

REPRESENTATIONS OF INFINITE PERMUTATIONS BY WORDS

JAN MYCIELSKI

ABSTRACT. We prove several cases of the following theorem: Every free group word which is not a proper power can represent every permutation of an infinite set. The remaining cases will be proved in a forthcoming paper of R. C. Lyndon.

F_X denotes a free group freely generated by the set X . The elements of X are called letters, and the elements of F_X are represented by reduced words in those letters. G denotes an arbitrary group.

We say that a word w can represent a in G if $a \in G$ and there exists a homomorphism $h: F_X \rightarrow G$ such that $h(w) = a$. In other words w can represent a in G iff the equation $w = a$ is solvable in G , where X is the set of unknowns.

Notice that, if ϕ is an endomorphism of F_X and $\phi(w)$ can represent a in G , then w can represent a in G . As was pointed out in [3], the sums of exponents of each letter of w have a greatest common divisor 1 iff w can represent every a in every G . This set of words with g.c.d. 1 is larger than the set of words w for which there exists an automorphism α of F_X such that $\alpha(w) \in X$. E.g., by a theorem of J. H. C. Whitehead (see [5]), the words $x^2yx^{-1}y^{-1}$ and x^2y^3 , for $x, y \in X$, are in the first set but not in the second set.

The solvability of equations $w = a$ for various groups G has been considered in several papers, see [2, 3, 4, 6, 7, 10]. In the present paper we will study this question for $G = S_Y$, the group of all permutations of an infinite set Y .

In [10] Silberger asks if every $w \in F_X$ which is not a power, i.e., is not of the form v^k with $k > 1$, can represent every π in S_Y , if Y is infinite. He shows that this is true if $w = x^m y^n$ for $x, y \in X$, $x \neq y$ and $m \neq 0 \neq n$. Another proof is given in [2]. (For finite Y sufficient conditions in terms of m and n were given in [4]). Our main result is the following partial solution of Silberger's problem (it was announced in [8]).

THEOREM 1. *If $w \in F_X$, w is not a power, $\pi \in S_Y$, and among the cycles of π at least one cycle size appears infinitely many times (fixed points are counted as cycles), then w can represent π in S_Y .*

REMARK ADDED IN MARCH 1986. R. C. Lyndon has just removed my assumption about the existence of repeating cycles in π . Thus Silberger's conjecture is true. My proof uses some rather difficult tools of combinatorial group theory (a theorem of Weinbaum about subwords of a relator and the asphericity theorem for Cayley complexes of groups with one relator) but Lyndon's addition is more direct. First he points out that Theorem 1 reduces the problem to the cases when $|Y| = \aleph_0$ and either π has at least one infinite cycle or π has no infinite cycles but

Received by the editors June 12, 1985 and, in revised form, October 1985 and March 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20F05; Secondary 20B07, 20E05.

©1987 American Mathematical Society
0002-9939/87 \$1.00 + \$.25 per page

it has finite cycles of arbitrarily large sizes. Then he settles both cases with the same clever construction.

REMARKS. 1. The case of Theorem 1 in which π has infinitely many fixed points and no more cycles than fixed points was proved first by R. C. Lyndon (unpublished) and the same proof was rediscovered later by the author. The present proof (Case 3) involves an additional idea. (It is easy to check that $xyx^{-1}y^{-1}$ can represent every even permutation of a finite set and every permutation of an infinite set (O. Ore), moreover, in this representation, x can be an involution. It is more tricky to represent the successor function in the form x^2y^2 (see [3]), and the theorem of Silberger [2, 10] about $x^m y^n$ is still harder.)

2. Of course we can assume without loss of generality that X consists of the letters which appear in w . Assume that $X = \{x_1, \dots, x_n\}$. Then the substitution $x_i \mapsto x^i y^i$ yields an isomorphism of F_X into $F_{\{x,y\}}$ which is pure, i.e., does not turn any nonpower into a power (a tedious exercise). Many other such isomorphisms are known since the commutator of $F_{\{x,y\}}$ is a pure subgroup and it is free of countable rank. Hence Theorem 1 reduces to the case where $X = \{x, y\}$.

