2-1992

Rewriteability, Commutators, and Fundamental n-Rewritings

Lawren Smithline
Harvard University

Advisors:
Gary Sherman

MSTR 92-02

REWRITEABILITY, COMMUTATORS, AND FUNDAMENTAL n-REWRITINGS

Lawren Smithline

MS TR 92-02

February 1992

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

FAX(812) 877-3198

Phone: (812) 877-8391

Rewritability, Commutators, and Fundamental n-Rewritings

Lawren Smithline*
Harvard University

Let G be a finite group and $X = (x_1, x_2, \ldots, x_n) \in G^n$. (We consider here only finite groups.) Let the elements of the symmetric group on n symbols, S_n, act on X by permuting the coordinates. That is, $\sigma \cdot (x_1, x_2, \ldots, x_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(n)})$. We introduce the following definitions to make this notion more precise.

Definition 1 $\Pi(X) = \prod_{i=1}^n x_i$, *as a formal product.* $\Pi_G(X) = \prod_{i=1}^n x_i$ *as a product in* G.

Definition 2 *We say that* $\sigma \in S_n$ *rewrites* $X \in G^n$ *if* $\Pi_G(X) = \Pi_G(\sigma \cdot X)$.

*Work supported by NSF Grant DMS-910059.

Definition 3 *The probability that $\sigma \in S_n$ rewrites an element of G^n is denoted by $\mathcal{P}_\sigma(G)$; i.e.*

$$\mathcal{P}_\sigma(G) = \frac{|\{X | X \in G^n, \Pi_G(X) = \Pi_G(\sigma \cdot X)\}|}{|G|^n}.$$

Our main theorem concerns the relationship of $\mathcal{P}_\sigma(G)$ to the commutator subgroup G' (Theorem 1). We also establish

i) the maximum of $\mathcal{P}_\sigma(G)$ over non-Abelian groups G (Theorem 2);

ii) the number of τ such that $\mathcal{P}_\tau(G) = \mathcal{P}_\sigma(G)$ (Section 3);

iii) the behavior of $\lim_{n\to\infty} \mathcal{P}_{\sigma_n}(G)$ (Section 4);

iv) a sufficient condition on groups G and H so that $\mathcal{P}_\sigma(G) = \mathcal{P}_\sigma(H)$ (Section 5).

1 $\mathcal{P}_\sigma(G)$ and G'

Clearly, $\mathcal{P}_e(G) = 1$ for all n and G. For $n = 2$ and $\sigma = (1\ 2)$, $\mathcal{P}_\sigma(G)$ may be interpreted as the probability that two group elements commute; i.e.

$$\mathcal{P}_{(1\ 2)}(G) = \frac{|\{(x, y) | xy = yx, x, y \in G\}|}{|G|^2}.$$

It is well known (see [3]) that $\mathcal{P}_{(1\ 2)}(G) = \frac{k(G)}{|G|}$, where $k(G)$ is the number of conjugacy classes in G. It is not so well known that $k(G)$ determines $\mathcal{P}_\sigma(G)$ for $\sigma \in \mathrm{S}_3$.

Proposition 1 [2] *Let $\sigma \in S_3$. Then* $\mathcal{P}_\sigma(G) = \begin{cases} 1 & \text{if } \sigma = e; \\ \mathcal{P}_{(1\ 2)}(G) & \text{otherwise.} \end{cases}$

Proof. Let $X = (x, y, z) \in G^3$. If σ is one of $(1\ 2), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$ then $\Pi(\sigma \cdot X)$ simply exchanges adjacent letters or blocks of letters in $\Pi(X)$; i.e. $\mathcal{P}_\sigma(G) = \mathcal{P}_{(1\ 2)}(G)$ in each of these cases. For $\sigma = (1\ 3)$, $\Pi_G(\sigma \cdot X) = zyx$. We see that σ rewrites X when $xyzy = zyxy$, or exactly when xy commutes with zy. The products xy and zy can be chosen independently, because for any choice of y, we can still choose xy arbitrarily by choosing x, and similarly for zy. So $\mathcal{P}_\sigma(G) = \mathcal{P}_{(1\ 2)}(G)$. ♠

We include the proof of Proposition 1 to motivate the next definition. Notice that $\Pi_G((1\ 3) \cdot X) = \Pi_G(X)$ was the only case which required any trick. This is because the permutation $(1\ 3)$ is also the only element of S_3 whose action cannot be realized in S_2.

