View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

J. Symbolic Computation (2001) **31**, 203–209
doi:10.1006/jsco.2000.1010
Available online at http://www.idealibrary.com on IDEAL®

A New Existence Proof for *Ly*, the Sporadic Simple Group of R. Lyons[*]

HOLGER W. GOLLAN[†]

Computing Center, University of Essen, Germany

This paper reports on a new and independent existence proof for the sporadic simple group *Ly* of Lyons, using only two permutations of degree 9 606 125, computed by Cooperman, Finkelstein, Tselman, and York. We will show that these two permutations generate a group $G \simeq Ly$, by first computing a base and strong generating set for G, and then checking the two hypotheses for *Ly* from Lyons' original paper. Moreover, this produces a new presentation for *Ly*.

© 2001 Academic Press

1. Introduction

The classification of the finite simple groups is one of the outstanding mathematical results in this century. One of the major parts deals with the sporadic groups, and Gorenstein, Lyons and Solomon remark in their book (Gorenstein, 1982) that "...the existence and uniqueness of the sporadic groups and the development of their properties form a very elaborate chapter of simple group theory, spread across a large number of articles. Moreover, some of the results are unpublished (e.g. Sims' computer calculations establishing the existence and uniqueness of the Lyons group *Ly*)".

This paper reports on a new and independent existence proof for Lyons' simple group *Ly*, using only two permutations of degree 9606 125, computed by Cooperman *et al.* (1997) and a lot of heavy computer calculations. These permutations have been computed as a test case for an algorithm to compute permutation representations from matrix representations (Cooperman *et al.*, 1997), using the 111-dimensional matrix representation of *Ly* over $GF(5)$ that has been constructed in Meyer *et al.* (1985), and a partially probabilistic algorithm to enumerate a conjugacy class of cyclic subgroups of type $\langle 3A \rangle$, knowing that there are 9606 125 of them, each with normalizer isomorphic to $3McL{:}2$.

Our proof is done by checking the two hypotheses from Lyons' original paper (Lyons, 1972) for the group G that is generated by these two permutations. Hence we have to search for an involution $t \in G$ such that

(i) $C = Cen_G(t) \simeq 2A_{11}$ and
(ii) $t \notin \mathbf{Z}^*(G)$.

[*]This work was supported by the Deutsche Forschungsgemeinschaft under grants Go 487/3–1 and Go 487/3–2.
[†]E-mail: gollan@hrz.uni-essen.de

0747–7171/01/010203 + 07 $35.00/0 © 2001 Academic Press

To do this, we first go into the stabilizer of a point and construct a subgroup of type $3McL\!:\!2$. In the next step we prove that this subgroup is already the full stabilizer of a point, therefore getting at least the correct order for our group G, by using a variation of the well known Schreier–Sims method, making use of double cosets to reduce the number of necessary tests. Finally, we check the two conditions above to prove that

$$G \simeq Ly.$$

To handle the heavy computer calculations, a standalone base and strong generating set program, written by the author, was used. Moreover, we have used MAGMA (Bosma *et al.*, 1997) to do a lot of useful calculations in smaller degrees. All the computations have been done on an IBM 9076–SP1 with eight nodes and some other IBM RS6000s at the Institute for Experimental Mathematics. To keep this paper short, we will omit nearly all the details of the calculations. They can be found either in Gollan (1995) or Gollan (1998); for any questions the reader can consult the author via electronic mail.

Other existence proofs for Lyons' simple group can be found in Gollan and Havas (1999), using the original presentation of Sims (1972) and results from this paper, and in the unpublished manuscript that was announced in Sims (1972).

2. The Double Coset Trick

We assume that the reader is familiar with the basic concepts of computational group theory like orbits, Schreier vectors, bases, and strong generating sets. These go back to the pioneering work of Sims (1970); a detailed description of the important algorithms can, for example, be found in Butler's lecture notes (Butler, 1991). One of the main tasks in this area is the construction of a base and strong generating set for a given permutation group to compute the order of the group in question and to set up the data for solving a lot of interesting tasks. Usually, this is either solved by random methods, or with the help of Schreier generators, a sufficient set of generators for the stabilizer of a base point. Although the second method is deterministic, the number of Schreier generators equals the number of generators for the full group times the index of the stabilizer (the length of the orbit), which makes this method unusable for our purposes. Hence we will present a modification of this method by using double cosets; this variation of the Schreier–Sims method is a reinvention of old and unpublished ideas of Sims, that were presented by him in several talks during the 1970s. Moreover, the Brownie–Cannon–Sims algorithm is also based on these ideas. It was first implemented in 1986 and has been included in CAYLEY (Cannon, 1984) and MAGMA (Bosma *et al.*, 1997). Cannon and Havas (1992) talk about this verification procedure that uses two point stabilizers, but again the details are undocumented in the literature.

