$$

we have a code $C(\Delta_i)$ on Δ_i, and the canonical decomposition of the core code C;

$$C=\sum_{i=1}^{\tau} C(\Delta_i)=C(\Delta_1)\oplus\cdots\oplus C(\Delta_\tau) . \tag{8}$$

This decomposition is unique upto permutations of its components.

Now we consider the core lattice M of L and its canonical decomposition. For each Δ_i, we put

$$L(\Delta_i)=\left\langle e_\alpha, \frac{1}{2}e_X : \alpha\in\Delta_i,\ X\subset\Delta_i,\ X\in\mathcal{H}_4\right\rangle=\bigcup_{X\in C(\Delta_i)}\left\{\frac{1}{2}e_X+\Lambda_i\right\},$$

where $\Delta_i=\sum_{\alpha\in\Delta_i} Ze_\alpha$, and $\Delta=\sum_{i=1}^{r}\Delta_i$. Putting

$$M=\sum L(\Delta_i)=L(\Delta_1)\perp\cdots\perp L(\Delta_r), \tag{9}$$

we call M the core lattice of L and (9) the canonical decomposition of M. Clearly $M\subset L\subset M^0$, and from Lemma C, there exists a subgroup $\Theta=L/M\subset M^0/M$ such that $L=M(\Theta)$. We call this subgroup Θ the *extra subgroup* for $L\supset M$. Note that, for any non-zero element $b\in\Theta$, we must have $l(b)\geqq 4$.

From definition, each $L(\Delta_i)$ is generated by 2-vectors and contains an orthogonal 2-frame $\{\pm e_\alpha : \alpha\in\Delta_i\}$. These lattices are well-known from the theory of root system of complex semi-simple Lie algebras [6], [19]. Each $L(\Delta_i)$ is isomorphic to the one of the following even lattices:

$$A_1,\ D_{2m},\ E_7 \text{ and } E_8, \tag{10}$$

where these are included in the following general lattices:

$$A_n=\Big\{x=\sum_{i=1}^{n+1} x_iv_i : x_i\in\boldsymbol{Z},\ \sum x_i=0\Big\},$$

$$D_n=\Big\{x=\sum_{i=1}^{n} x_iv_i : x_i\in\boldsymbol{Z},\ \sum x_i\equiv 0 \pmod 2\Big\},$$

$$E_8=\Big\{x=\sum_{i=1}^{8} x_iv_i : 2x_i,\ x_i-x_j\in\boldsymbol{Z},\ \sum x_i\equiv 0 \pmod 2\Big\},$$

and E_7 is the sublattice of E_8 consisting $x=\sum x_iv_i\in E_8$ such that $\sum x_i=0$, where $\{v_i\}$ is an orthonormal basis in the respective spaces. Note that E_8 is an even unimodular lattice and is always an orthogonal summand in even unimodular lattices which contain E_8.

It is easy to take orthogonal 2-frames in the lattices listed in (10). Thus the decomposition (9) of the core lattice M of even unimodular lattice L of 2-square type is easy to see. Conversely, from a direct (orthogonal) sum M of lattices listed in (10), we can construct an even unimodular lattice whose core is M, if and only if we can find a suitable extra subgroup in M^0/M. The same is also true for codes. We call these procedures the *saturations* of lattices and codes.

Clearly an automorphism of L induces an automorphism of its core lattice M (see the action on 2-vectors in L). Conversely, an automorphism of M induces an automorphism of L if and only if it stabilises the extra subgroup Θ modulo M. Thus we have

$$H=\mathcal{P}(\Omega)\rtimes \mathrm{Aut}\,\mathcal{H}\subset G(L)\subset G(M). \tag{11}$$

The group $G(M)$ is easy to determine. That is, $G(M)$ is described by the

groups $G(L(\Delta_i))$ and the interchanges between isomorphic factors in $L(\Delta_i)$ $(1\leqq i\leqq r)$. The group $G(X_n)$ is well-known, where X_n is a lattice listed in (10).

