The Monster is a Hurwitz group

Robert A. Wilson

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

published in J. Group Theory 4 (2001), 367–374

Abstract

We describe explicit calculations to find generators a and b for the Monster sporadic simple group, satisfying the relations $a^2 = b^3 = (ab)^7 = 1$.

MSC: 20D08, 20F05

1 Introduction

The Monster group $\mathbb{M}$ is the largest of the 26 sporadic simple groups, and has order

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$$

$$= 2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71.$$

Its existence was conjectured by Fischer and Griess independently in 1973, and proved by Griess [3] in 1980. The smallest dimension of a faithful representation over any field is 196882, and is realized over fields of characteristics 2 and 3 only (see [4]). In [6] the author, with Walsh, Parker and Linton, assuming existence of the group, constructed (and proved uniqueness of) the 196882-dimensional irreducible representation over $\mathbb{F}_2$. In the present paper

we present the first substantial result proved using this computer representation. This demonstrates that, against all reasonable expectations, it is now possible to do practical calculations in this enormous group.

A finite group is called a Hurwitz group if it is nontrivial and can be generated by elements g and h satisfying the relations

$$g^2 = h^3 = (gh)^7 = 1.$$

In this case we call the triple $(g, h, (gh)^{-1})$ a (2,3,7) generating triple for the group. Thus the Hurwitz groups are precisely the nontrivial finite quotients of the triangle group

$$\Delta = \Delta(2, 3, 7) = \langle g, h \mid g^2 = h^3 = (gh)^7 = 1 \rangle.$$

Note also that a Hurwitz group is necessarily perfect.

The motivation for the definition comes from the study of groups acting on Riemann surfaces as groups of conformal automorphisms. For a given group G, the genus g of such a surface is given by the Riemann–Hurwitz formula

$$g = 1 + \frac{1}{2}|G| \left(n - 2 - \sum_{i=1}^{n} \frac{1}{l_i} \right)$$

where the group is generated by elements $g_1, \ldots, g_n$ of orders $l_1, \ldots, l_n$ respectively, with $g_1 g_2 \cdots g_n = 1$. If the group has no action on a surface of genus 0, then necessarily

$$\sum_{i=1}^{n} \frac{1}{l_i} < n - 2$$

and the minimal possible genus, relative to the order of the group, is attained by the Hurwitz groups. In these cases, the group order is $84(g-1)$, where g is this minimal genus, also called the strong symmetric genus of G. For further background we refer the reader to the excellent survey article by G. A. Jones [5].

Whilst the classification of Hurwitz groups is little more than a curiosity, without great mathematical significance, it has attracted quite an interest over the years. In the 1960s Macbeath [9] initiated a study of finite simple Hurwitz groups by showing that the simple groups $\mathrm{PSL}_2(q)$ are Hurwitz groups just when $q = 7$, q is a prime with $q \equiv \pm 1 \pmod 7$, or $q = p^3$ with p prime and $p \not\equiv \pm 1 \pmod 7$. Graham Higman (unpublished) showed

that all alternating groups A_n are Hurwitz groups for sufficiently large n, and Conder [1] determined exactly which of the smaller alternating groups are Hurwitz groups. Much more recently, work of Lucchini, Tamburini and J. S. Wilson [7], [8] has revealed that most finite simple classical groups of sufficiently large dimension are Hurwitz groups.

The sporadic groups have been treated in a series of papers by Woldar and others (see [2] for a survey and references, and [13], [12] for updates). To date all but the Monster have been dealt with. All the large cases have required significant amounts of electronic computation, for although it is easy to count the $(2, 3, 7)$ triples in a group by calculating the structure constants from the character table, it is often extremely hard to decide whether or not all these triples generate proper subgroups. Often the only practical way to show that a given group is a Hurwitz group is to conduct a search (random or exhaustive) of pairs of elements of orders 2 and 3 until a pair is found which both generates the group and has product of order 7. In the case of the Monster, there is insufficient knowledge of the maximal subgroups to decide the question theoretically. However, the structure constants are very far from being accounted for by the presently known maximal subgroups, which suggests that it is overwhelmingly probable that the group is in fact a Hurwitz group.

