ON ALMOST p-RATIONAL CHARACTERS OF p'-DEGREE

NGUYEN NGOC HUNG, GUNTER MALLE, AND ATTILA MARÓTI

Abstract. Let p be a prime and G a finite group. A complex character of G is called *almost p-rational* if its values belong to a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for some $n \in \mathbb{Z}^+$ prime to p or precisely divisible by p. We prove that, in contrast to usual p-rational characters, there are always "many" almost p-rational irreducible characters in finite groups. We obtain both explicit and asymptotic bounds for the number of almost p-rational irreducible characters of G in terms of p. In fact, motivated by the McKay–Navarro conjecture, we obtain the same bound for the number of such characters of p'-degree and prove that, in the minimal situation, the number of almost p-rational irreducible p'-characters of G coincides with that of $\mathbf{N}_G(P)$ for $P \in \mathrm{Syl}_p(G)$. Lastly, we propose a new way to detect the cyclicity of Sylow p-subgroups of a finite group G from its character table, using almost p-rational irreducible p'-characters and the blockwise refinement of the McKay–Navarro conjecture.

1. Introduction

Let G be a finite group and p a prime. Recall that a character χ of G is called *p-rational* if its values lie in a cyclotomic field $\mathbb{Q}_n := \mathbb{Q}(e^{2i\pi/n})$ for some positive integer n prime to p. Extending this notion, we say that χ is *almost p-rational* if the values of χ are in $\mathbb{Q}_n$ for some n divisible by p at most once.

p-Rational characters appear in several contexts. One reason is that they behave nicely with regard to character extensions, see [Isa, Theorems 6.30 and 11.32]. Another is that they are pointwise fixed under the Galois group $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_{|G|_{p'}})$, where $|G|_{p'}$ is the p'-part of $|G|$, and therefore they play an important role in problems concerning Galois actions on irreducible characters and conjugacy classes, see [Nav2, Chapters 3 and 9].

In this paper we show that almost p-rational characters also occur naturally in group representation theory, but they are somewhat richer and more interesting than p-rational characters in at least one aspect: there are always "many" of them in finite groups. This

2010 *Mathematics Subject Classification.* Primary 20C15, 20E45, 20D20; Secondary 20D05, 20D10.

Key words and phrases. Finite groups, p-rational characters, p'-degree characters, McKay–Navarro conjecture, linear actions, coprime actions.

The second author gratefully acknowledges support by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Project-ID 286237555– TRR 195. The work of the third author on the project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 741420), and is supported by the Hungarian National Research, Development and Innovation Office (NKFIH) Grant No. K132951, Grant No. K115799 and Grant No. K138828. We thank Gabriel Navarro for his insightful comments on an earlier version of the manuscript.

is in contrast to p-rationality: every odd-order p-group has a unique p-rational irreducible character, for instance.

To conveniently state the results, let us use $\mathrm{Irr}_{p\text{-ar}}(G)$ to denote the set of almost p-rational irreducible characters of G.

Theorem 1.1. *Let G be a finite group and let p be a prime dividing the order of G. Then $|\mathrm{Irr}_{p\text{-ar}}(G)| \geq 2\sqrt{p-1}$. Moreover, equality occurs if and only if $p-1$ is a perfect square and G is isomorphic to the Frobenius group $C_{p^n} \rtimes C_{\sqrt{p-1}}$ for some $n \in \mathbb{Z}^+$.*

Theorem 1.2. *There exists a universal constant $c > 0$ such that for every prime p and every finite group G having a non-cyclic Sylow p-subgroup, $|\mathrm{Irr}_{p\text{-ar}}(G)| > c \cdot p$.*

Besides the fact that the notion of almost p-rationality naturally extends p-rationality and hence it is interesting in its own right, there are two other motivations for our results. The first comes from the results in [HK1, Mar3, HK2, MS] on bounding from below the number of conjugacy classes, which is also the number of irreducible characters, of a finite group. We show that similar bounds hold for the number of irreducible characters with a specific field of values, namely the field generated by roots of unity of order with p-part at most p.

Another motivation comes from the celebrated McKay–Navarro conjecture, which asserts that there exists a permutation isomorphism between the actions of a certain subgroup of the Galois group $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on the set of p'-degree irreducible characters of G and that of the normalizer $\mathbf{N}_G(P)$ of some $P \in \mathrm{Syl}_p(G)$ (see [Nav1]), and therefore produces a compatibility between the values of p'-characters of G and those of $\mathbf{N}_G(P)$. The next result is based on Theorem 1.1 and the McKay–Navarro conjecture. Here we use $\mathrm{Irr}_{p',p\text{-ar}}(G)$ for the set of those characters in $\mathrm{Irr}_{p\text{-ar}}(G)$ with p'-degree, and prove that $|\mathrm{Irr}_{p',p\text{-ar}}(G)|$ is minimal (in terms of p) if and only if $|\mathrm{Irr}_{p',p\text{-ar}}(\mathbf{N}_G(P))|$ is minimal, a result consistent with the McKay–Navarro conjecture.

Theorem 1.3. *Let G be a finite group, p a prime dividing the order of G and P a Sylow p-subgroup of G. Then $|\mathrm{Irr}_{p',p\text{-ar}}(G)| \geq 2\sqrt{p-1}$. Moreover, the following are equivalent:*

(i) $|\mathrm{Irr}_{p',p\text{-ar}}(G)| = 2\sqrt{p-1}$*;*
(ii) $|\mathrm{Irr}_{p',p\text{-ar}}(\mathbf{N}_G(P))| = 2\sqrt{p-1}$*;*
(iii) *P is cyclic and $\mathbf{N}_G(P)$ is isomorphic to the Frobenius group $P \rtimes C_{\sqrt{p-1}}$.*

This improves the main result of [MM] by bringing character values into consideration. We remark also that recent work [GHSV] on characters of π'-degree with small cyclotomic field of values implies that, for any pair $\{p, q\}$ of primes and any non-trivial group G, the two sets $\mathrm{Irr}_{p',p\text{-ar}}(G)$ and $\mathrm{Irr}_{q',q\text{-ar}}(G)$ always contain a non-trivial common character. This somewhat indicates that the sets $\mathrm{Irr}_{p',p\text{-ar}}(G)$ are "large" (see Theorem 9.2 for details), a phenomenon that is reinforced in a clearer way by Theorem 1.3.

Let $\Phi(P)$, as usual, denote the Frattini subgroup of a Sylow p-subgroup P of G. The conditions in Theorems 1.1, 1.2, and 1.3 on P being non-trivial and non-cyclic are equivalent to the conditions $p \mid |P/\Phi(P)|$ and $p^2 \mid |P/\Phi(P)|$, respectively. In view of the McKay–Navarro conjecture and other local/global conjectures, it is not surprising that the local group $P/\Phi(P)$ is a key invariant that controls the global numbers $|\mathrm{Irr}_{p',p\text{-ar}}(G)|$ and $|\mathrm{Irr}_{p\text{-ar}}(G)|$. In fact, when G is an abelian p-group we have $|\mathrm{Irr}_{p\text{-ar}}(G)| = |\mathrm{Irr}_{p',p\text{-ar}}(G)| = |P/\Phi(P)|$.

In the next main result we make an attempt to push the bound in Theorem 1.3 up to p, with the help of the (known) solvable case of the McKay–Navarro conjecture (due to Dade).

Theorem 1.4. *Let G be a finite group, p a prime and P a Sylow p-subgroup of G. If $|P/\Phi(P)| \geq p^3$, then $|\mathrm{Irr}_{p',p\text{-ar}}(G)| > p$ provided that any of the following two conditions holds.*

1. *G is solvable and $p > 7200$; or*
2. *the McKay–Navarro conjecture is true and p is sufficiently large.*

The conditions in Theorem 1.4 on G being solvable and p being large are perhaps superfluous but we are not able to remove either of them at this time. On the other hand, the condition $|P/\Phi(P)| \geq p^3$ is necessary. For every prime p there is a metacyclic group G such that $|P| = |P/\Phi(P)| = p$ and $|\mathrm{Irr}_{p\text{-ar}}(G)| \leq p$. Moreover, results in Section 7 show that there are infinitely many primes p for which there are examples of groups G and P with $|P/\Phi(P)| = p^2$ and $|\mathrm{Irr}_{p\text{-ar}}(G)| \leq p$.

The proof of Theorem 1.4 depends on a result concerning the existence of a linear p'-group $H \leq \mathrm{GL}(V)$, where V is a finite vector space in characteristic p, such that the class number $k(HV)$ of HV is at most p, see Theorems 7.11 and 8.9. This existence result may be of independent interest and useful in other purposes, as discussed at the beginning of Section 7. In fact, our results in Sections 7 and 8 point out a possible way to detect the cyclicity of Sylow p-subgroups of a finite group from its character table using almost p-rational p'-characters. This was known only for $p = 2, 3$, in a recent work of Rizo, Schaeffer Fry, and Vallejo [RSV].

The McKay–Navarro conjecture admits a blockwise refinement, which is often referred to as the Alperin–McKay–Navarro conjecture, see [Nav1, Conjecture B]. Let

$$\mathrm{Irr}_{p',p\text{-ar}}(B_0(G)) := \mathrm{Irr}_{p',p\text{-ar}}(G) \cap B_0(G),$$

where $B_0(G)$ is the principal p-block G. The refinement implies that

$$|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| = |\mathrm{Irr}_{p',p\text{-ar}}(B_0(\mathbf{N}_G(P)))| = |\mathrm{Irr}(\mathbf{N}_G(P)/\Phi(P)\mathbf{O}_{p'}(\mathbf{N}_G(P)))|,$$

where $P \in \mathrm{Syl}_p(G)$, see Section 2 for more details. As $\mathbf{N}_G(P)/\Phi(P)\mathbf{O}_{p'}(\mathbf{N}_G(P))$ is a semidirect product of the p'-group $\mathbf{N}_G(P)/P\mathbf{O}_{p'}(\mathbf{N}_G(P)))$ acting faithfully on the vector space $P/\Phi(P)$, to characterize the cyclicity of P, one would need to understand the values of the class numbers of these semidirect direct products.

Note that if $\dim(V) = 1$ then $k(HV) = e + \frac{p-1}{e}$, where $e = |H| \mid (p-1)$. Our work on the values of class numbers of affine groups seems to suggest that the class numbers $k(HV)$ with $\dim(V) = 1$ are distinguished from those with $\dim(V) > 1$. We indeed confirm this for p sufficiently large. This observation and the Alperin–McKay–Navarro conjecture lead us to the following deep question on the connection between Galois automorphisms and cyclic Sylow subgroups. Here $\mathcal{S}_p := \{e + \frac{p-1}{e} : e \in \mathbb{Z}^+, e \mid p-1\}$.

Question 1.5. *Let G be a finite group and p a prime dividing $|G|$. Is it true that Sylow p-subgroups of G are cyclic if and only if $|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| \in \mathcal{S}_p$?*

An affirmative answer to Question 1.5 would provide an(other) answer to Brauer's Problem 12 [Bra2], which asks for information about the structure of Sylow p-subgroups of G

one can obtain from the character table of G. The problem has inspired several interesting local/global results over the past two decades, such as [NTT, NT2, NST, SF, NT3, Mal2], to name a few. Note also that, when $p \leq 3$, $\mathcal{S}_p = \{p\}$, and thus the statement is equivalent to: Sylow p-subgroups of G are cyclic if and only if $|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| = p$, which is exactly what was shown in [RSV].

Theorems 1.1, 1.2, 1.3, and 1.4 are proved in Sections 3, 6, 4, and 9, respectively. In the last Section 10, we make some remarks on Question 1.5 and answer it for p-solvable groups with p sufficiently large.

2. The McKay–Navarro conjecture

Let $\mathrm{Irr}(G)$ denote the set of all irreducible ordinary characters of a finite group G, and let $\mathrm{Irr}_{p'}(G) := \{\chi \in \mathrm{Irr}(G) : p \nmid \chi(1)\}$, where p is a prime. The well-known McKay conjecture [McK] asserts that, for every G and every p, the number of p'-degree irreducible characters of G equals that of the normalizer $\mathbf{N}_G(P)$ of a Sylow p-subgroup P of G. That is,

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(\mathbf{N}_G(P))|.$$

Navarro proposed that there should be a bijection from $\mathrm{Irr}_{p'}(G)$ to $\mathrm{Irr}_{p'}(\mathbf{N}_G(P))$ that commutes with the action of the subgroup $\mathcal{H}$ of the Galois group $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ consisting of those automorphisms that send every root of unity $\xi \in \mathbb{Q}_{|G|}$ of order not divisible by p to ξ^q, where q is a certain fixed power of p, see [Nav2, Conjecture 9.8] and also [Nav1, Tur1, NSV] for more updates. This refinement of the McKay conjecture has now become the McKay–Navarro conjecture, also known as the Galois-McKay conjecture.

We define the *p-rationality level* of a character χ to be the smallest nonnegative integer $\alpha := \alpha_p(\chi)$ such that the values of χ belong to the cyclotomic field $\mathbb{Q}_n := \mathbb{Q}(e^{2\pi i/n})$ for some n divisible by p^α. Remark that χ is p-rational if and only if $\alpha_p(\chi) = 0$ and χ is almost p-rational if and only if $\alpha_p(\chi) \leq 1$. (In a very recent paper [NT4], Navarro and Tiep call the smallest positive integer n such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_n$ the *conductor* of χ, denoted by $c(\chi)$. The p-rationality level of χ simply is the logarithm to the base p of the p-part of $c(\chi)$; that is $\alpha_p(\chi) = \log_p(c(\chi)_p)$. We thank G. Navarro for pointing out this connection to us.)

As $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_{p^\alpha |G|_{p'}})$ is contained in $\mathcal{H}$ for every $\log_p |G|_p \geq \alpha \in \mathbb{Z}^{\geq 0}$, the McKay–Navarro conjecture implies that the number of p'-degree irreducible characters at any level α in G and $\mathbf{N}_G(P)$ would be the same:

$$|\{\chi \in \mathrm{Irr}_{p'}(G) : \alpha_p(\chi) = \alpha\}| = |\{\theta \in \mathrm{Irr}_{p'}(\mathbf{N}_G(P)) : \alpha_p(\theta) = \alpha\}|.$$

Since every irreducible character of $\mathbf{N}_G(P)$ of p'-degree has kernel containing the commutator subgroup P' of P and every irreducible character of $\mathbf{N}_G(P)/P'$ is automatically of p'-degree, we then have

$$|\{\chi \in \mathrm{Irr}_{p'}(G) : \alpha_p(\chi) \leq 1\}| = |\{\theta \in \mathrm{Irr}(\mathbf{N}_G(P)/P') : \alpha_p(\theta) \leq 1\}|,$$

which means that

$$|\mathrm{Irr}_{p',p\text{-ar}}(G)| = |\mathrm{Irr}_{p\text{-ar}}(\mathbf{N}_G(P)/P')|.$$

Now suppose for a moment that $|G|$ is divisible by p. Then $|\mathbf{N}_G(P)/P'|$ is also divisible by p, and thus, by Theorem 1.1 and the conclusion of the previous paragraph, the McKay–Navarro conjecture implies that the number of almost p-rational irreducible characters of p'-degree of G is at least $2\sqrt{p-1}$, as claimed in the Introduction.

The Alperin-McKay-Navarro conjecture refines further the McKay-Navarro conjecture by considering blocks. In a similar way as with the McKay-Navarro conjecture, it implies, for every block B with a defect group D, that

$$|\mathrm{Irr}_0(B) \cap \mathrm{Irr}_{p\text{-ar}}(B)| = |\mathrm{Irr}_0(b) \cap \mathrm{Irr}_{p\text{-ar}}(b)|,$$

where b is the Brauer correspondent of B and $\mathrm{Irr}_0(B)$ and $\mathrm{Irr}_{p\text{-ar}}(B)$ respectively denote the sets of height zero characters and almost p-rational characters in B. In particular, for principal blocks, we would have

$$|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| = |\mathrm{Irr}_{p',p\text{-ar}}(B_0(\mathbf{N}_G(P)))|$$

Note that both the McKay–Navarro conjecture and its blockwise refinement are known to be true for p-solvable groups, proved by Turull [Tur1, Tur2], and for groups with a cyclic Sylow p-subgroup, established by Navarro [Nav1].

3. An explicit bound for $|\mathrm{Irr}_{p\text{-ar}}(G)|$

In this section we prove Theorem 1.1. We do so by relating almost p-rationality of characters and almost p-regularity of conjugacy classes. This connection will be used in Section 6 as well to achieve the asymptotic bound.

We start with the easier case $p = 2$. Note that almost 2-rational characters are precisely 2-rational characters.

Lemma 3.1. *Let G be a finite group of even order. Then $|\mathrm{Irr}_{2\text{-rat}}(G)| \geq 2$ with equality if and only if G is a non-trivial cyclic 2-group.*

Proof. The bound $|\mathrm{Irr}_{2\text{-rat}}(G)| \geq 2$ is clear from Burnside's theorem that groups of even order always possess a non-trivial rational irreducible character. It is also clear that the number of 2-rational irreducible characters of a non-trivial cyclic 2-group is exactly 2. It remains to show that if $|\mathrm{Irr}_{2\text{-rat}}(G)| = 2$ then G must be a non-trivial cyclic 2-group. If G is non-solvable then it was shown in [HM, Lemma 9.2] that $|\mathrm{Irr}_{2\text{-rat}}(G)| \geq 3$ and thus we are done.

