Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 315–324

3-transposition automorphism groups of VOA

Masaaki Kitazume and Masahiko Miyamoto

Abstract.

We will consider some vertex operator algebras (VOAs) whose automorphism groups are generated by 3-transpositions. Our main examples are some code VOAs. We will classify the structures of the automorphism groups of the code VOAs. We give explicit constructions of such code VOAs, and determine the full automorphism groups for some cases.

§1. Introduction

A vertex operator algebra V is an infinite dimensional $\mathbb{Z}$-graded algebra, but it has sometimes a finite full automorphism group and a vertex operator subalgebra offers automorphisms of V, see [M1]. In this paper, we will treat the case where $\dim V_0 = 1$ and $V_1 = 0$. In this case, V_2 is a commutative (nonassociative) algebra with a symmetric invariant bilinear form $\langle *, * \rangle$ given by $\langle v, u \rangle \mathbf{1} = v_3 u$ for $u, v \in V_2$. This is called a Griess algebra in [M1]. Our purpose in this paper is to study several vertex operator algebras which have 3-transposition automorphism groups. A 3-transposition group is a group generated by a conjugacy class of involutions such that the product of two involutions in this class has the order less than or equal to 3. First examples are the code VOAs M_C which are constructed from even linear binary codes C in [M2]. If C has no codewords of weight 2, then $\dim(M_C)_0 = 1$ and $(M_C)_1 = 0$ and so $(M_C)_2$ is a Griess algebra. In this case, the full automorphism group of M_C is finite [M4] and the automorphism group of M_C has a normal subgroup which is a 3-transposition group. We will classify such 3-transposition groups G and construct code VOAs with automorphism groups G. Other examples are the Weyl groups of the root lattices of simply laced finite dimensional Lie algebras, which are also 3-transposition groups. Actually, for every root lattice, we will construct a VOA whose automorphism group contains a semidirect product

Received May 31, 1999.
Revised June 22, 2000.

of the Weyl group and some 2-group. Our most interesting example is a VOA constructed from the E_8-lattice. This VOA also has a structure of a code VOA. We will show its full automorphism group is isomorphic to $O^+(10, 2)$, which contains properly the semidirect product mentioned above. We note that this result is already shown by R. Griess [G].

The essential tool is a rational conformal vector with central charge $\frac{1}{2}$. Here a rational conformal vector e is an element in V_2 such that $\tilde{L}(n) = e_{n+1}$ satisfies Virasoro algebra relations:

$$[\tilde{L}(m), \tilde{L}(n)] = (m-n)\tilde{L}(m+n) + \delta_{m+n,0}\frac{m^3 - m}{24}1_V$$

with central charge $\frac{1}{2}$ and $\{e_n\}$ generates a rational Virasoro VOA $L(\frac{1}{2}, 0)$ over the vacuum $\mathbf{1}$, where $Y(e, z) = \sum_{n\in\mathbb{Z}} e_n z^{-n-1}$ is a vertex operator of e.

§2. Griess Algebras

Let $V = \oplus_{n=0}^{\infty} V_n$ be a vertex operator algebra (VOA) with the vacuum $\mathbf{1} \in V_0$ and the Virasoro element $\mathbf{w} \in V_2$. In this paper, we assume that V is a VOA over the real field $\mathbb{R}$ and has a positive definite invariant bilinear form $\langle \cdot, \cdot \rangle$. For example, a lattice VOA or a code VOA satisfies these conditions.

We further assume the following conditions:

$$\dim(V_0) = 1 \text{ (i.e.} V_0 = \langle \mathbf{1} \rangle), \quad \dim(V_1) = 0.$$

Then by [Li], the invariant bilinear form is uniquely determined up to scalar multiplication, and we may assume

$$\langle u, v \rangle \mathbf{1} = u_3 v$$

for every $u, v \in V_2$. Moreover we can define a binary symmetric product $u \times v$ on V_2 by

$$u \times v := u_1 v.$$

The triple $(V_2, \times, \langle \cdot, \cdot \rangle)$ is called a Griess algebra.

In [M1], the following theorems has been proved.

