Degree sum deficiency in finite groups

S.M. BUCKLEY, D. MACHALE, AND A. NÍ SHÉ

Abstract. We investigate the function $a(G) = |G| - T(G)$, where $T(G)$ is the sum of degrees of the absolutely irreducible complex representations of a finite group G. In particular, we prove some congruence relations, and find all G for which $a(G)$ is small.

1. Introduction

Suppose G is a finite group with $k(G)$ conjugate classes. Much has been written about connections between the structure of G and quantities defined in terms of the degrees d_i, $1 \le i \le k(G) = k$, of the absolutely irreducible complex representations of G. A basic quantity that arises in such work is $T(G) := \sum_{i=1}^{k} d_i$, and derived quantities such as $T(G)/k(G)$. We mention, for instance, the papers of Isaacs and Passman [9], [10] and, more recently, [2], [11], and [8].

In [3], we investigated the conjugate deficiency of G, $r(G) := |G| - k(G)$. In this paper, we analogously define the *degree sum deficiency*, $a(G)$, to be $|G| - T(G)$, and we also define $j(G) := T(G) - k(G) = r(G) - a(G)$. We will investigate $a(G)$ and, to a lesser extent, $j(G)$. It is clear that $a(G) = 0$ if and only if G is abelian and in what follows, we disregard these groups of which there is an infinite set. We will find all G for which $a(G)$ is small, and prove various properties of $a(G)$.

As might be expected, the properties of $a(G)$ and $j(G)$ run parallel to those of $r(G)$, but there are some intriguing differences. We based [3] on the spectacular congruence $|G| - k(G) \equiv 0 \pmod{16}$ when $|G|$ is odd. We will see that $a(G)$ and $j(G)$ also satisfy some congruence relations, though possibly not as dramatic as those satisfied by $r(G)$.

We use mostly standard notation: $|G|$ is the order of G, $(G : H) = |G|/|H|$ is the index of a subgroup H in G, $[x, y]$ is the *commutator* $x^{-1}y^{-1}xy$, G' is the *commutator subgroup* of G generated by all the commutators in G. We write $Z(G)$ for the *centre* of G. Throughout the remainder of the paper, an *(irreducible) representation* means a representation (that is irreducible) over the complex field.

We will need some special families of finite groups. C_n is the cyclic group of order $n \in \mathbb{N}$; D_n is the dihedral group of order $2n$, $n > 2$; Q_n is the dicyclic group of order $4n$, $n > 1$ (in particular, Q_2 is the quaternion group); and SD_n is the semidihedral group of order $2n$ whenever $n = 2^j$, for some $j > 2$. Whenever q is a prime power, $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}^q$, the finite field with q elements; and $\mathrm{GA}(1, q)$ is the general affine group of degree 1 over $\mathbb{F}_q$ (this group of order $q(q-1)$ consists of all formal maps $x \mapsto ax + b$, $a, b \in \mathbb{F}_q$, $a \neq 0$, under composition).

2010 *Mathematics Subject Classification.* 20D60, 20C15.

Key words and phrases. degree sum deficiency, complex representations.

It is convenient to assume that the degrees $d_1, \dots, d_k$ are always written in non-decreasing order; in particular $d_1 = 1$. We will repeatedly use the well-known facts that each d_i is a factor of $|G|$, and $|G| = \sum_{i=1}^k d_i^2$. This last equation, together with the fact that $d_i^2 - d_i$ is always even, immediately implies

Observation 1. $a(G) \equiv 0 \pmod 2$.

Note that 2 is the best possible modulus here, since $a(S_3) = 6 - 4 = 2$.

We will also need the following known result that summarises the representation degrees of dihedral, dicyclic, and related groups.

Theorem 2.

(a) For $n > 2$, D_n has two one-dimensional representations when n is odd, and four when n is even.
(b) More generally, if H is a finite abelian group in which the subgroup S of squares has index 2^k, $k \geq 0$, then the generalised dihedral group G arising from H has 2^{k+1} one-dimensional representations.
(c) For $n = 2^j > 4$, SD_n has four one-dimensional representations.
(d) For $n > 1$, Q_n has four one-dimensional representations.

All other irreducible representations for the groups in (a)–(d) have degree 2.

