Pacific Journal of Mathematics

WHAT IS THE PROBABILITY THAT TWO ELEMENTS OF A FINITE GROUP COMMUTE?

DAVID RUSIN

Vol. 82, No. 1 January 1979

PACIFIC JOURNAL OF MATHEMATICS
Vol. 82, No. 1, 1979

WHAT IS THE PROBABILITY THAT TWO ELEMENTS OF A FINITE GROUP COMMUTE?

DAVID J. RUSIN

We consider the probability that two elements of a finite group commute. Explicit computations are obtained for groups G with $G' \leqq Z(G)$ and $G' \cap Z(G) = \{1\}$. We classify the groups for which this probability is above 11/32.

I. Introduction. All groups considered will be supposed finite. We will denote by $\Pr(G)$ the probability that two elements of the group G, chosen randomly with replacement, commute. (This will loosely be called the "probability of G".) That is,

$$\Pr(G) = \frac{\text{Number of ordered pairs } (x, y) \in G \times G \text{ such that } xy = yx}{\text{Total number of ordered pairs } (x, y) \in G \times G}\,.$$

This concept has been considered by several authors, as indicated in the bibliography. The most important formula we will need is that $\Pr(G) = (k/|G|)$, where $k = k(G)$ is the number of conjugacy classes in G.

Let us fix our notation. If H is a subset (resp. subgroup, normal subgroup) of G, we write $H \subseteqq G$ (resp. $H \leqq G$, $H \trianglelefteq G$). For any element x of G, $[G, x]$ is a subset of G', while for any subset H of G, $[G, H]$ is the subgroup generated by all $[G, x]$ with $x \in H$. We write $C(H)$ and $N(H)$ for the centalizer and normalizer of a subgroup $H \leqq G$. We denote the center and derived subgroups of G by $Z(G)$ and G', respectively.

For any subset $H \subseteqq G$, let us write $H^* = \{x \in G\colon [G, x] \subseteqq H\} = (G' \cap H)^*$. If H is a normal subgroup, then it is easy to check that $H^*/H = Z(G/H)$; in particular, H^* is a subgroup of G. The $(\ )^*$ operation is meant as a partial inverse to the $(\ )'$ operation, since $(H^*)' \subseteqq H$, $H \subseteqq (H')^*$, and $(G')^* = G$ (in fact, $((H^*)')^* = H^*$). Note that $H_1 \subseteqq H_2$ implies $H_1^* \subseteqq H_2^*$ and that $\{1\}^* = Z(G)$.

II. Groups of nilpotence class 2. When $G' \leqq Z(G)$, we can compute $\Pr(G)$ in terms of the group structure in G. If we write $G = G_2 \times G_3 \times \cdots$, where G_p is a p-group, then we need only examine $\Pr(G_p)$ for each p, and use the general formula $\Pr(H \times K) = \Pr(H) \cdot \Pr(K)$, as noted in [4]. Thus, assume in what follows that G is a p-group with $G' \leqq Z(G)$.

In this case, the subset $[G, x]$ is actually a subgroup, since $[y, x][y', x] = [y'y, x]$. Thus, when considering the possibilities for

$[G, x]$, we need only consider the subgroups of G'; hence when we speak of H^* here, it will be assumed that H is a group. Since $H \leq Z, H \trianglelefteq G$; so as noted earlier, H^* is a group. Since G is a p-group, both $|H|$ and $|H^*|$ are powers of p.

For brevity, set $\bar{H} = H^* - \bigcup_{K<H} K^*$ (that is, $\bar{H}$ is the set of all elements for which $[G, x] = H$ precisely, and not any proper subgroup). We then have $H^* = \bigcup_{K \leq H} \bar{K}$ disjointly, so that $|H^*| = \sum_{K \leq H} |\bar{K}|$ for any $H \leq G'$.

Now, given any partially ordered lattice, there exists a function m (the Möbius Inversion function [6]) such that whenever two functions f and g are such that

$$g(x) = \sum_{y \leq x} f(y), \text{ then } f(x) = \sum_{y \leq x} m(x, y) g(y) .$$

Applying this to the lattice of subgroups of G' and to the functions $f = |(\overline{\ \ })|$ and $g = |(\ \ )^*|$, we get that $|\bar{H}| = \sum_{K \leq H} m(K, H) |K^*|$.