Theorem 2.1. *The following two conditions are equivalent to each other.*

(1) *$\frac{1}{2}e \in V_2$ is an idempotent (i.e. $e \times e = 2e$) with $\langle e, e \rangle = \frac{1}{4}$*

(2) *e is a rational conformal vector with central charge $\frac{1}{2}$, that is, the subVOA* Vir(e) *generated by e is isomorphic to $L(\frac{1}{2}, 0)$.*

Then V splits into the direct sum of irreducible Vir(e)-submodules, which is isomorphic to $L(\frac{1}{2},0), L(\frac{1}{2},\frac{1}{2})$ or $L(\frac{1}{2},\frac{1}{16})$. If there exist no Vir($e$)-submodules isomorphic to $L(\frac{1}{2},\frac{1}{16})$, then we say that e is of type 2. An idempotent which is not of type 2 is called of type 1.

Theorem 2.2. (1) *For an idempotent e of type 1, define an endomorphism τ_e on V by*

$\tau_e = id$ *on submodules isomorphic to* $L(\frac{1}{2},0)$ *or* $L(\frac{1}{2},\frac{1}{2})$
$\tau_e = -id$ *on submodules isomorphic to* $L(\frac{1}{2},\frac{1}{16})$.

Then τ_e is a automorphism of the VOA V, and $\tau_e^2 = id_V$.

(2) *For an idempotent e of type 2, define an endomorphism σ_e on V by*

$\sigma_e = id$ *on submodules isomorphic to* $L(\frac{1}{2},0)$
$\sigma_e = -id$ *on submodules isomorphic to* $L(\frac{1}{2},\frac{1}{2})$.

Then σ_e is a automorphism of the VOA V, and $\sigma_e^2 = id_V$.

Theorem 2.3. *If $e, f\ (e \neq f)$ are conformal vectors of type 2, then one of the following holds.*

(1) $\langle e,f\rangle = 0$ *and* $(\sigma_e\sigma_f)^2 = 1$
(2) $\langle e,f\rangle = \frac{1}{32}$ *and* $(\sigma_e\sigma_f)^3 = 1$

§3. Code Vertex Operator Algebras

Let C be a binary even code of length n. We further assume that the minimal weight of C is four. Let M_C be the code VOA defined in [M2], that is,

$$M_C = \bigoplus_{c\in C} M_c$$

and $M_c(c = (c_1, c_2, ..., c_n) \in C)$ consists of all linear combinations of the form $u_1 \otimes u_2 \otimes ... \otimes u_n \otimes e^c$ $(u_i \in L(\frac{1}{2}, \frac{c_i}{2}))$, where c_i are regarded as integers $0, 1$, and e^c is a symbol with $e^c e^{c'} = (-1)^{\langle c,c'\rangle} e^{c'} e^c$. The degree of $u_1 \otimes u_2 \otimes ... \otimes u_n \otimes e^c$ is the sum of the degrees of u_i and $\frac{1}{2}\langle c,c\rangle$ and so the degrees of elements in M_C are integers since C is an even code. The element $\hat{\mathbf{1}} = \mathbf{1}\otimes\mathbf{1}\otimes ... \otimes \mathbf{1} \otimes e^0$ is the vacuum of M_C. Set $\hat{\mathbf{w}}^i = \mathbf{1}\otimes\mathbf{1}\otimes ... \otimes \mathbf{w} \otimes ... \otimes \mathbf{1}\otimes e^0$ ($\mathbf{w}$ is on the i-th component) and define $\hat{\mathbf{w}} = \hat{\mathbf{w}}^1 + ... + \hat{\mathbf{w}}^n$. Then $\hat{\mathbf{w}}$ is the Virasoro element of M_C. The following Lemmas and Theorem are proved in [M2]. In particular, $(M_C)_2$ becomes a Griess algebra by Lemma 3.1.

Lemma 3.1 ([M2]). (1) *M_C has an invariant bilinear form.*
(2) $\dim(M_C)_0 = 1$ *and* $(M_C)_1 = \{0\}$.

