Journal of Algebra 454 (2016) 233–251

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Finite primitive permutation groups containing a permutation having at most four cycles ☆

Simon Guest [a], Joy Morris [b,*], Cheryl E. Praeger [c,1], Pablo Spiga [d]

[a] *133 Fleet St., London, EC4A 2BB, United Kingdom*
[b] *Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB, T1K 3M4, Canada*
[c] *Centre for Mathematics of Symmetry and Computation, School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia*
[d] *Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca, Via Cozzi 53, 20125 Milano, Italy*

ARTICLE INFO

Article history:
Received 17 May 2015
Available online 5 February 2016
Communicated by Martin Liebeck

MSC:
20B15
20H30

Keywords:
Primitive permutation groups
Conjugacy classes
Cycle structure

ABSTRACT

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

☆ The second author was supported in part by the National Science and Engineering Research Council of Canada Discovery Grant 238552-2011. The third author was supported by the Australian Research Council Federation Fellowship Project FF0776186. The fourth author was supported by a grant from the University of Western Australia, which formed part of the Federation Fellowship Project FF0776186.

* Corresponding author.
E-mail addresses: guest.simon@gmail.com (S. Guest), joy@cs.uleth.ca (J. Morris), cheryl.praeger@uwa.edu.au (C.E. Praeger), pablo.spiga@unimib.it (P. Spiga).
[1] Also affiliated with King Abdulaziz University, Jeddah, Saudi Arabia.

http://dx.doi.org/10.1016/j.jalgebra.2015.12.032
0021-8693/

1. Introduction

In this paper, we are interested in primitive permutation groups containing a permutation that has a small number of cycles (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 [8,14,17]. 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 [18] 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 [18].

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) $(n_1, \ldots, n_N)$ with $N \leq 4$. Then the socle $\mathrm{soc}(G) = T^\ell$ for some simple group T and integer ℓ, and one of the following holds:*

(i) $\mathrm{soc}(G) = \mathrm{Alt}(m)^\ell$ *in its natural product action of degree m^ℓ, with $\ell \leq 3$;*
(ii) $\mathrm{soc}(G) = \mathrm{PSL}_d(q)^\ell$ *in its natural product action of degree $((q^d-1)/(q-1))^\ell$, with $\ell \leq 3$ and $d \geq 2$;*
(iii) *T, ℓ, n and $(n_1, \ldots, n_N)$ are in one of the rows of Tables 3, 4 or 5;*
(iv) *$\mathrm{soc}(G)$ is elementary abelian, and g and G are described in Theorems 1.3 and 1.4 of* [13].

Moreover, Tables 1 and 2 list all of the possible N-tuples $(n_1, \ldots, n_N)$ 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 $\mathrm{Alt}(m)$ the possible cycle lengths depend upon the parity of m, but $\mathrm{Alt}(m)$ is the socle of $\mathrm{Sym}(m)$ and in $\mathrm{Sym}(m)$ 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 pigeonhole 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 [12, Theorem 1.3]. In particular, in order to prove Theorem 1.1 it suffices to investigate which groups in [12, Theorem 1.3] actually contain a permutation with at most four cycles. Comparing Theorem 1.1 with [12, 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 [12, Theorem 1.3] (numbered for reference later in the paper).

Proposition 1.2. *(See Theorem 1.3 in [12].) 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 $\mathrm{soc}(G) = T^\ell$ of G is isomorphic to either*

(i) $\mathrm{Alt}(m)^\ell$ *in its natural product action on a cartesian product of ℓ copies of the set of k-subsets of $\{1, \ldots, m\}$, or to*
(ii) $\mathrm{PSL}_d(q)^\ell$ *in its natural action on a cartesian product of ℓ copies of the set of points or hyperplanes of the projective space $\mathrm{PG}_{d-1}(q)$, or to*
(iii) *an elementary abelian group C_p^ℓ, and G and g are described in [13], or to*
(iv) *one of the groups in [12, Table 2].*

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

For each group G in [12, Table 2], the exact value of ℓ_T is given in [12, Table 6]. In particular, for each of the groups arising from [12, 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 [12, 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 [10] and magma [2], to determine whether or not a given set of permutations of n points generates $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$. 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 $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$. Other theoretical results have also been important in various computer tests. For example the studies in [15,20] 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 $\mathrm{Sym}(m)$ is our main motivation.

Given a finite group G, the normal coverings of G are the families $H_1, \ldots, H_r$ of proper subgroups of G such that each element of G has a conjugate in H_i for some $i \in \{1, \ldots, r\}$. The minimum r is usually denoted by $\gamma(G)$. For $G = \mathrm{Alt}(m)$ or $\mathrm{Sym}(m)$, it is shown in [3] that $a\varphi(m) \leq \gamma(G) \leq bm$ for positive constants a and b (where φ 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 [18]. Here we give a brief account of the relationship between these ostensibly unrelated topics and we refer the interested reader to the introduction of [18] 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 [18].

Table 1
Cycle lengths $(n_1, \ldots, n_N)$ for Theorem 1.1 (i), where $N \leq 4$.

Line	ℓ	Cycle lengths	Remarks
1	1	$n_1, \ldots, n_N$	$n_1 + \ldots + n_N = m$
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	$\frac{k_1 m}{2}$, $\frac{k_1 m}{2}$, 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	k_1m, k_1m, k_2m, k_2m	$m = 2k_1 + 2k_2$ $\gcd(m, 2k_i) = 2$ for $i = 1, 2$
8	2	3, 4, 6, 12 or 1, 8, 8, 8	$m = 5$
9	2	12, 12, 12	$m = 6$
10	2	16, 16, 16, 16	$m = 8$
11	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
12	3	5, 40, 40, 40 or 15, 20, 30, 60	$m = 5$

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 [9] for more details). Given a positive integer ℓ, a *lacunary* rational function (with respect to ℓ) is an expression $f(t) = P(t)/Q(t)$, with $P(t)$ and $Q(t)$ polynomials (not necessarily coprime) having altogether at most ℓ monomials. The main result of [9] 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 $\mathrm{Sym}(m)$ 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 $\mathrm{P\Gamma L}_d(q)$ in its natural action on the points or hyperplanes of the projective space $\mathrm{PG}_{d-1}(q)$ 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. Firstly, in order to avoid much longer tables and duplicates we have

Table 2
Cycle lengths $(n_1, \dots, n_N)$ for Theorem 1.1 (ii), where $N \leq 4$.