2 Results

In the present paper, we describe how we used our explicit representation [6] to compute explicitly a (2,3,7) generating triple for the Monster, and hence verify that it is indeed a Hurwitz group. The strategy was exactly the same as for smaller groups, namely conducting a random search in the haystack of $(2, 3)$ element pairs, for a needle of $(2, 3, 7)$-generators. Only the implementation is different, as the huge size of the Monster means that a simple-minded approach might take billions of years on presently available computers. (A matrix multiplication for the Monster in dimension 196882 would take some 90000 times as long as a matrix multiplication for the Baby Monster in dimension 4370. Thus a calculation which takes hours in the Baby Monster would take decades in the Monster.)

We began with the generators A, B, E, and T for the Monster, defined in [6]. These generators have the property that A, B and E generate a subgroup $3^{1+12}{\cdot}2{\cdot}Suz$, in which A and B generate a subgroup $6{\cdot}Suz$, and E is

a noncentral element of the normal subgroup 3^{1+12}. These three elements can be easily multiplied together to produce any desired element of the subgroup $3^{1+12}{\cdot}2{\cdot}Suz$. The element T acts as an outer automorphism of order 2 of a certain subgroup $3^{2+5+10}{:}M_{11}$, whose generators are given by words in A, B and E. It is not practically possible to multiply T by any of the other generators.

To define the $(2,3,7)$-generators which we eventually found, we let

$$\begin{aligned} x &= AB(ABAB^2)^2 \\ y &= (AB)^2(ABAB^2)^2AB^2 \\ \alpha &= xyxy^2xy(xyxy^2)^2 \\ \beta &= (xy)^3y(xy)^2(xyxy^2)^2 \\ g &= (A^2)^{E^2(AB)^2} \\ h &= ((ABABAB^2AB)^7)^{(AB^2)^{11}T\alpha^5T\beta^{41}T} \end{aligned}$$

It is straightforward to verify that A has order 4, and that $(ABABAB^2AB)$ has order 21, and therefore g has order 2 and h has order 3. To calculate the orders of elements given by words essentially involving T, we use the method described in [6]. There we found two vectors v_1 and v_2 in 196882-space over $\mathbb{F}_2$, whose joint stabilizer is trivial. Thus the order of a word W is the minimum positive value of n such that $v_iW^n = v_i$ for each i. Since this can be checked with $2nl$ vector-matrix multiplications, where l is the length of the word W, it is relatively quick to compute. (As an aside, it is worth remarking that a single vector-matrix multiplication of this size would take around 8×10^{10} field operations if done in a naive manner. Our program, while not easily analysed in this way, performs the same operation with a group generator in not much more than the equivalent of 10^8 field operations.) In particular, we show that gh has order 7. Similarly, defining

$$\begin{aligned} p &= ghgh^2 \\ q &= ghghgh^2 \\ r &= ghgh^2gh^2 \\ s &= ghghgh^2gh^2 \end{aligned}$$

we verified that $ppqsrpsrqsq$ has order 94, and $ppqsrqqrprq$ has order 41. Since all proper subgroups containing elements of order 94 are contained in the double cover $2{\cdot}\mathrm{B}$ of the Baby Monster, which contains no elements of order 41, it follows that g and h generate the Monster.

3 The search

The $(2,3,7)$-structure constants in $\mathbb{M}$ are given in [10], and show that $(2,3,7)$-generators of $\mathbb{M}$ must be of type $(2B,3B,7B)$ or $(2B,3C,7B)$. The search for such generators was performed by first picking a 2-element $a = (A^2)^{E^2}$ and a 3-element $b = (ABABAB^2AB)^7$. Now A^2 is the central involution of a subgroup $6{\cdot}Suz$, so is a $2B$-element, while easy calculations in $6{\cdot}Suz$ show that $ABABAB^2AB$ is an element of order 21 whose 7th power is in class $+3A$ in $6{\cdot}Suz$. The latter class fuses to M-class $3B$, as it is conjugate in M to the central 3-element in $6{\cdot}Suz$. Now we look at pseudorandom elements of the form $ab^\gamma = a\gamma^{-1}b\gamma$, where γ is an element of the Monster, to see if this product of conjugates of a and b could have order 7. If γ were a truly random element of the group, then the probability of ab^γ being of order 7 would be less than 1 in 64 000 000, so it is important to dispose of the unwanted cases very rapidly.

