# A New Existence Proof of the Monster by VOA Theory

ROBERT L. GRIESS JR. & CHING HUNG LAM

#### 1. Introduction

We define a finite group G to be of *Monster type* if it has an involution z whose centralizer  $C_G(z)$  has the form  $2^{1+24}$ Co<sub>1</sub> and is 2-constrained (i.e., satisfies  $\langle z \rangle = C_G(O_2(C_G(z)))$  and if z is conjugate to an element in  $C_G(z) \setminus \{z\}$ . A short argument proves that such a G must be simple (e.g., see [21; 46]). We use the abbreviation VOA for *vertex operator algebra* [17].

This paper gives a new and relatively direct existence proof of a group of Monster type. Our methods depend on vertex operator algebra representation theory and are free of many special calculations that traditionally occur in theory of the Monster. Most of this article is dedicated to explaining how existing VOA theory applies.

In fact, a group of Monster type is unique up to isomorphism [23], so the group we construct here can be called "the" Monster, the group constructed in [21]. To avoid specialized finite group theory in this article, we work with a group of Monster type and refer to [23] for uniqueness.

Our basic strategy is described briefly in the next paragraph. It was inspired by the article of Miyamoto [35], which showed how to make effective use of *simple current modules and extensions*. Later in this Introduction, we sketch these important concepts. In a sense, our existence proof is quite short. The hard group theory and case-by-case analysis of earlier proofs have essentially been eliminated.

In [41], Shimakura gives a variation of Miyamoto's construction. He takes  $(V_{EE_8}^+)^3$  and builds a candidate V for the Moonshine VOA using the theory of simple current extensions (a short account is given in Section 2.1). His treatment is more direct and shorter than Miyamoto's. Moreover, his method furnishes a large subgroup of Aut(V). From this subgroup, we take a certain involution and analyze  $V^+$ ,  $V^-$ , its fixed point VOA and its negated space on V, respectively. We can recognize  $V^+$  as a Leech lattice-type VOA. The group Aut( $V^+$ ) and its extension (by projective representations) to irreducibles of the fixed point VOA are understood. One of these irreducibles is  $V^-$ . We thereby get a new subgroup of Aut(V), which has the shape  $2^{1+24}$ Co<sub>1</sub> and is moreover isomorphic to the centralizer of a 2-central involution in the Monster. These two subgroups of Aut(V) generate the larger group Aut(V), which we then prove is a finite group of Monster type.

Received March 7, 2011. Revision received January 18, 2012.

We refer to the overVOA of  $(V_{EE_8}^+)^3$  described in Theorem 2.18 as a VOA of *Moonshine type*, meaning a holomorphic VOA  $V = \bigoplus_{n=0}^{\infty} V_n$  of central charge 24, so that  $V_0$  is 1-dimensional,  $V_1 = 0$ , and the Monster acts as a group of automorphisms with faithful action on  $V_2$ . We mention that such a VOA is isomorphic to the standard Moonshine VOA constructed in [17], by [10; 27]. For the purpose of this paper, it is not necessary to quote such characterizations.

The theory of simple current modules originated in the papers [18] and [38]. In [11; 29], certain simple current modules of a VOA are constructed using weight-1 semi-primary elements, and extensions of a VOA by its simple current modules are also studied. The notion of simple current extension turns out to be a powerful tool for constructing new VOAs from a known one [9; 28; 29; 31; 35]. Let V be a simple VOA and let  $\mathcal{M} = \{M^i \mid i \in I\}$  be a finite set of irreducible modules of V with integral weights. If  $V \in \mathcal{M}$  and  $\bigoplus_{M \in \mathcal{M}} M$  is closed under the fusion rules, then it is possible that  $\bigoplus_{M \in \mathcal{M}} M$  carries the structure of a simple VOA for which V is a subVOA. In general, it is extremely difficult to determine whether  $\bigoplus_{M \in \mathcal{M}} M$  has a structure of a simple VOA (see the following Remark). There may be no such VOA structures, or there could be many. When the simple current property holds (Definition 2.3), there is a simple VOA structure on  $\bigoplus_{M \in M} M$  extending the given action of V and the VOA structure is unique if the underlying field is algebraically closed [14, Prop. 5.3] (see also [15; 31]). This "rigidity" of simple current extensions is useful in structure analysis and leads to certain transitivity results that reduce the need for calculations.

As described in [21], existence of the Monster implies existence of several other sporadic groups that had originally been constructed with special methods, including computer work. We hope that the present article may suggest useful viewpoints for other sporadic groups.

**REMARK.** If the simplicity is not imposed then it is not difficult to give  $\bigoplus_{M \in \mathcal{M}} M$ a VOA structure, where  $\mathcal{M}$  is a finite set of irreducible modules of V with integral weights and  $V \in \mathcal{M}$ . For example, one may give  $V \oplus M$  a VOA structure by defining Y(a, z)v using the skew symmetry for  $a \in M$ ,  $v \in V$  and Y(a, z)b = 0 for any  $a, b \in M$ .

EXISTENCE PROOFS. The first existence proof of the Monster was made in 1980 and published in [21]; see also [20]. A group  $C \cong 2^{1+24}$ Co<sub>1</sub> and a representation of degree 196883 was described. The hard part was to choose a *C*-invariant algebra structure, give an automorphism  $\sigma$  of it that did not come from *C*, then identify the group  $\langle C, \sigma \rangle$  by proving finiteness and proving that *C* is an involution centralizer in it.

During the decade that followed the publication of [21], there were analyses, improvements, and alternate viewpoints by Tits [43; 44; 45; 46] and Conway [1]. In the mid-1980s, the theory of vertex algebras was developed. The Frenkel–Lepowsky–Meurman text [17] established the important construction of a Moonshine VOA and became a basic reference for VOA theory. The construction of the Monster done in [17] followed the lines of [21] but in a broader VOA setting. The

articles [4; 5] constructed a VOA and gave a physics field theory interpretation to aspects of [17; 21].

In 2004, Miyamoto [35] made significant use of simple current extensions to give a new construction of a Moonshine VOA and the Monster acting as automorphisms. An existence proof of the Monster was recently announced in [25], which uses theories of finite geometries and group amalgams.

Uniqueness was first proved in [23]. A different uniqueness proof is indicated in [25].

NOTATION. Table 1 summarizes the notation used in this paper.

ACKNOWLEDGMENTS. The first author thanks the United States National Science Foundation (NSF DMS-0600854) and the National Security Agency (NSA H98230-10-1-0201) for financial support as well as the Academia Sinica for hospitality during a visit in August 2010. The second author thanks the National Science Council (NSC 97-2115-M-006-015-MY3) and the National Center for Theoretical Sciences (Taiwan) for financial support.

# 2. Simple Current Extensions

In this section, we shall recall the notion of simple current extensions and their basic properties [11; 41].

Let *V* be a VOA and let  $M_1, M_2, M_3$  be *V*-modules. We denote the space of all *V*-intertwining operators of type  $\binom{M_3}{M_1 M_2}$  by  $I_V\binom{M_3}{M_1 M_2}$  and its dimension by  $N_{M_1 M_2}^{M_3}$  [16, Chap. 5].

DEFINITION 2.1 [11]. Let V be a rational  $C_2$ -cofinite VOA. An irreducible V-module M is called a *simple current module* if the fusion product  $M \times_V N$  is again irreducible for any irreducible V-module N, that is,  $\sum_{W \text{ irred}} N_{M N}^W = 1$ .

DEFINITION 2.2. A *full* subVOA is a subVOA that contains the principal Virasoro element of the larger VOA.

Now let  $V^0$  be a simple rational  $C_2$ -cofinite VOA of CFT type (see [27, Def. 3.1]) and let D be a finite abelian group. Let  $\{V^{\alpha} \mid \alpha \in D\}$  be a set of inequivalent irreducible  $V^0$ -modules indexed by D. Assume that the weights of  $V^{\alpha}$ ,  $\alpha \in D$ , are integral and that  $V^{\alpha} \times_{V^0} V^{\beta} = V^{\alpha+\beta}$  for all  $\alpha, \beta \in D$ .

DEFINITION 2.3 [11]. A simple VOA  $V = \bigoplus_{\alpha \in D} V^{\alpha}$  is called a (*D*-graded) simple current extension of  $V^0$  if  $V^0$  is a full subVOA of V and all  $V^{\alpha}, \alpha \in D$ , are simple current  $V^0$ -modules.

Next we shall recall the notion of g-conjugate modules [13; 41].

DEFINITION 2.4. Let  $(M, Y_M)$  be a *V*-module and  $g \in \text{Aut}(V)$  an automorphism. The *g*-conjugate module of *M* is defined to be the *V*-module  $(g \circ M, Y_{g \circ M})$ , where  $g \circ M = M$  is a vector space and  $Y_{g \circ M}(v, z) = Y_M(g^{-1}v, z)$  for all  $v \in V$ .

