

# FINITE PRIMITIVE PERMUTATION GROUPS CONTAINING A PERMUTATION HAVING AT MOST FOUR CYCLES

SIMON GUEST, JOY MORRIS, CHERYL E. PRAEGER, AND PABLO SPIGA

ABSTRACT. We classify the finite primitive groups containing a permutation with at most four cycles (including fixed points) in its disjoint cycle representation.

## 1. INTRODUCTION

In this paper, we are interested in primitive permutation groups containing a permutation that has a small number of cycle (including fixed points) in its disjoint cycle representation. Primitive permutation groups containing elements with few cycles have been studied for over a century, because of their importance in various areas of mathematics. In particular, interest in primitive groups on  $n$  points containing an  $n$ -cycle dates back to a 1911 theorem by Burnside [5, 1 §251–252], and a complete classification of such groups, based on the Finite Simple Group Classification, was achieved in 1997 [7, 13, 15]. This classification has important consequences, including the investigation of cyclic codes, cyclic designs, Cayley graphs on cyclic groups, and rotary embeddings of graphs in surfaces. Motivated by certain number-theoretic applications which we mention briefly in Section 1.2, Müller [16] classified primitive groups containing permutations with two cycles.

The aim of this paper is to classify the primitive groups containing a permutation with at most four cycles in its disjoint cycle representation, including fixed points. Our classification will be applied to a problem about normal coverings of symmetric and alternating groups, and we give some details about this application in Section 1.2.

Such primitive groups turn out to be quite rare, and we are able to classify them according to the permutation actions of their socles. We are further able to list the possible  $N$ -tuples of cycle lengths that can appear in a group with each possible socle, where  $N \leq 4$ . Some of the techniques used are similar to those used by Müller in [16].

**1.1. Main theorem and proof strategy.** Our main result is the following.

**Theorem 1.1.** *Let  $G$  be a finite primitive permutation group of degree  $n$ , and let  $g$  be an element of  $G$  having cycle lengths (counted with multiplicity)  $(n_1, \dots, n_N)$  with  $N \leq 4$ . Then the socle  $\text{soc}(G) = T^\ell$  for some simple group  $T$  and integer  $\ell$ , and one of the following holds:*

- (i)  $\text{soc}(G) = \text{Alt}(m)^\ell$  in its natural product action of degree  $m^\ell$ , with  $\ell \leq 3$ ;
- (ii)  $\text{soc}(G) = \text{PSL}_d(q)^\ell$  in its natural product action of degree  $((q^d - 1)/(q - 1))^\ell$ , with  $\ell \leq 3$  and  $d \geq 2$ ;
- (iii)  $T$ ,  $\ell$ ,  $n$  and  $(n_1, \dots, n_N)$  are in one of the rows of Tables 3, 4 or 5;
- (iv)  $\text{soc}(G)$  is elementary abelian, and  $g$  and  $G$  are described in Theorems 1.3 and 1.4 of [12].

---

2010 *Mathematics Subject Classification.* 20B15, 20H30.

*Key words and phrases.* primitive permutation groups; conjugacy classes; cycle structure.

Address correspondence to S. Guest, Email: s.d.guest@soton.ac.uk; Phone: +44 2381 786 896

The second author is supported in part by the National Science and Engineering Research Council of Canada. The third author is supported by the ARC Federation Fellowship Project FF0776186. The fourth author is supported by UWA as part of the ARC Federation Fellowship Project.

Moreover, Tables 1 and 2 list all of the possible  $N$ -tuples  $(n_1, \dots, n_N)$  arising from parts (i) and (ii) respectively.

The cycle lengths listed in Tables 1 and 2 do occur in at least one group that has the given socle, but may not appear in every such group. For example, in  $\text{Alt}(m)$  the possible cycle lengths depend upon the parity of  $m$ , but  $\text{Alt}(m)$  is the socle of  $\text{Sym}(m)$  and in  $\text{Sym}(m)$  any cycle lengths are possible, so this is what we have listed.

It is an elementary exercise to show that for a permutation group element  $g$ , the order of  $g$  is the least common multiple of the lengths of the cycles into which it can be decomposed. If  $g$  has at most four cycles and lies inside a permutation group of degree  $n$ , the pigeon-hole principle guarantees that one of those cycles must have length at least  $n/4$ ; so clearly  $|g| \geq \lceil n/4 \rceil$ . It is therefore natural that our proof of Theorem 1.1 uses the recent classification of the finite primitive groups  $G$  of degree  $n$  containing a permutation  $g$  with the order  $|g|$  of  $g$  at least  $n/4$ , see [11, Theorem 1.3]. In particular, in order to prove Theorem 1.1 it suffices to investigate which groups in [11, Theorem 1.3] actually contain a permutation with at most four cycles. Comparing Theorem 1.1 with [11, Theorem 1.3] we see that the number of examples is actually very limited. For the benefit of the reader we record the statement of [11, Theorem 1.3].

**Theorem.** (Theorem 1.3 [11]) *Let  $G$  be a finite primitive group of degree  $n$  and assume that  $G$  contains a permutation  $g$  with  $|g| \geq n/4$ . Then the socle  $\text{soc}(G) = T^\ell$  of  $G$  is isomorphic to either*

- (i)  $\text{Alt}(m)^\ell$  in its natural product action on  $\ell$  direct copies of the  $k$ -subsets of  $\{1, \dots, m\}$ , or to
- (ii)  $\text{PSL}_d(q)^\ell$  in its natural action on  $\ell$  direct copies of the points or hyperplanes of the projective space  $\text{PG}_{d-1}(q)$ , or to
- (iii) an elementary abelian group  $C_p^\ell$ , and  $G$  and  $g$  are described in [12], or to
- (iv) one of the groups in [11, Table 2].

Moreover, there exists a positive integer  $\ell_T$  depending only on  $T$  with  $\ell \leq \ell_T$ .

For each group  $G$  in [11, Table 2], the exact value of  $\ell_T$  is given in [11, Table 6]. In particular, for each of the groups arising from [11, Theorem 1.3 (iv)], the proof of Theorem 1.1 follows with an immediate computation in `magma` [2]: for each such group we have given in Tables 3, 4 and 5 all the examples admitting a permutation with at most four cycles. Therefore, for the rest of this paper, we may assume that the permutation group  $G$  is as in part (i) or (ii) of [11, Theorem 1.3].

**1.2. Motivation.** Classifications of this type are of interest from a computational and from a theoretical point of view. For instance, finding the order or the number of cycles of a permutation is a very inexpensive operation that a computer can perform as part of a recognition algorithm. In particular, an 1863 theorem of Jordan underpins a Monte Carlo algorithm that is used by major computer algebra systems, `GAP` [9] and `magma` [2], to determine whether or not a given set of permutations of  $n$  points generates  $\text{Alt}(n)$  or  $\text{Sym}(n)$ . Jordan's theorem guarantees that the only primitive groups of degree  $n$  containing an element with one cycle of prime length  $p$ , and  $n - p \geq 3$  fixed points, are  $\text{Alt}(n)$  or  $\text{Sym}(n)$ . Other theoretical results have also been important in various computer tests. For example the studies in [14, 18] on the primitive groups containing a permutation of prime order  $p$  and having at most  $p - 1$  cycles of length  $p$  have been used to improve the Monte Carlo algorithm described above.

Theoretical applications using lists of primitive groups containing permutations of a certain structure are numerous. We describe briefly a few of these applications here. The application to the covering number of  $\text{Sym}(m)$  is our main motivation.

Given a finite group  $G$ , the normal coverings of  $G$  are the families  $H_1, \dots, H_r$  of proper subgroups of  $G$  such that each element of  $G$  has a conjugate in  $H_i$  for some  $i \in \{1, \dots, r\}$ .

The minimum  $r$  is usually denoted by  $\gamma(G)$ . For  $G = \text{Alt}(m)$  or  $\text{Sym}(m)$ , it is shown in [3] that  $a\varphi(m) \leq \gamma(G) \leq bm$  for positive constants  $a$  and  $b$  (where  $\varphi$  denotes Euler's totient function). More recently, Bubboloni, Praeger and Spiga [4] developed some new research on this topic starting with the idea that primitive subgroups of the symmetric group are “few and small” and therefore cannot play a significant role in normal coverings. In particular, as an application of Theorem 1.1, they considerably improve the lower bound on  $\gamma(G)$ . The normal coverings of the symmetric and alternating groups also play a role in Galois theory. For example, let  $f(x) \in \mathbb{Z}[x]$  be a polynomial that has a root modulo  $p$  for all primes  $p$  and yet has no root in  $\mathbb{Q}$ . Consider the Galois group  $G$  of  $f(x)$  over  $\mathbb{Q}$ . Remarkably, the number of irreducible factors of  $f(x)$  over  $\mathbb{Q}$  is at least  $\gamma(G)$  by [1, Theorem 2].

Finite primitive groups containing a permutation with few cycles also play a crucial role in the study of the monodromy groups of Siegel functions and in the proof of a stronger version of Hilbert's irreducibility theorem [16]. Here we give a brief account of the relationship between these ostensibly unrelated topics and we refer the interested reader to the introduction of [16] for details. Let  $k$  be a number field, let  $\mathcal{O}_k$  denote the ring of integers of  $k$ , and let  $f(t, X) \in k(t)[X]$  be an irreducible polynomial (as usual  $k(t)$  denotes the field of  $k$ -rational functions in the variable  $t$ ). Hilbert's irreducibility theorem states that  $f(t_0, X)$  is irreducible over  $k$  for infinitely many integral specialisations  $t_0 \in \mathcal{O}_k$ . However, there is no control whatsoever on which values of  $t_0$  can be used. Using a remarkable theorem of Siegel, one can see that in order to obtain a refined version of Hilbert's irreducibility theorem, one has to obtain information on the rational functions  $g(X)$  such that  $\{g(a) \mid a \in k\} \cap \mathcal{O}_k$  has infinite cardinality. Such functions are now called Siegel functions. Another theorem of Siegel shows that a Siegel function  $g(X)$  has at most two poles on the Riemann sphere. Thus, the Galois group of  $g(X) - t$  over  $k(t)$  contains a permutation with at most two cycles. Therefore the list of the finite primitive groups containing a permutation with at most two cycles is essential for the refinement of Hilbert's irreducibility theorem obtained in [16].

There is another number theoretic application that we wish to discuss briefly and we thank Müller for bringing this to our attention (we refer the reader to the beautiful introduction in [8] for more details). Given a positive integer  $\ell$ , a *lacunary* rational function (with respect to  $\ell$ ) is an expression  $f(t) = P(t)/Q(t)$ , with  $P(t)$  and  $Q(t)$  polynomials (not necessarily coprime) having altogether at most  $\ell$  monomials. The main result of [8] describes the decompositions  $f(t) = g(h(t))$  with  $g, h \in k(t)$  of degree at least 2. In this deep investigation, again the list of the finite primitive groups admitting a permutation with at most two cycles is absolutely essential.

We consider it very likely that there are other applications of such results, and we hope that the existence of this result will prove useful and motivational to researchers in a variety of fields.