Sketch of proof. All groups in (a)–(d) have a normal abelian subgroup of index 2. By character theory, each degree d_i of G is a divisor of 2, and so it remains only to find the number of characters of degree 1.

The number of one-dimensional representations in any finite group G is $(G : G')$. The group in (b) is defined in terms of the index 2 subgroup H, a C_2 subgroup with generator x, and the equation $[x, h] = h^{-2}$ for all $h \in H$. It is routine to use this equation to show that $G' = S$ is the subgroup of squares in H, and so $(G : G') = 2^{k+1}$, as required. The arguments for (c) and (d) are similar. □

Theorem 2 readily implies that the function $a(G)$ is onto $2\mathbb{N}$. In fact it immediately implies the following corollary.

Corollary 3.

(a) For $n > 2$, $a(\mathrm{D}_n)$ is the largest even integer strictly less than n.
(b) If G, H, and k are as in Theorem 2(b), and $|H| = n$, then $a(G) = n - 2^k$.
(c) For $n = 2^j > 4$, $a(\mathrm{SD}_n) = n - 2$.
(d) For $n > 1$, $a(\mathrm{Q}_n) = 2n - 2$.

We next give another known result; this one summarises the representation degrees of the general affine group $\mathrm{GA}(1, q)$.

Theorem 4. *Suppose q is a power of a prime $p > 2$. Then $\mathrm{GA}(1, q)$ has q irreducible representations: $q - 1$ of degree 1, and one of degree $q - 1$.*

Sketch of proof. $G := \mathrm{GA}(1, q)$ is the semidirect product of $N := \mathbb{F}_q$ by $H := \mathbb{F}_q^*$, where the action is given by $g^{-1}ag = a^2$ for $a \in N$ and a specific generator g of H. It readily follows that $G' = N$, and so $(G : G') = q - 1$. It remains only to discover how many irreducible representations there are of degree exceeding 1. Writing a general element of G as $g^i a$ for some $0 \leq i < q - 1$ and $a \in N$, it is readily verified that there are q conjugacy classes: $q-2$ of them are cosets g^iN, $0<i<q-1$, and N itself splits into two cosets, $\{e_G\}$ and $N\setminus\{e_G\}$. Since we already have $q-1$ representations of degree 1, there is only one other irreducible representation, whose degree d satisfies

$$d^2+\sum_{i=1}^{q-1}1^2=q(q-1)\,.$$

It follows that $d=q-1$, as required. □

We will also need the following lemma.

Lemma 5. *If G is a direct product of groups H and K, then $a(G)\ge a(H)a(K)$, with equality if and only if H and K are both abelian. In the special case $K=\mathrm{C}_n$, we have $a(G)=na(H)$.*

Proof. The irreducible representations of G are direct products of the irreducible representations of H and K; note that it is crucial that we are considering complex representations. Thus $k(G)=k(H)k(K)$ and if we denote the character degrees of H and K as $d_{i,H}$ and $d_{j,K}$, respectively, then

$$a(G)=\sum_{i=1}^{k(H)}\sum_{j=1}^{k(K)}f(d_{i,H}d_{j,K})\,, \tag{1}$$

where $f(t):=t^2-t$ for $t\ge1$.

The equation $f(st)-f(s)f(t)=st(s+t-2)$ implies that $f(st)\ge f(s)f(t)$ for $s,t\ge1$, with equality if and only if $s=t=1$. Applying this to (1), the first statement of the lemma follows immediately. When $K=\mathrm{C}_n$, we have $k(K)=n$ and $d_{j,K}=1$ for each j, so (1) reduces to $a(G)=na(H)$, as required. □

The following lemma will allow us to improve the congruence relation in Observation 1 when $|G|$ is odd.

Lemma 6. *Let G be of odd order. Then $\{1\}$ is the only self-inverse conjugacy class in G.*

Proof. Suppose $g^{-1}xg=x^{-1}$ for some $g,x\in G$. Then

$$g^{-2}xg^2=g^{-1}(g^{-1}xg)g=g^{-1}x^{-1}g=(g^{-1}xg)^{-1}=(x^{-1})^{-1}=x\,.$$

so $[x,g^2]=1$.