Similarly, the automorphism group $\mathrm{Aut}\,\mathcal{H}$ of $\mathcal{H}$ is the subgroup of the group $\mathrm{Aut}\,C$ of its core code C which stabilises the extra subsets modulo C. If we denote by $\mathcal{X}_n$ the even code corresponding to the lattice X_n, the group $\mathrm{Aut}\,\mathcal{X}_n$ is also known, and the group $\mathrm{Aut}\,C$ is described by these groups and the interchanges of isomorphic factors. We list them in a table with some explanations;

A_1	$G(A_1)=2$	$\mathrm{Aut}\,\mathcal{A}_1=1$
D_4	$G(D_4)=(2^3S_4)\cdot S_3$	$\mathrm{Aut}\,\mathcal{D}_4=S_4$
D_{2m} $(m>2)$	$G(D_{2m})=2^{2m}\cdot S_{2m}$	$\mathrm{Aut}\,\mathcal{D}_{2m}=2^m\cdot S_m$
E_7	$G(E_7)=W(E_7)$	$\mathrm{Aut}\,\mathcal{E}_7=SL(3,2)=PSL(2,7)$
E_8	$G(E_8)=W(E_8)$	$\mathrm{Aut}\,\mathcal{E}_8=Af(3,2)=2^3\cdot SL(3,2)$

Explanations: The group $G=A\cdot B=AB$ means the extension of A by B. The group S_n is the symmetric group on n letters, and the group 2^n is an elementary 2-group of length n. $W(X_n)$ means the Weyl group of the root system X_n. Note that $G(D_n)=2\cdot W(D_n)=W(D_n)\cdot 2$ for $n>4$.

§3. The super codes and the related lattices.

For an even self-dual code $\mathcal{H}$ on the set Ω, if there are no tetrads in $\mathcal{H}$, that is, for any non-zero $X\in\mathcal{H}$, we have $|X|>4$, we call this $\mathcal{H}$ a *super code* on Ω. In this case, any two points in Ω are not equivalent to each other, and the core lattice of the lattice $L(\mathcal{H})$ defined by $\mathcal{H}$ is $\Lambda=N\times A_1$ (the direct sum of N lattices isomorphic to A_1). The automorphism group $G(\Lambda)=G(N\times A_1)$ is clearly $\mathcal{P}(\Omega)\rtimes S(\Omega)$, and the number of 2-vectors in $L(\mathcal{H})$ is equal to $2N$.

THEOREM 1. *Let $\mathcal{H}$ be a super code, and $L(\mathcal{H})$ be the corresponding lattice. Then we have*

$$G(L(\mathcal{H}))=\mathcal{P}(\Omega)\rtimes\mathrm{Aut}\,\mathcal{H}=2^N\cdot\mathrm{Aut}\,\mathcal{H}\,. \tag{12}$$

PROOF. Each automorphism λ stabilises the orthogonal 2-frame F, so we can write $\lambda=\varepsilon_Y\cdot\sigma$, with $Y\in\mathcal{P}(\Omega)$ and $\sigma\in S(\Omega)$, and we have

$$\lambda\Big(\frac{1}{2}e_X\Big)=\varepsilon_Y\Big(\frac{1}{2}e_{\sigma(X)}\Big)=\frac{1}{2}e_{\sigma(X)}-\sum_{\beta\in Z}e_\beta\,, \tag{13}$$

where $Z=\sigma(X)\cap Y$. Thus $\sigma\in\mathrm{Aut}\,\mathcal{H}$.

For any $Y\in\mathcal{P}(\Omega)$, ε_Y is clearly contained in $G(L(\mathcal{H}))$. Q.E.D.

