Discrete Mathematics 112 (1993) 41–47
North-Holland

Generating the Mathieu groups and associated Steiner systems

Marston Conder

Department of Mathematics and Statistics, University of Auckland, Private Bag 92019, Auckland, New Zealand

Received 13 July 1989
Revised 3 May 1991

Abstract

Conder, M., Generating the Mathieu groups and associated Steiner systems, Discrete Mathematics 112 (1993) 41–47.

With the aid of two coset diagrams which are easy to remember, it is shown how pairs of generators may be obtained for each of the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24}, and also how it is then possible to use these generators to construct blocks of the associated Steiner systems $S(4, 5, 11)$, $S(5, 6, 12)$, $S(3, 6, 22)$, $S(4, 7, 23)$ and $S(5, 8, 24)$ respectively.

1. Introduction

Suppose you land yourself in 24-dimensional space, and are faced with the problem of finding the best way to pack spheres in a box. As is well known, what you really need for this is the Leech Lattice, but alas: you forgot to bring along your Miracle Octad Generator. You need to construct the Leech Lattice from scratch. This may not be so easy! But all is not lost: if you can somehow remember how to define the Mathieu group M_{24}, you might be able to produce the blocks of a Steiner system $S(5, 8, 24)$, and the rest can follow.

In this paper it is shown how two coset diagrams (which are easy to remember) can be used to obtain pairs of generators for all five of the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24}, and also how blocks may be constructed from these for each of the Steiner systems $S(4, 5, 11)$, $S(5, 6, 12)$, $S(3, 6, 22)$, $S(4, 7, 23)$ and $S(5, 8, 24)$ respectively.

The significance of the Mathieu groups is well established. On one hand, they are examples of multiply-transitive permutation groups: M_{12} and M_{24} are 5-transitive groups of degree 12 and 24 respectively, the point-stabilizers M_{11} and M_{23} are 4-transitive on 11 and 23 points respectively, and the stabilizer of two points in M_{24} is

Correspondence to: Marston Conder, Department of Mathematics and Statistics, University of Auckland, Private Bag 92019, Auckland, New Zealand

0012-365X/93/$06.00

the group M_{22}, which is 3-transitive of degree 22. Also, following the classification of finite simple groups it is now known that the only other finite groups which are 4-transitive (or more) on a set of size n are the alternating group A_n (for $n \geqslant 6$) and the symmetric group S_n (for $n \geqslant 4$). Another reason for their importance is that all the Mathieu groups are sporadic simple groups; that is, they are five of the 26 finite simple groups which do not fall into any of the infinite families of finite simple groups (cyclic groups, alternating groups, and groups of Lie type over a finite field). Finally (and due to their multiple-transitivity), they are associated with some very nice combinatorial structures – notably Steiner systems and the Leech lattice, which will be discussed in Section 4. An excellent full account of these things is given in a recent book by Conway and Sloane [1].

It should be stated here that the Mathieu groups have been constructed and analysed in quite a number of different ways since their discovery over 100 years ago. One very elegant definition of M_{24} (appearing in [1]) is obtained by taking the natural action of the group PSL(2,23) on the projective line over the field $\mathbb{Z}_{23}$, and adjoining the permutation which takes x to $x^3/9$ if x is a square in $\mathbb{Z}_{23}$, or to $9x^3$ if x is a nonsquare in $\mathbb{Z}_{23}$. Also the pair of generators we give for M_{12} has certainly appeared before (in [3] for example), but the choice of generators for M_{24} and its subgroups is original. In any case our approach is quite different, and may at least be a good advertisement for the use of coset diagrams!

2. Generators for M_{11} and M_{12}

Let x and y be the following permutations of degree 12: $x=(3,4)(6,7)(9,10)(11,12)$, and $y=(1,2,3)(4,5,6)(7,8,9)(10,11,12)$. These can be depicted quite easily by the diagram in Fig. 1, where triangles are used to denote the cycles of y (with vertices permuted counter-clockwise), and where x interchanges the end-points of the additional edges. This is an example of a coset diagram: its vertices may be relabelled by the right cosets of the stabilizer of any given point. A more formal definition of such diagrams is given by Coxeter and Moser in [2].

