Rewritable Sequencings of Groups

Jeanne Nielsen

Department of Mathematics
Duke University
Durham, N.C.
U.S.A. 27706

Abstract. A finite group is called P_n-sequenceable if its nonidentity elements can be listed $x_1, x_2, \ldots, x_k$ so that the product $x_i x_{i+1} \cdots x_{i+n-1}$ can be rewritten in at least one nontrivial way for all i. It is shown that S_n, A_n, D_n are P_3-sequenceable, that every finite simple group is P_4-sequenceable, and that every finite group is P_5-sequenceable. It is conjectured that every finite group is P_3-sequenceable.

1. Introduction

Miller and Friedlander [6] have defined a finite group G to be *Z-sequenceable* if there exists a sequencing $\{x_i\}$ of the nonidentity elements of the group in which each element appears once and only once, and $x_i x_{i+1} = x_{i+1} x_i$ for all i. A group is called *strongly Z-sequenceable* if it has a Z-sequencing $(x_1, x_2, \ldots, x_m)$ such that $x_m x_1 = x_1 x_m$. If G is an abelian group, then every sequencing of the nonidentity elements of G is a strong Z-sequencing. However, a group need not be abelian in order to be Z-sequenceable; Miller and Friedlander demonstrate that if $|G/Z(G)| - 1 \leq |Z(G)|$, then G is Z-sequenceable, and that if $|G/Z(G)| \leq |Z(G)|$, then G is strongly Z-sequenceable. It is shown, moreover, that there exist groups which are not Z-sequenceable, and that in particular, the dihedral groups D_n $(n \geq 3)$, the symmetric groups S_n $(n \geq 3)$, and the alternating groups A_n $(n \geq 4)$ are not Z-sequenceable.

In this paper, we generalize these results by considering rewritability in the place of commutativity. A group G is said to be *n-rewritable* [1] if, for each n-element subset $\{x_1, \ldots, x_n\}$ of G, there are distinct permutations $\sigma, \tau \in S_n$ such that

$$x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)} = x_{\tau(1)} x_{\tau(2)} \cdots x_{\tau(n)} .$$

If one of σ, τ can always be chosen to be the identity, then G is said to be *totally n-rewritable*. Total n-rewritability is denoted by P_n, and this is the property which will be termed "rewritability" in this paper. Considerable research ([1], [2], [3], [5]) has been done recently on rewritability and total rewritability; one important result is that a group G is totally 3-rewritable if and only if $|G'| \leq 2$.

Rewriteability is a generalization of commutativity: a group has property P_2 if and only if the group is abelian. In light of this, a natural generalization of Z-sequenceability arises as follows: define a finite group to be P_n*-sequenceable* if

The author's work was supported by NSF grant DMS 8900507.

there exists a sequencing $\{x_i\}$ of the nonidentity elements of the group in which each element appears once and only once, and for all $i, 1 \leq i \leq |G| - n + 1$, the product $x_i x_{i+1} \cdots x_{i+n-1}$ can be rewritten in at least one nontrivial way (Z-sequenceability is equivalent to P_2-sequenceability.). A group will be called *strongly P_n-sequenceable* if the group has a P_n-sequencing $\{x_i\}$ such that the products $x_{m-n+2} \cdots x_m x_1, x_{m-n+3} \cdots x_1 x_2, \ldots, x_m x_1 \cdots x_{n-1}$ are all rewritable in at least one nontrivial way. Intuitively, this means that the sequencing can be thought of as a circular listing of the elements, so that x_m is followed by x_1, x_2, etc. In this paper, we consider the following questions concerning P_n-sequenceability:

1. Is there an integer n such that every finite group is P_n-sequenceable?
2. If so, what is the smallest such n? (Any group which is P_n-sequenceable is also P_{n+1}-sequenceable, P_{n+2}-sequenceable, etc.)

Our main results are that every finite group is P_5-sequenceable, that every finite simple group is P_4-sequenceable, and that S_n, A_n, and D_n are P_3-sequenceable for all n. We conjecture that every finite group is in fact P_3-sequenceable.

