PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 96, Number 1, January 1986

ON THE UNIVERSALITY OF WORDS FOR THE ALTERNATING GROUPS

MANFRED DROSTE

ABSTRACT. We prove the following theorem on the finite alternating groups A_n: For each pair (p, q) of nonzero integers there exists an integer $N(p, q)$ such that, for each $n \geqslant N$, any even permutation $a \in A_n$ can be written in the form $a = b^p \cdot c^q$ for some suitable elements $b, c \in A_n$. A similar result is shown to be true for the finite symmetric groups S_n provided that p or q is odd.

1. Results. Let F be a free group and $W = W(x_1, \ldots, x_n) \in F$ a word in free variables $x_1, \ldots, x_n \in F$. For a group G, we say that W is G-universal if for any $g \in G$ the equation $g = W$ can be solved in G, i.e. there are $g_1, \ldots, g_n \in G$ such that $g = W(g_1, \ldots, g_n)$.

In [**14**], Silberger asked whether for each pair (p, q) of nonzero integers there exists an integer $N(p, q)$ such that the word $W = W(x, y) = x^p \cdot y^q$ is universal for each finite alternating group A_n with $n \geqslant N(p, q)$. For $p = q$ this was shown to be true in [**11**]. Ehrenfeucht et al. [**5**] proved that if both p and q are not divisible by 3, then W is A_n-universal for indeed any $n \in \mathbb{N}$.

In the following, if p, q are nonzero integers, we let $m(p, q) \in \mathbb{N}$ denote the product of all primes dividing $p \cdot q$, with the convention that $m(p, q) = 1$ if $p, q \in \{-1, 1\}$. Using a result of Bertram [**1**], we show that Silberger's question can in general be answered positively:

THEOREM 1. *Let p, q be nonzero integers and $W(x, y) = x^p \cdot y^q$. Then W is A_n-universal for any $n \geqslant 4m + 1$ where $m = m(p, q)$. Moreover, for any $n \geqslant \max\{4m + 1, 9\}$ there exists $l = l(n, m) \leqslant n - 2$ with the following property: For any $a \in A_n$ there are $b, c \in A_n$ such that $a = b^p \cdot c^q$, and b and c each consist only of one cycle of length l and $n - l$ fixed points; in particular, b and c are conjugate to each other in A_n.*

Note that the conjugacy class of the elements b, c in Theorem 1 is independent of the special choice of $a \in A_n$.

We remark that Silberger [**15**] also obtained, independently, that $W = x^p \cdot y^q$ is A_n-universal for all sufficiently large n. An essential improvement of the bound $4m + 1$ is contained in a forthcoming paper by Brenner, Evans and Silberger [**2**].

Received by the editors July 30, 1984.

1980 *Mathematics Subject Classification*. Primary 20D06; Secondary 20B30; 20F05.

Key words and phrases. Alternating groups, finite symmetric group, permutation groups, universal words, conjugacy classes.

As is well known, already Ito [**9**] and Ore [**12**] showed that any element of A_n ($n \geqslant 5$) can be expressed as a single commutator. This was reproved and strengthened by various authors, cf. e.g. Hsü Ch'eng-hao [**8**], Bertram [**1**]. As a first immediate consequence of Theorem 1 we obtain

COROLLARY 1. *Let $0 \neq p \in \mathbf{Z}$, $m = m(p, p)$ and $n \geqslant \max\{4m + 1, 9\}$. Then there exists a conjugacy class C in A_n such that for any $a \in A_n$ there exists elements $c \in C$, $b \in A_n$ satisfying $a = [c^p, b]$.*

Ehrenfeucht and Silberger [**6**] characterized all pairs (p, q) of integers for which $W = x^p \cdot y^q$ is universal for each finite symmetric group S_n ($n \in \mathbb{N}$). Of course, this is the case whenever both p and q are odd, since any permutation is a product of two involutions. Moreover, also for some, but not all, pairs (p, q) with p odd and q even, W is S_n-universal for each $n \in \mathbb{N}$. For instance, for any $2 \leqslant n \in \mathbb{N}$ the word $x^n \cdot y^{n!}$ is not universal for S_n. This situation is different if we consider "S_n-universality for each sufficiently large $n \in \mathbb{N}$":

