

# IMPROVED BOUNDS FOR THE SPREAD OF SPORADIC GROUPS

J. D. BRADLEY AND P. E. HOLMES

## *Abstract*

The *spread* of a group  $G$  is the greatest number  $r$  such that, for every set of non-trivial elements  $\{x_1, \dots, x_r\}$ , there exists an element  $y$  with the property that  $\langle x_i, y \rangle = G$  for  $1 \leq i \leq r$ . In this paper we obtain good upper bounds for the spread of 14 sporadic simple groups computationally and determine the value of the spread of  $M_{11}$  by hand.

## 1. *Introduction*

It was shown by Binder in [1, 2] that given any two non-trivial elements  $x_1$  and  $x_2$  of the symmetric group  $S_n$ ,  $n > 4$ , there exists a third element  $y$  such that  $S_n = \langle x_1, y \rangle = \langle x_2, y \rangle$ . From this Brenner and Wiegold made the following definition in [6].

**DEFINITION 1:** Let  $r$  be a positive integer. A finite non-abelian group  $G$  is said to have spread  $r$ , if for every set  $\{x_1, x_2, \dots, x_r\}$  of distinct non-trivial elements of  $G$ , there exists an element  $y \in G$  such that  $G = \langle x_i, y \rangle$  for all  $i$ , and  $r$  is the maximum value for which this is true.

We denote the spread of a group  $G$  by  $s(G)$ .

It is clear from the above definition that  $s(G)=0$  if  $G$  is not semi-simple (*i.e.* has no proper soluble normal subgroup) or the semidirect product of two cyclic groups of prime order, as no element can be one of a generating pair if it is in a normal subgroup with non-cyclic quotient. It is proved in [12] that  $s(G) \geq 1$  for all finite simple groups  $G$ .

The generation properties of finite groups, especially finite simple groups, is something which has provoked interest from researchers over the years. An example of such a generation property is the probability of generating a group with a randomly chosen element [12], [15], but there are many others. The concept of the spread is another such generation property and has been studied, for example, by Guaralínck and Shalev using counting and probabilistic methods in [11]. The spread of sporadic groups has been studied before by Bradley, Ganief, Moori and Woldar, see below.

Pairwise generating sets are studied in [14] and [3]. These papers are interested in the maximal size  $\mu(G)$  of a set of elements of a group  $G$ , any two of which generate the whole group. This number is clearly an upper bound for the spread of a group. To see this, let  $S$  be a maximal pairwise generating set. Then if there was an element of  $G \setminus S$  that generated  $G$  with every member of  $S$ , it would contradict the maximality of  $S$ .

It can be observed from Table 1 that the spread of sporadic groups varies wildly and often bears little relation to the size of the group. For instance the spread of  $M_{23}$  is much greater than the spread of  $M_{24}$ . The groups with a high spread are often the ones with elements of large prime order only contained in a small number of small subgroups. For example the elements of order 23 in  $M_{23}$  are each only contained in an single subgroup of order  $23 \times 11$  and so to obtain a set of elements as described in section 3 we must have an element from each of these subgroups. In  $M_{24}$  however, the elements of order 23 are contained in one of the 24 the subgroups isomorphic to  $M_{23}$ , and so it takes far fewer elements to obtain a set of elements of the desired type.

In [10] Ganief and Moori compute lower bounds for the exact spread of the sporadic groups. Breuer *et al* use similar methods to improve these bounds in [7]. Upper bounds are given by Moori and the first author in [5].

In this paper we use the computer algebra system MAGMA [4] to calculate much improved upper bounds for the spread of some of the sporadic simple groups and give a hand proof that  $s(M_{11}) = 3$ . The latter result was proved independently by Woldar [19]. His proof differs substantially from ours and is less geometric. Our results are shown in Table 1. The best known lower bound is given in the first column. The result for  $M_{11}$  comes from our work, the other results come from [7] and [10], which both give a lower bound of 2 for  $s(M_{11})$ . The second column gives our results. The final column gives the previously known bounds from [5] for comparison purposes.

