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

THE UNIVERSALITY OF WORDS $x^r y^s$ IN ALTERNATING GROUPS

J. L. BRENNER, R. J. EVANS AND D. M. SILBERGER

ABSTRACT. If r, s are nonzero integers and m is the largest squarefree divisor of rs, then for every element z in the alternating group A_n, the equation $z = x^r y^s$ has a solution with $x, y \in A_n$, provided that $n \geqslant 5$ and $n \geqslant (5/2)\log m$. The bound $(5/2)\log m$ improves the bound $4m + 1$ of Droste. If $n \geqslant 29$, the coefficient 5/2 may be replaced by 2; however, 5/2 cannot be replaced by 1 even for all *large* n.

1. Introduction. For a group G, a word $W(x_1, \ldots, x_k)$ in free variables $x_1, \ldots, x_k$ is said to be G-universal if $G \subset W(G, \ldots, G)$, i.e., if for every $g \in G$, there exist $g_1, \ldots, g_k \in G$ such that $g = W(g_1, \ldots, g_k)$. Let A_n denote the alternating group contained in the symmetric group S_n on $\{1, \ldots, n\}$. For each pair of nonzero integers r, s, let $m = m(r, s)$ denote the product of the distinct prime factors of rs. It is known [**6**, Theorem 1; **9**] that the word $x^r y^s$ is A_n-universal for all $n \geqslant 4m + 1$. In Theorem 3, we show that the condition $n \geqslant 4m + 1$ may be replaced by the condition $n \geqslant (5/2)\log m$ if $n \geqslant 5$, and even by the condition $n \geqslant 2\log m$ if $n \geqslant 29$. Cases $n < 29$ are treated separately in Theorem 2. Theorem 1 is used to show that Theorem 2 is "best possible". In Theorem 3', we show that the bound $2\log m$ for $n \geqslant 29$ cannot be replaced by $\log m$, even just for $n \geqslant N_0$; however, $2\log m$ can be replaced by $C\log m$ for any constant $C > 8/5$, provided that $n \geqslant N_0(C)$.

2. Statements of theorems.

THEOREM 1. *Let n, a, b be positive integers with $n \geqslant 7$ and $a + b < 2[3n/4]$, where $[x]$ denotes the integer part of x. If $n \equiv 0$ or $1 \pmod 4$, let w be any product of $2[n/4]$ disjoint 2-cycles in S_n, and if $n \equiv 3 - \varepsilon \pmod 4$ with $\varepsilon = 0$ or 1, let w be any product of $2[n/4] - \varepsilon$ disjoint 2-cycles with a disjoint $(3 + \varepsilon)$-cycle in S_n. Then w does not equal a product of an a-cycle and a b-cycle in S_n.*

REMARK. Theorem 1 is best possible in the sense that, for each n, the symbol $<$ cannot be replaced by $\leqslant$. For, if $a = b = [3n/4]$, then by [**1**, or **3**, Corollary 2.10], every element of A_n is a product of two b-cycles in S_n.

THEOREM 2. *Let P_n denote the product of the distinct primes $\leqslant n$. For each $n \leqslant 28$, the word $x^r y^s$ is A_n-universal when $m < P_n/d_n$, where the values of d_n are given in*

Received by the editors January 15, 1985. Presented at the Western Number Theory Conference in Pacific Grove, California, December 22, 1985.

1980 *Mathematics Subject Classification*. Primary 20B35, 20F10; Secondary 10A25, 05A17.

the following table:

n	1,2	3,4	5,6,7,10,15	8,9,14	11,12,13	16,17,18	19,20,21	22,23	24,25	26	27,28
d_n	$0+$	2	1	5	7	11	$11 \cdot 13$	13	$13 \cdot 17$	17	$17 \cdot 19$

