Bull. Aust. Math. Soc. **86** (2012), 50–63
doi:10.1017/S0004972712000317

ALGORITHMS TO IDENTIFY ABUNDANT p-SINGULAR ELEMENTS IN FINITE CLASSICAL GROUPS

ALICE C. NIEMEYER, TOMASZ POPIEL and CHERYL E. PRAEGER ✉

(Received 3 March 2012)

Dedicated to John Cossey on the occasion of his 70th birthday

Abstract

Let G be a finite d-dimensional classical group and p a prime divisor of $|G|$ distinct from the characteristic of the natural representation. We consider a subfamily of p-singular elements in G (elements with order divisible by p) that leave invariant a subspace X of the natural G-module of dimension greater than $d/2$ and either act irreducibly on X or preserve a particular decomposition of X into two equal-dimensional irreducible subspaces. We proved in a recent paper that the proportion in G of these so-called *p-abundant* elements is at least an absolute constant multiple of the best currently known lower bound for the proportion of all p-singular elements. From a computational point of view, the p-abundant elements generalise another class of p-singular elements which underpin recognition algorithms for finite classical groups, and it is our hope that p-abundant elements might lead to improved versions of these algorithms. As a step towards this, here we present efficient algorithms to test whether a given element is p-abundant, both for a known prime p and for the case where p is not known *a priori*.

2010 *Mathematics subject classification*: primary 20G40; secondary 20P05.

Keywords and phrases: finite groups of Lie type, proportions of elements, large invariant subspaces.

1. Introduction

Estimates for the proportion of elements of order divisible by a certain prime in finite groups have not only provided a better theoretical understanding of these groups, but also underpinned the design of many algorithms for computing with them [3, 6, 11, 13, 18]. In a recent paper [16], we introduced a subfamily of p-singular elements (elements with order divisible by p) in finite classical groups G for p a prime divisor of $|G|$ distinct from the natural characteristic, defined as follows.

Definition 1.1. Let q be a prime power, n a positive integer, and G, δ, $d = d(n)$ as in one of the lines of Table 1. Let $V = V(d, q^{\delta})$ denote the natural G-module.

The first and third authors acknowledge the support of the Australian Research Council Discovery Project DP110101153. The second author acknowledges support within the Australian Research Council Federation Fellowship FF0776186 of the third author.

TABLE 1. The groups considered in this paper: G contains (p, m)-abundant elements if and only if the integer m, in addition to lying in the range $(d/2, d]$, satisfies the stated conditions.

G	δ	d	G contains (p, m)-abundant irreducible elements if and only if	G contains (p, m)-abundant quasi-irreducible elements if and only if
$\mathrm{GL}_n(q)$	1	n	$p \mid q^m - 1$	Never
$\mathrm{GU}_n(q)$	2	n	m odd and $p \mid q^m + 1$	m even and $p \mid q^m - 1$
$\mathrm{Sp}_{2n}(q)$	1	$2n$	m even and $p \mid q^{m/2} + 1$	m even and $p \mid q^{m/2} - 1$
$\mathrm{SO}_{2n+1}(q)$	1	$2n + 1$	m even and $p \mid q^{m/2} + 1$	m even and $p \mid q^{m/2} - 1$
$\mathrm{SO}^+_{2n}(q)$	1	$2n$	$m \neq d$, m even and $p \mid q^{m/2} + 1$	m even and $p \mid q^{m/2} - 1$
$\mathrm{SO}^-_{2n}(q)$	1	$2n$	m even and $p \mid q^{m/2} + 1$	$m \neq d$, m even and $p \mid q^{m/2} - 1$

Let p be a prime dividing $|G|$ and coprime to q, and m an integer with $d/2 < m \leq d$. An element $g \in G$ is said to be (p, m)-*abundant* if, in its action on V, g has an eigenvalue ζ in some extension field of $\mathbb{F}_{q^\delta}$ such that ζ has multiplicative order divisible by p and either:

(i) ζ has m Galois conjugates over $\mathbb{F}_{q^\delta}$; or

(ii) $G \neq \mathrm{GL}_n(q)$, m is even, ζ and ζ^{-1} are not Galois conjugate, and ζ and ζ^{-1} have together m Galois conjugates over $\mathbb{F}_{q^\delta}$.

The element g is called (p, m)-*abundant irreducible* in case (i) and (p, m)-*abundant quasi-irreducible* in case (ii), and is said to be of *type* ‘irreducible’ or ‘quasi-irreducible’, respectively, in these cases. In either case, a p-*abundant* element is one that is (p, m)-abundant for some m with $d/2 < m \leq d$.

The terms ‘irreducible’ and ‘quasi-irreducible’ are chosen to reflect certain properties of the actions of p-abundant elements on the natural G-module. The (p, m)-abundant irreducible elements leave invariant a unique irreducible subspace of dimension m (see Lemma 2.1). The (p, m)-abundant quasi-irreducible elements have a similar property, preserving a specific decomposition of a unique invariant m-dimensional subspace into two closely related irreducible subspaces of dimension $m/2$ (see Lemma 2.4).

Necessary and sufficient conditions for the existence of p-abundant elements are summarised in Table 1. The group G in a given line of the table contains (p, m)-abundant elements if and only if the integer m, in addition to lying in the range $(d/2, d]$, satisfies the conditions detailed in the final two columns. Note in particular that, in accordance with the definition, $\mathrm{GL}_n(q)$ contains no p-abundant quasi-irreducible elements. Justification for Table 1 is given in our other paper on p-abundant elements [16].

REMARK 1.2. In particular, it follows from Table 1 that a given element can be (p, m)-abundant for at most one value of m, because the definition requires that $m > d/2$. Similarly, the type of a p-abundant element is unique.

