

# Notes From Talk on the Paper “Rewriteability in Finite Groups”

Lindsay Orlando

August 3rd and 4th, 2009

## 1 Preliminaries

- We are considering finite groups  $G$  so assume  $G$  is finite.
- The center of  $G$  is  $Z = \{x \in G : xy = yx \text{ for all } y \in G\}$ .
- For  $x \in G$ , the centralizer of  $x$  in  $G$  is  $C(x) = \{y \in G : xy = yx\}$ .
- For  $x \in G$ , the conjugacy class of  $x$  is  $x^G = \{gxg^{-1} : g \in G\}$ . The conjugacy class of  $x$  in  $G$  is the orbit of  $x$  in  $G$  when  $G$  acts on itself by conjugation, so the conjugacy classes of  $G$  partition  $G$ . Also note that  $x \in Z$  iff  $|x^G| = 1$ .
- For a subgroup  $H$  of a finite group  $G$ ,  $|G| = [G : H] \cdot |H|$ . This is Lagrange’s Theorem.
- For  $x \in G$ ,  $|x^G| = [G : C(x)]$ .
- For a group  $G$ , if  $G/Z$  is cyclic then  $G$  is abelian. This is the  $G/Z$  Theorem.
- The definition of an  $n$ –rewriteable group, according to the paper:

Let  $S \subseteq S_n - \{id\}$ . An  $n$ –tuple  $(x_1, \dots, x_n)$  of elements of  $G$  is  $S$ –rewriteable if  $x_1 \cdots x_n = x_{\sigma(1)} \cdots x_{\sigma(n)}$  for some  $\sigma \in S$ . We have

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

where  $Rw_n(G; S) = \{(x_1, \dots, x_n) \in G^n : (x_1, \dots, x_n) \text{ is } S\text{–rewriteable}\}$ . Those groups for which  $Pr_n(G; S_n - \{id\}) = 1$  will be referred to as  $n$ –rewriteable groups.

## 2 Introduction

Paper: Rewriteability in Finite Groups

Authors: J. L. Leavitt, G. J. Sherman, M. E. Walker

Source: *The American Mathematical Monthly*, Vol. 99, No. 5 (May, 1992), pp. 446-452

According to the paper, rewriteability has its origins in automata theory. First we will figure out the probability of two elements commuting in  $G$ . Then we will show a connection between 3–rewriteability and the probability that two elements in  $G$  commute. The main result of the paper is:  $G$  is 3–rewriteable if and only if  $Pr_2(G) > \frac{1}{2}$ .

## 3 What is the probability that two elements in $G$ commute?

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

We will compute the top of this fraction, which is based on work by Erdos and Turan.

$$\begin{aligned}
|\{(x, y) \in G^2 : xy = yx\}| &= \sum_{x \in G} |C(x)| \\
&= \sum_{i=1}^k |x_i^G| \cdot |C(x_i)| \text{ where } \{x_1, \dots, x_k\} \text{ is a complete set of conjugacy class reps} \\
&= \sum_{i=1}^k [G : C(x_i)] \cdot |C(x_i)| \\
&= \sum_{i=1}^k |G| \\
&= k \cdot |G|
\end{aligned}$$

So  $Pr_2(G) = \frac{k \cdot |G|}{|G|^2} = \frac{k}{|G|}$ .

**Example** The group  $S_3$  has three cycle types, i.e. three conjugacy classes. So  $Pr_2(S_3) = \frac{3}{6} = \frac{1}{2}$ .

**Example** Consider  $D_4$ , the dihedral group of eight elements. The conjugacy classes of  $D_4$  are  $\{1_{D_4}\}, \{R_{180}\}, \{R_{90}, R_{270}\}, \{H, V\}, \{D, D'\}$ . So  $Pr_2(D_4) = \frac{5}{8}$ .