So suppose that G is solvable and $|\mathrm{Irr}_{2\text{-rat}}(G)| = 2$. First we have $\mathbf{O}^{2'}(G) = G$ and moreover $G/\mathbf{O}^2(G)$ is cyclic since otherwise $|\mathrm{Irr}_{2\text{-rat}}(G)| > 2$. We claim that $L := \mathbf{O}^2(G)$ is trivial. Assume otherwise, then $G_1 := G/\mathbf{O}^{2'}(L)$ is a semidirect product of a 2-group A isomorphic to G/L acting on a non-trivial odd-order group B isomorphic to $L/\mathbf{O}^{2'}(L)$. Since A is cyclic, every $\theta \in \mathrm{Irr}(B)$ is extendible to the inertia subgroup $I_{G_1}(\theta)$. In fact, by [Nav2, Corollary 6.4], θ has a unique extension $\chi \in \mathrm{Irr}(I_{G_1}(\theta))$ such that $\mathbb{Q}(\chi) = \mathbb{Q}(\theta)$. Now by Clifford's correspondence we have that $\chi^{G_1} \in \mathrm{Irr}(G_1)$ is 2-rational, implying that $|\mathrm{Irr}_{2\text{-rat}}(G_1)| \geq 3$, a contradiction.

We have shown that G is a 2-group. If $G/\Phi(G)$ is elementary abelian of 2-rank at least 2 then G would have at least 4 rational characters, a contradiction. We conclude that $G/\Phi(G)$ is cyclic, which means that G is cyclic as well. □

To bound the number of almost p-rational irreducible characters, it is helpful to work with the dual notion for conjugacy classes, namely almost p-regular classes. We therefore define the *p-regularity level* of a conjugacy class g^G of G to be $\log_p(|g|_p)$, where $|g|_p$ is the p-part of the order of g. Clearly a class g^G is p-regular if its p-regularity level is 0. We say that g^G is *almost p-regular* if its level is at most 1.

Let $\mathrm{Cl}_{p\text{-reg}}(G)$ denote the set of p-regular classes and $\mathrm{Cl}_{p\text{-areg}}(G)$ denote the set of almost p-regular classes of G. We use $k(G)$ to denote the number of conjugacy classes of G. Recall that $\mathrm{Irr}_{p\text{-rat}}(G)$ and $\mathrm{Irr}_{p\text{-ar}}(G)$ are the sets of p-rational and almost p-rational, respectively, irreducible characters of G. Finally, $n(G, X)$ denotes the number of orbits of a group G acting on a set X.

We observe that if the exponent of a finite group G is not divisible by p^2, then $k(G) = |\mathrm{Cl}_{p\text{-areg}}(G)| = |\mathrm{Irr}_{p\text{-ar}}(G)|$.

The following fact will be used often in our proofs.

Lemma 3.2. *Let G be a finite group and let p be an odd prime. Then $|\mathrm{Cl}_{p\text{-areg}}(G)| \leq |\mathrm{Irr}_{p\text{-ar}}(G)|$ and $|\mathrm{Cl}_{p\text{-reg}}(G)| \leq |\mathrm{Irr}_{p\text{-rat}}(G)|$.*

Proof. If $|G|$ is not divisible by p^2 then all the classes of G are almost p-regular and all the characters of G are almost p-rational, and hence the lemma follows. Suppose $p^2 \mid |G|$. Consider the natural actions of the Galois group $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_{p|G|_{p'}})$ on classes and irreducible characters of G. Note that this group is cyclic of order $|G|_p/p$, and let σ be a generator of the group. An irreducible character of G is almost p-rational if and only if it is σ-fixed, while if a class of G is almost p-regular then the class is σ-fixed. The first inequality then follows by Brauer's permutation lemma.

The second inequality is well-known and indeed can be proved similarly. □

Lemma 3.3. *Let N be a p'-group and $N \trianglelefteq G$. Then*

$$|\mathrm{Cl}_{p\text{-areg}}(G)| \geq |\mathrm{Cl}_{p\text{-areg}}(G/N)| + n(G, \mathrm{Cl}_{p\text{-areg}}(N)) - 1,$$

where $n(G, \mathrm{Cl}_{p\text{-areg}}(N))$ is the number of G-orbits on $\mathrm{Cl}_{p\text{-areg}}(N)$.

Proof. It is clear that the number of almost p-regular classes of G inside N is at least $n(G, \mathrm{Cl}_{p\text{-areg}}(N))$. Let gN be an element of G/N of order not divisible by p^2. Let $g = g_p g_{p'} = g_{p'} g_p$ where g_p is a p-element and $g_{p'}$ is a p'-element. Then $gN = g_pN \cdot g_{p'}N = g_{p'}N \cdot g_pN$. Now the order of g_pN is not divisible by p^2, and thus $g_p^pN = N$, which implies that $g_p^p = 1$ by the assumption on N. We have shown that if $(gN)^{G/N}$ is an almost p-regular class then g is an almost p-regular element of G. The lemma follows. □

Next we record a consequence of a recent result [HM] on bounding the number of $\mathrm{Aut}(S)$-orbits on the set of p-regular classes of a non-abelian finite simple group S.

Lemma 3.4. *Let S be a non-abelian simple group of order divisible by a prime p. The number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S is at least $2(p-1)^{1/4}$. Moreover, if this number is at most $2\sqrt{p-1}$ then $p \leq 257$ and $p^2 \nmid |S|$.*

Proof. This follows from [HM, Theorem 2.1]. □

Lemma 3.5. *Let G be a finite group having a non-abelian minimal normal subgroup N and p an odd prime such that $p \mid |N|$ but $p \nmid |G/N|$. Then $|\mathrm{Irr}_{p\text{-ar}}(G)| > 2\sqrt{p-1}$.*

Proof. By hypothesis N is isomorphic to a direct product of copies of a non-abelian simple group, say S. Let n be the number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S. First suppose that there are $k > 1$ simple factors in N. We then have $|\mathrm{Cl}_{p\text{-reg}}(G)| \geq \binom{n+k-1}{k} \geq n(n+1)/2$. By Lemma 3.4 we know that $n \geq 2(p-1)^{1/4}$. Therefore it follows that $|\mathrm{Cl}_{p\text{-reg}}(G)| > 2\sqrt{p-1}$ and we are done by Lemma 3.2. So we assume that N is a non-abelian simple group.

If $n > 2\sqrt{p-1}$, then by the same arguments we are also done. So we assume furthermore that $n \leq 2\sqrt{p-1}$. Using Lemma 3.4 again, we know that p is a prime divisor of $|S|$ such that $p^2 \nmid |S|$. Therefore, by the assumption, $p \mid |G|$ but $p^2 \nmid |G|$. It follows that

$$|\mathrm{Irr}_{p\text{-ar}}(G)| = k(G) \geq 2\sqrt{p-1},$$

by [Bra1]. The equality occurs only when G is the Frobenius group $C_p \rtimes C_{\sqrt{p-1}}$ by [Mar3, Theorem 1.1], which is not the case here. Thus we have $|\mathrm{Irr}_{p\text{-ar}}(G)| > 2\sqrt{p-1}$, and the proof is finished. □

We can now prove Theorem 1.1 for odd p.

Theorem 3.6. *Let G be a finite group and $p \geq 3$ a prime dividing the order of G. Then $|\mathrm{Irr}_{p\text{-ar}}(G)| \geq 2\sqrt{p-1}$. Equality occurs if and only if $p-1$ is a perfect square and G is isomorphic to the Frobenius group $C_{p^n} \rtimes C_{\sqrt{p-1}}$ for some $n \in \mathbb{Z}^+$.*

Proof. Let $F_n := C_{p^n} \rtimes C_{\sqrt{p-1}}$ (when, of course, $\sqrt{p-1}$ is an integer).

First we prove that $|\mathrm{Irr}_{p\text{-ar}}(F_n)| = 2\sqrt{p-1}$. Let $P := P_n = C_{p^n}$. As every almost p-rational irreducible character of P has kernel containing $\Phi(P)$ and $|\mathrm{Irr}(F_n/\Phi(P))| = |\mathrm{Irr}(F_1)| = 2\sqrt{p-1}$, it is sufficient to show that every $\chi \in \mathrm{Irr}_{p\text{-ar}}(F_n)$ lies above an almost p-rational irreducible character of P.

So assume that $\chi \in \mathrm{Irr}_{p\text{-ar}}(F_n)$ lies above some non-trivial $\theta \in \mathrm{Irr}(P)$. Let a be a generator of P and let $\xi := \theta(a)$. In particular, ξ is a primitive p^k-root of unity for some $k \in \mathbb{Z}^+$. Let $\theta = \theta_1, \theta_2, \ldots, \theta_{\sqrt{p-1}}$ be distinct F_n-conjugates of θ. We have

$$\chi(a) = \sum_{i=1}^{\sqrt{p-1}} \theta_i(a) = \sum_{i=1}^{\sqrt{p-1}} \xi^{m^i},$$

for some integer $m > 1$ such that $m^{\sqrt{p-1}} \equiv 1 \,(\mathrm{mod} |P|)$. We know that $\chi(a) \in \mathbb{Q}_{p(p-1)} \cap \mathbb{Q}_{|P|} = \mathbb{Q}_p$, and hence $\chi(a)$ is fixed under the cyclic group $\mathrm{Gal}(\mathbb{Q}_{p^k}/\mathbb{Q}_p)$ (of order p^{k-1}). Also, the powers ξ^{m^i} $(1 \leq i \leq \sqrt{p-1})$ are permuted by $\mathrm{Gal}(\mathbb{Q}_{p^k}/\mathbb{Q}_p)$, and it follows that $\mathrm{Gal}(\mathbb{Q}_{p^k}/\mathbb{Q}_p)$ fixes at least one, and hence all, of ξ^{m^i}. We have shown that $\xi \in \mathbb{Q}_p$, which means that θ is almost p-rational, as desired.

We now prove that if $\sqrt{p-1} \notin \mathbb{Z}$ or $\sqrt{p-1} \in \mathbb{Z}$ but $G \ncong F_n$ for all $n \in \mathbb{Z}^+$, then $|\mathrm{Irr}_{p\text{-ar}}(G)| > 2\sqrt{p-1}$. Let N be a minimal normal subgroup of G. By induction we may assume that $p \mid |N|$ and $p \nmid |G/N|$, or $\sqrt{p-1} \in \mathbb{Z}$ and $G/N \cong F_m$ for some $m \in \mathbb{Z}^+$.

Consider the case $p \mid |N|$ and $p \nmid |G/N|$. If N is abelian then the exponent of G is not divisible by p^2 and so every irreducible character of G is almost p-rational. Therefore $|\mathrm{Irr}_{p\text{-ar}}(G)| = k(G) \geq 2\sqrt{p-1}$ by [Mar3, Theorem 1.1], and moreover, the equality occurs if and only if $\sqrt{p-1} \in \mathbb{Z}$ and $G \cong F_1$. The case N non-abelian follows from Lemmas 3.5.

Next we consider the case $G/N \cong F_m$ for some m. Then $\mathrm{Irr}_{p\text{-ar}}(G/N) = 2\sqrt{p-1}$. If N is non-abelian then N is a direct product of copies of a non-abelian simple group, say S. By considering the restriction of the character labeled by $(n-1,1)$ from the symmetric group $\mathrm{Sym}(n)$ to the alternating group $\mathrm{Alt}(n)$ $(n \neq 6)$, the Steinberg character for simple groups of Lie type (see [Sch1]), and checking [Atl] directly for sporadic groups, we find that there exists a non-trivial character $\theta \in \mathrm{Irr}(S)$ such that θ extends to a rational-valued character of $\mathrm{Aut}(S)$. The tensor product of copies of θ then extends to a rational character of G by [Nav2, Corollary 10.5] and the tensor-induced formula [GI, Definition 2.1], which implies that G has a rational irreducible character whose kernel does not contain N. We now have

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq |\mathrm{Irr}_{p\text{-ar}}(G/N)| + |\mathrm{Irr}_{p\text{-ar}}(G|N)| \geq 2\sqrt{p-1} + 1,$$

as desired.

So we may assume that N is abelian and $G/N \cong F_m$. When N is a p'-group we have

$$\begin{aligned} |\mathrm{Cl}_{p\text{-areg}}(G)| &\geq |\mathrm{Cl}_{p\text{-areg}}(G/N)| + n(G,N) - 1 \\ &= 2\sqrt{p-1} + n(G,N) - 1 \end{aligned}$$

by Lemma 3.3, and it follows immediately by Lemma 3.2 that

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq |\mathrm{Cl}_{p\text{-areg}}(G)| > 2\sqrt{p-1}$$

since $n(G,N) \geq 2$.

We may now assume that N is an elementary abelian p-group and $G/N \cong F_m$. It follows that G has a normal Sylow p-subgroup, say P, and moreover, $G = PK$ is a semidirect product of a cyclic group K (of order $\sqrt{p-1}$) acting faithfully on P. We have

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq |\mathrm{Irr}_{p\text{-ar}}(G/\Phi(P))| = k(G/\Phi(P))$$

since every irreducible character of $G/\Phi(P)$ is almost p-rational. As above, since $G/\Phi(P)$ has order divisible by p, we have $k(G/\Phi(P)) \geq 2\sqrt{p-1}$ with equality if and only if $G/\Phi(P) \cong F_1$. Thus we may assume that $G/\Phi(P) \cong F_1$. In particular, $P/\Phi(P)$ is cyclic, and therefore so is P. Recall that $K \cong C_{\sqrt{p-1}}$ acts faithfully on P and observe that the automorphism group of the cyclic group P of odd prime power order is cyclic. We conclude that $G \cong F_n$ with $n = \log_p(|P|)$, and this finishes the proof. □

We have completed the proof of Theorem 1.1 for both $p = 2$ and p odd.

4. Almost p-rational characters of p'-degree

In this section we prove Theorem 1.3, using Theorem 1.1, the known cyclic Sylow case of the McKay–Navarro conjecture, and some representation theory of finite reductive groups.

4.1. **The case G has cyclic Sylow.** We start with the case where Sylow p-subgroups of G are cyclic. As discussed in Section 2, parts (i) and (ii) of the second statement of Theorem 1.3 are then equivalent and the first statement of Theorem 1.3 is true for G and p.

We now show that parts (ii) and (iii) in Theorem 1.3 are equivalent. In fact, the equality part of Theorem 1.1 easily implies that (iii) implies (ii).

Assume that $\sqrt{p-1}$ is an integer and $|\mathrm{Irr}_{p',p\text{-ar}}(\mathbf{N}_G(P))| = 2\sqrt{p-1}$. It follows that

$$|\mathrm{Irr}_{p\text{-ar}}(\mathbf{N}_G(P)/P')| = |\mathrm{Irr}_{p',p\text{-ar}}(\mathbf{N}_G(P)/P')| \leq 2\sqrt{p-1},$$

where we recall that P' is the commutator subgroup of P. Using Theorem 1.1, we deduce that $|\mathrm{Irr}_{p\text{-ar}}(\mathbf{N}_G(P)/P')| = 2\sqrt{p-1}$, and moreover, $\mathbf{N}_G(P)/P'$ must be isomorphic to the Frobenius group $F := C_{p^n} \rtimes C_{\sqrt{p-1}}$ for some $n \in \mathbb{Z}^+$. It follows that P is cyclic and indeed $\mathbf{N}_G(P) \cong P \rtimes C_{\sqrt{p-1}}$, as stated.

4.2. **Reduction to a p'-order quotient.** Let (G, p) be a counterexample to the theorem such that $|G|$ is as small as possible. By the previous subsection, G has minimal order subject to the conditions $|\mathrm{Irr}_{p',p\text{-ar}}(G)| \leq 2\sqrt{p-1}$ and the Sylow p-subgroups of G are not cyclic. Let N be a minimal normal subgroup of G. Then $p \mid |N|$ by the minimality of G.

We claim that $p \nmid |G : N|$. Assume otherwise. Then we have

$$|\mathrm{Irr}_{p',p\text{-ar}}(G)| = |\mathrm{Irr}_{p',p\text{-ar}}(G/N)| = 2\sqrt{p-1}$$

and the Sylow p-subgroups of G/N are cyclic.

Suppose that N is non-abelian, and let S be a simple direct factor of N. By [NT1, Theorem 3.3], there exists an $\mathrm{Aut}(S)$-orbit $\mathcal{O}$ of non-trivial p'-degree irreducible characters of S such that $p \nmid |\mathcal{O}|$ and every character in $\mathcal{O}$ extends to a $\mathbb{Q}_p$-valued character of its inertia subgroup in $\mathrm{Aut}(S)$. By [NT1, Proposition 3.1], this orbit produces some $\chi \in \mathrm{Irr}_{p'}(G)$ with $\mathbb{Q}_p$-values and $N \nsubseteq \mathrm{Ker}(\chi)$. This violates the above equality $|\mathrm{Irr}_{p',p\text{-ar}}(G)| = |\mathrm{Irr}_{p',p\text{-ar}}(G/N)|$.

The following lemma finishes the proof of the claim.

