J. Austral. Math. Soc. (Series A) **67** (1999), 223–253

A RECOGNITION ALGORITHM FOR NON-GENERIC CLASSICAL GROUPS OVER FINITE FIELDS

ALICE C. NIEMEYER and CHERYL E. PRAEGER

Dedicated to M. F. (Mike) Newman on the occasion of his 65th birthday

(Received 24 March 1999; revised 18 May 1999)

Communicated by E. A. O'Brien

Abstract

In a previous paper the authors described an algorithm to determine whether a group of matrices over a finite field, generated by a given set of matrices, contains one of the classical groups or the special linear group. The algorithm was designed to work for all sufficiently large field sizes and dimensions of the matrix group. However, it did not apply to certain small cases. Here we present an algorithm to handle the remaining cases. The theoretical background of the algorithm presented in this paper is a substantial extension of that needed for the original algorithm.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary: 20G40 and 20-04, secondary 60B99 and 20C20.
Keywords and phrases: matrix groups, recognition algorithm, non-generic.

1. Introduction

In [10] we described an algorithm for recognising whether a given subgroup G of the general linear group $\mathrm{GL}(d, q)$ contains the special linear group or one of the other classical matrix groups. The algorithm seeks special types of elements in a classical group by repeated independent random selection, and if the dimension d of the classical group is sufficiently large such elements may readily be found after a number of selections. However, for certain small values of the dimension d, depending on the type of the classical group and on the order q of the field, there are insufficient elements of the required kind in the classical groups and the algorithm presented in

[10] is not applicable in these cases. For these small values of d a modification of the algorithm is needed and is described here. We call this the non-generic version of the classical recognition algorithm. Since procedures for recognising the special linear group or one of the classical groups for $d = 2$ were given in [8] we shall assume that $d \geq 3$. As in [10] we shall assume that we know that G is irreducible on the underlying vector space V and also that we have identified any non-degenerate bilinear, sesquilinear, or quadratic forms which are left invariant modulo scalars by the group G.

In Section 2 we define the principal kinds of elements which we seek by random selection, and we also specify the values of d and q, for each type of classical group, which we need to consider in this paper. Classical groups with these values of d and q will be called *non-generic*. In Section 3 we derive from the results in [4] and [10] a restricted list of subgroups of $GL(d, q)$ which may contain elements of some of these types. The proportions of these elements in classical groups are determined in Section 4. All this information is brought together in Section 5. Here we determine, for each of the non-generic classical groups, a small set of elements such that the only subgroups of the classical groups containing such a set, are subgroups containing the relevant subgroup Ω, where Ω is $\mathrm{SL}(d, q)$, $\mathrm{Sp}(d, q)$, $\Omega^{\epsilon}(d, q)$, or $\mathrm{SU}(d, q)$ according to the type of classical group. We also provide lower bounds for the proportions in Ω of each type of element occurring in these sets. The main results are Theorem 5.1–Theorem 5.6. We note that the families $\mathrm{O}^{+}(8, q)$, $\mathrm{Sp}(4, q)$, and $\mathrm{O}^{+}(4, q)$ presented the greatest challenges for us in devising appropriate procedures for identifying them. Section 6 reports briefly on algorithms for identifying the additional special elements sought in this paper and the effectiveness of an implementation of the resulting algorithm for recognising when a given subgroup of a non-generic classical group contains the subgroup Ω.

2. Non-generic parameters

For integers $b, e > 1$ a *primitive prime divisor* (or ppd for short) of $b^e - 1$ is a prime dividing $b^e - 1$ but not dividing $b^i - 1$ for any integer i such that $1 \leq i < e$. Thus a prime divisor r of $b^e - 1$ is a primitive prime divisor if and only if b has order e modulo r, and hence $r \equiv 1 \pmod{e}$. The following result concerning their existence is due to Zsigmondy [13].

THEOREM 2.1. *If b and e are integers greater than 1, then there exists a primitive prime divisor of $b^e - 1$ unless $(b, e) = (2, 6)$, or $e = 2$ and b is of the form $2^s - 1$ for some integer $s \in \mathbb{N}$.*

From our remarks above it follows that if r is a primitive prime divisor of $b^e - 1$

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

then $r = ce + 1$ for some positive integer c and in particular $r \geq e + 1$. In many cases we either have $r > e + 1$, or $r = e + 1$ and r^2 divides $b^e - 1$. In these cases we shall say that r is a *large* primitive prime divisor of $b^e - 1$. Zsigmondy's result can be sharpened, see Feit [3] or Hering [5], to classify all pairs (b, e) with $e \geq 2$ for which $b^e - 1$ has no large primitive prime divisor.

THEOREM 2.2. *If b and e are integers greater than 1, then there exists a large primitive prime divisor of $b^e - 1$ except in the following cases*:

(i) $e = 2$ *and* $b = 2^s - 1$, *for some positive integer* s;
(ii) $e = 2$ *and* $b = 2^s 3 - 1$, *for some positive integer* s;
(iii) $b = 2$ *and* $e \in \{4, 6, 10, 12, 18\}$;
(iv) $b = 3$ *and* $e \in \{4, 6\}$;
(v) $b = 5$ *and* $e = 6$.

In this paper we shall be concerned with primitive prime divisors of $q^e - 1$ where $q = p^a$ for some prime p and positive integer a. It follows from the definition that each primitive prime divisor of $p^{ae} - 1$ is also a primitive prime divisor of $q^e - 1$, but the converse is not necessarily true, for example 7 is a primitive prime divisor of $4^3 - 1 = 63$, but not of $2^6 - 1$ since $2^3 - 1 = 7$. However, it follows from Theorem 2.1 that the only values of (q, e) for which there is a primitive prime divisor of $q^e - 1$ and for which there does not exist a primitive prime divisor of $p^{ae} - 1$ are $(q, e) = (4, 3)$ and $(q, e) = (8, 2)$.

The recognition algorithm in [10], and also the non-generic version presented in this paper, are based on searching in a matrix group for elements of certain orders as defined below.

DEFINITION 2.3. Let d, e be positive integers such that $d/2 < e \leq d$, and let $q = p^a$ with p a prime and $a \geq 1$.

(a) An element of $\mathrm{GL}(d, q)$ whose order is divisible by a primitive prime divisor of $q^e - 1$ is called a *primitive prime divisor element*, a ppd-*element*, or a ppd$(d, q; e)$-*element*.

(b) An element of $\mathrm{GL}(d, q)$ whose order is divisible by a primitive prime divisor of $p^{ae} - 1$ is called a *basic primitive prime divisor element*, a *basic* ppd-*element*, or a bppd$(d, q; e)$-*element*.

(c) An element of $\mathrm{GL}(d, q)$ whose order is divisible either by a large primitive prime divisor r of $q^e - 1$ such that $r > e + 1$, or by r^2 if $r = e + 1$ is a large ppd of $q^e - 1$, is called a *large primitive prime divisor element*, an lppd-*element*, or an lppd$(d, q; e)$-*element*.

It happens frequently that a ppd-element is both large and basic. Note that if r is a large primitive prime divisor of $q^e - 1$, where $d/2 < e \leq d$, then a Sylow r-subgroup

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

of GL (d, q) is cyclic. Consequently, for $G \leq \mathrm{GL}(d, q)$, the order$|G|$ is divisible by r^2 if and only if G contains an element of order r^2.

If a subgroup G of GL (d, q) has the ppd $(d, q; e_i)$-property for two distinct integers e_1, e_2 in the interval $(d/2, d] = \{e \in \mathbb{Z} \mid d/2 < e \leq d\}$, we shall say that G *contains two different* ppd *-elements.*

The notions of large and basic ppd $(d, q; e)$-elements were introduced in [10]. In that paper we showed that for most parameter sets such elements occur in sufficiently large proportions in the classical groups to be useful for our algorithm. However, for the small values of d we consider here the classical groups which do not contain all the types of elements required by the algorithm in [10] and we need to consider other elements in some of the classical groups. We therefore introduce another type of element, called a splitting ppd-element.

If r is a prime and an element g of a group has order $o(g) = r^a s$ where $a \geq 1$ and s is coprime to r, then the *r-part* of $o(g)$ is r^a, and the *r-part* of g is defined to be $h := g^s$. A *splitting* ppd $(d, q; d/2)$*-element* is an element $g \in \mathrm{GL}(d, q)$ with order divisible by a primitive prime divisor r of $q^{d/2} - 1$ such that, under the action of the r-part h of g, the underlying vector space V decomposes as a direct sum of two non-isomorphic $\mathbb{F}_q\langle h\rangle$-modules each of dimension $d/2$. If we wish to specify the primitive prime divisor r of $q^{d/2} - 1$, we say that g is a splitting ppd$(d, q; d/2)$-element *with respect to the prime r.*

For our algorithm we are given an irreducible subgroup $G \leq \mathrm{GL}(d, q)$, where $d \geq 3$, and we have complete information about the non-degenerate bilinear, quadratic or sesquilinear forms preserved by G modulo scalars. Thus exactly one of the following four cases holds.

DEFINITION 2.4. (i) *Linear case* (**L**): $G \leq \Delta = \mathrm{GL}(d, q)$, and G preserves no non-degenerate bilinear, quadratic or sesquilinear form on V. Here we set $\Omega = \mathrm{SL}(d, q)$ and $I = \mathrm{GL}(d, q)$.

(ii) *Symplectic case* (**Sp**): $G \leq \Delta = \mathrm{GSp}(d, q)$, with d even, and if q is also even then G preserves no non-degenerate quadratic form on V. Here we set $\Omega = I = \mathrm{Sp}(d, q)$.

(iii) *Orthogonal case* ($\mathbf{O}^\epsilon$): $G \leq \Delta = \mathrm{GO}^\epsilon(d, q)$, where $\epsilon = \pm$, if d is even, and $\epsilon = \circ$ if d is odd. Also, if d is odd then q is odd (since G is assumed to be irreducible). Here we set $\Omega = \Omega^\epsilon(d, q)$ and $I = \mathrm{O}^\epsilon(d, q)$.

(iv) *Unitary case* (**U**): $G \leq \Delta = \mathrm{GU}(d, q)$, where q is a square, and G preserves no non-degenerate bilinear or quadratic form on V. Here we set $\Omega = \mathrm{SU}(d, q)$ and $I = \mathrm{U}(d, q)$.

We shall say that G is in *case* **X**, where **X** is **L**, **Sp**, $\mathbf{O}^\epsilon$, or **U**, according to whether G is in case (i), (ii), (iii), or (iv), respectively. We call the triple $(\mathbf{X}, d, q)$ the *parameters of G.*

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

Clearly, the groups Ω, I and Δ are uniquely determined by G, and hence the case $\mathbf{X}$ of G is uniquely determined and is part of the information available as input to our algorithm. Our aim is to recognise whether G contains the group Ω. The recognition algorithm in [10] is based on the observation that, if G contains Ω and if d is sufficiently large, then with high probability we can find two different ppd-elements in G such that at least one of them is a large ppd-element and at least one of them is a basic ppd-element, (often a ppd-element is both large and basic). In this case we say that G has *generic parameters* and the algorithm described in [10] is particularly straightforward. In [10] we determined for each case $\mathbf{X}$, the precise values of d and q (where $d \geq 3$), for which the parameters $(\mathbf{X}, d, q)$ are generic. Our task in this paper is to deal with these remaining values of $(\mathbf{X}, d, q)$, which we call *non-generic parameters*: by [10, Theorem 3.3] they are precisely the following. (Note that in [9, Lemma 2.4] the result about non-generic parameters was inaccurate and was corrected in [10, Theorem 3.3].)

THEOREM 2.5. *The parameters* $(\mathbf{X}, d, q)$, *where* $d \geq 3$, *are non-generic if and only if*

(1) *case* $\mathbf{L}$: $(d, q) = (3, 2^s - 1)$ *for some integer* $s \in \mathbb{N}$;
(2) *case* $\mathbf{Sp}$: $d = 4$ *or* (d, q) *is one of* $(6, 2)$, $(6, 3)$ *or* $(8, 2)$;
(3) *case* $\mathbf{U}$: $d = 3, 4, 6$ *or* $(d, q) = (5, 4)$;
(4) *case* $\mathbf{O}^\epsilon$:
  (i) $\epsilon = +$: $d = 4, 6, 8$ *or* $(d, q) = (10, 2)$;
  (ii) $\epsilon = -$: $d = 4$ *or* (d, q) *is one of* $(6, 2)$, $(6, 3)$ *or* $(8, 2)$;
  (iii) $\epsilon = \circ$: $d = 3$ *or* $d = 5$ *with* q *odd, or* $(d, q) = (7, 3)$.

