1992

Rewriteability in Finite Groups

Judy Leavitt Walker
University of Nebraska - Lincoln, judy.walker@unl.edu

G. J. Sherman
Rose-Hulman Institute of Technology

Mark E. Walker
University of Nebraska - Lincoln, mark.walker@unl.edu

From: The American Mathematical Monthly, Vol. 99, No. 5 (May, 1992), pp. 446-452.
doi 10.1080/00029890.1992.11995873
Published by Taylor & Francis, Ltd. on behalf of the Mathematical Association of America.

Rewriteability in Finite Groups

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

INTRODUCTION. What's the probability that two elements in a finite group commute? A formal answer,

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

begs our next question. How many ordered pairs of elements of a finite group commute?

Let's be specific. Consider the "commutativity matrix" for the symmetric group on three symbols.

S_3	id	(1, 2)	(1, 3)	(2, 3)	(1, 2, 3)	(1, 3, 2)
id	1	1	1	1	1	1
(1, 2)	1	1	0	0	0	0
(1, 3)	1	0	1	0	0	0
(2, 3)	1	0	0	1	0	0
(1, 2, 3)	1	0	0	0	1	1
(1, 3, 2)	1	0	0	0	1	1

The xth row of this matrix identifies the subgroup, $C(x)$, of elements which commute with x; i.e., the centralizer of x. Here's the way to parse the commutativity count for S_3.

$$18 = 6 + 2 + 2 + 2 + 3 + 3 = 1 \cdot 6 + 3 \cdot 2 + 2 \cdot 3 = 6 + 6 + 6 = 3 \cdot 6$$

The elementary group theory at work in this count is:

- conjugate elements have centralizers of the same order

$$y = g^{-1}xg \text{ implies } C(y) = g^{-1}C(x)g,$$

- the order of a conjugacy class is the index of the centralizer of any element in the class

$$|x^G| = |\{g^{-1}xg | g \in G\}| = [G : C(x)],$$

- Lagrange's theorem

$$|G| = [G : H] \cdot |H|.$$

An abstraction of this example, originally due to Erdös and Turán [4], answers our second question.

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

where $\{x_1, x_2, \dots, x_k\}$ is a complete set of conjugacy class representatives of G.

Thus, an informative answer to our first question is

$$Pr_2(G) = \frac{k}{|G|}.$$

It comes as no surprise that G is abelian precisely when $Pr_2(G) = 1$. But what may surprise you is that if G is not abelian, then

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

where p_s is the smallest prime divisor of the order of G. The essence of these bounds is that the index of the center of a nonabelian group is at least p_s^2; i.e., $|G:Z] \ge p_s^2$.

The $5/8$ bound, which is assumed by the dihedral and quaternion groups of order eight, has been around for a long time. Yet, it doesn't seem to be commonly known—so be sure to tell your students about it. We do not know with whom it originated. Some say Max Zorn. But, many years ago, during a conversation with one of the authors (Sherman), Zorn declined credit for the bound. To the best of our knowledge the bound first appeared in print in 1973 when Gustafson [7] showed that an analogous bound holds for compact nonabelian groups. Gallian's recent textbook ([6, pages 329, 330]) also includes a discussion of the bound. Both upper and lower bounds on $Pr_2(G)$ for various classes of groups have been obtained ([1], [4], [5], [7], [10], [13]). And, since commutativity can be defined in terms of conjugation, analogous results have been pursued for various group actions ([11], [13], [15]).

Commutativity is a special case of rewriteability. Let $S \subseteq S_n - \{\text{id}\}$; i.e., S is a set of nontrivial permutations of $\{1, 2, \dots n\}$. An n-tuple $(x_1, x_2, \dots, x_n)$ 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

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

where

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

Those groups for which $Pr_n(G; S_n - \{\text{id}\}) = 1$ 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 three statements are equivalent.

i) *G is* 3-*rewriteable*; *i.e.*, $xyz \in \{yxz, zyx, xzy, zxy, yzx\}$ *for all* $x, y, z \in G$.
ii) *The order of the derived subgroup of* $G, G' = \langle x^{-1}y^{-1}xy | x, y \in G \rangle$ *is one or two.*
iii) *The order of the centralizer of each element of G is* $|G|$ *or* $|G|/2$.