**1.3. Structure of the paper.** In Section 3, we have a closer look at the action of  $\text{Sym}(m)$  on  $k$ -sets and we show that (for  $k \geq 2$ ) such a group contains a permutation with at most four cycles only when  $k \leq 3$  and  $m \leq 9$ . In Section 4 we study  $\text{PTL}_d(q)$  in its natural action on the points or hyperplanes of the projective space  $\text{PG}_{d-1}(q)$  and determine the cycle structure of the permutations that have at most four cycles. We use the results of Sections 3 and 4 in Section 5, to prove Theorem 1.1. All of our tables are contained in Section 2.

## 2. THE TABLES

**Remark 2.1.** In order to read Tables 1, 2, 3, 4 and 5 properly we need to make a few observations. First, in order to avoid much longer tables and duplicates we have taken into account the isomorphisms  $\text{Alt}(5) \cong \text{PSL}_2(4) \cong \text{PSL}_2(5)$ ,  $\text{PSL}_2(7) \cong \text{PSL}_3(2)$ ,

Line	$\ell$	Cycle lengths	Remarks
1	1	$k_1, k_2, k_3, k_4$	$k_1 + k_2 + k_3 + k_4 = m$
2	2	$mk, m(m-k)$	$\gcd(m, k) = 1$
3	2	$mk_1, mk_2, mk_3$	$m = k_1 + k_2 + k_3$ and $\gcd(m, k_i) = 1$ for $i = 1, 2, 3$
4	2	$k_1k_2, k_1(m-k_2), k_2(m-k_1),$ $(m-k_1)(m-k_2)$	$k_1$ and $m-k_1$ coprime to $k_2$ and $m-k_2$
5	2	$\frac{k_1m}{2}, \frac{k_1m}{2}, k_2m, k_3m$	$m = k_1 + k_2 + k_3,$ $\gcd(m, k_1) = 2,$ $\gcd(m, k_i) = 1$ for $i = 2, 3$
6	2	$k_1m, k_2m, k_3m, k_4m$	$m = k_1 + k_2 + k_3 + k_4$ $\gcd(m, k_i) = 1$ for $i = 1, 2, 3, 4$
7	2	3, 4, 6, 12 or 1, 8, 8, 8	$m = 5$
8	2	12, 12, 12	$m = 6$
9	2	16, 16, 16, 16	$m = 8$
10	3	$mk_1k_2, mk_1(m-k_2), mk_2(m-k_1),$ $m(m-k_1)(m-k_2)$	$m, k_1, m-k_1, k_2$ and $m-k_2$ pairwise coprime
11	3	5, 40, 40, 40 or 15, 20, 30, 60	$m = 5$

TABLE 1. Cycle lengths  $(n_1, \dots, n_N)$  for Theorem 1.1 (i)

$\text{Alt}(6) \cong \text{PSL}_2(9)$ ,  $\text{PSL}_4(2) \cong \text{Alt}(8)$  and  $\text{PSU}_4(2) \cong \text{PSp}_4(3)$ . So, for example, the permutation representation of degree 7 of  $\text{PSL}_2(7)$  is considered in Table 2 via the natural permutation representation of  $\text{PSL}_3(2)$ . Analogously, the permutation representation of degree 6 of  $\text{PSL}_2(9)$  is in Table 1 via the natural permutation representation of  $\text{Alt}(6)$ . So, the reader has to take into account these six isomorphisms in order to read our tables accurately.

Second, a group  $\text{PSL}_d(q)$  in its natural representation may appear in more than one row of Table 2. For example  $\text{PSL}_4(3)$  appears in Lines 1, 2, 6, 7 and 8 (by taking  $d_1 = 1$  and  $d_2 = 3$ ) and 21. The permutations of  $\text{PGL}_4(3)$  having at most four cycles are obtained by considering the contribution of all of these lines. A similar remark applies to any other group.

Line	$\ell$	$d$	$q$	Cycle lengths
1	1	any	any	$\frac{q^d-1}{q-1}$
2	1	even	odd	$\frac{1}{2} \left( \frac{q^d-1}{q-1} \right), \frac{1}{2} \left( \frac{q^d-1}{q-1} \right)$
3	1	even	$\equiv 2 \pmod{3}$	$\frac{1}{3} \left( \frac{q^d-1}{q-1} \right), \frac{1}{3} \left( \frac{q^d-1}{q-1} \right), \frac{1}{3} \left( \frac{q^d-1}{q-1} \right)$
4	1	$3 \mid d$	$\equiv 1 \pmod{3}$	$\frac{1}{3} \left( \frac{q^d-1}{q-1} \right), \frac{1}{3} \left( \frac{q^d-1}{q-1} \right), \frac{1}{3} \left( \frac{q^d-1}{q-1} \right)$
5	1	$4 \mid d$	$\equiv 1 \pmod{4}$	$\frac{1}{4} \left( \frac{q^d-1}{q-1} \right), \frac{1}{4} \left( \frac{q^d-1}{q-1} \right), \frac{1}{4} \left( \frac{q^d-1}{q-1} \right), \frac{1}{4} \left( \frac{q^d-1}{q-1} \right)$
6	1	even	$\equiv 3 \pmod{4}$	$\frac{1}{4} \left( \frac{q^d-1}{q-1} \right), \frac{1}{4} \left( \frac{q^d-1}{q-1} \right), \frac{1}{4} \left( \frac{q^d-1}{q-1} \right), \frac{1}{4} \left( \frac{q^d-1}{q-1} \right)$
7	1	$d = d_1 + d_2$ $\gcd(d_1, d_2) = 1$	any	$\frac{q^{d_1}-1}{q-1}, \frac{q^{d_2}-1}{q-1}, \frac{(q^{d_1}-1)(q^{d_2}-1)}{q-1}$
8	1	$d = d_1 + d_2$ $\gcd(d_1, d_2) = 1$ $d_1, d_2$ odd	odd	$\frac{q^{d_1}-1}{q-1}, \frac{q^{d_2}-1}{q-1}, \frac{(q^{d_1}-1)(q^{d_2}-1)}{2(q-1)}, \frac{(q^{d_1}-1)(q^{d_2}-1)}{2(q-1)}$
9	1	2	prime	1, $q$
10	1	2	4	1, 2, 2
11	1	2	8	1, 2, 6
12	1	2	9	1, 3, 3, 3, or 1, 3, 6, or 2, 4, 4, or 2, 8
13	1	2	16	1, 8, 8, or 2, 3, 12, or 2, 5, 10
14	1	2	25	2, 12, 12, or 1, 5, 10, 10
15	1	2	27	4, 12, 12, or 1, 9, 9, 9
16	1	2	32	3, 15, 15
17	1	2	49	2, 16, 16, 16
18	1	3	2	1, 2, 4
19	1	3	4	1, 4, 8, 8, or 7, 14
20	1	3	9	13, 26, 26, 26
21	1	4	2	3, 6, 6
22	1	4	3	4, 12, 12, 12
23	1	4	4	10, 15, 30, 30
24	2	$d = d_1 + d_2$ $\gcd(d_1, d_2) = 1$	$\gcd(q-1, d) = 1$	$\frac{(q^d-1)(q^{d_1}-1)}{(q-1)^2}, \frac{(q^d-1)(q^{d_2}-1)}{(q-1)^2},$ $\frac{(q^d-1)(q^{d_1}-1)(q^{d_2}-1)}{(q-1)^2}$
25	2	$d = d_1 + d_2$ $\gcd(d_1, d_2) = 1$	$\gcd(q-1, d) = 2$	$\frac{(q^d-1)(q^{d_1}-1)}{(q-1)^2}, \frac{(q^d-1)(q^{d_2}-1)}{(q-1)^2},$ $\frac{(q^d-1)(q^{d_1}-1)(q^{d_2}-1)}{2(q-1)^2}, \frac{(q^d-1)(q^{d_1}-1)(q^{d_2}-1)}{2(q-1)^2}$
26	2	2	prime	$q+1, q(q+1)$
27	2	2	prime	$\frac{q+1}{2}, \frac{q+1}{2}, \frac{q(q+1)}{2}, \frac{q(q+1)}{2}$
28	2	2	4	5, 10, 10
29	2	2	5	12, 12, 12
30	2	2	7	16, 16, 16, 16
31	2	2	9	10, 30, 30, 30
32	2	2	16	17, 136, 136, or 34, 51, 204, or 34, 85, 170
33	2	2	27	28, 252, 252, 252
34	2	3	2	7, 14, 28, or 7, 14, 14, 14
35	2	3	4	21, 84, 168, 168

TABLE 2. Cycle lengths  $(n_1, \dots, n_N)$  for Theorem 1.1 (ii)3. THE ACTION OF  $\text{Sym}(m)$  ON  $k$ -SETS

The main result of this section is Proposition 3.4, which determines the elements of  $\text{Sym}(m)$  having at most four cycles in their action on  $k$ -sets; that is, on the set of  $k$ -element subsets of  $\{1, \dots, m\}$ . So, throughout this section  $H$  denotes either  $\text{Sym}(m)$  or

Socle factor	$\ell$	degree	Cycle lengths
Alt(5)	1	10	(5, 5), (2, 4, 4), (1, 3, 6), (1, 3, 3, 3)
	2	60	(15, 15, 15, 15)
Alt(6)	1	15	(5, 5, 5), (3, 6, 6)
Alt(7)	1	15	(5, 5, 5), (3, 6, 6), (1, 7, 7)
	1	21	(7, 7, 7), (1, 5, 5, 10), (2, 3, 4, 12), (3, 6, 6, 6)
Alt(8)	1	28	(7, 7, 7, 7), (4, 8, 8, 8), (3, 5, 5, 15)
	1	35	(5, 15, 15)
Alt(9)	1	36	(9, 9, 9, 9)

TABLE 3. Cycle lengths for Theorem 1.1 (iii) with  $T$  alternating

Socle factor	$\ell$	degree	Cycle lengths
$M_{11}$	1	11	(11), (1, 5, 5), (2, 3, 6), (1, 2, 8)
	1	12	(4, 8), (1, 11), (2, 2, 4, 4), (1, 1, 5, 5), (1, 2, 3, 6)
	2	121	(11, 55, 55), (22, 33, 66), (11, 22, 88)
	2	144	(4, 8, 44, 88)
$M_{12}$	1	12	(4, 8), (6, 6), (2, 10), (1, 11), (3, 3, 3, 3), (2, 2, 4, 4) (1, 1, 5, 5), (1, 2, 3, 6), (1, 1, 2, 8)
	2	144	(6, 6, 66, 66), (4, 8, 44, 88), (2, 10, 22, 110)
$M_{22}$	1	22	(11, 11), (4, 6, 12), (1, 7, 14), (2, 10, 10), (1, 7, 7, 7), (2, 4, 8, 8)
$M_{23}$	1	23	(23), (1, 11, 11), (2, 7, 14), (3, 5, 15)
	2	529	(23, 253, 253), (46, 161, 322), (69, 115, 345)
$M_{24}$	1	24	(12, 12), (3, 21), (1, 23), (6, 6, 6, 6), (2, 2, 10, 10), (1, 1, 11, 11) (1, 2, 7, 14), (1, 3, 5, 15), (2, 4, 6, 12)
	2	576	(12, 12, 276, 276), (3, 21, 69, 483)