Notation	Explanation	Examples in the Text
$\overline{A.B, A:B,}_{A \cdot B}$	group extension of normal subgroup <i>A</i> by quotient <i>B</i> , split extension, nonsplit extension (respectively)	Prop. 2.22, Thm. 3.8
С	centralizer of an involution in $Aut(V)$	Not. 3.9
$\operatorname{cvcc}\frac{1}{2}$	simple conformal vector of central charge $\frac{1}{2}$	Sec. 3.1
Co <sub>1</sub>	first Conway group $O(\Lambda)/\{\pm 1\}$	p. 555
$EE_8$	lattice isometric to $\sqrt{2}$ times the famous $E_8$ lattice	p. 555, Sec. 2.1
$\mathbb{F}\{L\}$	twisted group algebra of a lattice $L$ over a field $\mathbb F$	Cor. 3.7
$g \circ M$	g-conjugate module of a V-module M	Def. 2.4
$H_{\Lambda}$	subgroup of Aut( $V_{\Lambda}^+$ ) generated by Miyamoto involutions of $AA_1$ -type	Not. 3.13
$ ilde{H}_{\Lambda}$	subgroup of Aut( $V_{\Lambda}$ ) generated by Miyamoto involutions of $AA_1$ -type	Rem. 3.18
Λ	Leech lattice, the unique even unimodular lattice of rank 24 with no roots	Sec. 3, Cor. 3.7
<i>M</i> (1)	unique irreducible $\hat{\mathfrak{h}}$ -module such that $\alpha \otimes t^n 1 = 0$ for all $\alpha \in \mathfrak{h}$ and $n > 0$ and $K = 1$ , where $\mathfrak{h} = \mathbb{C} \otimes_{\mathbb{Z}} L$ and $\hat{\mathfrak{h}} = \bigoplus_{n \in \mathbb{Z}} (\mathfrak{h} \otimes t^n) \oplus \mathbb{C} K$	Cor. 3.7
$M \times_V N$	fusion product of V-modules M, N	Def. 2.1
$O_p(G)$	maximal normal $p$ -subgroup of $G$	p. 570
$O_{p'}(G)$	maximal normal subgroup of $G$ of order prime to $p$	p. 570
R(U)	set of all inequivalent irreducible modules of $U$	Sec. 2.1
$\operatorname{Stab}_G(X)$	subgroup of the group $G$ that stabilizes the set $X$	Not. 4.10
t(e)	Miyamoto involution associated to a $\operatorname{cvcc} \frac{1}{2} e$	Not. 3.15
U	the VOA $V_{EE_8}^+$	Not. 2.13
$2^{1+2n}$	extra-special 2-group of order $2^{1+2n}$	p. 555, p. 565
$2^{1+24}Co_1$	an extension of $Co_1$ by $2^{1+24}$	p. 555, Sec. 3
V	a VOA that is a simple current extension of $U$	Not. 2.20
$V_L$	lattice VOA for positive definite even lattice L	Lemma 3.6, Cor. 3.7
$V_{L,\mathbb{R}}$	lattice VOA over $\mathbb R$ for positive definite even lattice $L$	Lemma 3.6, Cor. 3.7
$ ilde{V}_{L,\mathbb{R}}$	real form of the lattice VOA $V_L$ whose invariant form is positive definite	Prop. 4.18
$V_L^+$	the fixed point subVOA of $V_L$ by a lift of the $(-1)$ -isometry of $L$	Sec. 2.1, Cor. 3.7

Table 1

REMARK 2.5. By definition, there exists a linear isomorphism  $v: g \circ M \to M$ such that  $vY_{g \circ M}(v, z) = Y_M(g^{-1}v, z)v$  for any  $v \in V$ . In fact, one can assume  $v = \operatorname{id}_M$  by identifying  $g \circ M$  with M as vector spaces.

The following theorem follows easily by the fusion rules  $V^{\alpha} \times V^{\beta} = V^{\alpha+\beta}$ .

THEOREM 2.6. Let  $V^0$  be a rational  $C_2$ -cofinite VOA of CFT type and let  $V = \bigoplus_{\alpha \in D} V^{\alpha}$  be a (D-graded) simple current extension of  $V^0$ . Let  $D^*$  be the group of all irreducible characters of D. Then, for any  $\chi \in D^*$ , the linear map

$$\tau_{\chi}(v) = \chi(\alpha)v \text{ for any } v \in V^{\alpha}, \, \alpha \in D,$$

defines an automorphism of V. In particular,  $\{\tau_{\chi} \mid \chi \in D^*\} \cong D^*$  is an abelian subgroup of Aut(V).

NOTATION 2.7. By abuse of notation, we often denote the group  $\{\tau_{\chi} \mid \chi \in D^*\} < Aut(V)$  defined in Theorem 2.6 by  $D^*$ .

NOTATION 2.8. Let W be an irreducible V-module. We shall use [W] to denote the isomorphism class containing W.

The next theorem gives a criterion for lifting an automorphism of  $V^0$  to V and can be proved using the general arguments for simple current extensions [37; 39].

THEOREM 2.9 (cf. [39]). Let  $V^0$  be a rational  $C_2$ -cofinite VOA of CFT type and  $V = \bigoplus_{\alpha \in D} V^{\alpha}$  a (D-graded) simple current extension of  $V^0$ . Let  $g \in \operatorname{Aut}(V^0)$ . Then there exists an automorphism  $\tilde{g} \in \operatorname{Aut}(V)$  such that  $\tilde{g}|_{V^0} = g$  if and only if  $\{[g \circ V^{\alpha}] \mid \alpha \in D\} = \{[V^{\alpha}] \mid \alpha \in D\}.$ 

REMARK 2.10. Recall that  $g \circ W \cong g \circ W'$  if and only if  $W \cong W'$  [41]. Thus the isomorphism class  $[g \circ W]$  is independent of the choice of the representative  $W \in [W]$ .

THEOREM 2.11 [40, Cor. 2.2]. Let  $V = \bigoplus_{\alpha \in D} V^{\alpha}$  be a (D-graded) simple current extension of  $V^0$ . Denote

$$N_D = \{g \in \operatorname{Aut}(V^0) \mid \{[g \circ V^\alpha] \mid \alpha \in D\} = \{[V^\alpha] \mid \alpha \in D\}\}.$$

Then there exists an exact sequence

$$1 \to D^* \to N_{\operatorname{Aut}(V^0)}(D^*) \xrightarrow{\eta} N_D \to 1,$$

where  $\eta$  is the restriction map to  $V^0$  and  $D^*$  is identified with the group  $\{\tau_{\chi} \mid \chi \in D^*\}$ .

2.1. Simple Current Extension of  $(V_{EF_{\circ}}^+)^3$ 

In this section, we shall recall a description of the Moonshine VOA by Shimakura [41]. First we shall review some basic properties of the lattice-type VOA  $V_{EF_8}^+$  [22; 39].

NOTATION 2.12. Let R(U) be the set of all inequivalent irreducible modules of a VOA U. If  $U = V_{EE_8}^+$ , then it is known [39] (see also [27]) that all irreducible modules of  $V_{EE_8}^+$  are simple current modules and  $R(V_{EE_8}^+)$  forms a 10-dimensional quadratic space over  $\mathbb{Z}_2$  with respect to the fusion rules and the quadratic form

$$q([M]) = \begin{cases} 0 & \text{if the weights of } M \text{ are in } \mathbb{Z}, \\ 1 & \text{if the weights of } M \text{ are in } \frac{1}{2} + \mathbb{Z}. \end{cases}$$
(1)

We shall denote the corresponding bilinear form by  $\langle \cdot, \cdot \rangle$ .

Recall that  $\operatorname{Aut}(V_{EE_8}^+) \cong O^+(10, 2)$  and  $\operatorname{Aut}(V_{EE_8}^+)$  acts on  $R(V_{EE_8}^+)$  as a group of isometries [22; 39].

NOTATION 2.13. From now on, we use U to denote the VOA  $V_{EE_8}^+$  and  $U^n$  to denote the tensor product of n copies of U.

The proof of the following proposition can be found in [39].

**PROPOSITION 2.14.** The group  $\operatorname{Aut}(U) \cong O^+(10, 2)$  acts transitively on nonzero singular elements and nonsingular elements of R(U), respectively.

- (i) If [W] is a nonzero singular element in R(U), then the minimal weight of the *irreducible module W is* 1 and dim $(W_1) = 8$ .
- (ii) If [W] is a nonsingular element, then the minimal weight of W is 1/2 and  $\dim(W_{1/2}) = 1$ .

NOTATION 2.15. Since  $R(U^3) \cong R(U)^3$ , we shall view  $R(U^3)$  as a direct sum of quadratic spaces (cf. Notation 2.12). The quadratic form and the associated bilinear form are given by q(a, b, c) = q(a) + q(b) + q(c) and  $\langle (a, b, c), (a', b', c') \rangle = \langle a, a' \rangle + \langle b, b' \rangle + \langle c, c' \rangle$  for  $(a, b, c) \in R(U)^3$ .

Following the analysis of [41], let  $\Phi$  and  $\Psi$  be maximal totally singular subspaces of R(U) such that  $\Phi \cap \Psi = 0$ . Then the space

$$S := \operatorname{span}_{\mathbb{Z}_2}\{(a, a, 0), (0, a, a), (b, b, b) \mid a \in \Phi, b \in \Psi\}$$
(2)

is a maximal totally singular subspace of  $R(U)^3 \cong R(U^3)$ .

DEFINITION 2.16. Let W be an irreducible module. We define the minimal weight of [W] to be the minimal weight of W.

LEMMA 2.17 [41, Prop. 2.4, Lemma 2.6]. Let  $[W] \in S$ . Then the minimal weight of [W] is  $\geq 2$ . If the minimal weight of [W] is 2 then, up to a permutation of the three coordinates, [W] has the form:

- (i) (a, a, 0), where  $a \in \Phi \setminus \{0\}$ ; or
- (ii) (a + b + c, a + c, b + c), where  $a, b \in \Phi \setminus \{0\}$ ,  $c \in \Psi$ , a + c and b + c are nonsingular, and a + b + c is nonzero singular.

