ON THE UNIQUENESS OF THE MOONSHINE VERTEX OPERATOR ALGEBRA

CHONGYING DONG, ROBERT L. GRIESS JR., AND CHING HUNG LAM

Abstract. It is proved that the vertex operator algebra $V$ is isomorphic to the moonshine VOA $V^\natural$ of Frenkel-Lepowsky-Meurman if it satisfies conditions (a,b,c,d) or ($a',b,c,d$).

These conditions are:
- (a) $V$ is the only irreducible module for itself and $V$ is $C_2$-cofinite;
- (a') $\dim V_n \leq \dim V^\natural_n$ for $n \geq 3$;
- (b) the central charge is 24;
- (c) $V_1 = 0$;
- (d) $V_2$ (under the first product on $V$) is isomorphic to the Griess algebra.

Our two main theorems therefore establish a weak version of the FLM uniqueness conjecture for the moonshine vertex operator algebra. We believe that these are the first such results.

1. Introduction

The moonshine vertex operator algebra $V^\natural$ constructed by Frenkel-Lepowsky-Meurman [FLM1],[FLM2] not only proves a conjecture by McKay-Thompson but also plays a fundamental role in shaping the theory of vertex operator algebra. In the introduction of [FLM2], Frenkel-Lepowsky-Meurman conjectured that the $V^\natural$ can be characterized by the following three conditions:
- (a) the VOA $V^\natural$ is the only irreducible ordinary module for itself;
- (b) the central charge of $V^\natural$ is 24;
- (c) $V_1^\natural = 0$.

We call their conjecture the Frenkel-Lepowsky-Meurman conjecture. These conditions are natural analogues of conditions which characterize the binary Golay code and the Leech lattice.

Conditions (b) and (c) are clear from the construction. Condition (a) is proved in [D] by using the 48 commuting Virasoro elements of central charge $\frac{1}{2}$ discovered in [DMZ]. Furthermore, $V^\natural$ is rational [DM2],[DGH]. Although the theory of vertex operator algebra has developed a lot since [FLM2], including some uniqueness results for certain VOAs [LX], [DM2], [DM3], there has been no real progress in proving their conjecture.

In this paper we prove two weak versions of the Frenkel-Lepowsky-Meurman conjecture:

C.D. is supported by NSF grants, China NSF grant 10328102 and faculty research funds granted by the University of California at Santa Cruz.

R.L.G. is supported by NSA grant USDOD-MDA904-03-1-0098.

C.L. is supported by NSC grant 93-2115-M-006-012 of Taiwan and National Center for Theoretical Sciences, Taiwan.
Theorem 1. Let $V$ be a $C_2$-cofinite vertex operator algebra satisfying (a)-(c). We also assume that $V_2$ is isomorphic to the Griess algebra. Then $V$ is isomorphic to $V^2$.

In the second main theorem, we replace condition (a) by the assumption that $\dim V_n \leq \dim V_n^2$ for $n \geq 3$.

Theorem 2. Let $V$ be a simple vertex operator algebra satisfying (b)-(c). We also assume that $V_2$ is isomorphic to the Griess algebra and $\dim V_n \leq \dim V_n^2$ for $n \geq 3$. Then $V$ is isomorphic to $V^2$.

We now discuss the theorems and background. The weight two subspace $V_2^2$ of $V^2$ with the product which takes the pair $u,v$ to $u_1v$, where $u_1$ is the component operator of the vertex operator $Y(u,v) = \sum_{n \in \mathbb{Z}} u_n v_{-n}^{-1}$ [FLM2], is the Griess algebra [G], which is a commutative nonassociative algebra of dimension 196884. Moreover, $V^2$ is generated by $V_2^2$ and $V^2$ is an irreducible module for the affinization of the Griess algebra [FLM2]. So, in order to understand the moonshine vertex operator algebra, one must know the Griess algebra and its affinization very well. It seems that a complete proof of FLM’s uniqueness conjecture needs a better understanding of the Griess algebra. Unfortunately, there does not yet exist a characterization of the Griess algebra (independent of its connection to the monster simple group). Also, the affinization of the Griess algebra is not a Lie algebra and lacks a highest weight module theory. From this point of view, $V^2$ is a very difficult vertex operator algebra.

The study of the moonshine vertex operator algebras in terms of minimal series of the Virasoro algebras was initiated in [DMZ]. This is equivalent to the study the maximal associative subalgebra of the Griess algebra. In [DMZ], we find 48 mutually commutative Virasoro algebras with central charge $\frac{1}{2}$. As a result, a tensor product $T_{48}$ of 48 vertex operator algebras, associated to the highest weight unitary representations of the Virasoro algebra with central charge $\frac{1}{2}$ is a subalgebra of $V^2$ and $V^2$ decomposes into a direct sum of finitely many irreducible modules for $T_{48}$ as $T_{48}$ is rational and the homogeneous summands for $V$ are finite dimensional. A lot of progress on the study of the moonshine vertex operator algebra has been made by using the subalgebra $T_{48}$ and vertex operator subalgebras associated to the other minimal unitary series for the Virasoro algebras [DLMN], [DGH], [KLY], [M3]. The discovery of the $T_{48}$ inside $V^2$ also inspired the study of code vertex operator algebras and framed vertex operator algebras [M2], [DGH].

A frame in $V^2$ is a set of 48 mutually orthogonal Virasoro elements with central charge $\frac{1}{2}$. The subalgebra $T_{48}$ depends on a frame as studied in [DGH]. It is proved in [DGH] that for any choice of 48 commuting Virasoro algebras there are two codes $C$ and $D$ associated to the decomposition of $V^2$ into irreducible $T_{48}$-modules. Each irreducible $T_{48}$-module is a tensor product of 48 unitary highest weight modules $L(h)$ for the Virasoro algebra with central charge $\frac{1}{2}$ where $h$ can take only three values $0, \frac{1}{16}, \frac{1}{2}$. The code $C$ tells us the irreducible $T_{48}$-modules occurring in $V^2$ which are a tensor product of $L(\frac{1}{2}, h)$ for $h = 0$ or $\frac{1}{2}$. Similarly, the code $D$ indicates the appearance of irreducible $T_{48}$-modules whose tensor factors have at least one $L(\frac{1}{2}, h)$. The fusion rules for the vertex operator algebra $L(\frac{1}{2}, 0)$ indicate that we should consider a frame so that $C$ has maximal possible dimension and $D$ minimal possible dimension. These respective dimensions are 41 and 7. The reason for using our particular frame is that, for the code VOA which arises, all irreducible modules
are simple currents (see Theorem 6.10 in this paper). The uniqueness of $V^2$ then follows from known uniqueness results for certain smaller VOAs, those which are simple current extensions of code VOAs.

The main strategy in proving the theorem is to use this particular frame. Since we assume that the weight 2 subspace of the abstract vertex operator algebra in the theorem is isomorphic to the Griess algebra, we can use the theory of framed vertex operator algebra developed in [DGH] and [M2] to investigate the structure of such vertex operator algebras.

Although we assume that $V_2 \cong V_2^\circ$ (as algebras), we can not claim automatically that any VF in $V_2^\circ$ corresponds to a VF in $V$. The difficult point is to prove that a Virasoro vector in $V_2^\circ$ generates a subVOA which is simple, i.e. an irreducible highest weight module. This is where we make use of the other assumptions in our main theorems. The proof involves both character theory for the Virasoro algebra with central charge $\frac{1}{2}$ and an explicit expression for the $J$-function.

It seems that there is still a long way to go to settle the FLM conjecture. The main difficulty is that we do not have much theory of finite dimensional commutative nonassociative algebras which could be applicable to a 196884-dimensional degree 2 summand of a VOA satisfying our conditions (a,b,c) (see [G1]). In a sense, this paper reduces the uniqueness of the moonshine vertex operator algebra to the uniqueness of the Griess algebra.

2. Notations

Most of our notations are fairly standard in the VOA literature. For the reader, we note a few below.

- codes $C = C(F), D = D(F)$: see Section 4;
- codes $C, D$: see Section 6;
- $j(q), J(q)$: the elliptic modular function and the elliptic modular function with constant term set equal to 0, i.e., $J(q) = j(q) - 744$;
- $\langle \omega_i \rangle$: the subVOA generated by $\omega_i$;
- VF: Virasoro frame, see Section 4;
- $Vir(\omega_i)$: the Virasoro algebra spanned by the modes of the Virasoro element $\omega_i$ and the scalars;
- $V^I$: see Section 4;
- $V^0$ or $V^\emptyset$: the case of $V^I$ for $I = 0$ or $\emptyset$;
- $V^\circ$: the moonshine VOA, constructed in [FLM2];
- $(V^\circ)^\emptyset$: this is $V^0$ for $V = V^\circ$.

3. Various modules for vertex operator algebras

Let $(V, Y, 1, \omega)$ be a vertex operator algebra. We recall various notion of modules (cf. [FLM2], [DLM1]).

A weak $V$ module is a vector space $M$ with a linear map $Y_M : V \to \text{End}(M)[[z, z^{-1}]]$ where $v \mapsto Y_M(v, z) = \sum_{n \in \mathbb{Z}} v_n z^{-n-1}, v_n \in \text{End}(M)$. In addition $Y_M$ satisfies the following:
1) \( v_n w = 0 \) for \( n \gg 0 \) where \( v \in V \) and \( w \in M \);
2) \( Y_M(1, z) = Id_M \);
3) The Jacobi Identity

\[
\begin{align*}
    z_0^{-1} \delta \left( \frac{z_1 - z_2}{z_0} \right) & \cdot Y_M(u, z_1)Y_M(v, z_2) - z_0^{-1} \delta \left( \frac{z_2 - z_1}{-z_0} \right) \cdot Y_M(v, z_2)Y_M(u, z_1) \\
    &= z_2^{-1} \delta \left( \frac{z_1 - z_0}{z_2} \right) \cdot Y_M(Y(u, z_0)v, z_2)
\end{align*}
\]

holds.

An **admissible** \( V \) module is a weak \( V \) module which carries a \( \mathbb{Z}_+ \)-grading, \( M = \bigoplus_{n \in \mathbb{Z}_+} M(n) \), such that \( v_n M(n) \subseteq M(n + \text{wt} v - m - 1) \).

An **ordinary** \( V \) module is a weak \( V \) module which carries a \( \mathbb{C} \)-grading, \( M = \bigoplus_{\lambda \in \mathbb{C}} M_{\lambda} \), such that:
1) \( \text{dim}(M_\lambda) < \infty \) for all \( \lambda \in \mathbb{C} \);
2) \( M_{\lambda + n} = 0 \) for fixed \( \lambda \) and \( n << 0 \) (depending on \( \lambda \));
3) \( L(0)w = \lambda w = \text{wt}(w)w \), for \( w \in M_{\lambda} \).

It is easy to prove that an ordinary module is admissible.

A vertex operator algebra is called **rational** if every admissible module is a direct sum of simple admissible modules. That is, a VOA is rational if there is complete reducibility of the category of admissible modules. It is proved in [DLM2] that if \( V \) is rational there are only finitely many irreducible admissible modules up to isomorphism and each irreducible admissible module is ordinary.

