Computing with the Monster Group

(a public service announcement)

Tomasz Popiel

Monash University

joint work with Heiko Dietrich and Melissa Lee

using software developed by Martin Seysen

ACC 2023

"Motivation"

Typical theorem about "highly symmetric" combinatorial structures:

If S is some structure with a group G of automorphisms that acts with some symmetry property P, then (S, G) belongs to some list of examples.

Typical proof strategy:

- P restricts the structure of G;
- reduce to $T \leq G \leq \mathrm{Aut}(T)$ with T a non-abelian simple group;
- the CFSG tells you the candidates for T;
- the list of maximal subgroups of T tells you the candidates for (at least the overgroups of) the stabiliser of an 'element' of S.

Problem: the maximal subgroups of the non-abelian finite simple groups are not completely understood; a notorious case is the Monster.

The Monster

The Monster, $\mathbb{M}$, is the largest of the 26 sporadic finite simple groups.

Existence predicted by Fischer and Griess (1973), as a simple group with certain involution centralisers ($2.\mathbb{B}$ and $2^{1+24}.\mathrm{Co}_1$). It follows that

$$|\mathbb{M}| = 2^{46}.3^{20}.5^{9}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71 \approx 8 \times 10^{53}.$$

It was also predicted that $\mathbb{M}$ has an irreducible complex representation of dimension 196883. This gave the character table (Fischer et al. 1979).

Griess (1982) finally constructed $\mathbb{M}$ as the automorphism group of a certain commutative, non-associative algebra on $\mathbb{R}^{196884}$.

Uniqueness was proved by Griess, Meierfrankenfeld and Segev (1989).

Later: other descriptions (Moonshine), presentations.

The maximal subgroups of $\mathbb{M}$

Every maximal subgroup of $\mathbb{M}$ is the normaliser of a direct product H of isomorphic simple groups. Two cases:

- H is an elementary abelian p-group (the "p-local" case), or
- H is a direct product of isomorphic non-abelian simple groups.

An incomplete list appeared in the Atlas (1985), without proofs.

The p-local case was formally dealt with later:

- $p = 2$ — Meierfrankenfeld and Shpectorov (2002–2003);
- $p = 3$ — Wilson (1988);
- $p \geq 5$ — due to Norton but published by Wilson (1988).

Norton and Wilson (1998–2002) then began work on non-local maximals, reducing the unclassified simple subgroups of $\mathbb{M}$ to 19 partially open cases.

Unsettled cases, per Norton–Wilson (2002)

TABLE 3. *Class fusions not yet eliminated.*

Group	Class fusions
$L_2(7)$	$2B$, $3C$, 4, $7B$
A_6	$2B$, $3B$, $3B$, 4, $5B$
$L_2(8)$	$2B$, $3B$, $7B$, 9
$L_2(11)$	$2B$, $3B/B/C$, $5B$, $6B/E/F$, $11A$
$L_2(13)$	$2B$, $3B/B/C$, $6B/E/F$, $7B$, $13A$
$L_2(17)$	$2B$, $3B$, 4, 8, 9, $17A$
$L_2(19)$	$2B$, $3B$, $5B$, 9, $19A$
$L_2(16)$	$2B$, $3B/C$, $5B$, $15C/D$, $17A$
$L_3(3)$	$2B$, $3A/B/B$, $3C$, 4, $6C/B/E$, 8, 13
	$2B$, $3B$, $3B$, 4, $6B/E$, 8, $13A$
$U_3(3)$	$2B$, $3A/B/B$, $3B$, 4, $4C$, $6C/B/E$, $7A$, 8, 12
	$2B$, $3A/B/B$, $3C$, 4, 4, $6C/B/E$, $7B$, 8, 12
M_{11}	$2B$, $3B$, $4D$, $5B$, $6B/E$, $8F$, $11A$
$L_2(27)$	$2B$, $3B$, $7B$, 13, $14C$
$L_2(31)$	$2B$, $3B$, $4C$, $5B$, $8A/E$, $15C$, $16A/B$, $31AB$
$L_3(4)$	$2B$, $3B$, $4C$, $4C$, $4C$, $5B$, $7A$
$U_4(2)$	$2B$, $2B$, $3B$, $3B$, $3B$, 4, $4D$, $5B$, 6, 6, 6, 6, 9, 12
$\mathrm{Sz}(8)$	$2B$, 4, $5B$, 7, 13
$U_3(4)$	$2B$, $3C$, 4, $5B$, $5B$, $10D/E$, 13, $15D$
$L_2(71)$	$2B$, $3B$, $4C$, $5B$, $6E$, $7B$, $9B$, $12I$, $18D$, $35B$, $36D$, $71AB$
$U_3(8)$	$2B$, $3A/A/C$, $3B$, 4, 4, 4, $6C/C/F$, $7A$, $9A/B/A$, $19A$, $21A/A/C$

