Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Affine transformations of finite vector spaces with large orders or few cycles

Simon Guest, Joy Morris, Cheryl E. Praeger and Pablo Spiga

Abstract

Let V be a d-dimensional vector space over a field of prime order p. We classify the affine transformations of V of order at least $p^d/4$, and apply this classification to determine the finite primitive permutation groups of affine type, and of degree n, that contain a permutation of order at least $n/4$. Using this result we obtain a classification of finite primitive permutation groups of affine type containing a permutation with at most four cycles.

1. *Introduction*

That permutations of a set of size n can have order as great as $e^{(1+o(1))(n\log n)^{1/2}}$ was shown by Edmund Landau [**17**, **18**] in 1903. However many of these large ordered permutations do not belong to proper primitive subgroups of $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$. Indeed, in [**8**] it was shown that the primitive permutation groups on n points having a nonabelian socle, and containing a permutation of order at least $n/4$, are very restricted, with the natural actions of alternating groups $\mathrm{Alt}(r)$ on subsets, and projective groups $\mathrm{PSL}_r(q)$ on points or hyperplanes playing a special role: the socle of each such group is $\mathrm{Alt}(r)^\ell$ or $\mathrm{PSL}_r(q)^\ell$ acting on ℓ-tuples of subsets, points or hyperplanes. The case of primitive groups with an abelian socle was not treated in [**8**]. These primitive groups are groups of affine transformations of finite vector spaces, where the point set is the vector space itself.

The first aim of this paper is to determine the affine transformations of a vector space of size n which have order at least $n/4$, and the affine primitive groups in which they lie. Each affine transformation g of a finite vector space V has the form $g = t_v h$, with $t_v : x \mapsto x + v$ a translation, for some $v \in V$, and with $h \in \mathrm{GL}(V)$, where t_v is performed first followed by h.

Theorem 1.1. *Let V be a d-dimensional vector space over a field $\mathbb{F}_p$ of prime order p, and let $g = t_v h$ be an affine transformation of V with order at least $p^d/4$. Then g and h appear in one of the Tables* 2, 3, 4.

Remark 1. We note that each of the examples g in Tables 2, 3, 4 have order at least $p^d/4$ when p is odd. This is clear from the expressions for the orders of the elements in the tables. However there are a few instances where this is not the case when $p = 2$, so Theorem 1.1 is not in fact an 'if and only if' statement for $p = 2$. For example in line 12 of Table 3, when $(d, d_1, d_2, d_3, d_4) = (12, 2, 2, 3, 5)$, the element order is $|g| = (2^2 - 1)(2^3 - 1)(2^5 - 1) = 651 < 2^d/4 = 1024$.

2000 *Mathematics Subject Classification* 20B15, 20H30.

The second author is supported in part by the National Science and Engineering Research Council of Canada. This work forms part of Australian Research Council Project DP130100106 of the third author.

Theorem 1.2 in conjunction with the results in [**8**] gives a complete classification of all finite primitive groups of degree n containing elements of order at least $n/4$. The group of affine transformations of V is denoted $\mathrm{AGL}(V)$ and is called the affine general linear group of V. It is a semidirect product $T \cdot \mathrm{GL}(V)$, where T is the group of translations and $\mathrm{GL}(V)$ is the group of invertible linear transformations of V. Finite primitive groups of *affine type* are the subgroups of $\mathrm{AGL}(V)$, for some V, of the form $G = T \cdot G_0$, where $G_0 = G \cap \mathrm{GL}(V)$ acts irreducibly on V. For $V = \mathbb{F}_p^d$ with $d = 1$, each transitive subgroup of $\mathrm{AGL}(V)$ contains translations of order p, so all such groups are examples. Theorem 1.2 classifies the examples with $d \geq 2$.

THEOREM 1.2. *Let $G = T \cdot G_0 \leq \mathrm{AGL}(V)$ be an affine primitive group on V of degree p^d, where p is prime and $d \geq 2$. If G contains a permutation g of order at least $p^d/4$, then one of the following holds for G_0:*
(1) $\mathrm{SL}_{d/r}(p^r) \leq G_0 \leq \Gamma\mathrm{L}_{d/r}(p^r)$ *for some $r \mid d$ with $1 \leq r < d$;*
(2) $G_0 \leq \Gamma\mathrm{L}_1(p^d)$ *with* $[\mathrm{GL}_1(p^d) : G_0 \cap \mathrm{GL}_1(p^d)] \leq 3$*;*
(3) $G_0 \leq \mathrm{GL}_{d/r}(p) \operatorname{wr} \mathrm{Sym}(r)$ *for some $r \mid d$ with $1 < r \leq d$, and additionally, one of:*
  (i) $p = 2$, *and* $d = r \leq 5$, *or* $d = 2r \leq 6$, *or* $d \geq 3r$ *and* $4r^2 - 21r \leq d$,
  (ii) $p = 3$, *and* $d = r \leq 3$, *or* $r = 2$,
  (iii) $p \geq 5$ *and* $d = r = 2$*;*
(4) $p = 2$ *and* $d \leq 6$, *or* $p = 3$ *and* $d \leq 4$, *or* $d = 2$ *and* $p \leq 13$, *and G_0 is in Table* 1.

REMARK 2. We note that in case (3) the image of g in $\mathrm{Sym}(r)$ is trivial in most cases. We prove this in Lemma 5.1 where we also find the exact values where g has a possibly non-trivial image in $\mathrm{Sym}(r)$. Case (3) (i) does not always occur; a necessary condition for existence is for such a group to contain an element in one of the lines 7–18 of Table 3, or $d \leq 5$. The function $4r^2 - 21r$ in case (3) (i) is not the best possible lower bound of d and for a refined version we refer to Remark 4.

Since the order of a permutation is equal to the least common multiple of the cycle lengths in its disjoint cycle representation, permutations with a bounded number of cycles have orders which grow at least linearly with the degree n: if a permutation has c cycles, then one of its cycles has length at least n/c, and hence its order is at least n/c. Of course the converse is not true: permutations with order at least $n/4$ can have as many as $3n/4$ cycles of length 1. We apply our classification of affine transformations of order at least $n/4$ to determine all affine transformations which have at most 4 cycles, as well as the affine primitive groups which contain such elements.

THEOREM 1.3. *Let V be a d-dimensional vector space over a field $\mathbb{F}_p$ of prime order p, and let $g = t_v h$ be an affine transformation of V with at most four cycles in its action on V. Then g appears in one of the Tables* 5, 6, 7.

THEOREM 1.4. *Let $G = T \cdot G_0 \leq \mathrm{AGL}(V)$ be an affine primitive group on V of degree p^d, where p is prime and $d \geq 2$. If G contains a permutation with at most four cycles, then one of the following holds:*
(1) $\mathrm{SL}_{d/r}(p^r) \leq G_0 \leq \Gamma\mathrm{L}_{d/r}(p^r)$ *where r divides d and $1 \leq r \leq d$. Moreover, G_0 contains $s_{d/r}^i$, where $1 \leq i \leq 3$ and $s_{d/r}$ denotes a Singer cycle in $\mathrm{GL}_{d/r}(p^r)$;*
(2) $G_0 \leq \mathrm{GL}_{d/r} \operatorname{wr} \mathrm{Sym}(r)$ *for some $r \mid d$ with $r > 1$ and*
  (i) $p = 2$ *and* $r = 2$, *or* $d = r \leq 5$, *or* $(d, r) = (6, 3)$,
  (ii) $p = 3$ *and* $d = r \leq 3$,

(iii) $p \geq 5$ *and* $d = r = 2$*;*
(3) G_0 *is contained in one of the rows of Table* 1 *with a 'y' in the fourth column.*

Bamberg and Penttila [**4**] have obtained a very detailed classification of the groups satisfying part (1). The classification in Theorem 1.4 could be refined taking into account the results of [**4**].

In [**9**], we build on these results to classify all finite primitive groups containing elements with at most four cycles. These results have various applications; in particular to normal coverings of a group and to the study of monodromy groups of Siegel functions. We refer the reader to [**9**] for more details and also to [**21**], where the finite primitive groups that contain a permutation with at most two cycles are classified.

The choice of "$p^d/4$" in Theorems 1.1 and 1.2 and of "four" in Theorems 1.3 and 1.4 is to some extent arbitrary. On the one hand it allows a list of exceptions that is not too cumbersome to use and, on the other hand, it will be strong enough to determine in the forthcoming paper [**5**] the first sharp bound on the normal covering number of $\mathrm{Sym}(n)$.

d	p	G_0	G contains a permutation with at most four cycles?
4	2	$\mathrm{Alt}(5)$ or $\mathrm{Sym}(5)$	y
4	2	$\mathrm{Alt}(6)$ or $\mathrm{Sym}(6) \cong \mathrm{Sp}_4(2)$	y
4	2	$\mathrm{Alt}(7)$	y
6	2	$\mathrm{Sp}_6(2)$	y
6	2	$\mathrm{Sym}(8) \cong \mathrm{GO}_6^+(2)$ or $\mathrm{GO}_6^-(2)$	y
6	2	$\mathrm{Sym}(7)$	y
6	2	$3 \times \mathrm{GL}_3(2)$	y
6	2	$\mathrm{Sym}(3) \times \mathrm{GL}_3(2)$	y
3	3	$\Omega_3(3) \cong \mathrm{Alt}(4)$ or $\Omega_3(3) \times 2 \cong \mathrm{Alt}(4) \times 2$	y
3	3	$\mathrm{SO}_3(3) \cong \mathrm{Sym}(4)$ (two such groups)	y
3	3	$\mathrm{GO}_3(3) \cong \mathrm{Sym}(4) \times 2$	y
4	3	$8.\mathrm{Alt}(5)$ or $8.\mathrm{Sym}(5)$	y
4	3	$\mathrm{CSp}_4(3)$	n
4	3	$\mathrm{GO}_4^+(3)$ or $\mathrm{GO}_4^-(3)$	n
4	3	$\mathrm{GL}_2(3) : (3 \times \mathrm{Sym}(3))$	n
4	3	$((2 \times Q_8) : 2) : 5 : 4$	n
4	3	$\mathrm{GL}_2(3) : \mathrm{Sym}(4)$	n
4	3	$2.\mathrm{PGL}_2(9)$	n
4	3	$2^{1+4}.\mathrm{Alt}(5) : 2$	n
4	3	$(\mathrm{SA}_{16} : 2) : 3$	n
4	3	$(\mathrm{SA}_{16} : 2) : 6$ (two such groups)	n
4	3	$Q_8.\mathrm{Sym}(3) : 4$	n
4	3	$\mathrm{GL}(2,3) : D_8$	n
2	5	$\mathrm{SL}_2(3) : 2$	y
2	5	$\mathrm{SL}_2(3) : 4$	y
2	5	$\mathrm{Sym}(3)$	y
2	5	D_{12}	y
2	7	$\mathrm{SL}_2(3)$	y
2	7	$3 \times \mathrm{SL}_2(3)$	y
2	7	$3 \times \mathrm{SL}_2(3).2 = 3 \times 2.\mathrm{Sym}(4)$	y
2	7	D_{16}	y
2	11	$5 \times \mathrm{GL}_2(3)$	y
2	11	$5 \times \mathrm{SL}_2(5)$	y
2	13	$\mathrm{SL}_2(3) : 4$ or $3 \times \mathrm{SL}_2(3) : 4$	y

TABLE 1. *Primitive groups in Theorems 1.2(4) and 1.4(3)*

Line	d	p	Conditions	h	$\lvert g\rvert$	$\lvert g\rvert$ vs. $\lvert h\rvert$
1	≥ 1	–	$1 \leq i \leq 3$ and $i \mid p^d - 1$	s_d^i	$(p^d-1)/i$	$\lvert g\rvert = \lvert h\rvert$
2	≥ 2	–	$1 \leq i \leq 3$ and $i \mid p^{d-1} - 1$	$J_1 \oplus s_{d-1}^i$	$(p^d-p)/i$	$\lvert g\rvert = p\lvert h\rvert$
3	1	–		J_1	p	$\lvert g\rvert = p\lvert h\rvert$

TABLE 2. *Arbitrary p*

Line	p	d	Conditions	h	$\lvert g\rvert$	$\lvert g\rvert$ vs. $\lvert h\rvert$
1	3	≥ 3		$J_1 \oplus s_{d-1}$	$3^{d-1}-1$	$\lvert g\rvert = \lvert h\rvert$
2	3	≥ 3	$t = 2$, $(d_1, d_2) = 1$	$s_{d_1} \oplus s_{d_2}$	$\frac{1}{2}(3^{d_1}-1)(3^{d_2}-1)$	$\lvert g\rvert = \lvert h\rvert$
3	3	≥ 4	$i = 1, 2$ d odd if $i = 2$	$(s_1 \otimes J_2) \oplus s_{d-2}^i$	$3(3^{d-2}-1)$	$\lvert g\rvert = \lvert h\rvert$
4	3	≥ 4		$J_2 \oplus s_{d-2}$	$3(3^{d-2}-1)$	$\lvert g\rvert = \lvert h\rvert$
5	3	≥ 4	$h' \in \mathrm{GL}_{d-1}(p)$ as h in lines 1, 2	$J_1 \oplus h'$	$3\lvert h'\rvert$	$\lvert g\rvert = p\lvert h\rvert$
6	3	≥ 5		$J_3 \oplus s_{d-3}$	$9(3^{d-3}-1)$	$\lvert g\rvert = p\lvert h\rvert$
7	2	≥ 3	$t \geq 2$, $d_1 = 1$ with $d_2, \ldots, d_t \geq 2$ coprime	$\bigoplus_j s_{d_j}$	$\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
8	2	≥ 5	$t \geq 2$, with $d_j \geq 2$ coprime	$\bigoplus_j s_{d_j}$	$\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
9	2	≥ 4	$d_1 = 4$, and for $j \geq 2$ $d_j \geq 3$ odd and coprime	$(s_2 \otimes J_2) \oplus \bigoplus_{j\geq 2} s_{d_j}$	$6\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
10	2	≥ 5	$d_1 = 3$, and for $j \geq 2$ $d_j \geq 2$ and coprime	$J_3 \oplus \bigoplus_{j\geq 2} s_{d_j}$	$4\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
11	2	≥ 4	$t \geq 2$, and for $j \geq 2$ $d_j \geq 2$ and coprime	$J_2 \oplus \bigoplus_{j\geq 2} s_{d_j}$	$2\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
12	2	≥ 5	$t \geq 2$, $d_j \geq 2$ and coprime except $(d_1, d_2) = 2$	$\bigoplus_j s_{d_j}$	$\frac{1}{3}\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
13	2	≥ 5	$t \geq 2$, $d_1 \geq 4$ even, $d_j \geq 2$ and coprime	$s_{d_1}^3 \oplus \bigoplus_{j\geq 2} s_{d_j}$	$\frac{1}{3}\prod(2^{d_j}-1)$	$\lvert g\rvert = \lvert h\rvert$
14	2	≥ 4	$h' \in \mathrm{GL}_{d-1}(2)$ as h in lines 7, 8, 12, 13	$J_1 \oplus h'$	$2\lvert h'\rvert$	$\lvert g\rvert = p\lvert h\rvert$
15	2	≥ 5	$h' \in \mathrm{GL}_{d-2}(2)$ as h in lines 7, 8, 12, 13	$J_2 \oplus h'$	$4\lvert h'\rvert$	$\lvert g\rvert = p\lvert h\rvert$
16	2	≥ 5	$h' \in \mathrm{GL}_{d-4}(2)$ as h in line 8 or in Table 2 line 1	$J_4 \oplus h'$	$8\lvert h'\rvert$	$\lvert g\rvert = p\lvert h\rvert$
17	2	≥ 4	$i = 1, 3$	$J_2 \oplus s_{d-2}^i$	$4(2^{d-2}-1)/i$	$\lvert g\rvert = p\lvert h\rvert$

TABLE 3. *Other infinite families $p = 2$, 3*

REMARK 3.