Next, the elements of $\bar{H}$ each have $|H|$ conjugates, so the total number of conjugacy classes of G is $\sum_{H \leq G'} (\bar{H}/|H|)$, and thus

$$\begin{aligned} \Pr(G) = \frac{k}{|G|} &= \frac{1}{|G|} \sum_{H \leq G'} \frac{|\bar{H}|}{|H|} \\ &= \frac{1}{|G|} \sum_{H \leq G'} \frac{1}{|H|} \Big(\sum_{K \leq H} m(K, H) |K^*| \Big) \\ &= \frac{1}{|G|} \sum_{K \leq G'} |K^*| \Big(\sum_{K \leq H \leq G'} \frac{m(K, H)}{|H|} \Big) . \end{aligned}$$

The Möbius functions for the subgroup lattices of p-groups have been completely worked out [16]: If K is not normal in $H, m(K, H) = 0$; otherwise, $m(K, H) = m(1, H/K) = m(1, H^0)$, say. Since the lattice of subgroups of G' containing K is isomorphic to the lattice of subgroups of G'/K, we get

$$\Pr(G) = \frac{1}{|G|} \sum_{K \leq G'} |K^*| \Big(\sum_{H^0 \leq (G'/K)} \frac{1}{|K| \cdot |H^0|} m(1, H^0) \Big) .$$

It is also shown in [16] that $m(1, H^0)$ for p-groups is zero unless H^0 is an elementary abelian p-group of order p^i, say; in that case $m(1, H^0) = (-1)^i p^{i(i-1)/2}$. Therefore, the only terms that contribute to the above sum are those for which H^0 is an elementary abelian p-subgroup of (G'/K). If we let L be the subgroup of elements of order $\leq p$ in G'/K, then the formula above becomes

$$\Pr(G) = \frac{1}{|G|} \sum_{K \leq G'} \frac{|K^*|}{|K|} \Big(\sum_{H^0 \leq L} \frac{m(1, H^0)}{|H^0|} \Big) .$$

This L is isomorphic to a vector space of dimension n over $GF(p)$. If $\begin{bmatrix} n \\ j \end{bmatrix}$ denotes the number of subgroups of order p^j (subspaces of dimension j) then we have [6] $\begin{bmatrix} n \\ j \end{bmatrix} = p^j \cdot \begin{bmatrix} n-1 \\ j \end{bmatrix} + \begin{bmatrix} n-1 \\ j-1 \end{bmatrix}$ and $\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1$. Thus, if $(C_p)^i$ denotes the direct product of i copies of the cyclic group of order p, then

$$\sum_{H^0 \leqq L} \frac{m(1, H^0)}{|H^0|} = \sum_{i=0}^{n} m(1, (C_p)^i) \cdot \frac{1}{p^i} \begin{bmatrix} n \\ i \end{bmatrix} = \sum_{i=0}^{n} (-1)^i p^{i(i-3)/2} \begin{bmatrix} n \\ i \end{bmatrix} .$$

For $n = 0$, this comes out to 1, while for $n = 1$, it is $1 - (1/p)$. For $n \geqq 2$, it becomes

$$\begin{aligned}
&(-1)^0 p^{0(0-3)/2} \begin{bmatrix} n \\ 0 \end{bmatrix} + \sum_{i=1}^{n-1} (-1)^i p^{i(i-3)/2} \begin{bmatrix} n \\ i \end{bmatrix} + (-1)^n p^{n(n-3)/2} \begin{bmatrix} n \\ n \end{bmatrix} \\
&= 1 + (-1)^n p^{n(n-3)/2} + \sum_{i=1}^{n-1} (-1)^i p^{i(i-3)/2} \left(p^i \begin{bmatrix} n-1 \\ i \end{bmatrix} + \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} \right) \\
&= 1 + (-1)^n p^{n(n-3)/2} + \sum_{i=1}^{n-1} (-1)^i p^{i(i-3)/2} \cdot p^i \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
&\quad - \sum_{i=0}^{n-2} (-1)^i p^{(i+1)(i-2)/2} \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
&= 1 + (-1)^n p^{n(n-3)/2} - (-1)^0 p^{0(0-3)/2} \cdot p^0 \begin{bmatrix} n-1 \\ 0 \end{bmatrix} \\
&\quad + (-1)^{n-1} p^{n(n-3)/2} \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} + \sum_{i=0}^{n-1} (-1)^i p^{i(i-1)/2} \left(1 - \frac{1}{p}\right) \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
&= \left(1 - \frac{1}{p}\right) \sum_{i=0}^{n-1} m(1, (C_p)^i) \cdot \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
&= \left(1 - \frac{1}{p}\right) \sum_{H \leqq (C_p)^{n-1}} m(1, H) .
\end{aligned}$$

