1-1994

Finite Groups can be Arbitrarily Hamiltonian

Stephen Ahearn

Mark Huber

FINITE GROUPS CAN BE ARBITRARILY HAMILTONIAN

Stephen Ahearn and Mark Huber

MS TR 94-01

January 1994

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

FAX(812) 877-3198

Phone: (812) 877-8391

Finite groups can be arbitrarily Hamiltonian

Stephen Ahearn* Mark Huber*

January 25, 1994

Abstract

Let r be a rational in (0,1]. There exists a finite group G which is the direct product of at most four metacyclic groups and whose proportion of normal subgroups is r. An analogous result holds for three other measures of 'Hamiltonianess'.

1 Introduction

Suppose that the finite group G acts on the finite non-empty set X. We may interpret

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

as the probability that an element chosen at random from G fixes an element chosen at random from X. The numerator of P_G is just $k(X) \cdot |G|$, i.e., the number of distinct orbits of X under G multiplied by the number of elements of G. Hence $P_G(X) = (k(X) \cdot |G|)/(|G| \cdot |X|) = k(X)/|X|$. If we denote the fixed set of G (the number of orbits of X of length one) by $F(X)$ and the action set of G (the number of orbits of X of length greater than one) by $A(X)$, then $k(X) = |F(X)| + |A(X)|$ so

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

*Both authors supported by NSF grant DMS-9100509

This ratio has been studied for several group actions. For instance, if G acts on itself by conjugation, then $P_G(G)$ is the probability that two elements of G commute. This probability is one or at most 5/8 ([1], [2]).

We consider the action of G on its set of subgroups S 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. If $A(S)$ denotes the action set of G on S, then $P_G(S) = (|NS| + |A(S)|)/|S|$ and by restricting the action of G on S to C, $P_G(C) = (|NC| + |A(C)|)/|S|$. We also define $P_{\bar{G}}(S) = |NS|/|S|$ and $P_{\bar{G}}(C) = |NC|/|C|$. Each of these ratios will be 1 if and only if every subgroup of G is normal in G. Such a group is called Hamiltonian, and each such group is the direct product of the quaternion group of order eight, an elementary abelian 2-group, and an abelian group in which each element is of odd order.

Let $\mu = \mu(G)$ denote any of the ratios $P_G(S)$, $P_{\bar{G}}(S)$, $P_G(C)$, $P_{\bar{G}}(C)$. Sherman, Tucker, and Walker [3] showed that $\{ \mu(G) \}$ is dense in the interval [0,1]. Our question: For what rational numbers in the interval (0,1] can a group G be found such that $\mu(G)$ equals that rational number? In this paper we show that **Theorem.** *For each rational number $r \in (0,1]$, there exists a group G such that $\mu(G) = r$.*

If r is 1, then any Hamiltonian group will suffice. Given r between 0 and 1, we will construct a group G with the desired ratio. This group G will be the direct product of three groups taken from three different infinite families of metacyclic groups.

2 Groups and Facts

We define three families of groups. Let p be an odd prime and let n be a positive integer.

- $$G(p,n) = \langle a, b \mid a^{p^{n-1}} = b^p = e \text{ and } bab^{-1} = a^{p^{n-2}+1} \rangle, n \geq 3.$$

$$|G(p,n)| = p^n.$$

- $$H(p,n) = G(p,n) \times C_p, n \geq 3.$$

$$|H(p,n)| = p^{n+1}.$$

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

$$|J(p,n)| = p \cdot 2^n.$$

Fact 1 ([4]) $|S(G(p,n))| = (n-2)(p+1) - 3$.

Fact 2 ([3]) *$G(p,n)$ has $p+1$ subgroups of order p^j for $1 \leq j \leq n-1$. If $j \geq 2$, then p of these groups are cyclic, and one is non-cyclic. Since all subgroups of order p are cyclic,* $|C(G(p,n))| = (n-1)p + 2$.

Fact 3 ([3], [5]) $|NS(G(p,n))| = (n-2)(p+1) + 3$ *and* $|NC(G(p,n))| = (n-2)p + 2$. *All non-normal subgroups are conjugate so $A(S) = 1$, and $A(C) = 1$.*

Fact 4 $|S(H(p,n))| = (n-1)[(p^2 + 1 + p(p+1)] + p + 3$

Proof. Let $A \leq G(p,n)$, so that $|A| = p^i$, $1 \leq i \leq n$. Suppose A is cyclic, with generator $\hat{a}$. Then the subgroups $\langle(\hat{a},0)\rangle, \langle(\hat{a},1)\rangle, \ldots, \langle(\hat{a},p-1)\rangle$ of $H(p,n)$ are all distinct. Also $A \times C_p \leq H(p,n)$. Thus, each cyclic subgroup determines at least $p+1$ subgroups of $H(p,n)$.

