My life and times with the sporadic simple groups[1]

slides version 15 May, 2020

Robert L. Griess Jr.
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1043 USA
rlg@umich.edu

[1] **Mathematical Science Literature lecture series, Harvard University, 1-3pm, 6 May, 2020**; these slides revise and correct the slides used for the lecture; apologies for errors; material will soon be expanded to a written article, with references; comments and questions are welcome, email rlg@umich.edu

Abstract

Five sporadic simple groups were proposed in 19th century and 21 additional ones arose during the period 1965-1975. There were many discussions about the nature of finite simple groups and how sporadic groups are placed in mathematics. While in mathematics graduate school at University of Chicago, I became fascinated with the unfolding story of sporadic simple groups. It involved theory, detective work and experiments. During this lecture, I will describe some of the people, important ideas and evolution of thinking about sporadic simple groups. Most should be accessible to a general mathematical audience.

Notations

In a group, $\langle S\rangle$ means the subgroup generated by the subset S.
order of a group is its cardinality;
order of a group element is the order of the cyclic group it generates;
involution is an element of order 2 in a group;
G' commutator subgroup of the group G; $Z(G)$ is the center of G;
classical groups are $GL(n,q), PSL(n,q), O^{\varepsilon}(n,q)\cdots$ (n refers to the dimension of the square matrices and q the cardinality of the finite field $\mathbb{F}_q$). For unitary groups and others which involve a degree 2 field extension, q denotes the ground field;
FSG means finite simple groups, CFSG means classification of FSG;

$C_G(S)$, $N_G(S)$ means the centralizer, normalizer (resp.) of S in G; direct product notation: $2 \times 2 \times Alt_5$ means $\mathbb{Z}_2 \times \mathbb{Z}_2 \times Alt_5$;

group extensions ; in general $A.B$ means a group with normal subgroup A and quotient B; $A{:}B$ means split extension, $A{\cdot}B$ means nonsplit extension; example $2{\cdot}Alt_5 = SL(2,5)$

2_{ε}^{1+2r}, an extraspecial 2-group of type $\varepsilon = \pm$;
p^{1+2r} an extraspecial p-group;

Scope

I shall discuss how our discoveries of the 26 sporadic simple groups evolved, with emphasis on what I myself experienced or heard from witnesses. I became mathematically active starting in mid 1960s and felt the excitement and mystery of the ongoing events in finite group theory.

The earliest use of the term "sporadic group" may be Burnside (1911, p. 504, note N) where he comments about the Mathieu groups:

"These apparently sporadic simple groups would probably repay a closer examination than they have yet received".

It is worth mentioning that Burnside also wrote that probably groups of odd order were solvable, a theorem proved by Feit and Thompson in 1959 [**?**]. A consequence is that a nonabelian finite simple group has order divisible by 2 and so contains involutions.

The Mathieu groups were not part of natural infinite families, like the alternating groups, or classical matrix groups like $PSL(n, q)$.

The term *sporadic group* has come to mean a nonabelian finite simple group which is not a group of Lie type or an alternating group. There are 26 sporadic groups. It is a consequence of the CFSG that there are no more. There is no proof which is independent of CFSG.

In the group theory community, “discovery” meant presentation of strong evidence for existence. Proof of existence usually came later, frequently done by someone else.

Discoveries of previously unknown simple groups were strongly connected to the ongoing classification of the finite simple groups (CFSG). The program to classify finite simple groups came to life in the early 1950s and was mostly finished around the early 1980s, though some issues were identified and resolved later. It is generally believed to be settled and that the list is complete. Things I learned from working on CFSG helped me find my way in the world of sporadic groups.

I will not attempt to survey the CFSG. Apologies to the many researchers on CFSG who will not be mentioned. One could say that most effort in the CFSG program was directed towards achieving an upper bound on the possible finite simple groups. Those who sought new groups and tried to construct them contributed to achieving a lower bound on the possible finite simple groups. These two bounds met eventually.

Main themes which developed for the sporadic groups

Most finite simple groups are of Lie type (analogues of Lie groups over finite fields, and variations) and can be treated uniformly by Lie theory. Symmetric and alternating groups are easy to understand. The sporadic groups are not easily described. Listed below are several themes which are relevant for discovering or describing for most of the sporadic groups.

For certain sporadic groups, more than one category applies.

External themes:

Multiply transitive and rank 3 permutation representations (rank 3: transitive permutation representation for which point stabilizer has just three orbits)

Isometries of lattices in Euclidean space (Leech lattice and related lattices)

Automorphisms of commutative non associative algebras

Internal themes:

ω-transposition groups (two involutions in a group generate a dihedral group of restricted order)

pure group theoretic characterizations (such as characterization by centralizer of involution or other properties)

The list of FSG, changing over time

Now, I will give the view of KNOWN OR PUTATIVE finite simple groups at several moments in history. In some cases, finite simple groups were believed to exist and be unique but proofs came later.

The date given for sporadic groups is year of discovery, as well as I remember (or estimate). Accuracy is greater after 1968. Publication dates are found in the reference section.

1910 view of FSG

Cyclic groups of prime order

Alternating groups of degree at least 5

Some classical groups over finite fields (GL, GU, PSO, PSp), done by Galois and Jordan.

Groups of type G_2, E_6 (and possibly F_4) by L. E. Dickson (around 1901 or so), at least in odd characteristic.

Proposals by Émile Mathieu of the Mathieu groups: $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ [**?**, **?**, **?**] (1861-1873). Their existence was first made rigorous in 1937 by E. Witt [**?**, **?**].

[sporadic count=5]

1959 view of FSG

Cyclic groups of prime order

Alternating groups of degree at least 5

NEW LIE TYPE:

1955 Chevalley groups over finite fields (types $A_n(q), B_n(q), C_n(q), D_n(q), E_{6,7,8}(q), F_4(q), G_2(q)$, $q =$ prime power; some restrictions on n, q) [**?**]; includes classical groups: for example $A_n(q) \cong PSL(n+1, q)$.

NEW LIE TYPE:

1959 Steinberg variations of Chevalley groups, associated to graph times field automorphisms (types ${}^2A_n(q), {}^2D_n(q), {}^3D_4(q), {}^2E_6(q)$, $q =$ prime power; some restrictions on n, q); includes classical groups involving field automorphism: for example ${}^2A_n(q) \cong PSU(n+1, q)$.

A few Chevalley-Steinberg groups are nonsimple; there are some isomorphisms between groups from different families.

Mathieu groups

[sporadic count=5]

1962 view of FSG

Same as in 1959 plus these:

NEW LIE TYPE:

1960 The *series of Suzuki groups* $Sz(q), q =$ *odd power of 2,* $q \geq 8$, found by pure group theoretic internal characterization [**?**]; these *might* have been considered "sporadic" but in 1961 were shown by Takashi Ono to be of Lie type, ${}^2B_2(q)$, associated to an isomorphism of the group $B_2(q)$ but which does not come from a morphism of the Lie algebra [**?**, **?**].

