London Mathematical Society ISSN 1461–1570

ON THE NUMBER OF p-REGULAR ELEMENTS IN FINITE SIMPLE GROUPS

LÁSZLÓ BABAI, PÉTER P. PÁLFY AND JAN SAXL

Abstract

A p-regular element in a finite group is an element of order not divisible by the prime number p. We show that for every prime p and every finite simple group S, a fair proportion of elements of S is p-regular. In particular, we show that the proportion of p-regular elements in a finite classical simple group (not necessarily of characteristic p) is greater than $1/(2n)$, where $n-1$ is the dimension of the projective space on which S acts naturally. Furthermore, in an exceptional group of Lie type this proportion is greater than $1/15$. For the alternating group A_n, this proportion is at least $26/(27\sqrt{n})$, and for sporadic simple groups, at least $2/29$.

We also show that for an arbitrary field F, if the simple group S is a quotient of a finite subgroup of $GL_n(F)$ then for any prime p, the proportion of p-regular elements in S is at least $\min\{1/31, 1/(2n)\}$.

Along the way we obtain estimates for the proportion of elements of certain primitive prime divisor orders in exceptional groups, complementing work by Niemeyer and Praeger (1998). Our result shows that in finite simple groups, p-regular elements can be found efficiently by random sampling. This is a key ingredient to recent polynomial-time Monte Carlo algorithms for matrix groups.

Finally we complement our lower bound results with the following upper bound: for all $n \geqslant 2$ there exist infinitely many prime powers q such that the proportion of elements of odd order in $PSL(n,q)$ is less than $3/\sqrt{n}$.

1. *Introduction*

1.1. *Main results*

Let S be a finite simple group and p a prime number. Our objective is to show that a fair proportion of the elements of S is p-regular (i. e., its order is not divisible by p).

L. Babai's research was partially supported by NSF Grants CCR-9732205 and CCF-0830370. Work done in part at Rényi Institute and at Eötvös University, Budapest.
P. P. Pálfy's research was supported by the Hungarian Scientific Research Fund (OTKA) grants no. T38059 and NK72523.
Received 30 August, 2007, revised 17 December, 2008.
2000 Mathematics Subject Classification 20D06, 20F69, 20H30, 20P05, 68Q25
© ????, László Babai, Péter P. Pálfy and Jan Saxl

THEOREM 1.1. *For a prime p and a group G let $G(p')$ denote the set of p-regular elements of G. Let S be a finite simple group and p any prime number. Then*

(a) $|S(p')|/|S| \geqslant 26/(27\sqrt{n})$ *if $S = A_n$ is the alternating group of degree n;*

(b) $|S(p')|/|S| > 1/(2n)$ *if S is a classical simple group naturally acting on a projective space of dimension $n-1$;*

(c) $|S(p')|/|S| > 1/15$ *if S is an exceptional group of Lie type;*

(d) $|S(p')|/|S| > 2/29$ *when S is sporadic.*

REMARK 1.2. For some classes of classical simple groups, the value of n is not uniquely defined, e. g., $\Omega_{2k+1}(2^e) \cong Sp_{2k}(2^e)$. In such cases, we can use either definition in item (b), so for example for $S = \Omega_{2k+1}(2^e)$ we obtain the stronger lower bound $S(p')/|S| > 1/(4k)$.

The following compact corollary is particularly convenient for applications to the polynomial-time analysis of algorithms.

COROLLARY 1.3. *There exists a constant $c > 0$ such that for all finite simple groups S and for every prime p, the proportion of p-regular elements in S is $\geqslant c/\sqrt{\log |S|}$.*

This result allows p-regular elements to be discovered in S efficiently by random sampling, a key ingredient to several recent algorithms for matrix groups [**BB, BS**]. We emphasize that p may or may not be equal to the characteristic of the field of definition of S when S is of Lie type. We note that if p is the characteristic of the field of definition then almost all elements of S are p-regular; in fact the proportion of p-singular elements (i. e., of those of order divisible by p) is $O(1/q)$ where q is the order of the field of definition. More precisely, their proportion is less than $3/(q-1) + 2/(q-1)^2$ (Guralnick and Lübeck [**GL**]; see also Neumann and Praeger [**NeP**] and Fulman, Neumann, and Praeger [**FNP**] for certain classical groups).

In some applications, all we know about our simple group is that it is a section of a linear group. We can then give a lower bound on the proportion of p-regular elements in terms of the dimension of the linear group. In the following theorem, F is an arbitrary field.

THEOREM 1.4. *Let F be a field and S a finite simple group which is a quotient of a finite subgroup of $GL_n(F)$. Let $\gamma(n) = \max\{31, 2n\}$. Then for any prime r, at least a $1/\gamma(n)$ fraction of the elements of S is r-regular.*

Theorem 1.4 is a corollary to Theorem 1.20; both results will be derived in Section 1.4 from our main technical result, Theorem 1.6 (below).

This paper has been a long time in coming; versions of its main results have been quoted and applied in several papers, starting with [**BB**] in 1999. Theorem 1.1 has been quoted as "Theorem 4.9" in the paper [**BS**] in the following form.

THEOREM 1.5. *Let S be a finite simple group and p a prime number. Then at least a c/d fraction of the elements of S is p-regular, where $c > 0$ is an absolute constant and $d = d(S)$ is defined as follows. For the alternating group A_t we set $d(A_t) = \sqrt{t}$, for a classical simple group S we define $d(S)$ to be the dimension of the projective space on which S acts; for all other simple groups S, $d(S) = 1$.*

Theorem 1.5 follows from Theorem 1.1 with $c = 1/15$.

An earlier version of the result was mentioned in [**BB**, Theorem 4.2], where the estimate for the alternating groups was weaker, using $d(A_t) = t$ instead of $\sqrt{t}$.

The heart of the proof of Theorem 1.1 is the following result about simple groups of Lie type. For a group G and $T \subseteq G$ we use the notation $T^G = \bigcup_{g\in G} T^g$.

THEOREM 1.6. *Let S be a finite simple group of Lie type. Then S has two maximal tori T_1, T_2 of relatively prime orders such that for each i the set T_i^S has non-negligible density: $|T_i^S|/|S| \geqslant 1/(2n)$ if S is a classical simple group naturally acting on a projective space of dimension $n-1$, and $|T_i^S|/|S| \geqslant 1/31$ if S is an exceptional group of Lie type other than the Tits group ${}^2F_4(2)'$. The tori T_i can be chosen to be cyclic except for the case of the Tits group and the orthogonal groups $S = P\Omega_n^+(q)$ with $4 \mid n$.*

The bulk of this paper is devoted to proving this result.

Theorem 1.6 immediately implies part (b) of Theorem 1.1, in view of Proposition 1.12 (below). It also implies a weaker version of part (c) (with a lower bound of 1/31 instead of the claimed 1/15). The improvement is based on finding *sharp* (strongly self-centralizing, cf. Definition 1.13) tori in most classes of exceptional simple groups of Lie type (Theorem 3.1) and using the strategy of Proposition 1.15.

REMARK 1.7. This approach does apply to the Tits group as well, using the maximal tori of types 13 and 5^2, and yields the lower bound of 1/50. We achieve the better constant 1/15 in Theorem 1.1 (c) by treating the Tits group as sporadic (Section 5).

Theorem 1.6 will be proved for classical groups in Section 4 (Theorem 4.1) and for exceptional groups in Section 3 (Theorem 3.4).

REMARK 1.8. Theorem 1.6 was quoted somewhat inaccurately as Theorem 8.7 in [**BB**]. Specifically, the exceptions ${}^2F_4(2)'$ and $P\Omega_n^+(q)$ were omitted in [**BB**]. We emphasize that these inaccuracies do not affect the validity of any of the applications given in [**BB**]; the cyclicity of the tori is never used in [**BB**] and the Tits group can be treated as sporadic.

REMARK 1.9. The significance of Theorem 1.6 goes beyond proving Theorems 1.1 and 1.5. The principal motivation behind our results has been the analysis of algorithms for matrix groups and quotients of matrix groups by efficiently recognizable normal subgroups. The abundance of p-regular elements in simple groups was identified in [**BB**] as central to the analysis of certain algorithms such as factoring a semisimple group into its simple factors; the scope of applications was further broadened in [**BS**] to include testing membership in a simple normal subgroup and, in the case when $G/Z(G)$ is simple, finding $Z(G)$.

These applications work only under the assumption that a superset of prime divisors of the order of G is given. This could be achieved if we knew the prime factorization of $|SL_n(p)|$, but this is not known, and not expected, to be doable in time polynomial in $n^2 \log(p)$ (the bit-length of an $n \times n$ matrix over $\mathrm{GF}(p)$).

This difficulty is avoided by demonstrating the abundance not only of elements of order relatively prime to prime numbers but also relatively prime to certain composite numbers (cyclotomic and semicyclotomic factors of the numbers $p^j - 1$), a consequence of the presence of two maximal tori of relatively prime orders. The details are described in Section 1.4.

An anonymous referee asked how tight our lower bounds were. We discuss this question in Section 6. Here we mention the main upper bound result (see in a more detailed form as Theorem 6.1):

THEOREM 1.10. *For all $n \geqslant 2$ there exist infinitely many prime powers q such that the proportion of elements of odd order in $PSL(n,q)$ is less than $3/\sqrt{n}$.*

Acknowledgment. The authors wish to thank the organizers of the "Groups St Andrews 1997 in Bath" conference where the groundwork for this paper was done. We are grateful to the anonymous referee for the question about upper bounds; Sections 6 and 8 arose in response to that question. We wish to thank Ross Lawther for the data about sporadic groups, reproduced in Remark 5.3.

1.2. *Groups of Lie type: general strategy*

For the classical simple groups our proof will follow the following general pattern.

Let G be a finite group. For a self-centralizing subgroup $T \leqslant G$, we define $\Gamma(T) = \{x \in T : \mathbf{C}_G(x) = T\}$. We shall call $\mathbf{N}_G(T)/\mathbf{C}_G(T) = \mathbf{N}_G(T)/T$ the *automizer* of T.

PROPOSITION 1.11. *Let T be a self-centralizing subgroup of the finite group G. Then*

$$\frac{|T^G|}{|G|} > \frac{v}{u},$$

where $u = |\mathbf{N}_G(T)/T|$ and $v = |\Gamma(T)|/|T|$.

Proof. The sets $\Gamma(T^g)$ $(g \in G)$ are pairwise disjoint and their number is $|G : \mathbf{N}_G(T)|$. Therefore

$$|T^G| > |G : \mathbf{N}_G(T)| \cdot |\Gamma(T)| = |G| \cdot \frac{|T|}{|\mathbf{N}_G(T)|} \cdot \frac{|\Gamma(T)|}{|T|}.$$

The right hand side is then $|G|v/u$. □

PROPOSITION 1.12. *Assume T_1, T_2 are subgroups of relatively prime orders in the finite group G. Then, for any prime p, the proportion of p-regular elements in G is at least*

$$\min\left(\frac{|T_1^G|}{|G|}, \frac{|T_2^G|}{|G|}\right). \tag{1}$$

Proof. The coprimality of $|T_1|$ and $|T_2|$ ensures that at least one of T_1^G, T_2^G consists of p-regular elements only. □

For the classical simple groups, the T_i will be maximal tori. We shall choose T_i such that $v_i \geqslant 1/2$ and $u_i \leqslant n$, where $n-1$ is the dimension of the projective space on which the simple group acts in its natural representation. Note that our lower bounds do not depend on the order q of the underlying finite field. Our construction will be elementary and self-contained, using the geometry of classical groups. We include all cases for the sake of completeness, although the estimate in many, but not all, cases can be derived from results of Niemeyer and Praeger [**NP1**] (see Section 1.5).

For the exceptional simple groups of Lie type, pairs of maximal tori of coprime orders also exist, see Theorem 3.4. However, for these groups a different approach, which relies on the existence of *sharp tori*, yields better estimates.

DEFINITION 1.13. We call a nontrivial proper subgroup T of the group G *sharp* (or *strongly self-centralizing*) if $\mathbf{C}_G(t) = T$ for all $t \in T^\times = T \setminus \{1\}$.

In Theorem 3.1 we show that, with the exception of $E_7(q)$, all exceptional simple groups of Lie type contain sharp tori.

We make the following simple observation about sharp subgroups.

PROPOSITION 1.14. *Let T be a sharp subgroup of the finite group G. Then*

(a) T is a Hall subgroup;

(b) each element of G outside T^G has order relatively prime to $|T|$;

(c) $|\mathbf{N}_G(T)|$ divides $|T|(|T|-1)$;

(d) if G is simple then $\mathbf{N}_G(T) \neq T$.

Proof. Let p be a prime divisor of $|T|$ and P a Sylow p-subgroup of G which intersects T nontrivially. We claim that $P \leqslant T$; this in turn implies that T is a Hall subgroup, proving part (a).

Indeed, let $x \in T \cap P$ have order p and let $z \neq 1$ be a central element of P. Then the centralizer condition implies that $z \in T$; and then again the centralizer condition implies that $P \leqslant T$.

It also follows that every p-element of S lies in a conjugate of T, so every p-singular element is centralized by a nonidentity element in a conjugate of T. The centralizer condition now implies that every p-singular element belongs to a conjugate of T, proving part (b).

To estimate the order of $N = N_G(T)$, let us consider the action of N/T on $T^\times = T \setminus \{1\}$ by conjugation. The sharpness of T is equivalent to saying that this action is semiregular (the stabilizer of every point is the identity) and therefore $|N/T|$ divides $|T^\times|$, proving part (c).

Part (d) is immediate from Burnside's Normal Complement Theorem. □

Sharp subgroups allow the following estimation.

PROPOSITION 1.15. *Let G be a finite group containing a sharp subgroup T such that $\mathbf{N}_G(T) \neq T$, and let p be a prime number. Then the proportion of p-regular elements in G is at least $1/(|\mathbf{N}_G(T)/T|+1)$. Moreover, if G contains pairwise non-conjugate sharp subgroups $T_1, \ldots, T_k$, then the proportion of p-regular elements in G is at least*

$$\min\left(\sum_{i=1}^{k} \frac{1}{|\mathbf{N}_G(T_i)/T_i|+1}, \frac{1}{2}\right).$$

Proof. If p does not divide $|T|$ then every element in T^G is p-regular. Hence the proportion of p-regular elements in G is at least

$$\geqslant \frac{|T^G|}{|G|} > \frac{|\Gamma(T)|}{|T|} \cdot \frac{1}{|\mathbf{N}_G(T)/T|} = \frac{1-1/|T|}{|\mathbf{N}_G(T)/T|} \geqslant \frac{1}{|\mathbf{N}_G(T)/T|+1},$$

where the last inequality follows from the fact that since T is sharp, we have $|\mathbf{N}_G(T)/T| < |T|$ by Proposition 1.14(c).

If p divides $|T|$, then by Proposition 1.14, the proportion of p-regular elements is at least

$$1 - \frac{|T^G| - 1}{|G|} = 1 - \frac{|G : \mathbf{N}_G(T)|(|T| - 1)}{|G|} > 1 - \frac{1}{|\mathbf{N}_G(T)/T|} \geqslant \frac{1}{2},$$

since T is not self-normalizing by our assumption.

