2000

Two-groups with few conjugacy classes

Nigel Boston
University of Illinois at Urbana-Champaign, boston@math.uiuc.edu

Judy L. Walker
University of Nebraska - Lincoln, judy.walker@unl.edu

Published in Proceedings of the Edinburgh Mathematical Society 43 (2000), pp 211-217.
doi 10.1017/S0013091500020824

TWO-GROUPS WITH FEW CONJUGACY CLASSES

Nigel Boston and Judy L. Walker

An old question of Brauer asking how fast numbers of conjugacy classes grow is investigated by considering the least number c_n of conjugacy classes in a group of order 2^n. The numbers c_n are computed for $n \leq 14$ and a lower bound is given for c_{15}. It is observed that c_n grows very slowly except for occasional large jumps corresponding to an increase in coclass of the minimal groups G_n. Restricting to groups that are 2-generated or have coclass at most 3 allows us to extend these computations.

1991 *Mathematics Subject classification:* primary 20D15; secondary 20-04, 20D60.
Key words and phrases: p-groups, conjugacy classes, coclass

0. Introduction

There is a long history to the question of the possible number $k(G)$ of conjugacy classes of a finite group G. It began in 1903 when Landau [**8**] showed that only finitely many groups G have a given $k(G)$. This was made explicit in 1963 by Brauer [**3**] (see also [**4**]), who showed that $k(G) > \log_2 \log_2 |G|$. In general, $k(G)$ will be much larger than this. For example, Bertram [**1**] showed that for a given $\epsilon > 0$ and for almost all integers $n \leq x$, as $x \to \infty$, $k(G) > |G|^{1-\epsilon}$ for each group G of order n.

In his paper of 1963, Brauer asked what the "true" growth of a lower bound for $k(G)$ in terms of $|G|$ might be. One answer to this was provided by Pyber [**14**], who proved the lower bound $k(G) \geq \epsilon \log_2 |G|/(\log_2 \log_2 |G|)^8$. Experimentally, López and López ([**9**], [**10**]) have found that $k(G) > \log_3 |G|$ if $|G| \leq 3^{13}$ and in fact no group has been discovered for which this fails. The groups $G = PSL(3,4)$ and $G = M_{22}$ both satisfy $k(G) = \lceil \log_3 |G| \rceil$.

If we restrict attention to nilpotent groups (in particular if we restrict to $|G|$ being a prime power), the ideas of P. Hall immediately give $k(G) > \alpha \log |G|$ for some constant α depending only on p, as described in the next section. This was refined by Sherman [**16**], who showed that if G has nilpotency class c, then $k(G) > c(|G|^{1/c} - 1) + 1$. Kovaćs and Leedham-Green [**7**] produced for each odd prime p a group G_p of order p^p with less than $p^3 = (\log_p |G_p|)^3$ classes. A natural question, originally formulated by Pyber in [**14**], is whether, for a given p, there exists an absolute constant c and a sequence of p-groups (G_n), where G_n has order p^n and $k(G_n) < cn = c \log_p |G_n|$.

The aim of this paper is to address what Brauer asked in his 1963 paper by attacking the above question by computer. We focus on 2-groups, where we can make extensive calculations with the help of the computational software package MAGMA [**2**].

Let $c_n = \min\{k : \text{there is a group G of order } 2^n \text{ with } k(G) = k\}$. Our approach consists of three searches. In the first search, we find c_n for all $n \leq 14$ together with bounds for c_{15}. In the second search, we restrict attention to 2-generated 2-groups and find the smallest number of conjugacy classes for such groups of order 2^{15} and 2^{16}. In the third search, we restrict attention to 2-groups with coclass at most 3 and any order.

It appears that c_n grows tightly with n except for large occasional jumps. We provide an explanation for this behavior. The ultimate answer to Brauer's question will depend on a comparison between the frequency and the size of these jumps.

1. Basic Results

If $|G| = p^{2m+e}$ with $e = 0$ or 1, then a formula of P. Hall ([**13**]) states $k(G) = m(p^2-1) + p^e + r(G)(p-1)(p^2-1)$ where $r(G)$ is a non-negative integer. This formula has several implications. First, by noticing that the right hand side of the equality is at least $m(p^2-1) + p^e$, we get that $k(G) > \alpha \log |G|$, where α is a constant depending only on p. For $p = 2$, we obtain $k(G) = 3(m + r(G)) + 2^e$, so that $k(G) \equiv |G| \pmod 3$. In fact, Poland showed that if G is a p-group such that $r(G) = 0$, then $|G| \leq p^{p+2}$ and has coclass 1. Fernández-Alcober and Shepherd [**5**] recently proved that if $p \geq 11$ and $r(G) = 0$, then $|G| \leq p^{p+1}$. Computational evidence (such as that provided by this paper) suggests that there are bounds on the order and coclass of p-groups with a given $r(G)$, which if true explains phenomena later in this paper. Also, Poland showed that $k(G) > k(Q)$ and $r(G) \geq r(Q)$ if Q is a proper quotient of p-group G. We summarize the consequences for c_n.

