The taming of the Monster

Robert A Wilson

Wednesday 4th December 2002
Auckland

Groups are the abstract embodiment of symmetry in mathematics, and as such their study is of fundamental importance wherever symmetry can be used to simplify problems.

The trouble is that groups are complicated objects, despite their simple definition, and a complete classification of them is hopeless.

We can however sometimes break them down into smaller groups: if N is a normal subgroup of a group G, then the set $G/N = \{Ng : g \in G\}$ of cosets $Ng = \{ng : n \in N\}$ forms a *quotient group*. In these circumstances, we can study G by studying the smaller groups N and G/N, *and* the way they are stuck together to form G.

If we cannot break the group down in this way, it is called *simple*. Clearly a group of prime order is simple, as it has no subgroups at all. All other simple groups are non-abelian (i.e. non-commutative).

Galois initiated the study of non-abelian simple groups in the 1830s: the fact that the alternating group A_5 is simple proves that the general quintic equation is not soluble by radicals.

He found a number of other simple groups, including what we now call $\mathrm{PSL}_2(p)$, for primes $p \geq 5$.

The obvious question is, can we find *all* the finite simple groups? Well, to cut a long story short . . .

CFSG

the Classification theorem for Finite Simple Groups

Every finite simple group is either:

- *a cyclic group of prime order*
- *an alternating group of degree at least 5*
- *a group of Lie type, or*
- *one of 26 sporadic simple groups*

Alternating groups

The *symmetric group* of degree n consists of all permutations of n points. Half the $n!$ permutations are *even*, which means they can be written as the product of an even number of transpositions.

The *alternating group* A_n of degree n consists of these $\frac{1}{2}n!$ even permutations. For every $n \geq 5$, A_n is a simple group.

Groups of Lie type

can be thought of as matrix groups.

E.g. $\mathrm{GL}_n(q)$ consists of all invertible $n \times n$ matrices over the field of q elements.

$\mathrm{SL}_n(q)$ is the subgroup of matrices of determinant 1.

$\mathrm{PSL}_n(q)$ is the quotient of $\mathrm{SL}_n(q)$ by the subgroup of scalar matrices, and is simple for almost all values of n and q.

Sporadic groups

The sporadic simple groups range in size from

the smallest Mathieu group, M_{11}, discovered by Emile Mathieu in 1860, and having just 7920 elements,

to

the Monster, $\mathbb{M}$, discovered by Fischer and Griess in about 1973, and having

$$808017424794512875886459904961710$$

$$757005754368000000000$$

elements.

Families of sporadic groups

- The five **Mathieu groups**, M_{11}, M_{12}, M_{22}, M_{23} and M_{24}, permutation groups on 11, 12, 22, 23, 24 points respectively. The biggest one, M_{24}, contains all the others (as subgroups).

- The seven **Leech lattice groups**, J_2, Suz, HS, McL, Co_3, Co_2, Co_1, matrix groups in (up to) 24 dimensions. The biggest one, Co_1, involves all the others (as quotients of subgroups), as well as all the Mathieu groups.

- The three **Fischer groups**, Fi_{22}, Fi_{23}, Fi'_{24}. The biggest one, Fi'_{24}, involves all the others (as quotients of subgroups), as well as all the Mathieu groups.

- The **Monstrous groups**, He, HN, Th, B and $\mathbb{M}$. The Monster $\mathbb{M}$ involves all the groups we've seen so far.

- The **Pariahs** or **oddments**, J_1, J_3, J_4, Ru, ON, Ly, not involved in the Monster. These do not really form a family, although J_1 is a subgroup of ON.

Apart from the Monster and the Baby Monster B, all these groups are named after their discoverers: Mathieu, Janko, Suzuki, Higman, Sims, McLaughlin, Conway, Fischer, Held, Harada, Norton, Thompson, Rudvalis, O'Nan and Lyons.

How to calculate in the sporadic groups

as permutation groups:

Group	Number of points	
M_{11}	11	
M_{12}	12	
M_{22}	22	
M_{23}	23	
M_{24}	24	
J_2	100	
HS	100	
McL	275	
Co_3	276	
Suz	1782	
Co_2	2300	
Co_1	98280	if you dare!
Fi_{22}	3510	
Fi_{23}	31671	
Fi_{24}'	306936	ouch!

Group	Number of points	
J_1	266	
J_3	6156	
J_4	173067389	this is getting silly!
Ru	4060	
ON	122760	
Ly	8835156	
He	2058	
HN	1140000	
Th	143127000	
B	13571955000	seriously hard
$\mathbb{M}$	c. 10^{20}	impossible

or as matrix groups (over finite fields, sometimes modulo scalars):

Group	Dimension	Field size	
M_{11}	5	3	
M_{12}	6	3	
M_{22}	10	2	
M_{23}	10	2	
M_{24}	11	2	
J_2	6	4	
Suz	12	4	
HS	20	2	
McL	21	3	
Co_3	22	2	
Co_2	22	2	
Co_1	24	2	
Fi_{22}	77	3	
Fi_{23}	253	3	
Fi_{24}'	781	3	biggish

Group	Dimension	Field size	
J_1	7	11	
J_3	9	4	
J_4	112	2	
Ru	28	2	
ON	45	7	
Ly	111	5	
He	50	7	
HN	132	4	
Th	248	2	
B	4370	2	quite big
$\mathbb{M}$	196882	2	rather tricky

All these representations except the really big ones are available on my website

http://www.mat.bham.ac.uk/atlas/

But how can we calculate in the Monster, when each matrix occupies 5 gigabytes, and a matrix multiplication takes weeks of CPU time?