The same diagram, but with vertices labelled differently, would be obtained by taking x and y to be the elements D and $ACFE$ in the presentation given for M_{12} by Todd in [4]. As a consequence of this, the permutations x and y generate a subgroup of M_{12}. In fact they generate M_{12} itself, as we shall see.

First notice that this group is transitive on 12 points – the diagram is connected! With products read from left to right, the element xy is the 11-cycle $(1,2,3,5,6,8,9,11,10,7,4)$, fixing the point 12. Also the conjugate of x by yxy^{-1} fixes 12 (as yxy^{-1} moves 8 to 12), and in fact, if we take $u=(yxy^{-1})^{-1}x(yxy^{-1})=(2,7)(3,4)(5,11)(8,10)$, and $v=u(xy)^3=(1,5,4,8)(6,11,9,7)$, we have two elements that generate a subgroup of the stabilizer of 12, transitive on the remaining 11 points, as depicted by the diagram in Fig. 2 (where the heavy dots indicate fixed points of v). It turns out that u and v generate the Mathieu group M_{11}.

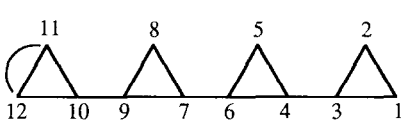

Fig. 1. Generators for the Mathieu group M_{12}.

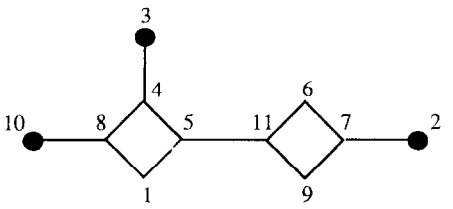

Fig. 2. Generators for the Mathieu group M_{11}.

The same sort of thing can be done with elements fixing the point 1 as well: take u (which fixes both 12 and 1), and conjugate v by each of uv and uv^2 (because v fixes 10 and 3), to obtain $a=u=(2,7)(3,4)(5,11)(8,10)$, and $b=v^{-1}u^{-1}vuv=(2,11,4,7)(3,10,5,9)$, and $c=v^{-2}u^{-1}vuv^2=(2,9,8,6)(3,10,4,7)$. These generate a group which is transitive on the set $\{2,3,4,\ldots,11\}$, fixing the other two points. Similarly, taking for example $p=c=(2,9,8,6)(3,10,4,7)$, $q=a^{-1}ca=(2,4,8,3)(6,7,9,10)$, and $r=b^{-1}c^{-1}bcb=(2,10,3,4)(5,7,9,8)$, we have elements generating a group which is transitive on $\{2,3,4,\ldots,10\}$, fixing the three points 12, 1 and 11, and in this case it is not difficult to see that p and q generate a group of order 8 (isomorphic to the quaternion group), fixing the points 12, 1, 11 and 5.

Working backwards, we find the stabilizer of the three points 12, 1 and 11 has order at least 9×8 (that is, 72), therefore the stabilizer of the two points 12 and 1 has order at least $10\times 9\times 8$ (that is, 720), and so on. Since the order of M_{12} is 95040 (which is $12\times 11\times 10\times 9\times 8$), this proves that x and y generate M_{12}, and also that u and v generate M_{11}.

3. Generators for M_{22}, M_{23} and M_{24}

Let x and y be the following permutations of degree 24:

$$x=(1,14)(4,5)(6,7)(8,9)(11,24)(16,17)(18,19)(20,21), \quad \text{and}$$

$$y=(1,2,3,4)(5,6,7,8)(9,10,11,12)(13,14,15,16)(17,18,19,20)(21,22,23,24).$$

These can be depicted by the coset diagram in Fig. 3, where squares instead of triangles are used to denote the cycles of y (again with vertices permuted counter clockwise).

