Proceedings of the Edinburgh Mathematical Society (2011) **54**, 423–430
DOI:10.1017/S001309150900176X

GROUPS WITH FEW CONJUGACY CLASSES

LÁSZLÓ HÉTHELYI[1], ERZSÉBET HORVÁTH[1],
THOMAS MICHAEL KELLER[2] AND ATTILA MARÓTI[3]

[1]*Department of Algebra, Institute of Mathematics,*
Budapest University of Technology and Economics,
Műegyetem rkp. 3–9, 1521 Budapest, Hungary
(hethelyi@math.bme.hu; he@math.bme.hu)
[2]*Department of Mathematics, Texas State University,*
601 University Drive, San Marcos, TX 78666, USA (keller@txstate.edu)
[3]*MTA Alfréd Rényi Institute of Mathematics,*
Reáltanoda utca 13–15, 1053 Budapest, Hungary (maroti@renyi.hu)

(Received 7 December 2009)

Abstract Let G be a finite group, let p be a prime divisor of the order of G and let $k(G)$ be the number of conjugacy classes of G. By disregarding at most finitely many non-solvable p-solvable groups G, we have $k(G) \geqslant 2\sqrt{p-1}$ with equality if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$. This extends earlier work of Héthelyi, Külshammer, Malle and Keller.

Keywords: finite group; conjugacy classes; lower bound; Frobenius group

2010 *Mathematics subject classification:* Primary 20D10; 20D99

1. Introduction

Throughout this paper let G be a finite group, let p be a prime divisor of the order of G and let $k(H)$ be the number of conjugacy classes of a finite group H.

Héthelyi and Külshammer [**5**] showed that if G is a solvable group, then $k(G) \geqslant 2\sqrt{p-1}$. They mentioned that equality can occur when $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$. Later, Malle [**9**] proved that if G is not p-solvable, then $k(G) \geqslant 2\sqrt{p-1}$. Finally, Keller [**6**] showed that there exists a universal positive constant C such that whenever $p > C$, $k(G) \geqslant 2\sqrt{p-1}$ for any finite group G.

In this paper we extend these results to show the following.

Theorem 1.1. *By disregarding at most finitely many non-solvable p-solvable groups G, we have $k(G) \geqslant 2\sqrt{p-1}$ with equality if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$* and *$C_G(C_p) = C_p$.*

The semidirect products mentioned in Theorem 1.1 are Frobenius groups unless $p = 2$.

It is an open problem of Landau whether there are infinitely many primes p with the property that $p-1$ is a square. For more information, see [**11**, § 19].

The next three sections of this paper (titled 'Solvable groups', 'Non-p-solvable groups' and 'p-solvable groups') closely follow the relevant papers [**5**], [**9**] and [**6**], respectively, and thus follow in order of the publication of those papers. For this reason, we have tried to keep the notation and assumptions of these papers. Section 5 puts the results of the previous sections together to prove Theorem 1.1.

2. Solvable groups

In this section we prove the following theorem.

Theorem 2.1. *Let G be a finite solvable group. We then have $k(G) \geqslant 2\sqrt{p-1}$ with equality if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$.*

Proof. By [**5**] it follows that $k(G) \geqslant 2\sqrt{p-1}$, so it is sufficient to see when equality can occur.

We conduct a case study similar to that found in the proof in [**5**]. Let G be a solvable group with $2\sqrt{p-1}$ conjugacy classes, where $p-1$ is a square.

Step 1. There is a unique minimal normal subgroup N in G, where N is an elementary abelian p-subgroup of order p^n with $N \in \mathrm{Syl}_p(G)$ and G/N acts on N faithfully and irreducibly. (This conclusion can even be drawn in the more general setting when G is p-solvable. This will be used in § 4.)