(a) The notation used in Tables 2–7 is explained in Notation 1.
(b) The elements in Table 4, line 11, with $h = J_1 \oplus s_2^3$ also occur in Table 2, line 2 with $(p, d, i) = (2, 3, 3)$.
(c) The elements in Table 4, line 8, with $h = J_2 \oplus s_2^3$ also occur in Table 3, line 18 with $(d, i) = (4, 3)$.
(d) Not all Singer cycles s_a in $\mathrm{GL}_a(p)$ are conjugate. Thus a line containing Singer cycles or their powers may represent several conjugacy classes of examples.

Line	p	d	Conditions	h	$\lvert g\rvert$	$\lvert g\rvert$ vs. $\lvert h\rvert$
1	≥ 3	2	$1 \leq i \leq 3$ and $i \mid p-1$	$s_1^i \otimes J_2$	$p(p-1)/i$	$\lvert g\rvert = \lvert h\rvert$
2	3	4		$s_2 \otimes J_2$	24	$\lvert g\rvert = \lvert h\rvert$
3	2, 3	p		J_p	p^2	$\lvert g\rvert = p\lvert h\rvert$
4	2	2, 3, 4, 5		J_d	2, 4, 4, 8	$\lvert g\rvert = \lvert h\rvert$
5	2	3		$J_2 \oplus J_1 = J_2 \oplus s_1$	2	$\lvert g\rvert = \lvert h\rvert$
6	2	4		$J_3 \oplus J_1$	4	$\lvert g\rvert = \lvert h\rvert$
7	2	4		J_4	8	$\lvert g\rvert = p\lvert h\rvert$
8	2	4		$J_2 \oplus J_2$	4	$\lvert g\rvert = p\lvert h\rvert$
9	2	4		$J_2 \oplus J_1 \oplus J_1$	4	$\lvert g\rvert = p\lvert h\rvert$
10	2	3		$J_2 \oplus J_1 = J_2 \oplus s_1$	4	$\lvert g\rvert = p\lvert h\rvert$
11	2	3		$J_1 \oplus J_1 \oplus J_1$	2	$\lvert g\rvert = p\lvert h\rvert$

TABLE 4. *Sporadic cases*

2. *Notation and preliminary observations*

Given a positive integer d and a prime p, we denote by V the d-dimensional vector space of row vectors over the field $\mathbb{F}_p$ of size p, and choose a basis $\{e_1, \ldots, e_d\}$. As in Section 1 we represent an element $g \in \mathrm{AGL}(V)$ uniquely as $g = t_v h$ with $t_v : x \mapsto x + v$ a translation, for some $v \in V$, and with $h \in \mathrm{GL}(V)$ (where t_v is performed first). We first seek conditions on v and h so that g has order at least $n/4 = p^d/4$ and then, using these results as a starting point, we find conditions so that g has at most 4 cycles in its action on V (including the zero vector). We let $|g|$ denote the order of the element g.

We use the following notation and information.

NOTATION 1.

(a) We denote by I the identity element of $\mathrm{GL}(V)$. For each $r \geq 1$ and $h \in \mathrm{GL}(V)$ define $h(r)$ by

$$h(r) = I + h + \ldots + h^{r-1}. \tag{2.1}$$

(b) For $v' \in V$ and $g = t_v h$, the g-cycle containing v' consists precisely of the vectors

$$\{v'h^{r-1} + vh(r) - v \mid r \geq 1\}.$$

(c) For $1 \leq j \leq d$, let s_j denote a generator of a Singer cycle in $\mathrm{GL}_j(p)$ (an element of order $p^j - 1$), and let J_j denote the cyclic unipotent element of $\mathrm{GL}_j(p)$ acting on $\langle e_1, \ldots, e_j\rangle$ sending e_i to $e_i + e_{i+1}$ for $i < j$ and fixing e_j. We suppress the parameter p as it will be clear from the context. For convenience we also let J_0 denote the identity on the zero vector space.
If we write, for example, $h = J_j \oplus J_i$ we will mean that h acts as J_j on $\langle e_1, \ldots, e_j\rangle$, and as J_i on $\langle e_{j+1}, \ldots, e_{j+i}\rangle$ in the sense of mapping e_{j+s} to e_{j+s+1} for $1 \leq s < i$ and fixing e_{j+i}.

(d) In Table 3, wherever the notation d_j is used, we have $1 \leq j \leq t$, and $\sum_{j=1}^{t} d_j = d$.

(e) Whenever $h_j \in \mathrm{GL}(V)$ is indecomposable (where V has dimension d_j) and we write $h_j = s_j u_j (= u_j s_j)$, this indicates the Jordan decomposition with u_j unipotent and s_j semisimple. Since h_j is indecomposable, $V = \oplus_{i=1}^{m_j} W_i$ is a sum of m_j pairwise isomorphic irreducible $\mathbb{F}_p\langle s_j\rangle$-submodules of dimension $d'_j = d_j/m_j$. If we have h instead of h_j, we omit the subscript j throughout this notation.

We start by recalling [**8**, Lemma 2.2]. (Here $\log_p(x)$ denotes the logarithm of x to the base p and $\lceil x \rceil$ denotes the least integer k satisfying $x \leq k$.)

LEMMA 2.1. *Let u be a unipotent element of $\mathrm{GL}_d(p^f)$ where p is prime and $f \geq 1$. Then $|u| \leq p^{\lceil \log_p(d) \rceil}$ and equality holds if and only if the Jordan decomposition of u has a block of size b such that $\lceil \log_p(d) \rceil = \lceil \log_p(b) \rceil$.*

If $g = t_v h \in \mathrm{AGL}_d(p)$, then $|g|$ is either $|h|$ or $p|h|$, and Lemma 2.2 explains which one holds.

LEMMA 2.2. *Let $h \in \mathrm{GL}(V)$ of order k and let $h(k)$ be as in (2.1). Then*
(a) *$(vh(k))h = vh(k)$, for every $v \in V$;*
(b) *$g = t_v h$ has order pk if and only if $vh(k) \neq 0$, and in this case $g^k = t_{vh(k)}$;*
(c) *the following are equivalent:*
  (i) *there exists v such that $t_v h$ has order pk;*
  (ii) *$h(k) \neq 0$;*
  (iii) *the minimal polynomial $m_h(x)$ of h is of the form $(x-1)^{(k)_p} f(x)$ for some polynomial $f(x)$ coprime to $x-1$, where $(k)_p$ denotes the p-part of k.*

Proof. Observe that the element $h(k)$ defined in (2.1) can also be written as $h(k) = I + h^{-1} + \ldots + h^{-k+1}$, and that $g^k = (t_v h)^k = t_u$, where $u = v + vh^{-1} + \ldots + vh^{-k+1} = vh(k)$. Also $h(k)(I-h) = I - h^k = 0$ and so $u = vh(k) = vh(k)h = (vh(k))h = uh$, proving (a). Since $g^k = t_u$, $|g| = pk$ if and only if $u \neq 0$, proving (b).

Now we prove part (c). Suppose that (i) holds and let $v \in V$ be such that $|t_v h| = pk$. Then by part (b), we have $vh(k) \neq 0$ and hence $h(k) \neq 0$, so (ii) holds. Next suppose that (ii) holds and let $v \in V$ be such that $vh(k) \neq 0$. Since $h(k) \neq 0$, $m_h(x)$ does not divide $x^{k-1} + x^{k-2} + \ldots + 1$, but since h has order k, $m_h(x)$ divides $x^k - 1$. Write $k = (k)_p m$ and observe that

$$\begin{aligned} x^k - 1 &= (x^m - 1)^{(k)_p} = (x-1)^{(k)_p} (x^{m-1} + \ldots + x + 1)^{(k)_p} \\ &= (x-1)^{(k)_p} \left(\prod_{\lambda \neq 1, \lambda^m = 1} (x - \lambda) \right)^{(k)_p}. \end{aligned}$$

Since $m_h(x)$ does not divide $(x^k - 1)/(x-1)$, we see that $m_h(x) = (x-1)^{(k)_p} f(x)$, where $f(x)$ divides $(x^{m-1} + \ldots + x + 1)^{(k)_p}$, and hence is coprime to $x-1$, proving (iii).

Finally suppose that (iii) holds with $m_h(x) = (x-1)^{(k)_p} f(x)$ for some polynomial $f(x)$ coprime to $x-1$. Since, as we showed above, $x-1$ has multiplicity $(k)_p$ in $x^k - 1$, the polynomial $m_h(x)$ does not divide $\ell(x) = (x^k - 1)/(x-1)$. Hence $\ell(h)$, which equals $h(k)$, is not the zero map, and so there exists $v \in V$ such that $vh(k) \neq 0$. By part (b), $t_v h$ has order pk, and (i) holds. □

We give a useful corollary for the case where $g = t_v h$ has order $p|h|$.

COROLLARY 2.3. *If $g = t_v h$ has order $p|h| = pk$, then h is conjugate to $J_{(k)_p} \oplus h'$ for some $h' \in \mathrm{GL}_{d-(k)_p}(p)$.*

Proof. Suppose $|g| = p|h|$ and write $k = |h|$. By Lemma 2.2(c), $(x-1)^{(k)_p}$ divides $m_h(x)$. It follows that there exists $v \in V$ such that the $\mathbb{F}_p\langle h \rangle$-submodule generated by v is cyclic of dimension $(k)_p$, and h induces $J_{(k)_p}$ on it. By Lemma 2.1, we have $|J_{(k)_p}| = (k)_p$. Since

$(x-1)^{(k)_p+1}$ does not divide $m_h(x)$, the map h does not involve $J_{(k)_p+1}$ by Lemma 2.1, and hence by [**12**, Theorem 8.2], h is conjugate to $J_{(k)_p} \oplus h'$ for some $h' \in \mathrm{GL}_{d-(k)_p}(p)$. □

LEMMA 2.4. *Let $g = t_v h \in \mathrm{AGL}(V)$ and let U be the $(x-1)$-primary component of the $\mathbb{F}_p\langle h\rangle$-module V. Then g is conjugate to $t_u h$ for some $u \in U$. In particular, if h is fixed point free on $V \setminus \{0\}$, then g is conjugate to $h \in \mathrm{GL}(V)$.*

Proof. Let $V = U \oplus W$ be an h-invariant decomposition (so W is the direct sum of the other primary components, if any). Then $h|_W$ is fixed point free, so also $(h^{-1})|_W$ is fixed point free and in particular $(I - h^{-1})|_W$ is nonsingular. Observe that from Lemma 2.2(a) we have $vh(k) \in U$. Now $v = u + w$, for some $u \in U$ and $w \in W$, and $vh(k) = (u+w)h(k) = uh(k) + wh(k)$ with $uh(k) \in U$ and $wh(k) \in W$. Thus $wh(k) = vh(k) - uh(k) \in U \cap W$, so $wh(k) = 0$. Since $(I - h^{-1})|_W$ is nonsingular, there exists $w' \in W$ such that $w = w' - w'h^{-1}$, and hence we have

$$t_{w'}^{-1}(t_v h)t_{w'} = t_{v-w'}(ht_{w'}h^{-1})h = t_{v-w'+w'h^{-1}}h = t_{v-w}h = t_u h.$$

Note that if h is fixed point free (that is, $U = 0$), then we have $u = 0$ and therefore g is conjugate to $h \in \mathrm{GL}(V)$. □

NOTATION 1 (EXTENDED).

(f) We add to our Notation 1 the subspaces U and W as defined in the statement and in the proof of Lemma 2.4, and define the integer a by the equation

$$|U| = p^a.$$

Since conjugate permutations have the same order and the same cycle structure we may, because of Lemma 2.4, assume from now on that $v \in U$.

(g) For a finite group G, we write $\mathrm{meo}(G) = \max\{|g| \mid g \in G\}$ for the maximal order of the elements of G. Given two natural numbers n and m, we write (n, m) for the greatest common divisor of n and m.

3. *Proof of Theorem 1.1*

Proof of Theorem 1.1. Suppose that $g = t_v h$ in $\mathrm{AGL}(V) = \mathrm{AGL}_d(p)$ has order $|g| \geq n/4$. We shall prove that g and h appear in one of the lines of Tables 2, 3 or 4. Several times in the proof we use the facts that $\mathrm{meo}(\mathrm{GL}_d(p)) = p^d - 1$ and $\mathrm{meo}(\mathrm{SL}_d(p)) = (p^d - 1)/(p-1)$. A proof of these facts can be deduced, for example, from [**8**, Corollary 2.7] and for odd p from [**13**, Table A.1].

The case $|g| = |h|$. First we assume that $|g| = |h|$. We use the notation in Section 2 and we suppose that $|h| \geq p^d/4$. Write $V = V_1 \oplus V'$, where V_1, V' are h-invariant and $h_1 = h|_{V_1}$ is indecomposable; let $h' = h|_{V'}$ (possibly $V' = 0$) so that $h = h_1 \oplus h'$, and let $k = \dim(V_1)$.

Case $|g| = |h|$, $p \geq 5$. We have $h^{p-1} = h_1^{p-1} \oplus (h')^{p-1}$, and h_1^{p-1}, $(h')^{p-1}$ have determinant 1. If $V' \neq 0$, then

$$|h^{p-1}| \leq \mathrm{meo}(\mathrm{SL}_k(p))\mathrm{meo}(\mathrm{SL}_{d-k}(p)) \leq \frac{(p^k-1)(p^{d-k}-1)}{(p-1)^2} < \frac{p^d}{(p-1)^2}.$$

Hence $|h| < p^d/(p-1) \leq p^d/4$, which is a contradiction since $p \geq 5$. Hence $V' = 0$ and $h = h_1$ is indecomposable.

If h is irreducible then $h = s_d^i$ for some i with $i \mid |s_d|$. As $|s_d| = p^d - 1$, we have $1 \leq i \leq 3$, as described in line 1 of Table 2. Suppose then that h is not irreducible. Let $h = su$. Since h is

not irreducible, $m \geq 2$ and $u \neq 1$. If $d' = 1$, then by Lemma 2.1 we get

$$|h| \leq (p-1)p^{\lceil \log_p(d) \rceil}.$$

If $d \geq 6$, this gives no examples since $(p-1)p^{\lceil \log_p(d) \rceil} \leq (p-1)dp < p^d/4$. If $d \leq 5$ then, since $p \geq 5$, $\lceil \log_p(d) \rceil = 1$ and a direct calculation shows that $(p-1)p$ is less than $p^d/4$ unless $m = d = 2$, which yields the example in line 1 of Table 4. Now assume that both $m, d' \geq 2$. Then h has a conjugate lying in the subgroup $\mathrm{GL}_m(p^{d'})$. Under this conjugation, s becomes a scalar matrix in $\mathrm{GL}_m(p^{d'})$ and u becomes a unipotent element of $\mathrm{GL}_m(p^{d'})$. Applying Lemma 2.1, we have

$$|h| \leq (p^{d'} - 1)p^{\lceil \log_p(m) \rceil}$$

and $\lceil \log_p(m) \rceil \leq m - 1$ (see the proof of [**8**, Lemma 2.4]). Therefore, noting that $d' + m \leq d'm = d$ for integers $d', m \geq 2$, we get

$$|h| \leq p^{d'} p^{m-1} = p^{d'+m-1} \leq p^{d'm-1} < p^d/4$$

so there are no further examples when $p \geq 5$.