This last sum may be evaluated. Define a function on the subgroups of $(C_p)^{n-1}$ by $f(\{1\}) = 1$, $f(H) = 0$ if $H \neq \{1\}$; then define the function $g(H) = \sum_{K \leqq H} f(K)$, which is identically equal to 1. If we apply the Möbius Inversion formula to this pair of functions, we get $f(H) = \sum_{K \leqq H} m(K, H) g(K)$. Since $n \geqq 2$, $(C_p)^{n-1} \neq \{1\}$, so that

$$\begin{aligned}
0 &= f((C_p)^{n-1}) \\
&= \sum_{K \leqq (C_p)^{n-1}} m(K, C_p^{n-1}) \cdot g(K) \\
&= \sum_{K \leqq (C_p)^{n-1}} m(1, C_p^{n-1}/K) \cdot 1 \\
&= \sum_{H \leqq (C_p)^{n-1}} m(1, H) .
\end{aligned}$$

We have thus evaluated $\sum_{H^0 \leqq L} (m(1, H^0)/|H^0|)$. First, if $n = 0$, ($L = \{1\}$), it equals 1; this is equivalent to G'/K having no elements of order p, and hence that $K = G'$. Second, if $n = 1$, the sum is $1 - (1/p)$. This happens just when G'/K has a unique subgroup of order p; since it is already abelian, G'/K is then cyclic and nontrivial. Finally, if $n \geqq 2$ (that is, all other cases), the sum is zero. Therefore, our formula for $\Pr(G)$ becomes

$$\Pr(G) = \frac{1}{|G|} \cdot \sum_{K \leqq G'} \frac{|K^*|}{|K|} \cdot \begin{cases} 1 & \text{if } K = G' \\ 1 - (1/p) & \text{if } G'/K \text{ is nontrivial cyclic} \\ 0 & \text{otherwise}. \end{cases}$$

We know that K^* is a subgroup of G, and hence its order is a power of p; therefore let us write $|K^*| = |G|/p^{n(K)}$. Then our result is:

(1) THEOREM. *If G is a p-group with $G' \leqq Z(G)$, then*

$$\Pr(G) = \frac{1}{|G'|}\left(1 + \sum_{\substack{G'/K \\ \text{cyclic}}} \frac{(p-1)\cdot[G' : K]/p}{p^{n(K)}}\right).$$

Now we look for some limiting conditions on the exponents $n(K)$. We write $n(K_i) = n_i$ when the subgroups are indexed. These are nonnegative integers, with $n(K) = 0$ iff $K = G'$. Furthermore, since we know $K_1 \leqq K_2$ implies $(K_1)^* \leqq (K_2)^*$, we must have $n_1 \geqq n_2$ in this case.

Next, if $K_i = K_j \cap K_k$ and $K_j, K_k \leqq K_l$, then we have $(K_jK_k) \leqq K_l$, so $K_j^*K_k^* \leqq (K_jK_k)^* \leqq K_l^*$ and $K_j^* \cap K_k^* = K_i^*$. Hence,

$$\frac{|G|}{p^{n_l}} = |K_l^*| \geqq |K_j^*K_k^*| = \frac{|K_j^*|\cdot|K_l^*|}{|K_j^* \cap K_k^*|} = \frac{|K_j^*|\cdot|K_k^*|}{|K_i^*|}$$
$$= \left(\frac{|G|}{p^{n_j}}\right)\cdot\left(\frac{|G|}{p^{n_k}}\right) \Big/ \left(\frac{|G|}{p^{n_i}}\right) = \frac{|G|}{p^{n_j+n_k-n_i}},$$

so that we get $n_j + n_k \geqq n_i + n_l$.

We also have the following

(2) PROPOSITION. *If H is a p-group with $H' \leqq Z(H)$ and H' cyclic, then $H/Z(H) \cong \prod_i (C_{p^{n_i}} \times C_{p^{n_i}})$ with all $n_i \leqq k$, and $n_1 = k$. (where, $p^k = |H'|$.) In particular, $[H: Z(H)]$ is a square, and is at least $|H'|^2$.*

Before giving the proof, let us indicate why we need Proposition 2. We will use it on Theorem 1 as follows. Recall that $n(K)$ was defined so that $|G|/p^{n(k)} = |K^*|$. Thus,

$$p^{n(K)} = |G/K^*| = \frac{|G/K|}{|K^*/K|} = [H\colon Z(H)]$$

where $H = G/K$. Note that $H' = G'/K$ is cyclic for the subgroups K appearing in Theorem 1, and $H' \leqq Z(G)/K \leqq K^*/K = Z(H)$. Hence by Proposition 2, all the $n(K)$ in Theorem 1 are *even*, and $p^{n(K)} \geqq [G'\colon K]^2$.