Definition 4 *We say $\sigma \in S_m$ is a* fundamental n-rewriting *if n is minimal such that for all $X \in G^m$, there exist $Y \in G^n$ and $\tau \in S_n$ such that $\Pi(X) = \Pi(Y)$ and $\Pi(\sigma \cdot X) = \Pi(\tau \cdot Y)$.*

The value n in the above definition is the *scrambling number* of σ. We will often be interested in a related quantity:

Definition 5 *For $\sigma \in S_m$, $\|\sigma\| = \left\lfloor \frac{n}{2} \right\rfloor$, where n is the scrambling number of σ.*

For example, $wxyz = zxyw$ expresses the fundamental 3-rewriting (1 4), since we really have a rewriting of (w, xy, z) and for no $Y \in G^2$, $\tau \in \mathrm{S}_2$ does $\Pi(Y) = wxyz$ and $\Pi(\tau \cdot Y) = zxyw$.

We have seen that when $\|\sigma\| = 0$, $\mathcal{P}_\sigma(G)$ is 1, and when $\|\sigma\| = 1$, $\mathcal{P}_\sigma(G)$ is $\mathcal{P}_{(1\ 2)}(G)$. We generalize the construction of $\mathcal{P}_{(1\ 2)}(G)$ before proving the main theorem.

Definition 6 *$\kappa_h(G)$ is the probability h commutators multiply to give e; i.e.*

$$\kappa_h(G) = \frac{\left|\{(a_1, b_1, a_2, b_2, \ldots, a_h, b_h) | \prod_{i=1}^{h} [a_i, b_i] = e, a_i, b_i \in G \text{ for } 1 \leq i \leq h\}\right|}{|G^{2h}|}.$$

When the choice of the parameter G is clear, it is often dropped. Notice that $\kappa_1 = \mathcal{P}_{(1\ 2)}(G)$.

In the following theorem and afterwards, when $x, y \in G$, x^y represents $y^{-1}xy$.

Theorem 1 (Main Theorem) *Let $\sigma \in S_m$. Then $\mathcal{P}_\sigma(G) = \kappa_{\|\sigma\|}(G)$.*

We precede the proof with a worked example. Let $G = \mathrm{S}_3$. We calculate $\mathcal{P}_\sigma(G)$ for $\sigma = (1\ 3\ 6\ 5)$, a four cycle in S_6. That is, what is the probability that $uvwxyz = yvuxzw$? First we observe that σ is a fundamental 6-rewriting, so $\|\sigma\| = 3$. Next, we construct three commutators which, when multiplied on the right of $yvuxzw$ give $uvwxyz$:

$$[ux, yv]^{zw} \quad \text{from} \quad yvuxzw[ux, yv]^{zw} = uxyvzw,$$

$$[vzw, xy] \quad \text{from} \quad uxyvzw[vzw, xy] = uvzwxy,$$

$$[wxy, z] \quad \text{from} \quad uvzwxy[wxy, z] = uvwxyz.$$

We can see that $(u, v, w, x, y, z) \mapsto (ux^{zw}, yv^{zw}, vzw, xy, wxy, z)$ is a 1-1 correspondence in G^6 by first choosing z and wxy, then w, which fixes xy, then v, then y and u. So $\mathcal{P}_\sigma(G) = \kappa_3$. The derived group of S_3 is $\mathbf{Z}_3$, and $\kappa_1 = \frac{1}{2}$. The other commutators occur with probability $\frac{1}{4}$. In order for three commutators to multiply to give the identity, we must have either three

copies of the same commutator, or one of each commutator. Hence we make the following calculation:

$$\kappa_3 = \left(\frac{1}{2}\right)^3 + 2\left(\frac{1}{4}\right)^3 + 6\left(\frac{1}{2}\right)\left(\frac{1}{4}\right)^2 = \frac{11}{32}.$$

Proof of theorem. The case $\|\sigma\| = 0$ is trivial. For $\|\sigma\| > 0$, we will use commutators to "untwist" $\sigma \cdot X$, for each $X \in G^m$ as in the preceding example. Let $X = (x_1, x_2, \ldots, x_m)$ and recall that $\sigma \cdot X = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(m)})$. For convenience, we adopt $\overline{\sigma} = \sigma^{-1}$. Let q be minimal so that $\overline{\sigma}(q) \neq q$. Choose i so that $\overline{\sigma}(i) = q$. There are two cases.