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

The p-abundant *irreducible* elements can be viewed as a generalisation of the subfamily of p-singular elements, called $\mathrm{ppd}(d, q^\delta; m)$ elements, considered in the first and third authors' recognition algorithm for finite classical groups [18]. Here the prime p is said to be a *primitive prime divisor* (ppd) of $q^e - 1$ if e is minimal such that p divides $q^e - 1$, namely if q has order e modulo p. The $\mathrm{ppd}(d, q^\delta; m)$ elements also leave invariant a unique irreducible subspace (of the natural G-module) of dimension $m > d/2$, and indeed all $\mathrm{ppd}(d, q^\delta; m)$ elements are (p, m)-abundant irreducible.

The $\mathrm{ppd}(d, q^\delta; m)$ elements are useful in practice because they can be found easily by random selection, arising with frequency $O(1/d)$, and because there exists an efficient algorithm to test whether a given element is a $\mathrm{ppd}(d, q^\delta; m)$ element for some m [18]. The following result shows that, in the cases where they exist, p-abundant elements are even easier to find by random selection, comprising a constant proportion of the elements in G as the dimension $d \to \infty$. The proof and an explicit expression for the constant $c(G; p)$ are given in our other paper on p-abundant elements [16, Theorem 1.3].

Theorem 1.3. *Let q be a prime power, n a positive integer, and G as in one of the lines of Table 1. Let p be an odd prime dividing $|G|$ and coprime to q, and e the smallest positive integer such that p divides $q^e - 1$. For $\mathtt{T} = \mathtt{I}$ or $\mathtt{T} = \mathtt{QI}$, let $Q(p; \mathtt{T}; G)$ denote the set of all p-abundant irreducible or quasi-irreducible elements in G, respectively. There is a constant $c(G; p)$ depending only on p and the type of G, and an absolute constant α, such that in all cases where $Q(p; \mathtt{T}; G)$ is nonempty (see Table 1),*

$$\left| \frac{|Q(p; \mathtt{T}; G)|}{|G|} - \frac{c(G; p)}{e} \right| < \frac{\alpha}{n}.$$

The assumption that $p \neq 2$ in Theorem 1.3 is made for technical reasons, as explained in our other paper [16]. We believe that a similar result holds in the case where $p = 2$.

An interesting implication of Theorem 1.3 is that, in all cases where the set $Q(p; \mathtt{T}; G)$ is nonempty, the proportion $|Q(p; \mathtt{T}; G)|/|G|$ is at least a constant multiple of the best currently known lower bound for the proportion of *all* p-singular elements in G, which can be deduced from two theorems of Isaacs *et al.* [11, Theorems 6.2 and 8.1]. This is explained in more detail in our other paper [16].

It is our hope that p-abundant elements might be used in new, improved recognition algorithms for finite classical groups, playing a role similar to that of the ppd elements in the first and third author's existing algorithm [18]. This paper is a step towards this aim. We prove the following two theorems, in which ω denotes the exponent of matrix multiplication (see Definition 3.1).

Theorem 1.4. *Let q be a prime power, n a positive integer, G and $d = d(n)$ as in one of the lines of Table 1, and p a prime dividing $|G|$ and coprime to q. Algorithm 1 determines in $O(d^{\omega+o(1)}(\log q)^{2+o(1)})$ bit operations whether a given element of G is (p, m)-abundant for some m.*

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

In many situations, it might be difficult to obtain a prime divisor p of $|G|$, because finding such primes might involve factorising large integers. Thus we also consider the situation where the prime p is not known in advance and we wish to determine whether there exists a pair (p, m) such that a given element is (p, m)-abundant.

Theorem 1.5. *Let q be a prime power, n a positive integer, and G, $d = d(n)$ as in one of the lines of Table 1. Algorithm 2 takes as input an element $g \in G$ and determines the integer m, if such exists, and all integers e for which a given element of G is (p, m)-abundant for some primitive prime divisor p of $q^e - 1$. This algorithm costs $O(d^{\omega+o(1)}(\log q)^{2+o(1)})$ bit operations.*

Preliminary results needed for proving Theorems 1.4 and 1.5 are collected in Section 2. Algorithms 1 and 2 are then presented and analysed in Section 3.

2. Preliminaries

Assume throughout this section that G, δ, $d = d(n)$ are as in one of the lines of Table 1, for q a prime power and n a positive integer, with $V = V(d, q^\delta)$ denoting the natural G-module. For brevity, these assumptions are not repeated explicitly in the following definitions and lemmas.

Recall that the definition of p-abundance, for p a prime dividing $|G|$ and coprime to q, is given in terms of the eigenvalues of an element $g \in G$ in some extension field of $\mathbb{F}_{q^\delta}$. As mentioned after Definition 1.1, the concept of p-abundance can also be viewed as a condition on irreducible g-invariant subspaces of V. There is also a third equivalent characterisation of p-abundance, in terms of the characteristic polynomial of g, which we use here as a condition for recognising p-abundance computationally. The equivalence of these three different characterisations of p-abundance is proved in Lemmas 2.1 and 2.4 below for the irreducible and quasi-irreducible cases, respectively.

For a positive integer k, define the *p'-part* of k to be k/p^a, where p^a is the highest power of the prime p that divides k.

Lemma 2.1. *Let p be a prime dividing $|G|$ and coprime to q, m an integer with $d/2 < m \leq d$, and Δ the p'-part of $q^{\delta m} - 1$. Let $g \in G$ and let $c_g(x)$ denote the characteristic polynomial of g in its action on V. The following are equivalent:*

(i) *g is (p, m)-abundant irreducible.*
(ii) *$c_g(x)$ has an irreducible factor $h(x)$ of degree m such that $x^\Delta \not\equiv 1 \pmod{h(x)}$.*
(iii) *V has a unique m-dimensional g-invariant subspace U such that $g|_U$ is irreducible and has order divisible by p.*

Proof. First suppose that g is (p, m)-abundant irreducible, and let ζ be an eigenvalue of g in some extension field of $\mathbb{F}_{q^\delta}$, such that ζ has multiplicative order divisible by p and m Galois conjugates over $\mathbb{F}_{q^\delta}$, say $\zeta_1, \ldots, \zeta_m$ where $\zeta_1 = \zeta$ and $\zeta_{i+1} = \zeta_i^q$ for $i = 1, \ldots, m-1$. Then $h(x) := \prod_{i=1}^m (x - \zeta_i)$ is an irreducible factor of $c_g(x)$ with degree m. Moreover, ζ is a generator of the extension field $\mathbb{F}_{q^{\delta m}}$, which may be constructed as the quotient of the polynomial ring $\mathbb{F}_{q^\delta}[x]$ modulo the ideal $(h(x))$.