Line	ℓ	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	$\equiv 2 \bmod 3$	$\frac{1}{3}\left(\frac{q^d-1}{q-1}\right), \frac{1}{3}\left(\frac{q^d-1}{q-1}\right), \frac{1}{3}\left(\frac{q^d-1}{q-1}\right)$
4	1	$3 \mid d$	$\equiv 1 \bmod 3$	$\frac{1}{3}\left(\frac{q^d-1}{q-1}\right), \frac{1}{3}\left(\frac{q^d-1}{q-1}\right), \frac{1}{3}\left(\frac{q^d-1}{q-1}\right)$
5	1	$4 \mid d$	$\equiv 1 \bmod 4$	$\frac{1}{4}\left(\frac{q^d-1}{q-1}\right), \frac{1}{4}\left(\frac{q^d-1}{q-1}\right), \frac{1}{4}\left(\frac{q^d-1}{q-1}\right), \frac{1}{4}\left(\frac{q^d-1}{q-1}\right)$
6	1	even	$\equiv 3 \bmod 4$	$\frac{1}{4}\left(\frac{q^d-1}{q-1}\right), \frac{1}{4}\left(\frac{q^d-1}{q-1}\right), \frac{1}{4}\left(\frac{q^d-1}{q-1}\right), \frac{1}{4}\left(\frac{q^d-1}{q-1}\right)$
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	$1, 2, 2$, or $1, 4$, or $2, 3$ or $1, 1, 1, 2$
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	3	2	$16, 16, 16, 16$
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	$7, 14, 28$
35	2	3	4	$21, 84, 168, 168$

taken into account the isomorphisms $\mathrm{Alt}(5) \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, $\mathrm{Alt}(6) \cong \mathrm{PSL}_2(9)$, $\mathrm{PSL}_4(2) \cong \mathrm{Alt}(8)$ and $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$. So, for example, the permutation representation of degree 7 of $\mathrm{PSL}_2(7)$ is considered in Table 2 via the natural permutation representation of $\mathrm{PSL}_3(2)$. Analogously, the permutation representation of degree 6 of $\mathrm{PSL}_2(9)$ is in Table 1 via the natural permutation representation of $\mathrm{Alt}(6)$, while that of $\mathrm{Alt}(5) \cong \mathrm{PSL}_2(4)$ of degree 6 is in Table 2 via the natural permutation representation of $\mathrm{PSL}_2(5)$. So, the reader has to take into account these six isomorphisms in order to read our tables accurately.

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

Socle factor	ℓ	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 4
Cycle lengths for Theorem 1.1 (iii) with T sporadic.

Socle factor	ℓ	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 5
Cycle lengths for Theorem 1.1 (iii) with T classical.

Socle factor	ℓ	degree	Cycle lengths
$\mathrm{PSL}_2(8)$	1	28	$(7,7,7,7)$, $(1,9,9,9)$
	1	36	$(9,9,9,9)$
$\mathrm{PSL}_2(11)$	1	11	(11), $(1,5,5)$, $(2,3,6)$
	2	121	$(11,55,55)$, $(22,33,66)$
$\mathrm{PSL}_2(16)$	1	68	$(17,17,17,17)$
$\mathrm{PSL}_2(19)$	1	57	$(19,19,19)$
$\mathrm{PSL}_4(3)$	1	130	$(10,40,40,40)$
$\mathrm{PSU}_3(3)$	1	28	$(7,7,7,7)$, $(1,3,12,12)$, $(4,8,8,8)$
	1	36	$(6,6,12,12)$
$\mathrm{PSU}_3(5)$	1	50	$(5,5,20,20)$
$\mathrm{PSU}_4(3)$	1	112	$(28,28,28,28)$
$\mathrm{PSp}_6(2)$	1	28	$(7,7,7,7)$, $(4,8,8,8)$, $(1,9,9,9)$, $(1,3,12,12)$, $(3,5,5,15)$
	1	36	$(9,9,9,9)$, $(6,6,12,12)$, $(1,5,15,15)$
$\mathrm{PSp}_4(3)$	1	27	$(9,9,9)$, $(3,12,12)$
	1	36	$(9,9,9,9)$, $(6,6,12,12)$
	1	40	$(10,10,10,10)$, $(4,12,12,12)$

Secondly, a group $\mathrm{PSL}_d(q)$ in its natural representation may appear in more than one row of Table 2. For example $\mathrm{PSL}_4(3)$ appears in Lines 1, 2, 6, 7 and 8 (by taking $d_1 = 1$ and $d_2 = 3$) and 22. The permutations of $\mathrm{PGL}_4(3)$ having at most four cycles are obtained by considering the contribution of all of these lines. A similar remark applies to any other group.

3. The action of $\mathrm{Sym}(m)$ on k-sets

The main result of this section is Proposition 3.2, which determines the elements of $\mathrm{Sym}(m)$ having at most four cycles in their action on k-sets; that is, on the set of k-element subsets of $\{1, \dots, m\}$. Throughout this section H denotes $\mathrm{Sym}(m)$ or $\mathrm{Alt}(m)$ in its action on k-sets. Replacing k by $m - k$ if necessary, we may assume that $k \leq m/2$.

Lemma 3.1. *If $k \geq 2$ and H contains a permutation g that has at most four cycles in its action on k-sets, then $m \leq 9$.*

Proof. First suppose that $k = 2$. Let $m_1, m_2, \dots, m_t$ be the cycle lengths of g on $\Omega = \{1, \dots, m\}$. If a cycle of g has length u on Ω, then the 2-subsets whose elements are in this cycle must lie in $\lfloor u/2 \rfloor$ different cycles of g. In addition, there are at least $\binom{t}{2}$ different cycles of g on 2-subsets formed by choosing the elements of a 2-subset from distinct g-cycles on Ω. In total, this means that g has at least

$$\binom{t}{2} + \sum_{i=1}^{t} \left\lfloor \frac{m_i}{2} \right\rfloor \geq \binom{t}{2} + \sum_{i=1}^{t} \frac{m_i - 1}{2} = \binom{t}{2} + \frac{m}{2} - \frac{t}{2} \geq \frac{m-1}{2}$$

cycles in its action on 2-subsets. Therefore $m \leq 9$.

Now suppose that $3 \leq k \leq m/2$. The Livingstone–Wagner Theorem ([16]; see [6] for a short and elegant proof) states that if a group G acts on m points, and $1 \leq k' \leq k \leq m/2$, then the number of orbits on the k-sets is at least the number of orbits on the k'-sets. Thus, taking $k' = 2$, we see by the argument in the previous paragraph that when $m \geq 10$ G has more than four cycles in its action on k-sets. □

The following proposition completes our consideration of the subset actions.