We refer to a group G as a *non-generic classical group* with parameters $(\mathbf{X}, d, q)$ if $\Omega \leq G \leq \Delta$ and $(\mathbf{X}, d, q)$ are as in Theorem 2.5.

3. Basic ppd-elements in linear groups

First we derive from [4] and [10] a classification of irreducible linear groups which contain a basic ppd-element. Note that Z denotes the subgroup of scalar matrices in $\mathrm{GL}(d, q)$.

THEOREM 3.1. *Let* $d \geq 3$ *and let* G *be an irreducible subgroup of* $\mathrm{GL}(d, q)$ *with parameters* $(\mathbf{X}, d, q)$ *so that* $G \leq \Delta$ *as in case* $\mathbf{X}$ *of Definition* 2.4. *Assume that* G *contains a basic* ppd$(d, q; e)$*-element* g *for some value of* e *with* $d/2 < e \leq d$. *Then one of the following holds*:

(a) **classical examples:** G *contains* Ω;

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

(b) **imprimitive examples:** *G preserves a direct sum decomposition $V = U_1 \oplus \cdots \oplus U_d$ of the underlying vector space V with $\dim U_i = 1$ for $i = 1, \ldots, d$, and G acts $(d-e)$-transitively on the set $\{U_1, \ldots, U_d\}$; also $e < d$ and g is not a large ppd$(d, q; e)$-element*;

(c) **extension field examples:** *either*

(i) *$r = d = e + 1$, G is a subgroup of $\mathrm{GL}(1, q^d).d$, and g is not a large* ppd $(d, q; e)$*-element; or*

(ii) *there is a prime b such that b divides d and e, and G is conjugate to a subgroup of $\mathrm{GL}(d/b, q^b).b$*;

(d) **extraspecial examples:** *$d = 2^m$, p is an odd prime, G is a subgroup of $Z \circ 2^{1+2m} \cdot \mathrm{Sp}(2m, 2)$, g is not a large* ppd $(d, q; e)$*-element, and either $e = d$ or $e = d - 2$*;

(e) **nearly simple examples:** *G is nearly simple and is one of the groups in* [4, Examples 2.6–2.9]. *In particular, if the parameters $(\mathbf{X}, d, q)$ are non-generic and if g is also a large* ppd $(d, q; e)$*-element with respect to the primitive prime divisor r of $q^e - 1$, then $G_0 \leq G \leq (\mathrm{Aut}\, G_0) \circ Z$, and G_0 is one of the groups in Table 1 below.*

PROOF. As in [4] and [10] we deal with the eight Aschbacher classes $\mathscr{C}_1, \ldots \mathscr{C}_8$, and then the nearly simple subgroups of $\mathrm{GL}(d, q)$. Suppose that G does not contain Ω. Now G is not of type $\mathscr{C}_1$ as G is irreducible. If G is an imprimitive example (in $\mathscr{C}_2$), then (b) holds by [10, Lemma 4.1]. If G is an extension field example (in $\mathscr{C}_3$), then (c) holds by [4]. Also G is not of type $\mathscr{C}_4$ or $\mathscr{C}_7$ by the main theorem of [4] and G is not a subfield example (in $\mathscr{C}_5$) by [10, Lemma 4.3]. If G is an extraspecial example (in $\mathscr{C}_6$) then by [10, Lemma 4.4] case (d) holds. Finally G is not in $\mathscr{C}_8$ by the definition of the type $\mathbf{X}$. This leaves the nearly simple examples which are listed in [4, Examples 2.6–2.9]. Finally in Case (e) if $(\mathbf{X}, d, q)$ are non-generic, as specified by Theorem 2.5, and if g is a large ppd-element, then the possibilities can be read off from [4, Examples 2.6–2.9] and are precisely those listed in Table 1. Note that in lines 10, 11 and 13, the field order q is not 2, 3, or 5 since in these cases, by Theorem 2.2, Δ does not contain a large ppd$(8, q; 6)$-element. Also, in line 14, since $d \leq 8$ or $d = 10$, we must have $r \leq 19$. □

We record a corollary of this result where in addition to a large and basic ppd-element g we also require a ppd$(d, q; d/2)$-element in G.

COROLLARY 3.2. *Let $d \geq 4$ with d even, and let G be an irreducible subgroup of $\mathrm{GL}(d, q)$ with parameters $(\mathbf{X}, d, q)$ so that $G \leq \Delta$ as in case $\mathbf{X}$ of Definition* 2.4. *Assume that G contains a large and basic* ppd $(d, q; e)$*-element g for some value of e with $d/2 < e \leq d$. Suppose further that G contains also a* ppd $(d, q; d/2)$*-element. Then either*

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

(a) **classical examples:** *G contains Ω; or*

(b) **extension field examples:** *there is a prime b such that b divides $d/2$ and e, and G is conjugate to a subgroup of* $\mathrm{GL}(d/b, q^b).b$; *or*

(c) **nearly simple examples:** *G is one of the nearly simple groups described in* [4, Examples 2.6–2.9] *and if the parameters $(\mathbf{X}, d, q)$ are non-generic then $G_0 \leq G \leq (\mathrm{Aut}\, G_0) \circ Z$ and G_0 is one of the groups described in Table* 1 *in lines* 5, 6, 8, 9, 11, 12, *or* 14 (*where r is the ppd of $q^e - 1$ dividing $o(g)$*).

TABLE 1. Nearly simple examples in non-generic classical groups

line	G_0	d	p	q	e	r
1	$3 \cdot A_7$	3	5	25	3	7
2	$3 \cdot A_6$	3		p or p^2	2	5
3	A_6	3	3	9	2	5
4	A_5	3		p or p^2	2	5
5	$2 \cdot A_7$	4	3, 5 (mod 7)	p^2	3	7
6	$4 \cdot \mathrm{PSL}(3, 4)$	4	3	9	3	7
7	$\mathrm{Sz}(q)$	4	2		4	
8	$3 \cdot M_{22}$	6	2	4	5	11
9	$G_2(q)$	6	2		6	
10	$\mathrm{SL}(2, q^3)$	8		$q \neq 2, 3, 5$	6	
11	$2 \cdot \Omega(7, q)$	8	odd	$q \neq 3, 5$	6	
12	$\mathrm{Sp}(6, q)$	8	2		6	
13	$\mathrm{PSU}(3, q)$	8	$p \neq 3$	$q \neq 2, 3, 5$	6	
14	$\mathrm{PSL}(2, r)$	$\frac{1}{2}(r-1), \frac{1}{2}(r+1)$			$\frac{1}{2}(r-1)$	$r \leq 19$

PROOF. Since g is a large ppd-element it follows from Theorem 3.1 that we have only the three cases listed. In case (c) for non-generic parameters with d even the examples must appear in Table 1 by Theorem 3.1. Line 7 does not arise since $|\mathrm{Sz}(q)|$ is not divisible by a primitive prime divisor of $q^2 - 1$. For a similar reason lines 10 and 13 do not arise. □

4. Probability computations

In this section we prove several results about the proportions of certain types of elements in classical groups. The methods used are refinements of those in [10]. First we determine the proportion of ppd $(d, q; d/2)$-elements in $\mathrm{GL}(d, q)$ which are fixed point free on V. Let r be a primitive prime divisor of $q^{d/2} - 1$ and let G

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

satisfy $\mathrm{SL}(d,q) \leq G \leq \mathrm{GL}(d,q)$. Then the elements $g \in G$ with order divisible by r for which the r-part h is fixed point free on V can be divided into two sets, namely those for which V is a homogeneous $\langle h\rangle$-module and those for which $V = W_1 \oplus W_2$ where W_1, W_2 are non-isomorphic irreducible $\langle h\rangle$-modules. The latter are the splitting $\mathrm{ppd}(d,q;d/2)$-elements of G with respect to the prime r and we denote their proportion by $\mathrm{sppd}(G,d/2;r)$. The former elements are called *homogeneous* $\mathrm{ppd}(d,q;d/2)$-elements with respect to r and their proportion in G is denoted $\text{hom-pdd}(G,d/2;r)$. Thus the proportion $\text{fpf-ppd}(G,d/2;r)$ of elements of G for which their r-part is fixed point free on the underlying vector space V, satisfies

$$\text{fpf-ppd}(G,d/2;r) = \mathrm{sppd}(G,d/2;r) + \text{hom-ppd}(G,d/2;r).$$

THEOREM 4.1. *Let d be an even integer, and let $\mathrm{SL}(d,q) \leq G \leq \mathrm{GL}(d,q)$. Suppose that $q^{d/2}-1$ has a primitive prime divisor r and let r^a be the r-part of $q^{d/2}-1$. Then*

$$\frac{1}{d} - \frac{2}{d(d+2)} \leq \frac{1}{d}\left(1-\frac{1}{r^a}\right) < \text{hom-ppd}\left(G,\frac{d}{2};r\right) \leq \frac{4}{3d}(1-r^a) < \frac{4}{3d}$$

and

$$0 \leq \mathrm{sppd}\left(G,\frac{d}{2};r\right) = \frac{2}{d^2}\left(1-\frac{1}{r^a}\right)\left(1-\frac{1+d/2}{r^a}\right) \leq \frac{2}{d^2}.$$

If r is not a large primitive prime divisor then $\mathrm{sppd}(G,d/2;r) = 0$, whereas if r is a large primitive prime divisor then

$$\text{hom-ppd}(G,d/2;r) > \frac{1}{d} - \frac{1}{d(d+1)}$$

and

$$\mathrm{sppd}(G,d/2;r) \geq \frac{1}{(d+1)^2}$$

and hence

$$\text{fpf-ppd}(G,d/2;r) \geq \frac{1}{d} - \frac{1}{d(d+1)^2}.$$

PROOF. First we discuss the structure of a Sylow r-subgroup R of G. Such a subgroup is contained in $\mathrm{SL}(d,q)$, and is of the form $R = \langle g_1\rangle \times \langle g_2\rangle \cong \mathbb{Z}_{r^a} \times \mathbb{Z}_{r^a}$. In its action on V, the group R preserves a direct sum decomposition $V = U_1 \oplus U_2$ where the U_i are subspaces of dimension $d/2$, and g_i is irreducible on U_i and acts trivially on U_{3-i}, for $i = 1, 2$. Moreover, the restrictions $g_1|_{U_1}$ and $g_2|_{U_2}$ can be represented by the

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

same element of $\mathrm{GL}(d/2, q)$ with respect to appropriate bases of the U_i. In addition $N_{\mathrm{GL}(d,q)}(R) \cong \Gamma\mathrm{L}(1, q^{d/2})$ wr S_2 and $N_G(R)/C_G(R) \cong \mathbb{Z}_{d/2}$ wr S_2. In particular the number n_1 of Sylow r-subgroups of G is the same as the number in $\mathrm{GL}(d, q)$ as they all lie in $\mathrm{SL}(d, q)$, and we have

$$n_1 = |G : N_G(R)| = \frac{|G|}{|C_G(R)|2(d/2)^2} = \frac{2|G|}{d^2|C_G(R)|}.$$

Let $g \in G$ have order divisible by r, let h be its r-part, and suppose that h has no fixed points in V. Then $V = W_1 \oplus W_2$ where the W_i are irreducible $\langle h \rangle$-invariant subspaces of dimension $d/2$. The number of elements g corresponding to a given element h depends on whether or not W_1, W_2 are isomorphic as $\langle h \rangle$-modules.