**Example** For an abelian group  $G$ ,  $Pr_2(G) = 1$ .

For a nonabelian group  $G$ , there exists an upper bound on  $Pr_2(G)$ . Specifically,  $Pr_2(G) \leq \frac{5}{8}$ . The following explanation can be found in J. Gallian's algebra book: In this nonabelian group  $G$  we want to maximize the number of conjugacy classes. So the center must be as large as possible (since the conjugacy class of each element in  $Z$  is the set containing that element) and in the extreme case, the rest of the elements of  $G$  are distributed into conjugacy classes each of length two. Note that  $|G/Z| \geq 4$  (or else  $G$  would be abelian by the  $G/Z$  Theorem). Thus  $|Z| \leq \frac{|G|}{4}$  so take  $|Z| = \frac{|G|}{4}$  and the other  $\frac{3}{4} \cdot |G|$  elements are distributed into conjugacy classes of length two. So  $k \leq \frac{|G|}{4} + \frac{3 \cdot |G|}{2} = \frac{5}{8} \cdot |G|$ . Thus  $Pr_2(G) = \frac{k}{|G|} \leq \frac{\frac{5}{8} \cdot |G|}{|G|} = \frac{5}{8}$ .

The history of this bound is not very well known (read from paper). Some interesting results from Gustafson, who expanded work on the bound to a compact group, are as follows:

Gustafson

- For a compact nonabelian group,  $Pr_2(G) \leq \frac{5}{8}$ .
- For a nonabelian  $p$ -group,  $Pr_2(G) \leq \frac{p^2+p-1}{p^3}$ .
- For a simple, nonabelian group,  $Pr_2(G) \leq \frac{1}{12}$  and equality holds for  $A_5$ .

**Example** Following are various values of  $Pr_2(G)$  for various nonabelian  $G$ , computed using GAP, where  $Dn$  is the dihedral group of  $2n$  elements,  $Sn$  is the symmetric group on  $n$  elements, and  $An$  is the alternating group on  $n$  elements. (These are not in the paper, just something I decided to show.)

$G$	$Pr_2(G)$
$D3$	.5
$D4$	.625
$D5$	.4
$D6$	.5
$S3$	.5
$A3$	1
$S4$	.208
$A4$	.333
$S5$	.058
$A5$	.083
$S6$	.015
$A6$	.019

## 4 Finding a connection between $Pr_2(G)$ and a 3–rewriteable group

The following results are cited in the paper from the underlined authors:

Curzio, Longobardo, Maj

**The following are equivalent:**

- 4.1  $G$  is 3–rewriteable, i.e. for all  $x, y, z \in G$ ,  $xyz \in \{xzy, yxz, yzx, zxy, zyx\}$ .
- 4.2 The order of the derived subgroup of  $G$ ,  $G' = \langle x^{-1}y^{-1}xy : x, y \in G \rangle$ , is one or two.
- 4.3 For each  $x \in G$ , the order of  $C(x)$  is  $|G|$  or  $\frac{|G|}{2}$ .

Note that if  $|G'|$  is one, then  $G$  is abelian, and if  $|G'|$  is two, then it is at least likely that a number of elements of  $G$  commute. Thus the authors see a connection between  $Pr_2(G)$  and a 3–rewriteable group. The authors also provide a fourth statement based on the following: Let  $x \in G$ . Then either  $|C(x)|$  is  $|G|$  or  $|C(x)|$  is  $\frac{|G|}{2}$ . If  $|C(x)| = |G|$  then  $|x^G| = [G : C(x)] = \frac{|G|}{|C(x)|} = 1$ . Similarly, if  $|C(x)| = \frac{|G|}{2}$ , then  $|x^G| = 2$ . Thus they add the following statement, equivalent to the three results above:

**Equivalent Statement:** For each  $x \in G$ ,  $|x^G| = 1$  or  $|x^G| = 2$ .

## 5 Main result

The authors of the paper establish this main result:

**Theorem 5.1.**  $G$  is 3–rewriteable if and only if  $Pr_2(G) > \frac{1}{2}$ .

To establish the forward direction, we note that in a 3–rewriteable group  $G$ , the average order of a conjugacy class is less than two, i.e.  $\frac{|G|}{k} < 2$ . Thus  $Pr_2(G) = \frac{k}{|G|} > \frac{1}{2}$ . To establish the converse, the authors appeal to character theory, which will not be presented here. The authors develop an “elementary” proof to establish the converse as well and we shall need three lemmas the authors provide in order to prove the converse.

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

The proof will not be shown. If we break down what this lemma says, we see that it makes sense. What  $[G : C(xy)] \geq [G : C(y)]$  means is  $\frac{|G|}{|C(xy)|} \geq \frac{|G|}{|C(y)|}$  and so  $|C(xy)| \leq |C(y)|$ , and this makes sense given the hypotheses in the statement of the lemma.