We fix an element α of Ω, and put

$$x=\frac{1}{4}e_\Omega, \quad \text{and} \quad y=\frac{1}{4}e_\Omega-e_\alpha. \tag{14}$$

As $\mathcal{H}$ is self-dual, so $\mathbf{1}=\Omega$ is contained in $\mathcal{H}$. Thus $x, y\in\frac{1}{2}L(\mathcal{H})$ and $l(x)=\frac{1}{8}N$, $l(y)=\frac{1}{8}N+1$. By easy computations, we know that K_x and K_y are equal to

$$K=\left\langle \frac{1}{2}e_X,\ \sum x_\beta e_\beta : X\in\mathcal{H},\ \sum x_\beta\equiv 0 \pmod 2\right\rangle,$$

where $K_x=\{z\in L(\mathcal{H}): l(z, x)\in\boldsymbol{Z}\}$, for example. We put

$$L_0(\mathcal{H})=K\cup\{x+K\}, \tag{15}$$

$$L_1(\mathcal{H})=K\cup\{y+K\}. \tag{16}$$

As $e_\alpha-e_\beta\in K$, $L_1(\mathcal{H})$ is independent on the choice of α.

From Lemma B, it follows that $L_0(\mathcal{H})$ and $L_1(\mathcal{H})$ are unimodular lattices whose arithmetic minima are 3 or 4. Especially $L_j(\mathcal{H})$ is even unimodular, if we put $\frac{1}{8}N\equiv j \pmod 2$.

Let i be 0 or 1. Though the lattice $L_i(\mathcal{H})$ does not contain the orthogonal 2-frame F, we define $G_0(L_i(\mathcal{H}))$ as the subgroup of $G(L_i(\mathcal{H}))$ which stabilises the frame F.

THEOREM 2. *Let $\mathcal{H}$ be a super code, and i be 0 or 1. Then*

$$G_0(L_i(\mathcal{H}))=\mathcal{H}\rtimes\operatorname{Aut}\mathcal{H}, \quad \textit{(semi-direct product)}. \tag{17}$$

PROOF. Any element $\lambda\in G_0(L_i(\mathcal{H}))$ can be written $\lambda=\varepsilon_Y\cdot\sigma$, with $Y\in\mathcal{P}(\Omega)$ and $\sigma\in S(\Omega)$. We have, respectively,

$$\lambda\left(\frac{1}{4}e_\Omega\right)=\frac{1}{4}e_\Omega-\frac{1}{2}e_Y,$$

$$\lambda\left(\frac{1}{4}e_\Omega-e_\alpha\right)=\frac{1}{4}e_\Omega-\frac{1}{2}e_Y+\delta e_{\sigma(\alpha)}$$

$$=\frac{1}{4}e_\Omega-e_\alpha+(e_\alpha+\delta e_{\sigma(\alpha)})-\frac{1}{2}e_Y,$$

where δ is 1 or -1. As $\frac{1}{2}e_Y$ should be in $L_i(\mathcal{H})$, so $Y\in\mathcal{H}$, that is, $\varepsilon_Y\in\mathcal{H}$. From (13), it follows that $\sigma(X)\in\mathcal{H}$ for all $X\in\mathcal{H}$. Thus $\sigma\in\operatorname{Aut}\mathcal{H}$. Note that $|\sigma(X)\cap Y|\equiv 0 \pmod 2$ for $X, Y\in\mathcal{H}$, if $\sigma\in\operatorname{Aut}\mathcal{H}$. Q.E.D.

The full automorphism group $G(L_i(\mathcal{H}))$ seems to be very difficult to deter-

mine. It is also remarkable that the index $[G: G_0]$ is odd for the known cases.

If $N<24$, there exist no super codes. If $N=24$, super code is unique upto equivalence. This code is the binary Golay code $\mathcal{G}$ generated by the octads of the Steiner system $S(5, 8, 24)$ whose automorphism group is the Mathieu group M_{24}. The corresponding even unimodular lattice $L_1(\mathcal{G})$ is the Leech lattice whose automorphism group is the Conway's perfect group .0 [10], [11]. Thus the index $[.0: 2^{12}\cdot M_{24}]$ is equal to $3^6 5^3\cdot 7\cdot 13$.