Proof of Proposition 2. We prove this by induction on the rank r of the abelian group $H/Z(H)$. The proposition is certainly true if $r = 0$. On the other hand, since $H/Z(H)$ is never cyclic, $r \neq 1$. Hence, we may assume $r \geqq 2$. Write $H/Z(H) = \langle a_1Z\rangle \times \langle a_2Z\rangle \times \cdots \times \langle a_rZ\rangle$.

Because H is generated by $Z(H)$ and the a_i, and $H' \leqq Z(H)$, we have

$$H' = \langle [a_i, a_j]\colon 1 \leqq i, j \leqq r\rangle .$$

Since H' is cyclic of order p^k, this implies in particular that some $[a_i, a_j]$ has order p^k. Without loss of generality, we may assume that $c = [a_1, a_2]$ is such an element. Since $c \in Z(H)$, $[a_1^m, a_j] = [a_1, a_j]^m$; so since $[a_1, a_j]^{p^k} = 1$ for all j but $[a_1, a_2]^{p^{k-1}} \neq 1$, $a_1^{p^k} \in Z(H)$ but $a_1^{p^{k-1}} \notin Z(H)$. Therefore, $\langle a_1Z\rangle \cong C_{p^k}$. Similarly, $\langle a_2Z\rangle \cong C_{p^k}$.

Since c generates H', for each i and j we may write $[a_i, a_j] = c^{e_{ji}}$. Then if we set $b_i = a_ia_2^{-e_{1i}}a_1^{e_{2i}}$ for each $i > 2$, we compute

$$\begin{aligned}[a_1, b_i] &= [a_1, a_i][a_1, a_2]^{-e_{1i}}[a_1, a_1]^{e_{2i}} \\ &= c^{e_{1i}}c^{-e_{1i}} = 1\end{aligned}$$

and similarly $[a_2, b_i] = 1$. Since $\langle a_i\rangle \cap \langle a_1, a_2\rangle \leqq Z(H)$, the order of $b_iZ(H)$ is the same as that of $a_iZ(H)$; from this it is easy to check that

$$H/Z(H) = \langle a_1Z\rangle \times \langle a_2Z\rangle \times \langle b_3Z\rangle \times \cdots \times \langle b_rZ\rangle .$$

Now let $K \leqq H$ be the subgroup $K = \langle Z(H), b_3, b_4, \cdots, b_r\rangle$. It is clear that $Z(H) \subseteqq Z(K)$; but conversely, since $H = \langle K, a_1, a_2\rangle$ and $[a_1, b_i] = [a_2, b_i] = 1$, we have $Z(K) \subseteqq Z(H)$. Thus we may use the inductive hypothesis on K:

(1) $K' \subseteqq H'$, so K' is cyclic

(2) $K' \subseteqq H' \subseteqq Z(H) = Z(K)$

(3) $K \subseteqq H$ is also a p-group

(4) $K/Z(K) = K/Z(H) = \langle b_3Z\rangle \times \cdots \times \langle b_rZ\rangle$ has rank $r-2 < r$.

So, we may assume $K/Z(K) \cong \prod (C_{p^{n_i}} \times C_{p^{n_i}})$ for some set of n_i. Thus,

$$H/Z(H) = \langle a_1 Z\rangle \times \langle a_2 Z\rangle \times \langle b_3 Z\rangle \times \cdots \times \langle b_r Z\rangle$$
$$\cong (C_{p^k} \times C_{p^k}) \times \prod (C_{p^{n_i}} \times C_{p^{n_i}}) ,$$

as desired.

III. Groups with $G' \cap Z(G) = \{1\}$. Now let us turn to the opposite extreme, where $G' \cap Z(G) = \{1\}$. We need a

(3) PROPOSITION. *If $N \trianglelefteq G$ and $N \cap G' = \{1\}$, then* $\Pr(G) = \Pr(G/N)$.

