PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 1, September 1992

A SHORT PROOF OF A THEOREM OF ADJAN

LOUXIN ZHANG

(Communicated by Warren J. Wong)

ABSTRACT. In this note, using the technique of rewriting, we give a short proof of a theorem of Adjan: the word problem is decidable for special one-relator monoids $(A;\ w = e)$.

The word problem for one-relator monoids is still open, in spite of the fact that the word problem for one-relator groups has been solved positively by Magnus [2]. A general result on the word problem for one-relator monoids is the following one due to Adjan [1]:

Theorem 1. *The word problem is decidable for special one-relator monoids* $(A;\ w = e)$.

Let A be a finite set, and let A^* be the free monoid generated by A, the identity of which is denoted by e. If $x, y \in A^*$, by $x = y$ we mean that x and y are the same element. Let R be a relation of A^*. The reduction $\to_R^*$ induced by R is the reflexive, transitive closure of the relation $\to_R$ defined by $u \to_R v$ iff $\exists x, y \in A^*$, $(l, r) \in R$ such that $u = xly$, $v = xry$. By $\leftrightarrow_R^*$ we denote the symmetric, transitive closure of $\to_R^*$, which is the smallest congruence containing R. Let $w \in A^*$, the special one-relator monoid $M = (A;\ w = e)$ is the quotient of A^* by $\leftrightarrow_R^*$, where $R = \{(w, e)\}$.

A relation R on A^* is called *Noetherian* if there exists no infinite sequence of reductions of the form $u_1 \to_R u_2 \to_R \cdots$; it is called *confluent* if for any $x, y \in A^*$ such that $x \leftrightarrow_R^* y$, $x \to_R^* z$ and $y \to_R^* z$ for some $z \in A^*$.

If a relation R on A^* is Noetherian and confluent, then each congruence class $[w]_R = \{u \in A^* | u \leftrightarrow_R^* w\}$ of w mod R contains exactly one element $\overline{w}$ such that there exists no element v satisfying $\overline{w} \to_R v$. Define $\overline{w}$ to be the *norm form* of w. Thus, if R is Noetherian and confluent and there is an algorithm to find the norm form for each element in A^*, then the word problem is decidable for the monoid $A^*/\leftrightarrow_R^*$ since $x = y$ in $A^*/\leftrightarrow_R^*$ iff $\overline{x}$ and $\overline{y}$ are identical.

Given a special one-relator monoid $M = (A;\ w = e)$, we construct a sequence of sets C_i as follows:

$C_1 = \{w\}$,

$C_{i+1} = C_i \cup \{xy | x \in W(C_i) \,\&\, yx \in C_i\} \cup \{zx | x \in W(C_i) \,\&\, xz \in C_i\}$,

for $i \geq 1$, where $W(C_i)$ denotes the set of all elements that are both left and

Received by the editors November 20, 1990 and, in revised form, February 11, 1991.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20M05, 03D03, 03D40.

right factors of elements of C_i. Obviously, $C_1 \subseteq C_2 \subseteq \cdots \subseteq C_i \subseteq C_{i+1} \subseteq \cdots$. On the other hand, for all elements $u \in C_j$, u has the same length as w. Thus, there exists k such that $C_k = C_{k+j}$ for $j \geq 1$. Denote the set of elements in $W(C_k)$ such that no proper right factor of them are in $W(C_k)$ by $E(M)$.

Proposition 1. *Let $x, y, z \in A^*$ and $M = (A; w = e)$ be a special one-relator monoid. Then*

(1) $xy, yz \in E(M) \Rightarrow y = e$ *or* $x = z = e$;

(2) $xy, yz \in E(M)^* \Rightarrow y \in E(M)^*$.

Proof. (1) Let $xy, yz \in E(M)$. Suppose $y \neq e$. Then, since $xy \in E(M)$, there exists $H \in A^*$ such that $Hxy \in C_k$. Symmetrically, there exists $F \in A^*$ such that $yzF \in C_k$; so, $y \in W(C_k)$. Since $xy \in E(M)$, $y \in W(C_k)$ implies $xy = y$ and so $x = e$. Similarly, $z = e$.

(2) Let $xy, yz \in E(M)^*$. Suppose $xy = x_1 x_2 \cdots x_k$, where $x_j \in E(M)$ for each j. Then $y = x_i'' x_{i+1} \cdots x_k$ for some nonempty right factor x_i'' of x_i. Since $yz = x_i'' x_{i+1} \cdots x_k z \in E(M)^*$, there is a $c \in E(M)$ that overlaps with x_i'', say $c = c_1 c_2$ and $x_i'' = v c_1$, where $c_1 \neq e$ and $c_2, v \in A^*$. Since $x_i = x_i' x_i'' = x_i' v c_1$ and $c = c_1 c_2$, $c_1 \neq e$ implies $x_i' v = e$ by (1) and so $y \in E(M)^*$. □

Let $E(M) = \{x_1, x_2, \ldots, x_n\}$. Introduce an alphabet B in bijection with $E(M)$ (say, through φ: $E(M) \to B$). Since w is a product of elements in $E(M)$, $\varphi(w)$ is defined. We say that the monoid presentation $(B; \varphi(w) = e)$ is obtained from the monoid presentation $(A; w = e)$ by the technique of rewriting. Let $s \in E(M)$ and $w = st$ for some $t \in A^*$, then $t \in E(M)^*$ and $ts \leftrightarrow^*_{\{(w,e)\}} e$; so $\varphi(t)\varphi(s) \leftrightarrow^*_{\{(\varphi(w),e)\}} e$. Thus, the presentation $(B; \varphi(w) = e)$ presents a one-relator group, say G.

