Complex group algebras of finite groups: Brauer's Problem 1

by

Alexander Moretó
Departament d'Àlgebra
Universitat de València
46100 Burjassot. València. SPAIN
E-mail: Alexander.Moreto@uv.es

Abstract. Brauer's Problem 1 asks the following: what are the possible complex group algebras of finite groups? It seems that with the present knowledge of representation theory it is not possible to settle this question. The goal of this paper is to present a partial solution to this problem. We conjecture that if the complex group algebra of a finite group does not have more than a fixed number m of isomorphic summands, then its dimension is bounded in terms of m. We prove that this is true for every finite group if it is true for the symmetric groups. The problem for symmetric groups reduces to an explicitly stated question in number theory or combinatorics.

2000 Mathematics Subject Classification: Primary 20C15; Secondary 11P83, 20C30, 20C33

Research partially supported by the FEDER, the Spanish Ministerio de Educación y Ciencia and Programa Ramón y Cajal.

1 Introduction

Let G be a finite group and $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ the set of irreducible characters of G. Put $\chi_i(1) = n_i$. Following B. Huppert [13], we say that $(n_1, \ldots, n_k)$ is the **degree pattern** of G. In recent years much information has been obtained on the possible sets of character degrees of finite groups, especially in the solvable case (even though a complete classification of such sets seems to be very far). However, as pointed out by Huppert, almost nothing is known about Brauer's Problem 1 (see [2]), which asks the following: What are the possible degree patterns of finite groups? (This problem also appears as Question 6.9 of [13] and as Question 1 of [12].) It was mentioned in [13] that the only known restrictions are the obvious ones, namely that the number of $n_i = 1$ has to divide $\sum_{i=1}^{k} n_i^2$ and that each n_i has to divide $\sum_{i=1}^{k} n_i^2$. As is well-known, if $(n_1, \ldots, n_k)$ is the degree pattern of G, the complex group algebra of G is $\mathbb{C}G = \bigoplus_{i=1}^{k} \mathrm{M}_{n_i}(\mathbb{C})$. So knowing the possible degree patterns of finite groups is equivalent to knowing the possible isomorphism types of complex group algebras.

Even though we think that with the present knowledge of representation theory it is not possible to settle Brauer's Problem 1, we think that it is possible to obtain significant restrictions on the structure of the complex group algebras. The goal of this paper is to provide the first such restriction. For the sake of discussion, we state the following.

Conjecture A. *The $\mathbb{C}$-dimension of the complex group algebra of any finite group G is bounded in terms of the maximum number of isomorphic summands in the decomposition $\mathbb{C}G = \bigoplus_{i=1}^{k} \mathrm{M}_{n_i}(\mathbb{C})$.*

In other words, Conjecture A says that the order of a finite group is bounded in terms of the largest multiplicity of its character degrees. Our main results are the following. As usual, we say that a quantity is $(a_1, \ldots, a_l)$-bounded if it is bounded by some real valued function that depends on $a_1, \ldots, a_l$.

Theorem B. *Conjecture A holds for every finite group if it holds for the symmetric groups.*

Theorem C. *Let G be a finite group and assume that G does not contain an alternating group bigger than $\mathrm{Alt}(t)$ as a composition factor. If the largest multiplicity of a character degree is m, then the order of G is (m, t)-bounded.*

Unfortunately, we have been unable to prove that Conjecture A holds for the symmetric groups. This seems to be a difficult number theoretical problem that will be discussed in Section 5. We describe it in an elementary way in purely combinatorial terms; so that any reader will be able to understand it and think about it. Note that an immediate consequence of Theorem C is that Conjecture A holds for solvable groups. (Actually, we prove this result in our way toward a proof of Theorems B and C.) Some possible generalizations of these results in different directions will be discussed in Section 6.

Following our proof, it would be possible to give explicit bounds in Theorem C. However, we think that this would just increase the technicality of the paper so we have not considered convenient to express these functions or to try to obtain the best possible bounds.

I thank M. Isaacs, A. Jaikin-Zapirain, G. Malle, J. Sangroniz and B. Srinivasan for helpful conversations. Most of this work was done while I was visiting the University of Wisconsin, Madison, during the Fall of 2002. I would like to take this opportunity to thank the Mathematics Department for its hospitality. The results in this paper have been announced in [22]

2 Solvable groups

We begin work toward a proof of Conjecture A for solvable groups. We need several lemmas. In the first of them, we show that the number of primes that divide the order of a solvable group that satisfies the hypothesis is bounded. It is an application of results and ideas from [6].

Lemma 2.1. *Let G be a solvable group with at most m irreducible characters of each degree and let p be a prime divisor of $|G|$. Then p is m-bounded.*

Proof. We may assume that $p \geq 1 + m^m$. Since the hypothesis is inherited by quotient groups, we may assume without loss of generality that G is a semidirect product of a p'-group $H > 1$ and a minimal normal p-subgroup V, on which H acts faithfully.

