PACIFIC JOURNAL OF MATHEMATICS
Vol. 55, No. 2, 1974

A DENSITY THEOREM ON THE NUMBER OF CONJUGACY CLASSES IN FINITE GROUPS

EDWARD A. BERTRAM

For each finite group G with $k(G)$ conjugacy classes and order g, it is well known that $g < 2^{2^k}$. On the other hand, all groups with a given small k ($\leqq 8$) have been determined, and these studies, along with the result that if G is nilpotent then $g < 2^k$, strongly suggest that the bound can be significantly improved. We prove that for each $c_2 < \log 2$, almost all integers $g \leqq n$, as $n \to \infty$, have the property that for each G of order g, $k(G) > (\log n)^{c_2}$.

The question of whether there exist finite groups G of arbitrarily large order $|G|$ with a fixed number of conjugacy classes k was first asked by Frobenius, and answered in the negative in 1903 by E. Landau [5], using the class equation. In 1919 G. A. Miller [6] discussed a definite upper bound for $|G|$ in terms of k; in 1968 P. Erdös and P. Turán [3], and independently M. Newman [8] gave proofs that $k(G) > \log_2 \log_2 |G|$, again all using Landau's method. When G is a p-group, P. Hall (unpublished) and later J. Poland [9] had already obtained a parametric equation for $k(G)$, from which it readily follows that if G is *nilpotent*, then $k(G) > \log_2 |G|$; however the latter inequality does not hold for all solvable groups. R. Brauer [1, p. 137] has asked for a substantial improvement on the bounds obtained by Landau's method, and our main theorem shows that for "most" group orders there is indeed a substantial improvement:

THEOREM. *For each $c_2 < \log 2$, almost all integers $g \leqq n$, as $n \to \infty$, have the property that if G is a group of order g, then $k(G) > (\log n)^{c_2}$.*

Thus, if we let $N(n)$ denote the number of integers $g \leqq n$ such that $k(G) > (\log n)^{c_2}$ for each group G of order g, we will prove that $\lim_{n\to\infty} N(n)/n = 1$.

A cryptic remark by G. A. Miller [7, p. 361, line 21] led us[1] to the following lemma, which has apparently never been formally stated, but is basic to the entire discussion. Let $d(m)$ denote the number of divisors of m, G a finite group, of order $|G|$, and partitioned into $k(G)$ conjugacy classes; for p a prime $P(p'; |G|)$ denotes

[1] The author would like to thank Professor Robert Gilman for helpful comments here.

the number of primes $\neq p$ which divide $|G|$ but do not divide $p-1$. For H a subgroup of G, $N(H)$ denotes the normalizer of H in G, and $C(H)$ the centralizer, that is $N(H) = \{x \in G \mid xH = Hx\}$ and $C(H) = \{x \in G \mid xh = hx \text{ for all } h \in H\}$. $\langle x \rangle$ denotes the subgroup generated by x.

LEMMA 1. *Suppose* $p \mid |G|$. *Then* $k(G) \geqq \min_{m \mid p-1}\{(p-1)/m + d(m)\} + P(p'; |G|)$.