NEW LIE TYPE:

1961 The *two series of groups defined by Ree,* ${}^2G_2(q)$*,* $q \geq 27$*,* $q =$ *odd power of 3; and* ${}^2F_4(q)'$*, for* q *an odd power of 2*. The group ${}^2F_4(2)$ is nonsimple; its derived group ${}^2F_4(2)'$, called the Tits group, has index 2 and is simple [**?**].

Mathieu groups

[sporadic count=5]

1970 view of FSG; the deluge, part 1

Same as in 1962 plus these:

NEW SPORADIC:

1965 Janko group J_1

1967 Hall-Janko group $(HJ = J_2)$; Janko group J_3; Higman-Sims group; McLaughlin, Suzuki sporadic group,

1968 Conway's Co_1, Co_2, Co_3; Held; Fischer's 3-transposition groups $Fi_{22}, Fi_{23}, Fi'_{24}$;

1969 Lyons group

[sporadic count=5+13=19]

1970-1972 blues

New real and putative groups were fun to examine. There were no announcements about sporadic group discoveries during 1970-1972. A mild depression spread within the finite group community.

1973 view of FSG: the deluge part 2

Same view as in 1970 with these additions:

NEW SPORADIC:

before mid-May 1973: $O'Nan$ (a group of order $2^9 3^4 5 \cdot 7^3 19 \cdot 31$)

early 1973: Ru (Rudvalis rank 3 group) order $2^{14} 3^3 5^3 7 \cdot 13 \cdot 29$

summer 1973: F_2 (Fischer's Baby Monster; a $\{3, 4\}$-transposition group)

November 1973: $\mathbb{M} = F_1$ (Monster, by Fischer and Griess) ($\{3, 4, 5, 6\}$-transposition groups);

F_3 (Thompson),

F_5 (Harada-Norton)

[sporadic group count=25]

1975 view of FSG

Same as 1973, plus

NEW SPORADIC:

May, 1975: Janko's fourth group J_4 order $2^{21}3^35{\cdot}11^311{\cdot}23{\cdot}29{\cdot}31{\cdot}37{\cdot}43$ found by centralizer of involution $2^{1+12}3M_{22}2$.
[sporadic group count=26]

THE FINAL LIST of FSG (after decades of CFSG):

(a) cyclic groups of prime order;

(b) the alternating groups (even permutations on a set of n symbols, $n \geq 5$);

(c) groups of Lie type over finite fields (17 families): Chevalley groups $A_n(q) \cong PSL(n+1, q)$, $B_n(q) = PSO(2n+1, q), \ldots, E_8(q)$; Steinberg, Suzuki and Ree variations:
${}^2A_n(q) = PSU(n+1, q), \ldots {}^2F_4(2^{2m+1})'$;

(d) 26 sporadic groups = 5 groups of Mathieu from 1860s, plus 21 others, discovered during period 1965-1975.

[sporadic count = 26]

Of the 26 sporadic groups, 20 are subquotients of the Monster, the largest sporadic. These twenty groups form *The Happy Family*. The set of six remaining groups are called *The Pariahs*. There is no single simply stated theme which explains or describes the sporadic groups in a useful or efficient manner. The broadest coverage so far is membership in the Happy Family.

Fuzzy boundary between sporadic simple groups and the others

(1) We see an easily expressed 3-transposition condition in symmetric groups and in some classical groups over fields of characteristic 2 and 3 (for reflections or transvections). The classification of nonsolvable 3-transposition groups includes three previously unknown sporadic groups, Fi_{22}, Fi_{23} and Fi_{24}. *What resulted from such a simple hypothesis is amazing.*

(2) The finite real and complex reflection groups were classified a long time ago. Their composition factors involve only cyclic groups, alternating groups and certain classical matrix groups over the fields of 2 and 3 elements.

The finite quaternionic reflection groups were classified in the 1970s by Arjeh Cohen [**?**]. Their composition factors involve only cyclic groups, alternating groups, a few classic matrix groups of small dimension over small fields, *and the sporadic group of Hall-Janko*.

(3) Timmesfeld's classification [**?**] of $\{4, odd\}^+$ transposition groups with no normal solvable subgroups gave most groups of Lie type in characteristic 2 (the groups ${}^2F_4(q)$ do not occur here), all of the 3-transposition groups of Fischer, *plus the sporadic Hall-Janko group* (which is not a 3-transposition group). The group HJ embeds into the group $G_2(4)$ and its $\{4, odd\}^+$-transpositions are contained in those of $G_2(4)$. So, HJ is close to being a group of Lie type in characteristic 2.

(4) Also the $\{3, 4, 5, 6\}$-transposition property of the $2A$-involutions in $\mathbb{M}$ (the Monster) feels like something close to Weyl groups in Lie algebra theory, particularly because of the theory of Miyamoto involutions [**?**] and Sakuma's theorem [**?**].

Beginnings of CFSG and sporadic encounters

The CFSG starts in early 1950s and, as a consequence, encourages a search for more finite simple groups.

In any group, two involutions generate a dihedral group. The following theorem [**?**] extends a thesis result of Kenneth Fowler at University of Michigan [**?**], under the direction of Richard Brauer.

Theorem

(Brauer-Fowler) There exists a function $f : \mathbb{N} \to \mathbb{R}$ so that if G is a finite simple group (of even order) and $t \in G$ is an involution, then $|G| \leq f(|C_G(t)|)$.

In other words, if H is a finite group then, up to isomorphism, only finitely many finite simple groups have an involution whose centralizer is isomorphic to H. (Usually, that number is zero.)

The function f is extravagant, of no practical value. However, *the psychological impact of limiting a finite simple group by a centralizer of involution was powerful.*

In Brauer's talk in Amsterdam ICM (1954), he gave an early theorem along this line. We first give some notation.

Let q be an odd prime power and let H be the centralizer of an involution $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ (mod scalars) in the simple group $PSL(3, q)$. So, H is the group of all matrices of the form $\begin{pmatrix} c & \\ & A \end{pmatrix}$ (mod scalars) where A is an invertible 2×2 matrix and $c \cdot det(A) = 1$. So, for all odd q, H is isomorphic to $GL(2, q)$.

Theorem

Assume that (i) G is a finite simple group with involution u so that $C_G(u) \cong GL(2, q)$;
(ii) for $x \neq 1$ in $Z(C_G(u))$, $C_G(x) = C_G(u)$;
Then $G \cong PSL(3, q)$ or $q = 3$ and $G \cong M_{11}$, the Mathieu group of order $7920 = 2^4 3^2 5 \cdot 11$.

Hypothesis (ii) was eventually removed.

Note that we get the expected answers $PSL(3, q)$ but in the proof there is a branch of the argument which leads to a sporadic group. *If you had never met M_{11} before, you would meet it this way.*

There were many results in CFSG which were intended to characterize known finite simple groups by some internal property. Occasionally, there was a branch in the argument which led to the discovery of a new (previously unknown) finite simple group.

Brauer's strategy applied "only" to simple groups of even order. In 1959, Feit and Thompson proved that all finite groups of odd order are solvable. After their theorem, it was clear that Brauer's viewpoint was more relevant to understanding finite simple groups.

Theorem

(Janko-Thompson) Let $q \geq 5$ be a prime power and G be a finite simple group with abelian Sylow 2-subgroups and an involution t so that $C_G(t) \cong 2 \times PSL(2, q)$. Then q is an odd power of 3 with $q \geq 27$ or $q = 5$.

