Progress in Mathematics, Vol. 173, © 1999 Birkhäuser Verlag Basel/Switzerland

Chapter 14

A Presentation for the Lyons Simple Group

George Havas and Charles C. Sims

Abstract

We give a presentation of the Lyons simple group together with information on a complete computational proof that the presentation is correct. This fills a longstanding gap in the literature on the sporadic simple groups. This presentation is a basis for various matrix and permutation representations of the group.

14.1 Introduction

Lyons [9, 10] gave a detailed description of a new simple group. Sims [13] outlined a presentation for the group and a proof of its correctness. The proof itself is in a long manuscript which was never published. That manuscript in fact does much more than just provide a presentation; it gives a proof of existence and uniqueness for the group. The original proof relied upon a large number of special purpose computer programs.

With the dramatic improvement of computer technology in both hardware and software we now give a complete presentation for the Lyons group and a proof of correctness which can be verified readily enough. This proof follows the initial lines of that in Sims' manuscript, with minor modifications. It requires a computer with adequate random access memory and also computational group theory facilities such as provided by GAP [12] or MAGMA [1]. A major procedural requirement is the ability to undertake large coset enumerations. All computations described in this paper can be carried out using GAP and/or MAGMA.

The lemmas in this paper are based on only a small part of the original (mainly hand-written) manuscript, which comprises four chapters and ten appendices. The four chapters run to 124 pages and the appendices are another 62 pages. The original manuscript gives the following theorem.

Theorem 14.1. *Up to isomorphism there is exactly one finite simple group G possessing an involution whose centralizer in G is isomorphic to the 2-fold covering group of A_{11}.*

The proof in the original manuscript goes this way. The group G is constructed as a permutation group of degree 8835156 in which the stabilizer of a point is $G_2(5)$. The proof uses in effect the presentation given in this paper. The existence and uniqueness proofs for G reduce essentially to the verification of a large number of facts about $G_2(5)$, much of which is done by computer. Algorithms and programs are explicitly provided. Chapter two of the manuscript presents the proof as a sequence of 58 traditional lemmas, traditional in the sense that their statements do not refer to computers or programs. However the proofs of these lemmas do rely heavily on computer results.

14.2 A Presentation for the Lyons Group

In this section we give an amended version of the presentation which appears in Sims' manuscript. (It has previously been noted by Jansen and Wilson [8] that the presentation in the original manuscript is not fully correct.)

The presentation given by Sims is on five generators: a, b, c, d, z, where $\langle a, b, c, d\rangle \simeq G_2(5)$. A number of redundant generators e, a_i, c_j, u and x_k, all in $\langle a, b, c, d\rangle$, are used as in the original construction.

Let G be the group generated by the 39 elements $\{a$, b, c, d, z, e, a_1, a_2, a_3, a_4, c_1, c_2, c_3, c_4, c_5, u, x_{23}, x_{24}, x_{25}, x_{29}, x_{47}, x_{96}, x_{129}, x_{162}, x_{163}, x_{164}, x_{165}, x_{166}, x_{167}, x_{168}, x_{169}, x_{364}, x_{365}, x_{366}, x_{367}, x_{368}, x_{369}, x_{370}, $x_{371}\}$ satisfying the following 86 relators and relations:

$$a^8, \tag{14.1}$$
$$b^5, \tag{14.2}$$
$$(ab)^4, \tag{14.3}$$
$$(a^2, b), \tag{14.4}$$
$$(a, b)^3, \tag{14.5}$$
$$c_1 = c, \tag{14.6}$$
$$c_2 = c^a, \tag{14.7}$$
$$c_3 = c^b, \tag{14.8}$$
$$c_4 = c^{b^{-1}}, \tag{14.9}$$
$$c_5 = (c_1, c_2), \tag{14.10}$$
$$c_1^5, \tag{14.11}$$
$$c_5^5, \tag{14.12}$$
$$(c_1, c_5), \tag{14.13}$$
$$(c_2, c_5), \tag{14.14}$$
$$(c_3, c_5), \tag{14.15}$$
$$(c_4, c_5), \tag{14.16}$$
$$(c_1, c_3) = c_5^{-2}, \tag{14.17}$$
$$(c_1, c_4) = c_5^2, \tag{14.18}$$
$$(c_2, c_3) = c_5^{-1}, \tag{14.19}$$