Now suppose that A is non-cyclic. From Fact 2 we know that $G(p,n)$ has only one non-cyclic subgroup of order p^i, $2 \leq i \leq n-1$. If we set $\hat{a} = a^{p^{n-i}}$ and $\hat{b} = b$, then

$$\hat{a}^{p^{i-1}} = \hat{b}^p = e$$

and

$$\hat{b}\hat{a}\hat{b}^{-1} = ba^{p^{n-i}}b^{-1} = a^{(p^{n-i})(p^{n-2}+1)}bb^{-1} = a^{p^{2n-i-2}}a^{p^{n-i}} = a^{p^{n-i}} = \hat{a}.$$

So,

$$A = \langle \hat{a}, \hat{b} \,|\, \hat{a}^{p^{i-1}} = \hat{b}^p = e,\ \hat{b}\hat{a}\hat{b}^{-1} = \hat{a} \rangle \cong C_{p^{i-1}} \times C_p$$

is the non-cyclic subgroup of $G(p,n)$ of order p^i.

Now $\langle (\hat{a}, c_1), (\hat{b}, c_2) \rangle$ are different subgroups of $H(p,n)$ for each different choice of $c_1, c_2 \in C_p$. Since C_p has p elements, p^2 choices exist for c_1, c_2. Also $A \times C_p$ is a subgroup of $H(p,n)$ of order p^{i+1} so that altogether A determines $p^2 + 1$ subgroups of $H(p,n)$.

Finally, $G(p,n)$ itself determines $p^2 + 1$ subgroups in $H(p,n)$ since it is generated by two elements. The identity subgroup determines just two subgroups, the identity in $H(p,n)$ and the direct product of the identity with C_p.

By Fact 2, $G(p,n)$ has p cyclic subgroups and 1 non-cyclic subgroup of order p^i, $2 \leq i \leq n-1$ and $p+1$ cyclic subgroups of order p. Hence,

$$\begin{aligned} |S(H(p,n))| &\geq (n-2)[p(p+1) + 1(p^2+1)] + (p+1)(p+1) + (p^2+1) + 2 \\ &= (n-1)[(p^2+1) + p(p+1)] + p + 3. \end{aligned}$$

Now we will show that $|H(p,n)| \leq (n-1)[(p^2+1) + p(p+1)] + p + 3$. Let $X \leq H(p,n)$, and X_G be the projection of X onto $G(p,n)$.

Suppose $|X_G| = |X|$. If $X_G = \langle \hat{a} \rangle$, then X must also be cyclic. So X must be generated by $(\hat{a}, c)$, where $c \in C_p$, but we have already counted these possibilities. Similarly, if $X_G = \langle \hat{a}, \hat{b} \rangle$, then X is just $\langle (\hat{a}, c_1), (\hat{b}, c_2) \rangle$, $c_1, c_2 \in C_p$, and we have also counted these possibilities.

Now suppose $|X_G| < |X|$. We know that $X \subseteq X_G \times C_p$, so $|X| \leq |X_G| \cdot p$. By Lagrange's Theorem, $|X_G| = |X|/p$ which implies $X = X_G \times C_p$, which we have already counted.

Therefore we have in fact counted all of the subgroups of $H(p,n)$ and

$$|S(H(p,n))| = (n-1)[(p^2+1) + p(p+1)] + p + 3. \square$$

Fact 5 $|NS(H(p,n))| = |S(H(p,n))| - 2p^2$.

Proof. We showed in the proof of Fact 4 how to construct the subgroups of $H(p,n)$ from the subgroups of $G(p,n)$. It is clear that any non-normal subgroup in $G(p,n)$ determines a non-normal subgroup in $H(p,n)$. However, it is possible for a normal subgroup in $G(p,n)$ to determine a non-normal subgroup in $H(p,n)$. Once these are counted, the number of non-normal subgroups of $H(p,n)$ may be shown to be $2p^2$, leaving $|S(H(p,n))| - 2p^2$ normal subgroups. We use a sequence of lemmas to find the number of non-normal subgroups in $H(p,n)$.

Lemma 1 *If $X_G \trianglelefteq G(p,n)$, then $X_G \times C_p \trianglelefteq H(p,n)$.*

Proof. Let (g,c) be any element of $H(p,n)$, and (x,y) be any element of $X_G \times C_p$. Then

$$(g,c)^{-1}(x,y)(g,c) = (g^{-1}xg, c^{-1}yc) = (x',y)$$

where $x' \in X_G$ because X_G is normal in $G(p,n)$. □

Now we examine the center of $G(p,n)$. Specifically, we note that $a^p \in Z(G(p,n))$ Let $a^t b^s \in G(p,n)$. Then

$$\begin{aligned} b^{-s}a^{-t}a^p a^t b^s &= b^{-s}a^p b^s \\ &= a^{p(p^{n-2}+1)^s} b^{-s} b^s \\ &= a^p. \end{aligned}$$

Thus, a^p is in the center of $G(p,n)$.

Also, note that $a^i \neq b^j$, where $0 \leq j \leq p-1$, $1 \leq i \leq p^{n-1} - 1$. Since this is trivial if $j = 0$, assume that $1 \leq j \leq p-1$. Suppose to the contrary that $a^i = b^j$. Then $b^j a = ab^j$. But, $b^j a b^{-j} = a^{(p^{n-2}+1)^j}$, so $a^{jp^{n-2}+1} = a$ and $a^{jp^{n-2}} = e$. However, $j \leq p-1$, which is a contradiction.