Lemma 4.1. *Let N be a normal p-subgroup of G. Suppose that the Sylow p-subgroups of G/N are cyclic but those of G are not. Then there exists $\chi \in \mathrm{Irr}_{p',p\text{-ar}}(G)$ whose kernel does not contain N.*

Proof. Let P be a Sylow p-subgroup of G. Since P is not cyclic, neither is $P/\Phi(P)$ and this implies that P has at least p^2 linear characters with values in $\mathbb{Q}_p$. On the other hand, as P/N is cyclic, the principal character $\mathbf{1}_N$ of N has at most p extensions to P with values in $\mathbb{Q}_p$ by Gallagher's theorem. We deduce that there exists $\theta \in \mathrm{Irr}_{p\text{-ar}}(P)$ such that $\theta(1) = 1$ and $N \nsubseteq \mathrm{Ker}(\theta)$.

Let σ be the automorphism in $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ that fixes p'-roots of unity and sends every p-power root of unity to its $(p+1)$th-power. Then σ has p-power order and a character of G or N is almost p-rational if and only if it is fixed by σ. In particular, θ is σ-fixed.

Consider the induced character θ^G of degree $|G : P|$. Then θ^G is also σ-fixed. If χ is an irreducible constituent of θ^G, we have $[\chi^\sigma, \theta^G] = [\chi^\sigma, (\theta^G)^\sigma] = [\chi, \theta^G]^\sigma = [\chi, \theta^G]$, and thus σ permutes the irreducible constituents of θ^G. Since σ has p-power order and θ^G has p'-degree, we deduce that σ fixes at least one p'-degree irreducible constituent of θ^G. This constituent lies over θ, and as $N \nsubseteq \mathrm{Ker}(\theta)$, its kernel does not contain N, as desired. $\square$

4.3. **Reduction to simple groups of Lie type in characteristic $\ell \neq p$.** We continue to work with a minimal counterexample (G, p). By the previous subsection, we know that, for every minimal normal subgroup M of G, we must have $p \nmid |G : M|$. We conclude that G has a unique minimal normal subgroup, say N, and furthermore, $p \nmid |G/N|$. If N is abelian then $|\mathrm{Irr}_{p\text{-ar}}(G)| = |\mathrm{Irr}_{p',p\text{-ar}}(G)| \leq 2\sqrt{p-1}$ by the Itô–Michler theorem, violating Theorem 1.1 as Sylow p-subgroups of G are not cyclic. Therefore N is isomorphic to a direct product of copies of a non-abelian simple group, say S, of order divisible by p.

The following lemma, which is essentially due to Navarro and Tiep, allows us to go back and forth between almost p-rational characters of N and those of G.

Lemma 4.2. *Let G be a finite group and $N \trianglelefteq G$ such that $p \nmid |G : N|$. Let $\theta \in \mathrm{Irr}(N)$ and let $\chi \in \mathrm{Irr}(G|\theta)$. Then θ is almost p-rational if and only if χ is almost p-rational.*

Proof. The *only if* implication is a consequence of [NT3, Lemma 5.1]. We now prove the *if* implication. So assume that $\chi \in \mathrm{Irr}(G|\theta)$ is almost p-rational.

Let $\theta = \theta_1, \theta_2, \ldots, \theta_t$ be all the G-conjugates of θ. In other words, the θ_i are all of the irreducible constituents of χ_N by Clifford's theorem. Let σ be the same Galois automorphism as in the proof of Lemma 4.1. Then σ permutes the θ_i. But since t is prime to p by hypothesis and σ has p-power order, there exists a θ_i that is σ-fixed, which implies that all of the θ_i are σ-fixed. □

By Lemma 4.2, if all p'-degree irreducible characters of S are almost p-rational, then so are the p'-degree irreducible characters of G, and thus $|\mathrm{Irr}_{p',p\text{-ar}}(G)| = |\mathrm{Irr}_{p'}(G)|$, which implies that (G, p) is not a counterexample by the main result of [MM]. As observed in the proof of [NT3, Theorem 5.8] (see also [TZ, Theorem 1.3]), when $p > 2$, every irreducible character of any alternating group, of any sporadic simple group (including the Tits group ${}^2F_4(2)'$), or of any simple group of Lie type in characteristic p, is almost p-rational. When $p = 2$, by [Mal2, Propositions 2.1–2.4], irreducible characters of these groups remain almost p-rational, except for 4 characters of degrees 27 and 351 of ${}^2F_4(2)'$.

Thus, from now on, we may assume that $S \neq {}^2F_4(2)'$ is a simple group of Lie type in characteristic ℓ different from p, or $S = {}^2F_4(2)'$ with $p = 2$.

4.4. **The case $p = 2, 3$.** Let us assume for a moment that $(S, p) \neq ({}^2F_4(2)', 2)$, so that the defining characteristic ℓ of S is not p. First suppose that $N < G$. Then G has at least two p-rational irreducible characters whose kernels contain N. On the other hand, the so-called Steinberg character St_S of S degree $\mathsf{St}_S(1) = |S|_\ell$ is extendible to a rational-valued character of $\mathrm{Aut}(S)$ (see [Sch1]), and thus, as before, G has a rational-valued irreducible character χ that extends $\mathsf{St}_S \times \cdots \times \mathsf{St}_S \in \mathrm{Irr}(N)$. We deduce that $|\mathrm{Irr}_{p',p\text{-ar}}(G)| \geq 3 > 2\sqrt{p-1}$, as desired.

We now suppose that $G = N$, and in fact, it suffices to suppose that $G = S$. By [GHSV, Theorem 2.1], there exists $\mathbf{1}_S \neq \chi \in \mathrm{Irr}(S)$ of $\{\ell, p\}'$-degree such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_\ell$ or $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_p$. In particular, $\chi \in \mathrm{Irr}_{p'}(S) \setminus \mathsf{St}_S$ and χ is almost p-rational and it follows again that $|\mathrm{Irr}_{p',p\text{-ar}}(S)| \geq |\{\mathbf{1}_S, \chi, \mathsf{St}_S\}| = 3$.

We are left with the case $p = 2$ and $S = {}^2F_4(2)'$. But a quick inspection of the character table of ${}^2F_4(2)'$ reveals that it has four rational-valued irreducible characters of degrees $1, 325, 351$, and 675, all of which are extendible to $\mathrm{Aut}(S) = {}^2F_4(2)$, and so the above arguments apply to this case as well.

4.5. **Finishing the proof of Theorem 1.3 (assuming Theorems 4.3 and 4.4).** We have shown that the counterexample G has a unique minimal normal subgroup N with

$p \nmid |G/N|$ and N is isomorphic to a direct product of t copies of a simple group S of Lie type in characteristic ℓ with $\ell \neq p$ and $5 \leq p \mid |S|$.

Assume first that Sylow p-subgroups of S are non-cyclic. If $N = S$ then it suffices to show that $|\mathrm{Irr}_{p',p\text{-ar}}(G)| > 2\sqrt{p-1}$. On the other hand, if $t \geq 2$ then, by using Lemma 4.2 and the same arguments as in [MM, §3.2], we deduce that $|\mathrm{Irr}_{p',p\text{-ar}}(G)| \geq k(k+1)/2$, where k is the number of $\mathbf{N}_G(S)$-orbits (here we view S as a simple factor of N) on $\mathrm{Irr}_{p',p\text{-ar}}(S)$, and therefore it suffices to show that there are at least $2(p-1)^{1/4}$ $\mathrm{Out}(S)$-orbits on $\mathrm{Irr}_{p',p\text{-ar}}(S)$. In summary, in this case, we wish to establish the following result on simple groups of Lie type.

Theorem 4.3. *Let $S \neq {}^2F_4(2)'$ be a simple group of Lie type and $p \geq 5$ a prime not equal to the defining characteristic of S such that Sylow p-subgroups of S are non-cyclic. Let $S \leq H \leq \mathrm{Aut}(S)$ be an almost simple group such that $p \nmid |H/S|$. Then*

(i) $|\mathrm{Irr}_{p',p\text{-ar}}(H)| > 2\sqrt{p-1}$.
(ii) *There are at least $2(p-1)^{1/4}$ H-orbits on $\mathrm{Irr}_{p',p\text{-ar}}(S)$.*

For the case when Sylow p-subgroups of S are cyclic, by Subsection 4.1, we may assume that the number t of copies of S in N is at least 2, and therefore we need to establish the following.

Theorem 4.4. *Let X be a finite group with a unique minimal subgroup $N = S^t$, where where $S \neq {}^2F_4(2)'$ is a simple group of Lie type, and $p \geq 5$ a prime not equal to the defining characteristic of S such that Sylow p-subgroups of S are cyclic and non-trivial. Suppose that $t \geq 2$ and $p \nmid |X : N|$. Then $|\mathrm{Irr}_{p',p\text{-ar}}(X)| > 2\sqrt{p-1}$.*

Proofs of Theorems 4.3 and 4.4, as expected, rely on the representation theory of finite groups of Lie type, and therefore are deferred to the next section.

5. Groups of Lie type

In this section we prove Theorems 4.3 and 4.4, which were left off at the end of Section 4.

We consider the following setup. Let $\mathbf{G}$ be a simple linear algebraic group of adjoint type with a Steinberg endomorphism $F : \mathbf{G} \to \mathbf{G}$. We consider the characters of the finite almost simple group $G := \mathbf{G}^F$. For this, let $(\mathbf{G}^*, F)$ be in duality with $(\mathbf{G}, F)$ (see [GM, Definition 1.5.17]) and $G^* := \mathbf{G}^{*F}$. According to Lusztig, there is a partition

$$\mathrm{Irr}(G) = \coprod_{s \in G^*/\sim} \mathcal{E}(G, s)$$

into Lusztig series, where the union runs over a system of representatives s of semisimple conjugacy classes in G^* (see [GM, Theorem 2.6.2]).

Lemma 5.1. *In the above setting, let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_{p|G|_{p'}})$. Assume that $p \geq 5$ and let $s \in G^*$ be an almost p-regular semisimple element. Then we have:*

(a) *The Lusztig series $\mathcal{E}(G, s)$ is σ-stable.*
(b) *The semisimple character in $\mathcal{E}(G, s)$ is almost p-rational.*

Proof. The first claim is well-known, see [GM, Proposition 3.3.15]. For the second, note that by the first $\mathcal{E}(G, s)$ is σ-stable. Since $|\mathbf{Z}(\mathbf{G}^F)| = 1$, there is exactly one semisimple character in $\mathcal{E}(G, s)$ (see [GM, Definition 2.6.9]), and it is uniquely distinguished among all characters in $\mathcal{E}(G, s)$ by having non-zero multiplicity in the rational valued class function $\Delta_{\mathbf{G}}$ from *loc. cit.*. Thus it is σ-stable. □

Let $\sigma : \mathbf{G} \to \mathbf{G}$ be an isogeny commuting with F. Then there exists a dual isogeny $\sigma^* : \mathbf{G}^* \to \mathbf{G}^*$ such that the following holds (see [Tay, Proposition 7.2]):

Proposition 5.2. *Let $s \in \mathbf{G}^{*F}$ be semisimple. Then*

$${}^{\sigma}\mathcal{E}(G, s) = \mathcal{E}(G, \sigma^{*-1}(s)).$$

In particular $\mathcal{E}(G, s)$ is σ-stable if the class of s is σ^*-stable.

We will employ this in case of Steinberg endomorphisms σ commuting with F, which induce field automorphisms on G. In this case, σ^* induces also a field automorphism on G^*.

The following strengthens [MM, Theorem 5.4] by taking almost p-rationality into account:

Theorem 5.3. *Let $\mathbf{G}$ be a simple exceptional group of adjoint type with a Steinberg endomorphism F such that $S := [\mathbf{G}^F, \mathbf{G}^F]$ is simple. Assume that Sylow p-subgroups of S are non-cyclic and $p \geq 5$ is not the underlying characteristic of $\mathbf{G}$. Then either*

$$|\mathcal{E}(G, 1) \cap \mathrm{Irr}_{p',p\text{-ar}}(G)| \geq 2\sqrt{p-1}$$

or

$$|\mathrm{Irr}_{p',p\text{-ar}}(G)| \geq 2g\sqrt{p-1}^{\,3},$$

where g denotes the order of the group of graph automorphisms of $\mathbf{G}$.

Proof. We follow the proof of [MM, Theorem 3.1]. There we had shown that the analogous statement holds for $\mathrm{Irr}_{p'}$ in place of $\mathrm{Irr}_{p',p\text{-ar}}$. In particular, in those cases when the characters constructed there happen to be almost p-rational, our claim will follow automatically. Now note that all unipotent characters of groups of Lie type $G := \mathbf{G}^F$ are almost p-rational for all primes $p \geq 3$. This follows, for example, from [GM, Proposition 4.5.5]. Thus, whenever only unipotent characters are used in the proof of [MM, Theorem 3.1], we may conclude.

Since the Sylow p-subgroups of ${}^2B_2(q^2)$ and ${}^2G_2(q^2)$ for all primes $p \geq 5$ are cyclic, we need not consider these. If p is at most equal to the bound given in Table 2 of [MM], the characters used in the proof of [MM, Proposition 5.4] are unipotent and so we are done by our previous remark. If p is larger than that bound, it does not divide the order of the Weyl group of G and so the Sylow p-subgroups of G are abelian [MT, Theorem 25.14]. Note that we need not consider the primes p corresponding to the second set of columns in [MM, Table 2] since for those p, Sylow p-subgroups of G are cyclic.

In the notation of [MM, Proposition 5.4], a Sylow p-subgroup of G^* contains an elementary abelian subgroup E of order p^{a_d} lying in a Sylow d-torus S_d of G^*, where d is the order of q modulo p, and G^*-fusion of elements of E is controlled by the relative Weyl group W_d of S_d. (Here q is the absolute value of all eigenvalues of F on the character group of an F-stable maximal torus of $\mathbf{G}$.) Since Sylow p-subgroups of G^* are abelian, the centraliser of any $s \in E$ contains a Sylow p-subgroup of G^*. Thus the semisimple character in the corresponding Lusztig series $\mathcal{E}(G,s)$ has degree prime to p by the degree formula [GM, Corollary 2.6.6].

Now from the known values of a_d, the orders of W_d and the lower bounds on p in [MM, Table 2] it is straightforward to check that there are at least

$$2g(p-1)\sqrt{p-1}$$

conjugacy classes of such elements s of order p in G^*, where $g \leq 2$ denotes the order of the group of graph automorphisms of $\mathbf{G}$. By Lemma 5.1 for each such s the semisimple character in $\mathcal{E}(G,s)$ is almost p-rational, of p'-degree by what we said before, so we conclude. □

Corollary 5.4. *Theorem 4.3 holds true for S a simple exceptional group of Lie type.*

Proof. Note that we are done if $|\mathcal{E}(G,1) \cap \mathrm{Irr}_{p',p\text{-ar}}(G)| \geq 2\sqrt{p-1}$. So assume otherwise. The proof of Theorem 5.3 indeed then shows that G then has at least $2g\sqrt{p-1}^3$ semisimple almost p-rational p'-characters. Also, by Lemma 4.2, for part (i) of the theorem it suffices to find enough almost p-rational p'-degree characters of S.

The diagonal automorphisms of S permute only the semisimple characters in a fixed Lusztig series and thus we obtain at least $2g\sqrt{p-1}^3$ orbits of (semisimple) almost p-rational p'-characters of S under diagonal automorphisms. Now by Proposition 5.2 any field automorphism of G stabilises $\mathcal{E}(G,s)$ if the dual automorphism of G^* fixes the class of s. Since s considered in the proof of Theorem 5.3 has order p, it lies in an orbit of length at most $p-1$ under the cyclic group of field automorphisms of G^*. Thus there are at least $2\sqrt{p-1}$ orbits of $\mathrm{Out}(G)$ on $\mathrm{Irr}_{p',p\text{-ar}}(S)$, which implies the same bound for the number of $\mathrm{Out}(S)$-orbits on $\mathrm{Irr}_{p',p\text{-ar}}(S)$. The theorem follows by noting that we do have strict inequality in part (i) by taking unipotent characters into account. □

Proposition 5.5. *Theorem 4.3 holds true for S a simple classical group.*

Proof. By [MM, Proposition 5.5] and our introductory remarks at the beginning of the proof of Theorem 5.3 we may assume that p does not divide the order of the Weyl group of G, so p is greater than the rank of G. Then a Sylow p-subgroup P of G^* is homocyclic with $a \geq 2$ factors, and the automiser W of P acts as a wreath product $C_d \wr \mathrm{Sym}(a)$ for some $d|(p-1)$, or a subgroup of index 2 thereof in groups of type D_n. Note that P contains an elementary abelian subgroup E of order p^a and that the wreath product has $k(d,a)$ irreducible characters, which is by definition the number of d-tuples of partitions of a, see [BMM, §3].