$$(c_2, c_4), \tag{14.20}$$
$$(c_3, c_4) = c_5^{-1}, \tag{14.21}$$
$$c_2^a = c_1^{-2}, \tag{14.22}$$
$$c_3^a = c_3^{-2} c_1 c_4, \tag{14.23}$$
$$c_4^a = c_1 c_2^{-1} c_3^{-1} c_4 c_1 c_4, \tag{14.24}$$
$$c_5^a = c_5^2, \tag{14.25}$$
$$c_2^b = c_2 c_3 c_4^{-1} c_1^{-1} c_4^{-1}, \tag{14.26}$$
$$c_3^b = c_1^2 c_4 c_3^{-2}, \tag{14.27}$$
$$c_5^b = c_5, \tag{14.28}$$
$$e = b^{-2}(a, c_1) a^{-1} c_1 a d c_1 b a b^{-1} d c_1 d, \tag{14.29}$$
$$e^2, \tag{14.30}$$
$$c_1^e = b c_3 b c_1^{-1}, \tag{14.31}$$
$$c_3^e = b^2 a c_2 c_1^{-1} c_4^{-1} a^{-1}, \tag{14.32}$$
$$c_4^e = b^2 c_3^{-1} c_4, \tag{14.33}$$
$$c_5^e = c_1 c_3^{-1} c_1 c_4^{-1}, \tag{14.34}$$
$$e a^2 e = a b^2 a b^{-1} a c_1 c_5 c_4^{-1}, \tag{14.35}$$
$$b^e = c_1 c_3^{-1} c_4^{-2}, \tag{14.36}$$
$$e a b^2 a b^{-1} a e = a^2 c_1 c_5 c_4^{-1}, \tag{14.37}$$
$$e c_2 e c_2^{-1} e c_2 c_4^{-1} a c_3 a^3, \tag{14.38}$$
$$d = a b^2 a^{-1} b^{-1} c_1^{-1} c_4^{-1} c_5^{-1} a e a e a c_2^{-1} b e, \tag{14.39}$$
$$d^2 = a^4, \tag{14.40}$$
$$(b, d), \tag{14.41}$$
$$a^d = a^3, \tag{14.42}$$
$$(d c_5)^5, \tag{14.43}$$
$$d c_5 d c_5^{-1} d c_5 a^{-2}, \tag{14.44}$$
$$a_1 = a, \tag{14.45}$$
$$a_2 = a^{b^{-1}}, \tag{14.46}$$
$$a_3 = a^{b^{-2}}, \tag{14.47}$$
$$a_4 = a^{b^2}, \tag{14.48}$$
$$u = a^2, \tag{14.49}$$
$$x_{23} = d, \tag{14.50}$$
$$x_{24} = d^{-1}, \tag{14.51}$$
$$x_{25} = b^2 a^{-1} b^{-1} a^{-1} b^2 c^{-1} a c a^{-1} c^{-1} d c^{-1} b^2 a^{-1} c b, \tag{14.52}$$
$$x_{29} = a b a^{-1} b^2 a^{-1} b^2 c^{-1} a c b c b^{-1} d c b^{-2} d c b c, \tag{14.53}$$
$$x_{47} = c^{-1} d^{-1} a^{-1} c^{-1} a^{-1} b c^{-1} d^{-1}, \tag{14.54}$$
$$x_{96} = b d, \tag{14.55}$$

