ON THE COMMUTING PROBABILITY OF p-ELEMENTS IN A FINITE GROUP

TIMOTHY C. BURNESS, ROBERT M. GURALNICK, ALEXANDER MORETÓ,
AND GABRIEL NAVARRO

ABSTRACT. Let G be a finite group, let p be a prime and let $\mathrm{Pr}_p(G)$ be the probability that two random p-elements of G commute. In this paper we prove that $\mathrm{Pr}_p(G) > (p^2+p-1)/p^3$ if and only if G has a normal and abelian Sylow p-subgroup, which generalizes previous results on the widely studied commuting probability of a finite group. This bound is best possible in the sense that for each prime p there are groups with $\mathrm{Pr}_p(G) = (p^2 + p - 1)/p^3$ and we classify all such groups. Our proof is based on bounding the proportion of p-elements in G that commute with a fixed p-element in $G \setminus \mathbf{O}_p(G)$, which in turn relies on recent work of the first two authors on fixed point ratios for finite primitive permutation groups.

1. INTRODUCTION

The *commuting probability* of a finite group G is the probability that two random elements of G commute, namely

$$\mathrm{Pr}(G) = \frac{|\{(x,y) \in G \times G \, : \, xy = yx\}|}{|G|^2}.$$

A celebrated, but elementary, result of Gustafson [11] asserts that $\mathrm{Pr}(G) > 5/8$ if and only if G is abelian, which is best possible since $\mathrm{Pr}(D_8) = 5/8$. This concept has been widely studied in recent years and some natural analogues for infinite groups have also been investigated (see, for instance, [1, 6, 10, 13, 17, 20]). In addition, the commuting variety of elements in Lie algebras and algebraic groups has been a subject of great interest for several decades. This was originally introduced by Motzkin and Taussky [16] and further studied by Richardson [19], Ginzburg [9], Premet [18] and others.

In this paper, we pursue a local version of Gustafson's theorem, which turns out to be significantly more challenging.

Definition. Let G be a finite group, let p be a prime and let G_p be the set of p-elements in G (that is, the set of elements in G of order p^m for some $m \geqslant 0$). Then

$$\mathrm{Pr}_p(G) = \frac{|\{(x,y) \in G_p \times G_p \, : \, xy = yx\}|}{|G_p|^2}$$

is the probability that two random p-elements of G commute. Note that $\mathrm{Pr}_p(G) = 1$ if and only if G has a normal and abelian Sylow p-subgroup.

Local versions of the commuting probability have also been studied in the context of algebraic groups and Lie algebras. In particular, Premet [18] identified the irreducible components of the commuting variety of nilpotent elements of a reductive Lie algebra defined over an algebraically closed field of good characteristic (and similarly, as an immediate consequence, for unipotent elements in the corresponding reductive algebraic groups). The set of commuting r-tuples of elements of order p (or commuting nilpotent elements of nilpotence degree p in a p-restricted Lie algebra) has also been studied for its connection to problems in representation theory (see [5]). For finite groups, a generating function is presented in [7] for counting the number of commuting pairs of p-elements in some finite classical groups in good characteristic.

In this paper we consider arbitrary finite groups. Given a prime number p, set

$$f(p) = \frac{p^2 + p - 1}{p^3}.$$

Our first main result is the following.

Theorem A. *Let G be a finite group and let p be a prime. Then $\mathrm{Pr}_p(G) > f(p)$ if and only if G has a normal and abelian Sylow p-subgroup.*

In particular, if G is a nonabelian finite simple group and $|G|$ is divisible by p, then $\mathrm{Pr}_p(G) \leqslant f(p)$. We can say more in this situation.

Theorem B. *Let G be a nonabelian finite simple group and let p be a prime divisor of $|G|$. Then $\mathrm{Pr}_p(G) = f(p)$ if and only if $p \geqslant 5$ and G is isomorphic to $\mathrm{PSL}_2(p)$.*

In fact, we can classify all the finite groups G with $G = \mathbf{O}^{p'}(G)$ and $\mathrm{Pr}_p(G) = f(p)$, where $\mathbf{O}^{p'}(G)$ is the subgroup of G generated by G_p. See Theorem 5.2 for a precise statement. In particular, we observe that there is no nonsolvable group with $\mathrm{Pr}_2(G) = 5/8$ and no nonsolvable group $G = \mathbf{O}^{3'}(G)$ with $\mathrm{Pr}_3(G) = 11/27$. In addition, if G is given as in Theorem B with p a fixed prime, then $\mathrm{Pr}_p(G)$ tends to 0 as $|G|$ tends to infinity; we refer the reader to the end of Section 5 for further details.

Our next result, which may be of independent interest, is a key ingredient in the proof of Theorem A. Recall that $\mathbf{O}_p(G)$ denotes the largest normal p-subgroup of G.

Theorem C. *Let G be a finite group and let p be a prime. Then*

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} \leqslant \frac{1}{p}$$

for every p-element $x \in G \setminus \mathbf{O}_p(G)$.

This can be extended as follows.

Theorem D. *Let G be a finite group and let p be a prime. If $x \in G$ is a p-element and*

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} > \frac{1}{p},$$

then $x \in \mathbf{Z}(\mathbf{O}_p(G))$.

Remark 1. It is easy to see that the converse of Theorem D is false. For example, if $G = D_{8(2m+1)}$, then $|\mathbf{C}_G(x)_2|/|G_2| = 1/(2m+2)$ if $x \in \mathbf{Z}(\mathbf{O}_2(G))$ has order 4. On the other hand, in Examples 3.16 (p odd) and 3.17 ($p = 2$) we present a family of examples (G, p, x), where $x \in \mathbf{Z}(\mathbf{O}_p(G))$ is nontrivial and $|\mathbf{C}_G(x)_p|/|G_p|$ tends to 1 as p tends to infinity.

Remark 2. Let G be a finite group with $\mathbf{O}_p(G) = 1$. Then the conclusions in Theorems A and C are still valid if we work with elements of order p instead of all p-elements (with essentially no change in the proofs). And similarly for Theorem 5.2, which includes Theorem B as a special case.

The proofs of our main results depend upon the classification of finite simple groups. However, it is worth noting that our proof of Theorem C does not require the classification if we assume that x normalizes, but does not centralize, some normal p'-subgroup of G. This implies that the classification is not required for Theorem A under the assumption that the generalized Fitting subgroup of G is a p'-group (and so in particular, if G is p-solvable). In order to handle the general case, we use a recent result of the first two authors [2] on fixed point ratios of elements of prime order in primitive permutation groups (see Theorem 3.4).

Remark 3. Let us observe that

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} = \frac{\Psi(x)}{\Psi(1)},$$

where Ψ is the permutation character for the action of G on its p-elements by conjugation. In the language of permutation groups, this number coincides with the fixed point ratio of x with respect to this action, which explains why the main theorem of [2] will be an important ingredient in the proof of Theorem C.

2. SOME PRELIMINARY RESULTS

For the remainder of this paper, all groups are finite and p is a prime number. We will frequently use the elementary fact that if G is a group and $H, K \leqslant G$ are subgroups, then

$$|H : H \cap K| \leqslant |G : K| \tag{1}$$

with equality if and only if $G = HK$.

Lemma 2.1. *Let G be a finite group and let N be a normal p-subgroup.*

(i) *If $x \in G$ is a p-element, then*

$$|\mathbf{C}_G(x)_p|/|G_p| \leqslant |\mathbf{C}_{G/N}(Nx)_p|/|(G/N)_p|.$$

(ii) $\mathrm{Pr}_p(G) \leqslant \mathrm{Pr}_p(G/N).$

Proof. Both parts quickly follow from the fact that $|G_p| = |(G/N)_p||N|$. $\square$

Remark 2.2. In the previous lemma, the assumption that N is a p-subgroup is essential. For example, there is a semidirect product $G = C_{35}{:}D_{12}$ with a normal subgroup N of order 3 such that $G/N = D_{10} \times D_{14}$ and we compute

$$\mathrm{Pr}_2(G) = \frac{211}{1296} > \frac{11}{72} = \mathrm{Pr}_2(G/N).$$

(Here G is `SmallGroup`$(420, 30)$ in the `GAP` Small Groups library [8].) One can check that this is the smallest finite group with $\mathrm{Pr}_p(G) > \mathrm{Pr}_p(G/N)$ for some prime p.

There is a special case where quotients by normal subgroups of order prime to p do not change the proportions.

