COMMUNICATIONS IN ALGEBRA, 25(12), 4023–4028 (1997)

FINITE COMPLETE REWRITING SYSTEMS FOR GROUPS

Deko V. Dekov
Zahari Knjazeski 81
6000 Stara Zagora
Bulgaria

1 Introduction

A finite complete rewriting system R for a group G gives a simple solution to the word problem for the group G as follows: Two words are equivalent if and only if their R-irreducible forms (often called normal forms, or canonical forms) are the same.

In recent years, the Knuth-Bendix completion procedure has been used for creating finite complete rewriting systems for many groups and classes of groups. For an overview see, e.g., N. Dershowitz [5].

In the present paper we give a finite complete rewriting system for the fundamental group of the surface $S^2\#gT\#n\mathbb{R}P^2$, where $g \geq 1$, $n \geq 0$ (Proposition 1), a finite complete rewriting system for the torus knot group (Proposition 2), and new proofs of the termination of the finite complete rewriting systems for the Greendlinger group, due to F. Otto [16] and Ph. Le Chenadec [12] (Propositions 3 and 4).

2 Preliminaries

The reader is referred to [2] or [1] for a survey on string-rewriting systems.

Let X be a set and let X^* be the free monoid on X, the empty word of which is denoted by 1. The length of a word w in X^* is denoted by $|w|$. A *rewriting system* (or a *string-rewriting system*) on X is a subset R of $X^* \times X^*$. An element $(l, r) \in R$, also written $l \to r$, is called a *rule* of R.

Henceforth we call an irreflexive and transitive binary relation an *ordering*. If $>$ is an ordering, then $u \geq v$ means that either $u > v$ or $u = v$.

Let $u, v \in X^*$ and let $\triangleright$ be a well-founded ordering on X, called a *precedence* on X. Define the *recursive path ordering from the left* (RPO-L, for short) as follows: $u >_{\mathrm{RPO-L}} v$ iff $u \neq 1$ and $v = 1$ or $u = au'$, $v = bv'$, $a, b \in X$, $u', v' \in X^*$ and one of the following three conditions holds:

(i) $a \triangleright b$ and $au' >_{\text{RPO-L}} v'$.
(ii) $a = b$ and $u' >_{\text{RPO-L}} v'$.
(iii) $u' \geq_{\text{RPO-L}} bv'$.

Let R be a rewriting system on X and let $>$ be an ordering on X^*. The ordering $>$ is called *compatible* with R if $l > r$ for each rule $(l \to r) \in R$.

Given a monoid M, a rewriting system R on X is called a *rewriting system for* M if

$$\text{mon}(X; l = r \text{ where } (l \to r) \in R)$$

is a presentation for M. A rewriting system for a group G is a rewriting system for G as a monoid.

The terminology used in the theorems below can be found, e.g., in [3, Section 2].

Theorem A (Dershowitz [4]). *The recursive path ordering from the left is a reduction ordering.*

Theorem B (Lankford [11]). *A rewriting system R on X is terminating if and only if there exists a reduction ordering on X^* which is compatible with R.*

Theorem C (Newman [14]). *Let R be a terminating rewriting system. Then R is confluent if and only if all critical pairs of R are resolved.*

Theorem D (Newman [14]). *If R is a complete rewriting system for a group G, then there exists exactly one R-irreducible word representing each element of G.*

A rewriting system R on X is *finite* if both X and R are finite sets. If R is a finite complete rewriting system for a group G, then, by Theorem D, R gives a simple solution to the word problem for G as follows: two words are equivalent if and only if their R-irreducible forms are the same.

3 Surface groups

In 1986, Ph. Le Chenadec [12, Chap. 6, Section 2] (see also [13]) gave a finite complete rewriting system for the fundamental group of a closed orientable surface of genus g,

$$\Phi_g = \langle A_1, A_2, \ldots, A_{2g};\ A_1 A_2 \ldots A_{2g} A_1^{-1} A_2^{-1} \ldots A_{2g}^{-1} = 1 \rangle.$$

In 1992, S. M. Hermiller [7] (see also [8]) gave a new finite complete rewriting system for Φ_g based on the usual presentation

$$\Phi_g = \langle a_1, \ldots, a_g, b_1, \ldots, b_g;\ a_1 b_1 a_1^{-1} b_1^{-1} \ldots a_g b_g a_g^{-1} b_g^{-1} = 1 \rangle.$$

Let $v \in X^* - \{1\}$ and $u \in X^*$. Define $\#(v, 1) = 0$, and for $v = x_1 x_2 \ldots x_m$, $u = y_1 y_2 \ldots y_n$, $m, n \geq 1$, define

$$\#(v, u) = \text{card}(\{(i_1, \ldots, i_m) \ : \ i_1 < i_2 < \ldots < i_m,\ y_{i_k} = x_k,\ k = 1, 2, \ldots, m\}).$$

E.g., $\#(ab, acb) = 1$ and $\#(ab, aabb) = 4$. Clearly, if $a \in X$, then $\#(a, u)$ denotes the number of occurrences of the letter a in the word u. We use the notation $\#(v, u)$ from U. Martin [15].

