ORBIT INVARIANTS AND AN APPLICATION TO THE BABY MONSTER

MAX NEUNHÖFFER, FELIX NOESKE, E.A. O'BRIEN, AND ROBERT A. WILSON

ABSTRACT. We prove that the minimal base size for the permutation action of the sporadic simple Baby monster group B on the cosets of its 7th and 8th maximal subgroup (in decreasing order of size) is 3 and 2 respectively. Motivated by the large sizes of these permutation actions, we develop new computational methods to prove that an orbit is regular and to show that two orbits are disjoint.

1. INTRODUCTION

Let G be a permutation group acting on a set X; we say that $B \subseteq X$ is a *base* for G if the pointwise stabiliser of B in G is trivial. The elements of G are uniquely determined by their action on B. Bases are critical to the computational study of finite permutation groups; see, for example, [HEO05, Chapter 4].

Base sizes for almost simple primitive permutation groups have been much studied in recent years. One motivation is a conjecture of Cameron and Kantor [CK93] bounding the minimal base size in *non-standard actions*. If G is a finite almost simple group with socle G_0 then a primitive G-set X is *standard* if either $G_0 = A_n$ and X is an orbit of subsets or partitions of $\{1, \ldots, n\}$, or G is a classical group in a subspace action (namely, X is an orbit of subspaces of the natural G-module, or pairs of subspaces of complementary dimension). We write $b(G)$ for the minimal size of a base for a permutation group G. Cameron and Kantor conjectured that there is an absolute constant c such that $b(G) \leq c$ for every almost simple group G in a faithful primitive non-standard action. The conjecture was proved by Liebeck and Shalev [LS99] using probabilistic methods based on fixed point ratio estimates. Subsequent work (see [Bur07, BLS09] for example) provides explicit values of c, in particular proving that $b(G) \leq 7$ for every finite almost simple group.

In [BOW10] we used a combination of the probabilistic approach introduced in [LS99] and various computational and character-theoretic techniques to obtain precise base sizes for primitive actions of all almost simple sporadic groups with just two exceptions: the action of the sporadic simple Baby monster group B on its 7th and 8th maximal subgroups (in decreasing order of size). Throughout we use ATLAS notation [CCN$^+$85]. Recall that

$$|B| = 4\,154\,781\,481\,226\,426\,191\,177\,580\,544\,000\,000 \approx 4 \cdot 10^{33}.$$

Date: June 17, 2011.

Key words and phrases. Babymonster, orbit invariants, non-standard action, base size.

We acknowledge the support of the Marsden Fund of New Zealand via grant UOA 1015 and thank Tim Burness for helpful comments.

The 7th maximal subgroup M_7 has structure $2^{2+10+20}.(M_{22} : 2 \times S_3)$ and

$$|M_7| = 22\,858\,846\,741\,463\,040 \approx 22 \cdot 10^{15}.$$

Thus the action of B on the right cosets of M_7 is on $181\,758\,140\,654\,146\,875 \approx 181 \cdot 10^{15}$ points. The 8th maximal subgroup M_8 has structure $[2^{30}].L_5(2)$ and

$$|M_8| = 10\,736\,731\,045\,232\,640 \approx 10 \cdot 10^{15}.$$

Thus the action of B on the right cosets of M_8 is on $386\,968\,944\,618\,506\,250 \approx 386 \cdot 10^{15}$ points.

Our methods in [BOW10] established that in each case $b(G) \leq 3$. We now obtain precise results.

Theorem 1. Let G be the sporadic simple Baby monster group B acting on a faithful primitive G-set with point stabiliser H. If $H = 2^{2+10+20}.(\mathrm{M}_{22} : 2 \times S_3)$, then $b(G) = 3$. If $H = [2^{30}].\mathrm{L}_5(2)$, then $b(G) = 2$.

A critical component in the proof of this theorem is the orbit algorithm using a chain of helper subgroups described by Müller, Neunhöffer and Wilson [MNW07]. We summarise the algorithm in Section 2. However, it alone is insufficient, and some improvements are needed, as described below. One reason is the degree of the permutation representation, now on approximately 10^{17} points rather than the 10^{15} considered in [MNW07]. Another is the unavailability of useful helper subgroups.

We expect that these methods will be useful in other cases where large permutation representations are studied. For example, it is reasonable to expect that one can soon study the permutation representation of the Monster on its approximately 10^{20} transpositions.

