9-1990

How Hamiltonian Can a Finite Group Be?

G.J. Sherman
Rose-Hulman Institute of Technology

T.J. Tucker
Harvard University

M.E. Walker
New Mexico State University - Main Campus

HOW HAMILTONIAN CAN A FINITE GROUP BE?

G.J. Sherman, T.J. Tucker and M.E. Walker

MS TR 90-05

September 1990

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198

Phone: (812) 877-8391

How Hamiltonian Can a Finite Group Be?

By

Gary J. Sherman*, Thomas J. Tucker* and Mark E. Walker*

Introduction. If the finite group G acts on the finite non-empty set X (i.e., G is represented as a group of permutations of X), then

$$P_G(X) = \frac{|\{(g,x)|\; gx = x \quad \text{for} \quad g \in G \quad \text{and} \quad x \in X\}|}{|G| \cdot |X|}$$

may be interpreted as the probability that an element chosen at random from G fixes an element chosen at random from X. Setting $G_x = \{g \in G | gx = x\}$ we find that the numerator of $P_G(X)$ is equal to $\sum_{x \in X} |G_x| = \sum_{i=1}^{k} [G : G_{x_i}] \cdot |G_{x_i}| = k \cdot |G|$ where $\{x_1, x_2, \ldots, x_k\}$ is a set of representatives of the distinct orbits in X under G. It follows that $P_G(X)$ is the ratio of the number of orbits in X under G to the order of X; i.e., $P_G(X) = k(X)/|X|$. If we denote the set of orbits of X of length one (the fixed set of G) by $F(X)$ and the set of orbits of length greater than one (the action set of G) by $A(X)$ then,

$$P_G(X) = \frac{|F(X)| + |A(X)|}{|X|}. \tag{1}$$

This ratio has been studied for several group actions. Here are three examples.

(i) G acts on itself by conjugation ([2],[3]): $P_G(G)$ is interpreted as the probability that two elements of G commute. If G is not abelian (i.e., $P_G(G) \neq 1$), then $P_G(G) \leq 5/8$.

(ii) G acts on its set of subsets 2^G by conjugation [8]: $P_G(2^G)$ is interpreted as the probability that an element of G normalizes a subset of G. If G is not abelian (i.e., $P_G(2^G) \neq 1$), then $P_G(2^G) \leq 7/16$.

(iii) The automorphism group A of G acts on G ([5],[7]). If $G \neq Z_2$ (i.e., $P_A(G) \neq 1$), then $P_A(G) \leq 3/4$.

---

*Work supported by NSF grant DMS-8900507

We are concerned with the action of G on its set of subgroups $S = S(G)$ by conjugation. Let $C = C(G)$, $NS = NS(G)$ and $NC = NC(G)$ denote the cyclic, the normal and the normal cyclic subgroups of G, respectively. From (1) we have $P_G(S) = (|NS| + |A(S)|)/|S|$ and, by restricting the action of G on S to C, $P_G(C) = (|NC| + |A(C)|)/|S|$. Setting $P_{\bar{G}}(S) = |NS|/|S|$ and $P_{\bar{G}}(C) = |NC|/|C|$ we have that $P_G(S) = P_{\bar{G}}(S) = P_G(C) = P_{\bar{G}}(C) = 1$ if, and only if, each subgroup of G is normal. Such a group is referred to as a Hamiltonian group. A group is Hamiltonian if, and only if, it is an abelian group or the direct product of the quaternion group of order eight, an elementary abelian 2-group and an abelian group of odd order [4].

Let $\mu = \mu(G)$ denote any one of $P_G(S)$, $P_{\bar{G}}(S)$, $P_G(C)$ or $P_{\bar{G}}(C)$. The preceding examples suggest the following question, which was first posed in [7] for $P_G(S)$: If G is not Hamiltonian (i.e., $\mu \neq 1$), does there exist $\rho = \rho(\mu) < 1$, independent of G, such that $\mu \leq \rho$? In this paper we show that the answer to this question is no. Indeed, we prove

Theorem. *For each* $r \in [0,1]$ *there exists a sequence of groups* $\{G_n\}$ *such that* $\lim_{n\to\infty} \mu(G_n) = r$.

Proof of the Theorem. It suffices to show that for each $\epsilon > 0$ there exists a group G such that $|\mu(G) - r| < \epsilon$. We will construct G as a direct product of groups of the form

$$G(p,n) = \langle a, b | a^{p^{n-1}} = b^p = e \quad \text{and} \quad bab^{-1} = a^{p^{n-2}+1} \rangle,$$

where p is an odd prime and $n \geq 3$ is an integer. $G(p,n)$ is of order p^n.

