9-1990

A Numerical Approach to Rewriteability in Finite Groups

J.L. Leavitt
University of Michigan

G.J. Sherman
Rose-Hulman Institute of Technology

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

A NUMERICAL APPROACH TO REWRITEABILITY IN FINITE GROUPS

J.L. Leavitt, G.J. Sherman and M.E. Walker

MS TR 90-02

September 1990

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

FAX(812) 877-3198

Phone: (812) 877-8391

A NUMERICAL APPROACH TO REWRITEABILITY IN FINITE GROUPS

J.L. LEAVITT*

University of Michigan, Ann Arbor, MI 48109

G.J. SHERMAN*

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

M.E. WALKER*

New Mexico State University, Las Cruces, NM 88003

Introduction. Let G be a finite group. The ratio

$$Pr_2(G) = \frac{|\{(x,y) \in G^2 | xy = yx\}|}{|G|^2} \tag{1}$$

can be interpreted as the probability that two randomly chosen elements of G commute. Denoting the centralizer of y in G by $C(y)$ and the number of conjugacy classes in G by k, we find that

$$\begin{aligned} |\{(x,y) \in G^2 | xy = yx\}| &= \sum_{y \in G} |C(y)| \\ &= \sum_{i=1}^{k} [G : C(y_i)] \cdot |C(y_i)| \\ &= k \cdot |G| \end{aligned} \tag{2}$$

where $\{y_1, y_2, \ldots, y_k\}$ is a complete set of conjugacy class representatives of G. Thus $Pr_2(G) = k/|G|$. Clearly, G is abelian if, and only if, $Pr_2(G) = 1$. If G is not abelian and p_s is the smallest prime divisor of $|G|$, then it follows from the class equation that

$$Pr_2(G) = \frac{k}{|G|} \leq \frac{p_s^2 + p_s - 1}{p_s^3} \leq \frac{5}{8}. \tag{3}$$

*Work supported by NSF grant DMS-8900507

Mathematics Subject Classification: 20D60

Both upper and lower bounds on $Pr_2(G)$ for various classes of groups have been obtained ([**1**], [**4**], [**5**], [**6**], [**7**], [**9**]). And, since commutativity can be defined in terms of conjugation, analagous results have been pursued for various group actions ([**8**], [**9**], [**11**]).

Commutativity is a special case of rewriteability. Let $S \subseteq S_n - \{\text{id}\}$; i.e., S is a set of nontrivial permutations of { 1,2,... n}. An n-tuple $(x_1, x_2, \ldots, x_n)$ of elements of G is S-rewriteable if $x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ for some $\sigma \in S$. We generalize (1) by setting

$$Pr_n(G; S) = \frac{|Rw_n(G; S)|}{|G|^n} \tag{4}$$

where

$$Rw_n(G; S) = \{(x_1, x_2, \ldots x_n) \in G^n | (x_1, x_2, \ldots x_n) \text{ is S-rewriteable}\}. \tag{5}$$

Those groups for which $Pr_n(G; S_n - \{\text{id}\}) = 1$ (or, in the infinite case, those groups for which $Rw_n(G; S - \{\text{id}\}) = G^n$) will be referred to as n-rewriteable groups. The notion of rewriteability has its origins in automata theory and is currently of considerable interest in group theory [**2**].

In particular, Curzio, Longobardo and Maj [**3**] have provided elementary proofs that the following statements are equivalent.

i) *G is 3-rewriteable; i.e., $xyz \in \{xzy, yxz.zyx, yxz, zyx\}$ for all $x, y, z \in G$.*

ii) The order of G', the derived group of G, is 1 or 2.

iii) Each conjugacy class of G is of order 1 or 2.

The equivalence of i) and iii) suggests a connection between 3-rewriteability and $Pr_2(G)$. Notice that the average order of a conjugacy class of a 3-rewriteable group is less than two; i.e., $|G|/k < 2$. Thus $Pr_2(G) = k/|G| > 1/2$ for 3-rewriteable groups. An appeal to character theory establishes the converse. G has k irreducible characters and $|G|/|G'|$ irreducible characters of degree one. Thus

$$|G| \geq (|G|/|G'|) \cdot 1^2 + (k - |G|/|G'|) \cdot 2^2$$

which implies

$$1 \geq -3/|G'| + 4k/|G|.$$

If $k/|G| > 1/2$ then $1 > -3/|G'| + 2$ from which it follows that $|G'| \leq 2$. So, we have the following theorem.

THEOREM. A finite group G is 3-rewriteable if, and only if, $Pr_2(G) > 1/2$.

The purposes of this note are to provide an elementary proof that $Pr_2(G) > 1/2$ is sufficient for 3-rewriteability and to prompt a numerical approach to rewriteability by making the following conjecture.

CONJECTURE. *If G is not n-rewriteable then there exists $\rho_n(S) < 1$, independent of G,* such that $Pr_n(G; S) \leq \rho_n(S) < 1$.

An elementary proof. We will assume that G is not 3-rewriteable and prove that $Pr_2(G) \leq 1/2$. The following three lemmas, which are of some interest in their own right, help organize the proof.

