Irish Math. Soc. Bulletin
Number 71, Summer 2013, 13–19
ISSN 0791-5578

Conjugate deficiency in finite groups

STEPHEN M. BUCKLEY AND DESMOND MACHALE

Abstract. We consider the function $r(G) = |G| - k(G)$, where the group G has exactly $k(G)$ conjugacy classes. We find all G where $r(G)$ is small and pose a number of relevant questions.

1. Introduction

Let G be a finite group and let G have exactly $k(G)$ conjugacy classes of elements. One of the most startling results in finite group theory is the following beautiful theorem of Burnside [3, p.295].

Theorem A. *If $|G|$ is odd, then $|G| - k(G) \equiv 0 \pmod{16}$.*

We note that no such result can hold if $|G|$ is even. For example, if S_3 is the symmetric group of order 6 and A_4 is the alternating group of order 12, then $k(S_3) = 3$, $k(A_4) = 4$, so that $r(S_3) = 3$, $r(A_4) = 8$, and $\gcd(3, 8) = 1$.

Burnside proved Theorem A using matrix representation theory, but later authors such as Hirsch [5] and Poland [7] proved Burnside's result by elementary means and in fact generalized it. Theorem A has some immediate consequences which are pretty and useful enough to impress students taking a first course in group theory.

Consequence B. *Groups of orders 3, 5, 7, 9, 11, 13, 15, and 17 are all abelian.*

Consequence C. *A non-abelian group of order 21 has exactly 5 conjugacy classes.*

The form of Theorem A suggests that it would be worthwhile to consider the function $r(G) := |G| - k(G)$, which we call the *conjugate deficiency* of a finite group G. In this note, we prove a number of results about $r(G)$ including the following.

2010 *Mathematics Subject Classification.* 20D60.
Key words and phrases. Finite group, deficiency.
Received on 8-2-2013; revised 4-3-2013.

Theorem 1. *There are only finitely many groups G with a given value of $r(G) > 0$.*

We note the obvious fact that there are infinitely many finite groups with $r(G) = 0$, and these are precisely the abelian groups. In what follows, we disregard these groups, so that throughout G will denote a finite non-abelian group.

We use the following notation for some families of groups: C_n is the cyclic group of order n; S_n is the symmetric group of order $n!$; A_n is the alternating group of order $n!/2$; D_n is the dihedral group of order $2n$, $n > 2$; and Q_n is the dicyclic group of order $4n$, $n > 1$ (in particular, Q_2 is the quaternion group).

Theorem 2. *There is no G with $r(G) = 1$, 2, 4, 5, or 7.*

Theorem 3. *The groups with $r(G) = 3$ are S_3, D_4, and Q_2.*

Theorem 4. *There are exactly nine groups with $r(G) = 6$.*

Theorem 5. *The only group with $r(G) = 8$ is A_4.*

This example A_4 knocks on the head the conjecture that $r(G) \equiv 0 \pmod 3$ if $|G|$ is even. However Hirsch [5] shows that if $|G|$ is even and $3 \nmid |G|$, then $r(G) \equiv 0 \pmod 3$. Also if $|G|$ is odd and $3 \nmid |G|$, then $r(G) \equiv 0 \pmod{48}$.

Theorem 6. *The odd order groups which satisfy $r(G) = 16$ are one group of order 21 and two groups of order 27.*

Theorem 7. *The only odd order group which satisfies $r(G) = 32$ is the non-abelian group of order 39.*

Theorem 8. *There are exactly six odd order groups satisfying $r(G) = 48$.*

We begin with the following elementary lemma which, combined with a knowledge of groups of small order, yields all the above results.

Lemma 9. *Suppose G is a non-abelian group. Let p be the least prime dividing $|G|$, and suppose $(G : Z(G)) \geq n$, where $Z(G)$ is the centre of G. Then*

$$k(G) \leq \frac{n+p-1}{pn} \cdot |G| \, .$$

In particular,

$$k(G) \le \frac{p^2+p-1}{p^3} \cdot |G|\,.$$

Proof. The number of single element conjugacy classes in G equals $|Z(G)|$, and so is at most $|G|/n$. Since the size of a conjugacy class is a divisor of $|G|$, any other class has at least p elements, so

$$k(G) \le \frac{1}{n}|G| + \frac{1}{p}\left(1 - \frac{1}{n}\right)|G| = \frac{n+p-1}{pn} \cdot |G|\,.$$

Since G is non-abelian, $G/Z(G)$ is not cyclic. Thus we can take $n = p^2$ to get the second estimate. □

We remark that this result is best possible, being attained for the non-abelian groups of order p^3, both for $p = 2$ and p an odd prime. It follows from Lemma 9 that

$$r(G) = |G| - k(G) \ge |G|\left(1 - \frac{n+p-1}{np}\right) = \frac{(n-1)(p-1)}{np}|G|\,.$$