Lemma 2.3. *Let G be a finite group and let N be a central p'-subgroup.*

(i) *If $x \in G$ is a p-element, then*

$$|\mathbf{C}_G(x)_p|/|G_p| = |\mathbf{C}_{G/N}(Nx)_p|/|(G/N)_p|.$$

(ii) *If N is central in G, then $\mathrm{Pr}_p(G) = \mathrm{Pr}_p(G/N)$.*

Proof. Let $x \in G$ be a p-element and suppose that $[x, y] \in N$ for some $y \in G$. Since $[x, N] = 1$ it follows that $[x^p, y] = [x, y]^p$, so $[x, y] = 1$. In addition, if y is a p-element, then y is the only p-element in the coset Ny and so (i) follows. Now (ii) follows from (i), noting that G and G/N both have the same number of p-elements. $\square$

Lemma 2.4. *Let P be a p-group acting on a p'-group K and let L be a P-invariant subgroup of K. If*

$$\frac{|\mathbf{C}_K(P) : \mathbf{C}_L(P)|}{|K : L|} < 1, \tag{2}$$

then

$$\frac{|\mathbf{C}_K(P) : \mathbf{C}_L(P)|}{|K : L|} \leqslant \frac{1}{p+1}.$$

Proof. Let $C = \mathbf{C}_K(P)$ and note that $K \neq CL$ in view of the inequality in (2). For any prime q, let L_q be a P-invariant Sylow q-subgroup of L, which is contained in a P-invariant Sylow q-subgroup K_q of K (see [12, Corollary 3.25]). Thus $K_q \cap L = L_q$. By coprime action, $C_q := C \cap K_q$ and $C \cap L_q$ are Sylow q-subgroups of C and $C \cap L$, respectively (see [12, Lemma 3.32], for example). In view of (2) we have

$$\prod_q \frac{|C_q : C_q \cap L|}{|K_q : L_q|} = \frac{|C : C \cap L|}{|K : L|} < 1$$

and we note that

$$\frac{|C_q : C_q \cap L|}{|K_q : L_q|} = \frac{|C_q : C_q \cap L_q|}{|K_q : L_q|} \leqslant 1$$

for every prime q (see (1)). Therefore,

$$\frac{|C : C \cap L|}{|K : L|} \leqslant \frac{|C_q : C_q \cap L|}{|K_q : L_q|}$$

for every q, so the bound in (2) implies that

$$\frac{|C_q : C_q \cap L|}{|K_q : L_q|} < 1$$

for some q. As a consequence, we are free to assume that K is a q-group.

Arguing by induction on $|K : L|$, we may assume that L is a maximal P-invariant subgroup of K. Then L is normal in K and K/L does not have any proper nontrivial P-invariant subgroups, whence (2) implies that $C = \mathbf{C}_K(P) = \mathbf{C}_L(P)$. If $|\mathbf{C}_K(y) : \mathbf{C}_L(y)| = |K : L|$ for every $y \in P$, then P acts trivially on K/L and thus $K = CL$, which is incompatible with (2). Therefore, we may assume that $P = \langle y \rangle$ is cyclic. Then the action of P on K/L is a Frobenius action, which implies that if $x \in K \setminus L$, then $\{L, Lx^z : z \in P\}$ is a set of distinct cosets of L in K. Therefore $|K : L| \geqslant |P| + 1 \geqslant p + 1$, as required. $\square$

Next we record the following well known result.

Lemma 2.5. *Let G be a finite group, let $x, y \in G$ and let $K \leqslant G$ be a subgroup normalized by x and y. If $Kx = Ky$ and $|K|$ is coprime with $o(x)o(y)$, then x and y are K-conjugate.*

Proof. We may assume $G = K\langle x, y \rangle$ and thus K is normal in G. Since $Kx = Ky$, it follows that $K\langle x \rangle = K\langle y \rangle = G$. Now, $K \cap \langle x \rangle = K \cap \langle y \rangle = 1$ and we also note that $o(x) = o(y)$ and $\langle x \rangle, \langle y \rangle$ are Hall π-subgroups of G, where π is the set of primes dividing $o(x)$. By the Schur-Zassenhaus theorem, we have $\langle x \rangle^k = \langle y \rangle$ for some $k \in K$ and thus $x^k = y^n$ for some integer n. Now, $Ky = Kx = Kx^k = Ky^n$ and $y^n y^{-1} \in K \cap \langle y \rangle = 1$, so $y^n = y$ and the result follows. $\square$

We shall need one more well known fact about coprime actions, which follows from [12, Theorem 3.27].

Lemma 2.6. *Let G and A be finite groups with coprime orders and suppose that A acts on G by automorphisms. Set $C = \mathbf{C}_G(A)$. Then $G = C[A, G]$ and $[A, [A, G]] = [A, G]$.*

3. Proofs of Theorems C and D

In this section we prove Theorems C and D. We begin by handling a special case of Theorem C, which relies on the following proposition. In part (i), we write $(Ky)_p$ for the set of p-elements in the coset Ky, where p is a fixed prime throughout this section.

Proposition 3.1. *Let G be a finite group and let K be a normal p'-subgroup of G. Let $x \in G$ be an element of order p such that $K = [x, K]$ and let $y \in G$ be a p-element with $[x, y] = 1$.*

   (i) *If $[y, K] \neq 1$, then the proportion of elements in $y^K = (Ky)_p$ which commute with x is at most $1/(p+1)$.*

   (ii) *If $L = \langle K, x \rangle$, then the proportion of p-elements in the coset Ly which commute with x is at most $1/p$.*

Proof. First consider (i). Since K is a p'-group, Lemma 2.5 implies that y^K is precisely the set of p-elements in the coset Ky. Next observe that $y^K \cap \mathbf{C}_G(x) = (yK)_p \cap \mathbf{C}_G(x) = (Ay)_p$, where $A = \mathbf{C}_K(x)$, and another application of Lemma 2.5 gives $(Ay)_p = y^A$. Therefore, the proportion of elements in y^K which commute with x is equal to

$$\frac{|y^K \cap \mathbf{C}_G(x)|}{|y^K|} = \frac{|\mathbf{C}_K(x) : \mathbf{C}_K(x) \cap \mathbf{C}_K(y)|}{|K : \mathbf{C}_K(y)|}. \tag{3}$$

If every element in y^K commutes with x, then $[y, K] \leqslant \mathbf{C}_K(x)$. But then the three subgroups lemma implies that y centralizes $[x, K] = K$, which is incompatible with the condition $[y, K] \neq 1$ in (i). Therefore, the proportion in (3) is less than 1 and by applying Lemma 2.4 (with $L = \mathbf{C}_K(y)$ and $P = \langle x \rangle$) we deduce that it is at most $1/(p+1)$ as required.

We now prove (ii). For $0 \leqslant i < p$, let a_i be the number of p-elements in $Kx^i y$ commuting with x and let $b_i = |(Kx^i y)_p|$, so $\alpha = \sum_i a_i / \sum_i b_i$ is the proportion of p-elements in Ly which commute with x. If $[x^i y, K] \neq 1$ for all i, then (i) implies that $a_i/b_i \leqslant 1/(p+1)$ and we immediately deduce that $\alpha \leqslant 1/(p+1)$. Therefore, we may assume $[y, K] = 1$ (otherwise replace y by $x^i y$ for some i). For $1 \leqslant i < p$ it follows that $[x^i y, K] \neq 1$ (since $[x, K] = K$) and thus $a_i/b_i \leqslant 1/(p+1)$. Since $|y^K| = 1$ we have $a_0 = b_0 = 1$ and we deduce that

$$\alpha \leqslant \frac{1}{p+1} + \frac{p}{(p+1)m},$$

where $m = |(Ly)_p|$. Finally, we note that $b_i \geqslant (p+1)a_i \geqslant p+1$ for $1 \leqslant i < p$ (since $x^i y \in Kx^i y$ is a p-element commuting with x), so $m \geqslant 1 + (p-1)(p+1) = p^2$ and we conclude that $\alpha \leqslant 1/p$. $\qquad\square$

We are now ready to prove a special case of Theorem C.

Theorem 3.2. *Let G be a finite group and let $x \in G$ be an element of order p. If there exists a normal p'-subgroup K of G with $[x, K] \neq 1$, then*

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} \leqslant \frac{1}{p}. \tag{4}$$

Proof. By Lemma 2.1, we may assume that $\mathbf{O}_p(G) = 1$. We can also assume that $G = K\mathbf{C}_G(x)$ and we may replace K by any proper normal subgroup of G contained in K that does not centralize x. In particular, by Lemma 2.6, we can replace K by $[x, K]$ and so we may assume that $K = [x, K]$.