Proof. From [8], it suffices to show that $\Pr(L) = \Pr(L/N) \cdot \Pr(N)$ for all subgroups $L = \langle N, g, h\rangle$ where $[g, h] \in N$. But all such L are abelian: L' is generated by the conjugates of $[N, N]$, $[N, g]$, $[N, h]$, and $[g, h]$, while each of these lies in $N \cap G' = \{1\}$. Thus, $N \leqq L$ and L/N are also abelian, so that

$$\Pr(L) = \Pr(L/N) \cdot \Pr(N) = 1 .$$

We may use this proposition in our case to conclude that $\Pr(G) = \Pr(G/Z)$; moreover, $(G/Z)' = (G'Z)/Z = (G' \times Z)/Z \cong G'$, and also $Z(G/Z) = (G' \cap Z)^*/Z = \{1\}^*/Z = Z/Z$. Thus, $\Pr(G) = \Pr(K)$ for some group with $K' \cong G'$, and $Z(K) = \{1\}$. Therefore, we must merely look for $\Pr(K)$ for all such groups K.

(4) PROPOSITION. *For any given G', then are at most a finite number of groups K with $K' \cong G'$ and $Z(K) = \{1\}$.*

Proof. This will follows from the "N over C" theorem [5, p. 20], which gives us that $L = K/C(K') = N(K')/C(K')$ is isomorphic to a subgroup of $\mathrm{Aut}(K')$. Now, $L' = K'C(K')/C(K')$, so that we have an abelian group $L/L' = (K/C(K'))/(K'C(K')/C(K')) \cong K/(K'C(K'))$; if $n = \mathrm{rank}(L/L')$, then $K/(K'C(K'))$ can be generated by n elements $x_i(K'C(K'))$ with $x_i \in K$.

Now we can use the result of P. Hall [5, p. 266] which states that $[C(K'), C(K')] \leqq Z(K)$. In our case, this means that $[C(K')]' \leqq Z(K) = \{1\}$, i.e., $C(K')$ is abelian; so if $y \in C(K')$, then $[K'C(K'), y] = \{1\}$. Since $K = \langle x_1, x_2, \cdots, x_n, K'C(K')\rangle$, this means that if $y \in C(K')$ commutes with each $x_i (1 \leqq i \leqq n)$ then $y \in Z(K) = \{1\}$.

Therefore, for $y_1, y_2 \in C(K')$, if $[y_1, x_i] = [y_2, x_i]$ for each i, then $y_1 x_i y_1^{-1} = y_2 x_i y_2^{-1}$, so that $y_2^{-1} y_1$ commutes with each x_i, and hence from the above we know $y_2^{-1} y_1 = 1$, or $y_1 = y_2$. This tells us that $|C(K')|$ is at most equal to the number of values the n-tuple $\{[y, x_i], 1 \leqq i \leqq n\}$ assumes as y ranges over $C(K')$, which is therefore at most

$$\prod_{i=1}^{n} |[C(K'), x_i]| \leqq \prod_{i} |[K, x_i]| \leqq |K'|^n .$$

Then, from $|K| = |C(K')| \cdot |K/C(K')|$, we have that $|K| \leqq |K'|^n \cdot |L| \leqq |K'|^{|\mathrm{Aut}(K')|} |\mathrm{Aut}(K')|$. Hence, with a given commutator subgroup G', the orders of groups K with $K' \cong G'$ and $Z(K) = \{1\}$ are bounded by a function of G' alone. This justifies the claim that there are only a finite number of such groups.

There are further restrictions when $Z(K) = \{1\}$. For example, no element x in K' except $x = 1$ can be fixed under each automorphism of $L \leqq \mathrm{Aut}(K')$, since that would mean $kxk^{-1} = x$ for all $k \in K$, and then $x \in Z(K) = \{1\}$. Furthermore, $L = K/C(K')$ is abelian iff $K' \leqq C(K')$, i.e., iff K' is abelian. In that case, we must have $|K'|$ dividing $|C(K')|$. In particular, if $n = 1$, then $|K'| \leqq |C(K')| \leqq |K'|$, and so $K' = C(K')$. (Actually, this is even true when $n > 1$.)

We may use these observations on a specific class of groups to get more detailed information than that supplied by Proposition 4. For example,

(5) PROPOSITION. *If K' is cyclic of prime order p, and $Z(K) = \{1\}$, then $K = \langle a, b \colon a^p = b^n = 1, bab^{-1} = a^r \rangle$, where $n \mid (p-1)$ and $r^j \equiv 1 \bmod p$ iff $n \mid j$.*