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

In this setting, ζ corresponds to multiplication by x modulo $h(x)$, and because the multiplicative order of ζ is divisible by p, $x^{\Delta} \not\equiv 1 \pmod{h(x)}$.

Now suppose that $c_g(x)$ has an irreducible factor $h(x)$ of degree m such that $x^{\Delta} \not\equiv 1 \pmod{h(x)}$. Since $m > d/2$, $c_g(x)$ is not divisible by $h(x)^2$. Let V_h be the h-primary component of V as a g-module. Then V_h is g-invariant and, since $h(x)^2$ does not divide $c_g(x)$, V_h has dimension m and g acts irreducibly on V_h. As a $g|_{V_h}$-module, V_h is isomorphic to the quotient $\mathbb{F}_{q^{\delta}}[x]/(h(x))$ with $g|_{V_h}$ acting as multiplication by x. Since $x^{\Delta} \not\equiv 1 \pmod{h(x)}$, it follows that $g|_{V_h}$ has order divisible by p.

Finally, suppose that U is an m-dimensional g-invariant subspace such that $g|_U$ is irreducible and has order divisible by p. Then the restriction $g|_U$ lies in a Singer cycle of $\mathrm{GL}(U)$ [8, Satz II.7.3, p. 187]. Moreover, U can be identified with the field $\mathbb{F}_{q^{\delta m}}$ in such a way that $g|_U$ acts as multiplication by some nonzero element $\zeta \in \mathbb{F}_{q^{\delta m}}$. This element ζ is an eigenvalue of g over the extension field $\mathbb{F}_{q^{\delta m}}$, and because $g|_U$ is irreducible, ζ has m Galois conjugates over $\mathbb{F}_{q^{\delta}}$. Moreover, since $g|_U$ has order divisible by p, so also does ζ. □

The analogous result for p-abundant quasi-irreducible elements involves what we call *abundant* polynomial pairs and *quasi-irreducible* actions on the natural G-module.

Definition 2.2. Assume here that $G \neq \mathrm{GL}_n(q)$, and define $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^{\delta}})$ by $\varphi : a \mapsto a^q$.

(i) Given a polynomial $f(x) = \prod_{i=1}^{d}(x - \zeta_i)$ with the ζ_i lying in some extension field of $\mathbb{F}_{q^{\delta}}$, write $f^*(x) = \prod_{i=1}^{d}(x - \zeta_i^{-\varphi})$ and call $f^*(x)$ the *φ-conjugate* of $f(x)$.

(ii) Given a degree d polynomial $f(x)$ over $\mathbb{F}_{q^{\delta}}$ and an even integer m with $d/2 < m \leq d$, two polynomials $f_1(x)$, $f_2(x)$ over $\mathbb{F}_{q^{\delta}}$ are said to form an *m-abundant polynomial pair* for $f(x)$ if $f_1(x)$, $f_2(x)$ are distinct monic irreducible divisors of $f(x)$, each of degree $m/2$, such that $f_2(x) = f_1^*(x)$.

(iii) Given $g \in G$ and an even-dimensional g-invariant subspace U of V, we say that g is *quasi-irreducible* on U if U is nondegenerate and $U = U_1 \oplus U_2$, where each U_i is a totally isotropic irreducible g-module, $\dim(U_1) = \dim(U_2)$, and there exist bases b_i for U_i such that if A is the matrix for $g|_{U_1}$ with respect to b_1 then the matrix for $g|_{U_2}$ with respect to b_2 is $(A^{\mathrm{tr}})^{-\varphi}$ and is not similar to A.

We remark that the actions considered in Definition 2.2(iii) correspond to those introduced by Huppert [9, Satz 2]. Part of the significance of φ-conjugate polynomials is explained by Lemma 2.3, the proof of which is straightforward and omitted here. Lemma 2.3 is used below in the proof of Lemma 2.4, which is the analogue of Lemma 2.1 for p-abundant quasi-irreducible elements. We note that parts of Lemmas 2.1 and 2.4 follow from another result of Huppert [10, Satz 1.7].

Lemma 2.3. *If $g \in G$ has characteristic polynomial $f(x)$ then the characteristic polynomial of $(g^{\mathrm{tr}})^{-\varphi}$ is $f^*(x)$.*

Lemma 2.4. *For $G \neq \mathrm{GL}_n(q)$, let p be a prime dividing $|G|$ and coprime to q, m an even integer with $d/2 < m \leq d$, and Δ the p'-part of $q^{\delta m} - 1$. Let $g \in G$ and let $c_g(x)$ denote the characteristic polynomial of g in its action on V. The following are equivalent:*

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

(i) *g is (p, m)-abundant quasi-irreducible.*

(ii) *$c_g(x)$ has irreducible factors $f_1(x)$, $f_2(x)$ that form an m-abundant polynomial pair, with $x^{\Delta} \not\equiv 1 \pmod{f_1(x)}$.*

(iii) *V has a unique nondegenerate m-dimensional g-invariant subspace U such that $g|_U$ is quasi-irreducible and has order divisible by p.*