2. P_3-Sequencing Results

Lemma 1. *If the nonidentity elements of a finite group G can be divided into disjoint sets, each containing two or more elements, so that all the elements in each set commute with one another, then the group is strongly P_3-sequenceable.*

Proof: Suppose that the elements of G have been partitioned into sets as above. Then simply list the elements of one set, followed by the elements of the second set, etc. For any three successive elements x_i, x_{i+1}, x_{i+2}, where $1 \leq i \leq n-2$, either x_i, x_{i+1} are in the same set and hence commute, or x_{i+1}, x_{i+2} are in the same set and hence commute. The product $x_i x_{i+1} x_{i+2}$ can therefore be rewritten as $x_{i+1} x_i x_{i+2}$ or as $x_i x_{i+2} x_{i+1}$. The same is true for the triples x_{m-1}, x_m, x_1 and x_m, x_1, x_2, so this sequence is a strong P_3-sequencing.

Proposition 1. *If $|Z(G)| > 1$, then G is strongly P_3-sequenceable.*

Proof: Let the sets of Lemma 1 be the cosets of $Z(G)$. The elements of any coset of $Z(G)$ commute with one another. Since $|Z(G)| > 1$, these sets have order at least 2, possibly excepting $Z(G)$ itself, since the identity is excluded. But in this case, since the central element commutes with every element of the group, it may be placed in any other set; commutativity will be preserved in the set. The hypotheses of Lemma 1 are thus satisfied, proving the proposition.

Proposition 2. *If $|G|$ is odd, then G is strongly P_3-sequenceable.*

Proof: Since $|G|$ is odd, G contains no involutions; i.e. each element $g \in G$ has an inverse g^{-1} distinct from g. Divide the nonidentity elements of G into sets of order 2, each consisting of an element and its inverse. These sets satisfy the hypotheses of Lemma 1; hence, G is strongly P_3-sequenceable.

This proposition demonstrates that the question of P_3-sequenceability of a group is largely concerned with sequencing the involutions. If the involutions in a group can be partitioned into commuting sets as in Lemma 1, the group will be P_3-sequenceable regardless of the number of involutions. We now use this strategy to sequence the symmetric and alternating groups:

Theorem 1. *The symmetric group S_n is strongly P_3-sequenceable for all positive integers n.*

Proof: Partition the nonidentity, non-involutions into sets consisting of inverse pairs. Then consider the involutions: these are all products of disjoint 2-cycles. First consider those involutions which consist of a single 2-cycle. Choose any one of these and denote it by x. Then choose an involution y which is a product of two or more disjoint 2-cycles, one of which is the 2-cycle x. (This is possible when $n \geq 4$; note that $S_3 = D_3$, so S_3 can be sequenced as in the dihedral case below.) Then from the set of involutions consisting of a single 2-cycle, take all those 2-cycles which are factors of y. All of these 2-cycles, together with x and y, form a commuting set as in Lemma 1.

Now, if any involutions consisting of a single 2-cycle remain, repeat this process, at each step choosing one such involution x, and then choosing a y as above. Form a commuting set from x, y, and any single 2-cycle factors of y which have not yet been assigned to a set. Since all single 2-cycle factors of the involutions y are accounted for at each step, there will always be sufficient such y to exhaust the single 2-cycles.

To illustrate this process, consider S_4. There are nine involutions: $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$, $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$. Begin by choosing, for example, $(1,2)$. The involution $(1,2)(3,4)$ contains this 2-cycle, so let the elements $(1,2)$, $(1,2)(3,4)$, and $(3,4)$ (the other factor of $(1,2)(3,4)$) form a commuting set. From the remaining 2-cycles, choose, for example, $(1,3)$. This is a factor of $(1,3)(2,4)$, so let $(1,3)$, $(1,3)(2,4)$, and $(2,4)$ form a commuting set. Finally, let the involutions $(1,4)$, $(1,4)(2,3)$, and $(2,3)$ form a commuting set.

In this example, when we had exhausted all the single 2-cycles, we found that we had also exhausted the other involutions, but this will not be the case in general. Now consider any involutions which are products of two or more disjoint 2-cycles and have not yet been assigned to a set. Any such involution $(a_1, b_1)(a_2, b_2) \ldots (a_m, b_m)$ is the mth power of the $2m$-cycle $(a_1, a_2, \ldots, a_m, b_1, \ldots, b_m)$ and so commutes with this element and its inverse. Insert each such remaining involution into the set containing the corresponding $2m$-cycle and its inverse.