Proof. Write $K' = \langle a \rangle$. Then $\mathrm{Aut}(K')$ is cyclic, so that $n = 1$ and $K' = C(K')$ as noted above. Further, $L \leqq \mathrm{Aut}(K')$ is also cyclic, say $L = \langle bK' \rangle$. We write $|L| = n$ and note that n divides $|\mathrm{Aut}(K')| = p - 1$. From $|L| = n$ have $b^n \in K' = \langle a \rangle$, say, $b^n = a^s$. If $s \neq 0$, then $\langle b \rangle = \langle b, a \rangle = K$, so K would be cyclic, and then would not have trivial center. Thus we have $s = 0$, and $b^n = 1$. Next, note that $K' \trianglelefteq K$ implies $bab^{-1} \in \langle a \rangle$, say $bab^{-1} = a^r$. If $r^j \equiv 1 \bmod p$, then $b^j a b^{-j} = a^{r^j} = a$, so b^j commutes with $\langle b \rangle$ and with $\langle a \rangle$, so $b^j \in Z = \{1\}$, and $j \equiv 0 (\mathrm{mod}\, n)$.

These are known as metacyclic groups. We remark that by computing the number of commuting pairs of elements by brute force, one sees that $\Pr(G) = (n^2 + p - 1)/n^2 p$.

There are some cases in which there are no K with $K' \cong G'$ and $Z(K) = \{1\}$. As noted before, this happens if there is an $x \in G' - \{1\}$ fixed under each automorphism in $L \leqq \mathrm{Aut}(G')$. One common case in which this occurs is when G' is isomorphic to C_{2^n}, $n \geqq 1$; since G' has a unique element of order 2, that element is fixed under all automorphisms, and hence must lie in $Z(G)$. This also happens if $G' \cong C_6$.

IV. Groups with $\Pr(G) > 11/32$. In some cases it is possible to find the possible set of values of $\Pr(G)$ in a given interval. We shall do this for the interval (11/32, 1]. We the use "degree equation" from character theory [5, Chapter 5]. It states that $|G| = \sum_{i=1}^{k} n_i^2$, where k is the number of conjugacy classes of G, and the n_i are positive integers; precisely $[G: G']$ of these are equal to 1. So,

$$\begin{aligned} |G| &= [G: G'] + \sum_{[G:G']+1}^{k} n_i^2 \\ &\geqq [G: G'] + 4(k - [G: G']) \\ &= 4k - 3[G: G'] \end{aligned}$$

so that

$$k \leqq \frac{1}{4}(|G| + 3[G: G'])\ ,$$

and so

$$\Pr(G) \leqq \frac{1}{4} + \frac{3}{4}\frac{1}{|G'|}\ . \tag{6}$$

Equation 6 enables us in principle to determine all possible values for $\Pr(G)$ greater than any fraction p_0, as long as $p_0 > 1/4$; we merely find all values of $\Pr(G)$ for those groups for which G' is one of the groups of order less than $3/(4p_0 - 1)$. For example, to compute the values of $\Pr(G) > 11/32$, we need only consider those G of order less than 8, viz. $G' = \{1\}$, C_2, C_3, C_4, C_2, $\times C_2$, C_5, C_6, S_3, and C_7. (The reason we stop at 11/32 is because continuing further would require a consideration of the groups of order 8. There are many of these, including some nonabelian ones, so we avoid them altogether.)

$G' = \{1\}$ means G is abelian, so $\Pr(G) = 1$. On the other hand, $G' \cong S_3$ is impossible, since S_3 is a complete group and $S_3 \neq S_3'$ [13]. Thus, we need only consider the seven remaining cases.

It turns out that even for a given G', the different possibilities for $G' \cap Z(G)$ require separate discussions. Since $G' \cap Z(G)$ is a subgroup of G', we must investigate the following combinations:

G'	C_2	C_3	C_4	$C_2 \times C_2$	C_5	C_6	C_7
$G' \cap Z(G)$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$
	C_2	C_3	C_2	C_2	C_5	C_2	C_7
			C_4	$C_2 \times C_2$		C_3	
						C_6	

Case 1. $G' < Z(G)$. A method for computing the probabilities for such groups was given in II.

For $G' \cong C_p$ with p a prime, the only proper subgroup of G' is $\{1\}$, which has index p, so that $\Pr(G) = 1/p \cdot (1 + (p-1)/p^{2n})$ for some n, where $G/Z(G) \cong C_p^{2n}$ by Proposition 2. For $p = 2$, we have the infinite family of values $1/2 \cdot (1 + 1/2^{2n})$. For $p = 3$, only $n = 1$ gives a value $(= 11/27)$ greater than 11/32. For $p = 5$ and $p = 7$, all the values of $\Pr(G)$ are too small.