In Section 2 we give the computer-free proof that the spread of  $M_{11}$  is 3. Section 3 describes the computational methods used to compute the bounds for the other groups.

We believe that it is essential that we ensure that our computational results are replicable. To this end, we have included the programs in the appendix, together with the seeds that MAGMA's random processes use to give our exact results.

Group	Lower bound	Upper bound	Old upper bound
$M_{11}$	3	3	16
$M_{12}$	3	9	211
$M_{22}$	21	26	720
$M_{23}$	1525	8064	41020
$M_{24}$	12	56	3152
$J_1$	77	179	5690
$J_2$	5	24	1071
$J_3$	78	597	43792
$M^cL$	71	308	31184
HS	19	33	1280
He	199	1223	275125
$Co_3$	99	1839	829200
Suz	41	956	532035
$Fi'_{24}22$	14	186	210897

Table 1

## 2. The exact spread of $M_{11}$

### 2.1. Background

The 5 sporadic simple Mathieu groups,  $M_{11}$ ,  $M_{12}$ ,  $M_{22}$ ,  $M_{23}$  and  $M_{24}$ , were discovered in the 19th century by E. Mathieu [16, 17]. The largest of the 5 groups is  $M_{24}$ , which can be defined to be the automorphism group of the unique Steiner system  $(5,8,24)$ , *i.e.* a set of 759 subsets of size 8 of a set  $\Omega$  of size 24 such that any five of the 24 points lie together in exactly one of the sets of size 8. We call these sets of size 8 *octads*.  $M_{24}$  is a 5-transitive permutation group on 24 points. The binary Golay code is a 12 dimensional code of length 24 over the field of order 2 spanned by the 759 octads, with addition defined as the symmetric difference of 2 sets. This code contains the vectors of weight 0 and 24, 759 vectors of weight 8 (*i.e.* the octads), 759 vectors of weight 16 (*i.e.* the complements of the octads) and 2576 vectors of weight 12. These sets of size 12 are called *dodecads*. Sets corresponding to a vector in the Golay code are called *C-sets*. More information about the group  $M_{24}$  can be found in [8] and [9]. In [9, chapter 12] detailed information can be found about  $M_{24}$  and its subgroup structure including a way of determining easily whether a given set is a C-set.

The stabiliser of a dodecad (and hence also the complementary dodecad) in  $M_{24}$  is  $M_{12}$ . The stabiliser of a dodecad and a point in the dodecad is the group  $M_{11}$ .  $M_{11}$  is then a permutation group on the 11 non-fixed points in one of the dodecads and the 12 points in the complementary dodecad. The point stabiliser in the 11 point action is  $M_{10} \cong A_6 \cdot 2$  and in the 12 point action the stabiliser is  $L_2(11)$ .

### 2.2. The main result

THEOREM 1:  $s(M_{11}) = 3$ .

*Proof.* By checking the orders of the maximal subgroups of  $M_{11}$  we see that the only maximal subgroups containing an element of order 11 are the ones isomorphic to  $L_2(11)$ . Furthermore, by a counting argument, or by observing that each  $L_2(11)$  is a stabiliser of a point in the 12 point action and elements of order 11 act with cycle shape  $1^1 11^1$ , we can see that each element of order 11 is contained in precisely one of these subgroups. Therefore if  $y$  is an element of order 11 fixing the point  $p$  in the 12 point action and  $x$  is any element not fixing  $p$ , then  $x$  does not lie in a maximal subgroup with  $y$  and hence  $\langle x, y \rangle = M_{11}$ . In light of this we seek to prove that for any set of 3 non-trivial elements  $\{x_1, x_2, x_3\}$  of  $M_{11}$  there is a point  $p$  in the 12-point action not fixed by any of the 3 elements. Then we choose an element  $y$  of order 11 fixing  $p$  and since the only maximal subgroup containing  $y$  is the stabiliser of  $p$  isomorphic to  $L_2(11)$ , not containing  $x_1, x_2$  or  $x_3$ , we will have  $\langle x_1, y \rangle = \langle x_2, y \rangle = \langle x_3, y \rangle = M_{11}$  and hence  $s(M_{11}) \geq 3$ .