Proof. First suppose that g is (p, m)-abundant quasi-irreducible, and let ζ be an eigenvalue of g in some extension field of $\mathbb{F}_{q^\delta}$, such that ζ has multiplicative order divisible by p, ζ is not Galois conjugate to ζ^{-1}, and ζ, ζ^{-1} have together m Galois conjugates over $\mathbb{F}_{q^\delta}$. Note that ζ^{-1} is also an eigenvalue of g, because $g, g^{-\mathrm{tr}}$ are conjugate by the matrix of the form preserved by G. Then ζ has $m/2$ Galois conjugates, say $\zeta_1, \ldots, \zeta_{m/2}$ where $\zeta_1 = \zeta$ and $\zeta_{i+1} = \zeta_i^q$ for $i = 1, \ldots, m-1$, and

$$f_1(x) := \prod_{i=1}^{m/2}(x - \zeta_i), \quad f_2(x) := \prod_{i=1}^{m/2}(x - \zeta_i^{-\varphi})$$

are distinct monic irreducible factors of $c_g(x)$ of degree $m/2$ satisfying $f_1^*(x) = f_2(x)$. Thus $f_1(x)$, $f_2(x)$ form an m-abundant polynomial pair for $c_g(x)$. Moreover, ζ is a generator of the extension field $\mathbb{F}_{q^{\delta m/2}}$ over $\mathbb{F}_{q^\delta}$, which may be constructed as a quotient of the polynomial ring $\mathbb{F}_{q^\delta}[x]$ modulo the ideal $(f_1(x))$. In this setting, ζ corresponds to multiplication by x modulo $f_1(x)$, and because the multiplicative order of ζ is divisible by p, $x^{\Delta} \not\equiv 1 \pmod{f_1(x)}$.

Now suppose that (ii) holds. Then the primary decomposition of V as a g-module has g-invariant summands U_1, U_2 such that $g|_{U_i}$ has characteristic polynomial $f_i(x)$ for $i = 1, 2$ [7, Lemma 8.10]. Since $f_1(x) \neq f_2(x)$, the induced actions $g|_{U_1}$, $g|_{U_2}$ are not similar, and because $f_1^*(x) = f_2(x)$, $g|_{U_1}$ is similar to $((g|_{U_2})^{\mathrm{tr}})^{-\varphi}$ by Lemma 2.3.

We claim that each U_i is totally isotropic. To prove this, let $u, v \in U_i$ and write

$$f_i(x) = \sum_{j=0}^{m/2} a_{ij}x^j \quad \text{where } a_{i(m/2)} = 1, a_{i0} \neq 0.$$

Note that

$$f_i^*(x) = a_{i0}^{-\varphi}x^{m/2}\sum_{j=0}^{m/2} a_{ij}^{\varphi}x^{-j}.$$

The given nondegenerate sesquilinear form on V satisfies $(au, v) = a(u, v) = (u, a^{\varphi}v)$ for all $a \in \mathbb{F}_{q^\delta}$. Since g preserves this form, we have in particular that $(u, vg^{-1}) = (ug, v)$. For a fixed u, consider any $v \in U_i$. By the definition of U_i, it follows that $uf_i(g) = 0$, and hence

$$\begin{aligned}0 = (uf_i(g), v) &= \sum_{j=0}^{m/2} a_{ij}(ug^j, v) = \sum_{j=0}^{m/2} a_{ij}(u, vg^{-j}) = \Big(u, v\sum_{j=0}^{m/2} a_{ij}^{\varphi}g^{-j}\Big)\\ &= (u, a_{i0}^{\varphi}vg^{-m/2}f_i^*(g)) = a_{i0}(u, vg^{-m/2}f_i^*(g)) = a_{i0}(ug^{m/2}, vf_i^*(g)).\end{aligned}$$

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

TABLE 2. Upper bounds on the values of e that give rise to p-abundant elements with p a ppd of $q^e - 1$.

G	Conditions on e
$\mathrm{GL}_n(q)$	$e \leq d$
$\mathrm{GU}_n(q)$	$e \leq d/2$ if e is odd, $e \leq d$ if $e \equiv 0 \pmod 4$, $e \leq 2d$ if $e \equiv 2 \pmod 4$
$\mathrm{Sp}_{2n}(q)$, $\mathrm{SO}_{2n+1}(q)$, $\mathrm{SO}^{\pm}_{2n}(q)$	$\begin{cases} e \text{ odd} : e \leq d/2, e \neq d/2 \text{ if } G = \mathrm{SO}^{-}_{2n}(q), \\ e \text{ even} : e \leq d, e \neq d \text{ if } G = \mathrm{SO}^{+}_{2n}(q) \end{cases}$

Since $a_{i0} \neq 0$ and $g^{m/2}$ is nonsingular and preserves U_i, this implies that $ug^{m/2} \in U_i \setminus \{0\}$ and, for all $v \in U_i$, $0 = (ug^{m/2}, vf^*(g))$. Then, because $f_i^*(x) = f_{3-i}(x) \neq f_i(x)$, the map $f_i^*(g)|_{U_i}$ is nonsingular and so $(ug^{m/2}, v) = 0$ for all $v \in U_i$, which implies that $ug^{m/2} \in U_i^{\perp}$. Since this holds for all $u \in U_i$, we conclude that $U_i = U_i g^{m/2} \subseteq U_i^{\perp}$. So U_i is totally isotropic, proving the claim.

Since $f_1(x) \neq f_2(x)$, we have $U_1 \cap U_2 = \{0\}$. Let $U = U_1 \oplus U_2$. The intersection $U_1 \cap U_2^{\perp}$ is g-invariant and, because g is irreducible on U_1, $U_1 \cap U_2^{\perp}$ is equal to either U_1 or $\{0\}$. If it were equal to U_1 then U would be totally isotropic and of dimension $m > d/2$, which is impossible. Hence $U_1 \cap U_2^{\perp} = \{0\}$, and similarly $U_2 \cap U_1^{\perp} = \{0\}$. It is then straightforward to verify that U is nondegenerate. Thus $g|_U$ is quasi-irreducible. Since $x^{\Delta} \not\equiv 1 \pmod{f_1(x)}$, it follows as in the second paragraph of the proof of Lemma 2.1 that $g|_U$ has order divisible by p. Uniqueness of U follows from Huppert's theorem [10, Satz 1.7] since $m > d/2$.