Set $L = \langle K, x \rangle$ and let $y \in G$ be a p-element. It suffices to show that the proportion of p-elements in the coset Ly which commute with x is at most $1/p$. Clearly, if no p-element in Ly commutes with x, then this proportion is 0, so we may assume $[x, y] = 1$. Now apply Proposition 3.1(ii). $\qquad\square$

Remark 3.3. Let $\mathbf{F}^*(G)$ be the generalized Fitting subgroup of G. If $\mathbf{F}^*(G)$ is a p'-group, then $\mathbf{O}_p(G) = 1$ and the statement of Theorem 3.2 holds for every nontrivial p-element x because we can replace x by an element of order p in $\langle x \rangle$. Of course, if the upper bound in (4) holds for all elements in G of order p (modulo $\mathbf{O}_p(G)$), then the same bound holds for every nontrivial p-element in G.

Recall that if G is a permutation group on a finite set Ω, then the *fixed point ratio* of an element $z \in G$, denoted $\mathrm{fpr}(z, \Omega)$, is the proportion of points in Ω fixed by z. It is easy to see that if G is transitive and H is a point stabilizer, then

$$\mathrm{fpr}(z, \Omega) = \frac{|z^G \cap H|}{|z^G|}.$$

The following is a simplified version of the main theorem of [2].

Theorem 3.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with point stabilizer H. If $z \in G$ has prime order p, then either*

$$\mathrm{fpr}(z, \Omega) \leqslant \frac{1}{p+1},$$

or one of the following holds (up to permutation isomorphism):

   (i) *G is almost simple and either*

      (a) *$G = S_n$ or A_n acting on k-element subsets of $\{1, \ldots, n\}$ with $1 \leqslant k < n/2$; or*

      (b) *$(G, H, z, \mathrm{fpr}(z, \Omega))$ is known.*

  (ii) *G is an affine group, $\mathbf{F}^*(G) = \mathbf{F}(G) = (C_p)^d$, $z \in \mathrm{GL}_d(p)$ is a transvection and $\mathrm{fpr}(z, \Omega) = 1/p$.*

 (iii) *$G \leqslant A \wr S_t$ is a product type group with its product action on $\Omega = \Gamma^t$ and $z \in A^t \cap G$, where $A \leqslant \mathrm{Sym}(\Gamma)$ is one of the almost simple primitive groups in part (i).*

We will also need the following corollary to Theorem 3.4 in the almost simple setting (see [2, Corollary 3]). Recall that the *socle* of an almost simple group G is its unique minimal normal subgroup, which coincides with $\mathbf{F}^*(G)$.

Corollary 3.5. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite almost simple primitive permutation group with socle J. If $z \in G$ has prime order p, then either*

$$\mathrm{fpr}(z, \Omega) \leqslant \frac{1}{p},$$

or one of the following holds (up to permutation isomorphism):

   (i) *$J = A_n$ and Ω is the set of k-element subsets of $\{1, \ldots, n\}$ for some $1 \leqslant k < n/2$;*

  (ii) *$(J, p) = (\mathrm{PSL}_2(q), q - 1), (\mathrm{Sp}_6(2), 3), (\mathrm{PSU}_4(2), 2), (\mathrm{Sp}_n(2), 2)$ or $(\Omega_n^\epsilon(2), 2)$.*

We will now use Theorem 3.4 and Corollary 3.5 to handle two more special cases of Theorem C, which will then be applied to obtain the result in full generality. In the following proposition, the *components* of K are the quasisimple groups referred to in the statement.

Proposition 3.6. *Let K be a central product of quasisimple groups with $\mathbf{O}_p(K) = 1$ and let $x, y \in \mathrm{Aut}(K)$ be nontrivial p-elements such that x does not normalize any component of K. Assume that the simple quotients of the components of K are isomorphic. Then the proportion of elements in y^K which commute with x is at most $1/(p+1)$.*

Proof. We may assume that $[x, y] = 1$ and x has order p. Let $K_1, \ldots, K_t$ be the components of K and set $L_i = K_i / \mathbf{Z}(K_i) \cong L$. Note that t is a multiple of p since x acts fixed point freely on the set of components. We can now view x and y as commuting automorphisms of the direct

product $J := L^t$, with $o(x) = p$ and $o(y) = p^m$ for some $m \geqslant 1$. Set $G = \langle J, x, y \rangle \leqslant \operatorname{Aut}(J)$ and note that J is the unique minimal normal subgroup of G. Now

$$\frac{|y^J \cap \mathbf{C}_G(x)|}{|y^J|} = \frac{|x^J \cap \mathbf{C}_G(y)|}{|x^J|}$$

and it suffices to show that

$$\frac{|x^J \cap \mathbf{C}_G(y)|}{|x^J|} \leqslant \frac{1}{p+1}. \tag{5}$$

Let M be a maximal subgroup of G containing $\mathbf{C}_G(y)$ and observe that M does not contain J since $G = J\mathbf{C}_G(y)$. This allows us to view G acting primitively on the set of cosets $\Omega = G/M$ and we note that

$$\frac{|x^J \cap \mathbf{C}_G(y)|}{|x^J|} \leqslant \frac{|x^G \cap M|}{|x^G|} = \operatorname{fpr}(x, \Omega).$$

Then by applying Theorem 3.4, noting that $x \notin \operatorname{Aut}(L)^t \cap G$ by hypothesis, it follows that $\operatorname{fpr}(x, \Omega) \leqslant 1/(p+1)$ and thus (5) holds. $\qquad \square$

Next we seek a version of Proposition 3.6 in the special case where K is quasisimple (see Propositions 3.10 and 3.12). In order to do this, we will need the following elementary result.

Lemma 3.7. *Let G be a finite group, let $x \in G \setminus \mathbf{O}_p(G)$ be a p-element and set*

$$D = \{y \in G : \langle y \rangle \text{ is } G\text{-conjugate to } \langle x \rangle\}.$$

Then $|D| \geqslant p^2 - 1$.

Proof. Without loss of generality, we may assume that $\mathbf{O}_p(G) = 1$ and x has order p. Consider the natural action of G on the set C of conjugates of $\langle x \rangle$ and note that $|D| = (p-1)|C|$, so it suffices to show that $|C| \geqslant p+1$. Note that x fixes $\langle x \rangle \in C$, so it has at least one fixed point on C. If x acts trivially on C, then x centralizes each of its conjugates and thus, by Baer's theorem, $x \in \mathbf{O}_p(G)$, which is a contradiction. Therefore, x acts nontrivially on C and we conclude that $|C| \geqslant p+1$. $\qquad \square$

Remark 3.8. Let G, D and p be given as in Lemma 3.7. Then $|D| = p^2 - 1$ if and only if $|G_p| = p^2$ and the groups with this property are determined in Lemma 5.1.

We also need the following result, which is a corollary of Theorem 3.4.

Lemma 3.9. *Let G be an almost simple group with socle J and assume J is not isomorphic to an alternating group. Let p be a prime divisor of $|J|$ and suppose $x \in G$ has order p. Then there exists an element $y \in J$ of order p such that*

$$\frac{|y^G \cap \mathbf{C}_G(x)|}{|y^G|} \leqslant \frac{1}{p+1}.$$

Proof. We may assume $G = \langle J, x \rangle$ and we may embed $\mathbf{C}_G(x)$ in a core-free maximal subgroup H of G, so

$$\frac{|y^G \cap \mathbf{C}_G(x)|}{|y^G|} \leqslant \frac{|y^G \cap H|}{|y^G|} = \operatorname{fpr}(y, G/H)$$

for every element $y \in J$ of order p. Clearly, the desired conclusion holds if there exists such an element with $\operatorname{fpr}(y, G/H) \leqslant 1/(p+1)$, so we may assume otherwise, in which case (G, H, y) is one of the special cases arising in part (i)(b) of Theorem 3.4. More precisely, [2, Theorem 1] implies that either G is a classical group in a subspace action (and the special cases that arise are recorded in [2, Table 6]), or $G = \mathrm{M}_{22}{:}2$, $H = \mathrm{PSL}_3(4).2_2$ and $p = 2$. In the latter case one can check that $\operatorname{fpr}(y, G/H) = 3/11$ if $y \in J$ is an involution, so we may assume G is a classical group in a subspace action. We now inspect the cases in [2, Table 6].