Looking at the character table of  $M_{11}$  we see that involutions fix 4 points in the 12 point action and all other non-trivial elements fix fewer. This means that if we have a set of 3 non-trivial elements, unless they are all involutions, there must be a point not fixed by any of the 3 elements. The only possibility is a set of 3 involutions whose fixed point sets are pairwise disjoint. Let us assume, without loss of generality, that  $D$  is a dodecad containing the point  $p$  and the the copy of  $M_{11}$  we are dealing with is the stabiliser in  $M_{24}$  of  $D$  and the point  $p \in D$ . Let  $x_1, x_2, x_3 \in M_{11}$  be three involutions, with fixed point sets  $O_1, O_2$  and  $O_3$  respectively, such that every

point in  $\Omega/D$ , the complement of  $D$ , is in one of  $O_1, O_2$  or  $O_3$ . Now  $O_1, O_2$  and  $O_3$  are octads so  $O_1 + O_2 + O_3$  is a C-set. By construction  $O_1 + O_2 + O_3$  contains the dodecad  $\Omega/D$  and also the point  $p \in D$ . The only C-set to strictly contain a dodecad is  $\Omega$ , and hence  $O_1 + O_2 + O_3 = \Omega$ . But this is a contradiction since  $|\Omega| = 24$  and  $|O_i| = 8$  and  $p \in O_i$  for  $i \in \{1, 2, 3\}$ . Hence  $s(M_{11}) \geq 3$ .

In order to show that  $s(M_{11}) = 3$  we must show that there exists a set of 4 non-trivial elements  $\{x_1, x_2, x_3, x_4\}$  such that one cannot find  $y \in M_{11}$  such that  $\langle x_1, y \rangle = \langle x_2, y \rangle = \langle x_3, y \rangle = \langle x_4, y \rangle = M_{11}$ .

We note from the character table that any element of  $M_{11}$  fixes either a point in the 11-point action or a point in the 12-point action. Therefore if we can find a set of 4 elements of  $M_{11}$  such that every point in  $\Omega$  is fixed by one of them then any element  $y$  lies in a maximal subgroup of  $M_{11}$  with at least one of our elements, *i.e.* the point stabiliser of one of the points fixed by  $y$ . In order to prove such sets of 4 elements exist we first prove a lemma.

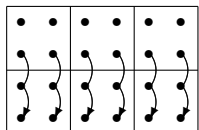
LEMMA 1: Consider the subgroup  $M_{11}$  of  $M_{24}$  fixing the dodecad  $D$  and the point  $p \in D$ . If  $O$  is an octad containing  $p$  and meeting  $D$  in 4 points, then there is an involution  $\pi \in M_{11}$  fixing  $O$  pointwise.

*Proof.* Consider the fixed point set of an involution in our copy of  $M_{11}$ . It is certainly an octad, it certainly contains  $p$  and since it contains 3 fixed points in the 11-point action and 4 in the 12-point action it is an octad satisfying the conditions of the lemma. Now let  $O$  be an octad satisfying the conditions of the lemma. Since  $M_{11}$  is 4-transitive (and hence 3-transitive) on the 11 points there is an involution  $\pi \in M_{11}$  fixing the 3 points of  $O$  which lie in  $D/\{p\}$ . Let  $O_\pi$  be the fixed point set of  $\pi$ . The set  $O + O_\pi$  is a C-set. It is also strictly contained in  $\Omega/D$ . This means that  $O + O_\pi$  is the empty set and hence  $O = O_\pi$  completing the proof of lemma. □

We now look at a particular copy of  $M_{11}$ . Here we use the notation of [9, chapter 12]. We take our copy of  $M_{11}$  to be the stabiliser of the following dodecad:

×	×	×
	×	×
×	×	×
×	×	×

and the point 0, corresponding to the point in the top left of the array. Consider the following element, well known to be in  $M_{24}$ :



It clearly fixes the point 0 and stabilises the above dodecad so is in our copy of  $M_{11}$ . In view of lemma 1, to prove the theorem we need to exhibit 3 octads all containing 0, all meeting the dodecad in 4 points and such that all 24 points lie either in one of our octads or in the fixed point set of the element of order 3 above. The following three octads will suffice:

## Improved bounds for the spread of sporadic groups



□

### 3. Computational methods

We use MAGMA [4] Version 2.18 to obtain upper bounds for the spread of 14 of the sporadic groups. This section describes the methods used and the programs themselves are in the appendix.

#### 3.1. Using coverings

This section uses the concept of a covering. A set  $S$  of proper subgroups of a group  $G$  is a *covering* of  $G$  if  $G = \bigcup_{s \in S} s$ . A minimal covering is a covering of minimal size. The size of a minimal covering is denoted by  $\sigma(G)$ . We use small and minimal coverings in this section. Minimal coverings of the sporadic groups are studied in [13] and [14].

Table 2 gives  $\sigma(G)$  for the sporadic groups studied in this paper. These are all the sporadic groups that have an upper bound for  $\sigma(G)$  of less than a million. We provide a single figure when  $\sigma(G)$  is known. Otherwise an interval containing  $\sigma(G)$  is given.

$G$	$\sigma(G)$
M <sub>11</sub>	23
M <sub>12</sub>	[12, 210]
M <sub>22</sub>	771
M <sub>23</sub>	41709
M <sub>24</sub>	3336
J <sub>1</sub>	[5165, 5415]
J <sub>2</sub>	[907, 1154]
J <sub>3</sub>	[23648, 44100]
Fi <sub>22</sub>	221521
Co <sub>3</sub>	[505288, 832835]
Suz	[338625, 540333]
McL	[24541, 24553]
He	464373
HS	1376

Table 2

We use the following lemma:

**LEMMA 2:** Let  $S$  be a covering of  $G$  and  $X$  a set of elements of  $G$  such that  $X \cap s$  is non-empty for each  $s \in S$ . Then  $|X| - 1$  is an upper bound for the spread of  $G$ .

*Proof.* Suppose that an element  $g \in G$  exists with  $\langle x, g \rangle = G$  for all  $x \in X$ . By the definition of a covering,  $g$  is contained in some member of  $S$ , say  $s$ . The lemma

states that  $s \cap X$  is non-empty and so contains some element  $x$ . So  $\langle g, x \rangle \leq s < G$ . □

We consider groups with different types of minimal coverings. Each type of covering requires a different approach, and so do different sizes of group. These approaches are described below.

### 3.2. *The easy case*

The simplest case is when  $G$  is fairly small (in this case  $|G| \leq |M_{24}|$ ), has a minimal covering that is the union of conjugacy classes of low-index maximal subgroups of  $G$ , and MAGMA [4] stores a list of its maximal subgroups. In this case we use the function `DoFullClassGroupStrong`. The groups successfully treated in this way are  $M_{11}$ ,  $M_{22}$ ,  $M_{24}$  and HS.

We note that this method gives  $s(M_{11}) \leq 3$ , which Section 2 shows is the actual value of  $s(M_{11})$ . This demonstrates the effectiveness of the program in at least that case.

We use  $M_{22}$  to illustrate the method. By [13] it has a minimal covering consisting of all maximal subgroups isomorphic to  $M_{21}$ ,  $L_2(11)$  or  $2^4:A_6$ . This covering has size 771.

The first task is to compute the permutation representation of  $G$  on the 771 cosets of subgroups in the covering. This is done by the function `MakeGroup`, which also returns the images in this representation of a representative of each conjugacy class of elements.

Next the function `MakeElts` computes a set  $F$  consisting of all non-trivial maximal fixed-point sets in this representation. By this we mean all maximal subsets of points  $s$  such that there exists a non-trivial element of  $G$  that fixes  $s$  pointwise, and  $s$  is not the full set. This is all we need by Lemma 2.