First assume that $a = 2$ and S is not of type D_n. Then there are at least $k(d,2) = (d^2+3d)/2$ unipotent characters of S, all of which are $\mathrm{Aut}(S)$-invariant (see [Mal1, Theorem 2.5]), of p-height zero corresponding to $\mathrm{Irr}(W)$. The number of G^*-classes of non-trivial p-elements in G^* is at least $(p^2-1)/(2d^2)$ and the field automorphisms can fuse at most $(p-1)/d$ of those, so we find at least $(p+1)/2dg \geq (p+1)/4d$ orbits of semisimple characters in $\mathrm{Irr}_{p',p\text{-ar}}(S)$ under the automorphism group. Together with the aforementioned $(d^2+3d)/2$ unipotent characters, we have proved part (ii) of the theorem in this case. For part (i) we let $\overline{H} := H/(H \cap G)$ (where H is the almost simple group given in Theorem 4.3), which can be viewed as a subgroup of the abelian group of the field and graph automorphisms of S. On one hand, the number of irreducible characters of H lying over the $(d^2+3d)/2$ unipotent characters of S exhibited above is at least

$$\frac{d^2+3d}{2}k(H/S) \geq \frac{d^2+3d}{2}k(\overline{H}) = \frac{d^2+3d}{2}|\overline{H}|,$$

since every unipotent character of S is fully extendible to H ([Mal1, Theorem 2.4]). (Here we use $k(X)$ to denote the conjugacy class number of X.) On the other hand, the number of irreducible characters of H lying over previously considered semisimple characters of S is at least

$$\frac{p^2-1}{2d^2|\overline{H}|},$$

as these semisimple characters are G-invariant and thus $(G\cap H)$-invariant. Note that all these characters are almost p-rational and of p'-degree by Lemma 4.2. We therefore have

$$|\mathrm{Irr}_{p',p\text{-ar}}(H)| \geq \frac{d^2+3d}{2}|\overline{H}| + \frac{p^2-1}{2d^2|\overline{H}|} \geq 2\sqrt{\frac{p^2-1}{4}} > 2\sqrt{p-1}$$

since $p\geq 5$, as required.

The case $a=2$ and S is of type D_n is argued similarly. Here S has at least $k(d,2)/2$ unipotent characters of p'-degree and at least $(p^2-1)/d^2$ (non-trivial) semisimple characters coming from semisimple elements in E.

So now let $a\geq 3$ and first assume that $W = C_d \wr \mathrm{Sym}(a)$ and S is not of the type D_4. There are $|\mathrm{Irr}(W)| = k(d,a)$ unipotent characters of S of p'-degree. Now $k(d,a)\geq 2da$ unless $(d,a)=(2,3)$. Assume we are not in the latter case. Then we are done whenever $p-1\leq (da)^2$. Assume that $p-1>(da)^2$. Then the elementary abelian p-subgroup $E\cong C_p^a$ of S has at least $(p^a-1)/(d^a\,a!)$ classes under the action of W, which is

$$\begin{aligned}\frac{p^a-1}{d^a\,a!} &\geq (p-1)^{3/2}\frac{(da)^{2a-3}}{d^a\,a!} = (p-1)^{3/2}\frac{d^{a-3}a^{2a-3}}{a!}\\ &\geq (p-1)^{3/2}\frac{a^{2a-3}}{a!} > 4(p-1)^{3/2}.\end{aligned}$$

By Lemma 5.1 this yields at least that many orbits of almost p-rational p'-characters of S under diagonal automorphisms. Moreover, the group of field automorphisms has orbits of length at most $(p-1)/d$ on this set of classes of elements of order p, the diagonal automorphisms do not decrease the number of classes, and the group of graph automorphisms of S has order at most 2. Thus there are more than $2\sqrt{p-1}$ $\mathrm{Aut}(S)$-orbits on $\mathrm{Irr}_{p',p\text{-ar}}(S)$, as desired. When $(d,a)=(2,3)$ we have to consider the case that $p=29,31$, but again the above inequality suffices.

Assume that $W=C_d\wr\mathrm{Sym}(a)$ and S is of the type D_4. Then one must have $a=4$, and so $d=2$, since $a\geq 3$. Now S has $k(2,4)=20$ unipotent characters of p'-degree but $\mathrm{Aut}(S)$ has two nontrivial orbits of length 3 on unipotent characters ([Mal1, Theorem 2.5]), and thus we are done if $2\sqrt{p-1}<16$. Otherwise we just repeat the above arguments (with $g=6$) and check that $(p^4-1)/(2^4\cdot 4!) > 12(p-1)^{3/2}$ to achieve the required bound.

Finally assume that $a\geq 3$ and W has index 2 in $C_d\wr\mathrm{Sym}(a)$. Then necessarily d is even. Here, $|\mathrm{Irr}(W)|\geq 2da$ and we can argue as before, unless $(d,a)=(2,3),(4,3),(2,4),(2,5)$.

Note that in these cases, the number of W-orbits on E is at least $2\frac{p^a-1}{d^a\, a!}$, and using the explicit value of $|\mathrm{Irr}(W)|$ we can again conclude. □

To prove Theorem 4.4 we need the following simple observation.

Lemma 5.6. *Let A be an abelian group and H a subgroup of $A \wr \mathrm{Sym}(t)$ for some $t \in \mathbb{Z}^+$. Then*

$$\frac{|\mathrm{Irr}(H)|}{|H|} \geq \frac{1}{(t!)^2}.$$

Proof. The factor $|H|/|\mathrm{Irr}(H)|$ is the average of the squares of all (irreducible) character degrees of H and so is at most $b(H)^2$ where $b(H)$ is the largest character degree of H. But $b(H)$ divides $|H/(A^t \cap H)|$ by Ito's theorem (see [Isa, Theorem 6.15]) and $|H/(A^t \cap H)| \leq t!$ since $H/(A^t \cap H)$ is isomorphic to the image of H under the natural homomorphism from $A \wr \mathrm{Sym}(t)$ to $\mathrm{Sym}(t)$, and thus the lemma follows. □

We now prove Theorem 4.4, which is restated.

Theorem 5.7. *Let X be a finite group with a unique minimal subgroup $N = S^t$, where $t \in \mathbb{Z}^+$ and $S \neq {}^2F_4(2)'$ is a simple group of Lie type. Let $p \geq 5$ be a prime not equal to the defining characteristic of S such that Sylow p-subgroups of S are cyclic and non-trivial. Suppose that $t \geq 2$ and $p \nmid |X : N|$. Then $|\mathrm{Irr}_{p',p\text{-ar}}(X)| > 2\sqrt{p-1}$.*

Proof. The assumptions on N and X imply that X is a subgroup of $\mathrm{Aut}(N) = \mathrm{Aut}(S) \wr \mathrm{Sym}(t)$.

(1) First we assume that S is of exceptional type. As before we let d be the order of q modulo p, where q is the size of the underlying field of S, S_d be a Sylow d-torus of G^*, and W_d the relative Weyl group of S_d. Since Sylow p-subgroups of S are cyclic, S_d is cyclic of order $\Phi_d(q)$, and thus W_d is cyclic, see [GM, pp. 260-261].

By d-Harish-Chandra theory (see [GM, §3.5]), there are at least $|\mathrm{Irr}(W_d)| = |W_d|$ many unipotent characters of G of p'-degree, each of which restricts irreducibly to S. (Recall that G is the finite reductive group of adjoint type with $S := [G,G]$.) These unipotent characters of S are all extendible to $\mathrm{Aut}(S)$, by [Mal1, Theorems 2.4 and 2.5]. (When S is $G_2(3^f)$ or $F_4(2^f)$, the graph automorphism of order 2 does fuse certain unipotent characters of S but they are not p'-degree, provided that Sylow p-subgroups of S are cyclic, see [Car, pp. 478–479].) Recall that unipotent characters are almost p-rational for odd p. It follows that there are at least $|W_d|+1$ orbits of characters in $\mathrm{Irr}_{p',p\text{-ar}}(S)$ under $\mathrm{Aut}(S)$ (note that there is at least one orbit of semisimple characters), and thus there are at least $\binom{t+|W_d|}{t}$ X-orbits on $\mathrm{Irr}_{p',p\text{-ar}}(N)$, and therefore it follows from Lemma 4.2 that

$$|\mathrm{Irr}_{p',p\text{-ar}}(X)| \geq \binom{t+|W_d|}{t}.$$

Note that $|W_d| \geq 4$ for all types and relevant values of d and $t \geq 2$ by the assumption, and therefore we are done if $t \geq 48^{1/4}(p-1)^{1/8}$ or if $|W_d| \geq 2(p-1)^{1/4}$. In fact, we are also done if $p < \binom{6}{2}^2 + 1 = 226$. So we assume that none of these occur.

For each unipotent character θ of p'-degree of S, the character

$$\psi_\theta := \theta \times \theta \times \cdots \times \theta \in \mathrm{Irr}(N)$$

is fully extendible to $\mathrm{Aut}(N)$ (see [Nav2, Corollary 10.5]), and hence to X. By Gallagher's lemma (see [Isa, Corollary 6.17]), the number of irreducible characters of X lying over those $|W_d|$ characters ψ_θ of N is at least $|W_d| \cdot |\mathrm{Irr}(X/N)|$, which in turns is at least

$$|W_d| \cdot |\mathrm{Irr}(X/(X \cap G^t))|.$$

Now a Sylow p-subgroup of G^* contains a cyclic subgroup of order p and the number of G^*-conjugacy classes of non-trivial p-elements in G^* is at least $(p-1)/|W_d|$, and thus G has at least $(p-1)/|W_d|$ semisimple characters that are all almost p-rational and of p'-degree, by Lemma 5.1 and Proposition 5.2. These characters also restrict irreducibly to (semisimple) characters of S since $p \geq 5$ is coprime to $|\mathbf{Z}(G^*)|$. Therefore, N has at least $((p-1)/|W_d|)^t$ irreducible characters that are products of non-trivial semisimple characters of copies of S. It follows that the number of irreducible characters of X lying over these characters of N is at least

$$\frac{(p-1)^t}{|W_d|^t \cdot |X/(X \cap G^t)|}.$$

This and the conclusion of the previous paragraph, together with Lemmas 4.2 and 5.6, yield

$$\begin{aligned} |\mathrm{Irr}_{p',p\text{-ar}}(X)| &\geq |W_d| \cdot |\mathrm{Irr}(X/(X \cap G^t))| + \frac{(p-1)^t}{|W_d|^t \cdot |X/(X \cap G^t)|} \\ &\geq 2\sqrt{\frac{(p-1)^t}{|W_d|^{t-1}} \cdot \frac{|\mathrm{Irr}(X/(X \cap G^t))|}{|X/(X \cap G^t)|}} \geq 2\sqrt{\frac{(p-1)^t}{(t!)^2 |W_d|^{t-1}}} \\ &\geq 2\sqrt{p-1}\left(\frac{p-1}{t^2|W_d|}\right)^{(t-1)/2}, \end{aligned} \tag{5.1}$$

which is larger than the required bound of $2\sqrt{p-1}$ by our earlier assumptions that $t < 48^{1/4}(p-1)^{1/8}$, $|W_d| < 2(p-1)^{1/4}$, and $p \geq 226$.

(2) We now consider the case when S is of classical type. As seen in the proof of Proposition 5.5, the number of p'-degree unipotent characters of S is at least $|\mathrm{Irr}(W)|$, where W is a certain cyclic group of order depending on p, q and the rank of G. Assume for now that S is not of untwisted type D_4 so that the group of the field and graph automorphisms of S is abelian and hence Lemma 5.6 applies. The arguments for exceptional types can also be used to achieve the desired bound. Here the order of W is always at least 2 and it is straightforward to show that

$$\min\left\{\binom{t+|W|}{t}, 2\sqrt{\frac{(p-1)^t}{(t!)^2|W|^{t-1}}}\right\} > 2\sqrt{p-1}$$

for all possibilities of t, p and W.

Finally we assume that S is of untwisted type D_4. The group of graph automorphisms of S is then $\mathrm{Sym}(3)$. Let B be the group of field and graph automorphisms of S (which is the direct product of the cyclic group of field automorphisms and $\mathrm{Sym}(3)$), H a subgroup of $B \wr \mathrm{Sym}(t)$, and set $H_1 := H \cap B^t$. Using [GR, Lemma 2(i)] (in the language of the so-called *commuting probability* of finite groups), we have

$$\frac{|\mathrm{Irr}(H)|}{|H|} \geq \frac{|\mathrm{Irr}(H_1)|}{|H_1|} \cdot |H : H_1|^2 \geq \frac{|\mathrm{Irr}(B^t)|}{(t!)^2\,|B|^t} \geq \frac{1}{2^t \cdot (t!)^2},$$

and therefore instead of the bound (5.1) we now only have

$$|\mathrm{Irr}_{p',p\text{-ar}}(X)| \geq 2\sqrt{\frac{(p-1)^t}{2^t\,|W|^{t-1}\,(t!)^2}}.$$

This and the bound $|\mathrm{Irr}_{p',p\text{-ar}}(X)| \geq \binom{t+|W|}{t}$ are again sufficient to reach the conclusion, with a notice that here $|W| = 3$ since Sylow p-subgroups of S are cyclic and so p must divide $q^2 \pm q + 1$. □

We have completed the proofs of Theorems 4.3 and 4.4, and hence the proof of the main Theorem 1.3.

6. An asymptotic bound for $|\mathrm{Irr}_{p\text{-ar}}(G)|$

In this section we prove Theorem 1.2.

We keep the notation introduced at the beginning of Section 3.

Lemma 6.1. *There exists a constant $c_1 > 0$ such that if G is any finite group having an elementary abelian minimal normal subgroup V of p-rank at least 2 and $p^2 \nmid |G/V|$, then $|\mathrm{Irr}_{p\text{-ar}}(G)| > c_1 \cdot p$.*

Proof. By choosing $c_1 < 1/2$ if necessary, we assume that p is odd. By Lemma 3.2, we then have $|\mathrm{Irr}_{p\text{-ar}}(G)| \geq |\mathrm{Cl}_{p\text{-areg}}(G)|$, and it follows that

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq \frac{1}{2}(|\mathrm{Irr}_{p\text{-ar}}(G)| + |\mathrm{Cl}_{p\text{-areg}}(G)|).$$

Recall that $p^2 \nmid |G/V|$. Thus every irreducible character of G/V is almost p-rational, and therefore we have

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq |\mathrm{Irr}_{p\text{-ar}}(G/V)| = k(G/V).$$

On the other hand, each G-orbit on V produces at least one conjugacy class of G of elements in V, and thus

$$|\mathrm{Cl}_{p\text{-areg}}(G)| \geq n(G,V),$$

where $n(G,V)$ is the number of G-orbits on V. The three above inequalities imply that

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq \frac{1}{2}(k(G/V) + n(G,V)).$$

It was shown in the proof of [MS, Proposition 2.2] that, under the same hypothesis, there exists a constant $c_1' > 0$ such that $k(G/V) + n(G,V) > c_1' \cdot p$. Now by choosing $c_1 := \min\{c_1'/2, 1/2\}$, we have the required bound $|\mathrm{Irr}_{p\text{-ar}}(G)| > c_1 \cdot p$. □

For the next lemma, we denote by $M(S)$ the Schur multiplier of a simple group S.

Lemma 6.2. *There exists a constant $c_2 > 0$ such that for any non-abelian finite simple group S and any prime p such that $p^2 \mid |S|$ or $p \mid |M(S)|$ or $p \mid |\mathrm{Out}(S)|$, we have $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > c_2 \cdot p$.*

Proof. It is sufficient to assume that $p \geq 5$ and S is an alternating group or a finite group of Lie type.

Let $S = \mathrm{Alt}(n)$ for $n \geq 5$. The assumption on p implies that $p \leq n$. Observe that there are $(p-1)/2$ cycle types of odd length up to $p-1$. Therefore $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq (p-1)/2 > p/3$.

Let S be a simple group of Lie type defined over the field of $q = \ell^f$ elements (ℓ is prime) with r the rank of the ambient algebraic group. By [HM, Theorem 1.4], we have

$$|\mathrm{Cl}_{p\text{-reg}}(S)| > \frac{q^r}{17r^2}$$

for every prime p. Also, using the known information on $|\mathrm{Out}(S)|$ (see [Atl] for instance), we find that there exists a constant $c_{21} > 0$ such that

$$|\mathrm{Out}(S)| < c_{21} \cdot fr.$$

It follows that

$$n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) \geq \frac{|\mathrm{Cl}_{p\text{-reg}}(S)|}{|\mathrm{Out}(S)|} > \frac{q^r}{17c_{21}fr^3}. \tag{6.1}$$

First suppose that $p \mid |M(S)|$ or $p \mid |\mathrm{Out}(S)|$. Then $p \leq \max\{r+1, f\}$. It follows from (6.1) that there exists a constant $c_{22} > 0$ such that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > c_{22} \cdot p$ for all possibilities of S and p.