Since G has at most m irreducible characters of any given degree, we have that $[\mathbb{Q}(\chi) : \mathbb{Q}] \leq m$ for any $\chi \in \mathrm{Irr}(G)$. (Otherwise, the Galois conjugates of χ would provide more than m characters of degree $\chi(1)$.) In particular, $[\mathbb{Q}(\chi) \cap \mathbb{Q}_p : \mathbb{Q}] \leq m$. (Here $\mathbb{Q}_p = \mathbb{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity.) For every divisor d of $p-1$ there is a unique intermediate field of the extension $\mathbb{Q}_p/\mathbb{Q}$ that is an extension of $\mathbb{Q}$ of degree d. We have seen that the extensions $\mathbb{Q}(\chi) \cap \mathbb{Q}_p/\mathbb{Q}$ have degree at most m, so $[K : \mathbb{Q}] \leq m^m$, where K is the field of values of the whole character table at the p-elements of G. Hence $k = [\mathbb{Q}_p : K]$ is a divisor of $p-1$ bigger than or equal to $(p-1)/m^m$.

For any $n \in V$, $\sigma \in \mathrm{Gal}(\mathbb{Q}_p/K)$ and $\chi \in \mathrm{Irr}(G)$ we have that $\chi(n) = \chi^\sigma(n)$. Also, $\chi(n) = \varepsilon_1 + \cdots + \varepsilon_t$ where ε_j is a pth root of unity for every j

and

$$\chi^\sigma(n) = \varepsilon_1^i + \cdots + \varepsilon_t^i = \chi(n^i)$$

for some i. But as σ runs over $\mathrm{Gal}(\mathbb{Q}_p/K)$, i runs over the subgroup of order $k = [\mathbb{Q}_p : K]$ of C_{p-1}. Therefore we have that $\chi(n) = \chi(n^i)$ for every $\chi \in \mathrm{Irr}(G)$ and every i in this subgroup. So for all such i, n and n^i are G-conjugate and we have that the action of H on V has the k-eigenvalue property (see Definition 2.8 of [6]).

We have that V is an irreducible $\mathrm{GF}(p)H$-module and let X be the corresponding irreducible $\mathrm{GF}(p)$-representation. Let F be an algebraic closure of $\mathrm{GF}(p)$. Let ψ be the F-character corresponding to the F-representation X^F. By Theorem 9.21 of [16], the characters that appear in the decomposition of ψ as a sum of irreducible F-characters have the same degree. Now, let ϕ be the p-Brauer character of H corresponding to ψ and note that it decomposes as a sum of irreducible Brauer characters of the same degree. Since p does not divide the order of H, we have that the set of (irreducible) Brauer characters coincides with the set of (irreducible) ordinary complex characters (by Theorem 15.13 of [16]), so using the hypothesis we conclude that ϕ is a sum of at most m irreducible ordinary characters. In particular, $[\mathbb{Q}(\phi) : \mathbb{Q}] \leq m^m$. Now, we can apply Theorem 2.9 of [6] to conclude that either $p \leq \sqrt{3}m^m$ or $\mathbb{Q}(\phi)$ contains a primitive $k/(4,k)$th root of unity. In the first case we are done and in the second case we deduce that $\varphi(k/(4,k)) \leq m^m$. Thus k is bounded in terms of m and it follows from the second paragraph of the proof that p is bounded in terms of m. $\square$

Given a group G, we write $\mathrm{cd}(G)$ to denote the set of degrees of the irreducible characters of G.

Lemma 2.2. *Let G be a finite group with at most m irreducible characters of each degree. Then $|G : G^{(i)}| \leq m^{4^i}$ for all i.*

Proof. We argue by induction on i. Since $\mathrm{Irr}(G/G')$ is the group of linear characters of G, we deduce that $|G : G'| \leq m \leq m^4$. Assume that $i > 1$ and $|G : G^{(i-1)}| \leq m^{4^{i-1}}$. By Ito's theorem (Theorem 6.15 of [16]) the degrees of the characters of $G/G^{(i)}$ divide $|G : G^{(i-1)}| \leq m^{4^{i-1}}$, so we conclude that $|\mathrm{cd}(G/G^{(i)})| \leq m^{4^{i-1}}$ and that the largest degree of the irreducible characters of $G/G^{(i)}$ is $b(G/G^{(i)}) \leq m^{4^{i-1}}$. Using the hypothesis and the degrees equation we have that

$$|G : G^{(i)}| \leq m \cdot m^{4^{i-1}} \cdot (m^{4^{i-1}})^2 \leq m^{4^i},$$

as desired. $\square$

We also need the following result. If a group G acts on a module V, we write $r(G, V)$ to denote the number of orbits of this action. We say that a finite module V for a group G has mixed characteristic if V is an abelian group all of whose Sylow subgroups are elementary abelian groups. For a solvable group G, we write $\mathrm{dl}(G)$ to denote the derived length of G.

Theorem 2.3. *Let G be solvable and let V be a finite faithful completely reducible G-module (possibly in mixed characteristic). Then there exist constants C_1 and C_2 such that*

$$\mathrm{dl}(G) \leq C_1 \log\log r(G,V) + C_2.$$

Proof. This immediate consequence of Theorem 2.4 of [18] appears as Theorem 7.2 of [23] □

Finally, we need the following result, which is the nilpotent case of Conjecture A.