Using the set $E(M)$ and the group G, we define a relation $R = R(M)$ over A^* in the following way:

$$R = \{(u, v) | u, v \in E(M)^*: u > v \,\&\, \varphi(u) = \varphi(v) \text{ in } G\},$$

where $<$ is a linear order defined by: $x < y$ iff $|x| < |y|$ or $|x| = |y|$ and $x <_{\text{lex}} y$. Here $<_{\text{lex}}$ denotes the lexicographical order on A^* induced by a given linear order on A.

Lemma 1. *Let $u \in A^*$ with $|u| < k = \max_{x \in E(M)} |x|$. Then u is irreducible* mod R, *i.e., there is no $v \in A^*$ such that $u \to_R v$.*

Proof. Let $u \in A^*$ with $|u| < k$. Suppose u is not irreducible mod R. Then, there are $u', u'' \in A^*$ and $x, y \in E(M)^*$ such that $u = u'xu''$ and $(x, y) \in R$. Since $|y| \leq |x| < k$, at least the letter corresponding to the word in $E(M)$ with the maximum length k does not occur in both $\varphi(x)$ and $\varphi(y)$, so by Freiheitssatz for one-relator groups [3], $\varphi(x) = \varphi(y)$ in G implies $\varphi(x) = \varphi(y)$, which in turn implies $x = y$ from Proposition 1(1), a contradiction. □

Proposition 2. *Let $T = \{(w, e)\}$. Then R is Noetherian, confluent, and equivalent to T, i.e., $\leftrightarrow^*_R = \leftrightarrow^*_T$.*

Proof. Since $<$ is a linear ordering on A^*, since this ordering is compatible with the product in A^* and since $u > v$ for each $(u, v) \in R$, R must be Noetherian.

To show R is confluent, we use Theorem 1 in [4]. For condition (1), let (xy, p), (yz, q) be two rules in R. Since $xy, yz \in E(M)^*$, by Proposition 1, $x, y, z \in E(M)^*$. Thus $xq, pz \in E(M)^*$. On the other hand, $\varphi(xq) = \varphi(x)\varphi(q) =_G \varphi(x)\varphi(yz) = \varphi(xy)\varphi(z) =_G \varphi(p)\varphi(z) = \varphi(pz)$. Since $<$ is a linear ordering, $xq = pz$, $xq < pz$, or $pz < xq$. Then, by the definition of R, either (xq, pz) or (pz, xq) must be a rule in R, or else $xq = pz$. For condition (2), if (xyz, p) and (y, q) are two rules in R, since $xyz \in E(M)^*$ and $y, q \in E(M)^*$, by Proposition 1, we have either (1) $x, y, z \in E(M)^*$ or (2) $x = c_1c_2\cdots c_sF$ and $z = Hd_1d_2\cdots d_t$ and $FyH \in E(M)$ for some $F, H \in A^+ = A^* - \{e\}$.

Case (1). We have $xqz \in E(M)^*$, $\varphi(xqz) = \varphi(x)\varphi(q)\varphi(z) =_G \varphi(x)\varphi(y)\varphi(z) =_G \varphi(p)$. So either (xqz, p) or (p, xqz) must be rule in R or $xqz = p$.

Case (2). Since $F, H \in A^+$, $|y| < k = \max_{x\in E(M)} |x|$, by Lemma 1, which implies y is irreducible mod R, a contradiction.

Therefore, R is confluent.

Since $w \in E(M)^*$ and $\varphi(w) = e$ in G, we have $(w, e) \in R$, i.e., $T \subseteq R$. On the other hand, for each rule $(u, v) \in R$, $\varphi(u) = \varphi(v)$ in G implies $u \leftrightarrow_T^* v$, so $\leftrightarrow_R^* \subseteq \leftrightarrow_T^*$. Hence R is equivalent to T. □

Proof of Theorem 1. Let M be a special one-relator monoid $(A; w = e)$. Since R is Noetherian, confluent and equivalent to $T = \{(w, e)\}$, given two elements $u, v \in A^*$, in order to decide whether $u = v$ in M, i.e., $u \leftrightarrow_T^* v$, we need only to find the norm forms $\overline{u}$ and $\overline{v}$ mod R of u and v respectively, and then compare $\overline{u}$ to $\overline{v}$. If $\overline{u}$ and $\overline{v}$ are identical, then $u \leftrightarrow_T^* v$; otherwise, $u \not\leftrightarrow_T^* v$.

Since G is a one-relator group, it has a decidable word problem. So, given two elements $x, y \in E(M)^*$, such that $x > y$, whether or not $\varphi(x) =_G \varphi(y)$ can be decided. Note that there are only finitely many words in $E(T)^*$ less than x w.r.t. $<$. Thus we can find $\overline{u}$ and $\overline{v}$ in a finite number of steps. Therefore the word problem is decidable for M. □

Acknowledgment

The author thanks the referee for a detailed report, which was very helpful in preparing the final version of this note.

References

1. S. Adjan, *Defining relations and algorithmic problems for groups and semigroups*, Trudy Mat. Inst. Steklov **85** (1966); English. transl. in Proc. Steklov. Inst. Math. **85** (1966).
2. W. Magnus, *Das identity problem fur grouppen mit einer definierenden relation*, Math. Ann. **106** (1932), 295–307.
3. W. Magnus, A. Karrass, and D. Solitar, *Combinatorial group theory*, Wiley, New York, 1966.
4. R. McNaughton and P. Narendran, *Special monoids and special Thue systems*, J. Algebra **108** (1987), 248–255.

Department of Pure Mathmatics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Department of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1