Pacific Journal of Mathematics

ON THE INVARIANTS OF FINITE GROUPS ARISING IN A TOPOLOGICAL QUANTUM FIELD THEORY

CHRISTOPHER A. SCHROEDER AND HUNG P. TONG-VIET

Volume 344 No. 1 September 2026

PACIFIC JOURNAL OF MATHEMATICS
Vol. 344, No. 1, 2026
https://doi.org/10.2140/pjm.2026.344.151

ON THE INVARIANTS OF FINITE GROUPS ARISING IN A TOPOLOGICAL QUANTUM FIELD THEORY

CHRISTOPHER A. SCHROEDER AND HUNG P. TONG-VIET

We investigate structural properties of finite groups that are detected by certain group invariants arising from Dijkgraaf–Witten theory, a topological quantum field theory, in one space and one time dimension. In this setting, each finite group G determines a family of numerical invariants associated with closed orientable surfaces, expressed in terms of the degrees of the complex irreducible characters of G. These invariants can be viewed as natural extensions of the commuting probability $d(G)$, which measures the probability that two randomly chosen elements of G commute and has been extensively studied in the literature. By analyzing these higher-genus analogues, we establish new quantitative criteria relating the values of these invariants to key structural features of finite groups, such as commutativity, nilpotency, supersolvability and solvability. Our results generalize several classical theorems concerning the commuting probability, thereby linking ideas from finite group theory and topological quantum field theory.

1. Introduction

There is a long history of using invariants to deduce structural properties of finite groups. These invariants are often constructed by counting objects associated with the group, such as elements, conjugacy classes or irreducible characters. In this paper, we take a different approach. Given the remarkable compatibility between mathematics and physics, it is reasonable to expect that group invariants arising naturally in physics are useful for characterizing group structure. Here, we consider Dijkgraaf–Witten theory, a topological quantum field theory (TQFT), in one space dimension and one time dimension. In short, such a TQFT determines a commutative Frobenius algebra that gives rise to invariants of surfaces. If we assume that this algebra is the center $\boldsymbol{Z}(\mathbb{C}G)$ of the complex group algebra of a finite group G, then the invariant of a genus-h surface takes the form

$$\mathcal{Q}_h(G) = \sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^{2h-2},$$

MSC2020: primary 20C15, 20E45; secondary 20C20, 20D10, 20D15, 20D20.
Keywords: character degree, conjugacy class, invariant, commuting probability, TQFT.

© 2026 MSP (Mathematical Sciences Publishers). Distributed under the Creative Commons Attribution License 4.0 (CC BY). Open Access made possible by subscribing institutions via Subscribe to Open.

where $\mathrm{Irr}(G)$ is the collection of complex irreducible characters of G. Note that $\mathcal{Q}_0(G) = 1/|G|$ and $\mathcal{Q}_1(G) = k(G)$, where $k(G)$ is the number of conjugacy classes of G (equivalently, the number $|\mathrm{Irr}(G)|$ of irreducible complex characters). If we consider the invariants $\mathcal{Q}_h(G)$ as arising from a sequence of increasingly complicated experiments, we might imagine that we first measure $\mathcal{Q}_0(G)$, then $\mathcal{Q}_1(G)$, and so on. With this in mind, it is natural to consider the following scaled invariants, which, as we will show, are very well-behaved:

$$q_h(G) := \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{1}{\chi(1)}\right)^{2h-2}.$$

Now note that $q_0(G) = 1$ and $q_1(G) = k(G)/|G|$, where the latter is the so-called commuting probability $d(G)$, which was first considered by Joseph [20; 21], then by Gustafson [15] and many others. Viewed in this way, the "quantum invariants" $q_h(G)$ are generalizations of the commuting probability, for which the following structure criteria are known:

(a) If $d(G) > d(\mathrm{D}_8) = \frac{5}{8}$, then G is abelian (Gustafson [15]).

(b) If $d(G) > d(\mathrm{S}_3) = \frac{1}{2}$, then G is nilpotent (Lescot [23]).

(c) If $d(G) > d(\mathrm{A}_4) = \frac{1}{3}$, then G is supersolvable (Barry, MacHale, Ní Shé [3]).

(d) If $d(G) > d(\mathrm{A}_5) = \frac{1}{12}$, then G is solvable (Dixon [10]).

In this paper, we investigate which structural properties of finite groups are witnessed by the invariants $q_h(G)$. Our main results establish broad generalizations of the classical structure criteria above to arbitrary genus $h \geq 1$. The bounds in our first theorem are clearly best possible.

Theorem 1.1. *Let G be a finite group, and let h be a positive integer.*

(a) *If $q_h(G) > q_h(\mathrm{D}_8)$, then G is abelian.*

(b) *If $q_h(G) > q_h(\mathrm{S}_3)$, then G is nilpotent.*

(c) *If $q_h(G) > q_h(\mathrm{A}_4)$, then G is supersolvable.*

(d) *If $q_h(G) > q_h(\mathrm{A}_5)$, then G is solvable.*

Guralnick and Robinson showed in [14, Lemma 2(x)] that if p is a prime and $d(G) > 1/p$, then G has a normal Sylow p-subgroup. Our next result generalizes this p-closed criterion to all genera.

Theorem 1.2. *Let G be a finite group, let p be a prime, and let h be a positive integer. If $q_h(G) > \gamma(h, p)$, where $\gamma(h, p) = (1 + 1/p^{2h-1})/(p+1)$, then G has a normal Sylow p-subgroup.*

This criterion is the best possible. For example, if $p = 2^f - 1$ is a Mersenne prime, then the Frobenius group $G = (C_2)^f \rtimes C_p$ satisfies $q_h(G) = \gamma(h, p)$ and does not have a normal Sylow p-subgroup. Although Theorem 1.2 implies Theorem 1.1(b) and much of part (c), we will in fact use the latter to prove this p-closed criterion.

Given a prime p, it is also natural to consider a p-local version of the invariants $q_h(G)$ by summing over irreducible p-Brauer characters instead of irreducible complex characters. We define

$$q_{h,p'}(G) = \frac{1}{|G|_{p'}} \sum_{\varphi \in \mathrm{IBr}(G)} \frac{1}{\varphi(1)^{2h-2}}.$$

Note that $q_{1,p'}(G) = k_{p'}(G)/|G|_{p'}$, where $k_{p'}(G)$ is the number of irreducible p-Brauer characters (equivalently, the number of p-regular conjugacy classes). This invariant is denoted by $d_{p'}(G)$ in the literature, and it was shown in [33, Theorem 1.1] that if p is an odd prime and $d_{p'}(G) > 1/(p-1)$, then G is p-solvable. This result is best possible for $p > 3$ since $d_{p'}(\mathrm{PSL}_2(p)) = 1/(p-1)$. Our next theorem extends this result to all values of the genus.

Theorem 1.3. *Let G be a finite group, h a positive integer, and p an odd prime. If $q_{h,p'}(G) > \alpha(h, p)/(p-1)$, where $\alpha(h, p) = (2^{2h-2} + \sqrt{p-1})/(2^{2h-2}\sqrt{p-1})$, then G is p-solvable.*

Note that $\alpha(h, p) < 1$ when both $h > 1$ and $p > 2$. Theorem 1.3 is not best possible for $h = 1$, in which case, again, the best bound is $1/(p-1)$ from [33]. We suspect, but have not proved, that the result is also not best possible for $h > 1$. Our proof relies on a lower bound for $k_{p'}(G)$ when G is not p-solvable. At the time of writing, the best known bound is $k_{p'}(G) > \sqrt{p-1}$, which was proved by Hung and Maróti in [30]. An improvement in this bound would lead directly to an improvement in Theorem 1.3.

Finally, it is natural to consider an invariant $\tilde{q}_h(G)$ dual to $q_h(G)$ by summing over the sizes of the conjugacy classes $C \in \mathrm{Cl}(G)$ of a finite group G, where $\mathrm{Cl}(G)$ denotes the set of all conjugacy classes of G. We define the invariant

$$\tilde{q}_h(G) = \frac{1}{|G|} \sum_{C \in \mathrm{Cl}(G)} \frac{1}{|C|^{h-1}}.$$

Note that $\tilde{q}_0(G) = 1$ and $\tilde{q}_1(G) = d(G)$. From the definition, $\tilde{q}_h(G) \geq \tilde{q}_{h+1}(G)$ for all integers $h \geq 0$. We again prove generalizations of the structure criteria witnessed by the commuting probability to all values of the genus h.

Theorem 1.4. *Let G be a finite group, and let h be a positive integer.*

(a) *If $\tilde{q}_h(G) > \tilde{q}_h(\mathrm{D}_8)$, then G is abelian.*

(b) *If $\tilde{q}_h(G) > \tilde{q}_h(\mathrm{S}_3)$, then G is nilpotent.*

(c) *If* $\tilde{q}_h(G) > \tilde{q}_h(\mathrm{A}_4)$, *then* G *is supersolvable.*

(d) *If* $\tilde{q}_h(G) > \tilde{q}_h(\mathrm{A}_5)$, *then* G *is solvable.*

We also prove a dual criterion for the existence of a normal Sylow p-subgroup.

Theorem 1.5. *Let* G *be a finite group, let* p *be a prime and let* h *be a positive integer. If* $\tilde{q}_h(G) > \tilde{\gamma}(h, p)$, *where* $\tilde{\gamma}(h, p) = (1+1/p^{h-1}+(p-1)/(p+1)^{h-1})/(p(p+1))$, *then* G *has a normal Sylow* p*-subgroup.*

This criterion is best possible, as again the Frobenius group $G = (C_2)^f \rtimes C_p$ with $p = 2^f - 1$ a Mersenne prime satisfies $\tilde{q}_h(G) = \tilde{\gamma}(h, p)$.

We conclude this Introduction with some remarks.

Remark 1.6. The content of Theorems 1.1(a)–(d) and 1.4(a)–(d) is that the group-theoretic properties of commutativity, nilpotency, supersolvability and solvability are witnessed by the value of $q_h(G)$ or $\tilde{q}_h(G)$ for a particular "minimal" group G for all $h \geq 1$. For example, Theorem 1.1(d) says that solvability is witnessed by A_5 for all values of the genus h. Of course, our theorems would have trivial content if the invariants preserved the ordering of finite groups for all h; that is, if for all finite groups G and H it were true that $q_h(G) > q_h(H)$ for some $h > 1$ implied that $d(G) > d(H)$, then all our theorems would follow trivially from the corresponding result for $d(G)$. But this is not the case. For example, if $G = \mathrm{S}_6$ and $H = \mathrm{PGL}_2(9)$, then $q_h(G) > q_h(H)$ and $\tilde{q}_h(G) > \tilde{q}_h(H)$ for all $h > 1$, but $d(G) = d(H)$.

Our next example illustrates a general phenomenon: Notice that for a finite group G, the invariant $q_h(G)$ approaches $1/|G'|$ as h approaches infinity, where G' denotes the derived subgroup of G. Therefore, if $d(G) > d(H)$ for some finite groups G and H, but $1/|G'| < 1/|H'|$, then there must exist some positive integer N such that $q_h(G) < q_h(H)$ for all $h > N$. For example, let $G = \mathrm{A}_5$, and let H be an extraspecial p-group of order p^3 for the prime $p = 59$. Then $d(G) = \frac{1}{12}$ and $1/|G'| = \frac{1}{60}$, while $d(H) = (p^2+p-1)/p^3$ and $1/|H'| = 1/p$. Then $d(G) > d(H)$, while $1/|G'| < 1/|H'|$, and the preceding observation applies. In fact, a calculation shows that $q_h(G) > q_h(H)$ for $h = 1, 2, 3$, while $q_h(G) < q_h(H)$ for $h \geq 4$.

For the dual invariant, take $G = \mathrm{A}_5$ and let H be an extraspecial p-group of order 11^3. Then $d(G) < d(H)$ yet $\tilde{q}_h(G) > \tilde{q}_h(H)$ for all integers $h \geq 2$.

Remark 1.7. By examining our proofs, it is easy to see that our results hold not only when the exponent in $q_h(G)$ is the negative of the Euler characteristic $2-2h$ of a genus-h surface, but for any real number $s \geq 1$. In this way, our results are related to the so-called zeta function $\zeta_G(s) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s}$ of a finite group G, which was used by Liebeck and Shalev to prove various results on Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random walks and representation varieties [24; 25; 26]. We also note that the zeta function for conjugacy class sizes was studied in [25] for finite groups of Lie type, with applications to base

sizes of primitive permutation groups. Since our motivation stems from topological quantum field theories, we have stated and proved our results in this special case.

Remark 1.8. It is known that $d(G) \leq d(N)d(G/N)$ when $N \trianglelefteq G$ [14, Lemma 2(ii)]. Our proofs would be simplified if $q_h(G) \leq q_h(N)q_h(G/N)$ for all h. We have not been able to prove this statement, however. If it were true, then it must of course be true for $N = \mathbf{Z}(G)$. But this already seems to be a hard question about projective character degrees: letting $Z = \mathbf{Z}(G)$,

$$q_h(G) = \frac{1}{|G/Z||Z|} \sum_{\lambda \in \mathrm{Irr}(Z)} \sum_{\chi \in \mathrm{Irr}(G|\lambda)} \frac{1}{\chi(1)^{2h-2}}.$$

So to prove that $q_h(G) \leq q_h(G/Z)$, it would suffice to show, for example, that

$$\sum_{\chi \in \mathrm{Irr}(G|\lambda)} \frac{1}{\chi(1)^{2h-2}} \leq \sum_{\chi \in \mathrm{Irr}(G/Z)} \frac{1}{\chi(1)^{2h-2}};$$

that is, we want to show the sum over projective character degrees of G/Z is less than the sum over ordinary character degrees. We know that they are fewer in number: $|\mathrm{Irr}(G|\lambda)| \leq k(G/Z)$ as a consequence of Gallagher's result on "θ-good" conjugacy classes (see Theorem 1.19 and Corollary 1.23 in [19]).