Here are some facts concerning the subgroup lattice of $G(p,n)$ which are necessary for the proof of our theorem.

Fact 1: $|S(G(p,n))| = (p+1) \cdot n - (p-1)$ [1].

Fact 2: $G(p,n)$ has $p+1$ subgroups of order p^j for $1 \leq j \leq n-1$. This follows from Fact 1 and the fact that in a non-cyclic p-group of odd order the number of subgroups of order p^j, $1 \leq j \leq n-1$, is congruent to $p+1 \pmod{p^2}$ ([9], page 154).

Fact 3: $|C(G(p,n))| = (n-1)p + 2$. Since $|\langle a \rangle| = p^{n-1}$ there is at least one cyclic subgroup of order p^j for $1 \leq j \leq n-1$. The number of cyclic subgroups of order p^j,

$2 \leq j \leq n-1$, in a non-cyclic p-group of odd order is divisible by p ([9], page 154). Therefore, Fact 2 implies there are exactly p cyclic subgroups of order p^j, $2 \leq j \leq n-1$. All of the subgroups of order p are cyclic.

Fact 4: $|NS(G(p,n))| = (n-2)(p+1)+3$. Passman [6] has shown that the only non-normal subgroups of $G(p,n)$ are of order p. Since $\langle b \rangle$ is not normal $\langle a^{p^{n-2}} \rangle$ is the only normal subgroup of order p.

Fact 5: $|k(S)| = |NS(G(p,n))| + 1 = (n-2)(p+1)+4$.

Fact 6: $|NC(G(p,n))| = (n-2)p+2$.

Fact 7: $|k(C)| = |NC(G(p,n))| + 1 = (n-2)p+3$. Facts 5, 6 and 7 follow because the only non-normal subgroups of $G(p,n)$ are the p cyclic subgroups in the orbit of $\langle b \rangle$.

Thus

$$P_G(S) = \frac{(n-2)(p+1)+4}{(n-1)(p+1)+2},$$

$$P_{\bar{G}}(S) = \frac{(n-2)(p+1)+3}{(n-1)(p+1)+2},$$

$$P_G(C) = \frac{(n-2)p+3}{(n-1)p+2},$$

$$P_{\bar{G}}(C) = \frac{(n-2)p+2}{(n-1)p+2}.$$

Therefore $\lim_{n\to\infty} \mu(G(p,n)) = 1$ and $\lim_{p\to\infty} \mu(G(p,n)) = (n-2)/(n-1)$

Lemma. Let $\mu : N^+ \times N^+ \longrightarrow (0,1)$ be such that

(i) $\lim_{m\to\infty} \mu(m,n) \searrow s_n$ where $0 < s_n < 1$ for each n,

(ii) $\lim_{n\to\infty} \mu(m,n) = 1$ for each m,

(iii) $\lim_{n\to\infty} s_n = 1$.

Then for each $r \in [0,1]$ and for each $\in > 0$ there exist positive integers m and n such that $|\prod_{i=1}^{m} \mu(i,n) - r| <\in$.

Proof. If $r = 1$, then some $\mu(1,n)$ will do. If $r = 0$, then some $\prod_{i=1}^{m}\mu(i,n)$ will do because $\prod_{i=1}^{m}\mu(i,n) \le (\mu(1,n))^m$.

Let $0 < r < 1$. We claim that for each k there exist $m = m(k)$ and $n = n(k)$ such that

$$(2) \qquad 1 \ge r/\prod_{i=1}^{m}\mu(i,n) > s_k.$$

If $r \ge s_k$, choosing n so large that $1 > \mu(1,n) > r \ge s_k$ yields $1 \ge r/\mu(1,n) > s_k$. If $r < s_k$, choosing $n = k$ and m such that

$$\prod_{i=1}^{m}\mu(i,k) \ge r \quad \text{and} \quad \prod_{i=1}^{m+1}\mu(i,k) < r$$

implies

$$1 \ge r/\prod_{i=1}^{m}\mu(i,k) > \mu(m+1,k) > s_k.$$

It follows from (2) and (iii) that $\lim_{k\to\infty}(r/\prod_{i=1}^{m}\mu(i,n)) = 1$; i.e., $\lim_{k\to\infty}(\prod_{i=1}^{m}\mu(i,n)) = r$.