Note. Alternatives where given should be read in parallel. For example, an $L_2(11)$ is of type $(3B, 6B)$ or $(3B, 6E)$ or $(3C, 6F)$.

Computation in $\mathbb{M}$, à la Holmes and Wilson

Many remaining cases required computation in $\mathbb{M}$, which was problematic:

- the smallest faithful matrix representation has dimension 196882;
- the smallest faithful permutation representation has degree $\approx 10^{20}$.

Holmes and Wilson (2003) constructed $\mathbb{M}$ computationally by restricting its 196882-dimensional $\mathbb{F}_3$-module to an involution centraliser $2^{1+24}.\mathrm{Co}_1$ (and adjoining a certain extra element, with a different representation).

Ignoring the details (!), the main point is that 196882×196882 matrices can be built from smaller pieces. They found further maximal subgroups

$$L_2(19){:}2,\ L_2(29){:}2,\ L_2(59),\ L_2(71).$$

Norton and Wilson (2013) also found a new maximal subgroup $L_2(41)$; some additional cases were handled theoretically by Wilson (2016–17).

Unsettled cases, circa 2017

At this point (based on some 15 papers!) it was known that any further maximal subgroup of $\mathbb{M}$ must be almost simple with socle

$$L_2(8),\ L_2(13),\ L_2(16),\ \text{or}\ U_3(4).$$

Wilson (2016–2017) reported that all cases apart from $L_2(13)$ had been eliminated, but proofs never appeared.

We decided to try our luck at settling these cases, beginning with $L_2(13)$.

Problem: Holmes and Wilson's computer construction was slow, and (more to the point) essentially impossible for anyone else to reproduce (not implemented in GAP/Magma, nor even publicly available).

A new computer construction of $\mathbb{M}$: `mmgroup`

Meanwhile, we had learned of a new computer construction of $\mathbb{M}$ due to Seysen[1] (2020+), which is much faster than previous implementations:

> An implementation [14] based on that idea multiplies two random elements of $\mathbb{M}$ in a bit less than 50 milliseconds on a standard PC with an Intel i7-8750H CPU at 4 GHz. This is about 100000 times faster than estimated by Wilson [15] in 2013.

Elements of $\mathbb{M}$ are represented as words in generators for a certain 'large' subgroup of a $2B$-involution centraliser $G_{x0} \cong 2^{1+24}.\mathrm{Co}_1$, plus a certain extra element. (Similar idea/different implementation to Holmes–Wilson.)

The details are complicated (conceptually, and in terms of code), but Seysen's main new idea is an efficient word-shortening algorithm:

> So we may reconstruct an element g of $\mathbb{M}$ as a word in the generators of $\mathbb{M}$ from the images of three fixed vectors in the representation ρ under the action of g. It suffices if these three fixed vectors (v_1, v^+, v^-) are known modulo 15. This leads to an extremely fast word shortening algorithm.

[1] https://github.com/Martin-Seysen/mmgroup (written in Python; freely available)

Capabilities of `mmgroup`

Some things that you can do in `mmgroup` (besides the group operation):

- Calculate the order of an arbitrary element of $\mathbb{M}$.
- Conjugate any involution into the centraliser $G_{x0} \cong 2^{1+24}.\mathrm{Co}_1$ of a distinguished $2B$-involution — computation in G_{x0} is especially fast.
- Calculate certain character values of an arbitrary element of G_{x0}.
- Select random elements from $\mathbb{M}$, G_{x0}, and certain subgroups of G_{x0}.

Some things that you can't do in any easy way (but that we need to do):

- Construct centralisers/conjugate elements within an arbitrary class.
- Construct the normaliser of e.g. a cyclic subgroup.
- Determine character values of elements outside of G_{x0}.
- Construct a subgroup from a set of generators.
- Select random elements from such a subgroup.