Let N be a minimal normal subgroup of G. Then it is elementary abelian. If p divides $|G/N|$, then, by [**5**], we have $2\sqrt{p-1} \leqslant k(G/N) < k(G) = 2\sqrt{p-1}$, which is a contradiction. Thus p is not a divisor of $|G/N|$, and hence N is an elementary abelian p-group, N is the unique minimal normal subgroup in G, the normal subgroup $O_{p'}(G)$ is trivial and $N \in \mathrm{Syl}_p(G)$. Let $\bar{G} = G/N$. Then $\bar{G}$ acts on N irreducibly. This action is also faithful, since otherwise $C_{\bar{G}}(N) = \bar{T}$, and $C_G(N) = T \times N$, where $T \neq 1$ is a normal p'-subgroup in G, which is a contradiction.

Step 2. We may assume that $k(G) \geqslant 20$ and $p \geqslant 101$.

By [**14**, **15**] we have the following.

(1) If $p = 2$, then $k(G) = 2$ and $G = C_2$.

(2) If $p = 5$, then $k(G) = 4$ and $G = D_{10}$.

(3) If $p = 17$, then $k(G) = 8$ and $G = C_{17} \rtimes C_4$.

(4) If $p = 37$, then $k(G) = 12$ and $G = C_{37} \rtimes C_6$.

The next smallest prime p, where $p-1$ is a square, is 101, in which case $k(G) = 20$.

Step 3. If $\bar{G} = G/N$ is isomorphic to a subgroup of the group of semilinear transformations $\Gamma(p^n) = \{x \mapsto a\sigma(x) \mid a \in \mathrm{GF}(p^n),\ a \neq 0,\ \sigma \in \mathrm{Gal}(\mathrm{GF}(p^n)/\mathrm{GF}(p))\}$, then G is of the required type.

https://doi.org/10.1017/S001309150900176X Published online by Cambridge University Press

In this case,

$$2\sqrt{p-1} = k(G) \geqslant \frac{p^n - 1}{nx} + \frac{x}{n}, \tag{2.1}$$

where x is the order of the cyclic normal subgroup $\bar{X}$ of $\bar{G}$ of index at most n, corresponding to scalar multiplications. The right-hand side of (2.1) takes its minimum when $x = \sqrt{p^n - 1}$ so we get $(2/n)\sqrt{p^n - 1} \geqslant 2\sqrt{p-1}$. Since the left-hand side of (2.1) is also $2\sqrt{p-1}$, we have equality and thus $n = 1$, i.e. $|N| = p$, $x = \sqrt{p-1}$ and $\bar{G} = \bar{X}$. Hence $G = NK$, where K is a complement of order x. Since every conjugacy class contained in N is of length $\sqrt{p-1}$, we have that G is a Frobenius group of the required form.

Step 4. If $\bar{G} = G/N$ is not isomorphic to a subgroup of $\Gamma(p^n)$, then $n \geqslant 4$.

$n = 2$ cannot hold, since, by Theorem 2.11 of [**10**], (a) or (c) of that theorem would occur, and in these cases equality cannot hold for $p \geqslant 101$.

$n = 3$ cannot hold either, since then, by Theorem 2.12 of [**10**], (a) or (c) of that theorem would occur, and in these cases equality cannot occur for $p \geqslant 101$.

Thus $n \geqslant 4$.

Step 5. N cannot be a primitive module over $\mathrm{GF}(p)\bar{G}$.

Suppose that N is a primitive module over $\mathrm{GF}(p)\bar{G}$. Then, by [**13**], we have $k(G) \geqslant p^{n/2}/12n > 2\sqrt{p-1}$, since $p \geqslant 101$, which is a contradiction.

Step 6. $|\bar{G}| \geqslant \frac{1}{2}p^{n-(1/2)}$.

Since $k(G) = 2\sqrt{p-1}$, the normal subgroup N contains fewer than $2\sqrt{p}$ conjugacy classes, each of which has length at most $|\bar{G}|$. Thus $p^n = |N| \leqslant 2\sqrt{p}|\bar{G}|$, which implies the above inequality.

Step 7. N cannot be an imprimitive module over $\mathrm{GF}(p)\bar{G}$.