3. The condition that w is not a power is essential. In fact π is a k th power iff for every $c \leq \aleph_0$ and every prime p dividing c , the number of cycles of π of size c is divisible by the largest power of p dividing k (a nice exercise). It follows that if, for every prime p , w can represent some π in some S_Y such that π consists of one cycle of size p and any number of fixed points, then w is not a power.

4. If Y is uncountable, then of course every $\pi \in S_Y$ satisfies the condition of Theorem 1. If π satisfies the condition of Theorem 1, then by elementary set theory one can partition Y into countable disjoint sets Y_i such that each Y_i consists of countably many cycles of π such that all except possibly one are of equal sizes. Therefore, by representing π restricted to Y_i in S_{Y_i} and joining those representations, Theorem 1 reduces to the case when Y is countable and π has countably many equal cycles and at most one cycle of a different size.

5. The case when there is no exceptional cycle, i.e., π consists of countably many cycles of the same size, say c , is very easy. We choose X such that $w \in F_X$ and $2 \leq |X| \leq \aleph_0$. In case $c = \aleph_0$ we look at the, say right, action of w upon F_X ; if $c < \aleph_0$, we look at the right action of w upon cosets aH , where $a \in F_X$ and H is the cyclic subgroup of F_X generated by w^c . In each case we get \aleph_0 cycles of size c .

6. It would be interesting to investigate the solvability of systems of two equations

$$u = a, \quad v = b,$$

in G , where $a, b \in G$, $u, v \in F_{\{x,y\}}$, and $uv \neq vu$, for various groups G . The groups $F_{\{x,y\}}$, S_Y , $GL_2(\mathbf{R})$, and $SO_3(\mathbf{R})$ are particularly interesting. Unfortunately nothing is known yet.

7. Let $G = PSL_2(\mathbf{R})$ or $SO_3(\mathbf{R})$, $u, v \in F_{\{x,y\}}$, and u does not commute with any conjugate of v . Problem: Does the range of the natural map

$$(u, v): G^2 \rightarrow G^2$$

contain an open set? The only known theorem related to this question is Theorem 1 in [0]. See also Problem 2, p. 263 in [9].

Our proof will be based on the concept of Cayley graphs and complexes. If G is a group and $x \mapsto \tilde{x}$ is a map of X into G , then for every $a \in G$ and $x \in X$ we create

an arrow $A(a, x)$ from a to $a\tilde{x}$. And x is called the *label* of $A(a, x)$. The whole graph will be called the Cayley graph of (G, \sim) . It is the “graph of action” of the labels x upon G . Of course \sim extends uniquely to a homomorphism $\sim : F_X \rightarrow G$.

Let e be the unity of G , and $v = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ be a fixed word of F_X , where $\epsilon_i = \pm 1$, such that $\tilde{v} = e$. Then for every $a \in G$ we have a loop $L(a)$ from $[0, 1]$ to a union of arows, with base point a , its arrows labeled consecutively by x_1, \dots, x_n and having varying directions determined by the ϵ_i 's. The image of this loop is denoted by $IL(a)$. The *Cayley complex* CG of G is obtained by spanning an n -gonal 2-cell over $IL(a)$ for each $a \in G$, obeying the natural ordering of edges of $L(a)$. Notice that if $v = w^m$, then $IL(a) = IL(a\tilde{w}^k)$ for each integer k , but, in agreement with the previous definition, the circuit $IL(a)$ gets only one 2-cell.

From now on we assume moreover that $v \in F_X$ is a *reduced* and *cyclically reduced* wod. N_v denotes the least normal subgroup of F_X containing v . We put $G = F_X/N_v$ and $\tilde{x} = xN_v$ for all $x \in X$. In this case our graph is called the Cayley graph of the presentation $\langle X, v \rangle$ and CG is called the Cayley complex of $\langle X, v \rangle$.

N_v may contain words which are shorter than v . E.g., if $v = tu^m$, then $uvu^{-1}v^{-1} \in N_v$, but, for large m , $uvu^{-1}v^{-1}$ can be much shorter than v . So G may have circuits shorter than n . Still the following theorem holds.

