Rose-Hulman Institute of Technology

Rose-Hulman Scholar

Mathematical Sciences Technical Reports (MSTR)

Mathematics

3-1992

A4 Rewriteability

Eric Wepsic

Kevin O'Bryant

Lawren Smithline

A_4–REWRITEABILITY

Eric Wepsic, Kevin O'Bryant, and Lawren Smithline

MS TR 92-03

March 1992

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

FAX(812) 877-3198

Phone: (812) 877-8391

A_4–rewritability

Eric Wepsic*, Kevin O'Bryant*, and Lawren Smithline*

Let S be a subset of S_n. A finite group G (in fact, every group we consider here will be finite!) is said to be S-rewritable if, for each n-tuple $(x_1, x_2, \ldots, x_n) \in G^n$, there exists $\sigma \in S - \{\text{identity}\}$ such that

$$x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}.$$

If $S = S_n$, G is termed n-rewritable. The class of all n-rewritable groups is denoted by P_n.

Much effort has gone into the classification of the P_n. It is easy to see that a group in P_2 is abelian. Curzio, Longobardi, and Maj [2] have shown that a group G is in P_3 if and only if the order of the derived group, G', is at most two. The class P_4, however, is much more complicated. Longobardi, Maj, and Stonehewer [1] have classified these groups.

Result 1 (Longobardi, Maj, and Stonehewer) *If $G \in P_4$, then either $|G'| \leq 5$ or $|G'| = 8$, or G contains an abelian subgroup of index 2. Moreover, if $G' \cong (\mathrm{Z}_2)^3$, then either $G/Z(G)$ is generated by 3 elements, or $G/Z(G)$ is generated by 4 elements and G is not the internal product of two abelian subgroups, that is, G is not diabelian.*

Extending these results to P_5 seems hopeless. We consider a somewhat simpler problem: the determination of PA_4, the set of A_4-rewritable groups. Rewritability with respect to subsets of S_n was first considered in [3], where this question was first posed. We consider this problem both for its own sake and in the hope that it will shed some light on, and possibly simplify, the classification of P_4 given in [1].

To fix notation, we represent the commutator $w^{-1}x^{-1}wx$ by $[w, x]$, the identity of a group by e, and the centralizer of x in G by $\mathrm{C}_G(x)$.

Theorem 1 (Main Theorem) *The group G is in PA_4 if, and only if, one of the following holds:*

a. $|G'| \leq 2$.

b. $G' \cong (\mathrm{Z}_2)^2$, *and* $G' \subseteq Z(G)$.

c. $|G'| = 3$, *and either* $G' \not\subseteq Z(G)$, *or G does not contain w, x, y, z satisfying* $[w, z]^2 = [w, x] = [w, y] = [x, y] = [x, z] = [y, z] \neq e$.

*Work supported by NSF grant number DMS-910059

1 Sufficient Conditions for Membership in PA_4

The group $G \in PA_4$ if one of the following holds:

a. $|G'| \leq 2$.

b. $G' \cong (\mathbb{Z}_2)^2$, *and* $G' \subseteq Z(G)$.

c. $|G'| = 3$, *and either* $G' \not\subseteq Z(G)$, *or* G *does not contain* w, x, y, z *satisfying* $[w,z]^2 = [w,x] = [w,y] = [x,y] = [x,z] = [y,z] \neq e$.

The next few propositions combine to prove this theorem.

Proposition 1 *If* G' *is isomorphic to a subgroup of* $(\mathbb{Z}_2)^2$, *and* $G' \subseteq Z(G)$, *then* $G \in PA_4$.

Proof. We will show that any 4–tuple $(w,x,y,z) \in G^4$ can be rewritten by an even permutation. When, for example, does $wxyz = xywz$? Well,

$$\begin{aligned} wxyz &= xw[w,x]yz \\ &= xwyz[w,x] \\ &= xyw[w,y]z[w,x] \\ &= xywz[w,y][w,x]. \end{aligned}$$

(We could slip the commutator out because $G' \subseteq Z(G)$.) So $wxyz = xywz$ when $[w,y][w,x] = e$.