Lemma 1.1. *$c_n \equiv 1 \pmod 3$ if n is even and $c_n \equiv 2 \pmod 3$ if n is odd. Moreover, $c_n > c_{n-1}$.*

Call a group G of order 2^n with $k(G) = c_n$ a best group. We can establish some properties of sequences of best groups.

Theorem 1.2. *Let G_n $(n = 1, 2, ...)$ be a sequence of best groups. The coclass of G_n grows without bound as $n \to \infty$.*

This follows by combining the following two lemmas.

Lemma 1.3. *For each positive integer c, there exists a positive real number α_c such that if G is a 2-group of coclass c, then $k(G) \geq \alpha_c |G|$.*

Proof. Shalev's proof [**12**] of the conjectures of Leedham-Green and Newman shows that if G is a 2-group of coclass c, then it contains an abelian normal subgroup A of index bounded by a function $f(c)$. This implies that $k(G) \geq k(A)/[G:A] = |A|/[G:A] = |G|/[G:A]^2 \geq |G|/f(c)^2$. Taking $\alpha_c = 1/f(c)^2$ gives the result.

Lemma 1.4 ([6]). *Let H_n be the Sylow 2-subgroup of $GL(n, \mathbf{F}_2)$. The order of H_n is $2^{T(n)}$ where $T(n) = (n-1)(n-2)/2$ and*

$$2^{(1/12-\epsilon_n)n^2} < k(H_n) < 2^{(1/4+\epsilon_n)n^2},$$

where $\epsilon_n \to 0$ as $n \to \infty$.

Proof of Theorem 1.2. Suppose G_n is a sequence of best groups whose coclasses form a finite set C. Let $\alpha = \min\{\alpha_c \mid c \in C\}$. Then $c_n/2^n = k(G_n)/|G_n| \geq \alpha > 0$

for all n. In particular, we have $k(H_n) \geq c_{T(n)} \geq 2^{T(n)}\alpha$, contradicting Lemma 1.4 for sufficiently large n.

2. The 1st Search - Exhaustive for Small n

Theorem 2.1. *The values of c_n for $n \leq 14$ are as follows (G_n a best group):*

n	c_n	$r(G_n)$	coclass(G_n)
1	2	0	1
2	4	0	1
3	5	0	1
4	7	0	1
5	11	1	1 *or* 2
6	13	1	2
7	14	1	2
8	19	2	2
9	26	4	3 *or* 4
10	28	4	3 *or* 4
11	29	4	3 *or* 4
12	34	5	3 *or* 4
13	35	5	3
14	37	5	3

The aim of this search is to compute c_n for as many n as possible. We originally used CAYLEY but later checked our results with the quicker system MAGMA. The databases of these systems contain all 2-groups of order ≤ 256 and this allows us immediately to find c_n for $n \leq 8$. To extend these results, we use the following refinement of lemma 1.1. We write $n(G) = \log_2(|G|)$.

Lemma 2.2. *If Q is a quotient of the 2-group G, then $2k(G) - 3n(G) \geq 2k(Q) - 3n(Q)$ if $n(G)$ is even, whereas $2k(G) - 3n(G) \geq 2k(Q) - 3n(Q) - 1$ if $n(G)$ is odd.*

Proof. If $|G| = 2^{2m+e}$ and $|Q| = 2^{2n+f}$ with $e, f \in \{0, 1\}$, then $(2k(G) - 3n(G)) - (2k(Q) - 3n(Q)) = 6(r(G) - r(Q)) + (2^{e+1} - 3e) - (2^{f+1} - 3f) = 6(r(G) - r(Q)) + f - e$. Since $r(G) \geq r(Q)$, this is nonnegative except possibly if $f = 0$ and $e = 1$, in which case it is at least -1.

The p-group generation process of O'Brien **[12]** creates for each $d > 1$ a tree whose vertices are the d-generated 2-groups (counted once up to isomorphism). An edge exists from P to Q if P is isomorphic to $Q/\gamma_c(Q)$ where $\gamma_c(Q)$ is the last nontrivial term of the lower exponent-p central series of Q. In that case we call Q an immediate descendant of P. If there is a path from P to Q, then we say Q is a descendant of P. O'Brien's process allows us to compute immediate descendants (and so descendants) of any given 2-group.