Proposition 3.2. *Let H be $\mathrm{Alt}(m)$ or $\mathrm{Sym}(m)$ in its natural action on the k-subsets of $\{1, \dots, m\}$ with $k \leq m/2$ and $m \geq 5$. Then H, in this action, contains a permutation with at most four cycles if and only if one of (i) $k = 3$ and $m = 6$; or (ii) $k = 2$ and $m \leq 9$; or (iii) $k = 1$. The examples are all listed in Table 1 (if $k = 1$) or Table 3 (for $k = 2, 3$).*

Proof. If $k = 1$ then H certainly contains elements with at most four cycles, as in Line 1 of Table 1. Suppose now that $k \geq 2$ and H contains such an element. Then by Lemma 3.1, $m \leq 9$. If $k \geq 3$ then since $k \leq m/2$, we must have $k = 3$ or 4 and $m \in \{6, 7, 8, 9\}$.

The cases $m = 7, 8, 9$ are eliminated with a straightforward computation, while if $m = 6$ then $k = 3$ and the 5-cycles and 6-cycles in Sym(6) have four cycles on 3-subsets, as in Table 3. Thus we may assume that $k = 2$ and $m \leq 9$. The examples of elements with at most four cycles on 2-subsets for $5 \leq m \leq 9$ precisely those listed in Table 3. □

Remark 3.3. Notice that the action of Sym(6) on 3-sets is imprimitive. This group does contain permutations with at most four cycles (for example a 6-cycle in 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 this action does not appear in our tables.

4. $\mathrm{P\Gamma L}_d(q)$ in its natural action

In this section we study $\mathrm{P\Gamma L}_d(q)$ acting on the points or hyperplanes of the projective space $\mathrm{PG}_{d-1}(q)$ with $d \geq 2$, and we determine the cycle structure of those of its elements with 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 [12, Section 2]).

Notation 4.1. For $g \in \mathrm{PGL}_d(q)$ let $\bar{g}$ be an element of $\mathrm{GL}_d(q)$ projecting to g in $\mathrm{PGL}_d(q)$. The action of the matrix $\bar{g}$ on the d-dimensional vector space $V = \mathbb{F}_q^d$ naturally defines the structure of an $\mathbb{F}_q\langle\bar{g}\rangle$-module on V. For a subspace W of $V = \mathbb{F}_q^d$, we denote by $P(W)$ the set of 1-dimensional subspaces of V contained in W.

First we deal with semilinear elements.

Lemma 4.2. *Let $g \in \mathrm{P\Gamma L}_d(q) \setminus \mathrm{PGL}_d(q)$, with $d \geq 2$. Then g has at most four cycles on the points of $\mathrm{PG}_{d-1}(q)$ if and only if d, q and the cycle lengths of g are as in lines* 10–17, 19–20, 23 *of Table 2.*

Proof. Here $q = p^f$, for a prime p and $f \geq 2$, and $g = x\psi^{-1}$ for some $x \in \mathrm{PGL}_d(q)$ and for some non-trivial field automorphism ψ of order e say, with $e > 1$. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of the finite field $\mathbb{F}_q$. From Lang's theorem [11, Theorem 2.1], there exists a in the algebraic group $\mathrm{PGL}_d(\overline{\mathbb{F}}_q)$ with $x = aa^{-\psi}$. Observe that $(x\psi^{-1})^e = xx^{\psi} \cdots x^{\psi^{e-2}} x^{\psi^{e-1}}$. Write $z = a^{-1}(x\psi^{-1})^e a$. Now,

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

and so z is invariant under the field automorphism ψ of order e. Thus $z \in \mathrm{PGL}_d(q^{1/e})$. By [12, Corollary 2.7] for example, we know that the maximal element order of

$\mathrm{PGL}_d(q^{1/e})$ 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 $\mathrm{P\Gamma L}_d(q) \setminus \mathrm{PGL}_d(q)$ contains a permutation with at most four cycles and we obtain only the cases listed in lines 10–17, 19–20, 23 of Table 2. □

From now on we deal with elements in $\mathrm{PGL}_d(q)$. We use Notation 4.1. First we make an observation about decomposable elements.

Lemma 4.3. *Suppose that $g \in \mathrm{PGL}_d(q)$ has at most four cycles on the points of $P(V)$, and that an element $\bar{g}$ of $\mathrm{GL}_d(q)$ projecting to g in $\mathrm{PGL}_d(q)$ preserves a non-trivial decomposition $V = V_1 \oplus V_2$. Then g has only one cycle on each of $P(V_1)$ and $P(V_2)$, and in particular, g is semisimple.*

Proof. The element $\bar{g}$ in $\mathrm{GL}_d(q)$ can be written as $g_1 g_2 = g_2 g_1$, with $g_i \in \mathrm{GL}(V_i)$ fixing V_{3-i} pointwise, for $i = 1, 2$. We claim that g_i has only one cycle in its action on $P(V_i)$ for $i = 1, 2$. For otherwise, if g_1 had two cycles on $P(V_1)$ say, then g would have two cycles on $P(V_1)$ and at least two cycles on $P(V) \setminus (P(V_1) \cup P(V_2))$. Since g also has at least one cycle on $P(V_2)$, g would have at least five cycles on $P(V)$, which is a contradiction. Thus each g_i has only one cycle on $P(V_i)$, and in particular g is semisimple. □

Next we complete our analysis of the semisimple elements.

Lemma 4.4. *Let $g \in \mathrm{PGL}_d(q)$ have at most four cycles on the points of $P(V)$, and suppose that an element $\bar{g}$ of $\mathrm{GL}_d(q)$ projecting to g in $\mathrm{PGL}_d(q)$ is semisimple. Then d, q and the cycle lengths of g are as in lines 1–8 of Table 2, and there are examples in each case.*

Proof. By Maschke's theorem, $V = V_1 \oplus \cdots \oplus V_t$, where each V_i is an irreducible $\mathbb{F}_q\langle \bar{g} \rangle$-module. If $t \geq 3$, then g would have at least 5 cycles on $P(V)$, since g has at least one cycle 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 $t \leq 2$. In the following note that $|g| \geq (q^d-1)/(4(q-1))$ since g has at most four cycles in $P(V)$.

