J. Math. Soc. Japan
Vol. 43, No. 1, 1991

Even lattices and doubly even codes

Dedicated to Professor Tosiro Tsuzuku on his 60th birthday

By Masaaki KITAZUME, Takeshi KONDO
and Izumi MIYAMOTO

(Received April 25, 1989)
(Revised Dec. 1, 1989)

§1. The main results.

1.0. Several methods to construct even (unimodular) lattices from doubly even (self-dual) codes are known (cf. [**1**], [**2**], [**4**], [**10**], [**11**]). For some of such constructions, we will deal with the problem whether non-equivalent codes yield non-isomorphic lattices. Our main results are Theorems 1, 2 and 3 stated below.

1.1. Let Ω_n be a set of n letters $1, 2, \cdots, n$ and $P(\Omega_n)$ be the power set of Ω_n, i.e. the set of all subsets of Ω_n. $P(\Omega_n)$ is regarded as a vector space over the field of 2 elements with respect to the symmetric difference: $X+Y=(X\cup Y)-(X\cap Y)$, where $X, Y\in P(\Omega_n)$. A code of length n is a subspace of $P(\Omega_n)$. Let $e_1, e_2, \cdots, e_n$ be vectors in an n-dimensional Euclidean space $\boldsymbol{E}^n$ satisfying

$$(1.1.1)\qquad (e_i, e_j)=2\delta_{ij} \qquad (1\leqq i,\ j\leqq n),$$

where (,) denotes an inner product in $\boldsymbol{E}^n$. Set

$$\Lambda=\Lambda(e_1, \cdots, e_n)=\sum_{i=1}^{n}\boldsymbol{Z}e_i$$

$$\Lambda_\varepsilon=\Lambda_\varepsilon(e_1, \cdots, e_n)=\left\{\sum_{i=1}^{n}x_ie_i \;\middle|\; x_i\in\boldsymbol{Z} \text{ and } \sum_{i=1}^{n}x_i\equiv\varepsilon \bmod 2\right\}.$$

where $\varepsilon=0$ or 1. Also, for $X\in P(\Omega_n)$, set

$$e_X=\sum_{i\in X}e_i\,.$$

Let C be a code of length n. Then we construct some lattices as follows:

$$L_A(C)=\bigcup_{X\in C}\left(\Lambda+\frac{1}{2}e_X\right),\qquad L_B(C)=\bigcup_{X\in C}\left(\Lambda_0+\frac{1}{2}e_X\right)$$

$$L_C^{\varepsilon}(C)=\bigcup_{X\in C}\left\{\left(\Lambda_0+\frac{1}{2}e_X\right)\cup\left(\Lambda_{\varepsilon}+\frac{1}{2}e_X+\frac{1}{4}e_{\Omega}\right)\right\},\quad \text{where } \Omega=\Omega_n.$$

It is not difficult to see that

(1.1.2) *for* $U=A$ *or* B, $L_U(C)$ *is integral (resp. even) if a code* C *is self-orthogonal (resp. doubly even),*

(1.1.3) $L_C^{\varepsilon}(C)$ *is integral (resp. even) if* C *is doubly even and* $n\equiv 0 \bmod 8$ *(resp.* $\varepsilon\equiv n/8 \bmod 2$).

REMARK 1.1.4. The constructions of $L_A(C)$ and $L_B(C)$ are those which are known in [**4**] or [**10**] as construction A and B respectively. The construction of $L_C^{\varepsilon}(C)$ can be found in [**1**], [**10**] or [**11**]. See Remark 2.1.4 and Lemma 2.2.3 for a slightly general form of $L_B(C)$ and $L_C^{\varepsilon}(C)$.

1.2. Let L be an integral lattice in $\boldsymbol{E}^n$ and $e_1, e_2, \cdots, e_n$ be vectors in $\boldsymbol{E}^n$ satisfying (1.1.1) and

$$(1.2.1) \qquad e_i\pm e_j\in L \qquad (1\leqq i,\ j\leqq n).$$

The set $\mathcal{F}_0=\{\pm e_1, \cdots, \pm e_n\}$ is called a *frame* of L. Now we consider the following three types of frames:

Type A: $e_1, \cdots, e_n \in L$

Type B: $e_i \notin L$ but $\frac{1}{2}\Lambda \supset L$

Type C: $\frac{1}{2}\Lambda \not\supset L$.

The first result of the present paper is the following

THEOREM 1. *Let* L *be an even lattice in* $\boldsymbol{E}^n$ *with a frame* $\mathcal{F}_0=\{\pm e_1, \cdots, \pm e_n\}$ *Let* C *be a code defined as follows:*

$$C=\left\{X\in P(\Omega_n)\ \middle|\ \left(\Lambda+\frac{1}{2}e_X\right)\cap L\neq\emptyset\right\}.$$

Then replacing some e_i *by* $-e_i$ *if necessary,* L *can be expressed as* $L_A(C)$, $L_B(C)$ *and* $L_C^{\delta}(C)$ ($\delta=0$ *or* 1 *and* $\delta\equiv n/8 \bmod 2$) *according as* $\mathcal{F}_0$ *is of Type A, B and C respectively.*

REMARK 2.2.1. (i) A code C defined in Theorem 1 is determined only by a frame $\mathcal{F}_0$ i.e. C does not change when we replace some e_i by $-e_i$. Also any permutation of $e_1, \cdots, e_n$ yields a code equivalent to C. (ii) In Theorem 1, it will be sufficient to assume that L is integral, when $\mathcal{F}_0$ is of Type A or B (cf. § 2.1 and also Lemma 2.2.3 for Type C).

The second result is as follows:

THEOREM 2. *Let L be an even lattice with a frame. Then* $\mathrm{Aut}(L)$, *the automorphism group of L, is transitive on the set of all frames of the same type if we assume $n>16$ (resp. $n>32$) for Type B (resp. Type C).*

REMARK 1.2.2. In Theorem 2, it will be sufficient to assume that L is integral, when $\mathcal{F}_0$ is of Type A or B (cf. § 3.2 and Remark 4.3.1). If $n \leqq 16$ (resp. $n \leqq 32$), Theorem 2 is not necessarily true for Type B (resp. Type C). Some counter examples are given in § 5 (cf. (5.3.1)-(5.3.3)).

Let $L_C(\mathcal{C})=L_C^{\delta}(\mathcal{C})$ where $\delta \equiv n/8 \bmod 2$. Combining Theorem 1 and Theorem 2, we have

THEOREM 3. *For $U=A$, B or C, a mapping $\mathcal{C} \rightarrow L_U(\mathcal{C})$ gives a one to one correspondence from the set of all isomorphism classes of doubly even codes of length n to the set of all isomorphism classes of even lattices in $\boldsymbol{E}^n$ with a frame of type U if it is assumed that $n>16$ (resp. $n>32$) for $U=B$ (resp. $U=C$).*

1.3. Let $\mathcal{H}_n$ be the set of all isomorphism classes of doubly even self-dual codes of length n with minimum weight $\geqq 8$. If $\mathcal{C} \in \mathcal{H}_n$, then $L_C(\mathcal{C})$ is an even unimodular lattice having no 2-vectors (i.e. a vector v with $(v, v)=2$). In particular, if $\mathcal{C} \in \mathcal{H}_{24}$, $\mathcal{C}$ is the Golay code (cf. [8]) and $L_C(\mathcal{C})$ is the Leech lattice (cf. [3]). In [6] and [7], Ozeki examined whether a mapping $\mathcal{C} \rightarrow L_C(\mathcal{C})$ ($\mathcal{C} \in \mathcal{H}_{40}$) is one to one, and showed that this is true for some subclasses of $\mathcal{H}_{40}$. Clearly Theorem 3 has generalized his results not only for all codes in $\mathcal{H}_{40}$, but also for the classes of all doubly even codes of length $\geqq 40$. It should be noted that a mapping $\mathcal{C} \rightarrow L_C(\mathcal{C})$ ($\mathcal{C} \in \mathcal{H}_n$) is one to one for $n=32$ too. In this case $n=32$, however, some additional arguments will be needed compared to the case $n \geqq 40$ (cf. § 6).

1.4. In § 2-§ 5, the following notations will be used:

$\boldsymbol{Z}$: the ring of rational integers,

$|X|$: the cardinality of a set X,

$\mathcal{C}^{\perp}$: the dual of a code $\mathcal{C} \subset P(\Omega_n)$, i.e. the set of $X \in P(\Omega_n)$ such that $|X \cap Y|$ is even for all $Y \in \mathcal{C}$,

$L^{\perp}$: the dual of a lattice $L \subset \boldsymbol{E}^n$, i.e. the set of $u \in \boldsymbol{E}^n$ such that $(u, v) \in \boldsymbol{Z}$ for all $v \in L$.

We note that $\Lambda(e_1, \cdots, e_n)^{\perp}=(1/2)\Lambda(e_1, \cdots, e_n)$. $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$ ($k=2, 3, \cdots$) are some doubly even codes generated by tetrads. See § 5 for the definition of those codes. Sometimes the terminology "*a natural basis*" of those codes will be used (cf. § 5.2). As for other terminologies and notations of codes and lattices, we refer to [4], [5] or [9].

§ 2. The proof of Theorem 1.

2.1. Throughout this section, let L be an integral lattice in $\boldsymbol{E}^n$ with a frame $\mathcal{F}_0=\{\pm e_1, \cdots, \pm e_n\}$, i.e. $e_1, \cdots, e_n$ are vectors in $\boldsymbol{E}^n$ satisfying (1.1.1) and (1.2.1).

LEMMA 2.1.1. *$L\subset(1/2)\Lambda\cup((1/2)\Lambda+(1/4)e_\Omega)$ where $\Lambda=\Lambda(e_1, \cdots, e_n)$ and $\Omega=\Omega_n$.*

PROOF. Let $x=\sum_i x_i e_i\in L$. Then

$$(*) \qquad (x, e_i\pm e_j)=2(x_i\pm x_j)\in \boldsymbol{Z}$$

as L is integral. From this we see $L\subset(1/4)\Lambda$. But if $x_i\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ for some x_i, (*) yields all $x_j\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ which proves Lemma 2.1.1.