TABLE 4. Cycle lengths for Theorem 1.1 (iii) with  $T$  sporadic

Socle factor	$\ell$	degree	Cycle lengths
PSL <sub>2</sub> (8)	1	28	(7, 7, 7, 7), (1, 9, 9, 9)
	1	36	(9, 9, 9, 9)
PSL <sub>2</sub> (11)	1	11	(11), (1, 5, 5), (2, 3, 6)
	2	121	(11, 55, 55), (22, 33, 66)
PSL <sub>2</sub> (16)	1	68	(17, 17, 17, 17)
PSL <sub>2</sub> (19)	1	57	(19, 19, 19)
PSL <sub>4</sub> (3)	1	130	(10, 40, 40, 40)
PSU <sub>3</sub> (3)	1	28	(7, 7, 7, 7), (1, 3, 12, 12), (4, 8, 8, 8)
	1	36	(6, 6, 12, 12)
PSU <sub>3</sub> (5)	1	50	(5, 5, 20, 20)
PSU <sub>4</sub> (3)	1	112	(28, 28, 28, 28)
PSp <sub>6</sub> (2)	1	28	(7, 7, 7, 7), (4, 8, 8, 8), (1, 9, 9, 9), (1, 3, 12, 12), (3, 5, 5, 15)
	1	36	(9, 9, 9, 9), (6, 6, 12, 12), (1, 5, 15, 15)
PSp <sub>4</sub> (3)	1	27	(9, 9, 9), (3, 12, 12)
	1	36	(9, 9, 9, 9), (6, 6, 12, 12)
	1	40	(10, 10, 10, 10), (4, 12, 12, 12)

TABLE 5. Cycle lengths for Theorem 1.1 (iii) with  $T$  classical

$\text{Alt}(m)$  in its action on  $k$ -sets. Replacing  $k$  by  $m - k$  if necessary, we may assume that  $k \leq m/2$ . Our arguments exploit the interplay between the action of  $H$  on  $k$ -sets and the action of  $H$  on  $\{1, \dots, m\}$ . To avoid confusion, for an element  $g \in H$ , by “a cycle of  $g$ ,” we mean a cycle of  $g$  in its action on  $k$ -sets; and by “a cycle of  $g$  on  $\{1, \dots, m\}$ ,” we mean a cycle of  $g$  in its natural action on  $\{1, \dots, m\}$ . Note that, in this section, we do not insist that  $H$  is primitive on  $k$ -sets, that is, we allow  $m = 2k$ .

Our first lemma is a simple computation. It will be used in subsequent results to show that whenever a permutation  $g$  has a long cycle in its action on  $\{1, \dots, m\}$ , it must have at least 5 distinct cycles in its action on  $k$ -sets.

**Lemma 3.1.** *If  $g \in H$  has a cycle  $C$  of length  $m'$  in its action on  $\{1, \dots, m\}$ , then the  $k$ -sets that contain  $k'$  elements from  $C$  lie in at least  $\binom{m'}{k'}/m'$  distinct cycles of  $g$ .*

*Proof.* The  $k$ -sets that intersect  $C$  in  $k'$  elements form a union of cycles of  $g$ . Moreover, the  $k$ -sets in any one of these cycles of  $g$  intersect  $C$  in at most  $m'$  distinct  $k'$ -subsets. Since we can choose  $k'$  elements from  $C$  in  $\binom{m'}{k'}$  different ways, the number of these  $g$ -cycles is at least  $\binom{m'}{k'}/m'$ .  $\square$

We are now ready to show that if  $m > 7$ , then the groups  $\text{Alt}(m)$  and  $\text{Sym}(m)$  have no elements with at most four cycles in their actions on  $k$ -sets, for  $k \geq 3$ .

**Lemma 3.2.** *If  $H$  contains a permutation  $g$  with at most four cycles and  $k \geq 3$ , then  $m \leq 7$ .*

*Proof.* Suppose that in the disjoint cycle representation for  $g$  on  $\{1, \dots, m\}$ , some cycle  $C$  has length  $m' \geq 7$ . Let  $c$  denote the set of elements of  $C$ , so  $|c| = m'$ . We claim that there exists a  $k$ -set  $x$  with  $|x \cap c| \leq m'/2$ . If for every  $k$ -set  $x$  we had  $|x \cap c| > m'/2$ , then  $\{1, \dots, m\} \setminus c$  would have size less than  $k$  and, furthermore, any  $k$ -set  $x$  containing  $\{1, \dots, m\} \setminus c$  would intersect  $c$  in a set of size at least  $\lfloor m'/2 \rfloor + 1$ . Therefore,  $(\lfloor m'/2 \rfloor + 1) + (m - m') \leq k$ . Since  $k \leq m/2$ , we obtain a contradiction and our claim is proved. Note that this means that  $m - m' \geq |x \setminus (x \cap c)| \geq k - m'/2$ ; that is,  $k \leq m - m'/2$ .

Recall that  $k \geq 3$ . If  $k - (m - m') \geq 3$  then let  $x$  be a  $k$ -set whose intersection with  $c$  is as small as possible. If  $k - (m - m') < 3$  then let  $x$  consist of 3 elements of  $c$  and  $k - 3$  elements that are not in  $c$  (this is possible since  $k - 3 < m - m'$ ). Let  $k' = |x \cap c|$ ; in both cases, we see that  $3 \leq k' \leq \lfloor m'/2 \rfloor$ . Now, for  $3 \leq k' \leq \lfloor m'/2 \rfloor$ , the binomial coefficient  $\binom{m'}{k'}$  is strictly increasing with  $k'$ . By Lemma 3.1, there are at least  $\binom{m'}{k'}/m'$  distinct cycles of  $g$  on  $k$ -sets whose intersection with  $c$  has cardinality  $k'$ . We obtain

$$\binom{m'}{k'}/m' \geq \binom{m'}{3}/m' = \frac{(m' - 1)(m' - 2)}{6} \geq \frac{6 \cdot 5}{6} = 5,$$

contradicting the assumption that  $g$  has at most four cycles. We conclude that every cycle of  $g$  on  $\{1, \dots, m\}$  has length at most 6. It follows that  $|g| \leq \text{lcm}\{2, 3, 4, 5, 6\} = 60$ .

In the remainder of the proof, we assume towards a contradiction that  $m \geq 8$ . Now the number of  $k$ -sets is  $\binom{m}{k} \geq \binom{m}{3}$ . So the number of cycles on  $k$ -sets is at least  $\binom{m}{3}/60$ , which is greater than 4 when  $m \geq 13$ . For  $m = 8, 9, 10, 11, 12$  we can replace 60 by the exact value for the maximum element order  $n$  in  $\text{Sym}(m)$  and replace 3 with  $k$  for each  $k$  between 3 and  $m/2$ . We find that the only possibilities with  $\binom{m}{k}/n \leq 4$  are  $m = 8, 10, 12$  with  $k = 3$ . These three remaining cases are easily eliminated in magma.  $\square$

We now consider the action of symmetric and alternating groups on 2-sets. Again, the groups must be very small to contain elements that have at most four cycles.

**Lemma 3.3.** *If  $k = 2$  and  $H$  contains a permutation  $g$  that has at most four cycles, then  $m \leq 9$ .*

*Proof.* Towards a contradiction, suppose that  $m \geq 10$ . Then since  $k = 2$ , for a subset  $x$  of  $\{1, \dots, m\}$  of cardinality  $k$ , there are at least 8 elements of  $\{1, \dots, m\}$  that are not in  $x$ .

Suppose that there is a cycle  $C$  of length  $m' \geq 10$  in the disjoint cycle representation for  $g$ . Let  $c$  be the set of elements in  $C$ . Then since  $k = 2$ , it is possible to choose  $x$  so that  $x \cap c$  has cardinality 2. By Lemma 3.1,  $g$  has at least  $\lfloor m'/2 \rfloor$  orbits on  $k$ -subsets of  $\{1, \dots, m\}$  whose intersection with  $c$  has cardinality 2. Since  $m' \geq 10$  we have  $\lfloor m'/2 \rfloor \geq 5$ , which is a contradiction.

If there is a cycle  $C$  of length  $m'$  in the disjoint cycle representation for  $g$ , with  $6 \leq m' \leq 9$ , then since  $k = 2$ , it is possible to choose  $x$  so that  $|x \cap c|$  takes on any value between  $\max\{0, m' - 8\}$  and 2 (inclusive). Now  $g$  has at least  $\lfloor m'/2 \rfloor$  orbits on  $k$ -subsets of  $\{1, \dots, m\}$  whose intersection with  $c$  has cardinality 2, and at least one orbit on  $k$ -subsets of  $\{1, \dots, m\}$  whose intersection with  $c$  has cardinality  $i$  as long as  $m' - 8 \leq i < 2$  (and  $i \geq 0$ ). In each case, this gives a total of at least five orbits of  $g$ , which is a contradiction.

Thus we may assume that each cycle of  $g$  has length at most 5, and hence that  $|g| \leq \text{lcm}\{2, 3, 4, 5\} = 60$ . Arguing as in Lemma 3.2, we have  $\binom{m}{2}/60 > 4$  for  $m \geq 23$  so in these cases  $g$  has at least five cycles. The remaining cases (where  $10 \leq m \leq 22$ ) are easily eliminated using magma. □

The following proposition summarises the previous results.

**Proposition 3.4.** *Let  $H$  be  $\text{Alt}(m)$  or  $\text{Sym}(m)$  in its natural action on the  $k$ -subsets of  $\{1, \dots, m\}$  with  $k \leq m/2$ . If  $H$  contains a permutation  $g$  that has at most four cycles in this action then either  $k = 3$  and  $m = 6$ ; or  $k = 2$  and  $m \leq 9$ ; or  $k = 1$ .*

*Proof.* By Lemma 3.2, if  $k \geq 3$ , then  $m \leq 7$ . Since  $k \leq m/2$ , we must have  $k = 3$  and  $m \in \{6, 7\}$ . The case  $k = 3$  and  $m = 7$  is eliminated with a straightforward computation. Therefore we may assume that  $k \leq 2$ . By Lemma 3.3, if  $k = 2$  then  $m \leq 9$ . □

**Remark 3.5.** Notice that the action of  $\text{Sym}(6)$  on 3-sets is imprimitive. This group does contain permutations with at most four cycles (for example a 6-cycle in  $\text{Sym}(6)$  has cycle lengths 2, 6, 6, 6, and a 5-cycle has cycle lengths 5, 5, 5, 5), but there is no primitive overgroup, so these elements do not appear in our tables.