Our results

Theorem (Dietrich, Lee, Popiel; 2023+)

The Monster has

- a unique class of maximal subgroups that are almost simple with socle $L_2(13)$ — these are isomorphic to $\mathrm{Aut}(L_2(13)) = L_2(13){:}2$;
- a unique class of maximal subgroups that are almost simple with socle $U_3(4)$ — these are isomorphic to $\mathrm{Aut}(U_3(4)) = U_3(4){:}4$;
- no maximal subgroups that are almost simple with socle $L_2(8)$ or $L_2(16)$.

Corollary

The classification of the maximal subgroups of $\mathbb{M}$ is complete.

Proof strategy — $L_2(13)$ case

$G = L_2(13)$ is generated by subgroups 13:6 and D_{12} intersecting in the 6.

Wilson (2015) implies that all elements of order 13 in G must lie in $\mathbb{M}$-class "13A", so first find some $g_{13} \in 13A$. (This is already hard.)

Construct $N_{\mathbb{M}}(\langle g_{13} \rangle) \cong ((13{:}6) \times L_3(3)).2$, and thereby construct all $\mathbb{M}$-classes of subgroups 13:6 containing g_{13}. There are five of them.

For each 13:6, find all involutions i_2 that invert an element g_6 of order 6, so that $\langle g_6, i_2 \rangle \cong D_{12}$. This is done via random search in $N_{\mathbb{M}}(\langle g_6 \rangle)$, which is constructed by projecting its overgroup $C_{\mathbb{M}}(g_6^3) \cong 2^{1+24}.\mathrm{Co}_1$ to $\mathrm{Co}_1 < \mathrm{GL}_{24}(2)$ in Magma using some 'hidden' functionality in `mmgroup`.

Check each involution to see whether it extends 13:6 to $G = L_2(13)$. If so, check whether G has trivial centraliser (if not, then G is not maximal).

One class of $L_2(13)$ with trivial centraliser arises — find an extra generator that extends it to a maximal subgroup $L_2(13){:}2$ of $\mathbb{M}$.

Generators for a maximal $L_2(13){:}2 < \mathbb{M}$

```
g13 = MM("M<y_519h*x_0cb8h*d_3abh*p_178084032*l_2*p_2344320*l_2*p_471482*l_1*t_1*l_
    2*p_2830080*l_2*p_22371347*l_2*t_2*l_1*p_1499520*l_2*p_22779365*l_2*t_1*l_2*p_
    2597760*l_1*p_11179396*t_1*l_1*p_1499520*l_2*p_85838017*t_2*l_1*p_1499520*l_1*p_
    64024721*t_2*l_2*p_2386560*l_2*p_21335269>")

g6 = MM("M<y_764h*x_590h*d_0bf6h*p_63465756*l_1*p_24000*l_2*p_528432*t_1*l_2*p_
    1457280*l_1*p_23214136*l_1*t_2*l_2*p_2344320*l_2*p_13038217*l_2*t_1*l_2*p_
    2956800*l_1*p_85332887*t_2*l_2*p_2830080*l_2*p_85335745*t_2*l_2*p_1900800*l_2*p_
    13472*t_2*l_2*p_2386560*l_2*p_85413728*t_1*l_2*p_2386560*l_2*p_53803593>")

i2 = MM("M<y_6ch*x_7ch*d_52ah*p_115885662*l_2*p_2787840*l_2*p_12552610*l_2*t_1*l_2*p
    _1900800*l_2*p_31998118*l_2*t_2*l_2*p_80762880*l_1*p_243091248*l_2*t_1*l_2*p_
    2597760*l_1*p_42794439*t_1*l_1*p_1394880*l_2*p_64015152*t_1*l_1*p_2027520*l_1*p_
    177984*t_1*l_2*p_79432320*l_1*p_161927136>")

a12 = MM("M<y_1afh*x_1661h*d_2ddh*p_208095583*l_2*p_1943040*l_2*p_1974295*l_2*t_2*l_
    2*p_1900800*l_2*p_10778*l_2*t_2*l_2*p_1900800*l_2*p_1868387*l_1*t_1*l_2*p_
    2956800*l_1*p_11159238*t_1*l_2*p_1985280*l_1*p_86275805*t_2*l_2*p_2386560*l_2*p_
    42712609*t_2*l_1*p_1499520*l_1*p_106699812>")
```

LISTING 6. Generators g_{13}, g_6, i_2, and a_{12} for a maximal subgroup of $\mathbb{M}$ isomorphic to $\mathrm{PSL}_2(13){:}2$ in `mmgroup` format; see also Proposition 3.5 and [12]. Note that g_{13} is the same element as in Listing 5, and that $g_6 = y_6 x_6$ with y_6 and x_6 as in Listing 5.

