Standard generators for sporadic simple groups

Robert A. Wilson

School of Mathematics and Statistics,
The University of Birmingham,
Edgbaston, Birmingham B15 2TT

published in J. Algebra 184 (1996), 505–515

1 Introduction

In recent years an increasing amount of our knowledge about finite groups, and especially the sporadic simple groups, has been obtained by computer calculations. This has many advantages over more traditional methods, especially speed and accuracy, and problems can be solved that are out of reach of theoretical methods. But there are also some disadvantages, the most frequently mentioned being problems of checking or reproducing results. (The accusation of unreliability need not detain us, as the average published proof 'by hand' is equally, if not more, unreliable.) Much progress has however been made in remedying these deficiencies. A properly carried out computational proof can be much more rigorously and thoroughly checked than any proof 'by hand', and if it is properly documented then there should be no problem with repeating the calculations and reproducing the results. It has to be admitted, however, that many computational results fall far short of these ideal standards.

The aim of the present paper is to make a small contribution towards improving the reproducibility of computational results on the sporadic simple groups. True reproducibility requires that both data and programs be produced independently. As regards programs, there are several independent systems capable of performing basic (or not so basic) calculations with

permutations or matrices. As regards data, the situation is much less satisfactory. Where two independent sets of generators for a given group exist on computers, the two sets usually bear no relation to each other, and it is often all but impossible to obtain one from the other. While it is not to be expected that everyone will agree on what are the 'best' generators for a given group, we should perhaps expect authors to present a method for obtaining the generators they use from any others. In this paper we shall discuss some choices for 'good' generators for the sporadic simple groups, and explain in general terms how to obtain such generators ('standard generators') from any other generators that may be available. In terms of abstract groups, we have an implicit isomorphism

$$\langle g_1, \ldots, g_r \rangle \cong \langle h_1, \ldots, h_s \rangle,$$

and we want to find an explicit isomorphism in the form

$$\phi : g_i \mapsto w_i(h_1, \ldots, h_s)$$

where the w_i are words in $h_1, \ldots, h_s$.

2 Criteria for 'good' generators

Fix the notation, $G = \langle g_1, \ldots, g_r \rangle$, and for simplicity assume that G is a simple group. The generating set $\{g_1, \ldots, g_r\}$ will be called **good** if given any $h_1, \ldots, h_s$ with $\langle h_1, \ldots, h_s \rangle \cong G$, it is easy to find an explicit isomorphism $\phi : g_i \mapsto w_i(h_1, \ldots, h_s)$, and it is easy to prove that ϕ is an isomorphism. Of course, these are vague criteria, and will depend both on the representation of G and on the hardware and software available.

For simplicity, we fix $r = 2$, on the (not necessarily valid!) assumption that two elements are easier to find than three or more. How easy is it to find words giving g_1 and g_2? If we just take random elements of the group, then there are $|G|^2$ ordered pairs of elements, and there are $|G|$ pairs conjugate to (g_1, g_2), so the probability of finding the right generators on each attempt is $1/|G|$. If however we restrict the choice of g_1 and g_2, for example by specifying their orders, then we can greatly increase this probability. Better still, if we specify the conjugacy classes $\mathcal{C}_1$ and $\mathcal{C}_2$ to which g_1 and g_2 belong, then we can make 'random' elements in these classes simply by conjugation, and the

probability of obtaining a conjugate of (g_1, g_2) is

$$Pr_G(\mathcal{C}_1, \mathcal{C}_2) = \frac{\text{no. of conjugates of } (g_1, g_2)}{|\mathcal{C}_1|.|\mathcal{C}_2|} = \frac{|C_G(g_1)|.|C_G(g_2)|}{|G|}.$$

Example 1 (The Thompson group) The Thompson group Th has order roughly 10^{17}, and it turns out that it can be generated by elements $g_1 \in 2A$ and $g_2 \in 3A$. In this case the probability of finding (g_1, g_2) on each attempt is $Pr_{Th}(2A, 3A) \approx 1.6\%$. (In this and later examples, we use the ATLAS notation (see [1]) for conjugacy classes.) How easy is it in this case to determine whether ϕ is an isomorphism? In other words, given $g_1' \in 2A$ and $g_2' \in 3A$, can we determine whether the map $\phi : g_i \to g_i'$ extends to an automorphism of Th? It turns out that if $g_1 g_2 \in 19A$, then ϕ is an isomorphism if and only if $g_1' g_2' \in 19A$. Clearly this is a necessary condition: the sufficiency follows from the theory of structure constants, which we now summarise.