Next we suppose that $p^2 \mid |S|$. It is an elementary result in number theory that for $m, n \in \mathbb{Z}^+$ we have $\gcd(q^m - 1, q^n - 1) = q^{\gcd(m,n)} - 1$ and $\gcd(q^m \pm 1, q^n + 1) = \gcd(2, q-1)$ or $q^{\gcd(m,n)} + 1$. Assume that S is a classical group of rank at least 2. By inspecting the order formulas, we observe that $|S| = \frac{1}{d(S)} q^{a(S)} P_S(q)$, where $a(S)$ is the order of the group of diagonal automorphisms of S, $a(S)$ is a suitable integer, and $P_S(q)$ is a polynomial in q that can be written as a product of certain polynomials of the form $q^i \pm 1$ with i at most $r+1$. We deduce that $p \leq q^{(r+1)/2} + 1$ for all S of classical type with rank $r \geq 2$. It follows from the bound (6.1) that there exists a constant $c_{23} > 0$ such that $n(\mathrm{Aut}(S), \mathrm{Cl}_{p'}(S)) > c_{23} \cdot p$ for all relevant S and p. For $S = \mathrm{PSL}_2(q)$ we have $p \leq (q+1)^{1/2}$ and the lemma also follows from the bound (6.1). Similar arguments apply when S is of exceptional type different from ${}^2B_2(q)$ with $q = 2^f$, ${}^2G_2(q)$ with $q = 3^f$, or ${}^2F_4(q)$ with $q = 2^f$, where $f \geq 3$ is an odd integer. For $S = {}^2B_2(q)$ we have $p = \ell$ or $p \leq (q + \sqrt{2q} + 1)^{1/2}$ and we are also done by the bound (6.1). The cases $S = {}^2G_2(q)$ and $S = {}^2F_4(q)$ are similar and we skip the details. □

Lemma 6.3. *There exists a constant $c_3 > 0$ such that for any non-abelian finite simple group S of order divisible by a prime p, we always have $|\mathrm{Cl}_{p\text{-reg}}(S)| > c_3 \cdot \sqrt{p}|\mathrm{Out}(S)|$.*

Proof. This essentially follows from the proof of Lemma 6.2. One just uses the inequality (6.1) and obvious upper bounds for a prime divisor of $|S|$. □

We are now in position to prove Theorem 1.2.

Theorem 6.4. *There exists a universal constant $c > 0$ such that for every prime p and every finite group G having a non-cyclic Sylow p-subgroup, we have $|\mathrm{Irr}_{p\text{-ar}}(G)| > c \cdot p$.*

Proof. Let G be a minimal counterexample with $c = \min\{c_1, c_2, c_3,\ 1/258\}$. First we observe that $p^2 \nmid |G/N|$ for every non-trivial $N \trianglelefteq G$. Therefore, by Lemma 6.1, every abelian minimal normal subgroup of G must be isomorphic to a cyclic group of order p. Suppose that there are more than one of them, which implies that there are exactly two, say A and B. Let

$$T := A \times B,\ C := \mathbf{C}_G(T),\ H := G/C, \text{ and } K := \mathbf{C}_H(A).$$

Note that H is an abelian group with exponent dividing $p-1$. Now $k(G/T) \geq k(G/C) = |H|$. Moreover, the number of K-orbits on A is $1 + (p-1)/|K|$ and the number of H/K-orbits on B is $1 + (p-1)/|H/K|$. We deduce that the number of G-orbits on T is at least

$$\left(1 + \frac{p-1}{|K|}\right)\left(1 + \frac{p-1}{|H/K|}\right),$$

which is greater than $1 + (p-1)^2/|H|$. We therefore have

$$k(G) \geq |H| + \frac{(p-1)^2}{|H|} \geq 2(p-1).$$

Note that the exponent of G is not divisible by p^2. So $|\mathrm{Irr}_{p\text{-ar}}(G)| = k(G) \geq 2(p-1)$, a contradiction.

We conclude that G has at most one abelian minimal normal subgroup and moreover, if there is one, it must be isomorphic to C_p.

First suppose that G has no non-abelian minimal normal subgroup. It then follows that G has a unique abelian minimal normal subgroup $N \cong C_p$, and furthermore, $p^2 \nmid |G/N|$ but $p \mid |G/N|$.

Since G has non-cyclic Sylow p-subgroup, we have $N < G$. Let M/N be a minimal normal subgroup of G/N such that $M \subseteq \mathbf{C}_G(N)$. Such an M exists since $p \mid |G/N|$ and $|G/\mathbf{C}_G(N)| \leq |\mathrm{Aut}(C_p)| = p - 1$. We claim that $p^2 \mid |M|$, and thus $p \nmid |G/M|$. Assume otherwise, then $M = N \times K$ for some non-trivial p'-subgroup K of M by the Schur–Zassenhaus theorem. This K is characteristic in M, and thus normal in G, violating the fact that G has a unique abelian minimal normal subgroup N. The claim follows.

Note that M/N is a direct product of copies of a simple group, but as $p^2 \nmid |G/N|$ and $p \mid |G/N|$, there is only one such copy. Suppose first that $M/N \cong C_p$. Then M is a (normal) Sylow p-subgroup of G. By the Schur–Zassenhaus theorem, we have $G = MK$ for some p'-subgroup K of G. From the assumption that Sylow p-subgroups of G are non-cyclic, we must have $M \cong C_p \times C_p$, and thus M can be viewed as a (completely reducible) K-module. In fact, since K normalizes N, as a K-module M is a direct sum of two K-modules of size p, and this contradicts what we have shown above that G has at most one abelian minimal normal subgroup.

So M/N must be isomorphic to a non-abelian simple group S, and therefore M is a quasisimple group with $\mathbf{Z}(M) = N \cong C_p$. In particular, p is a divisor of the size of the Schur multiplier of S. Therefore the number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S is at least $c_2 \cdot p$ by Lemma 6.2, implying that $|\mathrm{Cl}_{p\text{-areg}}(G/N)| > |\mathrm{Cl}_{p\text{-reg}}(G/N)| \geq c_2 \cdot p$. Using Lemma 3.2, we then obtain

$$|\mathrm{Irr}_{p\text{-ar}}(G)| \geq |\mathrm{Irr}_{p\text{-ar}}(G/N)| > c_2 \cdot p \geq c \cdot p,$$

a contradiction again.

Next we suppose that G does have a non-abelian minimal normal subgroup. We claim that every non-abelian minimal normal subgroup is simple. Assume otherwise that $N = S^k$ is a minimal normal subgroup of G such that S is non-abelian simple and $k \geq 2$. We then have

$$|\mathrm{Cl}_{p\text{-areg}}(G)| \geq |\mathrm{Cl}_{p\text{-reg}}(G)| \geq n(n+1)/2,$$

where n is the number of $\mathrm{Aut}(S)$-orbits on p-regular classes of S. By the definition of c, we know that $p > 257$, and it follows that $n > 2\sqrt{p-1}$ by Lemma 3.4. We now find that

$$|\mathrm{Cl}_{p\text{-areg}}(G)| \geq \sqrt{p-1}\left(2\sqrt{p-1}+1\right) > 2p,$$

and thus

$$|\mathrm{Irr}_{p\text{-ar}}(G)| > 2p,$$

by Lemma 3.2. This is a contradiction.

The above arguments also apply when G has more than one non-abelian minimal normal subgroup. So we conclude that G has exactly one non-abelian minimal normal subgroup, and this is isomorphic to a non-abelian simple group, say S. If $\mathbf{C}_G(S) = 1$ then G is an almost simple group with socle S, and hence $|\mathrm{Cl}_{p\text{-reg}}(G)| > c_2 \cdot p \geq c \cdot p$ by Lemma 6.2, which is again a contradiction.

Thus $\mathbf{C}_G(S)$ has order divisible by p, but not p^2 by the minimality of G. By a result of Brauer [Bra1], we then have $|\mathrm{Cl}_{p\text{-areg}}(\mathbf{C}_G(S))| = k(\mathbf{C}_G(S)) \geq 2\sqrt{p-1}$. Also, from Lemma 6.3 we know that $|\mathrm{Cl}_{p\text{-areg}}(S)| > c \cdot \sqrt{p}|\mathrm{Out}(S)|$. Now

$$\begin{aligned}|\mathrm{Cl}_{p\text{-areg}}(\mathbf{C}_G(S) \times S)| &= |\mathrm{Cl}_{p\text{-areg}}(\mathbf{C}_G(S))| \times |\mathrm{Cl}_{p\text{-areg}}(S)| \\ &> 2c\sqrt{p(p-1)}|\mathrm{Out}(S)|.\end{aligned}$$

Note that $G/(\mathbf{C}_G(S) \times S)$ can be viewed as a subgroup of $\mathrm{Out}(S)$. It follows that

$$\begin{aligned}|\mathrm{Cl}_{p\text{-areg}}(G)| &\geq |\mathrm{Cl}_{p\text{-areg}}(\mathbf{C}_G(S) \times S)|/|\mathrm{Out}(S)| \\ &> 2c\sqrt{p(p-1)} \geq cp,\end{aligned}$$

which is again a contradiction, by Lemma 3.2. The proof is complete. □

7. Affine groups with few conjugacy classes

In this section let H be a finite group acting faithfully on a finite vector space V. Let p be the prime divisor of the order of V. Assume that the order of H is not divisible by p. Let HV be the semidirect product of H and V.

7.1. **Overview.** In order to prove Theorem 1.4, we need to classify all groups HV with the property that the number $k(HV)$ of conjugacy classes of HV is at most p. For Theorem 1.4 we only need this classification when $|V| \geq p^3$, but with Conjecture 1.5 and other purposes in mind, we consider also the case $|V| \leq p^2$.

In fact, this problem was also mentioned to one of us by Gabriel Navarro. The following example of Navarro is mentioned in the paragraph after [RSV, Lemma 1.3]. If $p = 11$, $H = \mathrm{SL}_2(5)$ and $|V| = 11^2$, then $k(HV) = 10 < p$.

We begin with an asymptotic statement.

Theorem 7.1. *There exists a universal constant $c > 0$ such that whenever $p \geq c$ is a prime, V is a finite vector space of order at least p^3 where p is the characteristic of the underlying field and H is a finite group of order coprime to p acting faithfully on V, then $k(HV) > p$.*

Proof. This follows from an inspection of the proof of [MS, Proposition 2.2]. □

The purpose of this section is to work towards an explicit version of Theorem 7.1. Whenever we can we will follow a general approach to try and answer Navarro's question. At points we need to impose explicit lower bounds on the prime p. Since even the case of solvable groups H seems difficult to handle, we will not always treat the situation when H has a quasisimple subnormal subgroup.

In case H is solvable (or more precisely when H does not have a quasisimple subnormal subgroup) an explicit value of the constant c in Theorem 7.1 is computed, see Theorem 8.9. The list of solvable groups HV with $k(HV) \leq p$ and p sufficiently large is difficult to write down. Instead the complete list of large primes p is determined for which there are groups HV with $k(HV) \leq p$.

We accumulate most of the results in the following.

Theorem 7.2. *There exists a universal constant $c > 0$ such that the following is true. There is a vector space V of order p^n where $p \geq c$ is a prime and n is a positive integer and there is a subgroup H of $\mathrm{GL}(V)$ of order coprime to p such that $k(HV) \leq p$ if and only if $n = 1$ or any of the following holds.*

- (i) *$n = 2$ and $p \equiv 1 \pmod{m}$ for some even integer m with $12 \leq m \leq 36$.*
- (ii) *$n = 2$ and $p \equiv 1 \pmod{5}$ and there exists an integer m dividing $p - 1$ such that $5 \leq m \leq 55$ and $(p-1)/m$ is even or $12 \leq m \leq 48$ and $(p-1)/m$ is odd.*

Proof. Set c to be the maximum of 7300000 and the c in the statement of Theorem 7.1. Let $p \geq c$ be a prime. Let V be a vector space of size p^n for some positive integer n. Let H be a finite group of order coprime to p acting faithfully on V. If $n \geq 3$, then $k(HV) > p$ by Theorem 7.1. We may thus assume that $n = 1$ or $n = 2$. For $n = 1$ the result follows from Lemma 7.4. For $n = 2$ the statement follows from Theorem 7.11. □

7.2. **Setup.** Let V be a vector space of size p^n where p is a prime and n is a positive integer. Let H be a subgroup of $\mathrm{GL}(V)$. Assume that the size $|H|$ of H is not divisible by p. Let HV be the semidirect product of V and H with V viewed as an H-module.

Since V is a completely reducible H-module by Maschke's theorem, it may be written in the form $V = V_1 \oplus \cdots \oplus V_s$ where $V_1, \ldots, V_s$ are (non-zero) irreducible H-modules. For each i with $1 \leq i \leq s$, write V_i as a sum $V_{i,1} + \cdots + V_{i,s_i}$ of subspaces $V_{i,j}$ of V_i in such a way that the set $\{V_{i,1}, \ldots, V_{i,s_i}\}$ is left invariant by H and s_i is the largest positive integer with this property. Note that our condition ensures that for every i with $1 \leq i \leq s$ and every j with $1 \leq j \leq s_i$, the stabilizer $H_{i,j}$ in H of the vector space $V_{i,j}$ acts primitively (but not necessarily faithfully) on $V_{i,j}$, that is, $V_{i,j}$ is a primitive $H_{i,j}$-module. However, the $V_{i,j}$ do not necessarily have the same size. Without loss of generality, we assume that $p \leq |V_{1,1}| \leq \ldots \leq |V_{s,1}|$.

The group H acts on the set Ω of all subspaces $V_{i,j}$ with $1 \leq i \leq s$ and $1 \leq j \leq s_i$, that is, H/B may be viewed as a permutation group of degree $t = \sum_{i=1}^{s} s_i$ where B is the subgroup of all elements of H which leave every $V_{i,j}$ invariant.

The aim of this section is to describe pairs (H, V) such that the number $k(HV)$ of conjugacy classes of HV is at most p.

7.3. **Basics.** For a finite group X we denote the number of conjugacy classes of X by $k(X)$. We repeatedly use the bound $k(HV) \geq k(H) + (|V| - 1)/|H|$, which is a consequence of Clifford's theorem. This estimate can be generalized [Sch2, Proposition 3.1b] as follows.

Proposition 7.3. *Let $\{1 = v_1, \ldots, v_r\}$ be a set of representatives for the H-orbits on V. Then $k(HV) = \sum_{i=1}^{r} k(C_H(v_i))$.*

We remark that Proposition 7.3 may be generalized to the situation when the order of H is divisible by p. See a result of Guralnick and Tiep [GT, Corollary 2.5].

7.4. **The metacyclic case.**

Lemma 7.4. *Let H be any subgroup of $\mathrm{GL}_1(p^n).n \leq \mathrm{GL}_n(p) = \mathrm{GL}(V)$. Then $k(HV) \leq p$ if and only if $n = 1$.*

Proof. If $n = 1$, then $H = B$ is cyclic of order dividing $p - 1$ and so

$$k(HV) = |H| + \frac{p-1}{|H|} \leq p.$$

Assume that $k(HV) \leq p$. If $p = 2$, then $n = 1$ must hold. Assume also that $p \geq 3$.

Put $x = |H \cap \mathrm{GL}_1(p^n)|$. We have

$$p \geq k(HV) \geq \frac{x}{n} + \frac{p^n - 1}{xn} = \frac{1}{n}\Big(x + \frac{p^n - 1}{x}\Big) \geq \frac{2}{n}\sqrt{p^n - 1} \tag{7.1}$$

by Clifford's theorem. This is a contradiction for $n \geq 3$ and $p \geq 3$.

Assume that $n = 2$. A more careful estimate as in (7.1) gives

$$p \geq k(HV) \geq 1 + \frac{x-1}{2} + \frac{p^2 - 1}{2x}.$$

Since the function $f(x) = \frac{x}{2} + \frac{p^2-1}{2x}$ defined on the set $\{1, \ldots, p^2 - 1\}$ takes its minimum at $x = p - 1$ and $x = p + 1$ and this minimum is p, we arrive at a contradiction. $\square$

7.5. **The case $p < 17$.**

Lemma 7.5. *Let $p < 17$. Then $k(HV) \leq p$ if and only if $n = 1$ or $p = 11$ and $HV = (C_{11} \times C_{11}) : \mathrm{SL}_2(5)$.*

Proof. If $n = 1$ and H is a subgroup of $\mathrm{GL}_1(p) = \mathrm{GL}(V)$, then $k(HV) \leq p$ by Lemma 7.4. If $p = 11$ and $HV = (C_{11} \times C_{11}) : \mathrm{SL}_2(5)$, then $k(HV) = 10$ by [VL1]. If $n > 1$ and $HV \neq (C_{11} \times C_{11}) : \mathrm{SL}_2(5)$, then HV must have more than 13 conjugacy classes by the tables in [VL1], [VL2] and [VLS]. $\square$

7.6. **The case $n = 2$.**

Lemma 7.6. *Let $n = 2$. If $k(HV) \leq p$, then H is primitive and irreducible on V.*

Proof. If V is not an irreducible and primitive H-module, then B is a normal abelian subgroup (of exponent dividing $p-1$) inside H of index at most 2, and so

$$k(HV) \geq k(H) + \frac{p^2-1}{2|B|} \geq 1 + \frac{|B|-1}{2} + \frac{p^2-1}{2|B|} \geq \frac{1}{2}\Big(|B| + \frac{p^2}{|B|}\Big) > p,$$

since the function $f(x) = x + p^2/x$ takes its minimum at $x = p$ in the interval $[1, p^2]$ and $|B| \neq p$. ∎

Lemma 7.7. *If $n = 2$ and $k(HV) \leq p$, then*

$$k(H) + \frac{|V|-1}{|H|} \leq k(HV) \leq k(H) + \frac{|V|-1}{|H|} + 7200.$$

Proof. Let $n = 2$ and $k(HV) \leq p$. The lower bound for $k(HV)$ follows from Proposition 7.3. We proceed to establish the claimed upper bound.