A vertex operator algebra \( V \) is called **holomorphic** if it is rational and the only irreducible ordinary module is itself. In this case \( V \) is also the only irreducible admissible module.

A vertex operator algebra is called **regular** if every weak module is a direct sum of simple ordinary modules. So, regularity implies rationality.

A vertex operator algebra \( V \) is called **\( C_2 \)-cofinite** if \( V/C_2(V) \) is finite dimensional where \( C_2(V) = \langle u_{-2}v | u, v \in V \rangle \).

### 4. Framed vertex operator algebras

In this section we review the framed vertex operator algebras and related results from [DMZ] and [DGH].

Let \( L(c, h) \) be the irreducible highest weight module for the Virasoro algebra with central charge \( c \) and highest weight \( h \). The \( L(\frac{1}{2}, 0) \)-module \( L(\frac{1}{2}, h) \) is unitary if and only if \( h = 0, \frac{1}{2}, \frac{1}{16} \) [FQS], [GKO]. Moreover, \( L(\frac{1}{2}, 0) \) is a rational vertex operator algebra and \( L(\frac{1}{2}, h) \) for \( h = 0, \frac{1}{2}, \frac{1}{16} \) gives a complete list of inequivalent irreducible \( L(\frac{1}{2}, h) \)-modules.

We first recall the notion of framed vertex operator algebra. Let \( r \) be a nonnegative integer. A **framed vertex operator algebra** (FVOA) is a simple vertex operator algebra \( (V, Y, 1, \omega) \) satisfying the following conditions: there exist \( \omega_i \in V \) for \( i = 1, \ldots, r \) such that (a) each \( \omega_i \) generates a copy of the simple Virasoro vertex operator algebra \( L(\frac{1}{2}, 0) \) of central charge \( \frac{1}{2} \) and the component operators \( L^i(n) \) of \( Y(\omega_i, z) = \sum_{n \in \mathbb{Z}} L^i(n)z^{-n-2} \) satisfy \([L^i(m), L^i(n)] = (m - n)L^i(m + n) + \frac{m^3 - m}{24}\delta_{m, -n}\); (b) The \( r \) Virasoro algebras
Vir(ω₁), spanned by the modes of \(\{\omega_{i} \mid 1 \leq i \leq r\}\) and the identity, are mutually commutative; and (c) \(\omega = \omega_1 + \cdots + \omega_r\). The set \(\{\omega_1, \ldots, \omega_r\}\) is called a **Virasoro frame** (VF).

From now on we assume that \(V\) is a FVOA of central charge \(\frac{c}{2}\) with frame \(F := \{\omega_1, \ldots, \omega_r\}\). Let \(T_r\) be the vertex operator algebra generated by \(\omega_i\) for \(i = 1, \ldots, r\). Then \(T_r\) is isomorphic to \(L(\frac{1}{2}, 0) \otimes r\) and its irreducible modules are the \(L(h_1, \ldots, h_r) := L(\frac{1}{2}, h_1) \otimes \cdots \otimes L(\frac{1}{2}, h_r)\) for \(h_i = 0, \frac{1}{2}, \frac{1}{16}\). Since \(T_r\) is a rational vertex operator algebra, \(V\) is a completely reducible \(T_r\)-module. That is,

\[
V \cong \bigoplus_{h_i \in \{0, \frac{1}{2}, \frac{1}{16}\}} m_{h_1, \ldots, h_r} L(h_1, \ldots, h_r)
\]  
(4.1)

where the nonnegative integer \(m_{h_1, \ldots, h_r}\) is the multiplicity of \(L(h_1, \ldots, h_r)\) in \(V\). In particular, all the multiplicities are finite and \(m_{h_1, \ldots, h_r}\) is at most 1 if all \(h_i\) are different from \(\frac{1}{16}\).

There are two binary codes \(C = C(F)\) and \(D = D(F)\) associated to the decomposition (4.1). In order to define the code \(D\) we identify a subset \(I\) of \(\{1, \ldots, r\}\) with a codeword \(d = (d_1, \ldots, d_r) \in \mathbb{F}_2^r\) where \(d_i = 1\) if \(i \in I\) and \(d_0 = 0\) otherwise. Let \(I\) be a subset of \(\{1, \ldots, r\}\). Define \(V^I\) as the sum of all irreducible submodules isomorphic to one of the irreducibles \(L(h_1, \ldots, h_r)\) such that \(h_i = \frac{1}{16}\) if and only if \(i \in I\). Then

\[
V = \bigoplus_{I \subseteq \{1, \ldots, r\}} V^I.
\]

Set

\[
D = D(F) := \{I \in \mathbb{F}_2^r \mid V^I \neq 0\}
\]  
(4.2)

For \(c = (c_1, \ldots, c_r) \in \mathbb{F}_2^r\), we define \(V(c) = m_{h_1, \ldots, h_r} L(h_1, \ldots, h_r)\) where \(h_i = \frac{1}{2}\) if \(c_i = 1\) and \(h_i = 0\) otherwise. Set

\[
C = C(F) := \{c \in \mathbb{F}_2^r \mid V(c) \neq 0\}
\]  
(4.3)

Then \(V^0 = V^0 = \bigoplus_{c \in C} V(c)\).

Here we summarize the main result about FVOAs from [DGH]

**Theorem 4.1.** Let \(V\) be a FVOA. Then

(a) \(V = \bigoplus_{n \geq 0} V_n\) with \(V_0 = \mathbb{C}1\).

(b) \(V\) is rational.

(c) \(C\) and \(D\) are binary codes and

\[
C \subset D^\perp = \{x = (x_1, \ldots, x_r) \in \mathbb{F}_2^r \mid x \cdot d = 0 \forall d \in D\}.
\]

Moreover, \(V\) is holomorphic if and only if \(C = D^\perp\).

(d) \(V^0\) is a simple vertex operator algebra and the \(V^I\) are irreducible \(V^0\)-modules. Moreover \(V^I\) and \(V^J\) are inequivalent if \(I \neq J\).

(e) For any \(I, J \in D\) and \(0 \neq v \in V_J\) we have \(V^{I+J} = \text{span}\{u_n v \mid u \in V^I, n \in \mathbb{Z}\}\).

(f) Let \(I \subseteq \{1, \ldots, r\}\) be given and suppose that \((h_1, \ldots, h_r)\) and \((h'_1, \ldots, h'_r)\) are \(r\)-tuples with \(h_i, h'_i \in \{0, \frac{1}{2}, \frac{1}{16}\}\) such that \(h_i = \frac{1}{16}\) (resp. \(h'_i = \frac{1}{16}\)) if and only if \(i \in I\). If both \(m_{h_1, \ldots, h_r}\) and \(m_{h'_1, \ldots, h'_r}\) are nonzero then \(m_{h_1, \ldots, h_r} = m_{h'_1, \ldots, h'_r}\). That is, all irreducible modules inside \(V^I\) for \(T_r\) have the same multiplicities.

(g) For any \(c, d \in C\) and \(0 \neq v \in V(d)\) we have \(V(c + d) = \text{span}\{u_n v \mid u \in V(c), n \in \mathbb{Z}\}\).
5. Code VOA $M_C$

In this section we review and extend results on code VOAs and their modules, following [M1]-[M3] and [La].

We shall sometimes consider an integer modulo 2 as its Euclidean lift, i.e., its representative 0 or 1 in $\mathbb{Z}$, so that when $\alpha \in \mathbb{Z}_2$, $\frac{1}{2}\alpha$ makes sense as the rational number 0 or $\frac{1}{2}$.

Let $C$ be an even binary code. For any $\alpha = (\alpha_1, \ldots, \alpha_n) \in C$, denote $M_\alpha = L(\frac{1}{2}, \frac{\alpha_1}{2}) \otimes \cdots \otimes L(\frac{1}{2}, \frac{\alpha_n}{2})$ and $M_C = \bigoplus_{\alpha \in C} M_\alpha$.

Note that $M_C$ is a simple current extension of $T_n = L(\frac{1}{2}, 0)^{\otimes n}$ and it has a unique VOA structure over $\mathbb{C}$ (cf. [DM2], [M2]). This will be used to deduce the uniqueness of $V^2$.

Remark 5.1. We use $M_C$ for a code VOA instead of $M_D$ given in [M2] in this paper. This is consistent with our code $C$ defined in Section 3. In fact, $M_C$ is a framed VOA with frame $F$ satisfying $C(F) = C$ and $D(F) = 0$.

Remark 5.2. For any $\beta \in \mathbb{Z}_2^n$, one can define an automorphism $\sigma_\beta : M_C \to M_C$ by $\sigma_\beta(u) = (-1)^{\langle \alpha, \beta \rangle} u$ for $u \in M_\alpha$.

This automorphism is called a coordinate automorphism. Note that $\sigma_\beta = \sigma_{\beta'}$ if and only if $\beta + \beta' \in C^\perp$ and the subgroup $P$ generated by $\{\sigma_\beta : \beta \in \mathbb{Z}_2^n\}$ is isomorphic to $\mathbb{Z}_2^n/C^\perp$. Moreover, the fixed subalgebra $M_C^P$ is $T_n$ (cf. [M1]).

We first study the representations of the code VOA $M_C$. Let $W$ be an irreducible $M_C$-module. Then $W$ can be written as a direct sum of irreducible $T := T_n$-modules, $W \cong \bigoplus_{h_i \in \{0, \frac{1}{2}, \frac{1}{16}\}} m_{h_1, \ldots, h_n} L(h_1, \ldots, h_n)$.

Definition 5.3. Define $\tau(L(h_1, \ldots, h_n)) = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ such that $a_i = \begin{cases} 0 & \text{if } h_i = 0 \text{ or } \frac{1}{2} \\ 1 & \text{if } h_i = \frac{1}{16} \end{cases}$.

This binary word is called the $\tau$-word of $L(h_1, \ldots, h_n)$.

By the fusion rules for $L\left(\frac{1}{2}, 0\right)$, the $\tau$-words for all irreducible $T$-submodules of $W$ are the same. Thus, we can also define the $\tau$-word of $W$ by $\tau(W) = \tau(L(h_1, \ldots, h_n))$, where $L(h_1, \ldots, h_n)$ is any irreducible $T$-submodule of $W$.

The following proposition is an easy consequence of the fusion rules (cf. [DGH] and [M2]).

Proposition 5.4. Let $C$ be an even code and let $W$ be an irreducible module of $M_C$. Then $\tau(W)$ is orthogonal to $C$. 
Now we shall give more details about the structure of the irreducible module $W$. The details can be found in [M2]. Let $\beta \in C^\perp := \{ \alpha \in \mathbb{Z}_2^n \mid \langle \alpha, \gamma \rangle = 0 \text{ for all } \gamma \in C \}$ and $C_\beta := \{ \alpha \in C \mid \text{supp } \alpha \subseteq \text{supp } \beta \}$.