If $t = 1$, then $\bar{g}$ 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 some $i \leq 4$ 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 $t = 2$. By Lemma 4.3, $\bar{g} \in \mathrm{GL}_d(q)$ can be written as $\bar{g} = g_1g_2 = g_2g_1$, with $g_i \in \mathrm{GL}(V_i)$ trivial on V_{3-i} and transitive on $P(V_i)$, for $i = 1, 2$. Write $d_i = \dim_{\mathbb{F}_q} V_i$ and $a_i = (q^{d_i}-1)/(q-1)$, for $i = 1, 2$. Suppose that $\gcd(d_1, d_2) = e > 1$. Then $\gcd(a_1, a_2) = (q^e-1)/(q-1) \geq 3$. Choose non-zero $v_i \in V_i$ for $i = 1, 2$. Then the 1-spaces $\langle v_1 + v_2^j \rangle$, for $1 \leq j \leq (q^e-1)/(q-1)$, lie in pairwise distinct cycles of g on $P(V)$. This is impossible since g has at most four cycles, and hence $\gcd(d_1, d_2) = 1$ and therefore also $\gcd(a_1, a_2) = 1$.

To study the cycle length of g containing $U := \langle v_1 + v_2 \rangle$, we note that $g^{a_1a_2(q-1)}$ is trivial on $P(V)$. We compute the stabiliser of U in $\langle g \rangle$ as follows: clearly $v_i^{\bar{g}^{a_i}} = \lambda_i v_i$ for some $\lambda_i \in \mathbb{F}_q^*$. Suppose that g^k fixes U. Then both a_1 and a_2 divide k and hence $k = a_1a_2\ell$ for some integer ℓ. Thus

$$(v_1 + v_2)^{\bar{g}^k} = \lambda_1^{a_2\ell} v_1 + \lambda_2^{a_1\ell} v_2 = \lambda_2^{a_1\ell}(\mu^\ell v_1 + v_2), \text{ where } \mu = \frac{\lambda_1^{a_2}}{\lambda_2^{a_1}},$$

and therefore g^k fixes U if and only if $\mu^\ell = 1$. It follows that the cycle length of g containing U is a_1a_2r, where r is the order of μ. In particular, g has one cycle on $P(V) \setminus (P(V_1) \cup P(V_2))$ if and only if μ has order $q-1$. To see that there is an element g with the latter property, let ω be a primitive element of $\mathbb{F}_q$, and let r_1, r_2 be integers such that $r_1a_2 - r_2a_1 = 1$. Set $\lambda_i = \omega^{r_i}$, and note that $\gcd(r_i, a_i) = 1$, for each i. Thus if ω_i is a primitive element of $\mathbb{F}_{q^{d_i}}$ such that $\omega_i^{a_i} = \omega$, then $\omega_i^{r_i}$ has order a_i modulo $\mathbb{F}_q$, and $\omega_i^{r_ia_i} = \lambda_i$. It follows that we may choose $\bar{g}$ to be g_1g_2 with each $g_i \in \mathrm{GL}(V_i)$ transitive on $P(V_i)$ and such that $v_i^{g^{a_i}} = \lambda_i v_i$. Then $\mu = \lambda_1^{a_2}\lambda_2^{-a_1} = \omega^{r_1a_2 - r_2a_1} = \omega$. This element g then has three cycles in $P(V)$ with lengths as in line 7 of Table 2.

Suppose now that g has more than one cycle in $P(V) \setminus (P(V_1) \cup P(V_2))$, so μ has order a proper divisor of $q-1$. Then the g-cycle containing U has length at most $|P(V) \setminus (P(V_1) \cup P(V_2))|/2$, and the same must hold for arbitrary non-zero v_i. Thus g has exactly four cycles in $P(V)$, with two equal length cycles in $P(V) \setminus (P(V_1) \cup P(V_2))$. In particular μ has order $(q-1)/2$ so q is odd. If d_1, d_2 are both odd, then a_1, a_2 are also odd. Thus with r_i as in the previous paragraph, we have $\gcd(2r_i, a_i) = 1$ and $\omega_i^{2r_i}$ has order a_i modulo $\mathbb{F}_q$. If we take $\lambda_i = \omega^{2r_i}$ this time, then $\omega_i^{2r_ia_i} = \lambda_i$. Thus again we can choose $\bar{g} = g_1g_2$ with each $g_i \in \mathrm{GL}(V_i)$ transitive on $P(V_i)$ and such that $v_i^{g^{a_i}} = \lambda_i v_i$, yielding $\mu = \lambda_1^{a_2}\lambda_2^{-a_1} = \omega^{2r_1a_2 - 2r_2a_1} = \omega^2$. This element g then has four cycles in $P(V)$ with lengths as in line 8 of Table 2. On the other hand, if, say, d_1 is even then also a_1 is even. We require the a_1^{th} power of some ω_1^m to be an element of $\mathbb{F}_q^*$ of order $(q-1)/2$, and this

is only possible if m is even. However for m even, ω_1^m cannot have order a_i modulo $\mathbb{F}_q$. So there are no further examples. □

Finally we turn to the non-semisimple elements.

Lemma 4.5. *Let $g \in \mathrm{PGL}_d(q)$ be non-semisimple and have at most four cycles on the points of $P(V)$. Then d, q and the cycle lengths of g are as in lines $9, 10, 12, 18, 21$ or 22 of Table 2, and there are examples in each case.*

Proof. Let $q = p^f$ for a prime p and $f \geq 1$. It follows from Lemma 4.3 that an element $\bar{g} \in \mathrm{GL}_d(q)$ projecting to g in $\mathrm{PGL}_d(q)$ must act indecomposably on V. Then we know, from linear algebra, that the minimal polynomial for $\bar{g}$ on V is of the form $h(t)^r$ for some monic irreducible $h \in \mathbb{F}_q[t]$, and the $\mathbb{F}_q\langle\bar{g}\rangle$-module V is isomorphic to $V = \mathbb{F}_q[t]/(h(t)^r)$, where $\bar{g}$ acts as multiplication by t. With this identification we see that $\bar{g}$ leaves invariant the submodule chain $0 < \mathrm{Ker}(h(\bar{g})) < \mathrm{Ker}(h(\bar{g})^2) < \cdots < \mathrm{Ker}(h(\bar{g})^r) = V$ and since g has at most four cycles in $P(V)$ it follows that $r \leq 4$. Now $d = re$ where $e = \deg(h)$. Since g is not semisimple, we have $r > 1$ and the order of g is $p^s u$ for some $s \geq 1$ and some divisor u of $(q^e - 1)/(q - 1)$. By [12, Proposition 2.6], $s \leq \lceil \log_p r \rceil$, and hence either (i) $s = 1$, or (ii) $p + 1 \leq r \leq 4$ and $s = 2$.