We know that V is an irreducible and primitive H-module by Lemma 7.6. We also know that H is not a subgroup of $\mathrm{GL}_1(p^2).2$, for otherwise $k(HV) > p$ by Lemma 7.4. We then have $|H/Z(H)| \leq 60$ by [Hup, pp. 213–214].

We claim that there are at most $2(|H/Z(H)| - 1) \leq 118$ elements $h \in H$ such that $|C_V(h)| = p$. For this it is sufficient to see that every non-trivial coset of $Z(H)$ in H contains at most 2 elements h with $|C_V(h)| = p$. Let C be an arbitrary coset of $Z(H)$ in H with an element h fixing a non-zero vector v in V. Since the order of h is not divisible by p, there is a basis $\{v, w\}$ in V such that w is an eigenvector of h with eigenvalue λ say. Observe that $Z(H)$ is a group of scalars and that $C = hZ(H)$. If $\lambda = 1$, then $h = 1$, $C = Z(H)$ and there is no element x in C with $|C_V(x)| = p$. Assume that $\lambda \neq 1$. Let z be the scalar with λ^{-1} in the main diagonal. If $z \in Z(H)$, then hz and h are the only elements in C with a fixed point space of dimension 1. Finally, if $z \notin Z(H)$, then h is the only element in C with a fixed point space of dimension 1. This proves our claim.

Let $\{1 = v_1, \ldots, v_r\}$ be a set of representatives of the H-orbits on V. We have

$$k(HV) = \sum_{i=1}^{r} k(C_H(v_i)) = k(H) + \sum_{i=2}^{r} k(C_H(v_i)) \leq k(H) + \sum_{i=2}^{r} |C_H(v_i)|$$

by Proposition 7.3.

We claim that $\sum_{i=2}^{r} |C_H(v_i)| \leq r + 7079$.

Each non-trivial element of H that fixes a v_i for some i with $2 \leq i \leq r$ can only fix at most $(p-1)/|Z(H)|$ elements of the set $\{v_2, \ldots, v_r\}$. It follows that $\sum_{i=2}^{r} |C_H(v_i)| \leq r - 1 + 118 \cdot (p-1)/|Z(H)|$.

Observe that $|H| > p$ for otherwise $k(HV) > |V|/|H| \geq p$. Thus

$$(p-1)/|Z(H)| \leq |H|/|Z(H)| \leq 60$$

and so $\sum_{i=2}^{r} |C_H(v_i)| \leq r + 7079$, proving the claim.

We proceed to provide an upper bound for r. We proved that there are at most 118 elements $h \in H$ such that $|C_V(h)| = p$. It thus follows from the orbit counting lemma and the inequality $|H| > p$ that

$$r \leq \frac{1}{|H|} \sum_{h \in H} |C_V(h)| \leq \frac{1}{|H|}\Big(|V| + 118p + |H|\Big) < \frac{|V|}{|H|} + 119.$$

We conclude that $k(HV) \leq k(H) + r + 7079 < k(H) + \frac{|V|}{|H|} + 119 + 7079$. □

Lemma 7.8. *Let $n = 2$, $p > 270000$ and H solvable. Then $k(HV) \leq p$ if and only if H has a normal subgroup Q which is a quaternion group of order 8, the group $X = Z(H)$ is cyclic and $|X|$ divides $p - 1$, the Fitting subgroup $F(H)$ is equal to $Q \star X$ and $Q \cap X = Z(Q)$, the factor group $H/F(H)$ is isomorphic to* Sym(3)*, moreover if x denotes $|X : Z(Q)|$ then x divides $(p-1)/2$ and thus has the form $(p-1)/m$ for some even integer m with $12 \leq m \leq 36$.*

Proof. We may assume that the group H acts irreducibly and primitively on V by Lemma 7.6. We may also assume that H is not a subgroup of $\mathrm{GL}_1(p^2).2$ by Lemma 7.4.

We follow the argument of Héthelyi and Külshammer [HK2, p. 661–662]. By [MW, Theorem 2.11], we have $F(H) = Q \star X$ and $Q \cap X = Z(Q)$, where Q is a quaternion group of order 8, which is normal in H, and $X = Z(H)$ is cyclic and $|X|$ divides $p - 1$. Moreover, $H/F(H) \cong C_3$ or $H/F(H) \cong \mathrm{Sym}(3)$. Let $x := |X : Z(Q)|$, so that x divides $(p-1)/2$ (and p is odd). It is computed in [HK2, p. 662] that $k(H) = 7x$ (in which case $|H| = 24x$) if $H/F(H) \cong C_3$ and $k(H) = 8x$ (in which case $|H| = 48x$) if $H/F(H) \cong \mathrm{Sym}(3)$. In the first case the inequality $k(HV) \geq 7x + \frac{p^2-1}{24x} > p$ holds. Assume that the second case holds. We thus have

$$8x + \frac{p^2-1}{48x} \leq k(HV) \leq 8x + \frac{p^2-1}{48x} + 7200 \tag{7.2}$$

by Lemma 7.7.

It is observed on [HK2, p. 662] that the function $f : x \mapsto 8x + (p^2-1)/(48x)$ decreases for $x \leq (p-1)/20$ and increases for $x \geq (p-1)/18$.

If $x \leq (p-1)/48$, then $k(HV) \geq 8 \cdot \frac{p-1}{48} + \frac{p^2-1}{48 \cdot (p-1)/48} > p+1$. Assume that $x \geq (p-1)/46$.

Let $x = (p-1)/m$ where m is even and $2 \leq m \leq 46$. We may rewrite (7.2) as

$$\frac{8}{m}(p-1) + \frac{m}{48}(p+1) \leq k(HV) \leq \frac{8}{m}(p-1) + \frac{m}{48}(p+1) + 7200$$

from which we get

$$\Big(\frac{8}{m} + \frac{m}{48}\Big)p - 4 < k(HV) < \Big(\frac{8}{m} + \frac{m}{48}\Big)p + 7201. \tag{7.3}$$

We have $\frac{8}{m} + \frac{m}{48} < 1$ if and only if m is even and $12 \leq m \leq 36$. Moreover, if $\frac{8}{m} + \frac{m}{48} < 1$, then $\frac{8}{m} + \frac{m}{48} < 0.973$, and so $k(HV) < 0.973p + 7201$ by (7.3), which is at most p provided that $p > 270000$.

It is easy to see that when m is even (and in the range $2 \leq m \leq 46$) and $\frac{8}{m} + \frac{m}{48} \geq 1$, then $\frac{8}{m} + \frac{m}{48} > 1.002$. In this case $p < 1.002p - 4 < k(HV)$ since $p > 270000$. □

Lemma 7.9. *Let $n = 2$. The group H is non-solvable if and only if $H/Z(H)$ is isomorphic to* Alt(5) *and $p = 5$ or $p \equiv 1 \pmod 5$.*

Proof. Let H be a non-solvable subgroup of $\mathrm{GL}(V)$ having order coprime to p. Then $H \leq Z(\mathrm{GL}(V)) \cdot \mathrm{SL}(V)$ by [Giu, Theorem 3.5] and so $H/Z(H)$ is isomorphic to $\mathrm{Alt}(5)$ and $p = 5$ or $p \equiv 1 \pmod 5$ by [Hup, pp. 213–214]. The converse is clear. □

Lemma 7.10. *Let $n = 2$ and $p > 7300000$. There is a non-solvable subgroup H of $\mathrm{GL}(V)$ (of coprime order) with $k(HV) \leq p$ if and only if $p \equiv 1 \pmod 5$ and there exists an integer m dividing $p-1$ such that $5 \leq m \leq 55$ and $(p-1)/m$ is even or $12 \leq m \leq 48$ and $(p-1)/m$ is odd.*

Proof. We may assume by Lemma 7.9 that p is a prime with $p \equiv 1 \pmod 5$, for if $p = 5$ then $k(HV) > 5$ by Lemma 7.5. Write $H = Z(H) \star \mathrm{SL}_2(5)$ as the central product of the cyclic group $Z(H)$ of order dividing $p-1$ and the perfect group $\mathrm{SL}_2(5)$ of order 120 with center of order 2. There are two possibilities for H; the intersection $Z(H) \cap \mathrm{SL}_2(5)$ may have order 1 or 2. In the first case $k(H) = k(\mathrm{SL}_2(5)) \cdot |Z(H)| = 9 \cdot |Z(H)|$ and in the second case $k(H) = 9 \cdot (|Z(H)|/2)$ by [Nav2, Theorem 10.7]. Define c to be 9 if $Z(H) \cap \mathrm{SL}_2(5)$ is trivial and 4.5 if $|Z(H) \cap \mathrm{SL}_2(5)| = 2$. Observe that $c = 9$ if $|Z(H)|$ is odd and $c = 4.5$ if $|Z(H)|$ is even.

We have

$$c \cdot |Z(H)| + \frac{p^2-1}{60 \cdot |Z(H)|} \leq k(HV) \leq c \cdot |Z(H)| + \frac{p^2-1}{60 \cdot |Z(H)|} + 7200 \tag{7.4}$$

by Lemma 7.7. Write $|Z(H)|$ in the form $(p-1)/m$ where m is an integer. Inequality (7.4) becomes

$$\frac{c}{m}(p-1) + \frac{m}{60}(p+1) \leq k(HV) \leq \frac{c}{m}(p-1) + \frac{m}{60}(p+1) + 7200. \tag{7.5}$$

If $m \geq 60$, then $k(HV) > p$ by Lemma 7.5. Thus assume that $m \leq 59$.

We distinguish two cases; when $(p-1)/m$ is odd and when $(p-1)/m$ is even.

Assume first that $(p-1)/m$ is odd. In this case $c = 9$. If $m \leq 8$, then $k(HV) > p$ by (7.5). Thus assume that m is an integer with $9 \leq m \leq 59$. If $12 \leq m \leq 48$, then $\frac{9}{m} + \frac{m}{60} \leq 0.9875$, while if $9 \leq m \leq 11$ or $49 \leq m \leq 59$ then $\frac{9}{m} + \frac{m}{60} > 1.0003$. Inequalities (7.5) imply $k(HV) < 0.9875 \cdot p + 7201$ in the first case and $1.0003 \cdot p - 1 < k(HV)$ in the second case. If $p > 580000$, then $k(HV) < p$ in the first case and $p < k(HV)$ in the second.

Assume that $(p-1)/m$ is even. In this case $c = 4.5$. If $m \leq 4$, then $k(HV) > p$ by (7.5). Thus assume that m is an integer with $5 \leq m \leq 59$. If $5 \leq m \leq 55$, then $\frac{4.5}{m} + \frac{m}{60} < 0.999$, while if $56 \leq m \leq 59$ then $\frac{4.5}{m} + \frac{m}{60} > 1.01$. Inequalities (7.5) imply $k(HV) < 0.999 \cdot p + 7201$ in the first case and $1.01 \cdot p - 1 < k(HV)$ in the second case. If $p > 7300000$, then $k(HV) < p$ in the first case and $p < k(HV)$ in the second. □

Theorem 7.11. *Let $n = 2$ and $p > 7300000$. There exists a subgroup H of $\mathrm{GL}(V)$ (of coprime order) such that $k(HV) \leq p$ if and only if any of the following holds for the prime p.*

(i) $p \equiv 1 \pmod m$ *for some even integer m with $12 \leq m \leq 36$.*

(ii) $p \equiv 1 \pmod 5$ *and there exists an integer m dividing $p-1$ such that $5 \leq m \leq 55$ and $(p-1)/m$ is even or $12 \leq m \leq 48$ and $(p-1)/m$ is odd.*

Proof. There exists a solvable subgroup H of $\mathrm{GL}(V)$ such that $k(HV) \leq p$ if and only if (i) holds. This follows from Lemma 7.8. There exists a non-solvable subgroup H of $\mathrm{GL}(V)$ such that $k(HV) \leq p$ if and only if (ii) holds. This follows from Lemma 7.10. □

We remark that there are infinitely many primes p congruent to 1 modulo any given integer not divisible by p by Dirichlet's theorem on arithmetic progressions.

8. Affine groups with few conjugacy classes: the case $n \geq 3$

We continue to classify groups H acting coprimely and faithfully on a finite vector space V of order p^n ($n \geq 3$) with the property that $k(HV) \leq p$.

We use the setup at the beginning of Section 7.

8.1. **Some general restrictions.** For an index i with $1 \leq i \leq s$, let K_i denote the (faithful) action of H on V_i and B_i denote the kernel of the action of K_i on the set $\{V_{i,1}, \ldots, V_{i,s_i}\}$.

Lemma 8.1. *Let i be an index with $1 \leq i \leq s$. We have $k(K_iV_i) \leq p$ and $k(K_i/B_i) < p$.*

Proof. Let $V_{i'}$ denote the sum of all V_j with $j \neq i$. We have

$$p \geq k(HV) \geq k(HV/V_{i'}) \geq k(HV_i) \geq k(K_iV_i)$$

since HV_i modulo the kernel of the action of H on V_i is K_iV_i. We also have $p \geq k(K_iV_i) > k(K_i/B_i)$ since $B_iV_i \triangleleft K_iV_i$. □

For an index i with $1 \leq i \leq s$ and an index j with $1 \leq j \leq s_i$, the group $H_{i,j}$ was defined to be the stabilizer in H of the vector space $V_{i,j}$.

Lemma 8.2. *For any i and j with $1 \leq i \leq s$ and $1 \leq j \leq s_i$, the number of orbits of $H_{i,j}$ on $V_{i,j}$ is at most p.*

Proof. Fix i and j. The number $r_{i,j}$ of orbits of $H_{i,j}$ on $V_{i,j}$ is independent from j. Clearly, H and so K_i has at least $r_{i,j}$ orbits on V_i. Thus $k(K_iV_i) \geq r_{i,j}$ by Proposition 7.3. We conclude that $r_{i,j} \leq p$ by Lemma 8.1. □

8.2. **Maximal primitive linear groups.** Let i and j be arbitrary indices with $1 \leq i \leq s$ and $1 \leq j \leq s_i$. Let $K_{i,j}$ be the factor group of $H_{i,j}$ modulo the kernel of the action of $H_{i,j}$ on $V_{i,j}$. The vector space $V_{i,j}$ is a faithful, primitive and coprime $K_{i,j}$-module. The goal of this subsection is to show, in as many cases as possible, that the group $K_{i,j}$ has more than p orbits on $V_{i,j}$, under the assumption $p \geq 17$.

Forgetting the indices i and j, let W be a faithful, primitive and coprime P-module over the prime field of size p for some finite group P. Moreover, assume that P is a maximal subgroup of $\mathrm{GL}(W)$ subject to these conditions. There is a (unique and maximal) $\mathbb{F}_{p^k}$-vector space structure $W = W_d(p^k)$ on W for some integers d and k with $n = dk$, where $\mathbb{F}_{p^k}$ is the field of order p^k, such that $P \leq \Gamma\mathrm{L}(d, p^k)$, by [DHP, Theorem 5.1(3)].

If $d = 1$, then $k = n$ and $P = \Gamma\mathrm{L}(1, p^n)$. In this case P has only 2 orbits on W.

Assume that $d \geq 2$. We aim to show, in as many cases as possible, that P has more than p orbits on W, provided that $p \geq 17$. For this we will use the structure theorem given by Duyan, Halasi, Podoski in [DHP, Theorem 5.1] for the P-module W.

Lemma 8.3. *If $n \geq 3$, $d \geq 2$, $p > 3^6$ and P has no component, then P has more than p orbits on W.*

Proof. Let $Z = Z(\mathrm{GL}(W))$. We may assume by [DHP, Theorem 5.1(6)] that $(P \cap \mathrm{GL}(W))/Z$ has a unique minimal normal subgroup RZ/Z, where R is an r-group of symplectic type for some prime r. (The group R has the property that all of its characteristic abelian subgroups are cyclic.) The factor group $R/Z(R)$ has size r^{2a} for some positive integer a. The vector space W is an absolutely irreducible $\mathbb{F}_{p^k}R$-module of dimension $d = r^a$ where k is as before the statement of the lemma. Let the full normalizer of R in $\Gamma\mathrm{L}(W)$ be N. Observe that $P \leq N$. Put $M = N \cap \mathrm{GL}(W)$. The group M/RZ can be considered as a subgroup of the symplectic group $\mathrm{Sp}_{2a}(r)$. Moreover, $|N/M| \leq d$.

We have $|P| \leq p^k \cdot r^{2a^2+4a}$. If $p > 3^6$, $n \geq 3$ and $d \geq 2$, then it is easy to see that $p^k \cdot r^{2a^2+4a} < p^{k \cdot r^a - 1} = |W|/p$, so P has more than p orbits on W. □

8.3. **Permutation groups.**

Lemma 8.4. *Let R be a permutation group of degree r. If R has no alternating composition factor of degree larger than $d \geq 4$, then $|R| \leq d!^{(r-1)/(d-1)}$. Moreover, if R is a primitive permutation group not containing the alternating group $\mathrm{Alt}(r)$, then $|R| < 24^{(r-1)/3}$.*

Proof. The first statement is [Mar1, Corollary 1.5]. The second statement is the fifth sentence in [Mar1, Section 4]. □

For a non-negative integer d we denote the number of partitions of d by $\pi(d)$. For a finite group S let $k^*(S)$ be the number of orbits of $\mathrm{Aut}(S)$ on S.