Now $|G|=2n+1$ is odd, so $g^{2n+1}=1$. Thus $[x,g^{2n+1}]=1$ and, from the above, $[x,g^{2n}]=1$. Thus $[x,g]=1$, so $x^{-1}=g^{-1}xg=x$ and $x^2=1$. Since $|G|$ is odd, we deduce that $x=1$, as required. □

Theorem 7. *If G is an odd order non-abelian group, then $a(G)\equiv 0 \pmod 4$, and $a(G)\ge 12$.*

Proof. Using the equation $|G|=\sum_{i=1}d_i^2$, we see that $a(G)=\sum_{i=1}^k d_i(d_i-1)$ and, by Lemma 6, $\{1\}$ is the only self-inverse conjugacy class in G. By a result of Dixon [5, 11.7], we deduce that G has only one real irreducible character 1_G. For any representation R of G, we let R^* be the conjugate representation, with χ and χ^*

the characters of R and R^*, respectively. We see that $\chi = \chi^*$ if and only if $\chi = 1_G$, so with the exception of the degree of 1_G, degrees occur in pairs and so $k = 2m+1$ for some $m \in \mathbb{N}$.

Recalling our assumption that the degrees $d_1, \dots, d_k$ are written in increasing order, it follows that $d_{2j} = d_{2j+1}$ for all $1 \le j \le m$, and so

$$a(G) = \sum_{i=1}^{k} d_i(d_i - 1) = 0 + \sum_{j=1}^{m} 2d_{2j}(d_{2j} - 1) \equiv 0 \pmod 4 .$$

We now appeal to the fact that each d_i divides $|G|$. Since $d_i^2 - d_i$ is increasing as a function of d_i, it follows that to minimise $a(G)$, we should seek to have $d_i = 3$ for two indices i, and $d_i = 1$ for all other indices. This results in $a(G) = 2(3^2 - 3) = 12$. □

We claim that 4 and 12 are best possible in this result. Let G be the non-abelian group of order 21. Then $a(G) = 21 - 9 = 12$, so certainly 12 is minimal. Let K be the non-abelian group of order 55. Then $a(G) = 55 - 15 = 40$. Since $\gcd\{12, 40\} = 4$, the modulus 4 is also best possible.

Combining Theorem 7 with Burnside's result ([4, p.295]) that

$$|G| - k(G) \equiv 0 \pmod{16} \qquad \text{whenever } |G| \text{ is odd} ,$$

we immediately deduce

Corollary 8. *If $|G|$ is odd, then $j(G) \equiv 0 \pmod 4$.*

The non-abelian group of order 21 gives $j(G) = 9 - 5 = 4$, showing that this corollary is best possible. We note that $j(S_3) = 4 - 3 = 1$ shows that no similar nontrivial congruence result holds for groups of even order.

We can also improve Observation 1 when G is a p-group for some prime p. First, we state a theorem due to P. Hall [7]; for a more general result, see [12].

Theorem 9. *If G is a p-group, then $r(G) \equiv 0 \mod (p+1)(p-1)^2$.*

For $p = 2$, this result gives $|G| \equiv k(G) \pmod 3$, while for $p = 3$ it gives the Burnside congruence $|G| \equiv k(G) \pmod{16}$.

Our analogue for $a(G)$ is as follows.

Theorem 10. *If G is a p-group, then $a(G) \equiv 0 \mod p(p-1)^2$.*

Proof. Both $(G : G')$ and all $d_i > 1$ are positive powers of p. From a result of Mann [12], the number of algebraic conjugates of every non-principal irreducible character is divisible by $p - 1$. Hence,

$$|G| - T(G) = \sum_{i=1}^{k} d_i(d_i - 1) = \sum_{i=(G:G')+1}^{k} p^{r_i}(p^{r_i} - 1) ,$$

For each $i > (G : G')$, p divides p^{r_i}, and $p - 1$ divides $p^{r_i} - 1$. By Mann's result, each term $p^{r_i}(p^{r_i} - 1)$ occurs a multiple of $p - 1$ times. Thus $|G| - T(G)$ is divisible by $p(p-1)^2$, as required. □

We note that D_4 (for $p = 2$) and a non-abelian group of order p^3 (for odd p) show that this result is best possible: in both cases, there are p^2 irreducible representations of degree 1, and $p-1$ of degree p, so

$$T(G) = p^2 \cdot 1 + (p-1) \cdot p = 2p^2 - p\,,$$

and

$$|G| - T(G) = p^3 - 2p^2 + p = p(p-1)^2\,.$$

Combining the last two theorems, we immediately deduce

Corollary 11. *If G is a p-group, then $j(G) \equiv 0 \mod (p-1)^2$.*

A non-abelian group of order p^3 again shows that Corollary 11 is best possible; note that it gives no information when $p = 2$, but we cannot expect a nontrivial congruence in this case since $j(D_4) = 6 - 5$.