Lemma 3.2 ([M2]). (1) $\hat{\mathbf{w}}^i$ *is a conformal vector of type* 2.
(2) *Let* H *be a* $[8,4,4]$*-Hamming subcode of* C *with* $\mathrm{supp}(H) = \{i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8\}$. *Then for any* $\alpha \in \mathbb{F}_2^n$,

$$e = e_{\alpha,H} := \frac{1}{8}(\hat{\mathbf{w}}^{i_1} + \dots + \hat{\mathbf{w}}^{i_8}) + \frac{1}{8} \sum_{\beta \in C,\ |\beta|=4} (-1)^{(\alpha,\beta)} u_\beta$$

is a conformal vector of $(M_C)_2$.
(3) *If* $\mathrm{supp}H \subset C^\perp$, *then* $e_{\alpha,H}$ *is of type* 2.

Remark 3.3. *If* α *equals to* α' *modulo* $H^\perp$, *we have* $e_\alpha = e_{\alpha'}$. *Hence there exist* 2^4 *elements* $e_{\alpha,H}$ *for each* H.

Theorem 3.4 ([M2]). *Let* D_C *be the set of involutions* σ_e *such that* e *is a conformal vector of type* 2. *and let* K_C *be the subgroup of* $\mathrm{Aut}(M_C)$ *generated by* D_C. *Then* D_C *is a set of* 3*-transpositions of* K_C.

Lemma 3.5. *Let* $X = \{\sigma_1, \dots, \sigma_n\}$, *where* $\sigma_i = \sigma_{\hat{\mathbf{w}}^i}$ *for* $i = 1, \dots, n$. *Let* e *be a conformal vector of type* 2 *and assume* $\sigma_e \notin X$. *Then* $|C_X(\sigma_e)| = n - 8$.

Proof. By the equations: $\frac{1}{4} = \langle e, e\rangle = \langle \mathbf{w}, e\rangle = \langle \hat{\mathbf{w}}^1 + \dots + \hat{\mathbf{w}}^n, e\rangle$ and Theorem 2.3, there are exactly eight $\hat{\mathbf{w}}^i$, say $\hat{\mathbf{w}}^1, \dots, \hat{\mathbf{w}}^8$, such that $\langle \hat{\mathbf{w}}^i, e\rangle = \frac{1}{32}$ for $i = 1, \dots, 8$ and $\langle \hat{\mathbf{w}}^i, e\rangle = 0$ for $i = 9, \dots, n$. Q.E.D.

Corollary 3.6. *The maximal number of mutually commuting elements of* D_C *is equal to the length* n *of the code* C.

Let G be a 3-transposition group generated by D. We will describe a 3-transposition group by the graph whose vertices are the elements of D and edges are defined by :

$$\{a, b\} \text{ is an edge} \iff a \neq b, (ab)^2 = 1.$$

We will denote this graph by $\Gamma(G)$ or $\Gamma(D)$. The graph $\Gamma(G)$ is connected if and only if D is a single conjugacy class of G.

If $O_2(G) \neq 1$, then $\bar{D} = DO_2(G)/O_2(G)$ is a set of 3-transpositions of $\bar{G} = G/O_2(G)$, and the number of the elements of $dO_2(G) \cap D$ is a power of 2 for any $d \in D$. If $\Gamma(G)$ is connected, then this number ($= 2^k$, say) does not depend on the choice of $d \in D$. Then we write $\Gamma(G) = O_2^{(2^k)} \cdot \Gamma(\bar{G})$. The set $dO_2(G) \cap D$ consists of mutually commuting elements, and $e \in dO_2(G) \cap D$ if and only if $C_D(d) = C_D(e)$.

If any two elements of D do not commute, then $G' = O_3(G)$ and $|D|$ is some power of 3. If $|D| = 3^t$ then we write $\Gamma(G) = \Gamma(H_t)$. Notice that $\Gamma(S_3) = \Gamma(H_1)$.

Now we will state the main result of this section. Here we denote by $O^+(2n, 2)$ the group generated by symplectic transvections preserving a given quadratic form with Witt index n. The group $O^+(2n,2)$ is a 3-transposition group and contains a simple subgroup $\Omega^+(2n,2)$ with its index 2.