If J is a unitary, symplectic or orthogonal group, then it is easy to check that in every case (G, H) there exists an element $y \in J$ of order p such that $\mathrm{fpr}(y, G/H) \leqslant 1/(p+1)$. For example, if $J = \mathrm{PSp}_n(q)$ with $n \geqslant 4$, $H = P_1$ is the stabilizer of a 1-space and $p = q$, then we can take $y = (J_2^2, J_1^{n-4})$, where J_i denotes a standard unipotent Jordan block of size i.

To complete the proof, let us assume $J = \mathrm{PSL}_n(q)$ is a linear group and note that $H = P_1$ is the stabilizer of a 1-space. If $n \geqslant 4$ then once again it is straightforward to see that there is an element $y \in J$ of order p with $\mathrm{fpr}(y, G/H) \leqslant 1/(p+1)$, so we may assume $n \in \{2, 3\}$. Suppose $n = 3$. If $p = q \geqslant 3$ then we can choose $y = (J_3)$, while for $q = 2$ we must take $y = (J_2, J_1)$ and one can use GAP [8] to verify the desired bound in the statement of the lemma. Similarly, if $p = q - 1 \geqslant 3$ then we can take y to be the image (modulo scalars) of a diagonal matrix $(\omega, \omega^{-1}, I_1)$, where $\omega \in \mathbb{F}_q^\times$ has order p. And if $(q, p) = (3, 2)$ then $y = (-I_2, I_1)$ is the only option and the result can be checked using GAP.

Finally, suppose $J = \mathrm{PSL}_2(q)$, so $q \geqslant 7$ since $\mathrm{PSL}_2(4)$ and $\mathrm{PSL}_2(5)$ are both isomorphic to A_5. If $p = q - 1$ then $|y^G| = q(q+1)$ and $|\mathbf{C}_G(x)| < q$, so the desired bound holds. Now assume $q = p$. Here both x and y are regular unipotent elements and we compute $|y^G| = (p^2 - 1)/2$ and $|y^G \cap \mathbf{C}_G(x)| = (p-1)/2$, which implies that

$$\frac{|y^G \cap \mathbf{C}_G(x)|}{|y^G|} = \frac{1}{p+1}.$$

The result follows. $\square$

Proposition 3.10. *Let K be a quasisimple group such that $\mathbf{O}_p(K) = 1$ and $K/\mathbf{Z}(K)$ is not isomorphic to an alternating group. Let $x \in \mathrm{Aut}(K)$ be a nontrivial p-element.*

(i) *There is a normal subset D of nontrivial p-elements in K such that $|D| \geqslant p^2 - 1$ and the proportion of elements in D which commute with x is at most $1/(p+1)$.*

(ii) *Let $y \in \mathrm{Aut}(K)$ be a nontrivial p-element.*

  (a) *The proportion of elements in y^K which commute with x is at most $1/p$, unless $K = \Omega_n^+(2)$, $n \geqslant 8$, $p = 2$ and both x and y are transvections, in which case the proportion is $1/2 + 1/2(2^{\frac{n}{2}} - 1)$.*

  (b) *The proportion of elements in $(Ky)_p$ which commute with x is at most $1/p$.*

Proof. We may assume x has order p. Set $J = K/\mathbf{Z}(K)$ and view x as an automorphism of J of order p. Set $G = \langle J, x \rangle$. By Lemma 3.9, there exists an element $y \in J$ of order p such that

$$\frac{|y^J \cap \mathbf{C}_G(x)|}{|y^J|} \leqslant \frac{|y^G \cap \mathbf{C}_G(x)|}{|y^G|} \leqslant \frac{1}{p+1}. \tag{6}$$

If we write y for the corresponding element in K, then by applying Lemma 3.7 we deduce that the normal subset

$$D = \{z \in K \;:\; \langle z \rangle \text{ is } K\text{-conjugate to } \langle y \rangle\} = \bigcup_{i=1}^{t} z_i^K$$

contains at least $p^2 - 1$ elements. Moreover, (6) implies that the proportion of elements in z_i^K which commute with x is at most $1/(p+1)$ for $1 \leqslant i \leqslant t$ and thus part (i) follows.

Now let us turn to part (ii). We may assume $[x, y] = 1$ and we may view y as an automorphism of J with $o(y) = p^a$ for some $a \geqslant 1$. Set $G = \langle J, x, y \rangle \leqslant \mathrm{Aut}(J)$ and embed $\mathbf{C}_G(y)$ in a core-free maximal subgroup H of G, which allows us to view G as an almost simple primitive permutation group on $\Omega = G/H$.

For now, let us exclude the special cases (J, p) in Corollary 3.5(ii). Then Corollary 3.5 implies that

$$\frac{|y^J \cap \mathbf{C}_G(x)|}{|y^J|} = \frac{|x^J \cap \mathbf{C}_G(y)|}{|x^J|} \leqslant \frac{|x^G \cap H|}{|x^G|} = \mathrm{fpr}(x, G/H) \leqslant \frac{1}{p} \tag{7}$$

and thus the proportion of elements in y^K which commute with x is at most $1/p$.

Next consider the coset Ky. Write $(Ky)_p = y_1^K \cup \cdots \cup y_r^K$ as a disjoint union of K-classes. If $Ky \neq K$ then each y_i is a nontrivial p-element and so the proportion of elements in y_i^K commuting with x is at most $1/p$ by (7) and the desired result follows. A very similar argument applies when $Ky = K$, but here we have to account for the identity element. To do this, write $K_p = \{1\} \cup D \cup z_1^K \cup \cdots \cup z_s^K$, where D is the normal subset in (i) and each z_i is nontrivial. Set $a_0 = |D \cap \mathbf{C}_K(x)| + 1$, $b_0 = |D| + 1$, $a_i = |z_i^K \cap \mathbf{C}_K(x)|$ and $b_i = |z_i^K|$ for $i \geqslant 1$. As above, we have $a_i/b_i \leqslant 1/p$ for $i \geqslant 1$, so it suffices to show that $a_0/b_0 \leqslant 1/p$. If we write $D = y_1^K \cup \cdots \cup y_t^K$, then $|y_i^K \cap \mathbf{C}_K(x)|/|y_i^K| \leqslant 1/(p+1)$ for each i and thus

$$\frac{a_0}{b_0} \leqslant \frac{1}{p+1} + \frac{p}{m(p+1)},$$

where $m = |D| + 1$. Since $m \geqslant p^2$ we deduce that $a_0/b_0 \leqslant 1/p$ and the result follows.

To complete the proof of (ii), it remains to consider the special cases (J, p) in Corollary 3.5(ii). In each of these cases, G is an almost simple classical group in a subspace action with point stabilizer H and there exists an element $z \in G$ of order p with $\mathrm{fpr}(z, G/H) > 1/p$. The possibilities for (G, H, z) are recorded in [2, Table 1]. By inspection, we observe that either

(a) $\mathbf{C}_G(z)$ is contained in a maximal subgroup M of G such that $\mathrm{fpr}(z', G/M) \leqslant 1/p$ for all $z' \in G$ of order p; or

(b) $G = \mathrm{O}_n^+(2)$, $n \geqslant 8$, $p = 2$, H is the stabilizer of a nonsingular 1-space and $z = (J_2, J_1^{n-2})$.

So excluding the special case in (b), the previous argument goes through. In particular, the previous argument applies if $y \in K$ (note that in case (b), z is contained in $\mathrm{O}_n^+(2) \setminus J$).

We have now reduced to the case where $G = \mathrm{O}_n^+(2)$, $p = 2$ and both x and y are transvections. Here $y^J = y^G$ and $\mathbf{C}_G(x) = H$ is the stabilizer of a nonsingular 1-space, so [2, Theorem 1] gives

$$\frac{|y^J \cap \mathbf{C}_G(x)|}{|y^J|} = \mathrm{fpr}(y, G/H) = \frac{1}{2} + \frac{1}{2(2^{\frac{n}{2}} - 1)}$$

for the proportion of elements in y^K commuting with x. So this is an exception to the main bound in (ii)(a), but we still claim that the proportion of 2-elements in Ky commuting with x is at most $1/2$.