The next lemma is taken from [1]. In this lemma and subsequently, $\mathcal{G}_p$ is the class of all finite groups such that p is the least prime dividing $|G|$.

Lemma 12. *If G is non-abelian, and $G \in \mathcal{G}_p$ for some prime p, then*

$$T(G) \le \frac{2p-1}{p^2}|G|\,.$$

Equality holds if and only if $(G : Z(G)) = p^2$.

Lemma 12 immediately implies that if $G \in \mathcal{G}_p$ is non-abelian, then

$$|G| \le \frac{p^2 a(G)}{(p-1)^2}\,. \tag{2}$$

In particular, $|G| \le 4a(G)$ for every non-abelian G, and if additionally $|G|$ is odd, then $|G| \le 9a(G)/4$. We also record the following immediate consequence; here and later, we treat isomorphic groups as being equal.

Corollary 13. *There are only a finite number of groups with a given value of $a(G) > 0$ (and by Observation 1, this value must be even).*

In the following theorem, and subsequently, we use GAP IDs to name groups.

Theorem 14. *There are exactly three groups G with $a(G) = 2$, namely those with GAP IDs $[6,1]$, $[8,3]$, and $[8,4]$ (i.e. S_3, D_4, and Q_2).*

Although Theorem 14 is easily proven, it seems worthwhile to give two proofs.

Proof 1 of Theorem 14. The estimate $|G| \le 4a(G)$ implies that $|G| \le 8$. There are only three such non-abelian groups. By checking them, we see that all are of the required form. □

Proof 2 of Theorem 14. Note that $a(G)$ is a sum of terms of the form $d_i^2 - d_i$, $i = 1, \ldots, k$. Now $3^2 - 3 > 2$, so the only way that such a sum can equal 2 is if $d_i = 2$ for a single index i, and $d_i = 1$ for all other indices. By contrast, $r(G)$ is a sum of terms $d_i^2 - 1$. In this particular case, $r(G) - a(G) = -1 - (-2)$, and so $r(G) = 3$. The same type of argument shows that $r(G) = 3$ implies $a(G) = 2$. The solutions to $r(G) = 3$ are exactly the indicated groups according to [3, Theorem 3], so we are done. □

Proof 2 is slightly longer than Proof 1, but it throws fresh light on the result, and can also be adapted to analyze other small values of $a(G)$ using the results of [3]. We note that in [3], the number of groups G with $r(G) = n$ is denoted $t(n)$, and a table of values of $t(n)$ for $n \le 30$ is given at the top of p. 17. We will refer to those values below.

Theorem 15. *There are exactly nine groups G with $a(G) = 4$, namely those with GAP IDs* $[10, 1]$, $[12, 1]$, $[12, 4]$, $[16, 3]$, $[16, 4]$, $[16, 6]$, $[16, 11]$, $[16, 12]$, $[16, 13]$.

Proof. Because $3^2 - 3 > 4$, an argument like that in Proof 2 of Theorem 14 shows that $a(G) = 4$ occurs if and only if $d_i = 2$ for two indices i, and $d_i = 1$ for all other indices. Thus we must have $r(G) = 6$. In a similar manner, we see that if $r(G) = 6$ then $a(G) = 4$. This reduces the problem to listing the solutions of $r(G) = 6$. By [3, Theorem 4], there are nine such groups, and they are as listed (except that in [3] we use the IDs of Thomas and Wood [14], and here we have switched to GAP IDs). □

Remark 16. Some, but not all, of the groups in Theorem 15 can be discovered using Theorem 2 and Lemma 5. In particular, $[10, 1]$ is D_5, $[12, 1]$ is Q_3, $[12, 4]$ is D_6 (and also $S_3 \times \mathrm{C}_2$), $[16 : 11]$ is $D_4 \times \mathrm{C}_2$, and $[16 : 12]$ is $Q_2 \times \mathrm{C}_2$. The other four groups can be verified using GAP [6].