Case $|g| = |h|$, $p = 3$. Arguing in the same way as in the first paragraph of "Case $p \geq 5$" we obtain that V is not a direct sum of three non-zero $\mathbb{F}_p\langle h \rangle$-submodules. First suppose that h is indecomposable. If h is semisimple then it is irreducible and so $h = s_d^i$ with $i \leq 3$ as in line 1 of Table 2. Suppose now that h is not semisimple and let $h = su$. Then $m \geq 2$ and

$$|h| \leq (3^{d'} - 1)3^{\lceil \log_3(m) \rceil}.$$

A direct calculation shows that this is less than $3^d/4$ unless $(d', m) = (1, 2)$ or $(2, 2)$; these cases yield the examples in lines 1 and 2 of Table 4.

Finally suppose that $V = V_1 \oplus V_2$ and $h = h_1 \oplus h_2$ with $h_i = h|_{V_i}$ indecomposable and $d_i = \dim(V_i)$ for $i = 1, 2$. If h is semisimple then h_1 and h_2 are contained in Singer cycles. In this case if $(d_1, d_2) \geq 2$ then

$$|h| \leq \mathrm{lcm}\{3^{d_1} - 1, 3^{d_2} - 1\} = (3^{d_1} - 1)(3^{d_2} - 1)/(3^{(d_1,d_2)} - 1) < 3^d/4.$$

So $(d_1, d_2) = 1$ and we have the examples in lines 1 and 2 of Table 3 (the condition $d \geq 3$ follows from a calculation). Now assume that h is not semisimple. Then, replacing h_1 by h_2 if necessary, we may assume that $h_1 = u_1 s_1$ with V_1 and $m_1 \geq 2$. Since $\mathrm{meo}(\mathrm{GL}_{d-d_1}(3)) = 3^{d-d_1} - 1$ we have

$$|h| \leq |h_1| \cdot |h_2| \leq (3^{d_1'} - 1)3^{\lceil \log_3(m_1) \rceil} \,\mathrm{meo}(\mathrm{GL}_{d-d_1}(3)) = (3^{d_1'} - 1)3^{\lceil \log_3(m_1) \rceil}(3^{d-d_1} - 1).$$

Now a direct calculation shows that this is less than $3^d/4$ unless $(m_1, d_1') = (2, 1), (2, 2)$. In the second case, $h_1 \in \langle s_2 \otimes J_2 \rangle$ and so $|h^2| \leq |h_1^2||h_2^2| \leq 12\,\mathrm{meo}(\mathrm{SL}_{d-4}(3))$. But [**13**] implies that $\mathrm{meo}(\mathrm{SL}_{d-4}(3)) = (3^{d-4} - 1)/2$, and hence $|h| \leq 12(3^{d-4} - 1)$. However, since $d = 4 + d_2 \geq 5$, we have $12(3^{d-4} - 1) < 3^d/4$. Thus $(m_1, d_1') = (2, 1)$ and $h_1 \in \langle s_1 \otimes J_2 \rangle$. If h_2 is semisimple then it is contained in a Singer cycle, giving the examples in lines 3 (if $|h_1| = 6$) and 4 (if $|h_1| = 3$) of Table 3 (the conditions $d \geq 4$ and d odd, when $i = 2$, follow from a calculation; note that $i = 2, d = 3$ gives $h = (s_1 \otimes J_2) \oplus J_1$ of order $6 < 3^3/4$). If h_2 is not semisimple, then $h_2 = u_2 s_2$ and $m_2 \geq 2$. We have

$$|h| \leq |h_1| \cdot |h_2| \leq 6(3^{d_2'} - 1)3^{\lceil \log_3(m_2) \rceil} < 3^d/4$$

except for $d_2' = 1$ and $m_2 = 2$. In this exceptional case, $|h_2|$ divides 6 and, as $h_1 \in \langle s_1 \otimes J_2 \rangle$, we have $|h| \leq 6 < 3^d/4$. Therefore there are no further examples when $p = 3$.

Case $|g| = |h|, p = 2$. Suppose that $V = V_1 \oplus \ldots \oplus V_t$ and $h = h_1 \oplus \ldots \oplus h_t$, where the V_i are h-invariant with $\dim(V_i) = d_i$, and each $h_i = h|_{V_i}$ is indecomposable. Also let $h_i = s_i u_i$. First suppose that $t = 1$. If h is semisimple then it is contained in a Singer cycle giving the examples

in line 1 of Table 2. Suppose now that $u_1 \neq 1$, so that $m_1 \geq 2$. Then

$$|h| \ \leq (2^{d_1'}-1)2^{\lceil \log_2(m_1)\rceil},$$

which is less than $2^d/4$ unless $(d_1', m_1) = (1,2),(1,3),(1,4),(1,5),(2,2)$; thus we have the examples in line 4 of Table 4 and line 9 of Table 3 (by taking $d = 4$).

So we may assume $t \geq 2$. Observe that if $d = 2$, then $h = h_1 = h_2 = 1$ as in line 1 of Table 2 (by taking $i = 3$). Thus we may suppose that $d \geq 3$. If h is semisimple, then each h_i is irreducible and $|h| \leq \operatorname{lcm}\{2^{d_i}-1 \mid i = 1,\ldots,t\}$. If $(d_j, d_k) \geq 3$ for some distinct j and k, then

$$|h| \leq \operatorname{lcm}\{2^{d_i}-1 \mid i=1,\ldots,t\} \leq \left(\prod_{i=1}^{t}(2^{d_i}-1)\right)/(2^{d_j}-1, 2^{d_k}-1) < 2^d/7,$$

which is a contradiction. If there are at least three even d_i, then

$$|h| \leq \operatorname{lcm}\{2^{d_i}-1 \mid i=1,\ldots,t\} \leq \left(\prod_{i=1}^{t}(2^{d_i}-1)\right)/(2^2-1)^2 < 2^d/9,$$

again a contradiction. Moreover, as $d \geq 3$, if the fixed point subspace of h has dimension at least 2 (so at least two of the d_i equal 1), then $|h| \leq \operatorname{meo}(\mathrm{GL}_{d-2}(2)) = 2^{d-2}-1 < 2^d/4$. Thus $d \geq 3$, at most one d_i can be 1, at most 2 of the d_i are even, and $(d_j, d_k) \leq 2$ for distinct j, k. Observe further that if $d_i = 1$ and if $(d_j, d_k) = 2$ for some distinct j and k, then $|h| \leq (2^{d-1}-1)/3 < 2^{d-2}$: this shows that if $d_i = 1$ for some i, then $(d_j, d_k) = 1$ for distinct j and k. The only such examples (with $t \geq 2$) are listed in lines 7, 8, 12, 13 of Table 3. (Observe that in line 13 we have $d_1 \geq 4$ because $s_2^3 = 1$ fixes a subspace of dimension 2.)

Suppose now that h is not semisimple. Then we may assume that d_1 is maximal such that $h_1 = s_1 u_1$ is non-semisimple, and that $m_1 \geq 2$. Now

$$|h| \leq |h_1||h_2| \leq (2^{d_1'}-1)2^{\lceil \log_2(m_1)\rceil} \operatorname{meo}(\mathrm{GL}_{d-d_1}(2)) = (2^{d_1'}-1)2^{\lceil \log_2(m_1)\rceil}(2^{d-d_1}-1)$$

and a direct calculation shows that this is less than $2^d/4$ unless $(m_1, d_1') = (2,1)$, $(3,1)$ or $(2,2)$ (note that $(m_1, d_1') \in \{(2,1),(3,1),(4,1),(5,1),(2,2)\}$ if $d_1 \leq 5$ from our work above). We consider each possibility for (m_1, d_1').

If $(m_1, d_1') = (2,2)$, then $h_1 = s_2 \otimes J_2$, $|h_1| = 6$ and $h = h_1 \oplus h'$. Clearly h' must have odd order for otherwise $|h| = \operatorname{lcm}\{6, |h'|\} \leq 3|h'| < 3 \cdot 2^{d-4} < 2^d/4$. It follows that h' is semisimple with irreducible blocks of dimensions $d_2, \ldots, d_t$. Note that if one of the d_i $(i \geq 2)$ is even, then $2^{d_i} \equiv 1 \pmod 3$ and we have

$$|h| \leq \operatorname{lcm}\{6, 2^{d_j}-1 \mid j = 2,\ldots,t\} \leq 6 \cdot 2^{d-4}/3 < 2^d/4.$$

Hence each d_i is odd for $i \geq 2$. If two of the d_i have a common factor > 1, then similarly, we have

$$|h| \leq \operatorname{lcm}\{6, 2^{d_i}-1 \mid i = 2,\ldots,t\} \leq 6 \cdot 2^{d-4}/3 < 2^d/4.$$

Therefore the d_i must be pairwise coprime. A similar calculation shows that none of the $d_i = 1$, and that each of the h_i $(i \geq 2)$ is s_{d_i} (and not a proper power). Thus we have the examples in line 9 of Table 3.

If $(m_1, d_1') = (3,1)$, then $h_1 = J_3$ and $|h_1| = 4$. As in the previous case, $h = h_1 \oplus h'$ and h' must have odd order. So h' is semisimple with irreducible blocks of dimensions $d_2, \ldots, d_t$, and the same arguments show that the d_i are pairwise coprime. If each $d_i \geq 2$ then we have the examples in line 10 of Table 3. If some $d_i = 1$ then $t = 2$ and we have the example in line 6 of Table 4.

It remains to consider the case $(m_1, d_1') = (2,1)$, where $h_1 = J_2$ of order 2. As before, $h = h_1 \oplus h'$ where h' is semisimple, and the usual arguments give us the examples in line 11 of Table 3 and line 5 of Table 4.

The case $|g| = p|h|$. We have now classified the examples with $|g| = |h|$. Henceforth we assume that $|g| = p|h|$. By Lemma 2.2, the power $(x-1)^{(k)_p}$ divides $m_h(x)$, where $k = |h|$. If $d = 1$, then $h = 1$ and we have the examples in line 3 of Table 2. For the rest of the proof we assume then $d \geq 2$.

Case $|g| = p|h|, p \geq 5$. First suppose that h is semisimple. We seek conditions on h for which $|h| \geq p^{d-1}/4$. In this case, $x - 1 \mid m_h(x)$ and so we can write $h = J_1 \oplus h'$ where $h' \in \mathrm{GL}_{d-1}(p)$ is semisimple. (Recall that $d - 1 \geq 1$.) By our previous work, the only semisimple elements $h' \in \mathrm{GL}_{d-1}(p)$ of order at least $p^{d-1}/4$ appear in line 1 of Table 2; thus the only examples of h occur in line 2 of Table 2. If h is not semisimple then by Corollary 2.3 we have $h = J_{(k)_p} \oplus h'$, and $(k)_p \geq 5$. In particular,

$$|h| \leq (k)_p \,\mathrm{meo}(\mathrm{GL}_{d-(k)_p}(p)) = (k)_p(p^{d-(k)_p} - 1) < p^{d-1}/4$$

in all cases since $(k)_p \geq 5$. So there are no further examples when $p \geq 5$.

Case $|g| = p|h|, p = 3$. If h is semisimple then by Corollary 2.3 we can write $h = J_1 \oplus h'$ with $h' \in \mathrm{GL}_{d-1}(3)$ of order at least $3^{d-1}/4$. Therefore h' is contained in line 1 of Table 2 or lines 1, 2 of Table 3; so h is as in line 2 of Table 2 or line 5 of Table 3. If h is not semisimple then, by Corollary 2.3, h is of the form $J_{(k)_3} \oplus h'$ (with $k \geq 3$). If $h = J_{(k)_3}$, then $|h| = (k)_3 = d$ so $|g| = 3d$ and $3^d/4 > 3d$ for $d \geq 5$, so $h = J_3$ (line 3 of Table 4). Otherwise, $d > (k)_3$ and

$$|h| \leq (k)_3(3^{d-(k)_3} - 1),$$

which is less than $3^{d-1}/4$ unless $(k)_3 = 3$ and $d \geq 5$. So we may assume that $h = J_3 \oplus h'$ where $h' \in \mathrm{GL}_{d-3}(3)$. Now if 3 divides $|h'|$ then $|h| = |h'| \leq \mathrm{meo}(\mathrm{GL}_{d-3}(3)) = 3^{d-3} - 1 < 3^{d-1}/4$, which is a contradiction. So h' is semisimple and therefore appears in line 1 of Table 2 or lines 1, 2 of Table 3. However it is clear that $|h| < 3^{d-1}/4$ if h' is as in lines 1, 2 of Table 3: so the only additional examples are in line 6 of Table 3.

Case $|g| = p|h|, p = 2$. Again we first suppose that h is semisimple so that $h = J_1 \oplus h'$ and $|h'| \geq 2^{d-1}/4$; that is, h' is one of the semisimple examples in line 1 of Table 2 or lines 7, 8, 12 or 13 of Table 3; thus the only such examples are in line 2 of Table 2, or in line 11 of Table 4 (arising from h' as in line 1 of Table 2 with $d = 2$ and $i = 3$), or in line 14 of Table 3. Now suppose that h is not semisimple; so by Corollary 2.3, $h = J_{(k)_2} \oplus h'$ (with $k \geq 2$). If $h = J_{(k)_2}$, then $|h| = (k)_2 = d$ so $|g| = 2d$ and $2^d/4 > 2d$ for $d \geq 6$, so $h = J_2$ or J_4 (lines 3 and 7 of Table 4). Otherwise, $d > (k)_2$ and

$$|h| \leq (k)_2(2^{d-(k)_2} - 1),$$

which is less than $2^{d-1}/4$ unless $(k)_2 = 2$ or 4. Suppose first that $(k)_2 = 2$. Then $h = J_2 \oplus h'$, with $h' \in \mathrm{GL}_{d-2}(2)$. If h' is semisimple then $|h| = 2|h'|$ and $|h'| \geq 2^{d-2}/4$, so as in the previous paragraph, h' is a semisimple element as in line 1 of Table 2, or lines 7, 8, 12 or 13 of Table 3: hence h is one of the examples in lines 15, 17 of Table 3 or lines 9, 10 of Table 4. If h' is not semisimple then $|h| = |h'|$, which is at least $2^{d-1}/4$ if and only if $h' \in \mathrm{GL}_{d-2}(2)$ is a non semisimple element of this order; by our previous work, this only occurs if $d = 4$ and $h' = J_2$ (note that h' cannot be J_3 from line 4 of Table 4 since we are assuming $(k)_2 = 2$, but $k = |h| = 4$ if $h = J_2 \oplus J_3$); thus we have line 8 of Table 4. Suppose now that $(k)_2 = 4$ so that $h = J_4 \oplus h'$. If h' is not semisimple then $|h| \leq 2|h'|$ and $2|h'|$ is at least $2^{d-1}/4$; this holds if and only if $h' \in \mathrm{GL}_{d-4}(2)$ is a non semisimple element of order at least 2^{d-3}. There are therefore no such elements and we conclude that h' is semisimple and $|h| = 4|h'|$. Now $|h| \geq 2^{d-1}/4$ if and only if $|h'| \geq 2^{d-4}/2$ and the only such examples h' occur in line 1 of Table 2 (with $i = 1$ and $d - 4 \geq 2$) and line 8 of Table 3; thus we have the examples in line 16 of Table 3. □

4. *Classification of elements with at most four cycles*

We now refine the list of affine transformations of order at least $n/4$ to determine those elements that have at most 4 cycles in V. Recall the notation from Section 2, especially for $g = t_v h, V, U, W, p^a = |U|$, and assume that g has at most four cycles in V. By Lemma 2.4 we may assume that $v \in U$. We start with some further observations.