By Lemma 2.17, we have the following theorem.

THEOREM 2.18 [41, Thm. 4.10]. Let  $V := \mathcal{V}(S) = \bigoplus_{[W] \in S} W$ . Then V is a holomorphic framed VOA of central charge 24 and  $V_1 = 0$ .

REMARK 2.19. It was also shown in [41] that the singular space S defined in (2) is the unique (up to Aut( $U^3$ )) maximal totally singular subspace of  $R(U^3)$  such that  $\mathcal{V}(S) = \bigoplus_{[W] \in S} W$  has trivial weight-1 subspace.

NOTATION 2.20. For the rest of this paper, *V* shall denote the VOA  $V := \mathcal{V}(S) = \bigoplus_{|W| \in S} W$  of Theorem 2.18.

THEOREM 2.21 [41]. The automorphism group Aut(V) acts transitively on the set of all subVOAs of V that are isomorphic to  $U^3$ .

PROPOSITION 2.22 [41, Cor. 4.18]. Let S be defined as in (2). We identify  $S^*$ with the subgroup  $\{\tau_{\chi} \mid \chi \in S^*\}$  of Aut(V) that was defined in Theorem 2.6. Then  $N_{\operatorname{Aut}(V)}(\mathcal{S}^*) = \operatorname{Stab}_{\operatorname{Aut}(V)}(U \otimes U \otimes U) \cong 2^{15}(2^{20}:(L_5(2) \times \operatorname{Sym}_3)).$ 

# 3. Centralizer of an Involution

In this section, we shall show that the automorphism group of  $V = \mathcal{V}(S)$  (see Notation 2.20) has an involution z such that  $V^z \cong V_{\Lambda}^+$  and  $C_{Aut(V)}(z) \cong 2^{1+24}Co_1$ , where  $\Lambda$  denotes the Leech lattice.

NOTATION 3.1. Let  $\Phi$ ,  $\Psi$ , and S be defined as in Notation 2.15. Let  $x \in \Phi$  be a nonzero element. We denote

$$S^{0} = \{(a, b, c) \in S \mid \langle (a, b, c), (x, 0, 0) \rangle = 0\},\$$
  
$$S^{1} = \{(a, b, c) \in S \mid \langle (a, b, c), (x, 0, 0) \rangle = 1\}.$$

DEFINITION 3.2. Let  $V = \mathcal{V}(S) = \bigoplus_{[W] \in S} W$  be the VOA defined in Theorem 2.18. Define a linear map  $z: V \to V$  by

$$z = \begin{cases} 1 & \text{on } W \text{ for } [W] \in \mathcal{S}^0, \\ -1 & \text{on } W \text{ for } [W] \in \mathcal{S}^1. \end{cases}$$
(3)

Then z is an automorphism of order 2 of V.

The following lemma can be found in [41].

LEMMA 3.3. Let  $\mathcal{B}$  be the weight-2 subspace of V. Then dim $(\mathcal{B}) = 196884$ .

LEMMA 3.4. The trace of z on  $\mathcal{B}$  is 276.

*Proof.* Since  $x \in \Phi \setminus \{0\}$ , (x, 0, 0) is orthogonal to all elements of the shape (a, a, 0), (0, a, a), (a, a, 0) in S.

Moreover, (a + b + c, a + c, b + c) is orthogonal to (x, 0, 0) if and only if  $\langle x, c \rangle = 0$ . Therefore, there are  $(2^4 - 1) \times 2^4 \times 2^4 \times 3$  vectors of the form (a+b+c, a+c, b+c) in  $\mathcal{S}^0$  and  $2^4 \times 2^4 \times 2^4 \times 3$  vectors in  $\mathcal{S}^1$  that have minimal weights 2. Thus, the trace of z on  $\mathcal{B}$  is

$$(156 \times 3 + (2^{5} - 1) \times 3 \times 8^{2} + (2^{4} - 1) \times 2^{4} \times 2^{4} \times 3 \times 8) - (2^{4} \times 2^{4} \times 2^{4} \times 3 \times 8) = 276,$$
  
as desired.  $\Box$ 

as desired.

NOTATION 3.5. Let  $x \in \Phi \setminus \{0\}$  be as in Notation 3.1. Let A be an irreducible Umodule such that  $[A] = x \in R(U)$  and  $M = A \otimes U \otimes U$ . Then  $[M] = (x, 0, 0) \in$  $R(U)^3$ . Let V and z be as in Definition 3.2. Denote

$$\tilde{V} = V^z \oplus (V^z \times_{U^3} M).$$

Then  $\tilde{V}$  is also a holomorphic framed VOA of central charge 24 [28].

Note also that

$$V^{z} \times_{U^{3}} M = \left(\bigoplus_{[W]\in\mathcal{S}^{0}} W\right) \times_{U^{3}} M = \bigoplus_{[W]\in\mathcal{S}^{0}} (W \times_{U^{3}} M) = \bigoplus_{[W]\in(x,0,0)+\mathcal{S}^{0}} W.$$

Thus, we also have  $\tilde{V} = \bigoplus_{[W] \in \tilde{S}} W$ , where  $\tilde{S} = S^0 \cup ((x, 0, 0) + S^0)$ .

LEMMA 3.6. Let  $\tilde{V}$  be defined as in Notation 3.5.

(i)  $\dim(\tilde{V}_1) = 24$ .

(ii)  $\tilde{V}$  contains a subVOA isomorphic to  $(V_{EE_8})^3$ .

*Proof.* Let  $x \in \Phi \setminus \{0\}$  be as in Notation 3.1. Since  $V_1 = 0$ , we have  $(V^z)_1 = 0$  and thus  $\tilde{V}_1 < V^z \times_{U^3} M = \bigoplus_{[W] \in (x,0,0) + S^0} W$ . By the definition of S (Notation 2.15), we know that (0,0,0), (x,x,0),

By the definition of S (Notation 2.15), we know that (0,0,0), (x,x,0),  $(x,0,x) \in S^0$ . Thus, we have (x,0,0), (0,x,0), and (0,0,x) in  $(x,0,0) + S^0$  and they have minimal weight 1.

Now let (a + c, b + c, a + b + c),  $a, b \in \Phi$ ,  $c \in \Psi$ , be an element of  $S^0$ . If s = (x, 0, 0) + (a + c, b + c, a + b + c) = (x + a + c, b + c, a + b + c) has minimal weight 1, then at least one of the coordinates must be zero; otherwise, the minimal weight  $\geq \frac{3}{2}$ . Since  $\Phi \cap \Psi = 0$ , we have c = 0 and s = (x + a, b, a + b) for some  $a, b \in \Phi$ . Since x + a, a, and a + b are singular and s has minimal weight 1, only one coordinate is nonzero. Hence, (x, 0, 0), (0, x, 0), and (0, 0, x) are the only elements in  $(x, 0, 0) + S^0$  that have minimal weight 1. Moreover, by Proposition 2.14,  $\dim(A \otimes U \otimes U)_1 = \dim(U \otimes A \otimes U)_1 = \dim(U \otimes U \otimes A)_1 = 8$ . Hence, we have dim  $\tilde{V}_1 = 8 + 8 + 8 = 24$ .

Since Aut $(V_{EE_8}^+)$  acts transitively on nonzero singular vectors (by Proposition 2.14; see also [41]), we have  $V_{EE_8}^+ \oplus A \cong V_{EE_8}^+ \oplus V_{EE_8}^- = V_{EE_8}$ .

Now let  $\tilde{S}' = \text{span}\{(x, 0, 0), (0, x, 0), (0, 0, x)\} < \tilde{S}$ . Then  $\bigoplus_{[W] \in \tilde{S}'} W$  is isomorphic to  $(V_{EE_8})^3$  and thus  $\tilde{V}$  contains  $(V_{EE_8})^3$  as a subVOA.

As a direct consequence, we have the following result.

COROLLARY 3.7.  $\tilde{V} \cong V_{\Lambda}$  and  $V^z \cong V_{\Lambda}^+$  (see Definition 3.2 and Notation 3.5).

*Proof.* Since  $V_{EE_8^3} \cong (V_{EE_8})^3$  is a full subVOA of  $\tilde{V}, \tilde{V}$  is a direct sum of irreducible  $V_{EE_8^3}$ -modules. Thus, by [6], there exists an even lattice  $EE_8^3 < L < (EE_8^3)^*$  such that

$$\tilde{V} = \bigoplus_{\alpha + EE_8^3 \in L/(EE_8^3)} V_{\alpha + EE_8^3} = M(1) \otimes \mathbb{C}\{L\}.$$

Hence  $\tilde{V}$  is isomorphic to the lattice VOA  $V_L$  [29]. Note that  $V_{\alpha+EE_8^3}$ ,  $\alpha \in L/(EE_8^3)$ , are irreducible  $V_{EE_8^3}$ -modules and that  $\tilde{V}$  is a direct sum of simple current modules of  $V_{EE_8^3}$  [6]. Therefore,  $\tilde{V} \cong V_L$  also follows from the uniqueness of simple current extensions [14].

Recall that  $\dim(V_L)_1 = \operatorname{rank} L + |L(2)|$ , where  $L(2) = \{\alpha \in L \mid \langle \alpha, \alpha \rangle = 2\}$ [17]. Thus  $L(2) = \emptyset$  because rank L = 24 and  $\dim(\tilde{V}_1) = 24$ . Moreover, L is unimodular since  $\tilde{V}$  is holomorphic [6]. Since the Leech lattice is the only even unimodular lattice with no roots,  $L \cong \Lambda$  and  $\tilde{V} \cong V_{\Lambda}$ .