If $N=32$, there exist five classes of super codes, one of which is defined by a certain affine code $\mathcal{A}$ (or Reed-Muller code), whose automorphism group is the affine group $Af(5, 2)$ of the five dimensional affine space over $\boldsymbol{F}_2$. The automorphism group of the corresponding lattice $L_0(\mathcal{A})$ is determined by Broué and Enguehard [8]. This group is a non-splitting extension of extra special 2-group of plus type of order 2^{11} by the Chevalley group $D_5(2)$. Thus the index is equal to $3^5\cdot 5\cdot 17$. Note that Broué and Enguehard have determined the automorphism groups of even (unimodular) lattices in infinite series.

§ 4. Constructions of super codes.

For a finite set Ω such that $N=|\Omega|$ is a multiple of 8, we denote by $\mathcal{P}(\Omega)$ the set of all subsets of Ω which is a vector space over $\boldsymbol{F}_2$ of dimension N with respect to the symmetric difference. We denote by $\mathbf{0}$ the empty subset of Ω and by $\mathbf{1}$ the total subset Ω. The space $\mathcal{P}(\Omega)$ has the symmetric bilinear form φ defined by $\varphi(X, Y)=|X\cap Y| \pmod 2\in\boldsymbol{F}_2$. We denote by $\mathcal{P}_0(\Omega)$ the set of all subsets of Ω with even cardinality. Then we have

$$\mathcal{P}_0(\Omega)^0=\mathcal{P}_\infty(\Omega)=\{\mathbf{0}, \mathbf{1}\}, \tag{18}$$

where C^0 means the annihilator of C with respect to the form φ, for a subspace (a code) C of $\mathcal{P}(\Omega)$. Clearly $\mathcal{P}_0(\Omega)$ is a subspace of $\mathcal{P}(\Omega)$ of dimension $N-1$, and $\mathcal{P}_\infty(\Omega)$ is a subspace of dimension 1. On the subspace $\mathcal{P}_0(\Omega)$, we define a quadratic form q by putting $q(X)=0$ if $|X|\equiv 0 \pmod 4$ and $q(X)=1$ if $|X|\equiv 2 \pmod 4$. We have

$$q(X+Y)=q(X)+q(Y)+\varphi(X, Y),$$

so q is a quadratic form on $\mathcal{P}_0(\Omega)$ with the associated bilinear form φ. Now we consider the automorphism group $\mathrm{Aut}(\mathcal{P}(\Omega), \varphi)$ and the orthogonal group $O(\mathcal{P}_0(\Omega), q)$. These groups are determined in Dieudonné's [25] (pp. 60-63 and pp. 39-51). Fixing an element α of Ω, we have the decompositions;

$$\mathcal{P}(\Omega)=\mathcal{P}_0(\Omega)\oplus\langle\Omega_\alpha\rangle=\mathcal{P}_\infty(\Omega)\oplus\mathcal{L}_\alpha\oplus\langle\Omega_\alpha\rangle,$$