By passing a suitable vector through the word for ab^γ seven times, and comparing the resulting vector with the original, we can eliminate one case quickly. If there are k occurrences of T in the word γ, it turns out that we can eliminate one case in about k seconds of CPU time on a Pentium II 450MHz processor. Our C code (written in collaboration with Richard Parker) was carefully written to optimize the performance, and compiled with options `-O3 -funroll-loops` to `gcc`, both of which had dramatic effects on the runtime. (There are more improvements available, at the cost of extensive rewriting of the code, which seem to offer a further 10% or 20% speed-up.) Thus the total expected CPU time until finding a $(2,3,7)$ triple, using words with three occurrences of T, is something over 5 years. In fact, since not all of these triples will generate the Monster, the expected time to find a $(2,3,7)$ generating triple will be greater than this, perhaps 7 to 10 years (estimates vary according to your guess as to what undiscovered maximal subgroups there are of the Monster).

By using around 40 processors from a cluster of 64 in the University of St. Andrews, we were able to use this amount of CPU time in four months. As it turned out, the number of cases we had to consider was around 120 000 000, which is rather more than the expected number, but not unreasonably so (since this number follows a Poisson distribution, which has a very long tail). The search was parallelized by letting γ be of the form $(AB^2)^iT\alpha_m^jT\beta_n^kT(AB)^l$, and giving each process a different pair of elements α_m and β_n, given as pseudorandom words in A and B (or more particularly,

in x and y), to run through all possibilities for the integers i, j, k, l. Depending on the orders of α_m and β_n this could take anything from a few hours (if the product of the orders is around 10) to several weeks (if the product of the orders is over 1000).

In fact, we started our search with 'shorter' words for γ, involving only two occurrences of T rather than three. But we felt that these elements were insufficiently 'random', as we obtained a much larger than expected number of small groups among the subgroups generated by a and b^γ. (Here we made no serious attempt to prove that the groups were small, but the orders of elements suggested they were $L_2(8)$, $L_2(13)$, etc.) Therefore we continued the search with these 'longer' words.

4 The proof

Once we found a case in which ab^γ appeared to have order 7, we then proved it by applying the word to two vectors whose joint stabilizer is known to be trivial, as described above (see also [6]). We next calculated the orders of over fifty words in a and b^γ, in order to be reasonably confident of being able to prove that the given elements generate the whole group. We did this both systematically, by looking at all words in p, q, r and s of length at most 4, and randomly, by looking at two words of length 11 written down at random. The orders of these elements are given in Table 1.

The reason for using just these words is that all conjugacy classes of cyclic subgroups of a $(2, 3, 7)$ group (apart possibly from the classes of g, h, and gh) are represented by words in p, q, r, s. For every class, apart from these three, has a representative as a word in gh and gh^2, and we may cyclically permute the word to put the longest string of consecutive terms gh at the beginning. Now if there is a string of three consecutive terms gh, there is a subword

$$ghghghgh^2 = (gh)^4h = (gh)^{-3}h = h^2gh^2gh^2gh$$

so we can replace the word by one with fewer occurrences of g. Similarly if there is a string of three consecutive terms gh^2 we may reduce the number of occurrences of g. Thus every class can be represented by a word in p, q, r, and s, or the inverse of such a word. Moreover, by inverting the word if necessary, we may suppose that there are at least as many terms gh as gh^2, and therefore at least as many occurrences of q as of r. We reduce the list further by taking the lexicographically first word in each cyclic ordering, and

