ARTICLE IN PRESS YJABR:18010

Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

p-Regular conjugacy classes and p-rational irreducible characters ☆

Nguyen Ngoc Hung [a], Attila Maróti [b,*]

[a] Department of Mathematics, The University of Akron, Akron, OH 44325, USA
[b] Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

ARTICLE INFO

Article history:
Received 21 July 2020
Available online xxxx
Communicated by Robert Guralnick

To the memory of Jan Saxl

MSC:
primary 20E45, 20C15, 20D05, 20D06, 20D10

Keywords:
Finite groups
Conjugacy classes
p-Regular classes
Brauer characters
p-Rational characters

ABSTRACT

Let G be a finite group of order divisible by a prime p. The number of conjugacy classes of p-elements and p-regular elements of G is at least $2\sqrt{p-1}$. Also, the number of p-rational and p'-rational irreducible characters of G is at least $2\sqrt{p-1}$. Along the way we prove a uniform lower bound for the number of p-regular classes in a finite simple group of Lie type in terms of its rank and size of the underlying field.

☆ The work of the second author on the project leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 741420). The second author was also supported by the National Research Development and Innovation Office (NKFIH) Grant No. K132951 and Grant No. K115799.

* Corresponding author.
E-mail addresses: hungnguyen@uakron.edu (N.N. Hung), maroti.attila@renyi.hu (A. Maróti).

https://doi.org/10.1016/j.jalgebra.2021.02.007

1. Introduction

The number $k(G)$ of conjugacy classes of a finite group G, which is equal to the number of complex irreducible characters of G, is a fundamental invariant in group theory and representation theory. For instance, Higman's famous conjecture is to show that if p is a prime and G is a Sylow p-subgroup of the general linear group $\mathrm{GL}_n(q)$, then $k(G)$ is a polynomial in q with integer coefficients. The celebrated $k(GV)$ theorem states that if V is a finite, faithful, coprime G-module for a finite group G then the number $k(GV)$ of conjugacy classes of the semidirect product GV is at most $|V|$.

Lower bounds for the number of conjugacy classes of a finite group have a long history. Landau [28], in response to a question of Frobenius, proved in 1903 that for a given k there are only finitely many groups having k conjugacy classes. This result may be translated to a lower bound on the number of conjugacy classes of a finite group G only in terms of the order of G. Problem 3 of Brauer's list of problems [6] was to give a substantially better lower bound for $k(G)$. This was solved by Pyber [36] and his bound was later slightly improved by several authors, see [3,4,27]. In general it is not known whether there is a universal constant $c > 0$ such that for every finite group G we have $k(G) > c \cdot \log |G|$.

Bounding $k(G)$ only in terms of a prime divisor p of $|G|$ is another fundamental problem. It is related to Problem 21 of Brauer [6] and a conjecture of Héthelyi and Külshammer [19] that for any p-block B of any finite group G the number $k(B)$ of complex irreducible characters in B is 1 or is at least $2\sqrt{p-1}$. As observed by Pyber, work of Brauer [5] implies that $k(G) \geq 2\sqrt{p-1}$ for G a finite group whose order is divisible by a prime p but not by p^2. Since then, this bound had been conjectured to be true for all groups G and all primes p dividing $|G|$.

Proving $k(G) \geq 2\sqrt{p-1}$ for all G and p has turned out to be a hard problem. Building on a series of relevant works by Héthelyi-Külshammer [19,20], Malle [30], Keller [26], and Héthelyi-Horváth-Keller-Maróti [21], the conjecture was finally confirmed in [32].

One of the purposes of this paper is to obtain a p-modular analog of the bound $k(G) \geq 2\sqrt{p-1}$; that is, to obtain a bound for the number of p-regular classes, which is also the number of irreducible p-modular representations, of G. On the other hand, we observe that since the class number $k(G)$ is a global characteristic of G while the bound $2\sqrt{p-1}$ depends only on p, it is natural to expect that the same bound would hold for a certain subset of conjugacy classes or irreducible characters that are defined locally in terms of p. We confirm this expectation from both perspectives: classes and characters, by considering orders of group elements and fields of character values.

An element of a finite group G is called p-regular if it has order coprime to p. Throughout let $k_{p'}(G)$ denote the number of conjugacy classes of p-regular elements in G and let $k_p(G)$ denote the number of conjugacy classes of *non-trivial* p-elements in G.

Theorem 1.1. *If G is a finite group and p is a prime dividing the order of G, then*

$$k_p(G) + k_{p'}(G) \geq 2\sqrt{p-1}$$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

with equality if and only if $\sqrt{p-1}$ *is an integer,* $G = C_p \rtimes C_{\sqrt{p-1}}$ *and* $\mathbf{C}_G(C_p) = C_p$.

Let $\mathrm{IBr}_p(G)$ denote the set of irreducible p-modular representations of G. As $|\mathrm{IBr}_p(G)| = k_{p'}(G)$, Theorem 1.1 provides a somewhat unexpected lower bound for the number of irreducible p-Brauer characters, namely $|\mathrm{IBr}_p(G)| \geq 2\sqrt{p-1} - k_p(G)$, and therefore, it can be viewed as a modular version of the bound $k(G) \geq 2\sqrt{p-1}$ for the number of ordinary irreducible characters of G.

We make the bound $|\mathrm{IBr}_p(G)| \geq 2\sqrt{p-1} - k_p(G)$ more explicit in the case when G is non-p-solvable.

Theorem 1.2. *Let p be a prime. Let G be a non-p-solvable finite group. The number $|\mathrm{IBr}_p(G)|$ of irreducible p-Brauer characters of G is larger than $2\sqrt{p-1}$ unless possibly if $p \leq 257$. In any case, $|\mathrm{IBr}_p(G)| > \sqrt{p-1}$.*

Next we turn to fields of character values. For a positive integer n, let $\mathbb{Q}_n$ denote the cyclotomic field extending rational numbers $\mathbb{Q}$ by a primitive nth root of unity. We say that a character χ is p-rational if there is $n \in \mathbb{N}$ coprime to p such that $\chi(g) \in \mathbb{Q}_n$ for all $g \in G$. Also, χ is p'-rational if $\chi(g) \in \mathbb{Q}_{|G|_p}$ for all $g \in G$. Let $\mathrm{Irr}_{\mathrm{p-rat}}(G)$ and $\mathrm{Irr}_{\mathrm{p'-rat}}(G)$ respectively denote the sets of p-rational irreducible and p'-rational irreducible characters of G. Note that $\mathrm{Irr}_{\mathrm{p-rat}}(G) \cap \mathrm{Irr}_{\mathrm{p'-rat}}(G)$ is equal to $\mathrm{Irr}_{\mathbb{Q}}(G)$, the set of rational irreducible characters of G.

Theorem 1.3. *If G is a finite group and p is a prime dividing the order of G, then*

$$|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| \geq 2\sqrt{p-1}$$

with equality if and only if $\sqrt{p-1}$ *is an integer,* $G = C_p \rtimes C_{\sqrt{p-1}}$ *and* $\mathbf{C}_G(C_p) = C_p$.

Theorems 1.1 and 1.3 show that, in groups of order divisible by a prime p, there is a correlation between $k_p(G)$ and $k_{p'}(G)$ as well as $|\mathrm{Irr}_{\mathrm{p-rat}}(G)|$ and $|\mathrm{Irr}_{\mathrm{p'-rat}}(G)|$: if one is small, the other must be large (compared to p, of course). In the minimal situations where one number is minimal/small, the bound indeed could be improved. We plan to address this at another time.

On the way to the proofs of Theorems 1.1, 1.2 and 1.3, we have to bound the number of p-regular classes in finite simple groups. The following uniform bound for simple groups of Lie type is of independent interest and might be useful in other applications.

Theorem 1.4. *If S is a simple group of Lie type defined over the field of q elements with r the rank of the ambient algebraic group and p is any prime, then*

$$k_{p'}(S) > \frac{q^r}{17r^2}.$$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Better and more refined bounds for different types and different p are given in Sections 3, 4 and 5. We remark that the problem of bounding the class number (both upper and lower bounds) of finite groups of Lie type has been well studied, for instance in the influential work of Fulman and Guralnick [14]. To provide a relative comparison between $k_{p'}(S)$ and $k(S)$, we note that the best general lower bound for $k(S)$ is q^r/d, where d is the order of the group of diagonal automorphisms of S.

Theorems 1.1, 1.2, and 1.3 are proved in Sections 7, 8, and 9, respectively. In Sections 2, 3, 4 and 5 we prove various bounds for the number of p-regular and p'-regular classes in finite nonabelian simple groups S, as well as the number of $\mathrm{Aut}(S)$-orbits on those classes. Finally, Theorem 1.4 is proved in Section 6.

2. Orbits of p-regular and p'-regular classes of simple groups

Let p be a prime and let S be a nonabelian finite simple group. Recall that an element is p-regular in S if it has order coprime to p. We denote the set of p-regular elements in S by $S_{p'}$, the set of p-regular conjugacy classes in S by $\mathrm{Cl}_{p'}(S)$, and the number of p-regular conjugacy classes in S by $k_{p'}(S)$. We denote the set of *non-trivial* p-elements in S by S_p, the set of all conjugacy classes in S contained in S_p by $\mathrm{Cl}_p(S)$, and the number of conjugacy classes in S contained in $\mathrm{Cl}_p(S)$ by $k_p(S)$. The classes in $\mathrm{Cl}_p(S)$ are sometimes referred to as p'-regular classes. When a group G acts on a set X, we use $n(G, X)$ to denote the number of G-orbits on X.

To prove our main results we need to bound the number of $\mathrm{Aut}(S)$-orbits on p-regular and p'-regular classes of S for all nonabelian simple groups S, as presented in the following theorem. We will prove it in this and the next three sections.

Theorem 2.1. *Let S be a nonabelian finite simple group and let p be a prime divisor of $|S|$. We have*

(i) *The number of $\mathrm{Aut}(S)$-orbits on the set $\mathrm{Cl}_{p'}(S) \cup \mathrm{Cl}_p(S)$ is larger than $2\sqrt{p-1}$ except if (S, p) is equal to $(\mathsf{A}_5, 5)$ or to $(\mathrm{PSL}_2(16)), 17)$.*
(ii) *The number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S is at least $2(p-1)^{1/4}$. The equality occurs if and only if $(S, p) = (\mathrm{PSL}_2(16)), 17)$.*
(iii) *The number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S is greater than $2\sqrt{p-1}$ unless possibly when (S, p) is listed in Table 1.*

We mention an obvious consequence of Theorem 2.1(iii) that will be needed in the proof of Theorem 1.2.

Corollary 2.2. *Let S be a nonabelian finite simple group and let p be a prime divisor of $|S|$. Then the number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S is greater than $\sqrt{p-1}$.*

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Table 1
Possible exceptions for the bound $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$.

S	p	$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$
A_5	5	3
$\mathrm{PSL}_2(7)$	7	4
A_6	5	4
$\mathrm{PSL}_2(8)$	7	4
$\mathrm{PSL}_2(11)$	11	6
$\mathrm{PSL}_2(16)$	17	5
$\mathrm{PSL}_2(27)$	13	5
$\mathrm{PSL}_2(32)$	11	6
$\mathrm{PSL}_2(32)$	31	6
$\mathrm{PSL}_2(81)$	41	10
$\mathrm{PSL}_2(128)$	43	12
$\mathrm{PSL}_2(128)$	127	12
$\mathrm{PSL}_2(243)$	61	15
$\mathrm{PSL}_2(256)$	257	21
$\mathrm{PSL}_3(8)$	73	13
$\mathrm{PSU}_3(16)$	241	≥ 27
${}^2B_2(8)$	13	6
${}^2B_2(32)$	31	8
${}^2B_2(32)$	41	9
${}^2B_2(128)$	113	≥ 19
${}^2B_2(128)$	127	≥ 14
$\Omega_8^-(4)$	257	≥ 32

2.1. Some generalities

Observe that any nonabelian finite simple group has order divisible by at least three distinct primes by Burnside's Theorem. It immediately follows that

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 3$$

and so Theorem 2.1 is true for $p = 2$ and $p = 3$. Thus we may assume in this and the following sections that $p \geq 5$.

Lemma 2.3. *Theorem 2.1 is true for S a sporadic simple group, the Tits group, and groups of Lie type of rank $r \geq 3$ in characteristic $p \geq 5$.*

Proof. The statement follows for S a sporadic simple group or S the Tits group using [8,15]. Assume that S is of Lie type of rank $r \geq 3$ in characteristic p. Let S be of the form $G/\mathbf{Z}(G)$, where $G = \mathcal{G}^F$ is the set of fixed points of a simple algebraic group $\mathcal{G}$ of simply connected type defined in characteristic p, under a Frobenius endomorphism F. By [7, Theorem 3.7.6], the number of semisimple classes of G is q^r, where q is the size of the underlying field of $\mathcal{G}$ and r is the rank of $\mathcal{G}$. Therefore,

$$k_{p'}(S) \geq \frac{k_{p'}(G)}{k_{p'}(\mathbf{Z}(G))} \geq \frac{q^r}{|\mathbf{Z}(G)|} = \frac{q^r}{d},$$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

where d is the order of the group of diagonal automorphisms of S. Here the first inequality follows from [14, Lemma 2.3]. It follows that

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{q^r}{d \cdot |\mathrm{Out}(S)|}.$$

To prove the lemma, it is sufficient to show that $q^r/(d|\mathrm{Out}(S)|) > 2\sqrt{p-1}$. This turns out to be true for all S and relevant values of p, q, and r. □

The next result is essential in our proofs as it helps to reduce from a classical group to one of smaller rank. From now on q is always a prime power ℓ^f, where ℓ is a prime and f is a positive integer.

Let π be either of the symbols p or p'. We denote the number of $\mathrm{Aut}(S)$-orbits on the set $\mathrm{Cl}_\pi(S)$ by $n(\mathrm{Aut}(S), \mathrm{Cl}_\pi(S))$.

Lemma 2.4. *If S and T are (non-abelian) finite simple groups such that*

$$(S, T) \in \{(\mathsf{A}_n, \mathsf{A}_{n-1}), (\mathrm{PSL}_n(q), \mathrm{PSL}_{n-1}(q)), (\mathrm{PSU}_n(q), \mathrm{PSU}_{n-1}(q))\}$$

or $(S, T) = (\mathrm{PSp}_{2n}(q), \mathrm{PSp}_{2n-2}(q))$ with q odd, then

$$n(\mathrm{Aut}(S), \mathrm{Cl}_\pi(S)) \geq n(\mathrm{Aut}(T), \mathrm{Cl}_\pi(T)).$$

Proof. Let $(S, T) = (\mathsf{A}_n, \mathsf{A}_{n-1})$. Observe that $n \geq 6$ by assumption. The group T may be considered as a point-stabilizer in S. Note that $\mathrm{Aut}(\mathsf{A}_m) = \mathsf{S}_m$ for every integer m at least 5 and different from 6. Assume that $n \geq 8$. In this case $n(\mathrm{Aut}(S), \mathrm{Cl}_\pi(S))$ and $n(\mathrm{Aut}(T), \mathrm{Cl}_\pi(T))$ are equal to the number of elements in S_π and T_π of different cycle shapes. The desired bound follows since T_π is contained in S_π. Assume that $n \in \{6, 7\}$. The group $\mathrm{Aut}(\mathsf{A}_6)$ contains S_6 as a subgroup of index 2. Since $p \geq 5$ and since $\mathrm{Aut}(\mathsf{A}_6)$ fuses the two conjugacy classes of A_6 both consisting of elements of prime order 3, we see that $n(\mathrm{Aut}(\mathsf{A}_6), \mathrm{Cl}_p(\mathsf{A}_6))$ is equal to the number of possible cycle shapes of non-trivial p-elements in A_6 and $n(\mathrm{Aut}(\mathsf{A}_6), \mathrm{Cl}_{p'}(\mathsf{A}_6))$ is equal to the number of possible cycle shapes of p-regular elements in A_6 minus 1. The desired bound follows for $\pi = p$ and also for $n = 7$. Let $n = 6$ and $\pi = p'$. Since $p \geq 5$ and $n = 6$, we must have $p = 5$. Finally, $n(\mathrm{Aut}(\mathsf{A}_6), \mathrm{Cl}_{5'}(\mathsf{A}_6)) = 4 > 3 = n(\mathrm{Aut}(\mathsf{A}_5), \mathrm{Cl}_{5'}(\mathsf{A}_5))$.