#### 4. $\text{P}\Gamma\text{L}_d(q)$ IN ITS NATURAL ACTION

In this section we study  $\text{P}\Gamma\text{L}_d(q)$  acting on the points or hyperplanes of the projective space  $\text{PG}_{d-1}(q)$  with  $d \geq 2$ , and we determine the cycle structure of its elements that have at most four cycles. Since these actions are permutationally isomorphic, it is sufficient to study the action on points. In order to do so, we introduce some notation (we follow [11, Section 2]).

**Notation 4.1.** Let  $s$  be a semisimple element of  $\text{PGL}_d(q)$  and let  $\bar{s}$  be a semisimple element of  $\text{GL}_d(q)$  projecting to  $s$  in  $\text{PGL}_d(q)$ . The action of the matrix  $\bar{s}$  on the  $d$ -dimensional vector space  $V = \mathbb{F}_q^d$  naturally defines the structure of an  $\mathbb{F}_q\langle\bar{s}\rangle$ -module on  $V$ . Since  $\bar{s}$  is semisimple,  $V$  decomposes, by Maschke's theorem, as a direct sum of irreducible  $\mathbb{F}_q\langle\bar{s}\rangle$ -modules, that is,  $V = V_1 \oplus \dots \oplus V_l$ , with  $V_i$  an irreducible  $\mathbb{F}_q\langle\bar{s}\rangle$ -module. Relabelling the index set  $\{1, \dots, l\}$  if necessary, we may assume that the first  $t$  submodules  $V_1, \dots, V_t$  are pairwise non-isomorphic (for some  $t \in \{1, \dots, l\}$ ) and that for  $j \in \{t+1, \dots, l\}$ ,  $V_j$  is isomorphic to some  $V_i$  with  $i \in \{1, \dots, t\}$ . Now, for  $i \in \{1, \dots, t\}$ , let  $\mathcal{W}_i = \{W \leq V \mid W \cong V_i\}$ , the set of  $\mathbb{F}_q\langle\bar{s}\rangle$ -submodules of  $V$  isomorphic to  $V_i$  and write  $W_i = \sum_{W \in \mathcal{W}_i} W$ . The module  $W_i$  is usually referred to as the *homogeneous* component of  $V$  corresponding to the simple submodule  $V_i$ . We have  $V = W_1 \oplus \dots \oplus W_t$ . Set  $a_i = \dim_{\mathbb{F}_q}(W_i)$ . Since  $V$  is completely reducible, we have  $W_i = V_{i,1} \oplus \dots \oplus V_{i,m_i}$  for some  $m_i \geq 1$ , where  $V_{i,j} \cong V_i$ , for each  $j \in \{1, \dots, m_i\}$ . Thus we have  $a_i = d_i m_i$ , where  $d_i = \dim_{\mathbb{F}_q} V_i$ , and



$\sum_{i=1}^t d_i m_i = d$ . For  $i \in \{1, \dots, t\}$ , we let  $x_i$  (respectively  $y_{i,j}$ ) denote the element in  $\text{GL}(W_i)$  (respectively  $\text{GL}(V_{i,j})$ ) induced by the action of  $\bar{s}$  on  $W_i$  (respectively  $V_{i,j}$ ). In particular,  $x_i = y_{i,1} \cdots y_{i,m_i}$  and  $\bar{s} = x_1 \cdots x_t$ . We note further that

$$p(s) = \underbrace{(d_1, \dots, d_1)}_{m_1 \text{ times}} \underbrace{(d_2, \dots, d_2)}_{m_2 \text{ times}}, \dots, \underbrace{(d_t, \dots, d_t)}_{m_t \text{ times}}$$

is a partition of  $n$ .

We conclude this notation by introducing some basic facts about  $\mathbf{C}_{\text{GL}_d(q)}(\bar{s})$ , the centralizer of  $\bar{s}$  in  $\text{GL}_d(q)$ , that will be used later in the proof of Theorem 4.3. Let  $c \in \mathbf{C}_{\text{GL}_d(q)}(\bar{s})$ . Given  $i \in \{1, \dots, t\}$  and  $W \in \mathcal{W}_i$ , we see that  $W^c$  is an  $\mathbb{F}_q\langle \bar{s} \rangle$ -submodule of  $V$  isomorphic to  $W$  (because  $c$  commutes with  $\bar{s}$ ). Thus  $W^c \in \mathcal{W}_i$ . This shows that  $W_i$  is  $\mathbf{C}_{\text{GL}_d(q)}(\bar{s})$ -invariant. It follows that

$$\mathbf{C}_{\text{GL}_d(q)}(\bar{s}) = \mathbf{C}_{\text{GL}(W_1)}(x_1) \times \cdots \times \mathbf{C}_{\text{GL}(W_t)}(x_t)$$

and every unipotent element of  $\mathbf{C}_{\text{GL}_d(q)}(\bar{s})$  is of the form  $u = u_1 \cdots u_t$  with  $u_i \in \mathbf{C}_{\text{GL}(W_i)}(x_i)$  unipotent in  $\text{GL}(W_i)$ , for each  $i$ .

Now [11, Proposition 2.6] implies that  $|u| \leq \max\{p^{\lceil \log_p(m_1) \rceil}, \dots, p^{\lceil \log_p(m_t) \rceil}\}$ . (Although [11, Proposition 2.6] is stated for  $\text{PGL}_d(q)$ , its proof applies verbatim to  $\text{GL}_d(q)$  also.)

We start with a preliminary number-theoretic lemma.

**Lemma 4.2.** *Let  $q \geq 2$  and  $x_1, x_2 \geq 1$  be integers with  $\gcd(x_1, x_2) = 1$ . Then there exists an integer  $c$  with  $\gcd(c, q-1) = 1$  and*

$$\gcd(cx_1 - x_2, q-1) = \begin{cases} 2 & \text{if } q, x_1, x_2 \text{ are odd,} \\ 1 & \text{otherwise.} \end{cases}$$

*Proof.* If  $q = 2$ , we may choose  $c = 1$ . Now suppose that  $q > 2$  and write  $q-1 = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$  with  $p_1, \dots, p_t$  distinct primes and  $\alpha_1, \dots, \alpha_t \geq 1$ .

Observe that for each  $p_i > 2$ , either  $x_2 + 1$  or  $x_2 - 1$  is coprime to  $p_i$ . In particular, for  $p_i > 2$ , choose  $\varepsilon_i \in \{1, -1\}$  with  $x_2 + \varepsilon_i$  coprime to  $p_i$ .

Now using the Chinese Remainder Theorem, we choose  $c \in \mathbb{Z}$  with

$$\begin{aligned} cx_1 &\equiv x_2 + \varepsilon_i \pmod{p_i} && \text{if } p_i \text{ is coprime to } x_1, \text{ or} \\ c &\equiv 1 \pmod{p_i} && \text{if } p_i \text{ divides } x_1, \end{aligned}$$

for each  $p_i > 2$  and with

$$\begin{aligned} cx_1 &\equiv x_2 + 2 \pmod{4} && \text{if } x_1 \text{ and } x_2 \text{ are odd, or} \\ c &\equiv 1 \pmod{p_i} && \text{if } x_1 \text{ or } x_2 \text{ is even} \end{aligned}$$

if  $p_i = 2$ . Since  $\gcd(x_1, x_2) = 1$ , it follows that  $c$  and  $cx_1 - x_2$  are both coprime to  $p_i$  when  $p_i > 2$ . In particular, the result follows for  $q$  even. If  $q$  is odd then there is a  $p_i$  equal to 2 and so  $c$  is odd so  $\gcd(c, q-1) = 1$ . Moreover  $cx_1 - x_2$  is either congruent to 2 mod 4 (when  $x_1, x_2$  are odd, in which case  $\gcd(cx_1 - x_2, q-1) = 2$ ) or odd (when  $x_1$  or  $x_2$  is even, in which case  $\gcd(cx_1 - x_2, q-1) = 1$ ).  $\square$

**Theorem 4.3.** *The group  $\text{PGL}_d(q)$  contains a permutation  $g$  with at most four cycles if and only if  $d, q$  and the cycle lengths of  $g$  are as in Table 2 with  $\ell = 1$ .*

*Proof.* Let  $V = \mathbb{F}_q^d$  be the  $d$ -dimensional vector space of row vectors over the finite field  $\mathbb{F}_q$  of size  $q$  and let  $e_1, \dots, e_d$  be the canonical basis of  $V$ . Write  $q = p^f$  for some prime  $p$  and some integer  $f \geq 1$ . For a subspace  $W$  of  $V$ , we denote by  $P(W)$  the set of 1-dimensional subspaces of  $V$  contained in  $W$ . Moreover we use Notation 4.1.

We split the proof into two cases depending on whether  $g \in \text{PGL}_d(q)$ , or  $g \in \text{PGL}_d(q) \setminus \text{PGL}_d(q)$ .

Suppose that  $g \in \mathrm{PGL}_d(q)$  has at most four cycles and observe that  $|g| \geq (q^d - 1)/(4(q - 1))$ . Moreover, we start by dealing with the case that  $g$  is a semisimple element. By Maschke's theorem, as in Notation 4.1,  $V = V_1 \oplus \cdots \oplus V_t$ , where each  $V_i$  is an irreducible  $\mathbb{F}_q\langle g \rangle$ -module. If  $t \geq 3$ , then  $g$  has at least 5 orbits on  $P(V)$ . Indeed,  $g$  has at least one orbit on each of  $P(V_1)$ ,  $P(V_2)$ ,  $P(V_3)$ ,  $P(V_1 \oplus V_2) \setminus (P(V_1) \cup P(V_2))$  and  $P(V_1 \oplus V_3) \setminus (P(V_1) \cup P(V_3))$ . Thus  $t \leq 2$ .

If  $t = 1$ , then  $g$  acts irreducibly on  $V$  and so by Schur's lemma  $g$  lies in a Singer cycle of  $\mathrm{PGL}_d(q)$  of order  $(q^d - 1)/(q - 1)$ . As a Singer cycle acts regularly on  $P(V)$ , we have  $|g| = (q^d - 1)/(i(q - 1))$  for  $i = 1, 2, 3, 4$  such that  $i \mid (q^d - 1)/(q - 1)$ , and  $g$  has exactly  $i$  cycles in its action on  $P(V)$ . Note that 2 divides  $(q^d - 1)/(q - 1)$  if and only if  $q$  is odd and  $d$  is even. Similarly, 3 divides  $(q^d - 1)/(q - 1)$  if and only if  $3 \mid d$  and  $q \equiv 1 \pmod{3}$ , or  $2 \mid d$  and  $q \equiv 2 \pmod{3}$ . Finally, 4 divides  $(q^d - 1)/(q - 1)$  only if  $4 \mid d$  and  $q \equiv 1 \pmod{4}$ , or  $2 \mid d$  and  $q \equiv 3 \pmod{4}$ . This gives the first six lines of Table 2.