Set $\alpha = [w,x]$, $\beta = [w,y]$, $\gamma = [w,z]$, $\delta = [x,y]$, $\epsilon = [x,z]$, $\zeta = [y,z]$. If we use additive notation for G' (it is, after all, abelian), $wxyz$ can be rewritten by an even permutation exactly when one of the following capital–lettered sums of commutators is zero:

Commutator Equation	*From Rewriting*
$A = \alpha + \beta$	$xywz$
$B = \alpha + \zeta$	$xwzy$
$C = \beta + \delta$	$ywxz$
$D = \delta + \epsilon$	$wyzx$
$E = \epsilon + \zeta$	$wzxy$
$A' = \gamma + \delta + \epsilon + \zeta$	$zwyx$
$B' = \beta + \gamma + \delta + \epsilon$	$yzwx$
$C' = \alpha + \gamma + \epsilon + \zeta$	$zxwy$
$D' = \alpha + \beta + \gamma + \zeta$	$xzyw$
$E' = \alpha + \beta + \gamma + \delta$	$yxzw$
$V = \alpha + \beta + \gamma + \delta + \epsilon + \zeta$	$zyxw$

We note first that $A + A' = B + B' = \cdots = E + E' = V$. If $V = 0$, we are done; therefore, assume without loss of generality that $V = (1,0) \in (\mathbb{Z}_2)^2$. Then $A, B, C, D, E \in \{(0,1),(1,1)\}$, because if, say, C were equal to $(1,0) = V$, then C' would equal $V - C = (0,0)$. Hence $A+B+C+D+E \in \{(0,1),(1,1)\}$

as well. But $A+B+C+D+E = \alpha+\beta+\alpha+\zeta+\beta+\delta+\delta+\epsilon+\epsilon+\zeta = 2(\alpha+\beta+\delta+\epsilon+\zeta) = (0,0)$, a contradiction. Hence $G \in PA_4$. ■

Corollary 1 *If $|G'| = 1$ or 2, then $G \in PA_4$.*

Proof. If the derived group is of size 1 or 2, then it is certainly isomorphic to a subgroup of $(\mathbb{Z}_2)^2$. If $|G'| = 1$, then G' is trivially in the center of G. If $|G'| = 2$, then, as G' is normal in G, G' is the union of two conjugacy classes of G of size one. It follows that $G' \subseteq Z(G)$. Thus the hypotheses of Proposition 1 are satisfied. ■

Proposition 2 *If $|G'| = 3$ and $G' \not\subseteq Z(G)$, then $G \in PA_4$.*

Proof. If $|G'| = 3$, we first note that

$$|\mathrm{C}_G(g)| \geq |\mathrm{C}_{G/N}(Ng)|$$

for all normal subgroups N of G and all $g \in G$, by (2.24) of [4]. In particular,

$$|\mathrm{C}_G(g)| \geq |\mathrm{C}_{G/G'}(G'g)| = |G/G'|,$$

where the last equality follows because G/G' is abelian. Therefore, the index of each centralizer in G is at most 3. Hence, all the conjugacy classes are of length 1, 2, or 3. Chillag and Herzog have classified all groups with conjugacy classes of prime length [5]: their classification yields that either $G' \subseteq Z(G)$ (impossible by hypothesis), or $G/Z(G)$ is isomorphic to S_3.

If $G/Z(G) \cong S_3$, then $G \in PA_4$. This can be seen directly, making use of the fact that two elements a, b in G commute if their images $\bar{a}, \bar{b}$ generate a cyclic subgroup of G/Z. The procedure is tedious. We prefer to use the following lemma.