LEMMA 1. *If x and y are elements of G for which $[G : C(x)] = 2$ and $C(y) \bigcap (G - C(x)) \neq \emptyset$, then $[G : C(xy)] \geq [G : C(y)]$.*

Proof: The conjugacy class of y in G , y^G, may be written $\{y^{g_1}, y^{g_2}, \ldots, y^{g_n}\}$ where $\{g_1, g_2, \ldots, g_n\}$ is a complete set of right coset representatives for $C(y)$ in G. Moreover, we may choose each coset representative in $C(x)$. Otherwise $C(y)g_i \subseteq G - C(x)$, which means that $G - C(x) = C(x)g_i$ since $[G : C(x)] = 2$. Therefore $C(y)g_i \subseteq C(x)g_i$ and so $C(y) \subseteq C(x)$, a contradiction. The conclusion follows because the mapping $y^{g_i} \longrightarrow xy^{g_i}$ embeds y^G in $(xy)^G$.

LEMMA 2. *If at least $3 \cdot |Z|$ elements of G have centralizers of index at least 3, then $Pr_2(G) \leq 1/2$.*

Proof: Let $X = \{y \in G | [G : C(y)] \geq 3\}$ and let $Y = \{y \in G | [G : C(y)] = 2\}$. Then

$$\begin{aligned}
|Rw_2(G)| = k \cdot |G| &\leq (|X|/3 + |Y|/2 + |Z|) \cdot |G| \\
&= (|Z| + (|X| - 3 \cdot |Z|)/3 + |Y|/2 + |Z|) \cdot |G| \\
&\leq (|Z| + (|X| - 3 \cdot |Z|)/2) + |Y|/2 + |Z|) \cdot |G| \\
&= (|X| + |Y| + |Z|) \cdot |G|/2 \\
&= |G|^2/2.
\end{aligned}$$

Thus $Pr_2(G) \leq 1/2$ as claimed.

LEMMA 3. *If G is not 3-rewriteable, then $[G : Z] \geq 6$.*

Proof: If $[G : Z]$ is 1,2,3 or 5, then G is abelian since G/Z is cyclic. If $[G : Z] = 4$ and x is a non-central element, then $Z \subset C(x) \subset G$ implies $[G : C(x)] = 2$; i.e., G is 3-rewriteable.

To complete the proof note that $X \neq \emptyset$ since G is not 3-rewriteable. Choose $g \in X$ and set $n = [G : C(g)]$. Then, $Z \bigcup Zg \subseteq C(g)$ and $(Z \bigcup Zg) \bigcap Y = \emptyset$. Thus $|C(g) \bigcap Y| \leq |G|/n - 2|Z|$ and so $|(G - C(g)) \bigcap Y| \geq |Y| - |G|/n + 2 \cdot |Z|$. If $x \in (G - C(g)) \bigcap Y$, then $[G : C(x)] = 2$ and $C(g) \bigcap (G - C(x)) \neq \emptyset$ implies, by Lemma 1, that $[G : C(xg)] \geq [G : C(g)] \geq 3$. Therefore $|X| \geq |Y| - |G|/n + 2 \cdot |Z|$. But $Zg \subseteq X$ and $Zg \bigcap Yg = \emptyset$, so

$$|X| \geq |Y| - |G|/n + 3 \cdot |Z|. \tag{6}$$

In view of Lemma 2 and (6) we are done if $|Y| \geq |G|/3$, so assume $|Y| < |G|/3$. In this case Lemma 3 implies that $|X| > |G|/2$ and, therefore, that $|X| > 3 \cdot |Z|$. The theorem is proved.

COROLLARY. *If G is not 3-rewriteable, then at least $|G| \cdot (n-1)/2n + |Z|$ elements of G have centralizers of index at least 3 where n is the greatest centralizer index among the elements of G. In particular, more than 1/3 of the elements of G have centralizers of index at least 3.*

Proof: This follows directly from (6) by substituting $|G| - |X|$ for $|Y| + |Z|$.

The 1/2 bound for 3-rewriteability is sharp in two senses.

i) *$Pr_2(G) = 1/2$ if, and only if, $G/Z \cong S_3$.* This is a straight forward application of Lemma 3 and the Corollary.

ii) *There exists a sequence, $\{G_n\}$, of 3-rewriteable groups such that $Pr_2(G_n) \downarrow 1/2$.* Take G_n to be the extra-special 2-group generated by $x_1, x_2, \cdots x_{2n+1}$ subject to the relations

$$x_i^2 = e, \text{ for } 1 \leq i \leq 2n+1,$$

$$[x_i, x_j] = x_1 \text{ for } i \text{ even and } j = i+1$$

and

$$[x_i, x_j] = e \text{ otherwise.}$$

Then $|G_n| = 2^{2n+1}$ and $Z = G_n' = \{e, x_1\}$ so that $Pr_2(G_n) = k/|G_n| = 1/2 + 1/2^{2n+1}$.

A problem. We encourage study of the problem of determining bounds for $Pr_n(G; S)$. The following lemma generalizes (3) and is in support of the conjecture made in the introduction.