First, suppose there are j, k with $q \leq k < i < j \leq m$ such that $r = \overline{\sigma}(j) - 1 = \overline{\sigma}(k)$. Let

$$A = \prod_{f=q}^{k} x_{\overline{\sigma}(f)}, \quad B = \prod_{f=k+1}^{i-1} x_{\overline{\sigma}(f)}, \quad C = \prod_{f=i}^{j-1} x_{\overline{\sigma}(f)}, \quad D = \prod_{f=j}^{m} x_{\overline{\sigma}(f)}.$$

If $i = k + 1$, we define $B = e$. Then $ABCD[BC, BA]^D = CBAD =$

$$x_{\overline{\sigma}(i)} \cdots x_{\overline{\sigma}(j-1)} \cdot x_{\overline{\sigma}(k+1)} \cdots x_{\overline{\sigma}(i-1)} \cdot x_{\overline{\sigma}(q)} \cdots x_{\overline{\sigma}(k)} \cdot x_{\overline{\sigma}(j)} \cdots x_{\overline{\sigma}(m)}.$$

For some $\gamma \in S_m$, with $\|\gamma\| = \|\sigma\| - 1$, $CBAD = \Pi(\gamma \cdot X)$, because

i) no blocks of consecutive x's are split;

ii) x_q moves to its home position, either as x_1 or next to x_{q-1}; and

iii) x_r moves next to x_{r+1}.

Now suppose there are no such j, k. Then for $k < i$, $\overline{\sigma}(k) < m$ implies there is a $k' < i$ such that $\overline{\sigma}(k') = \overline{\sigma}(k) + 1$. So for some $k < i$, $\overline{\sigma}(k) = m$. Proceed as in the first case, with $j = m + 1$ and $D = e$; x_m always moves "next to something" if we imagine an extra coordinate in the m-tuple.

So by induction, we have that σ rewrites X if, and only if, $\Pi_G(X) = \Pi_G(X) \cdot \prod_{i=1}^{\|\sigma\|}[a_i, b_i]$, where A_i, B_i, C_i, D_i are the ith values constructed for A, B, C, D, $a_i = (B_i C_i)^{D_i}$, and $b_i = (B_i A_i)^{D_i}$. We need to show a $|G|^{m-2\|\sigma\|}$ to 1 correspondence between X and $(a_1, b_1, a_2, b_2 \ldots, a_{\|\sigma\|}, b_{\|\sigma\|})$.

Fix the a_i's and b_i's for $i > 1$. We claim that the choices of $a = a_1$ and $b = b_1$ are still free. The commutator $[a, b]$ moves x_{q_1} to its home position at the front of X, so no succeeding commutator is in terms of x_{q_1}. Now the argument bifurcates as it did for the construction of the a_i's and b_i's.

Suppose $[a, b]$ moves x_r next to x_{r+1}. Then in all succeeding commutators, x_r and x_{r+1} appear only together, so knowing the values of all of the other a_i's and b_i's can only determine the product $x_r x_{r+1}$. Since $B_1 {A_1}^{D_1}$ contains a single factor of x_r alone, the choice of b is free. Since $(B_1 C_1)^{D_1}$ contains a single factor of x_{q_1}, the choice of a is free.

The other case is that $[a, b]$ moves x_m to the end of the m-tuple. Then all of the D_i's have x_m as their last factor. Hence, knowing the other a_i's and b_i's can only determine $x_f^{x_m}$ for each f in some subset of $\{1, 2, \ldots, m-1\}$. Let $y_f = x_f^{x_m}$. The choice of x_m is still free, because no matter what value is selected for x_m, we simply compute $x_f = y_f^{x_m^{-1}}$. The conclusion is similar to the first case: a contains a single factor of x_{q_1} and b contains a single factor of x_m.

We have shown that, even when all but the first pair of the a_i's and b_i's are determined, the choice of a and b is still free. By descent from the last pair, we construct the desired correspondence. Hence $\mathcal{P}_\alpha(G) = \kappa_{\|\sigma\|}(G)$. ♠

2 Max$(\mathcal{P}_\sigma(G))$ for fixed σ

In a non-Abelian group, the probability two elements commute is bounded above by $\frac{5}{8}$. Using the previous theorem, we can find $\max(\mathcal{P}_\sigma(G))$ in terms of $\|\sigma\|$. First, we show a lemma about the distribution of $[\cdot, \cdot]$.