If there are several conjugacy classes of sharp subgroups in G and p does not divide the order of any of them, then the proportion of p-regular elements is at least

$$\frac{1}{|G|}\left|\bigcup_{i=1}^{k} T_i^G\right| > \sum_{i=1}^{k} \frac{|T_i| - 1}{|\mathbf{N}_G(T_i)|} \geqslant \sum_{i=1}^{k} \frac{1}{|\mathbf{N}_G(T_i)/T_i| + 1}.$$

□

REMARK 1.16. One advantage of using the quantity $|\mathbf{N}_G(T)/T|$ in our estimates is that for a family $X(q)$ of finite simple groups of Lie type and the family of maximal tori $T(q)$ in these groups defined by a particular class C of the corresponding Weyl group, the right hand side is independent of q (it depends only on the type X and the class C).

Regarding the sporadic simple groups we observe that each sporadic simple group has a self-centralizing subgroup of order r for some prime r, so every element of the group is either r-regular or has order r (see Proposition 5.1).

Sometimes we shall use the language of probabilities. For a nonempty finite set X and a subset $Y \subseteq X$ we set $\mathrm{Prob}_X(Y) = |Y|/|X|$. By a "random element" of a finite nonempty set X we mean a uniformly distributed random element of X.

1.3. *Erratum to a prior announcement of our results*

The paper [**BB**] announced the main results of the present paper and gave a number of applications. Since the applications given in [**BB**] served as the principal motivation for the present work, we review the results used in [**BB**], correcting some inaccuracies and giving more detailed versions. We emphasize that none of the changes affect the validity of the applications given in [**BB**].

The two principal results used in [**BB**] are Theorem 1.6 and Theorem 1.20. Theorem 1.6 corrects some inaccuracies of its [**BB**]-version (see Remark 1.8). Theorem 1.20 gives a more detailed version of the result stated as Corollary 8.10 in [**BB**] and fixes an omission in its proof.

In Section 8.3 of [**BB**] a summary form $(k_1k_2)/(k_3k_4)$, with appropriate constraints on the k_i, has been given for the orders of the tori constructed. From the list of possible values of k_i, [**BB**] erroneously omitted the values $k_2 = q^2 - 1$ (for $E_6(q)$ and ${}^2E_6(q)$), as well as $k_4 = 2$ or 4 (for certain orthogonal groups). (Cf. Tables II and III below.) Moreover, as noted in Remark 1.8, as a single exception, ${}^2F_4(2)'$ does not contain two maximal *cyclic* tori of coprime orders. (It does contain maximal tori of orders 13 and 5^2.)

1.4. *Pseudo-orders*

In algorithmic applications it is often impossible to calculate the order of an element, because it would require finding prime factors of large numbers. Instead, following [**BB**, Section 8], one is content with determining a so-called pseudo-order

of elements. To define this concept we start with a set $\mathcal{P}$ of pairwise relatively prime integers. We refer to the elements of $\mathcal{P}$ as *pretend-primes*. (The idea is that we may have difficulty splitting these numbers into their prime factors, so we pretend instead that they are prime.) We assume that every prime divisor of $|G|$ divides a suitable pretend-prime in $\mathcal{P}$, or, equivalently, that $|G|$ has a multiple of the form $\prod_{p\in\mathcal{P}} p^{k_p}$.

The $\mathcal{P}$-closure of a divisor n of $|G|$ is the smallest positive integer $n_{\mathcal{P}}$ which is a multiple of n and which can be written as a product of integers from $\mathcal{P}$. The *pseudo-order* of an element $g \in G$ with respect to the set $\mathcal{P}$ is defined to be the $\mathcal{P}$-closure of the actual order. Equivalently, the pseudo-order of $g \in G$ is the smallest positive integer ℓ such that $g^\ell = 1$ and ℓ is a product of pretend-primes (see [**BB**], p. 55). If the set $\mathcal{P}$ is explicitly given then it is easy to calculate the pseudo-order (with respect to $\mathcal{P}$) of any element of the group.

Given two sets of integers, $\mathcal{P}_1$ and $\mathcal{P}_2$, we say that $\mathcal{P}_1$ is *coarser* than $\mathcal{P}_2$ if

(a) every member of $\mathcal{P}_2$ divides some member of $\mathcal{P}_1$; and

(b) every member of $\mathcal{P}_1$ is the product of some members of $\mathcal{P}_2$.

Given a (finite or infinite) set $\mathcal{L}$ of positive integers, the *relatively prime refinement* of $\mathcal{L}$ is the coarsest set $\mathcal{P}$ of pairwise relatively prime integers such that $\mathcal{L}$ is coarser than $\mathcal{P}$. If $\mathcal{L}$ is an explicitly given finite set then $\mathcal{P}$ can be computed efficiently (see [**BB**, Claim 8.8]).

Now the task is to find nontrivial P-regular elements in G, i. e., elements of which the order is relatively prime to P, where P is a $\mathcal{P}$-closed number.

This can be accomplished, using Theorem 1.6, with reference to a certain explicitly computable set $\mathcal{P}$ obtained from the orders of the maximal tori mentioned in Theorem 1.6. Next we describe the set $\mathcal{P}$.

Let us fix the parameters n and p. [**BB**] defines a set of integers $\mathcal{L}(n,p)$ whose relatively prime refinement $\mathcal{P}(n,p)$ is then used as the set of pretend-primes for determining the pseudo-orders of elements in sections (quotients of subgroups) of $GL_n(p)$. Below we give a slightly modified definition to handle sections of $GL_n(q)$, q a power of p, as well as the case of characteristic zero.

For the definition we require the following result, obtained by combining a result by Landazuri and Seitz [**LS**] with another by Feit and Tits [**FT**].

THEOREM 1.17. *Let S be a finite simple group of Lie type of characteristic r over the field of order $q = r^e$. Let $m-1$ be the minimum dimension of projective spaces over* GF(q) *on which S acts nontrivially. Let H be a finite group which involves S (as a quotient of a subgroup). If H acts faithfully on a projective space of dimension $n-1$ over a field of characteristic other than r then $q^m \leqslant n^{c_1}$, where $c_1 = \dfrac{248}{27+\log_2 3} = 8.67589\ldots$. In particular, S has a faithful permutation representation of degree less than n^{c_1}. If S is a classical group, then a better estimate $q^m \leqslant n^{c_2}$ holds with $c_2 = 8\log 3/\log 6 = 4.90517\ldots$. Moreover, if we exclude $S = PSL_3(2)$ and $Sp_4(2)'$, then we have $m \leqslant n$ as well.*

For large n, the last inequality, $m \leqslant n$, is far weaker than the main inequalities which are of the form $q^m \leqslant n^c$; but this weaker inequality will be helpful for small values of n.

We indicate the proof of Theorem 1.17 in an Appendix (Section 7).

In order to define our sets $\mathcal{L}(n,p)$, we need to consider the cyclotomic polynomials. Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial, so $x^n - 1 = \prod_{d\,|\,n} \Phi_d(x)$.

Recall that we have

$$\begin{aligned}
\Phi_1(x) &= x - 1,\\
\Phi_3(x) &= x^2 + x + 1,\\
\Phi_4(x) &= x^2 + 1 = (x + \sqrt{2x} + 1)(x - \sqrt{2x} + 1),\\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1,\\
\Phi_6(x) &= x^2 - x + 1 = (x + \sqrt{3x} + 1)(x - \sqrt{3x} + 1),\\
\Phi_{12}(x) &= x^4 - x^2 + 1\\
&= (x^2 + \sqrt{2x^3} + x + \sqrt{2x} + 1)(x^2 - \sqrt{2x^3} + x - \sqrt{2x} + 1),\\
\Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.
\end{aligned}$$

DEFINITION 1.18. We displayed a factorization of $\Phi_4(x)$, $\Phi_6(x)$, and $\Phi_{12}(x)$ over $\mathbf{R}[\sqrt{x}]$; we refer to the factors in these particular factorizations as *semicyclotomic factors*. We denote the two semicyclotomic factors of $\Phi_n(x)$ $(n = 4, 6, 12)$ by $\Phi_n^+(x)$ and $\Phi_n^-(x)$; the first of of these has only "+" signs in its expression.

So, for instance, $\Phi_{12}^-(x) = x^2 - \sqrt{2x^3} + x - \sqrt{2x} + 1$, and in all the three cases, $\Phi_n(x) = \Phi_n^+(x)\Phi_n^-(x)$.

DEFINITION 1.19. We call the numbers $\pm\Phi_n(q)$ $(n, q$ integers, $n \geqslant 1)$ *cyclotomic numbers*. We call the numbers $\pm\Phi_n^\pm(q)$ *semicyclotomic numbers* if $n = 4$ or 12 and q is an odd power of 2; and if $n = 6$ and q is an odd power of 3.

We now define our sets $\mathcal{L}(n,p)$.

Let $n \geqslant 2$ and p a prime or $p = 0$. Let $\mathcal{L}(n,p)$ consist of the following numbers:

(i) all primes $\leqslant 47$ and the primes 59, 67, 71 (these are the primes occurring in sporadic groups, including the Tits group ${}^2F_4(2)'$);

(ii) all primes $\leqslant n^{c_1}$ where $c_1 = 8.67589\ldots$ is the constant from Theorem 1.17;

(iii) if $p \neq 0$ then additionally the cyclotomic numbers $|\Phi_i(\pm p^j)|$ for all $j \geqslant 1$ and $i \in \{1, 3, 5, 15\}$.

(iv) if $p = 2$, then additionally the semicyclotomic numbers $\Phi_4^\pm(2^{2t+1})$ and $\Phi_{12}^\pm(2^{2t+1})$ for all $t \geqslant 1$;

(v) if $p = 3$, then additionally the semicyclotomic numbers $\Phi_6^\pm(3^{2t+1})$ for all $t \geqslant 1$.

Let $\mathcal{P}(n,p)$ be the relatively prime refinement of $\mathcal{L}(n,p)$.

A corollary to the following strengthening of Theorem 1.4 is central to the polynomial-time claims made in [**BB**]. The corollary is given as Corollary 8.10 in [**BB**].

THEOREM 1.20. *Let F be a field of characteristic $p \geqslant 0$. Let S be a finite simple group which occurs as a quotient of a finite subgroup of $GL_n(F)$. Let $\gamma(n) = \max\{31, 2n\}$. Then for any prime r, at least a $1/\gamma(n)$ fraction of the elements $g \in S$ has pseudo-order relatively prime to r with respect to the set $\mathcal{P}(n,p)$ of pretend-primes.*

Proof. The proof is based on the fact that the orders of the maximal tori given in Tables II and III below are products of numbers from $\mathcal{L}(n,p)$, occasionally divided by an integer $d \leqslant n$ and by $q \pm 1 = |\Phi_1(\pm q)|$, where q is a power of p; and all prime divisors of the orders of any alternating groups that may be involved as well as all prime divisors of the orders of all sporadic groups belong to $\mathcal{L}(n,p)$. Note that we treat the Tits group ${}^2F_4(2)'$ as sporadic; all prime divisors of $|{}^2F_4(2)'| = 2^{11}\cdot 3^3\cdot 5^2\cdot 13$ belong to $\mathcal{L}(n,p)$.

We follow the lines of the proof of Corollary 8.10 from [**BB**]. If S is sporadic then $\pi(S) \subset \mathcal{P} = \mathcal{P}(n,p)$ so we only need to refer to Theorem 1.1 (d) to obtain $|S(r')|/|S| > 2/29 > 1/31$.

If S is alternating of degree $k \geqslant 9$ then $k \leqslant n+2$ by Proposition 1.22 (a) below. For $k \leqslant 8$, the prime divisors of $|A_k|$ are $\leqslant 7$. So, if S is alternating of any degree then $\pi(S) \subset \mathcal{P}$. Therefore we only need to consider the proportion $|S(r')|/|S|$, which, by Theorem 1.1 (a), is at least $26/(27\sqrt{k}) > 1/(2n)$ if $k \geqslant 9$, and $26/(27\sqrt{k}) > 1/31$ if $k \leqslant 8$.

If S is of Lie type of characteristic $s \neq p$ over the field of order s^e, then, by Theorem 1.17, we have $s^{ef} \leqslant n^{c_1}$, where $f-1$ is the minimum dimension of projective spaces over $\mathrm{GF}(s^e)$ on which S acts nontrivially and $c_1 = 8.67589\ldots$. In particular, S has a faithful permutation representation of degree less than n^{c_1}. Therefore all primes dividing the order of S are $\leqslant n^{c_1}$ and hence $\pi(S) \subset \mathcal{P}$. Therefore we only need to consider the proportion $|S(r')|/|S|$. This proportion is at least $1/15 > 1/31$ if S is exceptional, by Theorem 1.1 (c), and at least $1/(2f)$ if S is classical, by Theorem 1.1 (b). The last statement in Theorem 1.17 yields that $f \leqslant n$ with the exceptions of $S = PSL_3(2)$ and $Sp_4(2)'$, and so $|S(r')|/|S| \geqslant 1/(2n)$, as in the two exceptional cases one can easily check that $|S(r')|/|S| > 1/2$.

Finally, let S be of Lie type of characteristic p other than the Tits group ${}^2F_4(2)'$. Then, by Theorem 1.6, S has two maximal tori T_1 and T_2 of relatively prime orders with the properties given in Theorem 1.6. Now $|T_i|$ is a product of cyclotomic and semicyclotomic factors included in $\mathcal{L}(n,p)$ according to Tables II and III below, occasionally divided by an integer $d \leqslant n$ and by $q \pm 1 = |\Phi_1(\pm q)|$, where q is a power of p (the order of the field of definition of S); all these numbers are included in $\mathcal{L}(n,p)$. Therefore if r does not divide $|T_i|$ (which holds for at least one of $i = 1, 2$) then the pseudo-order of elements in T_i^S with respect to $\mathcal{P}$ is not divisible by r. The proportion $|T_i^S|/|S|$ is $\geqslant 1/31$ if S is exceptional and $\geqslant 1/(2f)$ if S is classical where $f-1$ is the dimension of the projective space on which S acts naturally.

The parameter f is associated with the name of the classical group but not with its isomorphism type (e. g., $\Omega_{2k+1}(2^e) \cong Sp_{2k}(2^e)$; under the first name we have $f = 2k+1$, under the second, $f = 2k$). In Proposition 1.22 below, we show that if S is a classical simple group then S has a name under which $f \leqslant n$, with the single exception of $Sp_4(2)'$ for which $n = 3$. This completes the proof for all but this exceptional case. Now for $Sp_4(2)'$ we have proved that the proportion in question is $\geqslant 1/8$ which is greater than $1/31$, the largest possible value of $1/\gamma(n)$. □

For characteristic $p \neq 0$, the sets $\mathcal{L}(n,p)$ and $\mathcal{P}(n,p)$ referred to in Theorem 1.20 are infinite. Although these sets are sufficiently explicit and sparse so they would support the polynomial time algorithms based on the result, explicit finite sets are preferable. For algorithmic applications, if $p \neq 0$ then we may assume that F is an explicitly given finite field. In this case we can impose the following bounds on the

parameters.

THEOREM 1.21. *Let $n, h \geqslant 1$ and let p be a prime. Define the set $\mathcal{L}(n,p,h)$ by the rules (i) through (v) stated before Theorem 1.20 with the following bounds imposed on the parameters i, j, t occurring in items (iii), (iv), (v):*

(iii') $1 \leqslant ij \leqslant nh$;

(iv') $1 \leqslant t \leqslant (nh-4)/8$ *for the first type of semicyclotomic polynomials given and* $1 \leqslant t \leqslant (nh-12)/24$ *for the second type;*

(v') $1 \leqslant t \leqslant (nh-6)/12$.