Theorem 3.7. *Let K_C be the subgroup of* $\mathrm{Aut}(M_C)$ *generated by D_C, and E be a subset of D_C such that $\Gamma(E)$ is a connected component of $\Gamma(D_C)$. Then $\Gamma(E)$ is isomorphic to one of the following.*

	$\Gamma(E)$	$\|E\|$	ℓ
(i)	$\Gamma(O^+(10,2))$	496	16
(ii)	$\Gamma(Sp(8,2))$	255	15
(iii)	$O_2^{(2)} \cdot \Gamma(O^+(8,2))$	240	16
(iv)	$O_2^{(2)} \cdot \Gamma(Sp(6,2))$	126	14
(v)	$O_2^{(4)} \cdot \Gamma(S_{2m}) \quad (m>1)$	$4m(2m-1)$	$4m$
(vi)	$O_2^{(8)} \cdot \Gamma(H_k) \quad (k>1)$	8×3^k	8

Here ℓ is the maximal number of mutually commuting elements of E.

Proof. Set $H=\langle E\rangle$ and let Y be a maximal set of mutually commuting element of E, that is, Y is the intersection of E and a Sylow 2-subgroup of H. By Lemma 3.5, $|Y\setminus C_Y(\tau)|=8$ for each $\tau\in E\setminus Y$, since each element of E commutes with $D_C\setminus E$,

Let $\bar{H}=H/O_2(H), \bar{E}=EO_2(H)/O_2(H), \bar{Y}=YO_2(H)/O_2(H)$. Then $\Gamma(H)=O_2^{(2^k)}\cdot\Gamma(\bar{H})$ for some k and $\Gamma(\bar{H})$ is also connected. Moreover $\bar{H}$ satisfies that $|\bar{Y}\setminus C_{\bar{Y}}(\tau)|=\frac{8}{2^k}$ for each $\tau\in\bar{E}\setminus\bar{Y}$. In particular, $k=0,1,2$ or 3.

Suppose $O_3(\bar{H})\not\subset Z(\bar{H})$. Let $\tau\in\bar{Y}$ and $\tau'\in\tau\in\bar{E}\setminus\{\tau\}$. Then $\bar{Y}\setminus C_{\bar{Y}}(\tau')=\{\tau\}$ and so $k=3$. Hence if $\bar{Y}=\{\tau_1,...,\tau_s\}$ for some s, then $\bar{E}=(\tau_1O_3(\bar{H})\cap\bar{E})\cup...\cup(\tau_sO_3(\bar{H})\cap\bar{E})$. Since $\Gamma(\bar{H})$ is connected, we have $s=1$ Hence $\Gamma(\bar{H})=\Gamma(H_t)$ for some t. By the same argument if $k=3$ then $\Gamma(\bar{H})=\Gamma(H_t)$ for some t.

Now we may assume $O_3(\bar{H})\subset Z(\bar{H})\supset O_2(\bar{H})$. Then we can use the list of Fischer's classification [Fi], and it is easily verified that $\Gamma(\bar{H})$ is one of the following

$$\begin{array}{lll} (k=0) & \Gamma(O^+(10,2)), & \Gamma(Sp(8,2)) \\ (k=1) & \Gamma(O^+(8,2)), & \Gamma(Sp(6,2)) \\ (k=2) & \Gamma(S_{2m})(m>2). & \end{array}$$

The proof of Theorem is completed. Q.E.D.

Remark 3.8. (1) *The main parts of the groups of the cases $(iii), (iv)$ are the Weyl groups $W(E_8)$, $W(E_7)$ respectively. Under such a viewpoint, the main parts of the groups of (v) are the Weyl groups $W(D_{2m})$ $(m=2 for (vi))$. (i.e. $O_2^{(4)}\cdot\Gamma(S_{2m})\cong O_2^{(2)}\cdot\Gamma(W(D_{2m}))$)*

(2) $O_2^{(4)} \cdot \Gamma(S_4)$ *is also written as* $O_2^{(8)} \cdot \Gamma(H_1)$.
(3) *We do not know any examples of (vi) of Theorem.*

In general, we can not determine the center $Z(K_C)$ from the graph $\Gamma(K_C)$. Under some assumption, we can prove $Z(K_C) = \{id\}$.