Table 1: Orders of specific elements of $\mathbb{M}$

Element	Order	Element	Order	Element	Order
p	42	s	39	pq	105
ps	19	qr	19	qs	30
ppq	60	pqq	60	pqr	42
pqs	34	pps	39	prq	39
psq	39	pss	22	qqr	34
qqs	39	qrs	22	qsr	35
qss	60	$pppq$	36	$ppps$	56
$ppqq$	35	$ppqr$	60	$ppqs$	36
$pprq$	56	$ppsq$	29	$ppss$	55
$pqpr$	60	$pqps$	46	$pqqq$	36
$pqqr$	60	$pqqs$	46	$pqrq$	46
$pqrs$	105	$pqsq$	57	$pqsr$	57
$pqss$	110	$prqq$	36	$prqs$	84
$prsq$	55	$psqq$	57	$psqs$	60
$pssq$	29	$psss$	66	$qqqr$	46
$qqqs$	29	$qqrr$	57	$qqrs$	110
$qqsr$	84	$qqss$	66	$qrss$	66
$qsrs$	105	$qssr$	105	$qsss$	24
$qrqs$	60	$ppqsrpsrqsq$	94	$ppqsrqqrprq$	41

eliminating obvious inverses and proper powers. Finally, using also the less obvious equivalence

$$\begin{aligned} q &= ghghgh^2 \\ &= (gh)^3 h \\ &= (gh)^{-4} h \\ &= h^2 gh^2 gh^2 gh^2 gh \\ &= (gh^2 gh)^{hgh} \\ &\sim p \end{aligned}$$

where we write $x \sim y$ to mean x is conjugate to $y^{\pm 1}$, we obtain the list in Table 1, apart from the last two entries.

[John Bray has pointed out to me that the above argument can be used to prove many further equivalences. For example, he has proved the following results:

$$\begin{aligned} pq^n &\sim p^n q \text{ for all } n \\ qqs &\sim psq \\ ppqq &\sim qsr \\ pqqr &\sim qss \\ pqqs &\sim pqps \\ qqqs &\sim ppsq \\ qqqr &\sim pqrq \end{aligned}$$

Indeed, any word containing qqq or qqs can be reduced to a word containing fewer occurrences of g, by the above method, although it may become longer as a word in p, q, r, s.]

We have already seen that g is a $2B$-element, and h is a $3B$-element, while the work of Norton [10] on $(2, 3, 7)$ structure constants in the Monster shows immediately that gh is a $7B$-element. Therefore our generating triple is of type $(2B, 3B, 7B)$.

5 Conclusion

This work now completes the determination of the symmetric genus of the sporadic simple groups. The symmetric genus of a perfect group G is given by the minimum value of the Riemann–Hurwitz formula. In the cases of the

Table 2: The symmetric genus of the sporadic groups

Group	(l,m,n)	$1-\frac{1}{l}-\frac{1}{m}-\frac{1}{n}$	Group	(l,m,n)	$1-\frac{1}{l}-\frac{1}{m}-\frac{1}{n}$
M_{11}	$(2,4,11)$	$\frac{7}{44}$	M_{12}	$(2,3,10)$	$\frac{1}{15}$
J_1	$(2,3,7)$	$\frac{1}{42}$	M_{22}	$(2,5,7)$	$\frac{11}{70}$
J_2	$(2,3,7)$	$\frac{1}{42}$	M_{23}	$(2,4,23)$	$\frac{19}{92}$
HS	$(2,3,11)$	$\frac{5}{66}$	J_3	$(2,4,5)$	$\frac{1}{20}$
M_{24}	$(3,3,4)$	$\frac{1}{12}$	McL	$(2,5,8)$	$\frac{7}{40}$
He	$(2,3,7)$	$\frac{1}{42}$	Ru	$(2,3,7)$	$\frac{1}{42}$
Suz	$(2,4,5)$	$\frac{1}{20}$	O'N	$(2,3,8)$	$\frac{1}{24}$
Co_3	$(2,3,7)$	$\frac{1}{42}$	Co_2	$(2,3,11)$	$\frac{5}{66}$
Fi_{22}	$(2,3,7)$	$\frac{1}{42}$	HN	$(2,3,7)$	$\frac{1}{42}$
Ly	$(2,3,7)$	$\frac{1}{42}$	Th	$(2,3,7)$	$\frac{1}{42}$
Fi_{23}	$(2,3,8)$	$\frac{1}{24}$	Co_1	$(2,3,8)$	$\frac{1}{24}$
J_4	$(2,3,7)$	$\frac{1}{42}$	Fi'_{24}	$(2,3,7)$	$\frac{1}{42}$
B	$(2,3,8)$	$\frac{1}{24}$	$\mathbb{M}$	$(2,3,7)$	$\frac{1}{42}$