To see this, write $(Ky)_2 = y^K \cup y_1^K \cup \cdots \cup y_r^K$ as a disjoint union. By [2, Theorem 1], the proportion of elements in y_i^K which commute with x is at most $1/3$ for each $1 \leqslant i \leqslant r$. As a consequence, we deduce that the proportion of 2-elements in Ky commuting with x is at most $1/2$ so long as

$$3.2^{\frac{n}{2}-1} = \frac{3|y^K|}{2^{\frac{n}{2}} - 1} \leqslant \sum_{i=1}^{r} |y_i^K|.$$

But this inequality clearly holds since $|z^G| \geqslant 2^{\frac{n}{2}-1}(2^{\frac{n}{2}} - 1)$ for every nontrivial 2-element $z \in G$. $\qquad\square$

Remark 3.11. Let us observe that the upper bound in Proposition 3.10(ii)(b) is best possible. For example, let $K = \mathrm{PSL}_2(p)$ and let x and y be inner automorphisms of K of order p. Then $|(Ky)_p| = p^2$ and $|\mathbf{C}_K(x)| = p$, so the relevant proportion is exactly $1/p$.

We need a different result to handle alternating and symmetric groups.

Proposition 3.12. *Let $L = S_n$ and $J = A_n$, where $n \geqslant 5$. Let $x \in L$ be an element of prime order p and let $y \in L$ be a transposition.*

(i) *If p is odd, then the proportion of p-elements in J which commute with x is at most $1/p$.*

(ii) *If $p = 2$ and x is not a transposition, then the proportion of 2-elements in J or Jy which commute with x is at most $1/2$.*

(iii) *If $p = 2$ and x is a transposition, then the proportion of 2-elements in L which commute with x is at most $1/2$.*

Proof. First assume p is odd and $|\mathrm{supp}(x)| = m \geqslant 5$ with respect to the natural action of L on $\{1, \ldots, n\}$. Note that p divides m and it suffices to work inside $H := A_m \times A_{n-m}$ since H contains $\mathbf{C}_J(x)_p$. In particular, we may assume that $m = n$. The result is clear if $m = p$, so assume $m > p$. Here $\mathbf{C}_J(x)$ is contained in an imprimitive subgroup $K = A_p \wr A_{m/p}$ and so if we write $J_p = x_0^J \cup \cdots \cup x_t^J$ with $x_0 = 1$, then

$$\frac{|\mathbf{C}_J(x)_p|}{|J_p|} \leqslant \frac{|K_p|}{|J_p|} = \frac{1 + \sum_{i=1}^{t} a_i}{1 + \sum_{i=1}^{t} b_i},$$

where $a_i = |x_i^J \cap K|$ and $b_i = |x_i^J|$. Now Theorem 3.4 implies that $a_i/b_i \leqslant 1/(p+1)$ for all i and we deduce that

$$\frac{|\mathbf{C}_J(x)_p|}{|J_p|} \leqslant \frac{1}{p+1} + \frac{p}{(p+1)c},$$

where $c = |J_p|$. Since $c \geqslant p^2$ (for example, this follows from Lemma 3.7) we conclude that this proportion is at most $1/p$, as required.

So to complete the proof of (i), it remains to handle the special case where $x = (1, 2, 3)$ is a 3-cycle. Set $d = |(S_{n-3})_3|$ and note that $|\mathbf{C}_J(x)_3| = 3d$. If $a = (1, 2, i) \in J$ with $i \geqslant 4$, then for each 3-element $b \in J$ fixing $1, 2$ and i we see that $a^{\pm}b \in J \setminus \mathbf{C}_J(x)$ is a 3-element. Therefore, $|J_3| \geqslant 2d(n-3) + 3d$ and thus

$$\frac{|\mathbf{C}_J(x)_3|}{|J_3|} \leqslant \frac{3}{2n - 3} \leqslant \frac{1}{3}$$

for $n \geqslant 6$. The case $n = 5$ can be handled directly.

For the remainder, let us assume $p = 2$ and write $|\mathrm{supp}(x)| = 2m$. For $m \geqslant 4$ we can essentially repeat the argument in (i). Write $\mathbf{C}_L(x) = (S_2 \wr S_m) \times S_{n-2m}$ and let a_1 and a_2 be the number of even and odd 2-elements in $S_2 \wr S_m$, respectively. Similarly, let $b_1 = |(A_{n-2m})_2|$ and $b_2 = |(S_{n-2m} \setminus A_{n-2m})_2|$. Then

$$|\mathbf{C}_J(x)_2| = a_1 b_1 + a_2 b_2, \quad |\mathbf{C}_L(x)_2 \cap Jy| = a_1 b_2 + a_2 b_1.$$

We claim that

$$a_1 \leqslant \frac{1}{2}|(A_{2m})_2|, \quad a_2 \leqslant \frac{1}{2}|(S_{2m} \setminus A_{2m})_2|. \tag{8}$$

To see this, set $K = A_{2m}$ and $H = (S_2 \wr S_m) \cap K$, so $a_1 = |H_2|$. By [2, Theorem 1], we observe that $|z^K \cap H|/|z^K| \leqslant 1/3$ for every nontrivial 2-element $z \in K$ and by arguing as in case (i) we deduce that $|H_2|/|K_2| \leqslant 1/2$. This justifies the first inequality in (8) and a very similar argument establishes the second. As an immediate consequence, we deduce that

$$|\mathbf{C}_J(x)_2| \leqslant \frac{1}{2}|(S_{2m} \times S_{n-2m})_2 \cap J|, \quad |\mathbf{C}_L(x)_2 \cap Jy| \leqslant \frac{1}{2}|(S_{2m} \times S_{n-2m})_2 \cap Jy|$$

and thus the proportion of 2-elements in J and Jy commuting with x is at most $1/2$. In the same way, if $m = 3$ then we can reduce to the case $n = 6$ and here we can check the result directly.

Next assume $m = 2$, say $x = (1, 2)(3, 4)$. Set $d = |(S_{n-4})_2|$ and note that

$$|\mathbf{C}_J(x)_2| = |\mathbf{C}_L(x)_2 \cap Jy| = 4d.$$

Fix i, j with $4 < i < j$. Let $Z(i, j)$ (respectively, $W(i, j)$) be the set of elements in L of the form uv, where u is a 4-cycle (respectively, a double transposition different from $(1, 2)(i, j)$) on $\{1, 2, i, j\}$ and v is a 2-element fixing each of these 4 points. Then $|Z(i, j)| = 6d$ and $|W(i, j)| = 2d$, so there are at least $2d$ distinct 2-elements of each parity in $Z(i, j) \cup W(i, j)$, none of which commute with x. Since there are $(n-4)(n-5)/2$ choices for $\{i, j\}$, and the

corresponding sets of 2-elements are pairwise disjoint, this implies that the proportion of 2-elements in each coset commuting with x is at most

$$\frac{4}{4 + (n-4)(n-5)} \leqslant \frac{1}{2}$$

for $n \geqslant 7$. The cases $n = 5, 6$ can be handled directly.

Finally, let us assume $x = (1, 2)$ is a transposition. Set $d = |(S_{n-2})_2|$ and note that $|\mathbf{C}_L(x)_2| = 2d$. For each $j \in \{3, \dots, n\}$, let Z_j denote the set of 2-elements in L which interchange 1 and j. Note that the Z_j are pairwise disjoint sets of size d and no element in Z_j commutes with x. Therefore, $|L_2| \geqslant nd$ and we conclude that the proportion of 2-elements in L centralizing x is at most $2/n$. $\qquad\square$

Remark 3.13. One can show that the conclusion in part (ii) of Proposition 3.12 also holds when x is a transposition. But the proof is more involved and we do not require the stronger result.

Remark 3.14. In the proof of Theorem C, we will need to extend Proposition 3.12 to central extensions K of A_n with $\mathbf{O}_p(K) = 1$. This follows by Lemma 2.3 unless an element of order p does not centralize $\mathbf{Z}(K)$. This only occurs when $p = 2$ and K is a 3-fold cover of A_n. One can check the result directly for these cases.

Finally, we are now ready to complete the proof of Theorem C.

Proof of Theorem C. Let G be a finite group and let $x \in G \setminus \mathbf{O}_p(G)$ be a p-element. Let $\mathbf{F}(G)$ and $\mathbf{F}^*(G)$ denote the Fitting and generalized Fitting subgroups of G, respectively, and note that $x \notin \mathbf{F}(G)$. By Lemma 2.1, we may assume that $\mathbf{O}_p(G) = 1$. Without loss of generality, we may assume $o(x) = p$.

If x does not centralize $\mathbf{O}_{p'}(G)$, then the result follows by Theorem 3.2. Therefore, we may assume $x \in \mathbf{C}_G(\mathbf{F}(G))$ and thus G is nonsolvable. Since x is not in $\mathbf{O}_p(G)$, x acts faithfully on $\mathbf{F}^*(G)$ and therefore it must act faithfully on some subgroup K, which is a central product of quasisimple components (each with order divisible by p). We may assume that K is a minimal such subgroup, which implies that G acts transitively on the components of K. Note that $\mathbf{O}_p(K) = 1$.