The nonidentity elements of S_n have now been partitioned as in Lemma 1, so simply listing these sets successively gives a strong P_3-sequencing for S_n.

Theorem 2. *The alternating group A_n is strongly P_3-sequenceable for all n.*

Proof: The procedure is similar to that for the symmetric groups. Divide the non-identity, non-involutions into sets each consisting of an element and its inverse, and then consider the involutions.

In the alternating groups, involutions are products of an even number of disjoint 2-cycles. First consider those involutions which are products of four or more disjoint 2-cycles. For each such product of m disjoint 2-cycles (m even), construct the single $2m$-cycle y as in the symmetric case. The element y is not in the alternating group, but y^2 is. Also, $|\langle y\rangle| \geq 8$, so $|\langle y^2\rangle| \geq 4$; thus y^2 is not an involution. Take each such involution x and add it to the set containing y^2 and its inverse.

Finally, consider those involutions which are products of two disjoint 2-cycles. These may be partitioned into sets of order 3, for given any such involution $(a,b)(c,d)$, the two involutions $(a,c)(b,d)$ and $(a,d)(b,c)$ commute with it and with each other. The nonidentity elements of A_n have now been partitioned as in Lemma 1, so listing the sets successively gives a strong P_3-sequencing for A_n.

We now move on to the question of P_3-sequencing arbitrary groups.

Lemma 2. *If a finite group G contains a self-centralizing involution (i.e. an involution x whose centralizer is the subgroup generated by x), then G has an abelian subgroup H of odd order which has index 2 in G, and G has a single conjugacy class of self-centralizing involutions, namely the coset Hx.*

Proof: Let $K = \langle x\rangle$ be the self-centralizing subgroup of order 2. We claim that any coset Ky has at most one element of order 2. To see this, suppose that

$$y^2 = 1 = (xy)^2$$

Then

$$yxy = y^{-1}xy = x^{-1} = x$$

Thus y centralizes x, and $Ky = K$, which clearly has only one involution. We have shown that G has at most $|G|/2$ involutions, but the conjugates of x produce exactly $|G|/2$ involutions.

The remaining elements pair off into $\{z, z^{-1}\}$, except for the identity, so $|G|/2$ is odd; say $|G| = 2m$, m odd. It is well-known that G must contain a normal subgroup H of order m. (Under the regular representation $G \to S_{2m}$, x must map to an odd permutation. Consider $G \cap A_{2m}$; let H be this subgroup.)

If y is a nontrivial element of H, then $x^{-1}yx \neq y$, since y can not centralize x. Thus the map $T : y \to x^{-1}yx$ is a fixed-point-free automorphism of H of order 2. Consider the map

$$y \to y^{-1}T(y)$$

defined on H. This map is one-to-one, and since H is finite, it is onto. Now

$$T(y^{-1}T(y)) = T(y^{-1})y = (y^{-1}T(y))^{-1}$$

and so $T(x) = x^{-1}$ for all $x \in H$. Thus for $x, y \in H$,

$$xy = T(x^{-1})T(y^{-1}) = T(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = yx$$

and H is abelian.

Theorem 3. *If a finite group G contains a self-centralizing involution, then G is strongly P_3-sequenceable.*

Proof: By Lemma 2, G has an abelian subgroup H of odd order of index 2 in G, and a single conjugacy class of self-centralizing involutions, the coset Hx. We construct a strong P_3-sequencing for these groups as follows: let $r = |\langle H \rangle|$. First list the $r-1$ nonidentity elements of H (denote the identity by h_0), followed by the r elements of Hx:

$$h_1, h_2, \ldots, h_{r-1}, h_0 x, h_1 x, \ldots, h_{r-1} x$$

That this is a strong P_3-sequencing is seen as follows:

1. For $1 \leq i \leq r-3$, the product $h_i h_{i+1} h_{i+2}$ is rewritable in any nontrivial way, because these elements commute.
2. The product $(h_{r-2})(h_{r-1})(h_0 x)$ is rewritable as $(h_{r-1})(h_{r-2})(h_0 x)$, because h_{r-2} and h_{r-1} commute.
3. The product $(h_{r-1})(h_0 x)(h_1 x)$ is rewritable as $(h_0 x)(h_1 x)(h_{r-1})$, because $(h_0 x)(h_1 x) \in H$ and hence commutes with h_{r-1}.
4. For $0 \leq i \leq r-3$, the product $(h_i x)(h_{i+1} x)(h_{i+2} x)$ is an involution and hence equal to its inverse. Since all three of its factors are also involutions, it can be rewritten as $(h_{i+2} x)(h_{i+1} x)(h_i x)$.
5. The product $(h_{r-2} x)(h_{r-1} x)(h_1)$ is rewritable as $(h_1)(h_{r-2} x)(h_{r-1} x)$, because the product $(h_{r-2} x)(h_{r-1} x) \in H$ and hence commutes with h_1.
6. The product $(h_{r-1} x)(h_1)(h_2)$ is rewritable as $(h_{r-1} x)(h_2)(h_1)$, because h_1, h_2 commute.

Corollary. *The dihedral group D_n is strongly P_3-sequenceable for all n.*

Proof: If n is even, then $|Z(D_n)| = 2$, and Proposition 1 applies; if n is odd, then every involution in D_n is self-centralizing, and Theorem 3 applies.

Theorem 4. *If for every involution $x \in G$, there exists an element y_x with $|\langle y_x \rangle| > 2$, such that $(y_x)^k = x$ for some $k > 1$, then G is strongly P_3-sequenceable.*

In particular, if there is no involution $x \in G$ such that $C(x)$ is a 2-group, then G is strongly P_3-sequenceable, for if $a \in C(x)$ has order p with p odd, then $y_x = ax \in C(x)$ satisfies $(y_x)^p = x$.

Proof: For each involution $x \in G$, choose a corresponding y_x. Let $\{x, y_x, y_x^{-1}\}$ form a commuting set. The y_x's are distinct, for there is at most one involution in $\langle y_x \rangle$. Divide the remaining elements into inverse pairs; by Lemma 1, G is strongly P_3-sequenceable.

In light of these results, we conjecture the following:

Conjecture. *Every finite group is strongly P_3-sequenceable.*

In order to prove the conjecture, it remains to be shown that groups containing involutions whose centralizers are 2-groups can be sequenced. It would be sufficient to show that the union of these centralizers can be sequenced, and then the remaining elements can be sequenced as in Theorem 4. Note that each of these centralizers, having prime power order, has nontrivial center and hence can be individually sequenced.

3. Other Sequencing Results

While we have not yet been able to show that all finite groups are P_3-sequenceable, we can demonstrate some slightly weaker properties. One important case is that of the simple groups. We have already demonstrated one large class of simple groups, namely the alternating groups, which are P_3-sequenceable. We now show that all finite simple groups are P_4-sequenceable; this is a corollary of the following:

Theorem 5. *Every finite group G with less than $|G|/3$ involutions is strongly P_4-sequenceable.*

Proof: Let $S = \{t_1, t_2, \dots, t_n\}$ be the set of all involutions of G. The other elements can be divided into at least n inverse pairs $\{g_1, g_1^{-1}\}, \dots, \{g_n, g_n^{-1}\}$. List the elements as follows:

$$g_1, g_1^{-1}, t_1, g_2, g_2^{-1}, t_2, \dots, g_n, g_n^{-1}, t_n,$$

followed by any remaining inverse pairs. Any four successive elements in the sequence include an adjacent inverse pair of elements which commute, so any product of four consecutive elements is rewritable by interchanging this pair. This is a strong P_4-sequencing of G.