The integers l, m, n are such that the group in question is generated by elements of order l and m with product of order n, and that $\frac{1}{l}+\frac{1}{m}+\frac{1}{n}$ is maximal with this property. The symmetric genus of the group G is $1+\frac{1}{2}|G|\left(1-\frac{1}{l}-\frac{1}{m}-\frac{1}{n}\right)$.

sporadic simple groups, this is the minimum value of $|G|(1-\frac{1}{l}-\frac{1}{m}-\frac{1}{n})$ such that G is a quotient of the triangle group

$$\Delta(l,m,n)=\langle g,h \mid g^l=h^m=(gh)^n=1\rangle.$$

For ease of reference we include in Table 2 a complete table of results, mostly taken from [2], with the results for Fi_{23} and B taken from [12], [13]. In particular, we note that exactly 12 of the sporadic simple groups are Hurwitz groups, namely J_1, J_2, He, Ru, Co_3, Fi_{22}, HN, Ly, Th, J_4, Fi'_{24} and $\mathbb{M}$.

Acknowledgements I am grateful to Steve Linton for permission to use his computing facilities, without which this project would have been impossible. Richard Parker and Steve Linton gave invaluable assistance in writing,

debugging and optimizing the computer program. I thank John Bray and the five referees for their useful comments which have significantly improved this paper.

References

[1] M. D. E. Conder, Generators for alternating and symmetric groups, *J. London Math. Soc.* **22** (1980), 75–86.

[2] M. D. E. Conder, R. A. Wilson and A. J. Woldar, The symmetric genus of sporadic groups, *Proc. Amer. Math. Soc.* **116** (1992), 653–663.

[3] R. L. Griess, The friendly giant, *Invent. Math.* **69** (1982), 1–102.

[4] R. L. Griess and S. D. Smith, Minimal dimensions for modular representations of the Monster, *Comm. Algebra* **22** (1994), 6279–6294.

[5] G. A. Jones, Characters and surfaces: a survey, in *The atlas of finite groups ten years on (ed. R. T. Curtis and R. A. Wilson)*, LMS Lecture Notes Series **249**. Cambridge University Press, 1998, pp. 90–118.

[6] S. A. Linton, R. A. Parker, P. G. Walsh and R. A. Wilson, Computer construction of the Monster, *J. Group Theory* **1** (1998), 307–337.

[7] A. Lucchini, M. C. Tamburini and J. S. Wilson, Hurwitz groups of large rank, *J. London Math. Soc.* **61** (2000), 81–92.

[8] A. Lucchini and M. C. Tamburini, Classical groups of large rank as Hurwitz groups, *J. Algebra* **219** (1999), 531–546.

[9] A. M. Macbeath, Generators of the linear fractional groups, *Number theory (Proc. Sympos. Pure Math., Vol XII, 1967)*, pp. 14–32. Amer. Math. Soc., 1969.

[10] S. P. Norton, The anatomy of the Monster, I, in *The atlas of finite groups ten years on (ed. R. T. Curtis and R. A. Wilson)*, LMS Lecture Notes Series **249**. Cambridge University Press, 1998, pp. 198–214.

[11] R. A. Wilson, The odd-local subgroups of the Monster, *J. Austral. Math. Soc. (A)* **44** (1988), 1–16.

[12] R. A. Wilson, The symmetric genus of the Fischer group Fi_{23}, *Topology* **36** (1997), 379–380.

[13] R. A. Wilson, The symmetric genus of the Baby Monster, *Quart. J. Math. Oxford* **44** (1993), 513–516.