Suppose that N is an imprimitive module over $\mathrm{GF}(p)\bar{G}$. Then $N = N_1 \times \cdots \times N_r$, where the N_i are permuted by $\bar{G}$. Let r be as large as possible. Let $H_i = N_G(N_i)$, $K_i = C_G(N_i)$ and $H = H_1 \cap \cdots \cap H_r$. Then $N = C_G(N) = K_1 \cap \cdots \cap K_r$. Then $r \leqslant k(G) = 2\sqrt{p-1}$. Let $|N_i| = p^m$. Since $G/H \leqslant S_r$, by Theorem 36.2 of [**3**], we have $|G/H| \leqslant 3^{r-1}$.

If $m = 1$ and $n = r$, then as in [**5**] one gets that the factor group H/N contains at least $p^{n-(1/2)}/(2 \cdot 9^{n-1})$ conjugacy classes of $\bar{G}$. Thus

$$2\sqrt{p-1} = k(G) > k(\bar{G}) \geqslant p^{n-(1/2)}/(2 \cdot 9^{n-1}).$$

This is impossible since $p \geqslant 101$ and $n \geqslant 4$.

If $m = 2$ and $n = 2r$, then one can apply Theorem 2.11 of [**10**]. If H_i/K_i is isomorphic to a subgroup of $\Gamma(p^2)$, or of $(Z_{p-1} \times Z_{p-1}){:}Z_2$, then H_i/K_i contains an abelian normal subgroup L_i/K_i of index at most 2. Let $L = L_1 \cap \cdots \cap L_r$. Then $|G{:}L| \leqslant 2^r \cdot 3^{r-1}$ and L/N contains at least $p^{n-(1/2)}/(2^{2r+1} \cdot 9^{r-1})$ conjugacy classes of $\bar{G}$, hence this quantity is strictly smaller than $2\sqrt{p-1}$, which cannot be true, since $p \geqslant 101$ and $n \geqslant 4$. If case (c) of Theorem 2.11 of [**10**] occurs, then $|H_i/Z_i| \leqslant 24$, where $Z_i = Z(H_i/K_i)$ for $i = 1, \ldots, r$. Let $Z = Z_1 \cap \cdots \cap Z_r$. Then $|\bar{G}{:}\bar{Z}| \leqslant 3^{r-1} \cdot 24^r$, which by Step 6 gives $2\sqrt{p-1} > k(\bar{G}) \geqslant p^{2r-(1/2)}/(2 \cdot 9^{r-1} \cdot 24^r)$, which cannot hold since $p \geqslant 101$ and $n \geqslant 4$.

Let $m \geqslant 3$.

If H_1/K_1 is isomorphic to a subgroup of $\Gamma(p^m)$, then $k(H_1) \geqslant 2\sqrt{p^m - 1}/m$. We also have $k(H_1) \leqslant |G{:}H_1|k(G) = r2\sqrt{p-1} < 4(p-1)$, which is impossible since $p \geqslant 101$ and $m \geqslant 3$.

If H_1/K_1 is not isomorphic to a subgroup of $\Gamma(p^m)$, then, by [**13**], it has at least $p^{m/2}/12m$ orbits on the non-identity elements of N_1, and G therefore also has at least as many different orbits on N. Thus $2\sqrt{p-1}k(G) \geqslant p^{m/2}/12m$, which is impossible since $m \geqslant 3$ and $p \geqslant 101$. Hence we are done. □

3. Non-p-solvable groups

In this section we prove the following theorem.

Theorem 3.1. *If G is a finite group that is not p-solvable, then $k(G) > 2\sqrt{p-1}$.*

Note that if p is a prime for which G is not p-solvable, then G has a non-cyclic composition factor S with p a factor of $|S|$. For a finite group X, let $k^*(X)$ be the number of $\mathrm{Aut}(X)$-orbits on X.