For a triple of conjugacy classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ in G, define the **symmetrised structure constant** $\xi_G(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3)$ by

$$\xi_G(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3) = \frac{|G|}{|C(g_1)|.|C(g_2)|.|C(g_3)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1).\chi(g_2).\chi(g_3)}{\chi(1)}$$

where $g_i \in \mathcal{C}_i$. Then it is well-known that

$$\xi_G(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3) = \sum \frac{1}{|C(g_1, g_2, g_3)|}$$

where the sum is taken over all conjugacy classes of triples (g_1, g_2, g_3) with $g_i \in \mathcal{C}_i$ and $g_1 g_2 g_3 = 1$. In particular, if $\xi_G(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3) = 1$, and there exists such a triple (g_1, g_2, g_3) with trivial centralizer, then all such triples are conjugate.

In the Thompson group, we have $\xi_{Th}(2A, 3A, 19A) = 1$, and $C_{Th}(3A)$ and $C_{Th}(19A)$ have coprime orders, so all triples $g_1 \in 2A, g_2 \in 3A, (g_1 g_2)^{-1} \in 19A$ have trivial centralizer, and are conjugate. The additional requirement that g_1 and g_2 generate Th has to be checked separately, either by explicit computation or by somehow eliminating the possibility that they generate a proper subgroup.

Table 1: Rationally rigid triples in sporadic simple groups

G	$\mathcal{C}_1$	$\mathcal{C}_2$	$\mathcal{C}_3$	$Pr_G(\mathcal{C}_1, \mathcal{C}_2)$
Ru	$2B$	$4A$	$13A$	$1:163$
Co_3	$2A$	$5B$	$24A$	$1:569$
Co_2	$2A$	$5A$	$28A$	$1:19$
Th	$2A$	$3A$	$19A$	$1:77$
Fi_{23}	$2A$	$12D$	$17A$	$1:12$
Co_1	$3A$	$4F$	$35A$	$1:201$
B	$2D$	$3A$	$55A$	$1:918$
M	$2A$	$3B$	$29A$	$1:68$

3 Rationally rigid generators

If G is a simple group with generators g_1, g_2, g_3 such that $g_1g_2g_3 = 1$ and $g_i \in \mathcal{C}_i$, where $\xi_G(\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3) = 1$, then G is called **rigid**. If also the three classes consist of rational elements, then G is called **rationally rigid**. We have seen in the previous section that Th is rationally rigid with respect to the triple of classes $(2A, 3A, 19A)$. The sporadic simple groups which have trivial outer automorphism groups, and are rationally rigid, are listed in Table 1, with a suitable triple of classes found by Pahlings [3].

The advantage of choosing a rigid triple of generators is that it is very easy to check the isomorphism of these with any other set of generators, provided we have an easy way of distinguishing conjugacy classes. Disadvantages are that, depending on the representations and software available, it may be difficult to distinguish classes of elements of the same order; groups often do not have such generators; and even if they do, the probability of finding them may be unreasonably small. In practice, it seems to be much easier to deal with a rationally rigid triple, rather than an arbitrary rigid triple, and in this section we will only consider the former case.

Example 2 (The Rudvalis group) We first need to find some elements in $2B$ and $4A$. This is easy, since if x is any element of order 26 or 14 then x^{13} or x^7 is in $2B$, while if y is any element of order 24, then $y^6 \in 4A$. We also need to recognise elements in class $13A$, but this is also easy since this is the only class of elements of order 13.

Example 3 (Conway's group Co_3) In most of the cases listed in Table 1

again the class $\mathcal{C}_3$ is the only class of elements of the given order, so the recognition problem is easily solved. In the case Co_3, however, there are two classes of elements of order 24, which may be difficult to distinguish. It is therefore advisable to look for some other rigid triple of classes.