Remark 1.9. The ratios $|G|/\chi(1)$ for $\chi \in \mathrm{Irr}(G)$ are the character degree quotients originally considered by Chillag and Herzog in [5]. In order to be compatible with group quotients, many authors have considered instead the character codegrees $[G : \ker(\chi)]/\chi(1)$. Note that if G is simple, then the character codegrees and character degree quotients of nontrivial characters coincide.

Remark 1.10. Our "dual invariant" $\tilde{q}_h(G)$ also has a physical interpretation in the context of lattice Hamiltonians for Yang–Mills gauge theories with finite gauge group [27]. These theories are motivated by the potential for quantum simulation of gauge theories.

Outline. Our paper is structured as follows. As our methods are purely group-theoretic, we defer an introduction to Dijkgraaf–Witten theory to Section 6. In Section 2, we make some remarks and collect some known facts that will be needed in the rest of the paper. In Section 3, we prove Theorems 1.1(a)–(d) and Theorem 1.3. In Section 4, we prove Theorem 1.2. In Section 5 we prove Theorems 1.4(a)–(d) and Theorem 1.5. Only the proof of Theorem 1.3 requires us to cite results that depend on the classification of finite simple groups. We do use Brauer's $k(GV)$-theorem in the proof of Theorem 1.1(c), but there the group G is solvable, and the proof in that case does not rely on the classification. All groups considered in this paper are assumed to be finite.

Notation. Our notation is standard. We follow [18] for finite group theory and [17] for the character theory of finite groups. Let n be a positive integer. We denote by A_n and S_n the alternating and symmetric groups of degree n, respectively. The dihedral group of order $2n$ is denoted by D_{2n}, and a cyclic group of order n by C_n. The special linear, projective general linear, and projective special linear groups of degree n over the finite field of size q are denoted by $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$, respectively. For a finite group G and a subset $X \subseteq G$, we write $\boldsymbol{C}_G(X)$ and $\boldsymbol{N}_G(X)$ for the centralizer and normalizer of X in G, respectively. The derived subgroup of G is denoted by G', and $\boldsymbol{Z}(G)$ denotes the center of G. The set of complex irreducible characters of G is denoted by $\mathrm{Irr}(G)$, and we let $k(G)$ be the number of conjugacy classes of G. We will repeatedly use that $k(G) = |\mathrm{Irr}(G)|$. We denote by $\mathrm{Cl}(G)$ the set of all conjugacy classes of G. If $N \leq G$ and $\lambda \in \mathrm{Irr}(N)$, then $\mathrm{Irr}(G|\lambda)$ denotes the set of all irreducible characters of G lying above λ. If p is a prime, the set of irreducible p-Brauer characters of G is denoted by $\mathrm{IBr}(G)$. All other notation is standard.

2. Preliminaries

As noted in the introduction, the invariants $q_h(G)$ can be viewed as generalizations of the commuting probability $d(G) = k(G)/|G|$ first considered by Joseph [20; 21], then by Gustafson [15]. Our proofs are based on the extensive literature on this invariant. Our first lemma collects some of the facts that are already known.

Lemma 2.1. *Let G be a finite group.*

(a) *We have $q_1(G) = d(G)$ and $q_h(G) \geq q_{h+1}(G)$ for all $h \geq 0$.*

(b) *If G is perfect and $d(G) > \frac{1}{20}$, then $G \cong \mathrm{A}_5$ or $G \cong \mathrm{SL}_2(5)$.*

(c) *If p is a prime such that a Sylow p-subgroup of G is not normal, then $d(G) \leq 1/p$.*

(d) *If G is a nonabelian p-group for some prime p, then $d(G) \leq 1/p + 1/p^2$.*

(e) *If G is nilpotent with a nonabelian Sylow p-subgroup for some prime p, then $d(G) < 1/p$ or $|G'| = p$.*

(f) *Whenever $N \trianglelefteq G$, we have $d(G) \leq d(G/N)d(N)$. In particular, we always have $d(G) \leq d(G/N)$.*

Proof. Part (a) follows from the definition using $|\mathrm{Irr}(G)| = k(G)$ and $\chi(1) \geq 1$ for all $\chi \in \mathrm{Irr}(G)$. Part (b) is [6, Proposition 1.6]. Part (c) is [14, Lemma 2(x)]. Part (d) is [14, Lemma 2(viii)]. Part (e) is [14, Lemma 2(ix)] and part (f) is [14, Lemma 2(ii)]. □

Our next lemma shows that $q_h(G)$ is monotone with respect to subgroups $H \leq G$ for all $h \geq 1$.

Lemma 2.2. *Let G be a finite group, and let h be any positive integer. If $H \leq G$, then $q_h(H) \geq q_h(G)$.*

Proof. We have

$$q_h(G) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{1}{\chi(1)^{2h-2}} \leq \frac{1}{|G|} \sum_{\psi \in \mathrm{Irr}(H)} \sum_{\chi \in \mathrm{Irr}(G|\psi)} \frac{1}{\chi(1)^{2h-2}}$$
$$\leq \frac{1}{|G|} \sum_{\psi \in \mathrm{Irr}(H)} \frac{[G:H]}{\psi(1)^{2h-2}} = \frac{1}{|H|} \sum_{\psi \in \mathrm{Irr}(H)} \frac{1}{\psi(1)^{2h-2}} = q_h(H).$$

The first inequality follows because we have enumerated all the $\chi \in \mathrm{Irr}(G)$ (possibly multiple times). The characters in $\mathrm{Irr}(G|\psi)$ are the constituents of ψ^G by Frobenius reciprocity, and $\psi^G(1) = [G:H]\psi(1)$. The sum $\sum_{\chi \in \mathrm{Irr}(G|\psi)} 1/\chi(1)^{2h-2}$ is as large as possible when all the degrees are as small as possible and $|\mathrm{Irr}(G|\psi)|$ is as large as possible. Since ψ lies under χ, $\chi(1) \geq \psi(1)$. If equality holds for all $\chi \in \mathrm{Irr}(G|\psi)$, then $\chi(1)$ is as small as possible and $|\mathrm{Irr}(G|\psi)| = [G:H]$ is as large as possible, which yields the second inequality. □

The next result slightly improves [14, Lemma 2(x)] for nonabelian simple groups.

Lemma 2.3. *Let G be a finite nonabelian simple group, and let p be a prime dividing $|G|$. Then $d(G) \leq 1/(p+1)$.*

Proof. Suppose for a contradiction that $d(G) > 1/(p+1)$. Since G is a finite nonabelian simple group, by [10] we know that $d(G) \leq \frac{1}{12}$. Hence $1/(p+1) < \frac{1}{12}$, which implies that $p \geq 13$ as p is a prime. Let P be a Sylow p-subgroup of G. Suppose that $[G : \boldsymbol{N}_G(P)] \leq p$. Since $[G : \boldsymbol{N}_G(P)]$ is coprime to p, we deduce that $[G : \boldsymbol{N}_G(P)] \leq p-1$. Since G is nonabelian simple, the core of $\boldsymbol{N}_G(P)$ in G is trivial, so G embeds into S_{p-1}, the symmetric group of degree $p-1$. But then $|G|$ is not divisible by p, which is a contradiction. Thus $[G : \boldsymbol{N}_G(P)] \geq p+1$. By Burnside's normal p-complement theorem [16, Theorem IV.2.6], we have $\boldsymbol{N}_G(P) \neq \boldsymbol{C}_G(P)$ and hence $|\boldsymbol{N}_G(P)| \geq 2p$. Combining these two inequalities, we obtain

$$|G| = [G : \boldsymbol{N}_G(P)] \cdot |\boldsymbol{N}_G(P)| \geq 2p(p+1).$$

Let d be the minimal degree of a nontrivial complex irreducible character of G. By [12, Theorem 1], we have $d \geq (p-1)/2$. By [14, Lemma 2(vi)], noting that $G' = G$, we have

$$d(G) < \frac{1}{d^2} + \Big(1 - \frac{1}{d^2}\Big)\frac{1}{|G'|} \leq \frac{4}{(p-1)^2} + \frac{1}{2p(p+1)}.$$

Since $d(G) > 1/(p+1)$, it follows that

$$\frac{1}{p+1} < \frac{4}{(p-1)^2} + \frac{1}{2p(p+1)}.$$

Simplifying this inequality gives $2p^3 - 13p^2 - 4p < 1$, i.e., $2p^3 - 13p^2 - 4p \leq 0$. This can be rewritten as $(2p-13)p \leq 4$ which is impossible for $p \geq 13$. Hence, the assumption $d(G) > 1/(p+1)$ leads to a contradiction, and the lemma follows. □

We also need the following easy lemma due to Lescot [23], whose proof we include for completeness.

Lemma 2.4. *If $d(G) > \frac{1}{4}$, then*

$$|G'| \leq \frac{3}{4d(G)-1}.$$

Proof. Since $|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2$ and the number of linear characters is $[G : G']$, we have

$$|G| - [G : G'] = \sum_{\chi(1)>1} \chi(1)^2 \geq 4(k(G) - [G : G']).$$

Dividing both sides by $|G|$ and rearranging yields the claim. □

Remark 2.5. We will repeatedly use the fact that if the smallest degree of a nonlinear irreducible character of G is n, then $d(G)$ and $q_h(G)$ can be bounded in terms of n and $|G'|$, with equality if all nonlinear characters have degree n:

$$q_h(G) \leq \frac{1}{|G|}\Big([G : G'] + \frac{k(G) - [G : G']}{n^{2h-2}}\Big) = \frac{1}{|G'|}\Big(1 - \frac{1}{n^{2h-2}}\Big) + \frac{d(G)}{n^{2h-2}}.$$

We will derive similar inequalities for $\tilde{q}_h(G)$ in the course of our proofs.

We now turn to the properties of a finite group G that are witnessed by the dual invariant $\tilde{q}_h(G) = 1/|G| \sum_{C \in \mathrm{Cl}(G)} 1/|C|^{h-1}$, where $\mathrm{Cl}(G)$ is the collection of conjugacy classes of G. Whereas we showed that $q_h(G)$ is monotone with respect to subgroups in Lemma 2.2, we now prove, in a nicely dual result, that $\tilde{q}_h(G)$ is monotone with respect to quotients.

Lemma 2.6. *Let G be a finite group, let $N \trianglelefteq G$, and let h be any positive integer. Then $\tilde{q}_h(G) \leq \tilde{q}_h(G/N)$.*

Proof. Let $\overline{G} = G/N$ and use the bar notation. Let $\pi : G \to G/N$ denote the canonical homomorphism. Given a conjugacy class $D \in \mathrm{Cl}(\overline{G})$, the preimage $\pi^{-1}(D) \subseteq G$ is closed under conjugation, so it is a union of conjugacy classes C_i of G, say

$$\pi^{-1}(D) = C_1 \cup C_2 \cup \cdots \cup C_k.$$

Let $S(D) = \{C_1, \ldots, C_k\}$. Choosing some $x_i \in C_i$ for $i = 1, \ldots, k$, we have $|C_i| = [G : \boldsymbol{C}_G(x_i)]$. Similarly, $|D| = [\overline{G} : \boldsymbol{C}_{\overline{G}}(\bar{x}_i)]$ for all $i = 1, \ldots, k$ since $\pi(x_i) \in D$. Writing $\boldsymbol{C}_{\overline{G}}(\bar{x}_i) = H/N$ for some subgroup $H \leq G$, we have $|D| = [G : H]$. Note

that $\boldsymbol{C}_G(x_i) \leq H$. Therefore,

$$|C_i| = [G : \boldsymbol{C}_G(x_i)] = [G : H][H : \boldsymbol{C}_G(x_i)] \geq |D|.$$

Furthermore, $|\pi^{-1}(D)| = |D||N|$ since π is an $|N|$-to-1 map. Since $|C_i| \geq |D|$, we have

$$|N||D| = \sum_{i=1}^{k} |C_i| \geq k|D|,$$

and so $k \leq |N|$.

Each conjugacy class of G lies in the preimage of exactly one conjugacy class of $\overline{G}$. Now we calculate

$$\tilde{q}_h(G) = \frac{1}{|G|} \sum_{D \in \mathrm{Cl}(\overline{G})} \sum_{C \in S(D)} \frac{1}{|C|^{h-1}} \leq \frac{1}{|G|} \sum_{D \in \mathrm{Cl}(\overline{G})} \frac{|N|}{|D|^{h-1}} = \tilde{q}_h(\overline{G}),$$

which is what we wanted to show. □

The following easy lemma is our main tool for proving the structure criteria in Theorem 1.4.

Lemma 2.7. *Let G be a finite group, and let n be the smallest size of the noncentral conjugacy classes of G. Let $h \geq 2$ be an integer, and assume that G is not abelian. Let N be an integer such that $d(G)/\tilde{q}_h(G) \leq N$. Then either*

(1) $n^{h-1} \leq N$, *or*

(2) $[G : \mathbf{Z}(G)] \leq \dfrac{N}{\tilde{q}_h(G)(N+1) - d(G)} \leq \dfrac{d(G)}{\tilde{q}_h(G)^2}$.