We use lemma 2.2 and O'Brien's trees to compute c_n for increasing n. To test, for instance, if there is a group of order 2^{12} with ≤ 31 conjugacy classes, we use O'Brien's routine to compute all 2-groups Q with smaller order and $2k(Q) - 3n(Q) \leq 26$. If our group existed, then it would be an immediate descendant of such a Q. A computational check shows that no such Q has an immediate descendant of order 2^{12} with ≤ 31 conjugacy classes. So $c_{12} \geq 34$ and we find all best groups of order

2^{12} by using O'Brien's routine to find all groups with $2k(Q) - 3n(Q) \leq 32$ and $|Q| \leq 2^{12}$.

This works well until we try to find c_{15}. The bound on $2k(Q) - 3n(Q)$ becomes so large that we have to consider too many groups in O'Brien's trees for this computation to be feasible. Just the case of 2-generated groups (see the next section) took a few months to complete. The best we have is that $53 \leq c_{15} \leq 68$.

We have data on the best groups of order 2^n ($n \leq 14$) that may be obtained by request from the authors. A few observations are in order. For each n there are 2-generated best groups. For $n = 9, 10, 11, 12$, there are also 3-generated best groups (these being the ones of coclass 4 of those orders). Note that jumps in c_n are apparently accompanied by jumps in coclass. The best groups of order 2^{14} are extensions of the same point group of order 2^6 by a normal subgroup isomorphic to the direct product C_4^4.

3. The 2nd Search - Two-Generated Groups

Since the search for the best groups of order 2^{15} ultimately involved too many groups to be feasible, we decided to restrict attention to 2-generated groups. This permits a lengthy but successful search.

Theorem 3.1. *There are* 142 2*-generated groups of order* 2^{15} *with* 68 *conjugacy classes. No* 2*-generated group of order* 2^{15} *has fewer conjugacy classes. There are* 92 2*-generated groups of order* 2^{16} *with* 70 *conjugacy classes. No* 2*-generated group of order* 2^{16} *has fewer conjugacy classes. Every* 2*-generated group of order* 2^{17} *has* ≥ 74 *conjugacy classes.*

This arises by use of the method of the previous section. We inductively construct all 2-generated 2-groups Q with $2k(Q) - 3n(Q) \leq 92$. The largest of these have order 2^{16}. The groups of order 2^{15} are of coclass 3 or 4. The ones of order 2^{16} are of coclass 4. Note that if G_n is one of these groups, then $r(G_n) = 15$. We know of no d-generated groups ($d \geq 3$) that have the same order as, but fewer conjugacy classes than, the above 2-generated groups.

4. The 3rd Search - Groups of Coclass ≤ 3

The paper of Newman and O'Brien **[11]** presents a method for obtaining all 2-groups of coclass 3. Since many of our best 2-groups have coclass ≤ 3, we decided to do an exhaustive study of the number of conjugacy classes of these groups using **[11]**. All but 1782 sporadic examples naturally fall into 82 families as follows. There are 82 pro-2 groups which correspond to the infinite ends of the subtree of coclass ≤ 3 groups of O'Brien's tree for $d = 2$. Mainline groups in family $\#i$ are obtained by taking the exponent-p central quotients of pro-2 group $\#i$. The rest are obtained by taking descendants of these mainline groups. The point is that above a certain vertex (the root) the pattern of descendants is conjecturally periodic. This regularity allows us to find the 2-groups of coclass 3 with fewest conjugacy classes for all orders n. Since the largest of the 1782 sporadic groups has order 2^{14}, we need not consider them when working with $n > 14$. The case of $n \leq 14$ was covered in section 2.

For family $\#i$, for each i, we compute the number $f_i(n)$ of conjugacy classes of its mainline quotient of order 2^n for sufficiently large n. For instance, family #2 yields dihedral groups and so $f_2(n) = 2^{n-2} + 3$.

There is a formula for $f_i(n)$ of the form $a2^n+$ lower terms (a independent of n). For instance, for family #34, setting $x = 2^{[n/4]}$, $f_{34}(n) = 2^{n-12} + cx^2 + dx + 9$ where the values of c and d depend on $n \pmod 4$ as follows: if $n \equiv 0 \pmod 4$ then $c = 27/128$ and $d = 51/16$; if $n \equiv 1 \pmod 4$ then $c = 3/8$ and $d = 27/8$; if $n \equiv 2 \pmod 4$ then $c = 27/64$ and $d = 33/8$; if $n \equiv 3 \pmod 4$ then $c = 3/4$ and $d = 39/8$.

It is easy to see then that no group in family #2 beats even the mainline groups in family #34. We carry this method through with all 82 families. It is interesting to observe that $f_{29}(n) = f_{34}(n) + 6$, and lengthy computations show that these are the only two families that compete for best coclass 3 groups, in the following sense.

Let $c_n^{(3)} = \min\{k :$ there is a group G of order 2^n and coclass ≤ 3 with $k(G) = k\}$. If the group G has order 2^n, coclass ≤ 3, and $k(G) = c_n^{(3)}$, then G will be called a best coclass 3 group.