4.1. *Invariant subsets of V*

For each h-invariant subspace V' of V, the subspace $U + V'$ is a g-invariant subset of V (recall that the subspace U is defined in Notation 1(f)). In fact, for $u' + v' \in U + V'$, we have $(u' + v')g = (u' + v')t_v h = (v + u')h + v'h \in U + V'$. In particular, taking $V' = 0$, we see that U is g-invariant.

4.2. *Three claims*

Claim 1: Suppose that $V \neq U$, and let W' be a nontrivial h-invariant subspace of W. Suppose that g has t cycles in U and that h has r cycles in W'. Then

(a) $t \cdot r \leq 4$ with $t \geq 1, r \geq 2$;
(b) if $t \geq 2$, then $t = r = 2$, $W' = W$, and $h|_W$ is transitive on $W \setminus \{0\}$; so $h = h|_U \oplus s_{d-a}$.

Proof of Claim 1. Since $v \in U$, it follows that $U \oplus W'$ is g-invariant. Let $w \in W'$ and $x \in U$. By Notation 1(b), the g-cycle containing $x + w$, where $x \in U, w \in W'$, consists precisely of the vectors $xh^i + vh(i+1) - v + wh^i = x^{g^i} + w^{h^i}$, for $i \geq 0$ (the equality can be easily proved by induction on i). This g-cycle is contained in $x^{\langle g \rangle} + w^{\langle h \rangle} = \{x^{g^i} + w^{h^j} \mid \text{for all } i, j\}$. It follows that there are at least tr cycles of g in $U \oplus W'$. Since g has at most 4 cycles, this implies part (a), and, if $t \geq 2$, then $t = r = 2$, $W' = W$, and $\langle h \rangle$ is transitive on the non-zero vectors of W'. □

Claim 2: Let $|h|_U| = p^c$, $|g| = p^\delta k$ where $\delta = 0, 1$, and let g have t cycles in U. Then

$$p^a \leq t|g|_U| = tp^{c+\delta} \leq \begin{cases} tp^\delta = t & \text{if } a = 0, \text{ that is, if } U = 0 \\ tp^{\delta + \lceil \log_p(a) \rceil} & \text{if } a > 0, \text{ that is, if } U \neq 0. \end{cases} \tag{4.1}$$

The subspace U is a single g-cycle if and only if either (i) $a = c = \delta = 0$ and $h|_U = J_0$, or (ii) $\delta = 1$, $h|_U = J_a$, and $a = 1$ or $(a, p) = (2, 2)$.

Proof of Claim 2. Since g has $t \leq 4$ cycles in U, we have $p^a = |U| \leq t|g|_U|$. If $a = 0$ then $c = 0$, $h|_U = J_0$, and $|g|_U| = p^\delta = 1$. Thus if $a = 0$ then the inequality (4.1) holds, U is a single g-cycle, and the conditions (i) hold. We may therefore assume that $a \geq 1$. Then, by Lemma 2.1, $|g|_U| = p^\delta \, |h|_U| \leq p^{\delta + \lceil \log_p(a) \rceil}$ with equality if and only if $h|_U$ involves a cyclic matrix J_b such that $\lceil \log_p(b) \rceil = \lceil \log_p(a) \rceil$. In particular (4.1) holds.

Suppose U is a single g-cycle. Then (4.1) holds with $t = 1$, and hence $p^a \leq p^{\delta + \lceil \log_p(a) \rceil}$, that is, $a \leq \delta + \lceil \log_p(a) \rceil$. It follows from a computation, since $a \geq 1$, that $\delta = 1$ and either $1 \leq a \leq 2$, or $(a, p) = (3, 2)$. If $a > 1$, then from the inequalities $p^a \leq p^{c+1} \leq p^{1 + \lceil \log_p(a) \rceil}$ in (4.1), we obtain $c = a - 1$, that is, $|h|_U| = p^{a-1}$. Therefore, by Corollary 2.3, $h|_U$ involves $J_{(k)_p}$. In particular if $(a, p) = (3, 2)$ then $(k)_p \geq p^c = 4$ but $h|_U$ does not involve J_4 because U has dimension 3 only. Similarly if $a = 2$ and p is odd, then $(k)_p \geq p^c = p$, but $h|_U$ does not involve J_p because U has dimension 2 only. So $a = 1$ or $(a, p) = (2, 2)$, and in either case, $h|_U = J_a$ so part (ii) holds.

Conversely if $\delta = 1$ and $h|_U = J_a$ with either $a = 1$ or $(a, p) = (2, 2)$, then $|h|_U| = p^{a-1}$ and so $|g|_U| = p^a = |U|$ so that U must form a single g-cycle. □

Line	d	# cycles	g	$\lvert g\rvert$	Cycle lengths
1	–	$i+1$ $(1 \le i \le 3$ and $i \mid p^d-1)$	s_d^i	$\lvert h\rvert$	1, and i of length $\frac{p^d-1}{i}$
2	2	3	$s_1 \otimes J_2$	$\lvert h\rvert$	$1, p-1, p(p-1)$
3	1	1	t_{e_1}	$p\lvert h\rvert$	p
4	≥ 2	$i+1$ $(1 \le i \le 3$ and $i \mid p^{d-1}-1)$	$t_{e_1}(J_1 \oplus s_{d-1}^i)$	$p\lvert h\rvert$	p, and i of length $\frac{p(p^{d-1}-1)}{i}$

TABLE 5. *At most 4-cycles, arbitrary p*

Line	d	# cycles	g	$\lvert g\rvert$	Cycle lengths
1	≥ 3	4	$s_{a_1} \oplus s_{a_2}$ $(a_1,a_2)=1$, $d=a_1+a_2$	$\lvert h\rvert$	$1, 2^{a_1}-1, 2^{a_2}-1,$ $(2^{a_1}-1)(2^{a_2}-1)$
2	≥ 3	4	$J_1 \oplus s_{d-1}$	$\lvert h\rvert$	$1, 1, 2^{d-1}-1, 2^{d-1}-1$
3	≥ 5	4	$t_{e_1}(J_3 \oplus s_{d-3})$	$\lvert h\rvert$	$4, 4, 2^{d-1}-4, 2^{d-1}-4$
4	≥ 4	4	$t_{e_1}(J_1 \oplus J_1 \oplus s_{d-2})$	$p\lvert h\rvert$	$2, 2,\ 2^{d-1}-2, 2^{d-1}-2$
5	≥ 4	$i+1 \in \{2,4\}$ d even if $i=3$	$t_{e_1}(J_2 \oplus s_{d-2}^i)$	$p\lvert h\rvert$	4, and i of length $\frac{2^d-4}{i}$
6	≥ 5	4	$t_{e_1}(J_2 \oplus J_1 \oplus s_{d-3})$	$p\lvert h\rvert$	$4, 4,\ 2^{d-1}-4, 2^{d-1}-4$
7	≥ 6	4	$t_{e_1}(J_a \oplus s_{a_1} \oplus s_{a_2})$ $1 \le a \le 2 \le a_1 < a_2$ $(a_1,a_2)=1$	$p\lvert h\rvert$	$2^a, 2^a(2^{a_1}-1), 2^a(2^{a_2}-1),$ $2^a(2^{a_1}-1)(2^{a_2}-1)$
8	≥ 6	4	$t_{e_1}(J_4 \oplus s_{d-4})$	$p\lvert h\rvert$	$8, 8,\ 2^{d-1}-8, 2^{d-1}-8$

TABLE 6. *At most 4-cycles, other infinite families ($p=2$)*

Claim 3*:* Suppose that there exist h-irreducible submodules W_1, W_2 of W, such that $|W_i| = p^{a_i}$ with $0 < a_1 \le a_2$ and $W_1 \cap W_2 = 0$. Then $V = U \oplus W_1 \oplus W_2$, $p = 2$, $(a_1, a_2) = 1$, $0 \le a \le 2 \le a_1 < a_2$, $d \ge 5$, and $h = J_a \oplus s_{a_1} \oplus s_{a_2}$ for some Singer cycles s_{a_1}, s_{a_2}. These elements have exactly four cycles and arise as examples in lines 1 (if $a = 0$), and 7 (if $a > 0$, with $v = e_1$) of Table 6.

Proof of Claim 3. The subspace $V' = U \oplus W_1 \oplus W_2 \le V$ is g-invariant, and we have the following nonempty g-invariant subsets: $U, (U \oplus W_i) \setminus U$ (for $i = 1, 2$), and $V' \setminus ((U \oplus W_1) \cup (U \oplus W_2))$, of sizes p^a, $p^a(p^{a_i} - 1)$ (for $i = 1, 2$), and $p^a(p^{a_1} - 1)(p^{a_2} - 1)$. Since g has at most four cycles, it follows that $V' = V$ and $\langle g \rangle$ acts transitively on each of these subsets.

Observe that if $(p^{a_1} - 1, p^{a_2} - 1) = \ell$, then g induces at least ℓ cycles on $V \setminus ((U \oplus W_1) \cup (U \oplus W_2))$. Thus $p^{a_1} - 1$ and $p^{a_2} - 1$ are coprime, and hence $p = 2$ and $(a_1, a_2) = 1$. Also transitivity of h on $W_i \setminus \{0\}$ implies that $h|_{W_i}$ is a Singer cycle s_{a_i}, and by Claim 2, $h|_U = J_a$ and $a \le 2$. Since $(a_1, a_2) = 1$ we have $a_1 < a_2$ and since $h|_{W_1} \ne 1$ (because $W_1 \ne 0$ and the 1-eigenspace of h is contained in U), we have $a_1 \ge 2$. Thus $d = a + a_1 + a_2 \ge 5 + a$, and the elements are the examples with 4 cycles in lines 1, 7 of Table 6 (if $a \ge 1$ we note that g has a conjugate of the form $g = t_{e_1}h$). □

4.3. *Four cycles: proof of Theorem 1.3*

Proof of Theorem 1.3. Let $g = t_v h \in \mathrm{AGL}_d(p)$ with at most four cycles in its action on V. Such an element g must appear in Table 2, 3, or 4. We consider each possibility on a line-by-line basis. As before we use Notation 1. Firstly, we suppose that $|g| = |h|$.

If g is as in line 1 of Table 2, then we may assume that $g = h$ and we have the examples in line 1 of Table 5. Similarly line 1 of Table 4 gives rise to line 2 of Table 5 and line 2 of Table 7. In

Line	d	p	# cycles	g	$\lvert g\rvert$	Cycle lengths
1	2	$2,3$	p	t_{e_1}	$p\lvert h\rvert$	p of length p
2	2	3	3	$t_{e_1}J_2$	$\lvert h\rvert$	$3,3,3$
3	3	2	2	$t_{e_1}J_3$	$\lvert h\rvert$	$4,4$
4	3	2	4	$t_{e_3}(J_2\oplus J_1)$	$\lvert h\rvert$	$2,2,2,2$
5	3	2	4	J_3	$\lvert h\rvert$	$1,1,2,4$
6	4	2	4	$t_{e_1}(J_3\oplus J_1)$	$\lvert h\rvert$	$4,4,4,4$
7	4	2	4	$s_2\otimes J_2$	$\lvert h\rvert$	$1,3,6,6$
8	5	2	4	$t_{e_1}J_5$	$\lvert h\rvert$	$8,8,8,8$
9	2	2	1	$t_{e_1}J_2$	$p\lvert h\rvert$	4
10	3	2	4	t_{e_1}	$p\lvert h\rvert$	$2,2,2,2$
11	3	2	2	$t_{e_1}(J_2\oplus J_1)$	$p\lvert h\rvert$	$4,4$
12	3	3	3	$t_{e_1}J_3$	$p\lvert h\rvert$	$9,9,9$
13	4	2	4	$t_{e_1}(J_2\oplus J_2)$ or $t_{e_1}(J_2\oplus J_1\oplus J_1)$	$p\lvert h\rvert$	$4,4,4,4$
14	4	2	2	$t_{e_1}J_4$	$p\lvert h\rvert$	$8,8$
15	5	2	4	$t_{e_1}(J_4\oplus J_1)$	$p\lvert h\rvert$	$8,8,8,8$

TABLE 7. *At most 4-cycles, sporadic cases*

line 1 of Table 3 we have $U=\langle e_1\rangle$ and we may assume that $v\in U$. But if $v\neq 0$ then $|g|=p|h|$; so we may assume $g=h$ (recall that $p=3$ for this line). But then g has 3 cycles on U and therefore has more than 4 cycles in total by Claim 1. In line 2 of Table 3 $g=h=s_{d_1}\oplus s_{d-d_1}$, but Claim 3 implies that $p=2$, whereas we have $p=3$. Suppose that g is as in line 3 of Table 3. Then by Lemma 2.4, $g=h=(s_1\otimes J_2)\oplus s^i_{d-2}$, since h is fixed point free on V, and V has a g-module decomposition $W_1\oplus W_2$, where $\dim W_1=2$ and g has 3 cycles on W_1; but there must also be at least one cycle on $W_2\setminus\{0\}$ and on $V\setminus(W_1\cup W_2)$; so these elements do not provide examples. Next, for g as in line 4 of Table 3, conjugating by a suitable $t_{v'}$, we may assume that $v\in\langle e_1\rangle$. So $g=t_{ae_1}(J_2\oplus s_{d-2})$ has cycle lengths on U equal to $1,1,1,3,3$ (if $a=0$), or $3,3,3$ (if $a=\pm1$), contradicting Claim 1. In line 2 of Table 4, again by Lemma 2.4, we have $g=h$ and direct calculation shows that the cycle lengths are $24,24,24,8,1$. In line 7 of Table 3, again we may assume $v=0$ and Claim 3 shows that $t=2$ and we have the examples in line 2 of Table 6. In line 8 of Table 3, $U=0$ so, by Lemma 2.4, $g=h$ and Claim 3 yields the examples in line 1 of Table 6. (Observe that Claim 3 immediately gives that the elements in lines 12 and 13 of Table 3 give rise to no examples.) In line 9 of Table 3, we have $g=h$ by Lemma 2.4; in this case $s_2\otimes J_2$ has cycle lengths $1,3,6,6$ on a 4-dimensional subspace W_1 and so the only examples occur when $d=4$; see line 7 of Table 7. In line 10 of Table 3, by conjugating by a suitable $t_{v'}$ we may assume that $v=0$ or $v=e_1$. Direct calculation shows that (within U) these two cases give cycle lengths $1,1,2,4$ and $4,4$ respectively. Clearly the first case cannot occur (since $d\geq 5$). In the second case, Claim 1 implies $g=t_{e_1}(J_3\oplus s_{d-3})$ as in line 3 of Table 6.Similarly in line 11 of Table 3, $v=0$ or $v=e_1$, but in the latter case we have $|g|=2|h|$. Thus $v=0$, but then g has cycle lengths $1,1,2$ on U contradicting Claim 1. In line 4 of Table 4 we have $h=J_d$, and conjugating by a suitable $t_{v'}$, we may assume that $v\in\langle e_1\rangle$. Recalling that we have $|g|=|h|$, we may assume $g=J_2$ (line 2 of Table 5), J_3 (line 5 of Table 7), $t_{e_1}J_3$ (line 3 of Table 7), J_4 (cycle lengths $1,1,2,4,4,4$), J_5 (cycle lengths 1,1,2,4,4,4,8,8) or $t_{e_1}J_5$ (line 8 of Table 7). In line 5 of Table 4, $h=J_2\oplus J_1$ and conjugating by a suitable $t_{v'}$ we may assume that $v\in\langle e_1,e_3\rangle$ and there are four possibilities for v. A computation shows that only the choices $v=0$ and $v=e_3$ give $|g|=|h|$; now another direct calculation shows that we only have an example when $v=e_3$; see line 4 of Table 7. In line 6 of Table 4, Claim 1 implies $g=t_{e_1}(J_3\oplus J_1)$ as in line 6 of Table 7. This completes the analysis of the case $|g|=|h|$.