Recall that  $\tilde{V} = V^z \oplus (V^z \times_{U^3} M)$  (Notation 3.5). We define an automorphism g on  $\tilde{V}$  by

$$g = \begin{cases} 1 & \text{on } V^z, \\ -1 & \text{on } V^z \times_{U^3} M. \end{cases}$$

Since  $V_1 = 0$ , we have  $V_1^z = 0$  and  $\tilde{V}_1 \subset V^z \times_{U^3} M$ . Therefore, g acts as -1 on  $\tilde{V}_1$  and thus it is conjugate to the automorphism  $\theta$ , a lift of the (-1)-isometry of  $\Lambda$  by [9]. Hence, we have  $V^z = \tilde{V}_{\Lambda}^g \cong V_{\Lambda}^+$  as desired.

Let  $V^-$  be the (-1)-eigenspace of z in V. Then  $V^- = \bigoplus_{[W] \in S^1} W$  is a direct sum of simple current modules of  $U^3$ . Since z acts trivially on  $U^3$ ,  $U^3 \subset V^z$ . Hence, by [32, Thm. 5.4], for any irreducible  $V^z$ -module X we have

$$\sum_{W} N_{V^- X}^W \le 1,$$

where W runs through all isomorphism types of irreducible  $V^z$ -modules. Moreover,  $V^- \times_{V^z} X \neq 0$  since  $V^z$  is rational. Thus  $V^-$  is also a simple current module of  $V^z$ .

Thus, by Theorem 2.11, we have the following.

**THEOREM 3.8.** Let z be defined as in Definition 3.2. Then we have an exact sequence

$$1 \to \langle z \rangle \to C_{\operatorname{Aut}(V)}(z) \xrightarrow{\eta} \operatorname{Aut}(V^z) \to 1$$

and  $C_{\text{Aut}(V)}(z)$  has the shape  $2 \cdot 2^{24} \text{Co}_1$ .

*Proof.* Let *N* be an irreducible  $V^z$ -module. Since *V* is a framed VOA, it follows from [28, Thm. 1] that the  $V^z$ -module  $V \times_{V^z} N$  has a structure of an irreducible *V*-module or an irreducible *z*-twisted *V*-module.

Thus, every irreducible module of  $V^z$  can be embedded into V or the unique irreducible *z*-twisted module of V. Note that V is holomorphic. Therefore, it has only one irreducible module, namely V and a unique *z*-twisted module, up to isomorphisms [12].

Note that  $V = V^z \oplus V^-$  and  $V \times_{U^3} M = (V^z \times_{U^3} M) \oplus (V^- \times_{U^3} M)$  is the unique *z*-twisted module [28], where *M* is defined as in Notation 3.5. Thus,  $V^z$  has exactly four inequivalent irreducible modules—namely,  $V^z$ ,  $V^-$ ,  $V^z \times_{U^3} M$ , and  $V^- \times_{U^3} M$ . Since  $V_1 = 0$ , it is clear that the minimal weight of  $V^z$  and  $V^-$  are 0 and 2, respectively. On the other hand, the minimal weight of  $V^z \times_{U^3} M$  is 1 and the weights of  $V^- \times_{U^3} M$  are in  $\frac{1}{2} + \mathbb{Z}$ . Thus,  $g \circ V^- \cong V^-$  for all  $g \in \operatorname{Aut}(V^z)$  since  $g \circ V^-$  and  $V^-$  have the same characters. The theorem now follows from Theorem 2.11 and the fact that  $\operatorname{Aut}(V_{\Lambda}^+) \cong 2^{24}\operatorname{Co}_1$  [39].

NOTATION 3.9. The group *C* is the group that is in the middle of the short exact sequence of Theorem 3.8. It has the shape  $2^{1+24}$ Co<sub>1</sub>. (There are two 2-constrained groups of the shape  $2^{1+24}$ Co<sub>1</sub> [19].)

REMARK 3.10. Recall from [7] that  $V_{\Lambda}^+$  has exactly four inequivalent irreducible modules—namely,  $V_{\Lambda}^+$ ,  $V_{\Lambda}^-$ ,  $V_{\Lambda}^{T,+}$  and  $V_{\Lambda}^{T,-}$ —and that their minimal weights are 0, 1, 2, and  $\frac{3}{2}$ , respectively. Since  $V^z \cong V_{\Lambda}^+$  and  $V_1 = 0$ , it is easy to see that  $V = V^z \oplus V^- \cong V_{\Lambda}^+ \oplus V_{\Lambda}^{T,+}$  as a  $V_{\Lambda}^+$ -module.

We can furthermore say that V is isomorphic to the Frenkel–Lepowsky–Meurman Moonshine VOA  $V^{\ddagger}$ , by the uniqueness of simple current extensions [14; 24] or by use of [27] or [10] since V is framed. If we wish to avoid quoting these results, then after we prove Theorem 4.25, we can claim the more modest result that V has Moonshine type.

3.1. Conformal Vectors of Central Charge  $\frac{1}{2}$ 

NOTATION 3.11. We shall use  $\operatorname{cvcc} \frac{1}{2}$  to mean simple conformal vectors of central charge  $\frac{1}{2}$ .

DEFINITION 3.12. For any  $\alpha \in \Lambda(4)$ , define

$$\omega^{\pm}(\alpha) = \frac{1}{16}\alpha(-1)^2 \cdot \mathbf{1} \pm \frac{1}{4}(e^{\alpha} + e^{-\alpha}).$$

Then  $\omega^{\pm}(\alpha)$  are  $\operatorname{cvcc}_{\frac{1}{2}}^{\frac{1}{2}}$  and we call them  $\operatorname{cvcc}_{\frac{1}{2}}^{\frac{1}{2}}$  of  $AA_1$ -type.

Since  $V^z \cong V_{\Lambda}^+$ , all  $\operatorname{cvcc} \frac{1}{2}$  in the VOA  $V^z$  are classified in [26]. There are exactly two classes of  $\operatorname{cvcc} \frac{1}{2}$ ,  $AA_1$ -type and  $EE_8$ -type, up to the conjugacy of  $\operatorname{Aut}(V_{\Lambda}^+)$ . Since  $\Lambda$  is generated by norm-4 vectors, it can be shown by [26, Prop. 3.2] that Miyamoto involutions associated to  $AA_1$ -type  $\operatorname{cvcc} \frac{1}{2}$  generate a normal subgroup  $H_{\Lambda} \cong \operatorname{Hom}(\Lambda/2\Lambda, \mathbb{Z}_2) \cong 2^{24}$  in  $V_{\Lambda}^+$ .

NOTATION 3.13. Let  $H_{\Lambda}$  be the normal subgroup generated by  $AA_1$ -type Miyamoto involution in  $V_{\Lambda}^+$ .

Next we shall show that  $\eta^{-1}(H_{\Lambda})$  is an extra-special group of order 2<sup>25</sup>. The following lemma can be proved easily by direct calculation.

LEMMA 3.14. Let  $\omega^{\varepsilon_1}(\alpha)$  and  $\omega^{\varepsilon_2}(\beta)$  be  $AA_1$ -type  $\operatorname{cvcc} \frac{1}{2}$  in  $V_{\Lambda}^+$ , where  $\alpha, \beta \in \Lambda(4)$ . Then

$$\langle \omega^{\varepsilon_1}(\alpha), \omega^{\varepsilon_2}(\beta) \rangle = \begin{cases} rac{1}{2^7} (\langle \alpha, \beta \rangle)^2 & \text{if } lpha \neq \pm eta, \ rac{1}{4} \delta_{\varepsilon_1, \varepsilon_2} & \text{if } lpha = \pm eta. \end{cases}$$

NOTATION 3.15. For a  $\operatorname{cvcc}_{\frac{1}{2}} e$ , we denote by t(e) the associated Miyamoto involution [30].

By Lemma 3.14 and Sakuma's theorem [36], we know that  $t(\omega^{\varepsilon_1}(\alpha))$  commutes with  $t(\omega^{\varepsilon_2}(\beta))$  unless  $\langle \alpha, \beta \rangle = \pm 1$ .

LEMMA 3.16. Let  $\omega^{\varepsilon_1}(\alpha)$  and  $\omega^{\varepsilon_2}(\beta)$  be  $AA_1$ -type  $\operatorname{cvcc}\frac{1}{2}$  in  $V_{\Lambda}^+$ , where  $\alpha, \beta \in \Lambda(4)$ . Then, as automorphisms of V,

$$(t(\omega^{\varepsilon_1}(\alpha))t(\omega^{\varepsilon_2}(\beta)))^2 = \begin{cases} 1 & \text{if } \langle \alpha, \beta \rangle \text{ is even,} \\ z & \text{if } \langle \alpha, \beta \rangle = \pm 1. \end{cases}$$

*Note that*  $\langle \alpha, \beta \rangle \neq \pm 3$  *since*  $\Lambda$  *has no roots.* 

*Proof.* Since 
$$t(\omega^{\varepsilon_1}(\alpha))t(\omega^{\varepsilon_2}(\beta))t(\omega^{\varepsilon_1}(\alpha)) = t(t(\omega^{\varepsilon_1}(\alpha))\omega^{\varepsilon_2}(\beta))$$
, we have  
 $t(\omega^{\varepsilon_1}(\alpha))t(\omega^{\varepsilon_2}(\beta))t(\omega^{\varepsilon_1}(\alpha)) = \begin{cases} t(\omega^{-\varepsilon_2}(\beta)) & \text{if } \langle \alpha, \beta \rangle = \pm 1, \\ t(\omega^{\varepsilon_2}(\beta)) & \text{if } \langle \alpha, \beta \rangle \text{ is even.} \end{cases}$ 

Thus, we have  $(t(\omega^{\varepsilon_1}(\alpha))t(\omega^{\varepsilon_2}(\beta)))^2 = t(\omega^{-\varepsilon_2}(\beta))t(\omega^{\varepsilon_2}(\beta)) = z$  by [26, Lemma 5.14] if  $\langle \alpha, \beta \rangle = \pm 1$  and  $(t(\omega^{\varepsilon_1}(\alpha))t(\omega^{\varepsilon_2}(\beta)))^2 = 1$  if  $\langle \alpha, \beta \rangle$  is even.