2. Enumerating large orbits – a summary

Let G be a group acting from the right on a set X. We denote the action of $g \in G$ on $x \in X$ by $x{\cdot}g$, and $x{\cdot}G$ is the G-orbit in X containing x.

The key idea of [MNW07] is the following: instead of enumerating a G-orbit $x{\cdot}G$ directly, choose a *helper subgroup* $U < G$ and enumerate only the set of U*-suborbits* $\{y{\cdot}U \mid y \in x{\cdot}G\}$.

To achieve a reduction in space, we must store $y{\cdot}U$ more efficiently than simply recording all of its points. Instead, we use an explicitly computable homomorphism of U-sets $\pi : X \to Y$; namely, U acts on Y and $\pi(x{\cdot}u) = \pi(x){\cdot}u$ for all $x \in X$ and all $u \in U$. We enumerate and store all U-orbits in Y completely, choose one point in each U-orbit of Y (under a fixed ordering), and call it U*-minimal*. We extend the concept of U-minimality to X: namely, $z \in X$ is U*-minimal* if $\pi(z)$ is.

We store a U-orbit $z{\cdot}U$ by storing only the set of U-minimal points contained in it, usually a much smaller set than $z{\cdot}U$. Given $w \in z{\cdot}U$, we use our stored information about $\pi(w)$ and $\pi(w){\cdot}U$ to find a U-minimal point in $w{\cdot}U$.

Müller *et al.* [MNW07] develop these ideas to decide quickly whether or not a given $z \in X$ lies in a known U-orbit or is in a new orbit. They use a *chain* of helper subgroups $U_1 < U_2 < \cdots < U_k < G$ to store U_k-suborbits, while ensuring that the memory needed for precomputed data is determined by $|U_1|+[U_2 : U_1]+\cdots+[U_k : U_{k-1}]$ rather than $|U_k|$.

If we can select effective helper subgroups and homomorphisms, then this method to enumerate $x{\cdot}G$ may save about a factor of $|U_k|$ in both memory usage and running time. Choosing such remains an art, since we often face conflicting demands. As one example, if the index of $\mathrm{Stab}_U(x)$ in $\mathrm{Stab}_U(\pi(x))$ is large, then some U-orbits in X may contain many U-minimal points; now the space saving is reduced, since we must store all U-minimal points.

3. Orbit invariants

A crucial step in our proof is to determine, given two points in a G-set, whether they are in the same G-orbit. Depending on the context, G may be either the group or a helper subgroup. Since the enumeration of a G-orbit is hard, we want to avoid enumerating the same orbit twice. Thus, in this section, we develop a criterion to prove that two points in a G-set are not contained in the same G-orbit. The basic problem is: given just one point in an orbit, find an orbit invariant which is not too time-consuming to compute.

Definition 2. Let G be a group acting from the right on a set X. A function $f : X \to Y$ for some set Y is a *G-orbit invariant* if $f(x) = f(x{\cdot}g)$ for all $x \in X$ and all $g \in G$.

Clearly, if $f(x) \neq f(y)$ for $x, y \in X$, then $x{\cdot}G \neq y{\cdot}G$. We omit the routine proofs of the next three propositions.

Proposition 3 (A generic G-orbit invariant)**.** Let G act on a set X and let $m : X \to Y$ be a homomorphism of G-sets. Let n be the number of G-orbits in Y and $\bigcup_{i=1}^{n} O_i$ be the decomposition of Y into its G-orbits. Then

$$f : X \to \{1, 2, \ldots, n\}, x \mapsto i \quad \text{if } m(x) \in O_i$$

is a G-orbit invariant.

Of course, if all G-orbits in Y have length one, then m is a G-orbit invariant.

We now describe more explicitly how to compute such invariants in the context of matrix group actions, where a typical G-set homomorphism is given by a G-linear map onto a quotient G-module. Let $G \leq \mathrm{GL}_d(\mathbb{F}_q)$ where $\mathbb{F}_q$ is a finite field of size q, and let $V := \mathbb{F}_q^{1\times d}$ be the natural (right) module. Let $H < G$ and let W be a submodule of the restricted module $V|_H$.