$$x_{129} = d^{-1}b^{-1}, \tag{14.56}$$
$$x_{162} = a^{-1}b^{-1}a^{-1}bc^{-1}b^{-1}ac^{-1}ba, \tag{14.57}$$
$$x_{163} = b^{-2}aca^{-1}bcb, \tag{14.58}$$
$$x_{164} = a^{-1}b^{-1}a^{-1}caba, \tag{14.59}$$
$$x_{165} = b^{-1}a^{-1}bcb^{-1}ab, \tag{14.60}$$
$$x_{166} = b^2a^{-1}b^{-1}cbacb^{-2}c^{-1}, \tag{14.61}$$
$$x_{167} = a^{-3}, \tag{14.62}$$
$$x_{168} = ba^{-1}b^{-1}a^{-2}, \tag{14.63}$$
$$x_{169} = ab^2ab^{-2}a^{-1}, \tag{14.64}$$
$$x_{364} = a^{-1}db^{-1}c^{-1}a^{-1}bc^{-1}d^{-1}bc^{-1}b^{-1}a^{-1}c^{-1}ab^{-1}abab^{-1}, \tag{14.65}$$
$$x_{365} = ab^{-2}a^{-1}cbc^{-1}ba^{-1}c^{-2}dcaca^{-1}cb^{-1}d^{-1}, \tag{14.66}$$
$$x_{366} = bab^{-1}a^{-1}b^{-2}a^{-1}b^{-1}cb^2cbdcb^{-2}dcbc, \tag{14.67}$$
$$x_{367} = c^{-1}b^{-1}c^{-1}d^{-1}b^2c^{-1}d^{-1}b^{-1}c^{-1}b^{-2}c^{-1}bab^2aba^{-1}b^{-1}, \tag{14.68}$$
$$x_{368} = a^{-1}c^{-1}d^{-1}ac^{-1}b^{-1}ac^{-1}d^{-1}a^{-1}c^{-1}acb^{-2}c^{-1}b^{-1}a^{-1}b^{-2}, \tag{14.69}$$
$$x_{369} = a^{-1}c^{-1}d^{-1}ba^{-1}b^{-1}c^{-1}d^{-1}ba^{-1}b^{-1}c^{-1}b^{-1}ab^{-2}ab^{-1}, \tag{14.70}$$
$$x_{370} = d^{-1}acbca^{-1}c^{-1}d^{-1}ab^{-1}a^{-1}ca^{-1}b^{-2}a^{-1}ba^{-1}, \tag{14.71}$$
$$x_{371} = c^{-1}a^{-1}cbc^{-1}d^{-1}ca^{-1}cacb^{-1}a^{-1}b^{-1}a^{-1}b, \tag{14.72}$$
$$c_1^z = x_{162}, \tag{14.73}$$
$$c_2^z = x_{163}, \tag{14.74}$$
$$c_3^z = x_{164}, \tag{14.75}$$
$$c_4^z = x_{165}, \tag{14.76}$$
$$c_5^z = x_{166}, \tag{14.77}$$
$$a_1^z = x_{167}, \tag{14.78}$$
$$a_2^z = x_{168}, \tag{14.79}$$
$$a_3^z = x_{169}, \tag{14.80}$$
$$z^2 = u, \tag{14.81}$$
$$(a_4z)^3u, \tag{14.82}$$
$$x_{47}zx_{364}zx_{368}z, \tag{14.83}$$
$$z^{-1}x_{24}z^{-1}x_{369}zx_{23}zx_{29}, \tag{14.84}$$
$$zx_{366}zx_{365}z^{-1}x_{367}z^{-1}x_{370}, \tag{14.85}$$
$$zx_{96}zx_{25}z^{-1}x_{129}z^{-1}x_{371}. \tag{14.86}$$

Theorem 14.2. *G is isomorphic to the Lyons simple group.*

The proof is given in the following section where we identify relations from this presentation by their numbers. It should be noted that it is this presentation (in effect) for the Lyons group which is used as part of proofs in [11, 8, 15]. Thus proofs that various matrix representations of the group are correct rely upon the fact that their generators satisfy all the relations in a presentation for the group.

Furthermore, the final coset enumeration described in this paper gives a minimal degree permutation representation. An alternative independent existence proof for the Lyons group is given in [5].

14.3 A computational Proof

We give steps in the proof that the presentation is correct as a sequence of lemmas. Each lemma is readily proved computationally. (The lemmas are derived from those given by Sims, but are varied in the light of current computational capabilities.)

Consider the following four 7×7 matrices over $GF(5)$ (given in [13]).

$$a = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 \end{pmatrix} \qquad b = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 2 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 1 & 4 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 1 & 0 & 3 & 2 & 4 \\ 1 & 3 & 0 & 1 & 4 & 3 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 3 & 0 & 0 & 2 & 0 & 1 \end{pmatrix} \qquad d = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Lemma 14.1. *The matrices a, b, c, d are elements of $G_2(5)$ and satisfy relations* (14.1–14.44). *(These are all the relations in the presentation for G which involve only $a, b, c, d, e, c_1, c_2, c_3, c_4, c_5$, wherein $c_1, c_2, c_3, c_4, c_5, e$ are defined.)*

The family of groups $G_2(q)$ was originally described by Dickson [3, 4]. That the matrices a, b, c and d are elements of $G_2(5)$ follows from Dickson's characterization of $G_2(5)$ as the group of 7×7 matrices with determinant 1 which preserve a particular quadratic form and map a specific subspace of alternating bilinear forms into itself. The group $G_2(5)$ has order 5859000000. That matrices a, b, c and d satisfy the specified relations for G can be verified by straightforward computation. We call the group presented by these generators and relations H. Further, by an easy computation with MAGMA we obtain the following result.