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

Note that if at least  $3 \cdot |Z|$  elements of  $G$  have centralizers of index at least 3, then we are saying that  $|X| \geq 3 \cdot |Z|$ . Also note that  $|X| + |Y| + |Z| = |G|$  and that  $k \leq \frac{|X|}{3} + \frac{|Y|}{2} + |Z|$ . Thus the authors have

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

Therefore  $Pr_2(G) = \frac{|Rw_2(G)|}{|G|^2} \leq \frac{\frac{|G|^2}{2}}{|G|^2} = \frac{1}{2}$ .

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

The authors prove this by contraposition. If  $[G : Z]$  is 1,2,3, or 5, then  $G/Z$  is cyclic (since  $|G/Z|$  is one or of prime order) and so  $G$  is abelian and hence 3–rewriteable. So consider the case when  $[G : Z] = 4$ . Let  $x \in G$ . If  $x \in Z$ , then  $|C(x)| = |G|$ . If  $x \in G - Z$  then  $Z \subset C(x) \subset G$  (proper containments) and  $[G : C(x)] \neq 1$  and  $[G : C(x)] \neq 4$ . Thus  $[G : C(x)] = 2$  and so  $|C(x)| = \frac{|G|}{2}$ . Thus by the second statement from Curzio, Longobardo, and Maj,  $G$  is 3–rewriteable.

**The Proof of the Converse** The proof that  $Pr_2(G) > \frac{1}{2}$  implies  $G$  is 3–rewriteable will not be shown in detail. What the authors do in their proof (by contraposition) is show through a series of set containments and use of the lemmas that  $|X| \geq |Y| - \frac{|G|}{n} + 3 \cdot |Z|$ , where  $n = [G : C(g)]$  and  $g$  is an element chosen in  $X$ . If  $|Y| \geq \frac{|G|}{3}$  then  $|X| \geq \frac{|G|}{3} - \frac{|G|}{n} + 3 \cdot |Z| = |G| \cdot (\frac{1}{3} - \frac{1}{n}) + 3 \cdot |Z|$  and  $n \geq 3$  so by Lemma 2,  $Pr_2(G) \leq \frac{1}{2}$ . If  $|Y| < \frac{|G|}{3}$  then we have

$$\begin{aligned}
|G| &= |X| + |Y| + |Z| \\
&\leq |X| + |Y| + \frac{|G|}{6} \text{ since } G \text{ not 3–rewriteable, } \frac{|G|}{|Z|} \geq 6 \\
&< |X| + \frac{|G|}{3} + \frac{|G|}{6}.
\end{aligned}$$

Thus  $|G| - \frac{|G|}{3} - \frac{|G|}{6} < |X|$  and hence  $|X| > \frac{|G|}{2}$ . Since  $|Z| \leq \frac{|G|}{6}$ ,  $3 \cdot |Z| \leq \frac{|G|}{2}$  and so  $|X| > 3 \cdot |Z|$ . So by Lemma 2,  $Pr_2(G) \leq \frac{1}{2}$ .

## 6 Sharpness of the $\frac{1}{2}$ bound for 3–rewriteability

The authors show sharpness of the  $\frac{1}{2}$  bound in two senses.

**6.1**  $Pr_2(G) = \frac{1}{2}$  if and only if  $G/Z \cong S_3$ .

**6.2** There exists a sequence  $\{G_n\}$  of 3–rewriteable groups such that  $Pr_2(G_n) \rightarrow \frac{1}{2}$  (from above).

To find this sequence of 3–rewriteable groups, the authors appeal to a result by Ito, which is as follows:

Ito

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 with this property and an abelian group.

So take  $p = 2$  and we have that groups in which each conjugacy class is of order one or two (i.e. a 3–rewriteable group) must be the direct product of a 2–group with this property and an abelian group. So for a 3–rewriteable group  $G$  we have

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

Thus the authors restrict their attention to 2–groups.