Now suppose that  $t = 2$ . Write  $d_i = \dim_{\mathbb{F}_q} V_i$  and  $a_i = (q^{d_i} - 1)/(q - 1)$ , for  $i = 1, 2$ . Now a lift of  $g$  in  $\mathrm{GL}_d(q)$  can be written as  $g_1 g_2 = g_2 g_1$ , with  $g_i \in \mathrm{GL}_{d_i}(q)$  fixing pointwise  $P(V_j)$ , for  $i \neq j$ . We claim that  $g_i$  has only one orbit on  $P(V_i)$  for  $i = 1, 2$ . For otherwise, if  $g_1$  had two orbits on  $P(V_1)$  say, then  $g$  would have two orbits on  $P(V_1)$  and at least two orbits on  $P(V) \setminus (P(V_1) \cup P(V_2))$ . Since  $g$  also has at least one orbit on  $P(V_2)$ ,  $g$  would have at least five orbits on  $P(V)$ . Therefore we argue as in the previous paragraph that, since  $g_i$  has only one cycle on  $P(V_i)$ , it is a Singer cycle in its action on  $P(V_i)$  and so has order  $a_i$  on  $P(V_i)$ . In particular, we have  $g_i = h_i^{j_i}$  for some Singer cycle  $h_i \in \mathrm{GL}_{d_i}(q)$  and some divisor  $j_i$  of  $q - 1$  such that  $\gcd(j_i, a_i) = 1$ . Since  $h_i$  is a Singer cycle in  $\mathrm{GL}_{d_i}(q)$ , we see that  $h_i^{a_i}$  corresponds to multiplication by some primitive element  $\lambda_i \in \mathbb{F}_q$ . Write  $\lambda = \lambda_1$ . Now,  $\lambda_2 = h_2^{a_2}$  is a generator of  $\langle \lambda \rangle$  and hence there exists  $a'_2$  with  $h_2^{a'_2} = \lambda$  and  $\gcd(a'_2, q^{d_2} - 1) = a_2$ . Thus  $a'_2 = a_2 c'$ , for some  $c'$  with  $\gcd(c', (q^{d_2} - 1)/a_2) = 1$ , that is,  $\gcd(c', q - 1) = 1$ . From Dirichlet's Theorem on primes in arithmetic progression, there exists  $t$  with  $c' + t(q - 1)$  a prime number greater than  $q^{d_2} - 1$ . In particular  $h_2^{c' + t(q - 1)}$  is a Singer cycle of  $\mathrm{GL}_{d_2}(q)$  and  $(h_2^{c' + t(q - 1)})^{a_2} = h_2^{a_2 c' + t(q^{d_2} - 1)} = h_2^{a'_2} = \lambda$ . This shows that replacing  $h_2$  by  $h_2^{c' + t(q - 1)}$ , we may assume that  $\lambda_2 = \lambda$ , that is,  $c = c' = 1$ .

As  $g$  has at most two cycles on  $P(V) \setminus (P(V_1) \cup P(V_2))$ , for at least one of these cycles the following is true for any vector  $w_2 \in V_2 \setminus \{0\}$ : at least half of the 1-spaces  $\langle w_1 \rangle$  of  $P(V_1)$  occur for vectors  $w_1 \in V_1$  such that  $\langle w_1 + w_2 \rangle$  lies in this cycle. A 1-space of the form  $\langle w'_1 + w_2 \rangle$  with  $w'_1 \in V_1 \setminus \{0\}$  can only occur as  $g^{a_2 j}(\langle w_1 + w_2 \rangle)$  for some  $j$ , since  $g_2$  acts regularly on  $P(V_2)$  with order  $a_2$ . Thus the element  $g^{a_2} = g_1^{a_2} g_2^{a_2}$  has a cycle of length at least  $a_1/2$  in its action on  $P(V_1)$  and hence  $\gcd(a_1, a_2) \leq 2$ . Moreover, since  $\gcd(a_1, a_2) = (q^{\gcd(d_1, d_2)} - 1)/(q - 1)$  (which cannot be equal to 2), we have  $\gcd(d_1, d_2) = 1$ .

As  $\gcd(d_1, d_2) = 1$ , we have  $\gcd(a_1, a_2) = 1$  and  $\langle g \rangle$  is transitive on the 2-spaces of the form  $\langle w_1 \rangle \oplus \langle w_2 \rangle$  with  $w_i \in V_i \setminus \{0\}$ . Each such 2-space contains exactly  $q - 1$  of the 1-spaces in  $P(V) \setminus (P(V_1) \cup P(V_2))$ , and a  $g$ -cycle in  $P(V) \setminus (P(V_1) \cup P(V_2))$  has size  $a_1 a_2 s$ , where  $s$  is the length of a cycle of  $g^{a_1 a_2}$  on the 1-spaces in a given 2-space  $W := \langle w_1 \rangle \oplus \langle w_2 \rangle$ . Thus  $g^{a_1 a_2}$  has at most two cycles on the  $q - 1$  spaces in  $P(V) \setminus (P(V_1) \cup P(V_2))$  lying in  $W$ .

We show that either

- $g^{a_1 a_2}$  has exactly one cycle on this set (giving rise to line 7 of Table 2), or
- $g^{a_1 a_2}$  has exactly two cycles of length  $(q - 1)/2$  on this set and  $q d_1 d_2$  is odd (giving rise to line 8 of Table 2).

To prove this claim, arbitrarily choose  $w_1, w'_1 \in V_1 \setminus \{0\}$  and  $w_2, w'_2 \in V_2 \setminus \{0\}$ . Since  $h_i$  is a Singer cycle on  $V_i$  and fixes  $V_{3-i}$  pointwise, there exist  $j_1, j_2$  such that  $(w_1 + w_2) h_1^{j_1} h_2^{j_2} = w'_1 + w'_2$ . Since  $h_1^{j_1} h_2^{j_2}$  commutes with  $g$ , it is straightforward to see that the orbits of  $w_1 + w_2$  and of  $w'_1 + w'_2$  under  $g$  must have the same length. In particular, if  $g^{a_1 a_2}$  has

two cycles on the  $q - 1$  spaces of  $P(V) \setminus (P(V_1) \cup P(V_2))$  lying in  $W$  then each has length  $(q - 1)/2$  and hence  $q$  is odd. Moreover,

$$|g| = \begin{cases} a_1 a_2 (q - 1) & \text{if } g \text{ has three cycles on } P(V), \\ a_1 a_2 (q - 1)/2 & \text{if } g \text{ has four cycles on } P(V). \end{cases}$$

Now, for any nonzero  $v_1 \in V_1$  and any nonzero  $v_2 \in V_2$ , we have

$$(1) \quad g^{a_1 a_2} : \langle v_1 \oplus v_2 \rangle \rightarrow \langle \lambda^{a_2 j_1} v_1 \oplus \lambda^{a_1 j_2} v_2 \rangle = \langle v_1 \oplus \lambda^{a_1 j_2 - a_2 j_1} v_2 \rangle.$$

This shows that  $|g^{a_1 a_2}| = |\lambda^{a_1 j_2 - a_2 j_1}|$ . Therefore  $\gcd(a_1 j_2 - a_2 j_1, q - 1) = 1$  when  $g$  has three cycles and  $\gcd(a_1 j_2 - a_2 j_1, q - 1) = 2$  when  $g$  has four cycles. Suppose now that  $g$  has four cycles and that  $d_1 d_2$  is even. Since  $\gcd(d_1, d_2) = 1$ , replacing  $d_1$  by  $d_2$  if necessary, we get that  $d_1$  is even and  $d_2$  is odd. As  $q$  is odd,  $a_1$  is even and  $a_2$  is odd. Now,  $\gcd(a_1 j_2 - a_2 j_1, q - 1) = 2$  forces  $j_1$  being even. This is a contradiction because  $\gcd(j_1, a_1) \neq 1$ . Therefore when  $g$  has four cycles  $q d_1 d_2$  is odd as predicted by line 8 of Table 2.

Conversely, we now show that when  $\gcd(d_1, d_2) = 1$  and  $q d_1 d_2$  is odd, there do exist permutations with exactly four cycles on  $P(V)$ . From Lemma 4.2, there exists  $c \in \mathbb{Z}$  with  $\gcd(c, q - 1) = 1$  and  $\gcd(ca_1 - a_2, q - 1) = 2$ . Take  $g = h_1 h_2^c$ . The computation in (1) shows that  $g$  has one orbit on each of  $P(V_1)$  and  $P(V_2)$ , and two orbits on  $P(V) \setminus (P(V_1) \cup P(V_2))$ .

It remains to show that, there do always exist permutations with exactly three cycles on  $P(V)$  when  $\gcd(d_1, d_2) = 1$ . Suppose that  $q$  is even, or that  $q$  is odd and  $d_1 d_2$  is even. (Recall that when  $q$  is odd  $d_1 d_2$  has the same parity as  $a_1 a_2$ .) Then, from Lemma 4.2, there exists  $c \in \mathbb{Z}$  with  $\gcd(c, q - 1) = 1$  and  $\gcd(ca_1 - a_2, q - 1) = 1$ . Take  $g = h_1 h_2^c$ . The computation in (1) shows that  $g$  has one orbit on each of  $P(V_1)$  and  $P(V_2)$ , and one orbit on  $P(V) \setminus (P(V_1) \cup P(V_2))$ . Finally, suppose that  $q$  is odd and that  $d_1 d_2$  is odd. Then  $a_1 a_2$  is odd and  $\gcd(a_1, a_2) = 1$ . Since  $\gcd(a_1, 2a_2) = 1$ , from Lemma 4.2, there exists  $c \in \mathbb{Z}$  with  $\gcd(c, q - 1) = 1$  and  $\gcd(ca_1 - 2a_2, q - 1) = 1$ . Take  $g = h_1 h_2^{2c}$ . The computation in (1) shows that  $g$  has one orbit on each of  $P(V_1)$  and  $P(V_2)$ , and one orbit on  $P(V) \setminus (P(V_1) \cup P(V_2))$ .

Next assume that  $g$  is not semisimple. Write  $g = g_{ss} g_u = g_u g_{ss}$ , with  $g_{ss}$  semisimple and  $g_u$  unipotent. We use Notation 4.1 for the element  $g_{ss}$  and for the partition  $p(g_{ss})$  associated to  $g_{ss}$ .

Assume that  $t = 1$  so that

$$p(g_{ss}) = \underbrace{(d_1, \dots, d_1)}_{m_1 \text{ times}}$$

for some  $d_1, m_1 \geq 1$ ; we note that  $d = d_1 m_1$ . Observe that since  $g$  is not semisimple  $m_1 \geq 2$ . Now, from Notation 4.1,  $|g| \leq p^{\lceil \log_p(m_1) \rceil} (q^{d_1} - 1)/(q - 1)$ . A computation shows that if  $d \geq 3$ , then this upper bound on  $|g|$  is greater than or equal to  $(q^d - 1)/(4(q - 1))$  only if  $(q, d_1, m_1, d) = (2, 1, 3, 3), (2, 1, 4, 4), (2, 1, 5, 5), (2, 2, 2, 4), (3, 2, 2, 4)$ . Analysing individually each of these examples, we find that only  $\text{PGL}_3(2)$ ,  $\text{PGL}_4(2)$  and  $\text{PGL}_4(3)$  contain an element with at most four cycles that is not semisimple (and the cycle structures are  $(1, 2, 4)$ ,  $(3, 6, 6)$  and  $(4, 12, 12, 12)$  respectively). Thus we obtain lines 18, 21 and 22 of Table 2. Now assume that  $d = 2$ . In this case, as  $g$  is not semisimple, we must have  $g_{ss} = 1$  and  $g = g_u$ , that is,  $g$  is unipotent. It is clear that  $g$  has at least  $1 + q/p$  cycles on  $P(V)$  and hence either  $q$  is prime, or  $q \in \{4, 9\}$  (and since  $p \mid |g|$ , the element  $g$  has cycle structure  $(1, q)$ ,  $(1, 2, 2)$  or  $(1, 3, 3, 3)$  respectively). Thus we obtain lines 9, 10 and 12 of Table 2.