Let

$$\mathcal{C}=\left\{X\in P(\Omega)\middle|\left(\Lambda+\frac{1}{2}e_X\right)\cap L\neq\emptyset\right\},$$

$$\mathcal{C}_0=\left\{X\in P(\Omega)\middle|\left(\Lambda_0+\frac{1}{2}e_X\right)\cap L\neq\emptyset\right\}.$$

LEMMA 2.1.2. (i) *$\mathcal{C}$ is self-orthogonal. If L is even, $\mathcal{C}$ is doubly even.* (ii) $[\mathcal{C}:\mathcal{C}_0]\leqq 2$.

PROOF. Let $X, Y\in\mathcal{C}$. Then there exist $x, y\in\Lambda$ such that $x+(1/2)e_X\in L$ and $y+(1/2)e_Y\in L$, and we have $0\equiv(x+(1/2)e_X, y+(1/2)e_Y)\equiv(1/2)|X\cap Y| \bmod 1$ and so $|X\cap Y|=$even which implies that $\mathcal{C}$ is self-orthogonal. If L is even, $((1/2)e_X, (1/2)e_X)=(1/2)|X|\equiv 0 \bmod 2$ for $X\in\mathcal{C}$ and so $|X|\equiv 0 \bmod 4$. Let $X, Y\in\mathcal{C}-\mathcal{C}_0$. There exist $\sum x_i e_i+(1/2)e_X, \sum y_i e_i+(1/2)e_Y\in L$ such that $\sum x_i\equiv\sum y_i\equiv 1 \bmod 2$. Then the sum of these two vectors is equal to $\sum(x_i+y_i)e_i+e_{X\cap Y}+(1/2)e_{X+Y}$ which belongs to $L\cap(\Lambda_0+(1/2)e_{X+Y})$ and so $X+Y\in\mathcal{C}_0$.

LEMMA 2.1.3. *Let $L_0=L\cap(1/2)\Lambda$. There exist $e_1', e_2', \cdots, e_n'\in\mathcal{F}_0$ such that*

$$L_0=\bigcup_{X\in C}\left(\Lambda+\frac{1}{2}e_X'\right) \quad \textit{or} \quad \bigcup_{X\in C}\left(\Lambda_0+\frac{1}{2}e_X'\right)$$

according as $\mathcal{F}_0$ is of Type A or not. In particular, Theorem 1 holds for a frame of Type A or B.

PROOF. If $\mathcal{F}_0$ is of Type A or $\mathcal{C}=\mathcal{C}_0$, it will be sufficient to put $e_i'=e_i$ $(1\leqq i\leqq n)$. So suppose $\mathcal{C}\neq\mathcal{C}_0$ and $\mathcal{F}_0$ is not of Type A. Take $T\in\mathcal{C}_0^\perp-\mathcal{C}^\perp$ and set

$$(**) \qquad e_i'=\begin{cases} e_i & i\notin T \\ -e_i & i\in T\,. \end{cases}$$

Let $L_0 \ni u+(1/2)e_X$ $(u\in \Lambda,\ X\in \mathcal{C})$. Then we have

$$u+\frac{1}{2}e_X = u+\frac{1}{2}(e_{X\cap T}+e_{X-(X\cap T)})$$

$$= u+\frac{1}{2}(-e'_{X\cap T}+e'_{X-(X\cap T)}) = u-e'_{X\cap T}+\frac{1}{2}e'_X .$$

If $X\in \mathcal{C}_0$, we have $u\in \Lambda_0$ and $|X\cap T|=$even. So $u-e'_{X\cap T}\in \Lambda_0$. If $X\in \mathcal{C}-\mathcal{C}_0$, we have $u\in \Lambda_1$ and $|X\cap T|=$odd. So $u-e'_{X\cap T}\in \Lambda_0$. Thus we get $L_0=\bigcup_{X\in \mathcal{C}}(\Lambda_0+(1/2)e'_X)$.

REMARK 2.1.4. If $\mathcal{F}_0$ is of Type B, we have another expression of L: when we choose $e_i\in \mathcal{F}_0$ suitably, we have

$$(***)\qquad L=\Big\{\bigcup_{X\in \mathcal{C}'}\Big(\Lambda_0+\frac{1}{2}e_X\Big)\Big\}\cup\Big\{\bigcup_{Y\in \mathcal{C}''}\Big(\Lambda_1+\frac{1}{2}e_Y\Big)\Big\}$$

where $\mathcal{C}'=\{X\in \mathcal{C}\mid |X|\equiv 0 \bmod 4\}$ and $\mathcal{C}''=\mathcal{C}-\mathcal{C}'$. In fact, let $L=\bigcup_{X\in \mathcal{C}}(\Lambda_0+(1/2)e_X)$ and $\mathcal{C}\neq \mathcal{C}'$. If we take $T\in \mathcal{C}'^{\perp}-\mathcal{C}^{\perp}$ and define e'_i $(1\leqq i\leqq n)$ as in (**) above, we see that L has an expression (***) with respect to a basis $\{e'_i\}$.

2.2. In the following, we assume that $\mathcal{C}=\mathcal{C}_0$ and $\mathcal{F}_0$ is of Type C, i.e. $L\not\subset(1/2)\Lambda$. Let

$$L_1=\Big(\frac{1}{2}\Lambda+\frac{1}{4}e_\Omega\Big)\cap L ,$$

$$\mathcal{C}_1=\Big\{X\in P(\Omega)\ \Big|\ \Big(\Lambda+\frac{1}{2}e_X+\frac{1}{4}e_\Omega\Big)\cap L\neq\emptyset\Big\}$$

and $Z\in \mathcal{C}_1$ so that there exists $x\in L$ which can be expressed as

$$x=v_Z+\frac{1}{2}e_Z+\frac{1}{4}e_\Omega \qquad (v_Z\in \Lambda).$$

We shall fix such a $Z\in \mathcal{C}_1$ and $v_Z\in \Lambda$ henceforward.

LEMMA 2.2.1. (i) $\Omega\in \mathcal{C}$. (ii) $n\equiv 0 \bmod 8$. (iii) $\mathcal{C}_1=\mathcal{C}+Z$.

PROOF. From $2x\in L\cap(\Lambda+(1/2)e_\Omega)$ we get $\Omega\in \mathcal{C}$. Also we have $(x,x)\equiv n/8 \bmod 1$ and then $n\equiv 0 \bmod 8$ as $(x,x)\in \boldsymbol{Z}$. Take $Y\in \mathcal{C}_1$. If $X=Y+Z$, we have, for some $u\in \Lambda$,

$$L\ni u+\frac{1}{2}e_{X+Z}+\frac{1}{4}e_\Omega=u-e_{X\cap Z}+\frac{1}{2}e_X+\frac{1}{2}e_Z+\frac{1}{4}e_\Omega$$

which yields $X\in \mathcal{C}$. Thus $\mathcal{C}_1\subset \mathcal{C}+Z$. Conversely if $\mathcal{C}\ni X$ and $y=u+(1/2)e_X\in L$ $(u\in \Lambda)$, from $x+y\in L$ we get $X+Z\in \mathcal{C}_1$ i.e. $\mathcal{C}_1\supset \mathcal{C}+Z$.

LEMMA 2.2.2. *Let* $\mathcal{C}'=\{X\in \mathcal{C}\mid |X|\equiv 0 \bmod 4\}$ *and* $\mathcal{C}''=\mathcal{C}-\mathcal{C}'$. *Then the* *followings hold:*

(i) $\mathcal{C}'=\mathcal{C}\cap\langle Z\rangle^{\perp}$ *and* $|Z|=$ *even.*

(ii) *Assume that* $v_Z\in\Lambda_\varepsilon$ ($\varepsilon=0$ *or* 1). *Then we have*

$$L_1=\Big\{\bigcup_{X\in\mathcal{C}'}\Big(\Lambda_\varepsilon+\frac{1}{2}e_{X+Z}+\frac{1}{4}e_\Omega\Big)\Big\}\cup\Big\{\bigcup_{Y\in\mathcal{C}''}\Big(\Lambda_{1-\varepsilon}+\frac{1}{2}e_{Y+Z}+\frac{1}{4}e_\Omega\Big)\Big\}.$$

PROOF. (i) If $X\in\mathcal{C}$, we have

$$\boldsymbol{Z}\ni\Big(\frac{1}{2}e_X,\ v+\frac{1}{2}e_Z+\frac{1}{4}e_\Omega\Big)\equiv\frac{|X\cap Z|}{2}+\frac{|X|}{4}\ \mathrm{mod}\ 1\,,$$

which yields $\mathcal{C}'=\mathcal{C}\cap\langle Z\rangle^{\perp}$. Also $|Z|$ is even as $\Omega\in\mathcal{C}'$.

(ii) If $L_1\ni u+(1/2)e_{X+Z}+(1/4)e_\Omega$ ($X\in\mathcal{C}$ and $u\in\Lambda$), we have

$$u+\frac{1}{2}e_{X+Z}+\frac{1}{4}e_\Omega=u+\frac{1}{2}e_X+\frac{1}{2}e_Z-e_{X\cap Z}+\frac{1}{4}e_\Omega\,.$$

Since $(1/2)e_X\in L$ and $L\cap\Lambda=\Lambda_0$, we must have $v_Z-(u-e_{X\cap Z})\in\Lambda_0$. This together with (i) proves (ii).

LEMMA 2.2.3. *Let*

$$e_i'=\begin{cases} e_i & i\notin Z\\ -e_i & i\in Z\end{cases}\quad(1\leqq i\leqq n).$$

Then the followings hold:

(i) $$L=\Big\{\bigcup_{X\in\mathcal{C}'}\Big(\Lambda_0+\frac{1}{2}e_X'\Big)\Big\}\cup\Big\{\bigcup_{Y\in\mathcal{C}''}\Big(\Lambda_1+\frac{1}{2}e_Y'\Big)\Big\}$$

$$\cup\Big\{\bigcup_{X\in\mathcal{C}'}\Big(\Lambda_\varepsilon+\frac{1}{2}e_X'+\frac{1}{4}e_\Omega'\Big)\Big\}\cup\Big\{\bigcup_{Y\in\mathcal{C}''}\Big\{\Lambda_{1-\varepsilon}+\frac{1}{2}e_Y'+\frac{1}{4}e_\Omega'\Big)\Big\}.$$

In particular, if $\mathcal{C}$ *is doubly even,* $L=L_{\mathcal{C}}^{\varepsilon}(\mathcal{C})$.