Algorithm 2.1. Let G be a group acting on the set Ω, generated by a set X. Furthermore, fix a point $\beta \in \Omega$, and let $S = Stab_G(\beta)$ be the stabilizer of β in G. Given a subgroup $H \leq S$, the following will either prove that $H = S$, or it will produce an element in S outside H.

(i) Let $\{\gamma_1, \ldots, \gamma_s\}$ be a set of representatives for the different orbits of H on $\beta^G \subseteq \Omega$.

(ii) For $1 \leq i \leq s$ let r_i be a fixed element of G with $\beta^{r_i} = \gamma_i$. Then $r_1, \ldots, r_s$ are representatives for different double cosets of H in G.

(iii) For each $\gamma \in \beta^G$ there is a unique $1 \leq i \leq s$ such that $\gamma \in \gamma_i^H$. Let g_γ be a fixed element of H with $\gamma = \gamma_i^{g_\gamma}$. Note that $\beta^{r_i g_\gamma} = \gamma$, hence different elements from β^G lead to different cosets of H.

(iv) Check whether

$$Hr_iH = \bigcup_{\gamma \in \gamma_i^H} Hr_ig_\gamma$$

for all $1 \leq i \leq s$. If this is true, then each of the double cosets is a union of cosets with representatives from (iii), hence the cosets Hr_ig_γ, $1 \leq i \leq s$, $\gamma \in \gamma_i^H$, form a union of double cosets. Otherwise an element in S outside H is found.

(v) If (iv) is true, then for each of the cosets Hr_ig_γ, $1 \leq i \leq s$, $\gamma \in \gamma_i^H$, and for each of the generators $t \in X$, decide whether $Hr_ig_\gamma t$ lies in one of the double cosets $Hr_1H, \dots, Hr_sH$. If this is always true, then $H = S$; otherwise we find an element in S that does not lie in H.

It is not hard to prove this algorithm, and at a first look it does not seem to do better than the old approach. But the following remark will show that we get a big improvement from using double cosets. To do this, we assume that the orbits are calculated in the usual way with the help of Schreier vectors, i.e. each g_γ is encoded in the Schreier vector as a word in the generators of H, and deleting a generator from the right will again produce another g_δ.

Remark 2.2. (i) Part (v) of the algorithm becomes trivial, whenever the generator t is an element of H already, since then each double coset is closed under multiplication with t.

(ii) For any other generator $t \notin H$, define

$$T = H \cap H^{t^{-1}}.$$

Then, for any $y \in T$, we have that $y^t \in H$, hence there exists an $h \in H$ with

$$yt = th.$$

As a consequence we see that, whenever a coset representative r_ig_γ with $\gamma \in \gamma_i^H$ ends with an element $y \in T$ in his description in the Schreier vector, then it follows that

$$r_ig_\gamma = r_ig_\delta y$$

with $\delta = \gamma^{y^{-1}}$ and we have that

$$r_ig_\gamma t = r_ig_\delta yt = r_ig_\delta th,$$

hence $r_ig_\gamma t$ lies in the same double coset as $r_ig_\delta t$.
It follows that, besides the trivial coset, we only have to check those coset representatives r_ig_γ that do end with a generator outside T.

This remark will reduce the number of necessary tests dramatically; in our application we will go from 9606 125 Schreier generators for each generator of the group to just 68 final relations that have to be checked.

Moreover, to prove the equality in part (iv) of the algorithm, it suffices to show that $H \cap H^{r_i} = Stab_H(\gamma_i)$, which can be further reduced to the proof of the statement that $Stab_H(\gamma_i) \leq H^{r_i}$, an easy membership problem.

3. Inside the Stabilizer

In this section we will sketch the way to find a subgroup $H \simeq 3McL:2$ inside the stabilizer of a point in our group G. We will start with the two permutations $t, z \in Sym_{9606\,125}$, computed by Cooperman *et al.* (1997). While z has order 67 and no fixpoints, the element t is an involution with 2685 fixpoints. We choose β_1 to be the smallest fixpoint of t and define

$$S = Stab_G(\beta_1) \leq G.$$

Computing the orbit of β_1 under t and the powers of z, we easily find an element

$$x = ztz^{65}tz^{34}tz^9 \in S$$

with order 10 and 5 fixpoints.