Next assume that  $t \geq 2$ . Moreover, assume also that  $m_1, m_2 \geq 2$ . Again from Notation 4.1 and from the fact that the maximal element order of  $\text{GL}_{d-d_1 m_1 - d_2 m_2}(q)$  is  $q^{d-d_1 m_1 - d_2 m_2} - 1$  (see for example [11, Corollary 2.7]), we have

$$|g| < (q^{d-d_1 m_1 - d_2 m_2} - 1) \text{lcm}(q^{d_1} - 1, q^{d_2} - 1) \max\{p^{\lceil \log_p(m_1) \rceil}, p^{\lceil \log_p(m_2) \rceil}\}.$$

Another computation shows that this upper bound on  $|g|$  implies that  $|g| < (q^d - 1)/(4(q - 1))$ , and hence  $g$  has more than four cycles.

It remains to consider the case

$$p(g_{ss}) = (\underbrace{d_1, \dots, d_1}_{m_1 \text{ times}}, d_2, d_3, \dots, d_t)$$

with  $m_1 \geq 1$ ,  $m_2 = \dots = m_t = 1$  and  $t \geq 2$ . Observe that since  $g$  is not semisimple, we have  $m_1 \geq 2$ . Now

$$(2) \quad |g| < (q^{d-d_1 m_1 - d_2} - 1) \text{lcm}(q^{d_1} - 1, q^{d_2} - 1) p^{\lceil \log_p(m_1) \rceil}$$

and hence another computation shows that  $|g| \geq (q^d - 1)/(4(q - 1))$  is possible only if  $d_1 \leq 2$  and  $m_1 \leq 3$ . And further, if  $m_1 = 3$ , then  $(q, d_1) = (2, 1)$ . First suppose that  $m_1 = 3$ . Then since  $(q, d_1) = (2, 1)$ , the element  $g$  in its Jordan decomposition has a  $3 \times 3$  unipotent block

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

which has three orbits on  $\langle e_1, e_2, e_3 \rangle$ . As  $t \geq 2$ , we have  $d \geq m_1 + 1 \geq 4$  and it is now clear that  $g$  has more than four orbits on  $P(V)$ . Thus we may assume that  $m_1 = 2$ . In this case, the Jordan form of  $g$  is

$$\begin{pmatrix} A & I & 0 \\ 0 & A & 0 \\ 0 & 0 & B \end{pmatrix}$$

where  $A \in \text{GL}_{d_1}(q)$ ,  $B \in \text{GL}_{d-2d_1}(q)$  is semisimple and  $I \in \text{GL}_{d_1}(q)$  is the identity matrix. It is clear that  $e_1, e_{d_1+1}, e_{2d_1+1}, e_{d_1+1} + e_{2d_1+1}$ , and  $e_1 + e_{2d_1+1}$  are all in different cycles of  $g$ , since  $g$  fixes setwise the subspaces  $\langle e_{d_1+1}, \dots, e_{2d_1} \rangle$ ,  $\langle e_1, \dots, e_{2d_1} \rangle$ ,  $\langle e_{2d_1}, \dots, e_d \rangle$ . (Note that we apply matrices from the right.) Thus  $g$  has at least 5 cycles, a contradiction. This concludes the case  $g \in \text{PGL}_d(q)$ .

Finally suppose that  $g \in \text{P}\Gamma\text{L}_d(q) \setminus \text{PGL}_d(q)$ . In particular,  $f \geq 2$  and  $g = x\psi$  for some  $x \in \text{PGL}_d(q)$  and for some non-trivial field automorphism  $\psi$  of order  $e > 1$ . Let  $\overline{\mathbb{F}}_q$  be the algebraic closure of the finite field  $\mathbb{F}_p$ . From Lang's theorem [10, Theorem 2.1], there exists  $a$  in the algebraic group  $\text{PGL}_d(\overline{\mathbb{F}}_q)$  with  $x = aa^{-\psi}$ . Observe that  $(x\psi)^e = xx^\psi \dots x^{\psi^{e-2}} x^{\psi^{e-1}}$ . Write  $z = a^{-1}(x\psi)^e a$ . Now,

$$\begin{aligned} z^\psi &= a^{-\psi}(x^\psi x^{\psi^2} \dots x^{\psi^{e-1}} x^{\psi^e}) a^\psi = a^{-\psi}(x^\psi x^{\psi^2} \dots x^{\psi^{e-1}} x) a^\psi \\ &= (a^{-\psi} x^{-1})(xx^\psi \dots x^{\psi^{e-2}} x^{\psi^{e-1}})(xa^\psi) = a^{-1}(xx^\psi \dots x^{\psi^{e-2}} x^{\psi^{e-1}}) a \\ &= a^{-1}(x\psi)^e a = z \end{aligned}$$

and so  $z$  is invariant under the field automorphism  $\psi$  of order  $e$ . Thus  $z \in \text{PGL}_d(q^{1/e})$ . From [11, Corollary 2.7] for example, we know that the maximal element order of  $\text{PGL}_d(q^{1/e})$  is  $(q^{d/e} - 1)/(q^{1/e} - 1)$ . Observe further that since  $g$  has at most four cycles, we have  $|g| \geq \lceil (q^d - 1)/(4(q - 1)) \rceil$ . Therefore

$$\left\lceil \frac{q^d - 1}{4(q - 1)} \right\rceil \leq |g| = e|g^e| = e|z| \leq e \left( \frac{q^{d/e} - 1}{q^{1/e} - 1} \right).$$

It follows by a direct computation that this inequality is satisfied only for

$$\begin{aligned} (p, f, e, d) \in & \{(2, 2, 2, 2), (3, 2, 2, 2), (5, 2, 2, 2), (7, 2, 2, 2), (2, 3, 3, 2), (3, 3, 3, 2), \\ & (2, 4, 2, 2), (2, 4, 4, 2), (2, 5, 5, 2), (2, 6, 2, 2), (2, 6, 6, 2), (2, 2, 2, 3), \\ & (3, 2, 2, 3), (2, 3, 3, 3), (2, 2, 2, 4)\}. \end{aligned}$$

For each of these quadruples, we can check with a computer whether  $\text{P}\Gamma\text{L}_d(q)$  contains a permutation with at most four cycles and we obtain only the cases listed in Table 2.  $\square$

### 5. PRIMITIVE GROUPS: ALMOST SIMPLE AND PRODUCT ACTION TYPE

In this section we assume that  $G = \text{Sym}(m) \text{ wr } \text{Sym}(\ell)$  in its product action (of degree  $n = \binom{m}{k}^\ell$ ) on a Cartesian product of  $\ell$  copies of the set of  $k$ -subsets of  $\{1, \dots, m\}$  (where  $1 \leq k < m/2$ ), or that  $G = \text{P}\Gamma\text{L}_d(q) \text{ wr } \text{Sym}(\ell)$  in its product action (of degree  $n = ((q^d - 1)/(q - 1))^\ell$ ) on a Cartesian product of  $\ell$  copies of the set of points of the projective space  $\text{P}\Gamma\text{G}_{d-1}(q)$ . We do not require that  $\ell \geq 2$  and so, in particular, we deal simultaneously with primitive groups of almost simple and product action type. Write  $\Delta$  for the family of  $k$ -subsets of  $\{1, \dots, m\}$  or for the point set of  $\text{P}\Gamma\text{G}_{d-1}(q)$  (depending on which group we are considering) and  $\Omega = \Delta^\ell$ .

We let  $\text{soc}(G)$  denote the socle of  $G$ ; here we have  $\text{soc}(G) = \text{Alt}(m)^\ell$  or  $\text{soc}(G) = \text{PSL}_d(q)^\ell$ . Moreover, in what follows we write  $H = \text{Sym}(m)$  or  $H = \text{P}\Gamma\text{L}_d(q)$  (again depending on which group we are considering) and we write the elements  $g \in G$  as  $(h_1, \dots, h_\ell)\sigma$ , with  $h_1, \dots, h_\ell \in H$  and  $\sigma \in \text{Sym}(\ell)$ . We reserve the letter  $T$  to denote the socle of  $H$  and  $r = |\Delta|$  to denote the degree of the permutation group  $H$  (so,  $r = \binom{m}{k}$  or  $r = (q^d - 1)/(q - 1)$ ). Since we are only interested in primitive groups of almost simple and product action type, we assume that  $m \geq 5$ ,  $d \geq 2$ , and  $q \geq 4$ . Since  $r \neq 1$ , this forces  $r \geq 5$ .

We start with a basic lemma that will be used repeatedly in the sequel.

**Lemma 5.1.** *Let  $\Delta_i$  be a finite set and let  $h_i \in \text{Sym}(\Delta_i)$  be a cycle of length  $|\Delta_i|$ , for  $i = 1, 2$ . Then  $(h_1, h_2)$  has  $\text{gcd}(|\Delta_1|, |\Delta_2|)$  cycles in its action on  $\Delta_1 \times \Delta_2$  and moreover each cycle has the same length.*

*Proof.* See [17, Lemma 3, page 92] or [6, 3.2.19].  $\square$

The following two results are the main tools used in this section.