Observe that since T is assumed to be non-abelian and simple, $n \geq 3$ in the linear and unitary cases and $n \geq 2$ in the symplectic case.

Consider the case when both S and T are projective special linear groups.

Let V be the natural $\mathrm{GL}_n(q)$-module of dimension n defined over the field of size q. The group $\mathrm{SL}_n(q)$ acts naturally on V. Let W be a 1-dimensional subspace in V and let U be a complementary $(n-1)$-dimensional subspace in V. There is a group $\mathrm{SL}_{n-1}(q)$ which acts naturally on U and fixes W. All automorphisms of S can be described by automorphisms of $\mathrm{SL}_n(q)$ and the group $\mathrm{Out}(S)$ is isomorphic to $D_{2(n,q-1)} \times C_f$, see

[45, Section 3.3.4]. The field automorphisms and the inverse transpose automorphism of $\mathrm{SL}_n(q)$ restrict naturally to the subgroup $\mathrm{SL}_{n-1}(q)$ just defined. Moreover, by [29, Section 1], elements a and b of $\mathrm{SL}_{n-1}(q)$ lie in the same $\mathrm{GL}_n(q)$-orbit if and only if a and b are conjugate in $\mathrm{GL}_{n-1}(q)$.

Let $\mathcal{C}$ be the set of all π-elements of $\mathrm{SL}_n(q)$ which fix some 1-dimensional subspace of V and leave invariant some complementary $(n-1)$-dimensional subspace. The group $\mathrm{Aut}(\mathrm{SL}_n(q))$ leaves $\mathcal{C}$ invariant. Let the number of orbits of $\mathrm{Aut}(\mathrm{SL}_n(q))$ on $\mathcal{C}$ be denoted by N. By the previous paragraph, $N \geq n(\mathrm{Aut}(\mathrm{SL}_{n-1}(q)), \mathrm{Cl}_\pi(\mathrm{SL}_{n-1}(q)))$. Since $T = \mathrm{PSL}_{n-1}(q)$ is a factor group of $\mathrm{SL}_{n-1}(q)$ and all automorphisms of T can be described by automorphisms of $\mathrm{SL}_{n-1}(q)$, we have

$$n(\mathrm{Aut}(\mathrm{SL}_{n-1}(q)), \mathrm{Cl}_\pi(\mathrm{SL}_{n-1}(q))) \geq n(\mathrm{Aut}(T), \mathrm{Cl}_\pi(T)).$$

By taking the images in $\mathrm{PSL}_n(q)$ of the elements of $\mathcal{C}$, we see that the set of $\mathrm{Aut}(\mathrm{SL}_n(q))$-orbits of $\mathcal{C}$ can injectively be mapped into the set of $\mathrm{Aut}(\mathrm{PSL}_n(q))$-orbits on $\mathrm{Cl}_\pi(\mathrm{PSL}_n(q))$. In particular,

$$N \leq n(\mathrm{Aut}(\mathrm{PSL}_n(q)), \mathrm{Cl}_\pi(\mathrm{PSL}_n(q))) = n(\mathrm{Aut}(S), \mathrm{Cl}_\pi(S)).$$

Let S and T be projective special unitary groups.

Let V be the natural $\mathrm{GU}_n(q)$-module of dimension n defined over the field of size q^2. The module V is equipped with a non-singular conjugate-symmetric sesquilinear form f. The group $\mathrm{SU}_n(q)$ acts naturally on V. Let W be a 1-dimensional non-singular subspace in V with respect to f. Let U be the $(n-1)$-dimensional non-singular subspace of V perpendicular to W with respect to the form f. There is a subgroup $\mathrm{SU}_{n-1}(q)$ which acts naturally on U and fixes W. The automorphisms of the simple group $\mathrm{PSU}_n(q)$ are described in [45, Section 3.6.3]. All outer automorphisms of $\mathrm{PSU}_n(q)$ come from outer automorphisms of $\mathrm{SU}_n(q)$, these are diagonal automorphisms or field automorphisms. Field automorphisms preserve the subgroup $\mathrm{SU}_{n-1}(q)$. By a result of Wall [44, p. 34, 13, 2], elements a and b of $\mathrm{SU}_{n-1}(q)$ lie in the same $\mathrm{GU}_n(q)$-orbit if and only if a and b are conjugate in $\mathrm{GU}_{n-1}(q)$.

The proof can now be completed as in the linear case by replacing the groups $\mathrm{SL}_n(q)$, $\mathrm{SL}_{n-1}(q)$, $\mathrm{PSL}_{n-1}(q)$, $\mathrm{PSL}_n(q)$ by $\mathrm{SU}_n(q)$, $\mathrm{SU}_{n-1}(q)$, $\mathrm{PSU}_{n-1}(q)$, $\mathrm{PSU}_n(q)$ respectively.

Let S and T be projective symplectic groups.

Let V be the natural $\mathrm{Sp}_{2n}(q)$-module of dimension n defined over the field of size q. The module V is equipped with a non-singular alternating bilinear form f. Let W be a 2-dimensional non-singular subspace in V with respect to f. Let U be the $(2n-2)$-dimensional non-singular subspace of V perpendicular to W with respect to the form f. There is a subgroup $\mathrm{Sp}_{2n-2}(q)$ which acts naturally on U and which fixes W. The automorphisms of the simple group $\mathrm{PSp}_{2n}(q)$ are described in [45, Section 3.5.5]. All outer automorphisms of $\mathrm{PSp}_{2n}(q)$ come from outer automorphisms of $\mathrm{Sp}_{2n}(q)$ and these are diagonal automorphisms and field automorphisms since we are assuming that q is

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

odd. All outer automorphisms of $\mathrm{Sp}_{2n}(q)$ preserve the subgroup $\mathrm{Sp}_{2n-2}(q)$. By a result of Wall [44, p. 36], elements a and b of $\mathrm{Sp}_{2n-2}(q)$ lie in the same $\mathrm{Sp}_{2n}(q)$-orbit if and only if a and b are conjugate in $\mathrm{Sp}_{2n-2}(q)$. See also [13, 210, 211].

The proof can now be completed as in the linear or unitary case. $\square$

To have good estimates of $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$ and $n(\mathrm{Aut}(S), \mathrm{Cl}_p(S) \cup \mathrm{Cl}_{p'}(S))$, especially for low rank classical groups and exceptional groups, we will use so-called strongly self-centralizing maximal tori. A subgroup T of G is said to be *strongly self-centralizing* if $\mathbf{C}_G(t) = T$ for every $1 \neq t \in T$. These groups are useful because of the following lemma due to Babai, Pálfy and Saxl.

Lemma 2.5. *Let G be a finite group with a strongly self-centralizing subgroup T. Let p be a prime.*

(i) *If $p \mid |T|$, then*

$$|G_{p'}| > |G| - \frac{|G|}{|\mathbf{N}_G(T)/T|}$$

and

$$|G_p| \geq \frac{|G|}{|\mathbf{N}_G(T)/T|}\frac{|T|-1}{|T|} > \frac{|G|}{|\mathbf{N}_G(T)/T|+1}.$$

(ii) *If $p \nmid |T|$, then*

$$|G_{p'}| \geq \frac{|G|}{|\mathbf{N}_G(T)/T|}\frac{|T|-1}{|T|} > \frac{|G|}{|\mathbf{N}_G(T)/T|+1}.$$

Moreover, if G contains pairwise non-conjugate strongly self-centralizing subgroups $T_1, T_2, \ldots, T_k$ such that $p \nmid |T_i|$ for all $1 \leq i \leq k$, then

$$|G_{p'}| > \sum_{i=1}^{k} \frac{|G|}{|\mathbf{N}_G(T_i)/T_i|+1}.$$

Proof. See [2, Proposition 1.15] and its proof. There the authors used the language of proportion of p-regular elements but one can transfer to the number of p-regular elements. $\square$

2.2. Alternating groups

We finish this section by proving Theorem 2.1 for the alternating groups.

Lemma 2.6. *Theorem 2.1 holds for $S = \mathsf{A}_n$ with $n \geq 5$.*

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Proof. Assume first that $p \geq 7$. We claim that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$. Assume for a contradiction that $S = \mathsf{A}_n$ is a counterexample to the claim with $n \geq 7$ minimal. The prime p divides $|\mathsf{A}_n|$ but does not divide $|\mathsf{A}_{n-1}|$ by Lemma 2.4. It follows that $n = p$. The group A_p has cycles of every odd length up to $p-2$ and has $\lfloor p/3 \rfloor$ cycle types of elements of order 3. Therefore we have

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq (p-1)/2 + \lfloor p/3 \rfloor > 2\sqrt{p-1},$$

from which the claim follows.

Let $p = 5$. From the previous paragraph we have $n(\mathrm{Aut}(\mathsf{A}_7), \mathrm{Cl}_{p'}(\mathsf{A}_7)) > 2\sqrt{p-1}$. This implies $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ for $n \geq 7$ by Lemma 2.4. We find $n(\mathrm{Aut}(\mathsf{A}_6), \mathrm{Cl}_{5'}(\mathsf{A}_6)) = 4$ and $n(\mathrm{Aut}(\mathsf{A}_5), \mathrm{Cl}_{5'}(\mathsf{A}_5)) = 3$. Parts (ii) and (iii) follow.

The number of orbits of $\mathrm{Aut}(S)$ on $\mathrm{Cl}_p(S) \cup \mathrm{Cl}_{p'}(S)$ is 4 if $S = \mathsf{A}_5$ and is 5 if $S = \mathsf{A}_6$. Part (i) follows and the proof is complete. □

3. Theorem 2.1: linear and unitary groups

In this section we prove Theorem 2.1 for S being $\mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$. To do so, we prove several general bounds for the number of $\mathrm{Aut}(S)$-orbits on p-regular and p'-regular classes, see Lemmas 3.1, 3.6, 3.8. These bounds and Lemma 2.4 allow us to achieve Theorem 2.1 in most cases when either n or q is large enough. For smaller n and q, some detailed analysis is needed with the help of Lemma 2.5 and [15].

3.1. Linear groups

In this subsection, we will prove Theorem 2.1(i) for $S = \mathrm{PSL}_n(q)$ with $n \geq 2$, $q = \ell^f$ where ℓ is a prime, and $(n, q) \notin \{(2, 2), (2, 3)\}$. We keep the notation introduced in Section 2 and start with the following technical lemma.

Lemma 3.1. *Let $n \geq 2$ be an integer and let ϵ be 1 or 2 depending on whether $n = 2$ or $n > 2$ respectively. Let $S = \mathrm{PSL}_n(q)$ be a simple group. Let*

$$m = \frac{q^n - 1}{(q-1)(n, q-1)}.$$

If p divides m, then

$$n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) \geq \frac{p-1}{\epsilon f n}.$$

If p does not divide m, then

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{\varphi(m)}{\epsilon f n}$$

where φ is Euler's totient function.

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Proof. Let $A = \mathrm{Aut}(S)$ and let a be an element of S. Let g be the preimage of a in $\mathrm{SL}_n(q) \leq \mathrm{GL}_n(q)$. Assume that g acts irreducibly on the natural module V for $\mathrm{GL}_n(q)$. The centralizer of g in $\mathrm{GL}_n(q)$ is a cyclic group C of order $q^n - 1$ and the normalizer of $\langle g \rangle$ in $\mathrm{GL}_n(q)$ is $C : \langle \sigma \rangle$ where σ is a field automorphism of order n. There is a subgroup B in A defined in a natural way which contains S and which is isomorphic to $\mathrm{PGL}_n(q)$. We have $|B : S| = (n, q-1)$ and $|A : B| = \epsilon f$. Observe that

$$|\mathbf{C}_B(a)| = \frac{|C|}{(n, q-1)}$$

and

$$|\mathbf{N}_B(\langle a \rangle)| = \frac{n|C|}{(n, q-1)}.$$

It follows that $|\mathbf{C}_A(a)| \geq |\mathbf{C}_B(a)| = |C|/(n, q-1)$ and

$$|\mathbf{N}_A(\langle a \rangle)| \leq \epsilon f |\mathbf{N}_B(\langle a \rangle)| \leq \frac{\epsilon f n |C|}{(n, q-1)}.$$

Thus $|\mathbf{N}_A(\langle a \rangle)/\mathbf{C}_A(\langle a \rangle)| \leq \epsilon f n$. Assume now that a is of order m. It follows that there are at least $\varphi(m)/(\epsilon f n)$ conjugacy classes of A all contained in S which consist of elements of order m. The desired bound now follows in the case when p does not divide m. If p divides m, then the bound also follows by noting that $\varphi(m) \geq p - 1$. $\square$

Lemma 3.2. *Theorem 2.1 holds for $S = \mathrm{PSL}_2(q)$ with $q \geq 4$.*

Proof. Let $q \leq 256$. By a Gap [15] calculation $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ unless $q \in \{4, 5, 7, 8, 9, 11, 16, 27, 32, 81, 128, 243, 256\}$. The exceptional cases account for the possibilities in Table 1. Furthermore, if q belongs to $\{512, 1024\}$, then $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ for every possible value of p.

Assume first that p divides $q+1$. There are $q-1$ diagonal elements in $\mathrm{SL}_2(q)$ with respect to a fixed basis. Thus there are at least $q-1$ conjugacy classes of p-regular elements in $\mathrm{GL}_2(q)$ and so at least $(q-1)/2$ conjugacy classes of $\mathrm{PGL}_2(q)$ consisting of p-regular elements in $\mathrm{PSL}_2(q)$. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq (q-1)/(2f)$. This is larger than $2\sqrt{q}$ subject to the restrictions $q > 256$ and $q \notin \{512, 1024\}$. This proves parts (ii) and (iii) in the case when p divides $q+1$. We now turn to the proof of part (i) in the case when p divides $q+1$. We may assume that the pair (S, p) appears in Table 1.

We have $n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) \geq (p-1)/(2f)$ by Lemma 3.1. The exact values of $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$ may be found in Table 1. Using this information, for any pair (S, p) in Table 1 such that p divides $q+1$, we get

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) + n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) > 2\sqrt{p-1},$$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

unless $(S, p) = (\mathrm{PSL}_2(16), 17)$ when $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) + n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) = 7$. This latter pair is an exception in part (i). This proves part (i) in the case p divides $q + 1$. The case $p = \ell$ or $p \mid q - 1$ is similar, and we skip the details. $\square$

Lemma 3.3. *Theorem 2.1 holds for $S = \mathrm{PSL}_3(q)$.*

Proof. We will show that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ in all cases except when $(S, p) = (\mathrm{PSL}_3(8), 73)$. We may exclude $q \le 19$ using [8,15]. By [37] we have $|\mathbf{C}_S(g)| \ge q^2/(3, q-1)$ for every $g \in S$. We also know that S has a strongly self-centralizing maximal torus T of order

$$(q^2 + q + 1)/(3, q - 1) = \Phi_3(q)/(3, q - 1)$$

with $|\mathbf{N}_S(T)/T| = 3$, see [2, p. 16] for instance.

Suppose first that $p \mid |T|$. Then by Lemma 2.5, we have $|S_{p'}| > \frac{2}{3}|S|$ and thus $k_{p'}(S) > 2q^2/(3(3, q - 1))$, which yields

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{q^2}{3f(3, q-1)^2} =: R(q).$$

It is easy to check that $R(q) \ge 2\sqrt{p-1}$, and we are done.

Now we suppose $p \nmid |T|$. By Lemma 2.5, we have $|S_{p'}| > |S|(|T| - 1)/3|T|$. Hence

$$k_{p'}(S) > \frac{q^2(|T| - 1)}{3(3, q - 1)|T|},$$

implying that

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{q^2(|T| - 1)}{6f(3, q - 1)^2|T|} := R'(q).$$

It is easy to check that $R'(q) \ge 2\sqrt{q} \ge 2\sqrt{p-1}$ unless $q \in \{25, 64\}$. In fact we still have $R'(q) \ge 2\sqrt{p-1}$ when $q \in \{25, 64\}$ since $p \le 13$ in those cases. This proves parts (ii) and (iii) by noting that the pair $(S, p) = (\mathrm{PSL}_3(8), 73)$ appears in Table 1.