The same diagram, but with vertices labelled differently, would be obtained by taking x and y to be (for instance) the elements $H^{-1}G^{-1}A^{-1}IAGH$ and $AGIJK$ in the presentation given for M_{24} in [4]. In particular, these permutations x and y generate a transitive subgroup of M_{24}, which we will show to be M_{24} itself.

First, the element xy has order 11, and fixes the points 7 and 19. Other elements which fix 7 may be obtained by conjugating x (for example). Letting

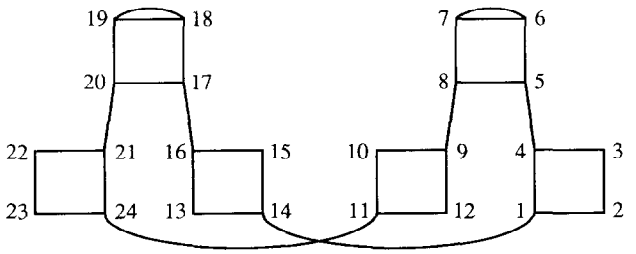

Fig. 3. Generators for the Mathieu group M_{24}.

$u=(yxy^{-1})^{-1}x(yxy^{-1})=(1,14)(3,9)(5,12)(6,13)(11,19)(15,21)(16,18)(17,24)$, and $v=(yxy)x(yxy)^{-1}=(2,12)(3,6)(5,11)(8,16)(9,22)(10,17)(14,24)(15,18)$, and $w=xy=(1,15,16,18,20,22,23,24,12,9,5)(2,3,4,6,8,10,11,21,17,13,14)$, the elements u and w generate a subgroup of the stabilizer of 7, transitive on the remaining 23 points, while the elements v and w generate a subgroup of the stabilizer of 7 and 19, transitive on the remaining 22 points. The former subgroup will be shown to be isomorphic to the Mathieu group M_{23}, and the latter isomorphic to M_{22}.

At this stage the coset diagrams for these pairs of generators could be drawn, but they are not particularly illuminating. One thing that can be seen is the fact that vw^2 has order 5, and also fixes the points 6 and 18. Drawing the coset diagram for v and vw^2 is then more helpful for finding other elements which fix these points. Indeed as $(vw^2)^3v$ moves 1 to 18, we may take $q=vw^2=(1,16,11,15,22)(2,5,17,21,13)(3,10,14,9,24)(4,8,20,23,12)$, and then $p=v^{-1}q^{-3}vq^3v=(1,13)(2,9)(3,22)(5,17)(6,24)(8,15)(12,14)(20,21)$, and we find the group generated by p and q fixes 7, 19 and 18, and is transitive on the remaining 21 points. Taking this further, if $a=q=(1,16,11,15,22)(2,5,17,21,13)(3,10,14,9,24)(4,8,20,23,12)$, and $b=p^{-1}q^{-3}pq^3p=(1,9)(2,11)(4,17)(5,8)(10,20)(12,24)(14,16)(21,22)$, and $c=(qpq^2p)^{-1}p(qpq^2p)=(1,24)(2,17)(4,11)(5,21)(8,22)(9,12)(10,16)(14,20)$, then a, b and c generate a transitive group of degree 20, fixing all four of the points 7, 19, 18 and 6.