Lemma 1 (Isoclinic Lemma [7]) *If $G/Z(G) \cong H/Z(H)$, $G' \cong H'$, and $G' \cap Z(G) = H' \cap Z(H) = \{e\}$, then G and H have the same rewritability structure; in particular, $G \in PA_4$ if, and only if, $H \in PA_4$.*

Proposition 2 follows easily from the lemma, since its hypotheses are satisfied when $H = S_3$, which can be shown A_4-rewritable. ■

Proposition 3 *If $|G'| = 3$, and $G' \subseteq Z(G)$, then $G \in PA_4$ if and only if G does not contain w, x, y, z satisfying $[w,z]^2 = [w,x] = [w,y] = [x,y] = [x,z] = [y,z] \neq e$.*

Proof. Suppose that $|G'| = 3, G' \subseteq Z(G)$, and $G \notin PA_4$. Let (w,x,y,z) be a non-rewritable 4-tuple of G. Using the labelling of Proposition 1, none of $V, A, A', B, B', \ldots E, E'$ are zero. Since $A+A' = V$, we must have $A = A' = 2V$. Similarly, $A = B = \cdots = D' = E' = 2V$. Therefore, $\alpha = \beta = \delta = \epsilon =$

$\zeta = V$, but $\gamma = 2V$. In other words, $[w,z]^2 = [w,x] = [w,y] = [x,y] = [x,z] = [y,z] \neq e$. Furthermore, since this is the only assignment satisfying $V, A, A', B, B', \ldots, E, E' \neq 0$, if $G \in PA_4$, then it does not contain w,x,y,z satisfying $[w,z]^2 = [w,x] = [w,y] = [x,y] = [x,z] = [y,z] \neq e$. ■

There are groups containing w,x,y,z satisfying $[w,z]^2 = [w,x] = [w,y] = [x,y] = [x,z] = [y,z] \neq e$. The smallest one is of order $3^5 = 243$, and is given by five order 3 generators (a,w,x,y,z) satisfying the following commutator relations: $[a,w] = [a,x] = [a,y] = [a,z] = e$, $[w,x] = [w,y] = [x,y] = [x,z] = [y,z] = a$, $[w,z] = a^2$.

2 Necessary Conditions for Membership in PA_4

The group $G \in PA_4$ only if one of the following holds:

a. $|G'| \leq 2$.

b. $G' \cong (\mathrm{Z}_2)^2$, and $G' \subseteq Z(G)$.

c. $|G'| = 3$, and either $G' \not\subseteq Z(G)$, or G does not contain w,x,y,z satisfying $[w,z]^2 = [w,x] = [w,y] = [x,y] = [x,z] = [y,z] \neq e$.

Proposition 4 *If $G \in PA_4$ has an abelian subgroup A of index 2, then $|G'| \leq 3$.*

Proof. Take $x \in G - A$. Any commutator $[g,h]$ in G' can be written in the form $[x,a]$ for some $a \in A$: to see this, note that $[a,b]$ is trivial for $a,b \in A$; that $[bx,a] = [ax,bx] = [x,(ab)^{-1}]$; that $[a,bx] = [x,a^{-1}]$. Hence, G' is generated by the image of the map $a \mapsto [x,a]$. A straightforward computation also shows that $[x,ab] = [x,a][x,b]$. This also proves that G' is abelian, and is actually equal to the set of commutators. (G' can also be seen abelian because $G' \subseteq A$.)

Suppose that G' contains a copy of Z, or Z_n for $n \geq 4$. Then take $a,b,c \in A$ so that $\alpha = [x,a] = 1$, $\beta = [x,b^{-1}] = 1$, $\gamma = [x,c^{-1}] = 1$. We cannot rewrite $a \cdot b \cdot x \cdot c$, because no sum $\alpha, \alpha+\beta, \alpha+\gamma, \alpha+\beta+\gamma, \beta+\gamma$ is equal to zero.

Suppose that G' contains a copy of $\mathrm{Z}_m \times \mathrm{Z}_n$, $m,n > 1$. Then take $a,b,c \in A$ so that $[x,a] = (0,1)$, $[x,b^{-1}] = [x,c^{-1}] = (1,0)$; we again cannot rewrite $a \cdot b \cdot x \cdot c$, since none of the above sums are zero.