Theorem 2.4. *Let G be a nilpotent group and assume that the largest multiplicity of a character degree is m. Then $|G|$ is m-bounded.*

Proof. This is Corollary 1.12 of [17]. Following that proof it is possible to give an explicit bound. □

Now, we are ready to prove Conjecture A for solvable groups.

Theorem 2.5. *Let G be a solvable group and assume that the largest multiplicity of a character degree is m. Then $|G|$ is m-bounded.*

Proof. First, assume that the derived length of the quotient by the Fitting subgroup of any group that satisfies the hypothesis of the theorem does not exceed a fixed integer s. Then Lemma 2.2 yields that $|G : F(G)| \leq m^{4^s}$. Now we claim that $F(G)$ does not have more than $m^{2\cdot 4^s+1}$ characters of any given degree. Assume not. Then $F(G)$ has more than $m^{2\cdot 4^s+1}$ irreducible characters of some given degree d. The number of G-conjugates of any such character is at most m^{4^s} , so we deduce that the number of G-orbits of irreducible characters of $F(G)$ of degree d is bigger than

$$m^{2\cdot 4^s+1}/m^{4^s} = m^{4^s+1}.$$

For any such G-orbit there is at least one irreducible character of G lying over the members of the orbit, i.e., the number of irreducible characters of G lying over characters of degree d of $F(G)$ is bigger than m^{4^s+1}. Now, we can use Corollary 11.29 of [16] do deduce that the degree of any such character is $d \cdot c$, where c is some divisor of $|G : F(G)|$. In particular, the number of possible degrees for these characters does not exceed m^{4^s}. We conclude that G has more than

$$m^{4^s+1}/m^{4^s} = m$$

irreducible characters of the same degree. This contradiction proves our claim. By Theorem 2.4, we have that $|F(G)|$, and hence $|G|$, is bounded in terms of m.

This means that if the theorem is false, then we can find a group G that satisfies the hypothesis and whose quotient by the Fitting subgroup has arbitrarily large derived length n. Write $H = G/F(G)$. It is clear that H satisfies the hypothesis of the theorem. Using Lemma 2.2, we deduce that $|H : H^{(i)}| \leq m^{4^i}$ for every $i > 0$. Since H acts faithfully and completely reducibly on $\mathrm{Irr}(F(G)/\Phi(G))$ (by Satz III.4.2 and III.4.5 of [11]), we can use Theorem 2.3 to deduce that H has at least $\exp(\exp(\frac{n-C_2}{C_1}))$ orbits on $\mathrm{Irr}(F(G)/\Phi(G))$, for some constants $C_1, C_2 > 0$.

The degree of any character of G that lies over a character of $F(G)/\Phi(G)$ divides $|G : F(G)| = |H| \leq m^{4^n}$. Write $|H| = p_1^{a_1} \dots p_t^{a_t}$ as a product of powers of different primes. We have that the number of divisors of $|H|$ is

$$\begin{aligned} d(|H|) &= (a_1+1)\dots(a_t+1) \leq 2^t a_1 \dots a_t \leq 2^t (\log_2 m^{4^n})^t \\ &\leq (2 \cdot 4^n \log_2 m)^{f(m)}, \end{aligned}$$

where we have used that by Lemma 2.1, $t \leq f(m)$ for some function f.

Since different H-orbits of characters of $F(G)/\Phi(G)$ lie under different characters of G, we deduce that the multiplicity of some character degree of G is at least $\exp(\exp(\frac{n-C_1}{C_2}))/(2 \cdot 4^n \log_2 m)^{f(m)}$. Observe that this quotient goes to infinity as n goes to infinity. Since n is arbitrarily large, it follows that we can make the multiplicity of some character degree to be larger than m. This contradiction completes the proof of the theorem. □

3 Groups of Lie type

In this section we prove that Conjecture A holds for simple groups of Lie type. We will present a proof, due to G. Malle, that gives pretty good explicit bounds. We will give the proof in a series of lemmas.

Lemma 3.1. *Let $s \in \mathrm{GL}(n, \overline{\mathbb{F}}_q)$ be semisimple. Then s is conjugate to at most $n!$ of its powers. If moreover all eigenvalues of s are powers of one among them, then s is conjugate to at most n of its powers.*

Proof. Without loss of generality, we may assume that s is of diagonal form. Clearly, any conjugate of s has the same eigenvalues, and all powers are again diagonal. The first assertion follows.

In the second case, the image of the generating eigenvalue already determines the image of all eigenvalues. There are at most n possibilities for this image. $\square$

Lemma 3.2. *The group* $\mathrm{GL}(n,q)$ *contains a semisimple element* s *of order* q^n-1 *all of whose eigenvalues are powers of one among them.*

Proof. Choose an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. This defines an action of the multiplicative group of $\mathbb{F}_{q^n}$ on $\mathbb{F}_q^n$ (via multiplication). Let ζ be a generator of $\mathbb{F}_{q^n}^\times$. Then the image of ζ in $\mathrm{GL}(n,q)$ has order q^n-1 and its eigenvalues are $\zeta, \zeta^q, \zeta^{q^2}, \ldots$. $\square$

Lemma 3.3. *Let* $G = \mathrm{SL}(n,q), \mathrm{SU}(n,q), \mathrm{Sp}(2n,q), \mathrm{SO}(2n{+}1,q), \mathrm{SO}^+(2n,q), \mathrm{SO}^-(2n,q)$. *Then* G *contains a semisimple element of order* $(q^n-1)/(q-1), q^{[n/2]}-1, q^n-1, q^n-1, q^n-1, q^{n-1}-1$ *conjugate to at most* $n, n, 2n, 2n+1, 2n, 2n$ *of its powers.*

Proof. For $\mathrm{SL}(n,q)$ take the $(q-1)$st power of the element of $\mathrm{GL}(n,q)$ constructed in the proof of Lemma 3.2.