Thank you!

$2{\cdot}\mathbf{B}$	$(7{:}3 \times \mathrm{He}){:}2$	$(\mathrm{PSL}_2(11) \times \mathrm{PSL}_2(11)){:}4$
$2^{1+24}{\cdot}\mathrm{Co}_1$	$(\mathrm{A}_5 \times \mathrm{A}_{12}){:}2$	$13^2{:}2\mathrm{PSL}_2(13).4$
$3{\cdot}\mathrm{Fi}_{24}$	$5^{3+3}{\cdot}(2 \times \mathrm{PSL}_3(5))$	$(7^2{:}(3 \times 2\mathrm{A}_4) \times \mathrm{PSL}_2(7)).2$
$2^{2.2}\mathrm{E}_6(2){:}\mathrm{S}_3$	$(\mathrm{A}_6 \times \mathrm{A}_6 \times \mathrm{A}_6).(2 \times \mathrm{S}_4)$	$(13{:}6 \times \mathrm{PSL}_3(3)).2$
$2^{10+16}{\cdot}\mathrm{P}\Omega^+_{10}(2)$	$(\mathrm{A}_5 \times \mathrm{PSU}_3(8){:}3){:}2$	$13^{1+2}{:}(3 \times 4\mathrm{S}_4)$
$2^{2+11+22}{\cdot}(\mathrm{M}_{24} \times \mathrm{S}_3)$	$5^{2+2+4}{:}(\mathrm{S}_3 \times \mathrm{GL}_2(5))$	$\mathrm{PSU}_3(4){:}4$
$3^{1+12}{\cdot}2{\cdot}\mathrm{Suz}{:}2$	$(\mathrm{PSL}_3(2) \times \mathrm{PSp}_4(4){:}2){\cdot}2$	$\mathrm{PSL}_2(71)$
$2^{5+10+20}{\cdot}(\mathrm{S}_3 \times \mathrm{PSL}_5(2))$	$7^{1+4}{:}(3 \times 2\mathrm{S}_7)$	$\mathrm{PSL}_2(59)$
$\mathrm{S}_3 \times \mathrm{Th}$	$(5^2{:}[2^4] \times \mathrm{PSU}_3(5)).\mathrm{S}_3$	$11^2{:}(5 \times 2\mathrm{A}_5)$
$2^{3+6+12+18}{\cdot}(\mathrm{PSL}_3(2) \times 3\mathrm{S}_6)$	$(\mathrm{PSL}_2(11) \times \mathrm{M}_{12}){:}2$	$\mathrm{PSL}_2(41)$
$3^8{\cdot}\mathrm{P}\Omega^-_8(3).2$	$(\mathrm{A}_7 \times (\mathrm{A}_5 \times \mathrm{A}_5){:}2^2){:}2$	$\mathrm{PSL}_2(29){:}2$
$(\mathrm{D}_{10} \times \mathrm{HN}){\cdot}2$	$5^4{:}(3 \times 2{\cdot}\mathrm{PSL}_2(25)){:}2$	$7^2{:}\mathrm{SL}_2(7)$
$(3^2{:}2 \times \mathrm{P}\Omega^+_8(3)){\cdot}\mathrm{S}_4$	$7^{2+1+2}{:}\mathrm{GL}_2(7)$	$\mathrm{PSL}_2(19){:}2$
$3^{2+5+10}.(\mathrm{M}_{11} \times 2\mathrm{S}_4)$	$\mathrm{M}_{11} \times \mathrm{A}_6{\cdot}2^2$	$\mathrm{PSL}_2(13){:}2$
$3^{3+2+6+6}{:}(\mathrm{PSL}_3(3) \times \mathrm{SD}_{16})$	$(\mathrm{S}_5 \times \mathrm{S}_5 \times \mathrm{S}_5){:}\mathrm{S}_3$	$41{:}40$
$5^{1+6}{:}2{\cdot}\mathrm{J}_2{:}4$		