(ii) *If* L *is even,* $L=L_{\mathcal{C}}^{\delta}(\mathcal{C})$ *where* $\delta=0$ *or* 1 *and* $\delta\equiv n/8\ \mathrm{mod}\ 2$. *Thus Theorem* 1 *holds for a frame of type C.*

PROOF. Let $u+(1/2)e_X\in L$ ($u\in\Lambda_0$ and $X\in\mathcal{C}$). Then

$$u+\frac{1}{2}e_X=u+\frac{1}{2}(e_{X\cap Z}+e_{X-(X\cap Z)})$$

$$=u+\frac{1}{2}(-e_{X\cap Z}'+e_{X-(X\cap Z)}')=u-e_{X\cap Z}'+\frac{1}{2}e_X'\,,$$

which yields, by Lemma 2.2.2 (i),

$$L_0=L\cap\frac{1}{2}\Lambda=\Big\{\bigcup_{X\in\mathcal{C}'}\Big(\Lambda_0+\frac{1}{2}e_X'\Big)\Big\}\cup\Big\{\bigcup_{Y\in\mathcal{C}''}\Big(\Lambda_1+\frac{1}{2}e_Y'\Big)\Big\}.$$

If $u+(1/2)e_{X+Z}+(1/4)e_\Omega\in L$ ($X\in\mathcal{C}$ and $u\in\Lambda_{\varepsilon'}$), we have $\varepsilon'=\varepsilon$ or $1-\varepsilon$ according as $X\in\mathcal{C}'$ or $\mathcal{C}''$. Also we see

$$u+\frac{1}{2}e_{X+Z}+\frac{1}{4}e_{\Omega}=u-e'_Z+\frac{1}{2}e'_X+\frac{1}{4}e'_{\Omega},$$

which yields

$$L_1=\Big\{\bigcup_{X\in C'}\Big(\Lambda_{\varepsilon}+\frac{1}{2}e'_X+\frac{1}{4}e'_{\Omega}\Big)\Big\}\cup\Big\{\bigcup_{Y\in C''}\Big(\Lambda_{1-\varepsilon}+\frac{1}{2}e'_Y+\frac{1}{4}e'_{\Omega}\Big)\Big\}$$

as $|Z|=$even. This proves (i). (ii) We have $L\ni x=v_Z+(1/2)e_Z+(1/4)e_{\Omega}$ and $v_Z\in\Lambda_{\varepsilon}$. Since L is even, we see $(x, x)\equiv(v_Z, v_Z)+(1/8)|\Omega| \bmod 2$ by using the fact $|Z|=$even. As $(v_Z, v_Z)\equiv\varepsilon \bmod 2$, we get $\varepsilon\equiv n/8 \bmod 2$. This proves Lemma 2.2.3.

REMARK 2.2.4. (i) If C is not doubly even, we can take $\varepsilon=0$ in the expression of L in Lemma 2.2.3 (i). In fact, let $Y\in C''$ and

$$e''_i=\begin{cases} e'_i & i\notin Y\\ -e'_i & i\in Y.\end{cases}$$

Then we easily see that the expression of L with $\varepsilon=1$ is changed into the one with $\varepsilon=0$. (ii) If C is doubly even, $L=L_C^{\varepsilon}(C)$ is even if and only if $n/8\equiv\varepsilon$ mod 2.

§ 3. Some automorphisms of L.

3.1. In this section, we will give some automorphisms of L which will be used in § 4 for the proof of Theorem 2.

Let L be an integral lattice with a frame $\mathfrak{F}_0=\{\pm e_1, \cdots, \pm e_n\}$. We assume that a code C and vectors $e_1, \cdots, e_n$ are chosen so that L can be expressed as in Theorem 1. Note that the code C is self-orthogonal (resp. doubly even) if L is integral (resp. even).

LEMMA 3.1.1. *Let $T\in C$ with $|T|=4$. Define an orthogonal transformation τ_T of $\boldsymbol{E}^n$ as follows:*

$$\tau_T(e_i)=\begin{cases}\frac{1}{2}e_T-e_i & i\in T\\ e_i & i\notin T.\end{cases}$$

Then $\tau_T\in\mathrm{Aut}(L)$.

PROOF. Let $\tau=\tau_T$. We easily see $\tau(e_i\pm e_j)\in L$, and also $\tau(e_i)\in L$ if $\mathfrak{F}_0$ is of Type A. Let $X\in C$. Then we have

$$\tau\Big(\frac{1}{2}e_X\Big)=\frac{1}{2}\tau(e_{X\cap T})+\frac{1}{2}\tau(e_{X-(X\cap T)})$$

$$=\frac{1}{2}\Big(\frac{|X\cap T|}{2}e_T-e_{X\cap T}\Big)+\frac{1}{2}e_{X-(X\cap T)}=\frac{|X\cap T|}{4}e_T+\frac{1}{2}e_X-e_{X\cap T}.$$

Since $T\in\mathcal{C}$ and so $|X\cap T|$ is even, we get $\tau((1/2)e_X)\in L$. Thus $\tau\in\mathrm{Aut}(L)$ if $\mathcal{F}_0$ is of Type A or B. As $\tau((1/4)e_\Omega)=(1/4)e_\Omega$, we have $\tau\in\mathrm{Aut}(L)$ also when $\mathcal{F}_0$ is of Type C. q. e. d.

3.2. Now we will prove Theorem 2 for $\mathcal{F}_0$ of type A. Let $\mathcal{F}=\{\pm f_1, \pm f_2, \cdots, \pm f_n\}$ be an arbitrary frame of Type A. Note that $f_i\in L$. If $f_i\in\mathcal{F}-(\mathcal{F}\cap\mathcal{F}_0)$, f_i is of the form $(1/2)\sum_{j\in T}\pm e_j$ for some $T\in\mathcal{C}$ with $|T|=4$. We note that, if ε is an orthogonal transformation of $\boldsymbol{E}^n$ such that $\varepsilon(e_j)=\varepsilon_j e_j$ ($\varepsilon_j=\pm 1$), ε is an automorphism of L. Applying a suitable ε to f_i, we have $\varepsilon(f_i)=(1/2)e_T-e_p$ where $p\in T$. Now apply τ_T defined in Lemma 3.1.1 to vectors in $\varepsilon(\mathcal{F})$. Then we have $\tau_T\varepsilon(f_i)=e_p$ and $\tau_T\varepsilon(f_j)\in\mathcal{F}_0$ if $f_j\in\mathcal{F}_0\cap\mathcal{F}$, and so $|\mathcal{F}\cap\mathcal{F}_0|<|\tau_T\varepsilon(\mathcal{F})\cap\mathcal{F}_0|$. Now proceeding by induction on $|\mathcal{F}_0\cap\mathcal{F}|$, we can get an automorphism σ such that $\sigma(\mathcal{F})=\mathcal{F}_0$. q. e. d.

3.3. DEFINITION. A partition $\Pi=\{T_1, T_2, \cdots, T_{n/4}\}$ of Ω_n is called a *T*-decomposition of a code $\mathcal{C}$ if the following conditions are satisfied:

$$\Omega_n = T_1\cup T_2\cup\cdots\cup T_{n/4} \tag{3.3.1}$$

$$|T_i| = 4 \quad \left(1\leqq i\leqq \frac{n}{4}\right) \tag{3.3.2}$$

$$T_i\cup T_j\in\mathcal{C} \qquad \text{for any } i\neq j. \tag{3.3.3}$$

LEMMA 3.3.1. *Let $\Pi=\{T_1, \cdots, T_{n/4}\}$ be a T-decomposition of $\mathcal{C}$. Define orthogonal transformations φ and ϕ as follows:*

$$\varphi(e_i)=\frac{1}{2}e_T-e_i \qquad i\in T\in\Pi$$

$$\phi(e_i)=\begin{cases}\dfrac{1}{2}e_T-e_i & i\in T\in\Pi,\ T\neq S\\[2mm] e_i-\dfrac{1}{2}e_S & i\in S\end{cases}$$

where S is an arbitrarily chosen tetrad in Π. If L is even, then the followings hold:

(i) *if $T_i\in\mathcal{C}^\perp$ for some i (and consequently for all i), then $\varphi\in\mathrm{Aut}(L)$,*

(ii) *if $\mathcal{F}_0$ is of type C, then $\mathrm{Aut}(L)\ni\varphi$ or ϕ according as $n/8\equiv 0$ or $1 \bmod 2$.*

PROOF. We easily see $\varphi(e_i\pm e_j)$, $\phi(e_i\pm e_j)\in L$. Let $X\in\mathcal{C}$. Then

$$\varphi\left(\frac{1}{2}e_X\right)=\frac{1}{2}\sum_{T\in\Pi}\varphi(e_{X\cap T})=\frac{1}{2}\sum_{T}\left(\frac{|X\cap T|}{2}e_T-e_{X\cap T}\right)$$

$$=\frac{1}{4}\sum_{T}|X\cap T|e_T-\frac{1}{2}e_X\cdots\cdots\cdots\cdots\cdots(\#).$$

Now in order to see $\varphi((1/2)e_X)\in L$, we divide into two cases:

Case I: $|X\cap T|$ is even for some $T\in\Pi$.

Case II: $|X\cap T|$ is odd for all $T\in\Pi$.