Suppose first that W_1, W_2 are isomorphic as $\langle h \rangle$-modules. Then $C := C_{\mathrm{GL}(d,q)}(h) \cong \mathrm{GL}(2, q^{d/2})$ and $g \in C \cap G$. By [7, Proposition 4.3.6(I), see also page 62] there is a single G-conjugacy class of such subgroups $C \cap G$ consisting of

$$|\mathrm{GL}(d, q) : N_{\mathrm{GL}(d,q)}(\mathrm{GL}(2, q^{d/2}))| = \frac{|\mathrm{GL}(d, q)|}{|\mathrm{GL}(2, q^{d/2})|(d/2)} = \frac{2|G|}{d|C \cap G|}$$

subgroups. For each element $g \in G$ of this type there is exactly one such subgroup $C \cap G$ which contains g and for which the r-part of g is in the centre of C. Thus we need to count the number of such elements g lying in a given subgroup $C \cap G$. Such a subgroup $C \cap G$ splits as $X \times Y$ with $Y \cong \mathbb{Z}_{r^a}$ and $X \geq \mathrm{SL}(2, q^{d/2})$. The element h can be any of the $r^a - 1$ non-trivial elements of Y, and given h there are x elements g in $X \times Y$ with r-part h, where x is the number of r'-elements in X. By [10, Lemma 5.6], $x = |X|(1 - y)$ where y, the proportion of elements of X of order a multiple of r, satisfies $1/3 \leq y < 1/2$, so $|X|/2 < x \leq 2|X|/3$. Thus we have $x(r^a - 1)$ elements of $C \cap G = X \times Y$ of the correct type, and so the proportion of these elements in G is

$$\text{hom-ppd}(G, d/2; r) = \frac{1}{|G|} \frac{2|G|}{d|C \cap G|} x(r^a - 1)$$

and therefore

$$\frac{1}{d}\left(1 - \frac{1}{r^a}\right) \leq \text{hom-ppd}(G, d/2; r) \leq \frac{4}{3d}(1 - r^a) < \frac{4}{3d}.$$

Note that this lower bound is at least $1/d - 2/(d(d+2))$ since $r^a \geq d/2 + 1$ with equality if r is not large. If r is a large primitive prime divisor then $r^a \geq d + 1$ so the expression is at least $1/d - 1/(d(d+1))$.

Now suppose that W_1 and W_2 are not isomorphic as $\langle h \rangle$-modules. Then h lies in a unique Sylow r-subgroup, R say, and g normalises R. Thus the number of elements g in this case is n_1 times the number contained in $N_G(R)$. So we assume

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

that $h \in R$ and $g \in N_G(R)$. Now $R = \langle g_1 \rangle \times \langle g_2 \rangle$ and $N_G(R) = \langle C_G(R), \sigma_1, \sigma_2, \tau \rangle$ where $g_i^\tau = g_{3-i}$, $\sigma_i^\tau = \sigma_{3-i}$, $g_i^{\sigma_i} = g_i^q$, $g_i^{\sigma_{3-i}} = g_i$ and σ_i and τ have orders $d/2$ and 2 respectively. We have $h = g_1^{u_1} g_2^{u_2}$ for some integers u_1, u_2 satisfying $0 < u_i < r^a$. The condition that W_1, W_2 are not isomorphic as $\langle h \rangle$-modules is equivalent to the condition that $u_2 \not\equiv u_1 q^i (\mathrm{mod}\ r^a)$ for any $i = 0, 1, \ldots, d/2 - 1$, and since $u_1, u_1 q, \ldots, u_1 q^{d/2-1}$ are pairwise distinct modulo r^a there are $r^a - 1 - d/2$ choices for u_2 for a given value of u_1 for which W_1, W_2 are non-isomorphic $\langle h \rangle$-modules. Thus there are $(r^a - 1)(r^a - 1 - d/2)$ possibilities for h in R. Now $g \in C_G(R)$ and $C_G(R)$ splits as $X \times R$. Given h, there are $|X|$ choices for g in $C_G(R)$ with r-part h. Hence the proportion sppd $(G, d/2; r)$ of elements g in this case is

$$\frac{n_1}{|G|}|X|(r^a - 1)\left(r^a - 1 - \frac{d}{2}\right) = \frac{2}{d^2}\left(1 - \frac{1}{r^a}\right)\left(1 - \frac{1 + d/2}{r^a}\right).$$

This expression is equal to 0 if $r^a = r = d/2 + 1$, that is if r is not large, while if r is a large primitive prime divisor then $r^a \geq d + 1$ and the expression is at least $1/(d + 1)^2$. □

Next we extend the argument in Theorem 4.1 to determine a lower bound for the proportion of large and splitting ppd $(d, q; d/2)$-elements in certain families of classical groups.

THEOREM 4.2. *Let $d \geq 4$ and let $G \leq \mathrm{GL}(d, q)$ be a subgroup with parameters $(\mathbf{X}, d, q)$ such that $\Omega \leq G \leq \Delta$, and either*

(a) $\mathbf{X} = \mathbf{Sp}$ *or* $\mathbf{O}^+$ *with* $d \equiv 0 (\mathrm{mod}\ 4)$, *or*

(b) $\mathbf{X} = \mathbf{U}$ *with* $d \equiv 2 (\mathrm{mod}\ 4)$.

Suppose that $q^{d/2} - 1$ has a large primitive prime divisor. Then the proportion in G of ppd $(d, q; d/2)$*-elements which are large and splitting is at least $2/(\delta(d + 1)^2)$ where $\delta = 2$ if $\mathbf{X} = \mathbf{Sp}$ and δ is 1 or 2 in the other cases. If $q^{d/2} - 1$ has a primitive prime divisor but not a large one then G contains no splitting* ppd $(d, q; d/2)$*-elements but the proportion of* ppd $(d, q; d/2)$*-elements of G which are fixed point free is at least $1/(d + 2)$.*

PROOF. Let r be a large primitive prime divisor of $q^{d/2} - 1$. In all cases a Sylow r-subgroup R of G is contained in Ω and is a Sylow r-subgroup of $\mathrm{GL}(d, q)$. Let r^a be the r-part of $q^{d/2} - 1$ so that $|R| = r^{2a}$.

Suppose that $g \in G$ is a splitting ppd $(d, q; d/2)$-element with respect to the prime r, so the r-part h of g has two irreducible constituents in V of dimension $d/2$ which are non-isomorphic as $\mathbb{F}_q\langle h \rangle$-modules. Then h lies in a unique Sylow r-subgroup R, and therefore g lies in $N_G(R)$. Thus the number of such elements g in G is $|G : N_G(R)|$ times the number in $N_G(R)$ for a given Sylow r-subgroup R. So we need

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

to determine the number of these elements g in $N_G(R)$. Now R preserves a unique decomposition $V = U_1 \oplus U_2$ where the U_i are mutually orthogonal non-singular R-invariant subspaces of dimension $d/2$ of the same type: for $\mathbf{X} = \mathbf{Sp}$, $\mathbf{O}^+$ or $\mathbf{U}$, both of the U_i have type $\mathbf{Sp}$, $\mathbf{O}^-$ or $\mathbf{U}$ respectively, see [7, Tables 3.5. B, C and E]. Moreover, as in Theorem 4.1, in each case, $C_G(R) = X \times R$ and $g \in C_G(R)$. Thus, for each possibility h for the r-part, there are $|X| = |C_G(R)|/|R|$ choices for a suitable element g with r-part h.

We need to determine the number of possibilities for h. As in the proof of Theorem 4.1, we have $R = \langle g_1 \rangle \times \langle g_2 \rangle$ where $o(g_i) = r^a$, and the restrictions $g_1|_{U_1}$ and $g_2|_{U_2}$ can be represented by the same irreducible matrix in $\mathrm{GL}(d/2, q)$ with respect to appropriate bases of the U_i. Moreover (see [7, Lemma 4.1.1 and Corollary 4.2.2] and the proof of [10, Theorem 5.7]) $|N_G(R)/C_G(R)|$ has order $(d/2)^2\delta$ where $\delta = 2$ if $\mathbf{X} = \mathbf{Sp}$ and δ is 1 or 2 in the other cases. Further, we obtain elements g which are splitting if $h = g_1^{u_1} g_2^{u_2}$ where $0 < u_i < r^a$ and, for a given value of u_1, the value of u_2 is any non-zero integer in the interval $(0, r^a)$ such that $u_2 \not\equiv u_1 q^i \pmod{r^a}$ for $i = 0, 1, \ldots, d/2 - 1$. Thus there are $(r^a - 1)(r^a - 1 - d/2)$ possibilities for h, and the proportion of splitting $\mathrm{ppd}(d, q; d/2)$-elements g in G is

$$\frac{1}{|G|}|G : N_G(R)||X|(r^a - 1)(r^a - 1 - d/2) = \frac{1}{(d/2)^2\delta}\left(1 - \frac{1}{r^a}\right)\left(1 - \frac{1 + d/2}{r^a}\right)$$

which is at least $2/(\delta(d+1)^2)$ since $r^a \geq d + 1$.

If r is not a large primitive prime divisor, that is, if $r^a = r = d/2 + 1$, then there are no splitting ppd $(d, q; d/2)$-elements. The ppd $(d, q; d/2)$-element g being fixed point free on V implies that $g \in C_G(h)$ and $C_G(h) = X \times Y$ where $Y \cong \mathbb{Z}_r$ and $X \geqslant \mathrm{SL}(2, q^{d/2})$. As in the proof of Theorem 4.1, the proportion of fixed point free r-elements g in G is equal to $2x(r-1)/(d|C_G(h)|)$ where x is the number of r'-elements in X, and $x \geq |X|/2$. Thus the proportion is at least

$$\frac{r-1}{dr} = \frac{1}{d+2}.$$

□

In the next two families of groups the relevant Sylow subgroups are cyclic and the proportions of ppd $(d, q; d/2)$-elements are obtained by a slightly different method.

PROPOSITION 4.3. *Let* $(\mathbf{X}, d, q)$ *be* $(\mathbf{U}, d, q)$ *with* $d \equiv 0 \pmod 4$ *or* $(\mathbf{O}^+, d, q)$ *with* $d \equiv 2 \pmod 4$ *and* $d \geq 6$ *and* $\Omega \leq G \leq \Delta$. *Suppose that* $q^{d/2} - 1$ *has a primitive prime divisor* r. *Then the proportion of elements of* G *of order divisible by* r *is at least* $1/(d+1)$.

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

PROOF. If R is a Sylow r-subgroup of G then R is also a Sylow r-subgroup of Ω and R is cyclic. Now R acts fixed point freely on V and preserves a unique decomposition $V = U_1 \oplus U_2$ with $\dim U_i = d/2$ for $i = 1, 2$, and both U_1 and U_2 are totally singular. The stabiliser of such a decomposition is of type $\mathrm{GL}(d/2, q).2$, see [7, Table 3.5. B, page 71 and Table 3.5. E, page 73]. Since Ω contains $\mathrm{SL}(d/2, q).2$, it follows that the proportion of elements of G of order a multiple of r is one half of the proportion of such elements in $G \cap \mathrm{GL}(d/2, q) \geqslant \mathrm{SL}(d/2, q)$. Also $N_G(R) = N_{\mathrm{GL}(d/2,q).2}(R) = C_G(R).[d]$. By [10, Lemma 5.6] it follows that the proportion of elements of G of order a multiple of r is at least $1/(d+1)$. □

Next we consider elements whose orders are certain divisors of $q^e - 1$ for various values of e. The idea of using such elements in the non-generic algorithm, and the techniques for computing their proportions in classical groups, were suggested by similar ideas and computations in [10] for large primitive prime divisor elements. The computations are presented here to deal with certain small dimensional infinite families of classical groups.

PROPOSITION 4.4. *Let* $(\mathbf{X}, d, q) = (\mathbf{Sp}, 4, q)$.

(a) *If* $g \in \Omega \cap (\mathrm{GL}(2, q^2).2)' = \mathrm{SL}(2, q^2)$ *has order dividing* $q + 1$, *and is fixed point free on* V, *then* V *is the direct sum of two isomorphic irreducible* 2*-dimensional* $\langle g \rangle$*-modules.*

(b) *If* $q = 2^s - 1 \geq 7$, *then the proportion of elements* $g \in \Omega$ *with order a multiple of* 4 *such that* V *is a direct sum of two non-isomorphic irreducible* 2*-dimensional* $\langle g \rangle$*-modules is at least*

$$\frac{1}{8}\left(1 - \frac{4}{q+1}\right)\left(1 - \frac{6}{q+1}\right) \geq \frac{1}{64}.$$

(c) *If* $q = 3 \cdot 2^s - 1 \geq 11$ *then the proportion of elements* $g \in \Omega$ *with order a multiple of* 3 *or* 4, *such that* V *is the direct sum of two non-isomorphic irreducible* 2*-dimensional* $\langle g \rangle$*-modules is at least*

$$\frac{1}{8}\left(1 - \frac{6}{q+1}\right)\left(1 - \frac{8}{q+1}\right) \geq \frac{1}{48}.$$

PROOF. (a) When represented as a 2×2 matrix in $\mathrm{SL}(2, q^2)$, g is conjugate to a matrix of the form

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

over $\mathbb{F}_{q^2}$. Hence, as a 4×4 matrix over $\mathbb{F}_q$, g is conjugate in $\mathrm{GL}(4, q)$ to a matrix of the form

$$\begin{pmatrix} A & 0 \\ 0 & A^{-1} \end{pmatrix}.$$

In particular this shows that V decomposes as the direct sum $V = U \oplus U^*$ of two isomorphic $\langle g \rangle$-modules.