The equivalence of ii) and iii) revolves around the relationship between commutators (elements of the form $x^{-1}y^{-1}xy$) and conjugates: $x^{-1}y^{-1}xy = g$ if, and only if $y^{-1}xy = xg$. The equivalence of i) with ii) or iii) is case-driven. For example, an application of the definition of 3-rewriteability to the product xyx^2 places x^2 in the center of the group. This means the centralizer of x is a "large" normal subgroup. In view of iii) and our discussion prior to (2), we may add the following statement to the list.

iv) *The order of each conjugacy class of G is one or two.*

Each of ii), iii) and iv) suggests a connection between 3-rewriteability and the probability of two elements commuting. In particular, the size of a group's derived subgroup is a classic measure of the degree of commutativity the group enjoys. If G' is small, then "most" commutators are trivial; i.e., it is "likely" that $xy = yx$.

Let's formalize this connection. 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 $|G'| \leq 2$. We have the following theorem.

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

It's interesting to formulate this theorem in terms conjugacy classes

Each conjugacy class has order one or two if, and only if, the average conjugacy class order is less than two.

and in terms of conditional probability.

The probability of x and y commuting, given y, is at least $1/2$ *for each y, if and only if* $Pr_2(G) > 1/2$.

AN ELEMENTARY PROOF. An elementary proof that *if* $Pr_2(G) > 1/2$, *then G is 3-rewriteable* follows. Think of "3-rewriteable" as a generic label for your favorite from among statements i)–iv) above. We will assume that G is not 3-rewriteable and prove that $Pr_2(G) \leq 1/2$.

The proof and subsequent discussion hinge on relationships among the orders of three subsets of G:

$$X = \{x \in G \mid [G : C(x)] \geq 3\},$$
$$Y = \{x \in G \mid [G : C(x)] = 2\},$$
$$Z = \{x \in G \mid [G : C(x)] = 1\}; \text{ i.e., the center of } G.$$

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 $C(y) \cap (G - C(x)) \neq \varnothing$, 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 $y^{g_i} \to xy^{g_i}$ 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: Observe that

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

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.

It isn't necessary to invoke the centralizer characterization of 3-rewriteability to complete the proof of Lemma 3. If $[G : Z] = 4$, then $G/Z \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$. Thus $G = Z \cup xZ \cup yZ \cup xyZ$. The only triple products from G whose 3-rewriteability we might question have form $(xz_1)(yz_2)(xyz_3)$ or $(xz_1)(xyz_2)(yz_3)$. But, notice that $(xz_1)(yz_2)(xyz_3) = (xyz_3)(xz_1)(yz_2)$ and that $(xz_1)(xyz_2)(yz_3) = (yz_3)(xz_1)(xyz_2)$ because $x^2 \in Z$. This proof makes Lemma 3, which is an analogue of the fact that $[G : Z] \geq 4$ for nonabelian G, an appealing student exercise.

Now we can weave that elementary proof we promised. Note that $X \neq \varnothing$ since G is not 3-rewriteable. Choose $g \in X$ and set $n = [G : C(g)]$. Then $Z \cup Zg \subseteq C(g)$ and $(Z \cup Zg) \cap Y = \varnothing$. Thus $|C(g) \cap Y| \leq |G|/n - 2|Z|$ and so $|(G - C(g)) \cap Y| \geq |Y| - |G|/n + 2 \cdot |Z|$. If $x \in (G - C(g)) \cap Y$, then $[G : C(x)] = 2$ and $C(g) \cap (G - C(x)) \neq \varnothing$ implies, by Lemma 1, that $[G : C(xg)] \geq [G : C(g)] \geq 3$.

Therefore $(G - C(g)) \cap Y \subseteq X$; in fact $(G - C(g)) \cap Y \subseteq X - Zg$ as $Zg \subseteq X \cap C(g)$. Thus $|X| - |Z| = |X - Zg| \geq |(G - C(g)) \cap Y| \geq |Y| - |G|/n + 2 \cdot |Z|$; i.e.,

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

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, $G/Z \cong S_3$.* Our opening example suggests the involvement of S_3. That $Pr_2(G) = 1/2$ implies $G/Z \cong S_3$ is a straight forward application of Lemma 3 and the Corollary. The converse follows since $|X| = 3 \cdot |Z|$ and $|Y| = 2 \cdot |Z|$ for groups satisfying $G/Z \cong S_3$.