As a corollary, we have the following statement.

THEOREM 3.17. The Miyamoto involutions  $\{t(\omega^{\pm}(\alpha)) \mid \alpha \in \Lambda(4)\}$  generate a subgroup isomorphic to  $2^{1+24}$  in Aut(V) and thus  $C_{Aut(V)}(z) \cong 2^{1+24} \text{Co}_1$ .

*Proof.* First we note that  $\Lambda$  is generated by norm-4 vectors. Moreover,  $\Lambda/2\Lambda$  forms a nondegenerate quadratic space over  $\mathbb{Z}_2$  that has the quadratic form  $q(\alpha + 2\Lambda) = \frac{1}{2} \langle \alpha, \alpha \rangle \mod 2$ .

Let *T* be the subgroup of Aut(*V*) generated by  $AA_1$ -type Miyamoto involutions. Then the restriction map  $\eta$  induces a group homomorphism  $\eta: T \to H_{\Lambda}$  (3.13) and we have an exact sequence

$$1 \to \langle z \rangle \to T \xrightarrow{\eta} H_{\Lambda} \cong \operatorname{Hom}(\Lambda/2\Lambda, \mathbb{Z}_2) \to 1.$$

Recall that  $H_{\Lambda}$  is generated by  $AA_1$ -type Miyamoto involutions in Aut $(V_{\Lambda}^+)$  (see Notation 3.13). Moreover, by Lemma 3.16, we have

$$[t(\omega^{\varepsilon_1}(\alpha)), t(\omega^{\varepsilon_2}(\beta))] = z^{\langle \alpha, \beta \rangle}$$

and thus  $T = \eta^{-1}(H_{\Lambda}) \cong 2^{1+24}$ . Note that  $z = t(\omega^{+}(\alpha))t(\omega^{-}(\alpha)) \in T$ .

REMARK 3.18. Let  $\omega^{\varepsilon}(\alpha)$  be an  $AA_1$ -type  $\operatorname{cvcc}_{\frac{1}{2}}$  in  $V_{\Lambda}^+ < V_{\Lambda}$ . Then we may also consider  $t(\omega^{\varepsilon}(\alpha))$  as an automorphism of  $V_{\Lambda}$ . In this case,  $t(\omega^{\varepsilon}(\alpha))$  acts trivially on the Heisenberg part M(1) and thus acts trivially on  $(V_{\Lambda})_1$  [26].

Recall Notation 3.13 and Theorem 3.17. Let  $\tilde{H}_{\Lambda} < \operatorname{Aut}(V_{\Lambda})$  be the group generated by  $\{t(\omega^{\pm}(\alpha)) \mid \alpha \in \Lambda(4)\}$ . Then  $\tilde{H}_{\Lambda} \cong \operatorname{Hom}(\Lambda, \mathbb{Z}_2) \cong 2^{24}$  and the restriction map

$$g \in H_{\Lambda} \to g|_{V_{\Lambda}^+} \in H_{\Lambda} < \operatorname{Aut}(V_{\Lambda}^+)$$

is an isomorphism from  $\tilde{H}_{\Lambda}$  to  $H_{\Lambda}$  [26]. By the foregoing discussion,  $\tilde{H}_{\Lambda}$  acts trivially on  $(V_{\Lambda})_1$ .

# **4.** Analysis of the Finite Group Aut(*V*)

In Section 4.1 we prove that Aut(V) is finite. This involves a discussion of framed VOAs over both the real and complex field. Our approach is essentially the same as

Miyamoto [35] but with simplifications and generalizations. In particular, Proposition 4.14 is new. Then, in Section 4.2, we use finite group theory to complete our analysis of Aut(V).

#### 4.1. Framed VOA over $\mathbb{R}$

First, we recall some facts about framed VOA over  $\mathbb{R}$  from [34; 35].

NOTATION 4.1. Let  $\operatorname{Vir}_{\mathbb{R}} = \bigoplus_{n \in \mathbb{Z}} \mathbb{R}L_n \oplus \mathbb{R}\mathbf{c}$  be the Virasoro algebra over  $\mathbb{R}$ . For  $c, h \in \mathbb{R}$ , let  $L(c, h)_{\mathbb{R}}$  be the irreducible highest-weight module of  $\operatorname{Vir}_{\mathbb{R}}$  of highest weight *h* and central charge *c* over  $\mathbb{R}$ .

The following results can be found in [35].

PROPOSITION 4.2 [35, Cor. 2.2, Cor. 2.3, Thm. 2.4].  $L(\frac{1}{2}, 0)_{\mathbb{R}}$  is a rational VOA; that is, all  $L(\frac{1}{2}, 0)_{\mathbb{R}}$ -modules are completely reducible. Moreover,  $L(\frac{1}{2}, 0)_{\mathbb{R}}$  has only three inequivalent irreducible modules (namely,  $L(\frac{1}{2}, 0)_{\mathbb{R}}$ ,  $L(\frac{1}{2}, \frac{1}{2})_{\mathbb{R}}$ , and  $L(\frac{1}{2}, \frac{1}{16})_{\mathbb{R}}$ ) and  $L(\frac{1}{2}, h) \cong \mathbb{C} \otimes L(\frac{1}{2}, h)_{\mathbb{R}}$  for all h = 0, 1/2, or 1/16.

LEMMA 4.3 [35, Lemma 2.5]. Let W be a VOA over  $\mathbb{R}$  and let  $M^1$ ,  $M^2$ ,  $M^3$  be W-modules. Then

$$\dim\left(I_W\binom{M^3}{M^1 M^2}\right) \leq \dim\left(I_{\mathbb{C}\otimes W}\binom{\mathbb{C}\otimes M^3}{\mathbb{C}\otimes M^1 \mathbb{C}\otimes M^2}\right)$$

PROPOSITION 4.4 (cf. [35, (2.5), (2.6)]). For  $h_1, h_2, h_3 \in \{0, 1/2, 1/16\}$ , we have

$$\dim \left( I_{L(\frac{1}{2},0)_{\mathbb{R}}} \begin{pmatrix} L(\frac{1}{2},h_3)_{\mathbb{R}} \\ L(\frac{1}{2},h_1)_{\mathbb{R}} & L(\frac{1}{2},h_2)_{\mathbb{R}} \end{pmatrix} \right) = \dim \left( I_{L(\frac{1}{2},0)} \begin{pmatrix} L(\frac{1}{2},h_3) \\ L(\frac{1}{2},h_1) & L(\frac{1}{2},h_2) \end{pmatrix} \right).$$

In particular, the fusion rules for  $L(\frac{1}{2},0)_{\mathbb{R}}$  over  $\mathbb{R}$  are exactly the same as the fusion rules for  $L(\frac{1}{2},0)$  over  $\mathbb{C}$ .

DEFINITION 4.5. A simple VOA *W* over  $\mathbb{R}$  is *framed* if it contains a full subVOA *T* isomorphic to  $L(\frac{1}{2}, 0)_{\mathbb{P}}^{n}$ .

NOTATION 4.6. For any  $\alpha = (\alpha_1, ..., \alpha_n) \in \{0, 1\}^n$  and an even binary linear code *E*, we define  $M_{\mathbb{R}}^{\alpha} = \bigotimes_{i=1}^n L(\frac{1}{2}, \frac{\alpha_i}{2})_{\mathbb{R}}$  and  $M_{E,\mathbb{R}} = \bigoplus_{\alpha \in E} M_{\mathbb{R}}^{\alpha}$ .

Unlike the complex case, a simple current extension over  $\mathbb{R}$  is no longer unique and there is more than one VOA structure on  $M_{E,\mathbb{R}}$  (see e.g. [35]). Nevertheless, the following propositions hold.

**PROPOSITION 4.7** [35, Prop. 3.5]. Let *E* be an even linear binary code. Then  $M_{E,\mathbb{R}}$  has a unique VOA structure over  $\mathbb{R}$  such that the invariant form on  $M_{E,\mathbb{R}}$  is positive definite.

**PROPOSITION 4.8.** Let W be a framed VOA over  $\mathbb{R}$  such that its invariant form is positive definite. Then there exist two binary codes E and D such that  $D < E^{\perp}$  and

$$W = \bigoplus_{\beta \in D} W^{\beta},$$

where  $W^0 \cong M_{E,\mathbb{R}}$  and, for each  $\beta \in D$ ,  $W^\beta$  is an irreducible  $M_E$ -module with the 1/16-word  $\beta$ . The 1/16-word for an irreducible  $M_{E,\mathbb{R}}$ -module is defined as in the complex case [33].