Firstly suppose that we have Case I. Then $|X\cap T|$ is even for all $T\in\Pi$ by (3.3.3) and the number of T with $|X\cap T|=2$ is also even because C is doubly even. Then from (#) we see $\varphi((1/2)e_X)\in L$. In particular, if $T\in C^{\perp}$, we have $\varphi((1/2)e_X)\in L$. Next suppose that we have Case II. Then from (#) we see

$$\varphi\left(\frac{1}{2}e_X\right)=\frac{1}{4}e_\Omega+\frac{1}{2}\Sigma' e_T-\frac{1}{2}e_X$$

where the summation Σ' runs over all $T\in\Pi$ with $|X\cap T|=3$. If $n/8\equiv 0 \bmod 2$, we have $\varphi((1/2)e_X)\in L$ as the number of $T\in\Pi$ with $|X\cap T|=3$ is even. Now we have $\varphi\in\mathrm{Aut}(L)$ as $\varphi((1/2)e_X)\in L$ in both cases and $\varphi((1/4)e_\Omega)=(1/4)e_\Omega$. Also we have

$$\begin{aligned}\phi\left(\frac{1}{2}e_X\right)&=\frac{1}{2}\left\{\sum_{T\neq S}\phi(e_{X\cap T})+\phi(e_{X\cap S})\right\}\\&=\frac{1}{2}\left\{\sum_{T\neq S}\left(\frac{|X\cap T|}{2}e_T-e_{X\cap T}\right)+\left(e_{X\cap S}-\frac{|X\cap S|}{2}e_S\right)\right\}\\&=\frac{1}{4}\sum_{T\in\Pi}|X\cap T|e_T-\frac{|X\cap S|}{2}e_S-\frac{1}{2}e_X+e_{X\cap S}.\end{aligned}$$

In the same way as above, if $n/8\equiv 1 \bmod 8$, we get $\phi((1/2)e_X)\in L$ and so $\phi\in \mathrm{Aut}(L)$ as $\phi((1/4)e_\Omega)=(1/4)e_\Omega-(1/2)e_S$. q. e. d.

LEMMA 3.3.2. *Let $\Pi=\{T_1, \cdots, T_{n/4}\}$ be a T-decomposition of C. Assume that $T_i\in C^{\perp}-C$ for all i. Then the followings hold:*

(i) *there exists $A\in C^{\perp}$ such that $|A\cap T_i|=1$ for all i,*

(ii) *define ρ as follows: if $i\in T\in\Pi$,*

$$\rho(e_i)=\begin{cases}\dfrac{1}{2}e_T & \text{if } \{i\}=A\cap T\\[2ex] e_{A\cap T}+e_i-\dfrac{1}{2}e_T & \text{if } i\in T-(A\cap T).\end{cases}$$

If $\mathfrak{T}_0$ is of Type B and L is even, then $\rho\in\mathrm{Aut}(L)$.

PROOF. (i) Let $C_2=\langle C, T|T\in\Pi\rangle$ which is a code generated by C and all $T\in\Pi$. Take $A'\in C^{\perp}-C_2^{\perp}$. Then $|A'\cap T|=$odd for all T. Let $A=A'+\Sigma T$ where the summation runs over all T with $|A'\cap T|=3$. Then A satisfies the condition in (i).

(ii) It will be sufficient to see $\rho((1/2)e_X)\in L$ for any $X\in C$. Since $\rho(e_T)=2e_{A\cap T}$, we see $\rho((1/2)e_X)\in L$ if X is a union of even number of $T\in\Pi$. As $|X\cap T|$ is even for any $T\in\Pi$, we may assume $|X\cap T|=0$ or 2 by adding even number of the $T\in\Pi$ to X. Furthermore, as $|X\cap A|$ is even, so is the number of $T\in\Pi$ with $|X\cap A\cap T|=1$. So we may assume $X\cap A\cap T=\emptyset$ for any $T\in\Pi$. Then we see

$$\rho\left(\frac{1}{2}e_X\right)=\frac{1}{2}\sum_{T\in\Pi}\rho(e_{X\cap T})=\frac{1}{2}\sum{}'(2e_{A\cap T}+e_{X\cap T}-e_T)$$
$$=\sum{}'e_{A\cap T}+\frac{1}{2}e_X-\frac{1}{2}\sum{}'e_T\in L\,,$$

where $\sum'$ runs over all T with $X\cap T\neq\emptyset$. (Note that C is doubly even and so the number of such T is even.)

REMARK 3.3.3. Let L be an integral lattice with a frame of type B. Then we can prove that if an orthogonal transformation ρ of L is defined in the same way as above by using an expression (***) of L in Remark 2.1.4, we still have $\rho\in\mathrm{Aut}(L)$.

§ 4. The proof of Theorem 2.

4.1. Let L be an even lattice in $\boldsymbol{E}^n$ with a frame $\mathcal{F}_0=\{\pm e_1,\cdots,\pm e_n\}$ of Type B or C. We will assume $n>16$ or $n>32$ according as $\mathcal{F}_0$ is of Type B or C. Through § 4, $\mathcal{F}=\{\pm f_1,\cdots,\pm f_n\}$ is a frame of L of the same Type as $\mathcal{F}_0$.

LEMMA 4.1. *$f_i=\pm e_j$ for some j or $f_i=(1/2)\sum_{t\in T}\varepsilon_t e_t$ where $\Omega\supset T$, $|T|=4$ and $\varepsilon_t=\pm 1$.*

PROOF. Let $f_i=\sum_{j=1}^n a_{ij}e_j$ $(1\leqq i\leqq n)$. Note that the matrix $A=(a_{ij})$ is an orthogonal matrix. Then it will be sufficient to see $a_{ij}\in(1/2)\boldsymbol{Z}$ for all i, j. Let $\mathcal{F}$ be of type B. Then $a_{ij}\in(1/4)\boldsymbol{Z}$ because $2f_i\in L\subset(1/2)\Lambda(e_1,\cdots,e_n)$. Suppose $a_{ij}\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ for some i, j. If $a_{ik}\in(1/2)\boldsymbol{Z}$ for some k, we have $e_j+e_k=\sum_t(a_{tj}+a_{tk})f_t$ and $a_{ij}+a_{ik}\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ which is impossible because $e_j+e_k\in L\subset(1/2)\Lambda(f_1,\cdots,f_n)$. Thus $a_{ik}\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ for all k. By interchanging the role of $\{e_i\}$ and $\{f_i\}$, we get $a_{kj}\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ for all k. Thus we must have $a_{ij}\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ for all i, j. Then $2=(e_i, e_i)=(1/8)\sum_j x_j^2$ $(0\neq x_j=4a_{ji}\in\boldsymbol{Z})$ and so $n\leqq 16$. As we are assuming $n>16$, we must have $a_{ij}\in(1/2)\boldsymbol{Z}$. Next let $\mathcal{F}$ be of Type C. Then $a_{ij}\in(1/8)\boldsymbol{Z}$. Suppose $a_{ij}\in(1/8)\boldsymbol{Z}-(1/4)\boldsymbol{Z}$ for some i, j. Then the same arguments as above yield $a_{ij}\in(1/8)\boldsymbol{Z}-(1/4)\boldsymbol{Z}$ for all i, j. Then e_j+e_k or $e_j-e_k\in(1/2)\Lambda(f_1,\cdots,f_n)+(1/4)e_\Omega$ and so (e_j+e_k, e_j+e_k) or $(e_j-e_k, e_j-e_k)=4=(1/8)\sum x_j^2$ $(0\neq x_j\in\boldsymbol{Z})$. Thus $n\leqq 32$. Next suppose $a_{ij}\in(1/4)\boldsymbol{Z}-(1/2)\boldsymbol{Z}$ for some i, j. If $a_{kj}=0$ for some k, we have $f_i+f_k=\sum_t(a_{it}+a_{kt})e_t\in(1/2)\Lambda(e_1,\cdots,e_n)+(1/4)e_\Omega$ and so we get $n\leqq 32$ from $(f_i+f_k, f_i+f_k)=4$. Therefore $a_{kj}\neq 0$ for all k. Then $n\leqq 16$ because $\sum_{k=1}^n a_{kj}^2=1$ and $0\neq a_{kj}\in(1/4)\boldsymbol{Z}$. Thus we have $a_{ij}\in(1/2)\boldsymbol{Z}$ for all i, j if $n>32$.

4.2. For $f_i\in\mathcal{F}$, set

$$\mathrm{supp}(f_i)=\{j \mid a_{ij}\neq 0\}, \qquad \text{where } f_i=\sum_{j=1}^{n} a_{ij}e_j\,.$$

Then $|\mathrm{supp}(f_i)|=1$ or 4 by Lemma 4.1. In the following, we assume that a code C and vectors $e_1, \cdots, e_n$ are chosen so that L can be expressed as in Theorem 1. The the following remark is important:

(4.0) *Let* $X\in C$. *Then* $(1/2)\sum_{i\in X}\varepsilon_i e_i\in L$ $(\varepsilon_i=\pm 1)$ *if and only if the number of* i *with* $\varepsilon_i=-1$ *is even.*

Now we will prove a lemma which is a key to the proof of Theorem 2.

LEMMA 4.2. *One of the following holds:*

(i) *There exists* $\sigma\in\mathrm{Aut}(L)$ *such that* $\sigma(\mathcal{F})=\mathcal{F}_0$.

(ii) *There exists a T-decomposition* $\Pi=\{T_1, \cdots, T_{n/4}\}$ *such that each tetrad* T_i *coincides with* $\mathrm{supp}(f_j)$ *for some* $f_j\in\mathcal{F}$.

The proof of Lemma 4.2 will be done by being divided into several steps.

(4.1) *If* $|\mathrm{supp}(f_i)|=1$ *for some* $f_i\in\mathcal{F}$, *then* (i) *of Lemma* 4.2 *holds.*

PROOF. If $|\mathrm{supp}(f_j)|=4$, we have $\mathrm{supp}(f_j)\in C$ as $f_i-f_j\in L$. Then as $f_j\in L$, (4.0) implies that f_j is of the shape $\pm((1/2)e_T-e_p)$ where $T=\mathrm{supp}(f_j)$ and $p\in T$. Applying τ_T defined in Lemma 3.1.1, we get $\tau_T(f_j)=\pm e_p$ and $\tau_T(f_k)\in\mathcal{F}_0$ for any $f_k\in\mathcal{F}$ with $|\mathrm{supp}(f_k)|=1$, and so $|\mathcal{F}_0\cap\mathcal{F}|<|\mathcal{F}_0\cap\tau_T(\mathcal{F})|$. Proceeding by induction on $|\mathcal{F}_0\cap\mathcal{F}|$, we can find $\sigma\in\mathrm{Aut}(L)$ such that $\sigma(\mathcal{F})=\mathcal{F}_0$.