Using GAP Version 3.1 [5], we found that $\xi_{Co_3}(3A, 4A, 14A) = 1$, and using the 'Meat-axe' [4] we found that such a triple of elements does in fact generate Co_3. This triple now has the required properties: a $3A$-element is easily found as a power of any element of order 9, 18, 24 or 30, and a $4A$-element as the fifth power of any element of order 20. Moreover, there is only one class of elements of order 14. Thus this triple looks good enough to take as standard generators for Co_3.

Example 4 (Conway's group Co_2) There should be no real problems here if we take the classes $(2A, 5A, 28A)$ given in Table 1. A $2A$-element can be obtained by taking the appropriate power of any element of order 16, 18 or 28. If there is any difficulty in finding a $5A$-element, or distinguishing the classes $5A$ and $5B$, the following procedure can be adopted. First find a subgroup McL, in which any element of order 10, 15 or 30 powers up to an element of Co_2-class $5A$. Finally there is only one class of elements of order 28.

Example 5 (Fischer's group Fi_{23}) In most of the cases listed in Table 1, it is not hard to find some elements in $\mathcal{C}_1$ and $\mathcal{C}_2$ to begin the search for standard generators. However, in Fi_{23} it may not be easy to obtain a $12D$-element. Using GAP again to search for rigid triples, we found that $\xi_{Fi_{23}}(2B, 3D, 28A) = 1$, and using the 'Meat-axe' we found such a triple which generates the whole group. The class $28A$ is determined as the unique class of elements of order 28. The classes $2B$ and $3D$ should be easier to find than the class $12D$. For example, a $2B$-element may be obtained as the 14th power of any element of order 28. There may be slight problems finding a $3D$-element, however, since something more than orders of elements is required to distinguish this class from other classes of elements of order 3.

Example 6 (The Monster) The triple $(2A, 3B, 29A)$ appears to satisfy all our criteria. However, we are not aware of the existence of any representation in which such generators could be explicitly computed!

Table 2: Fingerprints in J_1

Word	$Fp1$	$Fp2$	$Fp3$	$Fp4$	$Fp5$	$Fp6$	$Fp7$
ab	7	7	7	7	7	7	7
$abab^2$	10	10	11	11	15	15	19
$ababab^2$	10	10	11	11	15	15	19
$ababab^2abab^2$	15	15	10	10	6	6	15
$ababab^2abab^2ab^2$	10	6	5	10	5	6	10

4 $(2, 3, n)$-generators

If we cannot find a reasonable rationally rigid triple of generators, then we have to be content with a somewhat harder recognition problem.

For various reasons, it is often desirable to choose g_1 of order 2 and g_2 of order 3 if possible. We may also prefer that the order, n say, of g_1g_2 is fairly small (we necessarily have $n \geq 7$). All the sporadic simple groups can be generated in this way except for M_{11}, M_{22}, M_{23} and McL. This is proved by Woldar in [8].

Example 7 (Janko's group J_1) In J_1 there is one class each of elements of orders 2, 3 and 7, and $\xi_{J_1}(2A, 3A, 7A) = 7$. Since no proper subgroup can be generated by such a triple of elements, there are exactly 7 non-conjugate ways of generating J_1 with a (2,3,7)-triple. We should perhaps choose one of these to be our 'standard' generating set, and find a simple criterion for distinguishing it from the other six. In each case we have elements a of order 2 and b of order 3, and we can work out the orders of various words in a and b in each of the seven cases, as in Table 2.

There is not much to choose between the seven cases, except perhaps that the last one is easiest to recognise. The others come in pairs, related by inverting g_2. (The pair (a, b^{-1}) is called the **reciprocal** of the pair (a, b).)

