MAXIMAL ORDER THREE-REWRITEABLE SUBGROUPS OF SYMMETRIC GROUPS

John T. O'Bryan

MS TR 90-01

September 1990

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

FAX(812) 877-3198

Phone: (812) 877-8391

Maximal Order Three-Rewriteable Subgroups of Symmetric Groups

John T. O'Bryan *
Rose-Hulman Institute of Technology

Introduction

Recently, Burns and Goldsmith [**2**] characterized the maximal order Abelian subgroups of the symmetric groups using elementary techniques and the results of Hoffman [**5**]. This classification could also be directly inferred from the results of Kovács and Praeger [**7**]. A natural extension would be to consider the weaker, more general form of commutativity, three-rewriteability. The purpose of this paper is to completely characterize the maximal order three-rewriteable subgroups of the symmetric groups. The main result is the following:

THEOREM. *Let G be a maximal order three-rewriteable subgroup of S_n, the symmetric group of degree n. Then,*

$$n \leq 3 \;\Rightarrow\; G \cong Z_n,$$
$$n = 4 \text{ or } 5 \;\Rightarrow\; G \cong D_4,$$

and for $n \geq 6$,

$$n = 3k+4 \;\Rightarrow\; G \cong D_4 \times Z_3^k,$$
$$n = 3k+5 \;\Rightarrow\; G \cong D_4 \times Z_2 \times Z_2 \times Z_3^{k-1} \text{ or } D_4 \times Z_4 \times Z_3^{k-1} \text{ or } T_8 \times Z_3^{k-1},$$
$$n = 3k+6 \;\Rightarrow\; G \cong D_4 \times Z_2 \times Z_3^k,$$

where Z_n is the cyclic group of order n and degree n, D_4 is the dihedral group of order 8 and degree 4, and T_8 is an extra-special two-group of order 32 and degree 8.

The classification relies on a result of Curzio, Longobardi, and Maj [**3**]: *A group G is non-Abelian three-rewriteable if and only if the derived group, G', has order two.* It is also intimately related to the work of Kovács and Praeger [**7**], which deals with Abelian quotients of permutation groups. However, the classification does not follow directly from [**7**], as it does in the Abelian case. The results of Burns and Goldsmith [**2**], Itô [**6**], and Ljubich [**8**] will also be needed to obtain the final result.

*Research supported by NSF grant DMS 8922674.

About Three-Rewriteability

Definition. *A group, G, is defined to be three-rewriteable if* $\forall x, y, z \in G$,

$$xyz \;=\; \textit{at least one of} \begin{cases} xzy \\ yxz \\ yzx \\ zxy \\ zyx \end{cases}$$

Obviously, any Abelian group is three-rewriteable. Furthermore, Curzio, Longobardi, and Maj [**3**] have also shown the equivalence of the following statements:

(i) *G is three-rewriteable.*
(ii) *The derived group of G has order one or two.*
(iii) *Each conjugacy class of G has size one or two.*

Itô [**6**] has shown that if a group G has all conjugacy classes of size one or p, a prime, then G is the direct product of a p-group with this property and an Abelian group. Using this fact along with (iii) yields the following theorem:

Theorem 1. *If G is a three-rewriteable group, then* $G \cong T \times A$, *where T is an indecomposable, three-rewriteable two-group, and A is Abelian.*

Hence, the question of how to embed a three-rewriteable group in a symmetric group leads to the question of how to embed a direct product in a symmetric group. Let μ(G) represent the minimal degree of a permutation group isomorphic to G. Ljubich [**8**] has shown that $\mu(\mathrm{A}\times\mathrm{B}) = \mu(\mathrm{A}) + \mu(\mathrm{B})$ if A and B are nilpotent. Since T and A are nilpotent as defined in Theorem 1, there will always be enough symbols to embed the two component and the Abelian component of a three-rewriteable group onto disjoint sets of symbols, and this will be assumed when proving the main theorem. For more interesting results and information on minimal permutation representations, see Easdown and Praeger [4].

Empirical Results

The computer algebra system CAYLEY was used to determine the maximal order three-rewriteable subgroups of S_n up to $n = 12$. It will be shown when proving the theorem, though, that knowledge of three-rewriteable groups in S_n is only necessary for $n \leq 8$. These results follow:

$$\begin{aligned}
n \leq 3 &\Rightarrow G \cong Z_n \\
n = 4 &\Rightarrow G \cong D_4 \\
n = 5 &\Rightarrow G \cong D_4 \\
n = 6 &\Rightarrow G \cong D_4 \times Z_2 \\
n = 7 &\Rightarrow G \cong D_4 \times Z_3 \\
n = 8 &\Rightarrow G \cong D_4 \times Z_2 \times Z_2 \text{ or } D_4 \times Z_4 \text{ or } T_8
\end{aligned}$$