Lemma 8.5. *Let R be a permutation group of degree r. Let p be a prime at least 17 such that $k(R) \leq p$.*

(i) *If R has an alternating composition factor S of degree d at least 5, then $p > \pi(d)/(2 \cdot |\mathrm{Out(S)}|)$.*
(ii) $|R| \leq (\log p)^{2(r-1)}$.

Proof. Let $S \cong \mathrm{Alt}(d)$ be an alternating composition factor of R with $d \geq 5$. It follows from [Pyb, Lemma 2.5] that $p \geq k(R) \geq k^*(S)$. Thus $p \geq k^*(S) > k(S)/|\mathrm{Out}(S)|$. Since S is a normal subgroup of index 2 in the symmetric group of degree d, it follows that $k(S) \geq \pi(d)/2$ where $\pi(d)$ denotes the number of partitions of d. Statement (1) follows.

Assume again that R has an alternating composition factor of degree $d \geq 5$. From statement (1) and [Mar2, Corollary 3.1] it follows that $p > \pi(d)/8 \geq e^{2\sqrt{d}}/112$. This gives

$$d \leq \frac{(\log p)^2}{8} + 1.7 \log p + 6 < (\log p)^2$$

for $p \geq 17$. Applying Lemma 8.4, we get

$$|R| \leq d!^{(r-1)/(d-1)} \leq d^{r-1} < (\log p)^{2(r-1)}.$$

Finally, if R has no non-abelian alternating composition factor, then

$$|R| \leq 24^{(r-1)/3} \leq (\log p)^{2(r-1)}$$

by Lemma 8.4. □

8.4. **The case $|V_{1,1}| = p \geq 17$ and $s_1 > 1$.** Note that B_1 is an abelian normal subgroup (of exponent dividing $p-1$) of K_1.

Lemma 8.6. *If $|V_{1,1}| = p \geq 17$, then*

$$|K_1/B_1| \cdot (p - k(K_1/B_1)) \geq 2 \cdot (|V_1| - 1)^{1/2} - 1 > |V_1|^{1/2}.$$

Proof. Note that $k(K_1V_1)$ is the number of complex irreducible characters of the group K_1V_1. This is at least $k(K_1)$ plus the number of orbits of K_1 on $\mathrm{Irr}(V_1) \setminus \{1_{V_1}\}$ by Clifford's theorem where 1_{V_1} denotes the trivial character of V_1. Thus

$$p \geq k(K_1V_1) \geq k(K_1) + \frac{|V_1| - 1}{|K_1|} \tag{8.1}$$

by Lemma 8.1. Since B_1 is an abelian normal subgroup of K_1, we also have

$$k(K_1) \geq k(K_1/B_1) + \frac{|B_1| - 1}{|K_1/B_1|}, \tag{8.2}$$

again by Clifford's theorem. Inequalities (8.1) and (8.2) give

$$p \geq k(K_1/B_1) + \frac{|B_1| - 1}{|K_1/B_1|} + \frac{|V_1| - 1}{|K_1|},$$

that is,

$$|K_1/B_1| \cdot (p - k(K_1/B_1)) \geq |B_1| - 1 + \frac{|V_1| - 1}{|B_1|}. \tag{8.3}$$

The real valued function $f(x) = x + \frac{|V_1|-1}{x}$ defined on the interval $[1, |V_1| - 1]$ takes its minimum at $x = \sqrt{|V_1| - 1}$. We get

$$|K_1/B_1| \cdot (p - k(K_1/B_1)) \geq 2 \cdot (|V_1| - 1)^{1/2} - 1 > |V_1|^{1/2}$$

by applying this latter fact to the right-hand side of inequality (8.3). □

Lemma 8.7. *If $|V_{1,1}| = p \geq 17$, then $s_1 \notin \{2, 3, 4, 5\}$.*

Proof. If $|V_{1,1}| = p \geq 17$ and $s_1 \in \{2, 3, 4, 5\}$, then

$$|K_1/B_1| \cdot (p - k(K_1/B_1)) \leq s_1! \cdot (p - 1) < 2 \cdot (p^{s_1} - 1)^{1/2} - 1,$$

violating Lemma 8.6. □

Lemma 8.8. *If $|V_{1,1}| = p \geq 17$, then s_1 cannot be at least* 6.

Proof. Lemma 8.6 gives

$$|K_1/B_1|^2 \cdot p^2 > |K_1/B_1|^2 \cdot (p - k(K_1/B_1))^2 \geq 4 \cdot (|V_1| - 1) > p^{s_1},$$

that is,

$$|K_1/B_1|^2 > p^{s_1 - 2},$$

which implies

$$2.5 \cdot \log\left(|K_1/B_1|^{1/(s_1-1)}\right) \geq 2 \cdot \left(\frac{s_1 - 1}{s_1 - 2}\right) \log\left(|K_1/B_1|^{1/(s_1-1)}\right) > \log p \tag{8.4}$$

since $s_1 \geq 6$.

If K_1/B_1 has no non-cyclic alternating composition factor or if K_1/B_1 is a primitive permutation group not containing $\mathrm{Alt}(s_1)$, then $|K_1/B_1| \leq 24^{(s_1-1)/3}$ by Lemma 8.4. This contradicts (8.4) since $p \geq 17$.

Let $d \geq 5$ be the largest degree of an alternating composition factor S of K_1/B_1. Clearly, $s_1 \geq d$. We may thus modify (8.4) to

$$2 \cdot \left(\frac{d-1}{d-2}\right) \log\left(|K_1/B_1|^{1/(s_1-1)}\right) > \log p. \tag{8.5}$$

Applying the estimate $|K_1/B_1| \leq d!^{(s_1-1)/(d-1)} < d^{(s_1-1)(d-2)/(d-1)}$ from Lemma 8.4 to (8.5), we obtain

$$d^2 > d!^{2/(d-2)} > p. \tag{8.6}$$

It was noted before that the number $k(K_1V_1)$ of complex irreducible characters of the group K_1V_1 is, by Clifford's theorem, at least $k(K_1) \geq k(K_1/B_1)$ plus the number of orbits of K_1 on the set $\mathrm{Irr}(V_1) \setminus \{1_{V_1}\}$, where 1_{V_1} denotes the trivial character of the normal subgroup V_1 of K_1V_1.

Now $k(K_1/B_1) \geq k^*(S)$ by [Pyb, Lemma 2.5]. Since $\mathrm{Aut}(S) = \mathrm{Sym}(d)$ for every $d \geq 5$ different from 6, it is easy to see that $k^*(S)$ is equal to the number $\pi'(d)$ of partitions of d with sign 1, unless $d = 6$ when $k^*(S) = \pi'(d) - 1$.

The number of orbits of K_1 on the set $\mathrm{Irr}(V_1) \setminus \{1_{V_1}\}$ is equal, by Brauer's permutation lemma, to the number of orbits of K_1 on $V \setminus \{1\}$, which is at least s_1. Since K_1/B_1 is a permutation group having an alternating composition factor S of degree $d \geq 5$, we infer that $s_1 \geq d$.

The previous three paragraphs imply $k(K_1V_1) \geq \pi'(d) + s_1$ unless $d = 6$ and $B_1 = 1$. If $d = 6$ and $B_1 = 1$, then $|K_1| \leq 6!^{(s_1-1)/5} < 4^{s_1-1}$ by Lemma 8.4 and so the number of orbits of K_1 on $V \setminus \{1\}$ is at least

$$\frac{p^{s_1}-1}{4^{s_1-1}} \geq \frac{17^{s_1}-1}{4^{s_1-1}} \geq s_1 + 1.$$

We conclude that $k(K_1V_1) \geq \pi'(d) + s_1$ in all cases.

Writing this into (8.6), we obtain

$$d!^{2/(d-2)} > p \geq \pi'(d) + s_1 \geq \pi'(d) + d. \tag{8.7}$$

Using statement (1) of Lemma 8.5 and (8.6) we get

$$d^2 > \pi(d)/(2 \cdot |\mathrm{Out}(S)|). \tag{8.8}$$

It follows that $\pi(d) \geq e^{2\sqrt{d}}/14$ by [Mar2, Corollary 3.1]. Applying this to inequality (8.8), we obtain $d^2 > e^{2\sqrt{d}}/(28 \cdot |\mathrm{Out}(S)|)$ forcing $d < 32$. Furthermore, using Gap [GAP], we find that inequality (8.8) fails for every d with $27 \leq d < 31$. Thus we may assume that d satisfies $5 \leq d \leq 26$. This and (8.7) forces $d \leq 12$ and $p \leq 53$.

We claim that $s_1 < 2d$. For a contradiction assume that $s_1 \geq 2d$. We may modify (8.5) and (8.6) to

$$2 \cdot \left(\frac{2d-1}{2d-2}\right) \log\left(d!^{1/(d-1)}\right) > \log p. \tag{8.9}$$

Using the estimate $p \geq \pi'(d) + s_1 \geq \pi'(d) + 2d$ from (8.7), inequality (8.9) becomes

$$d!^{(2d-1)/(d-1)^2} > p \geq \pi'(d) + 2d. \tag{8.10}$$

There is no pair (d, p) with $5 \leq d \leq 12$ and p a prime satisfying (8.10). We conclude that $s_1 < 2d$.

Recall that K_1/B_1 is a transitive permutation group of degree s_1 such that K_1/B_1 has an alternating composition factor of degree d with $5 \leq d \leq 12$. Since $s_1 < 2d$, the group K_1/B_1 cannot be an imprimitive permutation group. Thus K_1/B_1 is a primitive permutation group. We observed above that K_1/B_1 must then contain $\mathrm{Alt}(s_1)$. We conclude that K_1/B_1 is equal to $\mathrm{Alt}(s_1)$ or $\mathrm{Sym}(s_1)$.

Since we now know that $d = s_1$ and K_1/B_1 is equal to $\mathrm{Alt}(s_1)$ or $\mathrm{Sym}(s_1)$, we may modify (8.7) to

$$|K_1/B_1|^{2/(d-2)} > p \geq k(K_1/B_1) + d \quad \text{with} \quad K_1/B_1 \in \{\mathrm{Alt}(d), \mathrm{Sym}(d)\}. \tag{8.11}$$

Let $K_1/B_1 = \mathrm{Sym}(d)$. A Gap [GAP] computation shows that if a pair (d, p) satisfies (8.11) with $6 \leq d \leq 12$ and p a prime, then

$$(d, p) \in \{(8, 31), (7, 29), (7, 23), (6, 23), (6, 19), (6, 17)\}.$$

Any of these exceptional cases contradicts Lemma 8.6. Thus $K_1/B_1 = \mathrm{Alt}(d)$, and therefore if (d, p) is a pair satisfying (8.11) with $6 \leq d \leq 12$ and $p \geq 17$ a prime, then

$$(d, p) \in \{(9, 31), (9, 29), (8, 23), (7, 19), (7, 17), (6, 17)\}.$$

Again, any of these exceptional cases contradicts Lemma 8.6. □

8.5. **Inducing from a subgroup which acts as a metacyclic group.** Define the integer $n_{1,1}$ by $|V_{1,1}| = p^{n_{1,1}}$. Observe that $n_{1,1} > 1$ by Lemma 7.5 and the previous subsection. Assume that $K_{1,1} \leq \Gamma\mathrm{L}(1, p^{n_{1,1}})$. Notice that $s_1 \geq 2$ by Lemma 7.4.

The normal subgroup B_1 of K_1 may be viewed as a subgroup of the direct product of s_1 copies of $\Gamma\mathrm{L}(1, p^{n_{1,1}})$. In particular, B_1 has an abelian subgroup A_1 of index at most $n_{1,1}^{s_1}$. Thus

$$p \geq k(K_1V_1) \geq k(K_1) \geq \frac{|A_1|}{|K_1 : A_1|} \geq \frac{|A_1|}{n_{1,1}^{s_1} \cdot |K_1/B_1|} \tag{8.12}$$

by Lemma 8.1 and by a result of Ernest [Ern, p. 502] saying that whenever Y is a subgroup of a finite group X then $k(Y)/|X : Y| \leq k(X)$.

Recall that K_1/B_1 may be viewed as a permutation group of degree s_1. Since $k(K_1/B_1) < p$ by Lemma 8.1, it follows that $|K_1/B_1| \leq (\log p)^{2(s_1-1)}$ by Lemma 8.5. Thus

$$|A_1| \leq p \cdot n_{1,1}^{s_1} \cdot (\log p)^{2(s_1-1)} \tag{8.13}$$

by (8.12).

Since $k(K_1V_1) \leq p$ by Lemma 8.1, the group K_1 has at most p orbits on V_1. In particular, $|V_1|/|K_1| \leq p$, which implies

$$p^{n_{1,1} \cdot s_1} = |V_1| \leq |A_1| \cdot p \cdot n_{1,1}^{s_1} \cdot (\log p)^{2(s_1-1)}. \tag{8.14}$$

We get

$$p^{n_{1,1}\cdot s_1} \leq \left(p \cdot n_{1,1}^{s_1} \cdot (\log p)^{2(s_1-1)}\right)^2 \tag{8.15}$$

by (8.13) and (8.14). Since $p^{n_{1,1}}/n_{1,1}^2$ is smallest when $n_{1,1} = 2$, for fixed $p \geq 17$ and with $n_{1,1} \geq 2$, we certainly have

$$p^{2\cdot s_1} \leq \left(p \cdot 2^{s_1} \cdot (\log p)^{2(s_1-1)}\right)^2 \tag{8.16}$$

by (8.15). Inequality (8.16) is equivalent to

$$\left(\frac{p^2}{4(\log p)^4}\right)^{s_1} \leq \frac{p^2}{(\log p)^4}. \tag{8.17}$$

Assume that $p > 256$. Then $p > 4(\log p)^2$. Since the base of the power on the left-hand side of (8.17) is larger than 1, the left-hand side takes its minimum at $s_1 = 2$, for any fixed prime p larger than 256. But (8.17) fails for $s_1 = 2$ and $p > 256$.

8.6. An explicit constant when H is solvable.

Theorem 8.9. *Let V be a vector space of order at least p^3 defined over a field of characteristic $p > 7200$. If $H \leq \mathrm{GL}(V)$ is a finite solvable group of order prime to p, then $k(HV) > p$.*

Proof. Let $n > 2$ and let $H \leq \mathrm{GL}(V)$ be of order prime to p such that $k(HV) \leq p$. Let us use the notation of Subsection 7.2.

Assume that some $V_{i,j}$ has order at least p^3. Let $n_{i,j}$ be such that $|V_{i,j}| = p^{n_{i,j}}$. Then $K_{i,j}$ cannot be a subgroup of $\Gamma\mathrm{L}(1, p^{n_{i,j}})$ by Subsection 8.5, since $p > 256$. Otherwise $K_{i,j}$ has more than p orbits on $V_{i,j}$, since $p > 3^6$, which also contradicts $k(HV) \leq p$. Thus every $V_{i,j}$ has order p or p^2.

Let $|V_{i,j}| = p^2$. If $K_{i,j} \leq \Gamma\mathrm{L}(1, p^2)$, then $s_i = 1$ by Subsection 8.5. Moreover, the case $K_{i,j} \leq \Gamma\mathrm{L}(1, p^2)$ and $s_i = 1$ cannot occur by Lemma 8.1 and Lemma 7.4. Otherwise $K_{i,j}$ has order less than $60p$ and so has more than $p/60$ orbits on $V_{i,j}$. In this case the number of orbits of H on V_i is at least $\binom{s_i+m-1}{m-1}$ by [Fou, Lemma 2.6] where m is the number of orbits of $H_{i,j}$ on $V_{i,j}$. If $s_i \geq 2$, this is more than $m^2/2 \geq p^2/7200 > p$, provided that $p > 7200$, contradicting the fact that H must have less than p orbits on V. We conclude that $|V_{i,j}| = p^2$ implies $s_i = 1$.

If $|V_{i,j}| = p$, then $s_i = 1$ by Subsection 8.4.

We proved not only that each s_i is equal to 1 but the previous argument also gives that whenever i_1 and i_2 are indices with $|V_{i_1,1}| = |V_{i_2,1}| = p^2$ then $i_1 = i_2$.

We claim that whenever i_1 and i_2 are indices with $|V_{i_1,1}| = |V_{i_2,1}| = p$ then $i_1 = i_2$. Assume that this is not the case and consider the faithful action K of H on $W = V_{1,1} + V_{2,1}$. Then $k(KW) \leq p$ by the proof of Lemma 8.1. Since K is an abelian group (of exponent dividing $p - 1$), we have

$$p \geq k(KW) \geq |K| + \frac{|W| - 1}{|K|} \geq 2(|W| - 1)^{1/2} = 2(p^2 - 1)^{1/2}.$$

This is a contradiction.

Since we are assuming that $n \geq 3$, the H-module V must now be a direct sum of a module $V_{1,1}$ of size p and a module $V_{2,1}$ of size p^2. Moreover $K_{2,1}$ acts primitively on $V_{2,1}$ and $|K_{2,1}/Z(K_{2,1})| \leq 60$. It is easy to see that H has an abelian normal subgroup A (of order at most $(p-1)^2$) of index at most 60. Thus

$$p \geq k(HV) \geq \frac{|A|}{60} + \frac{|V|-1}{60|A|} \geq \frac{1}{30}(p^3-1)^{1/2}.$$

This is again a contradiction since $p > 1000$. ☐

9. Proof of Theorem 1.4 and further remarks

We can finally prove Theorem 1.4, which is restated below.

