GROUPS WITH FEW CONJUGACY CLASSES

L. HÉTHELYI, E. HORVÁTH, T. M. KELLER, A. MARÓTI

ABSTRACT. Let G be a finite group, p a prime divisor of the order of G, and $k(G)$ the number of conjugacy classes of G. By disregarding at most finitely many non-solvable p-solvable groups G, we have $k(G) \geq 2\sqrt{p-1}$ 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.

1. INTRODUCTION

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

Héthelyi and Külshammer [5] showed that if G is a solvable group then $k(G) \geq 2\sqrt{p-1}$. 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 [10] proved that if G is not p-solvable then $k(G) \geq 2\sqrt{p-1}$. Finally Keller [6] showed that there exists a universal positive constant C so that whenever $p > C$ then $k(G) \geq 2\sqrt{p-1}$ for any finite group G.

In this paper we extend these results to show

Theorem 1.1. *By disregarding at most finitely many non-solvable p-solvable groups G, we have $k(G) \geq 2\sqrt{p-1}$ 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 Section 19 of [11].

The next three sections of this paper (Solvable groups, Non-p-solvable groups, p-solvable groups) are in chronological order and follow closely the relevant papers [5], [10], and [6], respectively. For this reason we tried to keep the notations and assumptions of these papers. The fifth section puts the results of the previous sections together to prove Theorem 1.1.

2. SOLVABLE GROUPS

In this section we prove the following

[1]All authors were supported by OTKA T049841.

[2]The first and second authors were supported by OTKA K77476.

[3]The research of the third author was supported by NSA Standard Grant MSPF 08G-206.

[4]The research of the fourth author was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme and partially by OTKA NK72523.

[5]Mathematics Subject Classification 2010: 20D10, 20D99

Date: 6th of December, 2009.

Theorem 2.1. *Let G be a finite solvable group. Then we have $k(G) \geq 2\sqrt{p-1}$ 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 $k(G) \geq 2\sqrt{p-1}$, hence it is sufficient to see when equality can occur.

We make a similar case study as it was in the proof of [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 be drawn even in the more general setting when G is p-solvable. This will be used in Section 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 $2\sqrt{p-1} \leq k(G/N) < k(G) = 2\sqrt{p-1}$, 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 $\overline{G} = G/N$. Then $\overline{G}$ acts on N irreducibly. This action is also faithful, since otherwise $C_{\overline{G}}(N) = \overline{T}$, 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 $k(G) \geq 20$ and $p \geq 101$.

By [14] 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 $\overline{G} = G/N$ is isomorphic to a subgroup of the group of semilinear transformations $\Gamma(p^n) = \{x \mapsto a\sigma(x) | a \in GF(p^n), a \neq 0, \sigma \in \mathrm{Gal}(GF(p^n)/GF(p))\}$ then G is of the required type.

In this case

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

where x is the order of the cyclic normal subgroup $\overline{X}$ of $\overline{G}$ of index at most n, corresponding to scalar multiplications. The right-hand-side of (1) takes its minimum when $x = \sqrt{p^n - 1}$ so we get $(2/n)\sqrt{p^n - 1} \geq 2\sqrt{p-1}$. Since the left-hand-side of (1) is also $2\sqrt{p-1}$, we have equality and thus $n = 1$, i.e. $|N| = p$, $x = \sqrt{p-1}$, and $\overline{G} = \overline{X}$. 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 $\overline{G} = G/N$ is not isomorphic to a subgroup of $\Gamma(p^n)$, then $n \geq 4$.

$n = 2$ cannot hold, since by Theorem 2.11. of [9] (a) or (c) would occur, and in these cases equality cannot hold for $p \geq 101$.

$n = 3$ cannot hold either, since then by Theorem 2.12 of [9] (a) or (c) would occur, and in these cases equality cannot occur for $p \geq 101$.

Thus $n \geq 4$.

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

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

Step 6: $|\overline{G}| \geq \frac{1}{2}p^{n-(1/2)}$.

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

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

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

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 $\overline{G}$. Thus

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

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

If $m = 2$ and $n = 2r$, then one can apply Theorem 2.11 of [9]. 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 $L = L_1 \cap \ldots \cap L_r$. Then $|G : L| \leq 2^r \cdot 3^{r-1}$ and L/N contains at least $p^{n-(1/2)}/(2^{2r+1} \cdot 9^{r-1})$ conjugacy classes of $\overline{G}$, hence this quantity is strictly smaller than $2\sqrt{p-1}$, which cannot be true, since $p \geq 101$ and $n \geq 4$. If the case (c) in Theorem 2.11 of [9] occurs, then $|H_i/Z_i| \leq 24$, where $Z_i = Z(H_i/K_i)$, for $i = 1, \ldots, r$. Let $Z = Z_1 \cap \ldots \cap Z_r$ then $|\overline{G} : \overline{Z}| \leq 3^{r-1} \cdot 24^r$ which by Step 6 gives $2\sqrt{p-1} > k(\overline{G}) \geq p^{2r-(1/2)}/(2 \cdot 9^{r-1} \cdot 24^r)$, which cannot hold since $p \geq 101$ and $n \geq 4$.