(b) and (c): Now Ω contains a subgroup $H = \mathrm{Sp}(2, q) \times \mathrm{Sp}(2, q)$ stabilising a decomposition $V = U_1 \oplus U_2$ with U_1, U_2 non-singular 2-dimensional subspaces, and H contains a subgroup $L = \langle g_1 \rangle \times \langle g_2 \rangle \cong \mathbb{Z}_{q+1} \times \mathbb{Z}_{q+1}$. As in the proof of Theorem 4.1 and Theorem 4.2, for elements $h = g_1^{u_1} g_2^{u_2}$ in L, with $u_i \neq 0$ the U_i are non-isomorphic $\langle h \rangle$-modules provided $u_2 \not\equiv u_1$ or $u_1 q \pmod{q+1}$. If $g_i^{u_i}$ has order divisible by 4 or, in the case $q = 3 \cdot 2^s - 1$, divisible by 3 or by 4, then $g_i^{u_i}$ will act irreducibly on U_i; there are $q-3$ or $q-5$ such elements in $\langle g_i \rangle$ according as $q = 2^s - 1$ or $3 \cdot 2^s - 1$, respectively. A similar argument to that in the proof of Theorem 4.2 shows that the proportion of elements g of Ω which lie in a subgroup $L = \langle g_1 \rangle \times \langle g_2 \rangle$ stabilising such a decomposition $V = U_1 \oplus U_2$, and are such that both $g|_{U_1}$ and $g|_{U_2}$ have order divisible by 4 (if $q = 2^s - 1$) or by 3 or 4 (if $q = 3 \cdot 2^s - 1$), and for which the U_i are non-isomorphic $\langle g \rangle$-modules is at least

$$\frac{1}{|\Omega|} |\Omega : N_\Omega(L)|(q-3)(q-5) = \frac{1}{8}\left(1 - \frac{4}{q+1}\right)\left(1 - \frac{6}{q+1}\right) \geq \frac{1}{64}$$

if $q = 2^s - 1 \geq 7$, or

$$\frac{1}{|\Omega|} |\Omega : N_\Omega(L)|(q-5)(q-7) = \frac{1}{8}\left(1 - \frac{6}{q+1}\right)\left(1 - \frac{8}{q+1}\right) \geq \frac{1}{48}$$

if $q = 3 \cdot 2^s - 1 \geq 11$. □

PROPOSITION 4.5. *The proportion of elements of order a multiple of* 4 *in* $\mathrm{SL}(3, q)$, *where* $q \equiv 3 \pmod 4$, *is at least* $1/3$.

PROOF. Now $\mathrm{SL}(3, q)$ contains matrices of the form

$$g = \begin{pmatrix} -1 & 0 \\ 0 & A \end{pmatrix},$$

where $A \in \mathrm{GL}(2, q)$ and $o(A) = 4t$ for some t. Such an element g preserves a unique decomposition $V = \langle v \rangle \oplus U$ and g is irreducible on U.

Each $g \in \mathrm{SL}(3, q)$ of order a multiple of 4 has a unique invariant 2-dimensional subspace U in its action on V such that g is irreducible on U. Since $\mathrm{SL}(3, q)$ is

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

transitive on the 2-dimensional subspaces of V an analogous argument to that of [10, Lemma 5.4] shows that the proportion of elements of $G = \mathrm{SL}(3, q)$ of order a multiple of 4 is equal to the proportion of such elements in G^U, where U is a fixed 2-dimensional subspace of V and G^U is the subgroup of $\mathrm{GL}(U)$ induced on U by G. It then follows from [10, Lemma 5.6] that this proportion is at least 1/3. □

We now consider the groups of type $\mathrm{O}^+(4, q)$. The group $\mathrm{GO}^+(4, q)$ is isomorphic to $(\mathrm{GL}(2, q) \circ \mathrm{GL}(2, q)).2$ and $\Omega^+(4, q)$ is isomorphic to $\mathrm{SL}(2, q) \circ \mathrm{SL}(2, q)$. Further, $\Omega^+(4, q)$ preserves a tensor product decomposition of the underlying vector space $V = U \otimes W$, where $\dim U = \dim W = 2$.

Let $\delta, \delta' \in \{1, -1\}$. An element $g \circ g' \in \mathrm{SL}(2, q) \circ \mathrm{SL}(2, q)$ is called a (δ, δ')-*element* if

- $o(g)$ divides $q + \delta$
- $o(g')$ divides $q + \delta'$

and g and g' both have order greater than 2, or 4 according as q is even or odd, respectively.

THEOREM 4.6. *Let* $(\mathbf{X}, d, q) = (\mathbf{O}^+, 4, q)$. *Then for* $\delta, \delta' \in \{1, -1\}$, *the proportion of* (δ, δ')*-elements in* $\Omega^+(4, q)$ *is at least*

$$\frac{1}{4}\left(1 - \frac{2\nu}{q+\delta}\right)\left(1 - \frac{2\nu}{q+\delta'}\right) = \frac{1}{4} - \frac{\nu}{q} + O\left(\frac{1}{q^2}\right),$$

where $\nu = 1$ *if* q *is even and* $\nu = 3$ *if* q *is odd. Moreover, if* $q^2 - 1$ *has a primitive prime divisor (or a large or basic primitive prime divisor) then the proportions of* $(1, 1)$*-elements in* $\Omega^+(4, q)$ *which induce a* ppd$(2, q; 2)$*-element (or a large or basic* ppd$(2, q; 2)$*-element, respectively) in each component is at least* 1/9.

PROOF. Let $g \circ g'$ be a (δ, δ')-element in Ω. First we determine the normaliser of g (and g') in $\mathrm{SL}(2, q)$. Consider first the case $\delta = 1$. Then $g \in \mathrm{SL}(2, q)$ is irreducible on U and thus $C_{\mathrm{GL}(2,q)}(g) \cong \mathbb{Z}_{q^2-1}$, a Singer Cycle containing all non-zero scalars in $\mathrm{GL}(2, q)$. Hence $C_{\mathrm{SL}(2,q)}(g) \cong \mathbb{Z}_{q+1}$. (This is the case also when q is odd because $\mathrm{PSL}(2, q)$ does not contain a subgroup of order $q + 1$.)

If $\delta = -1$ then $g \in \mathrm{SL}(2, q)$ is completely reducible and by Maschke's Theorem $U = U_1 \oplus U_2$ where U is a 2-dimensional vector space on which $\mathrm{SL}(2, q)$ acts naturally, and both U_1 and U_2 are g-invariant. So g is conjugate to a matrix of the form

$$g = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

and

$$C_{\mathrm{SL}(2,q)}(g) = \left\{ \begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix} \middle| \, b \neq 0 \right\} \cong \mathbb{Z}_{q-1}.$$

Thus $N_{\mathrm{SL}(2,q)}(g) = \mathbb{Z}_{q+\delta}.2$ whether δ is $+1$ or -1.

Now $C_\Omega(g \circ g') = C \circ C'$, where $C \cong \mathbb{Z}_{q+\delta}$ and $C' \cong \mathbb{Z}_{q+\delta'}$, the central product $C \circ C'$ has a subgroup of order $\gcd(q-1, 2)$ amalgamated, and $|N_\Omega(g \circ g') : C \circ C'| = 4$. Each element of the form $g \circ g'$ lies in a unique subgroup of the form $C \circ C'$. All subgroups of $\mathrm{SL}(2, q)$ which are cyclic of the same order $q \pm 1$ are conjugate. Thus the number $n_{\delta,\delta'}$ of elements of the form $g \circ g'$ is

$$n_{\delta,\delta'} = n_{C \circ C'} \cdot n_{g \circ g'}(C \circ C'),$$

where $n_{C \circ C'}$ denotes the number of subgroups of the form $C \circ C'$ and $n_{g \circ g'}(C \circ C')$ denotes the number of elements of the form $g \circ g'$ in a given $C \circ C'$. If q is even, then $\Omega = \mathrm{SL}(2, q) \times \mathrm{SL}(2, q)$, $C \circ C' = C \times C'$, and g, g' are such that $g^2 \neq 1$ and $g'^2 \neq 1$. Hence $n_{C \circ C'} = |\Omega|/(4|C \times C'|)$, and $n_{g \circ g'}(C \circ C') = (q + \delta - 2)(q + \delta' - 2)$. Thus

$$n_{\delta,\delta'} = \frac{|\Omega|}{4}\left(1 - \frac{2}{q+\delta}\right)\left(1 - \frac{2}{q+\delta'}\right) \geq |\Omega|\left(\frac{1}{4} - \frac{1}{q} + O\left(\frac{1}{q^2}\right)\right).$$

If q is odd then $C \circ C' = \mathbb{Z}_{q+\delta} \circ \mathbb{Z}_{q+\delta'}$ has order $(q + \delta)(q + \delta')/2$, and the elements g, g' have order larger than 4. Thus $n_{C \circ C'} = |\Omega|/(4|C \circ C'|)$, and $n_{g \circ g'}(C \circ C') \geq (q + \delta - 6)(q + \delta' - 6)/2$. Hence

$$n_{\delta,\delta'} \geq \frac{|\Omega|}{4}\left(1 - \frac{6}{q+\delta}\right)\left(1 - \frac{6}{q+\delta'}\right) = |\Omega|\left(\frac{1}{4} - \frac{3}{q} + O\left(\frac{1}{q^2}\right)\right).$$

Finally if $\delta = \delta' = 1$, if $q^2 - 1$ has a primitive prime divisor r, and if each of g, g' is a ppd $(2, q; 2)$-element with order divisible by r, the above argument applies, but g, g' must be chosen in C, C' to lie outside certain subgroups of index at least $r \geq 3$. Thus in this case

$$n_{g \circ g'}(C \circ C') \geq \left(\frac{2(q+1)}{3}\right)^2 / \gcd(2, q-1)$$

and hence

$$n_{1,1} \geq \frac{|\Omega|}{4|C \circ C'|} n_{g \circ g'}(C \circ C') \geq \frac{|\Omega|}{9}.$$

□

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

5. The main theorems

Let $G \leq \mathrm{GL}(d, q)$ be a group with parameters $(\mathbf{X}, d, q)$ as listed in Definition 2.4 such that G acts irreducibly on the underlying vector space V. In this section we determine for each of the non-generic cases in Theorem 2.5 a subset S of elements of Δ such that if G contains S, then G contains Ω. We also list lower bounds for the proportions of these elements in Ω. We limit the recording of these probability bounds to those for Ω. Bounds for the proportions in other subgroups of Δ containing Ω could be derived similarly. For example, if $\Delta = \Omega.2$ and all elements of a certain type are contained in Ω, then the proportion of these elements in Δ is half of their proportion in Ω. Throughout this section, if $\Omega \leq G \leq \Delta$, then we let $p(G, r)$ denote the proportion of elements in G of order a multiple of r.

REMARK 5.1. Notes for interpreting Table 2–Table 4 and Table 6–Table 8. We represent the set of elements to be sought in G as a list according to the values of $\mathbf{X}$, d and q. In most cases we list certain integers $i_1, i_2, \ldots$, in the column headed 'elements in G' and by this we shall mean that several elements are required in G, the first of which should have order a multiple of i_1, the second of which should have order a multiple of i_2, and so on. In the column labelled 'proportions' we list lower bounds for $p(\Omega, i_1), p(\Omega, i_2)$, and so on. In other cases, instead of an integer, an entry in the column 'elements in G' may be 'ppd $(d, q; e)$' and in this case the corresponding element should be a ppd $(d, q; e)$-element; in such a case the corresponding entry in the column labelled 'proportions' is a lower bound for the proportion of such elements in Ω. In some exceptional cases, the sensible approach is to compute a permutation representation for G on some set Y, and in these cases the entry in the column 'elements in G' is 'compute perm. rep.' together with the cardinality of the set Y.

First we treat groups with non-generic parameters $(\mathbf{L}, d, q)$. By Theorem 2.5, $(d, q) = (3, 2^s - 1)$, and by Theorem 2.2, it follows that $q^3 - 1$ has a primitive prime divisor which is both large and basic.