For the proof of part (i) we may now assume that $(S, p) = (\mathrm{PSL}_3(8), 73)$. Then S has a maximal torus of order $\Phi_3(8) = 73$ with the relative Weyl group of order 3, and thus S has at least $72/3 = 24$ conjugacy classes of elements of order 73. It follows that there are at least $24/3 = 8$ $\mathrm{Aut}(S)$-orbits on $\mathrm{Cl}_p(S)$. We now have $n(\mathrm{Aut}(S), \mathrm{Cl}_p(S) \cup \mathrm{Cl}_{p'}(S)) \ge 8 + 13 > 2\sqrt{p-1}$, as desired. $\square$

Lemmas 2.4, 3.1 and [14, Corollary 3.7] are used to establish the following.

Lemma 3.4. *Theorem 2.1(i) holds for $S = \mathrm{PSL}_n(q)$ with $n \ge 4$.*

Proof. Assume for a contradiction that part (i) fails for the group $S = \mathrm{PSL}_n(q)$ with $n \geq 4$ minimal. The prime p divides $|\mathrm{PSL}_n(q)|$ but does not divide $|\mathrm{PSL}_{n-1}(q)|$ by Lemma 2.4. This implies that p divides

$$m = \frac{q^n - 1}{(q-1)(n, q-1)}.$$

We get

$$n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) \geq \frac{p-1}{2fn}$$

by Lemma 3.1. By Lemma 2.4 and [14, Corollary 3.7 (2)] we also have

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{k(\mathrm{PSL}_{n-1}(q))}{2f(n-1, q-1)} \geq \frac{q^{n-2}}{2f(n-1, q-1)^2}.$$

From these it follows that

$$\begin{aligned} &n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) + n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \\ &\quad \geq \frac{p-1}{2fn} + 2fn + \frac{q^{n-2}}{\delta f(n-1, q-1)^2} - 2fn \geq 2\sqrt{p-1} + \frac{q^{n-2}}{2f(n-1, q-1)^2} - 2fn. \end{aligned}$$

We may thus assume that $q^{n-2} \leq 4f^2 n(n-1, q-1)^2$. An easy computation with [15] then shows that $n \leq 6$ and $q \leq 64$. For these exceptional cases, we find that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$, using Lemma 2.4 together with the bound

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq k(\mathrm{PSL}_{n-1}(q))/2f(n-1, q-1). \quad \square$$

3.2. Unitary groups

We continue to prove Theorem 2.1(i) for $S = \mathrm{PSU}_n(q)$.

Lemma 3.5. *Theorem 2.1 holds for $S = \mathrm{PSU}_3(q)$.*

Proof. The proof is similar to that of Lemma 3.3. We skip the details and just mention that S has a strongly self-centralizing maximal torus T of order $(q^2-q+1)/(3, q+1)$ with $|\mathbf{N}_S(T)/T| = 3$, and therefore Lemma 2.5 and [37] are applied to achieve the bound. $\square$

We proceed to prove part (i) for the groups $S = \mathrm{PSU}_n(q)$ with $n \geq 4$. If $(n, q) = (4, 2)$, then $p = 5$ since we are assuming $p \geq 5$ and so $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) = 14 > 4$ by [15]. Assume from now on that $(n, q) \neq (4, 2)$ (and $n \geq 4$). In this case $\mathrm{PSU}_{n-1}(q)$ is a simple group.

Lemma 3.6. *In order to prove Theorem 2.1(i) for $S = \mathrm{PSU}_n(q)$ with $n \geq 4$, we may assume that*

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{q^{n-2}}{2f(n-1, q+1)^2}$$

and that the prime p divides $q^n - (-1)^n$. Moreover, if n is odd then p is a primitive prime divisor of $q^{2n} - 1$.

Proof. The prime p divides $|S|$ by assumption and $p \geq 5$. Since $(n, q) \neq (4, 2)$, we may assume by Lemma 2.4 that p does not divide $|\mathrm{PSU}_{n-1}(q)|$. This has two implications. Firstly,

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{k(\mathrm{PSU}_{n-1}(q))}{2f(n-1, q+1)} \geq \frac{q^{n-2}}{2f(n-1, q+1)^2}$$

by Lemma 2.4 and [14, Corollary 3.11 (2)] and secondly $p \mid q^n - (-1)^n$.

Let $n \geq 5$ be odd. We claim that p is a primitive prime divisor of $q^{2n} - 1$. Assume for a contradiction that $p \mid q^k - 1$ for some integer k with $1 \leq k < 2n$. Since p does not divide $|\mathrm{PSU}_{n-1}(q)|$, it cannot divide $q^r + 1$ for $r < n$ odd and it cannot divide $q^r - 1$ for $r < n$ even.

Assume that $k \leq n$. By the previous paragraph, k must be odd. Since p divides $(q^n + 1) + (q^k - 1)$, the prime p must divide $q^{n-k} + 1$. Thus $k < n$. Since p divides $(q^k - 1) + (q^{n-k} + 1)$, it must divide $q^{|n-2k|} + 1$. This is a contradiction since $|n - 2k|$ is odd. It follows that $n < k$. Since p divides $(q^{2n} - 1) - (q^k - 1)$, it must divide $q^{2n-k} - 1$. This is a contradiction since $2n - k < n$. □

Lemma 3.7. *Theorem 2.1(i) holds for $S = \mathrm{PSU}_n(q)$ with $n \geq 4$ even.*

Proof. By Lemma 3.6, we may assume $p \mid q^n - 1$, and thus $p - 1 \leq q^{n/2}$. Also, we are finished if $q^{n-2}/(2f(n-1, q+1)^2) > 2q^{n/4}$, and thus we may assume that $q^{(3n/4)-2} \leq 4f(n-1, q+1)^2$. Taking into account that $p \geq 5$ divides $q^n - 1$ but p does not divide $|\mathrm{PSU}_{n-1}(q)|$ and using Lemma 2.4 as in the proof of Lemma 3.4, we find no counterexample for Theorem 2.1(i) with $S = \mathrm{PSU}_n(q)$ and $n \geq 4$ even. □

Lemma 3.8. *Let $n \geq 5$ be odd. Let $p \geq 5$ be a prime which divides $q^n + 1$ and which is a primitive prime divisor of $q^{2n} - 1$. Let $S = \mathrm{PSU}_n(q)$. The number of orbits of $\mathrm{Aut}(S)$ on the set of elements of S of orders divisible by p but not equal to p is*

$$\frac{\frac{q^n+1}{(q+1)(n,q+1)} - p}{2fn}.$$

Proof. Let $g \in \mathrm{GU}_n(q)$ be an element of order divisible by p. Since $\mathrm{GU}_n(q) \leq \mathrm{GL}_n(q^2)$ and p is a primitive prime divisor of $q^{2n} - 1$, we see that g acts irreducibly on the

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

underlying vector space of dimension n over the field of size q^2. It is contained in a Singer cycle C of $\mathrm{GU}_n(q)$ defined to be a cyclic irreducible subgroup of $\mathrm{GU}_n(q)$ of maximal possible order and whose existence is proved by Huppert in [24]. The group C is the intersection of $\mathrm{GU}_n(q)$ with the Singer cycle of $\mathrm{GL}_n(q^2)$ (which is a cyclic subgroup) containing g. Since the centralizer of g in $\mathrm{GL}_n(q^2)$ is the Singer cycle containing g, it follows that the centralizer of g in $\mathrm{GU}_n(q)$ is C. The group C has order q^n+1 by [24, Satz 4]. Since p is a primitive prime divisor of $q^{2n}-1$, C contains a Sylow p-subgroup P of $\mathrm{GU}_n(q)$. The centralizer in $\mathrm{GU}_n(q)$ of any non-trivial element of P is C. It follows that all Singer cycles in $\mathrm{GU}_n(q)$ are conjugate and also that the centralizer of g in $\mathrm{GU}_n(q)$ is C. The group $\mathbf{N}_{\mathrm{GL}_n(q^2)}(\langle g\rangle)/\mathbf{C}_{\mathrm{GL}_n(q^2)}(\langle g\rangle)$ is cyclic of order n, so $\mathbf{N}_{\mathrm{GU}_n(q)}(\langle g\rangle) = C.m$ for some divisor m of n. Since g is contained in an extension field subgroup $\mathrm{GU}_1(q^n).n$ of $\mathrm{GU}_n(q)$, we obtain $m=n$.

The image F of $C\cap\mathrm{SU}_n(q)$ in S has order $(q^n+1)/((q+1)(n,q+1))$. Cyclic subgroups of this order are all conjugate in $\mathrm{Aut}(S)$ by the previous paragraph. Every element of S of order divisible by p is contained in some conjugate of F in $\mathrm{Aut}(S)$. Observe that $|\mathbf{N}_{\mathrm{Aut}(S)}(F)/F| = 2fn$. The lemma follows. $\square$

We are now in position to complete the proof of Theorem 2.1(i) for the unitary groups.

Lemma 3.9. *Theorem 2.1(i) holds for $S=\mathrm{PSU}_n(q)$ with $n\geq 5$ odd.*

Proof. Let $n\geq 5$ be odd. We may assume that p is a primitive prime divisor of $q^{2n}-1$ by Lemma 3.6. Thus

$$n(\mathrm{Aut}(S),\mathrm{Cl}_{p'}(S)) + n(\mathrm{Aut}(S),\mathrm{Cl}_p(S)) \geq \frac{k(S)}{2f(n,q+1)} - \frac{q^n+1}{2fn(q+1)(n,q+1)} + \frac{p}{2fn}$$

by Lemma 3.8. This is at least

$$\frac{p}{2fn} + 2fn - 2fn + \frac{q^{n-1}}{2f(n,q+1)^2} - \frac{q^n+1}{2fn(q+1)(n,q+1)} \geq$$
$$\geq 2\sqrt{p} + \frac{q^{n-1}}{2f(n,q+1)^2} - \frac{q^n+1}{2fn(q+1)(n,q+1)} - 2fn$$

by [14, Corollary 3.11 (2)]. This latter expression is at least $2\sqrt{p}$ if and only if

$$q^{n-1} \geq \frac{(q^n+1)(n,q+1)}{n(q+1)} + 4f^2n(n,q+1)^2.$$

This is satisfied unless $(n,q)\in\{(5,2),(5,4),(5,9),(9,2)\}$. Taking into account that the prime $p\geq 5$ divides q^n+1, the triple (n,q,p) must belong to

$$\{(5,2,11),(5,4,5),(5,4,41),(5,9,5),(5,9,1181),(9,2,19)\}.$$

Among these exceptions, we have

$$\frac{q^{n-1}}{2f(n,q+1)^2} - \frac{q^n+1}{2fn(q+1)(n,q+1)} > 2\sqrt{p-1}$$

unless $(n,q,p) \in \{(5,4,5),(5,4,41),(5,9,1181)\}$. If $(n,q,p) \in \{(5,4,5),(5,4,41)\}$, then

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq n(\mathrm{Aut}(\mathrm{PSU}_4(q)), \mathrm{Cl}_{p'}(\mathrm{PSU}_4(q))) > 2\sqrt{p-1}$$

by Lemma 2.4 and [15]. Let $(n,q,p) = (5,9,1181)$. The precise number of conjugacy classes of S can be computed using [29]. This is $k(S) = 7596$. Plugging this into the first displayed expression of the present proof, we obtain

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{1181'}(S)) + n(\mathrm{Aut}(S), \mathrm{Cl}_{1181}(S)) > 2\sqrt{1180},$$

and this finishes the proof. □

3.3. Theorem 2.1(ii) and (iii): linear and unitary groups of dimension at least 4

The method in Subsections 3.1 and 3.2 can be revised to prove parts (ii) and (iii) for $S = \mathrm{PSL}_n(q)$ and $\mathrm{PSU}_n(q)$, but we present here another path to do it. As the case $n \leq 3$ has been proved in Lemmas 3.2, 3.3, and 3.5, we will assume that $n \geq 4$ in this subsection.

We use $\mathrm{PSL}_n^+(q)$ for the linear groups and $\mathrm{PSL}_n^-(q)$ for the unitary groups.

Lemma 3.10. *Let $S = \mathrm{PSL}_n^\epsilon(q)$ for $n \geq 4$ and p a prime divisor of $|S|$ but $p \nmid q$. Assume that $p \mid (q^n - (\epsilon 1)^n)$ but $p \nmid (q^i - (\epsilon 1)^i)$ for every $1 \leq i \leq n-1$. Then*

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{q^{n-1}(n-1)}{2nf(n,q-\epsilon 1)} H(n,q,\epsilon),$$

where

$$H(n,q,+) = \frac{1}{er}$$

with $r := \min\{x \in \mathbb{N} : x \geq \log_q(n+1)\}$ and

$$H(n,q,-) = \left(\frac{q^2-1}{er'(q+1)^2}\right)^{1/2}$$

with $r' := \min\{x \in \mathbb{N} : x$ odd and $x \geq \log_q(n+1)\}$.

Proof. By [14, Theorems 6.4 and 6.7] and their proofs, the minimal centralizer size of an element in $\mathrm{GL}_n^\epsilon(q)$ is at least

$$q^{n-1}(q-\epsilon 1)H(n,q,\epsilon).$$

Since $\mathrm{GL}_n^\epsilon(q)$ has center of order $q-\epsilon 1$, the minimal centralizer size of an element in $\mathrm{PGL}_n^\epsilon(q)$ is at least $q^{n-1}H(n,q,\epsilon)$. There exists a normal subgroup B of $\mathrm{Aut}(S)$ isomorphic to $\mathrm{PGL}_n^\epsilon(q)$ with the property that S is normal in B. Thus the minimal centralizer size in $\mathrm{Aut}(S)$ of an element in S is at least $q^{n-1}H(n,q,\epsilon)$. It follows that every $\mathrm{Aut}(S)$-orbit on S has size at most

$$\frac{|\mathrm{Aut}(S)|}{q^{n-1}H(n,q,\epsilon)}.$$

On the other hand, by [1, Lemmas 3.1 and 4.1], we know that the proportion of p-regular elements in $\mathrm{PSL}_n^\epsilon(q)$ is at least the proportion of elements in S_n that have no cycles of length divisible by n. As the latter proportion is $(n-1)/n$, we have $|S_{p'}| \geq (n-1)|S|/n$, and it follows from the conclusion of the previous paragraph that

$$n(\mathrm{Aut}(S),\mathrm{Cl}_{p'}(S)) > \frac{(n-1)|S|}{n|\mathrm{Aut}(S)|}\cdot q^{n-1}H(n,q,\epsilon).$$

The result now follows by $|\mathrm{Aut}(S)| = 2f(n,q-\epsilon 1)|S|$. $\square$

Proposition 3.11. *Let $S = \mathrm{PSL}_n^\epsilon(q)$ for $n \geq 4$ and $\epsilon = \pm$ and let p be a prime divisor of $|S|$. The number of* $\mathrm{Aut}(S)$*-orbits on p-regular classes of S is greater than $2\sqrt{p-1}$.*

Proof. Note that the case $p \mid q$ has been done in Lemma 2.3, and so we assume that $p \nmid q$. Furthermore, if $p \mid |\mathrm{PSL}_{n-1}^\epsilon(q)|$ then we are done by Lemma 2.4 and induction. So we assume also that $p \mid (q^n-(\epsilon 1)^n)$ but $p \nmid (q^i-(\epsilon 1)^i)$ for every $1 \leq i \leq n-1$, which means that p is a primitive prime divisor of q^n-1 when $\epsilon=+$ or $4 \mid n$ and $\epsilon=-$, and a primitive prime divisor of $q^{n/2}-1$ when $n \equiv 2 \pmod 4$ and $\epsilon=-$, and a primitive prime divisor of $q^{2n}-1$ when n is odd and $\epsilon=-$. Lemma 3.10 then implies that

$$n(\mathrm{Aut}(S),\mathrm{Cl}_{p'}(S)) > \frac{q^{n-1}(n-1)}{2nf(n,q-\epsilon 1)}H(n,q,\epsilon).$$

A straightforward computation shows that this bound is greater than $2\sqrt{p-1}$, and therefore we are done, unless $q=2$ and $n \leq 9$, or $q=3$ and $n \leq 5$, or $(n,q,\epsilon) \in \{(4,4,\pm),(4,5,+),(5,4,\pm)\}$.

We now consider these exceptions in a case by case basis.