Lemma *The most likely value of* $[a, b]$ *is the identity.*

Proof. Fix $a \in G$, and denote the centralizer of a by $\mathrm{C}(a)$. Take K to be a set of coset representatives of $\mathrm{C}(a)$. Recall that $[a, b] = g \Leftrightarrow a^b = ag$. Now fix $b = ck$ for some $c \in \mathrm{C}(a)$ and $k \in K$. Since $c \in \mathrm{C}(a)$, $[a, b] = [a, k]$. So all elements of a $\mathrm{C}(a)$ coset give the same commutator with a. But the conjugacy class of a has $|K|$ elements. Therefore, there are $|K|$ commutators with a, all occuring with equal frequency.

Now let a range over G. For all $a \in Z(G)$, and $g \in G$, we have $[a, g] = e$. Every element of G produces the identity as a commutator; $[g, g] = e$. So for a, b random over G, $[a, b] = e$ most often. ♠

Theorem 2 *If* G *is a non-Abelian group,*

$$\kappa_h(G) \leq \frac{1 + \left(\frac{1}{4}\right)^h}{2}.$$

Equality holds if, and only if, $G' \cong \mathbf{Z}_2$ *and* $G/\mathrm{Z}(G) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

Proof. For $h = 0$, the result is trivial. Otherwise, there are two cases: $\kappa_1 \leq \frac{1}{2}$ and $\kappa_1 > \frac{1}{2}$. For case 1, assume $\kappa_1 \leq \frac{1}{2}$. Let $p = \max_{g \neq e} (\mathrm{prob}([x, y] = g))$. By

the previous lemma, $p < \kappa_1$, so we have the following:

$$\kappa_{h+1} \leq \kappa_h \cdot \kappa_1 + (1 - \kappa_h) \cdot p < \kappa_1 \leq \frac{1}{2}.$$

In the second case, when $\kappa_1 > \frac{1}{2}$, we have $|G'| = 2$ [3]. Since $G' = \{e, g\}$, we have $\text{prob}([x, y] = e) = \kappa_1$ and $\text{prob}([x, y] = g) = 1 - \kappa_1$. Summing the even terms of $(1 + \kappa_1)^h$, we find that

$$\kappa_h = \frac{(\kappa_1 + (1 - \kappa_1))^h + (\kappa_1 - (1 - \kappa_1))^h}{2} = \frac{1 + (2\kappa_1 - 1)^h}{2} \leq \frac{1 + \left(\frac{1}{4}\right)^h}{2}$$

since $\kappa_1 \leq \frac{5}{8}$. By [3], $\kappa_h = \frac{1+\left(\frac{1}{4}\right)^h}{2}$ exactly when $G/Z(G) \cong \mathrm{Z}_2 \times \mathrm{Z}_2$. ♠

3 Counting fundamental n-rewritings

Definition 7 *$F(m, n)$ is the number of fundamental n-rewritings in S_m.*

The values of F can be calculated by the following rules:

i) $\sum_{i=1}^{m} F(m, i) = m!$,

ii) $F(m, 1) = 1$,

iii) $F(m, n) = \binom{m+1}{n+1} F(n, n)$, $1 < n < m$.

Rule i is obvious, since every $\sigma \in S_m$ is some kind of rewriting. The identity is the only fundamental 1-rewriting; this verifies rule *ii*. Rule *iii* follows from the definition of fundamental n-rewriting: an action which can be realized in S_n. Fundamental n-rewritings in S_m work by permuting n blocks of letters in an m-tuple X. Since there may be stationary blocks on either end of the m-tuple, we need to partition X into $n+2$ parts with $n+1$ cuts. Since either stationary block may be empty, there are $m+1$ places to put the cuts. So $\binom{m+1}{n+1}$ enumerates the ways that S_n can act on an m-tuple, but the action from S_n must still be an n rewriting, so we derive rule *iii*.

The three rules are sufficient to compute F, since $F(1,1) = 1$ and if we know every value of $F(m,n)$ for $m < M$, we can compute the values of $F(M,n)$ for $n < M$, and rule i determines the last value, $F(M,M)$.

4 $\lim_{n\to\infty} \mathcal{P}_{\sigma_n}(G)$

Consider a sequence $\{\sigma_i\}$ where $\|\sigma_i\| = i$. Theorem 1 tells us how to determine $\lim_{n\to\infty} \mathcal{P}_{\sigma_n}(G)$.