Proof. Since G is not abelian, $\tilde{q}_h(G) < d(G)$. If $n^{h-1} \leq N$, then part (1) is satisfied. Assume that $n^{h-1} > N$. So $n^{h-1} > N \geq d(G)/\tilde{q}_h(G)$. It follows that $\tilde{q}_h(G)n^{h-1} - d(G) > 0$ and

$$n^{h-1} \geq N + 1 \geq d(G)/\tilde{q}_h(G) + 1.$$

We have

$$\tilde{q}_h(G) \leq \frac{1}{|G|}\Big(|\mathbf{Z}(G)| + \frac{k(G) - |\mathbf{Z}(G)|}{n^{h-1}}\Big).$$

Using that $d(G) = k(G)/|G|$ and rearranging, we find that

$$[G : \mathbf{Z}(G)] \leq \frac{n^{h-1} - 1}{\tilde{q}_h(G)n^{h-1} - d(G)}.$$

Since the right-hand side is a decreasing function of n^{h-1}, we have

$$[G : \mathbf{Z}(G)] \leq \frac{N}{\tilde{q}_h(G)(N+1) - d(G)} \leq \frac{d(G)}{\tilde{q}_h(G)^2},$$

as claimed. □

3. Commutativity, nilpotency, supersolvability and solvability criteria

In this section, we prove the four claims of Theorem 1.1.

Proof of the commutativity criterion, Theorem 1.1(a). Suppose for a contradiction that G is a counterexample to the claim with minimal order. The degrees of the complex irreducible characters of D_8 are 1, 1, 1, 1 and 2. By a result due to Gustafson [15], $d(G) \leq \frac{5}{8}$ since G is nonabelian. Altogether, we have

$$\tfrac{1}{2} < \tfrac{1}{2}(1+2^{-2h}) = q_h(\mathrm{D}_8) < q_h(G) \leq d(G) \leq \tfrac{5}{8}.$$

We first claim that G is nilpotent; that is, all Sylow subgroups of G are normal in G. By Lemma 2.1(c), if a Sylow p-subgroup of G is not normal for some prime p, then $d(G) \leq 1/p$. But then $\frac{1}{2} < \frac{1}{p}$, which is impossible.

Next, we claim that all Sylow subgroups of odd order are abelian. Note that if $G = A \times B$, then $q_h(G) = q_h(A)q_h(B)$. Since G is nilpotent by the last paragraph, this means that $q_h(G) = \prod q_h(P)$, where the product runs over the set of Sylow subgroups of G. In particular, $q_h(P) > \frac{1}{2}$ for every Sylow subgroup P. However, by Lemma 2.1(d), if P is nonabelian then $d(P) < 1/p + 1/p^2$. Thus, $1/p + 1/p^2 > \frac{1}{2}$. This inequality only holds if $p = 2$, so all Sylow subgroups of odd order are abelian.

We may now assume that G is a nonabelian 2-group such that $q_h(G) > q_h(\mathrm{D}_8)$. Now, by Lemma 2.1(e), either $d(G) < \frac{1}{2}$ or $|G'| = 2$. We have $d(G) > \frac{1}{2}$ by the first paragraph, so $|G'| = 2$. Therefore,

$$q_h(\mathrm{D}_8) < q_h(G) \leq \tfrac{1}{2}(1 - 2^{-(2h-2)}) + d(G) \cdot 2^{-(2h-2)},$$

where we used that nonlinear irreducible characters of G have degree at least 2 and the observation in Remark 2.5. Thus,

$$d(G) > \tfrac{1}{2} + 2^{2h-2}\big(q_h(\mathrm{D}_8) - \tfrac{1}{2}\big) = \tfrac{1}{2} + 2^{2h-2} \cdot 2^{-(2h+1)} = \tfrac{1}{2} + \tfrac{1}{8} = \tfrac{5}{8}.$$

This contradicts the bound $d(G) \leq \frac{5}{8}$ from the first paragraph, proving the result. □

Next, we prove Theorem 1.1(b). We will show that a minimal counterexample is a *minimal nonnilpotent group*; that is, a nonnilpotent group whose proper subgroups are nilpotent. The structure of such groups, which we summarize in the following lemma, is well understood:

Lemma 3.1 [16, Theorem III.5.2]. *Suppose G is a minimal nonnilpotent group. Then $G \cong Q \rtimes P$, where Q is a Sylow q-subgroup for some prime q, while P is a cyclic Sylow p-subgroup for some prime p and $\Phi(P) \leq \mathbf{Z}(G)$.*

Proof of the nilpotency criterion, Theorem 1.1(b). Suppose for a contradiction that G is a counterexample to the claim with minimal order. The irreducible character degrees of S_3 are 1, 1 and 2. Since G is not nilpotent, it contains a nonnormal Sylow p-subgroup for some prime p dividing $|G|$. This means $d(G) \leq 1/p \leq \frac{1}{2}$ by

Lemma 2.1(c). Altogether, we have

$$\tfrac{1}{3} < \tfrac{1}{3}(1+2^{-(2h-1)}) = q_h(\mathrm{S}_3) < q_h(G) \le d(G) \le \tfrac{1}{p} \le \tfrac{1}{2}.$$

This means that the only nonnormal Sylow subgroup is the Sylow 2-subgroup.

Now, by the monotonicity of Lemma 2.2, every proper subgroup of G is nilpotent, so G is a minimal nonnilpotent group by induction and has the structure described in Lemma 3.1. We know that $p = 2$ by the last paragraph, and $q \neq 2$ since G is not nilpotent. As P is cyclic, $[P : \Phi(P)] = 2$.

Consider the structure of G': As G is not nilpotent, of course $G' > 1$. As $d(G) > \frac{1}{3}$, we have $|G'| < 9$ by Lemma 2.4. Since $G/Q \cong P$ is abelian, $G' \le Q$. So $q = 3$, 5 or 7 and G' is cyclic of prime order q. Since $G' \trianglelefteq Q$, we have $G' \cap \mathbf{Z}(Q) > 1$, so $G' \le \mathbf{Z}(Q)$ as G' has prime order. So Q centralizes G'. If $G' < Q$, then $G'P < G$ is nilpotent by induction on the group order, so P centralizes G', as well. But then $G' \le \mathbf{Z}(G)$ and G is nilpotent, a contradiction. So we have that $G' = Q$ is cyclic of order 3, 5 or 7.

Since $\Phi(P) \le \mathbf{Z}(G)$, the product $Q\Phi(P)$ is abelian of index 2 in G. So every nonlinear irreducible character of G has degree 2 since it is a constituent of a character induced from a (necessarily linear) character of $Q\Phi(P)$. As G has $[G : G'] = |P|$ linear characters, the remaining nonlinear characters must be $\frac{1}{4}(|Q| - 1)|P|$ in number since the resulting sum of squared degrees is $|P| + \frac{1}{4}(|Q|-1)|P| \cdot 2^2 = |G|$. Therefore,

$$q_h(G) = \frac{1}{|G|}\left(|P| + \frac{(|Q|-1)|P|}{4}\frac{1}{2^{2h-2}}\right) = \frac{1}{q}\left(1+\frac{q-1}{2^{2h}}\right) > \frac{1}{3}\left(1+\frac{2}{2^{2h}}\right) = q_h(\mathrm{S}_3).$$

But the inequality implies that $q < 3$. We have reached our final contradiction and proved the claim. □

To prove the supersolvability criterion of Theorem 1.1(c), we will show that a minimal counterexample is a *minimal nonsupersolvable group*; that is, a nonsupersolvable group whose proper subgroups are supersolvable. The structure of such groups was determined by Doerk [11], and can be read off from [2, Theorem 12] and [16, Chapter VI, Exercise 16]. We summarize the results we will initially need:

Lemma 3.2 [11]. *Suppose G is a minimal nonsupersolvable group. Then G has exactly one normal Sylow p-subgroup P and a complement Q such that $|Q|$ is divisible by at most two distinct primes. Furthermore, $P/\Phi(P)$ is a minimal normal subgroup of $G/\Phi(P)$ and is not cyclic, and $Q \cap \mathbf{C}_G(P/\Phi(P)) = Q \cap \Phi(G) = \Phi(Q) \cap \Phi(G)$.*

Proof of the supersolvability criterion, Theorem 1.1(c). Let G be a counterexample to the theorem with minimal order. The irreducible character degrees of A_4 are

1, 1, 1 and 3. Since G is not supersolvable, $d(G) \leq \frac{1}{3}$ by [3]. Altogether, we have

$$\tfrac{1}{4} < \tfrac{1}{4}(1 + 3^{-(2h-1)}) = q_h(\mathrm{A}_4) < q_h(G) \leq d(G) \leq \tfrac{1}{3}.$$

Then by Lemma 2.2, for every proper subgroup H of G, we have $q_h(H) \geq q_h(G) > q_h(\mathrm{A}_4)$ and hence by the minimality of $|G|$, H is supersolvable. As G is not supersolvable, G is a minimal nonsupersolvable group and has the structure described in Lemma 3.2. Now we work in $\overline{G} = G/\Phi(G)$, which is again minimal nonsupersolvable, since if $\overline{G}$ is supersolvable then G is supersolvable by [16, Theorem VI.8.5]. Recall that $\Phi(P) \leq \Phi(G)$ by [16, Lemma III.3.3]; since $P/\Phi(P)$ is minimal normal in $G/\Phi(P)$ by Lemma 3.2, $\Phi(P) = P \cap \Phi(G)$. Therefore, $\overline{P}$ is a minimal normal, elementary abelian, noncyclic subgroup of $\overline{G}$, where $\overline{G} = \overline{P}\,\overline{Q}$ and $\overline{Q}$ acts coprimely, faithfully and irreducibly on $\overline{P}$. By Brauer's $k(GV)$-theorem [13, Theorem], we know that $k(\overline{G}) = k(\overline{P} \rtimes \overline{Q}) \leq |\overline{P}|$. Using this and Lemma 2.1(f), we have

$$\frac{1}{4} < d(G) \leq d(\overline{G}) \leq \frac{1}{|\overline{Q}|},$$

and so $|\overline{Q}| \leq 3$. Since $\overline{Q}$ has prime order and $\overline{P}$ is an irreducible $\overline{Q}$-module, this means $\boldsymbol{C}_{\overline{G}}(\bar{x}) \leq \overline{P}$ for all nontrivial $\bar{x} \in \overline{P}$, so $\overline{G}$ is a Frobenius group. Now, if $\overline{Q} = \langle \bar{t} \rangle$ has order 2, then $\bar{t}$ acts as inversion on $\overline{P}$ (see [17, Lemma 7.21] and its proof). So every subgroup $\langle \bar{x} \rangle \leq \overline{P}$ is fixed by $\overline{Q}$, which means $\overline{P} = \langle \bar{x} \rangle$ is cyclic as it is an irreducible $\overline{Q}$-module. This contradiction implies that $|\overline{Q}| = 3$.

Now we count the characters of the Frobenius group $\overline{G}$: Since $\overline{G}' = \overline{P}$, there are $[\overline{G} : \overline{G}'] = |\overline{Q}|$ linear characters, and each of the nonlinear irreducible characters of $\overline{G}$ is induced from an irreducible character of $\overline{P}$ lying in one of the $(|\overline{P}| - 1)/|\overline{Q}|$ orbits under $\overline{Q}$. So

$$\frac{1}{4} < d(\overline{G}) = \frac{1}{|\overline{P}||\overline{Q}|}\left(|\overline{Q}| + \frac{|\overline{P}| - 1}{|\overline{Q}|}\right).$$

Rearranging and using that $|\overline{Q}| = 3$, we find that $p^2 \leq |\overline{P}| < \frac{32}{5} < 7$. Therefore, $|\overline{P}| = 4$ and so $\overline{G} \cong \mathrm{A}_4$. In particular, P is a 2-group.

Let r be a prime divisor of $|G|$, and let R be a Sylow r-subgroup of G. If R is not normal in G, then $d(G) \leq \frac{1}{r}$. Since $d(G) \geq q_h(G) > q_h(\mathrm{A}_4) > \frac{1}{4}$ we deduce that $\frac{1}{r} > \frac{1}{4}$ which forces $r < 4$ and hence $r \in \{2, 3\}$. In particular, Q is a π-group, where $\pi \subseteq \{2, 3\}$. Since we showed that the Sylow p-subgroup P is a 2-group, Q must then be a 3-group. Now, since $\Phi(Q) \geq \Phi(Q) \cap \Phi(G) = Q \cap \boldsymbol{C}_G(P/\Phi(P))$ and $\overline{Q} \cong Q/(\Phi(Q) \cap \Phi(G))$ is cyclic of order 3, we have $\Phi(Q) = \Phi(Q) \cap \Phi(G)$. So Q is itself cyclic by Burnside's basis theorem [16, Theorem III.3.15]. We have shown that $G = PQ$, where P is a 2-group and Q is a cyclic 3-group, and $\overline{G} = G/\Phi(G) \cong \mathrm{A}_4$.

Now we turn to the more precise classification of minimal nonsupersolvable groups in [2, Theorem 10]. Since Q is cyclic of 3-power order and $p=2$, inspecting the list of possibilities in [2, Theorem 9] shows that only Types 2 and 3 are possible. We inspect each of these in turn and derive contradictions:

Type 2: *$Q=\langle z\rangle$ is cyclic, P is an irreducible Q-module over the field of p elements with kernel $\langle z^q\rangle$ in Q.*

Since $P \trianglelefteq G$ is an irreducible Q-module, P has no Q-invariant nontrivial proper subgroup. In particular, $P\cap\Phi(G)=1$ and so $\bar{P}\cong P$ is elementary abelian of order 4 by what we showed above. The kernel $K=\langle z^3\rangle$ is central in G and has index 3 in Q, so $|Q|=3|K|$ and $|G|=12|K|$. We have $[G:G']=[G:P]=|Q|=3|K|$, and the nonlinear irreducible characters of G are induced from characters $\psi_1\times\psi_2\in\mathrm{Irr}(P\times K)$ with $\psi_1\neq 1$, which split into $|K|$ orbits under G. Thus, each of these $|K|$ nonlinear characters of G has degree 3. So

$$q_h(G)=\frac{1}{12|K|}\left(3|K|+\frac{|K|}{3^{2h-2}}\right)=\frac{1}{4}\left(1+\frac{1}{3^{2h-1}}\right)=q_h(\mathrm{A}_4),$$

which is a contradiction. Note that if $K=1$, then $G\cong\mathrm{A}_4$.