Lemma 2 *Let X be a cyclic subgroup of $H(p,n)$ such that $|X| \geq p^2$, and let X_G be the projection of X onto G. If $X_G \trianglelefteq G(p,n)$, then $X \trianglelefteq H(p,n)$.*

Proof. First, if $|X_G| < |X|$ then $X = X_G \times C_p$, a case covered by the previous lemma. So suppose that $|X| = |X_G|$. This implies that X_G is cyclic of order p^i, where $2 \leq i \leq n-1$.

We will now show that $X_G = \langle a^{p^{n-i-1}} b^j \rangle$ for some $0 \leq j \leq p-1$. Suppose that $(a^{p^{n-i-1}} b^j)^k = e$. Then $a^{kp^{n-i-1}} b^k = e$ since $a^p \in Z(G(p,n))$. The smallest value of k for which this expression holds is p^i, so $|\langle a^{p^{n-i-1}} b \rangle| = p^i$.

Now we will show that these groups are distinct for different values of j. Suppose that $a^{p^{n-i-1}} b^{j_1} \in \langle a^{p^{n-i-1}} b^{j_2} \rangle$. Then $(a^{p^{n-i-1}} b^{j_1})^m = a^{p^{n-i-1}} b^{j_2}$, for some $1 \leq m \leq p^i$, which in turn implies that $a^{(m-1)p^{n-i-1}} = b^{j_2 - mj_1}$. But this cannot happen unless $m = 1$, so $b^{j_2 - j_1} = e$ and thus $j_1 = j_2$. Hence $\langle a^{p^{n-i-1}} b^j \rangle$ are distinct cyclic subgroups of order p^i for $0 \leq j \leq p-1$. Thus the p cyclic subgroups of order p^i, $2 \leq i \leq n-1$ are all of this form, and in particular $\langle a^{p^{n-i-1}} b^j \rangle = X_G$ for some $0 \leq j \leq p-1$.

Hence $(a^{p^{n-i-1}} b^j, c_1)$, where $c_1 \in C_p$, generates X. To show that X is normal in $H(p,n)$ we conjugate $(a^{p^{n-i-1}} b^j, c_1)^m$ by (g, c_2), and an arbitrary element of $H(p,n)$.

$$(g^{-1}, c_2^{-1})((a^{p^{n-i-1}} b^j)^m, c_1^m)(g, c_2) = (g^{-1} a^{mp^{n-i-1}} b^{mj} g, c_1^m).$$

Letting $g = a^t b^s$, our expression becomes:

$$\begin{aligned}
(g^{-1} a^{mp^{n-i-1}} b^{mj} g, c_1^m) &= (b^{-s} a^{-t} a^{mp^{n-i-1}} b^{mj} a^t b^s, c_1^m) \\
&= (b^{-s} a^{-t} a^{mp^{n-i-1}} a^{t(p^{n-2}+1)^{mj}} b^{mj} b^s, c_1^m) \\
&= (b^{-s} a^{-t} a^{mp^{n-i-1}} a^{mjtp^{n-2}} a^t b^{mj} b^s, c_1^m) \\
&= (b^{-s} (a^{p^{n-i-1}})^m (a^{p^{n-i-1}})^{tmjpp^{i-2}} b^{mj} b^s, c_1^m) \\
&= (a^{p^{n-i-1}})^m (b^j)^m (a^{p^{n-i-1}})^{tmjpp^{i-2}} (b^j)^{pp^{i-2}}, c_1^m) \\
&= (a^{p^{n-i-1}} b^j, c_1)^m (a^{p^{n-i-1}} b^j, 0)^{tmjpp^{i-2}} \\
&= (a^{p^{n-i-1}} b^j, c_1)^m (a^{p^{n-i-1}} b^j, c_1)^{tmjpp^{i-2}} \\
&= (a^{p^{n-i-1}} b^j, c_1)^{m + tmjpp^{i-2}},
\end{aligned}$$

which is an element of $\langle (a^{p^{n-i-1}}b^j, c_1)\rangle$, and so X is normal in $H(p,n)$. □

Lemma 3 *Exactly p^2 of the subgroups of $H(p,n)$ of order p are non-normal.*

Proof. It was shown in the proof of the previous fact that all of the subgroups of $H(p,n)$ of order p are determined by subgroups of $G(p,n)$ of order p or 1. Now, the subgroup of $G(p,n)$ of order 1 is just the identity, and so it determines a normal subgroup of $H(p,n)$ of order p.

Out of the $p+1$ subgroups of $G(p,n)$ of order p, only one is normal [3]. Since $a^p \in Z(G(p,n))$, $\langle a^{p^{n-2}}\rangle$ is clearly this normal subgroup. Also $(g^{-1}, c_2^{-1})(a^{p^{n-2}}, c_1)^m(g, c_2) = (a^{p^{n-2}}, c_1)^m$ and so $\langle (a^{p^{n-2}}, c_1)\rangle$ is normal in $H(p,n)$. The other cyclic subgroups of order p of $G(p,n)$ are not normal in $G(p,n)$, and so the subgroups they determine in $H(p,n)$ cannot be normal. Each of these groups generates p cyclic subgroups in $H(p,n)$ of order p, so a total of p^2 subgroups of $H(p,n)$ of order p are non-normal. □

Lemma 4 *Exactly p^2 of the subgroups of $H(p,n)$ of order p^2 are non-normal.*

Proof. The proof of the previous fact showed that the subgroups of $H(p,n)$ of order p^2 are determined by subgroups of $G(p,n)$ of order p^2 or p. Each subgroup of $G(p,n)$ of order p determines one subgroup of $H(p,n)$ of order p^2. Since $G(p,n)$ has p non-normal subgroups and one normal subgroup of order p, it follows from Lemma 1 that these determine p non-normal subgroups and one normal subgroup of order p^2 in $H(p,n)$.