Proof. Suppose the prime $p \mid |G|$ and let x be an element in G of order p. To see how the elements of $\langle x \rangle$ are partitioned into (parts of the) conjugacy classes of G, we examine $N(\langle x \rangle)$ since, for $r, s \not\equiv 0 \pmod p$, $z^{-1}x^r z = x^s$ implies $z^{-1}\langle x \rangle z = \langle x \rangle$. Now $C(\langle x \rangle)$ is a normal subgroup of $N(\langle x \rangle)$; let m denote the index of $C(\langle x \rangle)$ in $N(\langle x \rangle) = C(\langle x \rangle) \dot{\cup} Cy_1 \dot{\cup} Cy_2 \dot{\cup} \cdots \dot{\cup} Cy_{m-1}$. Then the maximum number of elements in $\langle x \rangle$ which lie in the same conjugacy class in G is $\leqq m$. For if $z^{-1}x^r z = x^s$, then $z \in N(\langle x \rangle) \Rightarrow z = c$ or cy_j for some $c \in C(\langle x \rangle) = C(x)$, and $1 \leqq j \leqq m-1$. Thus we have a mapping from the set of all x^r which are conjugate to x^s into the set of coset representatives $\{e, y_1, y_2, \cdots, y_{m-1}\}$. This mapping is well defined, since if $z_1^{-1}x^r z_1 = x^s$ and $z_2^{-1}x^r z_2 = x^s$, then $z_2(z_1^{-1}x^r z_1)z_2^{-1} = x^r \Rightarrow z_2 z_1^{-1} \in C(x^r) \Rightarrow z_2 z_1^{-1} \in C(x)$, that is z_1 and z_2 lie in the same coset of $C(\langle x \rangle)$. The mapping is also one-to-one, since if $z^{-1}x^r z = x^s = z_0^{-1}x^t z_0$ with $r, s, t \not\equiv 0 \pmod p$, then $z = cy_i$, $z_0 = c_0 y_j$ with $c, c_0 \in C(x) \Rightarrow y_i^{-1}x^r y_i = y_i^{-1}(c^{-1}x^r c)y_i = z^{-1}x^r z = x^s = z_0^{-1}x^t z_0 = y_j^{-1}(c_0^{-1}x^t c_0)y_j = y_j^{-1}x^t y_j$. Thus $y_i = y_j \Rightarrow x^t = x^r$. We have now shown that the elements of $\langle x \rangle$ are partitioned into *at least* $(p-1)/m + 1$ (subsets of) conjugacy classes in G, counting the identity class.

Since $N(\langle x \rangle)/C(\langle x \rangle)$ is isomorphic to a subgroup of the cyclic group of automorphisms of $\langle x \rangle$, the factor group is cyclic and generated by $yC(x)$, for some $y \in N(\langle x \rangle)$. Since $N(\langle x \rangle) = \langle C(x), \langle y \rangle \rangle$ we have, either by counting or an Isomorphism Theorem, that

$$\frac{|\langle y \rangle|}{|C(x) \cap \langle y \rangle|} = \frac{|\langle C(x), \langle y \rangle \rangle|}{|C(x)|} = m\ .$$

Hence $m \mid |\langle y \rangle|$, $\langle y \rangle$ has a cyclic subgroup of order m, and for *each* different divisor l of m we have an element of order l. Since elements of different orders must lie in different classes of G, we have $d(m) - 1$ additional conjugacy classes. These have not been counted earlier since each nonidentity element in $\langle x \rangle$ has order p, whereas each $l \mid p-1$. Finally, every prime $q \neq p$ such that $q \mid |G|$ and $q \nmid m$ provides at least one new class, and then the same is true for each prime $q \neq p$ such that $q \mid |G|$ and $q \nmid p-1$. We have shown that for each prime $p \mid |G|$, $k(G)$ satisfies $k(G) \geqq (p-1)/m + d(m) + P(p'; |G|)$ for some $m \mid p-1$. But then $k(G) \geqq \min_{m \mid p-1}\{(p-1)/m + d(m)\} + P(p'; |G|)$ and the proof of the lemma is complete.

EXAMPLES. $|G| = 60 \Rightarrow k(G) \geqq 5$; $|G| = 156 \Rightarrow k(G) \geqq 6$.

Let $\nu(n)$ denote the number of distinct prime factors of n, and $d(m)$ the total number of divisors of m; p_j is the jth prime.

LEMMA 2. (Hardy and Wright, [4, § 18.1]). *Given* $\varepsilon > 0$,

(a) *there exists a constant* $c(\varepsilon) > 1$ *such that* $d(n) < c(\varepsilon)n^{\varepsilon}$ *for all* $n \geqq 2$; *and*

(b) $d(n) < n^{\varepsilon}$ *for all sufficiently large* n.

LEMMA 3. *Given* $\varepsilon > 0$, *there exists a positive constant* $c_0(\varepsilon) < 1$ *such that*

$$\min_{m \mid n}\left\{d(m) + \frac{n}{m}\right\} > c_0 2^{(1-\varepsilon)\nu(n)} \text{ for all } n \geqq 2 .$$

Furthermore, for sufficiently large $\nu(n)$, *this minimum is* $> 2^{(1-\varepsilon)\nu(n)}$.