Let $\mathcal{P}(n,p,h)$ be the relatively prime refinement of $\mathcal{L}(n,p,h)$. Let S be a finite simple group which occurs as a quotient of a subgroup of $GL_n(p^h)$. Let $\gamma(n) = \max\{31, 2n\}$. Then for any prime r, at least a $1/\gamma(n)$ fraction of the elements $g \in S$ has pseudo-order relatively prime to r with respect to the set $\mathcal{P}(n,p,h)$ of pretend-primes.

The proof is identical with the proof of Theorem 1.20.

The next proposition, used in the preceding proof, gives the maximum dimensions of classical simple sections and the maximum degrees of alternating sections of linear groups, combining results of Feit–Tits and Kleidman–Liebeck.

PROPOSITION 1.22. *(a) Let $S = A_k$ for $k \geqslant 9$. Assume S is a section of $GL_n(F)$ for some field F. Then $n \geqslant k-2$.*

(b) Let S be one of the classical simple groups $PSL_f(q)$ ($f \geqslant 2$; $(f,q) \neq (2,2), (2,3)$), $PSU_f(q)$ ($f \geqslant 3$; $(f,q) \neq (3,2)$), $PSp_f(q)$ ($f \geqslant 4$, even, $(f,q) \neq (4,2)$), $\Omega_f(q)$ ($f \geqslant 7$, odd; q odd), $\Omega_f^{\pm}(q)$ ($f \geqslant 8$, even), where $q = p^e$, p prime. Assume S is a section of $GL_n(F)$ where F is a field of characteristic p. Then $n \geqslant f$.
The only classical finite simple group not covered by this list is $PSp_4(2)'$ which indeed is an exception; in this case, $n \geqslant 3$.

Proof. We combine the proofs of the two parts of the Proposition. We may assume F is algebraically closed.

A result of Feit and Tits [**FT**] asserts that if S is an arbitrary finite simple group and S is a quotient of some subgroup of $PSL_n(F)$ where F is algebraically closed then either

(i) S is a subgroup of $PSL_n(F)$, or

(ii) $\operatorname{char} F \neq 2$ and S is of Lie type of characteristic 2.

In our case (a), S is not of Lie type; and in case (b), S and F have the same characteristic. In either case, therefore, part (ii) of the Feit–Tits result cannot occur. Thus, $S \leqslant PSL_n(F)$.

Now if $S = A_k \leqslant PGL_n(F)$ then $k \leqslant n+1$ if the characteristic of F is zero; and in finite characteristic, $k \leqslant n+2$ according to [**KL**, Proposition 5.3.7, p. 186]).

Let now S be one of the classical simple groups listed in case (b). Then, according to [**KL**, Proposition 5.4.13, p. 200], f is indeed the smallest value of n such that $S \leqslant PGL_n(F)$. For $PSp_4(2)'$, the smallest value of n is 3. □

1.5. *Comparison with results of Niemeyer and Praeger*

For certain classical groups, a lower bound for the proportion of p-regular elements can be obtained directly from the estimates for the proportion of ppd elements given by Niemeyer and Praeger [**NP1**]. Recall that $g \in G \leqslant GL_n(q)$ is called a *primitive prime divisor element*, or more precisely a $ppd(n, q; e)$-element in G if its order is divisible by a primitive prime divisor of $q^e - 1$ (i. e., a prime divisor which does not divide $q^j - 1$ for any j, $0 < j < e$).

THEOREM 1.23. [**NP1**, Theorem 5.7] *Let G be a finite classical simple group acting naturally on a projective space of dimension $n - 1$ over $\mathrm{GF}(q)$, and let e with $n/2 < e \leqslant n$ be such that the group G contains $ppd(n, q; e)$-elements. Then the proportion of $ppd(n, q; e)$-elements in G lies in the interval $[1/(e + 1), 1/e)$, except for some cases when G is an orthogonal group and $e \geqslant n - 1$, when this proportion belongs to the interval $[2/(e + 1), 2/e)$.*

(For the detailed description of the exceptional cases we refer to the original paper.)

An extension of the estimates to the case $e = n/2$ can be found in [**NP2**].

COROLLARY 1.24. *Let G be a finite classical simple group naturally acting on a projective space of dimension $n - 1$ over the q-element field, and let p be a prime number. If there exists an e with $n/2 < e \leqslant n$ such that the group G contains $ppd(n, q; e)$-elements and the order of no $ppd(n, q; e)$-element is divisible by p, then the proportion of p-regular elements in G is at least $1/(e + 1) \geqslant 1/(n + 1)$.*

Actually, when applicable, this is a better estimate than our $1/(2n)$. However, such an e does not always exist. If n is small, namely in the cases $G = PSL_2(q)$, $PSp_4(q)$, $PSU_3(q)$, $PSU_4(q)$, $PSU_6(q)$, or $P\Omega_8^+(q)$, there is only one possible value of $e > n/2$ of the required parity (namely 2, 4, 3, 3, 5, and 6, respectively), so the result is not applicable for the primitive prime divisors p of $q^e - 1$ for this e.

Even worse is the situation for $G = PSU_n(q)$ with $n \geqslant 8$ even. Let p be a prime divisor of $q + 1$ not dividing n. (Note that throughout the paper we use the convention that $PSU_n(q)$ is defined over $\mathrm{GF}(q^2)$; in contrast, in [**NP1**] the field of definition for $PSU_n(q)$ was taken to be $\mathrm{GF}(q)$ with q being a square.) Then for every odd e with $n/2 < e < n$ (for unitary groups only these should be considered), if we choose a $ppd(n, q^2; e)$-element $g \in G$ of prime order then its centralizer $\mathbf{C}_G(g)$ always has a normal subgroup of index p, hence at most a $\frac{1}{p}$ fraction of the $ppd(n, q^2; e)$-elements is p-regular. So the Niemeyer–Praeger estimates cannot be used directly in this case.

In Section 3 we obtain a result for exceptional groups of Lie type which is analogous to Theorem 5.7 of Niemeyer and Praeger [**NP1**]. We employ the following Lemma of Niemeyer and Praeger:

LEMMA 1.25. [**NP1**, Lemma 5.6] *Suppose G is a finite group with a self-centralizing cyclic subgroup C of order m and set $u = |\mathbf{N}_G(C) : C|$. Let t be a divisor of m. Suppose further that, if $g \in G$ has order dividing m and $g^t \neq 1$, then g is conjugate in G to an element g' of C and $\mathbf{C}_G(g') = C$. Then the proportion of elements of G of order dividing m which have non-trivial t-th power is equal to $(1 - t/m)/u$. In particular if $m/t \geqslant u + 1$, then this proportion lies in the interval $[1/(u + 1), 1/u)$.*

The following result, to be proved in Section 3.1, extends the work of Niemeyer and Praeger to exceptional groups.

THEOREM 1.26. *Let $G = G(q)$ be a simple exceptional group of Lie type. For the values of e as given in Table I, and also for $e = 7$ and 14 in the case of $G = E_7(q)$, the proportion of elements in G of order divisible by a primitive prime divisor of $q^e - 1$ lies in the interval*

(a) $[1/(u+1), 1/u)$ *for* ${}^3D_4(q)$, $G_2(q)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$;

(b) $[2/(u+1), 2/u)$ *for* ${}^2B_2(q)$, ${}^2G_2(q)$, ${}^2F_4(q)$ *($q \geqslant 8$ is an odd power of 2 for ${}^2B_2(q)$ (Suzuki groups) and ${}^2F_4(q)$ (Ree groups of rank two), and $q \geqslant 27$ is an odd power of 3 for ${}^2G_2(q)$ (Ree groups of rank one)),*

where the value of u can be found in Table I or $u = 14$ in the case of $E_7(q)$.

2. *The alternating groups*

For the symmetric group S_n the probability that a random element is p-regular has been determined by Erdős and Turán [**ET**, Lemma I]. Modifying their argument we obtain a similar result for the alternating group A_n. This was proved independently, in a slightly different form, by Beals, Leedham–Green, Niemeyer, Praeger and Seress [**BL+**]. More generally, Maróti [**Ma**] determined the proportion of l-regular elements in S_n and A_n for arbitrary natural number l. (A permutation is called l-regular if it does not contain a cycle of length divisible by l.)

THEOREM 2.1. *Let p be a prime number, $n \geqslant 3$ an integer and $k = \lfloor n/p \rfloor$. Then the proportion of p-regular elements in the alternating group A_n is given by the following formulas:*

(a) if $p = 2$:

$$2\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right);$$

(b) if $p > 2$ and $n \equiv 0$ or $1 \pmod p$:

$$\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right) + \frac{(-1)^k}{kp}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{2p}\right)\cdots\left(1+\frac{1}{(k-1)p}\right);$$

(c) if $p > 2$ and $n \not\equiv 0$ or $1 \pmod p$:

$$\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right).$$

Proof. Using the method of generating functions, Erdős and Turán [**ET**, Lemma I] obtained that the proportion of p-regular elements in the symmetric group S_n equals

$$\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right).$$

If $p = 2$ then all p-regular elements (i. e., permutations of odd order) lie in A_n, hence the proportion of such elements in A_n is the double of their proportion in S_n, proving part (a).

In order to obtain the proportion of p-regular elements in the case $p > 2$ we are also going to use generating functions. Following [**ET**], let $f(n, p)$ denote the

number of p-regular elements in S_n. Erdős and Turán show that $f(n,p)/n!$ is the coefficient of z^n in

$$\prod_\nu{}' \left(1 + \frac{1}{1!}\frac{z^\nu}{\nu} + \frac{1}{2!}\left(\frac{z^\nu}{\nu}\right)^2 + \dots\right),$$

where $\prod'$ indicates that the product is to be extended over all ν's not divisible by p. If we define $g(n,p)$ to denote the difference between the number of even and odd permutations that are p-regular, then we obtain analogously that $g(n,p)/n!$ is the coefficient of z^n in

$$\prod_\nu{}' \left(1 + (-1)^{\nu-1}\frac{1}{1!}\frac{z^\nu}{\nu} + \frac{1}{2!}\left(\frac{z^\nu}{\nu}\right)^2 + (-1)^{\nu-1}\frac{1}{3!}\left(\frac{z^\nu}{\nu}\right)^3 + \dots\right).$$

For $|z| < 1$ this can be written in the form

$$\begin{aligned}
&\prod_\nu{}' \exp\left((-1)^{\nu-1}\frac{z^\nu}{\nu}\right) = \exp\left(\sum_{\nu=1}^{\infty}(-1)^{\nu-1}\frac{z^\nu}{\nu} - \sum_{\nu=1}^{\infty}(-1)^{\nu p-1}\frac{z^{\nu p}}{\nu p}\right)\\
&= \exp\left(\log(1+z) - \frac{1}{p}\log(1+z^p)\right) = (1+z)(1+z^p)^{-1/p}\\
&= (1+z)\left(1 + \sum_{k=1}^{\infty}\binom{-1/p}{k} z^{kp}\right).
\end{aligned}$$

Since

$$\binom{-1/p}{k} = (-1)^k \frac{1}{kp}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{2p}\right)\cdots\left(1+\frac{1}{(k-1)p}\right),$$

we obtain (b) and (c). □

Remark 2.2. For a fixed prime p the order of magnitude of the proportion of p-regular elements in A_n as given in Theorem 2.1 is $\Theta(n^{-1/p})$ (i. e., it is between two positive constants times $n^{-1/p}$).

Since we want a universal lower bound, independent of p, we prove an estimate of the form $c/\sqrt{n}$. (Note that for every $\epsilon > 0$ we have the lower bound $(\sqrt{8/\pi} - \epsilon)/\sqrt{n}$ for every sufficiently large n. However, we need a constant c that works for all $n \geqslant 5$.)

Proposition 2.3. *For every $n \geqslant 5$ and every prime p, the proportion of p-regular elements in A_n is at least*

$$\frac{26}{27}\cdot\frac{1}{\sqrt{n}}.$$

Proof. First note that

$$1 - \frac{1}{kp} > \sqrt{\frac{k-1}{k}} \quad \text{if} \quad p \geqslant 2, k \geqslant 2,$$

and

$$1 + \frac{1}{(k-1)p} < \sqrt{\frac{k}{k-1}} \quad \text{if} \quad p \geqslant 3, k \geqslant 2.$$

Then in the formulas provided by Theorem 2.1 we obtain for $p = 2$:

$$2\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right) \geqslant 2\cdot\frac{1}{2}\cdot\sqrt{\frac{1}{2}}\cdot\sqrt{\frac{2}{3}}\cdots\sqrt{\frac{k-1}{k}} = \frac{1}{\sqrt{k}} \geqslant \frac{\sqrt{2}}{\sqrt{n}} > \frac{1}{\sqrt{n}};$$

for $p \geqslant 5$:

$$\begin{aligned}
&\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right)\\
&\quad-\frac{1}{kp}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{2p}\right)\cdots\left(1+\frac{1}{(k-1)p}\right)\\
&\geqslant \left(1-\frac{1}{p}\right)\cdot\sqrt{\frac{1}{2}}\cdot\sqrt{\frac{2}{3}}\cdots\sqrt{\frac{k-1}{k}} - \frac{1}{kp}\cdot\sqrt{\frac{2}{1}}\cdot\sqrt{\frac{3}{2}}\cdots\sqrt{\frac{k}{k-1}}\\
&= \left(\left(1-\frac{1}{p}\right)-\frac{1}{p}\right)\cdot\frac{1}{\sqrt{k}} \geqslant \left(\sqrt{p}-\frac{2}{\sqrt{p}}\right)\cdot\frac{1}{\sqrt{n}} > \frac{1}{\sqrt{n}};
\end{aligned}$$

for $p = 3$ and $n \geqslant 9$:

$$\begin{aligned}
&\left(1-\frac{1}{p}\right)\left(1-\frac{1}{2p}\right)\cdots\left(1-\frac{1}{kp}\right)\\
&\quad-\frac{1}{kp}\left(1+\frac{1}{p}\right)\left(1+\frac{1}{2p}\right)\cdots\left(1+\frac{1}{(k-1)p}\right)\\
&\geqslant \frac{2}{3}\cdot\frac{5}{6}\cdot\frac{8}{9}\cdot\sqrt{\frac{3}{4}}\cdots\sqrt{\frac{k-1}{k}} - \frac{1}{3k}\cdot\frac{4}{3}\cdot\frac{7}{6}\cdot\sqrt{\frac{4}{3}}\cdots\sqrt{\frac{k}{k-1}}\\
&= \frac{26}{27}\cdot\frac{1}{\sqrt{3k}} \geqslant \frac{26}{27}\cdot\frac{1}{\sqrt{n}}.
\end{aligned}$$

Finally, for $p = 3$ and $5 \leqslant n \leqslant 8$ the proportion of p-regular elements in A_n is 2/3, 7/9, 7/9, and 5/9, respectively, for which our estimate clearly holds. □

3. *The exceptional groups of Lie type*

In the case of exceptional groups of Lie type we offer two approaches. The second one is the same as in the case of classical groups: we construct pairs of maximal tori of coprime orders. Using this method we could prove the lower bound 1/31 for the number of p-regular elements for arbitrary prime p. We will not work out the details there, because the other method gives a better bound. Namely, our first approach, based on the existence of sharp tori (i. e., strongly self-centralizing tori in the sense of G. Higman) in all exceptional groups of Lie type with the exception of $E_7(q)$, will yield the lower bound 1/15.