Proposition 4 (A G-orbit invariant for matrix groups)**.** With the above notation, the natural projection $m : V \to V/W$ is an H-set homomorphism where H acts on V/W by $(v + W){\cdot}h := v{\cdot}h + W$. If $V/W = \bigcup_{i=1}^{n} O_i$ is the decomposition of V/W into its H-orbits, then

$$f : V \to \{1, 2, \ldots, n\}, x \mapsto i \quad \text{if } h(x) \in O_i$$

is an H-orbit invariant.

If the action of H on V/W is trivial (all cosets fixed by all elements of H), then m is an H-orbit invariant. Observe that the action of H on V/W is in fact linear:

$$(\lambda(v+W)+(w+W))\cdot h = \lambda((v+W)\cdot h)+(w+W)\cdot h,$$

for every $v, w \in V$ and $\lambda \in \mathbb{F}_q$. This is important later when we act on subspaces.

Let V be a vector space. We denote by $\mathcal{P}_k(V)$ the set of k-dimensional subspaces of V and by $\mathcal{P}_{\leq k}(V)$ the set of subspaces of V of dimension at most k.

Let $G \leq \mathrm{GL}_d(\mathbb{F}_q)$ and let $Z := G \cap (\mathbb{F}_q \cdot \mathbf{1})$ be the subgroup of G consisting of scalar multiples of the identity. Let $\tilde{G} := G/Z$ so $\tilde{G} \leq \mathrm{PGL}_d(\mathbb{F}_q)$. Let $V := \mathbb{F}_q^{1\times d}$ be the natural (right) module for G, let $H < G$ and let W be a submodule of the restricted module $V|_H$. Now set $\tilde{H} := (HZ)/Z \leq \tilde{G}$.

Proposition 5 (G-orbit invariants for projective groups and actions)**.** The natural projection $m : V \to V/W$ induces maps $m_k : \mathcal{P}_k(V) \to \mathcal{P}_{\leq k}(V/W)$ defined by $m_k(M) := (M+W)/W$ for $M \in \mathcal{P}_k(V)$ and $1 \leq k \leq d$. The maps m_k are both H-set homomorphisms and $\tilde{H}$-set homomorphisms. Thus, if $\mathcal{P}_{\leq k}(V/W) = \bigcup_{i=1}^n O_i$ is the decomposition of $\mathcal{P}_{\leq k}(V/W)$ into its H-orbits, then

$$f_k : \mathcal{P}_k(V) \to \{1,2,\ldots,n\}, M \mapsto i \quad \text{if } m_k(M) \in O_i$$

is both an H-orbit invariant and an $\tilde{H}$-orbit invariant.

Thus far, our invariants are already implicit in [MNW07]. We now introduce a new invariant. In particular, the following proposition yields a method to derive G-orbit invariants from an H-orbit invariant for $H < G$ using a left transversal.

Proposition 6 (Upgrading orbit invariants)**.** Let G act on a set X, let $H < G$ and let $f : X \to Y$ be an H-orbit invariant. Let $k := [G : H]$ be finite and let $t_1, t_2, \ldots, t_k$ be a left transversal of H in G; namely, $G = \bigcup_{i=1}^k t_i H$ is a disjoint union. Then $\tilde{f} : X \to \mathcal{P}(Y)$ (where $\mathcal{P}(Y)$ denotes the set of subsets of Y) with

$$\tilde{f}(x) := \{f(x\cdot t_i) \mid 1 \leq i \leq k\}$$

is a G-orbit invariant.

Proof. If $g \in G$, then $x\cdot G = (x\cdot g)\cdot G$. Since f is an H-orbit invariant, it is constant on H-orbits and thus

$$\begin{aligned} \tilde{f}(x) &= \{f(x\cdot t_i) \mid 1 \leq i \leq k\} = f(x\cdot G) = f((x\cdot g)\cdot G) \\ &= \{f(x\cdot(gt_i)) \mid 1 \leq i \leq k\} = \tilde{f}(x\cdot g). \quad \square \end{aligned}$$

Remark 7. In Proposition 6 we can replace the set

$$\{f(x\cdot t_i) \mid 1 \leq i \leq k\}$$

by the multiset of the values $f(x\cdot t_i)$ for $1 \leq i \leq k$ to get a (slightly) finer invariant (namely, we count the multiplicities of the values). We cannot use the k-tuple $(f(x\cdot t_i))_{1\leq i\leq k}$ of values since this in general differs for two points x and $x\cdot g$.