FINGERPRINTS. The question arises, what words in a and b are most useful? To obtain new information with each new word, we should ensure that no new word is conjugate to an old one, or to a power of it or its inverse. By suitable conjugation we can arrange that each word begins with a and ends with b. Therefore it consists of a string of 'terms' ab and ab^2. Inverting if necessary we may assume it has at least as many terms ab as ab^2, and

by conjugation we can put the longest string of consecutive terms ab at the beginning. Writing $x = ab$ and $y = ab^2$, we obtain the following words, up to length 6 in x and y:

$$x, xy, xxy, xxxy, xxyy, xxxxy, xxxyy, xxyxy,$$

$$xxxxxy, xxxxyy, xxxyxy, xxxyyy, xxyxyy, xxyyxy.$$

(Note that $xyxy$ and $xxyxxy$ are excluded since they are proper powers of shorter words.)

Replacing b by $b^2 = b^{-1}$ gives us a different set of $(2, 3, n)$-generators, (the reciprocal set) which may or may not be conjugate to the first set. The effect on the above words is to exchange x and y, or (by taking a conjugate of the inverse) to read the words backwards from a suitable point. Thus the shortest words which distinguish a pair and its reciprocal are $xxyxyy$ and $xxyyxy$, which are interchanged by this operation.

In Table 2 we gave a small set of words capable of distinguishing all seven cases. In fact the words xy and $xxyxyy$ on their own are sufficient, but of course we could not have known that in advance. In practice, therefore, we take the whole set of 14 words as a 'fingerprint'.

Note: Parker's fingerprint, used in some implementations of the 'Meat-axe', consists of the orders of the words

$$x, xy, xxy, xxyx, xxyxy, xxxyxy, xxxyxyy.$$

Example 8 (Mathieu's group M_{24}) In the Mathieu group M_{24} we have $\xi(2B, 3A, 23A) = \xi(2B, 3A, 23B) = 1$, and such triples generate M_{24}. Thus the group is rigid but not rationally rigid. The two triples look very similar, but are not automorphic. In fact, they are reciprocals of one another, and can be distinguished by a suitable fingerprint. Using the fingerprint

$$x, xy, xxy, xxyy, xxyxy, xxyxyy, xxyyxy, xxxyxyy, xxxyyxy$$

we obtain the lists of orders

$$23, 12, 12, 5, 10, 4, 5, 14, 21$$

and

$$23, 12, 12, 5, 10, 5, 4, 21, 14$$

in the two cases. We choose arbitrarily the first of these to be our 'standard generators' for M_{24}.

Example 9 (Conway's group Co_1) The triple given in Table 1 has the disadvantage that it may be difficult to distinguish an element of class $4F$ from other elements of order 4. For this reason, we prefer not to use this triple to define standard generators. We find instead that $\xi_{Co_1}(2B, 3C, 40A) = 2$, and we find computationally that there are exactly two classes of such triples, and both generate the whole group. They can be distinguished by the order of $xy = abab^2$, which is 6 and 21 in the two cases. We choose the former as our standard generators.

Example 10 (The Baby Monster) The triple given in Table 1 is probably as good as any. However, due to an unfortunate oversight, we actually found a triple of type $(2C, 3A, 55A)$ instead. In fact this has two advantages: firstly, a $2C$-element is easier to find than a $2D$-element; and secondly, the probability of finding a pair conjugate to the standard genertors is more than doubled, to about 1 in 405. In fact we have $\xi_B(2C, 3A, 55A) = 3$, and the three cases may be distinguished by the order of $xxxyxyy$, which is 23, 31 or 40. We took the first case, and verified computationally that our triple does indeed generate the whole group. (Note that in the first two cases xy has order 40, while in the last it has order 35.) A $2C$-element may be obtained for example as the 26th power of any element of order 52, and a $3A$-element as the appropriate power of any element of order 21, 33, 39, 42, 48 or 66. There is only one class of elements of order 55.

5 Other complete sporadic groups

The groups not so far considered, which do not have outer automorphisms, are M_{11}, M_{23}, Ly and J_4. The same basic considerations apply as in the previous section, but $(2, 3, n)$-generators either do not exist or are not convenient to use.