Theorem 17. *There are exactly eight groups G with $a(G) = 6$, namely those with GAP IDs* $[12, 3]$, $[14, 1]$, $[16, 7]$, $[16, 8]$, $[16, 9]$, $[18, 3]$, $[24, 10]$, $[24, 11]$.

Proof. Ignoring representations of degree 1, there are two ways of writing 6 as sums of numbers of the form $d_i^2 - d_i$: either as $3^2 - 3$ or as $2^2 - 2$ repeated three times. The first possibility corresponds to $r(G) = 3^2 - 1 = 8$, while the second corresponds to $r(G) = 3(2^2 - 1) = 9$. Conversely, $r(G) = 8$ arises only as $3^2 - 1$, and $r(G) = 9$ arises only as $3(2^2 - 1)$, so both lead to $a(G) = 6$. Thus $a(G) = 6$ is equivalent to $r(G) \in \{8, 9\}$. By [3, Theorem 5], A_4 is the only group with $r(G) = 8$; it has GAP ID $[12, 3]$.

As for $r(G) = 9$, [3] states that $t(9) = 7$. Corollary 3 gives four groups with $a(G) = 6$ and $r(G) = 9$, namely D_7, D_8, SD_8, and Q_4; these have GAP IDs $[14, 1]$, $[16, 7]$, $[16, 8]$, and $[16, 9]$, respectively. We get the other three such groups from Theorem 14 and Lemma 5: $S_3 \times \mathrm{C}_3$, $\mathrm{D}_4 \times \mathrm{C}_3$, and $\mathrm{Q}_2 \times \mathrm{C}_3$; these have GAP IDs $[18, 3]$, $[24, 10]$, and $[24, 11]$, respectively. □

Remark 18. In the proof of Theorem 17, we relied on the fact that $t(9) = 7$ to shorten the proof. Without this fact, we can still finish the proof as long as we know some basic information about all groups of order at most 24: in fact, it suffices to use Corollary 3, together with a knowledge of the number of nonabelian groups of order at most 24, and fact that for $\mathrm{GA}(1, 5)$ (GAP ID $[20, 3]$), we have $a(G) = 12$ and $r(G) = 15$; this last fact follows immediately from Theorem 4.

First, groups with $r(G) = 9$ and $a(G) = 6$ have order at most $4a(G) = 24$ and must have even order by Theorem 7. The order must be strictly greater than $3 \cdot 2^2 = 12$, leaving only $|G| \in \{14, 16, 18, 20, 22, 24\}$. Once we omit the groups considered in the proof of Theorem 17, there are no other non-abelian groups of order 14, and the other non-abelian groups of order 18 are D_9 and the generalised dihedral group arising from $C_3 \times C_3$, which by Corollary 3 both have degree sum deficiency $9 - 2^0 = 8$. Similarly, we can eliminate the one non-abelian group D_{11} of order 22, and all three non-abelian groups of order 20 (D_{10}, Q_5, and $GA(1,5)$). Finally, there are no non-abelian groups of 16 other than the nine listed in Theorems 15 and 17.

In a similar fashion to the above theorems, we see that $a(G) = 8$ is equivalent to $r(G) \in \{11, 12\}$ and, since $t(11) = 0$ and $t(12) = 23$, we have:

Theorem 19. *There are exactly twenty-three groups G with $a(G) = 8$.*

Remark 20. GAP [6] reveals that $a(G) = 8$ is satisfied for two groups of order 18, two of order 20, four of order 24, and fifteen of order 32.

Finally we consider $a(G) = 10$. This value is interesting because it is the smallest n for which $a(G) = n$ is not equivalent to $r(G)$ being in some related set of numbers, as we will see in the proof.

Theorem 21. *There are exactly seven groups G with $a(G) = 10$, namely those with GAP IDs* $[22, 1]$, $[24, 4]$, $[24, 6]$, $[24, 8]$, $[30, 1]$, $[40, 10]$, *and* $[40, 11]$.

Proof. Arguing as before, we see that the equation $a(G) = 10$ implies that $r(G) \in \{14, 15\}$. Again by [3], we have $t(14) = 0$ and $t(15) = 10$. However $r(G) = 15$ can be attained in two distinct ways: either $d_i = 2$ for five indices i, or $d_i = 4$ for a single index i. The first of these possibilities gives the desired $a(G) = 10$, but the second gives $a(G) = 12$.