We now look at the subgroups of $G(p,n)$ of order p^2. Exactly p of these groups are cyclic and normal and the subgroups of $H(p,n)$ which they determine are also cyclic. Hence by Lemma 2, these subgroups of $H(p,n)$ are all normal.

However, $G(p,n)$ has one non-cyclic subgroup of order p^2. In the proof of Fact 4 we showed that the generators for this group are $\hat{a} = a^{p^{n-2}}$ and $\hat{b} = b$ with

$$A = \langle \hat{a}, \hat{b} \mid \hat{a}^p = \hat{b}^p = e \text{ and } \hat{b}\hat{a}\hat{b}^{-1} = \hat{a}\rangle \cong C_p \times C_p.$$

We shall show that $\langle(\hat{a},0),(\hat{b},c)\rangle \lhd H(p,n)$, for all $c \in C_p$. Conjugating an arbitrary element of $\langle(\hat{a},0),(\hat{b},c)\rangle$ by an arbitrary element of $H(p,n)$ gives

$$(g_1^{-1},c_1^{-1})(\hat{a},0)^{m_1}(\hat{b},c)^{m_2}(g,c_1) = (g_1^{-1}\hat{a}^{m_1}\hat{b}^{m_2}g_1, c^{m_2})$$

Letting $g_1 = a^t b^s$ the expression becomes:

$$\begin{aligned}
(g_1^{-1}\hat{a}^{m_1}\hat{b}^{m_2}g_1, c_1^{m_2}) &= (b^{-s}a^{-t}\hat{a}^{m_1}\hat{b}^{m_2}a^t b^s, c^{m_2}) \\
&= (b^{-s}a^{-t}\hat{a}^{m_1}a^{t(p^{n-2}+1)^{m_2}}\hat{b}^{m_2}b^s, c^{m_2}) \\
&= (b^{-s}\hat{a}^{m_1}\hat{a}^{tm_2}\hat{b}^{m_2}b^s, c^{m_2}) \\
&= (\hat{a}^{m_1+tm_2}\hat{b}^{m_2}, c^{m_2}) \\
&= (\hat{a},0)^{m_1+tm_2}(\hat{b},c)^{m_2}
\end{aligned}$$

which is clearly an element of $\langle(\hat{a},0),(\hat{b},h)\rangle$.

On the other hand, $\langle(\hat{a},c_1),(\hat{b},c_2)\rangle \not\lhd H(p,n)$, where $c_1 \in C_p \setminus \{0\}$, $c_2 \in C_p$. Simply note that conjugation by $(a,0)$ yields:

$$\begin{aligned}
(a^{-1},0)(\hat{a},c_1)(\hat{b},c_2)(a,0) &= (a^{-1}\hat{a}\hat{b}a, c_1c_2) \\
&= (a^{-1}\hat{a}a^{p^{n-2}+1}\hat{b}, c_1c_2) \\
&= (\hat{a}^2\hat{b}, c_1c_2) \\
&= (\hat{a}^2,c_1)(\hat{b},c_2)
\end{aligned}$$

which is not an element of $\langle(\hat{a},c_1),(\hat{b},c_2)\rangle$.

Thus this non-cyclic subgroup of $G(p,n)$ of order p^2 generates p^2 subgroups of $H(p,n)$ of order p^2, only p of which are normal in $H(p,n)$. Hence p^2-p of these groups are non-normal in $H(p,n)$. Combined with the p non-normal subgroups of $H(p,n)$ which are determined by the p non-normal subgroups of $G(p,n)$, there are exactly p^2 non-normal subgroups of $H(p,n)$ of order p^2. □

Lemma 5 *All of the subgroups of $H(p,n)$ of order p^3 are normal.*

Proof. As before, we note that the subgroups of $H(p,n)$ of order p^3 are determined by subgroups of $G(p,n)$ of order p^2 or p^3. Each of the subgroups of $G(p,n)$ of order p^2 are normal and so, by Lemma 1, determine a normal subgroup of $H(p,n)$.

Of the subgroups of $G(p,n)$ of order p^3, all but one are cyclic. These cyclic subgroups determine cyclic subgroups of order p^3 in $H(p,n)$, which by Lemma 2 are normal in $H(p,n)$. The remaining subgroups of $H(p,n)$ of order p^3 are determined by the non-cyclic subgroup of $G(p,n)$ of order p^3. There are two cases to consider.