Lemma 3.2. *If G is a finite group that is not p-solvable and not simple, then $k(G) > 2\sqrt{p-1}$.*

Proof. We follow the proof of Lemma 2.5 of [**12**].

Let S be a non-abelian composition factor of G whose order is divisible by p. Let us consider a chief series $G = G_0 > G_1 > \cdots > G_r = 1$. Each of the factor groups G_i/G_{i+1} is isomorphic to a direct power of some simple group S_i. By the Jordan–Hölder Theorem, at least one of these simple groups, say S_j, is isomorphic to S.

Let us consider the group G/G_{j+1}. This group has a normal subgroup G_j/G_{j+1} that is a direct product of isomorphic copies of S, say $E_1 \times \cdots \times E_m$. It is well known that the E_i are the only minimal normal subgroups of G_j/G_{j+1}. Therefore, conjugation by elements of G/G_{j+1} permutes the E_i among themselves. It follows that if $e^g = f$ for some e, $f \in E_1$ and $g \in G/G_{j+1}$, then g normalizes E_1 and therefore e and f lie in the same automorphism orbit of E_1. This gives us

$$k(G) \geqslant k(G/G_{j+1}) \geqslant k^*(E_1) = k^*(S).$$

By [**9**, p. 656] we know that $k^*(S) \geqslant 2\sqrt{p-1}$. Hence it is sufficient to show that $k(G) \neq 2\sqrt{p-1}$.

If $j+1 \neq r$, then $k(G) > k(G/G_{j+1})$ and so we are done in this case. Hence we may assume that $j+1 = r$. First suppose that $G \neq G_j$. In this case (since G_j is normal in G), the invariant $k(G)$ is larger than the number of G-orbits on G_j, which in turn is greater than or equal to $k^*(E_1) = k^*(S) \geqslant 2\sqrt{p-1}$. Finally, we may assume that $G = G_j = E_1 \times \cdots \times E_m$ with $m > 1$. In this case,

$$k(G) = k(E_1)^m > k^*(E_1) = k^*(S) \geqslant 2\sqrt{p-1}.$$

□

Table 1. *Exceptions in Lemma 3.4*

G	$k(G)$	$2\sqrt{p-1}$
$L_2(5)$	5	4
$L_2(9)$	7	4
$U_3(11)$	48	12
$U_3(17)$	106	8
$U_4(2)$	20	4
$PSp_4(2)'$	7	4
$PSp_4(3)$	20	4
$PSp_8(2)$	81	8
$P\Omega_4^-(4)$	17	8
$P\Omega_4^-(13)$	87	8
$P\Omega_6^-(2)$	20	4
$P\Omega_8^-(2)$	39	8
$F_4(2)$	95	8

In view of Lemma 3.2, in order to prove Theorem 3.1 it is sufficient to assume that G is a non-abelian finite simple group and that p is a divisor of $|G|$. On [**9**, p. 656] it is shown that $k(G) \geqslant k^*(G) \geqslant 2\sqrt{p-1}$. Hence we may also assume that p is the largest prime divisor of $|G|$ and it is sufficient to conclude that $k(G) \neq 2\sqrt{p-1}$.

Lemma 3.3. *Let us use the notation and assumptions introduced above. Let G be an alternating group, a sporadic simple group or the Tits group. Then $k(G) \neq 2\sqrt{p-1}$.*

Proof. Let $G = A_n$ with $n \geqslant 5$. If n is even, then the $n-1$ partitions

$$(1,1,1,\dots,1),(2,2,1,\dots,1),\dots,(n-2,2),(n-1,1)$$

of n label conjugacy classes of S_n that lie in A_n. If n is odd, then the $n-1$ partitions

$$(1,1,1,\dots,1),(2,2,1,\dots,1),\dots,(n-2,1,1),(n)$$

of n label conjugacy classes of S_n that lie in A_n. This gives $k(A_n) \geqslant n-1$. Now $n-1 > 2\sqrt{n-1} \geqslant 2\sqrt{p-1}$ unless $n=5$. For $n=5$, inspection shows that $k(A_5) = 5 \neq 4 = 2\sqrt{5-1}$.