Together, this implies that $|G'| \leq 3$. ■

Therefore, we now know that $G \in PA_4$ implies $|G'| \leq 5$ or $|G'| = 8$. We now make an observation suggested by [2]:

Lemma 2 *If $G \in PA_4$, then for every $x \in G$, either $x^3 \in Z(G)$ or $x^2 \in Z(G)$.*

Proof. If we rewrite $x \cdot x \cdot y \cdot x^3$ according to A_4, we will see that one of x, x^2, x^3 commutes with y. So $G = C_G(x^2) \cup C_G(x^3)$, whence (since a group is never equal to the union of two proper subgroups) either $C_G(x^2) = G$ or $C_G(x^3) = G$, which means that either $x^2 \in Z$ or $x^3 \in Z$. ■

Let $H = G/Z$. This lemma tells us that if $G \in PA_4$, every element of H has order 1, 2, or 3. Deaconescu [8] has classified groups of this type. If G is nilpotent, then H is either a 2-group of exponent 2, or a 3-group of exponent 3. If G is not nilpotent, either $|H| = 2^a3$ and $|H'| = 2^a$, $a \geq 2$, or $|H| = 2 \cdot 3^a$ and $|H'| = 3^a$, with $a \geq 1$. We handle the nilpotent case first.

Lemma 3 *If $G \in PA_4$ is nilpotent, then $G' \leq Z(G)$ and either*

a. $|G'| = 3$; or

b. $G' \cong (\mathrm{Z}_2)^n$ with $n \leq 2$; or

c. $G' \cong (\mathrm{Z}_2)^3$ with $G/Z \cong (\mathrm{Z}_2)^3$ or $G/Z \cong (\mathrm{Z}_2)^4$.

Proof. If G is nilpotent, then it is the direct product of its Sylow subgroups. Then, H is also the direct product of its Sylow subgroups. Since we know from above that H is either a 2-group or a 3-group, we can infer that all of the Sylow subgroups of G are abelian except for possibly one of $Syl_2(G)$ or $Syl_3(G)$. Since $|G'| \leq 5$ or $|G'| = 8$, we have $|G'| = 3$, or $|G'| = 2^n, n \leq 3$. If $|G'| = 3$, then only the $Syl_3(G)$ factor is nonabelian. Since, the derived group and the center of a nonabelian p-group always intersect nontrivially, $G' \subseteq Z(G)$. If $|G'| = 2^n$, then $H = G/Z = Syl_2(G/Z) = (\mathrm{Z}_2)^k$, since H must be of exponent 2. We can see now, as G/Z is abelian, that $G' \subseteq Z(G)$. Proceeding further, we know that if $G/Z \cong (\mathrm{Z}_2)^k$, as it certainly is here, then $G' \cong (\mathrm{Z}_2)^t$ for some t by [6]. By [1] , any such group has G/Z generated by 3 or 4 elements–that is, $G/Z \cong (\mathrm{Z}_2)^3$ or $G/Z \cong (\mathrm{Z}_2)^4$. ■

Lemma 4 *If $G/Z \cong G' \cong (\mathrm{Z}_2)^3$, and $G' \subseteq Z(G)$, then $G \notin PA_4$.*

Proof. Pick elements a, b, c of G whose images generate G/Z. Since $G' \subseteq Z(G)$, the bracket $[\cdot,\cdot]$ which maps $(G/Z)^2 \to G'$ by taking (a, b) to the commutator $[a, b]$ is an alternating bilinear form whose image must be generated by $[a, b]$, $[a, c]$, $[b, c]$. Therefore these commutators generate G', and are linearly independent over Z_2. A calculation similar to those in Proposition 1 shows that we cannot rewrite $a \cdot c \cdot b \cdot c$ in this case. Therefore, $G \notin PA_4$. ■