For $G' = C_6 \cong C_2 \times C_3$, we know that G is nilpotent, say $G = H_2 \times H_3$ where $H_2' = C_2$ and $H_3' = C_3$. Taking the probabilities from the last paragraph, we have

$$\Pr(G) = \frac{1}{2} \cdot \left(1 + \frac{1}{2^{2n}}\right) \cdot \frac{1}{3}\left(1 + \frac{1}{3^{2m}}\right) \leqq \frac{5}{8} \cdot \frac{11}{27} < \frac{11}{32}.$$

For $G' = C_4$, the only subgroups in the lattice are C_4, C_2, and $\{1\}$; Theorem 1 becomes

$$\Pr(G) = \frac{1}{4} \cdot \left(1 + \frac{1}{2^{2m}} + \frac{2}{2^{2n}}\right),$$

with $2^{2n} \geqq [G' : \{1\}]^2 = 16$, $2^{2m} \geqq [G' : C_2]^2 = 4$, so that $\Pr(G) \leqq 11/32$.

For $G' = C_2 \times C_2$, Theorem 1 becomes

$$\frac{1}{4} \cdot \left(1 + \frac{1}{2^{2n_1}} + \frac{1}{2^{2n_2}} + \frac{1}{2^{2n_3}}\right).$$

Taking $n_1 \geqq n_2 \geqq n_3$ for definiteness, we must also have $n_2 + n_3 \geqq n_1$, so that $\Pr(G) = 7/16$ $(n_1 = n_2 = n_3 = 1)$ and 25/64 $(n_1 = 2, n_2 = n_3 = 1)$ are the only values greater than 11/32.

Case 2. $G' \cap Z(G) = \{1\}$. We saw at the end of III that the unique element of order 2 must lie in the center of G if $G' \cong C_2$, C_4, or C_6, so that these cases lead to a contradiction. (This also rules out the combination $G' \cong C_6$, $G' \cap Z(G) \cong C_3$.) If $G' = C_2 \times C_2$, then as in III, we may find that $G/Z(G) \cong A_4$, and $\Pr(G) = \Pr(A_4) = 1/3$.

The remaining cases are of the form $G' \cong C_p$ for p an odd prime; as we remarked after Proposition 5, these have probabilities $(n^2 + p - 1)/n^2p$ (where $n \mid p - 1$). The only values of $\Pr(G)$ above 11/32 for groups G in Case 2 are 1/2 ($G' \cong C_3$ and $G/Z(G) \cong S_3$) and 2/5 ($G' \cong C_5$ and $G/Z(G) \cong D_5$).

Case 3. *Remaining combinations.* The calculations here are rather involved, and not particularly interesting, so we just quote the results. First, when $|G'| = 4$ and $|G \cap Z(G)| = 2$, I have been able to show that $\Pr(G) = 1/4 \cdot (1 + 1/2^{2t} + 1/2 \cdot 1/2^{2s})$, with $2^{2s} = [C(G') : Z(C(G'))]$ and $2^{2t} = [H : Z(H)]$ where $H = G/(G' \cap Z(G))$; $s + 1 \geqq t \geqq 1$. The only value of this above 11/32 is 7/16.

The last case is $G' \cong C_6$ and $G' \cap Z(G) \cong C_2$. It is possible to show that for such G, we must have $\Pr(G) = 1/4 + 1/2^s$, $s \geqq 3$. The only value above 11/32 is 3/8 (for $s = 3$).

Summary. We have the following possibilities for $\Pr(G)$ above 11/32:

$\Pr(G)$	G'	$G' \cap Z(G)$	G/Z
$\frac{1}{2} \cdot (1 + 2^{-2s})$	C_2	C_2	$(C_2)^{2s}$
$1/2 = .5000$	C_3	$\{1\}$	S_3
$7/16 = .4375$	C_4 or $C_2 \times C_2$	C_2	D_4
	$C_2 \times C_2$	$C_2 \times C_2$	C_2^3 or C_2^4
$11/27 \doteq .4074$	C_3	C_3	$C_3 \times C_3$
$2/5 = .4000$	C_5	$\{1\}$	D_5
$25/64 \doteq .3906$	$C_2 \times C_2$	$C_2 \times C_2$	C_2^3 or C_2^4
$3/8 = .3750$	C_6	C_2	$C_2 \times S_3$ or T.

(We write T for the nonabelian group of order 12 besides A_4 and $C_2 \times S_3$.)

We have not discussed the last column for all cases in the paper, but have included it here for completeness. It bears out the intuitive feeling that a group which has a relatively large center is nearly abelian.