THEOREM 2 (C. M. WEINBAUM [11]). *No nonempty proper subword of v nor of any cyclic conjugate of v is in N_v . In other words, the vertices*

$$a, a\tilde{x}_1^{\epsilon_1}, \dots, a\tilde{x}_1^{\epsilon_1} \cdots \tilde{x}_{n-1}^{\epsilon_{n-1}}$$

are all distinct from each other. In still other words, $IL(a)$ is a simple closed curve consisting of n arrows.

We shall also use the following important theorem.

THEOREM 3 (D. E. Cohen and R. C. Lyndon, see [5, Chapter III, Proposition 11.1]; or I. M. Chiswell et al. [1]). *The complex CG is aspherical. In other words $\pi_n(CG) = 0$, for $n = 1, 2, \dots$*

(The part $\pi_1(CG) = 0$ is an easy exercise, and, by the theorem of Hurewicz, $\pi_2(CG) = H_2(CG)$, but $H_2(CG) = 0$ is not easy. Since CG is 2-dimensional, $\pi_1(CG) = \pi_2(CG) = 0$ imply $\pi_n(CG) = 0$ for $n > 2$.)

In connection with this material we mention an open problem about the Cayley graphs.

PROBLEM. *Is $IL(a) \cap IL(b)$ connected (or empty) for every $a, b \in G$?*

Let P be obtained from CG by removing the interior of the 2-cell of $IL(e)$.

LEMMA. *$\pi_1(P)$ is an infinite cyclic group and $L(e)$ represents its generator.*

We will deduce this from Theorem 3. First, every loop L with base point e consisting of edges of P corresponds to a word of N_v and hence one which is a product of a sequence whose terms are v, v^{-1} and their conjugates. Each loop with base point e corresponding to any term $uv^\epsilon u^{-1}$ of this product is homotopic to $(L(\tilde{u}))^\epsilon$ and hence either it is nulhomotopic in P or $IL(\tilde{u}) = IL(e)$. Hence L is homotopic to a power of $L(e)$.

Second, since $\pi_2(CG) = 0$, for $m = 1, 2, \dots$, the loop $(L(e))^m$ is not nulhomotopic in P . \square

PROOF OF THEOREM 1. By Remarks 4 and 5 we can assume that π consists of countably many cycles of size c , $c \leq \aleph_0$, and one exceptional cycle of size $k \neq c$, $k \leq \aleph_0$. By the remarks at the beginning of this paper we can assume that w is reduced and cyclically reduced relative to the basis X . Thus Theorems 2, 3 and the Lemma are true for $v = w^c$ (if $c < \aleph_0$).

Case 1. $c = \aleph_0$. We take the Cayley graph T of F_X (which is a tree). Let $w^k = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ in reduced form, where $x_i \in X$ and $\varepsilon_i = \pm 1$. We cut the arrow joining $x_1^{\varepsilon_1} \cdots x_{n-1}^{\varepsilon_{n-1}}$ to w^k and remove the connected part of T which contains w^k . We cut the arrow which connects $x_n^{-\varepsilon_n}$ to e and remove the connected part of T which contains $x_n^{-\varepsilon_n}$. We add an arrow between e and $x_1^{\varepsilon_1} \cdots x_{n-1}^{\varepsilon_{n-1}}$ with label x_n which points into e if $\varepsilon_n = 1$ and away from e if $\varepsilon_n = -1$. It is clear that, since w is not a power, the action of w upon the set of vertices of this graph according to the labeled arrows has one cycle of size k (e is an element of that cycle) and \aleph_0 cycles of size \aleph_0 .