We can further assume that $G = K\mathbf{C}_G(x)$ since both G and $K\mathbf{C}_G(x)$ contain the same number of p-elements commuting with x. Therefore, $\mathbf{C}_G(x)$ acts transitively on the components of K, so either

(a) every orbit of x on the components of K has size p; or

(b) x normalizes each component of K, inducing the same automorphism (up to conjugacy) on each component.

For each $y \in \mathbf{C}_G(x)_p$ it suffices to show that the proportion of p-elements in the coset Ky which commute with x is at most $1/p$. Fix such an element y and observe that we may assume that $G = \langle K, x, y \rangle$. In addition, by repeating the argument above, we can reduce to the case where $\langle x, y \rangle$ acts transitively on the components of K. We now consider cases (a) and (b) in turn.

First assume (a) holds, so x does not normalize any component of K. Let $z \in Ky$ be a nontrivial p-element. Then by Proposition 3.6, the proportion of elements in z^K commuting with x is at most $1/(p+1)$. Therefore, if $Ky \neq K$ then the proportion of p-elements in Ky which commute with x is at most $1/(p+1)$. Similarly, if $Ky = K$ then Lemma 3.7 implies that $|K_p| \geqslant p^2$ and by expressing K_p as a union of K-classes we quickly deduce that $|\mathbf{C}_K(x)_p|/|K_p| \leqslant 1/p$ as required.

Finally, let us assume (b) holds, in which case y must act transitively on the components of K. If K has two or more components, then y is nontrivial and we can just interchange x and y in the argument above (noting that any element in Ky still acts transitively on

the set of components). This allows us to reduce to the case where K is quasisimple. The result now follows by applying Propositions 3.10(ii)(b) and 3.12, except for the case where $K/\mathbf{Z}(K) = A_n$ is an alternating group, $p = 2$ and x acts as a transposition on K. In this case, set $L = \langle K, x \rangle \cong S_n$ and note that it suffices to show that the proportion of 2-elements in the coset Ly which commute with x is at most $1/2$. This follows from Proposition 3.12(iii). $\quad\square$

Theorem D now follows by combining Theorem C with the following result.

Proposition 3.15. *Let G be a finite group and let $x \in \mathbf{O}_p(G) \setminus \mathbf{Z}(\mathbf{O}_p(G))$. Then*

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} \leqslant \frac{1}{p}.$$

Proof. Set $Q = \mathbf{O}_p(G)$ and note that we may assume $G = Q\mathbf{C}_G(x)$. Let $y \in \mathbf{C}_G(x)$ be a p-element and note that $(Qy)_p = Qy$. Then the number of elements in the coset Qy commuting with x is equal to $|\mathbf{C}_Q(x)|$, which is at most $|Q|/p$ since $x \notin \mathbf{Z}(Q)$. Therefore, the proportion of p-elements in Qy commuting with x is at most $1/p$ and the result follows. $\quad\square$

To close this section, we present a family of examples to show that there exist finite groups G with a p-element x such that

$$\frac{1}{p} < \frac{|\mathbf{C}_G(x)_p|}{|G_p|} < 1.$$

Note that Theorem D implies that such an element x must be in $\mathbf{Z}(\mathbf{O}_p(G))$. In fact, our examples have the property that this ratio tends to 1 as $|G|$ tends to infinity.

We consider the cases p odd and $p = 2$ separately.

Example 3.16. Fix an odd prime p and consider the semidirect product $H = A{:}B$, where $A = (C_p)^3$ is elementary abelian and a generator b for $B = C_p$ acts on A with a single Jordan block. Let $a \in A$ be a generator for A as a module for B. Note that A contains a normal subgroup K of H with $|K| = p^2$. Fix an element $x \in K \setminus H$.

Let r be a prime with $r \equiv 1 \pmod{p}$ and fix a scalar $\mu \in \mathbb{F}_r^\times$ of order p. Let $V = (\mathbb{F}_r)^p$ be a p-dimensional vector space over $\mathbb{F}_r$ and consider the semidirect product $G = V{:}H$, where K acts trivially on V, a acts as $(\mu, \dots, \mu)$ and b acts via $(1, \mu, \dots, \mu^{p-1})$. We now compute

$$|\mathbf{C}_G(x)_p| = (p^3 - p^2)r^p + p^2, \quad |G_p| = (p^3 - p^2)r^p + (p^4 - p^3)r^{p-1} + p^2. \tag{9}$$

This follows by counting the p-elements in each coset Vh of V, noting that if h centralizes x, then the entire coset does as well. Here it is also helpful to observe that $|(hV)_p| = |h^V|$, where $|h^V| = r^p$ if $h \in A \setminus K$ and $|h^V| = r$ for $h \in H \setminus A$.

Finally, let us observe that both expressions in (9) are polynomials in r of degree p, with the same leading coefficient, whence $|\mathbf{C}_G(x)_p|/|G_p|$ tends to 1 as r tends to infinity.

Similarly, we can present a family of examples for $p = 2$.

Example 3.17. Let $H = \langle a, b \rangle = D_{16}$, where $o(a) = 8$ and $o(b) = 2$. Fix an odd prime r and let V be a 2-dimensional vector space over $\mathbb{F}_r$. Consider the semidirect product $G = V{:}H$, where a acts as $(-1, -1)$ on V and b acts as $(-1, 1)$. Let $x \in H$ be an element of order 4. Since

$$|\mathbf{C}_G(x)_2| = 4r^2 + 4, \quad |G_2| = 4r^2 + 8r + 4,$$

we conclude that the ratio $|\mathbf{C}_G(x)_2|/|G_2|$ tends to 1 as r tends to infinity.

4. Proof of Theorem A

In this section we prove Theorem A. We begin with some general observations. As always, G is a finite group and p is a prime. As in Section 1, we set

$$f(p) = \frac{p^2 + p - 1}{p^3}.$$

Lemma 4.1. *If G/N is a p'-group, then $\mathrm{Pr}_p(G) = \mathrm{Pr}_p(\langle G_p \rangle) = \mathrm{Pr}_p(N)$.*

Proof. This is clear because $G_p = \langle G_p \rangle_p = N_p$. $\qquad\square$

We need the following elementary generalization of Gustafson's theorem [11] on the commuting probability $\mathrm{Pr}(G)$. This result explains the presence of the term $f(p)$ in Theorem A and it extends [13, Lemma 1.3].

Lemma 4.2. *Let p be the smallest prime divisor of $|G|$. If $\mathrm{Pr}(G) > f(p)$, then G is abelian.*

Proof. Recall that $\mathrm{Pr}(G) = k(G)/|G|$, where $k(G)$ is the number of conjugacy classes in G (see [11]). Seeking a contradiction, let us assume G is nonabelian. Let $K_1, \ldots, K_r$ be the non-central conjugacy classes of G and note that $|K_i| \geqslant p$ for every i, so we have

$$|G| = |\mathbf{Z}(G)| + \sum_{i=1}^{r} |K_i| \geqslant |\mathbf{Z}(G)| + rp$$

and thus $r \leqslant (|G| - |\mathbf{Z}(G)|)/p$. Therefore,

$$k(G) = |\mathbf{Z}(G)| + r \leqslant \left(\frac{p-1}{p}\right)|\mathbf{Z}(G)| + \frac{|G|}{p}$$

and thus

$$\mathrm{Pr}(G) \leqslant \frac{(p-1)/p}{|G : \mathbf{Z}(G)|} + \frac{1}{p} \leqslant \frac{(p-1)/p}{p^2} + \frac{1}{p} = f(p),$$

where we have used the fact that $G/\mathbf{Z}(G)$ is not cyclic in the last inequality. This is a contradiction. $\qquad\square$

We now prove Theorem A. Note that if $\mathbf{F}^*(G)$ is a p'-group, then the proof does not require the classification of finite simple groups.

Proof of Theorem A. Let G be a finite group and let P be a Sylow p-subgroup of G. As previously noted, if P is both normal and abelian, then $\mathrm{Pr}_p(G) = 1$.

Now assume $\mathrm{Pr}_p(G) > f(p)$. We need to show that P is a normal abelian subgroup of G. To do this, we first use induction on $|G|$ to show that P is normal.