Note that this table allows us to characterize the groups with $\Pr(G) = 5/8$, say, or any of the numbers on the table. In the case of 5/8, it is precisely the set of groups G with $G' \cong C_2$ and $G/Z \cong C_2 \times C_2$ that have this value $\Pr(G)$. (Actually, the first constraint is superfluous: see [9].)

V. Concluding remarks. There are several open questions relating to $\Pr(G)$. For example, Joseph [7] has asked for a description of the set $V = \{x \in [0, 1]: x = \Pr(G)$ for some finite group $G\}$. V is a submonoid of $\boldsymbol{Q} \cap [0, 1]$, since $\Pr(G) \cdot \Pr(H) = \Pr(G \times H)$. (The abelian groups supply the identity.) If we set $V_k = \{x: x = \Pr(G)$ for some finite G of nilpotence class $k\}$, then it may be deduced from Theorem 1 that the closure $\bar{V}_2$ is well ordered by $\geqq$ above 1/4 and has order type at most ω^ω there. It is easy to imagine that the same is true for each $\bar{V}_k$, but the methods of II do not extend to this more general case. Using Equation 6 and §III, we also have that $V_0 \cap (1/4, 1]$ has order type ω, where V_0 is $\{\Pr(G): G' \cap Z = 1\}$.

One problem is that the method used here is inherently limited to any interval $[p_0, 1]$ for $p_0 > 1/4$. It would be interesting to discover some other method for finding the probabilities for Pr (G) in, say, (1/5, 1/4). It is possible, of course, that the set of probabilities is even dense there.

Another point to be looked at would be lower bounds for Pr (G); Erdös and Turán have shown [2] that Pr $(G) \geqq \log\log |G|/|G|$. Bertram [1] has that Pr $(G) > (\log |G|)^c/|G|$ for "most" groups G, where c is any constant less than log 2. Sherman [15] notes that Pr $(G) \geqq \log_2 |G|/|G|$ for nilpotent groups G.

References

1. E. A. Bertram, *A density theorem on the number of conjugacy classes in finite groups*, Pacific J. Math., **55** (1974), 329-333.
2. P. Erdös and P. Turán, *On some problems of a statistical group theory*, IV, Acta Math. Acad. Sci. Hung., **19** (1968), 413-435.
3. W. Feit and N. J. Fine, *Pairs of commuting matrices over a finite field*, Duke Math. J., **27** (1960), 91-94.
4. W. H. Gustafson, *What is the probability that two group elements commute*? Amer. Math. Monthly, **80** (1973), 1031-1034.
5. B. Huppert, *Endliche Gruppe I*, Springer Verlag, Berlin, 1967.
6. N. Jacobson, *Basic Algebra I*, W. H. Freeman and Co., San Francisco, (1974), 457-465.
7. K. Joseph, *Several conjectures on commutativity in algebraic structures*, Amer. Math. Monthly, **84** (1977), 550-551.
8. P. X. Gallagher, *The number of conjugacy classes in a finite group*, Math. Z., **118** (1970), 175-179.
9. D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly, **83** (1976), 30-32.
10. ———, *How commutative can a non-commutative group be*? Math. Gazette, **LVIII** (1974), 199-202.
11. I. D. MacDonald, *Some explicit bounds in groups with finite derived qroups*, Proc. London Math. Soc., Series 3 **11** (1961), 23-56.
12. M. Newman, *A bound for the number of conjugacy classes in a group*, J. London Math. Soc., **43** (1960), 108-110.
13. W. R. Scott, *Group Theory*, Prentice Hall, Englewood Cliffs (N. J.) (1964), (450).
14. G. Sherman, *What is the probability an automorphism fixes a group element*? Amer. Math. Monthly, **82** (1975), 261-264.
15. ———, *A lower bound for the number of conjugacy classes in a finite nilpotent group*, Notices Amer. Math. Soc., **25** (1978), A68.
16. L. Weisner, *Abstract Theory of Inversion of Finite Series*, Trans. Amer. Math. Soc., **38** (1935), 474-492.

Received March 17, 1978 and in revised form September 11, 1978. I would like to thank Dr. Joseph Gallian for his assistance and words of encouragement, which were responsible for the success of the NSF Undergraduate Research Participation program during which this paper was written (Grant # 76-83533, at the University of Minnesota, Duluth). I would also like to thank the referee for his many constructive comments.

UNIVERSITY OF CHICAGO
CHICAGO, IL 60637

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 82, No. 1 January, 1979