Suppose that $d = 2$. Then $e = 1$, $r = 2$, and g is unipotent. In this case g has a unique fixed point and q/p cycles of length p on $P(V)$, and hence either $q = p$, as in line 9 of Table 2, or $q \in \{4, 9\}$, as in line 10 or 12 of Table 2, respectively. Thus we may assume that $d \geq 3$.

Since g has at most four cycles in $P(V)$, g has order at least $(q^d - 1)/(4(q - 1))$, and hence

$$\frac{q^d - 1}{4(q-1)} \leq \frac{q^e - 1}{q - 1} p^s, \quad \text{whence} \quad \frac{q^d - 1}{q^e - 1} \leq 4p^s.$$

Since $d \geq 3$ and $d = er > e$ we have $q^2 < \frac{q^d - 1}{q^e - 1}$. Then $p^{2f} = q^2 < 4p^s$ which implies that $q = p \in \{2, 3\}, s \in \{1, 2\}$, and a careful checking shows that the displayed inequality holds only for the values of q, s, d, e in Table 6. Analysing individually each of these examples, we find that only $\mathrm{PGL}_3(2)$, $\mathrm{PGL}_4(2)$ and $\mathrm{PGL}_4(3)$ contain an element that is not semisimple and has at most four cycles (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, as shown in the relevant lines of Table 6. □

We summarise our findings from Lemmas 4.2, 4.4, and 4.5.

Corollary 4.6. *The group $\mathrm{P\Gamma L}_d(q)$ contains a permutation g with at most four cycles on the set of points or hyperplanes of $\mathrm{PG}_{d-1}(q)$ if and only if d, q and the cycle lengths of g are as in one of the Lines 1–23 of Table 2.*

Table 6
For proof of Lemma 4.5.

q	s	d	e	Line
2	1	4	2	21
2	1	3	1	none
2	2	3	1	18
2	2	4	1	none
3	1	4	2	22
3	2	3	1	none

5. Primitive groups: almost simple and product action type

In this section we study the groups $G = H \operatorname{wr} \mathrm{Sym}(\ell)$ in their product action on a Cartesian product $\Omega = \Delta^\ell$ of ℓ copies of a set Δ, with degree $n = |\Delta|^\ell = r^\ell$, where H, Δ, r are one of:

$$H = \mathrm{Sym}(m) \quad \text{where } \Delta = \text{set of } k\text{-subsets of } \{1, \dots, m\}, \qquad \text{and} \quad r = \binom{m}{k}, \quad \text{or}$$

$$H = \mathrm{P\Gamma L}_d(q) \quad \text{where } \Delta = \text{set of points of } \mathrm{PG}_{d-1}(q), \qquad \text{and} \quad r = \frac{q^d - 1}{q - 1}. \tag{1}$$

Here $1 \le k < m/2$, $d \ge 2$, and $\ell \ge 1$. Now H is almost simple, so $m \ge 5$, and if $d = 2$ then $q \ge 4$. In particular $r \ge 5$. Moreover, we do not require that $\ell \ge 2$ and so we deal simultaneously with primitive groups of almost simple and product action type. Note that in the case of $H = \mathrm{P\Gamma L}_d(q)$, the actions of H on points and hyperplanes of $\mathrm{PG}_{d-1}(q)$ are permutationally isomorphic so it is sufficient to consider the action on points.

Let $\mathrm{soc}(A)$ denote the socle of a group A, and in particular write $T := \mathrm{soc}(H)$. Then $\mathrm{soc}(G) = T^\ell$ is either $\mathrm{Alt}(m)^\ell$ or $\mathrm{PSL}_d(q)^\ell$. We write the elements $g \in G$ as $(h_1, \dots, h_\ell)\sigma$, with $h_1, \dots, h_\ell \in H$ and $\sigma \in \mathrm{Sym}(\ell)$. We start with a basic lemma that will be used repeatedly in the sequel. For an element g acting on a set Ω, let $c_g(\Omega)$ denote the number of g-cycles in Ω (including g-cycles of length 1).

Lemma 5.1. *Let $t \ge 2$. For $i = 1, \dots, t$, let Σ_i be a finite set, let $h_i \in \mathrm{Sym}(\Sigma_i)$, and let $g = (h_1, \dots, h_t) \in \mathrm{Sym}(\Sigma_1) \times \cdots \times \mathrm{Sym}(\Sigma_t)$ in its product action on $\Sigma_1 \times \cdots \times \Sigma_t$.*

(a) *If $t = 2$, and each h_i has just one cycle on Σ_i, then $c_g(\Sigma_1 \times \Sigma_2) = \gcd(|\Sigma_1|, |\Sigma_2|)$, and moreover each g-cycle has the same length $\mathrm{lcm}\{|\Sigma_1|, |\Sigma_2|\}$.*
(b) *If, for each i, the support sets of the h_i-cycles in Σ_i are $\Delta_{i1}, \dots, \Delta_{iu_i}$, then $c_g(\Sigma_1 \times \cdots \times \Sigma_t) = \sum_{i_1, \dots, i_t} c_g(\Delta_{1i_1} \times \cdots \times \Delta_{ti_t}) \ge u_1 \dots u_t$.*
(c) *If h_i has just one cycle on Σ_i, for each i, (and t is arbitrary), then each g-cycle in $\Sigma_1 \times \cdots \times \Sigma_t$ has the same length, namely $\mathrm{lcm}\{|\Sigma_1|, \dots, |\Sigma_t|\}$. Moreover, if in addition $C := c_g(\Sigma_1 \times \cdots \times \Sigma_t) \le 4$ then, relabelling the $n_i := |\Sigma_i|$ if necessary, one*

Table 7
For Lemma 5.1.