Finally, suppose that (iii) holds with respect to a subspace $U = U_1 \oplus U_2$ as in Definition 2.2(iii). For $i = 1, 2$, let $f_i(x)$ denote the characteristic polynomial of $g|_{U_i}$. Since $g|_{U_i}$ is irreducible, $f_i(x)$ is monic and irreducible of degree $m/2$. Let ζ be a root of $f_1(x)$ in the extension field $\mathbb{F}_{q^{\delta m/2}}$ of $\mathbb{F}_{q^{\delta}}$. Then ζ has $m/2$ Galois conjugates over $\mathbb{F}_{q^{\delta}}$. By Definition 2.2(iii), $g|_{U_2}$ is similar to $(g^{\mathrm{tr}})^{-\varphi}|_{U_1}$, and hence the characteristic polynomial $f_2(x)$ of $g|_{U_2}$ is the φ-conjugate of $f_1(x)$, by Lemma 2.3. In particular, ζ^{-1} is a root of $f_2(x)$, and ζ, ζ^{-1} are not Galois conjugate because $f_1(x) \neq f_2(x)$. The m eigenvalues of $g|_U$ are Galois conjugate to ζ or ζ^{-1}. Moreover, since $g|_U$ has order divisible by p, it follows as in the proof of Lemma 2.1 that ζ has order divisible by p. □

Recall that Table 1 gives necessary and sufficient conditions on the integer m for the group G to contain (p, m)-abundant elements. These conditions enter into Algorithm 1, for Theorem 1.4, where a prime p is specified in advance and we wish to test all possible values of m for which a given $g \in G$ could be (p, m)-abundant (with the test being to check the conditions in Lemmas 2.1 and 2.4). In our second scenario (Algorithm 2 for Theorem 1.5), p is not given and hence we also need to know the possible values of the order e of q modulo p that give rise to (p, m)-abundant elements.

LEMMA 2.5. *Let p be a prime not dividing q, and e the order of q modulo p. Then:*

(i) *p divides $|G|$ if and only if e satisfies the relevant condition in Table 2.*

(ii) *If p divides $|G|$ then G contains (p, m)-abundant elements if and only if either e divides m, or $G = \mathrm{GU}_n(q)$, m is odd, $e \equiv 2 \pmod 4$ and $e/2$ divides m.*

PROOF. Assertion (ii) follows from the conditions given in Table 1 upon noting the following facts [19, Lemma 4.5]:

(F1) p divides $q^\ell - 1$ if and only if e divides ℓ.

(F2) p divides $q^\ell + 1$ if and only if e divides 2ℓ and e does not divide ℓ.

For (i), the sufficiency of the conditions in Table 2 is clear in each case, so we assume that p divides $|G|$ to prove the converse. Since

$$|\mathrm{GL}_n(q)| = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - 1),$$

the entry in the first line of Table 2 is true, with $n = d$. Now consider

$$|G| = |\mathrm{GU}_n(q)| = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - (-1)^i).$$

If p divides $|G|$ then p divides $q^i - (-1)^i$ for some positive integer $i \le n = d$. Let ℓ be the least such positive integer. First suppose that ℓ is odd. Then by (F2), e divides 2ℓ but not ℓ. In particular, $e \equiv 2 \pmod 4$, p divides $q^{e/2} + 1$, and so by minimality $e/2 = \ell \le d$. Now suppose that ℓ is even. Then e divides ℓ, by (F1). If e is odd then $2e$ divides the even integer ℓ, and by minimality $2e = \ell \le d$. If e is even then by minimality $e = \ell \le d$. If $e \equiv 2 \pmod 4$ then we would also find $q^{\ell/2} + 1$ divisible by p, contradicting the minimality of ℓ. So $e \equiv 0 \pmod 4$ in this case.

Now consider

$$|G| = |\mathrm{Sp}_{2n}(q)| = q^{n^2}\prod_{i=1}^{n}(q^{2i} - 1),$$

and let ℓ be minimal such that p divides $q^{2\ell} - 1$. Then e divides 2ℓ. If e is even then by minimality $e = 2\ell \le 2n = d$, and if e is odd then minimality implies that $e = \ell \le n = d/2$. The same holds for $\mathrm{SO}_{2n+1}(q)$. For $G = \mathrm{SO}^{\varepsilon}_{2n}(q)$, where $\varepsilon = \pm$, the same conclusions follow unless the integer 2ℓ is $2n = d$, in which case we have the following additional restrictions: if e is even then $e = 2n$ and we need $\varepsilon = -$ for p (which divides $q^n + 1$) to divide $|G|$; if e is odd then $e = \ell = n$ and we need $\varepsilon = +$ for p (which divides $q^n - 1$) to divide $|G|$. □

The corresponding test for p-abundance in Algorithm 2 is based on Lemma 2.7 below. First we introduce some notation for later reference.

DEFINITION 2.6. Suppose that $q^e - 1$ has a primitive divisor, and let m be a positive integer. We denote by Ψ the product, counting multiplicities, of all primes dividing $q^{\delta m} - 1$ that are not primitive prime divisors of $q^e - 1$. (Here $\delta \in \{1, 2\}$, as before.)

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

Lemma 2.7. *Let m be an integer with $d/2 < m \leq d$. Let e be a positive integer such that either e divides m, or $G = \mathrm{GU}_n(q)$, m is odd, $e \equiv 2 \pmod 4$ and $e/2$ divides m. Suppose also that e satisfies the relevant condition in Table 2. Let $g \in G$ and let $c_g(x)$ denote the characteristic polynomial of g in its action on V. Then there is a prime p (dividing $|G|$ and coprime to q) such that q has order e modulo p and g is (p, m)-abundant if and only if one of the following conditions holds, with Ψ as in Definition 2.6:*

(i) *$c_g(x)$ has an irreducible factor $f(x)$ of degree m such that $x^{\Psi} \not\equiv 1 \pmod{f(x)}$.*

(ii) *$G \neq \mathrm{GL}_n(q)$, m is even, and $c_g(x)$ has irreducible factors $f_1(x)$, $f_2(x)$ that form an m-abundant polynomial pair, with $x^{\Psi} \not\equiv 1 \pmod{f_1(x)}$.*