Case: $n = 3$. We will conjugate an arbitrary element of $\langle (a,c_1),(b,c_2)\rangle$ by $(a^t b^s, c)$.

$$\begin{aligned}(b^{-s}a^{-t},c^{-1})(a,c_1)^{m_1}(b,c_2)^{m_2}(a^t b^s,c) &= (b^{-s}a^{-t}a^{m_1}b^{m_2}a^t b^s, {c_1}^{m_1}{c_2}^{m_2}) \\ &= (b^{-s}a^{-t}a^{m_1}a^{t(p^{n-2}+1)^{m_2}}b^{m_2}b^s, {c_1}^{m_1}{c_2}^{m_2}) \\ &= (b^{-s}a^{m_1}a^{ptm_2}b^{m_2}b^s, {c_1}^{m_1}{c_2}^{m_2}) \\ &= (a,c_1)^{m_1+ptm_2}(b,c_2)^{m_2}\end{aligned}$$

which is in $\langle (a,c_1),(b,c_2)\rangle$.

Case: $n \geq 4$. Then we showed in the proof of the previous fact that the non-cyclic subgroup is of the form $A = \langle \hat{a},\hat{b} \mid \hat{a}^p = \hat{b}^p = e \text{ and } \hat{b}\hat{a}\hat{b}^{-1} = \hat{a}\rangle \cong C_{p^2} \times C_p$, where we set $\hat{a} = a^{p^{n-3}}$, and $\hat{b} = b$. As before, we conjugate an element of $\langle (\hat{a},c_1),(\hat{b},c_2)\rangle$ by $(a^t b^s, c)$ to get

$$\begin{aligned}(b^{-s}a^{-t},c^{-1})(\hat{a},c_1)^{m_1}(\hat{b},c_2)^{m_2}(a^t b^s,c) &= (b^{-s}a^{-t}\hat{a}^{m_1}\hat{b}^{m_2}a^t b^s, {c_1}^{m_1}{c_2}^{m_2}) \\ &= (b^{-s}a^{-t}\hat{a}^{m_1}a^{t(p^{n-2}+1)^{m_2}}\hat{b}^{m_2}b^s, c_1^{m_1}c_2^{m_2}) \\ &= (b^{-s}\hat{a}^{m_1}\hat{a}^{ptm_2}\hat{b}^{m_2}b^s, {c_1}^{m_1}{c_2}^{m_2}) \\ &= (\hat{a},c_1)^{m_1+ptm_2}(\hat{b},c_2)^{m_2}\end{aligned}$$

which is in $\langle (\hat{a},c_1),(\hat{b},c_2)\rangle$. □

Passman [5] showed that in a p-group where p is an odd prime, if all the subgroups of order p^i are normal then the orders of the non-normal groups are either all smaller or all larger than p^i. In our case we have found that all the subgroups of order p^3 are normal, while some subgroups of order p^2 and p are not normal. Hence, all of the subgroups of order p^i, $3 \leq i \leq n$, are normal.

Now we may count the number of non-normal subgroups of $H(p,n)$. There are p^2 non-normal subgroups of order p, and p^2 non-normal subgroups of order p^2. Altogether, $H(p,n)$ has $2p^2$ non-normal subgroups.

Fact 6 ([4]) $|S(J(p,n))| = p + 1 + 2n$.

Proof. It follows from [4] that

$$\begin{aligned} |S(J(p,n))| &= \sum_{q|p} \sum_{t|2^n} \left(q, \frac{(p-1)^{2^n}-1}{(p-1)^t-1}\right) \\ &= \sum_{t|2^n} \left(1, \frac{(p-1)^{2^n}-1}{(p-1)^t-1}\right) + \sum_{t|2^n} \left(p, \frac{(p-1)^{2^n}-1}{(p-1)^t-1}\right) \\ &= n+1+\left(p, \frac{(p-1)^{2^n}-1}{p-2}\right) + \sum_{i=1}^{n} \left(p, \frac{(p-1)^{2^n}-1}{(p-1)^{2^i}-1}\right) \end{aligned}$$

Here we note that if $i \geq 1$ then by the binomial theorem $p \mid (p-1)^{2^i} - 1$ but $p^2 \nmid (p-1)^{2^i} - 1$. Hence, $\left(p, \frac{(p-1)^{2^n}-1}{p-2}\right) = p$ but $\left(p, \frac{(p-1)^{2^n}-1}{(p-1)^{2^i}-1}\right) = 1$. So $|S(J(p,n))| = n + 1 + p + n = 2n + 1 + p$.

Fact 7 *Every proper subgroup of $J(p,n)$ is cyclic; i.e., $|C(J(p,n))| = 2n + p$.*

Proof. We use two lemmas to establish the cyclicity of each proper subgroup.

Lemma 6 *There are exactly p Sylow 2-subgroups of $J(p,n)$ and they are all cyclic.*

Proof. The number of distinct Sylow 2-subgroups of $J(p,n)$ is either 1 or p. This number will be p if any of the Sylow 2-subgroups are not normal in $J(p,n)$. Now $\langle b \rangle$ has order 2^n and so is a cyclic Sylow 2-subgroup of $J(p,n)$. However, it is not normal in $J(p,n)$, since $a^{-1}ba = a^{-1}a^{-1}b = a^{-2}b$

which is not an element of $\langle b \rangle$. So there are p distinct Sylow 2-subgroups of $J(p,n)$, and since they are all conjugate to $\langle b \rangle$, they are all cyclic. □

Before examining the other subgroups, we first observe that $b^2 \in Z(J(p,n))$. Clearly b commutes with b^2 and so does a since $b^2a = ba^{-1}b = abb = ab^2$. Hence b^2 is in the center of $J(p,n)$.