THEOREM 2. *Let p, q be nonzero integers such that p or q is odd and $W = x^p \cdot y^q$. Then W is S_n-universal for any $n \geqslant \max\{4m - 4, 6\}$ where $m = m(p, q)$. Moreover, in this case, for any $a \in S_n$ there exist $b, c \in S_n$ such that $a = b^p \cdot c^q$ and b and c each consist only of precisely one nontrivial cycle (and, possibly, fixed points).*

Next we consider arbitrarily long and complex words which can be written as a product of three nontrivial words with disjoint sets of variables; here a word is called nontrivial if it does not reduce identically to 1. Using results of Hall [7] and Moran [**10**] we show

THEOREM 3. *Let $W_1 = W_1(x_1,\dots,x_p)$, $W_2 = W_2(y_1,\dots,y_q)$, $W_3 = W_3(z_1,\dots,z_r)$ be three nontrivial words in free pairwise different variables x_i, y_j, z_k, and $W = W(\mathbf{x}_i, \mathbf{y}_j, \mathbf{z}_k) = W_1 \cdot W_2 \cdot W_3$. Then there exists an $N \in \mathbb{N}$ such that, for each $n \geqslant \mathbb{N}$, A_n has the following property: For each $g \in A_n$ there are permutations a_i, b_j, $c_k \in A_n$ $(1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q, 1 \leqslant k \leqslant r)$ with orders all powers of 2 such that $g = W(\mathbf{a}_i, \mathbf{b}_j, \mathbf{c}_k)$. In particular, W is A_n-universal.*

P. Hall calls a group G W-elliptic of degree d, if any $g \in G$ is a product of at most d W-elements $W(g_1,\dots,g_n)$ with $g_1,\dots,g_n \in G$. (Hence W-ellipticity of degree 1 coincides, in the present notation, with universality of W.) As an immediate consequence of Theorem 3 we obtain

COROLLARY 2. *Let $W = W(x_1,\dots,x_m)$ be any nontrivial word. Then, for all sufficiently large $n \in \mathbb{N}$, A_n is W-elliptic of degree k for any $k \geqslant 3$.*

Here, as well as in Theorem 3, it remains an open problem whether the number 3 may be replaced by 2 or even by 1.

If M is an infinite set, we denote by S_M^0 the group of all permutations of M with finite support and by A_M the infinite alternating group on M, i.e. the (simple) group of all elements of S_M^0 which are, if restricted to their support, even permutations. As an obvious consequence of Theorems 1–3 we have

COROLLARY 3. *Let M be an infinite set.*

(a) *If W is a word of the kind described in Theorem* 1 *or in Theorem* 3, *then W is A_M-universal.*

(b) *If W is a word of the kind described in Theorem* 2, *then W is S_M^0-universal.*

For related results on this topic, in particular concerning universal words for infinite symmetric groups, we refer the reader to [**3**, **4**, **14**] and the literature cited there.

2. Proof of our results. As usual, we let $[x]$ denote the integer part of $x \in \mathbb{Q}$.

PROOF OF THEOREM 1. Since $n \geqslant 4m + 1$, an easy calculation shows that the interval $[[\frac{3}{4}n] - 1,\ n - 1]$ contains at least $m + 2$ elements, in particular some multiple M of m. Again by $n \geqslant 4m + 1$ (and $n \geqslant 9$ if $m = 1$), we can choose an odd number $l \in \{M - 2,\ M - 1,\ M + 1,\ M + 2\}$ (and possibly $l = M$ if $m = 1$) with $[\frac{3}{4}n] \leqslant l \leqslant n - 2$. Note that l is relatively prime with m. Now if $a \in A_n$, by Bertram [**1**] there exist two permutations $d, e \in S_n$, each consisting of precisely one cycle of length l and $n - l$ fixed points, such that $a = d \cdot e$. Since l is odd, we have $d, e \in A_n$, and since l, p and l, q are relatively prime, respectively, d^p and e^q each have again precisely one cycle of length l and are hence conjugate to d and e. Thus $d = b^p$, $e = c^q$ for some elements $b, c \in A_n$ which each have precisely one cycle of length l and $n - l \geqslant 2$ fixed points. As is well known (cf. [**13**, 11.1.5]), b and c are conjugate to each other in A_n. Since $a = d \cdot e = b^p \cdot c^q$, the result follows.