COROLLARY 4.9. Let W be a framed VOA over  $\mathbb{R}$  such that its invariant form is positive definite. Then W is finitely generated as a VOA.

*Proof.* By Proposition 4.8, W contains a subVOA  $W^0 \cong M_{E,\mathbb{R}}$  and W is a direct sum of finitely many irreducible  $W^0$ -modules.

It is clear that  $M^0 = \bigotimes_{i=1}^n L(\frac{1}{2}, 0)_{\mathbb{R}}$  is generated by  $n \operatorname{cvcc} \frac{1}{2}$ . Since  $W^0 \cong M_{E,\mathbb{R}}$  is direct sum of finitely many irreducible  $M^0$ -modules,  $W^0$  is finitely generated. Moreover, W is a direct sum of finitely many  $W^0$ -irreducible modules. Hence W is finitely generated.

NOTATION 4.10. Let *W* be a framed VOA with a positive definite invariant form over  $\mathbb{R}$  and let  $T \cong L(\frac{1}{2}, 0)_{\mathbb{R}}^n$  be a Virasoro frame. Denote

$$\operatorname{Stab}_{\operatorname{Aut}(W)}(T) = \{g \in \operatorname{Aut}(W) \mid g(T) = T\},$$
  
$$\operatorname{Stab}_{\operatorname{Aut}(W)}^{\operatorname{pt}}(T) = \{g \in \operatorname{Aut}(W) \mid g(v) = v \text{ for all } v \in T\}.$$

Since  $L(\frac{1}{2}, 0)$  and  $L(\frac{1}{2}, 0)_{\mathbb{R}}$  have the same fusion rules, the following can be proved by the same argument as in the complex case.

**PROPOSITION 4.11** [9; 28]. Let W be a framed VOA with a positive definite invariant form over  $\mathbb{R}$ . Then:

- (i)  $\operatorname{Stab}_{\operatorname{Aut}(W)}^{\operatorname{pt}}(T)$  is a finite 2-group;
- (ii)  $\operatorname{Stab}_{\operatorname{Aut}(W)}^{\operatorname{pt}}(T)$  is normal in  $\operatorname{Stab}_{\operatorname{Aut}(W)}(T)$ , and  $\operatorname{Stab}_{\operatorname{Aut}(W)}(T)/\operatorname{Stab}_{\operatorname{Aut}(W)}^{\operatorname{pt}}(T)$  is isomorphic to a subgroup of  $\operatorname{Aut}(D)$ .

In particular,  $Stab_{Aut(W)}(T)$  is a finite group.

LEMMA 4.12 [33, Thm. 5.1]. Let W be a CFT-type VOA over  $\mathbb{R}$ . Suppose  $W_1 = 0$  and the invariant form on W is positive definite. Then, for any pair of distinct  $\operatorname{cvcc} \frac{1}{2} e$  and f in W, we have

$$0 \le \langle e, f \rangle \le \frac{1}{12}.$$

In particular, W has only finitely many  $\operatorname{cvcc} \frac{1}{2}$ .

**PROPOSITION 4.13** (cf. [35]). Let W be a framed VOA over  $\mathbb{R}$ . Suppose the invariant form on W is positive definite and  $W_1 = 0$ . Then Aut(W) is a finite group.

*Proof.* By Lemma 4.12, W has only finitely many  $\operatorname{cvcc} \frac{1}{2}$  and thus W has only finitely many Virasoro frames. By Proposition 4.11 (see also [9]), the stabilizer of a Virasoro frame is a finite group. Hence  $\operatorname{Aut}(W)$  is finite.

**PROPOSITION 4.14.** Let W be a finitely generated VOA over  $\mathbb{R}$ . Suppose that Aut(W) is finite. Then  $Aut(\mathbb{C} \otimes_{\mathbb{R}} W)$  is a finite group.

*Proof.* In this proof,  $\otimes$  means  $\otimes_{\mathbb{R}}$ . There is a semilinear automorphism, denoted  $\gamma$ , on  $\mathbb{C} \otimes W$  that fixes  $\mathbb{R} \otimes W$  and is -1 on  $\mathbb{R}\sqrt{-1} \otimes W$ .

From [8], Aut( $\mathbb{C} \otimes W$ ) is a finite-dimensional algebraic group, and the fixed point subgroup for the action of  $\gamma$  on it is finite by Proposition 4.13. Its corresponding action on  $\text{Der}_{\mathbb{C}}(\mathbb{C} \otimes W)$ , the complex Lie algebra of derivations, is therefore fixed point free and so the action is -1. In fact, we note that the (-1)-eigenspace of  $\gamma$  on  $\text{End}_{\mathbb{C}}(\mathbb{C} \otimes W)$  may be identified with the real subspace  $\mathbb{R}\sqrt{-1} \otimes \text{End}(W)$ of  $\mathbb{C} \otimes \text{End}(W) \cong \text{End}_{\mathbb{C}}(\mathbb{C} \otimes W)$ . Since this real subspace contains no nontrivial complex subspaces, we conclude that  $\text{Der}_{\mathbb{C}}(\mathbb{C} \otimes W) = 0$ . It follows that the algebraic group  $\text{Aut}(\mathbb{C} \otimes W)$  is 0-dimensional and therefore is finite.  $\Box$ 

COROLLARY 4.15. Suppose that W is a framed VOA over  $\mathbb{R}$ ,  $W_1 = 0$ , and the invariant form on W is positive definite. Then  $\operatorname{Aut}(\mathbb{C} \otimes_{\mathbb{R}} W)$  is a finite group.

*Proof.* This follows from Propositions 4.13 and 4.14.

DEFINITION 4.16. A *real form* of a complex VOA V is a real subspace W that is closed under the VOA operations and such that a real basis for W is a complex basis for V. Given a real form W of V, a real form of a V-module M is a real subspace N that is closed under action by W and such that a real basis for N is a complex basis for M. We say that N is a real form of M with respect to the real form W of V.

Next we shall show that the VOA V constructed in Theorem 2.18 has a real form with a positive definite invariant form.

First we recall that the lattice VOA constructed in [17] can be defined over  $\mathbb{R}$ . Let  $V_{L,\mathbb{R}} = S(\hat{H}_{\mathbb{R}}^{-}) \otimes \mathbb{R}\{L\}$  be the real-lattice VOA associated to an even positive definite lattice, where  $H = \mathbb{R} \otimes_{\mathbb{Z}} L$  and  $\hat{H}^{-} = \bigoplus_{n \in \mathbb{Z}^{+}} H \otimes \mathbb{R}t^{-n}$ . As usual, we use x(-n) to denote  $x \otimes t^{-n}$  for  $x \in H$  and  $n \in \mathbb{Z}^{+}$ .

NOTATION 4.17. Let  $\theta: V_{L,\mathbb{R}} \to V_{L,\mathbb{R}}$  be defined by

$$\theta(x(-n_1)\cdots x(-n_k)\otimes e^{\alpha})=(-1)^k x(-n_1)\cdots x(-n_k)\otimes e^{-\alpha}.$$

Then  $\theta$  is an automorphism of  $V_{L,\mathbb{R}}$ , which is a lift of the (-1)-isometry of L [17]. We shall denote the  $(\pm 1)$ -eigenspaces of  $\theta$  on  $V_{L,\mathbb{R}}$  by  $V_{L,\mathbb{R}}^{\pm}$ .

The following result is well known [17; 35].

PROPOSITION 4.18 (cf. [35, Prop. 2.7]). Let L be an even positive definite lattice. Then the real subspace  $\tilde{V}_{L,\mathbb{R}} = V_{L,\mathbb{R}}^+ \oplus \sqrt{-1}V_{L,\mathbb{R}}^-$  is a real form of  $V_L$ . Furthermore, the invariant form on  $\tilde{V}_{L,\mathbb{R}}$  is positive definite.

NOTATION 4.19. Let  $U_{\mathbb{R}} = V_{EE_8,\mathbb{R}}^+$  be a real form of U. Since all  $\operatorname{cvcc} \frac{1}{2}$  in U are contained in  $V_{EE_8,\mathbb{R}}^+$  [15; 22],  $U_{\mathbb{R}}$  is a real framed VOA. In fact,  $U_{\mathbb{R}} \cong M_{\mathrm{RM}(2,4),\mathbb{R}}$  (see Notation 4.6) since  $V_{EE_8}^+ \cong M_{\mathrm{RM}(2,4)}$ , where  $\mathrm{RM}(2,4)$  is the second-order Reed–Muller code of degree 4.

LEMMA 4.20 [35, Lemma 3.10]. Let *E* be an even binary code. Let *X* be an irreducible  $M_{E,\mathbb{R}}$ -module. Then  $\mathbb{C} \otimes X$  is an irreducible  $M_E$ -module.

LEMMA 4.21. Let M be an irreducible module of U over  $\mathbb{C}$ . Suppose  $[M] \in R(U)$  is a nonzero singular element. Then M has a positive definite real form.

*Proof.* Since Aut $(V_{EE_8}^+)$  acts transitively on nonzero singular vectors (Proposition 2.14; see also [41]), there is a  $g \in Aut(U)$  such that  $M \cong g \circ V_{EE_8}^-$ . Recall from [22] that Aut(U) is generated by  $\sigma$ -involutions associated to  $\operatorname{cvcc}_2^1$  and that all  $\operatorname{cvcc}_2^1 \in U$  are contained in  $U_{\mathbb{R}}$ . Therefore, g keeps  $U_{\mathbb{R}}$  invariant and also defines an automorphism on  $U_{\mathbb{R}}$ .