Example 11 (Mathieu's group M_{11}) In this group there is no set of $(2, 3, n)$-generators for any n, but $(2, 4, 11)$-generators are quite convenient. The structure constants are $\xi(2A, 4A, 11A) = \xi(2A, 4A, 11B) = 1$, but the classes $11A$ and $11B$ are difficult to distinguish in general. Instead we can distinguish the two classes of triples by the order of $xxxyxyy$, which is 4 and 8 in the two cases, corresponding to $x \in 11A$ and $x \in 11B$ respectively. (Note: here we use the definition of the classes given in [2].)

Example 12 (Mathieu's group M_{23}) In this group again, there is no set of $(2,3,n)$-generators, but there are $(2,4,23)$-generators. Now the structure constants are $\xi(2A,4A,23A) = \xi(2A,4A,23B) = 2$. The Parker fingerprints of these four sets of generators are $(23,8,15,11,15,11,8)$, $(23,8,15,11,15,11,11)$, $(23,14,7,11,14,14,7)$, and $(23,14,7,11,14,14,15)$. We choose the first of these as our standard generators.

Example 13 (Janko's group J_4) In this case, the 'almost rigid' triple of classes $(2A,4C,11A)$ given by Pahlings is unusable since the probability of finding such a triple of generators at each attempt is about 1 in 92554, which is unreasonably small. The maximum probability is obtained by taking classes $2A$ and $4A$, when the probability is about 1 in 736. There are then many classes of triples that we could choose as standard generators. We chose to take $a \in 2A$ and $b \in 4A$ with ab of order 37, since in this case it is obvious that a and b generate the whole group. From the structure constants we find that there are 15 classes of such triples, and by a random search we find representatives of all of them, and calculate their Parker fingerprints as in Table 3. We chose the first of these as our standard generators. If p and q are the original two generators for J_4 produced by Norton and Parker, we can take $r = ((pq)^3qpq)^{10}$, and then $(r^2, q^{-6}p^{-14}rp^{14}q^6)$ is a pair of standard generators in this sense.

Example 14 (The Lyons group Ly) Since the Lyons group cannot be generated by $a \in 2A$ and $b \in 3A$, the largest probability is obtained by taking $a \in 2A$ and $b \in 5A$. In this case we have for example that $\xi(2A,5A,14A) = \frac{3}{2}$ (see [3]). Thus there can be at most one class of such triples which generate the group. We find by computation elements $a \in 2A$, $b \in 5A$ with $ab \in 14A$ and $(ab)^3b$ of order 67, from which it follows that these generate the group, and are (up to conjugacy) unique subject to these conditions.

6 Automorphism groups

The remaining twelve sporadic simple groups have outer automorphism groups of order 2. This complicates the issue somewhat, especially if we want to define standard generators for both the group and its automorphism group. We should perhaps find words which give standard generators for the simple

Table 3: Fingerprints in J_4

Case	x	xy	x^2y	x^2yx	$x(xy)^2$	$x^2(xy)^2$	x^3yxy^2
1	37	10	24	24	22	37	22
2	37	20	31	66	12	16	22
3	37	37	43	29	40	11	22
4	37	16	24	22	33	33	31
5	37	66	43	66	44	43	28
6	37	44	66	37	43	12	42
7	37	29	29	31	29	12	16
8	37	22	31	31	10	21	31
9	37	22	31	31	10	21	44
10	37	22	37	23	28	42	10
11	37	22	37	23	28	42	30
12	37	29	14	23	43	28	28
13	37	29	14	23	43	28	43
14	37	31	14	28	35	23	15
15	37	31	14	28	35	23	66