Indexing the odd primes with the positive integers enables us to apply the lemma to each choice of μ. Thus, for $r \in [0,1]$ and $\in > 0$ there exist groups $G(p_i,n)$, $1 \le i \le m$, such that $|\prod_{i=1}^{m}\mu(G(p_i,n)) - r| < \in$. It is straight forward to verify that if the orders of the groups K and H are relatively prime, then $\mu(K \times H) = \mu(K)\cdot\mu(H)$ for each choice of μ. Thus $\prod_{i=1}^{m}\mu(G(p_i,n)) = \mu(\prod_{i=1}^{m}(G(p_i,n))$, so $G = \prod_{i=1}^{m}G(p_i,n)$ satisfies the condition of the theorem.

A problem. A natural measure of 'Hamiltonianess' which we have yet to consider is given by

$$P_G^+(G) = \frac{|\{(x,y)|x^{-1}yx = y^k \text{ for some positive integer } k\}|}{|G|^2}$$

because $P_G^+(G) = 1$ if, and only if, each cyclic subgroup of G is normal; i.e., G is Hamiltonian. Thus, since the normalizers of $\langle x\rangle$ and $\langle y\rangle$ are equal when $\langle x\rangle = \langle y\rangle$, we have

$$(3) \qquad P_G^+(G) = \frac{\sum_{\langle x\rangle\in C}\phi(|\langle x\rangle|)|N(x)|}{|G|^2}$$

where ϕ is the Euler phi function and $N(x)$ is the normalizer of $\langle x \rangle$.

Does the theorem hold for $P_G^+(G)$? Setting $G = G(p,n)$ and using (3) yields

$$\begin{aligned} P_G^+(G(p,n)) &= \frac{\sum_{i=2}^{n-1} p \cdot \phi(p^i) \cdot |G| + p \cdot \phi(p) \cdot (|G|/p) + \phi(p) \cdot |G| + |G|}{|G|^2} \\ &= \frac{p^n - p^2 + 2p - 1}{p^n} \end{aligned}$$

since there are p normal cyclic subgroups of order p^i, $2 \leq i \leq n-1$, p cyclic subgroups of order p each with normalizer index p and there is one normal cyclic subgroup of order p and the trivial subgroup. Clearly $\lim_{n\to\infty} P_G^+(G(p,n)) = \lim_{p\to\infty} P_G^+(G(p,n)) = 1$. It is easy to verify that $P_{H\times K}^+(H \times K) \leq P_H^+(H) \cdot P_K^+(K)$; i.e. that $P_G^+(G)$ is sub-multiplicative. Thus for $G_k = \prod_{i=1}^{k} H$, $P_{G_k}^+(G_k) \leq (P_H^+(H))^k$ implies that $\lim_{k\to\infty} P_{G_k}^+(G_k) = 0$ for any non-Hamiltonian group H. However, the construction of the theorem will not work for $0 < r < 1$ because $\lim_{p\to\infty} P_G^+(G(p,n)) = 1$.

Problem: For each $r \in (0,1)$ does there exist a sequence of groups $\{G_n\}$ such that $\lim_{n\to\infty} P_{G_n}^+(G_n) = r$?

References

1. W.C. Calhoun, Counting the subgroups of some finite groups, Amer. Math. Monthly 94 (1987), 54-59.

2. P. Erdos and P. Turan. On some problems of a statistical group-theory, IV, Acta. Math. Acad. Sci. Hung. 19 (1968), 413-435.

3. W.H. Gustafson, What is the probability that two group elements commute? Amer. Math. Monthly 80 (1973), 1031-1034.

4. M. Hall, Jr., The Theory of Groups, Macmillan, 1959.

5. T.J. Laffey and D. MacHale, Automorphism orbits of finite groups, J. Austral. Math. Soc. (Series A), 40 (1986) 253-260.

6. D. Passman, Nonnormal subgroups of p-groups, J. Alg., 15 (1970) 352-370.

7. G.J. Sherman, What is the probability that an automorphism fixes a group element?, Amer. Math. Monthly 82 (1975), 261-264.

8. ———, A probabilistic estimate of invariance for groups, Ibid. 85 (1978). 361-363.

9. Hans Zassenhaus, The Theory of Groups, Chelsea Publishing Company, 2nd Edition, 1958.

Gary J. Sherman

Department of Mathematics

Rose-Hulman Institute of Technology

Terre Haute, IN 47803

USA

Thomas J. Tucker

Department of Mathematics

Harvard University

Cambridge, MA 02138

USA

Mark E. Walker

Department of Mathematics

New Mexico State University

Las Cruces, NM 88003

USA