$$\mathcal{P}_0(\Omega)=\mathcal{P}_\infty(\Omega)\oplus\mathcal{L}_\alpha,$$

where $\Omega_\alpha=\Omega\setminus\{\alpha\}$ and $\mathcal{L}_\alpha=\mathcal{P}_0(\Omega_\alpha)$. The space $\mathcal{P}_0(\Omega)$ is the subspace of all X such that $\varphi(X, X)=0$, the space $\mathcal{P}_\infty(\Omega)$ is $\mathcal{P}_0(\Omega)\cap\mathcal{P}_0(\Omega)^0$. The space $\mathcal{L}_\alpha$ is a complementary subspace of $\mathcal{P}_\infty(\Omega)$ in $\mathcal{P}_0(\Omega)$, and the space $\langle\Omega_\alpha\rangle$ is a complementary subspace of $\mathcal{P}_0(\Omega)$ in $\mathcal{P}(\Omega)$ which is also complementary to $\mathcal{P}_\infty(\Omega)$ in $\mathcal{L}_\alpha^0=\langle\mathbf{1}, \Omega_\alpha\rangle$. Note that φ induces a non-degenerate alternative form on $\mathcal{L}_\alpha$, and that q induces a non-degenerate and non-defective quadratic form on $\mathcal{L}_\alpha$. Then we have

$$1 \longrightarrow \langle\eta\rangle \longrightarrow \mathrm{Aut}(\mathcal{P}(\Omega), \varphi) \xrightarrow{\rho} G \longrightarrow 1,$$

$$G\cong\mathcal{L}_\alpha\rtimes S\mathfrak{p}(\mathcal{L}_\alpha),$$

$$O(\mathcal{P}_0(\Omega), q)\cong\mathcal{L}_\alpha\rtimes O(\mathcal{L}_\alpha, q),$$

where ρ is the restriction of automorphisms to the space $\mathcal{P}_0(\Omega)$, and η is the automorphism of $\mathcal{P}(\Omega)$ defined by $\eta(X)=X+|X|\mathbf{1}$, and $\mathcal{L}_\alpha$ is identified with the subgroup of G consisting the restrictions of λ_B $(B\in\mathcal{L}_\alpha)$ defined by $\lambda_B(\mathbf{1})=\mathbf{1}$, $\lambda_B(X)=X+\varphi(B, X)\mathbf{1}$ and $\lambda_B(\Omega_\alpha)=B+\Omega_\alpha$. Note that the quadratic form q is degenerate form with radical $\mathcal{P}_\infty(\Omega)$. The orthogonal group $O(\mathcal{L}_\alpha, q)$ is generated by orthogonal transvections [25], pp. 41-42;

$$t_A(X)=X+\varphi(A, X)A, \quad \text{for} \quad X\in\mathcal{L}_\alpha,$$

where A is an element of $\mathcal{L}_\alpha$ such that $q(A)=1$, that is, $|A|\equiv 2 \pmod 4$.

Looking the definition of t_A, we define a linear automorphism τ_A of $\mathcal{P}(\Omega)$ by

$$\tau_A(X)=X+\varphi(A, X)A=X+|A\cap X|A, \tag{19}$$

for any $X\in\mathcal{P}(\Omega)$, where A is an element of $\mathcal{P}_0(\Omega)$ such that $q(A)=1$. Clearly τ_A is in $\mathrm{Aut}(\mathcal{P}(\Omega), \varphi)$ and its restriction to $\mathcal{P}_0(\Omega)$ is an orthogonal transformation. Note that, if $|A|=2$, τ_A is the transformation induced by a transposition of Ω. From the formula

$$\tau_A(\tau_B(X))=X+|A\cap X|A+|B\cap X|B+|B\cap X|\cdot|A\cap B|A,$$

it follows that $\tau_A^2=\mathrm{id}$ and

$$\tau_B\tau_A\tau_B=\tau_{\tau_B(A)}. \tag{20}$$

That is, $\tau_B\tau_A=\tau_A\tau_B$ if $|A\cap B|\equiv 0 \pmod 2$, and $\tau_B\tau_A\tau_B=\tau_{A+B}=\tau_A\tau_B\tau_A$ if $|A\cap B|\equiv 1 \pmod 2$. Thus the group generated by τ_A is the group generated by 3-transpositions [26].

For an even self-dual code $\mathcal{H}$ on the set Ω, $\tau(\mathcal{H})$ is also an even self-dual code, where τ is in $O(\mathcal{P}_0(\Omega), q)$, and any even self-dual code can be obtained in this way. As λ_B stabilises any self-dual code, because $\lambda_B(X)=X$ or $X+\mathbf{1}$ for $X\in\mathcal{P}_0(\Omega)$, so it suffices to determine the actions of the transformations τ_A on

each even self-dual code.