Lemma 3.9. *If C is spanned by the elements of weight 4, then M_C is generated by $(M_C)_2$ as a VOA.*

Proof. Since $L(\frac{1}{2}, 0)$ is generated by its Virasoro element as a VOA, $M_0 (0 \in C)$ is generated by the vectors $\hat{\mathbf{w}}^i$. Since $L(\frac{1}{2}, \frac{1}{2})$ is generated by its highest weight vector as an $L(\frac{1}{2}, 0)$-module, $M_c (c \in C, wt(c) = 4)$ is generated by the element of degree 2 as an M_0-module. The assertion of Lemma is easily deduced from the fact $M_c M_{c'} \subset M_{c+c'}$ and $M_c M_{c'} \neq \{0\}$ for $c, c' \in C$. Q.E.D.

Lemma 3.10. (1) *If M_C is generated by $(M_C)_2$ as a VOA, then we have $Z(K_C) = \{id\}$.*
(2) *Furthermore if $(M_C)_2$ is spanned by the conformal vectors $e_{\alpha,H}$, then* $\mathrm{Aut}(M_C)$ *is a subgroup of* $\mathrm{Aut}(K_C)$

Proof. (1) is trivial. Let $\phi \in C_{\mathrm{Aut}(M_C)}(K_C)$. Then ϕ commutes with all the element of D_C, and thus ϕ stabilize all the vectors $e_{\alpha,H}$. By the assumption of (2), ϕ acts trivially on M_C and we have ϕ is the identity. Since K_C is a normal subgroup of $\mathrm{Aut}(M_C)$, Lemma is proved. Q.E.D.

§4. Weyl groups

Let L be a root lattice of type X_n with root system Φ, where X be one of A, D, E, and $n = 6, 7, 8$ if $X = E$. Let $V_{\sqrt{2}L}$ be the VOA constructed from $\sqrt{2}L$ as in [FLM]. Since there are no roots in $\sqrt{2}L$, $(V_{\sqrt{2}L})_1 = \mathbb{C} \otimes L$. Let θ be an automorphism induced from -1 on L and $V(X_n) = (V_{\sqrt{2}L})^\theta$ the fixed point space of θ. We will show that $\mathrm{Aut}(V(X_n))$ contains a semidirect product of the Weyl group $W(X_n)$ and some 2-group.

By the construction, $V(X_n)_2$ is spanned by the vectors $v(-1)v(-1)\mathbf{1}$ and $e^{\sqrt{2}x} + e^{-\sqrt{2}x}$ for $v \in L$ and $x \in \Phi$. The former are identified with the vectors of the symmetric tensor $S^2(\mathbb{R} \otimes L)$. In particular,

Lemma 4.1. $\dim V(X_n)_2 = \dfrac{n(n+1)}{2} + \dfrac{1}{2}|\Phi|.$

For example, $\dim V(E_8)_2 = 36 + 120 = 156$, and $\dim V(D_n)_2 = \frac{n(n+1)}{2} + n(n-1) = \frac{1}{2}(3n^2 - n)$.

Let $x \in \Phi$, then $\sqrt{2}x$ has a squared length 4 and so

$$e(x)^i = \frac{1}{8}x(-1)x(-1)\mathbf{1} - (-1)^i\frac{1}{4}(e^{\sqrt{2}x} + e^{-\sqrt{2}x}) \qquad (\#)$$

are conformal vectors with central charge $\frac{1}{2}$ for $i = 1, 2$. Since $V_{\sqrt{2}L}$ has a positive definite invariant bilinear form, $e(x)^1$ and $e(x)^2$ are both rational conformal vectors. As we showed in [M3],

$$x(-1) \in L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{1}{2}, \frac{1}{2})$$

and

$$e^y \in \left(L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2})\right) \otimes \left(L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2})\right)$$

as $\langle e(x)^1, e(x)^2\rangle$-modules for $y \in L$ with $\langle y, x\rangle \in 2\mathbb{Z}$. Therefore, we have proved the following result.