C	Conditions		
1			$n_1, n_2, \dots, n_t$ pairwise coprime
2	$2 \mid n_i \Leftrightarrow i \leq 2$,	$4 \nmid n_1$,	$n_1/2, n_2, \dots, n_t$ pairwise coprime
3	$3 \mid n_i \Leftrightarrow i \leq 2$,	$9 \nmid n_1$,	$n_1/3, n_2, \dots, n_t$ pairwise coprime
4	$4 \mid n_i \Leftrightarrow i \leq 2$,	$8 \nmid n_1$,	$n_1/4, n_2, \dots, n_t$ pairwise coprime
4	$2 \mid n_i \Leftrightarrow i \leq 3$,	$4 \nmid n_1, n_2$,	$n_1/2, n_2/2, n_3, \dots, n_t$ pairwise coprime

of the lines of Table 7 holds. In particular, if $C \leq 4$ and all the n_i are equal, then (t, n_1, C) is one of $(2,2,2), (2,3,3), (2,4,4)$, or $(3,2,4)$.

(d) *If for each i, h_i has at least u cycles of length j in Σ_i, then g has at least $u^t j^{t-1}$ cycles of length j in $\Sigma_1 \times \cdots \times \Sigma_t$.*

Proof. Part (a) is proved in [19, Lemma 3, page 92], or see [7, 3.2.19]. For part (b), note that $\Sigma_1 \times \cdots \times \Sigma_t$ is the disjoint union of the g-invariant subsets $\Delta_{1i_1} \times \cdots \times \Delta_{ti_t}$, where $1 \leq i_j \leq u_j$ for each j.

(c) For $t = 2$ the first assertion of part (c) is given by part (a). Assume inductively that $t \geq 3$ and the assertion is true for cartesian products of $t-1$ cycles. Write $\Sigma_2' := \Sigma_2 \times \cdots \times \Sigma_t$. By induction, each $(h_2, \dots, h_t)$-cycle in Σ_2' has length $\ell := \operatorname{lcm}\{n_2, \dots, n_t\}$, and by part (b), $C := c_g(\Sigma_1 \times \cdots \times \Sigma_t)$ is equal to $(\prod_{i=2}^t n_i)/\ell$ times $c_g(\Sigma_1 \times \Delta)$, where Δ is one of the $(h_2, \dots, h_t)$-cycles in Σ_2' (of length ℓ). Finally by part (a), each g-cycle in $\Sigma_1 \times \Delta$ has length $\operatorname{lcm}\{n_1, \ell\} = \operatorname{lcm}\{n_1, n_2, \dots, n_t\}$. Hence each g-cycle in $\Sigma_1 \times \cdots \times \Sigma_t$ has length $\operatorname{lcm}\{n_1, n_2, \dots, n_t\}$, and the first assertion is proved by induction. Now if $C \leq 4$, that is, if $\prod_{i=1}^t n_i \leq 4 \cdot \operatorname{lcm}\{n_1, n_2, \dots, n_t\}$, then it is straightforward to check that exactly one of the lines of Table 7 holds. The last assertion follows immediately.

(d) We prove part (d) by induction on t. If $t = 2$, then by part (b), $c_g(\Sigma_1 \times \Sigma_2) \geq u^2 c_g(\Delta_1 \times \Delta_2)$, where, for $i = 1, 2$, Δ_i is the support set of an h_i-cycle of length j. Then it follows from part (a) that g has j cycles of length j in $\Delta_1 \times \Delta_2$. This proves part (c) for $t = 2$. Now assume that $t \geq 3$ and that part (c) is true for $t-1$. Then by induction, $(h_2, \dots, h_t)$ has at least $u^{t-1} j^{t-2}$ cycles of length j in $\Sigma_2 \times \cdots \times \Sigma_t$. A further application of parts (a) and (b) yields that g has at least $u(u^{t-1} j^{t-2})j = u^t j^{t-1}$ cycles of length j in $\Sigma_1 \times \cdots \times \Sigma_t$. □

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 $y \in H^\ell$, $\sigma \in \operatorname{Sym}(\ell)$ and $\sigma \neq 1$. Then σ 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 σ. Relabelling the index set $\{1, \dots, \ell\}$ if necessary, we may assume that $(1, \dots, t)$ is a cycle of σ. Then $\tau = \sigma^t$ fixes each of $1, \dots, t$, and the element $x := g^t$ has the form

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

for some $h'_{t+1}, \ldots, h'_\ell \in H$. Now x induces a product action on the Cartesian product $\Omega' := \Delta^t$ of the first t copies of Δ as the element

$$x' := (x_1, \ldots, x_t) = (h_1 h_2 \cdots h_t,\ h_2 \cdots h_t h_1,\ \ldots,\ h_t h_1 \cdots h_{t-1}) \in H^t$$

We note that the entries $x_1, x_2 = x_1^{h_1}, \ldots, x_t = x_{t-1}^{h_{t-1}}$ are pairwise conjugate elements of H. Thus, replacing x by a suitable conjugate in G, we may assume that $x_1 = x_2 = \cdots = x_t = h$, say. Since $x = g^t$, it follows that $c_g(\Omega) \geq \lceil c_x(\Omega)/t \rceil$, and from the definition of x' that $c_{x'}(\Omega') \leq c_x(\Omega)$. Thus

$$c_{x'}(\Omega') \leq 4t. \tag{2}$$

Denote by d_i the number of h-cycles in Δ of length i, for $i \in \{1, \ldots, r\}$, so $c_h(\Delta) = \sum_i d_i$. By Lemma 5.1 (b), we have $4t \geq c_{x'}(\Omega') \geq c_h(\Delta)^t$, and this implies that either (i) $c_h(\Delta) = 1$, or (ii) $c_h(\Delta) = 2$ with $t \leq 4$.

Claim: $t = 2$ and $r \leq 8$. If $c_h(\Delta) = 1$, then by Lemma 5.1 (c), each x'-cycle in Ω' has length r so $c_{x'}(\Omega') = r^{t-1} \geq 5^{t-1}$. Then it follows from (2) that $t = 2$ and $r \leq 8$. In the other case (ii), we have $c_h(\Delta) = 2$ and $t \leq 4$. Let the h-cycle lengths in Δ be $j, r-j$, where $j \geq r/2$. If $j = r/2$, then an application of Lemma 5.1 (b) and (c) yields a contradiction. So $j \neq r - j$. We obtain a lower bound for $c_{x'}(\Omega')$ using Lemma 5.1 (b) and (c): for all except two of the summands in part (b) we use a lower bound of 1, and for the remaining summands where the Δ_{ki_k} have constant length (either j or $r-j$), we use part (c) to obtain $4t \geq c_{x'}(\Omega') \geq 2^t - 2 + j^{t-1} + (r-j)^{t-1}$. This implies that $t = 2$ and $r \in \{5, 6\}$. The Claim is proved.