Type 3: *P is a nonabelian special p-group of rank $2m$, the order of p modulo q being $2m$, $Q=\langle z\rangle$ is cyclic, z induces an automorphism on P such that $P/\Phi(P)$ is a faithful and irreducible Q-module, and z centralizes $\Phi(P)$. Furthermore, $|P/\Phi(P)|=p^{2m}$ and $|P'|\le p^m$.*

Since $|\bar{P}|=4$, we have $m=1$. So $|P'|\le 2$, which means P is an extraspecial 2-group of order 2^3. Since $P/\Phi(P)$ is a faithful Q-module, Q is cyclic of order 3. If P is an extraspecial 2-group of order 2^3, then P has 4 linear characters and 1 nonlinear irreducible character of degree 2. The nontrivial linear characters form one Q-orbit and induce irreducibly to the same nonlinear character of G of degree 3. The unique nonlinear character of P is necessarily G-invariant, and so extends to G since $[G:P]=3$ is prime (see [17, Corollary 6.19]). This gives rise to $|\mathrm{Irr}(G/P)|=3$ distinct irreducible characters of G of degree 2 by [17, Corollary 6.17]. There are $[G:G']=[G:P]=3$ linear characters. So

$$q_h(G)=\frac{1}{24}\left(3+\frac{3}{2^{2h-2}}+\frac{1}{3^{2h-2}}\right)\le\frac{1}{24}\left(6+\frac{1}{3^{2h-2}}\right)=\frac{1}{4}\left(1+\frac{1}{2\cdot 3^{2h-1}}\right)<q_h(\mathrm{A}_4),$$

again a contradiction. The result is proved. □

Proof of the solvability criterion, Theorem 1.1(d). If $h=1$, then $q_1(G)=d(G)>d(\mathrm{A}_5)=\frac{1}{12}$, and G is already known to be solvable by a result of Dixon [10]. So, now assume that $h\ge 2$, and suppose that G is a counterexample to the claim with minimal order. By Lemma 2.1(a), we have $d(G)\ge q_h(G)>q_h(\mathrm{A}_5)>1/|\mathrm{A}_5|=\frac{1}{60}$.

We first note that $q_h(G')\ge q_h(G)$ by Lemma 2.2. So if $G'<G$, then G' is solvable by induction on the order of the group. But then G is also solvable, a

contradiction. So $G = G'$ is perfect and nontrivial irreducible characters have degree at least 2. Thus,

$$q_h(G) \le \frac{1}{|G|}\left(1 + \frac{k(G)-1}{2^{2h-2}}\right) = \frac{1}{|G|}\left(\frac{k(G)+2^{2h-2}-1}{2^{2h-2}}\right).$$

Next, we have the following inequalities when $k(G) \ge 5$:

$$\frac{k(G)+2^{2h-2}-1}{2^{2h-2}} \le \frac{2k(G)}{5} \qquad \text{for } h = 2,$$
$$\frac{k(G)+2^{2h-2}-1}{2^{2h-2}} \le \frac{k(G)}{3} \qquad \text{for } h > 2.$$

It is not difficult to see that if $k(G) < 5$, then $|G| \le 12$, and so G is solvable (see [4, Note A] or [34, Table 1]). Since G is nonsolvable, we must have $k(G) \ge 5$. Therefore, we have

$$d(G) = k(G)/|G| \ge \tfrac{5}{2} q_2(G) > \tfrac{5}{2} q_2(\mathrm{A}_5) = \tfrac{5}{2}\,\tfrac{4769}{216000} > \tfrac{1}{20},$$
$$d(G) = k(G)/|G| \ge 3q_h(G) > 3q_h(\mathrm{A}_5) > \tfrac{3}{60} = \tfrac{1}{20} \qquad \text{for } h > 2.$$

Therefore, G is perfect with $d(G) > \frac{1}{20}$ for all $h \ge 2$. Then by Lemma 2.1(b), $G \cong \mathrm{A}_5$ or $G \cong \mathrm{SL}_2(5)$. But

$$q_h(\mathrm{SL}_2(5)) = \frac{1}{120}\left(1 + \frac{2}{2^{2h-2}} + \frac{2}{3^{2h-2}} + \frac{2}{4^{2h-2}} + \frac{1}{5^{2h-2}} + \frac{1}{6^{2h-2}}\right)$$
$$< \frac{1}{120}\left(2 + \frac{4}{3^{2h-2}} + \frac{2}{4^{2h-2}} + \frac{2}{5^{2h-2}}\right) = q_h(\mathrm{A}_5).$$

This is our final contradiction, and Theorem 1.1 is proved. □

Next, the proof of Theorem 1.3 runs along the lines of that of Theorem 1.1(d). Although it may be true that $q_{h,p'}(G)$ is monotone with respect to subgroups, the proof of Lemma 2.2 will not work when the prime p divides $|G|$, because Frobenius reciprocity does not hold in this case. However, we can again show that a minimal counterexample to the theorem must be perfect by using some basic results from the theory of Brauer characters. Before we begin, recall that we defined $\alpha(h, p) = (2^{2h-2} + \sqrt{p-1})/(2^{2h-2}\sqrt{p-1})$.

Proof of Theorem 1.3. Suppose for a contradiction that G is a counterexample to the claim with minimal order. We first show that if $N \le G$ is a normal subgroup with index equal to any prime r, then $q_{h,p'}(G) \le q_{h,p'}(N)$. This will then imply that G is perfect, since if not, then there exists such an $N \trianglelefteq G$ with $\alpha(h, p)/(p-1) < q_{h,p'}(G) \le q_{h,p'}(N)$, so N is p-solvable by induction on the order of the group. But then G is also p-solvable since the quotient G/N is cyclic, which is a contradiction.

Now, each character $\varphi \in \mathrm{IBr}(G)$ lies above at least one character $\theta \in \mathrm{IBr}(N)$. Denoting by $\mathrm{IBr}(G|\theta)$ the collection of irreducible p-Brauer characters of G lying

over $\theta \in \mathrm{IBr}(N)$, we have

$$q_{h,p'}(G) \leq \frac{1}{|G|_{p'}} \sum_{\theta \in \mathrm{IBr}(N)} \sum_{\varphi \in \mathrm{IBr}(G|\theta)} \frac{1}{\varphi(1)^{2h-2}}.$$

Since $N \trianglelefteq G$ has prime index r, there are two possibilities for each $\theta \in \mathrm{IBr}(N)$:

(1) θ is G-invariant, in which case θ extends to an irreducible Brauer character $\hat{\theta}$ of G by [29, Theorem 8.12] since G/N is cyclic. In addition, the characters $\beta\hat{\theta}$ for $\beta \in \mathrm{IBr}(G/N)$ are all the irreducible constituents of θ^G by [29, Corollary 8.20]. Note that $\beta(1)\hat{\theta}(1) = \theta(1)$ since β is linear. Finally, since $N \trianglelefteq G$, $\varphi \in \mathrm{IBr}(G)$ is an irreducible constituent of θ^G if and only if θ is an irreducible constituent of φ_N by [29, Corollary 8.7]. Therefore, $|\mathrm{IBr}(G|\theta)| = |\mathrm{IBr}(G/N)| = [G : N]_{p'}$.

(2) The stabilizer of θ in G is N, in which case the induced character $\varphi = \theta^G$ is irreducible by Clifford's theorem [29, Theorem 8.9]. So $|\mathrm{IBr}(G|\theta)| = 1$, again by [29, Corollary 8.7], and $\varphi(1) > \theta(1)$.

Therefore, for each $\theta \in \mathrm{IBr}(N)$ we have

$$\sum_{\varphi \in \mathrm{IBr}(G|\theta)} \frac{1}{\varphi(1)^{2h-2}} \leq \frac{[G : N]_{p'}}{\theta(1)^{2h-2}},$$

and so

$$q_{h,p'}(G) \leq \frac{[G : N]_{p'}}{|G|_{p'}} \sum_{\theta \in \mathrm{IBr}(N)} \frac{1}{\theta(1)^{2h-2}} = q_{h,p'}(N),$$

which is what we wanted to show.

Since we now know that the counterexample G is perfect, all nontrivial irreducible Brauer characters are nonlinear, and we have

$$q_{h,p'}(G) \leq \frac{1}{|G|_{p'}} \left(1 + \frac{k_{p'}(G) - 1}{2^{2h-2}}\right) = \frac{1}{|G|_{p'}} \left(\frac{k_{p'}(G) + 2^{2h-2} - 1}{2^{2h-2}}\right),$$

where the inequality follows since $\varphi(1) \geq 2$ for all nonlinear $\varphi \in \mathrm{IBr}(G)$.

Now, since G is non-p-solvable, it is known that $k_{p'}(G) > \sqrt{p-1}$ by [30, Theorem 1.2]. Note that the following inequality is satisfied for $k_{p'}(G) > \sqrt{p-1}$ and each $h \geq 1$:

$$\frac{k_{p'}(G) + 2^{2h-2} - 1}{2^{2h-2}} < \alpha(h, p) k_{p'}(G).$$

To see this, multiply through by 2^{2h-2}, move all terms involving $k_{p'}(G)$ to the right-hand side, and use that $k_{p'}(G) > \sqrt{p-1}$. This implies that

$$d_{p'}(G) = \frac{k_{p'}(G)}{|G|_{p'}} > \frac{1}{\alpha(h, p)} q_{h,p'}(G) > \frac{1}{p-1}.$$

But this contradicts [33, Theorem 1.1], and the theorem is proved. □

4. Criterion for the existence of normal Sylow subgroups

In this section, we prove Theorem 1.2, which is a criterion for the existence of a normal Sylow subgroup. Let p be a prime, and let h be a positive integer. Recall that for a finite group G and a prime p, G is said to be p-closed if G has a normal Sylow p-subgroup. Define

$$\gamma(h, p) = \frac{1}{p+1}\Big(1 + \frac{1}{p^{2h-1}}\Big).$$

Note that $\gamma(h, p) > 1/(p+1)$. We now prove Theorem 1.2.

Proof of Theorem 1.2. Let G be a counterexample to the theorem with minimal order. Then $q_h(G) > \gamma(h, p)$ but G does not have a normal Sylow p-subgroup. By Lemma 2.1(c), we have $d(G) \leq 1/p$. Consequently,

$$\frac{1}{p} \geq d(G) \geq q_h(G) > \gamma(h, p) > \frac{1}{p+1}.$$

By Lemma 2.2, for each proper subgroup H of G, we have $q_h(H) \geq q_h(G) > \gamma(h, p)$ and thus by the minimality of $|G|$, H is p-closed. In particular, every proper subgroup of G is p-closed. Also, if N is a normal subgroup of G, then every proper subgroup of the quotient group G/N is p-closed.

Assume that $p = 2$. Then $\gamma(h, p) = q_h(\mathrm{S}_3)$ and since $q_h(G) > q_h(\mathrm{S}_3)$, G is nilpotent by Theorem 1.1(b). But then G has a normal Sylow 2-subgroup, a contradiction. Therefore, we may assume that $p \geq 3$.

Let P be a Sylow p-subgroup of G.

Claim 1: *$\langle P^G \rangle = G$. Hence, G has no proper normal subgroup of p'-index.*

Let $L = \langle P^G \rangle$. Then $P \leq L \trianglelefteq G$. Suppose that $L < G$. By the minimality of $|G|$, L has a normal Sylow p-subgroup, which implies that $P \trianglelefteq L$. Since P is characteristic in L, we deduce that $P \trianglelefteq G$, which is a contradiction. Therefore, $G = L$ as desired.

Claim 2: *G is not a nonabelian simple group.*

Since $d(G) > 1/(p+1)$, this follows from Lemma 2.3.

Claim 3: *Let N be a maximal normal subgroup of G. Then $G = \langle x \rangle N$ with $[G : N] = p$, where N has a normal Sylow p-subgroup, which is $O_p(G)$, and $x \in P$ is a p-element and $P = \langle x \rangle O_p(G)$. In particular, G is p-solvable with a Hall p'-subgroup R and $G = PR$ with $[P : O_p(G)] = p$.*

Since G is not a simple group, G has a maximal normal subgroup, say N. It follows that N has a normal Sylow p-subgroup, say P_1. As $P_1 \trianglelefteq N \trianglelefteq G$, we deduce that $P_1 \trianglelefteq G$ and thus $P_1 \leq O_p(G)$. Since G/N is a simple group and $d(G/N) \geq d(G) > 1/(p+1)$ and p divides $|G/N|$ by Claim 1, Lemma 2.3 yields

that G/N is abelian. Hence, G/N is cyclic of order p. It follows that $G = PN$ and $P \cap N = P_1 \trianglelefteq G$. As $[G : N] = [P : P_1] = p$ and P is not normal in G, we deduce that $P_1 = O_p(G)$. Let $x \in P \setminus P_1$. Then $P = \langle x \rangle P_1 = \langle x \rangle O_p(G)$. Since $N/O_p(G)$ is a p'-group and both $O_p(G)$ and G/N are p-groups, G is p-solvable. So G has a Hall p'-subgroup R and thus $N = RO_p(G)$ and $G = PN = PR$ with $[G : N] = [P : O_p(G)] = p$.