(4.2) Now in order to prove Lemma 4.2, we may assume $|\mathrm{supp}(f_i)|=4$ for all $f_i\in\mathcal{F}$. Then the matrix $A=(a_{ij})$ has just four nonzero elements $\pm 1/2$ in each row and each column. Let Γ be a code generated by $\mathrm{supp}(f_i)$ $(f_i\in\mathcal{F})$. Then Γ is a doubly even code generated by tetrads. So, by Theorem 6.5 in Pless and Sloane [**9**], Γ is isomorphic to a direct sum of components $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$. (See §5 for the definition of $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$.) Correspondingly the matrix A becomes a direct sum of some orthogonal matrices of degree 7, 8 and $2k$.

(4.3) *If* $\mathrm{supp}(f_1)\cap\mathrm{supp}(f_2)\subset\mathrm{supp}(f_3)$ *for* $f_1, f_2, f_3\in\mathcal{F}$, *we have* $\mathrm{supp}(f_3)=\mathrm{supp}(f_1)$ *or* $\mathrm{supp}(f_2)$.

PROOF. This is clear if $\mathrm{supp}(f_1)=\mathrm{supp}(f_2)$. So let $\mathrm{supp}(f_1)\cap\mathrm{supp}(f_2)=\{a, b\}$. Then $\varepsilon_{1a}\varepsilon_{2a}+\varepsilon_{1b}\varepsilon_{2b}=0$ by orthogonality between f_1 and f_2 where $f_s=(1/2)\sum_{t=1}^{n}\varepsilon_{st}e_t$. From this fact, we see $\{\varepsilon_{3a}, \varepsilon_{3b}\}=\pm\{\varepsilon_{1a}, \varepsilon_{1b}\}$ (resp. $\pm\{\varepsilon_{2a}, \varepsilon_{2b}\}$) and then orthogonality yields $\mathrm{supp}(f_3)=\mathrm{supp}(f_1)$ (resp. $=\mathrm{supp}(f_2)$).

(4.4) *Let* Γ' *be a component of* Γ. *If there exist three elements* f_1, f_2, f_3 *of* $\mathcal{F}$ *whose supports coincide and are contained in* Γ', *we have* $\Gamma'\cong\mathcal{D}_4$.

PROOF. If f_4 is the 4th vector$\in\mathcal{F}$ with $\mathrm{supp}(f_1)\cap\mathrm{supp}(f_4)\neq\emptyset$, the orthogonality of columns of the matrix A yields $\mathrm{supp}(f_4)=\mathrm{supp}(f_1)$. Thus we must have $\Gamma'=\langle\mathrm{supp}(f_1)\rangle\cong\mathcal{D}_4$.

(4.5) *Let Γ' be a component of Γ. If there exist distinct elements f_1 and f_1' with* $\mathrm{supp}(f_1)=\mathrm{supp}(f_1')\in\Gamma'$, *then we have $\Gamma'\cong\mathcal{D}_{2m}$ for some m and vice versa.*

PROOF. Let $f_1, f_2, \cdots, f_{m-1}$ $(m\geqq 3)$ be a maximal set of $\mathcal{F}$ subject to the conditions that

(1) $\mathrm{supp}(f_t)\in\Gamma'$ $(1\leqq t\leqq m-1)$,

(2) there exists $f_1'\in\mathcal{F}$ such that $\mathrm{supp}(f_1)=\mathrm{supp}(f_1')$ and $f_1\neq f_1'$,

(3) $|\mathrm{supp}(f_i)\cap\mathrm{supp}(f_j)| = \begin{cases} 2 & \text{if } |i-j|=1 \\ 0 & \text{if } |i-j|>1 . \end{cases}$

Namely $\mathrm{supp}(f_1), \cdots, \mathrm{supp}(f_{m-1})$ is a natural basis of $\mathcal{D}_{2m}$ (cf. §5.2) if a suitable permutation is applied to $\{e_1, e_2, \cdots, e_n\}$. In the following arguments, it is important to recall a fact mentioned in (4.2):

(*) *The matrix A has just four non-zero elements $\pm 1/2$ in each row and each column.*

Let $\mathrm{supp}(f_1)\cap\mathrm{supp}(f_2)=\{a, b\}$. By (*), there exists $f_2'\in\mathcal{F}$ such that $f_2'\neq f_2$ and $a\in\mathrm{supp}(f_2')$. Then the orthogonality of columns of f_1, f_1', f_2, f_2' yields $b\in\mathrm{supp}(f_2')$. By (4.3) and (4.4), we must have $\mathrm{supp}(f_2)=\mathrm{supp}(f_2')$. Similarly we get $\mathcal{F}\ni f_t'\neq f_t$ $(t=1, 2, \cdots, m-1)$ with $\mathrm{supp}(f_t')=\mathrm{supp}(f_t)$. Furthermore we can find $f_m\in\mathcal{F}$ such that $f_m\neq f_{m-1}, f_{m-1}'$ and $\mathrm{supp}(f_m)\cap\mathrm{supp}(f_{m-1})\neq\emptyset$. Then by the maximality of $f_1, \cdots, f_{m-1}$ and (*), we have $|\mathrm{supp}(f_m)\cap\mathrm{supp}(f_1)|=2$ and $|\mathrm{supp}(f_m)\cap\mathrm{supp}(f_i)|=0$ $(1<i<m-1)$. Also, by (*) again, we can find $\mathcal{F}\ni f_m'\neq f_m$ with $\mathrm{supp}(f_m')=\mathrm{supp}(f_m)$. Then a $2m\times n$ matrix with $f_1, f_1', \cdots, f_m, f_m'$ as rows is of the shape $(X, 0)$ after a suitable permutation of columns, where 0 is a $2m\times(n-2m)$ zero-matrix and X is an orthogonal matrix of degree $2m$ which is a direct sum component of A corresponding to Γ' (cf. (4.2)). Then from the shape of X we see $\Gamma'=\langle\mathrm{supp}(f_t)\,|\,t=1, 2, \cdots, m\rangle\cong\mathcal{D}_{2m}$. Conversely let $\Gamma'\cong\mathcal{D}_{2m}$ $(m>1)$ and $\mathrm{supp}(f_1), \mathrm{supp}(f_2)\in\Gamma'$ with $|\mathrm{supp}(f_1)\cap\mathrm{supp}(f_2)|=2$. If f_3 is a vector with $\mathrm{supp}(f_1)\cap\mathrm{supp}(f_2)\cap\mathrm{supp}(f_3)\neq\emptyset$, then we get $\mathrm{supp}(f_1)\cap\mathrm{supp}(f_2)\subset\mathrm{supp}(f_3)$ from the structure of $\mathcal{D}_{2m}$ (cf. (5.2.1)) and so, by (4.3), $\mathrm{supp}(f_3)=\mathrm{supp}(f_1)$ or $\mathrm{supp}(f_2)$. This completes the proof of (4.5).

(4.6) *Suppose that Γ has a component Γ' which is isomorphic to $\mathcal{E}_7$ or $\mathcal{D}_{2m}$ where m is odd. Then* (i) *of Lemma* 4.2 *holds.*

PROOF. Firstly we will show that $\mathrm{supp}(f_i)\in\mathcal{C}$ for some $f_i\in\Gamma'$. Suppose that $\Gamma'\cong\mathcal{E}_7$. By (4.5), there exist seven distinct $f_i\in\mathcal{F}$ such that $\mathrm{supp}(f_i)\in\Gamma'$.

Since $\mathcal{E}_7$ posseses seven non-zero elements, we must have $\mathrm{supp}(f_s)+\mathrm{supp}(f_t)=\mathrm{supp}(f_u)$ for some f_s, f_t, f_u whose supports are in Γ'. But then $\mathrm{supp}(f_u)\in\mathcal{C}$, because $f_s+f_t\in L$ and so $\mathrm{supp}(f_s)+\mathrm{supp}(f_t)\in\mathcal{C}$. Next suppose $\Gamma'\cong\mathcal{D}_{2m}$. Let $f_1, \cdots, f_m$ be as in the proof of (4.5). Then as $f_s-f_{s+1}\in L$ $(1\leqq s\leqq m-2)$, we have $\mathcal{C}\cap\Gamma'\ni\mathrm{supp}(f_m)=\sum_{t=1}^{m-1}\mathrm{supp}(f_t)$ if m is odd. Now take $\mathrm{supp}(f_i)\in\mathcal{C}\cap\Gamma'$. Then as $f_i\in L$, (4.0) implies that f_i must be of the shape $\pm((1/2)e_T-e_p)$ where $T=\mathrm{supp}(f_i)\ni p$. Applying τ_T defined in Lemma 3.1.1 to f_i, we get $\tau_T(f_i)=\pm e_p$. Then (4.6) follows from (4.1) applied to $\tau_T(\mathcal{F})$.

(4.7) *Lemma* 4.2 *holds.*

PROOF. By (4.6) we may assume that each component of Γ is isomorphic to $\mathcal{E}_8$ or $\mathcal{D}_{2m}$ (m=even). If $f_1, \cdots, f_{m-1}$ are taken in a component$\cong\mathcal{D}_{2m}$ so that $\mathrm{supp}(f_1), \cdots, \mathrm{supp}(f_{m-1})$ is a natural basis of $\mathcal{D}_{2m}$, then any two of $\mathrm{supp}(f_{2t-1})$ $(1\leqq t\leqq m/2)$ are disjoint and any two union of them are in $\mathcal{C}$. Also we can get $\mathrm{supp}(f_i)$ and $\mathrm{supp}(f_j)$ in a component$\cong\mathcal{E}_8$ with $\mathrm{supp}(f_i)\cap\mathrm{supp}(f_j)=\emptyset$. Thus we can find a T-decomposition of $\mathcal{C}$ satisfying the condition in (ii) of Lemma 4.2.