Both of these possibilities occur, with the first occurring seven times and the second three times. In fact, we have already seen one group with a single irreducible degree-4 representation and all others of degree 1, namely $GA(1,5)$ (GAP ID $[20, 3]$). The other two such groups are the central product of D_4 and either another D_4 or a Q_2 (GAP IDs $[32, 49]$ and $[32, 50]$).

As for the groups with $a(G) = 10$, we can find most of these by the same methods as before, namely D_{11}, D_{12}, Q_6, $S_3 \times C_5$, $D_4 \times C_5$, and $Q_2 \times C_5$ (GAP IDs $[22, 1]$, $[24, 6]$, $[24, 4]$, $[30, 1]$, $[40, 10]$, and $[40, 11]$). The remaining group with $a(G) = 10$, provided by GAP [6], has GAP ID $[24, 8]$. $\square$

The above theorems give us the first five entries in the sequence $(N_a(n))_{n=1}^{\infty}$, where $N_a(n)$ is the number of groups with $a(G) = 2n$ for $n \in \mathbb{N}$. Using GAP, we can find more of the initial entries. Here are the values of $N_a(n)$ for $1 \le n \le 20$:

$$3,\ 9,\ 8,\ 23,\ 7,\ 39,\ 8,\ 52,\ 16,\ 23,\ 7,\ 113,\ 13,\ 62,\ 21,\ 163,\ 10,\ 102,\ 7,\ 66, \ldots$$

This does not have the appearance of a sequence for which we can find a nice formula, but it would be at least desirable to find good upper and lower bounds for this sequence.

By Theorem 7, $a(G) = 4n$ for some $n \ge 3$ if G is of odd order. The following result characterises the odd order non-abelian groups for which $a(G)$ is minimal.

Theorem 22. *There are exactly three odd order groups G with $a(G) = 12$, namely those with GAP IDs* $[21, 1]$, $[27, 3]$, *and* $[27, 4]$.

Proof. By (2), $a(G) = 12$ for odd $|G|$ implies $|G| \leq 9(12)/4 = 27$. By the proof of Theorem 7, we see that $a(G) = 12$ requires that two of the irreducible representations are of degree 3 and all others of degree 1 (and so $r(G) = 16$). Thus $|G| > 2 \cdot 3^2 = 18$, and $|G|$ must be a multiple of 3, so we need only check groups with $|G| \in \{21, 27\}$. There are three non-abelian groups of these orders, and $a(G) = 12$ for all of them. □

Remark 23. The odd order groups with $a(G) = 12$ are exactly the odd order groups with $r(G) = 16$ given by [3, Theorem 6].

If $f(G)$ is defined to be either $r(G)$ or $a(G)$, then $f(G) = 0$ if and only if G is abelian, and there is a positive constant C such that $|G| \leq Cf(G)$ whenever G is nonabelian; see [3] and Corollary 13. Consequently, there are only finitely many groups with a given value of $f(G) > 0$. We end by proving an analogous result for $f(G) := j(G)$, except that in this case, we can only get a quadratic bound $|G| \leq C(j(G))^2$. Of course, this still implies that there are only finitely many groups with a given value of $j(G) > 0$.

Note that $j(G) = \sum_{i=1}^{k}(d_i - 1)$. From this equation, it is clear that $j(G) = 0$ if and only if G is abelian. Before proceeding to prove that $|G| \leq C(j(G))^2$ when $j(G) > 0$, we need an elementary lemma.

Lemma 24. *For all $x, y \geq 4$, $\sqrt{x+y} + 1 < \sqrt{x} + \sqrt{y}$.*

Proof. By calculus, $f(x, y) := \sqrt{x} + \sqrt{y} - \sqrt{x+y} - 1$ is increasing as a function of both x and y, when $x, y \geq 4$. Thus $f(x, y) \geq f(4, 4) = 3 - \sqrt{8} > 0$. □

Theorem 25. *If G is non-abelian, then $|G| \leq 2(j(G) + 1)^2$. More generally, if $G \in \mathcal{G}_p$ is non-abelian, then $|G| \leq p(j(G) + 1)^2/(p - 1)$.*