Defining

$$H = \langle t, x\rangle \leq S,$$

and computing the orbits of H on Ω, we get five of them, and exactly the suborbit sizes of $3McL:2$ in Ly as stated in the ATLAS (Conway *et al.*, 1985), so we take this H as our candidate. The rest of the section deals with the proof that this guess is correct, hence $H \simeq 3McL:2$.

This proof is divided into three parts; first we will get to the sporadic group McL, after that we will deal with the central part of order 3 and the automorphism of order 2.

In the next step we restrict our group H to one of the above orbits, namely the one of length 15 400, since the central element of order 3 will fix this whole orbit. This eliminates the central part and gives two permutations $\widetilde{t}$ and $\widetilde{x}$, and a group $\widetilde{H} = \langle \widetilde{t}, \widetilde{x}\rangle$ on 15 400 points with $|\widetilde{H}| = |McL:2|$. Looking at the character table of $McL:2$ and the number of fixpoints of $\widetilde{t}$, which is 110, we see that $\widetilde{t}$ cannot lie in McL, hence we have to search for other elements. A few random calculations produce the elements

$$\widetilde{x_1} = \widetilde{x}^2,\ \widetilde{x_3} = (\widetilde{t}\widetilde{x})^3$$

with the property that

$$\widetilde{U} = \langle \widetilde{x_1}, \widetilde{x_3}\rangle$$

has order $|\widetilde{U}| = |McL|$.

It remains to show that $\widetilde{U}$ is in fact isomorphic to McL. But it is easier to go directly to the next step, lift $\widetilde{x_1}$ and $\widetilde{x_3}$ to $x_1 = x^2,\ x_3 = (tx)^3$, and try to prove that

$$U = \langle x_1, x_3\rangle \simeq 3McL.$$

This can be done by finding elements inside U for the ATLAS presentation of $3McL$; the details of this computation can be found in Gollan (1998).

The only thing left in this section is to add our involution t to the group U and to show that this gives a group of type $3McL:2$. This is done by showing that t normalizes U with the help of a certain base and strong generating set for U. Moreover, these relations, together with the relations from the ATLAS presentation for $3McL$, give a presentation for the group $3McL:2$. Some additional computations finally prove that

$$H = \langle t, x\rangle \simeq 3McL:2.$$

4. The Order of the Group

The aim of this section is to compute the order of the group G by using the double coset trick to prove that $H \simeq 3McL{:}2$ equals the stabilizer S.

To do this, we first compute a base of length 2 and a strong generating set for the subgroup H, where the intermediate stabilizer $T \leq H$ has order $|T| = 349\,920$. Then we extend H to a subgroup

$$K = \langle H, y \rangle \leq G$$

by adding an additional involution y to H. Since H has five orbits on Ω, we get five orbit representatives $\gamma_1, \ldots, \gamma_5$ and five double cosets for Algorithm 2.1. For the four non-trivial orbits we have to compute the stabilizers $Stab_H(\gamma_i)$, where one of them equals T, and we have to use them to check part (iv) of the double coset trick. Again, we omit the details here and refer the reader to Gollan (1998).

Looking at Remark 2.2 we note that y is the only generator of K outside our proposed stabilizer H, hence we have to check only this generator and only coset representatives that do end with a generator outside $T = H \cap H^y$. But the number of such representatives equals the number of orbits of T on Ω, and we can easily compute that we will end with 68 relations to check in part (v) of the double coset trick.

Producing these relations is an application of orbit calculations and Schreier vectors, together with the use of the known base and strong generating set for H. As it turns out, six of these relations are either trivial or direct consequences of the fact that y is an involution. Once knowing these relations, it is a lengthy, but routine computation with large permutations of degree 9606 125 to check that they are correct in our given permutation group K. The interested reader can obtain the relations from the author; they can also be found in Gollan (1998).

From this it follows that $H \simeq 3McL{:}2$ is the full stabilizer of β_1 in K, hence

$$|K| = |Ly|.$$

In addition, it is not hard to prove that

$$K = G,$$

and therefore

$$|G| = |Ly|.$$

Collecting these 62 relations, together with the ones needed to check part (iv) of the double coset trick and the relations for $3McL:2$ from Section 3, we get a presentation for G, and, as we will prove in the next section, for Lyons' simple group as well.