Let $m \geq 3$.

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

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 nonidentity elements of N_1, thus G also has at least so many different orbits on N. Thus $2\sqrt{p-1}k(G) \geq p^{m/2}/12m$, which is impossible since $m \geq 3$ and $p \geq 101$. Hence we are done. □

3. Non-p-solvable groups

In this section we prove

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 $G = G_0 > G_1 > \ldots > G_r = 1$. 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} which is a direct product of isomorphic copies of S, say $E_1 \times \ldots \times E_m$. It is well known that the E_i's 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's 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

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

By Page 656 of [10] we know that $k^*(S) \geq 2\sqrt{p-1}$. 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 or equal to $k^*(E_1) = k^*(S) \geq 2\sqrt{p-1}$. Finally, we may assume that $G = G_j = E_1 \times \ldots \times E_m$ with $m > 1$. In this case

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

□

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 p is a divisor of $|G|$. On Page 656 of [10] it is shown that $k(G) \geq k^*(G) \geq 2\sqrt{p-1}$. 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 notations 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 $n \geq 5$. If n is even, then the $n-1$ partitions

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

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

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

of n label conjugacy classes of S_n which lie in A_n. This gives $k(A_n) \geq n-1$. Now $n-1 > 2\sqrt{n-1} \geq 2\sqrt{p-1}$ 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 Page 656 of [10]. 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 $q^r/|Z(H)| \geq q^r/|M(G)|$ 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 $q^r \leq 2|M(G)|\sqrt{(q+1)^r - 1}$ 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 Tables 5.1.A, 5.1.B and Theorem 5.1.4 of [7] and [4]. □

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

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

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*

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

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

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 necessarily is $C_p \rtimes C_{\sqrt{p-1}}$.

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 H/V is a p'-group which acts faithfully and irreducibly on V. (This claim was already proved for solvable G in Step 1 of Section 2.)

To see this let V be a minimal abelian normal subgroup of H. If p divides $|H/V|$, then by [6] we have $2\sqrt{p-1} \leq k(G/V) < k(G) = 2\sqrt{p-1}$, 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 quadradic 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 $m \geq 2$. 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 "$\geq$"-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 $k(G) > 2\sqrt{p-1}$, also a contradiction. We are done. □

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 $p \leq C$ where C is a suitable constant in the statement of Theorem 4.1. Assume that $C \geq 2$. Furthermore we may assume that $k(G) < 2\sqrt{C-1}$. But, by a theorem of Landau [8] which 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.

Acknowledgments

Part of this work was done while the third author visited the Budapest University of Technology and Economics and the Alfréd Rényi Institute of Mathematics in Budapest for a week in October 2009, and he wishes to thank both institutions for their hospitality.

References

[1] Carter, R. W. Finite groups of Lie type, Wiley-Interscience, New York, 1985.
[2] Conway, J. H; Curtis, R. T; Norton, S. P; Parker, R. A; Wilson, R. A. Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. *Oxford University Press*, Eynsham, (1985).
[3] Dornhoff, L. Group representation theory, North Holland, Amsterdam, 1982.
[4] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version 4.4*; 2005, (http://www.gap-system.org).
[5] Héthelyi, L.; Külshammer, B. On the number of conjugacy classes of a finite solvable group. *Bull. London Math. Soc.* **32** (2000), 668-672.
[6] Keller, T. M. Lower bounds for the number of conjugacy classes of finite groups. *Math. Proc. Camb. Phil. Soc.* **147**, (2009), 567-577.
[7] Kleidman, P. B.; Liebeck, M. W. The subgroup structure of the finite classical groups. *London Math. Soc. Lecture Notes, Cambridge Univ. Press* **129**, (1990).
[8] Landau, E. Über die Klassenzahl der binären quadratischen Formen von negativer Diskriminante. *Math. Ann.* **56** (1903), 671-676.
[9] Manz, O.; Wolf, T. Representations of solvable groups. Cambridge University Press 1993.
[10] Malle, G. Fast-einfache Gruppen mit langen Bahnen in absolut irreduzibler Operation. *J. Algebra* **300** (2006), 655-672.
[11] Pintz, J. Landau's problems on primes. Preprint 2009.

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

[13] Seager, S. M. The rank of a finite primitive solvable permutation group. *J. Algebra* **105** (1987) 389–394.

[14] Vera Lopez, A.; Vera Lopez, J. Classification of finite groups according to the number of conjugacy classes I-II. *Israel J. Math.* **51** (1985) 305–338; **56** (1986) 188–221.

László Héthelyi, Department of Algebra, Institute of Mathematics, Budapest University of Technology and Economics, H building IV. floor 45, Hungary.

E-mail address: hethelyi@math.bme.hu

Erzsébet Horváth, Department of Algebra, Institute of Mathematics, Budapest University of Technology and Economics, H building IV. floor 45, Hungary.

E-mail address: he@math.bme.hu

Thomas Michael Keller, Department of Mathematics, Texas State University 601 University Drive, San Marcos, TX 78666, USA.

E-mail address: keller@txstate.edu

Attila Maróti, MTA Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary.

E-mail address: maroti@renyi.hu