Proof. We prove the first part; the second is proved similarly. If $\nu(n/m) \leqq \varepsilon\nu(n)$ then $d(m) \geqq 2^{\nu(m)} \geqq 2^{\nu(n)-\nu(n/m)} \geqq 2^{(1-\varepsilon)\nu(n)}$. If $\nu(n/m) > \varepsilon\nu(n)$, then $d(n/m) \geqq 2^{\nu(n/m)} > 2^{\varepsilon\nu(n)}$. But now from (a) of Lemma 2, $c(\varepsilon)\cdot(n/m)^{\varepsilon} > d(n/m) > 2^{\varepsilon\nu(n)}$ or $n/m > (1/(c(\varepsilon)))^{1/\varepsilon}2^{\nu(n)}$. Thus the inequality to be proved holds with $c_0(\varepsilon) = (1/(c(\varepsilon)))^{1/\varepsilon}$. That $1-\varepsilon$ may not be replaced by 1, no matter how small $c_0 > 0$, is seen by considering the sequence $n = \prod_{j=1}^{l} p_j$ as $l \to \infty$. If we let $m = \prod_{j=l-v+1}^{l} p_j$, v to be chosen such that, for example $l - v = [\sqrt{l}\,]$, then

$$\min_{m \mid n}\left\{d(m) + \frac{n}{m}\right\} \leqq 2^{v} + \prod_{j=1}^{l-v} p_j .$$

So

$$\frac{\min_{m \mid n}\{d(m) + n/m\}}{2^{\nu(n)}} < \frac{1}{2^{l-v}} + \frac{1}{2^{l-2p_{l-v}}} ,$$

since $\prod_{j=1}^{l-v} p_j < 4^{p_{l-v}}$. Now $p_{l-v} < 3/2(l-v)\log(l-v)$, for all large enough l, and then $l - 2p_{l-v} > l - 3(l-v)\log(l-v) > (2l)/3$. Thus $l - v$ and $l - 2p_{l-v}$ each $\to \infty$, and we are finished.

From Lemmas 1 and 3 follows immediately our first theorem.

THEOREM 1. *For each* $\varepsilon > 0$, *there exists a positive constant* $c_0(\varepsilon) < 1$ *such that for each prime* p *dividing* $|G|$, $k(G) > c_0 2^{(1-\varepsilon)\nu(p-1)}$.

THEOREM 2. (P. Erdös, [2]). *Given an arbitrarily small posi-*

tive ε, *then for almost all primes* $p \leqq n$, *i.e., except for* $o(n/\log n)$ *of the primes* $\leqq n$, *as* $n \to \infty$,

$$(1-\varepsilon)\log\log n < \nu(p-1) < (1+\varepsilon)\log\log n \,.$$

THEOREM 3. (S. Selberg, [10]). *Let* $\mathscr{P}$ *be a set of primes,* $C > 0$ *and* $h \geqq 1$ *constants, such that*

$$\sum_{\substack{p \leqq n \\ p \in \mathscr{P}}} \frac{1}{p} > \frac{\log\log n}{h} - C \,.$$

Then there exists a constant D *(depending only on* h *and* C*) such that, if* $A(n, \mathscr{P})$ *denotes the number of integers* $g \leqq n$ *and not divisible by any prime in* $\mathscr{P}$, $A(n, \mathscr{P})/n < D/(\log n)^{1/h}$.

In particular, if the inequality in the hypothesis can be shown to hold for all n large enough, we may conclude that, as $n \to \infty$, "almost all" integers $g \leqq n$ *are* divisible by at least one prime in $\mathscr{P}$. We now state and prove our main theorem:

THEOREM 4. *For each* $c_2 < \log 2$ *almost all integers* $g \leqq n$, *as* $n \to \infty$, *have the property that each group* G *of order* g *satisfies* $k(G) > (\log n)^{c_2}$.

Proof. For each fixed $\varepsilon > 0$ we know that for sufficiently large $\nu(p-1)$, if $p \mid |G|$ then $k(G) > 2^{(1-\varepsilon/2)\nu(p-1)}$, by Lemmas 1 and 3. Thus we need only show that, as $n \to \infty$, almost all $g \leqq n$ are divisible by a prime p satisfying $\nu(p-1) > (1-(1/2)\varepsilon)\log\log n$.