LEMMA 4. *If $n \geq 2$ and $\sigma \in S_n - \{id\}$, then $|Rw_n(G; \{\sigma\})| \leq k \cdot |G|^{n-1}$.*

Proof: The proof is by induction on n. The case for $n = 2$ was made in (2). Now assume the result holds for $n-1$.

If $\sigma(n) = n$, then $x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ if, and only if, $x_1 x_2 \cdots x_{n-1} = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n-1)}$. Therefore $|Rw_n(G; \{\sigma\})| = |Rw_{n-1}(G; \{\hat{\sigma}\})| \cdot |G|$ where $\hat{\sigma}$ is σ restricted to $\{1, 2, \ldots, n-1\}$. The induction hypothesis yields the result.

If $\sigma(n) < n$, say $\sigma(n) = m$, then $x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ if, and only if, $x_n^{-1} x_{\sigma(j-1)}^{-1} \cdots x_{\sigma(1)}^{-1} x_1 x_2 \cdots x_n = x_{\sigma(j+1)} x_{\sigma(j+2)} \cdots x_m$ where $\sigma(j) = n$. Let $g = x_{\sigma(j-1)}^{-1} x_{\sigma(j-2)}^{-1} \cdots x_{\sigma(1)}^{-1} x_1 x_2 \cdots x_{n-1}$ and $h = x_{\sigma(j+1)} x_{\sigma(j+2)} \cdots x_m$. Notice that $|\{x_n | x_n^{-1} g x_n = h\}|$ is $|C(g)|$ or 0 for fixed $x_1, x_2, \cdots x_{n-1}$, and that g varies over G as x_m varies over G. Thus

$$\begin{aligned}
|Rw_n(G;\{\sigma\})| &\leq \sum_{x_1}\cdots\sum_{x_m}\cdots\sum_{x_{n-1}}|C(g)| \\
&= \sum_{x_1}\cdots\sum_{x_{n-1}}(\sum_{x_m}|C(g)|) \\
&= \sum_{x_1}\cdots\sum_{x_{n-1}}(\sum_{g}|C(g)|) \\
&= \sum_{x_1}\cdots\sum_{x_{n-1}}(k\cdot|G|) \\
&= k|G|^{n-1} \quad \text{as claimed.}
\end{aligned}$$

It follows from (3) and Lemma 4 that

$$Pr_n(G;S) = |Rw_n(G;S)|/|G|^n| \leq |S|\cdot k/|G| \leq |S|\cdot(p_s^2+p_s-1)/p_s^3. \tag{7}$$

Since $(p_s^2+p_s-1)/p_s^3 \downarrow 0$ as $p_s \to \infty$ we may use (7) to conclude that, for $|S|$ fixed and sufficiently large p_s, a "5/8-like" bound exists for $Pr_n(G;S)$. Specifically, if $p_s \geq 7$, then $Pr_3(G;S_3-\{\text{id}\}) \leq 275/343$. If $p_s < 7$, extensive computation using CAYLEY suggests $Pr_3(G;S_3-\{\text{id}\})) \leq 17/18$. Thus for 3-rewriteability our conjecture is;

If G is not 3-rewriteable, then $Pr_3(G;S_3-\ \{\text{id}\}) \leq \rho_3(S_3-\ \{\text{id}\})= 17/18$.

If this conjecture proves to be true, then the 17/18 bound is sharp because $Pr_3(S_3;S_3-\{\text{id}\}) = 17/18$.

We conclude by observing that if G is a non-abelian finite simple group then, $Pr_3(G,S_3-\{\text{id}\}) \leq 5/12$. This follows from (7) because $Pr_2(G) \leq Pr_2(A_5)$ and $Pr_2(A_5) = 1/12$ [**5**]. It seems likely that the bound is actually 27/100 because CAYLEY shows $Pr_3(A_5,S_3-\{\text{id}\})$ to be 27/100.

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. R.D. Blyth and D.J.S. Robinson, 'Recent progress on rewriteability in groups', *J. London Math. Soc.*, to appear.

3. M. Curzio, P. Longobardi and M. Maj, 'Su di un problema combinatorio in teoria dei gruppi', *Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) 74 (1983), 136-142.

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

5. J.D. Dixon, 'Problem 176'. *Canad. Math. Bull.* 16 (1973) 302.

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

7. E. Landau, 'Klassenzahl binarer quadratischer Formen von negativer Discriminante', *Math. Annalen*, 56 (1903) 1031-1034.

8. T.J. Laffey and D. MacHale, 'Automorphism orbits of finite groups', *J. Austral. Math. Soc. (Series A)* 40 (1986) 253-260.

9. G.J. Sherman, 'A probabilistic estimate of invariance for groups', *Amer. Math. Monthly* 85 (1978) 361-363.

10. ——————, 'A lower bound for the number of conjugacy classes in a finite nilpotent group', *Pacific J. Math.*, 79 (1979) 253-254.

11. G.J. Sherman, T.J. Tucker and M.E. Walker, 'How Hamiltonian can a finite group be?' *Archives Math. (Basel)*, to appear.