Lemma 5 *If $G/Z \cong (\mathrm{Z}_2)^4$, $G' \cong (\mathrm{Z}_2)^3$, and $G' \subseteq Z(G)$, then $G \notin PA_4$.*

Proof. By [1], in this case G cannot be diabelian. We show that, for this reason, there must be $a \in G/Z$ so that there exist $b, c, d \in G/Z$ such that $[a, b]$, $[a, c]$, $[a, d]$ generate G'. Suppose to the contrary that $[a, \cdot]$ is never surjective. For every a, this linear function then has a kernel K_a containing at least 4 elements distinct in G/Z. Suppose $K_a = \{e, a, b, ab\}$. Now take any $c \in G - K_a$. The same must be true of c: say the kernel of $[c, \cdot]$ is $K_c = \{e, c, d, cd\}$.

If there is some c for which a, b, c, d are independent in G/Z, then take preimages $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$. We know that $G = \langle \bar{a}, \bar{b}, \bar{c}, \bar{d} \rangle Z$ because $G' \subseteq Z$. So we have $G = \langle \bar{a}, \bar{b} \rangle Z \cdot \langle \bar{c}, \bar{d} \rangle Z$, so G isn't in PA_4, by [1], because it is diabelian.

So we may assume that the set $\{a, b, c, d\}$ is always linearly dependent in the vector space $G/Z = \mathrm{Z}_2^4$. Hence $d = \alpha a + \beta b + \gamma c$, so $[c, \alpha a + \beta b + \gamma c] = 0$, whence

$[c, \alpha a + \beta b] = 0$, so c commutes with $\alpha a + \beta b \in K_a$. Therefore, c commutes with some nonzero element of K_a. But this holds for every $c \in G/Z - K_a$, and there are 12 of them. This means that each nonidentity element of K_a commutes with at least $4 + 12/3 = 8$ elements of G/Z. (None can commute with more, because the centralizer of an element which did would be all of G.) In particular, a does. Therefore, $[G : C_G(a)] = 2$ for all $a \neq e$. By [2], this implies that $|G'| = 2$, contradicting our hypothesis.

Hence, we can pick $a, b, c, d \in G$ such that $[a, b] = \alpha$, $[a, c] = \beta$, $[a, d] = \gamma$ generate G'. We now need only concern ourselves with the possible values of $[b, c]$, $[b, d]$, $[c, d]$. One helpful note: for no j, k, l can $[j, k]$, $[k, l]$, and $[j, l]$ be linearly independent. This follows from Lemma 4. Therefore, $[b, c] = m_1\alpha + n_1\beta$, $[b, d] = m_2\alpha + n_2\gamma$, $[c, d] = m_3\beta + n_3\gamma$ and $[c, d] = m_4[b, c] + n_4[b, d]$, for some $m_i, n_i \in \{0, 1\}$. We now consider cases.

$[b, c]$	$[b, d]$	$[c, d]$	Can't Rewrite This
e	e	e	$bacd$
e	e	β	$acbd$
e	e	$\beta\gamma$	$acbd$
e	α	β	$abcd$
α	α	e	$a \cdot d \cdot c \cdot db$
α	α	γ	$a \cdot d \cdot c \cdot db$
$\alpha\beta$	e	γ	$dacb$
$\alpha\beta$	e	β	$dbac$
$\alpha\beta$	γ	γ	$a \cdot b \cdot c \cdot bd$
$\alpha\beta$	$\alpha\gamma$	$\beta\gamma$	$a \cdot ac \cdot cd \cdot b$
$\alpha\beta$	$\alpha\gamma$	e	$acdb$
β	γ	$\beta\gamma$	$cabd$
β	$\alpha\gamma$	γ	$adcb$

We have exhausted all possibilites for G up to symmetry. Therefore, $G \notin PA_4$. ■

Combining Lemmas 3, 4, and 5, we arrive at the following proposition:

Proposition 5 *If $G \in PA_4$ is nilpotent, then it is of class 2 and one of the following holds:*

a. $|G'| \leq 2$,

b. $G' \cong (\mathbf{Z}_2)^2$,

c. $|G'| = 3$ *and G does not contain w, x, y, z satisfying* $[w, z]^2 = [w, x] = [w, y] = [x, y] = [x, z] = [y, z] \neq e$.