**Example** The authors provide this sequence of extra special 2–groups. Note that a finite  $p$ –group is called extra special if  $G' = Z$  and  $|G'| = |Z| = p$ . Also note in this sequence that  $G_1$  is the quaternion group.

$$G_n = \left\langle x_1, \dots, x_{2n+1} \mid x_i^2 = e \text{ for all } 1 \leq i \leq 2n+1, x_i^{-1} x_j^{-1} x_i x_j = \begin{cases} x_1, & \text{for } i \text{ even and } j = i+1 \\ e, & \text{otherwise} \end{cases} \right\rangle$$

The following facts regarding  $G_n$  are as follows:  $|G_n| = 2^{2n+1}$ ,  $Z = G'_n = \{e, x_1\}$ , and  $k = |Z| + \frac{|G| - |Z|}{2}$ . Thus  $Pr_2(G_n) = \frac{k}{|G_n|} = \frac{|Z| + \frac{|G_n| - |Z|}{2}}{2^{2n+1}} = \frac{|G_n| + |Z|}{2 \cdot 2^{2n+1}} = \frac{2^{2n+1} + 2}{2 \cdot 2^{2n+1}} = \frac{1}{2} + \frac{1}{2^{2n+1}}$ . So we have  $Pr_2(G_0) = 1$ ,  $Pr_2(G_1) = \frac{5}{8}$ ,  $Pr_2(G_2) = \frac{17}{32}$ , etc. We see that as  $n \rightarrow \infty$ ,  $Pr_2(G) \rightarrow \frac{1}{2}$  (from above).

## 7 Other Results and Conjecture

The authors give us Lemma 4:

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

The proof (by induction) will not be provided here. What we do have then is that

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

where  $p_s$  is the smallest prime divisor of the order of  $G$ . Note that  $Pr_2(G) \leq \frac{p_s^2+p_s-1}{p_s^3}$  is an earlier result in the paper. The authors note here that since  $\frac{p_s^2+p_s-1}{p_s^3} \rightarrow 0$  (from above) as  $p_s \rightarrow \infty$ , then for  $|S|$  fixed and  $p_s$  sufficiently large, a bound (similar to the  $\frac{5}{8}$  bound for 2–rewriteability) exists for  $Pr_n(G; S)$ . The authors provide the following two conjectures:

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

**Example** If  $p_s \geq 7$ ,  $Pr_3(G; S_3 - \{id\}) \leq |S| \cdot \frac{p_s^2+p_s-1}{p_s^3} = \frac{275}{343}$ . Using software called CAYLEY, the authors conjecture that  $Pr_3(G; S_3 - \{id\}) \leq \frac{17}{18}$ .

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

The authors note that if the conjecture is true then the  $\frac{17}{18}$  bound is sharp since  $Pr_3(S_3; S_3 - \{id\}) = \frac{17}{18}$ .

The authors cite the following result from Dixon:

Dixon

If  $G$  is a non-abelian finite simple group then  $Pr_2(G) \leq Pr_2(A_5)$ .

Thus, as  $Pr_2(A_5) = \frac{1}{12}$ , the authors conclude that for a non-abelian finite simple group,  $Pr_3(G; S_3 - \{id\}) \leq |S| \cdot Pr_2(G) = \frac{5}{12}$ . The authors' sampling with CAYLEY suggests the bound may be  $\frac{27}{100}$  since  $Pr_3(A_5, S_3 - \{id\})$  is  $\frac{27}{100}$ .

## 8 Related Results

A MathSciNet search of “rewritability” shows some interesting results that both confirm the conjectures in this paper and show a small sampling of what else has been researched in this area:

- (Ellenberg, Sherman, Smithline, Sugar, Wepsic, 1993, The combinatorics of rewritability in finite groups) This is more undergraduate research with Sherman, the year after Walker's and Leavitt's was done. Exciting result: The  $\frac{17}{18}$  bound is sharp, as is the  $\frac{27}{100}$  bound!
- (Bell, 1994, Rewritability in semigroups and rings) Result: Let  $n \geq 2$ . Let  $T$  be a semigroup or ring with the property that for each  $x_1, \dots, x_n \in T$ , there exists  $\sigma \in S_n - \{id\}$  such that  $x_1 \cdots x_n = x_{\sigma(1)} \cdots x_{\sigma(n)}$ . Under suitable restrictions on  $T$  and  $\sigma$ , we show that  $T$  must be finite or commutative.
- (Abdollahi, Mohammadi Hassanabadi, Taeri, 1999, A property equivalent to  $n$ -permutability for infinite groups) Result: Using infinite subsets  $X_n$  of  $G$ , these authors find a property equivalent to  $n$ -permutability (same definition as  $n$ –rewriteability in the presented paper) for infinite groups.