Let the group $\hat{C} = \{ \pm e^k \mid k \in C \}$ be a central extension of $C$ by $\{ \pm 1 \}$ such that

$$e^h e^k = (-1)^{(h,k)} e^k e^h$$

for any $h, k \in C$ and denote $\hat{C}_\beta := \{ \pm e^k \mid k \in C_\beta \} \subset \hat{C}$. Let $H$ be a maximal self-orthogonal subcode of $C_\beta$. Then $\hat{H} = \{ \pm e^\alpha \mid \alpha \in H \}$ is a maximal abelian subgroup of $\hat{C}_\beta$ (it is automatically normal since it contains the commutator subgroup of $\hat{C}_\beta$). Take a linear character $\chi : \hat{H} \rightarrow \{ \pm 1 \}$ with $\chi(-e^0) = -1$ and define a 1-dimensional $\hat{H}$-module $F_\chi$ by the action

$$e^\alpha p = \chi(e^\alpha) p \quad \text{for } p \in F_\chi, \alpha \in H.$$

We use “$h_1 \times h_2$” to abbreviate a few of the well-known fusion rules involving $L(\frac{1}{2}, h_1)$ and $L(\frac{1}{2}, h_2)$, i.e., $0 \times h = h \times 0 = h$ for $h \in \{ 0, \frac{1}{2}, \frac{1}{16} \}$, $\frac{1}{2} \times \frac{1}{2} = 0$ and $\frac{1}{2} \times \frac{1}{16} = \frac{1}{16} \times \frac{1}{2} = \frac{1}{16}$.

For any $h^i \in \{ 0, \frac{1}{2}, \frac{1}{16} \}, i = 1, \ldots, n$, with $\tau (\otimes_{i=1}^n L(\frac{1}{2}, h^i)) = \beta$, we define

$$U = \left( \otimes_{i=1}^n L(\frac{1}{2}, h^i) \right) \otimes F_\chi.$$

Then $U$ becomes an $M_H$-module with the vertex operator defined by

$$Y \left( (\otimes_{i=1}^n u^i) \otimes e^\alpha, z \right) = \left( \otimes_{i=1}^n I_{\frac{3}{2}, h^i}(u^i, z) \right) \otimes \chi(e^\alpha),$$

where $u^i \in L(\frac{1}{2}, a_i), (a_1, \ldots, a_n) \in H$, and $I_{\frac{3}{2}, h^i}$ is a nonzero intertwining operator of type

$$\left( L(\frac{1}{2}, a_i) L(\frac{1}{2}, h^i) \right).$$

We shall denote this $M_H$-module by $U((h^i), \chi)$ or $U(h^i) \otimes F_\chi$.

Let $\{ \beta_j = (b_j^i) \}_{j=1}^s$ be a transversal of $H$ in $C$ and

$$X = \bigoplus_{\beta_j \in C/H} \left\{ U \left( h^i \times \frac{b_j^i}{2} \right) \otimes (e^{\beta_j} \otimes_H F_\chi) \right\},$$

Note that $X$ does not depend on the choice of the transversal of $H$ in $C$ and $X$ is an $M_H$-module.

The following results can be found in Miyamoto [M2].

**Theorem 5.5.** $X$ is an $M_C$-module with

$$Y \left( u^\gamma \otimes e^\gamma, z \right) = \left( \otimes_{i=1}^n I_{\gamma}(u^i, z) \right) \otimes e^\gamma$$

for any $\gamma \in C$ and $u^\gamma = \otimes_{i=1}^n u^i \in M_\gamma$. We shall denote $X$ by $\text{Ind}_H^C U((h^i), \chi)$. 

Theorem 5.6. For any irreducible $M_C$-module $W$, there is a pair $((h^i), \chi)$ such that

$$W \cong \text{Ind}_{H}^{C}(U((h^i), \chi)),$$

where $\tau(W) = \tau(L(h^1, \cdots, h^n)) = \beta$, $H$ is a maximal self-orthogonal subcode of $C_{\beta} = \{ \alpha \in C | \text{supp} \alpha \subseteq \text{supp} \beta \}$ and $\chi$ is a linear character of $H$. Moreover, the structure of the $M_C$-module $W$ is uniquely determined by an irreducible $M_H$-submodule of $W$.

Next we shall give a description of all irreducible $M_C$-modules by using some binary words. Let $C$ be an even code of length $n$. For a given $\beta \in C^{\perp}$ and $\gamma \in Z_2^n$, we define

$$h_{\beta, \gamma} = (h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \in \left\{ 0, \frac{1}{2}, \frac{1}{16} \right\}^n$$

such that

$$h_{\beta, \gamma}^i = \begin{cases} \frac{1}{16} & \text{if } \beta_i = 1, \\ \frac{1}{2} & \text{if } \beta_i = 0. \end{cases}$$

Denote $U(h_{\beta, \gamma}) = U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) = L(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n)$. Fix a maximal self-orthogonal subcode $H_{\beta}$ of the code $C_{\beta} = \{ \alpha \in C | \text{supp} \alpha \subseteq \text{supp} \beta \}$ and define a character $\chi_{\gamma} : \hat{H}_\beta \rightarrow C$ of the abelian group $\hat{H}_\beta$ by

$$\chi_{\gamma}(-e^0) = -1 \quad \text{and} \quad \chi_{\gamma}(e^\alpha) = (-1)^{<\alpha, \gamma>} \quad \text{for } \alpha \in H_{\beta}.$$

Then $(\beta, \gamma)$ determines an irreducible $M_C$-module

$$M_C(\beta, \gamma) = \text{Ind}_{H_{\beta}}^{C} U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\chi_{\gamma}}.$$

When there is no confusion, we shall simply denote $M_C(\beta, \gamma)$ by $M(\beta, \gamma)$.

Lemma 5.7. The definition of $M(\beta, \gamma)$ is independent of the choice of the self-orthogonal subcode $H_{\beta}$ of $C_{\beta}$.

Proof: Let $H$ be another maximal self-orthogonal subcode of $C_{\beta}$ and let $\psi_{\gamma} : \hat{H} \rightarrow C$ be a character of $\hat{H}$ such that $\psi_{\gamma}(e^\xi) = (-1)^{<\xi, \gamma>}$ and $\psi_{\gamma}(-e^0) = -1$. Then we can construct another $M_C$-module

$$\text{Ind}_{H}^{C} U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\psi_{\gamma}}.$$

By Miyamoto’s Theorem (Theorem 5.6), the structure of this module is uniquely determined by the structure of the $M_H$ submodule $U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\psi_{\gamma}}$. Thus,

$$\text{Ind}_{H}^{C} U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\psi_{\gamma}} \cong \text{Ind}_{H_{\beta}}^{C} U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\chi_{\gamma}},$$

if and only if $\text{Ind}_{H_{\beta}}^{C} U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\chi_{\gamma}}$ contains an $M_H$-submodule isomorphic to $U(h_{\beta, \gamma}^1, \ldots, h_{\beta, \gamma}^n) \otimes F_{\psi_{\gamma}}$. It is equivalent to the fact that $\langle \text{Res}_{H} \text{Ind}_{H_{\beta}}^{C} \chi_{\gamma}, \psi_{\gamma} \rangle \neq 0$, where $\langle \text{Res}_{H} \text{Ind}_{H_{\beta}}^{C} \chi_{\gamma}, \psi_{\gamma} \rangle$ denotes the multiplicity of the character $\psi_{\gamma}$ in $\text{Res}_{H} \text{Ind}_{H_{\beta}}^{C} \chi_{\gamma}$.

On the other hand,

$$\text{Res}_{H} \text{Ind}_{H_{\beta} \oplus H}^{H} F_{\chi_{\gamma}} \cong \bigoplus_{\alpha \in (H \oplus H_{\beta})/H_{\beta}} e^\alpha \otimes F_{\chi_{\gamma}} \cong \bigoplus_{\alpha \in H/ H \cap H_{\beta}} e^\alpha \otimes F_{\chi_{\gamma}}.$$
Let 

\[ w_\psi = \frac{1}{|H \cap H_\beta|} \sum_{\alpha \in H} \psi_\alpha(\alpha)e_\alpha \otimes v, \]

where \( v \in F_\chi \). Then \( w_\psi \in \text{Ind}_{H_\beta}^{H_\beta + H_\beta} F_\chi \), and for any \( x \in H \),

\[ e^x \cdot w_\psi = \frac{1}{|H \cap H_\beta|} \sum_{\alpha \in H} (-1)^{\langle x, \alpha \rangle} e^x e_\alpha \otimes v \]

\[ = (-1)^{\langle x, \beta \rangle} \frac{1}{|H \cap H_\beta|} \sum_{\alpha \in H} (-1)^{\langle x, \alpha \rangle} e^{x+\alpha} \otimes v \]

\[ = (-1)^{\langle x, \beta \rangle} w_\psi = \psi_\gamma(e^x)w_\psi. \]

Hence \( Cw_\psi \) affords the \( \hat{H} \)-character \( \psi_\gamma \) inside \( \text{Ind}_{H_\beta}^{H_\beta + H_\beta} F_\chi \subset \text{Ind}_{H_\beta}^{C_\beta} F_\chi \), and

\[ \langle \text{Res}_H \text{Ind}_{H_\beta}^{C_\beta} \chi, \psi_\gamma \rangle \neq 0 \]

as desired. \( \square \)

**Lemma 5.8.** Let \( \beta_1, \beta_2 \in C^\perp \) and \( \gamma_1, \gamma_2 \in \mathbb{Z}_2^n \). Let \( H_\beta \) be a maximal self-orthogonal subcode of \( C_\beta \) and let

\( (H_\beta)^{\perp_\beta} := \{ \alpha \in \mathbb{Z}_2^n | \supp \alpha \subset \supp \beta \) and \( \langle \alpha, \xi \rangle = 0 \) for all \( \xi \in H_\beta \}. \)

Then the irreducible \( M_\alpha \)-modules \( M(\beta_1, \gamma_1) \) and \( M(\beta_2, \gamma_2) \) are isomorphic if and only if \( \beta_1 = \beta_2 \) and \( \gamma_1 + \gamma_2 \in C + (H_\beta)^{\perp_\beta} \).

**Proof:** By the definition of \( M(\beta, \gamma) \), it is easy to see that \( M(\beta_1, \gamma_1) \cong M(\beta_2, \gamma_2) \) if \( \beta_1 = \beta_2 \) and \( \gamma_1 + \gamma_2 \in C \). Moreover, if \( \beta_1 = \beta_2 = \beta \) and \( \gamma_1 + \gamma_2 \in (H_\beta)^{\perp_\beta} \), then \( h_{\beta_1, \gamma_1} = h_{\beta_2, \gamma_2} \) and \( \chi_{\gamma_1} = \chi_{\gamma_2} \) for any choice of \( H_\beta \). Thus, \( M(\beta_1, \gamma_1) \cong M(\beta_2, \gamma_2) \) if \( \beta_1 = \beta_2 \) and \( \gamma_1 + \gamma_2 \in C + (H_\beta)^{\perp_\beta} \).