In particular, this shows that the group we started with is 5-transitive, and must therefore be M_{24}. Furthermore, the group generated by a, b and c is imprimitive, permuting the five blocks $\{1,4,5,14\}$, $\{2,10,12,22\}$, $\{3,13,15,23\}$, $\{11,20,21,24\}$ and $\{8,9,16,17\}$ among themselves, and so it is not hard to see that a,b and c generate a group of order 960 (being an extension of an elementary Abelian group of order 16 by the alternating group A_5). It follows that p and q generate a group of order 21×960 (that is, 20 160), and then v and w generate a group isomorphic to M_{22}, of order 443 520. Similarly, but not so obviously, the group generated by u and w is isomorphic to M_{23}, of order 10 200 960 (and fixing the point 7); here is a nice reason why: $u^{-1}w^2u^{-1}w^{-1}uwuw^{-2}u$ (of order 2) and w^6 (of order 11) both fix the two points 7 and 19, and the associated coset diagram is just a relabelled version of the one corresponding to v and w, so they also generate the stabilizer of these two points!

4. The associated Steiner systems (and the Leech lattice)

As is well known, a Steiner system $S(t,k,v)$ is a combinatorial design consisting of a set of v points and a collection of subsets, called blocks, each of size k, with the property that every set of t points is contained in exactly one block. In the case where $(t,k,v)=(5,6,12)$, there is one such design, unique up to isomorphism, and its automorphism group is the Mathieu group M_{12}, which acts transitively on the set of 132 blocks. Also the complement of every block is a block. Moreover, there are 66 blocks containing any particular point α, and if α is removed from each of these then the resulting sets are the blocks of a Steiner system $S(4,5,11)$, with automorphism group M_{11}. Removing a second point gives rise to a Steiner system $S(3,4,10)$, with 30 blocks, and so on. Similarly, when $(t,k,v)=(5,8,24)$ there is only one such design, and its automorphism group is the Mathieu group M_{24}. This group acts transitively on the set of 759 blocks, and removal of any point α from the 253 blocks containing α produces a Steiner system $S(4,7,23)$, with automorphism group M_{23}, and removal of a second point then gives a Steiner system $S(3,6,22)$, with 77 blocks and automorphism group M_{22}, and so on.

We now use these facts together with the generators obtained for the Mathieu groups in Sections 2 and 3, to construct one each of the Steiner systems in question.

First recall that in Section 2, the stabilizer of the four points 12, 1, 11 and 5 was generated by $p=(2,9,8,6)(3,10,4,7)$ and $q=(2,4,8,3)(6,7,9,10)$. It is not hard to see that the four sets $\{2,8\}$, $\{3,4\}$, $\{6,9\}$ and $\{7,10\}$ are permuted by p and q among themselves, and also that they form the blocks of a Steiner system $S(1,2,8)$. We can extend this to a Steiner system $S(2,3,9)$, as follows: adjoin the point 5 to each of these sets, to obtain the blocks containing 5, and then apply permutations such as r, r^2, rp and rp^2 (moving 5 to different points from the set $\{2,3,4,5,6,7,8,9,10\}$), to produce the required twelve blocks. Similarly, adjoining the point 11 to each of these blocks, and then applying appropriate elements of the group generated by a, b and c, will give the 30 blocks of a Steiner system $S(3,4,10)$; and the same thing with the point 1 and selected permutations involving u and v will produce the 66 blocks of a Steiner system $S(4,5,11)$. Finally, adjoining the point 12 to each of these, and including all the complements, gives a Steiner system $S(5,6,12)$.

In particular, one of the resulting blocks is $B=\{1,2,5,8,11,12\}$, and every other block is obtainable as the image of B under some element in the group M_{12} generated in Section 2 – corresponding to the fact that the automorphism group of this design is transitive on blocks!

The diagram in Fig. 4 conveniently summarizes the situation: it gives generators for M_{12}, and the points labelled with asterisks make up a block of the associated Steiner system $S(5,6,12)$, all other blocks being obtainable as images of this one under elements of the group.

The same sort of thing can be done for M_{24}: the set $\{6,7,8,9,16,17,18,19\}$ and all its images under elements of the permutation group generated in Section 3 make up the blocks of a Steiner system $S(5,8,24)$. To see this, recall that the stabilizer of the

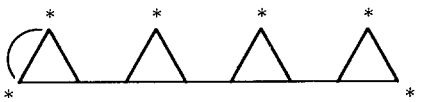

Fig. 4. A starting block for $S(5,6,12)$.