Since $t = 2$, the element σ is an involution. If σ has at least two cycles of length 2, say $(1, 2)$ and $(3, 4)$, then $x = g^2$ induces a product action on the Cartesian product Ω'' of the first four copies of Δ as an element $x'' \in H^4$, and arguing as above we may assume that $x'' = (h', h', h'', h'')$, and we have $c_{x''}(\Omega'') \leq c_x(\Omega) \leq 4t = 8$. By Lemma 5.1 (b), at least one, say h' has just one cycle in Δ and h'' has at most two cycles. If also $c_{h''}(\Delta) = 1$ then Lemma 5.1 (d) yields the contradiction $8 \geq r^3$, while if $c_{h''}(\Delta) = 2$ then Lemma 5.1 (b) and (c) imply $8 \geq 4c_{(h',h')}(\Delta^2) \geq 4r$, again a contradiction. Thus σ is a transposition.

Since r is bounded by 8, we see from [12, Theorem 1.3] that ℓ is also bounded above by a constant. In fact, using [12, 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 $\ell = 2$. □

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

Table 8
Cycle lengths for Proposition 5.3.

Line	ℓ	h_1-cycle lengths	h_2-cycle lengths	h_3-cycle lengths	Conditions
1	2	$t_1, r-t_1$	$t_2, r-t_2$	–	$\gcd(t_1,t_2)=\gcd(r-t_1,r-t_2)$ $=\gcd(r-t_1,t_2)=\gcd(t_1,r-t_2)=1$
2	2	r	$t_2, r-t_2$	–	$\gcd(r,t_2)\leq 2$
3	2	r	$t_2, t_2', r-t_2-t_2'$	–	$\gcd(r,t_2)+\gcd(r,t_2')+\gcd(r,t_2+t_2')\leq 4$
4	2	r	t_2, t_2', t_2'', t_2''' $r=t_2+t_2'+t_2''+t_2'''$	–	$\gcd(r,t_2)=\gcd(r,t_2')=\gcd(r,t_2'')$ $=\gcd(r,t_2''')=1$
5	3	r	$t_2, r-t_2$	$t_3, r-t_3$	$r, t_2, r-t_2, t_3, r-t_3$ pairwise coprime

Proposition 5.3. *Assume that H^ℓ (for $\ell \geq 2$) contains a permutation $g = (h_1, \ldots, h_\ell)$ having at most four cycles. Then, relabelling the index set $\{1, \ldots, \ell\}$ if necessary, one of the Lines of Table 8 holds.*

Proof. Set $c_i = c_{h_i}(\Delta)$, for each i, and replace g by a suitable conjugate in G if necessary so that $c_1 \leq c_2 \leq \cdots \leq c_\ell$. By Lemma 5.1(b), $c_g(\Omega) \geq \prod_{i=1}^{\ell} c_i$. If $c_1 \geq 2$ then the only possibility is $\ell = 2$ and $c_1 = c_2 = 2$. Thus the h_i-cycle lengths are as in Line 1 of Table 8, for some t_1, t_2. It follows further from Lemma 5.1 (a) and (b) that the Conditions for Line 1 must also hold. Thus we may assume that $c_1 = 1$, so h_1 is an r-cycle. If also $c_2 = 1$ then by Lemma 5.1 (c), we would have $c_g(\Omega) \geq r \geq 5$, which is a contradiction. Hence $c_i \geq 2$ for $i \geq 2$, and since $c_g(\Omega) \geq \prod_{i=1}^{\ell} c_i$, we see that either $\ell = 3$ and $c_2 = c_3 = 2$, or $\ell = 2$ and $2 \leq c_2 \leq 4$. Thus the h_i-cycle lengths are as in one of the Lines 2–5 of Table 8, and we must verify the conditions.

First consider Line 5 (where $\ell = 3$). By Lemma 5.1 (b) and (c), $c_g(\Omega)$ is a sum of 4 terms, each satisfying Line 1 of Table 7, and hence $r, t_2, r-t_2, t_3, r-t_3$ are pairwise prime. Thus we may assume further that $\ell = 2$. By Lemma 5.1 (b) and (c), $c_g(\Omega)$ is a sum of c_2 terms. If $c_2 = 4$ then each of these terms must satisfy Line 1 of Table 7, yielding the conditions in Line 4 of Table 8. If $c_2 = 2$ (Line 2 of Table 8), note that $\gcd(r, t_2) = \gcd(r, r-t_2)$. By Lemma 5.1 (a) and (b), $\gcd(r, t_2) \leq 2$, as required. Finally if $c_2 = 3$, then at least two of the three summands for $c_g(\Omega)$ satisfy Line 1 of Table 7, and the third summand might satisfy Line 2 of Table 7: thus the Condition of Line 3 of Table 8 holds. □

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

Proof of Theorem 1.1. From Proposition 1.2 and the discussion following it, we have only to consider the case where $G = H \operatorname{wr} \mathrm{Sym}(\ell)$ in its product action on a Cartesian product $\Omega = \Delta^\ell$ of ℓ copies of a set Δ, with degree $n = |\Delta|^\ell = r^\ell$, where H, Δ, r are one of the two possibilities in (1). Suppose that $g = (h_1, \ldots, h_\ell)\sigma \in G$ has cycle lengths $n_1, \ldots, n_N$ $(N \leq 4)$.

Assume that $\ell = 1$. If $G = \mathrm{Sym}(m)$ acting on k-sets with $k \geq 1$, then by Proposition 3.2 and Remark 3.3 either $k = 1$, or $k = 2$ with $m \leq 9$, and the structures of the

permutations having at most four cycles are listed in Table 3. If $G = \mathrm{P\Gamma L}_d(q)$, then the proof follows from Corollary 4.6 and we obtain Lines 1–23 of Table 2.

Now suppose that $\ell \geq 2$. If $g \notin H^\ell$, then from Proposition 5.2 we have either $\ell = 2$ with $5 \leq r \leq 8$, or $\ell = 3$ with $r \in \{5, 8\}$. For each of these cases, the various possibilities for $\mathrm{soc}(G)$ and cycle lengths $n_1, \ldots, n_N$ are reported in Table 1 and Table 2, depending on whether $\mathrm{soc}(G) = \mathrm{Alt}(m)^\ell$ or $\mathrm{soc}(G) = \mathrm{PSL}_d(q)^\ell$; this information was obtained and verified 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 8, 9, 10, and 12 of Table 1 arise from group elements $g \notin H^\ell$.