Now suppose that \( M(\beta_1, \gamma_1) \cong M(\beta_2, \gamma_2) \). Then they have the same \( \tau \)-word and \( \beta_1 = \beta_2 \). Let \( \beta := \beta_1 = \beta_2 \). Let \( H_\beta \) be a maximal self-orthogonal subcode of \( C_\beta \). Since \( M(\beta_1, \gamma_1) \cong M(\beta_2, \gamma_2) \), \( M(\beta_1, \gamma_1) \) contains the \( M_{H_\beta} \)-module \( U(h_{\beta, \gamma_2}) \otimes \chi_{\gamma_2} \). Thus, there exists an element \( \delta \in C \) such that

\[ h_{\beta, \gamma_1} \times \frac{\delta}{2} = h_{\beta, \gamma_2} \]

and \( e^\delta \otimes F_{\chi_{\gamma_1}} \cong F_{\chi_{\gamma_2}} \).

Since \( h_{\beta, \gamma_1} \times \frac{\delta}{2} = h_{\beta, \gamma_2} \), \( \delta + \gamma_1 + \gamma_2 \in \mathbb{Z}_2^\beta \), where \( \mathbb{Z}_2^\beta = \{ \alpha \in \mathbb{Z}_2^n | \supp \alpha \subset \supp \beta \} \).

Moreover, \( e^\delta \otimes F_{\chi_{\gamma_1}} \cong F_{\chi_{\gamma_2}} \) implies that

\[ (-1)^{\langle \delta + \gamma_1, \alpha \rangle} = (-1)^{\langle \gamma_2, \alpha \rangle} \]

for all \( \alpha \in H_\beta \).

Therefore, \( \delta + \gamma_1 + \gamma_2 \in H_\beta^{\perp_\beta} \) and we have \( \delta + \gamma_1 + \gamma_2 \in H_\beta^{\perp_\beta} \cap \mathbb{Z}_2^\beta = (H_\beta)^{\perp_\beta} \) and \( \gamma_1 + \gamma_2 \in C + (H_\beta)^{\perp_\beta} \). \( \square \)

**Lemma 5.9.** The code \( C + H_\beta^{\perp_\beta} \) is independent of the choice of the self-orthogonal subcode \( H_\beta \).
Proof. Let $H$ be another maximal self-orthogonal subcode of $C_\beta$. Then we have $|H| = |H_\beta|$. First we will consider the intersection $H \cap H_\beta$ of $H$ and $H_\beta$ and its orthogonal complement in $\mathbb{Z}_2^\beta$.

**Claim:** $(H \cap H_\beta)_{\perp, \beta} = H_{\perp, \beta} \oplus H$.

It is easy to see that $H_{\perp, \beta}$ and $H$ are both contained in $(H \cap H_\beta)_{\perp, \beta}$. Hence we have $H_{\perp, \beta} \oplus H \subset (H \cap H_\beta)_{\perp, \beta}$. Now note that $H_{\perp, \beta} \cap H = H_{\perp, \beta} \cap (C_\beta \cap H) = (H_{\perp, \beta} \cap C_\beta) \cap H = H_\beta \cap H$ and $\dim H = \dim H_\beta$. By computing the dimensions, we have

$$\dim(H_{\perp, \beta} \oplus H) = \dim H_{\perp, \beta} + \dim H - \dim(H_{\perp, \beta} \cap H) = (|\beta| - \dim H_\beta) + \dim H - \dim(H_\beta \cap H) = |\beta| - \dim(H_\beta \cap H) = \dim(H \cap H_\beta)_{\perp, \beta}.$$

Hence we have $(H \cap H_\beta)_{\perp, \beta} = H_{\perp, \beta} \oplus H$.

By the claim, we have

$$(H \cap H_\beta)_{\perp, \beta} = H + H_{\perp, \beta} \subset C + H_{\perp, \beta}.$$ 

Therefore, $C + (H \cap H_\beta)_{\perp, \beta} \subset C + H_{\perp, \beta}$. On the other hand, $C + H_{\perp, \beta}$ is clearly contained in $C + (H \cap H_\beta)_{\perp, \beta}$ and thus $C + H_{\perp, \beta} = C + (H \cap H_\beta)_{\perp, \beta}$. Similarly, we also have $C + H_{\perp, \beta} = C + (H \cap H_\beta)_{\perp, \beta}$ and hence $C + H_{\perp, \beta} = C + H_{\perp, \beta}$ as desired. \hfill \square

Next we shall compute the fusion rules among some irreducible $M_C$-modules. We recall a theorem proved by Miyamoto [M2, M3]. Let $C$ be an even linear code.

**Theorem 5.10.** For any $\alpha \in \mathbb{Z}_2^n$, the $M_C$-module $M(0, \alpha) = M_{\alpha + C} = \oplus_{\delta \in \alpha + C} M_\delta$ is a simple current module. Moreover,

$$M_{\alpha + C} \times M(\beta, \gamma) = M(\beta, \alpha + \gamma)$$

for any irreducible $M_C$-module $M(\beta, \gamma)$.

Now by using the associativity and commutativity of the fusion rules, we also have the following Lemma.

**Lemma 5.11.** Let $\beta_1, \beta_2 \in C_{\perp, \beta}$ and $\gamma \in \mathbb{Z}_2^n$. Then

$$\dim I_{M_C}
\begin{pmatrix}
M(\beta_1 + \beta_2, \gamma) \\
M(\beta_1, 0)
\end{pmatrix}
= \dim I_{M_C}
\begin{pmatrix}
M(\beta_1, \alpha_1 + \alpha_2 + \gamma) \\
M(\beta_1, \alpha_1)
\end{pmatrix}
$$

for any $\alpha_1, \alpha_2 \in \mathbb{Z}_2^n$.

**Proof:** For any $\gamma \in \mathbb{Z}_2^n$, let

$$m_\gamma = \dim I_{M_C}
\begin{pmatrix}
M(\beta_1 + \beta_2, \gamma) \\
M(\beta_1, 0)
\end{pmatrix}.$$ 

Then we have

$$M(\beta_1, 0) \times M(\beta_2, 0) = \sum_{\gamma \in \mathbb{Z}_2^n/K} m_\gamma M(\beta_1 + \beta_2, \gamma),$$

where $K$ is the kernel of the fusion map.
where $K = C + (H_{\beta_1+\beta_2})^{\perp}_{\beta_1+\beta_2}$.

Since the fusion product is associative and commutative, we have

$$M(\beta_1, \alpha_1) \times M(\beta_2, \alpha_2) = [M(0, \alpha_1) \times M(\beta_1, 0)] \times [M(0, \alpha_2) \times M(\beta_2, 0)]$$

$$= [M(0, \alpha_1) \times M(0, \alpha_2)] \times [M(\beta_1, 0) \times M(\beta_2, 0)]$$

$$= M(0, \alpha_1 + \alpha_2) \times (\sum_{\gamma \in \mathbb{Z}_n^2/K} m_\gamma M(\beta_1 + \beta_2, \gamma))$$

$$= \sum_{\gamma \in \mathbb{Z}_n^2/K} m_\gamma M(\beta_1 + \beta_2, \alpha_1 + \alpha_2 + \gamma).$$

Hence, we also have

$$m_\gamma = \text{dim} I_{MC} \left( \begin{array}{cc} M(\beta_1 + \beta_2, \alpha_1 + \alpha_2 + \gamma) \\ M(\beta_1, \alpha_1) \end{array} \right) \left( \begin{array}{cc} M(\beta_1, \alpha_2) \end{array} \right)$$

as desired. □

For the later purpose we also need some facts about the Hamming code VOA $M_{H_8}$ from [M2, M3] (see also [La]).

Let $H_8$ be the Hamming code $[8, 4, 4]$ code, i.e., the code generated by the rows of

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

Let $\{e^1, \cdots, e^8\}$ be the standard frame for $M_{H_8}$. Let $q^0 = 1$ be the vacuum element of $L(1/2, 0)$ and let $q^1$ be a highest weight vector of $L(1/2, 1/2)$ such that $q^0 q^1 = 1$. For any $\alpha = (\alpha_1, \ldots, \alpha_8) \in H_8$, let

$$q^\alpha = q^{\alpha_1} \otimes \cdots \otimes q^{\alpha_8} \in M_\alpha,$$

where $q^{\alpha_k}$ is a norm 1 highest weight vector for the $k$-th tensor factor with respect to the action of our $T_8$. Then $q^\alpha$ is a highest weight vector in $M_\alpha$. Moreover, we have

$$q^\alpha_1 q^\beta = \begin{cases} 2 \sum_{k=1}^8 \alpha_i e^i & \text{if } \alpha = \beta, \\
q^{\alpha+\beta} & \text{if } |\alpha \cap \beta| = 2, \\
0 & \text{otherwise}, \end{cases}$$

for any $\alpha, \beta \in H_8$ with $|\alpha| = |\beta| = 4$.

The following results are obtained in [M2].

**Lemma 5.12.** Let $\nu_i$ be the binary word whose $i$-th entry is 1 and all other entries are 0. Define $\alpha_i := \nu_1 + \nu_i$.

In the Hamming code VOA $M_{H_8}$, there exist exactly three Virasoro frames, namely, $\{e^1, \ldots, e^8\}, \{d^1, \ldots, d^8\}$, and $\{f^1, \ldots, f^8\}$.
where
\[ d^i = S^{\alpha_i} = \frac{1}{8}(e^1 + \cdots + e^8) + \frac{1}{8} \sum_{\beta \in H_8, |\beta|=4} (-1)^{\langle \alpha_i, \beta \rangle} q^\beta \otimes e^\beta, \]
\[ f^i = S^{\nu_i} = \frac{1}{8}(e^1 + \cdots + e^8) + \frac{1}{8} \sum_{\beta \in H_8, |\beta|=4} (-1)^{\langle \nu_i, \beta \rangle} q^\beta \otimes e^\beta. \]

**Theorem 5.13.** Let \( L \) be an irreducible \( M_{H_8} \)-module with half-integral or integral weight. Then, \( L \) is isomorphic to one of the following:

1. \( M_{\nu_1+\nu_5+H_8} \) with respect to \( \{e^1, \ldots, e^8\} \) for all \( i = 1, \ldots, 8 \).
2. \( M_{\nu_1+H_8} \) with respect to \( \{e^1, \ldots, e^8\} \) for all \( i = 1, \ldots, 8 \).
3. \( M_{\nu_i+H_8} \) with respect to \( \{d^1, \ldots, d^8\} \) for all \( i = 1, \ldots, 8 \).
4. \( M_{\nu_i+H_8} \) with respect to \( \{f^1, \ldots, f^8\} \) for all \( i = 1, \ldots, 8 \).

Moreover, all modules in (3) and (4) are isomorphic to \( \otimes_{i=1}^8 L(\frac{1}{2}, \frac{1}{16}) \) as \( T_8 \)-modules.

As a corollary, we have the following theorem. The proof can be found in [La] (see also [M2, M3]).

**Theorem 5.14.** For any \( \beta_1 = (0^8) \) or \( (1^8) \) and \( \beta_2 \in H_8 \), we have
\[ M(\beta_1, \alpha_1) \times_{M_{H_8}} M(\beta_2, \alpha_2) = M(\beta_1 + \beta_2, \alpha_1 + \alpha_2). \]

Consequently, all irreducible \( M_{H_8} \)-modules with half-integral or integral weight are simple current modules.