The case $q = 5$ was mistakenly eliminated due to an error in a character table for $PSL(2, 11)$. The error was found later by Janko, who obtained the following result.

Theorem

*(Janko [**?**]) Let G be a finite simple group with abelian Sylow 2-subgroups and an involution t so that $C_G(t) \cong 2 \times PSL(2, 5)$. Then G has order $175560 = 2^3 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$. Furthermore, such G exist and are unique up to isomorphism.*

Assuming that such a G exists, Janko gave two matrices A, B in $GL(7, 11)$, which would generate such a simple group (and incidentally prove uniqueness of such a group). In [**?**] M. A. Ward gave a nice proof that A and B do do generate a simple group of the right order and W. A. Coppel gave a nice proof that this subgroup lies in a $G_2(11)$-subgroup of $GL(7, 11)$ [**?**].

The group J_1 is another example of how a sporadic group comes up as a special case in a classification result.

Reaction to J_1, the first new sporadic simple group in a century

There was a lot of discussion about what the appearance of J_1 could mean. The Suzuki series discovered in 1960 turned out to be groups of Lie type. Were there more sporadics waiting to be discovered?

(1) Think about the order of $GL(n, q)$,

$$q^{\binom{n}{2}}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$$

There are similar polynomial expressions for orders of groups over Lie type over finite fields of q elements. Maybe the new group J_1, of order

$$175560 = 11 \cdot 12 \cdot 1330 = 11(11 + 1)(11^3 - 1)$$

is part of a series of groups of order $q(q + 1)(q^3 - 1)$ where q is a prime power (or maybe a power of 11). This was a nice idea, but it did not lead anywhere.

(2) Consider these amusing factorizations (found in [**?**]):

$$175560 = 2^3 3{\cdot}5{\cdot}7{\cdot}11{\cdot}19 = 19{\cdot}20{\cdot}21{\cdot}22 = 55{\cdot}56{\cdot}57$$

As far as I know, no one has done anything special with this.

(3) J_1 contains a subgroup isomorphic to $PSL(2, 11)$ of index $266 = 2 \cdot 133$. Since 133 is the dimension of the E_7 Lie algebra, maybe something is going on with the exceptional Lie group E_7?

The group J_1 has a 7-dimensional representation over $\mathbb{F}_{11}$ which embeds J_1 in $G_2(11)$! There is a containment of exceptional Lie groups $G_2 \leq F_4 \leq E_6 \leq E_7 \leq E_8$, so there is a from J_1 link to E_7, but somewhat distant.

Centralizer of involution examples

The strategy of characterization by centralizer of involution was pursued, refined and replaced as the years went by. One can not hope to try all finite groups as centralizer of involution candidates to finish CFSG. Still, it is remarkable that many small groups occurred as centralizers of involutions in previously unknown finite simple groups.

(1) *The dichotomy with* $C = 2^{1+4}{:}Alt_5$ *as a centralizer of involution in a simple group,* G*:* I am not sure why Janko chose this example, but it was fortunate. The group C has three conjugacy classes of involutions. Take involutions z in the center, w in $O_2(C)$ and $t \in C \setminus O_2(C)$. They represent the three conjugacy classes. The Glauberman Z^*-theorem [**?**] says that z must be conjugate to one of w, t. The case where z is conjugate to just one of w, t leads to the group HJ (and z is conjugate to w, in fact). The case where z is conjugate to both w and t leads to the group J_3 of order $50232960 = 2^7 3^5 \cdot 17 \cdot 19$.

(2) The sporadic group of McLaughlin has one conjugacy class of involutions with centralizer of shape $2{\cdot}Alt_8$, the double cover of Alt_8, described by Schur [**?**].

Richard Lyons, while a graduate student at U Chicago, produced strong evidence that there is a finite simple group with an involution centralizer isomorphic to $2{\cdot}Alt_{11}$ [**?**]. The Lyons group has order $2^8 3^7 5^6 7{\cdot}11{\cdot}31{\cdot}37{\cdot}67$.

No group $2{\cdot}Alt_n$, for $n \leq 7$ is the centralizer of an involution in a finite simple group (this follows from Glauberman's Z^* theorem [**?**]). The CFSG shows that the groups $2{\cdot}Alt_n, n \neq 8, 11$ are not centralizers of involutions in finite simple groups.

(3) With finitely many exceptions, finite groups of Lie type over a field of characteristic p have Schur multiplier of order relatively prime to p [**?**, **?**, **?**, **?**, **?**]. Certain associated exceptional central extensions appeared as normal subgroups in normalizers of small p-groups within sporadic groups. Some examples: (a) $2{\cdot}PSU(6,2)$ in Fi_{22}; (b) $3^2{\cdot}PSU(4,3)$ in Co_1; (c) $2{\cdot}F_4(2)$ in the Monster; (d) The group Co_3 has an involution centralizer of the form $2{\cdot}Sp(6,2)$; (e) certain central extensions of $PSL(3,4)$ in the groups of Held and O'Nan.

For a discussion of connections between exceptionally nonvanishing cohomology and sporadic groups, see [**?**].

I do not recall a case of a sporadic group being *discovered* by centralizer of involution procedure, starting with such an exceptional covering of a group of Lie type.

(4) Dieter Held studied the group $2_+^{1+6}{:}GL(3,2)$, which is a centralizer of involution in both $GL(5,2)$ and M_{24} and found that it is a centralizer of involution in a third group, the sporadic group of Held, order $4030387200 = 2^{10}3^3 5^2 7^3 17$.

From CFSG, we know that, given a particular group H, the number of finite simple groups, up to isomorphism, having H as centralizer of involution is at most 3. Only $H = 2_+^{1+6}{:}GL(3,2)$ achieves the upper bound of 3. Several groups occur as centralizer twice. The pair of simple groups $PSL(2,7), Alt_6$ each have one conjugacy class of involutions and common involution centralizer Dih_8. The pair of simple groups HJ, J_3 have involutions with common centralizer $2_-^{1+4}{:}Alt_5$.

(5) Janko went through many candidates for centralizer of involution, as he looked for more sporadic groups. I have been told that while he was on the Ohio State faculty, he gave weekly seminars about the cases he considered for centralizers of involution in a simple group. None of those led to a new simple group.

Janko even studied series of centralizer candidates. Jon Alperin told me that Janko considered $q^{1+8}Sp(6, q)$ for q a power of 2. This series generalizes the case of an involution centralizer $2^{1+8}Sp(6, 2)$ in the group Co_2. No simple group occurs for such a centralizer when $q > 2$. At a 1972 meeting in Gainesville, Florida, Janko proposed another infinite family of centralizers for possible new simple groups. Within a few weeks after the conference, this possibility was eliminated, but he reported on yet another family of centralizer candidates in the conference proceedings [**?**].

Don Higman's rank 3 theory

A permutation representation of a group G on a set Ω is a group homomorphism $G \to Sym(\Omega)$. Its *degree* is the cardinality $|\Omega|$. The *rank* of a transitive permutation representation of the group G on a set Ω is the number of orbits for the natural action on $\Omega \times \Omega$. Equivalently, it is the number of orbits of a point stabilizer $G_a := \{g \in G \mid ga = a\}$ on Ω.