Let G be a sporadic simple group or the Tits group. Then, by [**2**], $\sqrt{p-1}$ is not an integer except if $G = \mathrm{He}$, in which case $2\sqrt{p-1} = 8$. But $k(\mathrm{He}) = 33$, again by [**2**]. □

From now on, let G be a finite simple group of Lie type. In this case we use [**9**, p. 656]. Let H be a group of Lie type of rank r over the field of q elements with $H/Z(H) = G$. Then, by Theorem 3.7.6 of [**1**], H has at least q^r semisimple conjugacy classes; therefore G has at least $q^r/|Z(H)| \geqslant q^r/|M(G)|$ conjugacy classes, where $M(G)$ is the Schur multiplier of G. Moreover, p is bounded from above by the order of the largest maximal torus and this has at most $(q+1)^r$ elements. Thus if $q^r > 2|M(G)|\sqrt{(q+1)^r-1}$ or $\sqrt{p-1}$ is not an integer, then $k(G) \neq 2\sqrt{p-1}$.

Lemma 3.4. *Let G be a finite simple group of Lie type of rank r over the field of q elements. If $q^r \leqslant 2|M(G)|\sqrt{(q+1)^r - 1}$ and $\sqrt{p-1}$ is an integer, then (up to isomorphism) $G = L_2(5)$, $L_2(9)$, $U_3(11)$, $U_3(17)$, $U_4(2)$, $PSp_4(2)'$, $PSp_4(3)$, $PSp_8(2)$, $P\Omega_4^-(4)$, $P\Omega_4^-(13)$, $P\Omega_6^-(2)$, $P\Omega_8^-(2)$ or $F_4(2)$.*

Proof. This lemma was proved using [**7**, Tables 5.1.A and 5.1.B and Theorem 5.1.4] and [**4**]. □

By going through (using [**4**]) the exceptions in Lemma 3.4 (see Table 1), we are able to finish the proof of Theorem 3.1.

4. *p*-solvable groups

In this section we prove the following result.

Theorem 4.1. *There exists a constant C such that the following holds. If p is a prime number with $p > C$ and G is a p-solvable group of order divisible by p, then*

$$k(G) \geqslant 2\sqrt{p-1}$$

with equality if and only if $\sqrt{p-1}$ is an integer, $G = C_p \rtimes C_{\sqrt{p-1}}$ and $C_G(C_p) = C_p$.

Proof. From [**6**] we already know that there exists a constant C such that if p is a prime with $p > C$ and G is a finite group of order divisible by p, then $k(G) \geqslant 2\sqrt{p-1}$.

Hence we now assume that H is a p-solvable group with p being a prime such that $p > C$, p divides $|H|$ and $k(H) = 2\sqrt{p-1}$, and it suffices to show that if C was chosen large enough, then H is necessarily $C_p \rtimes C_{\sqrt{p-1}}$.

To prove this we first claim that there is a unique minimal normal subgroup V in H and that V is an elementary abelian p-group and that H/V is a p'-group that acts faithfully and irreducibly on V. (This claim was already proved for solvable G in Step 1 of § 2.)

To see this, let V be a minimal abelian normal subgroup of H. If p divides $|H/V|$, then by [**6**] we have $2\sqrt{p-1} \leqslant k(G/V) < k(G) = 2\sqrt{p-1}$, which is a contradiction. Thus p does not divide $|H/V|$. As p divides $|H|$, we conclude that p divides $|V|$, and as H is p-solvable, we conclude that V is an elementary abelian p-group. Since V was chosen arbitrarily, this also shows that V is unique. This proves the above claim.