**Proposition 5.2.** *Assume that  $G$  contains a permutation  $g = y\sigma$  having at most four cycles, with  $y \in H^\ell$ ,  $\sigma \in \text{Sym}(\ell)$  and  $\sigma \neq 1$ . Then  $\sigma$  is a transposition, and either  $r \in \{5, 6, 7, 8\}$  and  $\ell = 2$ , or  $r \in \{5, 8\}$  and  $\ell = 3$ .*

*Proof.* We have  $g = (h_1, \dots, h_\ell)\sigma$  with  $h_1, \dots, h_\ell \in H$ . Let  $t$  be the length of the longest cycle of  $\sigma$  and let  $c_g$  be the number of cycles of  $g$ . Relabelling the index set  $\{1, \dots, \ell\}$  if necessary, we may assume that  $(1, \dots, t)$  is a cycle of  $\sigma$ . Consider  $x = g^t$  and let  $c_x$  be the number of cycles of  $x$ . Clearly, we have  $c_g \geq \lceil c_x/t \rceil$  and so

$$(3) \quad \lceil c_x/t \rceil \leq 4.$$

Now we estimate  $c_x$ . We have

$$x = (h_1 \cdots h_t, h_2 \cdots h_t h_1, \dots, h_t h_1 \cdots h_{t-1}, h'_{t+1}, \dots, h'_\ell)\tau$$

with  $\tau = \sigma^t$  and with  $h'_{t+1}, \dots, h'_\ell \in H$ . We note that the elements

$$h_1 h_2 \cdots h_t, h_2 \cdots h_t h_1, \dots, h_t h_1 \cdots h_{t-1}$$

are pairwise conjugate permutations of  $H$ . In particular, replacing  $x$  by a suitable conjugate in  $G$ , we may assume that

$$x = \underbrace{(h, \dots, h)}_{t \text{ times}}, h'_{t+1}, \dots, h'_\ell)\tau$$

with  $h \in H$ . Note that  $\tau$  fixes point-wise the indices  $\{1, \dots, t\}$ . Denote by  $d_i$  the number of cycles of  $h$  of length  $i$ , for  $i \in \{1, \dots, r\}$ . Let  $(\alpha_{1,1}, \alpha_{2,1}, \dots, \alpha_{i,1}), \dots, (\alpha_{1,d_i}, \alpha_{2,d_i}, \dots, \alpha_{i,d_i})$

be the  $d_i$  cycles of length  $i$  of  $h$ . Write

$$X_i = \bigcup_{j=1}^{d_i} \{\alpha_{1,j}, \alpha_{2,j}, \dots, \alpha_{i,j}\}$$

and fix an element  $\bar{\alpha}$  of  $X_i$ . It is easy to check that for each choice  $\beta_1, \dots, \beta_{t-1} \in X_i$ , the point

$$(\bar{\alpha}, \beta_1, \dots, \beta_{t-1}, \underbrace{\bar{\alpha}, \dots, \bar{\alpha}}_{(\ell-t) \text{ times}})$$

is in a distinct cycle of  $x$ . Since  $|X_i| = d_i i$ , we have

$$(4) \quad c_x \geq \sum_{i=1}^r (d_i i)^{t-1}.$$

Recall that  $r = \sum_i d_i i$ . For  $t = 2$ , (3) and (4) imply that  $r \leq 8$ . For  $t \geq 6$ , we have  $a^{t-1} > 4t$  (for  $a \geq 2$ ) and so (3) and (4) are not satisfied. Assume that  $t = 3$ . Now  $a^{t-1} > 4t$  for  $a \geq 4$ . In particular, (3) and (4) are satisfied only if  $d_1 \leq 3$ ,  $d_2 \leq 1$ ,  $d_3 \leq 1$  and  $d_i = 0$  for  $i \geq 4$ . Thus  $r \leq 8$ . Now, with a direct inspection for every possible value of  $r \in \{5, \dots, 8\}$ , we see that (3) and (4) are never satisfied. A similar detailed analysis for  $t = 4$  and  $t = 5$  yields no solutions to (3) and (4).

Summing up, we have  $t = 2$  (so that  $\sigma$  is an involution) and  $r \leq 8$ . If  $\sigma$  has at least two cycles of length 2, then the same argument as above produces at least  $(\sum d_i i)(\sum d'_i i) = r^2$  distinct cycles of  $x$ . This is a contradiction since  $c_x \leq 2c_g \leq 8$  and  $r^2 \geq 25$ . Thus  $\sigma$  is a transposition.

Since  $r$  is bounded by 8, we see from [11, Theorem 1.3] that  $\ell$  is also bounded above by a constant. In fact, using [11, Table 6], we see that  $\ell \leq 3$  if  $r = 5$  or 6, and  $\ell \leq 4$  if  $r = 7$  or  $r = 8$ . Now the proof follows by a computer calculation. In particular, we have  $\ell \leq 3$  and, for  $r \in \{6, 7\}$ , we have  $\ell = 2$ .  $\square$

The following proposition deals with the case where our permutation  $g$  with at most four cycles lies in the base group  $H^\ell$  of  $G$ .

**Proposition 5.3.** *Assume that  $H^\ell$  (for  $\ell \geq 2$ ) contains a permutation  $g = (h_1, \dots, h_\ell)$  having at most four cycles. Then, relabelling the index set  $\{1, \dots, \ell\}$  if necessary, one of the following holds:*

- (i)  $\ell = 2$ ,  $h_1$  and  $h_2$  both have two cycles on  $\Delta$  of lengths  $t_1, r - t_1$  and  $t_2, r - t_2$ , and each of  $t_1, r - t_1$  is relatively prime to each of  $t_2, r - t_2$ ;
- (ii)  $\ell = 2$ ,  $h_1$  is an  $r$ -cycle,  $h_2$  has two cycles on  $\Delta$  of lengths  $t_2, r - t_2$ ; moreover  $\gcd(r, t_2) \leq 2$ ;
- (iii)  $\ell = 2$ ,  $h_1$  is an  $r$ -cycle,  $h_2$  has three cycles on  $\Delta$  of lengths  $t_2, t'_2, r - (t_2 + t'_2)$ , moreover  $\gcd(r, t_2) + \gcd(r, t'_2) + \gcd(r, t_2 + t'_2) \leq 4$ ;
- (iv)  $\ell = 3$ ,  $h_1$  is an  $r$ -cycle,  $h_2$  has two cycles on  $\Delta$  of lengths  $t_2, r - t_2$ , and also  $h_3$  has two cycles on  $\Delta$  of lengths  $t_3, r - t_3$ ; moreover  $r, t_2, r - t_2, t_3, r - t_3$  are pairwise relatively prime;
- (v)  $\ell = 2$ ,  $h_1$  is an  $r$ -cycle,  $h_2$  has four cycles on  $\Delta$  of lengths  $t_2, t'_2, t''_2, r - (t_2 + t'_2 + t''_2)$ ; moreover  $\gcd(r, t_2) = \gcd(r, t'_2) = \gcd(r, t''_2) = \gcd(r, t_2 + t'_2 + t''_2) = 1$ .

*Proof.* Let  $c_g$  be the number of cycles of  $g$  on  $\Omega$  and let  $c_i$  be the number of cycles of  $h_i$  on  $\Delta$ . Replacing  $g$  by a suitable conjugate in  $G$ , we may assume that  $c_1 \leq c_2 \leq \dots \leq c_\ell$ . Clearly,

$$(5) \quad c_g \geq \prod_{i=1}^{\ell} c_i.$$

Assume that  $c_1 \geq 2$ . As  $c_g \leq 4$ , from (5), we deduce that  $\ell = 2$  and  $c_1 = c_2 = 2$ . Write

$$\begin{aligned} h_1 &= (\alpha_1, \dots, \alpha_{t_1})(\alpha_{t_1+1}, \dots, \alpha_r) \\ h_2 &= (\beta_1, \dots, \beta_{t_2})(\beta_{t_2+1}, \dots, \beta_r). \end{aligned}$$

If  $\gcd(t_1, t_2) \geq 2$ , then  $g = (h_1, h_2)$  has at least two orbits on  $\{\alpha_1, \dots, \alpha_{t_1}\} \times \{\beta_1, \dots, \beta_{t_2}\}$  from Lemma 5.1. Thus,  $g$  has at least five orbits on  $\Omega$  (the elements  $(\alpha_{t_1+1}, \beta_1)$ ,  $(\alpha_{t_1+1}, \beta_{t_2+1})$  and  $(\alpha_1, \beta_{t_2+1})$  are in distinct  $g$ -orbits), which is a contradiction. Thus  $t_1$  and  $t_2$  are relatively prime. Similarly, each of  $t_1, r - t_1$  is relatively prime to each of  $t_2, r - t_2$ . This yields part (i).

Assume that  $c_1 = 1$ . Write  $h_1 = (\alpha_1, \dots, \alpha_r)$ . Suppose that  $c_2 = 1$ . From Lemma 5.1, we see that  $(h_1, h_2)$  has  $|\Delta| \geq 5$  orbits on  $\Delta \times \Delta$ , contradicting the fact that  $c_g \leq 4$ . Therefore  $c_2 \geq 2$ . In particular, (5) implies that either  $\ell = 3$  and  $c_2 = c_3 = 2$ , or  $\ell = 2$  and  $2 \leq c_2 \leq 4$ .

Assume that  $\ell = 3$ ,  $c_1 = 1$ ,  $c_2 = c_3 = 2$ . Let  $t_2, r - t_2$  and  $t_3, r - t_3$  be the cycle lengths of  $h_2$  and  $h_3$ . An application of Lemma 5.1 to each of  $(h_1, h_2)$ ,  $(h_1, h_3)$  and  $(h_2, h_3)$  implies that  $r, t_2, r - t_2, t_3, r - t_3$  are relatively prime. This yields part (iv).

Assume that  $\ell = 2$ ,  $c_1 = 1$ ,  $c_2 = 2$ . Let  $t_2, r - t_2$  be the cycle lengths of  $h_2$ . Note that  $\gcd(r, t_2) = \gcd(r, r - t_2)$ . An application of Lemma 5.1 to  $(h_1, h_2)$  implies that  $\gcd(r, t_2) \leq 2$ . This yields part (ii).

The remaining cases ( $c_2 = 3$  and  $c_2 = 4$ ) follow with a similar argument giving rise to parts (iii) and (v).  $\square$

With a slight improvement of Proposition 5.3 we are now able to prove Theorem 1.1.

*Proof of Theorem 1.1.* From [11, Theorem 1.3] (which we restated in Section 1.1) and the discussion that follows our restatement of this result, we have only to consider the case that  $G = \text{Sym}(m) \text{ wr } \text{Sym}(\ell)$  in its product action (of degree  $n = \binom{m}{k}^\ell$ ) on a Cartesian product of  $\ell$  copies of the set of  $k$ -subsets of  $\{1, \dots, m\}$  (with  $1 \leq k < m/2$ ), or that  $G = \text{P}\Gamma\text{L}_d(q) \text{ wr } \text{Sym}(\ell)$  in its product action (of degree  $n = ((q^d - 1)/(q - 1))^\ell$ ) on a Cartesian product of  $\ell$  copies of the point set of the projective space  $\text{P}\Gamma\text{L}_d(q)$ .

Assume that  $\ell = 1$ . If  $G = \text{Sym}(m)$  acting on  $k$ -sets with  $k \geq 2$ , then by Proposition 3.4 and Remark 3.5 we have  $k = 2$  and  $m \leq 9$ . For each of these cases, we list the structure of the permutations having at most four cycles in Table 3. If  $k = 1$ , then we have Line 1 of Table 1. If  $G = \text{P}\Gamma\text{L}_d(q)$ , then the proof follows from Theorem 4.3 and we obtain Lines 1–23 of Table 2.