REMARK. Theorem 2 is best possible in the sense that, for each n, the symbol $<$ cannot be replaced by $\leqslant$. To see this, first suppose that $n = 3$ or 4. Then x^3y^3 is a word with $m = 3 = P_n/2$ which is not A_n-universal, since the 3-cycle (123) does not have the form x^3y^3. Next suppose that $n = 5, 6, 7, 10$, or 15. Then $x^{n!}y^{n!}$ is a word with $m = P_n/1$ which is not A_n-universal since $x^{n!}$ is trivial for all $x \in A_n$. If $n = 8$ or 9, then $x^{n!/5}y^{n!/5}$ is a word with $m = P_n/5$ which is not A_n-universal since, by Theorem 1 with $a = b = 5$, (12)(34)(56)(78) is not the product of two 5-cycles. The values of n in the ranges 11–13, 16–28 may be handled similarly. For example, if $n = 19$, then $x^{n!/143}y^{n!/143}$ is a word with $m = P_n/143$ which is not A_n-universal since, by Theorem 1, (12)(34)(56)(78)(9 10)(11 12)(13 14)(15 16)(17 18 19) is not the product of two 13-cycles nor two 11-cycles nor an 11-cycle times a 13-cycle. (Note that there is no element of order 143 in A_{19}.) Finally, suppose that $n = 14$. Then $x^{n!/25}y^{n!/25}$ is a word with $m = P_n/5$ which is not A_n-universal, for it is known [**4**] that (12)(34)(56)(78)(9 10)(11 12 13 14) is not the product of two elements of order 5 in A_{14}. (It is stated incorrectly in [**5**, p. 39] that for $n > 11$, every element of A_n is the product of two elements of order 5.)

THEOREM 3. *The word x^ry^s is A_n-universal for all $n \geqslant (5/2)\log m$ if $n \geqslant 5$. If $n \geqslant 29$, then x^ry^s is A_n-universal for all $n \geqslant 2\log m$.*

THEOREM 3′. *Let C be any constant exceeding $8/5$. For all $n \geqslant N_0(C)$, x^ry^s is A_n-universal whenever $n \geqslant C\log m$. On the other hand, it is not true that, for all $n \geqslant N_0$, every word x^ry^s is A_n-universal whenever $n \geqslant \log m$.*

3. Lemmas.

LEMMA 4. *Choose a positive integer b such that $[3n/4] \leqslant b \leqslant n$. Then every element of A_n is a product of two b-cycles in S_n.*

PROOF. This is easily checked for $n \leqslant 4$, and for $n \geqslant 5$, it follows from [**3**, Corollary 2.10].

LEMMA 5. *Choose integers $u, v \geqslant 4$ such that $[3n/4] + 1 \leqslant u + v \leqslant n$. Then every element of A_n is a product of two words, each of which is a product of a u-cycle and a disjoint v-cycle in S_n.*

PROOF. This follows from the proof of [**3**, Corollary 2.10] and from the theorem in [**3**, p. 168].

REMARK. On lines 13, 17, 19, 20 of [**3**, p. 168], replace misprints $q = 3$, 4.07, l, and η by $q - 3$, 4.09, $|l|$, and ηe, respectively.

LEMMA 6. *Let $n \geqslant 5$, and choose an integer v such that $[3n/4] - 1 \leqslant v \leqslant n - 2$. Then every element of A_n is a product of two words, each of which is a product of a 2-cycle and a disjoint v-cycle in S_n.*

PROOF. Apply [**3**, Theorem 3.02] and the proof of [**3**, Corollary 2.10].

LEMMA 7. *If every element of A_n is a product of two words in A_n, each of whose orders is prime to m, then $x^r y^s$ is A_n-universal.*

PROOF. Given $z \in A_n$, write $z = w_1 w_2$, where $w_i \in A_n$ has order e_i and $(m, e_i) = 1$ for $i = 1, 2$. Define R, S by $Rr \equiv 1 \pmod{e_1}$, $Ss \equiv 1 \pmod{e_2}$. Then $z = x^r y^s$ where $x = w_1^R$, $y = w_2^S$.