Z_n is cyclic of order n and is thus three-rewriteable. D_4 has a derived group of order two and hence is three-rewriteable. In S_4,

$$D_4 = < (1,2,3,4),\ (1,4,2,3) > .$$

The quaternion group is also a three-rewriteable group of order eight, but, unlike D_4, it has degree eight. In S_8,

$$Q = < (1,3,2,4)(5,8,6,7),\ (1,7,2,8)(3,6,4,5) > .$$

The quaternion group and D_4 have the distinction of being the non-Abelian, three-rewriteable groups of smallest order. T_8, being extra-special of order 32, also has a derived group of order two. In S_8,

$$T_8 = < (1,6,2,5)(3,8,4,7),\ (1,7,2,8)(3,5,4,6),\ (1,5,2,6)(3,8,4,7),\ (1,8,2,7)(3,5,4,6) > .$$

For more information on D_4 and T_8 and how they are related to subgroups of S_n with large Abelian quotients, see Kovács and Praeger [**7**].

Proof of the Theorem

Consider the theorem stated in the introduction. In each case, $|G'| \leq 2$ and G is isomorphic to a subgroup of the claimed symmetric group. The proof will now be carried out by showing that any three-rewriteable subgroup of S_n with equal or larger order than G must be isomorphic to one of the conjectured groups. The main result of Burns and Goldsmith [**2**] will be helpful and is now stated as a theorem.

Theorem 2. *Let G be an Abelian subgroup of maximal order of the symmetric group, S_n. Then,*

$$\begin{array}{lll} n = 3k & \Rightarrow & G \cong Z_3^k, \\ n = 3k+1 & \Rightarrow & G \cong Z_2 \times Z_2 \times Z_3^{k-1} \text{ or } Z_4 \times Z_3^{k-1}, \\ n = 3k+2 & \Rightarrow & G \cong Z_2 \times Z_3^k. \end{array}$$

Recall that a three-rewriteable group is ismorphic to a direct sum of a three-rewriteable two-group and an Abelian group. Two lemmas are now stated yielding upper bounds on the order of these types of groups.

Lemma 1. *If G is an Abelian group with $G \subseteq S_n$, then $|G| \leq 3^{n/3}$.*

Proof. This follows from Theorem 2 or from [**7**]. It is interesting, though, that this is also a direct result of Bercov and Moser [**1**], which appeared over twenty years earlier than either [**2**] or [**7**].

Lemma 2. *If G is a three-rewriteable two-group with $G \subseteq S_n$, then $|G| \leq 2 \cdot 2^{n/2}$.*

Proof. A special case of the main theorem of [**7**] states that if G is a p-group and $G \subseteq S_n$, then $|G/G'| \leq p^{n/p}$. Since G is a three-rewriteable two-group, $|G'| = 2$, and $|G| \leq |G'| \cdot 2^{n/2} = 2 \cdot 2^{n/2}$.

Here is a summary of the notation used in the proof and a few assumptions:

- G is the conjectured maximal order three-rewriteable subgroup of S_n.
- H is an actual maximal order three-rewriteable subgroup of S_n.
- H $\cong$ T$\times$A, where T is an indecomposable, three-rewriteable two-group and A is an Abelian group.
- The minimal degree of T is m, and the minimal degree of A is $n-m$. T and A act on disjoint sets of symbols in S_n.
- It may be assumed that m is even, since, when i is even, the Sylow two-subgroups of S_i and S_{i+1} are isomorphic.
- It may also be assumed that $m \geq 4$, since $m < 4$ reduces to the Abelian case.

The theorem is trivial for $n \leq 3$ and an easy CAYLEY excercise for $n = 4$ and 5. The three cases for each $n \geq 6$ will be proved by obtaining bounds on m and constructing the maximal order T and A given these bounds. The result will be that H $\cong$ G.

$n = 3k + 4$: $G \cong D_4 \times Z_3^k$

Consider the order of the conjectured group, G,

$$|G| = 8 \cdot 3^k = 8 \cdot 3^{\frac{n-4}{3}} = \frac{8}{3^{4/3}} \cdot 3^{n/3} \geq (1.84) \cdot 3^{n/3}. \quad (1)$$

Now use Lemmas 1 and 2 to bound the order of H, using the fact that T and A use m and $n - m$ symbols, respectively.

$$|H| = |T| \cdot |A| \leq (2 \cdot 2^{m/2}) \cdot (3^{\frac{n-m}{3}}) = 2 \cdot (\frac{2^{1/2}}{3^{1/3}})^m \cdot 3^{n/3} \leq 2 \cdot (.981)^m \cdot 3^{n/3}. \quad (2)$$