Thus

$$|G| \le \frac{np \cdot r(G)}{(n-1)(p-1)}\,, \tag{1}$$

where p is the least prime dividing $|G|$ and $n \le (G : Z(G))$. Using the second estimate in Lemma 9, we get

$$|G| \le \frac{p^3 \cdot r(G)}{(p^2-1)(p-1)}\,, \tag{2}$$

Since $p^3/(p^2-1)(p-1)$ obviously decreases as p increases, we have the following:

$$|G| \le \frac{8r(G)}{3}\,, \qquad \text{for all finite non-abelian groups } G. \tag{3}$$

$$|G| \le \frac{27r(G)}{16}\,, \qquad \text{for all finite non-abelian groups } G \text{ of odd order.} \tag{4}$$

Moreover, we have equality in (3) if and only if $(G : Z(G)) = 4$, and equality in (4) if and only if $(G : Z(G)) = 9$. By (3), there is an upper bound on $|G|$ for any given $r(G) > 0$. Theorem 1 now follows since there are only finitely many finite groups whose order does not exceed a given number.

Using (3), we see that $|G| \le 16/3$ if $r(G) \le 2$, and no such non-abelian group exists. If $r(G) = 3$, then $|G| \le 8$. There are exactly 3 non-abelian groups of order at most 8, namely S_3, D_4 and Q_2, and $r(G) = 3$ in all three cases.

Using (3), we see that $|G| \le 16$ if $r(G) \le 6$, so to understand how $4 \le r(G) \le 6$ can arise, we need to examine all non-abelian groups of orders between 9 and 16 inclusive. There are fourteen such groups, and for nine of these we have $k(G) = 6$, namely D_5; Q_3; $D_6 = S_3 \times C_2$; and the six groups of order 16 with $(G : Z(G)) = 4$, namely $D_4 \times C_2$, $Q_2 \times C_2$, and 16/8, 16/9, 16/10, and 16/11, in the notation of [8]. The five remaining non-abelian groups with orders between 9 and 16 inclusive have larger deficiencies: $k(A_4) = 8$ and $k(D_7) = k(D_8) = k(Q_4) = k(SD_{16}) = 9$, where SD_{16} is the semidihedral group of order 16. Thus there are no groups with $r(G) \in \{4, 5\}$, and nine groups with $r(G) = 6$.

Using (3), we see that $|G| \le 64/3$ if $r(G) \le 8$, so to understand how $7 \le r(G) \le 8$ can arise, we need to examine the five non-abelian groups with order at most 16 and $r(G) > 6$, plus groups of order between 17 and 21 inclusive. Of the five with order at most 16 and $k(G) > 6$, the only one with $r(G) \le 8$ is A_4 giving $r(A_4) = 8$.

As for the groups of larger order between 17 and 21, we need only check the even order groups, since (4) tells us that $|G| \le 27/2 < 16$ if $|G|$ is odd and $r(G) \le 8$. It remains to check $|G| \in \{18, 20\}$, and there are six such groups: three of order 18 (D_9, $S_3 \times C_3$, and a semidirect product of $C_3 \times C_3$ by C_2) and three of order 20 (D_{10}, Q_5, and the general affine group of degree 1 over GF_5). In each case, $r(G) > 8$. This establishes Theorems 2, 3, 4, and 5.

We now turn to the case where G has odd order, as suggested by Theorem A. If $|G|$ is odd and $r(G) = 16$, then by (4), $|G| \le 27$, and just three groups emerge: the non-abelian group of order 21, and two groups of order 27. Again for $|G|$ odd and $r(G) = 32$, we must have $|G| \le 54$ and just one group emerges, namely the non-abelian group of order 39. For $|G|$ odd and $r(G) = 48$, we must have $|G| \le 81$, and we get 10 groups: one of order 55, one of order 57, two of order 63, and six of order 81. This establishes Theorems 6, 7, and 8.

Now let $t(n)$ be the number of groups which satisfy $r(G) = n$. Here is a table listing the values of $t(n)$ for $n \le 30$, obtained by the above methods.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$t(n)$	0	0	3	0	0	9	0	1	7	0	0	23	0	0	10

n	16	17	18	19	20	21	22	23	24	25	26	27	28	28	30
$t(n)$	4	1	31	1	0	12	0	0	49	0	0	15	0	0	32

The dihedral groups alone suffice to get $r(G)$ equal to any multiple of 3. In fact for $n > 1$, it is well known that $k(D(2n-1)) = n+1$ and $k(D(2n)) = n+5$, and so $r(D(2n-1)) = r(D(2n)) = 3(n-1)$.

It seems difficult to predict the values of $t(n)$, but it is easy to see that

$$r(A \times G) = |A| r(G)$$

whenever A is a finite abelian group. Since there are abelian groups of all orders, it follows that if a given number n is a value of $r(G)$, then so is mn for all $m \in \mathbb{N}$. Moreover $t(mn) \geq t(n)$ for all $m, n \in \mathbb{N}$. This suggests that it would be important to consider prime numbers p for which $t(p) > 0$.

We note that for each prime p, there is a group of order p^3 with p^2+p-1 classes, so that $r(G) = (p^2-1)(p-1)$ is always possible. In addition, if p and q are primes with $2 < p < q$, where $p \mid (q-1)$, then the nonabelian group of order pq has $p + (q-1)/p$ conjugacy classes, and so

$$r(G) = \frac{(q-1)(p^2-1)}{p}.$$

We close with a number of related problems, some of which could prove difficult to solve.

