Semi-presentations of sporadic simple groups

Simon Nickerson

simonn@maths.bham.ac.uk

School of Mathematics

University of Birmingham

United Kingdom

Standard generators

Let G be a finite group with generators x and y. Suppose we are able to characterise the elements x and y up to group automorphisms using group theoretic data. Such a characterisation is said to be a *definition of standard generators for* G. The generators x and y (satisfying this characterisation) are said to be *standard generators of* G.

Standard generators: some examples

Example 1. *Let $G = M_{12}$, the Mathieu group of order 95040. The group G is generated by elements x and y such that x is in class $2B$ (i.e. x has order 2 and $|C_G(x)| = 192$), y is in class $3B$ (i.e. y has order 3 and $|C_G(x)| = 36$) and xy has order 11.*

These conditions characterise x and y up to automorphisms of G, so they provide a definition of standard generators.

Example 2. *Let $G = M_{23}$, the Mathieu group of order 10200960. Standard generators of G are elements x and y where x has order 2, y has order 4, xy has order 23 and $xyxyxy^2xyxy^2xy^2$ has order 8.*

Black box groups

A *black box group (with order oracle)* is a group G is a group whose elements are coded as strings of length at most N over the alphabet $Q = \{0, 1\}$ for some positive integer N (an element may have more than one such coding) and where given strings representing group elements $g, h \in G$, we can:

- compute a string encoding gh;
- compute a string encoding g^{-1}; and
- decide whether $g = 1$; and
- compute the order of g.

Examples of black box groups are permutation groups of finite degree, matrix groups over finite fields and polycyclic representations of solvable groups.

Semi-presentation

A *semi-presentation* for a group G is essentially a method of testing whether two elements of a black box group H (known to be isomorphic to G) are standard generators.

More precisely, a semi-presentation is a collection of words in $w_i(x, y)$ in x and y together with some integers o_i such that for any elements $x, y \in G$ the following are equivalent:

- $o(w_i(x, y)) = o_i$ for all i;
- x and y are standard generators.

Semi-presentations: a simple example

Recall that standard generators of M_{23} are elements x and y where x has order 2, y has order 4, xy has order 23 and $xyxyxy^2xyxy^2xy^2$ has order 8.

We obtain the following semi-presentation for M_{23}:

$$\begin{aligned} M_{23} \approx \langle\langle x, y \mid o(x) = 2, o(y) = 4, o(xy) = 23, \\ o(xyxyxy^2xyxy^2xy^2) = 8\rangle\rangle \end{aligned}$$

So far, so easy. However, not all definitions of standard generators rely only on orders of words.

Standard relations

As we have seen, the definition of standard generators for G gives a number of relations for the semi-presentation. We are always able to write down the relations $o(x) = o_1$, $o(y) = o_2$ and $o(xy) = o_3$ (for integers o_1, o_2 and o_3) and we are sometimes able to write down a few others. These relations are known as the 'standard relations', and are abbreviated by '**std**' in semi-presentations.

For example, the semi-presentation we wrote down before can be abbreviated:

$$M_{23} \approx \langle\langle x, y \,|\, \mathbf{std} \rangle\rangle$$

The rest of this talk will be devoted to finding extra relations which establish the conjugacy classes (not just the orders) of x and y.

The dihedral trick

Most of the time, the first generator x is an involution. The following trick is useful in ensuring that an involution is in the correct conjugacy class.

We have the following fact:

Lemma 3. *If $t, u \in G$ are involutions and $m = o(tu)$ is odd, then t and u are conjugate.*

Proof. Let $H = \langle t, u \rangle$. Then $H \cong D_{2m}$. Then t and u are H-conjugate (because m is odd) and hence G-conjugate. $\square$

Hence we can show that an involution x is in the right conjugacy class if we find another involution t which is definitely in that class and finding a conjugate x^g such that tx^g has odd order. This is the *dihedral trick*.

The dihedral trick: an example

Let $G = J_4$, the largest Janko group. We need to establish that x is in class $2A$. Consulting the ATLAS, we see that all elements with orders 8, 16, 20, 24, 30, 40, 42, 44 and 66 power to class $2A$ in J_4. If x and y are standard generators, the element:

$$z = xyxyxy^2$$

has order 24, so z^{12} is in class $2A$. The element $x(z^{12})^{xy^3xy^3}$ has order 11, which proves that x is in class $2A$ too. Note that when we add the relations to the semi-presentation, we must add *both* of the following relations:

$$o(xyxyxy^2) = 24$$
$$o(x((xyxyxy^2)^{12})^{xy^3xy^3}) = 11$$

Fingerprinting

We can sometimes find a semi-presentation by finding all automorphism classes of pairs (x, y) with $o(x) = o_1$, $o(y) = o_2$ and $o(xy) = o_3$ and finding a word (or set of words) which picks out the class corresponding to standard generators.

We do this by taking a *fingerprint*, which is an n-tuple consisting of the orders of various words in x and y. If two pairs (x, y) and (x', y') are automorphic, then they will have the same fingerprint.

The structure constants of $\mathrm{Aut}(G)$ tell us the number κ of automorphism classes of pairs we should expect. We perform a random search until we find κ different fingerprints. If we fail to find this many, it either means we must search for longer, or we need a longer fingerprint.

Fingerprinting: a simple example

Let $G = M_{22}$. We need to consider the pairs (x, y) with $o(x) = 2$, $o(y) = 4$ and $o(xy) = 11$. There is only one class containing elements of order 2, but there are two classes ($4A$ and $4B$) of elements of order 4. The structure constants tell us that there are 2 fingerprints for the $(2, 4A)$ pairs, and 4 for the $(2, 4B)$ pairs.