For $\mathrm{SU}(n,q)$ use the embeddings $\mathrm{GL}([n/2],q) \leq \mathrm{SU}(n,q) \leq \mathrm{GL}(n,q^2)$ together with Lemmas 3.1 and 3.2. Similarly, in the remaining cases use the embeddings $\mathrm{GL}(n,q) \leq \mathrm{Sp}(2n,q) \leq GL(2n,q)$, $\mathrm{GL}(n,q) \leq \mathrm{SO}(2n+1,q) \leq \mathrm{GL}(2n+1,q)$, $\mathrm{GL}(n,q) \leq \mathrm{SO}^+(2n,q) \leq \mathrm{GL}(2n,q)$ and $\mathrm{GL}(n-1,q) \leq \mathrm{SO}^-(2n,q) \leq \mathrm{GL}(2n,q)$. (The first embedding is clear from the Dynkin diagram, see p. 40 of [4], for instance, or alternatively it is the stabilizer of a maximal totally isotropic subspace. The second embedding is obvious.) $\square$

Corollary 3.4. *Let* $G = \mathrm{PSL}(n,q), \mathrm{PSU}(n,q), \mathrm{PSp}(2n,q), \mathrm{PSO}(2n+1,q), \mathrm{PSO}^+(2n,q), \mathrm{PSO}^-(2n,q)$. *Then* G *contains a semisimple element of order at least* $(q^n-1)/n(q-1), (q^{[n/2]}-1)/n, (q^n-1)/2, (q^n-1)/2, (q^n-1)/2, (q^{n-1}-1)/2$ *conjugate to at most* $n, n, 2n, 2n+1, 2n, 2n$ *of its powers.*

Proof. Take the image of s from Lemma 3.3. $\square$

Now, we can prove the main result for the classical groups of Lie type.

Theorem 3.5. *Let* $G = \mathrm{PSL}(n,q), \mathrm{PSU}(n,q), \mathrm{PSp}(2n,q), \mathrm{PSO}(2n+1,q), \mathrm{PSO}^+(2n,q), \mathrm{PSO}^-(2n,q)$. *Then the largest multiplicity of the character degrees of* G *is at least* $\varphi(q^n-1)/n^2(q-1), \varphi(q^{[n/2]}-1)/n^2, \varphi(q^n-1)/4n, \varphi(q^n-1)/2(2n+1), \varphi(q^n-1)/4n, \varphi(q^{n-1}-1)/4n$.

Proof. Let $\tilde{G}$ be the corresponding group of simply connected type; so $\tilde{G} = \mathrm{SL}(n,q), \mathrm{SU}(n,q), \ldots, \mathrm{Spin}^-(2n,q)$ and $G = \tilde{G}/Z(\tilde{G})$. Let $\tilde{G}^*$ be the dual group of $\tilde{G}$. By Corollary 3.4, the derived group $(\tilde{G}^*)'$ contains a certain semisimple element s. By the Deligne-Lusztig theory, to s is associated the semisimple character χ_s of $\tilde{G}$ (see Section 8.4 of [3]), an irreducible character of $\tilde{G}$ which has $Z(\tilde{G})$ in its kernel (since $s \in (\tilde{G}^*)'$). Thus it is a character of G. Each conjugacy class of semisimple elements in $\tilde{G}^*$ defines a different character. The degree only depends on $|C_{\tilde{G}}(s)|$ (see Theorem 8.4.8 of [3]). Thus all primitive powers of s give characters of the same degree. Now, the result follows from Corollary 3.4. □

Theorem 3.6. *Conjecture A holds for simple groups of Lie type.*

Proof. For classical groups, this follows easily from Theorem 3.5 using the fact that for any $\varepsilon > 0$, $\varphi(k)/k^{1-\varepsilon} \to \infty$ when $k \to \infty$ (see Theorem 327 of [10]).

For exceptional groups, we can use, for example, that $(P)\,\mathrm{SL}(2,q) \leq G(q)$ for $G(q)$ of exceptional type different from ${}^2B_2(q)$ (see Dynkin diagram) and $G(q) \leq \mathrm{GL}(a,q)$ for some small a. For instance, $(P)\,\mathrm{SL}(2,q) \leq E_8(q) \leq \mathrm{GL}(248,q)$ (see p. 43 of [4]). Now, argue as in the proof of Lemma 3.3 using the first part of Lemma 3.1 to get that $E_8(q)$ contains a semisimple element of order $(q-1)/2$ conjugate to at most $(248)!$ of its powers. Now, argue as in the proof of Theorem 3.5.