Theorem 4.1. *For $n \leq 14$, $c_n^{(3)}$ is given by theorem 2.1, and for $15 \leq n \leq 26$, the values of $c_n^{(3)}$ are given by:*

n	$c_n^{(3)}$
15	68
16	76
17	110
18	148
19	242
20	373
21	617
22	1123
23	1493
24	4993
25	6341
26	11911

The best groups of coclass 3 of order 2^{15} are located in families #30, #32, #35, and #42. The best of order 2^{16} are in family #42 and of orders $2^{17}, 2^{18}, 2^{20}$, and 2^{21} in family #20. As for $n = 19$ and $n \geq 22$, the following claim is verified for $n \leq 26$ and is expected to hold in general. (A rigorous check of it would be far too lengthy - even the computational evidence for it takes several weeks to obtain.)

Claim 4.2. *Suppose $n = 19$ or $n \geq 22$. The best coclass 3 groups of order 2^n depend on $n \pmod 4$ as follows:*

If $n \equiv 1 \pmod 4$, then they are descendants of the mainline group of order 2^{n-2} of family #34.

If $n \equiv 2 \pmod 4$, then they are descendants of the mainline group of order 2^{n-3} of family #29.

If $n \equiv 3 \pmod 4$, then they are descendants of the mainline group of order 2^{n-4} of family #29.

If $n \equiv 0 \pmod 4$, then they are descendants of the mainline group of order 2^{n-5} of family #34.

In each of the four cases there is a formula for $c_n^{(3)}$ of the form $c_n^{(3)} = 2^{n-13} + bx^3 + cx^2 + dx + e$, where $x = 2^{[n/4]}$ and where b, c, d, and e are rational numbers *depending only on what n is* $\pmod 4$. *For instance, it appears that for* $n \equiv 1 \pmod 4$, $b = 107/14336$, $c = -11/256$, $d = 119/16$, *and* $e = -81/7$.

Acknowledgments. The first author was partially supported by the Sloan Foundation and NSF grant DMS 96-22590. He thanks God for leading him to results. The second author was partially supported by the Henry Luce Foundation and NSF grant DMS-9709388. Both authors thank Eamonn O'Brien for his generous software help.

References

1. E. A. Bertram, *On large cyclic subgroups of finite groups*, Proc. Amer. Math. Soc. **56** (1976), 63-66.
2. W. Bosma and J. J. Cannon, *Handbook of Magma Functions* (1996), Sydney.
3. R. Brauer, *Representations of finite groups*, Lectures on modern mathematics (T. L. Saaty, ed.), vol. I, Wiley, New York, 1963.
4. P. Erdös and P. Turán, *On some problems of a statistical group theory IV*, Acta Math. Acad. Sci. Hung. **19** (1968), 413-435.
5. G. A. Fernández-Alcober and R.T.Shepherd, *On the order of p-groups of abundance zero*, J. Algebra **201** (1998), no. 2, 392-400.
6. G. Higman, *Enumerating p-Groups. I: Inequalities*, Proc. London Math. Soc. Series 3 **10** (1960), 24-30.
7. L. G. Kovaćs and C. R. Leedham-Green, *Some normally monomial p-groups of maximal class and large derived length*, Quart. J. Math. Oxford (2) **37** (1986), 49-54.
8. E. Landau, *Klassenzahl binärer quadratischer Formen von negativer Discriminante*, Math. Ann. **56** (1903), 674-678.
9. A. V. López and J. V. López, *Classification of finite groups according to the number of conjugacy classes*, Isr. J. Math. **51** (1985), 305-338.
10. A. V. López and J. V. López, *Classification of finite groups according to the number of conjugacy classes II*, Isr. J. Math. **56** (1986), 188-221.
11. M. F. Newman and E. A. O'Brien, *Classifying* 2*-groups by coclass*, Trans. Amer. Math. Soc. (to appear).
12. E. A. O'Brien, *The p-group generation algorithm.*, J. Symbolic Comput. **9** (1990), no. 5-6, 677-698.
13. J. Poland, *Two problems on finite groups with k conjugate classes*, J. Austral. Math. Soc. **8** (1968), 49-55.
14. L. Pyber, *Finite groups have many conjugacy classes*, J. London Math. Soc. (2) **46** (1992), 239-249.
15. A. Shalev, *The structure of finite p-groups: effective proof of the coclass conjectures*, Invent. Math. **115** (1994), 315-345.
16. G. J. Sherman, *A lower bound for the number of conjugacy classes in a finite nilpotent group*, Pac. J. Math. **80** (1979), 253-254.

Department of Mathematics
University of Illinois
Urbana, Illinois 61801
boston@math.uiuc.edu

Department of Mathematics and Statistics
University of Nebraska
Lincoln, Nebraska 68588
jwalker@math.unl.edu