Notation

Let the finite group G act on the set Ω transitively with rank 3. For $a \in \Omega$, let the orbits of the point-stabilizer G_a be $\{a\}, \Delta(a), \Gamma(a)$. Assume that if $g \in G$, then $\Delta(g \cdot a) = g \cdot \Delta(a)$ and $\Gamma(g \cdot a) = g \cdot \Gamma(a)$.

Define $n := |\Omega|$, the degree;

$k := |\Delta(a)|$,

$\ell := |\Gamma(a)|$

$\lambda := |\Delta(a) \cap \Delta(b)|$ *for* $b \in \Delta(a)$,

$\mu := |\Delta(a) \cap \Delta(b)|$ *for* $b \in \Gamma(a)$.

Call k, ℓ the subdegrees and call k, ℓ, λ, μ the rank 3 parameters or the Higman parameters of the rank 3 representation.

Lemma

*[**?**] $\mu\ell = k(k - \lambda - 1)$ (the Higman condition).*

Call a sequence of nonnegative integers k, ℓ, λ, μ a *Higman quadruple* if they satisfy the Higman criterion. A Higman quadruple may arise from a rank 3 group, or not. Don Higman kept a list of such quadruples which might be relevant to finite groups.

There are other numerical conditions in [**?**]; above is all I need now.

The next example may be verified by counting. No specialized group theory is required.

Example

Let G be 4-transitive subgroup of Sym_m for $m \geq 4$, $\Omega =$ the set of unordered pairs of distinct integers from $\{1, 2, 3, \ldots, m\}$. The action of G is transitive. The stabilizer in G of (i, j) has two nontrivial orbits:

$\Delta((i, j))$:= the pairs which contain just one of i, j (cardinality $k = 2(m-2)$);

$\Gamma((i, j))$: = the pairs which avoid i, j (cardinality $\ell = \binom{m-2}{2}$).

The stabilizer of (i, j) in G is transitive on the sets $\Delta((i, j))$ and $\Gamma((i, j))$. So, we have a rank 3 permutation representation on $n = 1 + k + \ell = 1 + 2(m-2) + \frac{(m-2)(m-3)}{2} = \binom{m}{2}$ points. The remaining parameters for the Higman condition are:

$\lambda = m - 3 + 1 = m - 2$; $\mu = 4$.

The Higman condition $\mu\ell = k(k - \lambda - 1)$ here would say $4\binom{m-2}{2}$ equals $2(m-2)(2(m-2) - (m-2) - 1) = 2(m-2)(m-3)$, which is true.

1967, the sporadic groups of Hall-Janko and Higman-Sims

Now we jump to year 1967 and linked stories about the sporadic groups HJ and HS.

The Hall-Janko group, HJ, which has order $604800 = 2^7 3^3 5^2 7$, was discovered independently by Zvonimir Janko and Marshall Hall. Janko started starting by using $C := 2_-^{1+4}{:}Alt_5$ (split extension) as candidate for the centralizer of an involution in a simple group. Hall worked with a Higman quadruple $k = 36, \ell = 63, \lambda = 14, \mu = 12$, good for the group $H \cong PSU(3,3)$ to be a one-point stabilizer in a degree 100 rank 3 group of order $604800 = 2^7 3^3 5^2 7$. Marshall Hall worked out properties of a putative simple group. David Wales and Marshall Hall constructed one with computer [**?**, **?**].
The announcements of Zvonimir Janko and Marshall Hall referenced each other's work [**?**, **?**, **?**]. It is nice to learn about such courtesy.

The story I tell of the Higman-Sims group discovery and existence proof is taken from testimony of Charles Sims (see [**?**, **?**].

It took place at a conference "Computational problems in abstract algebra" in Oxford in 1967.

Marshall Hall lectured on his construction of his simple group HJ, order $2^7 3^3 5^2 7$. It acted in a rank 3 fashion on a graph on 100 points and valency 36.

On the last day of the conference, *2 September, 1967*, Higman and Sims thought about 100 and wondered if that number could come up in other ways for rank 3 groups. They may not have been so curious but for the fact that our number system is written in base 10 and $100 = 10^2$. Right away, they thought of the wreath product $Sym_{10} \wr 2$ acting on the cartesian product of two 10-sets. This is rank 3 with subdegrees 1, 18, 81. The Higman parameters are $(18, 81, 8, 2)$.

Higman had a table of Higman quadruples. One quadruple was $(22, 77, 0, 6)$. The number 22 suggested that the Mathieu group M_{22} could be a point stabilizer in a rank 3 group with these parameters (the symmetric and alternating groups on 22 points will not work here since they do not act transitively on a set of 77 points). For 77, it is well known that M_{22} acts on a Steiner system $\mathfrak{S}(3, 6, 22)$, which has 77 blocks $(77 = \binom{22}{3}/\binom{6}{3})$.

So, they defined a graph. For nodes of the graph, they used a set Ω of 100 points: *, with the 22 points Δ affording M_{22}, and with the 77 blocks Γ. It is clear that $Aut(M_{22}) = M_{22}{:}2$ acts on this set of 100 points. Work of E. Witt on existence and uniqueness of Steiner systems associated to Mathieu groups [**?**, **?**] was very helpful to Higman and Sims.

The edges in the graph are defined as follows: * is connected to just the 22 points of Δ. A point p in Δ is connected to * and the 21 blocks containing it. A block is connected to the 6 points in the block and the 16 blocks disjoint from it. (So Higman parameters have values $\lambda = 0$, $\mu = 6$.)

They needed to prove existence of some permutation π on Ω which preserved the graph and moved *. This will prove that the group G generated by π and the action of $Aut(M_{22})$ on the set Ω is a rank 3 group with parameters $(22, 77, 0, 6)$.

Higman and Sims talked all night and got such a π. By the morning of *Sunday, 3 September, 1967*, it was clear that their group G or a subgroup of index 2 was a new simple group. (It turns out that the commutator subgroup G' has index 2 and is simple of order $2^9 3^2 5^3 7 \cdot 11$.) Time from conception to existence proof for this sporadic group was about a day. Their performance was unique. For other sporadic groups, gap between discovery and construction ranged from weeks to years.

I learned in 2007 that Dale Mesner had constructed this Higman Sims graph in his 1956 doctoral thesis at the Department of Statistics, Michigan State University. This 291 page thesis explored several topics, including integrality conditions for strongly regular graphs (association schemes with two classes) related to Latin squares.

Mesner does not mention concerns about its automorphism group or acknowledge connections with Mathieu groups and Steiner systems. Jon Hall gives an account of this in [**?**].

Given Higman parameters, when is there a rank 3 group?

Don Higman maintained a list of parameter values which met his conditions. Some corresponded to actual rank 3 groups. *There are relevant group theoretical conditions besides arithmetic ones.* If G is a rank 3 group with point stabilizer H, the group H must have subgroups of indices k and ℓ. See [**?**], p.125 for Higman's table of parameters which apply to actual rank 3 groups.