We now examine the nonnilpotent case. Note that if $H = G/Z$ is nonnilpotent, then neither is G.

Proposition 6 *If $H = G/Z$ is nonnilpotent, and $|H| = 2^a 3$, where $a \geq 2$, then $G \notin PA_4$.*

Proof. (This can be shown by checking all groups of order 12 and 24.) Consider H', which is elementary abelian, normal, and of index 3 in H, by [8]. We take a subgroup of H of the form Z_3: then $H \cong H' \otimes \mathrm{Z}_3 \cong (\mathrm{Z}_2)^n \otimes \mathrm{Z}_3$, where the semidirect product action is nontrivial. What can Z_3 do to H'?

Let $k \in \mathrm{Z}_3$, and $g \in (\mathrm{Z}_2)^n$. Let $h = kgk^{-1}$. Now, what can $khk^{-1} = k^2gk^{-2}$ equal? Clearly, not g; the possibilities are either $khk^{-1} = gh$, or $khk^{-1} = i$, where $i \in (\mathrm{Z}_2)^n$ and g, h, i are linearly independent. In the first case, our Z_3 acts on a copy of $(\mathrm{Z}_2)^2$ as in A_4–in short, H will contain a subgroup isomorphic to A_4. In the second case, our Z_3 cyclically permutes the basis elements of the copy of $(\mathrm{Z}_2)^3$ generated by g, h, i. In this case H will contain a subgroup isomorphic to $(\mathrm{Z}_2)^3 \otimes \mathrm{Z}_3$ with this action.

Since PA_4 is closed under factor groups and subgroups and, by direct calculation using CAYLEY, neither A_4 nor $(\mathrm{Z}_2)^3 \otimes \mathrm{Z}_3$ is in PA_4, the statement follows. ■

Proposition 7 *If $G \in PA_4$, and $H = G/Z$ is nonnilpotent of order $2 \cdot 3^a$, with $a \geq 1$, then $H \cong S_3$. Furthermore, $|G'| = 3$ and $G' \not\subseteq Z(G)$.*

Proof. We know that $|H'| \leq 8$. In H, by [8], H' is a normal Sylow subgroup of index 2; $H' = 3^a$. But $|H'| \leq 8$, so $|H'| = 3$, whence $a = 1$, and we are done. ■

References

[1] P. Longobardi, M. Maj, and S. Stonehewer. *The Classification of Groups in which Every Product of Four Elements Can Be Reordered.* Technical Report, University of Warwick, England. 1988.

[2] 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.

[3] C. Grood. *Dihedral Rewriteability.* MS TR 90-08, Rose-Hulman Inst. of Tech. Technical Report Series.

[4] I. Isaacs. **Character Theory of Finite Groups.** Academic Press, Inc. San Diego. 1976.

[5] D. Chillag and M. Herzog. *On the Length of the Conjugacy Classes of Finite Groups.* Journal of Algebra **131**, 110-125 (1990).

[6] Ngọc Châu Nguyen. *On the isoclinic classes of the groups G with $G/Z(G) \cong \mathrm{Z}_p^n$.* Tạp chí Toán học **16**, no. 2, 10-20 (1988).

[7] Lawren Smithline. *Rewriteability, Commutators, and Fundamental* n-*Rewritings* MS TR 92-02, Rose-Hulman Inst. of Tech. Technical Report Series.

[8] Deaconescu, Marian. *Classification of Finite Groups with All Elements of Prime Order.* Proceedings of the American Mathematical Society **106**, no. 3, 625-629 (1989).

Eric Wepsic & Lawren Smithline
Harvard University
Cambridge, MA 02138

Kevin O'Bryant
Rose-Hulman Institute of Technology
Terre Haute, IN 47803