Let $\mathcal{H}$ be an even self-dual code on Ω and A be an element of $\mathcal{P}_0(\Omega)$ such that $q(A)=1$. Assume that $\tau_A(\mathcal{H})$ is a super code. Then for all tetrads X in $\mathcal{H}$, we must have

$$|A\cap X|=1 \text{ or } 3, \tag{21}$$

because $\tau_A(X)=X+|A\cap X|A$. Thus

THEOREM 3. *Any super code is obtained from a saturation of core code of type* $a\times\mathcal{A}_1\oplus b\times\mathcal{D}_4$, *by a transformation* τ_A.

PROOF. Except for A_1 and D_4, we can not find any subset A which satisfies the condition (21) for all tetrads in the codes corresponding to the even lattices listed in (10).

For a saturation of a code $\mathcal{C}=a\times\mathcal{A}_1\oplus b\times\mathcal{D}_4$ on the set

$$\Omega=\{1,\cdots,a\}\cup X_1\cup\cdots\cup X_b,$$

where $X_i=\{1_i, 2_i, 3_i, 4_i\}$, we must find extra subsets $Y_1,\cdots,Y_h$ with $h=\frac{1}{2}a+b$, such that any linear combination Z of X_i $(1\leqq i\leqq b)$ and Y_j $(1\leqq j\leqq h)$ other than $\mathbf{0}$ or X_i $(1\leqq i\leqq b)$ has the cardinality $|Z|\geqq 8$. Of course, we must have also $|Z|\equiv 0 \pmod 4$. We don't know whether one can obtain always super codes from these saturations.

Now we consider the special case, that is, the saturations of core code $b\times\mathcal{D}_4$. In the lattice D_4, we fix an orthogonal 2-frame;

$$e_1=v_1+v_2,\quad e_2=v_1-v_2,\quad e_3=v_3+v_4,\quad e_4=v_3-v_4.$$

Then D_4 is generated by e_i $(1\leqq i\leqq 4)$ and $\frac{1}{2}(e_1+e_2+e_3+e_4)=v_1+v_3$, and the quotient group D_4^0/D_4 has the representatives 0, $\frac{1}{2}(e_1+e_3)$, $\frac{1}{2}(e_1+e_2)$ and $\frac{1}{2}(-e_2+e_3)$. Thus for the corresponding even code $\mathcal{D}_4$, we have $\mathcal{D}_4=\{\mathbf{0}, \mathbf{1}=\{1, 2, 3, 4\}\}$, and $\{1, 2\}$, $\{1, 3\}$ and $\{2, 3\}$ are the pre-extra subsets for $\mathcal{D}_4^0\supset\mathcal{D}_4$.

We will show that some saturations of $b\times\mathcal{D}_4$ can be constructed by certain self-dual $\boldsymbol{F}_4$-codes over a set with b elements, where $\boldsymbol{F}_4$ is the field with four elements.

Let ω be a root of the quadratic equation $x^2+x+1=0$ over $\boldsymbol{F}_2$. Then ω^2 is another root, and we have $\omega^3=1$ and $1+\omega=\omega^2$. We fix the correspondence ϕ between $\boldsymbol{F}_4=\{0, 1, \omega, \omega^2\}$ and $\mathcal{D}_4^0/\mathcal{D}_4$, by putting

$$0\leftrightarrow\mathbf{0},\quad 1\leftrightarrow\{1, 2\},\quad \omega\leftrightarrow\{1, 3\},\quad \omega^2\leftrightarrow\{2, 3\}, \tag{22}$$

which is an isomorphism between abelian groups.