Combining (1) and (2) with the fact that $|H| \geq |G|$ yields

$$\begin{aligned} & 2 \cdot (.981)^m \cdot 3^{n/3} \geq (1.84) \cdot 3^{n/3} \\ \Rightarrow \quad & (.981)^m \geq 0.92 \\ \Rightarrow \quad & m \leq 4. \end{aligned}$$

But, it was assumed that $m \geq 4$, so $m = 4$. It follows from the empirical results and Theorem 2 that

$$m = 4 \Rightarrow T \cong D_4,$$

$$n - m = 3k \Rightarrow A \cong Z_3^k,$$

$$H \cong T \times A \Rightarrow H \cong D_4 \times Z_3^k.$$

$n = 3k + 5$: $G \cong D_4 \times Z_2 \times Z_2 \times Z_3^{k-1}$ *or* $D_4 \times Z_4 \times Z_3^{k-1}$ *or* $T_8 \times Z_3^{k-1}$

In this case, the order of the conjectured group, G, is

$$|G| = 8 \cdot 4 \cdot 3^{k-1} = 32 \cdot 3^{\frac{n-8}{3}} = \frac{32}{3^{8/3}} \cdot 3^{n/3} \geq (1.7) \cdot 3^{n/3}. \quad (3)$$

The bound on H remains the same as in the first case, so using (2) and (3) along with the fact that $|H| \geq |G|$ yields

$$\begin{aligned} & 2 \cdot (.981)^m \cdot 3^{n/3} \geq (1.7) \cdot 3^{n/3} \\ \Rightarrow \quad & (.981)^m \geq 0.85 \\ \Rightarrow \quad & m \leq 8. \end{aligned}$$

Thus, $m = 4, 6$, or 8. It can be shown via CAYLEY that there is no indecomposable, three-rewriteable two-group of degree six, so $m = 4$ or 8. Consider these two subcases.

(i) $m = 4 \Rightarrow T \cong D_4$,

$n - m = 3k + 1 \Rightarrow A \cong Z_2 \times Z_2 \times Z_3^{k-1}$ *or* $Z_4 \times Z_3^{k-1}$,

$H \cong T \times A \Rightarrow H \cong D_4 \times Z_2 \times Z_2 \times Z_3^{k-1}$ *or* $D_4 \times Z_4 \times Z_3^{k-1}$.

(ii) $m = 8 \Rightarrow T \cong T_8$,

$n - m = 3k - 3 = 3 \cdot (k-1) \Rightarrow A \cong Z_3^{k-1}$,

$H \cong T \times A \Rightarrow H \cong T_8 \times Z_3^{k-1}$.

$\underline{n = 3k + 6}$: $G \cong D_4 \times Z_2 \times Z_3^k$

The order of the conjectured group, G, is

$$|G| = 8 \cdot 2 \cdot 3^k = 16 \cdot 3^{\frac{n-6}{3}} = \frac{16}{9} \cdot 3^{n/3} \geq (1.77) \cdot 3^{n/3}. \tag{4}$$

Using (2) and (4) and the fact that $|H| \geq |G|$ yields

$$\begin{aligned} & 2 \cdot (.981)^m \cdot 3^{n/3} \geq (1.77) \cdot 3^{n/3}, \\ \Rightarrow\ & (.981)^m \geq .885, \\ \Rightarrow\ & m \leq 6. \end{aligned}$$

Again, $m = 6$ is impossible, so $m = 4$.

$m = 4 \Rightarrow T \cong D_4$,

$n - m = 3k + 2 \Rightarrow A \cong Z_2 \times Z_3^k$,

$H \cong T \times A \Rightarrow H \cong D_4 \times Z_2 \times Z_3^k$.

References

[1] R. Bercov and L. Moser, "On Abelian Permutation Groups," *Canad. Math. Bull.* 8 (1965) 627-630.

[2] J. Burns and B. Goldsmith, "Maximal Order Abelian Subgroups of Symmetric Groups," *Bull. London Math. Soc.* 21 (1989) 70-72.

[3] M. Curzio, P. Longobardi, and M. Maj, "Su di on problema combinatorio in teoria dei gruppi," *Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* 74 (1983) 136-142.

[4] D. Easdown and C. Praeger, "On Minimal Faithful Permutation Representations of Finite Groups," *Bull. Austral. Math. Soc.* 30 (1986) 207-220.

[5] M. Hoffman, "An Invariant of Finite Abelian Groups," *Amer. Math. Monthly* 94 (1987) 664-666.

[6] N. Itô, "On Finite Groups with Given Conjugate Types," *Nagoya Math. J.* 6 (1953) 17-28.

[7] L. Kovács and C. Praeger, "Finite Permutation Groups with Large Abelian Quotients," *Pacific J. Math.* 136 (1989) 283-292.

[8] M. Ljubich, "On the Logarithmic Property of a Degree of a Finite Group," *Publ. Math. Debrecen* 29 (1982) 73-78.