The following proof uses similar ideas as the previous one:

PROOF OF THEOREM 2. Assume $n \geqslant \max\{4m - 4, 6\}$. If $n \geqslant 9$, choose some multiple M of m in the interval $[[\frac{3}{4}n], n]$; if $n = 6\ (7, 8)$, let $M = 4\ (4, 6)$, respectively. Now let $a \in S_n$. If $a \in A_n$, choose $l \in \{M - 1,\ M + 1\}$ with $[\frac{3}{4}n] \leqslant l \leqslant n$. As in the proof of Theorem 1, we obtain $a = b^p \cdot c^q$ for some permutations $b, c \in S_n$ which have only one cycle of length l. Now assume $a \notin A_n$. Choose $l \in \{M - 2,\ M + 1\}$ such that $[\frac{3}{4}n] \leqslant l \leqslant n - 1$. We distinguish between two cases:

Case I. Assume p is even (hence q odd) and $l = M + 1$, or p is odd and $l = M - 2$. In this case, by Bertram [**1**, Corollary 3.1] there are $d, e \in S_n$ such that $a = d \cdot e$ and $d\ (e)$ consists only of one cycle of length $l\ (l + 1)$; note that l, p $(l + 1, q)$ are relatively prime, respectively.

Case II. Assume p is odd and $l = M + 1$, or p is even (hence q odd) and $l = M - 2$. Again by Bertram [**1**, Corollary 3.1], there are $d, e \in S_n$ such that $a = d \cdot e$ and $d\ (e)$ consists only of one cycle of length $l + 1\ (l)$; here $l + 1, p\ (l, q)$ are relatively prime, respectively.

In any case we can find permutations $b, c \in S_n$, each consisting only of one nontrivial cycle of length l or $l + 1$, such that $d = b^p$, $e = c^q$. Thus $a = d \cdot e = b^p \cdot c^q$ as claimed.

For the convenience of the reader, let us note two results of the literature which we will need for the proof of Theorem 3.

LEMMA 2.1 (HALL [7, LEMMA 7]). *Let $W = W(x_1,\dots,x_n)$ be any nontrivial word. Then there exists a finite 2-group G with elements $a_1,\dots,a_n \in G$ such that $a = W(a_1,\dots,a_n) \in G$ has order 2.*

LEMMA 2.2 (MORAN [**10**, THEOREM 0]). *Let $5 \leqslant n \in \mathbb{N}$ and $s \in S_n$ such that $s^2 = 1$ and s has l fixed points. Then each permutation in A_n is a product of three conjugates of s if and only if the following three conditions hold*:

(1) $l \equiv n \pmod 2$;

(2) $\frac{1}{2} \cdot (n - l) \equiv 0 \pmod 2$;

(3) $0 < l \leqslant \frac{1}{3}(n + 4)$ *if n is even, and* $0 < l \leqslant \frac{1}{3}(n + 2)$ *if n is odd.*

Now we give the

PROOF OF THEOREM 3. By Lemma 2.1, we can find a finite 2-group G with $|G| \geqslant 4$ and elements $a_i, b_j, c_k \in G$ $(1 \leqslant i \leqslant p, 1 \leqslant j \leqslant q, 1 \leqslant k \leqslant r)$ such that $a = W_1(\mathbf{a}_i)$, $b = W_2(\mathbf{b}_j)$, $c = W_3(\mathbf{c}_k)$ all have order 2 in G. We claim that $N = 3 \cdot |G| - 5$ satisfies the assertion of the theorem. Indeed, let $n \geqslant N$ and $g \in A_n$. Find $m, l \in \mathbb{N}$ with $m \cdot |G| + l = n$ and $1 \leqslant l \leqslant |G|$; then l, n satisfy conditions (1)–(3) of Lemma 2.2 since 4 divides $|G|$ and by our choice of N. Hence by Lemma 2.2 there are (conjugate) involutions $x, y, z \in S_n$, each having precisely l fixed points and hence $m \cdot |G|/2$ cycles of length 2, such that $g = x \cdot y \cdot z$.