4.3. Now we will prove Theorem 2. By Lemma 4.2, we may assume that there exists a T-decomposition $\{T_1, T_2, \cdots, T_{n/4}\}$ of $\mathcal{C}$ such that each T_i coincides with $\mathrm{supp}(f_i)$ for some $f_i\in\mathcal{F}$ $(1\leqq i\leqq n/4)$. The following two cases will be considered: Let $f_1=(1/2)\sum_{t\in T_1}\varepsilon_t e_t$.

Case I. The number of $t\in T_1$ with $\varepsilon_t=-1$ is odd. In other words, f_1 is of the shape $\pm((1/2)e_{T_1}-e_p)$ where $p\in T_1=\mathrm{supp}(f_1)$.

Case II. The number of $t\in T_1$ with $\varepsilon_t=-1$ is even.

We note that if f_1 is as in Case I (resp. Case II), so are all $f_k\in\mathcal{F}$ $(k=1, \cdots, n)$ as $f_1-f_k\in L$. Suppose that we have Case I. Let $\mathcal{F}$ be of Type B. If $T_1\notin\mathcal{C}^\perp$, there exists $X\in\mathcal{C}$ with $|X\cap T_1|$=odd and then we have $((1/2)e_X, f_1)\equiv|X\cap T_1|/2 \bmod 1$, which means that $(1/2)e_X\notin\Lambda(f_1, \cdots, f_n)^\perp=(1/2)\Lambda(f_1, \cdots, f_n)$, contrary to the assumption that $\mathcal{F}$ is of Type B. So we must have $T_1\in\mathcal{C}^\perp$. Then if φ is an automorphism of L defined in Lemma 3.3.1, we get $\varphi(f_1)=\pm e_p$. By (4.1) applied to $\varphi(\mathcal{F})$, we can get $\sigma\in\mathrm{Aut}(L)$ such that $\sigma\varphi(\mathcal{F})=\mathcal{F}_0$. Next let $\mathcal{F}$ be of Type C. Then by using φ or ϕ in Lemma 3.3.1 according as $n/8\equiv 0$ or $1 \bmod 2$ and applying (4.1) to $\varphi(\mathcal{F})$ (resp. $\phi(\mathcal{F})$), we get $\sigma\in\mathrm{Aut}(L)$ such that $\sigma\varphi(\mathcal{F})$ or $\sigma\phi(\mathcal{F})=\mathcal{F}_0$. Now we are in Case II. Firstly suppose there exists $X\in\mathcal{C}$ with $|X\cap T_1|$=odd. Then if ε_X is an orthogonal transformation defined by

$$\varepsilon_X(e_i)=\begin{cases} e_i & i\notin X \\ -e_i & i\in X, \end{cases}$$

$\varepsilon_X(f_1)$ has the shape as in Case I and so, by (4.1), we have $\sigma\in\mathrm{Aut}(L)$ such that $\sigma\varepsilon_X(\mathcal{F})=\mathcal{F}_0$. So we may assume $T_1\in\mathcal{C}^\perp$. Then $\mathcal{F}$ must be of Type B. In fact, as we see $((1/2)e_X, f_k)$, $((1/4)e_\Omega, f_k)\in\boldsymbol{Z}$ for all $X\in\mathcal{C}$ and all $f_k\in\mathcal{F}$, we have $(1/2)e_X$, $(1/4)e_\Omega\in\Lambda(f_1, \cdots, f_n)^\perp=(1/2)\Lambda(f_1, \cdots, f_n)$ which would be a contradiction if $\mathcal{F}$ were of Type C. If ρ is an automorphism of L defined in Lemma 3.3.2, we have $|\mathrm{supp}(\rho(f_1))|=1$ and then (4.1) yields $\sigma\in\mathrm{Aut}(L)$ such that $\sigma(\rho(\mathcal{F}))=\mathcal{F}_0$. This completes the proof of Theorem 2.

REMARK 4.3.1. (i) Let L be an integral lattice with a frame of Type B. If we use an expression of L in Remark 2.1.4 and an automorphism ρ in Remark 3.3.3, the same arguments as above apply. Therefore Theorem 2 holds for any integral lattice with a frame of Type B. (ii) For a frame of Type C, the situation is not the same. In fact, let $\mathcal{C}$ be a doubly even self-dual code and $L=L_C^\varepsilon(\mathcal{C})$ where $n/8\equiv-\varepsilon \bmod 2$. Then L is not even. Assume that $\mathcal{C}$ has a T-decomposition $\Pi=\{T_1, \cdots, T_{n/4}\}$, and set $f_i=(1/2)e_T-e_i$ $(i\in T\in\Pi)$. Then we see that $\mathcal{F}=\{f_1, \cdots, f_n\}$ is a frame of Type C of L and the code associated with $\mathcal{F}$ is $\langle X, A+T_1 \mid X\in\mathcal{C}\cap\langle T_1\rangle^\perp\rangle$ where A is an element of $\mathcal{C}$ with $|A\cap T_1|$ $=$odd. But this code is not doubly even as $|A+T_1|\equiv 2 \bmod 4$ and, in particular, is not isomorphic to $\mathcal{C}$.

§ 5. Some examples.

5.1. We denote by $\boldsymbol{F}_2^n$ a vector space of row vectors of length n over $\boldsymbol{F}_2$, the field of 2 elements. To $X\in P(\Omega_n)$ we assign a vector $v_X=(x_1, x_2, \cdots, x_n)$ in $\boldsymbol{F}_2^n$ as follows:

$$x_i=\begin{cases} 1 & i\in X \\ 0 & i\notin X \end{cases} \quad (1\leqq i\leqq n).$$

Then a mapping $X\to v_X$ yields an isomorphism $P(\Omega_n)\cong\boldsymbol{F}_2^n$ as a vector space over $\boldsymbol{F}_2$. Thus a code of length n, i. e. a subspace of $P(\Omega_n)$ can be regarded as a subspace of $\boldsymbol{F}_2^n$.

5.2. Let

$$D_i=\{2i-1, 2i, 2i+1, 2i+2\}\in P(\Omega_n) \qquad a_n=\{1, 3, \cdots, n_0\}\in P(\Omega_n),$$

where n_0 is the largest odd integer $\leqq n$.

Now we define codes $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$ as follows:

$$\mathcal{E}_7=\langle D_1, D_2, a_7\rangle\subset P(\Omega_7),$$
$$\mathcal{E}_8=\langle D_1, D_2, D_3, a_8\rangle\subset P(\Omega_8),$$
$$\mathcal{D}_{2k}=\langle D_i \mid i=1, 2, \cdots, k-1\rangle\subset P(\Omega_{2k}).$$

Then $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$ are doubly even codes generated by tetrads (4-element subsets of $P(\Omega_n)$) of length 7, 8 and $2k$ respectively. It is known that any self-orthogonal code generated by tetrads is isomorphic (equivalent) to a direct sum of components $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$ (cf. Theorem 6.5 in Pless and Sloane [9]). Let us call the set of the generators a_7, a_8, D_1, D_2, $\cdots$ etc. of $\mathcal{E}_7$, $\mathcal{E}_8$ and $\mathcal{D}_{2k}$ a *natural basis* of those codes. We see from the structure of $\mathcal{D}_{2k}$ that

(5.2.1) *if* X_i $(i=1, 2, 3)$ *are elements of* $\mathcal{D}_{2k}$ *such that* $|X_i|=4$ *and* $X_1\cap X_2\cap X_3 \neq \emptyset$, *then we must have* $X_1\cap X_2\subset X_3$.

Let

$$\mathcal{E}_{8k} = \langle D_i, a_{8k} \mid i=1, 2, \cdots, 4k-1\rangle \subset P(\Omega_n).$$

$\mathcal{E}_{8k}$ $(k\geqq 1)$ is a doubly even self-dual code of length $8k$. When we regard $\mathcal{E}_7$, $\mathcal{E}_{8k}$ and $\mathcal{D}_{2k}$ as a subspace of F_2^n, their generator matrices are

$$\begin{pmatrix}1111 & & \\ & 1111 & \\ 1\ 1\ 1\ 1 & & \end{pmatrix}, \quad \begin{pmatrix}1111 & & & \\ & 1111 & & \\ & & \ddots & \\ & & & 1111 \\ 1\ 1\ 1\cdots 1\ 1 & & & \end{pmatrix}, \quad \begin{pmatrix}1111 & & & \\ & 1111 & & \\ & & \ddots & \\ & & & 1111\end{pmatrix}$$

sizes 3×7 $\qquad (4k-1)\times 8k \qquad (k-1)\times 2k$

respectively.