Let $q=2$. First the cases $S=\mathrm{SL}_4^\pm(2)$, $\mathrm{SL}_5^\pm(2)$, and $\mathrm{PSU}_6(2)$ can be checked directly using [8]. The case of $\mathrm{SL}_6(2)$ is not under consideration since 2^6-1 has no primitive prime divisor. For $n=7,8,9$ we will show that the number of different element orders coprime to p is greater than $2\sqrt{p-1}$, and for that purpose it is enough to, and we will, assume that $n=7$ as the maximal prime divisor of S is a divisor of $|\mathrm{SL}_7^\epsilon(2)|$. Here in fact $p=127=2^7-1$ for $\epsilon=+$ and $p=43=(2^7+1)/3$ for $\epsilon=-$. We consider the embeddings $\mathrm{SL}_4^\epsilon(2) \times \mathrm{SL}_3^\epsilon(2) \subset \mathrm{SL}_7^\epsilon(2)$ and $\mathrm{SL}_5^\epsilon(2) \times \mathrm{SL}_2^\epsilon(2) \subset \mathrm{SL}_7^\epsilon(2)$ and inspect the element orders in the groups $\mathrm{SL}_k^\epsilon(2)$ for $2 \leq k \leq 5$ in [8] to produce more than $2\sqrt{p-1}$ element orders of $\mathrm{SL}_7^\epsilon(2)$, proving the desired inequality.

Let $q = 3$. Again the case of $S = \mathrm{PSL}_4^\pm(3)$ is available in [8], and so we assume that $S = \mathrm{PSL}_5^\pm(3)$. The case $S = \mathrm{PSL}_5(3)$ is in fact easy as $p = 11$ and $\mathrm{PSL}_5(3) = \mathrm{SL}_5(3)$ contains $\mathrm{SL}_4(3)$, which has more than 7 different element orders. So it remains to consider $S = \mathrm{PSU}_5(3)$, in which case p must be $61 = (3^5+1)/4$. But by using the embedding $\mathrm{SU}_4(3) \subset \mathrm{SU}_5(3) = \mathrm{PSU}_5(3)$ and inspecting the element orders of $\mathrm{SU}_4(3)$, we find that $\mathrm{PSU}_5(3)$ has at least 17 element orders coprime to $p = 61$, and hence the bound follows in this case.

Let $(n, q, \epsilon) = (4, 4, \pm)$. Then we have $p = 17$. From [8] we observe that $\mathrm{SL}_3^\epsilon(4)$ has more than $8 = 2\sqrt{p-1}$ different element orders, and thus, as $S = \mathrm{SL}_4^\epsilon(4) \geq \mathrm{SL}_3^\epsilon(4)$, it follows that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$. Similarly when $(n, q, \epsilon) = (5, 4, \pm)$, by using [8] and considering the embeddings $\mathrm{SL}_3(4) \subset \mathrm{SL}_5(4) = \mathrm{PSL}_5(4)$ and $\mathrm{SU}_3(4) \times \mathrm{SL}_2(4) \subset \mathrm{SU}_5(4)$ one can produce at least 13 different orders coprime to p of S, and therefore proving the inequality as $p \leq 41$ in this case.

Finally for $(n, q, \epsilon) = (4, 5, +)$ we have $p = 13$ and on the other hand, using the embeddings $\mathrm{SL}_2(5) \times \mathrm{SL}_2(5) \subset \mathrm{SL}_4(5)$ and $\mathrm{SL}_3(5) \subset \mathrm{SL}_4(5)$ one easily sees that S has element orders 1, 2, 3, 5, 6, 15, 31, implying that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 7 > 2\sqrt{p-1}$. □

4. Theorem 2.1: symplectic and orthogonal groups

The aim of this section is to prove the following theorem, which implies Theorem 2.1 for the symplectic and orthogonal groups.

Theorem 4.1. *Let $S = \mathrm{PSp}_{2n}(q)$, $\Omega_{2n+1}(q)$ for $n \geq 2$ and $(n, q) \neq (2, 2)$, or $S = P\Omega_{2n}^\pm(q)$ for $n \geq 4$. Let p be a prime divisor of $|S|$. Then*

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1},$$

with a single possible exception of $(S, p) = (\Omega_8^-(4), 257)$, in which case $2\sqrt{p-1} = 32 \leq n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$.

We note that for the exception $(S, p) = (\Omega_8^-(4), 257)$, we found by using [15] that S has exactly 32 different element orders coprime to p, and therefore it is unlikely that this pair is a true exception. In any case, since $n(\mathrm{Aut}(S), \mathrm{Cl}_p(S)) \geq 1$, the wanted bound $n(\mathrm{Aut}(S), \mathrm{Cl}_p(S) \cup \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ in Theorem 2.1(i) still holds for this exception.

To achieve Theorem 4.1, we prove a bound for the number of unipotent classes of S in terms of partition functions (see Lemmas 4.3 and 4.4) and the number of semisimple classes in terms of the size of certain large torus of S (see Lemmas 4.3 and 4.5).

As the cases $p = 2, 3$ or $p \mid q$ and $n \geq 3$ have been considered in Section 2, we will assume that $p \geq 5$. Moreover, we assume $p \nmid q$ except in the case of $S = \mathrm{PSp}_4(q) \cong \Omega_5(q)$, due to Lemma 2.3.

4.1. Symplectic groups and odd-dimensional orthogonal groups

Lemma 4.2. *Theorem 4.1 holds for $S = \mathrm{PSp}_4(q) \cong \Omega_5(q)$ with $q \neq 2$.*

Proof. We assume that $q \geq 7$ as the cases $q = 3, 4, 5$ can be confirmed directly using [8]. First suppose that $p \mid q$. Recall that $p \geq 5$, and so q is odd. Then $k_{p'}(S) \geq q^2/2$ and therefore $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > q^2/4f$. One can check that $q^2/(4f) > 2\sqrt{p-1}$ for all $q \geq 7$.

So it remains to assume that $p \nmid q$. From [11,38], we observe that $|\mathbf{C}_S(g)| \geq (q^2 - 1)/(2, q-1)$ for every $g \in S$. Suppose that $p \mid (q^2 - 1)$. [1, Lemma 5.1] then implies that the proportion of p-regular elements in S is at least $3/8$. Therefore $k_{p'}(S) \geq 3(q^2 - 1)/8(2, q-1)$, and thus

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{3(q^2-1)}{8f(2,q-1)^2(2,q)}.$$

This bound is larger than $2\sqrt{q} \geq 2\sqrt{p-1}$ if $q \geq 23$. When $q < 23$ we must have $p \leq 7$ since $p \mid (q^2 - 1)$ and we are done as $|S|$ is divisible by at least four primes.

The remaining case $p \mid (q^2 + 1)$ is treated similarly, with remark that the proportion of p-regular elements in S is now at least $1/2$ again by [1, Lemma 5.1]. □

Let $\mathbf{p}(i)$ be the number of distinct ways of representing i as a sum of positive integers and $\mathbf{p}_0(i)$ be the number of distinct ways of representing i as a sum of odd positive integers.

Lemma 4.3. *Let $p \geq 3$ be a prime not dividing q. We have*

$$k_{p'}(\mathrm{PSp}_{2n}(q)) \geq \begin{cases} \sum_{i=0}^{n} \mathbf{p}(i)\mathbf{p}_0(n-i) + \left\lceil \dfrac{q^n-2}{4n} \right\rceil & \text{if } q \text{ is odd} \\ \mathbf{p}(n) + \left\lceil \dfrac{q^n-2}{2n} \right\rceil & \text{if } q \text{ is even,} \end{cases}$$

and

$$k_{p'}(\Omega_{2n+1}(q)) \geq \begin{cases} \sum_{i=0}^{\lfloor (2n+1)/4 \rfloor} \mathbf{p}(i)\mathbf{p}_0(2n+1-4i) + \left\lceil \dfrac{q^n-2}{4n} \right\rceil & \text{if } q \text{ is odd} \\ \mathbf{p}(n) + \left\lceil \dfrac{q^n-2}{2n} \right\rceil & \text{if } q \text{ is even.} \end{cases}$$

Proof. Note that, by the assumption, p cannot divide both $q^n - 1$ and $q^n + 1$. So let T be a maximal torus of $G := \mathrm{Sp}_{2n}(q)$ of order $q^n \pm 1$ such that $p \nmid |T|$. Since the fusion of (semisimple) elements in this torus is controlled by the relative Weyl group of a Sylow n-torus with order $2n$ (see [31, Proposition 5.5] and its proof), there exist at least $(|T| - 1)/(2n)$ nontrivial semisimple classes of G with representatives in T. It follows that S has at least $(q^n - 2)/(2n(2, q-1))$ nontrivial p-regular semisimple classes.

Suppose first that q is odd. Let J_k denote the unipotent Jordan block of size k, which is the $k \times k$ matrix with 1 on the main and second main diagonals, and 0 everywhere else. Let r, s, $a_1, \dots, a_r$, $b_1, \dots, b_s$ be integers, $k_1, \dots, k_r$ be distinct non-negative integers, and $l_1, \dots, l_s$ be distinct positive integers such that $\sum_{i=1}^{r} a_i k_i + \sum_{j=1}^{s} b_j(2l_j + 1) = n$. Consider a matrix g in $\mathrm{GL}_{2n}(q)$ conjugate to a block matrix with a_i Jordan blocks J_{2k_i} and $2b_j$ Jordan blocks J_{2l_j+1} in the main diagonal. By [18, Proposition 2.3], there are 2^r unipotent classes of $\mathrm{Sp}_{2n}(q)$ (and therefore of $\mathrm{PSp}_{2n}(q)$) of elements having such form. These classes are all p-regular since $p \nmid q$. Since there are $\sum_{i=0}^{n} \mathbf{p}(i)\mathbf{p}_0(n-i)$ such Jordan forms, we obtain the desired bound in this case.

Symplectic groups in even characteristic and odd-dimensional orthogonal groups follow from [18, Proposition 2.4 and Theorem 3.1] in a similar way. $\square$

We are now ready to prove Theorem 4.1 for $S = \mathrm{PSp}_{2n}(q)$ and $S = \Omega_{2n+1}(q)$ for $n \geq 3$. The treatments for these two families are almost identical, so let us provide details only for symplectic groups.

Suppose first that q is odd. Then by Lemma 4.3 and its proof, we obtain

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 1 + \left\lceil \frac{\sum_{i=0}^{n} \mathbf{p}(i)\mathbf{p}_0(n-i) - 1}{2f} \right\rceil + \left\lceil \frac{q^n - 2}{8fn} \right\rceil =: R(q,n),$$

as $|\mathrm{Out}(S)| = 2f$ and note that the trivial class is an $\mathrm{Aut}(S)$-orbit itself. Note also that $p \leq (q^n+1)/2$ for $n \geq 4$ and $p \leq q^2 + q + 1$ for $n = 3$. One now can check that $R(q,n) > 2\sqrt{p-1}$ for all relevant values.

Next suppose that q is even. We now have

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 1 + \left\lceil \frac{\mathbf{p}(n) - 1}{f} \right\rceil + \left\lceil \frac{q^n - 2}{2fn} \right\rceil =: R'(q,n).$$

Again one can check that $\lceil (q^n-2)/(2fn) \rceil > 2q^{n/2} \geq 2\sqrt{p-1}$ unless $(n,q) \in \mathcal{S} := \{(3,2), (3,4), (4,2), (4,4), (5,2), (5,4)\}$ or $6 \leq n \leq 10$ and $q = 2$. We then observe that $R'(n,q) > 2\sqrt{p-1}$ in the latter case.

Note that if $n = 5$ then $p \leq (q^5-1)/(q-1)$ and the desired bound $R'(n,q) > 2\sqrt{p-1}$ still holds for $(n,q) = (5,4)$. For $(n,q) = (5,2)$, the only prime failing the inequality $R'(n,q) > 2\sqrt{p-1}$ is $p = 31 = q^n - 1$, but in this case we remark that there are at least $\lceil (q^n/10f) \rceil = 4$ nontrivial semisimple p-regular classes and at least $\mathbf{p}(5) - 1 = 6$ nontrivial unipotent classes, totaling to at least 11 p-regular classes of S, and hence $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) = k_{p'}(S) \geq 11 > 2\sqrt{p-1}$, as required.

For $n = 3$ we note that $p \leq q^2 + q + 1$ and $\mathrm{PSp}_6(q)$ has at least 9 unipotent classes, and thus the bound holds for $(n,q) = (3,2)$ or $(3,4)$. For $n = 4$ we note that $\mathrm{PSp}_8(q)$ has at least 24 unipotent classes and so we are done for $(n,q) = (4,2)$ and $(n,q) = (4,4)$ as well. The proof is complete.

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

4.2. Orthogonal groups in even dimension

Let $S = P\Omega^{\epsilon}_{2n}(q)$ for $n \geq 4$, $\epsilon = \pm$, and $q = \ell^f$ where ℓ is a prime.

We start this subsection by proving a lower bound for the number of unipotent classes in even-dimensional orthogonal groups.

Lemma 4.4. *The following holds:*

(i) $P\Omega^{\pm}_{2n}(q)$ *has at least* $\sum_{i=0}^{\lfloor n/2 \rfloor} \mathbf{p}(i)\mathbf{p}_0(2n-4i)$ *unipotent classes if* q *is odd.*
(ii) $P\Omega^{+}_{2n}(q)$ *has at least* $\mathbf{p}(n) + \sum_{i\neq j;i+j\leq n;i,j \ odd} \mathbf{p}(n-i-j)$ *unipotent classes if* q *is even.*
(iii) $P\Omega^{-}_{2n}(q)$ *has at least* $\sum_{1\leq i\leq n;i \ odd} \mathbf{p}(n-i)$ *unipotent classes if* q *is even.*

Proof. First suppose that q is odd. Recall that J_k denotes the unipotent Jordan block of size k, as defined in Subsection 4.1. Let r, s, $a_1, \dots, a_r$, $b_1, \dots, b_s$ be integers, $k_1, \dots, k_r$ be distinct non-negative integers, and $l_1, \dots, l_s$ be distinct positive integers such that

$$\sum_{i=1}^{r} a_i(2k_i+1) + 4\sum_{j=1}^{s} b_j l_j = 2n.$$

Consider a matrix g in $\mathrm{GL}_{2n}(q)$ conjugate to a block matrix with a_i Jordan blocks J_{2k_i+1} and $2b_j$ Jordan blocks J_{2l_j} in the main diagonal. It was shown in [18, Proposition 2.4] that the unipotent elements g with such a Jordan form fall into 2^{r-1} classes in each of $\mathrm{GO}^{+}_{2n}(q)$ and $\mathrm{GO}^{-}_{2n}(q)$, with the exception that if $r = 0$, it is 1 class in $\mathrm{GO}^{+}_{2n}(q)$ and none in $\mathrm{GO}^{-}_{2n}(q)$. As q is odd, these classes are inside $\Omega^{\pm}_{2n}(q)$ and different classes produce different corresponding classes of S. Now (i) follows since the number of those Jordan forms is $\sum_{i=0}^{\lfloor n/2 \rfloor} \mathbf{p}(i)\mathbf{p}_0(2n-4i)$, with the remark that there is at least one such form with $r \geq 2$.

In a similar way, (ii) and (iii) follow from the description of unipotent classes of $\mathrm{GO}^{\pm}_{2n}(2^f)$ as well as $P\Omega^{\pm}_{2n}(2^f) = \Omega^{\pm}_{2n}(2^f)$ in [18, Theorem 3.1]. □

Lemma 4.5. *Suppose that* p *is odd and* $(n, \epsilon) \neq (4, +)$*. There are at least*

$$1 + \left\lceil \frac{q^{n-1}-2}{4f(n-1)(4, q^n - \epsilon 1)^2} \right\rceil.$$

$\mathrm{Aut}(S)$*-orbits of* p*-regular semisimple classes of* $S = P\Omega^{\pm}_{2n}(q)$*.*

Proof. From the assumption on p, we know that p does not divide both $q^{n-1}-1$ and $q^{n-1}+1$. Let T be a torus of $G := \mathrm{Spin}^{\epsilon}_{2n}(q)$ of order $q^{n-1} \pm 1$ such that $p \nmid |T|$. The relative Weyl group of a Sylow $(n-1)$-torus has order $2(n-1)$, and thus there are at least $(|T|-1)/(2(n-1))$ nontrivial semisimple classes of G with representatives in

T. It follows that S has at least $(q^{n-1}-2)/(2(n-1)(4, q^n-\epsilon 1))$ nontrivial p-regular semisimple classes. The lemma now follows as $|\mathrm{Out}(S)| = 2f(4, q^n - \epsilon 1)$. $\square$

Now we are ready to prove Theorem 4.1 for even-dimensional orthogonal groups of rank at least 4. We recall that $p \geq 5$ and $p \nmid q$.