Finally, we consider the groups ${}^2B_2(q)$. It is well-known that they have $(q-2)/2$ characters of degree q^2+1 (see Theorem XI.5.10 of [14]). The result follows. □

Much better bounds could be obtained for the exceptional groups with a little more work.

4 Arbitrary groups

In order to prove Theorems B and C, we need two lemmas. The first one is a non-trivial number-theoretic result. Given an integer n, we write $d(n)$ to denote the number of divisors of n.

Lemma 4.1. (i) *If $\varepsilon > 0$, then $d(n) < 2^{(1+\varepsilon)\log n/\log\log n}$ for all $n > n_0(\varepsilon)$*

(ii)
$$\lim_{n\to\infty} \frac{d(n!)}{2^{\frac{c\log n!}{(\log\log n!)^2}}} = 1,$$

where c is some constant.

Proof. The first part is Theorem 317 of [10]. The second part is in [5]. □

We need one more lemma on the characters of the simple groups.

Lemma 4.2. *Let S be a finite simple group. Then there exist a non-principal irreducible character of S that extends to* $\mathrm{Aut}(S)$.

Proof. If S is an alternating group on n letters for $n \neq 6$, a sporadic group or the Tits group ${}^2F_4(2)'$, then $|\operatorname{Out}(S)| \leq 2$, so we may assume that $|\operatorname{Out}(S)| = 2$. If the only character of S that extends to $\mathrm{Aut}(S)$ is the principal character, then we would have that the multiplicity of any character degree other than 1 of S is even. Using the degree equation, we would have that the order of S is odd, a contradiction.

Finally, we may assume that S is a simple group of Lie type (note that $A_6 \cong L_2(9)$ is of Lie type). In this case, it is well-known that the p-Steinberg character of S, where p is the defining characteristic, extends to $\mathrm{Aut}(S)$ (see [7]). □

Before proceeding to prove Theorems B and C we state the following result.

Theorem 4.3. *Let G be a permutation group on a set Ω of cardinality k and assume that G does not contain any alternating group bigger than* $\mathrm{Alt}(t)$ *as a composition factor. Then the number of orbits of G on the power set $\mathcal{P}(\Omega)$ is at least $a^{k/t}$ where $a > 1$ is some constant.*

Proof. This appears in [1] □

Proof of Theorem C. Let $O_\infty(G)$ be the largest normal solvable subgroup of G. Using Theorem 2.5 and Clifford theory, it is easy to see that it suffices to prove that $|G : O_\infty(G)|$ is (m,t)-bounded. Since $G/O_\infty(G)$ satisfies the hypotheses of the theorem, we may assume without loss of generality that $O_\infty(G) = 1$.

Thus the generalized Fitting subgroup $F^*(G)$ is a direct product of minimal normal subgroups of G, each of which is a direct product of non-abelian simple groups. Since $C_G(F^*(G)) = 1$, G embeds into $\mathrm{Aut}(F^*(G))$ and we have that in order to bound $|G|$, it is enough to bound $|F^*(G)|$.

First, we want to prove that the number of times that a given simple group S appears as a direct factor of $F^*(G)$ is m-bounded. Let N be a normal subgroup of G isomorphic to the direct product of k copies of a non-abelian simple group S. We will bound k in terms of m. We have that $G/C_G(N)$ embeds into $\mathrm{Aut}(N) \cong \mathrm{Aut}(S) \wr S_k$. Put $H = G/C_G(N)$ and view this group as a subgroup of $\mathrm{Aut}(S) \wr S_k$. Let $B = H \cap \mathrm{Aut}(S)^k$ and note that H/B is a permutation group on k letters. Fix a non-linear character

$\varphi \in \mathrm{Irr}(S)$ that extends to $\mathrm{Aut}(S)$ (it exists by Lemma 4.2). Note that the hypotheses of Theorem 4.3 hold. It follows from this result that for some s, the number of orbits of H/B on the subsets of cardinality s is at least $a^{k/t}/(k+1)$. Considering the characters of B that extend products of s copies of φ and $k-s$ copies of the principal character of S, we deduce that there are at least $a^{k/t}/(k+1)$ H-orbits of characters of B of the same degree. Using Corollary 11.29 of [16], it follows that H (and hence G) has at least $a^{k/t}/(k+1)d(k!)$ characters of the same degree. Using part (ii) of Lemma 4.1 and Stirling's formula, one can see that this quotient goes to infinity as k goes to infinity. It follows that k has to be bounded in terms of m.

Next, we prove that the order of each of the simple groups S that appears in $F^*(G)$ is bounded in terms of t and m. By hypothesis and the classification of finite simple groups, we may assume that S is a group of Lie type. We want to bound $|S|$ in terms of m. We will write $N = S \times \cdots \times S$ to denote a minimal normal subgroup of G that contains S and more generally we will also use the same notation of the preceding paragraph. By Schreier's conjecture, B/N (which is isomorphic to a subgroup of $\mathrm{Out}(S)^k$) is solvable. If its order were not m-bounded, then it would have arbitrarily many characters of the same degree and since $|H : B|$ is m-bounded, the same would happen with H. Therefore $|B : N|$ is m-bounded, so $|H : N|$ is m-bounded. Using Theorem 3.6, we have that if $|S|$ is not m-bounded, then S would have arbitrarily many characters of the same degree. Hence, the same happens with N and, since $|H : N|$ is m-bounded, the same would happen with H, a contradiction. We conclude that $|S|$ is m-bounded, as desired. This completes the proof. □

Now, Theorem B will be an immediate consequence of the following lemma. Given a group G, we write $m(G)$ to denote the largest multiplicity of the character degrees of G.