Proof. Suppose that (i) or (ii) holds, write $h(x) = f(x)$ or $h(x) = f_1(x)$, respectively, and let p be a prime dividing the order of x^{Ψ} modulo $h(x)$. Then q has order e modulo p. Also, if Δ denotes the p'-part of $q^{\delta m} - 1$ then Δ is a multiple of Ψ and Δ/Ψ is not divisible by p, and hence $x^{\Delta} = (x^{\Psi})^{\Delta/\Psi}$ is not congruent to 1 modulo $h(x)$. Thus g is (p, m)-abundant by Lemmas 2.1 and 2.4. Conversely, if g is (p, m)-abundant for some prime p such that q has order e modulo p, then Lemmas 2.1 and 2.4 imply that either (i) or (ii) holds with Ψ replaced by Δ. However, because Δ is a multiple of Ψ, the required condition on x follows immediately. □

3. Algorithms

Assume again that G, δ, $d = d(n)$ are as in one of the lines of Table 1 for q a prime power and n a positive integer. We now present algorithms to test whether elements in G, given as $d \times d$ matrices, are p-abundant. As explained earlier, we consider two scenarios. In the first, we assume that we are given a prime p coprime to q and an element $g \in G$, and we wish to test whether g is (p, m)-abundant for some positive integer m (with $d/2 < m \leq d$). Algorithm 1, IsPrimeAbundant(G, p, g), presented in Section 3.1, returns either a positive integer m such that g is (p, m)-abundant, together with the type of g (irreducible or quasi-irreducible), or False if no such m exists. In the second scenario, we wish to determine all integer pairs (e, m) such that a given element $g \in G$ is (p, m)-abundant for some prime p for which e is the order of q modulo p. Algorithm 2, IsAbundant(G, g), described in Section 3.2, returns a list of all such pairs (e, m) together with the type of g, or False if no such pairs exist.

Our new algorithms exploit polynomial arithmetic in a similar manner to the first and third authors' procedure IsPpdElement [17, Section 4.2] for deciding whether an element in G has order divisible by a primitive prime divisor of $q^e - 1$ for some $e > d/2$ without determining such a prime. The third author's refinement of IsPpdElement [21, p. 620] tests whether a given $g \in G$ is a ppd$(d, q; e)$ element by computing the characteristic polynomial of g, testing for an irreducible factor of degree $e > d/2$, and then using polynomial arithmetic to test whether the order of g is divisible by a primitive prime divisor of $q^e - 1$. This procedure costs $O(d^{\omega+o(1)}(\log q)^{2+o(1)})$ bit operations, where ω is the exponent of matrix multiplication, defined as follows.

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

```
Algorithm 1: IsPrimeAbundant($G$, $g$, $p$)
  Input: A matrix $g \in G$ and a prime $p$ not dividing $q$, where $G, \delta, d = d(n)$ are as
         in one of the lines of Table 1 for a prime power $q$ and positive integer $n$;
  Output: An integer $m$ such that $g$ is $(p, m)$-abundant and the Type of $g$, either
          Irreducible or Quasi-Irreducible, or False if no such $m$ exists;

  Find $c_g(x)$, the characteristic polynomial of $g$;
  if $c_g(x)$ has an irreducible factor of degree $m > d/2$, $m \neq d$ if $G = \mathrm{SO}^{+}_{2n}(q)$ then
      Let $h(x)$ denote this factor and set Type = Irreducible;
      if $p$ does not divide $q^m - 1$ (for $G = \mathrm{GL}_n(q)$) or $q^m + 1$ (for $G = \mathrm{GU}_n(q)$ and $m$
      odd) or $q^{m/2} + 1$ (for $G = \mathrm{Sp}_{2n}(q)$, $\mathrm{SO}_{2n+1}(q)$ or $\mathrm{SO}^{\pm}_{2n}(1)$ and $m$ even) then
          return False;
      end
  else if $G \neq \mathrm{GL}_n(q)$ and $c_g(x)$ has an $m$-abundant polynomial pair $f_1(x)$, $f_2(x)$ for
  some even $m$ with $m > d/2$, $m \neq d$ if $G = \mathrm{SO}^{-}_{2n}(q)$ then
      Let $h(x)$ denote $f_1(x)$ and set Type = Quasi-Irreducible;
      if $p$ does not divide $q^m - 1$ (for $G = \mathrm{GU}_n(q)$) or $q^{m/2} - 1$ (otherwise) then
          return False;
      end
  else
      return False;
  end
  % at this point $h(x)$ has been defined;
  Compute $\Delta$, the $p'$-part of $q^{\delta m} - 1$;
  if $x^{\Delta} \not\equiv 1 \pmod{h(x)}$ then
      return $m$ and Type;
  else
      return False;
  end
```

Definition 3.1. The exponent of matrix multiplication, ω, is the infimum of the set of real numbers x such that there exists an algorithm for multiplying two $d \times d$ matrices in $O(d^x)$ field operations. (Note that ω is known to be at most 2.376 [2].)

The correctness and cost analyses for our new algorithms are similar to the aforementioned analyses for IsPpdElement. We prove that both algorithms also cost $O(d^{\omega+o(1)}(\log q)^{2+o(1)})$ bit operations. The algorithms have been implemented in the computer algebra system GAP, and their practical performance matches that of IsPpdElement. The latter is available in both the 'recog' package in GAP [4], and in MAGMA [1].

3.1. Proof of Theorem 1.4. Our first algorithm, IsPrimeAbundant, takes as input an element $g \in G$ and a prime p coprime to q, and tests whether g is (p, m)-abundant

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

for some m. Recall from Remark 1.2 that there is at most one value of m to test. Correctness follows from Table 1 and Lemmas 2.1 and 2.4.

For the cost analysis, first note that Δ can be found by repeatedly dividing $q^{\delta m} - 1$ by p. Since $m \leq d$, at most $\log_p(q^{\delta d} - 1) = O(d \log q)$ repetitions are required. Multiplying (or dividing) two ℓ-bit integers costs $O(\ell \log \ell \log \log \ell)$ bit operations [22], which is $O(\ell^{1+o(1)})$ bit operations. So each repetition costs $O(d^{1+o(1)}(\log q)^{1+o(1)})$ bit operations, and hence Δ can be computed in $O(d^{2+o(1)}(\log q)^{2+o(1)})$ bit operations.