LEMMA 8. *Suppose that $2 \nmid m$. Then $x^r y^s$ is A_n-universal for all $n \geqslant 5$.*

PROOF. Assume that $x^r y^s$ is not A_n-universal. In view of Lemma 7, the desired contradiction will be obtained if one can apply Lemma 5 or 6 to show that every element of A_n is a product of two nontrivial words in A_n, each of order a power of 2. If $n = 5$, 6, or 7, apply Lemma 6 with $v = 2$, 4, or 4, respectively. Thus assume that $n \geqslant 8$. Define the integer c by $n/2 \leqslant 2^c < n$, and choose the largest integer d such that $2^c + 2^d \leqslant n$. If $d = 0$, then $n = 2^c + 1$, so apply Lemma 5 with $u = v = 2^{c-1}$. If $d = 1$, then $n = 2^c + 2$ or $2^c + 3$, so apply Lemma 6 with $v = 2^c$. If $d > 1$, we can apply Lemma 5 with $u = 2^c$, $v = 2^d$; to see that $u + v = 2^c + 2^d > 3n/4$, note that by definition of d, $2^{d+1} + 2^c > n$, so $2(2^c + 2^d) > n + 2^c \geqslant 3n/2$.

LEMMA 9. *If $3 \nmid m$, then $x^r y^s$ is A_n-universal for all $n \geqslant 1$.*

PROOF. This follows from [**7**, Proposition 2].

REMARK. An analogue of Lemmas 8 and 9 with the condition $5 \nmid m$ is given in [**4**]. It would be interesting to find an analogue for a general prime $p \nmid m$.

Let $x = n/8$. Let $p_1 < \cdots < p_\alpha$ denote the primes in the interval $(x, 2x]$, $P_1 < \cdots < P_\beta$ the primes in $(5x, 6x]$, $q_1 < \cdots < q_\gamma$ the primes in $(2x, 3x]$, and $Q_1 < \cdots < Q_\delta$ the primes in $(4x, 5x]$.

LEMMA 10. *Let $n \geqslant 5$. Suppose that $x^r y^s$ is not A_n-universal. Then $6|m$. Also, m is divisible by each prime in $(3n/4 - 1, n]$ and each prime in $(3n/8, n/2]$. Further, for each $i = 1, 2, \ldots, \min(\alpha, \beta)$, at least one of p_i, P_i divides m, and, for each $j = 1, 2, \ldots, \min(\gamma, \delta)$, at least one of q_j, Q_j divides m.*

PROOF. By Lemmas 8 and 9, we have $6|m$. If $p \in (3n/4 - 1, n]$ is a prime $\geqslant 5$, then in view of Lemma 7, one can apply Lemma 4 with $b = p$ to show that $p|m$. If $p \in (3n/8, n/2]$ is a prime $\geqslant 5$, apply Lemma 5 with $u = v = p$ to see that $p|m$. Finally, apply Lemma 5 with $u = p_i$, $v = P_i$ or $u = q_j$, $v = Q_j$ to complete the proof.

4. Proofs of theorems.

PROOF OF THEOREM 1. This follows easily from a beautiful result of Boccara [**2**, Theorem 4.1].

PROOF OF THEOREM 2. Assume that $x^r y^s$ is not A_n-universal. If $n = 1$ or 2, then A_n would be trivial, so $n \geqslant 3$. If $n = 3$ or 4, then $m \geqslant P_n/2 = 3$, because $3|m$ by Lemma 9. If n is in the range 5–14, then $m \geqslant P_n/d_n$, since P_n/d_n divides m by

Lemma 10. If $n = 16$, 17, or 18, then $P_n/5d_n = P_n/55$ divides m by Lemma 10. Moreover, one of 5, 11 also divides m by Lemma 5 with $u = 5$, $v = 11$. Thus, $m \geqslant P_n/11 = P_n/d_n$ if $n = 16$, 17, or 18, and the same type of argument shows that $m \geqslant P_n/d_n$ if $n = 22$, 23, or 26. Now suppose that $n = 19$, 20, or 21. Then $P_n/35d_n = P_n/(5 \cdot 7 \cdot 11 \cdot 13) = 19 \cdot 17 \cdot 3 \cdot 2$ divides m by Lemma 10. Moreover, 7 or 11 must divide m by Lemma 5 with $u = 7$, $v = 11$, and 5 or 13 must divide m by Lemma 5 with $u = 5$, $v = 13$. Thus $m \geqslant P_n/143 = P_n/d_n$ if $n = 19$, 20, or 21, and the same type of argument shows that $m \geqslant P_n/d_n$ if $n = 24$, 25, 27, or 28. Finally, suppose that $n = 15$. Then $P_n/5$ divides m by Lemma 10. It is known [**4**] that every element of A_{15} is a product of two elements of order 5 in A_{15}, so by Lemma 7, $x^r y^s$ would be A_{15}-universal if $5 \nmid m$. Thus $5 | m$. It follows that $P_n | m$, so $m \geqslant P_n = P_n/d_n$.