We now apply these orbit invariants to obtain a method to deduce that a G-orbit is regular. The fundamental idea is to choose a suitable helper subgroup H, and show that H has (at least) $[G : H]$ orbits, at least one of which is regular. The orbit invariant is used to show that the H-orbits are distinct.

Proposition 8 (Using an orbit invariant to prove regularity)**.** Let a group G act on a set X and let $x \in X$. Let $H < G$ be such that $|x{\cdot}H| = |H|$. Let $k := [G : H]$ be finite and let $s_1, s_2, \dots, s_k$ be a left transversal of H in G with $s_1 = 1$ and let $f : X \to Y$ be an H-orbit invariant. If $f(x) \neq f(x{\cdot}s_i)$ for all $2 \leq i \leq k$, then $x{\cdot}G$ is regular.

Proof. Let $S := \mathrm{Stab}_G(x)$. By assumption $S \cap H = \{1\}$. If $1 \neq g \in S$ then $g = s_i h$ for some $i > 1$ and some $h \in H$. Thus $x = x{\cdot}g = x{\cdot}(s_i h)$ and so $x{\cdot}H = (x{\cdot}s_i){\cdot}H$. Since f is an H-orbit invariant, $f(x) = f(x{\cdot}s_i)$. □

Hence to prove $x{\cdot}G$ regular, we verify that $x{\cdot}H$ is regular and then compare all values $f(x{\cdot}s_i)$ to $f(x)$. In practice, we use two particular orbit invariants. One is the trivial H-orbit invariant consisting of the H-orbit itself: this is used when the orbit has been explicitly enumerated. The other is the helper subgroup invariant described in Proposition 6.

4. B ACTING ON THE COSETS OF ITS 7TH MAXIMAL SUBGROUP

This was the more difficult of the two cases, requiring the full power of our new techniques. We want to find the smallest base size for the action of B on the right cosets of M_7. We prove that this B-orbit does not contain a regular M_7-suborbit but one with point stabiliser of order 2. Thus the smallest base size is 3.

The smallest non-trivial simple module V of B has dimension 4370 over $\mathbb{F}_2$. Representing matrices for *standard generators* [Wil96] of B can be downloaded from [Wil99], as can words in these standard generators to construct generators for M_7. The action of B on the cosets of M_7 can be constructed as follows. The restriction of V to M_7 is reducible and the socle $\langle v \rangle$ is 1-dimensional. Since M_7 is maximal in B, the B-orbit $v{\cdot}B$ (acting on vectors of V) has point stabiliser M_7, and thus implements the action of B on the cosets of M_7.

To prove that the B-orbit with approximately $181 \cdot 10^{15}$ points does not contain a regular M_7-suborbit, we compute the lengths of enough shorter M_7-suborbits in $v{\cdot}B$ to exclude a regular M_7-suborbit. Since M_7 has approximately $22 \cdot 10^{15}$ elements, we must show that approximately $159 \cdot 10^{15}$ points of $v{\cdot}B$ lie in shorter orbits.

We first deduce that $v{\cdot}B$ contains 432 M_7-suborbits by considering the ordinary character tables of B and M_7, both available in the Character Table Library of GAP [GAP08]. The number of M_7-suborbits is the scalar product of the permutation character $1_{M_7}^B$ with itself. Of course, these orbits may (and do) vary significantly in size.

We use random sampling to find different M_7-suborbits in $v{\cdot}B$. We first create 2000 random points in $v{\cdot}B$, by using the product replacement algorithm [CLGM+95] to generate random $g \in B$ and then computing $v{\cdot}g$. (We use 300 product replacement steps for each random element to obtain sufficiently uniformly distributed random points; experiments with just 100 steps displayed too much statistical bias to be useful.) If these 2000 *seed vectors* are distributed in the M_7-suborbits of $v{\cdot}B$ according to their orbit lengths, then we expect to find, with high probability, large suborbits among them.

In the interests of efficiency, we do most of the computations not in the 4370-dimensional M_7-module, but in a smaller quotient module Q. This results in some loss of information, and we must choose Q to minimise this loss. We observe, using the MEATAXE (see [HEO05, Chapter 7] for example) that $V|_{M_7}$ is a reducible module which has a 356-dimensional quotient $Q := V/W$ and the linear action of M_7 on the quotient is faithful. As in Proposition 4, the canonical map m is an M_7-set homomorphism. Under this map, the image of an orbit is an orbit and it follows that the size of the original orbit is a multiple of the size of the image orbit, since the point stabiliser of $v \in V$ is a subgroup of the point stabiliser of $m(v) \in Q$. That is, we can enumerate M_7-suborbits on vectors of length 356 and first determine their lengths and point stabilisers. Expressing generators of the point stabilisers as straight-line programs [HEO05, p. 64] in the generators allows us to compute the point stabilisers in their 4370-dimensional representation. Since the point stabilisers are small, we can then easily determine the exact stabiliser on the vectors of length 4370. In most cases the stabilisers in M_7 of v and $m(v)$ coincide.