Discovery of the McLaughlin group

When I was in grad school at University of Chicago, Jack McLaughlin was in residence there during a sabbatical year (1968-69 maybe?) from University of Michigan. He was thinking about the Higman-Sims group and Don Higman's rank 3 theory. McLaughlin thought about the group $H = PSU(4,3)$, order $2^7 3^6 5{\cdot}7$ and considered a maximal parabolic subgroup of index 112. He next studied Higman quadruples k, ℓ, λ, μ with $k = 112$. Since ℓ must be the index of a subgroup of H, he reviewed ones he knew about and thought of a subgroup isomorphic to $PSL(3,4)$, order $2^6 3^2 5{\cdot}7 = 20160$, described by H. H. Mitchell around 1918 [**?**]. This gives $\ell = 162$ and the Higman condition forces $\lambda = 30$ and $\mu = 56$. McLaughlin defined a graph on 275 nodes and valency 112 at each node. Using strategy of Higman and Sims, he constructed an automorphism of the graph and thereby constructed a new sporadic group of order $2^7 3^6 5^3 7{\cdot}11$ [**?**]. I omit details.

That year, Janko came to University of Chicago to give a seminar. I joined the colloquium dinner party, which included Jack and Doris McLaughlin and possibly George Glauberman. I remember that Janko and McLaughlin were in good moods.

Looking for more sporadics

Lots of group theorists looked for sporadics, some probably in secret. I played with Higman criterion and "rediscovered" the parameters which McLaughlin used, as well as finding many interesting quadruples which led nowhere.

Remarkably, the Higman-Sims group, discovered as a rank 3 group, has doubly transitive representations, on cosets of $PSU(3,5)$-subgroups. A putative simple group with the latter property was investigated by Graham Higman, but he did not complete the work before Donald Higman and Charles Sims discovered and constructed their group. Some sporadics are multiply transitive permutation groups: all Mathieu groups; Higman-Sims group; Co_3 (on cosets of a subgroup isomorphic to $McL{:}2$).

My impression was that the search for sporadic groups was done more systematically in the world of centralizer of involution studies than in the world of permutation groups. Centralizer of involution results directly supported the ongoing CFSG program. Sometimes, a new sporadic group was a surprise conclusion of a standard centralizer of involution characterization, such as the Held group [**?**] and the Harada-Norton group [**?**].

Janko was the most openly energetic explorer of centralizer of involution problems. He found success four times, starting with centralizer candidates which puzzled observers. They wondered whether he had extremely good insight or just an amazing lucky streak. The most exotic-looking centralizer for his groups was $2^{1+12}.3.M_{22}.2$ for the pariah J_4. The context of his successes surely included a far greater number of trials which led to no new groups but strengthened his instincts.

The Leech lattice

This single object, the Leech lattice, is a rich mathematical world with some remarkable number theory, combinatorics and group theory. It was discovered by John Leech in the mid-1960s, as a dense lattice packing in 24-dimensional Euclidean space [**?**, **?**]. My understanding is that he wanted someone to analyze the isometry group. At the International Congress of Mathematicians in 1966, McKay (then a graduate student) suggested this to Conway, who took up the challenge.

First, a few definitions. A *lattice* L in Euclidean n-space is a $\mathbb{Z}$-linear combination of a basis. It is *integral* if all inner products $\langle x \mid y \rangle$ are integers and is *even* if all inner products are integers and $\langle x \mid x \rangle \in 2\mathbb{Z}$ for all $x \in L$. A *Gram matrix* for L with respect to the $\mathbb{Z}$-basis $v_1, \ldots, v_n$ of L is the $n \times n$ matrix whose i, j entry is $\langle v_i \mid v_j \rangle$. The *determinant* of L is the determinant of any Gram matrix. If a lattice is even and unimodular, n is divisible by 8. If $n = 24$, there are just 24 even unimodular lattices of determinant 1. The *Leech lattice* is the only one without vectors of norm 2; its minimum norm is 4.

A common notation for the Leech lattice is Λ.

Conway's story, reported in [**?**], is that he figured it all out in a single session of 12.5 hours. Some people told me that, for a short time, there was more than one candidate for the group order of the isometry group. The final result is that the order of the isometry group is $2^{22}3^{9}5^{4}7^{2}11{\cdot}13{\cdot}23$.

Common notation for this isometry group is Co_0 or $O(\Lambda)$.

Here is the *standard description of the Leech lattice*.

The Leech lattice is built from sublattices starting with a sublattice J which had 24×24 Gram matrix $diagonal(4, 4, \ldots, 4, 4)$. Take an orthogonal basis for this lattice, say $v_i, i \in \Omega$, where Ω is an index set of size 24. Now take a Golay code $\mathcal{G}$, a 12-dimensional linear subspace of $\mathbb{F}_2^\Omega$ so that the minimum weight of a vector is 8 (weight means the number of nonzero coordinates). This sublattice J was then made to a larger lattice K by taking the $\mathbb{Z}$-span of J and all sums $\frac{1}{2} v_A$, where A is the subset of Ω corresponding to a word in $\mathcal{G}$. Finally, we get the Leech lattice $\Lambda := K + \mathbb{Z}(-v_i + \frac{1}{4} v_\Omega)$ (this definition of Λ is independent of choice of $i \in \Omega$).

The group M_{24}, the group of the Golay code $\mathcal{G}$, acts on 24-dimensional space by permuting the basis $v_i, i \in \Omega$, as it permutes the index set. For this action, M_{24} preserves each of the lattices J, K, Λ. Using the same basis, there is for every subset S of Ω, a linear transformation defined by $\varepsilon_S : v_i \mapsto \begin{cases} -v_i & \text{if } i \in S \\ v_i & \text{if } i \notin S \end{cases}$. Self duality of the Golay code show that ε_S takes Λ to itself if and only if S corresponds to a Golay codeword. All these transformations give a monomial group H of shape $2^{12}{:}M_{24}$.

The full isometry group of Λ is larger than H. The order of the isometry group follows from the mass formula [**?**] involving all rank 24 even unimodular lattices. Conway gave an explicit formula for an isometry u not in H, then showed that the full isometry group of Λ is generated by u and H and has order $2^{22}3^{9}5^{4}7^{2}11{\cdot}13{\cdot}23$. His isometry was useful in computations.

A different style analysis of the Leech lattice, its properties and its isometry group was given by me in [**?**]. It emphasizes configurations of $\sqrt{2}E_8$-sublattices. It is relatively free of calculations with matrices, special counting arguments, etc.

Consequences of Leech lattice theory for finite groups

The quotient $Co_1 := Co_0/\{\pm 1\}$ is simple of order $2^{21}3^9 5^4 7^2 11{\cdot}13{\cdot}23$.

Stabilizers of sublattices gave then-new sporadic groups
Co_2 of order $2^{10}3^7 5^3 7{\cdot}11{\cdot}23$
Co_3 of order $2^{18}3^6 5^3 7{\cdot}11{\cdot}23$

and some familiar ones:
HS re-discovered, order $2^9 3^2 5^3 7{\cdot}11$
McL re-discovered, order $2^7 3^6 5^3 7{\cdot}11$

Centralizers of certain isometries gave the groups HJ of order $2^7 3^3 5^2 7$ and Suz of order $2^{13}3^7 5^2 7{\cdot}11{\cdot}23$; both re-discovered. (More precisely, perfect groups $2{\cdot}HJ$ and $6{\cdot}Suz$ occur as subgroups of centralizers within Co_0.)