Lemma 4.4. *Assume that* $\mathrm{Alt}(t)$ *is a composition factor of a finite group* G *for some* $t > 6$. *Then*

$$m(G) \geq m(\mathrm{Alt}(t))/4.$$

Proof. Let M/N be a chief factor of G that is a direct product of copies of $\mathrm{Alt}(t)$. We may assume, without loss of generality, that $N = 1$. Also, we may assume that $C_G(M) = 1$. Therefore, G is isomorphic to a subgroup of $\Gamma = S_t \wr S_k$, where k is the number of copies of $\mathrm{Alt}(t)$ in M. We will view G as a subgroup of Γ.

Fix an integer d such that $\mathrm{Alt}(t)$ has $m(\mathrm{Alt}(t))$ characters of degree d. Let $\psi_i \in \mathrm{Irr}(\mathrm{Alt}(t))$ with $\psi_i(1) = d$ for $i = 1, \ldots, m(\mathrm{Alt}(t))$. For $i = 1, \ldots, m(\mathrm{Alt}(t))$, let $\theta_1 = \psi_i \times \cdots \times \psi_i$. Assume first that at least one-half of the characters ψ_i extend to S_t. Let $\varphi \in \mathrm{Irr}(S_t)$ be one such extension. We have that $\varphi \times \cdots \times \varphi \in \mathrm{Irr}((S_t)^k)$ is Γ-invariant so by [20], for instance, it extends to Γ and therefore to G. In this way we obtain at least $m(\mathrm{Alt}(t))/2$ of the characters θ_i extend to G, so $m(G) \geq m(\mathrm{Alt}(t))/2$.

Now, we may assume that at least $m(\mathrm{Alt}(t))/2$ of the characters ψ_i do not extend to S_t. Let ψ_i be one of these characters. Then we have that $T = I_\Gamma(\theta_i) = \mathrm{Alt}(t) \wr S_k$. Using [20] again, we see that θ_i extends to its inertia group. Furthermore, we have that $I_G(\theta_i) = T \cap G$ does not depend on θ_i. Using Clifford theory, we can find characters $\chi_i \in \mathrm{Irr}(G|\theta_i)$ of the same degree. It is clear that any of the characters θ_i cannot have more than two G-conjugates and we conclude that the number of different characters among the χ_i's is at least $m(\mathrm{Alt}(t))/4$. This completes the proof of the lemma. □

Proof of Theorem B. We are assuming that Conjecture A holds for the symmetric groups. We want to prove that it holds for every finite group. Since for every t, $\mathrm{Alt}(t)$ is a normal subgroup of the symmetric group of degree t of index 2, we may assume that Conjecture A holds for the alternating groups (using Clifford's theory). By Theorem C, it suffices to see that if $\mathrm{Alt}(t)$ is the largest alternating group that appears as a composition factor of G, then t is m-bounded. This follows from the assumption that Conjecture A holds for alternating groups and Lemma 4.4 □

5 Symmetric groups

There is a well-known formula for the character degrees of the symmetric group. As was proved by A. Young at the beginning of the 20th century there is a nice correspondence between the irreducible characters of the symmetric group S_n and the partitions of n. Given a partition of n, $\mu = (a_1, \ldots, a_t)$, with $a_1 \geq a_2 \geq \cdots \geq a_t$, the Young diagram associated to μ is an array of n nodes with a_i nodes in the ith row. We assign numbers to the rows and columns and coordinates to the nodes. The *hook number* $H(i,j)$ of the node (i,j) is the number of nodes to the right and below the node (i,j), including the node (i,j). The degree of the character χ_μ associated to the partition μ is given by the *hook length formula*

$$\chi_\mu(1) = \frac{n!}{\prod_{i,j} H(i,j)}.$$

This description of the degrees was obtained by J. Frame, G. de B. Robinson and R. Thrall in [8].

So our Conjecture A reduces to the following problem. Given a partition μ of an integer n, let

$$P(\mu) = \prod_{i,j} H(i,j)$$

be the product of the hook numbers and

$$M(n) = \max_{m \geq 1} \#\{\mu \in \mathrm{Part}(n) \mid P(\mu) = m\}$$

be the maximum number of partitions of n with the same product of hook numbers. Conjecture A is now equivalent to the following.

Conjecture A′. *$M(n) \to \infty$ as $n \to \infty$.*

The first few values of $M(n)$ are given in the following graphic, where we have joined the dots between the different integers.

Figure 1: The function $M(n)$.

It seems clear from the graphic that this wants to be an increasing function but it is also clear that this function is far from being weakly monotonic. It would also be interesting to prove weaker results, like that $\limsup M(n) = \infty$.