We shall use the method of S. M. Hermiller [8] to give a finite complete rewriting system for the group $G = \langle A;\ aba^{-1}b^{-1}w = 1\rangle$, where A is a finite set, $a, b \in A$, and w is a word such that $\#(x, w) = 0$, for $x \in \{a, b, a^{-1}, b^{-1}\}$. The main special cases of the group G are the fundamental group Φ of the surface $S^2\#gT\#n\mathbb{R}P^2$, $g \geq 1$, $n \geq 0$,

$$\Phi = \langle a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots, c_n; \quad a_1b_1a_1^{-1}b_1^{-1} \ldots a_gb_ga_g^{-1}b_g^{-1}c_1^2 \ldots c_n^2 = 1\rangle,$$

(See C. Kosniowski [10, Theorem 26.1]), the group Φ_g, and the free abelian group on two generators, $F = \langle a, b;\ ab = ba\rangle$.

As in J. M. Howie [9, p. 104], $C(u)$ denotes the *content* of the word $u \in X^* - \{1\}$, i.e., the set of elements of X occuring in u. We define $C(1) = \emptyset$.

Define the rewriting system

$$R(G) = \{xx^{-1} \to 1, x^{-1}x \to 1, \text{ for all } x \in A,$$
$$ab \to w^{-1}ba, a^{-1}b^{-1} \to b^{-1}a^{-1}w^{-1}, ab^{-1} \to b^{-1}wa, a^{-1}w^{-1}b \to ba^{-1}\}.$$

Notice that if

$$A = \{a, a_2, \ldots, a_g, b, b_2, \ldots, b_g\} \text{ and } w = a_2b_2a_2^{-1}b_2^{-1} \ldots a_gb_ga_g^{-1}b_g^{-1},$$

then $R(G)$ coincides with the rewriting system R' due to S. M. Hermiller [8, p. 142]. The recursive path ordering from the left defined by the precedence

$$a \rhd a^{-1} \rhd b \rhd b^{-1} \rhd \cdots \rhd a_g \rhd a_g^{-1} \rhd b_g \rhd b_g^{-1},$$

used by Hermiller [8, p. 141] to prove the termination of R' is an extension to a total ordering of the recursive path ordering from the left, defined in the proof of Proposition 1.

Proposition 1. *$R(G)$ is a finite complete rewriting system for the group G.*

Proof. It is routine to verify that $R(G)$ is a rewriting system for the group G.

The rewriting system $R(G)$ is terminating. Indeed, let $>_{\mathrm{RPO-L}}$ denote the recursive path ordering from the left defined by the precedence $a \rhd x$, for all $x \in C(w)$, $a \rhd b$, $a \rhd b^{-1}$, $a^{-1} \rhd b$, $a^{-1} \rhd b^{-1} \rhd y$, for all $y \in C(w^{-1})$. Then $>_{\mathrm{RPO-L}}$ is compatible with the rewriting system $R(G)$. Hence, by Theorems A and B, $R(G)$ is terminating.

The rewriting system $R(G)$ is confluent. Indeed, $R(G)$ does not have any inclusion ambiguities. A straightforward verification shows that all critical pairs of $R(G)$ arising from overlap ambiguities, are resolved. Hence, by Theorem C, $R(G)$ is confluent.

$R(G)$ is complete, since it is terminating and confluent. Proposition 1 is proved.

We shall define a new simple ordering which proves the termination of $R(G)$. A similar ordering was defined by B. Benninghofen, S. Kemmerich and M. M. Richter [1, p. 211]. We use the abbreviation BKRO for the Benninghofen-Kemmerich-Richter ordering. Let $>$ denote the usual ordering on $\mathbb{N}$, and let $>_{\mathrm{Lex-L}}$ denote the lexicographic ordering from the left on 4-tuples of nonnegative integers, induced by $>$.