Claim 4: *R is a Sylow r-group of G for some prime r.*

Let $\overline{G} = G/O_p(G)$. Then $\overline{P} \cong C_p$ acts coprimely and nontrivially on $\overline{N} = \overline{R} \cong R$. Suppose for a contradiction that $|\overline{R}| = |R|$ is divisible by at least two distinct primes. Let q be a prime divisor of $|R|$. By the coprime action theorem [18, Theorem 3.23], $\overline{P}$ stabilizes a Sylow q-subgroup $\overline{Q}$ of $\overline{R}$. But then $\overline{P}\,\overline{Q}$ is a proper subgroup of $\overline{G}$, and hence it has a normal Sylow p-subgroup. Thus, $\overline{P}$ centralizes $\overline{Q}$. It follows that $|\overline{G} : \boldsymbol{C}_{\overline{G}}(\overline{P})|$ is not divisible by q. Clearly, this index is also not divisible by p. As this is true for all prime divisors of $|R|$, we must have $\overline{G} = \boldsymbol{C}_{\overline{G}}(\overline{P})$, which is a contradiction. Thus R is an r-group for some prime r, and so it is a Sylow r-subgroup of G.

Claim 5: *Let n be the smallest nontrivial character degree of G. Then $n \geq (p-1)/2$.*

Note that G is nonabelian and so such a minimal nontrivial degree n exists. Let $\chi \in \mathrm{Irr}(G)$ such that $\chi(1) = n$ and let K be the kernel of χ. Then K is a proper normal subgroup of G. We consider the following cases.

Case 1: G/K has a normal Sylow p-subgroup. Then $PK/K \trianglelefteq G/K$ as PK/K is a Sylow p-subgroup of G/K. By Claim 1, we have $G = PK$ and thus $G/K \cong P/P\cap K$, which is a p-group. Since $\chi \in \mathrm{Irr}(G/K)$ is nonlinear, G/K is a nonabelian p-group and thus $n = \chi(1) \geq p > (p-1)/2$.

Case 2: G/K does not have a normal Sylow p-subgroup. It follows that G/K has a faithful irreducible character of degree n and does not have a normal Sylow p-subgroup. By [12, Theorem 1], $p \leq 2n+1$ or $n \geq (p-1)/2$.

Claim 6: *$G' = RU$, where $U = G' \cap O_p(G) \trianglelefteq G$.*

Note that G is a $\{p, r\}$-group by Claim 4, so it is solvable and $G' \leq N \trianglelefteq G$. Since $\langle P^G \rangle = G$, we deduce that G/G' is an abelian p-group. Thus, G' contains a Sylow r-group of G. It follows that $R \leq G'$. By Dedekind's modular law, $G' = R(G' \cap O_p(G))$, where $G' \cap O_p(G)$ is a normal Sylow p-subgroup of G'.

Claim 7: *The quotient $G/R'O_p(G)$ is a Frobenius group with a cyclic complement of order p and Frobenius kernel an abelian 2-group of order 2^m for some $m \geq 2$, and $p = 2^m - 1$.*

Note that $N/O_p(G) = RO_p(G)/O_p(G) \trianglelefteq G/O_p(G)$ and thus $(N/O_p(G))' = R'O_p(G)/O_p(G)$. Hence, $R'O_p(G) \trianglelefteq G$. Let $\overline{G} = G/R'O_p(G)$. Then $O_p(\overline{G}) = 1$,

$\bar{R} \trianglelefteq \bar{G}$, $\bar{G}' = \bar{R}$ and $\bar{G} = \langle \bar{x} \rangle \bar{R}$ with $|\bar{x}| = p$. Moreover, $\bar{R}$ is an abelian r-group and $|\bar{G}'| = |\bar{R}| = r^m$ for some positive integer m. It follows that p is the only nontrivial character degree of G. Hence,

$$d(\bar{G}) = \frac{1}{p^2} + \left(1 - \frac{1}{p^2}\right)\frac{1}{|\bar{G}'|},$$

by [14, Lemma 2(vi)]. Since $d(\bar{G}) > 1/(p+1)$, we deduce that

$$r^m < \frac{(p+1)(p^2-1)}{p^2-p-1}.$$

Since $p \geq 3$, we can check that

$$\frac{(p+1)(p^2-1)}{p^2-p-1} \leq 2p+1.$$

Hence $r^m \leq 2p$. As $r \neq p$, we have $r^m \leq 2p-1$. Moreover, as

$$\frac{1}{|\bar{G}'|} \leq d(\bar{G}) \leq \frac{1}{p},$$

we deduce that $r^m \geq p$. Thus

$$(*) \qquad p \leq r^m \leq 2p-1.$$

By Fitting's theorem [18, Theorem 4.34], $\bar{R} = [\bar{R}, \bar{P}] \times \boldsymbol{C}_{\bar{R}}(\bar{P})$. If $\boldsymbol{C}_{\bar{R}}(\bar{P})$ is nontrivial, then $[\bar{R}, \bar{P}]\bar{P}$ is a proper subgroup of $\bar{G}$, which implies that it is p-closed and hence $\bar{P}$ centralizes $[\bar{R}, \bar{P}]$. This is impossible as it would imply that $\bar{P}$ centralizes $\bar{R}$ and thus $\bar{G}$ has a normal Sylow p-subgroup. Therefore, $\boldsymbol{C}_{\bar{R}}(\bar{P}) = 1$. It follows that $\bar{G}$ is a Frobenius group with kernel $\bar{R}$ and a cyclic complement $\bar{P}$. This implies that $r^m - 1 = kp$ for some positive integer k. Combining with $(*)$, we get $r^m - 1 = p$. As $p \geq 3$, $p+1 = r^m$ must be even. Hence $r = 2$ and

$$2^m - 1 = p.$$

In particular, $m \geq 2$ is a prime and p is a Mersenne prime.

For brevity, we define $\Gamma(p, m) := C_2^m \rtimes C_p$ to be a Frobenius group with kernel an elementary abelian 2-group of order 2^m and cyclic complement of order p with $2^m - 1 = p$.

Claim 8: *We have $R' = 1$, so $G/O_p(G) = G/R'O_p(G) \cong \Gamma(p, m)$ with $p = 2^m - 1 \geq 7$ and $m \geq 3$ an odd prime.*

Assume that $m = 2$. Then $p = 3$ and

$$\gamma(h, 3) = \tfrac{1}{4}(1 + 3^{-(2h-1)}) = q_h(\mathrm{A}_4).$$

Hence, $q_h(G) > q_h(\mathrm{A}_4)$ and so by Theorem 1.1(c), G is supersolvable. By [16, Theorem VI.9.1(c)], as G is a $\{2,3\}$-group, G has a normal Sylow 3-subgroup, which is a contradiction. Therefore, we may assume from now on that $m \geq 3$ and $p = 2^m - 1 \geq 7$.

Working in the quotient group $G/O_p(G)$, we may assume $O_p(G) = 1$. By Claim 6, $G' = R$ and so $G'' = R'$ with $[R : R'] = 2^m$ by Claim 7. Recall that n is the smallest nontrivial character degree of G. Assume first that $n \geq p$. By [14, Lemma 2(vi)], we have

$$\frac{1}{p+1} < d(G) \leq \frac{1}{n^2} + \left(1 - \frac{1}{n^2}\right)\frac{1}{|G'|} \leq \frac{1}{p^2} + \left(1 - \frac{1}{p^2}\right)\frac{1}{|G'|}.$$

As above, we deduce that $p \leq |G'| \leq 2p - 1$. Write $|G'| = |R| = 2^{m+c}$ for some integer $c \geq 0$. Recall that $2^m = 1 + p$ so

$$p \leq |G'| = (1+p)2^c = 2^c p + 2^c \leq 2p - 1.$$

This implies that $2^c = 1$, and hence $G' = R$ is abelian.

Now assume that $n < p$. As $|G| = 2^{m+c}p$ and n divides $|G|$ and is coprime to p, we deduce that $n = 2^a$ for some positive integer $a \geq 1$, and hence that

$$\tfrac{1}{2}(p-1) \leq 2^a < p = 2^m - 1,$$

the first inequality coming from Claim 5. It follows that

$$\tfrac{1}{2}(2^m - 2) \leq 2^a \leq p - 1 = 2^m - 2.$$

Therefore,

$$2^{m-1} - 1 = \tfrac{1}{2}(2^m - 2) \leq 2^a \leq 2^m - 2.$$

We deduce that $n = 2^a = 2^{m-1}$. By [14, Lemma 2 (vi)], we have

$$\frac{1}{p+1} = \frac{1}{2^m} < d(G) \leq \frac{1}{2^{2(m-1)}} + \left(1 - \frac{1}{2^{2(m-1)}}\right)\frac{1}{|G'|}.$$

Since $m \geq 3$, simplifying the previous inequality, we obtain

$$|G'| < 2^m + \frac{2^m - 1}{2^{m-2} - 1}.$$

Now, the second summand on the right hand side of the inequality is at most 7 and thus $2^{m+c} = |G'| < 2^m + 7$. However, this is impossible if $c \geq 1$ as $m \geq 3$.

We showed in both cases that $G' = R$ is abelian. If R is not elementary abelian, then the subgroup S generated by all elements of R of order 2 is a proper subgroup of R stabilized by P, so $SP < G$ has a normal Sylow p-subgroup. Then $P \trianglelefteq SP$ fixes every element of order 2 in R, and so P acts trivially on R by [18, Corollary 4.35].

But then $P \trianglelefteq G$, a contradiction. Thus, R is elementary abelian and $G \cong \Gamma(p, m)$, as claimed.

Claim 9: *The final contradiction.*

Assume $O_p(G) = 1$. Then $G \cong \Gamma(p, m)$, and so $[G : G'] = p$ and p is the unique nontrivial character degree of G. Hence, $q_h(G) = \gamma(h, p)$, which is a contradiction.

Assume that $O_p(G) > 1$. Note that $G' = RU$ and $U = G' \cap O_p(G)$ is a normal Sylow p-subgroup of G'.

(i) Assume that $p \nmid |G'|$. So $G' = R$ is a normal Sylow r-subgroup of G. Now $P = \langle x \rangle O_p(G)$ is abelian. In this case, $G'\langle x \rangle \trianglelefteq G$. If $G'\langle x \rangle < G$, then x centralizes G', which is impossible. Thus $G = G'\langle x \rangle$. In particular, $P = \langle x \rangle$ and $y = x^p$ centralizes $G' = R$.

By Claim 8, $G/O_p(G) \cong \Gamma(p, m)$ is a Frobenius group with $G' = R$ an elementary abelian subgroup of order $2^m = p + 1$. Thus $\boldsymbol{F}(G) = G' \times \langle y \rangle = G' \times O_p(G)$ is abelian and in fact $O_p(G) = \langle y \rangle$ is central in G. It follows that p is the only nontrivial character degree of G. Since $[G : G'] = |P|$, we have

$$q_h(G) = \frac{1}{|G|}\left(|P| + \frac{k(G) - |P|}{p^{2h-2}}\right) \text{ and } |G| = [G : G'] + p^2(k(G) - |P|).$$

Solving for $k(G) - |P|$ from the second equation and plugging it in the former, we get $q_h(G) = \gamma(h, p)$, a contradiction.

(ii) Assume $p \mid |G'|$. So $|G'| = |R|p^e$ for some positive integer e. Let n be the minimal nontrivial degree of G. By [14, Lemma 2 (vi)], we have

$$\frac{1}{p+1} < \frac{1}{n^2} + \left(1 - \frac{1}{n^2}\right)\frac{1}{|G'|}.$$

Assume first that $n \geq p$. The preceding inequality then implies that

$$|G'| < \frac{(p+1)(p^2-1)}{p^2 - p - 1}.$$

As in the proof of Claim 8, we deduce that $|G'| \leq 2p - 1$. However, since $|G'| = |R|p^e$ with $e \geq 1$ and $|R| = 2^m = 1 + p \geq 8$, we see that $|G'| > 2p - 1$, which is a contradiction.

Assume that $n < p$. By Claim 5, we have $n \geq (p-1)/2$. Thus $(p-1)/2 \leq n \leq p-1$. Let $\chi \in \mathrm{Irr}(G)$ with $\chi(1) = n$. Recall that $2^m = p+1$ and $G/O_p(G) \cong \Gamma(p, m)$. It follows that $\chi(1)$ divides $|R|$ where $|R| = 2^m$ since $p \nmid \chi(1)$ and $\chi(1) \mid |G|$. So $n = 2^a$ for some positive integer a. Since $(p-1)/2 = (2^m - 2)/2 = 2^{m-1} - 1 < 2^a \leq p - 1 = 2^m - 2$, we deduce that $n = 2^{m-1}$.

Employing the same argument as in the proof of Claim 8, we obtain a contradiction as $m \geq 3$.

The proof of the theorem is now complete. □

5. The dual invariant

In this section, we prove Theorems 1.4 and 1.5.