Henceforth, we shall assume that $|g|=p|h|$. First suppose that g is as in line 2 of Table 2. Then either $d=2$ and $p=2,3$, which gives the examples in line 1 of Table 7; or $(p,d,i)=(2,3,3)$, as in line 10 of Table 7 (these are the possibilities that have $s^i_{d-1}=1$); or else we have the examples in line 4 of Table 5 (when $s^i_{d-1}\neq 1$). If g is as in line 3 of Table 2 then $g=t_{e_1}$ as

in line 3 of Table 5. If g is in line 5 of Table 3 then $p = 3$ and either $g = t_{e_1}(J_1 \oplus J_1 \oplus s_{d-2})$, and g has three cycles on U contradicting Claim 1, or $g = t_{e_1}(J_1 \oplus s_{d_1} \oplus s_{d_2})$ with $(d_1, d_2) = 1$, and these examples do not occur by Claim 3 since $p = 3$. Next, if g is in line 6 of Table 3, then a direct calculation shows that g has cycle lengths $9, 9, 9$ on U and so there are no examples by Claim 1. Next, suppose that g is as in lines 14, 15 of Table 3. Using the notation in Table 3, we have either $d_1 = 1$ or $d_1 \geq 2$. In the former case, $g = t_{e_1}(J_1 \oplus J_1 \oplus h'')$ or $g = t_{e_1}(J_2 \oplus J_1 \oplus h'')$ and Claim 1 implies that h'' is a Singer cycle; see lines 4, 6 of Table 6. In the latter case, we apply Claim 3 to deduce that g must be as in line 7 of Table 6. Now suppose that g is as in line 16 of Table 3 so $g = t_{e_1}(J_4 \oplus h')$; if $h' = s^i_{d-4}$ then we have the examples in line 15 of Table 7 (when $h' = 1$) and line 8 of Table 6 (when $h' \neq 1$. Here, observe that $i = 1$ by Claim 1, and h' cannot be as in line 8 of Table 3 by Claim 3). If g is as in lines 8, 9 of Table 4 then $vh(2) \neq 0$, hence v generates a cyclic h-submodule of order 2^2 and we may assume that $v = e_1$. A direct calculation gives us the examples in line 13 of Table 7. Direct calculation shows that lines 7, 3, 11 of Table 4 give rise to the examples in lines 14, 9, 12, 10 of Table 7 respectively. Similarly line 17 of Table 3 and line 10 of Table 4 give the examples in line 5 of Table 6 and line 11 of Table 7 respectively. □

5. *Maximal subgroups of* $\mathrm{GL}_d(p)$ *containing elements of large order*

Let $g = t_v h \in \mathrm{AGL}(V)$ have order at least $|V|/4 = p^d/4$, so g is as in one of the lines of Tables 2, 3, or 4. In this section we determine which kinds of primitive subgroups of $\mathrm{AGL}(V)$ contain at least one such element. Each primitive subgroup of $\mathrm{AGL}(V)$ is a semidirect product $G = TH$ where T is the group of translations of V and $H \leq \mathrm{GL}(V)$ is irreducible on V. It is convenient to use Aschbacher's description in [**1**] of the maximal subgroups H of $\mathrm{GL}(V)$ not containing $\mathrm{SL}(V)$ (as exploited, for example in [**2**, **11**]). Thus we consider this problem class by class, for maximal subgroups in the various Aschbacher classes $\mathcal{C}_2, \ldots, \mathcal{C}_9$. We discover that subgroups in many Aschbacher classes seldom contain elements of sufficiently large order. First we consider Aschbacher class $\mathcal{C}_2$: here the subgroups are stabilizers $\mathrm{GL}_{d/r}(p) \operatorname{wr} \mathrm{Sym}(r)$ of decompositions $V = \oplus_{i=1}^r V_i$, for some divisor r of d with $r > 1$.

LEMMA 5.1. *Let $d \geq 3$ and let r be a divisor of d with $r > 1$. Let $G = TH$ be a subgroup of $\mathrm{AGL}_d(p)$ with H in the Aschbacher class $\mathcal{C}_2$ of type $\mathrm{GL}_{d/r}(p) \operatorname{wr} \mathrm{Sym}(r)$, and suppose that G contains an element $g = t_v h$ with $|g| \geq p^d/4$. Then $p \in \{2, 3\}$.*

If $p = 3$, then either $r = 2 < d$, or $d = r = 3$. Moreover, the image of h in $H/\mathrm{GL}_{d/r}(p)^r \cong \mathrm{Sym}(r)$ is non-trivial only when $d = r = 3$.

If $p = 2$, then either $d/r \geq 3$, or $d = r \leq 5$, or $d = 2r \leq 6$. For $d/r \geq 3$, the image of h in $\mathrm{Sym}(r)$ is trivial, and moreover, $4r^2 - 21r \leq d$.

Proof. Since $|g| \geq p^d/4$, by Theorem 1.1, the element h is as in Tables 2, 3, or 4. Moreover, $|h| \geq |g|/|t_v| \geq p^{d-1}/4$. In the proof of this lemma we repeatedly use both of these observations on h.

By an inspection of Table 2 it is clear that $h = s^i_d$ and $h = J_1 \oplus s^i_{d-1}$ (with $1 \leq i \leq 3$) are not contained in a $\mathcal{C}_2$ subgroup when $d \geq 3$. Therefore, since $d \geq 3$, h is as in one of the lines of Table 3, or 4, and in particular, $p \in \{2, 3\}$.

Assume that $p = 3$. Observe that, for every even d, $h = J_1 \oplus s_{d_1} \oplus s_{d_2}$ with $d_2 = d_1 + 1 = d/2$ (as in line 5 of Table 3) lies in $\mathrm{GL}_{d/2}(3) \operatorname{wr} \mathrm{Sym}(2)$. Now assume that $r \geq 3$: we show that only $r = d = 3$ is possible. For $d \geq 8$, the descriptions of h in Tables 3 or 4 and a case-by-case analysis immediately eliminates $\mathcal{C}_2$-subgroups not of type $\mathrm{GL}_{d/2}(3) \operatorname{wr} \mathrm{Sym}(2)$. For $3 \leq d \leq 7$, there are maximal $\mathcal{C}_2$-subgroups only when $r = d$, or when $(d, r) = (6, 3)$. A direct calculation

eliminates the possibility $\mathrm{GL}_2(3) \operatorname{wr} \mathrm{Sym}(3)$ (the maximal element order of $\mathrm{GL}_2(3) \operatorname{wr} \mathrm{Sym}(3)$ is 48, and $|h| \geq 3^{6-1}/4 > 48$, a contradiction). Thus $3 \leq r = d \leq 7$. Another direct calculation shows that $T \cdot (\mathrm{GL}_1(3) \operatorname{wr} \mathrm{Sym}(d))$ contains elements $g = t_v h$ of order at least $3^d/4$ only when $d = 3$.

It remains to show that the image of h in $H/\mathrm{GL}_{d/2}(3)^2$ is trivial when $r = 2$. Suppose that $h = (h_1, h_2)(12)$, with $h_1, h_2 \in \mathrm{GL}_{d/2}(3)$. Observe that $h^2 = (h_1h_2, h_2h_1)$ and that $(h_1h_2)^{h_1} = h_2h_1$. Therefore $|h| = 2|h_1h_2| \leq 2\,\mathrm{meo}(\mathrm{GL}_{d/2}(3)) \leq 2(3^{d/2} - 1)$. Since $|h|$ has order at least $3^{d-1}/4$, we get $3^{d-1}/4 \leq 2(3^{d/2} - 1)$, which has a solution only for $d = 4$. Finally a computation in $T \cdot (\mathrm{GL}_2(3) \operatorname{wr} \mathrm{Sym}(2))$ shows that there is no element $t_v h$ of order $\geq 3^4/4$ with h having non-trivial image in $\mathrm{Sym}(2)$.

Assume that $p = 2$. Write $m = d/r$. We consider separately the cases $m = 1$ and $m = 2$. From [**20**, Theorem 2], we see that

$$\log(\mathrm{meo}(\mathrm{Sym}(x))) \leq \sqrt{x \log(x)} \left(1 + \frac{\log(\log(x)) - 0.975}{2\log(x)}\right)$$

for $x \geq 3$, where log indicates the natural logarithm. For simplicity denote by $f(x)$ the exponential of the function on the right hand side of this inequality. For $m = 1$, we have $H = \mathrm{Sym}(d)$. Now $|h| \geq 2^{d-3}$ and hence $2^{d-3} \leq f(d)$. A computation shows that this inequality is satisfied only when $d \leq 9$. Now for these small values of d, by computing the exact value of $\mathrm{meo}(\mathrm{Sym}(d))$ we see with another computation that $d \leq 5$.

Now we consider $m = 2$, that is, $H = \mathrm{GL}_2(2) \operatorname{wr} \mathrm{Sym}(d/2)$. As $|\mathrm{GL}_2(2)| = 6$, we get $2^{d-3} \leq |h| \leq \mathrm{meo}(\mathrm{GL}_2(2) \operatorname{wr} \mathrm{Sym}(d/2)) \leq 6f(d/2)$ and a computation shows that this happens only for $d \leq 8$. Now for these small values of d we see with another explicit computation that $d \leq 6$.

For the rest of the proof we assume that $m \geq 3$. We start by showing that $h \in H$ has trivial image in $H/\mathrm{GL}_m(2)^r$. We write $h = (h_1, h_2, \ldots, h_r)\sigma$ where $h_i \in \mathrm{GL}_m(2)$ and $\sigma \in \mathrm{Sym}(r)$. We argue by contradiction and we assume that $\sigma \neq 1$. Suppose that σ has a cycle of length ℓ. If $\ell = r$ then without loss of generality, we may assume that $\sigma = (12 \ldots r)$. Now an easy computation shows that $(12 \ldots r)(h_1, h_2, \ldots, h_r) = (h_2, h_3, \ldots, h_r, h_1)(12 \ldots r)$. It follows that

$$\begin{aligned} h^r &= (h_1, h_2, \ldots, h_r)\sigma(h_1, h_2, \ldots, h_r)\sigma \ldots (h_1, h_2, \ldots, h_r)\sigma \\ &= (h_1h_2 \ldots h_r,\ h_2h_3 \ldots h_rh_1,\ \ldots,\ h_rh_1 \ldots h_{r-1}). \end{aligned}$$

But

$$h_1h_2 \ldots h_r = h_1(h_2 \ldots h_rh_1)h_1^{-1}$$

and similarly we see that all of the entries of h^r above are conjugate. In particular, they have the same order and since $p = 2$ we have $|h| \leq r\,\mathrm{meo}(\mathrm{GL}_m(2)) = r(2^m - 1) < 2^{m+r-1}$. If $\ell = r \geq 3$ then, since $m \geq 3$, this is less than 2^{d-3}. So the only possibility not eliminated yet in this case is $\ell = r = 2$, and hence σ is a transposition.

Next suppose that $\ell < r$. Then $h \in (\mathrm{GL}_m(2) \operatorname{wr} \mathrm{Sym}(\ell)) \times (\mathrm{GL}_m(2) \operatorname{wr} \mathrm{Sym}(r - \ell))$, which is isomorphic to a subgroup of $(\mathrm{GL}_m(2) \operatorname{wr} \mathrm{Sym}(\ell)) \times \mathrm{GL}_{d-m\ell}(2)$. Using $\ell \leq 2^{\ell-1}$, the same calculation as above shows that $|h| \leq \ell(2^m - 1)(2^{rm-m\ell} - 1) < 2^{rm+m+\ell-m\ell-1}$, and this is at most $2^{d-1}/4 = 2^{mr-3}$ when $m, \ell \geq 3$. Therefore all of the cycles of σ must have length at most 2. If σ has at least two 2-cycles then h can be embedded in $(\mathrm{GL}_m(2) \operatorname{wr} \mathrm{Sym}(2)) \times (\mathrm{GL}_m(2) \operatorname{wr} \mathrm{Sym}(2)) \times \mathrm{GL}_{d-4m}(2)$ and the same argument shows that $|h| < 2^{d-3}$. It follows that σ is a transposition.

When σ is a transposition, up to reordering we may assume that $\sigma = (12)$. Now $h = (h_1, \ldots, h_r)(12)$ and $h^2 = (h_1h_2, h_2h_1, h_3, \ldots, h_r)$. Since h_1h_2 and h_2h_1 are conjugate, we get $|h| \leq 2(\mathrm{meo}(\mathrm{GL}_m(2)))^{r-1} = 2(2^m - 1)^{r-1} < 2^{d-m+1}$. As $|h| \geq 2^{d-3}$, we obtain $d - 3 < d - m + 1$, which gives $m < 4$. Thus $m = 3$. With this information we can now refine our computations. In fact, for $m = 3$, the group $\mathrm{GL}_3(2)$ has exponent 84 and hence $\mathrm{GL}_3(2)^r$ also has exponent 84. Thus $|h| \leq 2 \cdot 84 = 168$. As $|h| \geq 2^{d-3} = 2^{3r-3}$, we have $168 \geq 2^{3r-3}$, which

is satisfied only for $r \leq 3$. For $r = 3$, it can be easily checked with a computer that the elements of $(\mathrm{GL}_3(2) \operatorname{wr} \mathrm{Sym}(2)) \times \mathrm{GL}_3(2)$ have order at most 56. As $56 < 64 = 2^{d-3}$, this case does not arise. For $r = 2$, it is a computation to verify that the maximal order of an element $g = t_v h$ of the affine group $T \cdot (\mathrm{GL}_3(2) \operatorname{wr} \mathrm{Sym}(2))$, with $h = (h_1, h_2)(12)$, is 14. As $14 < 16 = 2^{6-2}$, the case $r = 2$ does not arise either.