In the proofs below, we will use the number theoretic functions

$$\theta(x) = \sum_{p \leqslant x} \log p, \qquad \pi(x) = \sum_{p \leqslant x} 1,$$

where p runs through the primes $\geqslant 2$.

Proof of Theorem 3′. Assume that $x^r y^s$ is not A_n-universal. We will show that $\log m > n/C$ if $n \geqslant N_0(C)$. By Lemma 10,

$$\log m > \theta(n) - \theta(3n/4) + \theta(n/2) - \theta(3n/8) + \sum_{i=1}^{\min(\alpha,\beta)} \log p_i + \sum_{j=1}^{\min(\gamma,\delta)} \log q_j.$$

Thus,

$$\log m > \theta(n) - \theta(3n/4) + \theta(n/2) - \theta(3n/8) + \min(\alpha,\beta)\log(n/8) + \min(\gamma,\delta)\log(n/4), \tag{1}$$

where $\alpha = \pi(2n/8) - \pi(n/8)$, $\beta = \pi(6n/8) - \pi(5n/8)$, $\gamma = \pi(3n/8) - \pi(2n/8)$, $\delta = \pi(5n/8) - \pi(4n/8)$. Now apply the asymptotic formulas [**8**, p. 66] $\theta(n) \sim n$, $\pi(n) \sim n/\log n$ $(n \to \infty)$. Since $8/(5C) < 1$, it follows from (1) that, for $n \geqslant N_0(C)$,

$$\log m > \big(8/(5C)\big)\big(n/4 + n/8 + n/8 + n/8\big) = n/C.$$

This proves the first part of Theorem 3′.

Let n be any of the infinitely many integers for which $n \geqslant \theta(n)$ [**8**, p. 67]. Put $r = s = n!$. Then $\log m = \theta(n) \leqslant n$, yet $x^r y^s$ is not A_n-universal since x^r and y^s are trivial for all $x, y \in A_n$.

Proof of Theorem 3. Assume that $x^r y^s$ is not A_n-universal. We will first show that $\log m > n/2$ if $n \geqslant 29$. Write $x = n/8$. Then

$$\sum_{i=1}^{\min(\alpha,\beta)} \log p_i \geqslant \begin{cases} \theta(2x) - \theta(x) & \text{if } \alpha \leqslant \beta, \\ \beta \log x & \text{if } \alpha > \beta, \end{cases}$$

and

$$\sum_{j=1}^{\min(\gamma,\delta)} \log q_j \geqslant \begin{cases} \theta(3x) - \theta(2x) & \text{if } \gamma \leqslant \delta, \\ \delta \log 2x & \text{if } \gamma > \delta. \end{cases}$$

For brevity, write $\theta(i, j) := \theta(ix) - \theta(jx)$. Then, by (1),

$$\text{(2)} \qquad \log m > \begin{cases} \theta(8,6) + \theta(4,1) & \text{if } \alpha \leqslant \beta, \gamma \leqslant \delta, \\ \theta(8,6) + \theta(4,3) + \theta(2,1) + \delta \log 2x & \text{if } \alpha \leqslant \beta, \gamma > \delta, \\ \theta(8,6) + \theta(4,2) + \beta \log x & \text{if } \alpha > \beta, \gamma \leqslant \delta, \\ \theta(8,6) + \theta(4,3) + \delta \log 2x + \beta \log x & \text{if } \alpha > \beta, \gamma > \delta. \end{cases}$$