Lemma 4.2. *All conformal vectors $e(x)^i$ defined by roots in L as in (#) are of type* 2.

Let D be the set of all $\sigma_{e(x)^i}$ for $i = 1, 2$ and each root $x \in \Phi$. By Lemma 4.2 and Theorem 2.3, D is a set of 3-transpositions.

By direct calculations, we have:

Theorem 4.3. *Let x and y be distinct two roots. If $\langle x, y\rangle = 0$, then $\langle e(x)^i, e(y)^i\rangle = 0$ and $(\sigma_{e(x)^i}\sigma_{e(y)^i})^2 = 1$ for $i, j = 1, 2$. If $\langle x, y\rangle = \pm 1$, then $\langle e(x)^i, e(y)^i\rangle = \frac{1}{32}$ and $(\sigma_{e(x)^i}\sigma_{e(y)^i})^3 = 1$ for $i, j = 1, 2$.*

Notice that there exist two involutions $\sigma_{e(x)^1}, \sigma_{e(x)^2}$ for each root x. Hence the set $\{\sigma_{e(x)^1}, \sigma_{e(x)^2}\}$ is a nontrivial block of imprimitivity of the action of the group $\langle D\rangle$ on D by conjugation. ¿From a general theory of 3-transposition groups, all the products $\sigma_{e(x)^1}\sigma_{e(x)^2}$ generate the normal subgroup $O_2(\langle D\rangle)$. Hence the group $\langle D\rangle$ is a semidirect product of the Weyl group $W(X_n)$ and $O_2(\langle D\rangle)$, that is, $\Gamma(\langle D\rangle) \cong O_2^{(2)} \cdot \Gamma(W(X_n))$.

By [M5], we have the following Proposition.

Proposition 4.4. *The VOA $V(E_8)$ is isomorphic to the code VOA V_C, where C is the 2nd order Reed-Muller code $RM(4, 2)$ of length* 16.

Proof. We use the notation in Section 5 of [M5]. Let $\{x^1, ..., x^8\}$ be an orthonormal basis of an 8-dimensional Euclidean space. Set $L(1) = \langle x^i : i = 1, ..., 8\rangle$ and $E_8(4)$ be the lattice spanned by

$\frac{1}{2}(x^1 - x^3 - x^5 - x^7) + x^2$, $\frac{1}{2}(x^1 - x^2 + x^5 - x^6) - x^3$,
$\frac{1}{2}(-x^1 + x^2 - x^3 - x^4) - x^7$, $\frac{1}{2}(x^1 + x^3 - x^6 + x^8) + x^5$,
$2x^i$ $(i = 1, ..., 8)$,

which is isomorphic to the root lattice of type E_8. Then the lattice VOA $V_{E_8(4)}$ contains the following 16 mutually orthogonal conformal vectors of type 1 :

$$e^{2i-j} = \frac{1}{4}x^i(-1)^2\mathbf{1} - (-1)^j\frac{1}{4}(e^{2x^i} + e^{-2x^i})\ (i = 1, ..., 8,\ j = 1, 0).$$

Let $P(4) = \langle \tau_{e^i} : i = 1, ..., 16\rangle$ and $L(4) = E_8(4) \cap L(1)$. Then $L(4)$ is isomorphic to $\sqrt{2}E_8$ and $(V_{E_8(4)})^{P(4)}$ coincides with $V_{L(4)}$.

Let V be a VOA constructed by the orbifold construction from $V_{E_8(4)}$. Then V is isomorphic to $V_{E_8(4)}$. Let $P = \langle \tau_{e^i} : i = 1, ..., 16\rangle$. (Here we use the same symbols τ_{e^i}. Notice that $P \subset \mathrm{Aut}(V)$, and $P(4) \subset \mathrm{Aut}(V_{E_8(4)})$.) Then V^P is also constructed by the orbifold construction from $(V_{E_8(4)})^{P(4)}$, and V^P is isomorphic to M_C by Proposition 5.1 of [M5]. Clearly V^P contains $((V_{E_8(4)})^{P(4)})^\theta = (V_{L(4)})^\theta$, which is isomorphic to $V(E_8)$. By Lemma 4.1 we have $\dim V(E_8)_2 = 156$, and we will show that $\dim(M_C)_2 = 156$ in Section 5. Hence we have $(((V_{E_8(4)})^{P(4)})^\theta)_2 = (V^P)_2$ and thus $V(E_8)$ is isomorphic to M_C by Lemma 3.9. Q.E.D.