3.1. *Sharp tori in exceptional groups of Lie type*

THEOREM 3.1. *For the pairs (S, T) listed in Table I, where S is an exceptional simple group of Lie type and T is a cyclic maximal torus in S of the order stated in Table I, the torus T is sharp (strongly self-centralizing) in S, i. e., $\mathbf{C}_S(t) = T$ for every $t \in T^\times = T \setminus \{1\}$.*

Combining Theorem 3.1 with Proposition 1.15 we obtain part (c) of Theorem 1.1:

Table I: Sharp cyclic tori in exceptional groups of Lie type

S	conditions; d	$\lvert T\rvert$	e	$u = \lvert \mathbf{N}_S(T)/T\rvert$
${}^2B_2(q)$	$q = 2^{2k+1} \geqslant 8$	$\Phi_4^{\pm}(q)$	4	4
${}^3D_4(q)$		$\Phi_3(-q^2)$	12	4
$G_2(q)$	$q \not\equiv 1\,(3)$	$\Phi_3(q)$	3	6
	$q \not\equiv 2\,(3)$	$\Phi_3(-q)$	6	6
${}^2G_2(q)$	$q = 3^{2k+1} \geqslant 27$	$\Phi_6^{\pm}(q)$	6	6
$F_4(q)$		$\Phi_3(-q^2)$	12	12
${}^2F_4(q)$	$q = 2^{2k+1}$ *	$\Phi_{12}^{\pm}(q)$	12	12
$E_6(q)$	$d = (3, q-1)$	$\frac{1}{d}\Phi_3(q^3)$	9	9
${}^2E_6(q)$	$d = (3, q+1)$	$\frac{1}{d}\Phi_3(-q^3)$	18	9
$E_8(q)$		$\Phi_3(-q^4)$	24	24
		$\Phi_{15}(q)$	15	30
		$\Phi_{15}(-q)$	30	30
	$q \not\equiv \pm 2\,(5)$	$\Phi_5(-q^2)$	20	20

*For $q = 2$ the group ${}^2F_4(q)$ is not simple; in that case take $S = {}^2F_4(2)'$ (the Tits group) and $\lvert T\rvert = 13$.

COROLLARY 3.2. *For every finite exceptional simple group S of Lie type and every prime p, the proportion of p-regular elements in S is greater than* $1/15$.

Proof. First assume that S is not $E_7(q)$. Then Proposition 1.15 yields that the proportion of p-regular elements in S is at least

$$\sum_i \frac{1}{|\mathbf{N}_S(T_i)/T_i|+1} \geqslant \frac{1}{13}.$$

The case $S = E_7(q)$ requires a different method; Corollary 3.5 (below) asserts that in this case the proportion of p-regular elements is greater than $1/15$. □

For the proof of Theorem 3.1 we need the following observation.

LEMMA 3.3. *For each torus T listed in Table I, every prime divisor of $|T|$ is a primitive prime divisor of $q^e - 1$ for the exponent e stated in Table I.*

Proof. For explicit expressions of certain cyclotomic polynomials $\Phi_n(x)$ and their semicyclotomic factors $\Phi_n^{\pm}$ (for $n = 4, 6, 12$) we refer to Definition 1.18 and the table preceding it.

Let r be a prime divisor of $|T|$ and assume that k is the smallest positive exponent such that $r \mid q^k - 1$. Then $r \mid q^n - 1$ if and only if $k \mid n$.

Now we have $r \mid |T| \mid \Phi_e(q) \mid q^e - 1$, hence $k \mid e$ holds. We have to show $k = e$. Assume by way of contradiction that $k < e$; then $r \mid \Phi_e(q) \mid (q^e - 1)/(q^k - 1)$, so $r \mid (1 + q^k + q^{2k} + \cdots + q^{e-k}, q^k - 1) = (e/k, q^k - 1)$, hence r is a divisor of e. In our cases the only prime divisors of e can be 2, 3, or 5. It can easily be checked that none of the relevant primes divides the order of T. □

Proof of Theorem 3.1. To prove the Theorem, we first observe that S indeed has cyclic tori of orders as given in Table I. The theory of maximal tori is discussed in [**SS**, Section II] and [**Ca**]. In particular, the conjugacy classes of maximal tori are described via the conjugacy classes of the corresponding (untwisted) Weyl group, the automizers $\mathbf{N}_S(T)/T$ are given as certain subgroups of the Weyl groups, and the structure of the torus can be worked out using information obtained from the Weyl group. Then [**Ca**] gives in detail the conjugacy classes in the Weyl group, giving the orders of all the tori (at least in the untwisted case). One can use this to find these tori, and use the procedure given to check that they really are cyclic. This is done in detail in the thesis of Gager [**Ga**], where the information is also obtained for the twisted groups.

Alternatively, one can use various well-known subgroups of maximal rank, as in the paper [**LSS**]. For example, in [**LSS**, Example 1.4], the subsystem A_2^3 of E_6 is used to construct a subgroup $PSL_3(q^3)$ inside $E_6(q)$ (respectively $PSU_3(q^3)$ inside ${}^2E_6(q)$). This contains the cyclic torus indicated. Also, a complete list of maximal tori in exceptional groups of Lie type is accessible in [**KS**].

These sources also provide the value of $u = |\mathbf{N}_S(T)/T|$ as listed in Table I.

Now it is easy to check (using Lemma 3.3) that for all tori listed in Table I we have that $(|S : T|, |T|) = 1$. We want to show that for every $1 \neq t \in T$ the centralizer $\mathbf{C}_S(t)$ coincides with T. Without loss of generality we may assume that t has prime order r. By Lemma 3.3, r is a primitive prime divisor of $q^e - 1$. Observe that $|\mathbf{C}_S(t)|$ cannot be divisible by the characteristic of the field of definition, since otherwise t would lie in the centralizer of a unipotent element and hence in a parabolic subgroup of S, contrary to our choice of e. Now we can check that the only conjugacy class

of maximal tori of order divisible by r is the class of T, for example by using the lists in [**KS**]. Hence it follows that $\mathbf{C}_S(t) = T$. □

Next, we use Theorem 3.1 to prove Theorem 1.26.

Proof of Theorem 1.26. First let G be any of the groups ${}^3D_4(q)$, $G_2(q)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_8(q)$. We are going to apply Lemma 1.25. For C we take a cyclic sharp torus T as given in Table I, and set $t = 1$. Since every primitive prime divisor of $q^e - 1$ divides $\Phi_e(q)$, it divides $|T|$ as well. Conversely, every prime divisor of $|T|$ is a primitive prime divisor of $q^e - 1$ by Lemma 3.3. Using Theorem 3.1 and Sylow's Theorem we obtain that an element $g \in G$ has order divisible by a primitive prime divisor of $q^e - 1$ if and only if it lies in a conjugate of T. Hence Lemma 1.25 is applicable and it yields the desired result for the proportion of these elements.

The argument for the groups ${}^2B_2(q)$, ${}^2G_2(q)$, ${}^2F_4(q)$ is the same, but the desired elements appear in two different classes of maximal tori as indicated. The proportion of the appropriate elements in each of them is estimated as before (since the two tori have coprime orders) and the result follows.

Finally for $G = E_7(q)$ we take any of the tori T_1, T_2 from Table II and set for T_1: $e = 7$ and $t = (q-1)(7, q-1)/(2, q-1)$; and for T_2: $e = 14$ and $t = (q+1)(7, q+1)/(2, q+1)$. The proof of Theorem 3.4 yields that Lemma 1.25 is applicable here as well, with $u = 14$, thus finishing the proof. □

3.2. *Pairs of tori in exceptional groups of Lie type*

We use the letter X to represent the (Chevalley-Steinberg) *type* of a finite simple group of Lie type, such as $X = B_n$ or $X = {}^3D_4$. The group itself is denoted by $S = X(q)$ where q is the order of the field of definition.

THEOREM 3.4. *For every exceptional type X, there exists a constant $c(X) \geqslant 1/31$ such that every finite exceptional simple group $X(q)$ of type X, except the Tits group ${}^2F_4(2)'$, contains cyclic maximal tori T_1 and T_2 of relatively prime orders such that for $i = 1, 2$ we have*

$$\frac{|T_i^S|}{|S|} > c(X).$$

The orders of the T_i as well as the lower bounds $c(X)$ are listed in Table II. Note that those listed are not the only pairs of maximal tori with the given properties.

Proof. We are going to apply Proposition 1.11. Following the notation of Proposition 1.11, let $v_i = |\Gamma(T_i)|/|T_i|$ and $u_i = |\mathbf{N}_S(T_i)/T_i|$. In accordance with Proposition 1.11, our goal is to prove that $v_i/u_i \geqslant c(X)$ for the values of $c(X)$ stated in Table II.

We give a detailed proof only in the case $S = E_7(q)$. As in the proof of Theorem 3.1 we can show the existence of two maximal tori T_1 and T_2 of respective orders $\frac{1}{d}(q^7 - 1)$ and $\frac{1}{d}(q^7 + 1)$, where $d = (2, q-1)$. Their orders are coprime. A primitive prime divisor of $q^7 - 1$ divides the order only of the parabolic of type A_6; an easy calculation shows that an element whose order is a primitive prime divisor of $q^7 - 1$ cannot centralize any unipotent element there. Hence we see similarly as in the proof of Theorem 3.1 that if the order of an element $t \in T_1$ is divisible by a

Table II: Pairs of cyclic maximal tori in exceptional groups of Lie type

$S = X(q)$	conditions; d	$\lvert T_1\rvert$	$\lvert T_2\rvert$	u_i	$c(X)$
${}^2B_2(q)$	$q = 2^{2k+1} \geqslant 8$	$\Phi_4^+(q)$	$\Phi_4^-(q)$	4, 4	1/5
${}^3D_4(q)$		$\Phi_3(-q^2)$	$-\Phi_1(-q)\Phi_1(q^3)$	4, 4	3/26
$G_2(q)$	$q > 2$	$\Phi_3(q)$	$\Phi_3(-q)$	6, 6	1/7
${}^2G_2(q)$	$q = 3^{2k+1} \geqslant 27$	$\Phi_6^+(q)$	$\Phi_6^-(q)$	6, 6	1/7
$F_4(q)$		$\Phi_3(-q^2)$	$-\Phi_1(-q)\Phi_1(q^3)$	12, 12	1/26
${}^2F_4(q)$	$q = 2^{2k+1} \geqslant 8$	$\Phi_{12}^+(q)$	$\Phi_{12}^-(q)$	12, 12	1/13
$E_6(q)$	$d = (3, q-1)$	$\frac{1}{d}\Phi_3(q^3)$	$-\frac{1}{d}\Phi_1(-q^4)\Phi_1(q^2)$	9, 8	1/10
${}^2E_6(q)$	$d = (3, q+1)$	$\frac{1}{d}\Phi_3(-q^3)$	$-\frac{1}{d}\Phi_1(-q^4)\Phi_1(q^2)$	9, 8	1/10
$E_7(q)$	$d = (2, q-1)$	$\frac{1}{d}\Phi_1(q^7)$	$-\frac{1}{d}\Phi_1(-q^7)$	14, 14	1/15
$E_8(q)$		$\Phi_{15}(q)$	$\Phi_{15}(-q)$	30, 30	1/31

Notation: $u_i = |\mathbf{N}_S(T_i)/T_i|$.

primitive prime divisor of $q^7 - 1$, then its centralizer coincides with T_1. Since the product of all primitive prime divisors (with multiplicities) of $q^7 - 1$ is $\frac{q^7-1}{(q-1)(7,q-1)}$ we have that

$$v_1 = \frac{|\Gamma(T_1)|}{|T_1|} \geqslant 1 - \frac{(q-1)(7,q-1)}{q^7-1}.$$

Furthermore, $u_1 = |\mathbf{N}_S(T_1)/T_1| = 14$, hence $v_1/u_1 > 1/15$. Similarly, if the order of an element of T_2 is divisible by a primitive prime divisor of $q^{14} - 1$ then its

centralizer is T_2; the product of all primitive prime divisors (with multiplicities) of $q^{14}-1$ is $(q^7+1)/(q+1)(7,q+1)$, hence

$$v_2 = \frac{|\Gamma(T_2)|}{|T_2|} \geqslant 1 - \frac{(q+1)(7,q+1)}{q^7+1}.$$

Since $u_2 = |\mathbf{N}_S(T_2)/T_2| = 14$ as well, $v_2/u_2 > 1/15$ also holds.

Similarly, for the torus T_2 in ${}^3D_4(q)$ one can show that $\Gamma(T_2)$ contains those elements of T_2, whose order is divisible by an integer kl, where $2 < k \mid q+1$ and $3 < l \mid q^2+q+1$. Hence

$$v_2 = \frac{|\Gamma(T_2)|}{|T_2|} \geqslant \left(1 - \frac{(2,q+1)}{q+1}\right)\left(1 - \frac{(3,q^2+q+1)}{q^2+q+1}\right) \geqslant \frac{6}{13},$$

and $|T_2^S|/|S| > v_2/u_2 \geqslant 3/26$.

The same estimate is valid for v_2 for the torus T_2 in $F_4(q)$, hence in that group we obtain the lower bound $v_2/u_2 \geqslant 1/26$.

Consider now the torus T_2 in $E_6(q)$ or in ${}^2E_6(q)$, and let $x \in T_2$ be such that its order is divisible by an integer k with $2 < k \mid q^4+1$. If x lies in a parabolic, then that must be of type D_5 or ${}^2D_5$, respectively. Observe that x does not centralize any unipotent element there. Hence we obtain that $\mathbf{C}_S(x) = T_2$, i.e., $x \in \Gamma(T_2)$. Thus in this case we have

$$v_2 = \frac{|\Gamma(T_2)|}{|T_2|} \geqslant 1 - \frac{(2,q-1)}{q^4+1} \geqslant \frac{16}{17},$$

and $v_2/u_2 \geqslant 2/17$.

In $G_2(q)$ at least one of the tori T_1 and T_2 is sharp. If T_i is not sharp, then 3 divides $|T_i|$ and we get that

$$v_i \geqslant 1 - \frac{3}{|T_i|} \geqslant \frac{6}{7},$$

hence $v_i/u_i \geqslant 1/7$.

All the other tori in Table II are sharp (and cyclic), hence $v_i/u_i \geqslant 1/(u_i+1)$ holds for them (cf. Proposition 1.15). □

Since $E_7(q)$ does not contain sharp tori, we needed the estimate just proved in order to show Corollary 3.2. We state this result separately.

COROLLARY 3.5. *For any prime p the proportion of p-regular elements in $E_7(q)$ is greater than* $1/15$.

4. *The classical groups*

Let S be any of the finite classical simple groups, i. e., $PSL_n(q)$, $PSU_n(q)$, $PSp_n(q)$, $P\Omega_n^\varepsilon(q)$ with the appropriate parameters. Notice that we reserve n to denote the dimension of the vector space on which the corresponding quasisimple group $G = SL_n(q)$, $SU_n(q)$, $Sp_n(q)$, $\Omega_n^\varepsilon(q)$ acts naturally, where $S = G/\mathbf{Z}(G)$. Let us emphasize that the field of definition for $U_n(q)$ is $\mathrm{GF}(q^2)$.

Our main result is the following.

THEOREM 4.1. *In any finite classical simple group S there exist maximal tori T_1 and T_2 of relatively prime orders such for $i = 1, 2$ we have*

$$\frac{\left|T_i^S\right|}{|S|} > \frac{1}{2n},$$

where $n-1$ denotes the dimension of the projective space on which S acts naturally.