On the vector space $\boldsymbol{F}_4^{\Delta}=\boldsymbol{F}_4^b$ over $\boldsymbol{F}_4$ of dimension b, where $\Delta=\{1, 2, \cdots, b\}$, we consider a hermitian form h;

$$h(u, v)=\sum_{i=1}^{b} u_i\cdot\bar{v}_i,$$

where $u=(u_1, \cdots, u_b)$, $v=(v_1, \cdots, v_b)\in\boldsymbol{F}_4^b$, and $\bar{v}_i=v_i^2$ (the canonical conjugation in $\boldsymbol{F}_4$). A self-dual $\boldsymbol{F}_4$-code $\mathcal{F}$ on Δ is a subspace $\mathcal{F}$ of $\boldsymbol{F}_4^b$ such that $\mathcal{F}^*=\mathcal{F}$, where $\mathcal{F}^*$ means the annihilator of $\mathcal{F}$ with respect to the form h[22]. The weight of $u\in\boldsymbol{F}_4^b$ is the number of non-zero components of u and will be denoted by $w(u)$. Then for a self-dual $\boldsymbol{F}_4$-code $\mathcal{F}$, we have $w(u)\equiv 0 \pmod 2$ for all $u\in\mathcal{F}$. We consider a self-dual $\boldsymbol{F}_4$-code $\mathcal{F}$ on Δ such that

$$w(u)>2, \quad \text{for all non-zero } u\in\mathcal{F}. \tag{23}$$

For a binary code $b\times\mathcal{D}_4$ on the set $\Omega=X_1\cup\cdots\cup X_b$, we define the extra subsets Y_u and Z_u, by the correspondence ϕ of (22),

$$Y_u=\sum_i \phi(u_i)_i, \quad Z_u=\sum_i \phi(\omega u_i)_i, \tag{24}$$

where $u\in\mathcal{F}$, and the sums are the symmetric differences (the disjoint sums in this case). Note that $Z_u=Y_{\omega u}$ and there corresponds the subset Y_u+Z_u to the vector $\omega^2 u$. As $\mathcal{F}$ is of dimension $\frac{1}{2}b$ over $\boldsymbol{F}_4$, we can choose b linearly independent (over $\boldsymbol{F}_2$) extra subsets. From the condition (23), we have

$$|Y_u|\equiv 0 \pmod 4 \quad \text{and} \quad |Y_u|\geqq 8,$$

for all non-zero $u\in\mathcal{F}$. The same holds for Z_u. Thus

THEOREM 4. *Some saturation of $b\times\mathcal{D}_4$ is constructed by self-dual code over $\boldsymbol{F}_4$ on a set with b elements which satisfies the condition* (23), *in the above-mentioned way.*

The converse of Theorem 4 is not true in general. That is, there could exist some saturation of $b\times\mathcal{D}_4$ which does not correspond to any self-dual $\boldsymbol{F}_4$-code.

It seems that there are no general methods to choose the subset A of Theorem 3, in order to construct super codes from the saturations of $a\times\mathcal{A}_1\oplus b\times\mathcal{D}_4$. Here we indicate two examples, though the derived codes are already known ones.

In $\boldsymbol{F}_4^6$, there is only one self-dual code, upto equivalence, which satisfies the condition (23). Its generator matrix is

$$\begin{pmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{pmatrix},$$

that is, three rows of this matrix is a basis of our code [22]. The corresponding binary code is a saturation of $6\times\mathcal{D}_4$. Putting

$$A=\{4_1, 4_2, \cdots, 4_6\},$$

we consider the transformation τ_A of (19). Checking the effects of τ_A on the tetrads and the other elements of the code, we see that the derived code is super code which is equivalent to the Golay code.

In $\boldsymbol{F}_4^8$, we consider a code with the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Then this code is a self-dual code satisfying the condition (23), which is also unique upto equivalence [22]. In the corresponding binary code which is a saturation of $8\times\mathcal{D}_4$, we consider the transformation τ_A, by putting $A_0=\{4_1, 4_2, \cdots, 4_8\}$ and $A=A_0+X_1$. Similarly as above, the derived code is a super code.