ii) *There exists a sequence, $\{G_n\}$, of 3-rewriteable groups such that $Pr_2(G_n) \downarrow 1/2$.* But where? A result of Ito **[9]** says that groups in which each conjugacy class is of order one or p, for a fixed prime p, must be the direct product of a p-group (a group whose order is a power of p) with this property and an abelian group. Thus, if G is 3-rewriteable we may write $G \cong T \times A$, where T is a 3-rewriteable 2-group and A is abelian. Conjugacy classes in direct products are direct products of conjugacy classes, so

$$Pr_2(G) = Pr_2(T \times A) = Pr_2(T) \cdot Pr_2(A) = Pr_2(T).$$

Net result: we may restrict our attention to 2-groups.

The quaternion group of order eight, mentioned in conjunction with the $5/8$ bound, is worth a look:

$$Q = \langle x, y, z | x^2 = y^2 = z^2 = x^{-1}y^{-1}xy = x^{-1}z^{-1}xz = e, y^{-1}z^{-1}yz = x \rangle.$$

The relevant facts are;

$$\begin{gathered} |Q| = 8 = 2^3, \\ Z = Q' = \{e, x\}, \\ k = 5 = |Z| + (|G| - |Z|)/2 = (|G| + |Z|)/2, \\ Pr_2(Q) = 5/8 = 1/2 + |Z|/(2 \cdot |G|). \end{gathered}$$

We generalize by taking G_n to be (an extra-special 2-group **[12]**) generated by $x_1, x_2, \ldots, x_{2n+1}$ subject to the relations

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

$$x_i^{-1}x_j^{-1}x_ix_j = \begin{cases} x_1 & \text{for } i \text{ even and } j = i+1, \\ e & \text{otherwise.} \end{cases}$$

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 prompts a conjecture.

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

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

It follows from (3) and Lemma 4 that

$$
\begin{aligned}
Pr_n(G;S) &= |Rw_n(G;S)|/|G|^n \leq |S| \cdot k/|G| = |S| \cdot Pr_2(G) \\
&\leq |S| \cdot \left(p_s^2 + p_s - 1\right)/p_s^3. \qquad (7)
\end{aligned}
$$

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 $Pr_n(G;S)$. Random sampling (using CAYLEY [**8**]) of the "S-rewriteability hypercube" of various groups suggests such bounds exist independent of p_s.

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

Specifically, if $p_s \geq 7$, then $Pr_3(G; S_3 - \{\text{id}\}) \leq 275/343$. However, 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 $Pr_2(G) \leq Pr_2(A_5)$ [**5**] and $Pr_2(A_5) = 1/12$. 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.

ACKNOWLEDGMENT. The authors thank the referees for their suggestions.

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. Erdös and P. Turán, 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. J. A. Gallian, *Contemporary Abstract Algebra*, 2nd edition, D. C. Heath, 1990.
7. W. H. Gustafson, What is the probability that two group elements commute?, *Amer. Math. Monthly*, 80 (1973) 1031–1034.
8. D. F. Holt, The CAYLEY group theory system, *Notices of the American Mathematical Society*, 35 (1988). No. 8, 1135–1140.
9. N. Itô, On finite groups with given conjugate types, *Nagita Math. J.*, 6 (1953), 17–28.
10. E. Landau, Klassenzahl binarer quadratischer Formen von negativer Discriminante, *Math. Annalen*, 56 (1902) 671–676.
11. T. J. Laffey and D. MacHale, Automorphism orbits of finite groups, *J. Austral. Math. Soc.* (*Series A*), 40 (1986) 253–260.
12. D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, 1982.
13. G. J. Sherman, A probabilistic estimate of invariance for groups, *Amer. Math. Monthly 85* (1978) 361–363.
14. ______, A lower bound for the number of conjugacy classes in a finite nilpotent group, *Pacific J. Math.*, 79 (1979) 253–254.
15. G. J. Sherman, T. J. Tucker and M. E. Walker, How Hamiltonian can a finite group be? *Archives Math.*, (*Basel*), to appear.

University of Michigan
Ann Arbor, MI 48109

Rose-Hulman Institute of Technology
Terre Haute, IN 47803

New Mexico State University
Las Cruces, NM 88003

The beginning of wisdom is the definition of terms.

—*Socrates* (*470?–399 B.C.*)