With the exception of T_1 for $\Omega_n^+(q)$ with $n \equiv 0\ (4)$, these tori are the same as those in [**MSW**, p. 96].

In certain cases, the name of the group and the corresponding "natural action" are not uniquely defined. In these cases, we give the proof only for one name of the group, namely the one which produces the stronger lower bound. Specifically, the proof omits the following group names (in parenthesis, we give the isomorphic groups appearing in the proof): $\Omega_3(q)$ $(PSL_2(q))$, $\Omega_5(q)$ $(PSp_4(q))$, $P\Omega_6^-(q)$ $(PSU_4(q))$, $P\Omega_6^+(q)$ $(PSL_4(q))$, $\Omega_{2k+1}(2^e)$ $(Sp_{2k}(2^e))$.

The orders of the T_i are listed in Table III. To express these orders through cyclotomic numbers, note that $q^k - 1 = \Phi_1(q^k)$ and $q^k + 1 = -\Phi_1(-q^k)$.

Applying Corollary 1.12 we obtain part (b) of Theorem 1.1:

COROLLARY 4.2. *For every finite classical simple group S and every prime p, the proportion of p-regular elements in S is $> 1/(2n)$.*

This section is devoted to the proof of Theorem 4.1. We will work in the corresponding quasisimple group G. First we will construct the appropriate tori T_i in G. (It will cause no confusion if we denote by T_i a subgroup in G as well as its image in $S = G/\mathbf{Z}(G)$.) Then we show that for at least half of the elements $x \in T_i$ we have $\mathbf{C}_G(x) = T_i$. We also prove that $|\mathbf{N}_G(T_i) : T_i| \leqslant n$, which will yield the stated estimate on the probabilities. Finally, easy number theoretic calculations will give the coprimality of the orders of the two tori in each case. To achieve all these, we need quite a long preparation.

First we define some large cyclic subgroups in certain finite classical groups. By Huppert [**Hu**] there exist irreducible cyclic subgroups in the following cases (in each case we choose a maximal such subgroup):

$C_L(n,q) \leqslant GL_n(q)$ of order $q^n - 1$;

$C_U^1(n,q) \leqslant U_n(q)$ of order $q^n + 1$, provided n is odd;

$C_S^1(n,q) \leqslant Sp_n(q)$ of order $q^{n/2} + 1$, provided n is even;

$C_O^1(n,q) \leqslant O_n^-(q)$ of order $q^{n/2} + 1$, provided n is even.

In certain even dimensional cases we can decompose the underlying space into a direct sum of two totally singular subspaces. Fixing a standard basis (see [**KL**, 2.3.2, 2.4.1, and 2.5.3(i)]) we can define the following cyclic subgroups:

$C_U^2(n,q) \leqslant U_n(q)$ of order $q^n - 1$, provided n is even;

$C_S^2(n,q) \leqslant Sp_n(q)$ of order $q^{n/2} - 1$, provided n is even;

$C_O^2(n,q) \leqslant O_n^+(q)$ of order $q^{n/2} - 1$, provided n is even,

Table III: Some maximal tori in classical simple groups

S	conditions	d	$\lvert T_1\rvert$	$\lvert T_2\rvert$
$PSL_n(q)$	$n \geqslant 2$; $q \geqslant 4$ if $n = 2$	$(n, q-1)$	$\frac{1}{d} \cdot \frac{q^n - 1}{q-1}$	$\frac{1}{d}\left(q^{n-1} - 1\right)$
$PSU_n(q)$	$n \geqslant 3$ odd; $q \geqslant 3$ if $n = 3$	$(n, q+1)$	$\frac{1}{d} \cdot \frac{q^n + 1}{q+1}$	$\frac{1}{d}\left(q^{n-1} - 1\right)$
$PSU_n(q)$	$n \geqslant 4$ even	$(n, q+1)$	$\frac{1}{d} \cdot \frac{q^n - 1}{q+1}$	$\frac{1}{d}\left(q^{n-1} + 1\right)$
$PSp_n(q)$	$n \geqslant 4$ even; $q \geqslant 3$ if $n = 4$	$(2, q-1)$	$\frac{1}{d}\left(q^{\frac{n}{2}} + 1\right)$	$\frac{1}{d}\left(q^{\frac{n}{2}} - 1\right)$
$\Omega_n(q)$	$n \geqslant 7$ odd, q odd	2	$\frac{1}{d}\left(q^{\frac{n-1}{2}} + 1\right)$	$\frac{1}{d}\left(q^{\frac{n-1}{2}} - 1\right)$
$P\Omega_n^-(q)$	$n \geqslant 8$ even	$(4, q^{\frac{n}{2}} + 1)$	$\frac{1}{d}\left(q^{\frac{n}{2}} + 1\right)$	$\frac{\left(q^{\frac{n}{2}-1} + 1\right)(q-1)}{d}$
$P\Omega_n^+(q)$	$n \geqslant 8$, $n \equiv 0\ (4)$	$(2, q-1)^2$	$\frac{\left(q^{\frac{n}{2}-1} - 1\right)(q-1)}{d}$	$\frac{\left(q^{\frac{n}{2}-1} + 1\right)(q+1)}{d}$
$P\Omega_n^+(q)$	$n \geqslant 10$, $n \equiv 2\ (4)$	$(4, q^{\frac{n}{2}} - 1)$	$\frac{1}{d}\left(q^{\frac{n}{2}} - 1\right)$	$\frac{\left(q^{\frac{n}{2}-1} + 1\right)(q+1)}{d}$

where

$$C_U^2(n,q) = \left\{ \begin{pmatrix} g & 0 \\ 0 & (g^*)^{-1} \end{pmatrix} \ : \ g \in C_L(n/2, q^2) \right\},$$
$$C_S^2(n,q) = C_O^2(n,q) = \left\{ \begin{pmatrix} g & 0 \\ 0 & (g^t)^{-1} \end{pmatrix} \ : \ g \in C_L(n/2, q) \right\}.$$

(Here g^t denotes the transpose of the matrix g and g^* denotes the image of g^t under the involutory field automorphism $\alpha \mapsto \alpha^q$ of $\mathrm{GF}(q^2)$.)

The following is obvious.

LEMMA 4.3. *Let g be an element of one of the cyclic subgroups defined above, and let λ be an eigenvalue of g (in the algebraic closure of $\mathrm{GF}(q)$). Then the n eigenvalues of g are the following:*

(a) for $g \in C_L(n,q),\ C_S^1(n,q),\ C_O^1(n,q)$: $\lambda, \lambda^q, \dots, \lambda^{q^{n-1}}$;

(b) for $g \in C_U^1(n,q)$: $\lambda, \lambda^{q^2}, \dots, \lambda^{q^{2(n-1)}}$;

(c) for $g \in C_S^2(n,q),\ C_O^2(n,q)$: $\lambda, \lambda^q, \dots, \lambda^{q^{n/2-1}}, \lambda^{-1}, \lambda^{-q}, \dots, \lambda^{-q^{n/2-1}}$;

(d) for $g \in C_U^2(n,q)$: $\lambda, \lambda^{q^2}, \dots, \lambda^{q^{n-2}}, \lambda^{-q}, \lambda^{-q^3}, \dots, \lambda^{-q^{n-1}}$.

LEMMA 4.4.

(a) The image of $C_L(n,q)$ by the determinant map has order $q-1$.

(b) The image of $C_U^i(n,q)$ ($i = 1,2$) by the determinant map has order $q+1$.

(c) The group $C_O^i(n,q)$ ($i = 1,2$) is contained in $SO_n^\varepsilon(q)$ ($\varepsilon = -$ for $i = 1$; $\varepsilon = +$ for $i = 2$), but if q is odd then $C_O^i(n,q) \not\leqslant \Omega_n^\varepsilon(q)$.

Proof. (a) By Lemma 4.3(a) we have $\det g = \lambda^{(q^n-1)/(q-1)}$. Since λ can be any element of $\mathrm{GF}(q^n)$, the claim follows.

(b) Similarly, we obtain for $C_U^1(n,q)$ with n odd that $\det g = \lambda^{(q^{2n}-1)/(q^2-1)}$. Since λ is an arbitrary (q^n+1)-th root of unity in $\mathrm{GF}(q^{2n})$, it follows that $\lambda^{(q^n+1)/(q+1)}$ is an arbitrary $(q+1)$-th root of unity in $\mathrm{GF}(q^2)$. Now $(q+1, (q^n-1)/(q-1)) = (q+1, q^{n-1}+\cdots+q+1) = 1$, as n is odd. Hence $\det g = \left(\lambda^{(q^n+1)/(q+1)}\right)^{(q^n-1)/(q-1)}$ is indeed an arbitrary $(q+1)$-th root of unity.

Let us take now $C_U^2(n,q)$ with n even. Then Lemma 4.3(d) yields $\det g = \lambda^{(1-q)(q^n-1)/(q^2-1)} = \lambda^{-(q^n-1)/(q+1)}$. Now λ is an arbitrary nonzero element of $\mathrm{GF}(q^n)$, hence the claim follows.

(c) If q is a power of 2, then $|C_O^i(n,q)| = q^{n/2} - (-1)^i$ is odd, hence $C_O^i(n,q) \leqslant \Omega_n^\varepsilon(q)$, as $|O_n^\varepsilon(q) : \Omega_n^\varepsilon(q)| = 2$ in this case. Now let q be an odd prime power. For an element of $C_O^1(n,q)$ the determinant is $\lambda^{(q^n-1)/(q-1)} = (\lambda^{q^{n/2}+1})^{(q^{n/2}-1)/(q-1)} = 1$, since λ is a $(q^{n/2}+1)$-th root of unity. It is obvious that the determinant of any element of $C_O^2(n,q)$ is 1. In order to check whether $C_O^i(n,q) \leqslant \Omega_n^\varepsilon(q)$ we have to calculate the spinor norm of the elements $g \in C_O^i(n,q)$. We do this using the Wall form (see [**Ta**, p. 163 and p. 153]):

$$\Theta(g) = \mathrm{disc}(\chi_g), \quad \chi_g(u,v) = \beta\left((1-g)^{-1}u, v\right),$$

where β is the symmetric bilinear form defining $O_n^\varepsilon(q)$, and $\mathrm{disc}(\chi_g)$ is the determinant of χ_g modulo the subgroup of squares in $\mathrm{GF}(q)$, i. e.,

$$\Theta(g) = \det\beta \cdot \det(1-g) \bmod \mathrm{GF}(q)^2.$$

For $O_n^+(q)$ we have $\det\beta = (-1)^{n/2}$, hence for $O_n^-(q)$ it must be $(-1)^{n/2}\delta$, where δ is a non-square element of $\mathrm{GF}(q)$.

Now let g be a generator of $C_O^i(n,q)$, and λ an eigenvalue of g. We treat the two cases separately. If $i = 1$, then $C_O^1(n,q) \leqslant O_n^-(q)$ has order $q^{n/2}+1$, hence λ is a

primitive $(q^{n/2}+1)$-th root of unity in $\mathrm{GF}(q^n)$, so $\lambda^{q^{n/2}} = 1/\lambda$. Now $\sqrt{\lambda} \in \mathrm{GF}(q^n)$ exists, and $\sqrt{\lambda}^{q^{n/2}} = -1/\sqrt{\lambda}$. Therefore we obtain that

$$\det \beta \cdot \det(1-g) = (-1)^{n/2}\delta \prod_{j=0}^{n-1} \left(1-\lambda^{q^j}\right)$$
$$= \delta \cdot \prod_{j=0}^{n/2-1} (\lambda-1)^{q^j} \left(1-\lambda^{q^{n/2}}\right)^{q^j} = \delta \cdot \left(\lambda - 2 + \lambda^{-1}\right)^{\frac{q^{n/2}-1}{q-1}}$$
$$= \delta \cdot \left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{2\frac{q^{n/2}-1}{q-1}}.$$

We claim that the second factor is a square in $\mathrm{GF}(q)$, hence the spinor norm of g is nontrivial, indeed. An element $\alpha \in \mathrm{GF}(q)$ is a square iff $\alpha^{(q-1)/2} = 1$. Testing the second factor we obtain

$$\left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{2\frac{q^{n/2}-1}{q-1}\cdot\frac{q-1}{2}} = \left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{q^{n/2}} \left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{-1}$$
$$= \left(-\frac{1}{\sqrt{\lambda}} + \sqrt{\lambda}\right)\left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{-1} = 1,$$

as we wanted.

Let us now consider $C_O^2(n,q) \leqslant O_n^+(q)$ of order $q^{n/2}-1$, so in this case λ is a primitive element of $\mathrm{GF}(q^{n/2})$. Obviously, $\lambda^{q^{n/2}} = \lambda$ holds. Take $\sqrt{\lambda} \in \mathrm{GF}(q^n)$, then $\sqrt{\lambda}^{q^{n/2}} = -\sqrt{\lambda}$. We obtain that

$$\det \beta \cdot \det(1-g) = (-1)^{n/2} \prod_{j=0}^{n/2-1} \left(\left(1-\lambda^{q^j}\right)\left(1-\lambda^{-q^j}\right)\right)$$
$$= \left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{2(q^{n/2}-1)/(q-1)}.$$

Applying the same test as above, we get

$$\left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{2\frac{q^{n/2}-1}{q-1}\cdot\frac{q-1}{2}} = \left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{q^{n/2}} \left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{-1}$$
$$= \left(-\sqrt{\lambda} + \frac{1}{\sqrt{\lambda}}\right)\left(\sqrt{\lambda} - \frac{1}{\sqrt{\lambda}}\right)^{-1} = -1,$$

hence the spinor norm of the generator g is nontrivial in this case as well, so $g \notin \Omega_n^+(q)$. □

We will say that $g \in GL_n(q)$ has *simple spectrum* if g has n distinct eigenvalues. The following is our last preparatory result.

LEMMA 4.5. *Let C be any of the cyclic groups from Table IV. Then at least half of the elements in C have simple spectra.*

Observe that again, to express the orders of these groups through cyclotomic numbers, we only need to note that $q^k - 1 = \Phi_1(q^k)$ and $q^k + 1 = -\Phi_1(-q^k)$.

Table IV: The basic cyclic subgroups

C	conditions	$\lvert C\rvert$	k
$C_L(n,q)$	$n \geqslant 1$	q^n-1	n
$C_L(n,q)\cap SL_n(q)$	$n \geqslant 2,\ (n,q)\neq(2,3)$	$(q^n-1)/(q-1)$	n
$C_U^1(n,q)$	$n \geqslant 3$ odd	q^n+1	$2n$
$C_U^1(n,q)\cap SU_n(q)$	$n \geqslant 3$ odd, $(n,q)\neq(3,2)$	$(q^n+1)/(q+1)$	$2n$
$C_U^2(n,q)$	$n \geqslant 4$ even	q^n-1	n
$C_U^2(n,q)\cap SU_n(q)$	$n \geqslant 4$ even	$(q^n-1)/(q+1)$	n
$C_S^1(n,q)$	$n \geqslant 4$ even	$q^{n/2}+1$	n
$C_S^2(n,q)$	$n \geqslant 4$ even, $(n,q)\neq(4,2)$	$q^{n/2}-1$	$n/2$
$C_O^1(n,q)$	$n \geqslant 6$ even	$q^{n/2}+1$	n
$C_O^1(n,q)\cap\Omega_n^-(q)$	$n \geqslant 6$ even, q odd	$(q^{n/2}+1)/2$	n
$C_O^2(n,q)$	$n \geqslant 6$ even	$q^{n/2}-1$	$n/2$
$C_O^2(n,q)\cap\Omega_n^+(q)$	$n \geqslant 6$ even, q odd	$(q^{n/2}-1)/2$	$n/2$

Proof. Making use of Lemma 4.3 we are going to determine which elements of C have eigenvalues with multiplicity greater than one. In case (a) it happens iff $\lambda \in \mathrm{GF}(q^j)$ for some proper subfield of $\mathrm{GF}(q^n)$, i. e., for $j|n$, $1 \leqslant j < n$. Similarly,

in case (b) we obtain the condition that $\lambda \in \mathrm{GF}(q^{2j})$ for some $j|n$, $1 \leqslant j < n$.