By Proposition 4.18, the invariant form on  $\tilde{V}_{EE_8,\mathbb{R}} = U_{\mathbb{R}} \oplus (\mathbb{R}\sqrt{-1} \otimes V_{EE_8,\mathbb{R}})$  is positive definite. Set  $W = \mathbb{R}\sqrt{-1} \otimes V_{EE_8,\mathbb{R}}$ . Then  $U_{\mathbb{R}} \oplus (g \circ W) \cong \tilde{V}_{EE_8,\mathbb{R}}$  also has a positive definite invariant form. Moreover,  $\mathbb{C} \otimes (g \circ W) \cong g \circ V_{EE_8}^- \cong M$ . Thus,  $g \circ W$  is a positive definite real form of M.

NOTATION 4.22. Let  $\Phi$ ,  $\Psi$ , and S be as in Notation 2.15. Then

$$\mathcal{V}(\Phi) = \bigoplus_{[M] \in \Phi} M \cong V_{E_8}.$$

By Proposition 4.18,  $\mathcal{V}(\Phi)$  has a positive definite real form  $W \cong \tilde{V}_{E_8,\mathbb{R}}$ . Then W is a direct sum of irreducible  $U_{\mathbb{R}}$ -modules. Let X be an irreducible  $U_{\mathbb{R}}$ -submodule of W. Then,  $\mathbb{C} \otimes X$  is an irreducible U-module by Lemma 4.20. Since  $\mathbb{C} \otimes W =$  $\mathcal{V}(\Phi)$ ,  $[\mathbb{C} \otimes X] = a$  for some  $a \in \Phi$ . Hence, for each  $a \in \Phi$ , there exists a real  $U_{\mathbb{R}}$ module  $M^a$  such that  $a = [\mathbb{C} \otimes M^a]$  and  $\bigoplus_{a \in \Phi} M^a \cong \tilde{V}_{E_8,\mathbb{R}}$ . Similarly, for each  $b \in \Psi$ , there exists a real submodule  $N^b$  such that  $b = [\mathbb{C} \otimes W^b]$  and  $\bigoplus_{a \in \Psi} N^b \cong$  $\tilde{V}_{E_8,\mathbb{R}}$ .

Recall that a general element in S has the form (a + b + c, a + c, b + c) for some  $a, b \in \Phi$  and  $c \in \Psi$  (cf. Notation 2.15 and Lemma 2.17). For any  $s = (a + b + c, a + c, b + c) \in S$ , we define

$$W^{s} := (M^{a+b} \times_{U_{\mathbb{R}}} N^{c}) \otimes (M^{a} \times_{U_{\mathbb{R}}} N^{c}) \otimes (M^{b} \times_{U_{\mathbb{R}}} N^{c})$$

as a  $(U_{\mathbb{R}})^3$ -module. Note that  $W^0 \cong (U_{\mathbb{R}})^3$ .

THEOREM 4.23. Let V be the framed VOA constructed in Theorem 2.18. Then V has a real form W such that the invariant form on W is positive definite and W is framed. Thus, Aut(V) is finite by Corollary 4.15.

*Proof.* Let  $W^s$ ,  $s \in S$ , be defined as in Notation 4.22. We shall show that  $W = \bigoplus_{s \in S} W^s$  has a real VOA structure such that the invariant form on W is positive definite.

By Lemma 4.3, we know that all  $W^s$ ,  $s \in S$ , are simple current modules of  $(U_{\mathbb{R}})^3$ . Thus, by [35, Thm. 5.25], it suffices to show  $\bigoplus_{s \in \mathcal{T}} W^s$  has a real VOA structure with a positive definite invariant form for any 2-dimensional subspace  $\mathcal{T}$  of S.

Let (a + b + c, a + c, b + c) and (a' + b' + c', a' + c', b' + c') be a basis of  $\mathcal{T}$ , where  $a, b, a', b' \in \Phi$  and  $c, c' \in \Psi$ . Take  $0 \neq x \in \Phi$  such that x is orthogonal to c, c'. Then as in Definition 3.2, we define z' on W by ROBERT L. GRIESS JR. & CHING HUNG LAM

$$z' = \begin{cases} 1 & \text{on } W^s \text{ if } \langle s, (x, 0, 0) \rangle = 0, \\ -1 & \text{on } W^s \text{ if } \langle s, (x, 0, 0) \rangle = 1. \end{cases}$$

Then, by the same argument as in Corollary 3.7, one can show that the fixed point subspace  $W^z$  can be embedded into  $V_{\Lambda,\mathbb{R}}^+$ , which has a real VOA structure with a positive definite invariant form.

Since  $\mathcal{T}$  is orthogonal to (x, 0, 0), we have  $\bigoplus_{s \in \mathcal{T}} W^s < W^z$  and  $\bigoplus_{s \in \mathcal{T}} W^s$  has a real VOA structure with a positive definite invariant form.

## 4.2. Aut(V) Is of Monster Type

**PROPOSITION 4.24.** Let *H* be a finite group containing an involution *z* such that  $C_H(z) \cong C$ , the group of Notation 3.9. Then:

(i) 
$$H = O_{2'}(H)C$$
; or

(ii) *H* is a simple group of order  $2^{46}3^{20}5^97^611^213^317 \cdot 19 \cdot 23 \cdot 39 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ .

*Proof* [46]. A similar conclusion was obtained in [42] under the additional assumption that z is conjugate in H to an element of  $O_2(C) \setminus \{z\}$ . That fusion assumption was verified in the situation of [21]. For completeness, we give a verification of this fusion result for  $H = \operatorname{Aut}(V)$  in the Appendix.

THEOREM 4.25. (i) Aut(V) is a finite simple group. (ii)  $|Aut(V)| = 2^{46}3^{20}5^97^611^213^317 \cdot 19 \cdot 23 \cdot 39 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$ 

*Proof.* By Theorem 4.23, Aut(V) is a finite group. By Theorem 3.8,  $C_{Aut(V)}(z) = C$ . By Proposition 2.22, C is a proper subgroup of Aut(V).

To prove (i), we quote Proposition 4.24 or [46]. Observe that the structure of the group in Proposition 2.22 shows that 31 divides the order of  $\operatorname{Aut}(V)/O_{2'}(\operatorname{Aut}(V))$ , whence the alternative (i) of Proposition 4.24 does not apply here.

 $\square$ 

For (ii), use Proposition 4.24 or [23].

REMARK 4.26. (i) So far, determinations of the group order still depend on [42] or [23].

(ii) Our VOA construction of the Monster has an easy proof of finiteness (see Lemma 4.12), whereas proof of finiteness in [21] was more troublesome. A short proof of finiteness, using the theory of algebraic groups, is given in [46].

COROLLARY 4.27. The VOA V (Notation 2.20), defined by Shimakura [41], is of Moonshine type (see the Introduction for the definition).

## **Appendix: A Fusion Result**

The following is relevant to the alternate argument for Proposition 4.24 and in fact proves more about fusion. It could be of some independent interest.

LEMMA A.1. The involution z is conjugate in Aut(V) to elements of  $O_2(C) \setminus \langle z \rangle$ and to elements of  $C \setminus O_2(C)$ .

*Proof.* We see this by examination of the group in Proposition 2.22.

Let  $x \in \Phi$ ,  $S^0$ ,  $S^1$ , and  $z \in Aut(V)$  be defined as in Notation 3.1 and Definition 3.2. Without loss of generality, we may assume  $x = [V_{EE_x}^-]$ .

570

Recall the bilinear form on R(U) from [39] for which

$$\langle [V_{\alpha/2+EE_8}^{\pm}], [V_{\beta/2+EE_8}^{\pm}] \rangle = \left\langle \alpha, \frac{\beta}{2} \right\rangle \mod 2,$$

$$\langle [V_{EE_8}^{-}], [(V_{EE_8}^{T_{\chi}})^{\pm}] \rangle = 1,$$
(4)

where  $\alpha, \beta \in EE_8$  and  $V_{EE_8}^{T_{\chi}}$  is an irreducible twisted module  $V_{EE_8}$  for some character  $\chi$  of  $EE_8^*/EE_8$ .

Let  $p_1: R(U)^3 \to R(U)$  be the natural projection to the first component. Then, for any  $s \in S^0$ ,  $\langle p_1(s), x \rangle = 0$  and by (4) we have  $p_1(s) = [V_{\beta/2 + EE_8}^{\varepsilon}]$  for some  $\beta \in EE_8$ .

Let  $x' \in \Phi$  with  $x' \neq x$ . Then, as in (3.2), we can define an automorphism z' by

$$z' = \begin{cases} 1 & \text{on } W \text{ if } [W] \in \mathcal{S}, \langle [W], (x', 0, 0) \rangle = 0, \\ -1 & \text{on } W \text{ if } [W] \in \mathcal{S}, \langle [W], (x', 0, 0) \rangle = 1. \end{cases}$$

Again we may assume  $x' = [V_{\alpha/2+EE_8}^{\varepsilon}]$  for some  $\alpha \in EE_8$  and  $\varepsilon = +$  or -. Then z' acts on  $V^z = \bigoplus_{[W] \in S^0} W$ , and by (4) we have

$$z'|_{V^z} = (-1)^{\langle \alpha, \beta/2 \rangle}$$
 on W with  $p_1([W]) = [V^{\pm}_{\beta/2 + EE_8}]$ .