By Lemma 2.1, $\mathrm{Pr}_p(G/\mathbf{O}_p(G)) > f(p)$. If $\mathbf{O}_p(G) \neq 1$, then the inductive hypothesis implies that $G/\mathbf{O}_p(G)$ has a normal Sylow p-subgroup, so $\mathbf{O}_p(G)$ is a Sylow p-subgroup of G and we are done. Now assume $\mathbf{O}_p(G) = 1$. By Theorem C, we have

$$\mathrm{Pr}_p(G) = \frac{1}{|G_p|^2} \sum_{x \in G_p} |\mathbf{C}_G(x)_p| \leqslant \frac{1}{|G_p|}\left(1 + \frac{|G_p| - 1}{p}\right). \tag{10}$$

Consider the real-valued function

$$\varphi_p(x) = \frac{1}{x}\left(1 + \frac{x-1}{p}\right) = \frac{1}{x}\left(1 - \frac{1}{p}\right) + \frac{1}{p},$$

which is a decreasing function for $x > 0$. Seeking a contradiction, assume that P is not normal. Then $|G_p| \geqslant p^2$ (this is clear if $|P| \geqslant p^2$, and for $|P| = p$ it follows from the fact that G has at least $p + 1$ Sylow p-subgroups by Sylow's theorem). Hence,

$$\varphi_p(|G_p|) \leqslant \varphi_p(p^2) = \frac{1}{p^2}\left(1 - \frac{1}{p}\right) + \frac{1}{p} = f(p)$$

and we conclude that

$$\mathrm{Pr}_p(G) \leqslant \varphi_p(|G_p|) \leqslant f(p),$$

a contradiction. Therefore, P is a normal subgroup of G.

Finally, Lemma 4.1 yields

$$\mathrm{Pr}(\mathbf{O}_p(G)) = \mathrm{Pr}_p(\mathbf{O}_p(G)) = \mathrm{Pr}_p(G) > f(p)$$

and thus Lemma 4.2 implies that $\mathbf{O}_p(G)$ is abelian. $\square$

5. Proof of Theorem B

In this final section we determine the finite groups G with $\mathrm{Pr}_p(G) = f(p)$, which will allow us to prove Theorem B as a special case. We will need the following auxiliary result.

Lemma 5.1. *Let p be a prime and let G be a finite group such that $G = \mathbf{O}^{p'}(G)$ and G has a Sylow p-subgroup of order p. If $\mathrm{Pr}_p(G) = f(p)$, then either*

(i) *G is isomorphic to $\mathrm{PSL}_2(p)$ or $\mathrm{SL}_2(p)$; or*

(ii) *$p = 2^r - 1 \geqslant 7$ is a Mersenne prime and $G = (C_2)^r{:}C_p$, where C_p acts as a Singer cycle on $(C_2)^r$.*

Proof. If $x \in G$ is a nontrivial p-element, then $|\mathbf{C}_G(x)_p| = p$ and we easily deduce that $\mathrm{Pr}_p(G) = f(p)$ if and only if $|G_p| = p^2$, or equivalently if G has precisely $p + 1$ Sylow p-subgroups. Let P be a Sylow p-subgroup and let K be the largest normal subgroup of G normalizing each Sylow p-subgroup of G. Then K is a p'-group and so $[K, P] \leqslant K \cap P = 1$. Therefore, K is centralized by every p-element in G, so the condition $G = \mathbf{O}^{p'}(G)$ implies that $K \leqslant \mathbf{Z}(G)$ and G/K is a doubly transitive subgroup of S_{p+1}. Moreover, each point stabilizer in this action is the normalizer of a Sylow p-subgroup and thus $|G/K| \leqslant p(p^2 - 1)$.

If $p = 2$, then $G/K \cong S_3$ and it is easy to check that $G = S_3 \cong \mathrm{PSL}_2(2)$ is the only possibility. Similarly, if $p = 3$ then $G/K \cong A_4$ and $G = A_4 \cong \mathrm{PSL}_2(3)$ or $\mathrm{SL}_2(3) \cong Q_8{:}C_3$ are the only options. For the remainder we may assume that $p \geqslant 5$.

Suppose p is not a Mersenne prime. Then G/K is nonsolvable and by inspecting the list of doubly transitive groups [4, Theorem 5.3] we see that $G/K \cong \mathrm{PSL}_2(p)$. Since $\mathrm{PSL}_2(p)$ is perfect and K is central in G, by considering the Schur multiplier of $\mathrm{PSL}_2(p)$ we deduce that $G = \mathrm{PSL}_2(p)$ or $\mathrm{SL}_2(p)$.

Finally, let us assume $p = 2^r - 1 \geqslant 7$ is a Mersenne prime, so r is an odd prime. If G/K is almost simple, we deduce as above that $G = \mathrm{PSL}_2(p)$ or $\mathrm{SL}_2(p)$. The other possibility is that G/K has a normal elementary abelian 2-subgroup of order $p+1 = 2^r$. Thus $G/K \leqslant \mathrm{AGL}_r(2)$. Here each element in $\mathrm{AGL}_r(2)$ of order p corresponds to a Singer cycle in $\mathrm{GL}_r(2)$ and by considering the overgroups of such elements (noting that G/K is generated by p-elements and that a point stabilizer has order at most $p(p-1)$) we deduce that $G/K = (C_2)^r{:}C_p$. Since G is the normal closure of P, it follows that K is a 2-group. But since r is an odd prime, we deduce that $K = 1$ is the only possibility. $\square$

We can now classify all the finite groups with $\mathrm{Pr}_p(G) = f(p)$, which yields Theorem B as an immediate corollary.

Theorem 5.2. *Let p be a prime and G a finite group with $G = \mathbf{O}^{p'}(G)$ and $\mathrm{Pr}_p(G) = f(p)$. Let $Q = \mathbf{O}_p(G)$ and let k be a positive integer. Then one of the following holds:*

(i) *G is a p-group with $|G : \mathbf{Z}(G)| = p^2$.*

(ii) *$p \geqslant 5$, Q is abelian and $G = \mathrm{SL}_2(p) \times Q$ or $\mathrm{PSL}_2(p) \times Q$.*

(iii) *$p = 2^r - 1 \geqslant 3$ is a Mersenne prime and $G = (C_2)^r{:}C_{p^k} \times A$, where C_{p^k} acts as a Singer cycle of order p on $(C_2)^r$ and $A \leqslant Q$ is abelian.*

(iv) *$p = 3$ and $G = Q_8{:}C_{3^k} \times A$, where $A \leqslant Q$ is abelian.*

(v) $p = 2$ and $G = C_3{:}C_{2^k} \times A$, where $A \leqslant Q$ is abelian.

Proof. Set $Q = \mathbf{O}_p(G)$. If G/Q is abelian, then G is a p-group and by arguing as in the proof of Lemma 4.2, we see that $\mathrm{Pr}_p(G) = f(p)$ if and only if $|G : \mathbf{Z}(G)| = p^2$.

For the remainder, we may assume G/Q is nonabelian and thus $\mathrm{Pr}_p(G) = \mathrm{Pr}_p(G/Q)$ by Lemma 2.1. This implies that if $x, y \in G_p$ commute modulo Q, then $[x, y] = 1$, which in turn implies that $Q \leqslant \mathbf{Z}(G)$.

First assume that $Q = 1$. Let P be a Sylow p-subgroup of G and let n_p be the number of Sylow p-subgroups of G. As noted in the proof of Theorem A (see (10)), we have

$$\mathrm{Pr}_p(G) \leqslant \frac{1}{|G_p|}\left(1 + \frac{|G_p| - 1}{p}\right).$$

If $|G_p| > p^2$ then

$$\mathrm{Pr}_p(G) \leqslant \frac{p+1}{p^2+1} < \frac{p^2+p-1}{p^3}$$

so we may assume $|G_p| \leqslant p^2$ and thus P is abelian. If $|P| = p^2$, then P is normal and abelian and so $\mathrm{Pr}_p(G) = 1$, a contradiction. So we can reduce further to the case where $|P| = p$ and $n_p = p + 1$. Now apply Lemma 5.1 to conclude.

Finally, let us assume $Q \neq 1$ and note that G/Q is one of the groups described in Lemma 5.1. First assume G/Q is nonsolvable, so $p \geqslant 5$ and G is a central extension of $\mathrm{PSL}_2(p)$ or $\mathrm{SL}_2(p)$ by Q. Here (ii) holds since every p-central extension of one of these groups is split.