Case 2. $k = \aleph_0$. (This part of the proof is very similar to the argument of Lyndon quoted in Remark 1. It could be easily extended to all the cases when c divides k .) Let $v = w^c$ and P be defined as above (prior to the Lemma), by means of v . Let $f: Q \rightarrow P$ be a simply connected covering of P . By the Lemma each fiber $f^{-1}(p)$, for $p \in P$, is infinite. We lift to Q all the vertices, arrows, 2-cells and labels of P . Those arrows define the action of F_X upon the vertices of Q . By the Lemma it is clear that $f^{-1}(e)$ is an infinite cycle under the action of v . Hence the set $C = f^{-1}(\{\tilde{w}^i | i = 0, 1, \dots, c-1\})$ is an infinite cycle under the action of w . Let p be a vertex of Q , $p \notin C$. Then $IL(f(p))$ has a 2-cell D in P (recall that if $p \in C$, then $IL(f(p)) = IL(e)$ and the interior of the 2-cell of $IL(e)$ is missing in P). Let D' be a 2-cell of Q such that $f(D') = D$ and p is on the boundary of D' . It is clear from our definition of the arrows of Q that, under the action of w , p marches around the boundary of D' and its trajectory is a cycle of size c .

Thus the action of w upon the vertices of Q has one cycle of size \aleph_0 and \aleph_0 cycles of size c .

Case 3. $c, k < \aleph_0$. First we build P and Q with their vertices, labeled arrows and 2-cells in the same way as in Case 2. Recall that the arrows of CG were defined by means of multiplication on the right. Hence multiplication on the left preserves the arrows, their labels, and the 2-cells of CG ; thus F_X under left action is a group of automorphisms of CG . Notice also that multiplication on the left by \tilde{w} preserves $IL(e)$. (In general it does not preserve $IL(a)$.) Hence w can be interpreted as an automorphism of Q of order \aleph_0 . (Also an automorphism of CG and of P of order c .)

We will define an equivalence relation \equiv over the vertices of Q , which naturally extends to a label-preserving equivalence among the arrows and 2-cells of Q . Namely $a \equiv b$ iff there exists an integer r such that

$$w^{kr}a = b.$$

We form the factor Q/\equiv . It is clear that Q/\equiv carries a structure of labeled arrows and 2-cells similar to that of Q .

We can see in the same way as in Case 2 that multiplication on the right (i.e. chasing the arrows of Q/\equiv) by w turns the set $f^{-1}(\{\tilde{w}^i | i = 0, \dots, c-1\})/\equiv$ into a

cycle of size k , and every vertex of Q/\equiv which is not in that cycle belongs to a cycle of size c . Since F_X/N_w is infinite, there are \aleph_0 such vertices.

This concludes the proof of Theorem 1.

REFERENCES

0. A. Borel, *On free subgroups of semisimple groups*, Enseign. Math. **29** (1983), 151–164.
1. I. M. Chiswell, D. J. Collins and J. Huebschmann, *Aspherical group presentations*, Math. Z. **178** (1981), 1–36.
2. M. Droste, *Classes of universal words in the infinite symmetric groups*, Algebra Universalis **20** (1985), 205–216.
3. A. Ehrenfeucht, S. Fajtlowicz, J. Malitz and J. Mycielski, *Some problems on the universality of words in groups*, Algebra Universalis **11** (1980), 261–263.
4. A. Ehrenfeucht and D. M. Silberger, *Universal terms of the form $B^n A^m$* , Algebra Universalis **10** (1980), 96–116.
5. R. C. Lyndon and P. E. Shupp, *Combinatorial group theory*, Springer-Verlag, 1977.
6. J. Mycielski, *Can one solve equations in groups?*, Amer. Math. Monthly **84** (1977), 723–726.
7. —, *Equations unsolvable in $GL_2(C)$ and related problems*, Amer. Math. Monthly **85** (1978), 263–265.
8. —, *Representations of permutations by words*, Abstracts Amer. Math. Soc. **5** (1984), 473.
9. J. Mycielski and S. Wagon, *Large free groups of isometries and their geometrical uses*, Enseign. Math. **30** (1984), 247–267.
10. D. M. Silberger, *Are primitive words universal for infinite symmetric groups?*, Trans. Amer. Math. Soc. **276** (1983), 841–852.
11. C. M. Weinbaum, *On relators and diagrams*, Illinois J. Math. **16** (1972), 308–322.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER, COLORADO
80309-0426