We want to represent an element of the Monster, in effect as a matrix. But what is a matrix really? It is encoding an *action* on the underlying vector space. And the action is computed by a familiar algorithm called ‘matrix multiplication’.

But what if we encode the action in a different way, and devise a more efficient algorithm for computing the action of a particular group element on a particular vector?

Joint work with RA Parker, PG Walsh, SA Linton (published 1998), constructed the 196882-dimensional representation over $\mathbb{F}_2$ (i.e. the field $\{0,1\}$ defined by $1+1=0$) in this way.

The idea is to

take some nice, big, 3-local subgroups (i.e. normalizers of 3-subgroups),

write their elements in a reasonably compact ('sparse') form,

and glue them together to make the whole group.

Joint work with PE Holmes (to appear in JLMS), constructed the 196882-dimensional representation over the field $\mathbb{F}_3 = \{0, 1, 2\}$ of integers modulo 3.

Here we can work with 2-local subgroups, which are much bigger and nicer than the 3-local subgroups we used before.

We start with the centralizer $C_{\mathbb{M}}(x)$ of an element x of order 2. This subgroup has the shape

$$2^{1+24}{}^{\cdot}\mathrm{Co}_1$$

and the 196882-space breaks up as

$$298 \oplus 98280 \oplus 98304$$

But what makes this really nice is that the 98304 is a tensor product $24 \otimes 4096$, and the 98280 is monomial, so that all the information for this representation can be stored in a relatively small amount of space.

Moreover, the action of such an element on a vector in the 196882-space is easy to compute.

Also, the product of two elements in this subgroup can be computed fairly quickly, as can the inverse of an element.

Now all we need is one more element to generate the Monster.

To find one, centralize another involution:

$$C_{\mathbb{M}}(x,y) = 2^2.2^{11}.2^{22}.\mathrm{M}_{24}$$

acting on the space as

$$(22 \oplus 276)$$

$$\oplus$$

$$(276 \oplus 276 \oplus 48576 \oplus 49152)$$

$$\oplus$$

$$(49152 \oplus 49152)$$

Then we adjoin a suitable element t cycling the three 276-spaces and the three 49152-spaces.

To summarise, we generate the Monster with three elements

a, b generating the centralizer $2^{1+24}\cdot\mathrm{Co}_1$ of a certain involution x.

t conjugating x to y and y to xy, where y is a certain involution in $C(x)$.

a and b are each stored as: a 24×24 matrix, a 4096×4096 matrix, a 298×298 matrix, and a monomial permutation on 98280 points and their negatives.

t is stored as a monomial permutation on 147456 points, a 64×64 matrix (acting identically on 759 64-spaces), and an 850×850 matrix.

Words in a and b can be readily evaluated, to give another element of $C(x)$ in the same format.

Words involving t cannot be evaluated.

Applications

Elements of the Monster are now stored as words $x_1t_1x_2t_2\cdots$ where $x_i \in C(x)$ and $t_i = t^{\pm 1}$.

Element orders can be guessed by picking a ‘random’ vector v and finding the smallest n such that $v(x_1t_1x_2t_2\cdots)^n = v$.

Indeed, we can use the structure of $\mathbb{M}$ to find two vectors v_1 and v_2 with the property that if $v_1g = v_1$ and $v_2g = v_2$ then $g = 1$. Thus we can prove that an element has the order we guessed.

The Monster is a Hurwitz group

i.e. it can be generated by X of order 2 and Y of order 3, with XY of order 7.

Proof: take random elements of orders 2 and 3, until you find a pair whose product has order 7. (Patience will be required: the probability in each case is about 10^{-8}, roughly equal to the chance of throwing ten sixes in a row.)

Check the orders of lots of words in X and Y, until you find elements of orders incompatible with being in a proper subgroup (orders 71 and 94, say).

The central problem

is that we cannot multiply elements of the Monster together: the words just get longer and longer until we are completely swamped. We need:

a word-shortener

We have one!

which relies on

- the fact that if a word represents an element of $C(x)$, then we can calculate the compact form of this element by evaluating just 36 rows of the full 196882×196882 matrix, and

- if an involution conjugate to x commutes with x, then we can find a word of length 4 giving an element which realises this conjugation.

With these amazing tools, we can tackle real problems, such as determining the

maximal subgroups

It is easy to show that if H is a maximal subgroup of a simple group G, and K is a minimal normal subgroup of H, then

- $H = N_G(K)$, and

- K is a direct product of isomorphic simple groups

Now let $G = \mathbb{M}$. The case when K is a p-group was handled by RAW for p odd and Meierfrankenfeld and Shpektorov for $p = 2$.

The case when K is non-abelian was studied by Norton, RAW, etc., and reduced to the case K simple, and isomorphic to one of a specified list of 22 simple groups.

The 22 cases are:

$\mathrm{PSL}_2(q)$ for $q = 7, 8, 9, 11, 13, 16, 17, 19, 23, 27, 29, 31, 59, 71$, and

$\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSU}_3(3)$, $\mathrm{PSU}_3(4)$, $\mathrm{PSU}_3(8)$, $\mathrm{PSU}_4(2)$, Sz(8) and M_{11}.

Joint work with PE Holmes: we have dealt with 15 of these 22 cases.

In particular there are (previously unknown) maximal subgroups

$\mathrm{PSL}_2(59)$, $\mathrm{PSL}_2(71)$, $\mathrm{PGL}_2(29)$, $\mathrm{PGL}_2(19)$.