References

[1] Milnor, J. and D. Husemoller, Symmetric bilinear forms, Springer, 1973.

[2] O'Meara, O. T., Introduction to quadratic forms, Springer, 1971.

[3] Serre, J.-P., Cours d'arithmétique, Presses Univ. France, 1970.

[4] Siegel, C. L., Über die analytische Theorie der quadratischen Formen, Ann. of Math. **36** (1935), 527-606. (Gesam. Abh. I, pp. 326-405.)

[5] Siegel, C. L., Über die Fourierschen Koeffizienten der Eisensteinschen Reihen, Danske Vid. Selsk. Mat.-fys. Medd. **34** (1964), Nr. 6. (Gesam. Abh. III, pp. 443-458.)

[6] Bourbaki, N., Groupes et algèbres de Lie, Chap. IV, V, VI, Hermann, 1968.

[7] Broué, M. and M. Enguehard, Polynômes des poids de certains codes et fonctions théta de certains reseaux, Ann. Sci. Ećole Norm. Sup. **5** (1972), 151-181.

[8] Broué, M. and M. Enguehard, Une famille infinie de formes quadratiques entieres; leur groupes d'automorphismes, Ann. Sci. Ećole Norm. Sup. **6** (1973), 17-52.

[9] Broué, M., Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux elements et formes quadratiques entieres definies positives à discriminant +1, Discrete Math. **17** (1977), 247-269.

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

[11] Conway, J. H., Three lectures on exceptional groups, pp. 215-247 of Finite Simple Groups, edited by M. B.Powell and G. Higman, Acad. Press, 1971.

[12] Kneser, M., Zur Theorie der Kristallgitter, Math. Ann. **127** (1954), 105-106.
[13] Kneser, M., Klassenzahlen definiter quadratischer Formen, Arch. Math. 8 (1957), 241-250.
[14] Leech, J., Notes on sphere packings, Canad. J. Math. **19** (1967), 251-267.
[15] Milnor, J., On simply connected manifolds, Symp. Mexico, 1958, p. 122-126.
[16] Niemeier, H.-V., Definite quadratische Formen der Dimension 24 und Diskriminante 1, J. Number Theory **5** (1973), 142-178.
[17] Tits, J., Quaternions over $Q(\sqrt{5})$, Leech's lattice and the sporadic group of Hall-Janko, J. Algebra **63** (1980), 56-75.
[18] Witt, E., Eine Identität zwischen Modulformen zweiten Grades, Abh. Math. Sem. Univ. Hamburg **14** (1941), 323-337.
[19] Witt, E., Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe, Abh. Math. Sem. Univ. Hamburg 14 (1941), 289-322.
[20] MacWilliams, F. J. and N. J. A. Sloane, The theory of error-correcting Codes, North-Holland, 1978.
[21] Pless, V. and N. J. A. Sloane, Binary self-dual codes of length 24, Bull. Amer. Math. Soc. 80 (1974), 1173-1178.
[22] Sloane, N. J. A., Self dual codes and lattices, pp. 273-308 of Proc. Symp. Pure Math. 34, Amer. Math. Soc., 1979.
[23] Carter, R. W., Simple groups of Lie type, John Wiley and Sons, 1972.
[24] Coxeter, H. S. M. and W. O. J. Moser, Generators and relations for discrete groups, 2nd Ed. Springer, 1965.
[25] Dieudonné, J., Sur les groups classiques, Hermann, 1967.
[26] Fischer, B., Finite groups generated by 3-transpositions, I. Invent. Math. **13** (1971), 232-246.

(Received April 3, 1981)

Department of Mathematics
College of General Education
University of Tokyo
Komaba, Meguro-ku, Tokyo
153 Japan