A) Suppose that $p \mid (q^m \pm 1)$ for some $m \leq n/2$. One can check that the bound in Lemma 4.5 is greater than $2\sqrt{p-1}$ unless $n = 5$ and $q = 2, 3, 5, 7, 9$; $n = 6$ and $q = 2, 3, 5$; or $(n, q) = (7, 2), (7, 3), (8, 2), (8, 3)$.

For these exceptional cases, we will prove the desired bound by also taking into account the unipotent classes of S. For instance, when $(n, q) = (8, 3)$ we have that S has at least $\sum_{i=0}^{4} \mathbf{p}(i)\mathbf{p}_0(16-4i) = 69$ unipotent classes by Lemma 4.4(i), producing at least $\lceil 69/8 \rceil = 9$ orbits of $\mathrm{Aut}(S)$ on unipotent classes of S. Together with at least 5 orbits on nontrivial p-regular semisimple classes by Lemma 4.5, we obtain $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 14 > 2\sqrt{p-1}$ since $p \leq 41$. Other cases are treated similarly.

B) Suppose that p does not divide $q^i \pm 1$ for every $i \leq n/2$. Let m be minimal subject to the condition $p \mid q^m \pm 1$. In particular, $m \geq 3$. Using [1, Lemma 6.1], we then know that the proportion of p-regular elements in S is at least the proportion of elements in S_n that have no cycles of length divisible by m. As the latter proportion is $(m-1)/m$, we deduce that

$$|S_{p'}| \geq \frac{m-1}{m}|S| > \frac{n-2}{n}|S|,$$

where we recall that $S_{p'}$ denotes the set of p-regular elements in S.

On the other hand, according to the proof of [14, Theorem 6.13], the centralizer size of an element in $\mathrm{SO}^{\pm}_{2n}(q)$ is at least

$$q^n \left[\frac{1-1/q}{2^r e}\right]^{1/2},$$

where

$$r := \min\{x \in \mathbb{N} : \max\{4, \log_q(4n)\} \leq 2^x\}.$$

Thus, for every $g \in S$, we have

$$|\mathbf{C}_S(g)| \geq \frac{q^n(2, q^n-\epsilon 1)}{2(4, q^n-\epsilon 1)} \left[\frac{1-1/q}{2^r e}\right]^{1/2},$$

and therefore

$$k_{p'}(S) \geq \frac{q^n(n-2)(2, q^n-\epsilon 1)}{2n(4, q^n-\epsilon 1)} \left[\frac{1-1/q}{2^r e}\right]^{1/2}$$

for every prime p, since $|S_{p'}| \geq (n-2)|S|/n$. It follows that

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{q^n(n-2)(2, q^n - \epsilon 1)}{4fn(4, q^n - \epsilon 1)^2} \left[\frac{1 - 1/q}{2^r e}\right]^{1/2} =: R(n, q)$$

as $|\mathrm{Out}(S)| = 2f(4, q^n - \epsilon 1)$.

Taking into account the maximum value of p and assuming that $n \geq 5$, we get $R(n, q) > 2\sqrt{p-1}$ unless possibly if $n = 5$ and $q \in \{2, 3, 4, 5\}$, or $n \in \{6, 7\}$ and $q \in \{2, 3\}$, or $(n, q, \epsilon) = (8, 3, +)$, or $q = 2$ and $n \in \{8, 9, 10\}$. For these small cases, we use various techniques, including Lemmas 4.4 and 4.5, counting element orders, and embeddings of classical groups to prove the bound $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$.

As an example let us consider the case $(n, q, \epsilon) = (7, 3, \pm)$ or $(8, 3, +)$, perhaps the most difficult one. The bound then is still straightforward unless $p = 547 = (3^7 + 1)/4$ or $p = 1093 = (3^7 - 1)/2$. We consider the natural embeddings

$$\mathrm{Spin}_8^+(3) \times \mathrm{SL}_4(3) \cong \mathrm{Spin}_8^+(3) \times \mathrm{Spin}_6^+(3) \subset \mathrm{Spin}_{14}^+(3) \subset \mathrm{Spin}_{16}^+(3)$$

and

$$\mathrm{Spin}_8^-(3) \times \mathrm{SU}_4(3) \cong \mathrm{Spin}_8^-(3) \times \mathrm{Spin}_6^-(3) \subset \mathrm{Spin}_{14}^-(3),$$

which lead to the embeddings

$$\mathrm{P}\Omega_8^+(3) \times \mathrm{PSL}_4(3) \subset \mathrm{P}\Omega_{14}^+(3) \subset \mathrm{P}\Omega_{16}^+(3)$$

and

$$\mathrm{P}\Omega_8^-(3) \times \mathrm{PSU}_4(3) \subset \mathrm{P}\Omega_{14}^-(3),$$

respectively (see [35, Lemma 2.5]). We now use the information on element orders of $P\Omega_8^{\pm}(3)$ and $\mathrm{PSL}_4^{\pm}(3)$ (here $\mathrm{PSL}_4^-(3) := \mathrm{PSU}_4(3)$) in [8,15] to find that the set of element orders of $P\Omega_{14,16}^{\epsilon}(3)$ coprime to both 547 and 1093 is greater than 67. It then follows that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 67 > 2\sqrt{1092} \geq 2\sqrt{p-1}$ as wanted.

The proof of Theorem 4.1 is completed by the following lemma.

Lemma 4.6. *Theorem 4.1 holds for* $S = \mathrm{P}\Omega_8^{\pm}(q)$

Proof. We provide details only for $S = \mathrm{P}\Omega_8^+(q)$. Note that

$$|S| = q^{12}\Phi_1(q)^4\Phi_2(q)^3\Phi_3(q)\Phi_4(q)^2\Phi_6(q)/(4, q^4 - 1).$$

First we suppose that p divides $\Phi_3(q)$, $\Phi_4(q)$ or $\Phi_6(q)$. According to [1, Lemma 6.1], the proportion of p-regular elements in S is then at least the proportion of elements in S_4 with no cycles of length divisible by 2, which is 13/24. As above, we get

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{13q^4}{288f(2,q-1)^3}\left[\frac{1-1/q}{4e}\right]^{1/2}.$$

The assumption on p guarantees that this bound is greater than $2\sqrt{p-1}$, unless $q \in \{2,3,4,5,7,9\}$.

If $q=2$, then $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 24 > 2\sqrt{p-1}$ by [15], as $p \leq 7$. Let $q=3$. Since $p \geq 5$, we have $p \in \{5,7,13\}$. The number of different orders of elements in S which are coprime to p is at least 12 by [15]. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 12 > 2\sqrt{13-1}$. Let $q=4$. The set of prime divisors of the order of S is $\{2,3,5,7,13,17\}$. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 6$. This forces $p \in \{13,17\}$. Using random searches by [15] one finds that S contains elements of orders 15, 21, 30. It follows that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 9 > 2\sqrt{p-1}$. Let $q=5$. The set of prime divisors of $|S|$ is $\{2,3,5,7,13,31\}$. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 6$. Assume that $p \in \{13,31\}$. Using random searches by [15], one finds that S contains elements of orders 10, 62, 63 from which we obtain the desired bound for $p=13$, and elements of orders 10, 26, 39, 63, 156, from which we get the bound for $p=31$. Let $q=7$. The set of prime divisors of $|S|$ is $\{2,3,5,7,19,43\}$. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 6$. Assume that $p \in \{19,43\}$. Using random searches by [15], one finds that S contains elements of orders 16, 25, 168, 600, from which the desired bound follows for $p=19$, and 16, 24, 25, 57, 168, 171, 600, from which we get the bound for $p=43$. Let $q=9$. The set of prime divisors of $|S|$ is $\{2,3,5,7,13,41,73\}$. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 7$. Assume that $p \in \{41,73\}$. Since $\mathrm{GO}_6^+(9) \times \mathrm{GO}_2^+(9)$ is a subgroup of $\mathrm{GO}_8^+(9)$, there is a subgroup of S isomorphic to $\mathrm{P}\Omega_6^+(9) \cong \mathrm{PSL}_4(9)$. Using random searches by [15], one sees that $\mathrm{P}\Omega_6^+(9)$ (and so S) contains elements of orders 9, 16, 20, 24, 40, 60, 80, 91, 182, from which the desired bound follows for $p=41$, and an additional element of order 205 from which the case $p=73$ follows.

Next we suppose that p divides $\Phi_1(q)$ or $\Phi_2(q)$. Arguing similarly as in Lemma 4.5, we then have that S has at least

$$1+\left\lceil\frac{q^3-2}{36f(2,q-1)^4}\right\rceil$$

$\mathrm{Aut}(S)$-orbits on its p-regular semisimple classes. This bound is greater than $2\sqrt{p-1}$ unless $q \in \{2,3,4,5,7,9,11\}$. For all these exceptions, we have $p \leq 5$ as $p \mid (q^2-1)$, and the bound easily holds as $|S|$ has at least 5 different prime divisors. □

5. Theorem 2.1: exceptional groups

In this section S will be a simple exceptional group of Lie type, but not the Tits group. Then S is of the form $G/\mathbf{Z}(G)$, where $G = \mathcal{G}^F$ is the set of fixed points of a simple algebraic group of simply connected type, under a Frobenius endomorphism F associated to the field of $q = \ell^f$ elements, where ℓ is a prime. Let r be the rank of $\mathcal{G}$, which we also call the rank of S. We then have $|\mathbf{C}_G(g)| \geq (q-1)^r$ for all $g \in G$, which implies that $|\mathbf{C}_S(g)| \geq (q-1)^r/|\mathbf{Z}(G)|$ for all $g \in S$.

Table 2
Upper bounds for $p(S)$.

S	upper bound for $p(S)$
${}^2B_2(q), q = 2^{2m+1}$	$\Phi_4^+(q)$
$G_2(q)$	$\Phi_3(q)$
${}^2G_2(q), q = 3^{2m+1}$	$\Phi_6^+(q)$
$F_4(q)$	$\Phi_8(q)$
${}^2F_4(q), q = 2^{2m+1}$	$\Phi_{12}^+(q)$
${}^3D_4(q)$	$\Phi_{12}(q)$
$E_6(q)$	$\Phi_9(q)$
${}^2E_6(q)$	$\Phi_{18}(q)$
$E_7(q)$	$\Phi_7(q)$
$E_8(q)$	$\Phi_{30}(q)$

Table 3
Strongly self-centralizing maximal tori of exceptional groups.

S	conditions	$\|T\|$	$\|\mathbf{N}_S(T)/T\|$
${}^2B_2(q)$	$q = 2^{2m+1}$	$\Phi_4^\pm(q)$	4
$G_2(q)$	$q \not\equiv 1(\mathrm{mod}3)$	$\Phi_3(q)$	6
	$q \not\equiv 2(\mathrm{mod}3)$	$\Phi_6(q)$	
${}^2G_2(q)$	$q = 3^{2m+1}$	$\Phi_6^\pm(q)$	6
$F_4(q)$		$\Phi_{12}(q)$	12
${}^2F_4(q)$	$q = 2^{2m+1}$	$\Phi_{12}^\pm(q)$	12
${}^3D_4(q)$		$\Phi_{12}(q)$	4
$E_6(q)$		$\Phi_9(q)/(3, q-1)$	9
${}^2E_6(q)$		$\Phi_{18}(q)/(3, q+1)$	9
$E_8(q)$		$\Phi_{24}(q)$	24
		$\Phi_{15}(q)$	30
		$\Phi_{30}(q)$	30

Let $\Phi_n(q)$ denote the value of the n-cyclotomic polynomial at q and let $p(S)$ be the maximal prime divisor of S. Also, let $\Phi_4^\pm(q) := q \pm \sqrt{2q} + 1$ for $q = 2^{2m+1}$, $\Phi_6^\pm(q) := q \pm \sqrt{3q} + 1$ for $q = 3^{2m+1}$, and $\Phi_{12}^\pm(q) := q^2 \pm \sqrt{2q^3} + q \pm \sqrt{2q} + 1$ for $q = 2^{2m+1}$. Using the order formulas of S [8], one can find an upper bound for $p(S)$, which we record in Table 2. We observe that in all the cases $p(S) \le \Psi_S(q)$ for a polynomial Ψ_S of degree at most $r(S)$. In fact, $\deg(\Psi_{n(S)}) = r$ in all cases except $S = E_7(q)$.

We recall from Section 2 that a subgroup T of G is said to be strongly self-centralizing if $\mathbf{C}_G(t) = T$ for every $1 \ne t \in T$. It turns out that every group of exceptional types other than $E_7(q)$ has one or more strongly self-centralizing torus, as worked out in [2]. This information is collected in Table 3 for convenient reference.

We will follow the following strategy to prove Theorem 2.1 for groups of exceptional types. First we use a strongly self-centralizing torus and Lemma 2.5 to obtain a lower bound for $|S_{p'}|$. This and the lower bound $|\mathbf{C}_S(g)| \ge (q-1)^r/|\mathbf{Z}(G)|$ on the centralizer size then yield lower bounds for $k_{p'}(S)$ and $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$. This turns out to be sufficient when q is large enough. For smaller q, some ad hoc arguments are needed.

1) $S = {}^2B_2(q)$ with $q = 2^{2m+1} \ge 2^3$. We will assume that $m \ge 3$ as information on ${}^2B_2(8)$ and ${}^2B_2(32)$ are available in [8]. As seen in Table 3, S contains two strongly self-centralizing tori T_1 and T_2 of order $\Phi_4^\pm(q)$ such that $|\mathbf{N}_S(T_i)/T_i| = 4$. Assume first

that p divides either $\Phi_4^+(q)$ or $\Phi_4^-(q)$. We then have $|S_{p'}| > 3|S|/4$ by Lemma 2.5(i). Therefore,

$$k_{p'}(S) > \frac{3(q-1)}{4},$$

which implies that

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{3(q-1)}{4(2m+1)},$$

as $|\mathrm{Out}(S)| = 2m+1$. We observe that

$$3(q-1)/(4(2m+1)) > 2\sqrt{\Phi_4^+(q)-1} \geq 2\sqrt{p-1}$$

for all $q \geq 2^9$. So we are done unless $q = 2^7$. In fact, when $q = 2^7$ we still have $3(q-1)/(4(2m+1)) > 2\sqrt{p-1}$ unless $p = 113$.

Next we assume $p \nmid \Phi_4(q) = \Phi_4^+(q) \cdot \Phi_4^-(q)$, which means that $p \mid 2(q-1)$. By Lemma 2.5(ii), we have $|S_{p'}| > 2|S|/5$. Therefore, $k_{p'}(S) > 2(q-1)/5$, and it follows that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2(q-1)/5(2m+1)$. As $p \leq q-1$, we deduce that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ for $q \geq 2^{13}$. Indeed, we have $p \leq 89$ when $q = 2^{11}$ and $p \leq 73$ when $q = 2^9$ and thus the desired bound still holds in those cases. We are left with $(S,p) = ({}^2B_2(2^7), 127)$.

Let $S = {}^2B_2(2^7)$. We have $|\mathrm{Out}(S)| = 7$. Suzuki [39] proved that S has 2^7+3 conjugacy classes. The trivial element of S forms a single $\mathrm{Aut}(S)$-orbit. The group S has 1 class of involutions. It has 2 classes of elements of order 4 accounting for 2 $\mathrm{Aut}(S)$-orbits. The group S has 63 conjugacy classes of elements of order 127 accounting for at least 9 $\mathrm{Aut}(S)$-orbits. It has 28 conjugacy classes of elements of order 113 forming at least 4 orbits. There are 36 classes of elements in a cyclic torus of order 145, where 1 of them is for elements of order 5, 7 of them for elements of order 29, and 28 of them for elements of order 145. These give at least 6 orbits. Adding all these together we have $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 14$ for the pair $(S,p) = ({}^2B_2(2^7), 127)$ and $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 19$ for the pair $(S,p) = ({}^2B_2(2^7), 113)$, as appearing in Table 1. We also note that for these two exceptions, $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 14 > 2(p-1)^{1/4}$ and $n(\mathrm{Aut}(S), \mathrm{Cl}_p(S) \cup \mathrm{Cl}_{p'}(S)) = 23 > 2\sqrt{p-1}$.

The cases $S = {}^2G_2(q)$ with $q = 3^{2m+1} \geq 3^3$ and $S = {}^2F_4(q)$ with $q = 2^{2m+1} \geq 8$ are treated similarly.