Fischer's ω-transposition group theory

(1) **Definition of ω-transposition group.** Let ω be a nonempty subset of $\{3, 4, 5, \dots\}$. Recall that in any group, two involutions generate a dihedral group. An *ω-transposition group* is a finite group G generated by D, a union of conjugacy classes of involutions, so that for $x \neq y$ in D, then either x, y commute or xy has order $|xy| \in \omega$. So $\langle x, y \rangle$ is a dihedral group of order $2|xy|$.

Examples for the case $\omega = \{3\}$:
(a) $D =$ the set of transpositions (i,j) in a symmetric group $G = Sym_n$. If (i,j) and (k,ℓ) do not commute, their product is a 3-cycle. So the group generated by (i,j) and (k,ℓ) is a copy of $Sym_3 \cong Dih_6$.
(b) Orthogonal reflections in $O^{\varepsilon}(2m,2)$, $(\varepsilon = \pm)$. Other examples in classical groups over fields of 2 and 3 elements.
Fischer classified such groups provided that a solvable normal subgroup is in the center. We get symmetric groups, some classical groups over small fields AND three previously unknown almost-simple groups $Fi_{22}, Fi_{23}, Fi_{24}$. *To me, finding these sporadic groups from the simple-looking 3-transposition property is one of the most surprising aspects of sporadic group theory.*

Examples for the case $\omega = \{3,4\}$**:** (a) $GL(n,2)$, for D the conjugacy class of *transvections* = identity + rank 1 nilpotent, e.g. $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Easy to check that two different transvections generate a dihedral group of order at most 8.
(b) some sporadic groups: Co_2, Baby Monster F_2. The Baby Monster was Fischer's fourth sporadic group.

(c) **Examples of unlikely ω-transposition theories :** A finite group generated by a conjugacy class of involutions is an ω-transposition group for some ω. Such a set may be difficult to work with compared to $\omega = \{3\}$. The Suzuki group $Sz(8)$, order $29120 = 2^6 5 \cdot 7 \cdot 13$ has one class of involutions. Two distinct involutions commute or their product has order 5, 7 or 13.

For $PSL(2, 2^n)$, the involutions are the transvections (with Jordan canonical form $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$) and ω must contain all divisors of $2^n + 1$ and $2^n - 1$.

Computer constructions of sporadic groups

The Higman-Sims group was envisioned and constructed in about a day. Other sporadic groups were constructed by hand, including Mathieu groups and most 3-transposition groups. Several groups were constructed by computer. The first such constructions were for $HJ, J_3, Held, Lyons, O'Nan, Rudvalis, BabyMonster, J_4$ by McKay, Sims, Leon, Norton, Benson, Conway, Wales, et al. [**?**]

The Rudvalis group has a subgroup of index “only” 4060. Some sporadic groups required computations with permutation representations on cosets of subgroups with large indices. For example, the O'Nan group has a permutation representation on 122760 symbols and the Lyons group has a permutation representation on 8835156 points. For each of the latter two groups, Sims took two years or so for construction with computer work [**?**, **?**]. Computational challenges got tougher with larger groups.

In a few cases, there were subsequent constructions by hand.

The simple group of Fischer and Griess

During summer 1973, I received a letter from Ulrich Dempwolff who reported that Fischer had evidence for a new group, a $\{3, 4\}$-transposition group, of order $2^{41}3^{13}5^{6}7^{2}11{\cdot}13{\cdot}17{\cdot}19{\cdot}23{\cdot}31{\cdot}47$, about 4×10^{33}; it would become Fischer's fourth sporadic group. This group was eventually called the Baby Monster. For the moment, I will denote it H, Properties of this group suggested that there could be a larger group.

For example H contains a subgroup $2^{1+22}Co_2$. To me this suggested a larger group $2^{1+24}Co_1$. Also H contains a subgroup $3^{1+10}PSU(5,2)$. To me, this suggested a larger group $3^{1+12}2Suz$. These larger groups, plus other information about H came together to suggest a simple group G with all these larger groups as subgroups.

After initial studies, I felt that there were no obvious reasons to reject the possibility that such a G may exist. I add that H was not a subgroup of G but instead G had a subgroup $2{\cdot}H$ which was a nonsplit central extension of H by $\mathbb{Z}_2$. The first weekend in November 1973, in Ann Arbor, was when I felt there was a serious chance of a new sporadic group. At a meeting in Bielefeld the same weekend, Fischer spoke about his ideas for the same group. We had no direct communications about this topic until weeks or months after that.

Fischer's thinking may have overlapped with mine. He was also thinking about the class of $\{3, 4\}$-transpositions in H and what they would correspond to in a larger simple group which contained $2{\cdot}H$ as a centralizer of involution. This group would eventually be called the Monster and become Fischer's fifth sporadic group, and my first (and only).

Monstrous Moonshine

The starting point for *Monstrous Moonshine* of Conway and Norton were two ideas.

First, John McKay's surprising observation that 196884 (the first nontrivial coefficient of the elliptic modular function $j(z)$ equals $1+196883$ (z varies over the upper half complex plane). The number $196883 = 47 \cdot 59 \cdot 71$ was expected to be the smallest degree of a nontrivial irreducible representation of the Monster. It is easy to show that the degree of a faithful matrix representation of the Monster is at least 196883.

Second, John Thompson looked at a few of the the higher coefficients of $j(z) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$, where $q = e^{2\pi iz}$ and noticed that they were nonnegative linear combinations of degrees of irreducible representations of the Monster, $1, 196883, 21296876, 842609326, \ldots$. He then asked whether there could be a graded space $V = \bigoplus_{n \geq -1} V_n$, where V_n is a finite dimensional module for the monster, so that the formal series $\sum_{n \geq -1} dim(V_n)q^n$ equals $j(z) - 744$ and that the series $\sum_{n \geq -1} tr(g|_{V_n})q^n$ could be interesting for all g in the Monster.

It was indeed interesting. It was the basis of the Monstrous Moonshine theory of Conway and Norton, a near-bijective correspondence between conjugacy classes of the Monster and a family of genus 0 function fields on the upper half plane. This was a surprising connection between deep parts of finite group theory and number theory. The impact on mathematics would be great.

Existence proof for the Monster

Difficulty of a construction

The order of the Monster was about 8×10^{53}, so construction was expected to be difficult. Some sporadic groups were constructed with computer work, which in some cases took years. The problem with trying a computer construction of the Monster was that there were no small representations.

The smallest index of a subgroup was believed to be about 10^{20}, so a permutation representation would involve that many symbols. The smallest degree of a faithful matrix representation in characteristic 0 had been known since 1973 to be at least 196883 [**?**]; in fact the smallest degree of a faithful matrix representation over a field of characteristic not 2 or 3 turns out to be at least 196883, and the smallest degree in characteristics 2 and 3 is at least 196882 by a result of Steve Smith and myself [**?**].

Worth the effort?

In the mid 1970s, there was an increasing awareness of large and larger sporadic groups. The Monster was really large compared to predecessors. The difficulty of constructing it seemed orders of magnitude beyond past experiences.