Lemma 14.2. *The matrices a, b, c, d generate $G_2(5)$.*

We now identify H by studying subgroups. In H let $M = \langle a, b, c \rangle$, $T = \langle a, b \rangle$, and $P = \langle c_1, c_2, c_3, c_4, c_5 \rangle$.

Lemma 14.3. *T is a homomorphic image of $GL(2, 5)$.*

This can be verified by straightforward computation. Coset enumeration shows that the group $\langle a, b \mid a^8, b^5, (ab)^4, (a^2, b), (a, b)^3 \rangle$ defined by relations (14.1–14.5) of the presentation for G has order $480 = |GL(2,5)|$. In $GL(2,5)$ define $a' = \left(\begin{smallmatrix} 0 & 3 \\ 1 & 0 \end{smallmatrix}\right)$, $b' = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 0 \end{smallmatrix}\right)$. Then relations (14.1–14.5) are satisfied if a and b are replaced by a' and b'. Since a', b' and (a', b') have orders 8, 5 and 3, respectively, it follows that $GL(2,5) = \langle a', b' \rangle$ and so relations (14.1–14.5) give a presentation for $GL(2,5)$. (This presentation omits a redundant relator which appeared in earlier presentations.)

Lemma 14.4. *The order of P divides 5^5, T normalizes P, and $M = PT$. The order of M divides* 1500000.

That the order of P divides 5^5 follows from its generators satisfying relations (14.10–14.21) which, together with the orders of c_2, c_3 and c_4 being 5, define a group of order 5^5 (easily verified by coset enumeration, for example). That T normalizes P follows from relations (14.7–14.9) and (14.22–14.28), which show the actions of a and b on the generators of P. It follows that $|M|$ divides $5^5|GL(2,5)|$.

Lemma 14.5. *The index of M in H is* 3906. *The order of H divides* 585900000. *H is isomorphic to $G_2(5)$.*

The coset enumeration for $|H : M|$ is straightforward. That $H \simeq G_2(5)$ follows. Since the matrices a, b, c, d satisfy the defining relations for H and generate $G_2(5)$, that group is a quotient group of H. But the order of H is at most the order of $G_2(5)$. Therefore they are isomorphic. Also, each of the subgroups T, P and M are isomorphic to the above specified preimages, with orders 480, 5^5 and 1500000, respectively.

The final step in the proof comes from the following lemma.

Lemma 14.6. *The index of H in G is* 8835156. *G has order* 51765179004000000.

That the permutation representation coming from this enumeration is a Lyons group is shown in [6]. (Here we choose to refer to this more accessible description of a construction, rather than follow the method used in the original manuscript, which accounts for much of its length.) The coset enumeration involved in this step is the only one which is challenging in the context of todays computing facilities. We give some details in the next section.

14.4 The Large Coset Enumeration

The enumeration to determine $|G : H|$ requires the definition of some nine million cosets, at least. Thus this step requires some care. Recent descriptions of relevant aspects of coset enumeration are given in [7, 14, 2]. Of particular importance is the fact that in broad terms the space required (memory locations) for a standard coset enumeration to complete is at least the maximum number of cosets defined times twice the number of group generators.

The presentation for G is given on 39 generators, most of which are redundant. A regular coset enumeration using this presentation would need about three gigabytes of random access memory, at least, which is more than available on all but the biggest supercomputers. Furthermore, it would take a very long time.

This can be readily alleviated by eliminating most of the redundant generators. Thus, using Tietze transformations, it is easy to obtain a six generator presentation on $\{a, b, c, d, e, z\}$. This is straightforward, even by hand, using relators (14.6–14.10) and (14.45–14.72), and can be done using built-in capabilities of either GAP or MAGMA. It yields a 53 relator presentation.

Using this presentation reduces the memory requirements by a factor of better than six. This brings the computation within the range of computers with as little as half a gigabyte of random access memory.

Coset enumerations using such six generator presentations have now been performed a number of times using two independent coset enumeration programs. With Felsch-type methods the maximum number of cosets defined is equal to the index and the total is less than 13 million, depending somewhat on specific details of presentation used and enumeration strategy. The first time it was done (in July 1996), using a descendant of the program described in [7] and available in MAGMA, the enumeration completed in about 15 cpu hours on a CONVEX computer, indeed using about half a gigabyte of random access memory.