Proof of the abelian criterion, Theorem 1.4(a). Assume for a contradiction that G is a counterexample to the claim with minimal order. Note that the sizes of the conjugacy classes of D_8 are 1, 1, 2, 2, 2. Since $\tilde{q}_1(G) = d(G)$, we must have $h \geq 2$. As G is nonabelian, we have $d(G) \leq \frac{5}{8}$ by [15]. Every noncentral conjugacy class of G has size at least 2, so we have

$$\begin{aligned}\frac{1}{4}\Big(1+\frac{3}{2^h}\Big) = \tilde{q}_h(\mathrm{D}_8) < \tilde{q}_h(G) &\leq \frac{1}{|G|}\bigg(|\mathbf{Z}(G)| + \frac{k(G)-|\mathbf{Z}(G)|}{2^{h-1}}\bigg)\\ &= \frac{1}{[G:\mathbf{Z}(G)]}\Big(1-\frac{1}{2^{h-1}}\Big)+\frac{d(G)}{2^{h-1}}\\ &\leq \frac{1}{[G:\mathbf{Z}(G)]}\Big(1-\frac{1}{2^{h-1}}\Big)+\frac{1}{4}\cdot\frac{5}{2^h}.\end{aligned}$$

We find immediately from these inequalities that $[G:\mathbf{Z}(G)] < 4$. But then $G/\mathbf{Z}(G)$ is cyclic and G is abelian, a contradiction. □

Proof of the nilpotency criterion, Theorem 1.4(b). Assume for a contradiction that G is a counterexample to the claim with minimal order. Since $\tilde{q}_1(G) = d(G)$, we must have $h \geq 2$. We have

$$\frac{1}{6} < \frac{1}{6}\Big(1+\frac{1}{2^{h-1}}+\frac{1}{3^{h-1}}\Big) = \tilde{q}_h(\mathrm{S}_3) < \tilde{q}_h(G) \leq d(G) \leq \frac{1}{2}.$$

As $\tilde{q}_h(G/\mathbf{Z}(G)) \geq \tilde{q}_h(G)$ by Lemma 2.6, the quotient $G/\mathbf{Z}(G)$ is nilpotent if $\mathbf{Z}(G) > 1$ by the minimality of $|G|$. But then G is nilpotent, a contradiction. Therefore, we may assume that $|\mathbf{Z}(G)| = 1$.

Since $d(G)/\tilde{q}_h(G) \leq \frac{1}{2}/\frac{1}{6} = 3$, we may take $N = 3$ in Lemma 2.7. Letting $n \geq 2$ be the minimal nontrivial class size, if $n^{h-1} \leq N = 3$, then we must have $h = 2$. In this case,

$$\frac{11}{36} = \tilde{q}_2(\mathrm{S}_3) < \tilde{q}_2(G) \leq \frac{1}{|G|}\Big(1+\frac{k(G)-1}{2}\Big) = \frac{1}{2|G|}+\frac{d(G)}{2} \leq \frac{1}{2|G|}+\frac{1}{4},$$

which means $|G| < 9$ and so $G \cong \mathrm{S}_3$, a contradiction. Therefore, it only remains to consider case (2) of Lemma 2.7; that is, $|G| \leq d(G)/\tilde{q}_h(G)^2 < 18$. The only nonnilpotent groups with trivial center of order less than 18 are dihedral groups D_{2k} for $k = 3, 5, 7$ and A_4. Since

$$\tilde{q}_h(\mathrm{D}_{2k}) = \frac{1}{2k}\Big(1+\frac{(k-1)/2}{2^{h-1}}+\frac{1}{k^{h-1}}\Big)$$

when k is odd, $\tilde{q}_h(D_{2k})$ is a decreasing function of k, and so $\tilde{q}_h(G) \leq \tilde{q}_h(S_3)$ for all h in these cases. The class sizes of A_4 are $1, 3, 4, 4$, so

$$\begin{aligned}\tilde{q}_h(A_4) &= \frac{1}{12}\Big(1 + \frac{1}{3^{h-1}} + \frac{2}{4^{h-1}}\Big) \\ &< \frac{1}{12}\Big(2 + \frac{2}{3^{h-1}} + \frac{2}{4^{h-1}}\Big) = \frac{1}{6}\Big(1 + \frac{1}{3^{h-1}} + \frac{1}{4^{h-1}}\Big) < \tilde{q}_h(S_3),\end{aligned}$$

a contradiction. The result is proved. □

Proof of the supersolvability criterion, Theorem 1.4(c). Assume for a contradiction that G is a counterexample to the claim with minimal order. Since $\tilde{q}_1(G) = d(G)$, we must have $h \geq 2$. We have

$$\frac{1}{12} < \frac{1}{12}\Big(1 + \frac{1}{3^{h-1}} + \frac{2}{4^{h-1}}\Big) = \tilde{q}_h(A_4) < \tilde{q}_h(G) \leq d(G) \leq \frac{1}{3}.$$

Since $d(G) > \frac{1}{12}$, G is solvable by [10]. Since G is supersolvable if $G/\Phi(G)$ is supersolvable by [16, Theorem VI.8.6(a)] and G is supersolvable if $G/\boldsymbol{Z}(G)$ is supersolvable by the definition of supersolvability [16, Definition VI.8.5(b)], it follows by Lemma 2.6 and induction that both the Frattini subgroup and the center of G are trivial.

Suppose that G has two distinct minimal normal subgroups, say M_1 and M_2. By Lemma 2.6 and the minimality of $|G|$, both G/M_1 and G/M_2 are supersolvable, and so G is supersolvable as G embeds into a supersolvable group $G/M_1 \times G/M_2$. This is a contradiction. Therefore, G has a unique minimal normal subgroup, say M, and since G is solvable, M is an elementary abelian p-group of order p^m for some prime p and positive integer $m \geq 1$. If $m = 1$, then G is supersolvable, so we may assume that $m > 1$. As $\Phi(G) = 1$, we have $\boldsymbol{F}(G) = M$ by Gaschütz' theorem [16, Theorem III.4.5], and hence $\boldsymbol{C}_G(M) = M$ by [16, Theorem III.4.2 b)].

First assume that $n = 2$, where n is the minimal size of a noncentral class of G. Let $x \in G$ be such that $|x^G| = [G : \boldsymbol{C}_G(x)] = 2$. Then $\boldsymbol{C}_G(x) \trianglelefteq G$, and so $M \leq \boldsymbol{C}_G(x)$ as M is the unique minimal normal subgroup of G. Hence, x lies in $\boldsymbol{C}_G(M) = M$. Since $\langle x^G \rangle$ is a normal subgroup of G and $x \in M$, we must have $\langle x^G \rangle = M$. As $|x^G| = 2$, $M = \langle x, x^t \rangle$ for some $t \in G \setminus \boldsymbol{C}_G(x)$. In particular, $|M| = p^2$ as M is noncyclic elementary abelian and generated by two elements. Now, $M = \boldsymbol{C}_G(M) = \boldsymbol{C}_G(x) \cap \boldsymbol{C}_G(x^t) = \boldsymbol{C}_G(x) \cap \boldsymbol{C}_G(x)^t = \boldsymbol{C}_G(x)$ as $\boldsymbol{C}_G(x)$ is normal in G. Thus, $[G : M] = [G : \boldsymbol{C}_G(x)] = 2$, and so $|G| = 2p^2$. If $p = 2$, then G is a finite 2-group, so it is nilpotent and hence it is supersolvable. Therefore, we may assume that $p \geq 3$. Since $|G| = 2p^2$, G has a cyclic Sylow 2-subgroup $Q = \langle g \rangle$, where g is an involution, acting on the unique minimal normal subgroup $M \cong C_p \times C_p$ of G by conjugation. But this is impossible. To see this, let $1 \neq a \in M$. We have $(aa^g)^g = a^g a = aa^g$, so $\langle aa^g \rangle$ is a normal subgroup of G. If $aa^g \neq 1$, then $\langle aa^g \rangle$ is a nontrivial cyclic normal subgroup of G properly contained in the

noncyclic group M, contradicting the fact that M is minimal normal. On the other hand, if $aa^g = 1$, then $a^g = a^{-1}$ and $\langle a \rangle$ is again a nontrivial normal subgroup of G properly contained in M.

Therefore, may assume that $n \geq 3$. Since $d(G)/\tilde{q}_h(G) \leq \frac{1}{3}/\frac{1}{12} = 4$, we may choose to set $N = 8$ in Lemma 2.7. Since $3^{h-1} \leq n^{h-1} \leq N = 8$, we must have $h = 2$. We have

$$\frac{11}{72} = \tilde{q}_2(\mathrm{A}_4) < \tilde{q}_2(G) \leq \frac{1}{|G|} + \frac{d(G)}{n} \leq \frac{1}{|G|} + \frac{1}{9}.$$

Simplifying this inequality, we obtain $|G| < 24$. Since G is nonsupersolvable with trivial center, the only possibility for G is A_4. This is a contradiction.

There remains to consider case (2) of Lemma 2.7. Since $\boldsymbol{Z}(G) = 1$ by the first paragraph and we chose $N = 8$, we have

$$|G| \leq \frac{8}{\frac{1}{12} \cdot 9 - \frac{1}{3}} = \frac{96}{5} < 20.$$

The only nonsupersolvable group of order less than 20 with trivial center is again A_4. This contradiction completes the proof of this item. □

Proof of the solvability criterion, Theorem 1.4(d). Assume for a contradiction that G is a counterexample to the claim with minimal order. Since $\tilde{q}_1(G) = d(G)$, we must have $h \geq 2$. We have

$$\tfrac{1}{60} < \tilde{q}_h(\mathrm{A}_5) < \tilde{q}_h(G) \leq d(G) \leq \tfrac{1}{12}.$$

As $\tilde{q}_h(G/\mathrm{Sol}(G)) \geq \tilde{q}_h(G)$ by Lemma 2.6, the quotient $G/\mathrm{Sol}(G)$ is solvable if the solvable radical $\mathrm{Sol}(G)$ is nontrivial by the minimality of $|G|$. But then G is solvable, a contradiction. Therefore, we may assume that $|\mathrm{Sol}(G)| = 1$.

Let n be the minimal nontrivial class size of G. If n is a prime power, then the subgroup generated by that class is a solvable normal subgroup of G by [22]. As G has no nontrivial solvable normal subgroups, we must have $n \geq 6$. Since $d(G)/\tilde{q}_h(G) \leq (\frac{1}{12})/(\frac{1}{60}) = 5$, we may take $N = 5$ in Lemma 2.7. This means that $n^{h-1} \leq N$ never occurs, and we need only consider case (2) of Lemma 2.7; that is,

$$|G| \leq d(G)/\tilde{q}_h(G)^2 < 300.$$

The only nonsolvable groups of order less than 300 with trivial solvable radical are A_5, S_5, and $\mathrm{PSL}_3(2)$. The conjugacy class sizes of A_5 are 1, 12, 12, 15, 20; those of S_5 are 1, 10, 15, 20, 20, 24, 30; and those of $\mathrm{PSL}_3(2)$ are 1, 21, 24, 24, 42, 56. Then one can check by direct calculation that $\tilde{q}_h(\mathrm{PSL}_3(2)) < \tilde{q}_h(\mathrm{S}_5) < \tilde{q}_h(\mathrm{A}_5)$. This means G is not isomorphic to A_5, S_5, or $\mathrm{PSL}_3(2)$, and we are done. □

We now prove Theorem 1.5. For a prime p and a positive integer h, define

$$\tilde{\gamma}(h, p) = \frac{1}{p(p+1)}\left(1 + \frac{1}{p^{h-1}} + \frac{p-1}{(p+1)^{h-1}}\right).$$

Proof of Theorem 1.5. Since $\tilde{\gamma}(h, 2) = \tilde{q}_h(\mathrm{S}_3)$, if $p = 2$, then G is nilpotent by Theorem 1.4(b) and thus has a normal Sylow 2-subgroup. Therefore, we may assume $p \geq 3$. As $\tilde{q}_1(G) = d(G)$ and $\tilde{\gamma}(1, p) = 1/p$, the theorem follows from Lemma 2.1(c) when $h = 1$. So we may assume that $h \geq 2$. Let G be a counterexample to the theorem with minimal order. Then

$$\frac{1}{p} \geq d(G) \geq \tilde{q}_h(G) > \tilde{\gamma}(h, p) > \frac{1}{p(p+1)}$$

but G is not p-closed. Let P be a Sylow p-subgroup of G. We may assume that $O_p(G) = 1$ as otherwise, by Lemma 2.6 and the minimality of $|G|$, we deduce that $G/O_p(G)$ has a normal Sylow p-subgroup and so does G, a contradiction. Next, assume that $\boldsymbol{Z}(G) > 1$. Then $\boldsymbol{Z}(G)$ is a p'-group, and $G/\boldsymbol{Z}(G)$ has a normal Sylow p-subgroup $P\boldsymbol{Z}(G)/\boldsymbol{Z}(G)$ again by Lemma 2.6. It follows that $P \trianglelefteq P\boldsymbol{Z}(G) \trianglelefteq G$ which implies that $P \trianglelefteq G$, a contradiction. Therefore, $\boldsymbol{Z}(G) = 1$.

Next, we claim that G has a unique minimal normal subgroup. Suppose that G has two distinct minimal normal subgroups, say N_1 and N_2. By Lemma 2.6 and the minimality of $|G|$, both G/N_1 and G/N_2 are p-closed. Since G embeds into $G/N_1 \times G/N_2$, the group G is p-closed as subgroups and direct products of p-closed groups are p-closed. It follows that G has a unique minimal normal subgroup N, and $N \cong S^m$ for some simple group S and some integer $m \geq 1$.

Let $H = \boldsymbol{N}_G(P)$. Since $PN \trianglelefteq G$ by Lemma 2.6 and the minimality of $|G|$, we have $G = HN$ by Frattini's argument.