Now (by the Schur–Zassenhaus Theorem) let G be a complement of V in H. Then $H = GV$, and so we are exactly in the situation of Theorem 2.6 of [**6**]. Let $|V| = p^m$. If $m = 1$, then clearly H is a Frobenius group with kernel V and

$$2\sqrt{p-1} = k(H) = k(GV) = (p-1)/|G| + |G|.$$

Then $|G|$ is a solution of the quadratic equation

$$0 = x^2 - 2\sqrt{p-1}x + p - 1 = (x - \sqrt{p-1})^2.$$

Thus $|G| = \sqrt{p-1}$ and H has the structure as stated in the theorem.

So now suppose $m \geqslant 2$. From here on we proceed exactly as in the proof of Theorem 2.6 of [**6**] and always get a contradiction, assuming C has been chosen sufficiently large. Only minimal changes in the proof of Theorem 2.6 of [**6**] are required here, such as changing some '$\geqslant$' inequalities to strict '$>$' inequalities, so we leave this verification to the reader. The only thing we point out here is that if $n = 2$ and $|V_1| = p$ (for n and V_1 as in the proof of Theorem 2.6 of [**6**]), then we know from Theorem 2.1 that $k(G) > 2\sqrt{p-1}$, which is also a contradiction. We are done. $\square$

5. Proof of Theorem 1.1

By Theorems 2.1, 3.1 and 4.1, it is sufficient to assume that G is non-solvable and p-solvable, where p is a prime divisor of the order of G with $p \leqslant C$, where C is a suitable constant in the statement of Theorem 4.1. Assume that $C \geqslant 2$. Furthermore, we may assume that $k(G) < 2\sqrt{C-1}$. But, by a theorem of Landau [**8**] that states that there are only at most finitely many finite groups with a fixed number of conjugacy classes, we see that there are only at most finitely many possibilities for G. This proves Theorem 1.1.

Acknowledgements. All authors were supported by OTKA T049841. L.H. and E.H. were supported by OTKA K77476. The research of T.M.K. was supported by NSA Standard Grant MSPF 08G-206. The research of A.M. was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme and partially by OTKA NK72523.

Part of this work was done while T.M.K. was visiting the Budapest University of Technology and Economics and the Alfréd Rényi Institute of Mathematics in Budapest for a week in October 2009. He thanks both institutions for their hospitality.

References

1. R. W. Carter, *Finite groups of Lie type* (Wiley, 1985).
2. J. H. Conway, R. T Curtis, S. P Norton, R. A Parker and R. A. Wilson, *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups* (Oxford University Press, 1985).
3. L. Dornhoff, *Group representation theory* (North-Holland, Amsterdam, 1982).
4. GAP Group, GAP—groups, algorithms, and programming, Version 4.4 (available at www.gap-system.org; 2005).
5. L. Héthelyi and B. Külshammer, On the number of conjugacy classes of a finite solvable group, *Bull. Lond. Math. Soc.* **32** (2000), 668–672.
6. T. M. Keller, Lower bounds for the number of conjugacy classes of finite groups, *Math. Proc. Camb. Phil. Soc.* **147** (2009), 567–577.
7. P. B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Notes, Volume 129 (Cambridge University Press, 1990).
8. E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante, *Math. Annalen* **56** (1903), 671–676.
9. G. Malle, Fast-einfache Gruppen mit langen Bahnen in absolut irreduzibler Operation, *J. Alg.* **300** (2006), 655–672.
10. O. Manz and T. Wolf, *Representations of solvable groups* (Cambridge University Press, 1993).

11. J. Pintz, Landau's problems on primes, *J. Théorie Nombres Bordeaux* **21**(2) (2009), 357–404.
12. L. Pyber, Finite groups have many conjugacy classes, *J. Lond. Math. Soc.* **46** (1992), 239–249.
13. S. M. Seager, The rank of a finite primitive solvable permutation group, *J. Alg.* **105** (1987), 389–394.
14. A. Vera López and J. Vera López, Classification of finite groups according to the number of conjugacy classes, I, *Israel J. Math.* **51** (1985), 305–338.
15. A. Vera López and J. Vera López, Classification of finite groups according to the number of conjugacy classes, II, *Israel J. Math.* **56** (1986), 188–221.