It remains to prove that $4r^2 - 21r \leq d$. From the previous paragraphs, we have $h = h_1 \oplus \ldots \oplus h_r$, with $h_1, \ldots, h_r \in \mathrm{GL}_m(2)$. Recall that $|h| = \mathrm{lcm}\{|h_i| \mid i \in \{1, \ldots, r\}\} \geq 2^{d-3}$. If $|h_i|, |h_j|, |h_k| \leq 2^{m-1}$ for some distinct indices i, j and k, then $|h| \leq 2^{3(m-1)}(2^m - 1)^{r-3} < 2^{d-3}$, a contradiction. This shows at most two entries of h have order $\leq 2^{m-1}$. Up to reordering we may assume that $|h_j| > 2^{m-1}$, for every $j \geq 3$, and an inspection of Tables 2, 3, or 4 reveals that h_j is as in line 1 of Table 2 with $i = 1$, or as in line 8 of Table 3, for each $j \geq 3$. If $h_j = h_k = s_m$ for some distinct indices j and k, then $\mathrm{lcm}(|h_j|, |h_k|) = 2^m - 1$ and hence $|h| \leq (2^m - 1)^{r-1} < 2^{d-m} \leq 2^{d-3}$. This shows that there exists at most one index with h_j as in line 1 of Table 2. Therefore, up to reordering, we may assume that h_j is as in line 8 of Table 3 for each $j \geq 4$.

For $i \in \{4, \ldots, r\}$ write $h_i = s_{d_{i,1}} \oplus \ldots \oplus s_{d_{i,t_i}}$, with $d_{i,1}, \ldots, d_{i,t_i} \geq 2$ pairwise coprime and $t_i \geq 2$. Suppose that $d_{i,j}, d_{i',j'}, d_{i'',j''}$ are even, for some i, j, i', j', i'', j'' with i, i' and i'' pairwise distinct. Then $\gcd(|h_i|, |h_{i'}|, |h_{i''}|) \geq 3$ and hence, arguing as above, $|h| \leq (2^m - 1)^r / 3^2 < 2^{d-3}$. So, up to reordering, we may assume that $d_{i,j}$ is odd for every $i \geq 6$ and for every $1 \leq j \leq t_i$.

Repeating the argument in the previous paragraph, we see that (up to the usual reordering) $d_{i,j} \neq 3$ for every $i \geq 7$ and for every $1 \leq j \leq t_i$. Now, if $d_{i,j} = d_{i',j'}$ for some distinct i and i' with $i, i' \geq 7$, then we have $\gcd(|h_i|, |h_j|) \geq 2^5 - 1 = 31$ and a computation shows that $|h| \leq (2^m - 1)^r / 31 < 2^{d-3}$, which is a contradiction. Therefore the numbers $d_{i,j}$, with $7 \leq i \leq r$ and $1 \leq j \leq t_i$, are pairwise coprime, odd and not equal to 3. Since $t_i \geq 2$, we have at least $2(r-6)$ such integers in $\{1, \ldots, m\}$. Since the number of odd numbers greater than 3 in $\{1, \ldots, m\}$ is $\leq (m-3)/2$, we get $2(r-6) \leq (m-3)/2$, which gives the desired result. □

Remark 4. The lower bound on d (as as function of r) when $p = 2$ given in Lemma 5.1 can be improved, as follows:

$$2(r-5) \leq \frac{d/r}{\log(d/r)} \left(1 + \frac{3}{2\log(d/r)}\right).$$

This is essentially a consequence of the last paragraph of the proof of Lemma 5.1, which shows that in the interval $\{1, \ldots, d/r\}$ there are at least $2(r-6)$ distinct pairwise coprime numbers greater than 3, odd, and coprime to 3. Therefore, there must be at least $2(r-5)$ distinct primes in $\{1, \ldots, d/r\}$, and so $2(r-5) \leq \pi(d/r)$, where as usual $\pi(x)$ is the function counting the number of primes $\leq x$. Now $\pi(x) \leq x/\log(x)(1 + 3/(2\log(x)))$ by [**22**, Theorem 1].

In fact, we will now show (assuming the truth of the extended Goldbach conjecture, explained below,) that this improved bound is close to having the correct order of magnitude. Let $\pi_2(n)$ represent the number of ordered pairs of primes (p, q) with $p < q$ and $n = p + q$. Suppose that d' is large and even and $r = \pi_2(d')$, then if $d = d'r$ there is a $g \in \mathrm{GL}_{d/r}(2) \operatorname{wr} \mathrm{Sym}(r)$ with $|g| \geq 2^d/4 = 2^{d-2}$. By the definition of π_2, there exist $(p_1, q_1), \ldots (p_r, q_r)$ pairs of primes with $p_i < q_i$ and $p_i + q_i = d' = d/r$. Clearly, the primes $\{p_i, q_i \mid 1 \leq i \leq r\}$ are all distinct, and hence the numbers in $\{2^{p_i} - 1, 2^{q_i} - 1 \mid 1 \leq i \leq r\}$ are pairwise coprime (since $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$). Let $g = (h_1, \ldots, h_r)$, where $h_i = s_{p_i} \oplus s_{q_i}$. Then

$$|g| = \prod_{i=1}^{r} (2^{p_i} - 1)(2^{q_i} - 1) = 2^d \prod_{i=1}^{r} \left(1 - \frac{1}{2^{p_i}}\right)\left(1 - \frac{1}{2^{q_i}}\right).$$

Observe that $p_i > 2$ since d' is even. So this gives $|g| > 2^d\varepsilon^2$, where

$$\varepsilon = \prod_{i=3}^{\infty}\left(1 - \frac{1}{2^i}\right).$$

It is not hard to compute that $\varepsilon^2 \sim 0.59$ so that $|g| > 2^{d-2}$.

Now, the extended Goldbach conjecture claims that for n large and even, there is a constant C (given in the conjecture) such that

$$\pi_2(n) \geq C\frac{n}{(\log(n))^2}.$$

When $r = \pi_2(d') = \pi_2(d/r)$, this gives

$$r \geq C\frac{d/r}{(\log(d/r))^2}.$$

This shows, as claimed, that (assuming the extended Goldbach conjecture) there exist d and r for which some $g \in \mathrm{GL}_{d/r}(2) \operatorname{wr} \mathrm{Sym}(r)$ has $|g| > 2^d/4$ and d and r come close (asymptotically) to meeting the improved bound given in the first paragraph of this remark.

LEMMA 5.2. *If H is a maximal subgroup of $\mathrm{GL}_d(p)$ of type $\mathcal{C}_4$ containing an element h of order at least $p^{d-1}/4$, then $d = 6$, $p \in \{2, 3\}$ and $H = \mathrm{GL}_2(p) \otimes \mathrm{GL}_3(p)$. Moreover $\mathrm{GL}_2(p) \otimes \mathrm{GL}_3(p)$ contains elements of order at least $p^6/4$ if and only if $p = 2$.*

Proof. By [**16**, Table 3.5A and (4.4.10)], $H = \mathrm{GL}_{d_1}(p) \otimes \mathrm{GL}_{d_2}(p)$ where $2 \leq d_1 < d_2$ and $d = d_1d_2$. It follows that

$$|h| \leq \mathrm{meo}(H) \leq (p^{d_1} - 1)(p^{d_2} - 1) < p^{d_1+d_2}$$

and the last quantity is greater than $p^{d-1}/4$ if and only if $(d_1, d_2) = (2, 3)$, or $p \in \{2, 3\}$ and $(d_1, d_2) = (2, 4)$.

For $(d_1, d_2) = (2, 4)$ and $p \in \{2, 3\}$, a direct computation shows that $\mathrm{meo}(H) \leq p^7/4$ (in fact, $\mathrm{meo}(H) = 30$ when $p = 2$, and 240 when $p = 3$). Hence we may assume that $(d_1, d_2) = (2, 3)$; that is, $H = \mathrm{GL}_2(p) \otimes \mathrm{GL}_3(p)$, and $d = 6$.

Assume $p \geq 5$ and write $h = h_1 \otimes h_2$ with $h_1 \in \mathrm{GL}_2(p)$ and $h_2 \in \mathrm{GL}_3(p)$. If $|h_1| \leq (p^2 - 1)/4$ or $|h_2| \leq (p^3 - 1)/4$, then $|h| \leq |h_1||h_2| \leq (p^2 - 1)(p^3 - 1)/4 < p^5/4$, a contradiction. Thus we may assume that $|h_1| > (p^2 - 1)/4$ and $|h_2| > (p^3 - 1)/4$. Since $|h_1|$ and $|h_2|$ are both integers and since $p \geq 5$, we must have $|h_1| \geq p^2/4$ and $|h_2| \geq p^3/4$. From Tables 2, 3 and 4 we have $h_1 = s_2^i$ and $h_2 = s_3^j$ (with $1 \leq i, j \leq 3$), and a quick computation gives $|h| = |h_1 \otimes h_2| < p^5/4$, which is a contradiction.

Finally, two straightforward computations show that $\mathrm{meo}(\mathrm{GL}_2(2) \otimes \mathrm{GL}_3(2)) = 21 > 2^6/4$ and $\mathrm{meo}(\mathrm{GL}_2(3) \otimes \mathrm{GL}_3(3)) = 104 < 3^6/4$. □

LEMMA 5.3. *If H is a maximal subgroup of $\mathrm{GL}_d(p)$ of type $\mathcal{C}_6$, then $p \geq 5$.*

Proof. When $p = 2$, we note that there are no $\mathcal{C}_6$-subgroups of $\mathrm{GL}_d(2)$. For the conditions in Table 3.5.A of [**16**] would require that $d = r^m$ for some prime $r \neq 2$ and that $p \equiv 1 \pmod{r}$, which is not possible when $p = 2$. If $p = 3$ then the conditions in Table 3.5.A of [**16**] imply that either $r = 2$, $d = 2^m$ and $p \equiv 1 \pmod{4}$, or $r \geq 5$ and $p \equiv 1 \pmod{r}$. Clearly, neither condition holds. □

LEMMA 5.4. *If H is a maximal subgroup of $\mathrm{GL}_d(p)$ of type $\mathcal{C}_7$, where $p = 2, 3$, then H does not contain an element of order at least $p^{d-1}/4$.*

Proof. By [**16**, (4.7.6)], $H = \mathrm{GL}_m(p) \operatorname{wr} \mathrm{Sym}(t)$ where $d = m^t$, $t \geq 2$ and $m \geq 3$. If $p = 2$, it follows that

$$\mathrm{meo}(H) \leq (2^m - 1)^t \,\mathrm{meo}(\mathrm{Sym}(t)) < 2^{mt+t}$$

since $\mathrm{meo}(\mathrm{Sym}(t)) \leq 2^t$ for all t (see, for instance, [**20**, Theorem 2]). The last quantity is at most 2^{d-3} if and only if $mt + t \leq m^t - 3$. It is easily verified that this is the case unless $(m, t) = (3, 2)$. But a direct computation for $(m, t) = (3, 2)$ shows that $\mathrm{meo}(H) = 28$, which is less than 2^6. A similar calculation shows that there are no examples when $p = 3$. □

LEMMA 5.5. *If $d \geq 3$ and H is a maximal subgroup of $\mathrm{GL}_d(p)$ of type $\mathcal{C}_8$ and contains an element h as in Tables 2, 3, or 4, then $H = \mathrm{CSp}_4(2)$, $\mathrm{CSp}_4(3)$, $\mathrm{CSp}_6(2)$ or $\mathrm{GO}_4^+(3)$ or $\mathrm{GO}_3(3)$.*

Proof. Note that $|h| \geq p^{d-1}/4$. First observe that since p is prime, there are no $\mathcal{C}_8$-subgroups of unitary type. Now suppose that H is of symplectic type. In particular, d is even. By [**8**, Lemma 2.10], we have

$$p^{d-1}/4 \leq |h| \leq \mathrm{meo}(H) \leq p^{d/2+1};$$

we seek conditions on p and d for which $p^{d/2+1} \geq p^{d-1}/4$ or equivalently $4p^{d/2+1} \geq p^{d-1}$.

Assume that $p \geq 5$. We have

$$4p^{d/2+1} < p^{d/2+2}$$

and $p^{d/2+2} \leq p^{d-1}$ if and only if $d \geq 6$. Thus $d = 4$. By Tables 2, 3, 4 either $h = s_4^i$ or $J_1 \oplus s_3^i$, with $1 \leq i \leq 3$. In the first case, h acts irreducibly on V and hence lies in a maximal torus of $\mathrm{CSp}_4(p)$ of order $(p-1)(p^2+1)$. Thus $(p^4-1)/3 \leq |h| \leq (p-1)(p^2+1)$, which is easily seen to be false. In the second case, h acts irreducibly on a 3-dimensional subspace of V, however $\mathrm{CSp}_4(p)$ does not contain such elements.

Assume that $p = 3$. Then

$$4p^{d/2+1} < p^{d/2+3}$$

and $p^{d/2+3} \leq p^{d-1}$ if and only if $d \geq 8$. A direct calculation shows that $\mathrm{meo}(\mathrm{CSp}_6(3)) = 56 < 3^5/4$ and $\mathrm{meo}(\mathrm{CSp}_4(3)) = 24 \geq 3^4/4$, in fact $\mathrm{CSp}_4(3)$ is one of the groups in the statement of this lemma.

Assume that $p = 2$. Then $p^{d/2+1} < p^{d-1}/4$ if and only if $d/2 + 1 < d - 3$ if and only if $d > 8$. Direct calculation yields that $\mathrm{meo}(\mathrm{CSp}_8(2)) = 30 < 2^5$, but $\mathrm{meo}(\mathrm{CSp}_6(2)) = 15 \geq 2^3$ and $\mathrm{meo}(\mathrm{CSp}_4(2)) = 6 > 2^3/4$. So if H is of symplectic type then all of the examples are listed in the Lemma.

Now suppose H is of orthogonal type, that is, $H = \mathrm{GO}_d^\varepsilon(p)Z$ where Z is the subgroup of $\mathrm{GL}_d(p)$ of scalar matrices. Observe that by [**16**, Table 3.5A, Column IV], p is odd because H is maximal.

Assume that $p \geq 5$. By Tables 2, 3, 4 since $d \geq 3$ we have two possibilities for h: either $h = s_d^i$ or $h = J_1 \oplus s_{d-1}^i$, with $1 \leq i \leq 3$. In the first case, h acts irreducibly on V and hence (by considering the structure of the maximal tori of H) d is even and h lies in a maximal torus of order $(p-1)(p^{d/2}+1)$. Thus $(p^d-1)/3 \leq |h| \leq (p-1)(p^{d/2}+1)$, which is easily seen to be false for every $d \geq 3$. In the second case, h acts irreducibly on a subspace of V of dimension $d-1$ and fixes a non-zero vector of V. By considering the structure of the maximal tori of H, we get that d is odd and that h lies in a maximal torus of order $\leq (p-1)(p^{(d-1)/2}+1)$. Thus $(p^{d-1}-1)/3 \leq |h| \leq (p-1)(p^{(d-1)/2}+1)$, which is easily seen to be false for every odd $d \geq 5$.