Problem 1. *Give a realistic upper bound for $t(n)$ for each n.*

Problem 2. *Characterize the numbers n for which $t(n) = 0$.*

With the help of [8] and GAP [4], we see that the numbers in the above problem begin

1, 2, 4, 5, 7, 10, 11, 13, 14, 20, 22, 23, 25, 26, 28, 29,
31, 37, 41, 43, 46, 47, 49, 50, 52, 53, 58, 59, 61, 62, ...

Are there infinitely many such numbers?

Problem 3. *Are there infinitely many primes p for which $t(p) > 0$?*

The primes less than 199 for which $t(p) > 0$ are as follows:

$$3, 17,\ 19,\ 83,\ 97,\ 107,\ 113,\ 137,\ 149,$$
$$151,\ 157,\ 167,\ 173,\ 179,\ 181,\ 193,\ 197.$$

These values were found using the Small Groups Library of GAP ([4], [1]) by searching through groups of order at most 511.

Problem 4. *Are there infinitely many pairs* $(n, n+1)$ *where* $3 \nmid n$ *and* $3 \nmid (n+1)$ *such that* $t(n) = t(n+1) = 0$*?*

Problem 5. *For each* $k \geq 4$*, is there an odd order group* G *with* $r(G) = 2^k$*?*

If the answer to this last problem is positive, then we can find a group of odd order with $r(G) = 16l$ for all $l \in \mathbb{N}$ by taking direct products as previously described. The answer is indeed positive for $4 \leq k \leq 12$, because of groups of order 21, 39, 75, 147, 291, 579, 1161, 2307, 4221; the largest three of these orders were found with the help of GAP. The desired group is given in all except two cases by a semidirect product $C_n \rtimes C_3$, for $n = |G|/3$. The two exceptional cases are $|G| = 75$ in which case $G = C_5^2 \rtimes C_3$, and $|G| = 4221$ in which case G is of type $(C_7 \rtimes C_3) \times (C_{67} \rtimes C_3)$. There does not seem to be a clear enough pattern to these examples to justify a conjecture that the answer is always positive.

Problem 6. *Is the function* $t(n)$ *onto* $\mathbb{N}$*? Is there, for example, an* n *with* $t(n) = 2$*?*

Problem 7. *For* n *odd and* $n > 3$*, do there exist primes* p *and* q *with* $2 < p < q$ *where* $p \mid (q-1)$*, such that* $n = p + (q-1)/p$*?*

Computer results [2] show that this result is true for all n, $3 < n < 10\,000\,001$. If it is true in general, then it provides an answer to the following question posed by the second author in [6].

> *For each odd* $k > 3$*, does there exist an odd order non-abelian group with exactly* k *conjugacy classes?*

Of particular interest is $r(S_n) = n! - p(n)$, where $p(n)$ is the number of partitions of n. This purely arithmetic function is of some interest in its own right, so we ask:

Problem 8. *What is the range of values of* $r(S_n)$*?*

We say that n is primitive if $t(n) \neq 0$, but $t(d) = 0$ for each proper divisor d of n. For example, 3, 8, 17, and 19 are primitive.

Problem 9. *Are there infinitely many primitive values of n?*

References

[1] H.U. Besche, B. Eick, and E. O'Brien, *The Small Groups Library* (`http://www.icm.tu-bs.de/ag_algebra/software/small/`).
[2] Ch. van den Bosch, personal communication.
[3] W. Burnside, *Theory of Groups of Finite Order. 2nd ed.*, Dover, New York, 1955.
[4] The GAP Group, *GAP — Groups, Algorithms, and Programming, Version 4.4.12*, 2008 (`http://www.gap-system.org`).
[5] K.A. Hirsch, *On a theorem of Burnside*, Quart. J. Math. Oxford Ser. (2) **1** (1950), 97–99.
[6] *The Kourovka Notebook: Unsolved problems in Group Theory. 17th edition.* E.I. Khukhro and V.D. Mazurov (Eds.), Institute of Mathematics, Novosibirsk, 2010.
[7] J. Poland, *Two problems of finite groups with k conjugate classes*, J. Aust. Math. Soc. **8** (1968), 49–55.
[8] A.D. Thomas and G.V. Wood, *Group tables*, Shiva, 1980.

Stephen Buckley received his Ph.D. from the University of Chicago. He is a Professor of Mathematics at NUI Maynooth, where he has taught for twenty years. His research interests include metric space curvature, geometric analysis, harmonic analysis, and ring theory.

Desmond MacHale received his Ph.D. from the University of Keele and is Emeritus Professor of Mathematics at University College Cork where he taught for nearly forty years. His research interests include commutativity in groups and rings, automorphisms of groups, Euclidean geometry, number theory, and mathematical humour.

(S. Buckley) Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland

(D. MacHale) School of Mathematical Sciences, University College Cork, Cork, Ireland

E-mail address, S. Buckley: `stephen.buckley@maths.nuim.ie`

E-mail address, D. MacHale: `d.machale@ucc.ie`