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 \(\rightarrow^*_R\) induced by \(R\) is the reflexive, transitive closure of the relation \(\rightarrow_R\) defined by \(u \rightarrow_R v\) 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 \(\rightarrow^*_R\), 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 \(u_1 \rightarrow_R u_2 \rightarrow_R \cdots\); it is called confluent if for any \(x, y \in A^*\) such that \(x \leftrightarrow_R^* y\), \(x \rightarrow_R^* z\) and \(y \rightarrow_R^* z\) 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 \(\overline{w} \rightarrow_R v\). 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
right factors of elements of \( C_j \). 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 \( xy = x_1x_2\cdots x_k \), where \( x_j \in E(M) \) for each \( j \). Then \( y = x_1''x_{i+1}\cdots x_k \) for some nonempty right factor \( x_i'' \) of \( x_i \). Since \( yz \in x_1''x_{i+1}\cdots x_kz \in E(M)^* \), there is a \( c \in E(M) \) that overlaps with \( x_1'' \), say \( c = c_1c_2 \) and \( x_i'' = vc_1 \), where \( c_1 \neq e \) and \( c_2, v \in A^* \). Since \( x_i = x_1''x_{i}'' = x_1''vc_1 \) and \( c = c_1c_2 \), \( c_1 \neq e \) implies \( x_1''v = e \) by (1) and so \( y \in E(M)^* \). \( \square \)

Let \( E(M) = \{x_1, x_2, \ldots, x_n\} \). Introduce an alphabet \( B \) in bijection with \( E(M) \) (say, through \( \phi: E(M) \rightarrow B \)). Since \( w \) is a product of elements in \( E(M) \), \( \phi(w) \) is defined. We say that the monoid presentation \( (B; \phi(w) = e) \) 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 \( ts \leftrightarrow^*_T(e) \); so \( \phi(t)\phi(s) \leftrightarrow^*_T(\phi(w), e) \). Thus, the presentation \( (B; \phi(w) = e) \) 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:

\[ R = \{(u, v) | u, v \in E(M)^* : u > v \& \phi(u) = \phi(v) \in G\}, \]

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 \( u \_R v \).

**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 \( \phi(x) \) and \( \phi(y) \), so by Freiheitssatz for one-relator groups \([3] \), \( \phi(x) = \phi(y) \) in \( G \) implies \( \phi(x) = \phi(y) \), which in turn implies \( x = y \) from Proposition 1(1), a contradiction. \( \square \)

**Proposition 2.** Let \( T = \{\langle w, e \rangle\} \). 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, $x, y, z \in E_iM)^*$. 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, $xq = pz$ or $xq < pz$, 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) $x = c_1c_2\cdots c_tF$ 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 $\langle A; w = e \rangle$. 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 $\bar{u}$ and $\bar{v}$ mod $R$ of $u$ and $v$ respectively, and then compare $\bar{u}$ to $\bar{v}$. If $\bar{u}$ and $\bar{v}$ are identical, then $u \leftrightarrow^*_T v$; otherwise, $u \leftrightarrow^*_T v$.

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 $\bar{u}$ and $\bar{v}$ 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


DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA, N2L 3G1

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA, N2L 3G1