Therefore $d = 3$ and $H = \mathrm{GO}_3(p)Z$. A computation shows that the matrix $h = J_1 \oplus s_2^i$ lies in $\mathrm{GO}_3(p)Z$ only if h lies in $\mathrm{GO}_3(p)$. Therefore, h has order at most $p+1$. Thus $(p^2-1)/3 \leq |h| \leq p+1$, a contradiction.

Assume that $p = 3$. Now from [**8**, Corollary 2.12] we see that $\mathrm{meo}(\mathrm{GO}_d^\epsilon(3)) \leq 3^{d/2+1}$; a direct calculation shows that this is less than $3^{d-1}/4$ unless $d \leq 6$. Now it is straightforward to check that the only groups of orthogonal type containing elements in Tables 2, 3, 4 are those listed in the lemma. □

LEMMA 5.6. *Let $d \geq 3$, let $p \in \{2,3\}$ and let H be a subgroup of type $\mathcal{C}_9$ with H maximal in $\mathrm{SL}_d(p)$ or maximal in $\mathrm{GL}_d(p)$. If H contains an element h with $|h| \geq p^{d-1}/4$, then $p = 2$ and $(H,d) = (\mathrm{Alt}(6),3)$ or $(\mathrm{Alt}(7),4)$, or $p = 3$ and $(H,d) = (2.M_{11},5)$.*

Proof. We use the "bar notation" to denote the natural projection of $\mathrm{GL}_d(p)$ onto $\mathrm{PGL}_d(p)$. Observe that $\overline{H}$ is an almost simple group containing an element of order $\geq p^{d-1}/(4(p-1))$. Let $\overline{H}_0$ be the socle of $\overline{H}$. By [**19**, Corollary 4.3], if $H \in \mathcal{C}_9$ then either

(i) $|\overline{H}| < p^{2d+4}$; or
(ii) $d = (m-1)m/2$ and $\overline{H}_0 = \mathrm{PSL}_m(p)$; or
(iii) $d = 27$, 16 or 11 and $\overline{H}_0 = E_6(p)$, $\mathrm{P\Omega}_{10}^+(p)$ or M_{24} respectively.

Note that the alternating groups $\mathrm{Alt}(n)$ acting on their deleted permutation modules of dimensions $n-1$ or $n-2$ do not arise since such groups are contained in an orthogonal or symplectic group and so do not give rise to maximal $\mathcal{C}_9$-subgroups [**19**, p. 440-441]. Suppose that (iii) holds. It is easy to check with [**7**] that for $\overline{H_0} = E_6(2)$, $\mathrm{P\Omega}_{10}^+(2)$ and M_{24}, the group $\mathrm{Aut}(\overline{H}_0)$ does not contain an element of order at least $2^{d-1}/4$. If $p = 3$, then using [**13**, Table A.7], we have

$$\mathrm{meo}(\mathrm{Aut}(E_6(p))) \leq |\mathrm{Out}(E_6(p))|\,\mathrm{meo}(E_6(p)) = 2(3,p-1)\frac{(p+1)(p^5-1)}{(3,p-1)} < \frac{p^{27-1}}{(4(p-1))}.$$

Similarly, using [**13**, Table A.5], if $p = 3$, then

$$\mathrm{meo}(\mathrm{Aut}(\mathrm{P\Omega}_{10}^+(p))) \leq |\mathrm{Out}(\mathrm{P\Omega}_{10}^+(p))|\,\mathrm{meo}(\mathrm{P\Omega}_{10}^+(p)) \leq 2(p-1,4)\frac{(p^4+1)(p+1)}{(p-1,4)} < \frac{p^{16-1}}{4(p-1)}.$$

Suppose that (ii) holds. Observe that $m \geq 3$ because $\overline{H}_0$ must be simple. Moreover, for $m = 3$, we have $d = 3 = m$ and hence $\mathrm{SL}_d(p) \leq H$, which is a contradiction. For $m = 4$, we have $d = 6$ and the embedding of $\mathrm{PSL}_4(p)$ into $\mathrm{PSL}_d(p)$ described in [**19**, Section 4] is determined by the action of $\mathrm{PSL}_4(p)$ on the wedge product $\wedge^2 W$, where W is the natural 4-dimensional module of $\mathrm{PSL}_4(p)$. However, this is exactly the embedding that determines the isomorphism $\mathrm{PSL}_4(p) \cong \mathrm{P\Omega}_6^+(p)$. Therefore, since we are assuming that $H \in \mathcal{C}_9$, we must also have $m \neq 4$. Thus $m \geq 5$. From [**8**, Table 3], for $(m,p) \neq (3,2)$, we have $\mathrm{meo}(\overline{H}) \leq \mathrm{meo}(\mathrm{Aut}(\overline{H}_0)) = (p^m - 1)/(p-1)$. Now a computation shows that the inequality $(p^m-1)/(p-1) \geq p^{d-1}/(4(p-1))$ is never satisfied.

Now suppose that (i) holds. Assume that $d \geq 10$ and $p = 2$. In particular, $\overline{H} = H$ and H contains an element of order $\geq 2^{d-1}/4 = 2^{d-3}$. We claim that there are no examples here. For suppose that $H_0 = \mathrm{PSL}_m(q)$, for some m and for some prime power q. From [**8**, Table 3] we have $\mathrm{meo}(H) \leq (q^m-1)/(q-1)$ or $(m,q) \in \{(2,4),(3,2)\}$. If $\mathrm{meo}(H) \leq (q^m-1)/(q-1)$ then $2^{d-3} \leq (q^m-1)/(q-1)$, while $2^{2d+4} > |H| > \frac{1}{2(m,q-1)}q^{m^2-1}$ (see [**6**, Proposition 3.9(i)] for example). A direct calculation shows that these bounds cannot both hold when $d \geq 10$. If $(m,q) = (2,4)$ or $(3,2)$ and $d \geq 10$ then it is clear that H cannot contain an element of order at least 2^{d-3}. Similarly we take each possible simple group of Lie type in turn and direct calculation shows that the analogous bounds cannot hold when $d \geq 10$. We use the bounds on $\mathrm{meo}(H)$ from [**8**, Table 5]. For example if $H_0 = {}^2F_4(q)$, where $q = 2^f$, then we

have $q^{26}/2 < |H| < 2^{2d+4}$ but $\mathrm{meo}(H) \leq 16f(q^2\sqrt{2q^3} + q + \sqrt{2q} + 1)$ and so $16f(q^2\sqrt{2q^3} + q + \sqrt{2q} + 1) \geq 2^{d-3}$. If $d \geq 10$ then these bounds can only hold when $d = 11$ and $q = 2$ but it is straightforward to check in [**7**] that in this case $\mathrm{meo}(H) \leq 20 < 2^{d-3}$. As a final example, if $H_0 = {}^2B_2(q)$ where $q = 2^f \geq 8$, then we have $\mathrm{meo}(H) \leq f(q + \sqrt{2q} + 1)$ so we have the bounds $f(q + \sqrt{2q} + 1) \geq 2^{d-3}$, $q^5/2 \leq |H| < 2^{2d+4}$, and $d \geq 10$. Direct calculation finds that these bounds are only satisfied when $f = 5$ and $d = 10$, but then we can check in `magma` that $\mathrm{meo}(\mathrm{Aut}({}^2B_2(2^5))) = 41 < 2^{10-3}$. If $H_0 = \mathrm{Alt}(m)$ $(m \geq 5)$, then we have $2^{d-3} \leq \mathrm{meo}(H) < e^{3/2\sqrt{m\log(m)}}$ by [**17**, **20**]. We also have $m!/2 < |H| < 2^{2d+4}$ and a direct calculation shows that these bounds can only hold if $d \leq 16$. But if $10 \leq d \leq 16$ then the bounds imply $m \leq 14$ and we can obtain a much sharper upper bound on $\mathrm{meo}(H)$ by calculating the explicit value of $\mathrm{meo}(\mathrm{Aut}(\mathrm{Alt}(m)))$ in `magma`. Further direct calculation then shows that these stronger bounds cannot hold when $d \geq 10$. We note that if H is a sporadic group, then [**7**] tells us that we have $2^{d-3} \geq \mathrm{meo}(H)$ for $d \geq 10$.

Assume that $d \geq 10$ and $p = 3$. We carry out the same analysis as for $p = 2$ and $d \geq 10$ and we see that no example arises.

Assume that $d \leq 9$. Using the tables in Kleidman's thesis [**15**], the only $\mathcal{C}_9$ subgroups in $\mathrm{GL}_d(2)$ with $d \leq 9$ are $\mathrm{Alt}(6) \leq \mathrm{GL}_3(2)$, $\mathrm{Alt}(7) \leq \mathrm{GL}_4(2)$ and $\mathrm{PGL}_3(4).2 \leq \mathrm{GL}_9(2)$. But $\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(4))) = 21 < 2^6$ and so we are left with the two examples in the lemma. The only $\mathcal{C}_9$ subgroups in $\mathrm{PGL}_d(3)$ with $d \leq 9$ have $(\overline{H}_0, d) = (M_{11}, 5)$, $(\mathrm{PSL}_2(11), 6)$, $(\mathrm{PSL}_3(3), 6)$ and $(\mathrm{PSL}_3(9), 9)$. Calculating $\mathrm{meo}(\mathrm{Aut}(\overline{H}_0))$ precisely in `magma` in each case yields that this is less than $3^{d-1}/8$ unless $(\overline{H}_0, d) = (M_{11}, 5)$ and this case is listed in the lemma. □

REMARK 5. The reader may have noticed that the lemmas in this section consider the Aschbacher classes $\mathcal{C}_2$, $\mathcal{C}_4$, $\mathcal{C}_6$, $\mathcal{C}_7$, $\mathcal{C}_8$, and $\mathcal{C}_9$. Since $G_0 = G \cap \mathrm{GL}(V)$ acts irreducibly on V, type $\mathcal{C}_1$ cannot arise. The elements in $\mathcal{C}_5$ are stabilizers of subfields of $\mathbb{F}_p$, however, since $|\mathbb{F}_p|$ is prime, there is no proper subfield and hence $\mathcal{C}_5$ is empty. The groups of type $\mathcal{C}_3$ will be considered in our proof of Theorem 1.2, and will give rise to some examples. When G_0 is contained in a $\mathcal{C}_3$-subgroup, note that elements of $\mathcal{C}_3$ are stabilizers of extension fields of $\mathbb{F}_p$ of prime index, that is, subgroups isomorphic to $\mathrm{GL}_a(p^b) \rtimes C_b$ with $d = ab$ and b prime. In particular, if h lies in one of these groups we see that the dimensions of an indecomposable decomposition of h^b can be grouped together so that the dimension of every group is a multiple of b. A tedious inspection of Tables 2, 3, and 4 eliminates most of the cases.

6. *Proofs of Theorems 1.2 and 1.4*

Proof of Theorem 1.2. Write $g = t_v h$, with $t_v \in T$ and $h \in G_0$, and observe that g and h are in Tables 2, 3, or 4. In particular $|h| \geq p^{d-1}/4$. If $G_0 \geq \mathrm{SL}_d(p)$ then part (1) of the statement holds, so we assume that $G_0 \not\geq \mathrm{SL}_d(p)$. We divide the proof into various cases.

CASE $d = 2$. For $p \leq 13$, we use `magma` to verify that the only examples occur in Theorem 1.2. So we may assume that $p \geq 17$; in particular, $h = s_2^i$, or $J_1 \oplus s_1^i$ or $s_1^i \otimes J_2$, for some $1 \leq i \leq 3$. Let $Z = Z(\mathrm{GL}_2(p))$ and consider $\mathrm{PGL}_2(p) = \mathrm{GL}_2(p)/Z$. We note that in all three cases, $|hZ| \geq (p-1)/3$. Now G_0Z/Z is a (not necessarily proper) subgroup of a group M, where either M is a maximal subgroup of $\mathrm{PGL}_2(p)$ (not equal to $\mathrm{PSL}_2(p)$) or M is a maximal subgroup of $\mathrm{PSL}_2(p)$. The maximal subgroups of $\mathrm{PGL}_2(p)$ for p odd are described in [**14**, Corollary 2.3] (we use the terminology introduced in [**14**, Section 2]), and the maximal subgroups of $\mathrm{PSL}_2(p)$ were determined by Dickson (see [**23**, Chapter 3, Section 6]). Thus G_0Z/Z is contained in one of the following groups M:

(i) a dihedral group of order $2(p-1)$ (setwise stabilizer of a pair of points),
(ii) a dihedral group of order $2(p+1)$ (setwise stabilizer of a pair of imaginary points),

(iii) a reducible subgroup of order $p(p-1)$ (point stabilizer),
(iv) Sym(4), Alt(4), or Alt(5).

Since G_0 is irreducible, M cannot be of type (iii). If M is of type (iv), then $(p-1)/3 \leq |h| \leq \max\{\mathrm{meo}(\mathrm{Sym}(4)), \mathrm{meo}(\mathrm{Alt}(4)), \mathrm{meo}(\mathrm{Alt}(5))\} = 5$, which is a contradiction since $p \geq 17$. If M is of type (i), then $G_0 \leq \mathrm{GL}_1(p) \operatorname{wr} \mathrm{Sym}(2)$ and part (3)(iii) of Theorem 1.2 holds. Suppose finally that M is of type (ii). Then $G_0 \leq \Gamma\mathrm{L}_1(p^2)$ and, in order to conclude that part (2) of Theorem 1.2 holds, we need to show that $[\mathrm{GL}_1(p^2) : G_0 \cap \mathrm{GL}_1(p^2)] \leq 3$. Observe that $|G_0|$ is coprime to p and hence $h = s_2^i$ or $h = J_1 \oplus s_1^i$. In the first case $[\mathrm{GL}_1(p^2) : G_0 \cap \mathrm{GL}_1(p^2)] \leq [\mathrm{GL}_1(p^2) : \mathrm{GL}_1(p^2) \cap \langle s_2^i \rangle] \leq i \leq 3$. In the second case $h = J_1 \oplus s_1^i$ fixes a non-zero vector and, as every non-identity element of $\mathrm{GL}_1(p^2)$ acts fixed point freely on $V \setminus \{0\}$, we have $\langle h \rangle \cap \mathrm{GL}_1(p^2) = 1$. Since $|\Gamma\mathrm{L}_1(p^2) : \mathrm{GL}_1(p^2)| = 2$, we must have $|h| \leq 2$, contradicting the facts that $|h| \geq (p-1)/3$ and $p \geq 17$.

Case $d \geq 3$ and $p \geq 5$. We have that $g = s_d^i$ or $t_{e_1}(J_1 \oplus s_{d-1}^i)$ (with $1 \leq i \leq 3$) by Tables 2, 3, 4. If $(d,p) \neq (6,5), (7,5)$, then [**10**, Lemma 2.1 and Theorem 2.2] imply that $h \in \mathrm{GL}_d(p)$ is either contained in a $\mathcal{C}_3$- or a $\mathcal{C}_8$-subgroup, or h is contained in one of the $\mathcal{C}_9$-subgroups listed in [**10**, Table 1]. Analysing the possibilities in [**10**, Table 1], we see that either $d = 9$ and G_0 normalises $\mathrm{SL}_3(p^2)$, or G_0 is contained in a $\mathcal{C}_3$-subgroup, or G_0 is contained in a $\mathcal{C}_8$-subgroup. In the third case, Lemma 5.5 shows that none of these subgroups contain elements of the required order.