Lemma 7 *There are exactly $2n-1$ non-trivial cyclic subgroups of $J(p,n)$ distinct from the Sylow 2-subgroups and each one is cyclic.*

Proof. Recall from the previous Fact that $J(p,n)$ has exactly $2n+1+p$ subgroups. We have found p Sylow 2-subgroups, which together with the two trivial subgroups leaves $2n-1$ subgroups. So we have at most $2n-1$ non-trivial cyclic subgroups, now we must show that there are at least $2n-1$ non-trivial cyclic subgroups. It suffices to show that $J(p,n)$ has a cyclic subgroup of order $p \cdot 2^{n-1}$. This subgroup is $\langle a, b^2 \rangle$. Note that the generating elements commute and that $a^p = (b^2)^{2^{n-1}} = e$: $\langle a, b^2 \rangle \cong C_p \times C_{2^{n-1}} \cong C_{p \cdot 2^{n-1}}$. Therefore $\langle a, b^2 \rangle$ is cyclic of order $p \cdot 2^{n-1}$. □

Fact 8 *The p distinct Sylow 2-subgroups are the only non-normal subgroups of $J(p,n)$. This implies that $|NS(J(p,n))| = 1+2n$ and $|NC(J(p,n))| = 2n$.*

Proof. The p Sylow 2-subgroups are non-normal in $J(p,n)$, by Lemma 6. It remains to show that the remaining subgroups are normal. Recall that if a subgroup of $J(p,n)$ is not a Sylow 2-subgroup, then it is a subgroup of $\langle a, b^2 \rangle \cong C_p \times C_{2^{n-1}}$, and so either has the form $\langle a, b^{2^i} \rangle \cong C_p \times C_{2^{n-i-1}}$, or the form $\langle b^{2^i} \rangle \cong C_{2^{n-i-1}}$, where $1 \leq i \leq n-1$. However, $\langle b^2 \rangle \in Z(J(p,n))$, so clearly $\langle b^{2^i} \rangle \lhd J(p,n)$ for all $i \geq 1$.

Since $\langle b^2 \rangle \in Z(J(p,n))$, the subgroup $\langle a, b^{2^i} \rangle$ may be written as $\langle a \rangle \times \langle b^{2^i} \rangle$. We know that $\langle b^{2^i} \rangle$ is normal, so it remains to show that $\langle a \rangle$ is normal is $J(p,n)$. This follows from the defining relations for $J(p,n)$. So every subgroup of $\langle a, b^2 \rangle$ is normal in $J(p,n)$. Thus the p Sylow 2-subgroups are the only non-normal subgroups of $J(p,n)$.

Fact 9 *For $J(p,n)$, $|A(S)| = |A(C)| = 1$.*

Proof. The only non-normal subgroups of $J(p,n)$ are the Sylow 2-subgroups. These are all conjugate, so $|A(S)| = 1$. Clearly $|A(C)| \leq |A(S)|$, so $|A(C)| = 1$ as well.

3 Some Number Theory

We are now able to construct a group G such that $\mu(G) = r$ for any r between 0 and 1. First note that for each measure μ, if the orders of the groups X and Y are relatively prime, then $\mu(X \times Y) = \mu(X) \cdot \mu(Y)$

We begin by proving the theorem for $\mu(G) = P_{\bar{G}}(S)$. Recall from the facts that

$$P_{\overline{G(3,n)}}(S) = \frac{(n-2)(3+1)+3}{(n-1)(3+1)+2} = \frac{4n-5}{4n-2}, \tag{1}$$

$$P_{\overline{H(7,n)}}(S) = \frac{106n-194}{106n-96} = \frac{53n-97}{53n-48}, \tag{2}$$

$$P_{\overline{J(p,n)}}(S) = \frac{1+2n}{p+1+2n}. \tag{3}$$

If the prime p is neither 3 nor 7, then the orders of $G(3,n)$, $H(7,n)$, $J(p,n)$ are relatively prime, and

$$\mu(G(3,n) \times H(7,n) \times J(p,n)) = \mu(G(3,n)) \cdot \mu(H(7,n)) \cdot \mu(J(p,n)).$$

We show through a series of lemmas that every rational number between 0 and 1 may be written as the product of three fractions of the form of (1), (2), and (3).

Lemma 8 *Let $a, b \in \mathbf{Z}^+$ be such that $a < b$, a is odd, and $b = c \cdot 2^k$, where c is odd and $k \geq 3$ is an integer. Then*

$$\frac{a}{b} = \frac{1+2n_1}{1+2n_1+p} \cdot \frac{4n_2-5}{4n_2-2}$$

for suitable integers $n_1, n_2 \geq 3$ and some prime not equal to 2, 3 or 7.

Proof. We first show that we can solve

$$\frac{a}{b} = \frac{am}{bm} = \frac{am}{am+p} \cdot \frac{bm - 2^{k-1}}{bm}.$$

Or more simply, we solve $bm - 2^{k-1} = am + p$ which may be reduced further to $m(b-a) - 2^{k-1} = p$. Because $b - a$ and 2^{k-1} are relatively prime, $m(b-a) - 2^{k-1} = p$ has a solution for an integer m and prime p by Dirichlet's Theorem. In fact, it has solutions for an infinite number of primes p, so we may choose one which is not equal to 2, 3, or 7.