In case (c) either $\lambda \in \mathrm{GF}(q^j)$ for some $j|\frac{n}{2}$, $1 \leqslant j < \frac{n}{2}$, or $\lambda^{-1} = \lambda^{q^m}$ for some $0 \leqslant m < \frac{n}{2}$. Assume that λ does not belong to any subfield $\mathrm{GF}(q^j)$, $j|\frac{n}{2}$, $1 \leqslant j < \frac{n}{2}$, but $\lambda^{q^m} = \lambda^{-1}$ holds. If $m = 0$, then $\lambda^2 = 1$, hence $\lambda \in \mathrm{GF}(q)$, so we must have $\frac{n}{2} = 1$. However, if (c) occurs then $n \geqslant 4$. So let $0 < m < \frac{n}{2}$, then $\lambda^{q^{2m}} = (\lambda^{-1})^{q^m} = \lambda$. Since λ has degree $n/2$ over $\mathrm{GF}(q)$, we obtain that $\frac{n}{2}|2m < n$. Thus $n/2$ is even and $m = n/4$. We have shown that in case (c) the multiplicities of the eigenvalues are greater than one iff one of the following holds:

(i) $\lambda \in \mathrm{GF}(q^j)$ for some $j|\frac{n}{2}$, $1 \leqslant j < \frac{n}{2}$;

(ii) $n/2$ is even and $\lambda^{q^{n/4}+1} = 1$.

In case (d) similar calculation yields the conditions

(iii) $\lambda \in \mathrm{GF}(q^{2j})$ for some $j|\frac{n}{2}$, $1 \leqslant j < \frac{n}{2}$; or

(iv) $n/2$ is odd and $\lambda^{q^{n/2}+1} = 1$.

Now we are going to estimate the number of elements in C satisfying one of the properties implying the coincidence of certain eigenvalues. Recall that a prime $p|q^k - 1$ is called a *primitive prime divisor* if p does not divide $q^j - 1$ for $1 \leqslant j < k$. By Zsigmondy's theorem [**Zs**] there almost always exists a primitive prime divisor p of $q^k - 1$ with the only exceptions $k = 2$ and q a Mersenne prime, and $k = 6$, $q = 2$. If $k \geqslant 2$, then obviously $p \geqslant 3$. Now let k be as in Table IV for the individual cases, and assume that there exists a primitive prime divisor p of $q^k - 1$. Then it is easy to check that in each case $p||C|$. If the order of $g \in C$ is divisible by p then an eigenvalue λ of g cannot belong to any proper subfield $\mathrm{GF}(q^j)$, $j|k$, $1 \leqslant j < k$. It follows that the probability that an eigenvalue of a random element of C belongs to a proper subfield is at most $1/p \leqslant 1/3$ (under the assumption that $q^k - 1$ has a primitive prime divisor).

If $k = 2$ and q is a Mersenne prime then one of the cases $C_L(2, q)$, $C_L(2, q) \cap SL_2(q)$ (here $q \neq 3$), and $C_S^2(4, q)$ occurs. The probability that an eigenvalue of $g \in C$ belongs to $\mathrm{GF}(q)$ is $(q-1)/(q^2-1)$, $2/(q+1)$, $(q-1)/(q^2-1)$, respectively, so it is always $\leqslant 1/4$. If $k = 6$ and $q = 2$, then $|C| = 2^6 - 1$, $2^3 + 1$, or $C = C_U^2(6, 2) \cap SU_6(2)$. The probability that an eigenvalue of $g \in C$ belongs to $\mathrm{GF}(2^3)$ or to $\mathrm{GF}(2^2)$ is $9/63$, $3/9$, and $9/21$, respectively.

Summarizing, we obtain that the probability that an eigenvalue of $g \in C$ belongs to a proper subfield is at most $1/3$ with the sole exception $C = C_U^2(6, 2) \cap SU_6(2)$.

The other causes for coincidence of eigenvalues occur in the case (c) of Lemma 4.3 if $n/2$ is even, and in the case (d) if $n/2$ is odd. The probability that a random element of C satisfies condition (ii) above is

$$\frac{q^{n/4} + 1}{q^{n/2} - 1} = \frac{1}{q^{n/4} - 1}$$

for $C = C_S^2(n, q)$ or $C_O^2(n, q)$, and twice as much for $C = C_O^2(n, q) \cap \Omega_n^+(q)$. The groups $C_S^2(4, q)$, $2 < q < 8$, $C_S^2(8, 2)$, $C_O^2(8, 2)$, $C_O^2(8, 3) \cap \Omega_8^+(3)$ will be dealt with separately, for all other groups falling in case (c) the probability that condition (ii) holds is at most $1/7$.

Similarly, in case (d) with $n/2$ odd the probability that a random element of C

Table V: Some exceptional cases

C	$\lvert C\rvert$	$*$	$**$	Prob†
$C_S^2(4,q),\ q=3,5,7$	q^2-1	$q+1$	$q-1$	$2/(q+1)$
$C_S^2(4,4)$	4^2-1	$4+1$	$4-1$	$7/15$
$C_S^2(8,2)$	2^4-1	2^2+1	2^2-1	$7/15$
$C_O^2(8,2)$	2^4-1	2^2+1	2^2-1	$7/15$
$C_O^2(8,3)\cap\Omega_8^+(3)$	$(3^4-1)/2$	3^2+1	3^2-1	$16/40$
$C_U^2(6,2)\cap SU_6(2)$	$(2^6-1)/(2+1)$	$(2^3+1)/3$	2^2-1	$3/21$
$C_U^2(6,3)\cap SU_6(3)$	$(3^6-1)/(3+1)$	$(3^3+1)/2$	$(3^2-1)/4$	$14/182$

* The number of elements of C satisfying (ii) or (iv)
**The number of elements of C with eigenvalues belonging to a proper subfield
† The probability that an element of C has multiple eigenvalues

satisfies (iv) is at most

$$\frac{q^{n/2}+1}{(q^n-1)/(q+1)}=\frac{q+1}{q^{n/2}-1},$$

which is again at most $1/7$ with the exception of $C_U^2(6,2)\cap SU_6(2)$ and $C_U^2(6,3)\cap SU_6(3)$.

So with the noted exceptions we have established that the probability that an element $g\in C$ has eigenvalues of multiplicity greater than one, is at most $1/3+1/7<1/2$.

For the remaining groups we have to do case-by-case calculations, see Table V. Note that the total number of elements has to be determined using the inclusion-exclusion principle. □

Now we are able to define our maximal tori. In each case our construction will employ the following general method. Let V be the vector space (possibly equipped

Table VI: Construction of the maximal tori

G	conditions	T_1	T_2
$SL_n(q)$	$n \geqslant 2$	$C_L(n) \cap G$	$(C_L(n-1) \times C_L(1)) \cap G$
$SU_n(q)$	$n \geqslant 3$ odd	$C_U^1(n) \cap G$	$(C_U^2(n-1) \times C_U^1(1)) \cap G$
$SU_n(q)$	$n \geqslant 4$ even	$C_U^2(n) \cap G$	$(C_U^1(n-1) \times C_U^1(1)) \cap G$
$Sp_n(q)$	$n \geqslant 4$ even	$C_S^1(n)$	$C_S^2(n)$
$\Omega_n(q)$	$n \geqslant 7$ odd, q odd	$(C_O^1(n-1) \times \{1\}) \cap G$	$(C_O^2(n-1) \times \{1\}) \cap G$
$\Omega_n^-(q)$	$n \geqslant 8$ even	$C_O^1(n) \cap G$	$(C_O^1(n-2) \times C_O^2(2)) \cap G$
$\Omega_n^+(q)$	$n \geqslant 8$, $n \equiv 0\ (4)$	$(C_O^2(n-2) \times C_O^2(2)) \cap G$	$(C_O^1(n-2) \times C_O^1(2)) \cap G$
$\Omega_n^+(q)$	$n \geqslant 10$, $n \equiv 2\ (4)$	$C_O^2(n) \cap G$	$(C_O^1(n-2) \times C_O^1(2)) \cap G$

Notation: $C_X^i(k)$ stands for $C_X^i(k, q)$.

with a form) on which the quasisimple group G acts. We decompose $V = V_1 \oplus V_2$ (where the sum is orthogonal in the presence of a nontrivial form), with $0 \leqslant \dim V_2 \leqslant 2$, and choose cyclic subgroups $C_1,\ C_2$ acting on V_1 and V_2, respectively, and let $T = (C_1 \times C_2) \cap G$. The individual cases are given in Table VI.

It is easy to see that each torus T contains $\mathbf{Z}(G)$. Now it is routine to check the order formulae in Table III, noticing that in the case of orthogonal groups we have

in virtue of Lemma 4.4(c) that

$$\frac{|C_1 \times C_2|}{|((C_1 \times C_2) \cap G)/\mathbf{Z}(G)|} = \frac{|SO_n^\varepsilon(q)|}{|P\Omega_n^\varepsilon(q)|} = d.$$

For $T = (C_1 \times C_2) \cap G$ acting on $V_1 \oplus V_2$ let us define T^* to be the subset of T consisting of those elements which have simple spectrum on V_1. (These are actually the *regular semisimple elements* in the torus. However, we shall not use this term in order to avoid confusion with p-regularity.) The action of T restricted to V_1 yields one of the groups listed in Table IV, hence Lemma 4.5 ensures that $|T^*| \geqslant |T|/2$. If $G = SL_2(q)$ then we have to modify the definition of T_2^* (since V_1 and V_2 are both 1-dimensional in this case): we require that the elements must have simple spectrum on the whole space V. Then $|T_2^*| = q - 1 - d \geqslant (q-1)/2 = |T_2|/2$ holds again.

LEMMA 4.6. *Let T be one of the tori in Table VI. Then $\mathbf{C}_G(g) = T$ for all $g \in T^*$.*

Proof. Let $g \in T^*$. Then we claim that the eigenvalues of g on V_1 and on V_2 are different. (So the only eigenvalue with multiplicity greater than one can be ± 1 with multiplicity two on V_2.) Indeed, the eigenvalue(s) on V_2 belong to $\mathrm{GF}(q)$ or $\mathrm{GF}(q^2)$, but the eigenvalues on V_1 generate larger fields, except for T_2^* in the cases $G = SL_2(q)$ or $G = SU_3(q)$. For $SL_2(q)$ we have chosen the definition of T_2^* exactly as it is needed here. An element of $T_2^* \leqslant SU_3(q)$ has eigenvalues $\lambda, \lambda^{-q}, \lambda^{q-1}$ with $\lambda \in \mathrm{GF}(q^2)$, $\lambda \neq \lambda^{-q}$. However, if $\lambda = \lambda^{q-1}$, then $\lambda^{-q} = \lambda^{-q(q-1)} = \lambda^{-q^2+q} = \lambda^{-1+q}$, hence $\lambda = \lambda^{-q}$, which is not the case. We get the same contradiction from $\lambda^{-q} = \lambda^{q-1}$ as well.

Let $\widetilde{G} = GL_n(q)$, $U_n(q)$, $Sp_n(q)$, or $O_n^\varepsilon(q)$, so as $\widetilde{G} \geqslant G$. Furthermore, let $\widetilde{G}(V_i)$ be the action on V_i induced by the subgroup of $\widetilde{G}$ leaving V_i invariant. Then the above claim implies that $\mathbf{C}_{\widetilde{G}}(g) = \mathbf{C}_{\widetilde{G}(V_1)}(g_{V_1}) \times \mathbf{C}_{\widetilde{G}(V_2)}(g_{V_2})$. Now g_{V_1} has simple spectrum, hence its centralizer is abelian. From the maximality of C_1 (which is obvious for the groups $C_X^2(n,q)$ and follows from [**Hu**] for the other groups), we deduce that $\mathbf{C}_{\widetilde{G}(V_1)}(g_{V_1}) = C_1$, so $\mathbf{C}_{\widetilde{G}}(g) \leqslant C_1 \times \widetilde{G}(V_2)$, therefore $\mathbf{C}_G(g) \leqslant (C_1 \times \widetilde{G}(V_2)) \cap G$. In the case of orthogonal groups we have $C_1 \leqslant SO(V_1)$ (see Lemma 4.4(c)), thus $(C_1 \times \widetilde{G}(V_2)) \cap G = (C_1 \times SO(V_2)) \cap G$. However, $SO(V_2) = C_2$ in all cases, hence $\mathbf{C}_G(g) = T$ holds. If G is not an orthogonal group, then $\dim V_2 \leqslant 1$, and $\widetilde{G}(V_2) = C_2$, so $\mathbf{C}_G(g) = T$ again. □

LEMMA 4.7. *Let T be one of the tori in Table VI. Then we have $|\mathbf{N}_G(T) : T| \leqslant n$.*

Proof. Looking at the dimensions of the minimal T-invariant subspaces (which can be n; $n/2, n/2$; $n-1, 1$; $(n-1)/2, (n-1)/2, 1$; $n-2, 2$; $n-2, 1, 1$; and $(n-2)/2, (n-2)/2, 1, 1$) we see that no other T-invariant subspace has the same dimension as V_1 except in the cases $T_2 \leqslant SL_2(q)$ and $T_2 \leqslant SU_3(q)$. In $SL_2(q)$ T_2 is the group of diagonal matrices (of determinant 1), and obviously $|\mathbf{N}_{SL_2(q)}(T_2) : T_2| = 2$ holds. In $SU_3(q)$ T_2 has three 1-dimensional invariant subspaces, two of them are singular, the third is not. Hence again $|\mathbf{N}_{SU_3(q)}(T_2) : T_2| = 2$ follows. In all other cases the normalizer of T must leave V_1 invariant. Since V_2 is the unique T-invariant complement of V_1, V_2 is also invariant for $\mathbf{N}_G(T)$. Hence we have $\mathbf{N}_G(T) = \left(\mathbf{N}_{\widetilde{G}(V_1)}(C_1) \times \mathbf{N}_{\widetilde{G}(V_2)}(C_2)\right) \cap G$.