5.3. It is not difficult to see that, for $C=\mathcal{E}_7$, $\mathcal{E}_8$ or $\mathcal{D}_{2k}$, $L_A(C)$ is a lattice of root system of type E_7, E_8 or D_{2k} respectively. Now we will show

(5.3.1) $\qquad L_B(2\mathcal{E}_8)\cong L_B(\mathcal{E}_{16})$ but $L_C(2\mathcal{E}_8)\not\cong L_C(\mathcal{E}_{16})$,

(5.3.2) $\qquad L_C(3\mathcal{E}_8)\cong L_C(\mathcal{E}_8+\mathcal{E}_{16})$,

(5.3.3) $\qquad L_C(4\mathcal{E}_8)\cong L_C(2\mathcal{E}_{16})\not\cong L_C(2\mathcal{E}_8+\mathcal{E}_{16})$,

which give counter examples to Theorem 2 or 3 in small dimension cases ($m\mathcal{E}_8$ denotes a direct sum of m copies of $\mathcal{E}_8$). Every lattice exhibited in (5.3.1)-(5.3.3), more generally of the form $L_U(k\mathcal{E}_8+l\mathcal{E}_{16})$ ($U=B$ or C), possesses a frame $\mathcal{F}=\{\pm f_i \mid i=1, 2, \cdots\}$ of Type A:

$$(f_1, f_2, f_3, f_4)=(e_1, e_2, e_3, e_4)H, \qquad \text{where } H=\frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

where indices of the f_i and the e_i should be taken mod 4. Let C' be a code associated with the frame $\mathcal{F}$ of Type A for each lattice. The proof of (5.3.1)-(5.3.3) can be done by calculating a code C'. Now we will prove (5.3.1). Let $L=L_B(C)=L_A(C')$ where C is $2\mathcal{E}_8$ or $\mathcal{E}_{16}$. From the fact that $L\ni(1/2)(e_1\pm e_2+e_5\pm e_6)$ $=(1/2)(f_1+f_2+f_5+f_6)$ or $(1/2)(f_3+f_4+f_7+f_8)$, we see

(5.3.4) $\qquad C\ni\{1, 2, 5, 6\} \bmod 8, \qquad \{3, 4, 7, 8\} \bmod 8.$

Expressing $(1/2)(e_{i+1}+e_{i+3}+e_{i+5}+e_{i+7})$ ($i=0$ or 8) or $(1/2)(e_7\pm e_8+e_9\pm e_{10})$ by the f_j, we see

$$\mathcal{C}' \ni \begin{cases} \{1, 3, 5, 7\},\ \{9, 11, 13, 15\} & \text{if } \mathcal{C}\cong\mathcal{E}_8, \\ \{5, 6, 9, 10\},\ \{7, 8, 11, 12\} & \text{if } \mathcal{C}\cong\mathcal{E}_{16}. \end{cases} \tag{5.3.5}$$

Also expressing e_1-e_9 or $(1/2)(e_1+\cdots+e_{15})$ by the f_j, we see

$$\mathcal{E}' \ni \begin{cases} \{1, 2, 3, 4, 9, 10, 11, 12\} & \text{if } \mathcal{C}\cong\mathcal{E}_8, \\ \{1, 3, 5, 7, 9, 11, 13, 15\} & \text{if } \mathcal{C}\cong\mathcal{E}_{16}. \end{cases} \tag{5.3.6}$$

Thus, from (5.3.4)-(5.3.6), we get generator matrices for $\mathcal{C}'$,

$$\left(\begin{array}{cccccccccccccccc}
1&1&&&1&1&&&&&&&&&& \\
&&1&1&&&1&1&&&&&&&& \\
&&&&&&&&1&1&&&1&1&& \\
&&&&&&&&&&1&1&&&1&1 \\
1&&1&&1&&1&&&&&&&&& \\
&&&&&&&&1&&1&&1&&1& \\
1&1&1&1&&&&&1&1&1&1&&&&
\end{array}\right), \quad
\left(\begin{array}{cccccccccccccccc}
1&1&&&1&1&&&&&&&&&& \\
&&1&1&&&1&1&&&&&&&& \\
&&&&&&&&1&1&&&1&1&& \\
&&&&&&&&&&1&1&&&1&1 \\
&&&&1&1&&&1&1&&&&&& \\
&&&&&&1&1&&&1&1&&&& \\
1&&1&&1&&1&&1&&1&&1&&1&
\end{array}\right)$$

(blank denotes 0)

according as $\mathcal{C}$ is $2\mathcal{E}_8$ or $\mathcal{E}_{16}$. By rearranging columns suitably, we find that these generator matrices yield equivalent codes both of which are generated by $2\mathcal{D}_8$ and a_{16}. Thus we get $L_B(2\mathcal{E}_8)\cong L_B(\mathcal{E}_{16})$. When we add a word (1000100010001000) to the last row of the above matrices, we get a generator matix of $\mathcal{E}_{16}$ or $2\mathcal{E}_8$ respectively. Since $(1/4)(e_1+\cdots+e_{16})=(1/2)(f_1+f_5+f_9+f_{13})$ corresponds to a word (1000100010001000), we get

$$L_C(2\mathcal{E}_8)\cong L_A(\mathcal{E}_{16}) \quad \text{and} \quad L_C(\mathcal{E}_{16})\cong L_A(2\mathcal{E}_8).$$

In particular, $L_C(2\mathcal{E}_8)\not\cong L_C(\mathcal{E}_{16})$ because $2\mathcal{E}_8\not\cong\mathcal{E}_{16}$ and so $L_A(2\mathcal{E}_8)\not\cong L_A(\mathcal{E}_{16})$ by Theorem 3. Similarly we can give a generator matrix of a code $\mathcal{C}'$ for each lattice in (5.3.2) and (5.3.3). In fact, for lattices in (5.3.2), $\mathcal{C}'$ is generated by $3\mathcal{D}_8$ and row vectors of the following matrix (glue words for the direct sum $3\mathcal{D}_8$):

$$\begin{pmatrix} a\,a\,0 \\ 0\,a\,a \\ c\,b\,b \end{pmatrix}, \quad \begin{pmatrix} a\,b\,b \\ 0\,a\,a \\ c\,a\,0 \end{pmatrix}, \qquad \text{where } a=a_8,\ b=(11000000) \text{ and } c=a+b$$

according as $\mathcal{C}$ is $3\mathcal{E}_8$ or $\mathcal{E}_8+\mathcal{E}_{16}$. Those two codes are equivalent and so we get (5.3.2). Also for lattices in (5.3.3), $\mathcal{C}'$ is generated by $4\mathcal{D}_8$ and glue words for the $4\mathcal{D}_8$:

$$\begin{pmatrix} a\,a\,0\,0 \\ 0\,a\,a\,0 \\ 0\,0\,a\,a \\ b\,b\,b\,b \end{pmatrix}, \quad \begin{pmatrix} a\,a\,0\,0 \\ 0\,0\,a\,a \\ b\,b\,b\,b \\ a\,0\,a\,0 \end{pmatrix}, \quad \begin{pmatrix} a\,a\,0\,0 \\ 0\,a\,b\,b \\ 0\,0\,a\,a \\ b\,b\,a\,0 \end{pmatrix}$$

according as $\mathcal{C}$ is $4\mathcal{E}_8$, $2\mathcal{E}_{16}$ or $2\mathcal{E}_8+\mathcal{E}_{16}$ respectively. Clearly the first and the second matrices yield equivalent codes, while the third one is not equivalent to others.

REMARK. There exist four doubly even self dual codes of length 40 with the core (a subcode generated by all tetrads) $5\mathcal{D}_8$ and the following glue words:

$aa000$	$aa000$	$abb00$	$aa000$
$0aa00$	$0aa00$	$0bbbb$	$cbb00$
$00aa0$,	$00abb$,	$0aa00$,	$0aca0$
$000aa$	$000aa$	$000aa$	$00bbc$
$cbbbb$	$cbba0$	$ca0a0$	$000aa$

respectively. The first three codes come from lattices of the form $L_C(k\mathcal{E}_8+l\mathcal{E}_{16})$ where $(k, l)=(5, 0)$, $(3, 1)$ or $(1, 2)$, while the last one does not.

§ 6. The family $\mathcal{H}_{32}$.

6.1. In this section, we will see that Theorem 2 holds for the family $\mathcal{H}_{32}$ (§ 1.3), although just a brief outline will be given.

Let $\mathcal{F}_0=\{\pm e_1, \cdots, \pm e_n\}$ be a frame of an even lattice L of Type B or C and $\mathcal{F}=\{\pm f_1, \cdots, \pm f_n\}$ be a frame of L of the same type as $\mathcal{F}_0$. Set, as in § 4,

$$f_i=\sum_{j=1}^{n} a_{ij}e_j \quad (i=1, 2, \cdots, n) \qquad \text{and} \qquad A=(a_{ij}).$$

If $n\leqq 32$, the orthogonal matrix A has several possibilities other than those in Lemma 4.1. In particular, we see from the proof of Lemma 4.1 that

(6.1) *If $n=32$ and A is not as in Lemma 4.1, $\mathcal{F}_0$ is of Type C and $4A$ is a direct sum of two Hadamard matrices H_1 and H_2 of degree* 16: $4A=\begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}$.

6.2. Now let L be an even unimodular lattice in E^n having no 2-vectors. Then $\mathcal{F}_0$ is a frame of Type C. If A is as in Lemma 4.1, the same arguments as in § 4 can be applied and so Theorem 2 holds in this case. Therefore, by (6.1), we may assume that $4A$ is a direct sum of two Hadamard matrices H_1 and H_2 of degree 16. But as we are assuming that C has the minimum weight $\geqq 8$, we see that both H_1 and H_2 must be equivalent to the Hadamard matrix H_0 of the character table of an elementary abelian group of order 16:

$$H_0=\begin{array}{cccc}
++++ & ++++ & ++++ & ++++ \\
++++ & ++++ & ---- & ---- \\
++++ & ---- & ++++ & ---- \\
++++ & ---- & ---- & ++++ \\[1ex]
++-- & ++-- & ++-- & ++-- \\
++-- & ++-- & --++ & --++ \\
++-- & --++ & --++ & ++-- \\
++-- & --++ & ++-- & --++ \\[1ex]
+-+- & +-+- & +-+- & +-+- \\
+-+- & +-+- & -+-+ & -+-+ \\
+-+- & -+-+ & +-+- & -+-+ \\
+-+- & -+-+ & -+-+ & +-+- \\[1ex]
+--+ & +--+ & +--+ & +--+ \\
+--+ & +--+ & -++- & -++- \\
+--+ & -++- & +--+ & -++- \\
+--+ & -++- & -++- & +--+
\end{array}$$

where $+$ and $-$ denote $+1$ and -1 respectively. In fact, it is known that there exist five inequivalent Hadamard matrices of degree 16, but those other than H_0 yield codes with minimum weight 4.