Now, a is odd and b is even, so $b - a$ is odd. Also, p is odd, but 2^{k-1} is even, hence m is also odd. This implies that am is odd and so it may be written as $1 + 2n_1$. Also

$$\begin{aligned} \frac{bm - 2^{k-1}}{bm} &= \frac{cm2^k - 2^{k-1}}{cm2^k} \\ &= \frac{2cm - 1}{2cm} \\ &= \frac{3 \cdot 2cm - 3}{3 \cdot 2cm} \end{aligned}$$

Since $2c \equiv_4 2$, we may write $2c = 4n - 2$, so $3 \cdot 2c = 4n_2 - 2$, where n is an integer. Hence

$$\frac{a}{b} = \frac{1 + 2n_1}{1 + 2n_1 + p} \cdot \frac{4n_2 - 5}{4n_2 - 2}$$

for some integers $n_1 \geq 1, n_2 \geq 3$. □

Lemma 9 *If $a, b \in \mathbf{Z}^+$, such that $a < b$, then*

$$\frac{a}{b} = \frac{53n - 97}{53n - 48} \cdot \frac{\hat{a}}{\hat{b}}$$

where $\hat{a}$ is an odd integer, $\hat{b}$ is an integer divisible by 8, and n is an integer greater than or equal to 3.

Proof. First note that

$$\frac{a}{b} = \frac{53n - 97}{53n - 48} \cdot \frac{(53n - 48)a}{(53n - 97)b}.$$

Let k denote the largest integer such that $2^k|a$. Since 53 and 2^{k+3} are relatively prime, we can find an integer $n \geq 3$ such that $2^{k+3} \mid 53n - 97$. For this n, we note that $2 \not| 53n - 48$. So $(53n - 48)a = c_1 \cdot 2^k$, where $2 \not| c_1$ and $(53n - 97)b = c_2 \cdot 2^{k+3}$.

Hence

$$\begin{aligned} \frac{a}{b} &= \frac{53n - 97}{53n - 48} \cdot \frac{c_1 \cdot 2^k}{c_2 \cdot 2^{k+3}} \\ &= \frac{53n - 97}{53n - 48} \cdot \frac{c_1}{c_2 \cdot 2^3} \end{aligned}$$

and we are done. □

Lemma 10 *Let $a, b \in \mathbf{Z}^+$ be such that $a < b$, then*

$$\frac{a}{b} = \frac{53n_1 - 97}{53n_1 - 48} \cdot \frac{1 + 2n_2}{1 + 2n_2 + p} \cdot \frac{4n_3 - 5}{4n_3 - 2}$$

for integers $n_1 \geq 3, n_2 \geq 1, n_3 \geq 3$ and a prime p different from 2, 3, and 7.

Proof. This follows directly from Lemmas 8 and 9. □

Now if a/b is any rational number between 0 and 1, we use Lemma 3 and let

$$G = H(7, n_1) \times J(p, n_2) \times G(3, n_3),$$

so that $P_G(S) = a/b$.

We now turn our attention towards finding G such that $P_G(S) = a/b$. First note that

$$P_{J(p,n)}(S) = \frac{2n + 2}{2n + p + 1}$$

where p is an odd prime.

Lemma 11 *Let $a, b \in \mathbf{Z}^+$ be such that $a < b$. Then*

$$\frac{a}{b} = \frac{2n + 2}{2n + p + 1}$$

for some integer $n \geq 1$ and some odd prime p.

Proof. We will find an integer m such that

$$\frac{a}{b} = \frac{2am}{2bm} = \frac{2am}{2am - 1 + p};$$

i.e., we will find a solution m to the equation $2bm = 2am - 1 + p$, or equivalently $m(b-a)+1 = p$. By Dirichlet's Theorem, $m(b-a)+1 = p$ has a solution for $p \geq 3$, and $m \geq 2$. Since $2am$ is even and is greater than or equal to 4, it may be written as $2n+2$ for some suitable positve integer n, and the denominator becomes $2n+2-1+p$, or more simply $2n+1+p$, and we are done. □

Thus for any a/b, we use the preceeding Lemma to find n such that

$$P_{J(p,n)}(S) = \frac{a}{b}.$$

To find a group G such that $P_G(C) = a/b$, note that

$$\begin{aligned} P_{J(p,n)}(C) &= \frac{2n+1}{2n+p} \\ P_{G(3,n)}(C) &= \frac{3n-3}{3n-1} \end{aligned}$$

and use the following lemma.

Lemma 12 *Let a, b be relatively prime positve integers such that $a < b$, then*

$$\frac{a}{b} = \frac{2n_1+1}{2n_1+p} \cdot \frac{3n_2-3}{3n_2-1}$$

for some integers $n_1 \geq 1$, $n_2 \geq 3$ and some prime $p \geq 5$.