THEOREM 5.1 (Linear Case). *Let $G \leq \mathrm{GL}(3, q)$ be an irreducible subgroup with parameters $(\mathbf{L}, 3, q)$, with $q = 2^s - 1$ for some s, and suppose that G contains two elements as in Table 2. Then G contains $\Omega = \mathrm{SL}(3, q)$. Moreover, lower bounds for the proportions of elements of these types in Ω are given in the last column of Table 2.*

PROOF. Let r be a large primitive prime divisor of $q^3 - 1$ which divides $|G|$. Note that $q^2 + q + 1 = 2^{2s} - 2^s + 1 \equiv 1, 0, -1 \pmod 7$ and $q - 1 = 2(2^{s-1} - 1) \equiv -1, 0, 2 \pmod 7$ according as $s \equiv 0, 1, 2 \pmod 3$, respectively. It follows that $r \neq 7$. Thus by Theorem 3.1, either G contains Ω, or $G \leq \mathrm{GL}(1, q^3).3$. However, since $q^3 - 1 \equiv 2 \pmod 4$, $\mathrm{GL}(1, q^3).3$ contains no elements of order 4, so $G \not\leq \mathrm{GL}(1, q^3).3$. Hence

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

TABLE 2. $\mathbf{X} = \mathbf{L}$

d	q	elements in G	proportions
3	$2^s - 1$	basic lppd $(3, q; 3), 4$	1/4, 1/3

TABLE 3. $\mathbf{X} = \mathbf{Sp}$

d	q	elements in G	proportions
8	2	5, 9, 17	1/4, 1/9, 2/17
6	2	5, 7, 9	1/5, 1/7, 1/9
6	3	5, 7	1/5, 1/7
4	2	perm. rep. of degree 15	
4	3	5, 9	1/5, 2/9
4	5	13, 15	1/5, 1/5
4	$q \neq 2^s - 1, 3 \cdot 2^s - 1, 2$	basic lppd $(4, q; 4)$,	1/5
		splitting lppd $(4, q; 2)$	1/25
4	$q = 2^s - 1 \geq 7$	basic lppd $(4, q; 4)$, 4	1/5, 1/64
4	$q = 3 \cdot 2^s - 1 \geq 11$	basic lppd $(4, q; 4)$, 3 or 4	1/5, 1/48

G contains Ω. By [10, Theorem 5.8] the proportion of lppd $(3, q; 3)$-elements in Ω is at least 1/4 and by Proposition 4.5 the proportion of elements of order a multiple of 4 in Ω is at least 1/3. □

Next we deal with the symplectic case for d, q as in Theorem 2.5 (2).

THEOREM 5.2 (Symplectic Case). *Let $G \leq \mathrm{GL}(d, q)$ be an irreducible subgroup with parameters* $(\mathbf{Sp}, d, q)$, *with (d, q) as in Theorem* 2.5 (2). *If $(d, q) = (4, 2)$ and $|G|$ is divisible by $360 = |A_6|$ then G contains $\mathrm{Sp}(4, 2)'$. If $(d, q) \neq (4, 2)$, and G contains elements as in the relevant line of Table* 3 *then G contains $\Omega = \mathrm{Sp}(d, q)$. Moreover, lower bounds for the proportions of elements of these types in Ω are given in the last column of Table* 3.

PROOF. We consider the various cases for (d, q) listed in Table 3. For individual groups we often compute the proportion in Ω of elements of various orders from the character tables in the Atlas [1], which list the orders of the centralisers in Ω for each conjugacy class of elements. In such cases we will not make a separate reference to [1]. Put $G_0 = G \cap \Omega$.

Case $(d, q) = (8, 2)$. The group $\Omega = \mathrm{Sp}(8, 2)$ has elements of order divisible by 17 (ppd $(8, 2; 8)$-elements), 9 and 5, and their proportions in Ω are 2/17, 1/9, and at least 1/4, respectively. By [1, page 123] the only maximal subgroups of $\mathrm{Sp}(8, 2)$ with order divisible by $5 \cdot 9 \cdot 17$ are $\mathrm{Sp}(4, 4).2$ and $\mathrm{O}^-(8, 2) : 2$. However, $\mathrm{Sp}(4, 4).2$ does

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

not contain elements of order 9 by [1, page 45]. As G does not preserve a quadratic form it is not contained in $O^-(8,2):2$. Hence G contains Ω.

Case $(d,q)=(6,2)$. The group $\Omega=\mathrm{Sp}(6,2)$ has elements of order divisible by 5 (ppd $(6,2;4)$-elements), 7 and 9 with proportions in Ω equal to $1/5$, $1/7$ and $1/9$, respectively. By [1, page 46 and 14] no maximal subgroup of Ω contains elements of orders 5, 7 and 9, so G contains Ω.

Case $(d,q)=(6,3)$. The group $\Omega=\mathrm{Sp}(6,3)$ has elements of order a multiple of 7 (ppd $(6,3;6)$-elements) and 5 (ppd $(6,3;4)$-elements) with proportions $1/7$ and $1/5$. By [1, page 113], Ω has no maximal subgroups of order divisible by $5\cdot 7$, so G contains Ω.

Case $(d,q)=(4,2)$. The group $\Omega'\cong A_6$ in this case and one can simply compute the order of G by representing it as a permutation group on the 15 non-zero vectors. If $|A_6|$ divides $|G|$ then G contains Ω'.

Case $(d,q)=(4,3)$. The group $\Omega=\mathrm{Sp}(4,3)$ contains elements of order divisible by 5 (ppd $(4,3;4)$-elements) and 9 and their proportions in Ω are $1/5$ and $2/9$. By [1, page 26] no maximal subgroup of Ω contains elements of order 5 and 9, so G contains Ω.

Case $d=4$ with $q\geq 4$. Here $\Omega=\mathrm{Sp}(4,q)$ contains large and basic ppd$(4,q;4)$-elements and by [10, Theorem 5.7 and Theorem 5.8] the proportion of these elements in Ω is at least $1/5$. If $q=5$ then these elements have order a multiple of 13. By Theorem 3.1, either G contains Ω, or $G'=\mathrm{Sz}(q)$ (with $q=2^{2k+1}$), or G is conjugate to a subgroup of $\Delta\cap(\mathrm{GL}(2,q^2).2)$. Suppose first that q^2-1 has a large primitive prime divisor, that is (by Theorem 2.2) q is not of the form 2^s-1 or $3\cdot 2^s-1$. By Theorem 4.2 the proportion of large and splitting ppd $(4,q;2)$-elements in Ω is at least $1/25$. Suppose that G also contains a large and splitting ppd $(4,q;2)$-element g with respect to the prime r. Then $G'\neq\mathrm{Sz}(q)$ by Corollary 3.2. If $g\in(\Omega\cap\mathrm{GL}(2,q^2).2)'=\mathrm{SL}(2,q^2)$ then by Proposition 4.4(a), V is the sum of two isomorphic $\langle g\rangle$-modules and hence g is not splitting which is a contradiction. Thus G is not conjugate to a subgroup of $\Delta\cap(\mathrm{GL}(2,q^2).2)$, and so by Corollary 3.2, G contains Ω.

Now suppose that $q=3\cdot 2^s-1$ or 2^s-1 for some s. Then $G'\ncong\mathrm{Sz}(q)$. Moreover, if $q\geq 7$ then by Proposition 4.4 (b) and (c), an element g of order a multiple of 4, (if $q=2^s-1$) or a multiple of 3 or 4 (if $q=3\cdot 2^s-1$) does not lie in an extension field subgroup so G contains Ω; further the proportion of such elements is as listed.

The single case remaining is $q=5$. In this case $p(\Omega,15)\geq 1/5$ and $\mathrm{SL}(2,25).2$ contains no elements of order a multiple of 15. □

Next we tackle the groups of type $\mathbf{O}^+$. Here our general strategy of finding several elements in G is effective for recognising whether or not G contains Ω in all but two cases. The exceptions are for $(d,q)=(8,3)$ or $(8,2)$ and we discuss in the proof a

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

TABLE 4. $\mathbf{X} = \mathbf{O}^+$

d	q	elements in G	proportions
10	2	17, 31	2/17, 6/31
8	2	7, 9, 10 or 15, perm. rep.	1/7, 1/9, 3/20 or 1/5
8	3	7, 13, perm. rep.	1/7, 2/13
8	5	7, 13	1/7, 1/81
8	$q = 4$ or $q > 5$	basic lppd $(8, q; 6)$,	1/7
		splitting lppd $(8, q; 4)$	1/81
6	2	7, 15	2/7, 2/15
6	3	5, 13	1/5, 4/13
6	$q \geq 4$	basic lppd $(6, q; 4)$, ppd $(6, q; 3)$	1/5, 1/7
4	$q = 8$ or $q \geq 11$	$(+1, +1)$-element (large order),	see Theorem 4.6
		$(+1, -1)$ or $(-1, +1)$-element,	
		$(-1, -1)$-element	
4	$q \leq 7$ or $q = 9$	perm. rep., (see Table 5)	

method for handling them and record the elements sought in these cases in Table 4.

THEOREM 5.3 (Orthogonal $\mathbf{O}^+$ case). *Let $G \leq \mathrm{GL}(d, q)$ be an irreducible subgroup with parameters $(\mathbf{O}^+, d, q)$ with (d, q) as in Theorem 2.5 (4) (i), and suppose that G contains several elements as in the relevant line of Table 4. Then provided $(d, q) \neq (8, 3)$ or $(8, 2)$, or $d = 4$ with $q \leq 7$ or $q = 9$, the group G contains $\Omega = \Omega^+(d, q)$. Moreover, lower bounds for the proportions of each type of element in Ω are given in the last column of Table 4. If $(d, q) = (8, 3)$ or $(8, 2)$ and the permutation group induced on an orbit on 1-spaces has order divisible by $|\Omega|/\gcd(2, q-1)$; then G contains Ω. If $d = 4$ with $q \leq 7$ or $q = 9$, and $|\Omega|$ divides $|G|$, and the extra condition in Table 4 holds, then G contains Ω.*

PROOF. Case $(d, q) = (10, 2)$. The group $\Omega = \Omega^+(10, 2)$ has elements of order divisible by 17. These are basic lppd$(10, 2; 8)$-elements and their proportion in Ω is 2/17. Also the proportion in Ω of elements of order 31 is 6/31. By [1, page 146] there are no maximal subgroups of Ω with order divisible by $17 \cdot 31$.

Case $(d, q) = (8, 2)$. The group $\Omega = \Omega^+(8, 2)$ contains elements of orders 7, 9, 10 and 15 and their proportions are 1/7, 1/9, 3/20 and 1/5, respectively. If G contains elements of orders 7, 9, and also an element of order 10 or 15, then either G contains Ω or G is nearly simple with $G' = A_9$ or $G' = \mathrm{Sp}(6, 2)$. Note that the group Ω acts transitively on the 135 isotropic points and on the 120 non-isotropic points of V. It is very difficult to distinguish these nearly simple groups from Ω, as two of the three conjugacy classes of subgroups $\mathrm{Sp}(6, 2)$ and A_9 also act transitively on the isotropic

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

and non-isotropic points. In this case we choose a non-zero vector in V and compute its orbit under G. If the orbit does not have length either 120 or 135 then G does not contain Ω. Otherwise we construct the permutation representation of G on this orbit of 120 or 135 vectors and then compute the order of G.

Case $(d, q) = (8, 3)$. The group $\Omega = \Omega^+(8, 3)$ contains ppd $(8, 3; 6)$-elements, which are elements of order divisible by 7. Their proportion is $1/7$ by [1, pages 136–139]. Further, Ω contains elements of order 13 and by [1, pages 136–139] their proportion is $2/13$. The only maximal subgroup of Ω whose order is divisible by $7 \cdot 13$ is isomorphic to $\Omega(7, 3)$.

Four of the six conjugacy classes of subgroups $\Omega(7, 3)$ are transitive on the two Ω-orbits of length 1080 on non-isotropic points (1-spaces) as well as being transitive on the Ω-orbit of length 1120 on isotropic points (1-spaces). In this case we find a G-orbit on 1-spaces in V. If the length of this orbit is not 1080 or 1120 then G does not contain Ω. Otherwise we compute the order of the permutation representation of G on this orbit. If this order is divisible by $|\Omega|/2$ then G contains Ω.

Case $d = 8$ and $q = 4$ or $q > 5$. The group $\Omega = \Omega^+(8, q)$ contains basic lppd $(8, q; 6)$-elements and their proportion is at least $1/7$. Further, by Theorem 4.2, Ω contains splitting lppd $(8, q; 4)$-elements and their proportion is at least $1/81$. Suppose that G contains elements of each of these types, and let r be a large primitive prime divisor of $q^4 - 1$ corresponding to a splitting lppd $(8, q; 4)$-element in G. Then by Corollary 3.2 either G contains Ω, or $G \leq \Delta \cap (\mathrm{GL}(4, q^2).2)$, or G is nearly simple and G' is $[2].\Omega(7, q)$ or $\mathrm{Sp}(6, q)$ (as in line 11 or line 12 of Table 1).