**Remark 5.15.** For any \( \alpha \in \mathbb{Z}_8^8/H_8 \), \( \alpha \) uniquely determines a character \( \chi_\alpha \in \text{Irr} \ H_8 \) such that \( \chi_\alpha(\gamma) = (-1)^{\langle \alpha, \gamma \rangle} \) for any \( \gamma \in H_8 \). By using this identification, our module \( M(\beta, \alpha) \) actually corresponds to the class \([\beta, \chi_\alpha]\) defined in Section 5 of [La].

6. The moonshine vertex operator algebra \( V^2 \)

Let \( V^2 \) be the moonshine vertex operator algebra [FLM1]-[FLM2]. The following theorem can be found in [DGH].

**Theorem 6.1.** There exists a VF in \( V^2 \), called \( F := \{\omega_1, \ldots, \omega_{48}\} \), so that the code \( \mathcal{C} := \mathcal{C}(F) \) associated to this VF has length 48 and dimension 41. The code \( \mathcal{D} := \mathcal{D}(F) = \mathcal{C}^\perp \) has generator matrix
\[
\begin{pmatrix}
1111111111111111 & 0000000000000000 & 0000000000000000 \\
0000000000000000 & 1111111111111111 & 0000000000000000 \\
0000000000000000 & 0000000000000000 & 1111111111111111 \\
0000000000000000 & 0000000000000000 & 0000000000000000 \\
0000000000000000 & 0000000000000000 & 0000000000000000 \\
0001111100001111 & 0001111100001111 & 0001111100001111 \\
0011001100110011 & 0011001100110011 & 0011001100110011 \\
0101010101010101 & 0101010101010101 & 0101010101010101 
\end{pmatrix}
\]

**Remark 6.2.** The weight enumerator of \( \mathcal{D} \) is given by
\[ X^{48} + 3X^{32} + 120X^{24} + 3X^{16} + 1 \]
and the minimal weight of \( \mathcal{C} \) is 4. Moreover, \( \mathcal{D} \) is self-orthogonal and hence \( \mathcal{D} \subset \mathcal{C} \). (The codes \( \mathcal{D} \) and \( \mathcal{C} \) are denoted by \( S^2 \) and \( D^2 \), respectively in [M3].)
Lemma 6.3. The code $C$ in Theorem 6.1 is generated by the weight 4 codewords.

Proof: First we note that the code $D = D(F)$ is generated by the elements of the form $(1^{16}, 0^{16}, 0^{16}), (0^{16}, 1^{16}, 0^{16}), (0^{16}, 0^{16}, 1^{16})$ and $(\alpha, \alpha, \alpha), \; \alpha \in \text{RM}(1, 4),$ where $\text{RM}(r, m)$ denote the $r$-th order Reed-Muller code of length $2^m$ (cf. [CS]). Since $\text{RM}(1, 4)^\perp = \text{RM}(2, 4),$ we have

$$C = D^\perp = \{(\alpha, \beta, \gamma) | \alpha + \beta + \gamma \in \text{RM}(2, 4), \; \alpha, \beta, \gamma \text{ even}\}.$$  

Hence the code $C$ can be generated by the elements

$$(\alpha, 0, 0), (0, \beta, 0), (0, 0, \gamma), \; \alpha, \beta, \gamma \text{ are generators of } \text{RM}(2, 4)$$

and

$$(\alpha, \beta, 0), (\alpha, 0, \beta), (0, \alpha, \beta), \; \alpha, \beta \text{ are even and } \alpha + \beta \text{ is a generator of } \text{RM}(2, 4).$$

Note that the Reed Muller code $\text{RM}(2, 4)$ is of dimension 11 and is generated by the elements of the form

$$(\alpha, 0), (0, \alpha), \; \alpha \in H_8,$$

and

$$(1100\,0000, 1100\,0000), (1010\,0000, 1010\,0000), (1000\,1000, 1000\,1000).$$

Since the Hamming code $H_8$ is generated by its weight 4 elements, the codes $\text{RM}(2, 4)$ and $C$ are generated by the weight 4 codewords also. □

Lemma 6.4. The vertex operator subalgebra $(V^s)^0$ is isomorphic to $M_C$ and is uniquely determined by the set of weight 4 codewords of $C$.

Proof: By the uniqueness of the code VOA, $(V^s)^0$ and $M_C$ are isomorphic. Since $C$ is generated by the weight 4 codewords of $C$, the vertex operator algebra structure of $(V^s)^0$ is uniquely determined by the generators of the group $C$. □

We now determine the irreducible modules and the fusion rules for the code VOA $M_C$.

Remark 6.5. In the next result, $\text{RM}(r, m)$ denote the $r$-th order Reed-Muller code of length $2^m$ (cf. [CS]). Note that the Reed Muller codes are nested in the sense that $\text{RM}(r + 1, m) \supset \text{RM}(r, m)$ and $\text{RM}(r + 1, m + 1) \supset \text{RM}(r, m) \oplus \text{RM}(r, m)$, where the direct sum corresponds to a partition of indices by an affine hyperplane and its complement.

The following properties of the code $C$ can be derived easily from the definition.

Proposition 6.6. Let $D$ and $C$ be defined as above. For any $\beta \in D$, denote

$$C_\beta := \{\alpha \in C | \text{supp } \alpha \subseteq \text{supp } \beta\}.$$

1. If $|\beta| = 16$, then $C_\beta \cong \text{RM}(2, 4)$.
2. If $|\beta| = 24$, then $C_\beta \cong \{ (\alpha, \gamma, \delta) | \alpha + \gamma + \delta \in H_8 \text{ and } \alpha, \gamma, \delta \text{ even} \}$.
3. If $|\beta| = 32$, then $C_\beta \cong \text{RM}(3, 5)$.
4. If $|\beta| = 48$, then $C_\beta = C$.

Note that the Hamming code $H_8 \cong \text{RM}(1, 3)$. Hence, for $\beta \neq 0$, $C_\beta$ contains a self-dual subcode which is isomorphic to a direct sum of $|\beta|/8$ copies of the Hamming code $H_8$. 

**Proof:** Let $\beta \in \mathcal{D}$ and $n = |\beta|$, the weight of $\beta$. Let $p_\beta : \mathbb{Z}_2^{48} \rightarrow \mathbb{Z}_2^n$ be the natural projection of $\mathbb{Z}_2^{48}$ to the support of $\beta$. Since $\mathcal{C} = \mathcal{D}^\perp$, it is easy to see that $\mathcal{C}_\beta \cong p_\beta(\mathcal{D})^\perp$.

**Case 1.** $|\beta| = 16$. In this case, $p_\beta(\mathcal{D})$ is generated by the codewords $(1^{16}), (0^8 1^8), (0^4 1^4)^2$, $(0^2 1^2)^4$ and $(0 1)^8$ and is isomorphic to the Reed Muller code $\text{RM}(1, 4)$. Since $\text{RM}(r, m)^\perp \cong \text{RM}(m - r - 1, m)$ for any $1 \leq r \leq m$ we have $\mathcal{C}_\beta \cong \text{RM}(2, 4)$ as desired.

**Case 2.** $|\beta| = 24$. In this case, $p_\beta(\mathcal{D})$ is of dimension 6 and is isomorphic to a code generated by

$$ (1^8 0^8 0^8), (0^8 1^8 0^8), (0^8, 0^8, 1^8) \text{ and } (\alpha, \alpha, \alpha), \alpha \in H_8. $$

Hence $\mathcal{C}_\beta \cong \{(\alpha, \gamma, \delta) | \alpha + \gamma + \delta \in H_8 \text{ and } \alpha, \gamma, \delta \text{ even}\}$.

**Case 3.** $|\beta| = 32$. $p_\beta(\mathcal{D}) \cong \text{RM}(1, 5)$ and hence $\mathcal{C}_\beta \cong \text{RM}(3, 5)$.

**Case 4.** $|\beta| = 48$. It is clear that $\mathcal{C}_\beta = \mathcal{C}$ in this case. \hfill $\Box$

Now by using Lemma 5.8, we have the following theorem.

**Theorem 6.7.** Let $\mathcal{D}$ and $\mathcal{C}$ be defined as above. Then

$$ \{M_\mathcal{C}(\beta, \gamma) \mid \beta \in \mathcal{D} \text{ and } \gamma \in \mathbb{Z}_2^{48}/\mathcal{C}\} $$

is the set of all inequivalent irreducible modules for $M_\mathcal{C}$.

**Proof:** By the previous proposition, we can choose $H_\beta$ such that it is a direct sum of $|\beta|/8$ copies of the Hamming code $H_8$. In this case, $(H_\beta)^\perp = H_\beta$ and we have $\mathcal{C} = \mathcal{C} + (H_\beta)^\perp$. Hence $\{M_\mathcal{C}(\beta, \gamma) \mid \beta \in \mathcal{D} \text{ and } \gamma \in \mathbb{Z}_2^{48}/\mathcal{C}\}$ is the set of all inequivalent irreducible modules for $M_\mathcal{C}$ by Lemma 5.8.

Next we shall compute the fusion rules among irreducible $M_\mathcal{C}$-modules. The main tool is the representation theory of the Hamming code VOA $M_{H_8}$ given in Section 4. First we recall the following theorem from [DL].

**Theorem 6.8.** Let $W^1, W^2$ and $W^3$ be $V$-modules and let $I$ be an intertwining operator of type

$$ \begin{pmatrix} W^1 & W^3 \\ W^3 & W^2 \end{pmatrix}. $$

Assume that $W^1$ and $W^2$ have no proper submodules containing $v^1$ and $v^2$, respectively. Then $I(v^1, z)v^2 = 0$ implies $I(v, z) = 0$.

**Lemma 6.9.** For any $\beta_1, \beta_2, \beta_3 \in \mathcal{D}$ and $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_2^{48}$, we have

$$ \dim I_{M_\mathcal{C}}\begin{pmatrix} M(\beta_3, \alpha_3) \\ M(\beta_1, \alpha_1) \end{pmatrix} \leq 1 $$

and

$$ \dim I_{M_\mathcal{C}}\begin{pmatrix} M(\beta_3, \alpha_3) \\ M(\beta_1, \alpha_1) \end{pmatrix} = 0 $$

unless $\beta_3 = \beta_1 + \beta_2$ and $\alpha_3 \equiv \alpha_1 + \alpha_2 \text{ mod } \mathcal{C}$. 

Proof: Recall that \( \dim \mathcal{D} = 7 \) and the weight enumerator of \( \mathcal{D} \) is \( X^{48} + 3X^{32} + 120X^{24} + 3X^{16} + 1 \).

Without loss, we may assume that \( \beta_3 = \beta_1 + \beta_2 \); otherwise,
\[
\dim I_{\mathcal{M}} \left( \begin{array}{c}
M(\beta_3, \alpha_3) \\
M(\beta_1, \alpha_1) \\
M(\beta_2, \alpha_2)
\end{array} \right) = 0.
\]

Let \( \bar{\beta}_1 = (1^{48}) + \beta_1 \). Then \( \bar{\beta}_1 \) is also in \( \mathcal{D} \). Thus, there exist self-orthogonal codes \( H_{\beta_1} \) and \( H_{\bar{\beta}_1} \) of \( \mathcal{C} \) such that both \( H_{\beta_1} \) and \( H_{\bar{\beta}_1} \) are direct sums of Hamming codes and are both contained in \( E \). Note that \( H_{\beta_1} \) and \( H_{\bar{\beta}_1} \) are irreducible \( \mathcal{M} \)-modules.