The cost of computing the characteristic polynomial $c_g(x)$ of g deterministically is $O(d^{\omega+o(1)})$ field operations [12]. Next we test whether $c_g(x)$ is divisible by either an irreducible polynomial of degree m or an m-abundant polynomial pair, with $m > d/2$ in either case. This can be done deterministically at a cost of $O(d^{\omega+o(1)} + d^{1+o(1)} \log q)$ field operations [21, p. 620]. We then determine whether $x^{\Delta} \not\equiv 1 \pmod{h(x)}$ in the polynomial ring modulo $h(x)$. This involves $O(d \log q)$ multiplications modulo $h(x)$ of polynomials of degree at most d, and hence costs $O(d^2 \log d \log \log d \log q)$ field operations [21, p. 620].

Therefore, the algorithm IsPrimeAbundant costs $O(d^{\omega+o(1)} \log q)$ field operations and $O(d^{2+o(1)}(\log q)^{2+o(1)})$ bit operations. Estimating the cost of a field operation as $O((\log q)^{1+o(1)})$ bit operations, the total cost is $O(d^{\omega+o(1)}(\log q)^{2+o(1)})$ bit operations.

3.2. Proof of Theorem 1.5. Our second algorithm, IsAbundant, takes as input an element $g \in G$ and identifies all pairs (e, m) such that g is (p, m)-abundant for some prime p for which q has order e modulo p. If no such pairs exist, it returns False. Recall Definition 2.6 for the quantity Ψ, namely the product, counting multiplicities, of all primes dividing $q^{\delta m} - 1$ that are not primitive prime divisors of $q^e - 1$.

The value of m can be determined by the degrees of certain irreducible factors of the characteristic polynomial of g, as in Lemma 2.7. For a given m, the possibilities for e must satisfy the conditions of Table 2 and Lemma 2.5(ii), the latter stating that e should divide m or, if $G = \mathrm{GU}_n(q)$ and m is odd, that $e \equiv 2 \pmod 4$ and $e/2$ should divide m. The correctness of IsAbundant then follows from Lemma 2.7. Note that more than one pair (e, m) may be 'reported', though each pair will have the same value of m (by Remark 1.2). For example, $\mathrm{GL}_n(2)$ with $6 \leq n \leq 11$ contains elements of order 21 that are both $(3, 6)$-abundant (with $e = 2$) and $(7, 6)$-abundant (with $e = 3$).

We now determine the cost of IsAbundant. For a prime p and a positive integer k, let $(k)_p$ denote the highest power of p dividing k. Let Φ denote the product of all primitive prime divisors, counting multiplicities, of $q^e - 1$. Neumann and Praeger [15, pp. 578–579] describe a procedure to compute Φ for $3 \leq e \leq \delta d$, and Praeger's analysis of this procedure [21, p. 620] shows that it costs $O(d^{1+o(1)}(\log q)^2)$ bit operations. For $e = 2$ we have $\Phi = (q + 1)/(q + 1)_2$. For $e = 1$, we instead define Φ by setting $\Phi = q - 1$ if δm is odd and $\Phi = (q + 1)_2(q - 1)/2$ if δm is even. Computing Φ for $e = 1, 2$ requires $O(\log(q)^2)$ bit operations, which is again $O(d^{1+o(1)}(\log q)^2)$ bit operations (as for $e \geq 3$).

Observe that in all cases, the primes dividing Φ are precisely the primitive prime divisors of $q^e - 1$. Thus the quantity Ψ can be computed by initialising $\Psi := q^{\delta m} - 1$ and then repeatedly redefining Ψ as $\Psi/\gcd(\Psi, \Phi)$ until $\gcd(\Psi, \Phi) = 1$. Now, given a primitive prime divisor p of $q^e - 1$, we have $(q^{\delta m} - 1)_p = p^{t+j}$, where $p^t = (\Phi)_p$

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

Algorithm 2: IsAbundant(G, g)

```
Input: A matrix $g \in G$, where $G$, $\delta$, $d = d(n)$ are as in one of the lines of Table 1
       for a prime power $q$ and positive integer $n$;
Output: A list of pairs $(e, m)$ such that $g$ is $(p, m)$-abundant for some prime $p$
        with $e$ the order of $q$ modulo $p$, and the Type of $g$, either Irreducible or
        Quasi-Irreducible, or False if no such pairs exist;

Find $c_g(x)$, the characteristic polynomial of $g$;
if $c_g(x)$ has an irreducible factor of degree $m > d/2$, $m \neq d$ if $G = \mathrm{SO}^+_{2n}(q)$ then
    Let $h(x)$ denote this factor and set Type = Irreducible;
else if $G \neq \mathrm{GL}_d(q)$ and $c_g(x)$ has an $m$-abundant polynomial pair $f_1(x)$, $f_2(x)$ for
some even $m$ with $m > d/2$, $m \neq d$ if $G = \mathrm{SO}^-_{2n}(q)$ then
    Let $h(x)$ denote $f_1(x)$ and set Type = Quasi-Irreducible;
else
    return False;
end
for all $e$ that satisfy the bounds in Table 2 and are either divisors of $m$ or, if
$G = \mathrm{GU}_n(q)$ and $m$ is odd, satisfy $e \equiv 2 \pmod 4$ with $e/2$ dividing $m$ do
    % at this point $h(x)$ has been defined;
    Compute $\Psi$ (see Definition 2.6);
    if $x^\Psi \not\equiv 1 \pmod{h(x)}$ then
        Report $(e, m)$;
    end
end
if at least one pair $(e, m)$ was found then
    return all reported pairs $(e, m)$ and Type;
else
    return False;
end
```

and $p^j = (\delta m/e)_p$. This is proved for $p \neq 2$ in our other paper [16], and for $p = 2$ by Guest and Praeger [5]. Since the first step already divides Ψ by p^t, it follows that at most $1 + j \leq 1 + \log_p(\delta m/e) = O(\log d)$ repetitions are required. The greatest common divisor of two ℓ-bit integers can be computed in $O(\ell(\log \ell)^2 \log\log \ell)$ bit operations [14]. This is $O(\ell^{1+o(1)})$ bit operations, the same as the cost of ℓ-bit integer division quoted in Section 3.1. So once Φ is known, Ψ is computed in $O(d^{1+o(1)} \log d(\log q)^{1+o(1)})$, namely $O(d^{1+o(1)}(\log q)^{1+o(1)})$, further bit operations. Recalling that Φ can be computed in $O(d^{1+o(1)}(\log q)^2)$ bit operations, we see that the total cost of computing Ψ is also $O(d^{1+o(1)}(\log q)^2)$ bit operations.