Suppose next that $d = 9$ and that G_0 normalises $\mathrm{SL}_3(p^2)$. This possibility is eliminated since the image of G_0 in $\mathrm{PGL}_d(p)$ is almost simple and hence $\mathrm{meo}(G_0) \leq (p-1)\,\mathrm{meo}(\mathrm{Aut}(\mathrm{PSL}_3(p^2))) = (p^6-1)/(p+1)$, which is less than $p^8/4$. If $(d,p) = (6,5), (7,5)$ then we can check in `magma` that G_0 must be contained in a $\mathcal{C}_3$ subgroup in this case as well.

For $d \geq 3$, only the elements of the form s_d^i are contained in $\mathcal{C}_3$ subgroups and (in this case) we can use [**11**] and [**2**] to show that the only possibility for G_0 is either to be as in (1), or as in (2) (here, the condition $[\mathrm{GL}_1(p^d) : G_0 \cap \mathrm{GL}_1(p^d)] \leq 3$ follows from $1 \leq i \leq 3$).

Case $3 \leq d \leq 8$ and $p = 2$, or $3 \leq d \leq 7$ and $p = 3$. Here we can check the primitive groups of affine type in the libraries stored in `magma`. We list the possibilities in Table 1.

Case $d \geq 8$ and $p = 3$. By Tables 2, 3, 4, we may assume that either $h = J_1 \oplus s_{d/2} \oplus s_{d/2-1}$, or some power of h has order a primitive prime divisor of $3^e - 1$ with $e > d/2$. Applying Aschbacher's theorem, we see that $G_0 \leq \mathrm{GL}_d(3)$ must be contained in a subgroup of type $\mathcal{C}_i$ for some $i = 1, \ldots, 9$. Since $d \geq 8$, Lemmas 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, and Remark 5 imply that either G is as in (3)(ii), or G_0 is contained in a $\mathcal{C}_3$-subgroup. In the latter case, Tables 2, 3, 4 imply that $g = s_d^i$. Now we can use [**11**] and [**2**] to show that G is as in (1) or (2). We note that all of these subgroups contain elements from Tables 2, 3, 4.

Case $d \geq 9$ and $p = 2$. Again we apply Aschbacher's theorem together with Lemmas 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, and Remark 5. Since $d \geq 9$, we find that the only possibilities are that G is as in (3)(i), or G_0 is contained in a $\mathcal{C}_3$-subgroup. In the latter case, Tables 2, 3, 4 imply that $g = s_a \oplus s_b$ with $(a,b) = 2$ and $G_0 \leq \mathrm{GL}_{d/2}(4) : 2 = \Gamma\mathrm{L}_{d/2}(4)$, or $g = s_d^i$. Using [**2**] we find that G is as in (1) or (2) when $g = s_d^i$.

Next suppose then $g = s_a \oplus s_b$ and $G_0 \leq \Gamma\mathrm{L}_{d/2}(4)$. We claim that the only possibility is that G_0 contains $\mathrm{SL}_{d/2}(4)$ as in case (1). We argue by contradiction and we suppose that G_0 does not contain $\mathrm{SL}_{d/2}(4)$. Observe that since g has odd order, we have $g \in G_0 \cap \mathrm{GL}_{d/2}(4)$. Since $g \in G_0 \cap \mathrm{GL}_{d/2}(4)$, the element g, when viewed as an element of $\mathrm{GL}_{d/2}(4)$, is of the form $s_{a/2} \oplus s_{b/2}$ (and $(a/2, b/2) = 1$). Without loss of generality, suppose that $a/2 > b/2$. Let ℓ be the largest divisor of $4^{a/2} - 1$ that is relatively prime to $4^m - 1$ for every $1 \leq m < a/2$. By [**10**, Lemma 2.1 (c)] and the comments that precede that lemma, we see that either $\ell > a + 1$, or $a/2 \in \{3, 6\}$. Observe that when $a/2 = 3$ we must have $(d,a,b) = (10,6,4)$ (because $(a,b) =$

2 and $d \geq 9$), and when $a/2 = 6$ we must have $(d, a, b) \in \{(14, 12, 2), (22, 12, 10)\}$ (because $(a, b) = 2$).

Now we deal with the three possibilities $(d, a, b) \in \{(10, 6, 4), (14, 12, 4), (22, 12, 10)\}$. Here $g \in G_0 \leq \mathrm{GL}_{d/2}(4)$ and some power of g has order $a + 1$, a primitive prime divisor of $4^{a/2} - 1$. We can check easily in `magma` that if $G_0 \leq \mathrm{GL}_5(4)$ is irreducible and contains $g = s_6 \oplus s_4$, then G_0 contains $\mathrm{SL}_5(4)$. So we may assume that $(d, a, b) \neq (10, 6, 4)$. Now an analysis (using [**11**]) shows that if $(d, a, b) = (22, 12, 10), (14, 12, 2)$, then the only irreducible G_0 containing g must contain $\mathrm{SL}_{d/2}(4)$ as in case (1) (the analysis in our two cases is straightforward since, in the notation of [**11**], we have $r = 13$, $e = 6$, $r = 2e + 1$, and $d = 7$ or 11, and so there are very few possibilities for G_0).

It remains to consider the case that $\ell > a + 1$, where ℓ is the largest divisor of $4^{a/2} - 1$ coprime to $4^m - 1$ for every $1 \leq m < a/2$. Now a power of g has order ℓ, and [**10**, Theorem 2.2] applied to this power of g implies that the irreducible subgroup $G_0 \cap \mathrm{GL}_{d/2}(4)$ of $\mathrm{GL}_{d/2}(4)$

(i) contains $\mathrm{SL}_{d/2}(4)$ (but we are assuming this is not the case), or
(ii) is contained in $\mathrm{GU}_{d/2}(2)$, $\mathrm{GSp}_{d/2}(4)$, or $\mathrm{GO}^{\epsilon}_{d/2}(4)$, or
(iii) preserves an extension field structure (but this is not the case since $(a/2, b/2) = 1$), or
(iv) normalizes $\mathrm{GL}_{d/2}(2)$, or
(v) normalizes one of the nine subgroups listed in [**10**, Table 1].

In particular, $G_0 \cap \mathrm{GL}_{d/2}(4)$ satisfies either (ii), (iv) or (v). Using $d \geq 9$ and $(a/2, b/2) = 1$, an immediate check of [**10**, Table 1] reveals that no example arises in our case. A calculation shows that $\mathrm{GU}_{d/2}(2)$, $\mathrm{GSp}_{d/2}(4)$, and $\mathrm{GO}^{\epsilon}_{d/2}(4)$ do not contain elements of order $|g| = (4^{a/2} - 1)(4^{b/2} - 1)/3$ (see [**8**] for example) so $G_0 \cap \mathrm{GL}_{d/2}(4)$ does not satisfy (ii) either. Similarly, if G_0 satisfies (iv), then G_0 cannot contain elements of order as large as $|g|$.

Thus we have shown in all cases that G_0 satisfies one of the conditions (1)–(4) in the statement of Theorem 1.2. □

Proof of Theorem 1.4. Since G contains an element $g = t_v h$ with at most four cycles on V, we have $|g| \geq p^d/4$ and hence G and G_0 appear in Theorem 1.2. The examples in (2) of Theorem 1.2 contain elements of the form s^i_d (for $1 \leq i \leq 3$), and these elements have at most four cycles; thus we have the examples in (1) of Theorem 1.4 with $r = d$. Now suppose that G is as in (1) of Theorem 1.2. When $d \leq 8$ and $p = 2$, or $d \leq 7$ and $p = 3$, or $d = 2$ and $p \leq 13$ we check in `magma` that the only examples appear in Theorem 1.4. So we suppose that d and p do not satisfy these bounds.

First suppose that $r = 1$. If $p = 2$ then $G_0 = \mathrm{GL}_d(2)$ as in (1) of Theorem 1.4. If $p = 3$ then G_0 contains $\mathrm{SL}_d(3)$, which contains s^2_d as in (1) of Theorem 1.4. If $p \geq 5$ then Tables 5, 6, 7 imply that $h = s_1 \otimes J_2$ (and $d = 2$) or $h = s^i_d$ or $h = J_1 \oplus s^i_{d-1}$ (for $i = 1, 2, 3$). Since G_0 contains $\mathrm{SL}_d(p)$ and h, and since $\det(h)$ has multiplicative order $(p - 1)$, $(p - 1)/2$ or $(p - 1)/3$, it follows that G_0 contains s^i_d as in (1) of Theorem 1.4.

Now suppose that $r \geq 2$. The analysis in the proof of Theorem 1.2 implies that (under our restrictions on d and p) if $g \in G$ then $g = s^i_d$, or $p = 2$ with $g = s_a \oplus s_b$, $(a, b) = 2$ and (therefore) $r = 2$. But if $p = r = 2$ then G_0 contains $\mathrm{SL}_{d/2}(4)$, which contains s^i_d. Thus G satisfies (1) of Theorem 1.4 in all cases of (1) of Theorem 1.2.

We verify using `magma` that the only groups in (4) of Theorem 1.2 that admit a permutation with at most four cycles are those indicated with a "y" in Table 1.

Finally, suppose that G and G_0 are as in (3) of Theorem 1.2. Assume that $p = 2$. Thus $G_0 \leq \mathrm{GL}_{d/r}(2) \operatorname{wr} \mathrm{Sym}(r)$ for some divisor r of d with $r > 1$. If $d/r \leq 2$, then from Lemma 5.1 we have either $d = r \leq 5$ or $d = 2r \leq 6$. It is a computation to show that in each of these cases G contains an element with at most four cycles. So now suppose that $d/r \geq 3$. Now Lemma 5.1 implies that $h \in \mathrm{GL}_{d/r}(2)^r$. For $d > 9$, with a direct inspection of Tables 5, 6, 7, we see that h is the sum of at most three indecomposable summands and hence $r \leq 3$. Moreover, a more careful

inspection shows that in each case h has an indecomposable summand acting irreducibly on a subspace of V of dimension $\geq d/2$. Clearly this shows that $r = 2$. (Observe that the case $r = 2$ does arise from line 7 of Table 6 with $a = 1$, $a_1 = d/2 - 1$ and $a_2 = d/2$.) The cases $d \leq 8$ can be easily dealt with the help of a computer.

Assume that $p = 3$. Thus $G_0 \leq \mathrm{GL}_{d/r}(3) \operatorname{wr} \mathrm{Sym}(r)$ for some divisor r of d with $r > 1$. If $d = r$, then Lemma 5.1 implies that $d = r \leq 3$. Now a computation shows that in each of these cases G contains an element with at most four cycles. So now suppose that $d > r$, and Lemma 5.1 implies that $r = 2$. A computation shows that $T \cdot (\mathrm{GL}_2(3) \operatorname{wr} \mathrm{Sym}(2))$ has no element with at most four cycles and hence we may assume that $d \neq 4$. Now Lemma 5.1 implies that $h \in \mathrm{GL}_{d/2}(3)^2$. Since $d \geq 6$, a direct inspection of Tables 5, 6, 7 implies that h has an indecomposable summand acting irreducibly on a subspace of V of dimension $\geq d - 1$, which is clearly a contradiction.

Finally suppose that $p \geq 5$. In this case the element $J_1 \oplus s_d$ is always contained in $\mathrm{GL}_1(p) \operatorname{wr} \mathrm{Sym}(2)$. □

References

1. M. Aschbacher, 'On the maximal subgroups of the finite classical groups', *Invent. Math.* **76** (1984), no. 3, 469–514.

2. J. Bamberg and T. Penttila, 'Overgroups of cyclic Sylow subgroups of linear groups', *Comm. Algebra* **36** (2008), 2503–2543.

3. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24** (1997), 235–265.

4. D. Bubboloni and C. E. Praeger, 'Normal coverings of finite symmetric and alternating groups', *J. Combin. Theory Ser. A* **118** (2011), 2000–2024.

5. D. Bubboloni, C. E. Praeger and P. Spiga, 'A sharp upper bound on the normal covering number of $\mathrm{Sym}(n)$', in preparation.

6. T. C. Burness, 'Fixed point ratios in actions in finite classical groups II', *Journal of Algebra* **309** (2007), 80–138.

7. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

8. S. Guest, J. Morris, C. E. Praeger and P. Spiga, 'On the maximum orders of elements of finite almost simple groups and primitive permutation groups', submitted, arXiv:1301.5166 [math.GR].

9. S. Guest, J. Morris, C. E. Praeger and P. Spiga, 'Finite primitive permutation groups containing a permutation with at most four cycles', in preparation.

10. R. M. Guralnick and G. Malle, 'Products of conjugacy classes and fixed point spaces', *J. Amer. Math. Soc.*, May 2011.

11. R. M. Guralnick, T. Penttila, C. E. Praeger and J. Saxl, 'Linear groups with orders having certain large prime divisors', *Proc. London Math. Soc.* **78** (1999), 167–214.

12. B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, London, 1971.

13. W. M. Kantor and Á. Seress, 'Large element orders and the characteristic of Lie-type simple groups', *J. Algebra* **322** (2009), 802–832.

14. O. H. King, 'The subgroup structure of finite classical groups in terms of geometric configurations'. *Surveys in combinatorics 2005, London Math. Soc. Lecture Note Ser.*, 327, Cambridge Univ. Press, Cambridge, 2005.

15. P. B. Kleidman, 'The subgroup structure of some finite simple groups', PhD thesis, University of Cambridge, 1987.

16. P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Notes Series **129**, Cambridge University Press, Cambridge.

17. E. Landau, 'Über die Maximalordnung der Permutationen gegebenen Grades', *Arch. Math. Phys.* **5** (1903), 92–103.

18. E. Landau, *Handbuch der Lehre vor der Verteilung der Primzahlen*, Teubner, Leipzig, 1909.

19. M. W. Liebeck, 'On the orders of maximal subgroups of the finite classical groups', *Proc. London Math. Soc. (3)* **50** (1985), 426–446.

20. J. P. Massias, J. L. Nicolas and G. Robin, 'Effective Bounds for the Maximal Order of an Element in the Symmetric Group', *Mathematics of Computation* **53** (1989), 665–678.

21. P. Müller, 'Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials', *Ann. Scuola Norm. Sup. Pisa* **12** (2013), to appear.

22. J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

23. M. Suzuki, *Group theory I*, Springer-Verlag, New York, 1982.

Simon Guest
Department of Mathematics,
University of Southampton,
Highfield,
Southampton, SO17 1BJ,
United Kingdom

s.d.guest@soton.ac.uk

Joy Morris
Department of Mathematics and Computer Science,
University of Lethbridge,
Lethbridge, AB. T1K 3M4,
Canada

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

Cheryl.Praeger@uwa.edu.au

Pablo Spiga
Dipartimento di Matematica e Applicazioni,
University of Milano-Bicocca,
Via Cozzi 53,
20125 Milano,
Italy

pablo.spiga@unimib.it