Now suppose that  $\ell \geq 2$ . Write  $H = \text{Sym}(m)$  or  $H = \text{P}\Gamma\text{L}_d(q)$  depending on which group we are considering. If  $g \notin H^\ell$ , then from Proposition 5.2 we have  $5 \leq r \leq 8$  and  $\ell = 2$  or  $r \in \{5, 8\}$  and  $\ell = 3$ . For each of these cases, the various possibilities for  $\text{soc}(G)$  and  $(n_1, \dots, n_N)$  (depending on whether  $\text{soc}(G) = \text{Alt}(m)^\ell$  or  $\text{soc}(G) = \text{PSL}_d(q)^\ell$ ) are reported in Table 1 and Table 2 (which have been obtained by computations in `magma`). For example the cycle lengths 12, 12, 12 in Line 29 and the cycle lengths 16, 16, 16, 16 in Line 30 of Table 2 arise only from group elements  $g \notin H^\ell$ . Similarly, Lines 7, 8, 9, and 11 of Table 1 arise from group elements  $g \notin H^\ell$ . So from now on we may assume that  $g = (h_1, \dots, h_\ell) \in H^\ell$ .

Assume that  $H = \text{Sym}(m)$ . If  $k > 1$  then there is no  $g$  with four or fewer cycles. This follows at once from Proposition 3.4 and another computation with `magma`. In fact, if  $k > 1$ , then  $m \leq 9$  and also  $\ell \leq 4$  from [11, Table 6]. Thus we only have a finite number of relatively small groups to check. Assume that  $k = 1$ . Now Proposition 5.3 describes the cycles lengths of  $g$  and implies that  $\ell \leq 3$ . If  $g$  satisfies Proposition 5.3 part (i), then  $(n_1, \dots, n_N)$  is in Line 4 of Table 1. If  $g$  satisfies Proposition 5.3 part (ii), then  $(n_1, \dots, n_N)$  is in Line 2 of Table 1 if  $\gcd(r, t_2) = 1$  and in Line 6 of Table 1 if  $\gcd(r, t_2) = 2$  (with  $k_1 = k_2 = t_2/2$  and  $k_3 = k_4 = (r - t_2)/2$ ). If  $g$  satisfies Proposition 5.3 part (iii), then  $(n_1, \dots, n_N)$  is in Line 3 of Table 1 if  $\gcd(r, t_2) = \gcd(r, t'_2) = \gcd(r, t_2 + t'_2) = 1$  and in

Line 5 of Table 1 if  $\gcd(r, t_2) + \gcd(r, t'_2) + \gcd(d, t_2 + t'_2) = 4$ . If  $g$  satisfies Proposition 5.3 part (iv), then  $(n_1, \dots, n_N)$  is in Line 10 of Table 1. Finally, if  $g$  satisfies Proposition 5.3 part (v), then  $(n_1, \dots, n_N)$  is in Line 6 of Table 1.

Now assume that  $H = \text{P}\Gamma\text{L}_d(q)$ . Again,  $g = (h_1, \dots, h_\ell)$  satisfies one of parts (i)–(v) of Proposition 5.3 with  $r = (q^d - 1)/(q - 1)$ . Since  $\text{PSL}_2(4) = \text{Alt}(5)$ , we may assume that  $(d, q) \neq (2, 4)$ . Note that we can use Table 2 for the cycle lengths of the elements  $h_1, \dots, h_\ell$ . Recall when examining the table that we may assume  $r = (q^d - 1)/(q - 1) \geq 5$ .

Assume that  $g = (h_1, h_2)$  satisfies Proposition 5.3 part (i). A careful inspection of Table 2 shows that  $d = 2$  and either  $q$  is prime,  $h_1$  and  $h_2$  have cycle lengths  $1, q$  and  $(q + 1)/2, (q + 1)/2$ , or  $q = 9$  and  $h_1$  and  $h_2$  have cycle lengths  $2, 8$  and  $5, 5$ . In the first case  $(h_1, h_2)$  has cycle lengths  $(q + 1)/2, (q + 1)/2, q(q + 1)/2, q(q + 1)/2$  and this example is in Table 2 Line 27. In the second case,  $(h_1, h_2)$  has cycle lengths  $10, 10, 40, 40$  and this example (simply by an arithmetical coincidence) is in Table 2 Line 25.

Now suppose that  $g = (h_1, h_2)$  satisfies Proposition 5.3 part (ii). A careful inspection of Table 2 shows that  $d = 2$  and either (a)  $q$  is prime and  $h_1$  and  $h_2$  have cycle lengths  $q + 1$  and  $1, q$ , or (b)  $q = 9$  and  $h_1$  and  $h_2$  have cycle lengths  $10$  and  $2, 8$ . In case (a),  $(h_1, h_2)$  has cycle lengths  $q, (q + 1)q$  and this example is in Line 26 of Table 2. In case (b),  $(h_1, h_2)$  has cycle lengths  $10, 10, 40, 40$  and this example is in Line 25 of Table 2 (again by coincidence).

Next, suppose that  $g = (h_1, h_2)$  satisfies Proposition 5.3 part (iii). A careful inspection of Table 2 shows that one of the following holds:

- (1)  $d = d_1 + d_2$ ,  $\gcd(d_1, d_2) = 1$  and  $h_2$  has cycle lengths  $(q^{d_1} - 1)/(q - 1), (q^{d_2} - 1)/(q - 1), (q^{d_1} - 1)(q^{d_2} - 1)/(q - 1)$ ; or
- (2)  $d = 2$ ,  $q = 4$  and  $h_2$  has cycle lengths  $1, 2, 2$ ; or
- (3)  $d = 2$ ,  $q = 9$  and  $h_2$  has cycle lengths  $1, 3, 6$ ; or
- (4)  $d = 2$ ,  $q = 16$  and  $h_2$  has cycle lengths  $1, 8, 8$ , or  $2, 3, 12$ , or  $2, 5, 10$ ; or
- (5)  $d = 3$ ,  $q = 2$  and  $h_2$  has cycle lengths  $1, 2, 4$ .

The examples in Cases (2)–(5) are in Lines 28 31, 32 and 34 of Table 2. We now consider Case 1. Note that  $\gcd((q^d - 1)/(q - 1), (q^{d_i} - 1)/(q - 1)) = 1$  for  $i = 1, 2$ . Also,

$$\gcd\left(\frac{q^d - 1}{q - 1}, \frac{(q^{d_1} - 1)(q^{d_2} - 1)}{q - 1}\right) = \gcd(d, q - 1).$$

In particular, we obtain Line 24 of Table 2 if  $\gcd(d, q - 1) = 1$  and Line 25 of Table 2 if  $\gcd(d, q - 1) = 2$ .

A careful inspection of Table 2 shows that there are no permutations  $h_2, h_3 \in \text{P}\Gamma\text{L}_d(q)$  satisfying all of the requirements of Proposition 5.3 part (iv).

Finally, suppose that  $g = (h_1, h_2)$  satisfies Proposition 5.3 part (v). A careful inspection of Table 2 shows that one of the following holds:

- (1)  $d = d_1 + d_2$ ,  $\gcd(d_1, d_2) = 1$ ,  $d_1, d_2$  and  $q$  are odd,  $h_2$  has cycle lengths  $(q^{d_1} - 1)/(q - 1), (q^{d_2} - 1)/(q - 1), (q^{d_1} - 1)(q^{d_2} - 1)/(2(q - 1)), (q^{d_1} - 1)(q^{d_2} - 1)/(2(q - 1))$ ; or
- (2)  $d = 2$ ,  $q = 9$  and  $h_2$  has cycle lengths  $1, 3, 3, 3$ ; or
- (3)  $d = 2$ ,  $q = 27$  and  $h_2$  has cycle lengths  $1, 9, 9, 9$ ; or
- (4)  $d = 3$ ,  $q = 4$  and  $h_2$  has cycle lengths  $1, 4, 8, 8$ .

The examples in Cases (2)–(4) are in Lines 31, 33 and 35 of Table 2. Arguing in the same way as when  $g$  is as in part (iii) of Proposition 5.3 yields Line 25 of Table 2.  $\square$

## REFERENCES

- [1] D. Berend, Y. Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math. Soc.* **124** (1996), 1663–1671.
- [2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.



- [3] D. Bubboloni, C. E. Praeger, Normal coverings of finite symmetric and alternating groups, *J. Combin. Theory Ser. A* **118** (2011), 2000–2024.
- [4] D. Bubboloni, C. E. Praeger, P. Spiga, Normal coverings and pairwise generation of finite alternating and symmetric groups, *J. Algebra* **390** (2013), 199–215.
- [5] W. Burnside, *Theory of groups of finite order*, 2nd ed. (Cambridge University Press, 1911).
- [6] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics vol. 163 (Springer-Verlag, New York, 1996).
- [7] W. Feit, Some consequences of the classification of finite simple groups. In *The Santa Cruz conference on finite groups*, Proc. Sympos. Pure Math. **37** (American Mathematical Society, 1980), 175–181.
- [8] C. Fuchs, U. Zannier, Composite rational functions expressible with few terms, *J. Eur. Math. Soc.* **14** (2012), 175–208.
- [9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.6.4*; 2013, (<http://www.gap-system.org>).
- [10] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups number 3 part I chapter A. Almost simple K-groups*, Mathematical Surveys and Monographs vol. 40 (American Mathematical Society, Providence, RI, 1998).
- [11] S. Guest, J. Morris, C. E. Praeger, P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, submitted, arXiv:1301.5166 [math.GR]
- [12] S. Guest, J. Morris, C. E. Praeger, P. Spiga, Affine transformations of finite vector spaces with large orders or few cycles, submitted, arXiv:1306.1368 [math.GR]
- [13] G. A. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory* **5** (2002), 403–407.
- [14] M. W. Liebeck, J. Saxl, Primitive permutation groups containing an element of large prime order, *J. London Math. Soc.* **31** (1985), 237–249.
- [15] J. P. McSorley, Cyclic permutations in doubly-transitive groups, *Comm. Algebra* **25** (1997), 33–35.
- [16] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials, *Ann. Scuola Norm. Sup. Pisa* **12** (2013), 369–438.
- [17] P. M. Neumann, Finite permutation groups, edge-coloured graphs and matrices, in: *Topics in group theory and computation* (M. P. J. Curran, ed., Acad. Press, London, 1977), 82–118.
- [18] C. E. Praeger, On elements of prime order in primitive permutation groups, *J. Algebra* **60** (1979), 126–157.

SIMON GUEST, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHAMPTON,  
HIGHFIELD, SO17 1BJ, UNITED KINGDOM  
*E-mail address*: [s.d.guest@soton.ac.uk](mailto:s.d.guest@soton.ac.uk)

JOY MORRIS, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE,  
LETHBRIDGE, AB. T1K 3M4. CANADA  
*E-mail address*: [joy@cs.uleth.ca](mailto:joy@cs.uleth.ca)

CHERYL E. PRAEGER, CENTRE FOR MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF  
MATHEMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA,  
CRAWLEY, WA 6009, AUSTRALIA  
*E-mail address*: [cheryl.praeger@uwa.edu.au](mailto:cheryl.praeger@uwa.edu.au)

PABLO SPIGA, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICOCCA,  
VIA COZZI 53, 20125 MILANO, ITALY  
*E-mail address*: [pablo.spiga@unimib.it](mailto:pablo.spiga@unimib.it)