For any fixed positive ε, let $\mathscr{P}$ be the set of all primes $p \leqq n$ such that $\nu(p-1) > (1-2\varepsilon)\log\log n$. Then, if $n'+1 =$ the least integer $\geqq \exp(\log^{1-\varepsilon} n)$ we obtain

$$\sum_{p \in \mathscr{P}} \frac{1}{p} \geqq \sum_{\substack{n'+1 \leqq p \leqq n \\ \nu(p-1) \geqq (1-\varepsilon)\log\log p}} \frac{1}{p}$$

since in the latter sum

$$\begin{aligned}(1-\varepsilon)\log\log p &\geqq (1-\varepsilon)\log\log(n'+1) \\ &\geqq (1-\varepsilon)^2\log\log n > (1-2\varepsilon)\log\log n \,.\end{aligned}$$

Let $N(l, \varepsilon)$ denote the cardinality of the collection of all primes $p \leqq l$ such that $\nu(p-1) \geqq (1-\varepsilon)\log\log p$. Then the smaller sum above is

$$\begin{aligned}\sum_{n'+1 \leqq l \leqq n} \frac{N(l, \varepsilon) - N(l-1, \varepsilon)}{l} &= \sum_{n'+1 \leqq l \leqq n} \frac{N(l, \varepsilon)}{l} - \sum_{n' \leqq l < n} \frac{N(l, \varepsilon)}{l+1} \\ &> \sum_{n'+1 \leqq l < n} \frac{N(l, \varepsilon)}{l(l+1)} - 1 \,.\end{aligned}$$

Now by the theorem of Erdös, for each $l > l_0(\varepsilon)$, $N(l, \varepsilon) > (3/4)l/\log l$. Hence for all n (and thus n' and l) large enough, we find that $(l/(l+1)) > 2/3$ and)

$$\sum_{n'+1 \leqq l < n} \frac{N(l, \varepsilon)}{l(l+1)} > \frac{3}{4} \sum_{l=n'+1}^{n-1} \frac{1}{(l+1)\log l}$$
$$> \frac{1}{2} \int_{n'+1}^{n} \frac{dt}{t \log t} = \frac{\varepsilon}{2} \log\log n\ .$$

Now that $\sum_{p \in \mathscr{P}} 1/p > \frac{\varepsilon}{2} \log\log n - 1$, for sufficiently large n, we may apply Selberg's theorem to our $\mathscr{P}$, obtaining the conclusion desired.

Finally, the author acknowledges with gratitude the comments of Professor Patrick X. Gallagher, which resulted in this improvement of the original theorem, announced in the Notices of the A.M.S., August, 1974.

REFERENCES

1. R. Brauer, *Representations of Finite Groups*, in Lectures on Modern Mathematics, ed. T. L. Saaty, Vol. 1, Wiley, New York, 1963.
2. P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's, ϕ-function*, Quart. J. Math., Oxford Series, **6** (1935), 205-213.
3. P. Erdös and P. Turán, *On some problems of a statistical group theory IV*, Acta Math. Acad. Sci. Hung., **19** (1968), 413-435.
4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 4th edition, 1960.
5. E. Landau, *Klassenzahl binärer quadratischer Formen von negativer Discriminante*, Math. Annalen, **56** (1903), 674-678.
6. G. A. Miller, *Groups possessing a small number of sets of conjugate operators*, Trans. Amer. Math. Soc., **20** (1919), 260-270.
7. ———, *Groups involving a small number of sets of conjugate operators*, Proc. Nat. Acad. Sci., **30** (1944), 359-362.
8. M. Newman, *A bound for the number of conjugacy classes in a group*, J. London Math. Soc., **43** (1968), 108-110.
9. J. Poland, *Two problems on finite groups with k conjugacy classes*, J. Austral. Math. Soc., **8** (1968), 49-55.
10. S. Selberg, *A theorem in analytic number theory*, Norske Vid. Selsk. Forh., **23** (1951), 1-2.

Received May 22, 1974 and in revised form November 26, 1974.

UNIVERSITY OF HAWAII
AND
UNIVERSITY OF CALIFORNIA, LOS ANGELES