Now embed $\varphi\colon G \hookrightarrow S_G$ via Cayley's right-regular representation. Then a_i^φ, b_j^φ, $c_k^\varphi \in S_G$ all have orders powers of 2 and satisfy $a^\varphi = W_1(\mathbf{a}_i^\varphi)$, $b^\varphi = W_2(\mathbf{b}_j^\varphi)$, $c^\varphi = W_3(\mathbf{c}_k^\varphi)$, where a^φ, b^φ, c^φ are permutations of G each consisting of $|G|/2$ cycles of length 2. By taking m copies of (G, S_G) and an additional set with l elements, we can construct permutations $d, e, f, d_i, e_j, f_k \in S_n$ such that $d = W_1(\mathbf{d}_i)$, $e = W_2(\mathbf{e}_j)$, $f = W_3(\mathbf{f}_k)$ each consist of $m \cdot |G|/2$ cycles of length 2 and l fixed points and d_i, e_j, f_k have the same orders as a_i^φ, b_j^φ, c_k^φ, respectively, and also l fixed points (in fact, we may perform our construction such that all these elements have identical fixed point sets), for $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, $1 \leqslant k \leqslant r$. Now x, y, z are conjugate to d, e, f, respectively. So we obtain $x = W_1(\mathbf{x}_i)$, $y = W_2(\mathbf{y}_j)$, $z = W_3(\mathbf{z}_k)$ for suitable conjugates $x_i, y_j, z_k \in S_n$ of d_i, e_j, f_k, respectively; thus x_i, y_j, z_k all have orders powers of 2. Hence $g = x \cdot y \cdot z = W(\mathbf{x}_i, \mathbf{y}_j, \mathbf{z}_k)$, as claimed.

REFERENCES

1. E. A. Bertram, *Even permutations as a product of two conjugate cycles*, J. Combin. Theory Ser. (A) **12** (1972), 368–380.

2. J. L. Brenner, R. J. Evans and D. M. Silberger, *The universality of words $x^r y^s$ in alternating groups*, Proc. Amer. Math. Soc. 96 (1986), 23–28.

3. M. Droste, *Classes of words universal for the infinite symmetric groups*, Algebra Universalis (to appear).

4. M. Droste and S. Shelah, *On the universality of systems of words in permutation groups*, Pacific J. Math. (to appear).

5. A. Ehrenfeucht, S. Fajtlowicz, J. Malitz and J. Mycielski, *Some problems on the universality of words in groups*, Algebra Universalis **11** (1980), 261–263.

6. A. Ehrenfeucht and D. Silberger, *Universal terms of the form B^nA^m*, Algebra Universalis **10** (1980), 96–116.

7. P. Hall, *Some constructions for locally finite groups*, J. London Math. Soc. **34** (1959), 305–319.

8. Hsü Ch'eng-hao, *The commutators of the alternating group*, Sci. Sinica **14** (1965), 339–342.

9. N. Itô, *A theorem on the alternating group* A_n $(n \geqslant 5)$, Math. Japon. **2** (1951), 59–60.

10. G. Moran, *Reflection classes whose cubes cover the alternating group*, J. Combin. Theory Ser. A **21** (1976), 1–19.

11. G. Moran and others, *Product of* p^m*th powers in* A_n, *solution of advanced problem* 6315, Amer. Math. Monthly **89** (1982), 705.

12. O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.

13. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964.

14. D. M. Silberger, *Are primitive words universal for infinite symmetric groups*?, Trans. Amer. Math. Soc. **276** (1983), 841–852.

15. D. M. Silberger, *For k big the word* $x^m y^n$ *is universal for* A_k, Abstracts Amer. Math. Soc. **3** (1982), 293.

FACHBEREICH 6, MATHEMATIK, UNIVERSITÄT GHS ESSEN, 4300 ESSEN 1, FEDERAL REPUBLIC OF GERMANY