Suppose that $G \leq \Delta \cap (\mathrm{GL}(4, q^2).2)$. Then by [7, Table 3.5. E] it follows that $G \leq \mathrm{GU}(4, q^2).2$, (for $G \not\leq Z \circ \mathrm{O}^+(4, q^2).2$ since G contains a ppd $(8, q; 6)$-element). A Sylow r-subgroup R_0 of G is therefore cyclic of order r^a where r^a is the r-part of $q^4 - 1$, and R_0 preserves a decomposition of V as $U \oplus W$ where U, W are irreducible $\mathbb{F}_q R_0$-modules of dimension 4. We claim that U, W are isomorphic as $\mathbb{F}_q R_0$-modules. Now $U^\perp$ is R_0-invariant as is $U \cap U^\perp$, and $U \cap U^\perp = U$ or 0 since R_0 is irreducible on U. If $U \cap U^\perp = 0$ then U is non-singular, and hence (see [7, Proposition 4.3.18, Table 4.3. A]) U is also non-singular with respect to the $\mathbb{F}_{q^2}$-unitary form preserved by $\mathrm{U}(4, q^2)$; this implies that the subgroup of $\mathrm{GL}(U)$ induced by $\mathrm{GU}(4, q^2)$ is $\mathrm{GU}(2, q^2) = \mathrm{GL}(2, q) \circ \mathbb{Z}_{q^2-1}$. However the order of this group is not divisible by r. Hence $U \cap U^\perp = U$, that is U and hence also W are totally singular, and R_0 is contained in the stabiliser in Δ of this decomposition $V = U \oplus W$, namely $\mathrm{GL}(4, q).2$. This means that a generator of R_0 is similar to

$$\begin{pmatrix} A & 0 \\ 0 & A^{\mathrm{tr}} \end{pmatrix}$$

for some irreducible $A \in \mathrm{GL}(4, q)$ and hence U and W are isomorphic as $\mathbb{F}_q R_0$-modules. Thus R_0, and also $\Delta \cap (\mathrm{GL}(4, q^2).2)$ contain no splitting ppd $(8, q; 4)$-

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

elements. Hence $G \not\leq \Delta \cap (\mathrm{GL}(4, q^2).2)$.

A Sylow r-subgroup of an irreducible $[2].\Omega(7, q)$ or $\mathrm{Sp}(6, q)$ lies in a subgroup $\Omega(6, q)$ which acts on V as $\mathrm{SL}(4, q)$ preserving a decomposition $V = U \oplus W$, where U and W are totally singular 4-dimensional subspaces and W is the dual of U under the action of $\mathrm{SL}(4, q)$. By the argument of the previous paragraph this group contains no splitting ppd $(8, q; 4)$-elements, and hence $G' \neq [2].\Omega(7, q)$. Hence $G \geq \Omega$.

Case $(d, q) = (8, 5)$. Here the argument is analogous to the general case above for $q > 5$, except that the bppd $(8, 5; 6)$-elements have order a multiple of 7 and so are not large. However the ppd $(8, 5; 4)$-elements have order a multiple of 13, and so applying Theorem 3.1 to a group G containing elements of both types yields the same possibilities as above because the subgroups in cases (d) and (e) do not contain elements of order 13.

Case $(d, q) = (6, 2)$. The group $\Omega = \Omega^+(6, 2)$ is isomorphic to A_8. The proportion of elements in A_8 of order 7 or 15 is 2/7 or 2/15, respectively. The only maximal subgroups of A_8 whose order is divisible by 7 and 15 is A_7. However, this group does not contain elements of order 15.

Case $(d, q) = (6, 3)$. The group $\Omega = \Omega^+(6, 3)$ contains ppd $(6, 3; 4)$-elements, which are elements of order divisible by 5. Their proportion is 1/5. Further, Ω contains elements of order 13. By [1, page 68] the proportion of elements of order 13 is 4/13 and there are no maximal subgroups of $\Omega^+(6, 3)$ whose order is divisible by $5 \cdot 13$.

Case $d = 6$, $q \geq 4$. The group $\Omega = \Omega^+(6, q)$ contains basic lppd $(6, q; 4)$-elements and their proportion is at least 1/5. Also by Proposition 4.3 the proportion of ppd $(6, q; 3)$-elements in Ω is at least 1/7. If G contains an element of each of these types then, by Theorem 3.1, if follows that G contains Ω (since $\mathrm{GL}(3, q^2).2$ contains no ppd $(6, q; 3)$-elements).

Case $(d, q) = (4, q)$. The group $\Omega = \Omega^+(4, q)$ is isomorphic to $\mathrm{SL}(2, q) \circ \mathrm{SL}(2, q) = L_1 \circ L_2$, say, and Ω preserves a tensor product decomposition $V = U_1 \otimes U_2$, where the U_i are maximal totally singular subspaces of V of dimension 2.

Suppose first that $q = 8$ or $q \geq 11$. By Theorem 4.6, the proportion of (δ, δ')-elements in Ω, (where $\delta, \delta' \in \{1, -1\}$) is at least $(1 - 2\nu/(q + \delta))(1 - 2\nu/(q + \delta'))/4$ where $\nu = 1$ if q is even, and $\nu = 3$ if q is odd. For all q such that $q = 8$ or $q \geq 11$, this proportion is at least 1/25 (and it approaches 1/4 for large q). Thus we suppose that $G \cap \Omega$ contains a $(-1, -1)$-element g, a $(+1, +1)$-element h and a $(+1, -1)$-element or $(-1, +1)$-element k. (Note that $\Delta = (\mathrm{GL}(2, q) \circ \mathrm{GL}(2, q)).2$ so that we may in practice obtain elements of $G \cap \Omega$ by taking products of commutators of squares of random elements of G.) If $q \neq 2^s - 1$ for any s we may assume that h induces a bppd $(2, q; 2)$-element on each of the U_i of order at least 9 and not both equal to 10, while if $q = 2^s - 1 \geq 31$ we may assume that h induces an element of order at least $2^{s-1} \geq 16$ on each of the U_i. Let $\pi_i : \Omega \to L_i$ for $i = 1, 2$. Then $\pi_i(G \cap \Omega) \not\cong G \cap \Omega$

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

TABLE 5. Subgroups of SL $(2, q) \circ$ SL $(2, q)$.

q	$2(q-1)\gcd(2, q-1)$	possibilities for H	extra conditions
9	32	—	—
7	24	$\mathbb{Z}_7 \times \mathrm{SL}(2,7) \leq H$	$3 \mid \lvert\pi_i(G \cap \Omega)\rvert$, $i = 1, 2$
5	16	—	—
4	6	$D_{10} \times A_5$	$3 \mid \lvert\pi_i(G \cap \Omega)\rvert$, $i = 1, 2$
3	8	$\mathbb{Z}_6 \times \mathrm{SL}(2,3)$	$4 \mid \lvert\pi_i(G \cap \Omega)\rvert$, $i = 1, 2$
2	2	$\mathbb{Z}_3 \times \mathbb{Z}_3 \leq H$	$2 \mid \lvert\pi_i(G \cap \Omega)\rvert$, $i = 1, 2$

TABLE 6. $\mathbf{X} = \mathbf{O}^-$.

d	q	elements of G	proportions
8	2	9, 17	1/9, 4/17
6	2	5, 9	1/5, 2/9
6	3	5, 7, 9	1/5, 2/7, 4/27
4	2	3, 5	1/3, 2/5
4	3	5, perm. rep.	2/5, –
4	$q \geq 4$	large bppd $(4, q; 4)$, and special method	1/5

since $k \in G \cap \Omega$. Hence if $\pi_i(G \cap \Omega)$ were equal to L_i for both $i = 1$ and $i = 2$, then G contains Ω. Now for each i, $\pi_i(G \cap \Omega)$ contains $\pi_i(g)$ and $\pi_i(h)$ which have orders dividing $q-1$ and $q+1$, respectively, and greater than 2 (greater than 4 if q is odd); and if $q \neq 2^s - 1$ then $\pi_i(h)$ is a bppd $(2, q; 2)$-element of L_i of order modulo scalars at least 6, while if $q = 2^s - 1$ then $\pi_i(h)$ has order modulo scalars at least $2^{s-1} \geq 8$. No proper subgroup of SL $(2, q)$ contains such elements. (This can be seen by examining the list of subgroups of PSL $(2, q)$ in Dickson [2, Chapter XII].)

Now suppose that $q \in \{2, 3, 4, 5, 7, 9\}$. We construct a permutation representation for G on one-dimensional subspaces of V and find $|G|$. If $|\Omega|$ does not divide $|G|$ then G does not contain Ω. Hence we may suppose that $|\Omega|$ divides $|G|$.

If $G \cap \Omega < \Omega$ then $|G \cap \Omega||\Delta : \Omega| = |G \cap \Omega| 2(q-1)\gcd(2, q-1)$ is divisible by $|G|$, and so in particular $|\Omega|/|G \cap \Omega|$ divides $2(q-1)\gcd(2, q-1)$. Thus we need to find all subgroups H of $\Omega \cong \mathrm{SL}(2, q) \circ \mathrm{SL}(2, q)$ whose index divides $2(q-1)\gcd(2, q-1)$. These subgroups are listed in Table 5.

If there are no possibilities for H then G contains Ω. In all other cases we test whether $G \cap \Omega$ projects modulo scalars as SL $(2, q)$ onto both central factors, in which case G has to contain Ω. □

THEOREM 5.4 (Orthogonal $\mathbf{O}^-$ case). *Let $G \leq \mathrm{GL}(d, q)$ be an irreducible subgroup with parameters $(\mathbf{O}^-, d, q)$ with (d, q) as in Theorem* 2.5 (4) (ii), *and suppose*

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

that G contains several elements as in the relevant line of Table 6. Then the group G contains $\Omega = \Omega^-(d, q)$. Moreover, lower bounds for the proportions of each type of element in Ω are given in the last column of Table 6.

PROOF. Case $(d, q) = (8, 2)$. The group $\Omega = \Omega^-(8, 2)$ contains elements of order 17 (ppd $(8, 2; 8)$-elements) and 9 with proportions $4/17$ and $1/9$, respectively. By [1, page 89] there are no maximal subgroups of this group of order divisible by $9 \cdot 17$.

Case $(d, q) = (6, 2)$. The group $\Omega = \Omega^-(6, 2)$ is isomorphic to $\mathrm{Sp}(4, 3)$ and can be handled in the same way as that group.

Case $(d, q) = (6, 3)$. The group $\Omega = \Omega^-(6, 3)$ is isomorphic to $U(4, 3)$. Now Ω contains ppd $(6, 3; 4)$-elements of order 5, ppd $(6, 3; 6)$-elements of order 7 and elements of order 9 with proportions $1/5$, $2/7$ and $4/27$, respectively. The only maximal subgroups of Ω with order divisible by 35 are $\mathrm{PSL}(3, 4)$ and A_7. However, neither of these groups has elements of order 9. (Note that the outer automorphism group of $\Omega^-(6, 3)$ is isomorphic to D_8. Therefore, if $\Omega \leq G \leq \Delta$ then G contains no elements of order 9.)

Case $(d, q) = (4, 2)$. The group $\Omega = \Omega^-(4, 2)$ is isomorphic to $\mathrm{PSL}(2, 4)$. It has ppd $(4, 2; 4)$-elements of order 5 with proportion $2/5$ and elements of order 3 with proportion $1/3$. Further, there are no maximal subgroups of $\Omega^-(4, 2)$ with order divisible by $3 \cdot 5$. Alternatively one can just compute the order of the group in its permutation action on an orbit in V.

Case $(d, q) = (4, 3)$. The group $\Omega = \Omega^-(4, 3)$ is isomorphic to $\mathrm{PSL}(2, 9)$. It has elements of order 5 modulo scalars (ppd $(4, 3; 4)$-elements) and elements of order 3 modulo scalars with proportions is $2/5$ and $1/9$, respectively. By [1, page 4] the only maximal subgroup of $\Omega^-(4, 3)$ of order divisible by 15 is D_{10} or A_5. Now Ω has one orbit on isotropic points, and two orbits on non-isotropic points, thus a total of 3 orbits on 1-spaces. Each maximal subgroup of $\Omega^-(4, 3)$ isomorphic to A_5 or S_5 has 1 orbit on isotropic points and is transitive on one of the Ω-orbits on the non-isotropic points and not transitive on the other. This is also true for subgroups S_5 of $\mathrm{O}^-(4, 3)$. This fact can be used to distinguish a group G such that $G \cap \Omega \leq A_5$ from a group containing Ω.