Similarly the following isomorphism can be proved.

$$V(E_7) \cong M_{C''}, V(D_{2m}) \cong M_{C_m},$$

where m is a integer and C' and C_m will be defined in the next section.

§5. Examples

In this section, we will give some examples and consider the full automorphism groups. The notation of (1) will be used in (2)-(4).

(1) $M_C \cong V(E_8)$: Let Ω be the set of all the vectors of the 4-dimensional vector space V over the two element field F_2, that is, a point of Ω is a vector of V. We regard the power set $P(\Omega)$ of Ω (i.e. the set of all the subsets of Ω) as a vector space over F_2 by defining the sum $X + Y$ as their symmetric difference $(X \cup Y) \setminus (X \cap Y)$ for $X, Y \subset \Omega$.

We define the code $C \subset P(\Omega)$ as the subspace spanned by all the 2-dimensional affine subspaces of V. Then C is a $[16, 11, 4]$-code and is known as the extended Hamming code of length 16 or the 2nd order Reed-Muller code $RM(4, 2)$ of length 16.

A codeword of minimal weight of C corresponds with a 2-dimensional affine subspace of V. Hence C contains $140(= \frac{(16-1)(16-2)}{(4-1)(4-2)} \times 4)$ vectors of weight 4, and thus $\dim(M_C)_2 = 156$.

Let W be a 3-dimensional affine subspace of V, and H_W be a subcode of C spanned by all the 2-dimensional affine subspaces of W.

Then it is easy to see that H_W is a [8,4,4]-Hamming subcode of C, and supp$H_W \subset C^{\perp}$. Since the number of the 3-dimensional affine subspaces of V is $30(=\frac{(16-1)(16-2)(16-4)}{(8-1)(8-2)(8-4)} \times 2)$, we can obtain $480(=30\times 2^4)$ involutions defined by a conformal vector e_{α,H_W} for some W. Hence the set D_C contains at least 496 elements. By Theorem 3.7, we have $|D_C| = 496$ and $\Gamma(K_C) \cong \Gamma(O^+(10,2))$. By Lemmas 3.9, 3.10 and the fact $|\mathrm{Out}(\Omega^+(10,2))| = 2$, we have $K_C = \mathrm{Aut}(M_C) \cong O^+(10,2)$.

We note that this result is already obtained by R. L. Griess ([G]).

(2) Let $\mathbf{0}$ be the zero vector of V, and set $\Omega' = \Omega \setminus \{\mathbf{0}\}$. We define the code $C' \subset P(\Omega')$ as the subspace spanned by all the 2-dimensional affine subspaces W of V satisfying $\mathbf{0} \notin W$. Then C' is a $[15, 10, 4]$-code.

By a similar calculations as in (1), we have that $\dim(M_{C'})_2 = 15 + \frac{(16-1)(16-2)}{(4-1)(4-2)} \times 3 = 120$, $|D_{C'}| = 15 + \frac{(16-1)(16-2)(16-4)}{(8-1)(8-2)(8-4)} \times 2^4 = 255$, and $\Gamma(K_{C'}) \cong \Gamma(Sp(8,2))$. By Lemma 3.10 and the fact $|\mathrm{Out}(Sp(8,2))| = 1$, we have $K_C = \mathrm{Aut}(M_C) \cong Sp(8,2)$.

(3) $M_{C''} \cong V(E_7)$: Let U be a one-dimensional subspace of V, and set $\Omega'' = \Omega \setminus U$. We define the code $C'' \subset P(\Omega'')$ as the subspace spanned by all the 2-dimensional affine subspaces W of V satisfying $U \cap W = \emptyset$. Then C'' is a $[14, 7, 4]$-code. There exist seven 2-(resp. 3-) dimensional linear subspaces containing U. Hence $\dim(M_{C''})_2 = 14 + 7 \times 3 + 28 \times 2 = 91$ and $|D_{C''}| = 14 + 7 \times 2^4 = 126$. Moreover we have $\Gamma(K_{C''}) \cong O_2^{(2)} \cdot \Gamma(Sp(6,2))$.