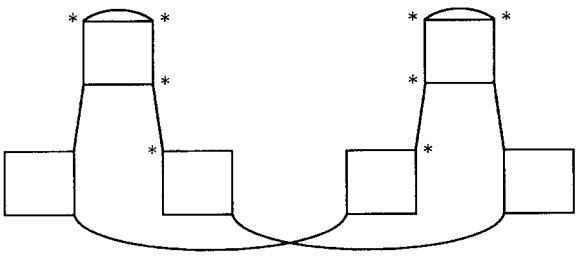

Fig. 5. A starting block for $S(5,8,24)$.

four points 7, 19, 18 and 6 was imprimitive, permuting the five sets $\{1,4,5,14\}$, $\{2,10,12,22\}$, $\{3,13,15,23\}$, $\{11,20,21,24\}$ and $\{8,9,16,17\}$ among themselves. In particular, these sets form the blocks of a Steiner system $S(1,4,20)$; and then adjoining the point 6 to each of them and applying elements of the group generated by the permutations p and q will produce the 21 blocks of a Steiner system $S(2,5,21)$. At the next stage, if the point 18 is adjoined, application of the permutations w^k and $w^{-1}vw^k$ (for various k) is enough to obtain the blocks of a Steiner system $S(3,6,22)$, as these all move 18 to different points. Similarly, the permutations uw^k and uvw^k (for $0 \leqslant k < 11$) can be applied when the next point, 19, is adjoined, to give the blocks of a Steiner system $S(4,7,23)$, and finally, when the last point, 7, is adjoined to all these, application of xw^k and yxw^k (for $0 \leqslant k < 11$) is enough to obtain the blocks of a Steiner system $S(5,8,24)$.

Obviously this is not going to be the most efficient way of constructing the blocks, but on your desert island in 24-dimensional space one thing you will not be short of is time! All you need to remember is summarized in the diagram in Fig. 5: there are generators for M_{24}, and the points labelled with asterisks make up a block of the associated Steiner system $S(5,8,24)$, all other blocks obtainable as images of this one under elements of the group.

Incidentally, one of the blocks is $\{3,6,7,13,15,18,19,23\}$, the set of all fixed points of the permutation b, which is a conjugate of the original generator x. It follows that the set of fixed points of x is also a block – and this is even easier to remember!

To finish off, we briefly consider the Leech lattice Λ_{24}. This is a beautiful example of an integral lattice in $\mathbb{R}^{24}$, particularly significant because of the fact that spheres can be centred at each of its points to give the best known packing (in terms of density and other considerations) for this space or indeed for any Euclidean space of about the same dimension. As stated earlier, an excellent account of such things is given in [1]. To construct Λ_{24}, all that is really necessary is to know the blocks of a Steiner

system $S(5, 8, 24)$: for each block B of this design, let v_B be the vector in $\mathbb{R}^{24}$ which has a 2 in each of the eight positions corresponding to points of B, and 0's elsewhere. Also define w_{24} as the vector with a 1 in every position except the last, where it has a -3. Then Λ_{24} simply consists of all integral linear combinations of these 760 vectors!

Acknowledgment

The CAYLEY system was used (and is recommended) for the analysis of the groups and designs described in this paper.

References

[1] J.H. Conway and N.J.A. Sloane, Sphere Packings, Lattices and Groups (Springer, New York, 1988).
[2] H.S.M. Coxeter and W.O.J. Moser, Generators and Relations for Discrete Groups, 4th ed. (Springer, Berlin, 1980).
[3] J. Leech, A presentation for the Mathieu group M_{12}, Canad. Math. Bull. 12 (1969) 41–43.
[4] J.A. Todd, Abstract definitions for the Mathieu groups, Quart. J. Math. Oxford Ser. 2 21 (1970) 421–424.