We first use a helper subgroup orbit-invariant to try to distinguish the M_7-suborbits of our 2000 seed vectors. We choose a subgroup $A < M_7$ of index 6144 such that $Q|_A$ has a 24-dimensional quotient R. Enumerating all A-orbits in R provides us with an A-orbit invariant f using Proposition 4. Using a left transversal of A in M_7 upgrades this to an M_7-suborbit invariant $\tilde{f}$, which takes 39 different values on the 2000 seed vectors in $v{\cdot}B$. Two vectors taking different values are guaranteed to lie in different M_7-suborbits.

For the rest of the computation we employ the methods of [MNW07]. As a requisite, we must carefully choose and construct a suitable chain of helper subgroups. Here, we use 3 helper subgroups $U < H < K < M_7$ with structures $U = M_{22}$, $H = 2^{10}.M_{22}$ and $K = 2^{1+20}.M_{22}$ of orders $443\,520$ and $454\,164\,480$ and $930\,128\,855\,040$ respectively. If two or more M_7-suborbits have the same invariant, then we enumerate them by using K-suborbits.

In practice, we enumerate only 51% of each orbit and also compute the point stabiliser of the seed vector. This saves about half the memory for each orbit and much time: near the end of an orbit enumeration much time is spent producing known points. Since we know $|M_7|$, it suffices to enumerate just over half of an M_7-suborbit O to determine its length.

Once we learn the length of an orbit O, we can determine which other seed vectors lie in O by acting on a seed vector with 40 random elements of M_7. If a seed vector lies in O, then with very high probability at least one of the 40 images will lie in the half of the orbit we have enumerated. To *prove* disjointness of two M_7-suborbits O_1 and O_2 of the same size and the same invariant, we look up all stored K-suborbit representatives of O_2 in the list of stored K-minimal points for O_1. Since we have enumerated more than half of each orbit, if O_1 is equal to O_2, then at least one K-suborbit must be contained in both enumerated halves.

We make one additional modification to the methods of [MNW07]: we use a randomised approach to compute elements of the stabiliser, since using Schreier generators is too costly. During the orbit enumeration, we produce random elements of M_7 and act with them on the seed vector. When we hit a known K-suborbit, we can construct a random element of the stabiliser, and usually generate it with a few such elements. As we enumerate more of the orbit, the probability of a hit increases and so the stabiliser is computed rapidly.

The entire computation was lengthy. For some M_7-suborbits the methods from [MNW07] do not work with our set of helper subgroups. The most difficult was orbit invariant number 25, where we eventually found 14 M_7-suborbits using a GAP session with 207 GB of main memory and $6\,071$ minutes of CPU time. We abandoned at least one other M_7-suborbit with the same invariant to avoid running out of memory. The calculations were run on a machine with an 8 core Intel Xeon CPU E7520 running at 1.87 GHz and 256 GB of main memory.

Table 1 contains information about the M_7-suborbits we found. Each row describes one suborbit: the first entry is the value of the orbit invariant (simply numbered 1 to 39), the second is the length of the orbit, the third is the order of the point stabiliser in the 4370-dimensional representation, the fourth is the order of the point stabiliser in the 356-dimensional representation, and the fifth is the number of seed vectors which lie in the suborbit. We could only enumerate M_7-suborbits for 35 of the 39 orbit invariant values.

In total these 113 suborbits account for $174\,882\,083\,221\,536\,768$ points, so the rest of $v{\cdot}B$ cannot contain a regular M_7-suborbit. Since two of the M_7-suborbits have stabiliser order 2, the minimal base size is 3.