Claim 1: *If C is a noncentral conjugacy class of G, then $|C| \geq p$.*

If $C_0 = x^G$ is a noncentral conjugacy class of G having minimal size, we claim that $|C_0| \geq p$. For if $|C_0| = [G : \boldsymbol{C}_G(x)] < p$ instead, and $U = \bigcap_{g \in G} \boldsymbol{C}_G(x)^g$ is the core of $\boldsymbol{C}_G(x)$ in G, then $U \trianglelefteq G$ and $[G : U] = |C_0| \cdot [\boldsymbol{C}_G(x) : U]$. As G/U embeds into the symmetric group S_t, where $t = |C_0| = [G : \boldsymbol{C}_G(x)] < p$, $|G/U|$ is not divisible by p. Since $U \trianglelefteq G$ and Sylow subgroups are conjugate by Sylow's theorems, $P \leq U$. Hence U is nontrivial and thus $N \leq U \leq \boldsymbol{C}_G(x)$. In particular, $x \in \boldsymbol{C}_G(N)$.

If N is nonabelian, then $\boldsymbol{C}_G(N) = 1$, which leads to a contradiction. Now assume that N is abelian. Then $S \cong C_r$ for some prime r and so N is an elementary abelian r-group of order r^m. Since $G = HN$ and N is the unique minimal normal subgroup of G, we must have $\Phi(G) = 1$ and that $\boldsymbol{F}(G) = O_r(G)$ is a product of minimal normal subgroups of G by Gaschütz' theorem [16, Theorem III.4.5]. Thus $\boldsymbol{F}(G) = N$ and so $\boldsymbol{C}_G(N) = N$ by [16, Theorem III.4.2 b)]. It follows that $x \in N$. Furthermore, since $P \leq \boldsymbol{C}_G(x)$, we have $x \in \boldsymbol{C}_N(P)$. Observe that P

acts coprimely and nontrivially on N. By Fitting's Theorem [18, Theorem 4.34], $N = [N, P] \times \boldsymbol{C}_N(P)$. Note that $\boldsymbol{N}_N(P) = N \cap \boldsymbol{N}_G(P) = N \cap H$. As $N \trianglelefteq G$, we have $H \cap N \trianglelefteq H$ and since N is abelian, $H \cap N \trianglelefteq N$. It follows that $H \cap N \trianglelefteq G = NH$, and by the minimality of N, we have $N \cap H = 1$. Now $\boldsymbol{C}_N(P) \leq \boldsymbol{N}_N(P) = 1$, which implies that $x \in \boldsymbol{C}_N(P) = 1$, a contradiction.

Therefore, we have shown that $|C_0| \geq p$, and thus since $\boldsymbol{Z}(G) = 1$, for each nontrivial conjugacy class C of G, we have $|C| \geq p$.

Claim 2: *$|G| < 2p(p+1)$ and $|P| = p$. Let $n_p = [G : \boldsymbol{N}_G(P)]$. Then $n_p = 1 + p$ or $1 + 2p$. In particular, $H = P$ and $G = PN$.*

Assume for a contradiction that $|G| \geq 2p(p+1)$. The hypothesis yields

$$\frac{1}{p(p+1)} < \tilde{q}_h(G) \leq \frac{1}{|G|}\left(1 + \sum_{\substack{C \in \mathrm{Cl}(G) \\ C \neq 1}} \frac{1}{|C|^{h-1}}\right) \leq \frac{1}{|G|}\left(1 + \frac{k(G)-1}{p^{h-1}}\right)$$

$$= \frac{1}{|G|}\left(1 - \frac{1}{p^{h-1}}\right) + \frac{d(G)}{p^{h-1}}.$$

Then

$$\frac{1}{p(p+1)} < \frac{1}{2p(p+1)} + \frac{d(G)}{p^{h-1}}.$$

Since $d(G) \leq 1/p$, we obtain $p^h < 2p(p+1)$, which implies $h = 2$ as $p \geq 3$.

For $h = 2$, the hypothesis yields (noting that $d(G) \leq 1/p$):

$$\tilde{\gamma}(2, p) = \frac{1}{p(p+1)}\left(1 + \frac{1}{p} + \frac{p-1}{p+1}\right) < \tilde{q}_h(G) \leq \frac{1}{|G|}\left(1 - \frac{1}{p}\right) + \frac{d(G)}{p}$$

$$\leq \frac{1}{|G|}\left(1 - \frac{1}{p}\right) + \frac{1}{p^2}.$$

Simplifying, we obtain $|G| < (p+1)^2 < 2p(p+1)$, a contradiction.

Assume that $|P| \geq p^2$. If N is nonabelian, then $|N|$ is divisible by 4 and $|G| \geq 4p^2 > 2p(p+1)$, a contradiction. Assume that N is abelian. Since $\boldsymbol{C}_G(N) = N$, P acts nontrivially and coprimely on N. Hence $|N| > p$ as P has at least one nontrivial orbit on $N \setminus \{1\}$. Then $H \cap N = 1$ by the argument in Claim 1, and thus $|G| = |H||N| \geq p^2|N| > p^3 > 2p(p+1)$. In both cases, we obtain a contradiction. Thus, $|P| = p$ as claimed.

By Sylow's theorem, we know that $n_p \equiv 1 \bmod p$, so that $n_p = 1 + kp$ for some positive integer k. Since $n_p = [G : H] \leq [G : P] < 2(p+1)$, we have $n_p < 2(p+1)$ and so $n_p \in \{1 + p, 1 + 2p\}$.

Now since $|G| = |H| n_p \in \{(1+p)|H|, (1+2p)|H|\}$ and $|G| < 2p(p+1)$, we must have $|H| < 2p$, forcing $|H| = p$ and thus $H = \boldsymbol{C}_G(P) = P$. In particular, $G = PN$.

Claim 3: *N is abelian.*

Suppose otherwise. Then $N \cong S^m$ for some nonabelian simple group S. By the uniqueness of N, we deduce that G has a trivial solvable radical.

If $|C| = p$ for some class C, then by [22], $\langle C \rangle$ is a normal solvable subgroup of G, which is impossible. Thus $|C| \geq p+1$ for every nontrivial class C of G.

If p divides $|S|$, then $p = |G|_p \geq (|S|_p)^m$ means that $m = 1$ and $G = PS = S$ is simple. However, in this case, $|G| \geq 2p(p+1)$ by the proof of Lemma 2.3. Thus p does not divide $|S|$ and so N is a p'-group. So $|G| = p|S|^m$ with $m = 1$ or $m = p$. (If N is not simple, then $m = p$ since P acts transitively on the simple factors of N as N is a minimal normal subgroup of G.)

Now $|N| = [G : H] = n_p \in \{1 + p, 1 + 2p\}$, so we have $|N| = |S|^m = 1 + p$ or $1 + 2p$. Since P has order p and $\boldsymbol{C}_G(P) = P$ by the last step, the only point of N fixed by P under conjugation is the identity and every other orbit has size p. This implies that P has at most 3 orbits in its conjugation action on N, which is impossible since $|N|$ is divisible by at least 3 distinct primes by Burnside's $p^a q^b$-theorem, so N must have at least 4 orbits under the action of P.

Claim 4: *The final contradiction.*

We now have that $G = PN$ with $|P| = p$, and N is an elementary abelian r-group of order r^m for some prime r and $r^m = |N| = 1 + p$ or $1 + 2p$. Since $\boldsymbol{Z}(G) = 1$, we see that G is a Frobenius group with Frobenius kernel N and complement P. Therefore, G has the following class structure: the $r^m - 1$ elements of order r split into classes of size p, and the $r^m(p-1)$ elements of order p split into classes of size r^m. Since $r^m = 1 + kp$ for $k = 1$ or $k = 2$, we have

$$\tilde{q}_h(G) = \frac{1}{|G|}\left(1 + \frac{(r^m - 1)/p}{p^{h-1}} + \frac{p-1}{(r^m)^{h-1}}\right) = \frac{1}{p(1+kp)}\left(1 + \frac{k}{p^{h-1}} + \frac{p-1}{(1+kp)^{h-1}}\right).$$

If $|N| = 1 + p$, then substituting $k = 1$ into the equation above yields $\tilde{q}_h(G) = \tilde{\gamma}(h, p)$, a contradiction. So $r^m = |N| = 1 + 2p$, and we can calculate $\tilde{q}_h(G)$ by substituting $k = 2$ into the equation above.

Since

$$\frac{1}{p(p+1)} < \tilde{q}_h(G) \leq \frac{1}{|G|} + \frac{d(G)}{p^{h-1}} \leq \frac{1}{p(1+2p)} + \frac{1}{p^h},$$

we deduce that $p^h < (1 + p)(1 + 2p)$, forcing $h = 3$ and $p = 3$, or $h = 2$. In the former case, we calculate directly that $\tilde{\gamma}(3, 3) > \tilde{q}_3(G)$, a contradiction. Similarly, if $h = 2$, then we calculate directly that we must have

$$\frac{1}{p(p+1)}\left(1 + \frac{1}{p} + \frac{p-1}{p+1}\right) = \tilde{\gamma}(2, p) < \tilde{q}_2(G) = \frac{1}{p(1+2p)}\left(1 + \frac{2}{p} + \frac{p-1}{1+2p}\right).$$

This can be simplified to $5p^4 + 2p^3 - 3p^2 - 3p < 1$, which is impossible since $p \geq 3$. The proof is now complete. □

6. Introduction to Dijkgraaf–Witten theory

For mathematicians, a topological quantum field theory (TQFT) is a machine for generating topological invariants of manifolds. For example, Witten [35] showed that the Jones polynomial is a topological invariant of manifolds in a certain TQFT. Atiyah [1] axiomatized topological quantum field theories in the language of category theory as a functor from a particular category of bordisms to the category of vector spaces. The invariants that we consider arise in the context of Dijkgraaf–Witten theory [7; 9] in one space dimension and one time dimension. Such a TQFT determines a commutative Frobenius algebra that gives rise to topological invariants of surfaces. The new contribution of this paper is that, upon assuming this Frobenius algebra is the center of a complex group algebra, we instead consider these invariants as invariants of groups. It should be noted, however, that Dijkgraaf–Witten theory has already been used to study finite groups; for example, row and column sums in their character tables [28; 31; 32]. In this section, we derive these topological invariants in an elementary, explicit way, without assuming any previous knowledge of quantum field theory. For a similarly gentle introduction, we recommend Dijkgraaf's 2015 lecture at the Institute for Advanced Study [8].

Let X, Y be two closed $(n-1)$-dimensional manifolds. A bordism from X to Y is a quadruple (Z, p, f_X, f_Y) where Z is an n-manifold with boundary δZ, $p : \delta Z \to \{0, 1\}$ is a continuous map (partition of the boundary into two components), $f_X : X \to p^{-1}(0)$, $f_Y : Y \to p^{-1}(1)$ are diffeomorphisms. (The empty set is considered an $(n-1)$-manifold for all n.) Two such bordisms Z, Z' from X to Y are considered equivalent if there is a diffeomorphism from Z to Z' respecting the maps p and f in the obvious way. Declaring Mor (X,Y) to be the set of all equivalence classes of bordisms from X to Y, we get the structure of a category $B(n-1)$ on closed $(n-1)$-manifolds. The composition of two bordisms is obtained by gluing them. This category $B(m)$ is a symmetric monoidal category with disjoint union as the monoidal product. Any covariant functor of symmetric monoidal categories from $B(m)$ to vector spaces Vect_k over a field k, with tensor product as the monoidal product, is an example of a topological quantum field theory.

When $n = 2$, closed 1-manifolds are just disjoint unions of a finite number of circles S^1. So a TQFT T of the above type on objects of $B(1)$ is determined by specifying $T(S^1) = V$. The images of morphisms via T are linear maps between appropriate tensor powers of V. For example, a cylinder is a bordism between two circles, and it corresponds to the identity map $\mathrm{id} : V \to V$. Perhaps most importantly, the "pair of pants" corresponds to a multiplication of quantum states $V \otimes V \to V$, which gives V the structure of an algebra. This multiplication is commutative, which we can see from topological considerations: Interchanging the legs in a pair of pants (which corresponds, on the vector space side, to switching the order

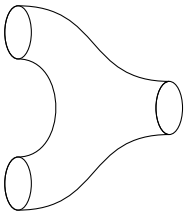
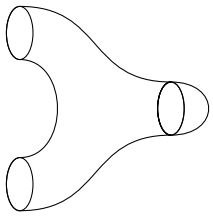
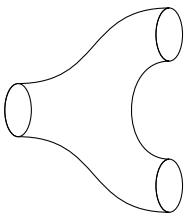
bordism	map	$V = \mathbf{Z}(\mathbb{C}G)$
	$V \otimes V \to V$	$e_\chi \cdot e_{\chi'} = \delta_{\chi,\chi'} e_\chi$
	$\langle\,\rangle : V \otimes V \to \mathbb{C}$	$\langle e_\chi, e_{\chi'}\rangle = \delta_{\chi,\chi'}\left(\frac{\chi(1)}{\lvert G\rvert}\right)^2$
	$\mathbb{C} \to V, \quad 1 \mapsto e$	$e = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi$
	$V \to \mathbb{C}$	$e_\chi \mapsto \left(\frac{\lvert G\rvert}{\chi(1)}\right)^2$
	$V \to V \otimes V$	$e_\chi \mapsto \left(\frac{\lvert G\rvert}{\chi(1)}\right)^2 e_\chi \otimes e_\chi$

Table 1. Bordisms giving rise to linear maps of vector spaces.

of the tensor product) is a diffeomorphism, so two such bordisms are equivalent. The bordisms giving rise to a multiplicative identity $e \in V$, a comultiplication $V \to V \otimes V$ and a bilinear form $\langle\,\rangle : V \otimes V \to \mathbb{C}$ are pictured in Table 1. By considering appropriate bordisms, it is not difficult to show that the multiplication is associative and the bilinear form satisfies the identity

$$\langle a, b \cdot c\rangle = \langle a \cdot b, c\rangle$$

of a Frobenius algebra. A genus-h surface can be decomposed into a composition of the bordisms in Table 1, giving rise to a map $\mathbb{C} \to \mathbb{C}$. Since the map is linear, it is defined by the image of 1, and this complex number is a topological invariant of the surface.