Let \( \bar{\beta}_1 \) be an irreducible \( \mathcal{M}_E \)-module.
\[
M_{\mathcal{C}}(\beta_1, \alpha_i) = \bigoplus_{\delta \in \mathcal{C}/E} M_E(\beta_i, \alpha_i + \delta).
\]

Note that \( H_{\beta_1} \subset E \) for any \( i = 1, 2, 3 \) and hence \( M_{\mathcal{C}}(\beta_i, \alpha_i) \) is a direct sum of inequivalent irreducible \( \mathcal{M}_E \)-modules. Thus by Theorem 5.14 and 6.8, we have
\[
\dim I_{\mathcal{M}} \left( \begin{array}{c}
M(\beta_1 + \beta_2, \alpha_3) \\
M(\beta_1, \alpha_1) \\
M(\beta_2, \alpha_2)
\end{array} \right) \leq \dim I_{\mathcal{M}} \left( \begin{array}{c}
M_E(\beta_1 + \beta_2, \alpha_3) \\
M_E(\beta_1, \alpha_1) \\
M_E(\beta_2, \alpha_2)
\end{array} \right) \leq 1
\]
and
\[
\dim I_{\mathcal{M}} \left( \begin{array}{c}
M(\beta_1 + \beta_2, \alpha_3) \\
M(\beta_1, \alpha_1) \\
M(\beta_2, \alpha_2)
\end{array} \right) = 0
\]
unless \( \alpha_3 = \alpha_1 + \alpha_2 \).

Finally, we shall treat the case for which all \( \beta_1, \beta_2 \) and \( \beta_1 + \beta_2 \) are of weight 24. For simplicity, we may assume that \( \beta_1 = (1^8 \, 0^8 \, 1^8 \, 0^8 \, 0^8) \) and \( \beta_2 = (1^4 \, 0^4 \, \ldots \, 1^4 \, 0^4) \). Then \( \beta_3 = \beta_1 + \beta_2 = (0^4 \, 1^8 \, 0^8 \, 1^8 \, 0^8 \, 0^8 \, 0^4) \). In this case, we have \( E = H_{\beta_1} \oplus H_{\bar{\beta}_1} \cong H_8 \oplus H_8 \).

Note that \( E + H_{\beta_1 + \beta_2} = E + H_{\beta_1} \) in this case. Moreover, we have
\[
E_{\beta_2} = \{ \alpha \in E \mid \text{supp } \alpha \subset \text{supp } \beta_2 \} = E \cap H_{\beta_2} \quad \text{and} \quad E_{\beta_3} = E_{\beta_1 + \beta_2} = E \cap H_{\beta_1 + \beta_2}.
\]

Let \( \mathcal{H} := E + H_{\beta_2} = E + H_{\beta_1 + \beta_2} \). Then the \( \mathcal{M}_E \)-module \( M_{\mathcal{C}}(\beta_i, \alpha_i), i = 2, 3, \) can be decomposed as
\[
M_{\mathcal{C}}(\beta_i, \alpha_i) = \bigoplus_{\delta \in \mathcal{C}/\mathcal{H}} M_{\mathcal{H}}(\beta_i, \alpha_i + \delta).
\]

Claim: \( M_{\mathcal{H}}(\beta_i, \alpha_i + \delta) \) is irreducible as an \( \mathcal{M}_E \)-module for any \( \delta \in \mathcal{C}/\mathcal{H} \).

Proof. Let \( W = M_{\mathcal{H}}(\beta_i, \alpha_i + \delta) \) and \( \mathcal{H}_{\beta_i} = \{ \alpha \in \mathcal{H} \mid \text{supp } \alpha \subset \text{supp } \beta_i \} \). Then \( \mathcal{H}_{\beta_i} \) is a maximal self-orthogonal subcode of \( \mathcal{H}_{\beta_i} \). Let \( U(h) \otimes F_X \) be an irreducible \( M_{\mathcal{H}_{\beta_i}} \)-submodule of \( W \). Then
\[
W = \text{Ind}_{\mathcal{H}_{\beta_i}}^{\mathcal{H}} U(h) \otimes F_X = \bigoplus_{\delta \in \mathcal{H}/\mathcal{H}_{\beta_i}} U(h \times \delta) \otimes (e^\delta \otimes F_X).
\]
Since $E_{\beta_{i}} = E \cap H_{\beta_{i}} \subset H_{\beta_{i}}$, $U(h) \otimes F_{\chi}$ is also an irreducible $M_{E_{\beta_{i}}}$-module. Hence,

$$W' = \text{Ind}_{E_{\beta_{i}}}^{E} U(h) \otimes F_{\chi} = \bigoplus_{\delta \in E/E_{\beta_{i}}} U(h) \times (\delta) \otimes (e^{\delta} \otimes F_{\chi})$$

is an irreducible $M_{E}$-submodule of $W$. Note that

$$|\mathcal{H}/H_{\beta_{i}}| = |(E + H_{\beta_{i}})/H_{\beta_{i}}| = |E/(E \cap H_{\beta_{i}})| = |E/E_{\beta_{i}}|.$$

Therefore, we have $W = W'$ and $W$ is an irreducible $M_{E}$-module.

Now, by Theorem 5.14 and 6.8, we have

$$\dim I_{M_{C}} \left( \begin{array}{c} M(\beta_{1} + \beta_{2}, \alpha_{3}) \\ M(\beta_{1}, \alpha_{1}) \\ M(\beta_{2}, \alpha_{2}) \end{array} \right)$$

$$\leq \dim I_{M_{H}} \left( \begin{array}{c} M_{H}(\beta_{1} + \beta_{2}, \alpha_{3}) \\ M_{H}(\beta_{1}, \alpha_{1}) \\ M_{H}(\beta_{2}, \alpha_{2}) \end{array} \right)$$

$$\leq \dim I_{M_{E}} \left( \begin{array}{c} M_{E}(\beta_{1} + \beta_{2}, \alpha_{3}) \\ M_{E}(\beta_{1}, \alpha_{1}) \\ M_{E}(\beta_{2}, \alpha_{2}) \end{array} \right) \leq 1$$

and

$$\dim I_{M_{C}} \left( \begin{array}{c} M(\beta_{1} + \beta_{2}, \alpha_{3}) \\ M(\beta_{1}, \alpha_{1}) \\ M(\beta_{2}, \alpha_{2}) \end{array} \right) = 0$$

unless $\alpha_{3} = \alpha_{1} + \alpha_{2}$. Note that $M_{H}(\beta_{2}, \alpha_{2}) = M_{E}(\beta_{2}, \alpha_{2})$ and $M_{H}(\beta_{1} + \beta_{2}, \alpha_{1} + \alpha_{2}) = M_{E}(\beta_{1} + \beta_{2}, \alpha_{1} + \alpha_{2})$ as $M_{E}$-modules.

\[\square\]

**Theorem 6.10.** The fusion rules among irreducible $M_{C}$ modules are given by

$$M(\beta_{1}, \alpha_{1}) \times M(\beta_{2}, \alpha_{2}) = M(\beta_{1} + \beta_{2}, \alpha_{1} + \alpha_{2}),$$

where $\beta_{1}, \beta_{2} \in \mathcal{D}$ and $\alpha_{1}, \alpha_{2} \in \mathbb{Z}_{2}^{48}/\mathcal{C}$. In particular, each irreducible $M_{C}$-module is a simple current.

**Proof:** By Lemma 5.11 and 6.9, it remains to show that

$$I_{M_{C}} \left( \begin{array}{c} M(\beta_{1} + \beta_{2}, \alpha_{1} + \alpha_{2}) \\ M(\beta_{1}, \alpha_{1}) \\ M(\beta_{2}, \alpha_{2}) \end{array} \right) \neq 0,$$

for some $\alpha_{1}, \alpha_{2} \in \mathbb{Z}_{2}^{48}$. Nevertheless, such kind of intertwining operators does exist and can be realized inside the Leech lattice VOA $V_{\Lambda}$. In fact, there exists a Virasoro frame of $V_{\Lambda}$ such that $V_{\Lambda}$ can be decomposed as

$$V_{\Lambda} \cong \bigoplus_{\beta \in \mathcal{D}} M_{C}(\beta, \gamma_{\beta}),$$

for some $\gamma_{\beta} \in \mathbb{Z}_{2}^{48}/\mathcal{C}$.

We shall refer to [DGH] or [M3] for details. \[\square\]
7. Proof of the main theorems

We first prove Theorem 1. So we assume that (1) \( V \) is a vertex operator algebra satisfying conditions (a)-(c), (2) \( V_2 \) is isomorphic to the Griess algebra, (3) \( V \) is \( C_2 \)-cofinite.

Lemma 7.1. \( V \) is truncated below 0 and \( V_0 = C1 \).

**Proof:** First we prove that \( V_n = 0 \) if \( n \) is negative. If this is not true, take the smallest \( n \) such that \( V_n \neq 0 \). Then each \( 0 \neq v \in V_n \) generates a highest weight module for the Lie algebra \( CL(1) \oplus CL(0) \oplus CL(-1) \) (which is isomorphic to \( sl(2, \mathbb{C}) \)). According to the structure of the highest weight modules for \( sl(2, \mathbb{C}) \) we know that \( L(-1)^iv \neq 0 \) for \( i = 0, \ldots, -2n \). Since \( n \) is less than or equal to \(-1 \) we see that \( L(-1)^{-n+1}v \neq 0 \). Since the weight of \( L(-1)^{-n+1}v \) is 1, we immediately have a contradiction as \( V_1 = 0 \) by assumption.

We now prove that \( V_0 \) is one dimensional. Note that \( L(-1)V_0 = 0 \). So each nonzero vector \( v \in V_0 \) is a vacuum-like vector [Li]. As a result, we have a \( V \)-module isomorphism \( f_v : V \to V \) by sending \( u \) to \( u_{-1}v \) for \( u \in V \) [Li]. By Schur’s lemma, \( f_v \) must be a multiple of the identity map. As a result, \( f_v(1) = v \) is a multiple of the vacuum. This shows that \( V_0 \) is spanned by the vacuum. \( \square \)

Lemma 7.2. \( V \) is a holomorphic vertex operator algebra.

**Proof:** It is proved in [DLM2] that if \( U \) is a vertex operator algebra such that \( U = \oplus_{n \geq 0} U_n \) with \( U_0 \) being 1-dimensional and \( U_1 = 0 \) and that \( U \) is the only irreducible ordinary module for itself then any ordinary module is completely reducible. So any ordinary \( V \)-module is a direct sum of copies of \( V \). Since \( V \) is \( C_2 \)-cofinite, any submodule generated by a single vector in any admissible module is an ordinary module (see [ABD]). This shows that any admissible \( V \)-module is completely reducible. That is, \( V \) is rational. This together with condition (a) gives conclusion that \( V \) is holomorphic. \( \square \)

Lemma 7.3. The \( q \)-dimension \( ch_q V = q^{-1} \sum_{n \geq 0} (\dim V_n)q^n \) of \( V \) is \( J(q) \).