As foreshadowed in [2] this enumeration has successfully been done in parallel. In this case it used a version of the enumerator which is in GAP and due to Martin Schönert. It has been done in a four processor environment on a CONVEX and in a 16 processor environment on an SGI Power Challenge. In each case, approximately linear speed-up with processors was realized.

Input files to reproduce this coset enumeration in GAP, MAGMA, or with stand-alone programs are available from the first author.

Of course it is simple to derive presentations for the Lyons group on fewer generators. In our presentation, relation (14.29) allows us to express e in terms of a, b, c and d, and relation (14.39) allows us to express d in terms of a, b, c and e. However, how easy it is to find a presentation suitable for coset enumeration on fewer than six generators is unclear.

Thus, it is trivial to use Tietze transformations to eliminate generator e from the six generator presentation. However this replaces 23 occurrences of the generator e by a product 17 symbols long. It is possible that coset enumeration in such a presentation would be much more difficult than compensated for by the saving due to fewer generators. This is evidenced by coset enumeration behaviour in $G_2(5)$. For index 3906 enumerations of $\langle a, b, c\rangle$ in $G_2(5)$ (that is, corresponding to the enumeration $H|M$), the maximum number of cosets required explodes from 3906 for five generator presentations on $\{a, b, c, d, e\}$ to the extent that enumerations do not complete given a maximum of five million cosets for corresponding four generator presentations on $\{a, b, c, d\}$.

It is likewise easy to eliminate d from the six generator presentation for G. This replaces occurrences of the generator d by a product 18 symbols long. In one sense this is more promising, since the index 3906 enumerations in corresponding four generator presentations for $H|M$ require the same maximum and similar total cosets as for the five generator presentations. However, there are many more occurrences of d in the presentation for G in view of the way many of the x_i are defined involving d. At the time of writing, enumerations in five generator presentations for G have not been attempted.

Acknowledgements

The first author was partially supported by the Australian Research Council.

Bibliography

[1] W. Bosma, J. Cannon and C. Playoust: *The Magma algebra system I: The user language*, J. Symbolic Comput. **24**, (1997) 235–265. See also `http://www.maths.usyd.edu.au:8000/comp/magma/Overview.html`

[2] G. Cooperman and G. Havas: *Practical parallel coset enumeration*, in: Workshop on High Performance Computing and Gigabit Local Area Networks, Lecture Notes in Control and Information Systems **226**, (1997) 15–27.

[3] L.E. Dickson: *Theory of linear groups in an arbitrary field*, Trans. Amer. Math. Soc. **2**, (1901) 363–394.

[4] L.E. Dickson: *A new system of simple groups*, Math. Ann. **60**, (1905) 137–150.

[5] H.W. Gollan: *A new existence proof for Ly, the sporadic simple group of R. Lyons*, Preprint 30, Institut für Experimentelle Mathematik, Universität GH Essen, 1995.

[6] H.W. Gollan and G. Havas: *On Sims' presentation for Lyons' simple group*, These proceedings, chapter 13.

[7] G. Havas: *Coset enumeration strategies*, in: ISSAC'91, Proc. 1991 Internat. Sympos. Symbolic and Algebraic Computation (ACM Press, New York, 1991) 191–199.

[8] C. Jansen and R.A. Wilson: *The minimal faithful 3-modular representation for the Lyons group*, Commun. Algebra **24**, (1996) 873–879.

[9] R. Lyons: *Evidence for a new finite simple group*, J. Algebra **20**, (1972) 540-569.

[10] R. Lyons: *Evidence for a new finite simple group*, (Errata) J. Algebra **34**, (1975) 188–189.

[11] W. Meyer, W. Neutsch and R. Parker: *The minimal 5-representation of Lyons' sporadic group*, Math. Ann. **272**, (1985) 29–39.

[12] M. Schönert et al.: GAP – *Groups, Algorithms and Programming*, (Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995). See also `http://www-groups.dcs.st-and.ac.uk/~gap`

[13] C.C. Sims: *The existence and uniqueness of Lyons' group*, in: Finite Groups '72 (North Holland, 1973) 138–141.

[14] C.C. Sims: *Computation with finitely presented groups*, Cambridge University Press (1994).

[15] R.A. Wilson: *A representation for the Lyons group in* $GL_{2480}(4)$*, and a new uniqueness proof*, Arch. Math. **70**, (1998) 11–15.