6 Further comments

We begin with an application of Theorem C that might have some application in the context of [21]. We recall that a group G is an M_l-group if every irreducible character is induced from a character of degree at most l of some subgroup of G.

Corollary 6.1. *Let G be an M_l-group for some integer l. If the largest multiplicity of any character degree of G is m, then the order of G is (m, l)-bounded.*

Proof. By Proposition 4.1 of [21] (which is an easy consequence of Jordan's theorem on linear groups and results of Isaacs [15]), we have that G does not contain (as a composition factor) an alternating group bigger that $\mathrm{Alt}(cl)$ for some constant c. The result follows from Theorem C. $\square$

Our results indicate that a large group has some character degree that occurs with large multiplicity. For solvable groups, it might be true that the average multiplicity of the character degrees of a large group is large. More precisely, we ask the following, where $k(G)$ is the number of conjugacy classes of G and $\mathrm{cd}(G) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$.

Question 1. *Let G be a solvable group. Is it true that $k(G)/|\,\mathrm{cd}(G)| \to \infty$ as $|G| \to \infty$?*

In p. 249 of [24], L. Pyber asked whether there exists an infinite sequence of p-groups of increasing order such that $k(P) \leq c \log_p |P|$ for some constant $c = c(p)$. It is easy to see that an affirmative answer to Question 1 for p-groups follows from a negative answer to Pyber's question. In fact, as the following result shows, Question 1 is equivalent to Pyber's question in the p-group case. This result is due to Jaikin-Zapirain.

Theorem 6.2. *Let P be a group of order p^m. Then*

$$k(P) \geq Ckp^{m/k},$$

where $k = |\operatorname{cd}(P)|$ and C is a positive constant. In particular, an affirmative answer to Question 1 implies a negative answer to Pyber's question.

Proof. Let $\operatorname{cd}(P) = \{1 = p^{a_0}, p^{a_1}, \ldots, p^{a_{k-1}}\}$. Let $\{P_i\}_{i=1}^k$ be a descending series of normal subgroups of P such that $|P : P_i| = p^{2a_i}$ for $i < k$ and $P_k = 1$. Put $|P : P_i| = p^{b_i}$ for $i = 0, \ldots, k$. Note that the degree of the characters of P/P_i does not exceed $p^{a_{i-1}}$, so

$$\begin{aligned} |P/P_i| &= \sum_{\chi \in \operatorname{Irr}(P/P_{i-1})} \chi(1)^2 + \sum_{\chi \in \operatorname{Irr}(P/P_i|P/P_{i-1})} \chi(1)^2 \\ &\leq |P/P_{i-1}| + p^{2a_{i-1}}(|\operatorname{Irr}(P/P_i)| - |\operatorname{Irr}(P/P_{i-1})|) \\ &= |P/P_{i-1}| + p^{2a_{i-1}}(k(P/P_i) - k(P/P_{i-1})), \end{aligned}$$

where $\operatorname{Irr}(P/P_i|P/P_{i-1})$ is the set of irreducible characters of P/P_i whose kernel does not contain P/P_{i-1}. Now, we have that

$$p^{b_i} - p^{b_{i-1}} = |P/P_i| - |P/P_{i-1}| \leq p^{2a_{i-1}}(k(P/P_i) - k(P/P_{i-1}))$$

and it follows that

$$k(P/P_i) - k(P/P_{i-1}) \geq p^{b_i - b_{i-1}} - 1 \geq Cp^{b_i - b_{i-1}}.$$

Adding for $i = 1, \ldots, k$ and using the fact that the multiplicative mean does not exceed the arithmetic mean, we conclude that

$$k(P) \geq C \sum_{i=1}^{k} p^{b_i - b_{i-1}} \geq Ck(p^{\sum_{i=1}^{k}(b_i - b_{i-1})})^{1/k} = Ckp^{m/k},$$

as desired.

Now, assume that Pyber's question has an affirmative answer. We will show that this implies that our question has a negative answer. We have a sequence of groups of increasing order $\{P_m\}$ with $|P_m| = p^m$ and $k(P_m) \leq Dm$ for some constant D. Let $k_m = |\operatorname{cd}(P_m)|$. then

$$Ck_m p^{m/k_m} \leq k(P_m) \leq Dm$$

so $(k_m/m)p^{(m/k_m)} \leq D/C$ is bounded by a constant, and so is m/k_m. Since $k(P_m) \leq Dm$, this would yield that our question has a negative answer, as we wanted to prove. $\square$

Using MAGMA, we have checked that $1.75 \leq k(S_n)/|\operatorname{cd}(S_n)| \leq 2.525$ for all $5 \leq n < 55$ and that this function is far from being monotonic (at least for these small values of n). This might indicate that the asymptotic behaviour of the number of character degrees of the symmetric groups is similar to that of the number of partitions, but it would be interesting to confirm this.

When this paper was in the final stages of its preparation, we received a preprint of M. Liebeck and A. Shalev [19] were they prove that $k(G)/|\operatorname{cd}(G)| \to \infty$ when $|G| \to \infty$ for groups G of Lie type.