Theorem 9.1. *Let G be a finite group, p a prime and P a Sylow p-subgroup of G. If $|P/\Phi(P)| \geq p^3$, then $|\mathrm{Irr}_{p',p\text{-ar}}(G)| > p$ provided that any of the following two conditions holds.*

1. *G is solvable and $p > 7200$; or*
2. *the McKay–Navarro conjecture is true and p is sufficiently large.*

Proof. As mentioned in Section 2, since the McKay–Navarro conjecture is known to be true for solvable groups, we see that the number of almost p-rational irreducible characters of p'-degree of G is $|\mathrm{Irr}_{p\text{-ar}}(\mathbf{N}_G(P)/P')|$, which is at least $|\mathrm{Irr}_{p\text{-ar}}(\mathbf{N}_G(P)/\Phi(P))|$. As every irreducible character of $\mathbf{N}_G(P)/\Phi(P)$ is almost p-rational, it follows that the number of almost p-rational irreducible characters of p'-degree of G is at least $k(\mathbf{N}_G(P)/\Phi(P))$. Since $|P/\Phi(P)|$ is divisible by p^3, this class number $k(\mathbf{N}_G(P)/\Phi(P))$ of $\mathbf{N}_G(P)/\Phi(P)$ is greater than p by Theorem 8.9, and thus the first part of the theorem is proved.

The second part follows in the same way, but using Theorem 7.1 instead. ☐

We now prove the statement following Theorem 1.3 in the introduction.

Theorem 9.2. *Let G be a non-trivial finite group and p and q be (possibly equal) primes. Then G possesses a non-trivial irreducible character that is of $\{p,q\}'$-degree and almost $\{p,q\}$-rational.*

Proof. It was proved in [GHSV, Theorem 2.1] that, for every nonabelian simple group S and every set of primes $\pi = \{p,q\}$, there exists $\mathbf{1}_S \neq \chi \in \mathrm{Irr}(S)$ of π'-degree such that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(e^{2\pi i/p})$ or $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(e^{2\pi i/q})$, unless (S,π) is $({}^2F_4(2)', \{3,5\})$, $(J_4, \{23,43\})$, or $(J_4, \{29,43\})$. One can check from [Atl] that, for these exceptions, there still exists $\mathbf{1}_S \neq \chi \in \mathrm{Irr}(S)$ of π'-degree such that χ is both almost p-rational and q-rational. The same arguments as in the proof of [GHSV, Theorem C] then yield the conclusion. ☐

We put forward the following, which is based on the McKay–Navarro conjecture and another well-known conjecture that the number of conjugacy classes of any finite group is bounded below logarithmically by the order of the group.

Conjecture 9.3. *There exists a universal constant $c > 0$ such that whenever G is a finite group and P is a Sylow p-subgroup of G then the number of almost p-rational irreducible characters of p'-degree of G is greater than $c \cdot \log_2(|P/\Phi(P)|)$.*

Even the weaker statement that $|\mathrm{Irr}_{p',p\text{-ar}}(G)| \to \infty$ as $|P/\Phi(P)| \to \infty$ seems non-trivial to us (in the case when G is not p-solvable). By Theorem 1.3, this is reduced to showing that $|\mathrm{Irr}_{p',p\text{-ar}}(G)| \to \infty$ as the minimum number of generators of P approaches infinity.

We conclude this section by remarking that, as p-rationality and almost p-rationality of irreducible characters can be seen from the character table, it would be interesting to know a group-theoretic characterization of groups having the property that all irreducible characters are (almost) p-rational for a fixed prime p. Let σ_e ($e \geq 1$) be the Galois automorphism in $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ that fixes p'-roots of unity and sends every p-power root of unity to its $(1+p^e)$-th power. Navarro and Tiep [NT3] proved a consequence of the McKay–Navarro conjecture that if all p'-degree irreducible characters of G are σ_e-fixed, then P/P' has exponent at most p^e, where $P \in \mathrm{Syl}_p(G)$. Therefore, if all irreducible p'-characters of G are almost p-rational, then P/P' is elementary abelian. The converse is expected to be also true, and has been reduced to the same statement for almost quasi-simple groups in [NT3, Theorem C], which in turns has been solved for $p = 2$ in [Mal2].

10. Almost p-rational characters and cyclic Sylow p-subgroups

In this last section we make some remarks on Question 1.5, which predicts that Sylow p-subgroups of a finite group G of order divisible by p are cyclic if and only if

$$|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| \in \mathcal{S}_p := \{e + \frac{p-1}{e} : e \in \mathbb{Z}^+, e \mid p-1\}.$$

Note that, when $P \in \mathrm{Syl}_p(G)$ is cyclic, the Alperin–McKay–Navarro conjecture is known to be true [Nav1], and thus $|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))|$ is the class number of a semidirect product of a certain p'-group acting faithfully on $P/\Phi(P) \cong C_p$, which then belongs to the set $\mathcal{S}_p$. The 'only if' implication therefore easily follows.

Question 1.5 is related to the following, which came out of the results in Sections 7 and 8.

Question 10.1. *Let H be a p'-group acting faithfully on a finite vector space V of size p^n. Is it true that $k(HV) \notin \mathcal{S}_p$ whenever $n \geq 2$?*

We are able to answer this in some cases.

Theorem 10.2. *Question 10.1 has an affirmative answer, provided that any of the following conditions hold.*

1. *$p < 17$;*
2. *p is sufficiently large; or*
3. *the group H is solvable and $p > 7300000$.*

Proof. Let p be a prime and let H be a p'-group acting faithfully on a finite vector space V of size p^n.

Assume that (1) holds. The result follows from Lemma 7.5, the observation of Navarro that $k(HV) = 10$ when $HV = (C_{11} \times C_{11}) : \mathrm{SL}_2(5)$ and by noting that $10 \notin \mathcal{S}_{11}$.

We may assume that $n = 2$ by Theorem 7.1 (if p is sufficiently large) and by Theorem 8.9 (if H is solvable and $p > 7200$).

Assume that $k(HV) \leq p$ (and $p \geq 17$). It follows that H is primitive and irreducible on V by Lemma 7.6.

Let H be solvable. Assume that $p > 270000$. Then (7.3) from the proof of Lemma 7.8 is

$$\Big(\frac{8}{m}+\frac{m}{48}\Big)p-4 < k(HV) < \Big(\frac{8}{m}+\frac{m}{48}\Big)p+7201,$$

for some even integer m with $12 \leq m \leq 36$.

Let H be non-solvable. Assume that $p > 7300000$. Then (7.5) from the proof of Lemma 7.10 is

$$\frac{c}{m}(p-1)+\frac{m}{60}(p+1) \leq k(HV) \leq \frac{c}{m}(p-1)+\frac{m}{60}(p+1)+7200,$$

where m divides $p-1$ such that $5 \leq m \leq 55$ (and $(p-1)/m$ is even) or $12 \leq m \leq 48$ (and $(p-1)/m$ is odd) and $c = 9$ if $|Z(H)|$ is odd and $c = 4.5$ if $|Z(H)|$ is even.

It follows from (7.3) and (7.5) together with a bit of computer calculation that

$$\frac{263}{480}p-4 < k(HV) < \frac{659}{660}p+7201.$$

For $p > 5\cdot 10^6$, we have $\frac{263}{480}p-4 > \frac{p-1}{2}+2$ and $\frac{659}{660}p+7201 < p$. The result follows. □

Theorem 10.3. *An affirmative answer to Question 10.1 and the principal block case of the Alperin–McKay–Navarro imply an affirmative answer to Question 1.5.*

Proof. Assume that both the statement in Question 10.1 and the principal block case of the Alperin–McKay–Navarro conjecture hold true, and that $|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| \in \mathcal{S}_p$. As discussed in Section 2, we then have

$$|\mathrm{Irr}_{p',p\text{-ar}}(B_0(\mathbf{N}_G(P)))| \in \mathcal{S}_p,$$

where $P \in \mathrm{Syl}_p(G)$. By Fong's theorem (see [Nav98, Theorem 10.20]), it follows that

$$|\mathrm{Irr}_{p',p\text{-ar}}(\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P)))| \in \mathcal{S}_p.$$

Since $\chi \in \mathrm{Irr}(\mathbf{N}_G(P)/\mathbf{O}_{p'}(\mathbf{N}_G(P)))$ is almost p-rational and of p'-degree if and only if χ lies over some $\theta \in \mathrm{Irr}(P/\Phi(P))$ (by Lemma 4.2), we now have

$$|\mathrm{Irr}(\mathbf{N}_G(P)/\Phi(P)\mathbf{O}_{p'}(\mathbf{N}_G(P)))| \in \mathcal{S}_p.$$

It then follows that $\dim(P/\Phi(P)) = 1$, and therefore P is cyclic, as desired. □

As the Alperin–McKay–Navarro conjecture is known for p-solvable groups (see Section 2), we have the following for now.

Theorem 10.4. *Let p be a sufficiently large prime. Then for any finite p-solvable group G of order divisible by p, the Sylow p-subgroups of G are cyclic if and only if $|\mathrm{Irr}_{p',p\text{-ar}}(B_0(G))| \in \mathcal{S}_p$.*

References

[Bra1] R. Brauer, On groups whose order contains a prime number to the first power I, *Amer. J. Math.* **64**, (1942), 401–420.

[Bra2] R. Brauer, Representations of finite groups, *Lectures on Modern Mathematics*, Wiley, New York, Vol. I (1963), 133–175.

[BMM] M. Broué, G. Malle, and J. Michel, Generic blocks of finite reductive groups, *Astérisque* **212** (1993), 7–92.

[Car] R. W. Carter, *Finite groups of Lie type. Conjugacy classes and complex characters*, Wiley and Sons, New York et al, 1985.

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

[DHP] H. Duyan, Z. Halasi, and K. Podoski, Random bases for coprime linear groups, *J. Group Theory* **23** (2020), 133–157.

[Ern] J. A. Ernest, Central intertwining numbers for representations of finite groups, *Trans. Amer. Math. Soc.* **99** (1961), 499–508.

[Fou] D. A. Foulser, Solvable primitive permutation groups of low rank, *Trans. Amer. Math. Soc.* **143** (1969), 1–54.

[GM] M. Geck and G. Malle, *The character theory of finite groups of Lie type: a guided tour*, Cambridge University Press, Cambridge, 2020.

[GAP] The GAP Group, GAP Groups, Algorithms, and Programming, Version 4.4, 2004. http://www.gap-system.org

[GHSV] E. Giannelli, N. N. Hung, A. A. Schaeffer Fry, and C. Vallejo, Characters of π'-degree and small cyclotomic fields, *Ann. Math. Pura Appl.* (2020). https://doi.org/10.1007/s10231-020-01025-x.

[Giu] M. Giudici, Maximal subgroups of almost simple groups with socle $\mathrm{PSL}(2, q)$. https://arxiv.org/abs/math/0703685

[GI] D. Gluck and I. M. Isaacs, Tensor induction of generalized characters and permutation characters, *Illinois J. Math.* **27** (1983), 514–518.

[GR] R. M. Guralnick and G. R. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006), 509–528.

[GT] R. M. Guralnick and P. H. Tiep, The non-coprime $k(GV)$ problem, *J. Algebra* **293** (2005), 185–242.

[HK1] L. Héthelyi and B. Külshammer, On the number of conjugacy classes of a finite solvable group, *Bull. London Math. Soc.* **32** (2000), 668–672.

[HK2] L. Héthelyi and B. Külshammer, On the number of conjugacy classes of a finite solvable group II, *J. Algebra* **270** (2003), 660–669.

[HM] N. N. Hung and A. Maróti, p-Regular conjugacy classes and p-rational irreducible characters, *J. Algebra*, (2021). https://doi.org/10.1016/j.jalgebra.2021.02.007

[Hup] B. Huppert, *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York, 1967.

[Isa] I. M. Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, Rhode Island, 2006.

[Mal1] G. Malle, Extensions of unipotent characters and the inductive McKay condition, *J. Algebra* **320** (2008), 2963–2980.

[Mal2] G. Malle, The Navarro–Tiep Galois conjecture for $p = 2$, *Arch. Math.* **112** (2019), 449–457.

[MM] G. Malle and A. Maróti, On the number of p'-degree characters in a finite group, *Int. Math. Res. Not.* **20** (2016), 6118–6132.

[MT] G. Malle and D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, 133. Cambridge University Press, Cambridge, 2011.

[MW] O. Manz and T. R. Wolf, *Representations of solvable groups*, London Mathematical Society Lecture Note Series **185**, Cambridge University Press, Cambridge, 1993.

[Mar1] A. Maróti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631–640.

[Mar2] A. Maróti, On elementary lower bounds for the partition function. *Integers* **3** (2003), A10, 9 pp.

[Mar3] A. Maróti, A lower bound for the number of conjugacy classes of a finite group, *Adv. Math.* **290** (2016), 1062–1078.

[MS] A. Maróti and I. I. Simion, Bounding the number of classes of a finite group in terms of a prime, *J. Group Theory* **23** (2020), 471–488.

[McK] J. McKay, Irreducible representations of odd degree, *J. Algebra* **20** (1972), 416–418.

[Nav98] G. Navarro, *Characters and blocks of finite groups*, London Mathematical Society Lecture Note Series, Vol. 250, Cambridge University Press, Cambridge, 1998.

[Nav1] G. Navarro, The McKay conjecture and Galois automorphisms, *Ann. of Math. (2)* **160** (2004), 1129–1140.

[Nav2] G. Navarro, *Character theory and the McKay conjecture*, Cambridge Studies in Advanced Mathematics **175**, Cambridge University Press, Cambridge, 2018.

[NST] G. Navarro, R. M. Solomon, and P. H. Tiep, Abelian Sylow subgroups in a finite group II, *J. Algebra* **421** (2015), 3–11.

[NSV] G. Navarro, B. Späth, and C. Vallejo, A reduction theorem for the Galois–McKay conjecture, *Trans. Amer. Math. Soc.* **373** (2020), 6157–6183.

[NT1] G. Navarro and P. H. Tiep, Degrees of rational characters of finite groups, *Adv. Math.* **224** (2010), 1121–1142.

[NT2] G. Navarro and P. H. Tiep, Abelian Sylow subgroups in a finite group, *J. Algebra* **398** (2014), 519–526.

[NT3] G. Navarro and P. H. Tiep, Sylow subgroups, exponents, and character values, *Trans. Amer. Math. Soc.* **372** (2019), 4263–4291.

[NT4] G. Navarro and P. H. Tiep, The fields of values of characters of degree not divisible by p, *Forum Math. Pi* **9** (2021), 1–28.

[NTT] G. Navarro, P. H. Tiep, and A. Turull, p-Rational characters and self-normalizing Sylow p-subgroups, *Represent. Theory* **11** (2007), 84–94.

[Pyb] L. Pyber, Finite groups have many conjugacy classes, *J. London Math. Soc.* **46** (1992), 239–249.

[RSV] N. Rizo, A. A. Schaeffer Fry, and C. Vallejo, Galois action on the principal block and cyclic Sylow subgroups, *Algebra & Number Theory* **14** (2020), 1953–1979.

[SF] A. A. Schaeffer Fry, Action of Galois automorphisms on Harish-Chandra series and Navarro's self-normalizing Sylow 2-subgroup conjecture, *Trans. Amer. Math. Soc.* **372** (2019), 457–483.

[Sch1] P. Schmid, Extending the Steinberg representation, *J. Algebra* **150** (1992), 254–256.

[Sch2] P. Schmid, *The solution of the $k(GV)$ problem*, ICP Advanced Texts in Mathematics **4**, Imperial College Press, London, 2007.

[Tay] J. Taylor, Action of automorphisms on irreducible characters of symplectic groups, *J. Algebra* **505** (2018), 211–246.

[TZ] P. H. Tiep and A. E. Zalesskii, Unipotent elements of finite groups of Lie type and realization fields of their complex representations, *J. Algebra* **271** (2004), 327–390.

[Tur1] A. Turull, Above the Glauberman correspondence, *Adv. Math.* **217** (2008), 2170–2205.

[Tur2] A. Turull, The strengthened Alperin-McKay conjecture for p-solvable groups, *J. Algebra* **394** (2013), 79–91.

[VL1] A. Vera López and J. Vera López, Classification of finite groups according to the number of conjugacy classes, *Israel J. Math.* **51** (1985), 305–338.

[VL2] A. Vera López and J. Vera López, Classification of finite groups according to the number of conjugacy classes II, *Israel J. Math.* **56** (1986), 188–221.

[VLS] A. Vera López and J. Sangroniz, The finite groups with thirteen and fourteen conjugacy classes, *Math. Nachr.* **280** (2007), 676–694.

Department of Mathematics, The University of Akron, Akron, OH 44325, USA
Email address: hungnguyen@uakron.edu

FB Mathematik, TU Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany
Email address: malle@mathematik.uni-kl.de

Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
Email address: maroti.attila@renyi.hu