5. The End of the Proof

This final section finishes the existence proof for Lyons' simple group by going back to Lyons' original paper (Lyons, 1972) and proving that the two assumptions needed there are true in our group G. Thus we have to show that the centralizer of an involution in G is isomorphic to the double cover of the alternating group A_{11}, and that such an involution does not lie in $\mathbf{Z}^*(G)$.

The first thing to notice is that, since $H \simeq 3McL{:}2$ has only two classes of involutions and the index of H in G is odd, there can be at most two conjugacy classes of involutions in G. Using a well known formula for induced characters, it follows easily that G has exactly one class of involutions, and we can take t as its representative. For the rest of the paper let

$$C = Cen_G(t)$$

be the centralizer of t in G. Another application of the character formula gives the order of C as

$$|C| = |2A_{11}|,$$

and we are close to our final goal. To prove that

$$C \simeq 2A_{11},$$

we have to find elements in C for the classical presentation of $2A_{11}$ by Schur (1911). Once again, details are in Gollan (1998). Knowing that the centralizer C has the right isomorphism type, we are left with a proof for the fact that

$$t \notin \mathbf{Z}^*(G).$$

But this follows from Corollary 1 of Glauberman's $\mathbf{Z}^*(G)$ paper (Glauberman, 1966), since t is central in C and G has only one class of involutions. This proves that both assumptions from Lyons' original paper are true for our group G, and we have proved the following theorem.

Theorem 5.1. *$G \simeq Ly$, hence Lyons' simple group exists.*

Acknowledgements

The author thanks G. Michler for all his support, and G. Cooperman, W. Lempken, and R. Staszewski for fruitful discussions and inspiring ideas.

Note added in proof: V. Gebhardt (Essen) has proved that the 62 non-trivial relations from part (v) of the double coset trick can be replaced by just one additional relation to produce a presentation for Ly in Section 4.

References

Bosma, W., Cannon, J., Playoust, C. (1997). The MAGMA algebra system I: The user language. *J. Symb. Comput.*, **24**, 235–265.

Butler, G. (1991). *Fundamental Algorithms for Permutation Groups.* Berlin, Springer.

Cannon, J. (1984). An introduction to the group theory language CAYLEY. In Atkinson, M. ed., *Computational Group Theory*, pp. 145–183. London, Academic Press.

Cannon, J., Havas, G. (1992, May). Algorithms for groups. *Austr. Comput. J.*, **24**, 51–60.

Conway, J., Curtis, R., Norton, S., Parker, R., Wilson, R. (1985). *Atlas of Finite Groups*, Oxford, Clarendon Press.

Cooperman, G., Finkelstein, L., Tselman, M., York, B. (1997). Constructing permutation representations for matrix groups. *J. Symb. Comput.*, **24**, 471–488.

Glauberman, G. (1966). Central elements in core-free groups. *J. Algebra*, **4**, 403–420.

Gollan, H. (1995). A new existence proof for *Ly*, the sporadic simple group of R. Lyons. Preprint 30, Institute for Experimental Mathematics, University of Essen.

Gollan, H. (1998). *A Contribution to the Revision Project of the Sporadic Groups: Lyons' Simple Group Ly,* volume 26 of *Vorlesungen aus dem Fachbereich Mathematik der Universität GH Essen*, Department of Mathematics, University of Essen.

Gollan, H., Havas, G. (1999). On Sims' presentation fr Lyons' simple group. In Dräxler, P., Michler, G., Ringel, C. eds, *Computational Methods for Representations of Groups and Algebras*, pp. 235–240. Basel, Germany, Birkhäuser Verlag.

Gorenstein, D. (1982). *Finite Simple Groups.* New York, Plenum Press.

Lyons, R. (1972). Evidence for a new finite simple group. *J. Algebra*, **20**, 540–569.

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

Schur, I. (1911). Über die darstellung der symmetrischen und der alternierenden gruppe durch gebrochene lineare substitutionen. *J. Reine Ang. Math.*, **139**, 155–250.

Sims, C. (1970). Computational methods in the study of permutation groups. In Leech, J. ed., *Computational Problems in Abstract Algebra*, pp. 169–183. Oxford, Pergamon Press.

Sims, C. (1972). The existence and uniqueness of Lyons' group. In Gagen, T., Hale, M., Shult, E. eds, *Finite Groups '72 (Gainsville Conference)*, pp. 138–141. Amsterdam, North–Holland.

Originally Received 15 August 1996
Accepted 20 April 2000