Finally, `StrongSearch` searches for a small set  $X \subset F$ , where  $\bigcup_{x \in X} x$  is the whole set of points. With each pass through the loop, it collects from  $F$  all optimal candidates for the next member of  $X$  and adjoins a random one of these to  $X$ .

### 3.3. *Variations on the theme*

When the group is larger then there are likely to be a large number of maximal fixed-point sets. In this case, we cannot store them all, so we use one of the functions `DoXXXClassGroupFast`. These two functions call `FastSearch` instead of `StrongSearch`. This function does not search the whole of  $F$  for optimal candidates each time. Instead, it takes a small sample  $F'$  from  $F$ , and then adjoins an optimal choice from  $F'$  to  $X$ .

Additional savings in space and time are given by not explicitly computing the whole of  $F$ . The function `MakeEltsWeak` computes at least one maximal fixed-point set from each  $G$ -orbit, and possibly some which are not maximal. The responsibility for making other members of the  $G$ -orbits is passed to `FastSearch`, which only makes those that it needs for creating the sets  $F'$ .

We use `DoFullClassGroupFast` for the groups  $M_{23}$  and  $J_3$ .

Sometimes  $G$  has a minimal covering  $C$  that is not a union of conjugacy classes of maximal subgroups. This case is dealt with using the functions `DoPartialClassGroupXXX`. This begins by assuming that the covering is in fact  $\bar{C}$ , the smallest covering that contains  $C$  as a subset but is closed under conjugacy

in  $G$ . It then calls `MakeNeeds` to create a subset  $P$  of the points, where the set of the point stabilisers in  $P$  is a covering of  $G$ . It passes this set to one of the two `Search` functions, where it is used instead of the full point set. All members of  $F$  are replaced by their intersections with  $P$ .

The groups that needed `DoPartialClassGroupStrong` were  $M_{12}$ ,  $J_1$  and  $J_2$ . For `MCL`, we used `DoPartialClassGroupFast`.

When a minimal covering  $C$  for  $G$  is too large for the above methods then we can use the orbits of a subgroup. (At the time of writing, ‘too large’ means ‘over 100,000 subgroups’). We look at the orbits of subgroups in their action on  $P$ . We choose a subgroup  $K$  that has  $n$  orbits on  $P$  for some  $n < 100,000$  and where most of these orbits are regular. The functions `XXXWithOrbits` use the above methods to find  $P' \subset P$  such that  $P'$  intersects every  $K$ -orbit non-trivially and  $P' = \bigcup X$  for a small set  $X \subset F$ . Then it is clear that  $P = \bigcup_{x \in X} x^K$ , so  $|K| \cdot |X| - 1$  is an upper bound for the spread of  $G$ .

The function `DoFullClassGroupWithOrbits` dealt with the groups  $Fi_{22}$ ,  $Co_3$ ,  $Suz$  and  $He$ . The subgroup  $K$  is a cyclic group of order 11, 23, 11 and 17 respectively.

### 3.4. *Obtaining the larger groups*

If the reader wishes to verify our calculations, then it is important that they use identical input. Not all the permutation groups that we use are available with their maximal subgroups in `MAGMA`, so this section gives the necessary details for the reader to recreate these representations. The groups concerned are  $Fi_{22}$  and  $Suz$ .

All representations are taken from the Web Atlas [18]. The input to `MAGMA` was an eight generator group for  $Suz$  and a ten generator group for  $Fi_{22}$ . In both cases, the first two generators were the group generators in the smallest permutation representation as given in the Web Atlas. The other generators come in pairs, and each pair generates a maximal subgroup. These were obtained by using the words for maximal subgroups given in the Web Atlas.