6.3. Let $\mathcal{Q}_{16}$ be a code of length 16 generated by vectors

$$\frac{1}{2}(v_1 \pm v_2) \bmod 2 \qquad (\in \boldsymbol{F}_2^{16}),$$

where v_1 and v_2 run over all row vectors of H_0. Then a generator matrix of $\mathcal{Q}_{16}$ is

$$\begin{array}{l} uu00 \\ 0uu0 \\ 00uu \\ yyyy \\ xxxx \end{array} \qquad \text{where} \quad \begin{array}{l} u=(1111) \\ x=(0101) \\ y=(0011). \end{array}$$

Moreover $\mathcal{Q}_{16}^{\perp}$ is generated by $\mathcal{Q}_{16}$ and six vectors of length 16:

(6.3.1) $u000$, $yy00$, $xx00$, $y0y0$, $x0x0$, $vvvv$, *where* $v=(1000)$.

Also we have that

(6.3.2) *the minimum weight of vectors in each coset* ($\neq \mathcal{Q}_{16}$) *of the quotient space* $\mathcal{Q}_{16}^{\perp}/\mathcal{Q}_{16}$ *is either* 4 *or* 6, *and*

(6.3.3) *there exist* 35 *cosets of* $\mathcal{Q}_{16}^{\perp}/\mathcal{Q}_{16}$ *with minimum weight* 4 *whose representatives are as follows:*

(i) $u000$, $vvvv$,

(ii) $ww00$, $w'w00$, $w0w0$, $w'0w0$, $0ww0$, $0w'w0$
where $w=x$, y *or* $z=(0110)=x+y$ *and* $w'=u+w$,

(iii) v_iv_ivv, v_ivvv_iv, vv_iv_iv *where* $i=1, 2, 3, 4$ *and* $v_i=(00\overset{i}{1}0)$, $v_iv_jv_kv$
where $\{i, j, k\}$ *is any permutation of* 2, 3, 4.

REMARK. $\mathcal{Q}_{16}$ (resp. $\mathcal{Q}_{16}^{\perp}$) is the 1st (resp. 2nd) order Reed-Müller code of length 16.

6.4. Since $4A$ is a direct sum of two H_0's, $\mathcal{Q}$ contains a direct sum $2\mathcal{Q}_{16}$ of two $\mathcal{Q}_{16}$'s. Let $w_1w_2 \in C$ be a glue word for $2\mathcal{Q}_{16}$, where w_1 and w_2 are vectors of length 16. Then from (6.3.2) and the fact that the minimum weight of $C \geqq 8$, we see that a coset of $\mathcal{Q}_{16}^{\perp}/\mathcal{Q}_{16}$ containing w_2 is uniquely determined by w_1. So we write $w_2 = f(w_1)$. Now we will determine $f(w_1)$ where w_1 runs over all vectors in (6.3.1). Note that $f(w_1)$ can be taken as a vector of weight 4 by (6.3.2). When we rearrange $e_{17}, \cdots, e_{32}$ and $f_{17}, \cdots, f_{32}$ suitably by permutations which are induced from automorphisms of H_0 and $\mathcal{Q}_{16}$ (cf. (ii) and (iii) of Lemma 6.5.1 below), it turns out that we may assume

$$f(u000) = u000 \qquad \text{and} \qquad f(yy00) = yy00\,.$$

Instead of the details of the proof of this fact, typical examples will be given:

EXAMPLE. (1) From (ii) and (iii) of Lemma 6.5.1 we see that $\mathrm{Aut}(\mathcal{Q}_{16})$ acts transitively on the set of the cosets of $\mathcal{Q}_{16}^{\perp}/\mathcal{Q}_{16}$ of minimum length 4. For example we have

$$(yy00)w_2 = u000, \quad (y'y00)a_2r_2 = yy00 \ (y'=y+u), \quad (xx00)w_1 = yy00,$$
$$(x00x)r_3w_3w_1 = yy00, \quad (vvvv)w_2w_3w_1w_2 = u000 \text{ etc.}$$

Thus we may assume $f(u000) = u000$. (2) We have eighteen possibilities for $f(yy00)$ i.e. vectors listed in (ii) of (6.3.3). For example let $f(yy00) = 0xx0$ (the sum of vectors $xx00$ and $x0x0$ in (6.3.1)). Then we have $0xx0 \equiv x00x \bmod \mathcal{Q}_{16}$, $(x00x)r_3w_3w_1 = yy00$ and $(u000)r_3w_3w_1 = u000$. In this way, we can find a permutation which sends $f(yy00)$ to $yy00$ and leaves $u000$ invariant for all possibilities of $f(yy00)$.

Now we see that $f(y0y0)$ must be one of $y0y0$, $y'0y0$, $0yy0$, $0y'y0$, $xx00$, $x'x00$, $zz00$ or $z'z00$. Then by rearranging the e_i and f_i $(17 \leqq i \leqq 32)$ by permutations which leave $u000$ and $yy00$ invariant, we may assume $f(y0y0) = y0y0$ or $xx00$, and then $f(xx00) = xx00$ or $y0y0$ according as $f(y0y0) = y0y0$ or $xx00$. Also we may assume $f(x0x0) = x0x0$ as $f(x0x0) = x0x0$ or $x'0x0$. Finally we must have $f(vvvv) = vvvv$. Thus C is equivalent to one of two codes generated by $2\mathcal{Q}_{16}$ and glue words for $2\mathcal{Q}_{16}$

$u000\,u000$		$u000\,u000$
$yy00\,yy00$		$yy00\,yy00$
$xx00\,xx00$	or	$y0y0\,xx00$
$y0y0\,y0y0$		$xx00\,y0y0$
$x0x0\,x0x0$		$x0x0\,x0x0$
$vvvv\,vvvv$		$vvvv\,vvvv$

respectively. (The first code is the 2nd order Reed-Müller code of length 32.) Then noting that the matrix A is still a direct sum of two H_0's, we easily see that an orthogonal transformation $e_i \to f_i$ leaves $L = L_C(\mathcal{C})$ invariant. This proves Theorem 2 for the family $\mathcal{H}_{32}$.

REMARK. It is known (cf. [5]) that $\mathcal{H}_{32}$ consists of five codes among which just two codes contain $2\mathcal{Q}_{16}$.

6.5. We will give a lemma about $\mathrm{Aut}(H_0)$, $\mathrm{Aut}(\mathcal{Q}_{16})$ which was used in § 6.3. The proof is left to the readers.

LEMMA 6.5.1. (i) $\mathrm{Aut}(H_0) \cong 2^{1+8} \cdot GL_4(2)$ *(an extension of* $GL_4(2)$ *by an extra-special group of order* 2^9*) and* $\mathrm{Aut}(\mathcal{Q}_{16}) \cong \mathrm{Aut}(\mathcal{Q}_{16}^{\perp}) \cong 2^4 \cdot GL_4(2)$ *(an extension of* $GL_4(2)$ *by an elementary abelian group of order* 2^4*).*

(ii) *A complement* $GL_4(2)$ *of these groups is generated by the following permutations of columns of* H_0 *or those of a generator matrix of* $\mathcal{Q}_{16}$ *or* $\mathcal{Q}_{16}^{\perp}$:

$$w_1 = (2, 3)(6, 7)(10, 11)(14, 15), \quad w_2 = (3, 5)(4, 6)(11, 13)(12, 14)$$

$$w_3 = (5, 9)(6, 10)(7, 11)(8, 12), \quad r_1 = (3, 4)(7, 8)(11, 12)(15, 16)$$

$$r_2 = (5, 7)(6, 8)(13, 15)(14, 16), \quad r_3 = (9, 13)(10, 14)(11, 15)(12, 16).$$

For $\mathrm{Aut}(H_0)$, *also permutations of rows of* H_0 *should be accompanied:*

$$w_1 = (5, 9)(6, 10)(7, 12)(8, 11), \quad w_2 = (3, 5)(4, 6)(11, 13)(12, 14)$$

$$w_3 = (2, 3)(6, 8)(10, 11)(14, 15), \quad r_1 = (9, 13)(10, 14)(11, 15)(12, 16)$$

$$r_2 = (5, 8)(6, 7)(13, 15)(14, 16), \quad r_3 = (3, 4)(7, 8)(11, 12)(15, 16).$$

(iii) *The following permutations of columns of the generator matrix of* $\mathcal{Q}_{16}$ *are in* $\mathrm{Aut}(\mathcal{Q}_{16})$:

$$a_1 = (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)(11, 12)(13, 14)(15, 16),$$

$$a_2 = (1, 3)(2, 4)(5, 7)(6, 8)(9, 11)(10, 12)(13, 15)(14, 16).$$

These are in $\mathrm{Aut}(H_0)$ *too, if suitable permutations of rows of* H_0 *are accompanied.*

References

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

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

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

[4] ——— and N. J. A. Sloane, Sphere Packings, Lattices and Groups, Grundlehren Math. Wiss., **290**, Springer, 1988.

[5] ——— and Vera Pless, On the enumeration of self-dual codes, J. Combin. Theory Ser. A, **28** (1980), 26-53.
[6] M. Ozeki, Examples of even unimodular extremal lattices of rank 40 and their Siegel theta-series of degree 2, J. Number Theory, **28** (1988), 119-131.
[7] ———, On the relation between the invariants of a doubly even self-dual code C and the invariants of the even unimodular lattice $L(C)$ defined from the code C, Research Institute for Mathematical Sciences, Kyoto Univ. RIMS Kokyuroku, 1988, pp. 126-138.
[8] Vera Pless, On the uniqueness of the Golay codes, J. Combin. Theory, **5** (1968), 215-228.
[9] ——— and N. J. A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory, Ser. A, **18** (1975), 313-335.
[10] N. J. A. Sloane, Self-dual codes and lattices, Proc. Sympos. Pure Math., **34** (1979), 273-308.
[11] T. Tasaka, On even lattices of 2-square type and self-dual codes, J. Fac. Sci. Univ. Tokyo Sect. IA., **28** (1982), 701-714.

Masaaki KITAZUME
Department of Mathematics
Faculty of General Education
Gifu University
Yanagido, Gifu 501-11
Japan

Takeshi KONDO
Department of Mathematics
Tokyo Woman's Christian University
Zenpukuji Suginami, Tokyo 167
Japan

Izumi MIYAMOTO
Department of Computer Sciences
Faculty of Engineering
Yamanasi University
Takeda, Kofu 400
Japan