An effort to construct it may go a long time without reward. Not only that, but there could be even larger and larger sporadic groups to deal with in the years to come. The sense of what was important to CFSG could change.

I recall a group theorist telling me that he/she could have envisioned the same expansion of ideas from Baby Monster to Monster as I did. This person did not want to pursue consequences because they foresaw only a thankless labor with little likelihood of payoff. There was no lack of challenging problems to work on in the ongoing CFSG.

Shifting winds in late 1970s

In the late 1970s, there was a sense that the classification of finite groups might close in the near future since Daniel Gorenstein and Richard Lyons had outlined an end game [**?**]. No sporadics had been discovered since May 1975. Also Monstrous Moonshine came along and suddenly made resolving existence of the Monster important. I began to think about how a construction would go.

The attempt, late 1979

In fall 1979, about six years after Fischer and I discovered evidence for the Monster, I decided to make a serious try at a construction. I was at the Institute for Advanced Study, on a one year sabbatical from the University of Michigan.

To me, the most reasonable setting seemed to be a degree 196883 complex representation, which was expected to be writeable over the rationals. Work of Simon Norton suggested that if B is an irreducible 196883-dimensional representation of the Monster, B is self-dual and has a degree 3 invariant symmetric tensor. This means that B would have the structure of a commutative algebra with an associative bilinear form, for which the Monster acts as algebra automorphisms.

Let us say a finite simple group has *Monster type* if it has an involution whose centralizer has the form $2^{1+24}Co_1$, My goal was to create a finite group which has Monster type.

I started by trying to construct a dimension 196883 representation B for a *suitable* group C of shape $2^{1+24}Co_1$ and consider the family of C-invariant algebra structures. Then I had to (1) make a choice of C-invariant algebra structure which *could* be invariant under a finite group larger than C; (2) define an invertible linear transformation σ on B, then prove that σ preserves the algebra structure; (3) Show that the group $\langle C, \sigma \rangle$ generated by C and σ is a finite simple group in which C is the centralizer of an involution. Then $\langle C, \sigma \rangle$ would be a group of Monster type.

We can describe C with a fiber product, $\widehat{C}$:

$$\begin{array}{ccc} \widehat{C} & \dashrightarrow & C_\infty \\ \vdots & & \downarrow \\ \vee & & \\ Co_0 & \rightarrow & Co_1 \end{array}$$

where C_∞ is a subgroup of $GL(2^{12}, \mathbb{Q})$ of the form $2^{1+24}.Co_1$. We can think of $\widehat{C}$ as the subgroup of the direct product $Co_0 \times C_\infty$ consisting of all pairs (u, v) so that the images in Co_1 of $u \in Co_0$ and $v \in C_\infty$ are equal. Then we take $C := \widehat{C}/\langle(-1, -1)\rangle$ where the first component of $(-1, -1)$ means the scalar -1 on the rational span of the Leech lattice and where the second component means -1 in $GL(2^{12}, \mathbb{Q})$.

The smallest faithful representation of C has dimension $98304 = 24{\cdot}2^{12}$.

We use notation similar to that in [**?**]. Let z be the involution which generates the center of C and let $R := O_2(C)$.
Define $B := U \oplus V \oplus W$, a direct sum of irreducible C-modules, where U has dimension 299, $dim(V) = 98280$ and W has dimension $98304 = 24 \cdot 2^{12}$.

Think of U as 24×24 symmetric matrices of trace 0; V has a basis of all unordered pairs $\{\lambda, -\lambda\}$ where λ is a minimum norm vector in the Leech lattice; and W can be thought of as a tensor product of a degree 24 representation of C_0 and a degree 2^{12} representation of C_∞.

The spaces $Hom_C(X \otimes Y, Z)$ were described, where $X, Y, Z \in \{U, V, W\}$. This information enables a description of the multi-parameter space of C-invariant algebra structures $B \times B \to B$. A choice of algebra and automorphism σ of the algebra, $\sigma \notin C$, were sought.

If the Monster were to exist, there would be a subgroup K of the form $2^{2+11+22}[M_{24} \times Sym_3]$ for which $C \cap K$ would look like $2^{2+11+22}[M_{24} \times 2]$. The right hand factor in $[M_{24} \times 2]$ can be thought of as representing a subgroup generated by the transposition $(1, 2)$ inside the symmetric group on $\{1, 2, 3\}$. My choice of σ would be an element of K which, in the quotient $[M_{24} \times Sym_3]$ of K, represents the transposition $(2, 3)$ in the right hand factor.

Such a σ would not leave the subspaces U, V, W invariant. I found that certain direct sum decompositions of $U = U_1 \oplus U_2 \oplus \ldots, V = V_1 \oplus V_2 \oplus \ldots, W = W_1 \oplus W_2 \oplus \ldots$ were helpful to imagine an approximation of a good σ of order 2 (σ would permute these smaller summands, for example, fixing certain ones while switching some U_i and V_j and some V_k and W_ℓ, etc.).

Getting signs right in a matrix for σ was a big problem, solved by trial and error. Without knowing signs exactly, the procedure of the previous paragraph enabled me to determine a product, uniquely up to scalar multiple, at an early stage. Call the product *.

When I chose an invertible linear transformation σ, I had to check whether it preserved the algebra product. This involved taking a convenient basis b_i of B, then asking whether $\sigma(b_i * b_j)$ equals $(\sigma b_i) * (\sigma b_j)$, for all i, j.

A check typically took about a week of verifications by hand. Failures of equality were studied and new formulas for σ were proposed. I tested a long series of candidates before finding one which worked. Sometimes, I ran a second test for a candidate using a different basis to understand failures better.

This construction took a few months, roughly October 1979 to early January, 1980. I worked around the clock, sleeping as needed and taking little time off. Enrico Bombieri, an IAS faculty member, encouraged me a lot during this intense time. I was very grateful for his support. I announced the construction on 14 January, 1980, by mailing copies of a typed announcement to many group theorists. Later, I wrote up consequences of the construction, such as short existence proofs for other sporadic groups and table of involvement of sporadic groups in one another. The article was submitted to Inventiones and appeared in 1982 [**?**].

Uniqueness of the Monster was proved by Griess, Meierfrankenfeld and Segev in 1989 [**?**]. There is still no uniqueness proof for $(B, *)$ as an algebra (though it is essentially unique, given that a group of Monster type acts as algebra automorphisms for a commutative algebra of dimension 196883).

Graded spaces

A graded space for the Monster was announced by Igor Frenkel, James Lepowsky and Arne Meurman in 1983, a response to the Thompson suggestion. They used a blend of theory for hightest weight modules for affine Lie algebras and the techniques from the Monster construction [**?**]. They proved graded traces were right for many but not all group elements of the Monster. Later, Borcherds proved that the traces were right for all group elements.[**?**]

VOAs and MVOA

In the mid 1980s, Richard Borcherds introduced vertex operator algebras [**?**]. Authors Frenkel, Lepowsky and Meurman then enriched their graded representation of the Monster with vertex operator algebra theory to produce the *Moonshine VOA* or *MVOA*, whose automorphism group is the Monster [**?**]. They use the symbol $V^\natural$ for this VOA.