Table 4: Standard generators of complete sporadic groups

Group	Triple (a, b, ab)	Further conditions	Probability
M_{11}	$2, 4, 11$	$o(abababab^2abab^2ab^2) = 4$	$1 : 9$
M_{23}	$2, 4, 23$	$o(abababab^2abab^2ab^2) = 8$	$1 : 119$
M_{24}	$2B, 3A, 23$	$o(ababab^2abab^2ab^2) = 4$	$1 : 30$
Co_3	$3A, 4A, 14$	$-$	$1 : 61$
Co_2	$2A, 5A, 28$	$-$	$1 : 19$
Co_1	$2B, 3C, 40$	$o(abab^2) = 6$	$1 : 164$
Fi_{23}	$2B, 3D, 28$	$-$	$1 : 59$
Th	$2, 3A, 19$	$-$	$1 : 77$
B	$2C, 3A, 55$	$o(abababab^2abab^2ab^2) = 23$	$1 : 405$
M	$2A, 3B, 29$	$-$	$1 : 68$
J_1	$2, 3, 7$	$o(abab^2) = 19$	$1 : 49$
J_4	$2A, 4A, 37$	$o(abab^2) = 10$	$1 : 736$
Ru	$2B, 4A, 13$	$-$	$1 : 163$
Ly	$2, 5A, 14$	$o(ababab^2) = 67$	$1 : 576$

Table 5: Standard generators for the remaining sporadic simple groups

Group	Triple (a, b, ab)	Further conditions
M_{12}	$2B, 3B, 11$	$-$
M_{22}	$2A, 4A, 11$	$o(abab^2) = 11(\iff o(ab^2) = 5)$
HS	$2A, 5A, 11$	$-$
McL	$2A, 5A, 11$	$o((ab)^2(abab^2)^2ab^2) = 7$
J_2	$2B, 3B, 7$	$o([a, b]) = 12$
Suz	$2B, 3B, 13$	$o([a, b]) = 15$
Fi_{22}	$2A, 13, 11$	$o((ab)^2(abab^2)^2ab^2) = 12$
$Fi_{24}{}'$	$2A, 3E, 29$	$o((ab)^3b) = 33$
He	$2A, 7C, 17$	$-$
HN	$2A, 3B, 22$	$o([a, b]) = 5$
J_3	$2A, 3A, 19$	$o([a, b]) = 9$
$O'N$	$2A, 4A, 11$	$-$

group in terms of those of the automorphism group. Conversely, we can give methods for constructing the automorphism group from standard generators for the simple group. The case J_3 is considered in some detail in [6], while J_2 and M_{22} are dealt with by P. G. Walsh in [7].

Since the criteria for choosing standard generators are very much the same as before, we content ourselves here with giving a list of the choices we made (see Tables 5 and 6).

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An Atlas of Finite Groups*, Oxford University Press, 1985.

[2] C. Jansen, K. Lux, R. A. Parker and R. A. Wilson, *An Atlas of Brauer Characters*, Oxford University Press, 1995.

[3] H. Pahlings, Realizing finite groups as Galois groups, *Bayreuth. Math. Schr.* No. 33 (1990), 137–152.

Table 6: Standard generators for automorphism groups of sporadic groups

Group	Triple (a, b, ab)	Further conditions
M_{12}:2	$2C, 3A, 12$	$ab \in 12A(\iff o([a,b]) = 11)$
M_{22}:2	$2B, 4C, 11$	–
HS:2	$2C, 5C, 30$	–
McL:2	$2B, 3B, 22$	$o((ab)^2(abab^2)^2ab^2) = 24$
J_2:2	$2C, 5AB, 14$	–
Suz:2	$2C, 3B, 28$	–
Fi_{22}:2	$2A, 18E, 42$	–
Fi_{24}':2	$2C, 8D, 29$	–
He:2	$2B, 6C, 30$	–
HN:2	$2C, 5A, 42$	–
J_3:2	$2B, 3A, 24$	$o([a,b]) = 9$
$O'N$:2	$2B, 4A, 22$	–

[4] R. A. Parker, The computer calculation of modular characters (The 'Meat-axe'), *Computational Group Theory (ed. M. D. Atkinson)*, Academic Press 1984, pp. 267–274.

[5] M. Schönert et al., *GAP (Groups, Algorithms and Programming)*, RWTH, Aachen, 1992.

[6] I. A. I. Suleiman and R. A. Wilson, Standard generators for J_3, *Experimental Math.* (1995), to appear.

[7] P. G. Walsh, *Standard Generators of some Sporadic Simple Groups*, M. Phil. thesis, University of Birmingham, 1994.

[8] A. J. Woldar, On Hurwitz generation and genus actions of sporadic groups, *Illinois J. Math.* **33** (1989), 416–437.