The extra generators for  $Suz$  generate  $2^{1+6} \cdot U_4(2)$ ,  $U_5(2)$  and  $J_2:2$ , in that order. The subgroups of  $Fi_{22}$  given by the extra generators are  $U_6(2)$ ,  $O_7(3)$ ,  $O_8^+(2) \cdot S_3$  and  $2^{10} : M_{22}$ .

## 4. *Conclusions*

We have given a hand proof that  $s(M_{11}) = 3$ . Computational methods have given us good upper bounds for  $s(G)$  for 13 of the other sporadic groups.

This deals with all sporadic groups known to have a covering of size less than a million. The two groups that seem most open to attack next are  $Co_2$  and  $Ru$ , as these have minimal coverings of sizes at most 5 and 12 million respectively.

We note that better results were obtained for some of the groups in trial runs, but our table only gives the results that were given by known seeds.

## 5. *Acknowledgements*

The second author is supported by a Royal Society Dorothy Hodgkin fellowship and the EPSRC grant EP/C523229/1 held by members of the CIRCA group in St Andrews. We would like to thank Robert Curtis for a discussion about Section

2. We would also like to thank Jamshid Moori for useful discussions on the subject of the spread of sporadic simple groups.

*References*

1. Binder, The bases of the symmetric group *Izv. Vyss. Ucebn. Zaved. Matematika* 78 (1968), 19–25.
2. Binder, The two element bases of the symmetric group *Izv. Vyss. Ucebn. Zaved. Matematika* 90 (1970), 9–11.
3. Blackburn, S. Sets of permutations that generate the symmetric group pairwise. *J. Comb. Th. - Series A* 113(2006):1132–1138.
4. Bosma, W. and Cannon, J. J. *Handbook of Magma functions*. School of Mathematics and Statistics, University of Sydney, Sydney, 1995.
5. Bradley, J. D. and Moori, J. On the exact spread of sporadic simple groups. *Communications in Algebra*, to appear.
6. Brenner, J. L. and Wiegold, J. Two generator groups, I. *Michigan Math. J.* 22(1975), 53–64.
7. Breuer, T, Guralnick, R. M. and Kantor, W. M. Probabilistic generation of finite simple groups II. Submitted to *J. Alg.*
8. Conway, J. H. , Curtis, R. T. , Norton, S. P. , Parker, R. A. and Wilson, R. A. *An Atlas of Finite Groups*, Clarendon Press, 1985.
9. Conway, J. H. and Sloane, N. A. *Sphere packings lattices and groups*. Springer – Verlag, 1988
10. Ganief, S. and Moori, J. On the spread of sporadic simple groups. *Communications in Algebra* 29(8), (2001) 3239–3255.
11. Guralnick, R. M. and Shalev, A. On the spread of finite simple groups. *Combinatorica* 23(1), (2003) 73–87.
12. Guralnick, R. M. and Kantor, W. M. Probabilistic generation of finite simple groups. *J. Algebra* 234, (2000) 743–792.
13. Holmes, P. E. Subgroup coverings of some sporadic groups, *J. Combin. Theory, Ser. A*, to appear.
14. Holmes, P. E. and Maróti, A. Covering and generating sporadic simple group pairwise. Submitted to *Communications in Algebra*.
15. Kantor, W. M. and Lubotzky, A. The probability of generating a finite classical group. *Geom. Ded.* 36 (1990), 67–87.
16. Mathieu, E. Memoire sur l’etude des fonctions de plusieurs quantites. *J. Math. Pures Appl.* 6 (1861) 241–243.
17. Mathieu, E. Sur les fonctions cinq fois transitives de 24 quantites. *J. Math. Pures Appl.* 18 (1873) 25–46.
18. Wilson, R. A. *et al.* A World-Wide-Web Atlas of group representations. <http://www.mat.bham.ac.uk/atlas>.
19. Woldar, A. The exact spread of the Mathieu group  $M_{11}$ , *J. Group Th.* , to appear.

J. D. Bradley

National University of Rwanda,  
Butare, Rwanda

P. E. Holmes

DPMMS,  
Centre for Mathematical Sciences,  
Cambridge CB3 0BW, UK