2) $S = G_2(q)$ with $q = \ell^f \geq 3$. We will assume that $q \geq 7$ as the cases $q = 3, 4, 5$ are available in [8]. First we consider $p \mid \Phi_3(q)$. If $q \not\equiv 1 \pmod 3$ then S has a strongly self-centralizing torus T of order $\Phi_3(q)$ such that $|\mathbf{N}_S(T)/T| = 6$. Lemma 2.5 then implies that $|S_{p'}| > 5|S|/6$. Thus $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 5(q-1)^2/(6fg)$ for $g = 2$ if $\ell = 3$ and $g = 1$ otherwise. Therefore $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{\Phi_3(q)-1} \geq 2\sqrt{p-1}$ unless $q = 9$, but in this exceptional case p is at most 13 and the bound still follows.

So assume that $q \equiv 1 \pmod 3$. Then S has a maximal torus of order $\Phi_6(q)$ with the relative Weyl group of order 6 as above, implying that there are $(q^2-q)/6$ classes of S with representatives being nontrivial elements in this torus. Consider another torus of order $(q+1)^2$ with the relative Weyl group of order 12, we find another $(q^2+2q)/12f$ nontrivial different classes. We now have

$$k_{p'}(S) \geq 1 + \frac{q^2-q}{6} + \frac{q^2+2q}{12},$$

and thus

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 1 + \frac{q^2-q}{6f} + \frac{q^2+2q}{12f}.$$

This bound is greater than $2\sqrt{\Phi_3(q)-1} \geq 2\sqrt{p-1}$, and hence we are done, unless $q=7$. When $q=7$ we have $p=19$ and the above bound is still greater than $2\sqrt{p-1}$.

The case $p \mid \Phi_6(q)$ is similar, so suppose that $p \nmid \Phi_3(q)\Phi_6(q)$. Then by Lemma 2.5 we have $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > (q-1)^2/(7fg)$ for $g=2$ if $\ell=3$ and $g=1$ otherwise, but now $p \leq q+1$. One can check that $(q-1)^2/(7fg) > 2\sqrt{q} \geq 2\sqrt{p-1}$ unless $q=7$ or 9. But in those cases we have $p \leq 7$ or 5, respectively, and hence we still have $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$.

Similar arguments also work for $S = F_4(q)$ and ${}^3D_4(q)$.

3) $S = E_6(q)$ with $q = \ell^f$. We again assume $q \geq 3$ as the case $E_6(2)$ is available in [8]. We know that S has a strongly self-centralizing tori T of order $\Phi_9(q)/(3,q-1)$ such that $|\mathbf{N}_S(T)/T| = 9$. Assume that $p \mid |T|$. Recall that $\mathbf{C}_S(g) \geq (q-1)^6/(3,q-1)$ for all $g \in S$ and $|\mathrm{Out}(S)| = 2f(3,q-1)$. Now we have

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{4(q-1)^6}{9f(3,q-1)^2}.$$

It turns out that $4(q-1)^6/9f(3,q-1)^2 > 2\sqrt{p-1}$ unless $q=3$ or 4. When $q=4$ we have $p \leq 73$ so the bound $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$ still holds. When $q=3$ the only prime we need to check is $p = 757 = \Phi_9(3)$. So let $(S,p) = (E_6(3), 757)$. The union of the set of prime divisors of $|E_6(3)|$ with the set of element orders of the sections $\mathrm{PSL}_6(3)$, $\mathrm{PSL}_3(3) \times \mathrm{PSL}_3(3) \times \mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(27)$ and $\mathrm{PSL}_5(3) \times \mathrm{PSL}_2(3)$ consists of 47 integers none of which is divisible by 757. The group $\mathrm{P}\Omega_{10}^+(3)$ is also a section of $E_6(3)$ and by finding orders of random elements in $\mathrm{P}\Omega_{10}^+(3)$ using [15], we may obtain 8 extra integers, namely 21, 35, 45, 70, 82, 84, 90 and 164, apart from the 47 previously found. Finally, $55 > 2\sqrt{757-1}$.

Suppose $p \nmid |T|$, and so we have $p \leq q^4+1$. Let G be the extension of S be diagonal automorphisms. Then G has a maximal torus of order $\Phi_9(q) = q^6+q^3+1$ with the relative Weyl group of order 9. Therefore there are at least $(q^6+q^3)/9$ nontrivial classes with representatives in that torus. Therefore G has at least $(q^6+q^3)/9$ nontrivial p-regular classes, and thus, by the orbit counting formula,

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq 1 + \frac{q^6+q^3}{18f(3,q-1)},$$

which is larger than $2q^2 \geq 2\sqrt{p-1}$ for all $q \geq 3$.

The cases $S = {}^2E_6(q)$ and $S = E_8(q)$ are similar.

4) $S = E_7(q)$ with $q = \ell^f$. As the case $q = 2$ is available in [8], we assume that $q \geq 3$. This is the only family of exceptional groups that do not always possess a strongly self-centralizing maximal torus. It was shown in [2, Theorem 3.4] that the proportion of p-regular elements in S is at least $1/15$, for every prime p. Therefore

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > \frac{(q-1)^7}{15f(2,q-1)^2} =: R(q).$$

Recall from Table 2 that $p \leq \Phi_7(q) = (q^7-1)/(q-1)$ and one can check that $R(q) > 2\sqrt{\Phi_7(q)-1}$ for all $q \geq 5$. When $q = 4$ we observe that the largest prime divisor of S is 257 and hence the inequality $R(q) > 2\sqrt{p-1}$ still holds. For $q = 3$ the bound is also good unless $p = 757 = \Phi_9(3)$ or $1093 = \Phi_7(3)$. The case of $(S,p) = (E_7(3), 757)$ follows from the case $(S,p) = (E_6(3), 757)$ we already examined above. Finally let $(S,p) = (E_7(3), 1093)$. We know that $E_6(3)$, and hence $E_7(3)$, has at least 55 different element orders coprime to 757 as well as 1093. On the other hand elements in a maximal torus of $(E_7)_{ad}(3)$ of order $\Phi_9(3)\Phi_1(3) = 2 \cdot 757$ are controlled by its relative Weyl group of order 18, implying that there are at least 42 classes of elements of order 757 with representatives in this torus, which in turn produce at least 21 $\mathrm{Aut}(S)$-orbits on those classes. We now have at least $55 + 21 > 2\sqrt{1092}$, orbits of $\mathrm{Aut}(S)$ on p-regular classes of S.

We have finished the proof of Theorem 2.1.

6. Bounding the number of p-regular classes in finite groups of Lie type

The following is Theorem 1.4 in the introduction.

Theorem 6.1. *Let S be a simple group of Lie type defined over the field of q elements with r the rank of the ambient algebraic group. We have*

$$k_{p'}(S) > \frac{q^r}{17r^2}$$

for every prime p.

Proof. The theorem is known in the case $p \nmid |S|$, as we already mentioned in the introduction that $k(S) > q^r/d$ where d is the order of the group of diagonal automorphisms of S and the values of d for various groups are known, see [8] for instance. We are also done in the case p is the defining characteristic of S, since in which case $k_{p'}(S) > q^r/d$ by using the same arguments as in the proof of Lemma 2.3 and $d < 17r^2$ by directly checking the available values of the order d of the group of diagonal automorphisms of S from [8, Table 5]. For S an exceptional group, the theorem follows from our work in Section 5. Here we note that all the bounds obtained are of the form $c(q-1)^r$ where c is a constant depending on the rank r only. It is then straightforward to check that $c(q-1)^r > q^r/(17r^2)$ for all types and all $q > 2$. The case $q = 2$ can be proved by a direct check using [8,15].

Suppose $S = \mathrm{PSp}_{2r}(q)$ or $\Omega_{2r+1}(q)$. The case of odd p follows from Lemma 4.3. When $p = 2$ similar arguments as in the proof of Lemma 4.3 apply, with the remark that either $(q^r-1)/2$ or $(q^r+1)/2$ is odd (when q is odd), and hence the bound is $k_{p'}(S) > q^r/8r > q^r/(17r^2)$.

Let $S = \mathrm{P}\Omega^{\pm}_{2r}(q)$. From Subsection 4.2 we know that the minimum centralizer size of an element in S is at least

$$\frac{q^r(2, q^r - \epsilon 1)}{2(4, q^r - \epsilon 1)} \left[\frac{1 - 1/q}{2^k e}\right]^{1/2},$$

where $k := \min\{x \in \mathbb{N} : \max\{4, \log_q(4r)\} \leq 2^x\}$. On the other hand, by [2, Theorem 1.1], the proportion of p-regular elements in S is at least $1/4r$. Since $k_{p'}(S) \geq m|S_{p'}|/|S|$ where m is the minimum centralizer size of an element in S, we deduce that

$$k_{p'}(S) \geq \frac{q^r(2, q^r - \epsilon 1)}{8r(4, q^r - \epsilon 1)} \left[\frac{1 - 1/q}{2^k e}\right]^{1/2},$$

which is greater than $q^r/17r^2$ for all possible values of $q \geq 2$ and $r \geq 4$.

Finally let $S = \mathrm{PSL}^{\epsilon}_{r+1}(q)$ for $\epsilon = \pm$. From the proof of Lemma 3.10, we know that the minimum centralizer size of an element in S is at least

$$\frac{q^r H(r, q, \epsilon)}{(r+1, q - \epsilon 1)},$$

where

$$H(r, q, +) = \frac{1}{ek}$$

with $k := \min\{x \in \mathbb{N} : x \geq \log_q(r+2)\}$ and

$$H(r, q, -) = \left(\frac{q^2 - 1}{ek'(q+1)^2}\right)^{1/2}$$

with $k' := \min\{x \in \mathbb{N} : x \text{ odd and } x \geq \log_q(r+2)\}$. Moreover, by [1, Theorem 1.1], the proportion of p-regular elements in S is at least $1/(r+1)$ (note that $p \nmid q$). We deduce that

$$k_{p'}(S) \geq \frac{q^r H(r, q, \epsilon)}{(r+1)(r+1, q - \epsilon 1)}.$$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

It is straightforward to check that this bound is again larger than $q^r/(17r^2)$ for all possible q and r. $\square$

We remark that it is possible to prove that $k_{p'}(S) > q^r/(12r^2)$ for every S but the estimates are a lot more tedious. Also, when S is an even-dimensional orthogonal group, there is an explicitly computed constant $c > 0$ such that $k_{p'}(S) > cq^r/r$. By following the proof of Theorem 6.1, we therefore have:

Theorem 6.2. *Let S be a simple group of Lie type defined over the field of q elements with r the rank of the ambient algebraic group. Suppose that S is not linear or unitary. There exists a universal constant $c > 0$ such that*

$$k_{p'}(S) > \frac{cq^r}{r}$$

for every prime p.

7. p-Regular and p'-regular conjugacy classes

In this section we prove Theorem 1.1.

We start with an easy observation.

Lemma 7.1. *Let G be a finite group and $N \trianglelefteq G$. Then $k_p(G/N) \leq k_p(G)$ and $k_{p'}(G/N) \leq k_{p'}(G)$.*

Proof. Recall that $k_{p'}(G)$ is exactly the number of p-Brauer irreducible characters of G and every character of G/N can be viewed as a character of G. Therefore the inequality $k_{p'}(G/N) \leq k_{p'}(G)$ follows.

Now let gN be a p-element of G/N. Suppose that $g = g_p g_{p'} = g_{p'} g_p$ where g_p is a p-element and $g_{p'}$ is a p'-element. Then we have $gN = g_pNg_{p'}N = g_{p'}Ng_pN$ where g_pN is a p-element and $g_{p'}N$ is a p-regular element of G/N. Since gN is a p-element, it follows that $g_{p'}N = N$. Thus $gN = g_pN$, which means that every p-element of G/N has a representative which is a p-element of G, proving that $k_p(G/N) \leq k_p(G)$. $\square$

Next we improve a key result of [32].

Lemma 7.2. *Let V be an irreducible and faithful FH-module for some finite group H and finite field F of characteristic p. Suppose that p does not divide $|H|$. Then we have $k(H) + n(H,V) - 1 \geq 2\sqrt{p-1}$ with equality if and only if $\sqrt{p-1}$ is an integer, $|V| = |F| = p$ and $|H| = \sqrt{p-1}$.*

Proof. This follows from [32, Theorem 2.1] for $p \geq 59$. We take this opportunity to note that [32, Lemma 3.2] should be replaced by a different but similar statement, namely by "With the above notation and assumptions,

$$\max\{t+1,k\} \le \binom{t+k-1}{k-1} \le n(G,V).''$$

(in the notation of [32]). The statement is [12, Lemma 2.6]. This does not affect the proof of [32, Theorem 2.1], only straightforward and minor changes are to be made.

Assume that $p < 59$. For convenience, let $f(H,V) = k(H) + n(H,V) - 1$.

If $|V| = p$, then H is cyclic of order dividing $p-1$ and

$$f(H,V) = |H| + \frac{p-1}{|H|} \ge 2\sqrt{p-1}$$

with equality if and only if $\sqrt{p-1}$ is an integer and $|H| = \sqrt{p-1}$. From now on assume that $|V| > p$.

Let $|V| = p^2$. Assume first that H is solvable. The argument of Héthelyi, Külshammer [20, p. 661-662] gives $f(H,V) \ge (49p+1)/60$. It is easy to see that $(49p+1)/60 > 2\sqrt{p-1}$ unless $p \in \{2,3\}$. Let $p \in \{2,3\}$. We are finished if $k(H) \ge 3 > 2\sqrt{p-1}$. Otherwise $|H| \le 2$ and the integer $f(H,V)$ is at least $1+(p^2-1)/2 \ge 5/2$, and so $f(H,V) \ge 3 > 2\sqrt{p-1}$.

Assume now that $|V| = p^2$ and H is non-solvable. Then $H \le \mathbf{Z}(\mathrm{GL}(V))\cdot\mathrm{SL}(V)$ by [17, Theorem 3.5] and so $H/\mathbf{Z}(H)$ is isomorphic to A_5 and $p \in \{5,11,31,41\}$ by [23, p. 213-214] or [9, p. 285]. Moreover, since $|\mathbf{Z}(\mathrm{SL}(V))| = 2$, the factor group $H/(\mathbf{Z}(\mathrm{SL}(V)) \cap H)$ is a direct product of A_5 and a cyclic group of order (at least) $|\mathbf{Z}(H)|/2$. This implies that $k(H) \ge 2.5 \cdot |\mathbf{Z}(H)|$. We thus have

$$f(H,V) \ge 2.5 \cdot |\mathbf{Z}(H)| + \frac{p^2-1}{60 \cdot |\mathbf{Z}(H)|} = 2.5 \cdot |\mathbf{Z}(H)| + \frac{(2.5/60)\cdot(p^2-1)}{2.5 \cdot |\mathbf{Z}(H)|}. \tag{7.1}$$

The right-hand side of (7.1) is at least $2\sqrt{(2.5/60)\cdot(p^2-1)} > 0.4\sqrt{p^2-1}$, which is larger than $2\sqrt{p-1}$ unless $p \in \{5,11\}$. If $p = 5$, then $H = \mathrm{SL}(2,5) = \mathrm{SL}(V)$ and $f(H,V) = 10 > 2\sqrt{p-1}$. Assume that $p = 11$. If $\mathbf{Z}(H)$ is non-trivial, then $k(H) \ge 9$ and so $f(H,V) \ge 7 > 2\sqrt{10-1}$. If H is isomorphic to A_5 (a case which probably does not occur), then $k(H) = 5$ and $(11^2-1)/|H| = 2$ and so $f(H,V) \ge 7$.

Assume that $|V| \ge p^3$. Let $c = (p-1)/(p^3-1)$. If $k(H) > c \cdot |H|$, then

$$f(H,V) > c \cdot |H| + \frac{p^3-1}{|H|} = c \cdot |H| + \frac{c\cdot(p^3-1)}{c \cdot |H|} \ge 2\sqrt{c\cdot(p^3-1)} = 2\sqrt{p-1}.$$

Thus assume that $k(H) \le c \cdot |H|$.

Observe that $c \le 1/7$. The list of finite groups X with $k(X) \le 4$ found in [41] shows that $k(X) > |X|/7$. We may thus assume that $k(H) \ge 5$.

If $p \le 7$, then $f(H,V) \ge 5+1 > 2\sqrt{7-1} \ge 2\sqrt{p-1}$. We may have $p \ge 11$.

Observe that $c \le 1/133$. The list of finite groups X with $k(X) \le 8$ found in [41] shows that $k(X) > |X|/133$. We may thus assume that $k(H) \ge 9$.

If $p \le 23$, then $f(H,V) \ge 9+1 > 2\sqrt{23-1} \ge 2\sqrt{p-1}$. Assume that $p \ge 29$.