Case 1. $n > 10^8$. By [**8**, Theorems 9 and 10],

$$\theta(2,1) > (.98)(2x) - (1.02)x = .94x,$$

$$\theta(4,3) > .86x, \quad \theta(4,2) > 1.88x, \quad \theta(4,1) > 2.9x,$$

$$\theta(8,6) > 1.72x, \quad \theta(6,5) > .78x, \quad \theta(5,4) > .82x,$$

$$\beta \log x = (\log x)(\pi(6x) - \pi(5x)) > \frac{\log x}{\log 6x}(\theta(6x) - \theta(5x))$$

$$> \frac{\log(10^8/8)}{\log(6 \cdot 10^8/8)}(.78x) > .7x,$$

and

$$\delta \log 2x = (\log 2x)(\pi(5x) - \pi(4x)) > \frac{\log 2x}{\log 5x}(\theta(5x) - \theta(4x))$$

$$> \frac{\log(2 \cdot 10^8/8)}{\log(5 \cdot 10^8/8)}(.82x) > .77x.$$

Thus, in all four cases of (2), $\log m > 4x = n/2$.

Case 2. $7481 \leqslant n \leqslant 10^8$. By [**8**, Theorems 10 and 18],

$$\theta(2,1) > (.96)(2x) - x = .92x,$$

$$\theta(4,3) > .88x, \quad \theta(4,2) > 1.88x, \quad \theta(4,1) > 2.88x,$$

$$\theta(8,6) > 1.84x, \quad \theta(6,5) > .85x, \quad \theta(5,4) > .85x,$$

$$\beta \log x > \frac{\log x}{\log 6x}\theta(6,5) > \frac{\log 7481}{\log 6 \cdot 7481}(.85x) > .67x,$$

and

$$\delta \log 2x > \frac{\log 2x}{\log 5x}\theta(5,4) > \frac{\log 2 \cdot 7481}{\log 5 \cdot 7481}(.85x) > .75x.$$

Again by (2), $\log m > 4x = n/2$.

Case 3. $223 \leqslant n < 7481$. It is easily checked by computer that $\log m > n/2$ as a consequence of (2) and the fact that $6|m$ (see Lemma 10).

Case 4. $29 \leqslant n \leqslant 222$. Here one proceeds as in Case 3, except that judicious use of Lemmas 5 and 10 must also be made for several values of n. We illustrate with the most troublesome value, $n = 36$. By Lemma 10, m is divisible by $2 \cdot 3 \cdot 17 \cdot 29 \cdot 31$. By Lemma 5 with $n = 36$, $u = 5$, $v = 25$, m is divisible by 5. By Lemma 5 with $u = 13$, $v = 19$, m is divisible by one of 13, 19. Similarly, m is divisible by one of 13, 23, by one of 11, 19, by one of 11, 23, and by one of 7, 23. Thus m is divisible by $7 \cdot 11 \cdot 13$ (if $23 \nmid m$) or $23 \cdot 19$ or $23 \cdot 11$. In any event, $\log m > n/2 = 18$, since $\log(2 \cdot 3 \cdot 5 \cdot 11 \cdot 17 \cdot 23 \cdot 29 \cdot 31) > 18$.

Case 5. $5 \leqslant n \leqslant 28$. By Theorem 2, $\log m \geqslant \log P_n/d_n > 2n/5$, as claimed.

References

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

2. G. Boccara, *Décompositions d'une permutation d'un ensemble fini en produit de deux cycles*, Discrete Math. **23** (1978), 189–205.

3. J. L. Brenner, *Covering theorems for finite nonabelian simple groups*. IX, *How the square of a class with two nontrivial orbits in S_n covers A_n*, Ars Combin. **4** (1977), 151–176.

4. J. L. Brenner and R. J. Evans, *Even permutations as a product of two elements of order* 5, Preprint 1985.

5. J. L. Brenner and J. Riddell, *Noncanonical factorization of a permutation*, Amer. Math. Monthly **84** (1977), 39–40.

6. M. Droste, *On the universality of words for the alternating groups.* Proc. Amer. Math. Soc. 96 (1986), 18–22.

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

8. J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

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

10 Phillips Road, Palo Alto, California 94303 (J. L. Brenner)

Department of Mathematics C - 012, University of California, San Diego, La Jolla, California 92093 (R. J. Evans)

Department of Mathematics, State University of New York at New Paltz, New Paltz, New York 12561 (D. M. Silberger)

Department of Mathematics, Universidade de Santa Catarina, 88000 Florianópolis-SC, Brazil (D. M. Silberger)