Inv	Length	$\mathrm{Stab}(4370)$	$\mathrm{Stab}(356)$	Samples
1	1 904 903 895 121 920	12	12	22
1	5 714 711 685 365 760	4	4	69
1	5 714 711 685 365 760	4	4	64
1	1 142 942 337 073 152	20	20	11
1	5 714 711 685 365 760	4	4	73
1	2 857 355 842 682 880	8	8	34
1	1 904 903 895 121 920	12	12	21
1	79 370 995 630 080	288	288	1
2	5 714 711 685 365 760	4	4	54
2	714 338 960 670 720	32	32	10
2	1 428 677 921 341 440	16	16	17
2	952 451 947 560 960	24	24	7
2	1 428 677 921 341 440	16	16	16
2	1 428 677 921 341 440	16	16	16
2	1 428 677 921 341 440	16	16	18
2	1 428 677 921 341 440	16	16	17

2	1 428 677 921 341 440	16	16	14
2	178 584 740 167 680	128	128	2
2	158 741 991 260 160	144	144	1
3	11 429 423 370 731 520	2	2	131
3	5 714 711 685 365 760	4	4	51
3	1 904 903 895 121 920	12	12	25
3	5 714 711 685 365 760	4	4	56
3	5 714 711 685 365 760	4	4	64
3	1 904 903 895 121 920	12	12	27
4	1 428 677 921 341 440	16	16	12
4	5 714 711 685 365 760	4	4	70
4	1 428 677 921 341 440	16	16	18
4	714 338 960 670 720	32	32	10
4	714 338 960 670 720	32	32	5
5	1 428 677 921 341 440	16	32	20
5	357 169 480 335 360	64	128	3
6	5 714 711 685 365 760	4	4	64
6	11 429 423 370 731 520	2	2	135
7	1 428 677 921 341 440	16	32	11
7	357 169 480 335 360	64	256	7
7	714 338 960 670 720	32	64	6
8	952 451 947 560 960	24	48	6
9	952 451 947 560 960	24	24	8
9	952 451 947 560 960	24	24	12
9	3 809 807 790 243 840	6	6	33
9	1 428 677 921 341 440	16	16	13
9	714 338 960 670 720	32	32	14
9	714 338 960 670 720	32	32	7
9	476 225 973 780 480	48	48	9
9	952 451 947 560 960	24	24	8
9	476 225 973 780 480	48	48	3
9	714 338 960 670 720	32	32	2
9	190 490 389 512 192	120	120	1
10	5 714 711 685 365 760	4	4	73
10	2 857 355 842 682 880	8	8	29
10	476 225 973 780 480	48	48	4
11	5 714 711 685 365 760	4	4	67
12	357 169 480 335 360	64	128	5
12	119 056 493 445 120	192	384	2
12	357 169 480 335 360	64	128	3
12	952 451 947 560 960	24	48	11
12	1 428 677 921 341 440	16	32	13
12	1 428 677 921 341 440	16	32	15
12	1 428 677 921 341 440	16	32	17

12	357 169 480 335 360	64	128	2
12	119 056 493 445 120	192	1536	2
12	714 338 960 670 720	32	64	5
12	714 338 960 670 720	32	64	8
12	357 169 480 335 360	64	128	3
12	1 428 677 921 341 440	16	32	16
12	357 169 480 335 360	64	512	7
13	1 904 903 895 121 920	12	12	31
14	1 428 677 921 341 440	16	32	21
15	952 451 947 560 960	24	48	11
15	1 428 677 921 341 440	16	32	14
15	1 428 677 921 341 440	16	32	14
15	95 245 194 756 096	240	480	2
16	1 428 677 921 341 440	16	16	15
16	1 428 677 921 341 440	16	16	16
16	476 225 973 780 480	48	48	5
17	1 428 677 921 341 440	16	16	16
17	714 338 960 670 720	32	32	9
18	2 857 355 842 682 880	8	8	27
19	1 428 677 921 341 440	16	16	16
19	714 338 960 670 720	32	32	9
19	476 225 973 780 480	48	48	3
20	1 428 677 921 341 440	16	16	15
21	357 169 480 335 360	64	64	2
21	178 584 740 167 680	128	128	1
22	714 338 960 670 720	32	32	8
22	29 764 123 361 280	768	1536	2
22	89 292 370 083 840	256	512	2
22	357 169 480 335 360	64	128	5
22	357 169 480 335 360	64	64	2
22	714 338 960 670 720	32	32	7
22	178 584 740 167 680	128	256	3
22	178 584 740 167 680	128	256	1
23	476 225 973 780 480	48	48	5
23	357 169 480 335 360	64	64	5
23	476 225 973 780 480	48	48	9
24	476 225 973 780 480	48	48	6
25	357 169 480 335 360	64	64	2
25	1 904 903 895 121 920	12	12	21
26	357 169 480 335 360	64	128	8
27	357 169 480 335 360	64	128	6
27	238 112 986 890 240	96	384	2
27	119 056 493 445 120	192	384	2
27	357 169 480 335 360	64	128	1