(4) $M_{C_m} \cong V(D_{2m})$: For an integer $m > 1$, we define a $[4m, 3m-2, 4]$-code C_m by the following generating matrix

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

Then $\dim(M_{C_m})_2 = 6m^2 - m$, $|D_{C_m}| = 8m^2 - 4m$, and $\Gamma(K_{C_m}) \cong O_2^{(4)} \cdot \Gamma(S_{2m})$.

(5) Let r be a integer greater than 1. Let $V_i, \Omega_i, C_i \subset P(\Omega_i)$ be a copy of V, Ω, C of (1) respectively for $i = 1, ..., r$. We fix a 1-dimensional subspace U_i of V_i for each i.

Set $\tilde{C} = C_1 \oplus C_2 \oplus ... \oplus C_r$, $\tilde{V_i} = \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\} \oplus V_i \oplus \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\}$, $\tilde{U_i} = \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\} \oplus U_i \oplus \{\mathbf{0}\} \oplus ... \oplus \{\mathbf{0}\}$, and $\tilde{U_{ij}} = \tilde{U_i} \cup \tilde{U_j}$ for $i \neq j$. Then the weight of $\tilde{U_{ij}}$ is 4. Let $C(r)$ be a code of length $16r$ spanned by $\tilde{C}$ and all $\tilde{U_{ij}}$ for $i \neq j$.

Let $\tilde{W}_i$ be a 3-dimensional affine subspace of $\tilde{V}_i$, and $H(\tilde{W}_i)$ be a subcode of $C(r)$ spanned by all the 2-dimensional affine subspaces of $\tilde{W}_i$. Then the condition $\mathrm{supp} H(\tilde{W}_i) \subset C(r)^{\perp}$ holds if and only if $\tilde{W}_i$ contains $\tilde{U}_i + a$ for any $a \in \tilde{W}_i$. The number of $\tilde{W}_i$ satisfying this condition is $14(= \frac{(16-2)(16-4)}{(8-2)(8-4)} \times 2)$ for each i. It is easy to see that $|D_{C(r)}| = 240r$ and $\Gamma(K_{C(r)}) \cong \{O_2^{(2)} \cdot \Gamma(O^+(8,2))\}^r$. We note that this VOA does not satisfy the assumption of Lemma 3.10(2).

References

[Fi] B. Fischer, Finite groups generated by 3-transpositions, University of Warwick, Lecture notes, 1969.

[FLM] I. B. Frenkel, J. Lepowsky and A. Meurman, "Vertex Operator Algebras and the Monster", Pure and Applied Math., Vol. 134, Academic Press, 1988.

[G] R. L. Griess, A vertex operator algebra related to E_8 with automorphism group $O^+(10,2)$, *The Monster and Lie algebras (Columbus, OH, 1996)*, 43–58, Ohio State Univ. Math. Res. Inst. Publ., **7**, de Gruyter Berlin, 1998.

[Li] H. Li, Symmetric invariant bilinear forms on vertex operator algebras, *J. Pure and Applied Algebra*, **96** (1994), 279–297.

[M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra*, **179** (1996), 523–548.

[M2] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra*, **181** (1996), 207–222.

[M3] M. Miyamoto, Representation theory of code vertex operator algebra, *J. Algebra*, **201** (1998), 115–150.

[M4] M. Miyamoto, The moonshine VOA and a tensor product of Ising models, *The Monster and Lie algebras (Columbus, OH, 1996)*, 99–110, Ohio State Univ. Math. Res. Inst. Publ., **7**, de Gruyter Berlin, 1998.

[M5] M. Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, preprint.

Masaaki Kitazume
Department of Mathematics and Informatics
Faculty of Science, Chiba University
Chiba 263-8522, Japan

Masahiko Miyamoto
Institute of Mathematics
University of Tsukuba
Tsukuba 305-8571, Japan