A more difficult question would be the following. Is it true that if G is solvable then $k(G)/d(|G|) \to \infty$ as $|G| \to \infty$? This is a reformulation of Pyber's question in the p-group case. This is true, for instance, for the exceptional groups of Lie type. In fact, we can prove a bit more.

Given a group G, $k^*(G)$ denotes the number of orbits of elements of G under the action of $\operatorname{Aut}(G)$.

Lemma 6.3. *The following holds:*

$$\frac{k^*(S)}{d(|\operatorname{Aut}(S)|)} \to \infty \quad \text{as } S = G_l(q) \text{ is a simple group of Lie type and } q \to \infty.$$

Proof. Let S be a simple group of Lie type of rank l over the field with q elements. It was proved in Lemma 4.2 of [24] that if $l \leq 4$, then $k^*(S) \geq q^{l/2}/120 \log q$ and that if $l > 4$, then $k^*(S) \geq q^{l/2-2}/24 \log q$. As claimed in p. 246 of [24], $|\operatorname{Aut}(S)| \leq q^{4l^2}$. Now the result follows using part (i) of Lemma 4.1. $\square$

However, the quotient $k(S_n)/d(|S_n|)$ goes to 0 as n goes to infinity. In order to see this it suffices to use the classical result of Hardy and Ramanujan [9] on the number of partitions and part (ii) of Lemma 4.1 (together with Stirling's formula).

One reason why many different characters have the same degree is that any two Galois conjugate characters have the same degree. It would be interesting to decide whether or not it is possible to extend these results in the following direction. Given an integer n, $\Omega(n)$ is the number of prime divisors of n counting multiplicities.

Question 2. *Assume that G is a solvable group and that for any $n \in \mathrm{cd}(G)$ the number of Galois conjugacy classes of characters of degree n does not exceed k. Is $\Omega(|G|)$ k-bounded?*

References

[1] L. Babai, L. Pyber, Permutation groups without exponentially many orbits on the power set, J. Combin Theory Ser. A **66** (1994), 160–168.

[2] R. Brauer, Representations of finite groups, Lectures on Modern Mathematics, Vol I, New York, 1963.

[3] R. W. Carter, "Finite Groups of Lie Type. Conjugacy Classes and Complex Characters", John Wiley & Sons, Chichester, 1985.

[4] R. W. Carter, "Simple Groups of Lie Type", John Wiley & Sons, London, 1972.

[5] P. Erdos, S. Graham, A. Ivic, C. Pomerance, On the number of divisors of $n!$, in Analytic Number Theory, Progr. Math. **138**, Birkhäuser, Boston, 1996.

[6] E. Farias e Soares, Big primes and character values for solvable groups, J. Algebra **100** (1986), 305–324.

[7] W. Feit, Extending Steinberg characters, Linear Algebraic Groups and their Representations (Los Angeles, CA, 1992), 1–9, Contemp. Math., **153**, Amer. Math. Soc., Providence, RI, 1993.

[8] J. S. Frame, G. de B. Robinson, R. M. Thrall, The hook graphs of the symmetric group, Canadian J. Math. **6** (1954, 316–324.

[9] G. Hardy, S. Ramanujan, Asymptotic formulae in combinatory analysis, Proc. London Math. Soc. **17** (1918), 75–115.

[10] G. Hardy, E. Wright, "An Introduction to the Theory of Numbers", Clarendon Press, Oxford, 1979.

[11] B. Huppert, "Endliche Gruppen I", Springer-Verlag, Berlin, 1983.

[12] B. Huppert, Research in representation theory at Mainz (1984–1990), in Representation Theory of Finite Groups and Finite-Dimensional Algebras, Progr. Math. **95**, Birkhauser, Boston, 1991.

[13] B. Huppert, "Character Theory of Finite Groups", deGruyter, Berlin, 1998.

[14] B. Huppert, N. Blackburn, “Finite Groups III”, Springer-Verlag, New York, 1982.

[15] I. M. Isaacs, Generalizations of Taketa’s theorem on the solvability of M-groups, Proc. Amer. Math. Soc. **91** (1984), 192–194.

[16] I. M. Isaacs, “Character Theory of Finite Groups”, Dover, New York, 1994.

[17] A. Jaikin-Zapirain, On the number of conjugacy classes of finite p-groups, J. London Math. Soc. **68** (2003), 699–711.

[18] T. M. Keller, Orbits in finite group actions, In: “Groups St. Andrews 2001 in Oxford”,Vol II, 306–331, Cambridge University Press, Cambridge, 2003.

[19] M. Liebeck, A. Shalev, Character degrees and random walks in finite groups of Lie type, Proc. London Math. Soc. **90** (2005), 61–86.

[20] S. Mattarei, On character tables of wreath products, *J. Algebra* **175**, 157–178.

[21] R. Meshulam, A. Wigderson, Expanders in group algebras, Combinatorica **24** (2004), 659–680.

[22] A. Moretó, Complex group algebras of finite groups: Brauer’s Problema 1, Electronic Research Announcements of the AMS. **11** (2005), 34–39.

[23] A. Moretó, J. Sangroniz, On the number of conjugacy classes of zeros of characters, *Israel J. Math.* **142** (2004), 163–187.

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