Proof. Since $d_i = 1$ if and only if $i \leq (G : G')$, we have

$$j(G) = \left(\sum_{i=1}^{k} d_i\right) - k = \sum_{i=(G:G')+1}^{k} (d_i - 1)\,.$$

Consider the problem of minimizing the sum $\sum_{i=i_0}^{k}(\sqrt{e_i} - 1)$ subject to a constraint $\sum_{i=i_0}^{k} e_i = M$, where we assume that $i_0 \in \mathbb{N}$ and $M \geq 4$ are constants, but k and the numbers $e_{i_0}, \ldots, e_k$ are allowed to vary, subject to $k \geq i_0$ and $e_i \geq 4$ for each i. By Lemma 24, we see that

$$\sqrt{e_i + e_j} - 1 < (\sqrt{e_i} - 1) + (\sqrt{e_j} - 1)\,,$$

i.e. combining terms in the sum makes the sum strictly smaller. Thus to minimise the sum, we must take $k = i_0$ and $e_k = M$.

Applying this to $j(G)$ with data

$$(\, i_0,\, M,\, e_{i_0}, \ldots, e_k\,) := (\, (G : G') + 1, \quad |G| - (G : G'), \quad d_{i_0}^2, \ldots, d_k^2\,)\,,$$

we deduce that

$$j(G) \geq \sqrt{|G| - (G : G')} - 1\,.$$

If $G \in \mathcal{G}_p$ is non-abelian, then $(G : G') \leq |G|/p$, so $|G| - (G : G') \geq (p-1)|G|/p$, and

$$j(G) + 1 \geq \sqrt{\frac{(p-1)|G|}{p}}\,. \qquad \square$$

Remark 26. A quadratic bound is the best that we can hope for in Theorem 25. In fact, $|G| > (j(G)+1)^2$ for arbitrarily large groups G. It suffices to consider $G := \mathrm{GA}(1, q)$, where q is some prime power. It follows immediately from Theorem 4 that $j(G) = q - 2$, and so $|G| = q(q-1) > (j(G)+1)^2$.

References

[1] F. Barry, D. MacHale, and Á. Ní Shé, *Some supersolvability conditions for finite groups*, Math. Proc. Royal Ir. Acad. **106** (2006), 163-177.

[2] Y. Berkovich and A. Mann, *Sums of degrees of irreducible characters*, J. Algebra **199** (1998), 646–665.

[3] S.M. Buckley and D. MacHale, *Conjugate deficiency in finite groups*, Bull. Irish Math. Soc. 71 (2013), 13–19.

[4] W. Burnside, *Theory of Groups of Finite Order. 2nd ed.*, Dover, New York, 1955.

[5] J.D. Dixon, *Problems in group theory*, Dover, New York, 1973.

[6] The GAP Group, *GAP — Groups, Algorithms, and Programming, Version 4.4.12*, 2008 (`http://www.gap-system.org`).

[7] P. Hall, unpublished.

[8] I.M. Isaacs, M. Loukaki, and A. Moretó, *The average degree of an irreducible character of a finite group*, Israel J. Math. **197** (2013), 55–67.

[9] I.M. Isaacs and D.S. Passman, *A characterization of groups in terms of the degrees of their characters*, Pacific J. Math. **15** (1965), 877–903.

[10] I.M. Isaacs and D.S. Passman, *A characterization of groups in terms of the degrees of their characters. II*, Pacific J. Math. **24** (1968), 467–510.

[11] K. Magaard and H.P. Tong-Viet, *Character degree sums in finite nonsolvable groups*, J. Group Theory 14 (2011), 54–57.

[12] A. Mann, *Conjugacy classes in finite groups*, Israel J. Math. **31** (1978), 78–84.

[13] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics 42, Springer, New York, 1977.

[14] A.D. Thomas and G.V. Wood, *Group tables*, Shiva, 1980.

S.M. Buckley:
Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.
E-mail address: `stephen.buckley@maths.nuim.ie`

D. MacHale:
School of Mathematical Sciences, University College Cork, Cork, Ireland.
E-mail address: `d.machale@ucc.ie`

A. Ní Shé:
Department of Mathematics, Cork Institute of Technology, Cork, Ireland.
E-mail address: `aine.nishe@cit.ie`