Proof. We begin by showing that

$$\frac{a}{b} = \frac{3n_2-3}{3n_2-1} \cdot \frac{\hat{a}}{\hat{b}},$$

where both $\hat{a}$ and $\hat{b}$ are odd postive integers. Suppose that $2|a$, so that b is odd. Then let $n_2 = 2a+1$ so $6a = 3n_2 - 3$ and

$$\frac{a}{b} = \frac{6a}{6b} = \frac{3n_2-3}{3n_2-1} \cdot \frac{3n_2-1}{6b}.$$

Since 4 divides $3n_2 - 3$, 4 does not divide $3n_2 - 1$, and so $(3n_2 - 1)/(6b)$ reduces to an odd number over an odd number. Now suppose that $2|b$, so that a is odd. Then $b = c \cdot 2^k$, where c is odd, and either $2^k \equiv_3 2$ or $5 \cdot 2^k \equiv_3 2$. Hence, by choosing m to be either 1 or 5 we may find a positive integer n_2 such that $2 \cdot 2^k \cdot m = 3n_2 - 1$. Then

$$\frac{a}{b} = \frac{2am}{2bm} = \frac{2am}{c(3n_2 - 3)} \cdot \frac{3n_2 - 3}{3n_2 - 1}.$$

Since $4|3n_2 - 1$, $3n_2 - 3$ is divisible by two but not by four, and $(2am)/[c(3n_2 - 3)]$ reduces to an odd number over an odd number.

Now we look at the fraction $\hat{a}/\hat{b}$ where both $\hat{a}$ and $\hat{b}$ are odd. We wish to solve

$$\frac{\hat{a}}{\hat{b}} = \frac{\hat{a}m}{\hat{b}m} = \frac{2n_1 + 1}{2n_1 + p},$$

which leads to the equation $m(b - a) + 1 = p$. Now we want m to be odd, so let $m = 2\hat{m} + 1$. This changes our equation to

$$\hat{m}[2(b - a)] + (b - a) + 1 = p.$$

To see that $2(b-a)$ and $(b-a)+1$ are relatively prime, we first obvserve that their greatest common divisor can be no greater than two, since $2[(b - a) + 1] - 2(b - a) = 2$. However, $2|(b - a)$ so 2 does not divide $(b - a) + 1$. Hence the greatest common divisor of the two expressions is 1, and we can solve this equation for a prime p not equal to 2 or 3 by Dirichlet's Theorem. Since a and m are both odd, am will be odd, and so we let $n_1 = (am - 1)/2$ and the lemma is proved. □

Now we use the above lemma and let $G = J(p, n_1) \times G(3, n_2)$ so that $P_G(C) = a/b$.

Finally, to find a group G such that $P_{\bar{G}}(C) = a/b$, recall that

$$\begin{aligned} P_{\overline{G(p,n)}}(C) &= \frac{(n-2)p + 2}{(n-1)p + 2}, \\ P_{\overline{J(p,n)}}(C) &= \frac{2n}{2n + p}. \end{aligned}$$

Lemma 13 *Let $a, b \in \mathbf{Z}^+$ be such that $a < b$, then*

$$\frac{a}{b} = \frac{2n_1}{2n_1 + p} \cdot \frac{(n_2 - 2)q + 2}{(n_2 - 1)q + 2}$$

where $n_1 \geq 1$ and $n_2 \geq 3$ are integers and p and q are distinct odd primes.

Proof. We may write

$$\frac{a}{b} = \frac{2am_1m_2}{2am_1m_2 + p} \cdot \frac{2bm_1m_2 - q}{2bm_1m_2}$$

where q and p are distinct odd primes such that $m_1 b \equiv_q 1$, and $m_2 \equiv_q 1$, so that $m_2 = qm_3 + 1$ for some positive integer m_3. Let q be an odd prime such that q does not divide either $b - a$ or b. We then let m_1 be any positive integer which solves $m_1 b \equiv_q 1$. Then we must solve

$$2bm_1(qm_3 + 1) - q = 2am_1(qm_3 + 1) + p$$

or equivalently,

$$m_3q[2(bm_1 - am_1)] + 2(bm_1 - am_1) - q = p.$$

Since $q[2(bm_1 - am_1)]$ and $2(bm_1 - am_1) - q$ are relatively prime, the above two equations have a solution by Dirichlet's Theorem for some positive integer m_3 and odd prime p distinct from q. Now just let $n_1 = am_1m_2$, and note that n_1 is a positve integer. Also, note that $2m_1m_2b \equiv_q 2$ because of our choices for q, m_1, and m_2. So we may let $2m_1m_2b = (n_2 - 2)q + 2$, where $(n_2 - 2) \geq 3$ since $m_2 \geq q$. This proves the lemma. □

Using this lemma for a/b we let $G = J(p, n_1) \times G(q, n_2)$ and so $P_{\bar{G}}(C) = a/b$. This completes the proof of the theorem for all the ratios $\mu(G)$.

References

[1] P. ERDÖS and P. TURAN, On some problems of a statistical group-theory, IV. Acta. Math. Acad. Sci. Hung. **19**, 413-435 (1968).

[2] W. H. GUSTAFSON, What is the probability that two group elements commute? Amer. Math. Monthly **80**, 1031-1034 (1973).

[3] G. J. SHERMAN, T. J. TUCKER, and M. E. WALKER, How Hamiltonian can a finite group be? Sonderdruck aus Arch. Math., **57**, 1-5 (1991).

[4] W. C. CALHOUN, Counting the subgroups of some finite groups. Amer. Math Monthly **94**, 54-59 (1987).

[5] D. PASSMAN, Nonormal subgroups of p-groups. J. Algebra **15**, 352-370 (1970).