Thus,  $z'|_{V^z} \in H_{\Lambda}$  and  $z' \in O_2(C)$ , where  $H_{\Lambda}$  is defined as in Notation 3.13.

By the same argument as in Lemma 3.6 and Corollary 3.7, we also have  $V^{z'} \cong V_{\Lambda}^+$ . Thus, by the uniqueness of simple current extensions, there exists an automorphism g that maps  $V^z$  to  $V^{z'}$  and hence  $z' = gzg^{-1}$ .

Next we shall show that *z* is conjugate to an element in  $C \setminus O_2(C)$ . Let  $y \in \Psi$  such that  $\langle x, y \rangle = 1$ . Define  $z_y$  by

$$z_{y} = \begin{cases} 1 & \text{on } W \text{ if } [W] \in \mathcal{S}, \ \langle [W], (y, 0, 0) \rangle = 0, \\ -1 & \text{on } W \text{ if } [W] \in \mathcal{S}, \ \langle [W], (y, 0, 0) \rangle = 1. \end{cases}$$

Then we again have  $V^{z_y} \cong V_{\Lambda}^+$  and  $z_y$  is conjugate to z in Aut(V). Note that  $z_y$  also acts on  $\tilde{V} = V^z \oplus (V^z \times_{U^3} M) \cong V_{\Lambda}$  (see Notation 3.5).

Since  $\langle x, y \rangle = 1$ , it follows that  $z_y$  acts as -1 on M and thus acts nontrivially on  $\tilde{V}_1$ . By Remark 3.18,  $z_y \notin \tilde{H}_{\Lambda}$  and thus  $z_y|_{V^z} \notin H_{\Lambda}$ . Therefore,  $z_y \in C \setminus O_2(C)$  as desired.

#### References

- J. H. Conway, A simple construction for the Fischer–Griess monster group, Invent. Math. 79 (1985), 513–540.
- [2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, Atlas of finite groups, Oxford Univ. Press, Oxford, 1985.
- [3] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Grundlehren Math. Wiss., 290, Springer-Verlag, New York, 1999.
- [4] L. Dolan, P. Goddard, and P. Montague, *Conformal field theory, triality and the Monster group*, Phys. Lett. B 236 (1990), 165–172.
- [5] —, Conformal field theory of twisted vertex operators, Nuclear Phys. B 338 (1990), 529–601.

- [6] C. Y. Dong, Vertex algebras associated with even lattices, J. Algebra 161 (1993), 245–265.
- [7] ——, Representations of the moonshine module vertex operator algebra, Mathematical aspects of conformal and topological field theories and quantum groups (South Hadley, 1992), Contemp. Math., 175, pp. 27–36, Amer. Math. Soc., Providence, RI, 1994.
- [8] C. Dong and R. L. Griess Jr., Automorphism groups and derivation algebras of finitely generated vertex operator algebras, Michigan Math. J. 50 (2002), 227–239.
- [9] C. Dong, R. L. Griess Jr., and G. Höhn, *Framed vertex operator algebras, codes and the moonshine module,* Comm. Math. Phys. 193 (1998), 407–448.
- [10] C. Dong, R. L. Griess Jr., and C. H. Lam, Uniqueness results for the moonshine vertex operator algebra, Amer. J. Math. 129 (2007), 583–609.
- [11] C. Dong, H. Li, and G. Mason, Simple currents and extensions of vertex operator algebras, Comm. Math. Phys. 180 (1996), 671–707.
- [12] ——, Modular-invariance of trace functions in orbifold theory and generalized moonshine, Comm. Math. Phys. 214 (2000), 1–56.
- [13] C. Dong and G. Mason, Nonabelian orbifolds and the boson-fermion correspondence, Comm. Math. Phys. 163 (1994), 523–559.
- [14] ——, Rational vertex operator algebras and the effective central charge, Int. Math. Res. Not. 56 (2004), 2989–3008.
- [15] C. Dong, G. Mason, and Y. Zhu, *Discrete series of the Virasoro algebra and the moonshine module*, Algebraic groups and their generalizations: Quantum and infinite-dimensional methods (University Park, 1991), Proc. Sympos. Pure Math., 56, part 2, pp. 295–316, Amer. Math. Soc., Providence, RI, 1994.
- [16] I. Frenkel, Y. Z. Huang, and J. Lepowsky, On axiomatic approaches to vertex operator algebras and modules, Mem. Amer. Math. Soc. 104, Amer. Math. Soc., Providence, RI, 1993.
- [17] I. Frenkel, J. Lepowsky, and A. Meurman, Vertex operator algebras and the Monster, Pure Appl. Math., 134, Academic Press, Boston, 1988.
- [18] J. Fuchs and D. Gepner, On the connection between WZW and free field theories, Nuclear Phys. B 294 (1998), 30–42.
- [19] R. L. Griess Jr., *The structure of the "Monster" simple group*, Proceedings of the conference on finite groups (Park City, 1975), pp. 113–118, Academic Press, New York, 1976.
- [20] —, A construction of  $F_1$  as automorphisms of a 196,883-dimensional algebra, Proc. Natl. Acad. Sci. USA 78 (1981), 689–691.
- [21] —, The friendly giant, Invent. Math. 69 (1982), 1–102.
- [22] —, A vertex operator algebra related to  $E_8$  with automorphism group  $O^+(10, 2)$ , The Monster and Lie algebras (Columbus, 1996), Ohio State Univ. Math. Res. Inst. Publ., 7, pp. 43–58, de Gruyter, Berlin, 1998.
- [23] R. L. Griess Jr., U. Meierfrankenfeld, and Y. Segev, A uniqueness proof for the Monster, Ann. of Math. (2) 130 (1989), 567–602.
- [24] Y. Z. Huang, A nonmeromorphic extension of the moonshine module vertex operator algebra, Moonshine, the Monster and related topics (South Hadley, 1994), Contemp. Math., 193, pp. 123–148, Amer. Math. Soc., Providence, RI, 1996.
- [25] A. A. Ivanov, *The Monster group and Majorana involutions*, Cambridge Tracts in Math., 176, Cambridge Univ. Press, Cambridge, 2009.
- [26] C. H. Lam and H. Shimakura, *Ising vectors in the vertex operator algebra*  $V_{\Lambda}^+$  *associated with the Leech lattice*  $\Lambda$ , Int. Math. Res. Not. 2007 (2007), no. 24.

- [27] C. H. Lam and H. Yamauchi, A characterization of the moonshine vertex operator algebra by means of Virasoro frames, Int. Math. Res. Not. 2007 (2007), no. 1.
- [28] ——, On the structure of framed vertex operator algebras and their pointwise frame stabilizers, Comm. Math. Phys. 277 (2008), 237–285.
- [29] H. S. Li, Extension of vertex operator algebras by a self-dual simple module, J. Algebra 187 (1997), 236–267.
- [30] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, J. Algebra 179 (1996), 523–548.
- [31] ——, Binary codes and vertex operator (super)algebras, J. Algebra 181 (1996), 207–222.
- [32] ——, *Representation theory of code vertex operator algebra*, J. Algebra 201 (1998), 115–150.
- [33] ——, The moonshine VOA and a tensor product of Ising models, The Monster and Lie algebras (Columbus, 1996), Ohio State Univ. Math. Res. Inst. Publ., 7, pp. 99–110, de Gruyter, Berlin, 1998.
- [34] —, 3-State Potts model and automorphisms of vertex operator algebras of order 3, J. Algebra 239 (2001), 56–76.
- [35] ——, *A new construction of the moonshine vertex operator algebra over the real field*, Ann. of Math. (2) 159 (2004), 535–596.
- [36] S. Sakuma, 6-Transposition property of  $\tau$ -involutions of vertex operator algebras, Int. Math. Res. Not. 2007 (2007), no. 9.
- [37] S. Sakuma and H. Yamauchi, Vertex operator algebra with two Miyamoto involutions generating S<sub>3</sub>, J. Algebra 267 (2003), 272–297.
- [38] A. N. Schellekens and S. Yankielowicz, *Extended chiral algebras and modular invariant partition functions*, Nuclear Phys. B 327 (1989), 673–703.
- [39] H. Shimakura, *The automorphism group of the vertex operator algebra*  $V_L^+$  *for an even lattice L without roots*, J. Algebra 280 (2004), 29–57.
- [40] ——, Lifts of automorphisms of vertex operator algebras in simple current extensions, Math. Z. 256 (2007), 491–508.
- [41] ——, An  $E_8$  approach to the moonshine vertex operator algebra, J. London Math. Soc. (2) 83 (2011), 493–516.
- [42] S. Smith, *Large extraspecial subgroups of widths 4 and 6*, J. Algebra 58 (1979), 251–281.
- [43] J. Tits, Résumé de cours, Annuaire du Collège de France, 1982/83, pp. 89-102.
- [44] ——, *Remarks on Griess' construction of the Griess–Fischer sporadic group, I, II, III, IV,* mimeographed letters, December 1982 – July 1983.
- [45] ——, Le Monstre (d'après R. Griess, B. Fischer et al.), Séminaire Bourbaki, 26, exp. no. 620, pp. 105–122.
- [46] —, On R. Griess' "friendly giant", Invent. Math. 78 (1984), 491–499.

R. L. Griess Jr. Department of Mathematics University of Michigan Ann Arbor, MI 48109

rlg@umich.edu

C. H. Lam Institute of Mathematics Academia Sinica Taipei 10617 Taiwan

chlam@math.sinica.edu.tw