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Now $c \leq 1/871$. The list of finite groups X with $k(X) \leq 9$ found in [41] shows that $k(X) > |X|/871$. We may thus assume that $k(H) \geq 10$.

If $p \leq 31$, then $f(H,V) \geq 10+1 > 2\sqrt{31-1} \geq 2\sqrt{p-1}$. Assume that $p \geq 37$.

Let $k(H) = 10$ or $k(H) = 11$. The list in [41] shows that $|H| \leq 20160$ in the first case and $|H| \leq 29120$ in the second. Thus $f(H,V) \geq k(H) + (p^3-1)/|H| > 2\sqrt{p-1}$ for every prime p with $37 \leq p \leq 53$. Thus $k(H) \geq 12$.

We have $f(H,V) \geq 12+1 > 2\sqrt{p-1}$ for $p \leq 53$, unless $p = 47$ or $p = 53$. Moreover, if $k(H) \geq 14$, then $f(H,V) \geq 14+1 > 2\sqrt{53-1} \geq 2\sqrt{p-1}$. Thus we may assume that $(k(H),p) \in \{(12,47),(12,53),(13,47),(13,53)\}$.

Let $k(H) = 12$. Then $|H| \leq 43320$ or H is isomorphic to the Mathieu group M_{22} by [42]. In the former case $f(H,V) \geq 12 + (p^3-1)/43320 > 2\sqrt{p-1}$. Observe that $|M_{22}|$ is equal to 443520, which does not divide $|\mathrm{GL}(3,p)|$ (for $p \in \{47,53\}$). Thus in the second case $f(H,V) \geq 12 + (p^4-1)/|H| > 23 > 2\sqrt{p-1}$.

Finally, let $k(H) = 13$ and $p \in \{47,53\}$. If $p = 47$, then $f(H,V) \geq 14$ which is larger than $2\sqrt{p-1}$. Let $p = 53$. If H is not a nilpotent group, then the list in [43] shows that $|H| \leq 4840$ and so $f(H,V) \geq 13 + (53^3-1)/4840 > 2\sqrt{53-1}$. Let H be nilpotent. Since $13 = k(H) = \prod_{i=1}^{t} k(P_i)$ where P_i is a Sylow p_i-subgroup of H and $\{p_1,\dots,p_t\}$ is the set of distinct prime divisors of $|H|$ and since 13 is prime, we must have $t = 1$ and that H is a p_1-group. Now H cannot be transitive on $V \setminus \{0\}$ since $52 = (p-1) \mid (|V|-1)$ cannot divide $|H|$. This means that $f(H,V) \geq 13+2 > 2\sqrt{53-1}$. The proof is complete. $\square$

We finally can prove Theorem 1.1, which is restated below.

Theorem 7.3. *Let p be a prime and G be a finite group of order divisible by p. We have*

$$k_p(G) + k_{p'}(G) \geq 2\sqrt{p-1}.$$

Moreover, the equality occurs if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $\mathbf{C}_G(C_p) = C_p$.

Proof. If $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $\mathbf{C}_G(C_p) = C_p$, then

$$k_p(G) + k_{p'}(G) = 2\sqrt{p-1}.$$

Assume that G is different from the group $G = C_p \rtimes C_{\sqrt{p-1}}$ with $\mathbf{C}_G(C_p) = C_p$ when $\sqrt{p-1}$ is an integer. We proceed to show by induction on the size of G that $k_p(G) + k_{p'}(G) > 2\sqrt{p-1}$.

This is clearly true in case G is a cyclic group of order p (different from C_2). If G is an almost simple group, the claim follows from Theorem 2.1 unless $(\mathrm{Soc}(G),p) = (\mathsf{A}_5,5)$ or $(\mathrm{Soc}(G),p) = (\mathrm{PSL}_2(16),17)$. Even in these two exceptional cases the bound can be checked using [8].

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Let N be a non-trivial normal subgroup of G. We have

$$k_p(G/N) + k_{p'}(G/N) \leq k_p(G) + k_{p'}(G)$$

by Lemma 7.1. We may assume by induction that $p \nmid |G/N|$, or $\sqrt{p-1}$ is an integer, $G/N = C_p \rtimes C_{\sqrt{p-1}}$ with $\mathbf{C}_{G/N}(C_p) = C_p$ and

$$2\sqrt{p-1} = k_p(G/N) + k_{p'}(G/N) \leq k_p(G) + k_{p'}(G).$$

In this latter case we are finished by Lemma 7.1 unless $k_p(G/N) = k_p(G)$ and $k_{p'}(G/N) = k_{p'}(G)$. However, $k_p(G/N) < k_p(G)$ if $p \mid |N|$ and $k_{p'}(G/N) < k_{p'}(G)$ if $p \nmid |N|$. We are thus left with the case that $p \nmid |G/N|$ and $p \mid |N|$. Since $p \nmid |G/N|$ and $p \mid |N|$ hold for every non-trivial normal subgroup N of G, the group G must have a unique minimal normal subgroup V.

Assume that V is elementary abelian. Then G has a complement H for V by the Schur-Zassenhaus theorem. The subgroup H of G acts faithfully, coprimely and irreducibly on V. We have $k(H) + n(H, V) - 1 > 2\sqrt{p-1}$ by Lemma 7.2. Observe that $k_{p'}(G) \geq k_{p'}(G/V) = k_{p'}(H) = k(H)$ and that $k_p(G) \geq n(H, V) - 1$ since each H-orbit on V produces a G-conjugacy class of p-elements. These give the desired $k_{p'}(G) + k_p(G) > 2\sqrt{p-1}$ bound.

It remains to assume that V is non-abelian and thus it is isomorphic to a direct product of copies of a non-abelian simple group S. Since almost simple groups G have been treated before, we may assume that V is the direct product of at least two copies of S. As $p \mid |V|$, we have $p \mid |S|$. First suppose that (S, p) is neither $(\mathsf{A}_5, 5)$ nor $(\mathrm{PSL}_2(16), 17)$. From Theorem 2.1, we know that there are more than $2\sqrt{p-1}$ $\mathrm{Aut}(S)$-orbits of conjugacy classes of p-regular and p'-regular elements of S, and therefore there are more than $2\sqrt{p-1}$ G-orbits of those classes of V. Clearly, the number of these orbits is at most $k_p(G)+k_{p'}(G)$, and hence the theorem follows. Even in the case $(S, p) \in \{(\mathsf{A}_5, 5), (\mathrm{PSL}_2(16), 17)\}$ we are also done since the number of G-orbits on p-regular classes of V is, by [31, Section 3.2] (and, in case S is abelian, by [12, Lemma 2.6]), at least $k(k+1)/2$, where $k = n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) = 4$ for $(S, p) = (\mathsf{A}_5, 5)$ and 5 for $(S, p) = (\mathrm{PSL}_2(16), 17)$. We have finished the proof. $\square$

8. The number of Brauer characters of non-p-solvable groups

In this section we prove Theorem 1.2. Let p be a prime. The set of irreducible p-Brauer characters of a finite group G is denoted by $\mathrm{IBr}_p(G)$. We give two lower bounds for $|\mathrm{IBr}_p(G)|$ in case G is a non-p-solvable finite group. Our result can be compared to [33, Theorem 1.1] where it was shown that $|\mathrm{IBr}_p(G)|$ is bounded below by a function of $|G/\mathbf{O}_\infty(G)|$ where $\mathbf{O}_\infty(G)$ denotes the largest solvable normal subgroup of G.

Let G be a non-p-solvable finite group. Let $N := \mathbf{O}_\infty(G)$. We have $|\mathrm{IBr}_p(G)| = k_{p'}(G) \geq k_{p'}(G/N) = |\mathrm{IBr}_p(G/N)|$ by Lemma 7.1. It is sufficient to establish the bounds

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

for the group G/N, that is, we may assume that G has no elementary abelian minimal normal subgroup. We may also assume by the same argument that every minimal normal subgroup of G has order divisible by p.

Let $\mathrm{Soc}(G)$ denote the socle of G which is defined to be the product of all minimal normal subgroups of G. In this case this is a characteristic subgroup which is a direct product of non-abelian simple groups. Let S be a non-trivial direct summand of $\mathrm{Soc}(G)$.

Assume first that S is G-invariant. Observe that $k_{p'}(G)$ is at least the number of G-orbits of p-regular elements in S. This latter number is greater than $2\sqrt{p-1}$ by (iii) of Theorem 2.1, unless S and p appear in Table 1 and thus $p \leq 257$. In any case, $k_{p'}(G) > \sqrt{p-1}$.

We are left with the case when S is not G-invariant. Let $k = n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$. By Corollary 2.2, we have $k > \sqrt{p-1}$. Let t denote the number of different conjugates of S under G. By [31, Section 3.2] (and, in case S is abelian, by [12, Lemma 2.6]), we have

$$k_{p'}(G) \geq n(G, \mathrm{Cl}_{p'}(\mathrm{Soc}(G))) \geq \binom{k+t-1}{t} \geq \frac{k(k+1)}{2}.$$

If $p > 257$, then $k(k+1)/2 > 2(p-1) > 2\sqrt{p-1}$. If $p \leq 257$, then

$$k(k+1)/2 > (p-1)/2 \geq \sqrt{p-1},$$

unless $p \leq 3$. Finally, assume that $p \leq 3$. The group G has at least three different prime divisors by Burnside's Theorem. Thus $k_{p'}(G) \geq 3 > \sqrt{p-1}$.

9. p-Rational and p'-rational characters

In this section we prove Theorem 1.3.

We first prove Theorem 1.3 for p-solvable groups. In fact, we can do a bit more. The following implies Theorem 1.3 for p-solvable groups. Here $\mathbb{Q}_p$ denotes the cyclotomic extension of rational numbers by a primitive pth root of unity. Also, we use the standard notation $\mathbb{Q}(\chi)$ for the field of values of a character χ.

Theorem 9.1. *Let G be a finite p-solvable group of order divisible by p. Then*

$$|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathbb{Q}_p}(G)| \geq 2\sqrt{p-1}.$$

Proof. By induction we may assume that for every minimal normal subgroup N of G we have $p \nmid |G/N|$. It follows that G has a unique minimal normal subgroup V and $p \nmid |G/V|$. The group V has a complement H in G by the Schur-Zassenhaus theorem. The group V can be viewed as an irreducible and faithful FH-module where F is a finite field F of characteristic p. It follows by Lemma 7.2 that

$$k(H) + n(H, V) - 1 \geq 2\sqrt{p-1}.$$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

Note that every irreducible character of H, viewed as a character of G, has values in $\mathbb{Q}_{|H|}$, and hence is p-rational. Therefore G has exactly $k(H)$ p-rational characters whose kernels contain V.

We claim that G has at least $m := n(H, V) - 1$ irreducible characters with values in $\mathbb{Q}_p$ and their kernels do not contain V. Note that all characters of V have values in $\mathbb{Q}_p$.

Let $\theta_1, \theta_2, \ldots, \theta_m$ be representatives of the H-orbits on $\mathrm{Irr}(V)\backslash\{\mathbf{1}_H\}$. For each $1 \le i \le m$, the character θ_i has a *canonical extension* to $I_G(\theta_i)$, say $\widehat{\theta_i}$ such that $\mathbb{Q}(\widehat{\theta_i}) = \mathbb{Q}(\theta_i) \subseteq \mathbb{Q}_p$ (see [34, Corollary 6.4] for instance). It follows that $\mathbb{Q}(\widehat{\theta_i}^G) \subseteq \mathbb{Q}_p$. Also, by Clifford's theorem we have $\widehat{\theta_i}^G \in \mathrm{Irr}(G)$. Note that the $\widehat{\theta_i}^G$ are pairwise different. Therefore the claim follows.

Now we have

$$|\mathrm{Irr}_{\mathbb{Q}_p}(G) \cup \mathrm{Irr}_{\mathrm{p-rat}}(G)| \ge k(H) + n(H, V) - 1 \ge 2\sqrt{p-1},$$

which proves the theorem. $\square$

Lemma 9.2. *Let G be a nonsolvable group. Then $|\mathrm{Irr}_{2-rat}(G)| \ge 3$. Consequently, Theorem 1.3 holds for $p = 2$.*

Proof. By modding out a solvable normal subgroup if necessary, we assume that G has a nonabelian minimal normal subgroup N, which is a direct product of copies of a nonabelian simple group S. By [22, Lemma 4.1], there exists a non-principal character $\theta \in \mathrm{Irr}(S)$ that is extendible to a rational-valued character of $\mathrm{Aut}(S)$, and therefore G has a rational irreducible character χ which extends $\theta \times \cdots \times \theta \in \mathrm{Irr}(N)$.

If G/N has even order, then by Burnside's theorem it has a nontrivial rational irreducible character, and together with χ above and the trivial character, it follows that $|\mathrm{Irr}_{\mathbb{Q}}(G)| \ge 3$, as wanted. If $|G/N| > 1$ is odd, then every $\varphi \in \mathrm{Irr}(G/N)$ is 2-rational and thus all the characters of the form $\chi\varphi \in \mathrm{Irr}(G)$ are 2-rational, implying that $|\mathrm{Irr}_{2-rat}(G)| \ge 3$.

We now can assume that $G = N$. It is in fact sufficient to show that $|\mathrm{Irr}_{2-rat}(S)| \ge 3$ for every nonabelian simple group S. This is easy to check when S is a sporadic group, the Tits group, $\mathrm{PSL}_2(q)$ with $q \in \{5, 7, 8, 9, 17\}$, $\mathrm{PSL}_3(3)$, $\mathrm{PSU}_3(3)$, or $\mathrm{PSU}_4(2)$ using [8]. It is also easy for $S = \mathsf{A}_n$ by considering the restrictions of the irreducible characters of S labeled by the partitions $(n-1, 1)$ and $(n-2, 2)$. So we can, and we will, assume that S is not one of these groups. First note that the trivial and Steinberg characters of S are rational. We claim that S has a 2-rational semisimple character, and thus the required bound follows.

By the classification, we can find a simple algebraic group $\mathcal{G}$ of adjoint type and a Frobenius endomorphism $F : \mathcal{G} \to \mathcal{G}$ such that $S = [G, G]$ for $G := \mathcal{G}^F$. Let $(\mathcal{G}^*, F^*)$ be dual to $(\mathcal{G}, F)$ and let $G^* := {\mathcal{G}^*}^{F^*}$. By Lusztig's classification of the complex irreducible characters of finite reductive groups [10], each G^*-conjugacy class s^{G^*} of a semisimple element $s \in G^*$ corresponds to a semisimple character $\chi_s \in \mathrm{Irr}(G)$. This χ_s has values in $\mathbb{Q}_{|s|}$ by [16, Lemma 4.2] and moreover, by [40, Proposition 5.1], if $|s|$ is coprime to $|\mathbf{Z}(G^*)|$ then χ_s restricts irreducibly to S.

From the assumption on S, we have that $|G^*|$ is divisible by at least three different odd primes, and thus G^* always possesses a semisimple element s such that $(|s|, 2|\mathbf{Z}(G^*)|) = 1$. This s then corresponds to a semisimple character $\chi_s \in \mathrm{Irr}(G)$ such that χ_s restricts irreducibly to S and $\mathbb{Q}(\chi_s) \subseteq \mathbb{Q}_{|s|}$. Thus $(\chi_s)_S$ is 2-rational.

Theorem 1.3 follows for $p = 2$ since the solvable case was already treated in Theorem 9.1. $\square$

The following observation is crucial in the proof of Theorem 1.3 for odd p. It is well-known but we could not find a reference.

Lemma 9.3. *For every finite group X and odd prime p, $|\mathrm{Irr}_{\mathrm{p-rat}}(X)| \geq k_{p'}(X)$.*

Proof. The lemma is obvious when $p \nmid |X|$. So we assume $p \mid |X|$. Consider the natural actions of $\Gamma := \mathrm{Gal}(\mathbb{Q}_{|X|}/\mathbb{Q}_{|X|_{p'}}) \cong \mathrm{Gal}(\mathbb{Q}_{|X|_p}/\mathbb{Q})$ on classes and irreducible characters of X. Note that Γ is cyclic of order $|X|_p(p-1)/p$. Let ξ be a generator of Γ. By Brauer's permutation lemma, ξ fixes the same number of irreducible characters and classes. Each irreducible character fixed by ξ has values in $\mathbb{Q}_{|X|_{p'}}$ and therefore p-rational. On the other hand, for each conjugacy class $\mathrm{Cl}(g)$ of a p-regular element g, we have $\chi(g) \in \mathbb{Q}_{|X|_{p'}}$ for all $\chi \in \mathrm{Irr}(X)$, implying that $\mathrm{Cl}(g)$ is fixed by ξ. The lemma now follows. $\square$

Using the theory of the so-called B_p-characters [25], one can similarly show that, for a p-solvable group G, $|\mathrm{Irr}_{\mathrm{p'-rat}}(G)|$ is no less than the number of classes of p-elements. This seems to be true for all finite groups but remains to be confirmed.