27	178 584 740 167 680	128	256	1
28	357 169 480 335 360	64	128	3
29	714 338 960 670 720	32	32	6
30	357 169 480 335 360	64	128	5
31	1 428 677 921 341 440	16	16	16
32	357 169 480 335 360	64	64	1
33	119 056 493 445 120	192	192	1
34	476 225 973 780 480	48	48	7
35	285 735 584 268 288	80	160	2

Table 1: Known orbit information for the action of B on M_7

5. B ACTING ON THE COSETS OF ITS 8TH MAXIMAL SUBGROUP

We want to find the smallest base size for the action of B on the right cosets of M_8. We prove that this B-orbit contains a regular M_8-suborbit and thus the smallest base size is 2. This is easier than the M_7 case, since we only need to enumerate one M_8-suborbit. We prove this orbit is regular using our new orbit invariant and Proposition 8.

As before, representing matrices for standard generators of B can be downloaded from [Wil99], as can words in these standard generators to construct generators for M_8. The action of B on the cosets of M_8 can be constructed as follows. The restriction of V to M_8 is reducible and the socle S is 10-dimensional. Since M_8 is maximal in B, the B-orbit $S{\cdot}B$ (acting on 10-dimensional subspaces of V) has point stabiliser M_8, and thus implements the action of B on the cosets of M_8.

Recall that $M \in \mathbb{F}^{k\times d}$ is in *full echelon form* if there are indices $1 \leq i_1 < i_2 < \cdots < i_k \leq d$ such that $M_{l,i_j} = \delta_{l,j}$ for $1 \leq j \leq k$ and $1 \leq l \leq k$ and $M_{j,l} = 0$ for $1 \leq j \leq k$ and $l < i_j$. We store a 10-dimensional subspace U as a (10×4370)-matrix M in full echelon form, so the 10 rows form a uniquely determined basis for U. The action of $g \in B$ on U is determined by first calculating the matrix product Mg and then computing its full echelon form.

To find a point in a regular M_8-suborbit, we use random methods. If the B-orbit contains a regular M_8-suborbit, then of course the latter contains $|M_8|$ of the $[B : M_8]$ points. Hence, if we choose a (nearly) uniformly distributed random point in $S{\cdot}B$, the probability is about $10/387$ to hit any particular regular M_8-suborbit. Our methods described below prove that we found it, or fail if the point lies in a shorter M_8-suborbit. In fact, it is likely that there are several regular orbits, so that the probability of success will be much greater than this. We produce a random point in $S{\cdot}B$ by constructing the image of a point under a random element of B. Again, we use the product replacement algorithm to construct random elements.

We need one more improvement since (10×4370)-matrices still need too much memory and too much time to act on. We observe, using the MEATAXE, that $V|_{M_8}$ is a reducible module which has a 215-dimensional quotient $Q := V/W$. As in Proposition 5, M_8 acts on Q and the canonical map m induces a map $m_{10} : \mathcal{P}_{10}(V) \to \mathcal{P}_{\leq 10}(Q)$ which is an M_8-set homomorphism. Under this map, the image of an orbit is an orbit; if the image orbit is M_8-regular, then the original orbit is also M_8-regular.

It remains to prove for some 10-dimensional subspace x of Q that $x{\cdot}M_8$ is regular. To achieve this, we use the techniques from Section 3, especially Proposition 8. Our choice of helper subgroups is somewhat restricted by the structure of M_8. The largest helper subgroup in the chain needs to map to a large proper subgroup of the quotient $\mathrm{L}_5(2)$. We choose $2^4.A_8$ as the proper subgroup of this quotient, and a suitable subgroup H of index $2^6 \cdot 31 = 1984$ in M_8. We then choose a *normal* subgroup U of H as the next helper subgroup, in order to compute U-orbit invariants easily. In more detail, we choose our chain of helper subgroups $1 < U \triangleleft H < M_8$ such that:

- U has order 16 777 216 and structure 2^{5+19}. Since $|U|$ is small, we can compute $x{\cdot}U$ using a standard orbit algorithm [HEO05, Chapter 4] and so establish that $x{\cdot}U$ is regular.
- $Q|_U$ has a 19-dimensional quotient on which U acts trivially. Thus we can explicitly compute all the H-orbits on the 2^{19} vectors of this quotient space.
- The structure of H is $[2^{28}].A_8$, so $[H : U] = 322\,560$ and we can compute a left transversal $(s_i)_{1 \le i \le 322560}$ of U in H. Thus we obtain a U-orbit invariant f using Proposition 5.
- $[M_8 : H] = 1\,984$ and we can compute a left transversal $(t_i)_{1 \le i \le 1984}$ of H in M_8. This allows us to use Proposition 6 to upgrade f to an H-orbit invariant $\tilde{f}$. Indeed, we apply Remark 7, using multisets to get a finer invariant.

Now we apply Proposition 8 (with the trivial U-orbit invariant) to prove that $x{\cdot}H$ is regular. Finally, the left transversal $(t_i)_{1 \le i \le 1984}$ together with the H-orbit invariant $\tilde{f}$ allows us to use Proposition 8 again to prove that $x{\cdot}G$ is regular. We compute orbit invariants using multisets. As soon as we find a value $f(x{\cdot}(t_i s_j))$ which does not occur in the multiset $\tilde{f}(x)$, we deduce that $\tilde{f}(x{\cdot}t_i) \neq \tilde{f}(x)$.

Both computation time and memory usage is dominated by the enumeration of the regular U-orbit of length 2^{24}. Since the points are 10-dimensional subspaces of a 215-dimensional space, each point needs about 760 bytes; the total memory requirement for the orbit $x{\cdot}U$ is about 15.2 GB. This enumeration took about 1122 minutes using GAP on a machine with a 16 core Intel Xeon CPU E7330 running at 2.40 GHz and 128 GB of main memory. The rest of the computation took only 71 seconds.

REFERENCES

[BLS09] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev. Base sizes for simple groups and a conjecture of Cameron. *Proc. Lond. Math. Soc. (3)*, 98(1):116–162, 2009.

[BOW10] Timothy C. Burness, E.A. O'Brien, and Robert A. Wilson. Base sizes for sporadic simple groups. *Israel J. Math.*, 177:307–334, 2010.

[Bur07] Timothy C. Burness. On base sizes for actions of finite classical groups. *J. Lond. Math. Soc. (2)*, 75(3):545–562, 2007.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, 1985.

[CK93] P.J. Cameron and W.M. Kantor. Random permutations: some group-theoretic aspects. *Combin. Probab. Comput.*, 2:257–262, 1993.

[CLGM+95] Frank Celler, Charles R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer, and E.A. O'Brien. Generating random elements of a finite group. *Comm. Algebra*, 23:4931–4948, 1995.

[GAP08] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[LS99] M.W. Liebeck and A. Shalev. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.*, 12:497–520, 1999.

[MNW07] Jürgen Müller, Max Neunhöffer, and Robert A. Wilson. Enumerating big orbits and an application: B acting on the cosets of Fi_{23}. *J. Algebra*, 314(1):75–96, 2007.

[Wil96] Robert A. Wilson. Standard generators for sporadic simple groups. *J. Algebra*, 184(2):505–515, 1996.

[Wil99] Robert Wilson et al. The WWW Atlas of Finite Group Representations, 1999. (http://brauer.maths.qmul.ac.uk/Atlas/).

E-mail address: neunhoef@mcs.st-and.ac.uk

SCHOOL OF MATHEMATICS AND STATISTICS, MATHEMATICAL INSTITUTE, UNIVERSITY OF ST ANDREWS, NORTH HAUGH, ST ANDREWS, FIFE, KY16 9SS, SCOTLAND, UNITED KINGDOM

E-mail address: felix.noeske@math.rwth-aachen.de

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN UNIVERSITY, 52056 AACHEN, GERMANY

E-mail address: e.obrien@auckland.ac.nz

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF AUCKLAND, PRIVATE BAG 92019, AUCKLAND, NEW ZEALAND

E-mail address: r.a.wilson@qmul.ac.uk

SCHOOL OF MATHEMATICAL SCIENCES, QUEEN MARY, UNIVERSITY OF LONDON, MILE END ROAD, LONDON E1 4NS, UNITED KINGDOM