The graded dimension for a MVOA is $q \cdot (j(z) - 744)$, representing removal of constant term from the elliptic modular function, then a shift of degree.

Some consequences of VOA axioms

The definition of a VOA is too long to present here. A VOA is a graded space over a field of characteristic 0. I mention a few points about the case of VOAs graded over the nonnegative integers.

Given a VOA $V = \oplus_{i \geq 0} V_i$, the k-th product gives a bilinear map $V_i \times V_j \longrightarrow V_{i+j-k-1}$. So, V_n under the $(n-1)^{th}$ product is a finite dimensional algebra, denoted $(V_n, (n-1)^{th})$.

In addition, (a) if $dim(V_0) = 1$, $(V_1, 0^{th})$ is a Lie algebra; (b) if $dim(V_0) = 1$ and $dim(V_1) = 0$, then $(V_2, 1^{st})$ is a commutative algebra with a symmetric, associative form $(ab, c) = (a, bc)$.

Algebras as in (b) are sometimes called *Griess algebras.*

A *vertex algebra (VA)* over a commutative ring K is a graded K-module with a set of axioms similar to the VOA axioms. There is an analogue of a vacuum element but there is not necessarily an analogue of a Virasoro element [**?**, **?**].

In the Frenkel-Lepowsky-Meurman VOA $V^\natural$, $(V_2^\natural, 1^{st})$ is a commutative nonassociative algebra of dimension 196884, essentially the algebra I defined to construct the Monster.

Automorphism group of a finitely generated VOA is an algebraic group, a theorem of Chongying Dong and myself [**?**]. Our paper has some results about derivation algebras of VOAs.

Graded complex representations for other groups?

The authors Duncan, Mertens and Ono [**?**] have constructed graded spaces for the O'Nan sporadic group, order $2^9 3^3 5 \cdot 7^3 11 \cdot 19 \cdot 31$ with number theoretic properties. The graded traces in one version are weight $\frac{3}{2}$ modular forms. These graded spaces do not (yet?) have additional algebraic properties like a VOA does. This is a very interesting advance. Moonshine for other pariahs has been sought for decades. This "O'Nanshine" seems to be the best so far.

There is an automorphism of order 2 of the O'Nan group whose fixed point subgroup is isomorphic to J_1. So the O'Nanshine space gives a kind of Moonshine for J_1.

Lattices, vertex algebras and applications

The articles [**?**, **?**] by Chongying Dong and myself establish a beginning to a theory of (group-invariant) integral forms in VOAs, and give an integral form in $V^\natural$ which is invariant under the Monster. Carnahan [**?**] shows that there is even one which is self-dual. None of these Monster-invariant forms is given an explicit description, unfortunately.

There is a standard integral form in the lattice VOA V_L, for any even lattice L, given with explicit generators [**?**]. Moreover, when L is a root lattice of type ADE, those natural generators which lie in the degree 1 term form a standard Chevalley basis of the finite dimensional simple complex Lie algebra $((V_L)_1, 0^{th})$ as well as a basis for the intersection of the standard integral form in V_L with $(V_L)_1$. So, we have a natural generalization of usual Chevalley basis and root lattice to an integral form in the lattice VOA V_L.

Is every finite group the automorphism group of a VOA?

There is a natural question, in the spirit of Noether's inverse Galois problem (given a finite group, G, is there a Galois field extension K of the rationals $\mathbb{Q}$ so that $Gal(K/\mathbb{Q}) \cong G$?). The Noether problem is not settled.

Given a finite group G, is there a VOA whose automorphism group is G? The answer is unknown in general but is yes for $G = \mathbb{M}$ and a variety other finite groups. Automorphism groups of VOAs are studied in articles of Dong, Griess, Nagaomo and Ryba [**?**, **?**, **?**]. One of the interesting cases of large rank is the occurrence of $2^{27}.E_6(2)$; see Shimakura [**?**]

For VAs over fields of positive characteristic, there are more results. In particular, there is a fairly natural affirmative answer for G which is an adjoint form Chevalley or Steinberg group extended upwards by diagonal and graph automorphisms, proved by Ching Hung Lam and myself [**?**, **?**]. This result makes use of the standard integral form in V_L.

Short existence proof of the Monster and MVOA

Shimakura [**?**] gave a relatively short existence proof of a Moonshine VOA using a theory of Miyamoto about simple current modules for a VOA [**?**]. Ching Hung Lam and I used this construction of an MVOA to give a relatively short existence proof for the Monster [**?**]. The very long calculations in earlier proofs [**?**, **?**] are now avoidable, a sign of progress.

The relationship between VOA theory and finite simple groups has become stronger.

So far, there is no uniqueness result for an MVOA or for its 196884-dimensional algebra $(MVOA_2, 1^{st})$ associated to the Monster construction. For some partial results, see [**?**].

Final remarks

(1) Uniqueness of Monster was proved by Griess, Meierfrankenfeld and Segev [**?**]. This article contains a proof of the group order $2^{46}3^{20}5^{9}7^{6}11^{2}13^{3}17{\cdot}19{\cdot}23{\cdot}29{\cdot}31{\cdot}41{\cdot}47{\cdot}59{\cdot}71$ and the first proof that the action of the Monster on pairs of $2A$-involutions has nine orbits.

(2) In year 1975, during the Rutgers special year in finite groups, Bernd Fischer visited for a few weeks and lectured on aspects of his ω-transposition groups, especially his $\{3, 4\}$-transposition groups. In conversations, he showed me work on the so-called Y-diagrams. The nodes corresponded to $2A$-involutions in the Monster. Two nodes are disconnected if the pair of involutions commute and are connected if the two involutions generate a dihedral group of order 6. He showed me examples of such involutions forming diagrams which look like Y, with arms of various lengths.

Interesting results on Y-diagrams are discussed in the Atlas of Finite Groups [**?**], though sometimes without references or indications of proofs.

(4) Serge Lang noted the Monstrous Moonshine excitement, which got started with the number $196884 = 1 + 196883$. Serge, who was very conscious about politics, told me that the way he remembers 196884 is to recall 1968 (year of political conflict in Paris and Chicago) and 1984 (the title of George Orwell's famous novel).

(5) I learned about the O'Nan sporadic group from Jon Alperin's lecture in Warwick, May, 1973. Mike O'Nan was interested in finite groups G with the following property: given E, F, a pair of elementary abelian 2-group contained in G of maximal rank, and two maximal flags $1 = E_0 < E_1 < \cdots, E_r = E$ and $1 = F_0 < F_1 < \cdots, F_r = F$, then there exists an element $g \in G$ so that $gE_ig^{-1} = F_i$ for $i = 0, 1, \ldots r$. This property could be called *transitivity on maximal flags of 2-subgroups*. O'Nan thereby found a new sporadic group, now called *the O'Nan group*. See [**?**, **?**].

The group J_1 has this property; this easy to see because the Sylow 2-normalizer is a semidirect product of an elementary abelian group of order 8 by a nonabelian group of order 21, acting faithfully. See [**?**] for a list.

The O'Nan group is the only sporadic group found by a strategy which was not one of the main themes I indicated early in this lecture.