Corollary. *Every finite simple group G is strongly P_4-sequenceable.*

Proof: We show that the number of involutions in G is less than $|G|/3$. Let n be the number of involutions in G, and let k be the number of conjugacy classes in G. It is proved in [7] (pp. 110-112) that

$$n^2 = \sum_{i=0}^{k-1} c_i |G : C(x_i)|,$$

where x_i is an element of the ith conjugacy class, and c_i is the number of ordered pairs of involutions (u, v) such that $uv = x_i$. It is also shown that

$$c_i \leq |C(x_i)|$$

for all i. Then we have that

$$n^2 \leq \sum_{i=0}^{k-1} |C(x_i)||G : C(x_i)|,$$

Hence

$$n^2 \leq \sum_{i=0}^{k-1} |G| = k|G|.$$

Since G is simple, the number of conjugacy classes $k \leq |G|/12$ [4]; hence, we have

$$n^2 \leq |G|^2/12,$$

and

$$n \leq |G|/\sqrt{12} < |G|/3.$$

Even in an arbitrary group, we can find an upper bound on the number of non-commuting involutions:

Lemma 3. *If a group G does not contain a self-centralizing involution, then the number of involutions in G which cannot be divided into commuting sets is less than $|G|/2$.*

Proof: We show that any involutions in excess of $|G|/2 - 1$ can be inserted into commuting sets as follows: partition the nonidentity, non-involutions into inverse pairs as in the proof of Proposition 2. Suppose there are exactly $|G|/2$ involutions in G, and let x be any involution. By our hypothesis, there is another element in G which commutes with x. If there is another involution y which commutes with x, then let $\{x, y\}$ form a commuting set. Otherwise, there is a non-involution z which commutes with x; put x in the set containing z and z^{-1}.

Now suppose there are more than $|G|/2$ involutions in G. Two involutions commute if and only if their product is an involution. Let S be the set of involutions in G, and let t be any involution in G. Since $|S| > |G|/2$, the intersection $S \cap tS$ is nonempty; i.e. there exists an involution $u \neq t$ such that tu is an involution, and hence $tu = ut$. If $|G|/2$ is odd, then let $\{u, t, ut\}$ form a commuting set. If $|G|/2$ is even, then let $\{u, t\}$ form a commuting set. Repeat this process, letting S be the set of involutions which have not yet been assigned to a set. However, after the first step, put only two involutions in each set, regardless of the parity of $|G|/2$. (The initial step was constructed in this way to ensure strict inequality.) It is easily seen that this process may be continued until the number of involutions remaining is less than $|G|/2$.

Using this result, we can now answer in the affirmative our question as to the existence of an integer n such that every finite group is P_n-sequenceable:

Theorem 6. *Every finite group is P_5-sequenceable.*

Proof: If a group G contains a self-centralizing involution, then G is P_3-sequenceable and so is P_5-sequenceable. Suppose that G does not contain a self-centralizing involution. By Lemma 3, there are less than $|G|/2$ nonidentity elements of the group which cannot be placed in commuting sets (and at most one of these sets is not of order 2, as in the above lemma). Denote these elements by $x_1, \ldots, x_m$. Denote the sets of commuting elements by $(r_1, s_1), \ldots, (r_n, s_n)$ (possibly the last set is (r_n, s_n, t_n)). Since $m < |G|/2$, we have that $2n \geq m$. Then the sequence

$$x_1, x_2, r_1, s_1, x_3, x_4, r_2, s_2, \ldots, x_m,$$

followed by the remaining commuting sets (we have shown that at least one such set remains) is a strong P_5-sequencing of G: any five consecutive elements contain an adjacent commuting pair, and their product may be rewritten by exchanging these two elements.

Acknowledgement

Group-theoretic experimentation and computation were facilitated with the computer algebra system CAYLEY.

1. R.D. Blyth, *Rewriting products of group elements—I*, J. Alg. **116** (1988), 506–521.
2. R.D. Blyth, *Rewriting products of group elements—II*, J. Alg. **119** (1988), 246–259.
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. **74** (1983), 136–142.
4. J.D. Dixon, *Problem 176*, Canad. Math. Bull. **16** (1973), 302.
5. P. Longobardi, M. Maj, and S. Stonehewer, *The classification of groups in which every product of four elements can be reordered.* preprint.
6. M.D. Miller and R.J. Friedlander, *On Some Sequencing Problems in Finite Groups*, Discrete Math. 19 (1977), 77–84.
7. J.S. Rose, "A Course on Group Theory", Cambridge University Press, Cambridge, 1978.