Let $m = \dim V_1$. Let us consider first the case when C_1 acts irreducibly on V_1. Then the linear span $[C_1]$ of C_1 in the ring of matrices over $\mathrm{GF}(q)$ (or over $\mathrm{GF}(q^2)$ in the unitary case) is isomorphic to the field $\mathrm{GF}(q^m)$ (or $\mathrm{GF}(q^{2m})$). Every element of the normalizer induces not only a group automorphism of C_1 but at the same time a relative field automorphism of $[C_1]$ as well. Hence we have

$$|\mathbf{N}_{\widetilde{G}(V_1)}(C_1) : C_1| = |\mathbf{N}_{\widetilde{G}(V_1)}(C_1) : \mathbf{C}_{\widetilde{G}(V_1)}(C_1)| \leqslant m.$$

In the other case, when C_1 has two minimal invariant subspaces $V_{11} \oplus V_{12} = V_1$, the existence of elements with simple spectrum in C_1 implies that the representations of C_1 on V_{11} and on V_{12} are not equivalent. Hence an element of $\mathbf{N}_{\widetilde{G}(V_1)}(C_1)$ either leaves both subspaces invariant or interchanges them. If it leaves them invariant then its action on V_{11} uniquely determines its action on V_{12}, so we obtain

$$|\mathbf{N}_{\widetilde{G}(V_1)}(C_1) : C_1| \leqslant 2 \cdot |\mathbf{N}_{\widetilde{G}(V_{11})}(C_1\,|_{V_{11}}) : C_1\,|_{V_{11}}\,| \leqslant 2 \cdot \frac{m}{2} = m,$$

in this case as well.

Now we look at the kernel of the projection of $\mathbf{N}_G(T)$ to $\mathbf{N}_{\widetilde{G}(V_1)}(C_1)$. If $\dim V_2 = 1$, then it is trivial, since every element of G has determinant 1. If $\dim V_2 = 2$, then the kernel is contained in $\Omega_2^\varepsilon(q) \leqslant C_2$. So in any case we get

$$|\mathbf{N}_G(T) : T| \leqslant |\mathbf{N}_{\widetilde{G}(V_1)}(C_1) : C_1| \leqslant m \leqslant n. \qquad \square$$

LEMMA 4.8. *For each group S in Table III, the orders of $|T_1|$ and $|T_2|$ are relatively prime.*

Proof. Observe that $\big((q^n-1)/(q-1), q^{n-1}-1\big)$ divides $(q^n-1, q^{n-1}-1) = q-1$, hence

$$\big((q^n-1)/(q-1), q^{n-1}-1\big) = (q^{n-1}+q^{n-2}+\cdots+q+1, q-1) = (n, q-1).$$

Substituting $-q$ for q we obtain for n odd: $\big((q^n+1)/(q+1), q^{n-1}-1\big) = (n, q+1)$; for n even: $\big((q^n-1)/(q+1), q^{n-1}+1\big) = (n, q+1)$. Obviously, $(q^k+1, q^k-1) = (2, q^k-1) = (2, q-1)$. Furthermore, we have $(q^k+1, q^{k-1}+1) = (q^k+1, q-1) = (2, q-1)$. If k is odd, replacing q by $-q$ we obtain $(q^k-1, q^{k-1}+1) = (q^k-1, q+1) = (2, q+1)$.

These formulae imply that the tori T_1 and T_2 in S have coprime orders. This is obvious, except for the even dimensional orthogonal groups. In that case we see immediately that $(|T_1|, |T_2|)$ is a power of 2. If q is even, then both $|T_1|$ and $|T_2|$ are odd, so we are done. So let q be odd. For $P\Omega_n^-(q)$ and for $P\Omega_n^+(q)$ with $n \equiv 2 \pmod 4$ we have $(|T_1|, |T_2|) = \frac{1}{d}\big(q^{n/2}-\varepsilon, (q^{n/2-1}+1)(q+\varepsilon)\big)$. Here the g. c. d. $\big(q^{n/2}-\varepsilon, (q^{n/2-1}+1)(q+\varepsilon)\big)$ divides 4, hence $(|T_1|, |T_2|) = \frac{1}{d}(4, q^{n/2}-\varepsilon) = 1$. Finally, for $P\Omega_n^+(q)$ with $n \equiv 0 \pmod 4$ we have that $d = (2, q-1)^2 = 4$. If $q \equiv 1 \pmod 4$, then T_2 has odd order, if $q \equiv 3 \pmod 4$, then T_1. So in all cases $(|T_1|, |T_2|) = 1$. $\square$

Proof of Theorem 4.1. The coprimality was proved in the previous lemma. We have to give a lower bound for the cardinality of $A_i := T_i^S$. We may work in G instead of S, since each T_i contains $\mathbf{Z}(G)$.

We apply Proposition 1.11. We have that $T_i^* \subseteq \Gamma(T_i)$ by Lemma 4.6, $|\mathbf{N}_G(T_i) : T_i| \leqslant n$ by Lemma 4.7, and $|T_i^*|/|T_i| \geqslant 1/2$ by Lemma 4.5 (and also for $T_2 \leqslant SL_2(q)$

by its particular definition). We conclude, by Proposition 1.12, that the proportion of p-regular elements in S is $> 1/(2n)$. □

All tori but the ones constructed for $P\Omega_n^+(q)$ with $4 \mid n$ are cyclic. Unfortunately, it is not always possible to find two cyclic tori of coprime orders as the following result shows.

PROPOSITION 4.9. *Let $n \geqslant 8$ be a power of 2 and $q \geqslant 5$ be an odd prime power. Then the order of every cyclic maximal torus in $P\Omega_n^+(q)$ is divisible by $(q^2-1)/4$.*

Proof. Let $G = SO_n^+(q)$ then every maximal torus in G has the form $T = \prod C_O^{\epsilon(i)}(2k_i, q)$ with $\sum 2k_i = n$ and an even number of indices i for which $\epsilon(i) = 1$. We have $|T| = \prod(q^{k_i} - (-1)^{\epsilon(i)})$ and $|(T \cap \Omega_n^+(q))/\mathbf{Z}(\Omega_n^+(q))| = |T|/4$. Suppose that $q^2 - 1$ does not divide $|T|$. Then we want to show that $T_0 = (T \cap \Omega_n^+(q))/\mathbf{Z}(\Omega_n^+(q))$ is not cyclic. Clearly, the number of direct factors of T cannot exceed 3, otherwise the Sylow 2-subgroup of T has at least four direct factors, so T_0 cannot be cyclic. We have to consider the following cases:

$T = C_O^2(n, q)$;

$T = C_O^2(2k, q) \times C_O^2(2l, q)$ with $k + l = n/2$;

$T = C_O^1(2k, q) \times C_O^1(2l, q)$ with $k + l = n/2$;

$T = C_O^2(2k, q) \times C_O^2(2l, q) \times C_O^2(2m, q)$ with $k + l + m = n/2$;

$T = C_O^1(2k, q) \times C_O^1(2l, q) \times C_O^2(2m, q)$ with $k + l + m = n/2$

of order $q^{n/2} - 1$, $(q^k - 1)(q^l - 1)$, $(q^k + 1)(q^l + 1)$, $(q^k - 1)(q^l - 1)(q^m - 1)$, $(q^k + 1)(q^l + 1)(q^m - 1)$, respectively. Clearly, $q^2 - 1 \mid q^{n/2} - 1$. Since $q - 1 \geqslant 4$ divides both $q^k - 1$ and $q^l - 1$, the second group cannot give rise to a cyclic group. In the third case let $k = 2^r k_1$ with $r \geqslant 0$, k_1 odd. Then we have $l = 2^r l_1$ with l_1 odd, as $k_1 + l_1 = n/2^r$ is a power of 2. So $q^{2^r} + 1$ divides both $q^k + 1$ and $q^l + 1$ in this case, hence the group is not cyclic. In the last two cases if m is even then $q^2 - 1 \mid q^m - 1$. So let m be odd. In the fourth case one of k and l, say, k is even, and so $q^2 - 1 \mid q^k - 1$. In the last case one of them, say, l is odd, hence $q + 1 \mid q^l + 1$ and $q - 1 \mid q^m - 1$. □

5. *The sporadic groups*

We handle the sporadic groups by a method analogous to finding sharp tori in the case of exceptional groups of Lie type. Using the ATLAS [**Co**] we observe the following fact.

PROPOSITION 5.1. *For every sporadic simple group S there exists at least one prime r such that the Sylow r-subgroups of S are self-centralizing of order r.*

Table VII gives the appropriate prime divisors r. Notice that the largest prime divisor of $|S|$ always has this property. In parentheses we give the number of conjugacy classes of elements of order r in S.

Table VII: Prime divisors of the orders of sporadic groups satisfying Prop. 5.1

S	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}
r	5(1), 11(2)	11(2)	5(1), 7(2), 11(2)	11(2), 23(2)	11(1), 23(2)

S	J_1	J_2	J_3	J_4
r	7(1), 11(1), 19(3)	7(1)	17(2), 19(2)	23(1), 29(1), 31(3), 37(3), 43(3)

S	HS	McL	Suz	Ly	He	Ru
r	7(1), 11(2)	11(2)	11(1), 13(2)	31(5), 37(2), 67(3)	17(2)	29(2)

S	$O'N$	Co_3	Co_2	Co_1	Fi_{22}	Fi_{23}
r	11(1), 19(3), 31(2)	23(2)	11(1), 23(2)	23(2)	13(2)	17(1), 23(2)

S	Fi'_{24}	Th	HN	B	M
r	17(1), 23(2), 29(2)	19(1), 31(2)	19(2)	31(2), 47(2)	41(1), 59(2), 71(2)

The same is true for the Tits group ${}^2F_4(2)'$ with $r = 13$ (and there are 2 conjugacy classes of elements of order 13). However, it is not a general property of finite simple groups, as for example $PSL_2(49)$ of order $2^4 \cdot 3 \cdot 5^2 \cdot 7^2$ has no self-centralizing Sylow 3-subgroup.

Of course, one could tabulate the proportion of p-regular elements for all pairs (S, p), but we are content with drawing the following conclusion from Proposition 5.1:

COROLLARY 5.2. *(Theorem 1.1 (d)) For every sporadic simple group S and every prime number p, the proportion of p-regular elements is greater than $2/29$.*

Proof. If $r = p$ satisfies the statement of Proposition 5.1, then every element of S is either of order p or p-regular. If we denote by c the number of conjugacy classes of elements of order p, then we obtain that the proportion of p-regular elements is $1 - \frac{c}{p} \geqslant \frac{5}{7}$, by considering Table VII. If p does not satisfy Proposition 5.1, then let $r_1, \ldots, r_n$ be the primes which do satisfy it, and let c_i $(i = 1, \ldots, n)$ be the number of conjugacy classes of elements of order r_i in S. Since any element of order r_i is p-regular now, we obtain that the proportion of p-regular elements is greater than $\sum c_i/r_i \geqslant 2/29$, the identity element making the inequality strict. □

REMARK 5.3. The Atlas lists both the orders of elements in each conjugacy class and the sizes of the conjugacy classes, so improving our lower bound and obtaining more specific information is a matter of arithmetic. Ross Lawther has done this calculation and found that the worst case occurs with $p = 2$ and the Rudvalis group; the proportion of elements of odd order is ≈ 0.195. If we include the Tits group ${}^2F_4(2)'$ among the sporadic groups (as we do in Theorem 1.1 and Corollary 5.2), it will be the champion with $p = 2$: the proportion of elements of odd order is ≈ 0.175. For other primes, the Tits group produces proportions greater than $1/2$. So the quantity ≈ 0.175 replaces our $2/29 \approx 0.069$ lower bound, valid for all pairs (S, p) where S is a sporadic simple group and p is a prime.

Lawther [**La**] found that in most cases, the proportion of p-regular elements was greater than $1/2$. Here we reproduce his list of 24 exceptions (S, p) in increasing

order of the proportion of p-regular elements. (The proportions are rounded to 3 decimals.)

$(Ti, 2)$ 0.175, $(Ru, 2)$ 0.195, $(Th, 3)$ 0.269, $(Co_1, 2)$ 0.279, $(Co_2, 2)$ 0.316, $(M_{12}, 2)$ 0.328, $(J_2, 2)$ 0.352, $(Fi_{23}, 2)$ 0.357, $(B, 2)$ 0.359, $(Co_3, 2)$ 0.372, $(M, 2)$ 0.377, $(O'N, 2)$ 0.385, $(Fi_{22}, 2)$ 0.398, $(He, 2)$ 0.403, $(Th, 2)$ 0.428, $(Fi'_{24}, 3)$ 0.438, $(HS, 2)$ 0.439, $(McL, 2)$ 0.441, $(Co_1, 3)$ 0.446, $(HN, 2)$ 0.448, $(HN, 5)$ 0.471, $(M_{24}, 2)$ 0.474, $(Suz, 3)$ 0.478, $(Ly, 2)$ 0.488.

6. *Upper bounds*

As pointed out by the anonymous referee, it is natural to ask how good our lower bounds stated in Theorem 1.1 are. Of course the constants in the general lower bounds can be improved for most classes; in most cases our proofs indicate, how. We commented on the sporadic groups in Remark 5.3.

Our main concern in this section is the asymptotic tightness of the lower bounds.

As observed in Remark 2.2, for the alternating groups A_n, for every fixed p, the proportion of p-regular elements is $\Theta(n^{-1/p})$. In particular, the $\Omega(1/\sqrt{n})$ lower bound is tight for $p = 2$.

Regarding part (b) of Theorem 1.1 (classical groups), the question arises whether the lower bound $\Omega(1/n)$ could be replaced by a positive absolute constant. We shall see that this is not the case; in fact, the best lower bound one can hope for (in terms of the parameter n alone) is of the form $c/\sqrt{n}$. Indeed, for every $n \geqslant 2$ and for an infinite sequence of values of q we give an $O(1/\sqrt{n})$ upper bound for the proportion of elements of odd order in $PSL(n, q)$.

THEOREM 6.1. *For all $n \geqslant 2$ and for all prime powers $q \equiv -1 \pmod 4$ such that $(q-1, n) \leqslant 2$, the proportion of elements of odd order in $PSL(n, q)$ is less than*

$$\frac{4}{q} + \frac{4}{\sqrt{\pi n}}.$$

First we prove a similar bound for the general linear groups.

THEOREM 6.2. *For all $n \geqslant 2$ and for all odd prime powers q, the proportion of elements of odd order in $GL(n, q)$ is less than*

$$\frac{1}{q} + \frac{1}{\sqrt{\pi n}}.$$

LEMMA 6.3. *Let $n \geqslant 2$ and let q be a prime power. Let us view the matrix algebra $M_n(q)$ as a probability space with the uniform distribution. Then there is a subset $T \subset M_n(q)$ such that*

(a) $\mathrm{Prob}(T) > 1 - 1/(q-1)$*;*

(b) if $A \in T$ then A is similar to the companion matrix of its characteristic polynomial; and

(c) if the matrix A is selected uniformly from T then the characteristic polynomial of A is uniformly distributed among the monic polynomials of degree n over $\mathrm{GF}(q)$.

Proof. Fix a nonzero vector $e_0 \in \mathrm{GF}(q)^n$. Let $A \in M_n(q)$. Let us consider the sequence $e_k = A^k e_0$ of vectors. We define the set $T \subset M_n(q)$ by saying that $A \in T$ if $e_0, \ldots, e_{n-1}$ form a basis of $\mathrm{GF}(q)^n$.

It is clear that

$$\mathrm{Prob}(T) = \prod_{i=1}^{n-1}(1 - 1/q^i) > 1 - \frac{1}{q-1}. \tag{2}$$

Moreover, with respect to this basis, A is a companion matrix. Having fixed this basis, we still have complete freedom in choosing Ae_{n-1}; this gives the last row of the matrix with respect to this basis, which also defines the coefficients of the characteristic polynomial. This implies statement (c). □

Let $T_0 = T \cap GL(n, q)$. Then $A \in T_0$ exactly if $A \in T$ and the constant term of the characteristic polynomial of A is not zero. It follows from equation (2) that

$$\mathrm{Prob}(T_0) = \mathrm{Prob}(T)(1 - 1/q) = \frac{1 - 1/q}{1 - 1/q^n}\,\mathrm{Prob}(GL(n, q)). \tag{3}$$

Next we observe that if q is odd then $A \in GL(n, q)$ has odd order if and only if all eigenvalues of A have odd multiplicative order in the algebraic closure of $\mathrm{GF}(q)$. Therefore Theorem 6.2 will follow from the next lemma.