Suppose that p is a Mersenne prime with $p \geqslant 7$. Let T be a Sylow 2-subgroup of G. Then T is elementary abelian and $K := TQ = T \times Q$. Thus, T is normal in G and $G = TP$ with P a Sylow p-subgroup of G. Since P/K has order p, P is abelian and so $P = \langle x \rangle \times A$ where A is central and x induces an automorphism of order p on T, whence (iii) holds. If $p = 3$, the same argument applies except that T is either elementary abelian of order 4 or a quaternion group of order 8, leading to (iv).

If $p = 2$, the same argument applies with $T \cong C_3$ a Sylow 3-subgroup of G. This leads to (v). $\qquad\square$

Corollary 5.3. *Let G be a finite group such that $\mathrm{Pr}_p(G) = f(p)$.*

  (i) *If $p = 2$, then G is solvable and $\mathbf{O}^{2'}(G)$ is metabelian.*
  (ii) *If $p = 3$, then $\mathbf{O}^{3'}(G)$ is solvable.*

Finally, we turn to the asymptotic behaviour of $\mathrm{Pr}_p(G)$ with respect to a fixed prime p and a sequence of simple groups of order divisible by p. Set

$$f_p(G) = \max\{f_p(x) : 1 \neq x \in G_p\},$$

where $f_p(x) = |\mathbf{C}_G(x)_p|/|G_p|$. Note that

$$\mathrm{Pr}_p(G) = \frac{1}{|G_p|}\sum_{x \in G_p} f_p(x) \leqslant \frac{1}{|G_p|} + \left(1 - \frac{1}{|G_p|}\right)f_p(G).$$

Proposition 5.4. *Fix a prime p and let $G = A_n$ be the alternating group of degree n. Then $\mathrm{Pr}_p(G) \to 0$ as $n \to \infty$.*

Proof. Since $|G_p|$ tends to infinity with n, it suffices to show that $f_p(G)$ tends to 0. Let $y \in S_n$ be a nontrivial p-element. It is a straightforward exercise to check that for n large enough, $|\mathbf{C}_{S_n}(y)_p|$ is maximal when y is a p-cycle. Let us also observe that S_n contains an equal number of even and odd 2-elements commuting with a given 2-element $z \in S_n$ (this

is because $\mathbf{O}_2(\mathbf{C}_{S_n}(z))$ contains odd permutations when z is nontrivial). Therefore, if n is large enough we have

$$f_p(G) \leqslant \frac{|\mathbf{C}_G(x)_p|}{|G_p|}$$

with $x = (1, \ldots, p) \in S_n$ a p-cycle. For each integer $p < j \leqslant n$, let $y_j \in S_n$ be a p-cycle with an orbit $\{1, \ldots, p-1, j\}$ and let Z_j be the set of p-elements in $\mathbf{C}_{S_n}(y_j)$ that act nontrivially on $\{1, \ldots, p-1, j\}$. Note that the Z_j are pairwise disjoint.

If p is odd, then $|Z_j| = (p-1)!|(A_{n-p})_p|$ and we have $|\mathbf{C}_G(x)_p| = p|Z_j|/(p-1)! \geqslant 2|Z_j|/3$, whence

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} \leqslant \frac{2}{3(n-p)}$$

and this upper bound tends to 0 as n tends to infinity. Similarly, if $p = 2$ then

$$|Z_j| = |(S_{n-2})_2| = |\mathbf{C}_G(x)_2|$$

and the result follows. $\qquad\square$

It is possible to establish an analogous result for simple groups of Lie type, but the details are more complicated and they will be given elsewhere. Here we just sketch some of the main ideas. Fix a prime p. Let G be a simple group of Lie type over $\mathbb{F}_q$ of (untwisted) rank r and assume p divides $|G|$. As before, it suffices to show that $f_p(G) \to 0$ as $|G| \to \infty$.

First suppose that q is increasing. Let $x \in G$ be a nontrivial p-element such that $f_p(x) = f_p(G)$ and note that we may assume x has order p. Let $y \in G$ be a nontrivial p-element and observe that

$$\frac{|y^G \cap \mathbf{C}_G(x)|}{|y^G|}$$

is the probability that x commutes with a random conjugate of y. By the main theorem of [14], this ratio goes to 0 as q tends to infinity. Since this is true for every nontrivial conjugacy of p-elements, and since the number of p-elements in G tends to infinity as q increases (recall that we are assuming p divides $|G|$), we conclude that $f_p(G) \to 0$.

Now suppose q is fixed and r is increasing, so we may assume G is a classical group and we note that p divides $|G|$ if $r \geqslant p$. First assume p divides q, so we are considering unipotent elements. By a result of Steinberg (see [15, Lemma 2.16], for example) we have $|G_p| = q^{\dim X - r}$, where X is the ambient simple algebraic group. By inspecting [15], it is easy to see that $|\mathbf{C}_G(x)_p|$ is maximal when x is a long root element and the result follows easily.

Finally, let us assume that p does not divide q and so x is a semisimple element. This situation is somewhat more complicated, but there are several ways to proceed and much stronger results can be established. For example, [3, Theorem 16] implies that if p is odd and $r > 2$ then the probability that two random elements of order p generate G tends to 1 as $|G|$ tends to infinity (in particular, the probability that two such elements commute tends to 0). With some additional work, this can be extended to p-elements, including the case $p = 2$ (of course, a pair of involutions will not generate G, but the probability that they commute still goes to 0 as r increases). This stronger result implies that $\mathrm{Pr}_p(G) \to 0$ as r tends to infinity.

It is interesting to consider some extensions of this problem. For example, suppose G is a finite group such that $\mathbf{O}_p(G) = 1$ and $G = \mathbf{O}^{p'}(G)$. Do we have $\mathrm{Pr}_p(G) \to 0$ as $|G| \to \infty$?

REFERENCES

[1] Y. Antolin, A. Martino and E. Ventura, *Degree of commutativity of infinite groups* Proc. Amer. Math. Soc. **145** (2017), 479–485.

[2] T.C. Burness and R.M. Guralnick, *Fixed point ratios for finite primitive groups and applications*, submitted (arXiv:2112.03967), 2021.

[3] T.C Burness, S. Gerhardt and R.M. Guralnick, *Topological generation of simple algebraic groups*, submitted (arXiv:2108.06592), 2021.

[4] P.J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[5] J.F. Carlson, E.M. Friedlander and J. Pevtsova, *Vector bundles associated to Lie algebras*, J. Reine Angew. Math. **716** (2016), 147–178.

[6] S. Eberhard, *Commuting probabilities of finite groups*, Bull. London Math. Soc. **47** (2015), 796–808.

[7] J. Fulman and R.M. Guralnick, *Enumeration of commuting pairs in Lie algebras over finite fields*, Ann. Comb. **22** (2018), 295–316.

[8] The GAP group, GAP - *Groups, Algorithms, and Programming*, Version 4.11.1, 2021. http://www.gap-system.org

[9] V. Ginzburg, *Principal nilpotent pairs in a semisimple Lie algebra, I*, Invent. Math. **140** (2000), 511–561.

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

[11] W.H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[12] I.M. Isaacs, *Finite Group Theory*, Graduate Studies in Mathematics, vol. 92, AMS, Providence, RI, 2008.

[13] P. Lescot, *Isoclinism classes and commutativity degree of finite groups*, J. Algebra **177** (1995), 847–869.

[14] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces*, Proc. London Math. Soc. **63** (1991), 266–314.

[15] M.W. Liebeck and G.M. Seitz, *Unipotent and nilpotent classes in simple algebraic groups and Lie algebras*, Mathematical Surveys and Monographs, 180. American Mathematical Society, Providence, RI, 2012.

[16] T. Motzkin and O. Taussky, *Pairs of matrices with property L, II*, Trans. Amer. Math. Soc. **80** (1955), 387–401.

[17] P.M. Neumann, *Two combinatorial problems in group theory*, Bull. London Math. Soc. **21** (1989), 456–458.

[18] A. Premet, *Nilpotent commuting varieties of reductive Lie algebras*, Invent. Math. **154** (2003), 653–683.

[19] R.W. Richardson, *Commuting varieties of semisimple Lie algebras and algebraic groups*, Compositio Math. **38** (1979), 311–327.

[20] M.C.H. Tointon, *Commuting probabilities of infinite groups*, J. London Math. Soc. **101** (2020), 1280–1297.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK

Email address: t.burness@bristol.ac.uk

R.M. Guralnick, Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA

Email address: guralnic@usc.edu

A. Moretó, Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain

Email address: alexander.moreto@uv.es

G. Navarro, Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain

Email address: gabriel@uv.es