Case $d = 4$ and $q \geq 4$. The group $\Omega = \Omega^-(4, q)$ is isomorphic to $\mathrm{PSL}(2, q^2)$ and contains basic lppd $(4, q; 4)$-elements with proportion at least $1/5$. Suppose that G contains such an element, g say. Then by Theorem 3.1, either G contains Ω or G is an extension field group conjugate to a subgroup of $\Delta \cap (\mathrm{GL}(2, q^2).2)$ (note that $\Omega \cong \mathrm{PSL}(2, q^2)$ does not have $\mathrm{Sz}(q)$ as a subgroup). In the latter case $G \leq \mathrm{O}^-(2, q^2) \cong D_{2(q^2+1)}$ by [7, Table 4.3.A] and [12, Theorem 11.4]. In this case each generator x_i of G normalises g; either $[x_i, g] = 1$ or $[x_i, g] = g^{q^2+1}$. If $[x_i, g] \neq 1$ we check that $[x_i, g]$ centralises g; if not then we conclude that G contains Ω, while if it does then $[x_i, g] \in C_\Omega(g) \cong \mathbb{Z}_{(q^2+1)/(2,q-1)}$, whence $g^{x_i} \in C_\Omega(g)$ and

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

TABLE 7. $\mathbf{X} = \mathbf{O}^\circ$

d	q	elements of G	proportions
7	3	5, 7, 13	1/5, 1/7, 2/13
5	3	5, 9	1/5, 2/9
5	$q \geq 5$	basic lppd $(5, q; 4)$	1/5
3	3	3	2/3
3	5	3, 5	1/3, 2/5
3	7	4, 7	1/4, 2/7
3	9	3, 4 (special kind), 5	2/9, 1/4, 2/5
3	11	3, 11	1/6, 2/11
3	19	5, 9, 19	1/5, 1/3, 2/19
3*	$2^s - 1 \geq 31$	2^{s-1}, t ($t > 2$ and $t \mid q - 1$)	1/3, 1/3
3*	$3.2^s - 1 > 11$	2^{s-1}, t ($t > 2$ and $t \mid q - 1$)	1/6, 1/3
3*	$q \neq 2^s - 1, 3 \cdot 2^s - 1$	basic lppd $(3, q; 2)$,	1/3
		t ($t > 2$ and $t \mid q - 1$)	1/3

* see last paragraph of proof for extra conditions on these elements.

$x_i \in N_\Omega(C_\Omega(g)) \leq \mathrm{O}^-(2, q^2)$. In this case we deduce either that G contains Ω or we report that $G \leq \mathrm{O}^-(2, q^2)$ (the normaliser of $\langle g \rangle$). □

Now we deal with the odd dimensional orthogonal groups $\mathrm{O}^\circ(d, q)$. Note that since we are considering only irreducible subgroups G of $\mathrm{GL}(d, q)$ in this case the field size q must be odd.

THEOREM 5.5 (Orthogonal $\mathbf{O}^\circ$ case). *Let $G \leq \mathrm{GL}(d, q)$ be an irreducible subgroup with parameters $(\mathbf{O}^\circ, d, q)$ with (d, q) as in Theorem* 2.5 (4) (iii) *and suppose that G contains several elements as in the relevant line of Table* 7. *Then the group G contains $\Omega = \Omega^\circ(d, q)$. Moreover, lower bounds for the proportions of each type of element in Ω are given in the last column of Table* 7 *(with certain extra conditions if $d = 3$ and $q \geq 13$ and $q \neq 19$ as specified in the last paragraph of the proof).*

PROOF. Case $(d, q) = (7, 3)$. The group $\Omega = \Omega^\circ(7, 3)$ contains both ppd $(7, 3; 4)$-elements of order divisible by 5 and ppd $(7, 3; 6)$-elements of order divisible by 7. Their proportions in Ω are $1/5$ and $1/7$, respectively. Further, by [1, page 108] the proportion of elements of order 13 in Ω is $2/13$ and there are no maximal subgroups of order divisible by $5 \cdot 7 \cdot 13$.

Case $(d, q) = (5, 3)$. The group $\Omega^\circ(5, 3)$ is isomorphic to $\mathrm{Sp}(4, 3)$ and can be handled in the same way.

Case $d = 5$, $q \geq 5$. The group $\Omega^\circ(5, q)$ for $q > 3$ contains basic lppd $(5, q; 4)$-elements and their proportion is at least $1/5$. Suppose that G contains such an element.

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

Then by Theorem 3.1, G contains Ω.

Case $d = 3$. The group $\Omega = \Omega^\circ(3, q) \cong \mathrm{PSL}(2, q)$ and $\Delta = \mathrm{GO}(3, q) \cong \mathbb{Z}_{q-1} \times \mathrm{PGL}(2, q)$. We deal with several small values of q first and then with the general case. For $q = 3, 5, 7, 9, 11, 19$ it is easy to check that Ω contains elements of the orders and in the proportions listed in Table 7. Suppose that G contains such elements. Then since G is irreducible it follows from [1] that G contains Ω except possibly if $q = 9$ and $G \leq \mathbb{Z}_8 \times A_5 < \mathrm{GO}(3, 9) = \mathbb{Z}_8 \times \mathrm{PGL}(2, 9)$. In this case the proportion of elements of any subgroup of $\mathrm{GO}(3, q)$ containing Ω which are 2-elements and which project onto an element of order 4 or 8 in $\mathrm{PGL}(2, 9)$ is at least 1/5; such elements g may be detected by requiring that $o(g)$ is 4 or 8 and that g^2 does not centralise G. With this extra restriction on this particular element of G we can deduce that G contains Ω.

Now assume that $q \notin \{3, 5, 7, 9, 11, 19\}$. If $q \neq 2^s - 1$ or $3 \cdot 2^s - 1$ then Ω contains basic lppd $(3, q; 2)$-elements of order strictly greater than 5 while if $q = 3 \cdot 2^s - 1 > 11$ then Ω contains elements of order $3 \cdot 2^{s-1} \geq 12$, and if $q = 2^s - 1 \geq 31$ then Ω contains elements of order 2^{s-1}. If $q \neq 3 \cdot 2^s - 1$ then the proportion of such elements in Ω is at least $1/3$, while if $q = 3 \cdot 2^s - 1$ then $|\mathbb{Z}_{3 \cdot 2^{s-1}} \setminus (\mathbb{Z}_{2^{s-1}} \cup \mathbb{Z}_{3 \cdot 2^{s-2}})| = 3 \cdot 2^{s-1} - (2^{s-1} + 3 \cdot 2^{s-2}) + 2^{s-2} = 2^{s-1}$, so the proportion of these elements in Ω is $1/6$. Similarly, Ω contains elements of order greater than 2 and dividing $q - 1$, and the proportion of these elements in Ω is at least $1/3$.

Suppose that G contains an element of each of these types with the following extra condition on the first element g : if g is an lppd $(3, q; 2)$-element and the primitive prime divisor of $q^2 - 1$ dividing $o(g)$ is 5, then g^5 does not centralise G. (This guarantees that g projects onto an element of $\mathrm{PGL}(2, q)$ of order greater than 5.) We also require of the second element h that h^2 does not centralise G. (This guarantees that h projects onto an element of $\mathrm{PGL}(2, q)$ of order greater than 2.) Then it follows, on examining the list of subgroups of $\mathrm{PSL}(2, q)$ in Dickson [2, Chapter XII], that the image of the projection of G onto $\mathrm{PGL}(2, q)$ is not contained in any maximal subgroup of Ω, and it follows that G contains Ω. □

Finally we deal with the non-generic unitary groups. In Table 8, g_i denotes an element of order a multiple of i.

THEOREM 5.6 (Unitary case). *Let $G \leq \mathrm{GL}(d, q)$ be an irreducible subgroup with parameters $(\mathbf{U}, d, q)$ with (d, q) as in Theorem 2.5(3) and suppose that G contains several elements as in the relevant line of Table 8. Then the group G contains $\Omega = \mathrm{SU}(d, q)$. Moreover, lower bounds for the proportions of each type of element in Ω are given in the last column of Table 8.*

PROOF. Case $d = 6$. The group $\Omega = \mathrm{SU}(6, q)$ (q a square) contains basic lppd $(6, q; 5)$-elements and their proportion is at least $1/6$. (If $q = 4$ these elements

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

TABLE 8. $\mathbf{X} = \mathbf{U}$

d	q	elements of G	proportions
6	4	7, 10, 11	1/7, 1/10, 2/11
6	$q \geq 9$	basic lppd $(6, q; 5)$, ppd $(6, q; 3)$	1/6, 1/49
5	4	11, 12	2/11, 1/5
4	4	5, 9	1/5, 2/9
4	9	5, 7, 9	1/5, 2/7, 4/27
4	$q > 9$	bppd $(4, q; 3)$, (order > 7), ppd $(4, q; 2)$	1/4, 1/5
3	4	perm. rep.	
3	9	7, 6 (g_6^3 non-central)	2/7, 1/4
3	16	5 (non-central), 13	2/5, 4/13
3	25	5, 7, 8 ($\langle g_8 \rangle \cap Z = 1$)	11/50, 2/7, 1/4
3	$q \geq 49$	basic lppd $(3, q; 3)$ (order > 7 mod scalars),	1/4
		g, $o(g \bmod \text{scalars}) > 3$ and dividing $q - 1$	1/3

have order a multiple of 11 and their proportion in Ω is 2/11.) Also by Theorem 2.2 and Theorem 4.2 the proportion of ppd $(6, q; 3)$-elements in Ω is at least 1/49. (If $q = 4$ these elements have order a multiple of 7 and their proportion in Ω is 1/7.) Suppose that G contains elements g, h of each of these types. Suppose first that $q = 4$. By Corollary 3.2, either G contains Ω, or $G' \cong 3.M_{22}$. Since $\Delta = \Omega.3$, if the latter holds then $G \cong 3.M_{22}$ and in particular G does not contain $3.M_{22}.2$ and so G does not contain any elements of order 10. The proportion of elements of order 10 in Ω is 1/10, so if G also contains an element of order 10 then G must contain Ω. Suppose now that $q > 4$. By Corollary 3.2, either G contains Ω, or $o(g)$ is a multiple of 11 and $G' \cong \mathrm{PSL}(2, 11)$. In the latter case the ppd $(6, q; 3)$-element h must have order a multiple of 5. However, no integer q can have order 3 modulo 5, so G contains Ω.

Case $(d, q) = (5, 4)$. The group $\Omega = \mathrm{SU}(5, 4)$ contains ppd $(5, 4; 5)$-elements of orders 11 and 12 and their proportions are 2/11 and $17/72 \geq 1/5$, respectively. Since in this case $\Delta = \Omega$, there are no maximal subgroups of Ω of order divisible by $11 \cdot 12$ which contain elements of order 12, so G contains Ω.

Case $(d, q) = (4, 4)$. This group is isomorphic to $\mathrm{Sp}(4, 3)$ and can be handled in the same way.

Case $(d, q) = (4, 9)$. By [1, page 52] the proportions in Ω of elements of order a multiple of 5, 7, 9 are 1/5, 2/7, 4/27, respectively. If G is nearly simple (in the sense of Aschbacher's classification) then G is absolutely irreducible so $Z(G)$ is a group of scalar matrices and hence is a 2-group. Also $(G \cap \Omega)/Z(G) \cong A_7$ or $\mathrm{PSL}(3, 4)$ and $G/(G \cap \Omega)$ is isomorphic to a subgroup of Δ/Ω which is a 2-group. It follows that the nearly simple groups do not contain elements of order 9. Thus, if G contains elements with orders which are multiples of 5, 7 and 9, then G contains Ω.

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

Case $d = 4$, $q > 9$. The group Ω contains large and basic ppd $(4, q; 3)$-elements of order a multiple of a prime r say, and their proportion is at least $1/4$. Also, since $q + 1 = q_0^2 + 1 \not\equiv 0 \pmod 3$, a primitive prime divisor s of $q^2 - 1$ exists and is greater than 3, so either $\{r, s\} = \{5, 7\}$ or the larger of r and s is at least 11. By Proposition 4.3, Ω contains elements of order a multiple of s with proportion at least $1/5$. Suppose that G contains an element of each type. Then by Corollary 3.2, either G contains Ω, or G is nearly simple and G' is $2.A_7$ with $q_0 = p \equiv 3, 5 \pmod 7$, $r = 7$ and $s = 5$. If 7 is a primitive prime divisor of $q^3 - 1$ then Ω contains elements of order a proper multiple of 7 which divides $q^3 - 1$ but not $7(q - 1)$, and their proportion is at least $1/4$. Thus if, in this case, we also require that G contains such an element then G contains Ω.