So from now on we may assume that $g = (h_1, \ldots, h_\ell) \in H^\ell$. In particular, by Proposition 5.3, ℓ is 2 or 3, and ℓ and the h_i-cycle lengths are as in one of the Lines of Table 8. In what follows we use Lemma 5.1 without explicit mention.

Assume that $H = \mathrm{Sym}(m)$ with $r = \binom{m}{k}$. If $k > 1$, then $k = 2$ and $m \leq 9$ by Proposition 3.2 and Remark 3.3. Thus we only have a finite number of relatively small groups to check. A computation with `magma` shows that there is no g with four or fewer cycles. Assume that $k = 1$, so $r = m$. The elements in Line 1 of Table 8 yield g-cycle lengths as in Line 4 of Table 1. The elements in Line 2 of Table 8 yield g-cycle lengths as in Line 2 of Table 1 if $\gcd(r, t_2) = 1$ or Line 7 of Table 1 if $\gcd(r, t_2) = 2$ (with $k_1 = t_2/2$ and $k_2 = (r - t_2)/2$). The elements in Line 3 of Table 8 yield g-cycle lengths as in Line 3 of Table 1 if $\gcd(r, t_2) = \gcd(r, t_2') = \gcd(r, t_2 + t_2') = 1$, or Line 5 of Table 1 if $\gcd(r, t_2) + \gcd(r, t_2') + \gcd(d, t_2 + t_2') = 4$. Finally, the elements in Line 4 or 5 of Table 8 yield g-cycle lengths as in Line 6 or Line 11 of Table 1, respectively.

Now assume that $H = \mathrm{P\Gamma L}_d(q)$ with $r = (q^d - 1)/(q - 1)$. Since $\mathrm{PSL}_2(4) = \mathrm{Alt}(5)$, we may assume that $(d, q) \neq (2, 4)$. Note that ℓ is 2 or 3, we can use Table 2 for the cycle lengths of the elements $h_1, \ldots, h_\ell$, and moreover one of the Lines of Table 8 holds. Recall when examining Table 2 that we may assume $r = (q^d - 1)/(q - 1) \geq 5$.

If Line 1 of Table 1 holds, then 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 $(q+1)/2, (q+1)/2, q(q+1)/2, q(q+1)/2$ as 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 Line 2 of Table 1 holds. A careful inspection of Table 2 shows that $d = 2$, h_1 is a $(q+1)$-cycle, and either (a) q is prime and h_2 has cycle lengths $1, q$, or (b) $q = 9$ and h_2 has cycle lengths $2, 8$. In case (a), (h_1, h_2) has cycle lengths $q, q(q + 1)$ as in Line 26 of Table 2. In case (b), (h_1, h_2) has cycle lengths $10, 10, 40, 40$ as in Line 25 of Table 2 (again by coincidence).

Next, suppose that Line 3 of Table 1 holds, so that h_1 is an r-cycle. 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 $1, 2, 4$.

Cases (2)–(5) lead to examples in Lines 28 31, 32 and 34 of Table 2. For Case (1),

$$\gcd(\frac{q^d-1}{q-1}, \frac{q^{d_i}-1}{q-1}) = 1 \text{ for } i = 1, 2, \text{ and}$$
$$\gcd\left(\frac{q^d-1}{q-1}, \frac{(q^{d_1}-1)(q^{d_2}-1)}{q-1}\right) = \gcd(d, q-1).$$

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

Now suppose that Line 4 of Table 1 holds, so again h_1 is an r-cycle. 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 $1, 4, 8, 8$.

Cases (2)–(4) lead to examples in Lines 31, 33 and 35 of Table 2. Arguing in the same way as for Line 3 of Table 8 yields Line 25 of Table 2.

Finally, a careful inspection of Table 2 shows that there are no permutations $h_2, h_3 \in \mathrm{P\Gamma L}_d(q)$ satisfying all of the requirements of Line 5 of Table 1. □

Acknowledgment

We are grateful to an anonymous referee for extensive and very helpful suggestions of approaches that simplified several of the proofs, and encouraged us to simplify several more of them. We hope that this has significantly improved the exposition.

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] P.J. Cameron, Transitivity of permutation groups on unordered sets, Math. Z. 148 (1976) 127–139.
[7] J.D. Dixon, B. Mortimer, Permutation Groups, Grad. Texts in Math., vol. 163, Springer-Verlag, New York, 1996.
[8] W. Feit, Some consequences of the classification of finite simple groups, in: The Santa Cruz Conference on Finite Groups, in: Proc. Sympos. Pure Math., vol. 37, American Mathematical Society, 1980, pp. 175–181.
[9] C. Fuchs, U. Zannier, Composite rational functions expressible with few terms, J. Eur. Math. Soc. (JEMS) 14 (2012) 175–208.
[10] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.4, http://www.gap-system.org, 2013.
[11] D. Gorenstein, R. Lyons, R. Solomon, The Classification of the Finite Simple Groups Number 3 Part I Chapter A. Almost Simple K-Groups, Math. Surveys Monogr., vol. 40, American Mathematical Society, Providence, RI, 1998.
[12] S. Guest, J. Morris, C.E. Praeger, P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, Trans. Amer. Math. Soc. 367 (2015) 7665–7694.
[13] S. Guest, J. Morris, C.E. Praeger, P. Spiga, Affine transformations of finite vector spaces with large orders or few cycles, J. Pure Appl. Algebra 219 (2015) 308–330.
[14] G.A. Jones, Cyclic regular subgroups of primitive permutation groups, J. Group Theory 5 (2002) 403–407.
[15] M.W. Liebeck, J. Saxl, Primitive permutation groups containing an element of large prime order, J. Lond. Math. Soc. 31 (1985) 237–249.
[16] D. Livingstone, A. Wagner, Transitivity of finite permutation groups on unordered sets, Math. Z. 90 (1965) 393–403.
[17] J.P. McSorley, Cyclic permutations in doubly-transitive groups, Comm. Algebra 25 (1997) 33–35.
[18] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials, Ann. Sc. Norm. Super. Pisa Cl. Sci. 12 (2013) 369–438.
[19] P.M. Neumann, Finite permutation groups, edge-coloured graphs and matrices, in: M.P.J. Curran (Ed.), Topics in Group Theory and Computation, Acad. Press, London, 1977, pp. 82–118.
[20] C.E. Praeger, On elements of prime order in primitive permutation groups, J. Algebra 60 (1979) 126–157.