Now we assume that $V = \boldsymbol{Z}(\mathbb{C}G)$ is the center of the complex group algebra of a finite group G. We compute the maps in terms of a basis for $\boldsymbol{Z}(\mathbb{C}G)$ that is indexed by the irreducible complex characters $\chi \in \mathrm{Irr}(G)$ of G; namely, the primitive central idempotents

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \overline{\chi(g)} g.$$

In this basis, the multiplicative identity decomposes as $e = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi$, and the multiplication takes the form $e_\chi \cdot e_{\chi'} = \delta_{\chi,\chi'} e_\chi$. We define the bilinear form to be

$$\langle e_\chi, e_{\chi'} \rangle = \delta_{\chi,\chi'} \left(\frac{\chi(1)}{|G|} \right)^2,$$

which is the coefficient of the identity in the product $e_\chi \cdot e_{\chi'}$ times $1/|G|$. This is the so-called special Frobenius algebra structure on $\boldsymbol{Z}(\mathbb{C}G)$.

To show that the "cup" in the third row of Table 1 gives rise to a multiplicative identity of V, note that the bordism in Figure 1, top left, is homeomorphic to the cylinder, which is the identity map. To show that the "cap" in the fourth row of Table 1 sends e_χ to $(\chi(1)/|G|)^2$, note that the cap is homeomorphic to adding a cup to the bordism for the bilinear form, as in Figure 1, top middle. Finally, to show that the comultiplication is $e_\chi \mapsto (|G|/\chi(1))^2 e_\chi \otimes e_\chi$ in the last row of Table 1, note that capping off the comultiplication is homeomorphic to the cylinder, which represents the identity map, as in Figure 1, top right.

Now, we compute the map $\mathbb{C} \to \mathbb{C}$ for a genus-h surface by composing the maps

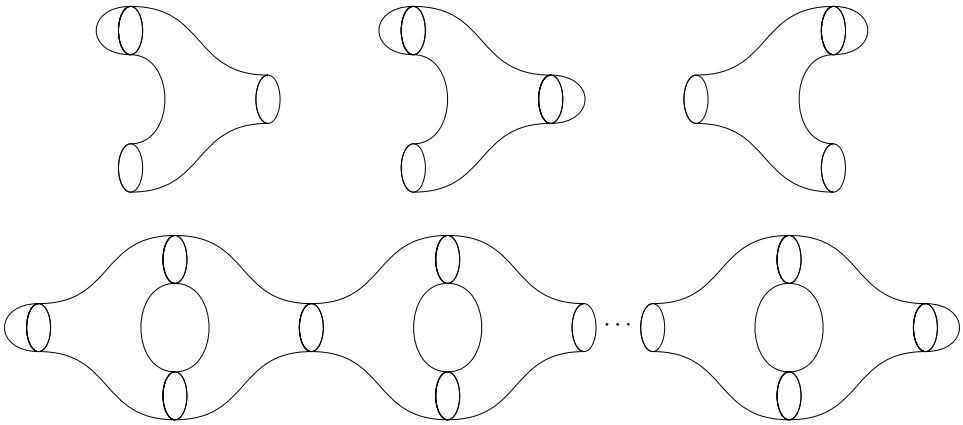


Figure 1. Bordisms for calculating (top row from the left) the cup, the cap and the comultiplication. Decomposing the genus-h surface on the bottom into bordisms calculated in Table 1 yields an invariant $\mathcal{Q}_h(G)$ of the surface.

in Table 1:

$$1 \overset{\cap}{\longmapsto} \sum_{\chi\in\mathrm{Irr}(G)} e_\chi \overset{\curlyvee}{\longmapsto} \sum_{\chi\in\mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^2 e_\chi \otimes e_\chi \overset{\curlyvee}{\longmapsto} \sum_{\chi\in\mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^2 e_\chi$$
$$\overset{\curlyvee}{\longmapsto} \cdots \overset{\curlyvee}{\longmapsto} \sum_{\chi\in\mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^{2h} e_\chi \overset{\cap}{\longmapsto} \sum_{\chi\in\mathrm{Irr}(G)} \left(\frac{|G|}{\chi(1)}\right)^{2h-2} = \mathcal{Q}_h(G).$$

The number $\mathcal{Q}_h(G)$ is the topological invariant of a genus-h surface in this TQFT. In this paper, we considered a more well-behaved invariant of groups by scaling $\mathcal{Q}_h(G)$ by an appropriate factor of $|G|$, namely

$$q_h(G) = \frac{1}{|G|} \sum_{\chi\in\mathrm{Irr}(G)} \left(\frac{1}{\chi(1)}\right)^{2h-2}.$$

Acknowledgment

The authors would like to thank Dr. Alessandro Mariani and Prof. Marcin Mazur for comments on a previous version of the paper, as well as the anonymous referee for their close reading of the paper and helpful comments.

References

[1] M. Atiyah, "Topological quantum field theories", *Inst. Hautes Études Sci. Publ. Math.* **68** (1988), 175–186. MR

[2] A. Ballester-Bolinches and R. Esteban-Romero, "On minimal non-supersoluble groups", *Rev. Mat. Iberoam.* **23**:1 (2007), 127–142. MR

[3] F. Barry, D. MacHale, and A. Ní Shé, "Some supersolvability conditions for finite groups", *Math. Proc. R. Ir. Acad.* **106A**:2 (2006), 163–177. MR

[4] W. Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge University Press, 1911. Reprinted Dover, New York, 1955; reissued in TEX by Project Gutenberg. MR

[5] D. Chillag and M. Herzog, "On character degrees quotients", *Arch. Math.* (*Basel*) **55**:1 (1990), 25–29. MR

[6] Y. Choi, "Small values and forbidden values for the Fourier anti-diagonal constant of a finite group", *J. Aust. Math. Soc.* **118**:3 (2025), 297–316. MR

[7] R. Dijkgraaf, "Fields, strings and duality", pp. 3–147 in *Symétries quantiques* (Les Houches, 1995), North-Holland, Amsterdam, 1998. MR

[8] R. Dijkgraaf, "PiTP 2015: Introduction to topological and conformal field theory", video lecture part 1, available at http://youtu.be/jEEQO-tcyHc.

[9] R. Dijkgraaf and E. Witten, "Topological gauge theories and group cohomology", *Comm. Math. Phys.* **129**:2 (1990), 393–429. MR

[10] J. D. Dixon, "Solution to Problem 176", *Canadian Math. Bull.* **16** (1973), 302.

[11] K. Doerk, "Minimal nicht überauflösbare, endliche Gruppen", *Math. Z.* **91** (1966), 198–205. MR

[12] W. Feit and J. G. Thompson, "Groups which have a faithful representation of degree less than $(p-1/2)$" [sic; for $(p-1)/2$], *Pacific J. Math.* **11** (1961), 1257–1262. MR

[13] D. Gluck, K. Magaard, U. Riese, and P. Schmid, "The solution of the $k(GV)$-problem", *J. Algebra* **279**:2 (2004), 694–719. MR

[14] R. M. Guralnick and G. R. Robinson, "On the commuting probability in finite groups", *J. Algebra* **300**:2 (2006), 509–528. MR

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

[16] B. Huppert, *Finite groups, I*, Grundl. Math. Wissen. **364**, Springer, 2025. MR

[17] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York, 1976. Corrected reprint, Dover, New York, 1994. MR

[18] I. M. Isaacs, *Finite group theory*, Graduate Studies in Mathematics **92**, Amer. Math. Soc., 2008. MR

[19] I. M. Isaacs, *Characters of solvable groups*, Graduate Studies in Mathematics **189**, Amer. Math. Soc., 2018. MR

[20] K. S. Joseph, *Commutativity in non-abelian groups*, Ph.D. thesis, University of California, Los Angeles, 1969, available at https://www.proquest.com/docview/302401138. MR

[21] K. S. Joseph, "Research problems: several conjectures on commutativity in algebraic structures", *Amer. Math. Monthly* **84**:7 (1977), 550–551. MR

[22] L. S. Kazarin, "Burnside's p^α-lemma", *Mat. Zametki* **48**:2 (1990), 45–48, 158. In Russian; translated in *Math. Notes* **48**:1–2 (1990), 749–751. MR

[23] P. Lescot, "Sur certains grupes finis", *Rev. Math. Spéciales* **8** (1987), 267–277.

[24] M. W. Liebeck and A. Shalev, "Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks", *J. Algebra* **276**:2 (2004), 552–601. MR

[25] M. W. Liebeck and A. Shalev, "Character degrees and random walks in finite groups of Lie type", *Proc. London Math. Soc.* (3) **90**:1 (2005), 61–86. MR

[26] M. W. Liebeck and A. Shalev, "Fuchsian groups, finite simple groups and representation varieties", *Invent. Math.* **159**:2 (2005), 317–367. MR

[27] A. Mariani, S. Pradhan, and E. Ercolessi, "Hamiltonians and gauge-invariant Hilbert space for lattice Yang–Mills-like theories with finite gauge group", *Phys. Rev. D* **107**:11 (2023), art. id. 114513, 15 pp. MR

[28] R. de Mello Koch, Y.-H. He, G. Kemp, and S. Ramgoolam, "Integrality, duality and finiteness in combinatoric topological strings", *J. High Energy Phys.* **2022**:1 (2022), art. id. 071, 56 pp. MR

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

[30] H. N. Nguyen and A. Maróti, "p-regular conjugacy classes and p-rational irreducible characters", *J. Algebra* **607** (2022), 387–425. MR

[31] A. Padellaro, R. Radhakrishnan, and S. Ramgoolam, "Row-column duality and combinatorial topological strings", *J. Phys. A* **57**:6 (2024), art. id. 065202, 68 pp. MR

[32] S. Ramgoolam and E. Sharpe, "Combinatoric topological string theories and group theory algorithms", *J. High Energy Phys.* **2022**:10 (2022), art. id. 147, 56 pp. MR

[33] C. A. Schroeder, "Finite groups with many p-regular conjugacy classes", *J. Algebra* **641** (2024), 716–734. MR

[34] A. Vera López and J. Vera López, "Classification of finite groups according to the number of conjugacy classes", *Israel J. Math.* **51**:4 (1985), 305–338. MR

[35] E. Witten, "Quantum field theory and the Jones polynomial", pp. 239–329 in *Braid group, knot theory and statistical mechanics*, Advanced Series in Mathematical Physics **9**, World Sci. Publ., Teaneck, NJ, 1989. MR

Received December 3, 2025. Revised April 26, 2026.

CHRISTOPHER A. SCHROEDER
DEPARTMENT OF MATHEMATICS AND STATISTICS
BINGHAMTON UNIVERSITY
BINGHAMTON, NY 13902-6000
UNITED STATES

cschroe2@binghamton.edu

HUNG P. TONG-VIET
DEPARTMENT OF MATHEMATICS AND STATISTICS
BINGHAMTON UNIVERSITY
BINGHAMTON, NY 13902-6000
UNITED STATES

htongvie@binghamton.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

EDITORS

Don Blasius (Managing Editor)
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
blasius@math.ucla.edu

Matthias Aschenbrenner
Fakultät für Mathematik
Universität Wien
Vienna, Austria
matthias.aschenbrenner@univie.ac.at

Vyjayanthi Chari
Department of Mathematics
University of California
Riverside, CA 92521-0135
chari@math.ucr.edu

Atsushi Ichino
Department of Mathematics
Kyoto University
Kyoto 606-8502, Japan
atsushi.ichino@gmail.com

Kefeng Liu
School of Sciences
Chongqing University of Technology
Chongqing 400054, China
liu@math.ucla.edu

Sucharit Sarkar
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
sucharit@math.ucla.edu

Dimitri Shlyakhtenko
Department of Mathematics
University of California
Los Angeles, CA 90095-1555
shlyakht@ipam.ucla.edu

Ruixiang Zhang
Department of Mathematics
University of California
Berkeley, CA 94720-3840
ruixiang@berkeley.edu

PRODUCTION

Silvio Levy, Scientific Editor, production@msp.org

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2026 is US $710/year for the electronic version, and $965/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2026 Mathematical Sciences Publishers

PACIFIC JOURNAL OF MATHEMATICS

Volume 344 No. 1 September 2026

Minimal rational graphs admitting a $\mathbb{Q}$HD smoothing 1
MÁRTON BEKE

Iwahori–Hecke model for the universal supersingular representation 27
ANAND CHITRAO and ASFAK SONEJI

The canonical exact sequence of differential modules for 0-dimensional schemes 47
TRAN N. K. LINH and LE NGOC LONG

On the measure of primitive representations of an integer by a quadratic form 69
MANABU MURATA

Group topologies on groups of absolutely bicontinuous homeomorphisms 103
J. DE LA NUEZ GONZÁLEZ

Adjunction inequality for spatially refined s-invariants 145
QIUYU REN

On the invariants of finite groups arising in a topological quantum field theory 151
CHRISTOPHER A. SCHROEDER and HUNG P. TONG-VIET

From brick manifolds to Grassmannians of bimodules 183
EVGENY FEIGIN and MARKUS REINEKE

On mixed curvature for Hermitian manifolds 201
KAI TANG

The size of a set from the size of its countable power set 219
WILLIAM CHAN