Case $(d, q) = (3, 4)$. The group SU $(3, 4)$ is isomorphic to $[3^3].Q_8$. Here we can just determine the order of the group G by computing a permutation representation on vectors.

Case $(d, q) = (3, 9)$. The group Ω contains elements of orders 7 and a multiple of 6 with proportions 2/7 and 1/4 respectively, and no maximal subgroup of Ω contains elements of both these orders. Thus if G contains elements g_7, g_6 of orders a multiple of 7 and 6 such that g_6^3 is non-central, then G contains Ω.

Case $(d, q) = (3, 16)$. The group Ω contains elements of orders multiples of 5 and 13 with proportions at least 2/5 and 4/13 respectively and no maximal subgroup of Ω contains elements of both types. Thus if G contains elements g_5, g_{13} of orders a multiple of 5 and 13 with g_5 non-central, then G contains Ω.

Case $(d, q) = (3, 25)$. The group Ω contains elements of orders multiples of 5,7 and 8 with proportions at least 11/50, 2/7 and 1/4 respectively and no maximal subgroup of Ω contains elements of all these types. Thus if G contains elements g_5, g_7, g_8 of orders a multiple of 5, 7 and 8 such that the involution in $\langle g_8 \rangle$ is non-central, then G contains Ω.

Case $d = 3$, $q = q_0^2 \geq 49$. The group Ω contains basic lppd $(3, q; 3)$- elements of order dividing $(q_0^2 - q_0 + 1)/\gcd(3, q_0 + 1)$, and strictly greater than $7 \gcd(3, q_0 + 1)$, with proportion greater than 1/4. If G contains a basic lppd $(3, q; 3)$-element of order modulo scalars greater than 7, then by Theorem 3.1, either G contains Ω or G is conjugate to a subgroup of an extension field group $\Delta \cap (\mathrm{GL}(1, q^3).3) = (\mathbb{Z}_{(q_0^3+1)(q_0-1)}).3$. Now Ω also contains a unique conjugacy class of self-centralising cyclic subgroups of order $(q - 1)/\gcd(3, q_0 + 1)$ modulo scalars with normaliser twice that order; and we note that the quotient group of $\Delta \cap (\mathrm{GL}(1, q^3).3)$ modulo scalars is $(\mathbb{Z}_{q_0^2-q_0+1}).3$. Thus an element of Δ of order s modulo scalars, where $s > 3$ and s divides $q - 1$, cannot lie in any extension field subgroup, so if G also contains such an element then G contains Ω. Moreover, the proportion of such elements in Ω is at least 1/3. □

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

6. Implementation issues

The algorithm described in this paper to recognise non-generic classical groups over finite fields has been implemented in both GAP and MAGMA. It has become part of our previously implemented recognition algorithm for recognising classical groups over finite fields. In most of the non-generic cases methods used in the implementation are virtually identical to those used in the implementation of the generic cases (see [9] for details) and require no further comment. However, in some cases different techniques had to be developed and these deserve special attention here.

In many of the examples of non-generic classical groups we search for elements of certain orders, which is straightforward. In some cases we need to compute permutation representations of the given group. The largest example for which we compute a permutation representation is in case $\mathbf{O}^+$ for $(d, q) = (8, 3)$. This is a routine computation in both GAP and MAGMA.

6.1. Splitting ppd-elements In the case **Sp** for $d = 4$ and $q \neq 2^s - 1, 3 \cdot 2^s - 1$ or 2, and in case $\mathbf{O}^+$ for $d = 8$ and $q = 4$ or $q > 5$, we search for splitting ppd $(d, q; d/2)$-elements.

We use the following method to test whether a ppd $(d, q; d/2)$-element g of a group G is splitting. First we test whether g is a ppd $(d, q; d/2)$-element in the usual way. In doing this, we compute the characteristic polynomial $c_g(x)$ of g. Suppose that $c_g(x)$ has two irreducible factors of degree $d/2$, since otherwise g is not splitting. Let r be a primitive prime divisor of $q^{d/2} - 1$ which divides $o(g)$ and let $h = g^s$ be the r-part of g as defined in Section 2. As r is coprime to q the underlying vector space viewed as an $\mathbb{F}_q\langle h\rangle$-module is completely reducible. If it has two non-isomorphic composition factors then g is a splitting ppd $(d, q; d/2)$-element. This can be tested using the Meataxe (see [6, 11]).

6.2. Kronecker decompositions for matrices in $\mathrm{O}^+(4, q)$ In the groups $\mathrm{O}^+(4, q)$ we search for $(+1, +1)$, $(-1, -1)$ and $(+1, -1)$-elements.

Let U denote a 4-dimensional vector space over the field $\mathbb{F}_q$ with basis $\{e_1, e_2, e_3, e_4\}$. We use Taylor's description [12, page 199] of $\mathrm{O}^+(4, q)$ as a subgroup of the general linear group of the exterior square $\Lambda_2 U$ of U. Consider the map $\alpha_2 : U \times U \to \Lambda_2 U$ defined by $(u, v) \mapsto u \wedge v$. The latter is a six dimensional vector space with basis $\{e_i \wedge e_j \mid 1 \leq i < j \leq 4\}$ and Taylor defines a certain quadratic form Q of Witt index 3 on $\Lambda_2 U$. Set $\xi := e_1 \wedge e_2$ and $\eta := e_3 \wedge e_4$. Taylor [12, pages 187 and 199] shows that the restriction of Q to $V := \langle \xi, \eta \rangle^\perp$ is a non-degenerate quadratic form of Witt index 2. Further, Taylor shows that $O(V)$ can be identified with the subgroup of $O(\Lambda_2 U)$ fixing ξ and η; and that V has the following vectors as basis: $E_1 := e_1 \wedge e_3$, $E_2 := e_1 \wedge e_4$, $F_1 := e_2 \wedge e_4$ and $F_2 := e_2 \wedge e_3$. Then, if $v \in W$ has the form

$v = a_1E_1 + a_2E_2 + b_1F_1 + b_2F_2$, it follows from the definition of Q in [12, page 187] that $Q(v) = -a_1b_1 + a_2b_2$ and in particular $Q(E_i) = Q(F_i) = 0$ for $i = 1, 2$. Therefore the polar form φ of Q with respect to the (ordered) basis $\{E_1, E_2, F_2, F_1\}$ has the form

$$\begin{pmatrix} & & & -1 \\ & & 1 & \\ & 1 & & \\ -1 & & & \end{pmatrix}.$$

Now let $E := \langle e_1, e_2\rangle$ and $F := \langle e_3, e_4\rangle$, and identify $\mathrm{GL}(E)$ (or $\mathrm{GL}(F)$) with the subgroup of $\mathrm{GL}(U)$ fixing F (or E) pointwise and acting naturally on E (or F). Then, $\mathrm{GL}(E) \times \mathrm{GL}(F)$ induces an action on V preserving the quadratic form Q with kernel a diagonal subgroup of the direct product of the subgroups of scalar matrices on E and F. Moreover, Taylor shows that $\mathrm{O}^+(V)$ is isomorphic to $\mathrm{GL}(E) \circ \mathrm{GL}(F)$ and that $\Delta = \mathrm{GO}^+(V)$ contains $\mathrm{GL}(E) \circ \mathrm{GL}(F)$ as a subgroup of index 2 (and Δ interchanges $\mathrm{GL}(E)$ and $\mathrm{GL}(F)$). The matrices representing elements of $\mathrm{O}^+(V)$ with respect to the ordered basis $\{E_1, E_2, F_2, F_1\}$ are Kronecker products $A \otimes B$, where $A, B \in \mathrm{GL}(2, q)$, and each element of $\mathrm{O}^+(V)$ determines the "factors" A, B up to a scalar multiple.

Now suppose that $G \leq \mathrm{GL}(4, q)$ with parameters $(\mathbf{O}^+, 4, q)$ and that G contains $\Omega^+(4, q)$ and fixes a non-degenerate quadratic form Q_0 on V with polar form ψ. By Witt's Theorem (see [12, Theorem 7.4]) it follows that ψ is conjugate to φ, that is, there is a matrix $X \in \mathrm{GL}(4, q)$ such that $X^{Tr}\varphi X = \psi$. We determine this matrix X which maps the given symmetric bilinear form to φ thereby mapping the given basis to $\{E_1, E_2, F_2, F_1\}$. Then $g^X = X^{-1}gX$ rewrites an element g in G with respect to this basis and we can then read off the Kronecker decomposition of g, that is we can determine two 2×2 matrices A and B such that $g^X = A \otimes B$. Note that by the nature of the Kronecker Product A and B are only determined up to a scalar multiple since $aA \otimes a^{-1}B = A \otimes B$ for all $a \neq 0$. Having decomposed g^X in this form it is easy to determine whether or not g is a $(+1, +1)$, $(+1, -1)$ or $(-1, -1)$-element by computing the orders of the matrices A and B.

If q is odd then Q, Q_0 are determined uniquely by φ, ψ, respectively and hence $Q(vX) = Q_0(v)$, for all $v \in V$. On the other hand if q is even then φ, ψ are symplectic forms and there are several quadratic forms corresponding to each of φ, ψ. However, since $\mathrm{Sp}(V)$ is transitive on the quadratic forms of $+$-type corresponding to ψ there is an $X \in \mathrm{Sp}(V)$ such that $Q(vX) = Q_0(v)$ for all $v \in V$.

In the case of $\mathrm{O}^+(4, q)$ where $q \in \{2, 3, 4, 5, 7, 9\}$ we do not search for $(+1, +1)$, $(+1, -1)$ or $(-1, -1)$-elements. In the proof of Theorem 5.3 we needed to be able to decide whether a subgroup G of $2.(\mathrm{GL}(2, q) \circ \mathrm{GL}(2, q))$ projects to a subgroup containing $\mathrm{SL}(2, q)$ in each factor of the central product. In this case we can use the

https://doi.org/10.1017/S1446788700001191 Published online by Cambridge University Press

method we just described. We select some matrices of G at random and compute their Kronecker decompositions. We compute two subgroups of GL $(2, q)$, that is, the subgroups generated by the first and the second factors of the Kronecker decompositions of these elements. We then compute the orders of these subgroups modulo scalars and are thus able to decide whether the projections modulo scalars contain SL $(2, q)$. We can also decide (for example by finding a $(+1, -1)$-element) that G is not a diagonal subgroup of SL $(2, q) \circ$ SL $(2, q)$.

Acknowledgements

We are grateful to Tim Penttila, Bob Liebler and Martin Liebeck for helpful advice about the groups of type $O^+(4, q)$, $O^-(4, q)$ and $O^+(8, q)$, respectively. We also thank one of our referees for useful comments.

References

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

[2] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, with an introduction by W. Magnus (Dover Publications Inc., New York, 1958).

[3] W. Feit, 'On large Zsigmondy primes', *Proc. Amer. Math. Soc.* **102** (1988), 29–36.

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

[5] C. Hering, 'Transitive linear groups and linear groups which contain irreducible subgroups of prime order', *Geom. Dedicata* **2** (1974), 425–460.

[6] Derek F. Holt and Sarah Rees, 'Testing modules for irreducibility', *J. Austral. Math. Soc. Ser. A* **57** (1994), 1–16.

[7] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Ser. vol. 129 (Cambridge University Press, Cambridge, 1990).

[8] P. M. Neumann and C. E. Praeger, 'A recognition algorithm for special linear groups', *Proc. London Math. Soc.* **65** (1992), 555–603.

[9] A. C. Niemeyer and C. E. Praeger, 'Implementing a recognition algorithm for classical groups', in: *Groups and computation II* (eds. L. Finkelstein and W. M. Kantor), Amer. Math. Soc. DIMACS Series vol. 28 (DIMACS, 1995) (1997) pp. 273–296.

[10] ———, 'A recognition algorithm for classical groups over finite fields', *Proc. London Math. Soc.* (3) **77** (1998), 117–169.

[11] R. A. Parker, 'The computer calculation of modular characters (the Meat-Axe)', in: *Computational group theory* (ed. M. D. Atkinson), (Durham, 1982) (Academic Press, New York, 1984) pp. 267–274.

[12] D. E. Taylor, *The geometry of the classical groups*, Sigma Series in Pure Mathematics vol. 9 (Heldermann, Berlin, 1992).

[13] K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. Math. Phys.* **3** (1892), 265–284.

Department of Mathematics and Statistics
University of Western Australia
Nedlands WA 6907
Australia
e-mail: alice@maths.uwa.edu.au, praeger@maths.uwa.edu.au