Proposition 2 $\lim_{n\to\infty} \mathcal{P}_{\sigma_n}(G) = \frac{1}{|G'|}$.

Proof. By Theorem 1, $\mathcal{P}_{\sigma_n}(G)$ is the probability that the product of n commutators is the identity. Let $c_1, c_2, \ldots$ be a sequence of random commutators, with $c_i = [a, b]$ with probability $\frac{|\{(g,h)|[a,b]=[g,h]\}|}{|G|^2}$. Let $d_1, d_2, \ldots$ be a sequence of products of the c_i's, where $d_i = \prod_{j=1}^{i} c_i$. Since commutators generate G', the "random walk" the d_i's take on G' hits every element. Modelling this procedure as a Markov process, we have that, in the limit, all elements of G' are produced with equal probability [1]. ♠

5 A condition for $\mathcal{P}_\sigma(G) = \mathcal{P}_\sigma(H)$

We conclude with a condition for two groups to have the same rewritability structure. The theorem is in terms of products of commutators, which is equivalent, by Theorem 1, to a statement about rewritings. The following definitions will be useful.

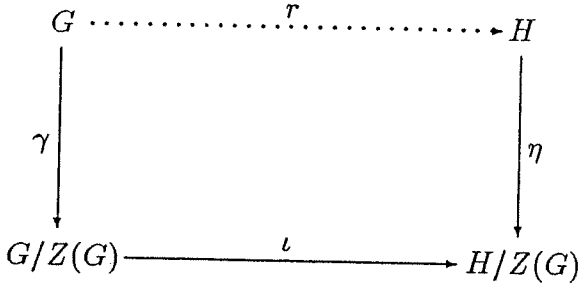
Definition 8 *Groups G and H are* isoclinic *if $G' \cong H'$ and $G/\mathrm{Z}(G) \cong H/\mathrm{Z}(H)$.*

Definition 9 $[U, V] = \{[u, v] | u \in U, v \in V\}$.

Note that if U is a coset of $Z(G)$, then for $u \in U, [U, V] = [\{u\}, V]$.

Theorem 3 (Isoclinic Lemma) *Let G and H be isoclinic, with $G' \cap \mathrm{Z}(G) = H' \cap \mathrm{Z}(H) = e$. Let $\gamma : G \to G/\mathrm{Z}(G)$, $\eta : H \to H/\mathrm{Z}(H)$, and $\iota : G/\mathrm{Z}(G) \to H/\mathrm{Z}(H)$, the natural homomorphisms. Then there is a relation $r : G \to H$ such that $r(a) = B$, a coset of $\mathrm{Z}(H)$; $r^{-1}(r(a)) = A$, a coset of $\mathrm{Z}(G)$; and $[r(a), r(c)] = r([a, c]) \cap H'$.*

Proof. Let $r = \eta^{-1}\iota\gamma$. We need to establish the following commutative diagram:



We have that $r(a)$ and $r(c)$ are both $Z(H)$ cosets, so $[r(a), r(c)]$ contains exactly one element. Since $r([a, c])$ is also a $Z(H)$ coset, it contains at most one element of H'. But $[a, c] \in G'$ and ι is an isomorphism, so $r([a, c]) \cap H' \neq \emptyset$. The construction of γ and η shows that $[r(a), r(c)] = r([a, c]) \cap H'$. ♠

We have constructed a one-to-one correspondence between $Z(G)$ cosets and $Z(H)$ cosets which preserves commutators, so we draw the following conclusion.

Corollary 3.1 *Let G and H be isoclinic with their derived groups intersecting their centers trivially. Let $\sigma \in S_n$. Then $\mathcal{P}_\sigma(G) = \mathcal{P}_\sigma(H)$.*

Proof. The corollary follows immediately from the Theorem 1 and the isoclinic lemma applied to the product of $\|\sigma\|$ commutators. ♠

References

[1] D. Aldous and P. Diaconis. *Shuffling Cards and Stopping Times.* Amer. Math. Monthly 93 (May 1986), 333-348.

[2] J. Ellenberg. Unpublished data. July 1990.

[3] J. L. Leavitt, G. J. Sherman, and M. E. Walker. *Rewriteability in Finite Groups.* Amer. Math. Monthly (to appear).