For our fingerprint, we will take the following 5-tuple:

$$\begin{aligned} f(x, y) = (&o(xy^2), o(xyxy^2), o([x, y]),\\ &o(xyxyxy^2), o(xyxy^2xy^3)) \end{aligned}$$

which we abbreviate to

$$f(x, y) = (o_4, o_5, \ldots o_8)$$

Fingerprinting: a simple example (ctd)

Then the 6 fingerprints are:

Class	o_4	o_5	o_6	o_7	o_8
4A	5	11	6	11	5
4A	6	8	5	8	5
4B	5	11	5	11	6
4B	6	7	4	7	5
4B	4	8	6	6	6
4B	6	7	4	7	6

The relation $o_5 = 11$ is part of the definition of standard generators, so if we add $o_6 = 6$, then we can complete the semi-presentation:

$$M_{22} \approx \langle\langle x, y \mid \mathbf{std}, o([x, y]) = 6 \rangle\rangle \tag{1}$$

Fingerprinting: a harder example

Let $G = Co_1$, the largest Conway group. We are able to find conditions that establish $x \in 2B$ using the dihedral trick. To find conditions showing $y \in 3C$, we could try fingerprinting the $(2, 3, 40)$-pairs, but there are a lot of them, and they are hard to analyse because not all of them generate G. Instead, we find a $2A$-element t and a $(2A, 3, 36)$ pair (t, y^g) and find fingerprints for all such. This enables us to find conditions which prove that y is a $3C$-element.

Elements of even order

If y is an element of even order, we can sometimes find its class by looking at $t = y^{o(y)/2}$ and using the dihedral trick. Often though, there is more than one class of a given order which powers up to the same class of involution.

However, we may be able to use $C_G(y)$ to distinguish these classes. This is because it is relatively easy to find elements in the centralizer of an involution as words in x and y.

The 2-centralizer trick

Let y be an element of order $2m$ and let $y_1, y_2, \ldots y_k$ be a complete set of class representatives of elements of order $2m$. Suppose p is a prime dividing $|C_G(y_1)|$ but not dividing $|C_G(y_i)|$ for $1 < i \leq k$. To show y is conjugate to y_1, we do the following:

1. Find words in standard generators which generate the involution centralizer $C_G(t)$
2. Find words in the generators of $C_G(t)$ which commute with y, generating a sufficiently large subgroup of $C_G(y)$.
3. Find an element in $C_G(y)$ with order divisible by p. By the centralizer orders, we must have that y is conjugate to y_1.

We call this the 2-centralizer trick.

The 2-centralizer trick: an example

Let $G = J_4$ again. We have shown that x is in class $2A$, but we need to show that y is in $4A$. The group G has three classes of elements of order 4:

$$|C_G(4A)| = 2^{15}.3.5.11$$
$$|C_G(4B)| = 2^{15}.3$$
$$|C_G(4C)| = 2^{11}.3.7$$

So we will try to look for an element t with order divisible by 5 or 11 which commutes with y. Let:

$$c = xyxy^3xyxy$$
$$d = xy^2xy^3xy^2xy$$
$$e = c(y^2(y^2)^c)^5$$
$$f = d(y^2)(y^2)^d$$

The 2-centralizer trick: an example (ctd)

Then e and f are contained in $C_G(y^2)$. A random search shows that:

$$g = (efe)^3(fe)^4 f$$

is an element of order 20 which commutes with y. Hence y must be in class $4A$. We can now write down the full semi-presentation for J_4:

$$\begin{aligned} J_4 \approx \langle\langle x, y, (z, c, d, e, f, g) \,|\, \mathbf{std}, o(z) = 24,& \\ o(x(z^{12})^{xy^3xy^3}) = 11, o(g) = 20,& \\ o([g, y]) = 1; z := xyxyxy^2,& \\ c := xyxy^3xyxy, d := xy^2xy^3xy^2xy,& \\ e := c(y^2(y^2)^c)^5, f := d(y^2)(y^2)^d,& \\ g := (efe)^3(fe)^4 f\rangle\rangle.& \end{aligned}$$

The Monster group

Using the construction of Linton et al., the Monster group $G = \mathbb{M}$ was surprisingly easy to deal with:

1. Find a word c in x and y whose order is in:

   $$S = \{34, 38, 50, 54, 62, 68, 94, 104, 110\}$$

   and power it up to a give an element $d \in 2A$.

2. Find a word e such that $o(xd^e)$ is odd. This would prove that x is a $2A$-element, and also that y is not a $3A$-element (because $o(xy) = 29$).

3. Find a word f such that $o(xy^f)$ is in:

   $$V = \{19, 25, 31, 34, 50, 55, 68, 94\}.$$

   The structure constants then imply that y is not a $3C$-element, so it must be a $3B$-element.

An application

The Web Atlas of Finite Group Representations can currently be found at:

`http://web.mat.bham.ac.uk/atlas/`

We ran our semi-presentations against the representations of sporadic (almost)-simple groups listed in the Web Atlas, and found a few errors:

- The 483-dimensional representation of M_{23} over GF(7) does not exist.
- One of the 896-dimensional representations of HS over GF(4) was wrong.
- The 104-dimensional representation of $He.2$ over GF(5) in fact generated a subgroup of order 30240.
- The 924-dimensional representation of $Fi_{22}.2$ over GF(3) had non-standard generators.