Lemma 9.4. *Let G be a finite group with a non-abelian normal subgroup*

$$N \cong S \times \cdots \times S,$$

where S is simple, $2 < p \mid |S|$, and there are at least two factors of S in N. Then $|\mathrm{Irr}_{\mathrm{p-rat}}(G)| > 2\sqrt{p-1}$.

Proof. Let $k := n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S))$. Since there are at least two factors of S in N, as before we have $n(\mathrm{Aut}(N), \mathrm{Cl}_{p'}(N)) \geq k(k+1)/2$. Since $k \geq 2(p-1)^{1/4}$ by Theorem 2.1(ii) and G acts naturally on $\mathrm{Cl}_{p'}(N)$, it follows that $n(G, \mathrm{Cl}_{p'}(N)) > 2\sqrt{p-1}$, which in turn implies that $k_{p'}(G) > 2\sqrt{p-1}$. The lemma now follows by Lemma 9.3. $\square$

Theorem 9.5. *Let S be a nonabelian simple group of order divisible by $p > 2$ and $S \leq G \leq \mathrm{Aut}(S)$ be an almost simple group. Then*

$$|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| > 2\sqrt{p-1}.$$

Proof. Suppose first that S is not listed in Table 1. Then by Theorem 2.1(iii) we have $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > 2\sqrt{p-1}$. It follows that $k_{p'}(G) > 2\sqrt{p-1}$, implying that $|\mathrm{Irr}_{\mathrm{p-rat}}(G)| > 2\sqrt{p-1}$ by Lemma 9.3.

We now go over the simple groups in Table 1 and establish the bound for each of them. Indeed we are able to check most of them directly using [8,15], except the ones below.

Let $(S,p) = (\mathrm{PSU}_3(16), 241)$. In the proof of Lemma 3.5, we have shown that $k_{p'}(S) > 2(16^2 - 16 + 1)/3 > 160$. Therefore, if $|G/S| \leq 4$ then $k_{p'}(G) > 160/4 > 2\sqrt{p-1}$ and we are done. It remains to assume that $G = \mathrm{Aut}(S) = S \rtimes C_8$. Again in the proof of Lemma 3.5, we already showed that $G = \mathrm{Aut}(S)$ has at least 27 orbits on p-regular classes of S, and so $k_{p'}(G) \geq n(G, \mathrm{Cl}_{p'}(S)) + k_{p'}(G/S) - 1 \geq 27 + 7 = 34$. We now have $|\mathrm{Irr}_{\mathrm{p-rat}}(G)| > 2\sqrt{p-1}$, as desired.

Let $S = {}^2B_2(128)$ and $p = 113$ or 127. If $G = S$ then we have $k_{p'}(G) > 2\sqrt{p-1}$ as analyzed in Section 5 (1). So suppose $G > S$ and thus $G = \mathrm{Aut}(S) = S \rtimes C_7$. First we note that the trivial and Steinberg characters of S have rational extensions to $\mathrm{Aut}(S)$. Also, S has a rational class of elements of order 5 that is $\mathrm{Aut}(S)$-invariant, this semisimple class corresponds to a rational semisimple character of S of odd degree, which therefore has a rational extension to $\mathrm{Aut}(S)$ as well. By Gallagher's theorem, we obtain 21 irreducible characters of G with values in $\mathbb{Q}_7$.

As mentioned in Section 5, $\mathrm{Aut}(S)$ has four orbits of size 7 on classes of elements of order 145. One (semisimple) element in such an orbit produces an irreducible semisimple character of S with values in $\mathbb{Q}_{145}$ and moreover has S as the stabilizer group in $\mathrm{Aut}(S)$, and thus gives rise to 1 irreducible character of $\mathrm{Aut}(S)$ with values in $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{145}$, by Clifford's theorem. We now have 4 more irreducible p-rational characters of $G = \mathrm{Aut}(S)$, different from the 21 characters produced in the previous paragraph. We have shown that G has at least 25, which is larger than $2\sqrt{p-1}$, p-rational irreducible characters.

For $(S,p) = (\Omega_8^-(4), 257)$, using GAP we find that S has $32 = 2\sqrt{p-1}$ different element orders coprime to p, and so clearly $k_{p'}(G) > 32$ if $G \neq S$ since there is at least one p-regular class of G outside S. In fact we still have $k_{p'}(G) > 32$ when $G = S$ since S has at least four unipotent classes by Lemma 4.4 and at least 29 semisimple classes coming from 29 different odd element orders coprime to p. $\square$

We are now in position to prove Theorem 1.3 for all finite groups.

Theorem 9.6. *Let G be a finite group and p a prime divisor of $|G|$. Then*

$$|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| \geq 2\sqrt{p-1}.$$

Moreover, the equality occurs if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $\mathbf{C}_G(C_p) = C_p$.

Proof. First we prove the inequality. The case $p = 2$ is done by Lemma 9.2, so we will assume that p is odd. We proceed in the same way as in the proof of Theorem 9.1 to come up with the situation where G has a unique minimal normal subgroup N of order divisible by p such that $p \nmid |G/N|$. If N is abelian then we are done by Theorem 9.1, so we assume furthermore that N is nonabelian, which means that N is isomorphic to a direct product of say k copies of a nonabelian simple group S.

If $k \geq 2$, then we are done by Lemma 9.4. On the other hand, if $N = S$ then G is an almost simple group with socle S, and thus we are done as well by Theorem 9.5. This completes the proof of the first part of the theorem.

We now move on to prove the second part. If $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $\mathbf{C}_G(C_p) = C_p$, then

$$|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| = |\mathrm{Irr}(G)| = 2\sqrt{p-1}.$$

Assume that G is different from the group $C_p \rtimes C_{\sqrt{p-1}}$ with $\mathbf{C}_G(C_p) = C_p$ in case $\sqrt{p-1}$ is an integer. We proceed to prove by induction on the size of G that $|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| > 2\sqrt{p-1}$. This is clear in case G is a cyclic group of order p (excluding the case $p = 2$).

Let N be a minimal normal subgroup of G. We have $\mathrm{Irr}_{\mathrm{p-rat}}(G/N) \subseteq \mathrm{Irr}_{\mathrm{p-rat}}(G)$, $\mathrm{Irr}_{\mathrm{p'-rat}}(G/N) \subseteq \mathrm{Irr}_{\mathrm{p'-rat}}(G)$ and

$$\mathrm{Irr}_{\mathrm{p-rat}}(G/N) \cap \mathrm{Irr}_{\mathrm{p'-rat}}(G/N) = \mathrm{Irr}_{\mathbb{Q}}(G/N) \subseteq \mathrm{Irr}_{\mathbb{Q}}(G) = \mathrm{Irr}_{\mathrm{p-rat}}(G) \cap \mathrm{Irr}_{\mathrm{p'-rat}}(G).$$

We may assume by induction that $p \nmid |G/N|$, or that $\sqrt{p-1}$ is an integer, $G/N = C_p \rtimes C_{\sqrt{p-1}}$ with $\mathbf{C}_{G/N}(C_p) = C_p$.

In fact the case $p \nmid |G/N|$ is done by Lemma 9.4 and Theorem 9.5 when N is nonabelian and by Lemma 7.2 when N is abelian.

Assume that the latter case holds. First suppose that N is an elementary abelian r-group. It then may be viewed as an irreducible G/N-module. If the cyclic normal subgroup C_p of G/N acts fixed-point-freely on N and thus also on $\mathrm{Irr}(N)$, then there must be at least 1 p-rational irreducible character of G by Clifford's theorem which does not contain N in its kernel. This proves the desired bound. Assume that the cyclic normal subgroup C_p of G/N has a non-trivial fixed point on N. In this case $|N| = r$ and G contains an abelian normal subgroup M of order rp. Just as before, there is at least 1 p-rational irreducible character of G by Clifford's theorem which does not contain N in its kernel. Next we suppose N is non-abelian. As mentioned in the proof of Lemma 9.2, N has a nontrivial irreducible character that is extendible to a rational character of its inertia subgroup in G, and thus producing a rational irreducible character of G which does not contain N in its kernel. In either case we always have

$$|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| > |\mathrm{Irr}_{\mathrm{p-rat}}(G/N) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G/N)| > 2\sqrt{p-1},$$

as wanted. The proof is completed. $\square$

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

We conclude by remarking that although $|\mathrm{Irr}_{\mathrm{p-rat}}(G)| \geq k_{p'}(G)$ by Lemma 9.3 and $|\mathrm{Irr}_{\mathrm{p'-rat}}(G)|$ is conjecturally at least $1 + k_p(G)$ (see the discussion after Lemma 9.3), it does not follow that $|\mathrm{Irr}_{\mathrm{p-rat}}(G) \cup \mathrm{Irr}_{\mathrm{p'-rat}}(G)| \geq k_{p'}(G) + k_p(G)$, as $\mathrm{Irr}_{\mathrm{p-rat}}(G)$ and $\mathrm{Irr}_{\mathrm{p'-rat}}(G)$ have those rational characters, including the trivial character, in common. However, at the time of this writing, we have not found a counterexample yet.

Acknowledgments

The authors are grateful to the anonymous referees for their careful reading of the manuscript and helpful suggestions that led to a clearer exposition.

References

[1] L. Babai, S. Guest, C.E. Praeger, R.A. Wilson, Proportions of r-regular elements in finite classical groups, J. Lond. Math. Soc. 88 (2013) 202–226.
[2] L. Babai, P.P. Pálfy, J. Saxl, On the number of p-regular elements in finite simple groups, LMS J. Comput. Math. 12 (2009) 82–119.
[3] B. Baumeister, A. Maróti, H.P. Tong-Viet, Finite groups have more conjugacy classes, Forum Math. 29 (2017) 259–275.
[4] E.A. Bertram, Lower bounds for the number of conjugacy classes in finite groups, in: Ischia Group Theory 2004, in: Contemporary Mathematics, vol. 402, American Mathematical Society, Providence, RI, 2006, pp. 95–117.
[5] R. Brauer, On groups whose order contains a prime number to the first power, I, Am. J. Math. 64 (1942) 401–420.
[6] R. Brauer, Representations of Finite Groups, Lectures on Modern Mathematics, vol. I, Wiley, New York, 1963, pp. 133–175.
[7] R.W. Carter, Finite Groups of Lie Type. Conjugacy Classes and Complex Characters, Wiley and Sons, New York, 1985, 544 pp.
[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
[9] L.E. Dickson, Linear Groups: With an Exposition of the Galois Field Theory. With an Introduction by W. Magnus, Dover Publications, Inc., New York, 1958.
[10] F. Digne, J. Michel, Representations of finite groups of Lie type, Lond. Math. Soc. Stud. Texts 21 (1991), 159 pp.
[11] H. Enomoto, The characters of the finite symplectic group $\mathrm{Sp}(4, q)$, $q = 2^f$, Osaka Math. J. 9 (1972) 75–94.
[12] D.A. Foulser, Solvable primitive permutation groups of low rank, Trans. Am. Math. Soc. 143 (1969) 1–54.
[13] J. Fulman, A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups, J. Algebra 234 (2000) 207–224.
[14] J. Fulman, R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, Trans. Am. Math. Soc. 364 (2012) 3023–3070.
[15] The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.4, http://www.gap-system.org, 2004.
[16] E. Giannelli, N.N. Hung, A.A. Schaeffer Fry, C. Vallejo, Characters of π'-degree and small cyclotomic fields, Ann. Mat. Pura Appl. (2021), https://doi.org/10.1007/s10231-020-01025-x, in press.
[17] M. Giudici, Maximal subgroups of almost simple groups with socle PSL(2,q), arXiv:math/0703685.
[18] S. Gonshaw, M.W. Liebeck, E.A. O'Brien, Unipotent class representatives for finite classical groups, J. Group Theory 20 (2017) 505–525.
[19] L. Héthelyi, B. Külshammer, On the number of conjugacy classes of a finite solvable group, Bull. Lond. Math. Soc. 32 (2000) 668–672.
[20] L. Héthelyi, B. Külshammer, On the number of conjugacy classes of a finite solvable group. II, J. Algebra 270 (2003) 660–669.

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007

[21] L. Héthelyi, E. Horváth, T.M. Keller, A. Maróti, Groups with few conjugacy classes, Proc. Edinb. Math. Soc. 54 (2011) 423–430.
[22] N.N. Hung, A.A. Schaeffer Fry, H.P. Tong-Viet, C.R. Vinroot, On the number of irreducible real-valued characters of a finite group, J. Algebra 555 (2020) 275–288.
[23] B. Huppert, Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, vol. 134, Springer-Verlag, Berlin-New York, 1967.
[24] B. Huppert, Singer-Zyklen in klassischen Gruppen, Math. Z. 117 (1970) 141–150.
[25] I.M. Isaacs, Characters of π-separable groups, J. Algebra 86 (1984) 98–128.
[26] T.M. Keller, Lower bounds for the number of conjugacy classes of finite groups, Math. Proc. Camb. Philos. Soc. 147 (2009) 567–577.
[27] T.M. Keller, Finite groups have even more conjugacy classes, Isr. J. Math. 181 (2011) 433–444.
[28] E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante, Math. Ann. 56 (1903) 671–676.
[29] I.G. Macdonald, Numbers of conjugacy classes in some finite classical groups, Bull. Aust. Math. Soc. 23 (1981) 23–48.
[30] G. Malle, Fast-einfache Gruppen mit langen Bahnen in absolut irreduzibler Operation, J. Algebra 300 (2006) 655–672.
[31] G. Malle, A. Maróti, On the number of p'-degree characters in a finite group, Int. Math. Res. Not. 20 (2016) 6118–6132.
[32] A. Maróti, A lower bound for the number of conjugacy classes of a finite group, Adv. Math. 290 (2016) 1062–1078.
[33] A. Moretó, H.N. Nguyen, Variations of Landau's theorem for p-regular and p-singular conjugacy classes, Isr. J. Math. 212 (2016) 961–987.
[34] G. Navarro, Character Theory and the McKay Conjecture, Cambridge Studies in Advanced Mathematics, vol. 175, Cambridge University Press, Cambridge, 2018.
[35] H.N. Nguyen, Low-dimensional complex characters of the symplectic and orthogonal groups, Commun. Algebra 38 (2010) 1157–1197.
[36] L. Pyber, Finite groups have many conjugacy classes, J. Lond. Math. Soc. 46 (1992) 239–249.
[37] W.A. Simpson, J.S. Frame, The character tables for $\mathrm{SL}(3,q)$, $\mathrm{SU}(3,q^2)$, $\mathrm{PSL}(3,q)$, $\mathrm{PSU}(3,q^2)$, Can. J. Math. 25 (1973) 486–494.
[38] B. Srinivasan, The characters of the finite symplectic group $\mathrm{Sp}(4,q)$, Trans. Am. Math. Soc. 131 (1968) 488–525.
[39] M. Suzuki, A new type of simple groups of finite order, Proc. Natl. Acad. Sci. USA 46 (1960) 868–870.
[40] P.H. Tiep, Real ordinary characters and real Brauer characters, Trans. Am. Math. Soc. 367 (2015) 1273–1312.
[41] A. Vera López, J. Vera López, Classification of finite groups according to the number of conjugacy classes, Isr. J. Math. 51 (1985) 305–338.
[42] A. Vera López, J. Vera López, Classification of finite groups according to the number of conjugacy classes II, Isr. J. Math. 56 (1986) 188–221.
[43] A. Vera López, J. Sangroniz, The finite groups with thirteen and fourteen conjugacy classes, Math. Nachr. 280 (2007) 676–694.
[44] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Aust. Math. Soc. 3 (1963) 1–62.
[45] R.A. Wilson, The Finite Simple Groups, Graduate Texts in Mathematics, vol. 251, Springer-Verlag, London, Ltd., London, 2009.

Please cite this article in press as: N.N. Hung, A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, J. Algebra (2021), https://doi.org/10.1016/j.jalgebra.2021.02.007