**Proof:** Since \( V \) is holomorphic and \( C_2 \)-cofinite, by the modular invariance result in [Z], \( ch_q V \) is a modular function on the full modular group, and thus equal to \( J(q) \) by noting that \( V_0 = C1 \) and \( V_1 = 0 \). \( \square \)

Since \( V \) is irreducible and \( V_0/L(1)V_1 \) is one dimensional, there is a unique nondegenerate symmetric invariant bilinear form \( \langle \cdot, \cdot \rangle \) on \( V \) such that \( \langle 1, 1 \rangle = 1 \) (see [Li]). That is,

\[
(Y(u, z)v, w) = (-z^{-2})^{wu}(v, Y(\gamma_{L(1)}u, z^{-1})w)
\]

for homogeneous \( u \in V \). In particular, the restriction of \( \langle \cdot, \cdot \rangle \) to each \( V_n \) is nondegenerate. As a result, \( \langle \cdot, \cdot \rangle \) defines a nondegenerate symmetric invariant bilinear form on the Griess algebra \( V_2 \) such that \( \langle u, v \rangle = u_3v \) for \( u, v \in V_2 \).

From now on we will fix the vectors \( \{\omega_1, \ldots, \omega_{48}\} \) of \( V_2 \) given in Theorem 6.1. Since we only assume that \( V_2 \) is isomorphic to the Griess algebra we do not know if the bilinear form \( \langle u, v \rangle = u_3v \) defined on \( V_2 \) is the same as the bilinear form defined on \( V_2^2 \) using the same formula. So it is not clear that \( \{\omega_1, \ldots, \omega_{48}\} \) forms a VF in \( V \).
Since $V_2$ is a simple commutative nonassociative algebra, we need a result on the bilinear forms over a finite dimensional simple commutative nonassociative algebra $B$. A bilinear form $(\cdot,\cdot)$ on $B$ is called invariant if $(ab,c) = (b,ac)$, for all $a,b,c \in B$. The next result applies to any finite dimensional simple algebra.

**Lemma 7.4.** The space of nondegenerate symmetric invariant bilinear forms on $B$ is at most one-dimensional.

**Proof:** Let $(\cdot,\cdot)$ and $(\cdot,\cdot)$ be two nondegenerate symmetric invariant bilinear forms on $B$. Then there is a linear isomorphism $f : B \rightarrow B$ such that $(u,v) = (f(u),v)$ for all $u,v \in V$. For any $a \in B$ we have

$$(f(au),v) = (au,v) = (u,av) = (f(u),av) = (af(u),v).$$

That is, $f(au) = af(u)$. Let $B_\lambda$ be the eigenspace of $f$ with eigenvalue $\lambda \neq 0$. Then $B_\lambda$ is an ideal of $B$. This shows that $B = B_\lambda$. So $f = \lambda \ id_B$. As a result, $(\cdot,\cdot) = \lambda (\cdot,\cdot)$, as desired. \hfill $\square$

**Lemma 7.5.** Each $\omega_i$ is a Virasoro vector with central charge $\frac{1}{2}$ and for all $m,n$,

$$[L_i^i(m),L_j^j(n)] = 0$$

if $i \neq j$ where $Y(\omega_i,z) = \sum_{n \in \mathbb{Z}} L_i^i(n) z^{-n-2}$.

**Proof:** We first prove that each $\omega_i$ is a Virasoro vector of central charge $\frac{1}{2}$. That is, the component operators $L_i^i(n)$ of $Y(\omega_i,z) = \sum_{n \in \mathbb{Z}} L_i^i(n) z^{-n-2}$ satisfies the Virasoro algebra relation with central charge $\frac{1}{2}$.

Clearly $\omega_i \cdot \omega_i = L_i^i(0) \omega_i = 2 \omega_i$ by the product in $B$. So, $\omega_i$ is a Virasoro vector with central charge $c_i$ defined by $c_i 1 = 2 L_i^i(2) \omega_i$. Note that $L_i^i(0)$ is semisimple on $V_2$ and the eigenvalues of $L_i^i(0)$ are $2,0,\frac{1}{2}$ and $\frac{1}{16}$ (see [DGH]). Since the bilinear form is invariant, we see that the eigenspaces with different eigenvalues are orthogonal. So the restriction of the bilinear form to each eigenspace is nondegenerate. It is known from [DGH] that the eigenspace with eigenvalue $2$ is one dimensional and is spanned by $\omega_i$. As a result, $L_i^i(0) \omega_i$ is nonzero and $c_i \neq 0$. We must prove that $c_i = \frac{1}{2}$.

Recall from [DM3] that the Griess algebra is a simple commutative nonassociative algebra. Let $(\cdot,\cdot)$ be the bilinear from defined on $V_2^2$ and $(\cdot,\cdot)$ be the bilinear form defined on $V_2$. By Lemma 7.4, $(\cdot,\cdot)$ is a multiple of $(\cdot,\cdot)$. Note that $(\omega,\omega) = (\omega,\omega) = 12$. We conclude that these two bilinear forms are exactly the same. So $(\omega_i,\omega_j) = (\omega_i,\omega_j) = \frac{1}{4}$. That is $c_i = \frac{1}{2}$.

Let $i \neq j$. Since $(\omega_i,\omega_j) = 0$ and $L_i^i(0) \omega_j = 0$, we see immediately that $[L_i^i(m),L_j^j(n)] = 0$ for all $m,n \in \mathbb{Z}$. \hfill $\square$

**Theorem 7.6.** The $\{\omega_1,\ldots,\omega_{18}\}$ forms a VF in $V$ and $V$ is a FVOA.

**Proof:** We only need to prove that vertex operator subalgebra $\langle \omega_i \rangle$ generated by $\omega_i$ is isomorphic to $L(\frac{1}{2},0)$ for the Virasoro algebra $Vir_i$ generated by $L_i^i(m)$ for $m \in \mathbb{Z}$. It is clear that $\langle \omega_i \rangle$ is a highest weight module with highest weight $0$ for $Vir_i$. Then there are two possibilities. Either $\langle \omega_i \rangle$ is the Verma module modulo the submodule generated by $L_i^i(-1) 1$ or $\langle \omega_i \rangle$ is isomorphic to $L(\frac{1}{2},0)$, according to the structure theory of highest
weight modules for the Virasoro algebra with central charge $\frac{1}{2}$ [FF]. We now assume that the first possibility happens.

In this case the $q$-character of $\langle \omega_i \rangle$ is equal to

$$\text{ch}_q \langle \omega_i \rangle = q^{-1/48} \frac{1}{\prod_{n \geq 2}(1-q^n)}.$$ 

Let $U$ be the vertex operator subalgebra of $V$ generated by $\omega_j$ for $j = 1, \ldots, 48$. Then we have

$$U = \langle \omega_1 \rangle \otimes \cdots \otimes \langle \omega_{48} \rangle$$

is a tensor product. Let $f(q^{\frac{1}{2}}), g(q^{\frac{1}{2}}) \in \mathbb{R}[[q^{1/n}, q^{-1/n}]]$ for some positive integer $n$. We write $f(q^{\frac{1}{2}}) \leq g(q^{\frac{1}{2}})$ if the coefficient of $q^m$ in $f(q^{\frac{1}{2}})$ is less than or equal to that in $g(q^{\frac{1}{2}})$ for all $m$. It is well known that the $q$-character of $L(\frac{1}{2}, 0)$ is equal to

$$\frac{1}{2} q^{-1/48} \left( \prod_{n \geq 0} (1 + q^{n+\frac{1}{2}}) + \prod_{n \geq 0} (1 - q^{n+\frac{1}{2}}) \right)$$

(cf. [KR]). Thus we have

$$\text{ch}_q U \geq f(q^{\frac{1}{2}}) \quad (7.1)$$

where

$$f(q^{\frac{1}{2}}) := q^{-1} \frac{1}{247} \left( \prod_{n \geq 0} (1 + q^{n+\frac{1}{2}}) + \prod_{n \geq 0} (1 - q^{n+\frac{1}{2}}) \right)^{47} \prod_{n \geq 2} \frac{1}{(1-q^n)}. $$

Clearly, both $\text{ch}_q U$ and $f(q^{\frac{1}{2}})$ are convergent for $0 < |q| < 1$, when $q$ is regarded as a complex number. So, we can and do treat both $\text{ch}_q U$ and $f(q^{\frac{1}{2}})$ as functions for $0 < q < 1$ and the inequality (7.1) still holds as functions.

We have already proved in Lemma 7.3 that the graded dimension of $V$ is $J(q)$ which of course also converges for $0 < |q| < 1$. In the following we will take $q$ to be a real number in the domain $(0, 1)$. Since $U$ is a subspace of $V$, we have

$$\frac{\text{ch}_q U}{J(q)} \leq 1.$$

Let $L$ be the Niemeier lattice of type $D_{24}$. Then the lattice vertex operator algebra $V_L$ is a module for the affine Lie algebra $D^{(1)}_{24}$. Denote the irreducible highest weight module for $D_{24}^{(1)}$ of level $k$ by $L_k(\lambda)$ where $\lambda$ is a dominant weight of the finite dimensional Lie algebra of type $D_{24}$. Let $\lambda_i$ be the fundamental weights of Lie algebra of type $D_{24}$ for $i = 1, \ldots, 24$ so that $\lambda_{23}$ and $\lambda_{24}$ are the half spin weights. (We are using the labelling of simple roots given in [H].) Then as a module for $D^{(1)}_{24}$ $V_L$ is a direct sum

$$V_L = L_1(0) \oplus L_1(\lambda_{23})$$

following from the structure of lattice $L$. It is well-known that

$$\text{ch}_q V_L = \frac{\theta_L(q)}{\eta(q)^{24}} = J(q) + 2 \times (24)^2 - 24$$
where $2 \times (24)^2 - 24 = 1128$ is the dimension of the Lie algebra of type $D_{24}$,
\[
\theta(q) = \sum_{\alpha \in L} q^{(\alpha, \alpha)/2}
\]
is the theta function of the lattice $L$ and
\[
\eta(q) = q^{1/24} \prod_{n \geq 1} (1 - q^n).
\]
So we have
\[
J(q) < ch_q V_L
\]
as a function in $q \in (0, 1)$.