As in Section 3.1, the total cost of finding the characteristic polynomial of g, determining the existence (or not) of an appropriate factor $h(x)$ and computing x^Ψ modulo $h(x)$ is $O(d^{\omega+o(1)} \log q)$ field operations.

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

Now, the number $\operatorname{div}(k)$ of divisors of an integer k satisfies $\operatorname{div}(k) = k^{o(1)}$ [20, pp. 395–396]. Hence the loop over all divisors e of m (and also, if $G = \mathrm{GU}_n(q)$ and m is odd, those $e \equiv 2 \pmod 4$ such that $e/2$ divides m) is executed $O(d^{o(1)})$ times (because $m \le d$). So the overall cost of IsAbundant is $O(d^{1+o(1)}(\log q)^2)$ bit operations plus $O(d^{\omega+o(1)} \log q)$ field operations. Estimating (as in Section 3.1) the cost of a field operation as $O((\log q)^{1+o(1)})$ bit operations, we conclude that IsAbundant costs $O(d^{\omega+o(1)}(\log q)^{2+o(1)})$ bit operations.

References

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

[2] D. Coppersmith and S. Winograd, 'Matrix multiplication via arithmetic progressions', *J. Symbolic Comput.* **9** (1990), 251–280.

[3] A. Gambini Weigel and T. S. Weigel, 'On the orders of primitive linear p'-groups', *Bull. Aust. Math. Soc.* **48** (1993), 495–521.

[4] 'GAP—groups, algorithms, programming—a system for computational discrete algebra', http://www.gap-system.org/.

[5] S. Guest and C. E. Praeger, 'Proportions of elements with given 2-part order in finite classical groups of odd characteristic', Preprint, 2011, http://arxiv.org/abs/1007.2983v4.

[6] R. M. Guralnick and F. Lübeck, 'On p-singular elements in Chevalley groups in characteristic p', in: *Groups and Computation III*, Ohio State University Mathematical Research Institute Publications, 8 (de Gruyter, Berlin, 2001), pp. 169–182.

[7] B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra* (Chapman and Hall, London, 1970).

[8] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, 134 (Springer, Berlin, 1967).

[9] B. Huppert, 'Singer-Zyklen in klassischen Gruppen', *Math. Z.* **117** (1970), 141–150.

[10] B. Huppert, 'Isometrien von Vektorräumen 1', *Arch. Math.* **35** (1980), 164–176.

[11] I. M. Isaacs, W. M. Kantor and N. Spaltenstein, 'On the probability that a group element is p-singular', *J. Algebra* **176** (1995), 139–181.

[12] W. Keller-Gehrig, 'Fast algorithms for the characteristics polynomial', *Theoret. Comput. Sci.* **36** (1985), 309–317.

[13] F. Lübeck, 'Finding p'-elements in finite groups of Lie type', in: *Groups and Computation III*, Ohio State University Mathematical Research Institute Publications, 8 (de Gruyter, Berlin, 2001), pp. 249–256.

[14] N. Möller, 'On Schönhage's algorithm and subquadratic integer gcd computation', *Math. Comp.* **77** (2008), 589–607.

[15] P. M. Neumann and C. E. Praeger, 'A recognition algorithm for special linear groups', *Proc. Lond. Math. Soc.* (3) **65** (1992), 555–603.

[16] A. C. Niemeyer, T. Popiel and C. E. Praeger, 'Abundant p-singular elements in finite classical groups', Preprint, 2012, http://arxiv.org/abs/1205.1454.

[17] A. C. Niemeyer and C. E. Praeger, 'Implementing a recognition algorithm for classical groups', in: *Groups and Computation, II*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 28 (American Mathematical Society, Providence, RI, 1997), pp. 273–296.

[18] A. C. Niemeyer and C. E. Praeger, 'A recognition algorithm for classical groups over finite fields', *Proc. Lond. Math. Soc.* (3) **77** (1998), 117–169.

[19] A. C. Niemeyer and C. E. Praeger, 'Estimating proportions of elements in finite groups of Lie type', *J. Algebra* **324** (2010), 122–145.

[20] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edn (John Wiley & Sons, New York, NY, 1991).

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press

[21] C. E. Praeger, 'Primitive prime divisor elements in finite classical groups', in: *Groups St. Andrews 1997 in Bath, II*, London Mathematical Society Lecture Note Series, 261 (Cambridge University Press, Cambridge, 1999), pp. 605–623.

[22] A. Schönhage and V. Strassen, 'Schnelle Multiplikation großer Zahlen', *Computing* **7** (1971), 281–292.

ALICE C. NIEMEYER, The University of Western Australia, 35 Stirling Highway,
Crawley, WA 6009, Australia
e-mail: alice.niemeyer@uwa.edu.au

TOMASZ POPIEL, The University of Western Australia, 35 Stirling Highway,
Crawley, WA 6009, Australia
e-mail: tomasz.popiel@uwa.edu.au

CHERYL E. PRAEGER, The University of Western Australia, 35 Stirling Highway,
Crawley, WA 6009, Australia
and
King Abdulaziz University, Jeddah, Saudi Arabia
e-mail: cheryl.praeger@uwa.edu.au

https://doi.org/10.1017/S0004972712000317 Published online by Cambridge University Press