LEMMA 6.4. *For an odd prime power q, the probability that all roots of a random polynomial of degree $n \geqslant 1$ over $\mathrm{GF}(q)$ have odd multiplicative orders is less than $1/\sqrt{\pi n}$.*

Proof. Let $\mathbb{F}$ denote the algebraic closure of $\mathrm{GF}(q)$. Irreducibility will always be understood with respect to $\mathrm{GF}(q)$. Let $P(n)$ denote the set of *monic* polynomials of degree n over $\mathrm{GF}(q)$. Among these polynomials, let $I(n)$ denote the set of those which are irreducible; $F(n)$ the set of those which have only roots of odd multiplicative orders (in particular, the constant term of such a polynomial is not zero); and $D(n) = I(n) \cap F(n)$. Note that $|P(0)| = |F(0)| = 1$ and $|I(0)| = |D(0)| = 0$.

If $z \in \mathbb{F}^\times$ has odd multiplicative order and it is a root of $f(x) \in I(n)$ then $-z$ is a root of $f(-x)$, which is also irreducible of the same degree, and $-z$ has even order. Hence $|D(n)| \leqslant |I(n)|/2$.

Applying the method of generating functions we observe that

$$\prod_{k=1}^{\infty}(1 + t^k + t^{2k} + t^{3k} + \ldots)^{|I(k)|} = \sum_{n=0}^{\infty}|P(n)|t^n = \sum_{n=0}^{\infty} q^n t^n.$$

Similarly,

$$\prod_{k=1}^{\infty}(1 + t^k + t^{2k} + t^{3k} + \ldots)^{|D(k)|} = \sum_{n=0}^{\infty}|F(n)|t^n.$$

Now $|D(k)| \leqslant |I(k)|/2$ implies that $|F(n)|$ is less than or equal to the coefficient of t^n in the power series

$$\prod_{k=1}^{\infty}(1 + t^k + t^{2k} + \ldots)^{|I(k)|/2} = \sqrt{1 + qt + q^2t^2 + \ldots} = (1 - qt)^{-1/2}.$$

This coefficient is $\binom{-1/2}{n}(-q)^n$. So the probability in question is at most $(-1)^n\binom{-1/2}{n}$ $= \binom{2n}{n}4^{-n}$. This quantity is always less than $1/\sqrt{\pi n}$ because the sequence $\sqrt{n}\binom{2n}{n}4^{-n}$ is monotone increasing and by Stirling's formula its limit is $1/\sqrt{\pi}$. □

Proof of Theorem 6.2. Let $G = GL(n,q)$ and let $R \subset G$ denote the set of matrices of odd order. Let $S \subset T_0$ consist of those matrices in T_0 of which every eigenvalue has odd multiplicative order. Then $R \subset (G \setminus T_0) \cup S$. Now we have

$$\frac{|R|}{|G|} \leqslant \frac{|G|-|T_0|}{|G|} + \frac{|S|}{|G|} = 1 - \frac{|T_0|}{|G|} + \frac{|S|}{|T|}\frac{|T|}{|T_0|}\frac{|T_0|}{|G|} \leqslant 1 - \frac{|T_0|}{|G|}\left(1 - \frac{1}{\sqrt{\pi n}}\frac{q}{q-1}\right)$$

$$= 1 - \frac{1-1/q}{1-1/q^n}\left(1 - \frac{1}{\sqrt{\pi n}}\frac{q}{q-1}\right) < 1 - \left(1-\frac{1}{q}\right)\left(1 - \frac{1}{\sqrt{\pi n}}\frac{q}{q-1}\right) = \frac{1}{q} + \frac{1}{\sqrt{\pi n}},$$

completing the proof. □

Proof of Theorem 6.1. By our assumptions $(q-1)/2$ is odd and coprime to n. Let Z denote the subgroup of index 2 in $\mathbf{Z}(GL(n,q))$. So $|Z| = (q-1)/2$; hence Z intersects $SL(n,q)$ trivially and $Z \times SL(n,q)$ has index 2 in $GL(n,q)$. Therefore, under our assumptions, the proportion of elements of odd order in $SL(n,q)$ is the same as in $Z \times SL(n,q)$, which is in turn the double of that proportion in $GL(n,q)$. If n is odd, then $PSL(n,q) = SL(n,q)$. If n is even, then $SL(n,q)$ has a center of order 2. Hence in that case the number of elements of odd order in $PSL(n,q)$ is the same as in $SL(n,q)$, hence the proportion of elements of odd order is the double of that proportion in $SL(n,q)$. Thus, in all cases under consideration, the proportion of elements of odd order in $PSL(n,q)$ is at most four times as much as in $GL(n,q)$. Hence Theorem 6.1 follows from Theorem 6.2. □

7. *Appendix: Representations in cross characteristic*

In this section we indicate how to combine the results of Landazuri–Seitz [**LS**] and Feit–Tits [**FT**] and tables from Kleidman–Liebeck [**KL**] to obtain Theorem 1.17.

Proof. Let now $\lambda : H \to PGL_n(F)$ be the given faithful representation in characteristic other than r. Without loss of generality we may assume that F is algebraically closed, H is minimal in the sense that no proper subgroup of H involves S, and n is the smallest degree of a nontrivial projective representation of H over F.

Under the conditions given in the previous paragraph, [**FT**] asserts that either (i) λ factorizes through S, or (ii) $r = 2$, $S \leqslant PSp_{2\ell}(2)$, and $n = 2^\ell$ for some $\ell \geqslant 4$.

In case (ii), we conclude that $em \leqslant 2\ell$ (recall that $q = r^e$, i. e., $q = 2^e$ in this case). Therefore, $q^m = 2^{em} \leqslant 2^{2\ell} = n^2 < n^{c_1}$ and we are done.

Assume now that we are in case (i) and therefore we may assume $H = S$.

Let $m'-1$ denote the minimum dimension of projective spaces in characteristic r on which S acts nontrivially. First we note that $m = m'$ for all S with the exception of $S = PSU_{m'}(q)$, when $m = 2m'$ by our notational convention, and the further

exceptions of $S = {}^2E_6(q)$ where $m = 2m'$ and $S = {}^3D_4(q)$ where $m = 3m'$ [**KL**, Section 5.4].

We shall estimate n in terms of m'.

Landazuri and Seitz give lower bounds on n for each class of finite simple groups of Lie type. It is easy to check that $m \leqslant n$ holds with the two noted exceptions.

To prove the bound $q^m \leqslant n^{c_1}$, assume first that S is a classical simple group. A comparison of the [**LS**] estimates with the dimensions of the natural modules on which S acts projectively yields the bound $q^m \leqslant n^{c_2}$ where $c_2 = 8\log 3/\log 6 = 4.90517\cdots < c_1$. Equality holds for $S = PSU_4(3)$ ($q = 9$, $m = 4$, and, by [**LS**], $n \geqslant 6$; and $9^4 = 6^{c_2}$). This completes the proof for classical S.

For exceptional groups S, a comparison of the Landazuri–Seitz estimates on n with the dimensions of modules given by Kleidman–Liebeck [**KL**], Table 5.4.C (p. 200) yields the bound $q^{m'} \leqslant n^{c_1}$; equality holds for $S = E_8(2)$ ($q = 2$, $m' = 248$; and, by [**LS**], $n \geqslant q^{27}(q^2-1) = 2^{27}\cdot 3$; and $2^{248} = (2^{27}\cdot 3)^{c_1}$). This settles all cases when $m = m'$. Next we consider the exceptions of $S = {}^2E_6(q)$ and $S = {}^3D_4(q)$.

For $S = {}^2E_6(q)$ we obtain $q^{m'} \leqslant n^{c_3}$ where $c_3 = 27/(9 + \log 3/\log 2) = 2.55078\ldots$ (equality holds for $q = 2$). Now, $m \leqslant 2m'$, therefore $q^m \leqslant n^{2c_3} < n^{c_1}$.

For $S = {}^3D_4(q)$ we obtain $q^{m'} \leqslant n^{c_4}$ where $c_4 = 8/(3+\log 3/\log 2) = 1.74483\ldots$ (equality holds for $q = 2$). Now, $m \leqslant 3m'$, therefore $q^m \leqslant n^{3c_4} < n^{c_1}$. □

8. *Open questions*

Let X be the symbol which denotes one of the classes of classical simple groups; and let $X_n(q)$ denote the member of this class that acts naturally on a projective space of dimension $n-1$ over GF(q). Let p be a prime, and let $\rho(p, X, n, q)$ denote the proportion of p-regular elements in $X_n(q)$. By part (b) of Theorem 1.1, we have

$$\rho(p, X, n, q) > 1/(2n) \tag{4}$$

for all p, X, q. On the other hand, from Theorem 6.1 we know that if $X_n(q) = PSL(n, q)$ then

$$\rho(2, X, n, q) < 3/\sqrt{n} \tag{5}$$

holds for every n for infinitely many values of q. The question is to close this quadratic gap. More precisely, let

$$\alpha(p, X, q) = \limsup_{n\to\infty} \frac{-\log \rho(p, X, n, q)}{\log n}. \tag{6}$$

Let $\alpha = \sup_{p,X,q} \alpha(p, X, q)$. Then we know that

$$1/2 \leqslant \alpha \leqslant 1. \tag{7}$$

The lower bound follows from inequality (5); the upper bound from inequality (4). Our main question is to determine the exact value of α (or reduce the gap).

The values

$$\alpha(p, X) = \inf_q \alpha(p, X, q) \tag{8}$$

are also of interest for specific choices of the prime p and the class X. The upper bound of $\alpha(p, X) \leqslant 1$ always holds. Generalizing the method of Section 6 one can show that for every p,

$$\alpha(p, PSL) \geqslant 1/p. \tag{9}$$

Question: is $\inf_p \alpha(p, PSL) = 0$?

Of special interest is the quantity $\alpha(2, PSL)$; in this case we have

$$1/2 \leqslant \alpha(2, PSL) \leqslant 1 \tag{10}$$

for the same reason as inequality (7). The question again is to close or reduce this gap.

We expect that $\alpha(2, X) \geqslant 1/2$ holds for all classes X of classical simple groups.

Another direction of study would fix q; a special case of interest is the value $\alpha(2, PSL, 3)$. Here we have no lower bound; the question is to prove or disprove that $\alpha(2, PSL, 3) > 0$. In other words, can a positive ϵ be found such that the proportion of elements of odd order in $PSL(n, 3)$ is (at most) $O(n^{-\epsilon})$?

References

BB. L. Babai and R. Beals, *A polynomial-time theory of black box groups I*, in **Groups St Andrews 1997 in Bath, I** (C. M. Campbell *et al.*, eds.), pp. 30–64, London Math. Soc. Lecture Note Ser. Vol. 260, Cambridge University Press, Cambridge, 1999.

BS. L. Babai and A. Shalev, *Recognizing simplicity of black-box groups and the frequency of p-sigular elements in affine groups*, in **Groups and Computation, III** (W. M. Kantor and Á. Seress, eds.), 39–62, Ohio State Univ. Math. Res. Inst. Publ., Vol. 8, de Gruyter, Berlin, 2001.

BL+. R. Beals, C. Leedham–Green, A. C. Niemeyer, C. E. Praeger, and Á. Seress, *Permutations with restricted cycle structure and an algorithmic application*. **Combinatorics, Probability and Computing** 11 (2002), 446–464.

Ca. R. Carter, *Conjugacy classes in the Weyl group*, in **Seminar on algebraic groups and related finite groups** (A. Borel *et al.*, eds.), pp. 297–318. Lecture Notes in Mathematics 131, Springer, Berlin, 1970.

Co. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, **ATLAS of Finite Groups**, Clarendon Press, Oxford, 1985.

ET. P. Erdős and P. Turán, *On some problems of a statistical group theory, II*, **Acta Math. Acad. Sci. Hungar.** 18 (1967), 151–163.

FT. W. Feit and J. Tits, *Projective representations of minimum degree of group extensions*, **Canad. J. Math.** 30 (1978), 1092–1102.

FNP. J. Fulman, P. M. Neumann and C. E. Praeger, *A Generating Function Approach to the Enumeration of Matrices in Groups over Finite Fields*, **Memoires of the A. M. S.** Vol. 176, No. 830, 2005.

Ga. P. C. Gager, *Maximal tori in finite groups of Lie type*, Ph.D. Thesis, University of Warwick, 1973.

GL. R. M. Guralnick and F. Lübeck, *On p-singular elements in Chevalley groups in characteristic p*, in **Groups and Computation, III** (W. M. Kantor and Á. Seress, eds.), 169–182, Ohio State Univ. Math. Res. Inst. Publ., Vol. 8, de Gruyter, Berlin, 2001.

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

IKS. 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.

KS. W. M. Kantor and Á. Seress, *Prime power graphs for groups of Lie type*, **J. Algebra** 247 (2002), 370–434.

KL. 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.

La. R. Lawther, personal communication, April 2008.

LS. V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, **J. Algebra** 32 (1974), 418–443.

LSS. M. W. Liebeck, J. Saxl, and G. M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, **Proc. London Math. Soc.** 65 (1992), 297–325.

MSW. G. Malle, J. Saxl, and T. Weigel, *Generation of classical groups*, **Geom. Dedicata** 49 (1994), 85–116.

Ma. A. Maróti, *Symmetric functions, generalized blocks and permutations with restricted cycle structure*, **European J. Combin.** 28 (2007), 942–963.

NeP. P. M. Neumann and C. E. Praeger, *Cyclic matrices in classical groups over finite fields*, **J. Algebra** 234 (2000), 367–418.

NP1. A. C. Niemeyer and C. E. Praeger, *A recognition algorithm for classical groups over finite fields*, **Proc. London Math. Soc.** 77 (1998), 117–169.

NP2. A. C. Niemeyer and C. E. Praeger, *A recognition algorithm for non-generic classical groups over finite fields*, **J. Austral. Math. Soc. (Series A)** 67 (1999), 223–253.

SS. T. A. Springer and R. Steinberg, *Conjugacy classes*, in **Seminar on algebraic groups and related finite groups** (A. Borel *et al.*, eds.), pp. 167–266. Lecture Notes in Mathematics 131, Springer, Berlin, 1970.

Ta. D. E. Taylor, **The Geometry of the Classical Groups**, Sigma Series in Pure Math. Vol. 9, Heldermann Verlag, Berlin, 1992.

Zs. K. Zsigmondy, *Zur Theorie der Potenzreste*, **Monatsh. Math. Phys.** 3 (1892), 265–284.

László Babai `laci@cs.tod.uchicago.tod.edu`
`http://people.cs.uchicago.edu/∼laci`

University of Chicago

On the number of p-regular elements in finite simple groups

Péter P. Pálfy ppp@renyi.tod.hu

Rényi Institute and
Eötvös University, Budapest

Jan Saxl J.Saxl@dpmms.tod.cam.tod.ac.tod.uk

Gonville and Caius College, Cambridge