On the other hand, using the Boson-Fermion correspondence given in [F], we see that the characters of the fermion realizations of $L_1(0)$ and $L_1(\lambda_{23})$ satisfy the following relations
\[
ch_q L_1(0) \leq ch_q L_1(0) + ch_q L_1(\lambda_1) = q^{-1} \prod_{n \geq 0} (1 + q^{n+\frac{1}{2}})^{48}
\]
\[
ch_q L_1(\lambda_{23}) = q^{-1} \prod_{n \geq 0} (1 + q^n)^{48} < 2q^{-1} \prod_{n \geq 0} (1 + q^{n+\frac{1}{2}})^{48}
\]
As a result we have
\[
J(q) \leq ch_q V_L \leq 3q^{-1} \prod_{n \geq 0} (1 + q^{n+\frac{1}{2}})^{48}.
\]

Note that
\[
f(q^{\frac{1}{2}}) \geq q^{-1} \frac{1}{2^{47}} \prod_{n \geq 0} (1 + q^{n+\frac{1}{2}})^{47} \prod_{n \geq 2} \frac{1}{(1 - q^n)}
\]
So finally we have
\[
\frac{ch_q U}{ch_q V} \geq \frac{1}{2^{47}3} \prod_{n \geq 0} \frac{1}{(1 + q^{n+\frac{1}{2}})} \prod_{n \geq 2} \frac{1}{(1 - q^n)}. \tag{7.2}
\]
Clearly, the right hand side of (7.2) goes to infinity as $q$ goes to 1. This is a contradiction to $\frac{ch_q U}{ch_q V} \leq 1$.

\[\square\]

**Remark 7.7.** From the proof Theorem 7.6 we see that we in fact prove a stronger result: If $\{u_1, ..., u_{48}\}$ are 48 mutually commutative Virasoro elements of central charge $\frac{1}{2}$ then $\{u_1, ..., u_{48}\}$ is a VF.

**Remark 7.8.** In the proof of Theorem 7.6 we only use the fact that $ch_q V = J(q)$. In fact, the proof goes through if we assume that $\dim V_n \leq V_n^2$ for $n \geq 3$. So Theorem 7.6 holds with the assumptions given in Theorem 2.

**Proof of Theorem 1:** By Theorem 7.6, $V$ is an FVOA with VF $F := \{\omega_1, ..., \omega_{48}\}$. Let $U$ be the vertex operator subalgebra generated by $V_2$. Then $U$ is also a FVOA with the same VF. Since $F$ is a VF in both $U$ and $V$, we use a subscript $U$ to indicate dependence of the associated binary codes on $U$. We have that $\mathcal{C}$ is a subcode of $C_U(F)$ and $\mathcal{D}$ is a subcode of $D_U(F)$. Since $D_U(F) \subset C_U(F)^\perp$, and $\mathcal{D} = \mathcal{C}^\perp$ we immediately see that $\mathcal{C} = C_U(F)$ and $\mathcal{D} = D_U(F)$. 
Note that $\mathcal{C}$ is a subgroup of $C(V)$ and $\mathcal{D}$ is a subgroup of $D(F)$. Since $V$ is holomorphic by Lemma 7.3, $C(F) = D(F) \perp$ (see Theorem 4.1). This implies that $C_U(F) = C(F) = \mathcal{C}$ and $D_U(F) = D(F) = \mathcal{D}$.

Now $M_C = U^0$ is a vertex operator subalgebra of $V$. Then by Theorem 4.1, $V$ is a direct sum of inequivalent irreducible $M_C$-modules. By Theorem 6.7, for each $\delta \in \mathcal{D}$ there exists a unique $\gamma_\delta \in \mathbb{Z}_{48} / \mathcal{C}$ such that $M(\delta, \gamma_\delta)$ is isomorphic to a submodule of $V$. Then

$$V \cong \bigoplus_{\delta \in \mathcal{D}} M(\delta, \gamma_\delta)$$

as $M_C$-module. Similarly, $V^z$ has a decomposition

$$V^z \cong \bigoplus_{\delta \in \mathcal{D}} M(\delta, \beta_\delta)$$

where $\beta_\delta \in \mathbb{Z}_{48} / \mathcal{C}$. In the case that the lowest weight of $M(\delta, \beta_\delta)$ is 0 or 2, we have $\beta_\delta = \gamma_\delta$. Since every module for $M_C$ is a simple current by Theorem 6.10, by the uniqueness of simple current extension theorem in [DM2], it is sufficient to show that $M(\delta, \gamma_\delta)$ and $M(\delta, \beta_\delta)$ are isomorphic $M_C$-modules.

For $\delta \in \mathcal{D}$ we denote the lowest weight of $M(\delta, \beta_\delta)$ by $w(\delta)$. Set

$$X = \{ (\delta, \beta_\delta) | \delta \in \mathcal{D}, w(\delta) = 0, 2 \}.$$

Since $V^z$ is generated by $V^z_2$ (see [FLM2]), the group $G := \{ (\delta, \beta_\delta) | \delta \in \mathcal{D} \}$ is a subgroup of $\mathcal{D} \times \mathbb{Z}_{48} / \mathcal{C}$ generated by $X$. So, the group $H := \{ (\delta, \gamma_\delta) | \delta \in \mathcal{D} \}$ is a subgroup of $\mathcal{D} \times \mathbb{Z}_{48} / \mathcal{C}$ and contains $G$ as a subgroup. As a result, $G = H$. By Theorem 6.7, $M(\delta, \gamma_\delta)$ and $M(\delta, \beta_\delta)$ are indeed isomorphic $M_C$-modules.

**Proof of Theorem 2:** In this case, the conclusions of Lemmas 7.1, 7.4, 7.5 and Theorem 7.6 still hold (see Remark 7.8).

Let $U$ be as in the proof of Theorem 1. Since $U$ is generated by the Griess algebra, and $\mathcal{D} \subset \mathcal{C}$, $C(U) = \mathcal{C}$ and $M_C$ is a subalgebra of $U$. From the proof of Theorem 1 we see that

$$U \cong \bigoplus_{\delta \in \mathcal{D}} M(\delta, \gamma_\delta)$$

as $M_C$-modules. The same argument used in the proof of Theorem 1 shows that $U$ and $V^z$ are isomorphic. So we have

$$J(q) = ch_q V^z \geq ch_q V \geq ch_q U = J(q).$$

As a result, $U = V$. This completes the proof. \qed

We give an application of Theorem 2. Let $U$ be the $\mathbb{Z}_3$ orbifold construction given in [DM1]. It has been expected for a long time that $U$ and $V^z$ are isomorphic vertex operator algebras. The isomorphism follows from Theorem 2 easily now.

**Corollary 7.9.** $V^z$ and $U$ are isomorphic.

**Proof:** $U$ satisfies the conditions in Theorem 2. In particular, $ch_q U = J(q)$. \qed
References

[ABD] T. Abe, G. Buhl and C. Dong, regularity, and $C_2$-cofiniteness, Trans. Amer. Math. Soc. 356 (2004), 3391–3402.

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

[D] C. Dong, Representations of the moonshine module vertex operator algebra, Contemporary Math. 175 (1994), 27–36.

[DGH] C. Dong, R. Griess Jr. and G. Hoehn, Framed vertex operator algebras, codes and the moonshine module, Comm. Math. Phys. 193 (1998), 407–448.

[DL] C. Dong and J. Lepowsky, Generalized vertex algebras and relative vertex operators, Progress in Math. Vol. 112, Birkhäuser, Boston 1993.

[DLM1] C. Dong, H. Li and G. Mason, Regularity of rational vertex operator algebras, Adv. in Math. 132 (1997), 148–166.

[DLM2] C. Dong, H. Li and G. Mason, Twisted representations of vertex operator algebras, Math. Ann. 310 (1998), 571–600.

[DLMN] C. Dong, H. Li, G. Mason and S. Norton, Associative subalgebras of the Griess algebra and related topics, in: Proc. of the Conference on the Monster and Lie algebras at The Ohio State University, May 1996, ed. by J. Ferrar and K. Harada, Walter de Gruyter, Berlin-New York, 1998, 27–42.

[DM1] C. Dong and G. Mason, The construction of the moonshine module as a $Z_p$-orbifold, Contemporary Math. 175 (1994), 37-52.

[DM2] C. Dong and G. Mason, Rational vertex operator algebras and the effective central charge, Int. Math. Res. Not. 56 (2004), 2989–3008.

[DM3] C. Dong and G. Mason, Holomorphic vertex operator algebras of small central charges, Pacific J. Mathematics 213 (2004), 253–266.

[DMZ] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, Proc. Symp. Pure. Math., American Math. Soc. 56 II (1994), 295–316.

[F] I. B. Frenkel, Two constructions of affine Lie algebra representations and boson-fermion correspondence in quantum field theory, J. Funct. Anal. 44 (1981), 259–327.

[FF] B. Feigin and D. Fuchs, Verma modules over the Virasoro algebra, Lecture Notes in Mathematics, 1060, Springer Verlag, (1984), 230-245.

[FLM1] I. B. Frenkel, J. Lepowsky and A. Meurman, A natural representation of the Fischer-Griess Monster with the modular function $J$ as character, Proc. Natl. Acad. Sci. USA 81 (1984), 3256–3260.

[FLM2] I. B. Frenkel, J. Lepowsky and A. Meurman, Vertex Operator Algebras and the Monster, Pure and Applied Math., Vol. 134, Academic Press, 1988.

[FQS] D. Friedan, Z. Qiu and S. Shenker, Details of the non-unitarity proof for highest weight representations of Virasoro Algebra, Comm. Math. Phys. 107 (1986), 535–542.

[GKO] P. Goddard, A. Kent and D. Olive, Unitary representations of the Virasoro algebra and super-Virasoro algebras Comm. Math. Phys. 103, 105–119 (1986).

[G] Robert L. Griess, Jr., the Friendly Giant, Inventiones Math., 69 (1982), 1–102.

[G1] Robert L. Griess, Jr., GNAVOA, I. (studies in groups, nonassociative algebras and vertex operator algebras), article in Vertex Operator Algebras in Mathematics and Physics, with S. Berman, Y. Billig and J. Lepowsky, Fields Institute Communications, Vol. 39, Amer. Math. Soc., Providence, 2003.

[H] J. Humphreys, Introduction to Lie Algebras and Representation Theory, Second printing, revised. Graduate Texts in Mathematics, 9. Springer-Verlag, New York-Berlin, 1978.

[KR] V. Kac and A. Raina, Highest Weight Representations of Infinite Dimensional Lie Algebras, Advanced Series in Mathematical Physics, Vol. 2, World Scientific, 1987.

[KLY] M. Kitazume, C. Lam and H. Yamada, 3-state Potts model, Moonshine vertex operator algebra, and 3A-elements of the Monster group, Int. Math. Res. Not. 23 (2003), 1269–1303.
C. Lam, Fusion rules for the Hamming code vertex operator algebra, Comm. Algebra, 29(5), 2001, 2125-2145.

H. Li, Symmetric invariant bilinear forms on vertex operator algebras, J. Pure and Appl. Math. 96(1994), 279–297.

H. Li and X. Xu, A characterization of vertex algebras associated to even lattices. J. Algebra 173 (1995), no. 2, 253–270.

M. Miyamoto, Binary codes and vertex operator (super)algebras, J. Algebra 181 (1996), 207-222.

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

M. Miyamoto, A new construction of the Moonshine vertex operator algebra over the real number field, Ann. of Math. 159 (2004), 535–596.

A. N. Schellekens, Meromorphic $c = 24$ Conformal Field Theories, Commu. Math. Phys. 153 (1993), 159.

Y. Zhu, Modular invariance of characters of vertex operator algebras, J. Amer, Math. Soc. 9 (1996), 237–302.

Department of Mathematics, University of California, Santa Cruz, CA 95064
Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1109
Department of Mathematics, National Cheng Kung University, Tainan, Taiwan 701