Denote

$$\begin{aligned} V_a(u) &= \#(a,u) + \#(a^{-1},u), \\ V_b(u) &= \#(b,u) + \#(b^{-1},u), \\ V(u) &= \#(ab,u) + \#(a^{-1}b,u) + \#(ab^{-1},u) + \#(a^{-1}b^{-1},u). \end{aligned}$$

Define

$$u >_{\mathrm{BKRO}} v \quad \text{iff} \quad (V_a(u), V_b(u), V(u), |u|) >_{\mathrm{Lex-L}} (V_a(v), V_b(v), V(v), |v|).$$

It is easy to verify that $>_{\mathrm{BKRO}}$ is a reduction ordering which is compatible with $R(G)$. E.g., if $x \in A - \{a,b\}$, then $xx^{-1} >_{\mathrm{BKRO}} 1$, since

$$(0,0,0,2) >_{\mathrm{Lex-L}} (0,0,0,0),$$

$aa^{-1} >_{\mathrm{BKRO}} 1$, since

$$(2,0,0,2) >_{\mathrm{Lex-L}} (0,0,0,0),$$

and $ab^{-1} >_{\mathrm{BKRO}} b^{-1}wa$, since

$$(1,1,1,2) >_{\mathrm{Lex-L}} (1,1,0,2+|w|).$$

Hence, by Theorem B, $R(G)$ is terminating.

4 The torus knot group

In 1994, J. Pedersen and M. Yoder [17] gave a finite complete rewriting system for the braid group $B_3 = \langle a,b,c;\ a^3 = b^2 = c\rangle$. We shall use the method of Pedersen and Yoder [17] to give a finite complete rewriting system for the torus knot group $G = \langle a,b,c;\ a^n = b^m = c\rangle$, where $m,n > 1$. (See C. Kosniowski [10, Theorem 27.4]).

Define the rewriting system

$$R(G) = \Big\{ cc^{-1} \to 1, c^{-1}c \to 1, a^{-1} \to c^{-1}a^{n-1}, b^{-1} \to c^{-1}b^{m-1}, \\ a^n \to c, b^m \to c, ac \to ca, ac^{-1} \to c^{-1}a, bc \to cb, bc^{-1} \to c^{-1}b\Big\}.$$

Notice that if $n = 3$ and $m = 2$, then $R(G)$ coincides with the rewriting system T for B_3 due to Pedersen and Yoder [17].

Proposition 2. *$R(G)$ is a finite complete rewriting system for the group G.*

Proof. In order to prove the termination of $R(G)$, we use the recursive path ordering from the left defined by the precedence $a^{-1} \triangleright a \triangleright c$, $a \triangleright c^{-1}$, $b^{-1} \triangleright b \triangleright c$, $b \triangleright c^{-1}$. The rest of the proof is similar to the proof of Proposition 1.

5 The Greendlinger group

In 1960, M. Greendlinger [6] proved that the Dehn's algorithm cannot solve the word problem for the group $G = \langle a,b,c;\ abc = cba\rangle$. In 1984, F. Otto [16] gave a finite complete rewriting system $R_1(G)$ for the Greendlinger group G. The rewriting system $R_1(G)$ is defined as follows:

$$R_1(G) = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, cc^{-1} \to 1, c^{-1}c \to 1,$$
$$ac^{-1} \to b^{-1}c^{-1}ab, a^{-1}b^{-1} \to c^{-1}b^{-1}a^{-1}c, abc \to cba, a^{-1}cb \to bca^{-1}\}.$$

We shall give a new proof of the termination of $R_1(G)$.

Proposition 3. *The rewriting system $R_1(G)$ is terminating.*

Proof. Let $>_{\mathrm{RPO-L}}$ be the recursive path ordering from the left defined by the precedence $a \rhd b^{-1} \rhd c$, $a \rhd c^{-1}$, $a^{-1} \rhd c^{-1} \rhd b$, $a^{-1} \rhd b^{-1}$. Then the ordering $>_{\mathrm{RPO-L}}$ is compatible with $R_1(G)$. Hence, by Theorems A and B, $R_1(G)$ is terminating. Proposition 3 is proved.

In 1986, Ph. Le Chenadec [12, Chap. 6, Section 2] gave another finite complete rewriting system $R_2(G)$ for the Greendlinger group G. The rewriting system $R_2(G)$ is defined as follows:

$$R_2(G) = \{aa^{-1} \to 1, a^{-1}a \to 1, bb^{-1} \to 1, b^{-1}b \to 1, cc^{-1} \to 1, c^{-1}c \to 1,$$
$$cba \to abc, bca^{-1} \to a^{-1}cb, b^{-1}a^{-1}c \to ca^{-1}b^{-1}, a^{-1}b^{-1}c^{-1} \to c^{-1}b^{-1}a^{-1},$$
$$ac^{-1}b^{-1} \to b^{-1}c^{-1}a, c^{-1}ab \to bac^{-1}\}.$$

Notice that the four standard orderings, namely, the weight-plus-lexicographic ordering from the left, the weight-plus-lexicographic ordering from the right, the recursive path ordering from the left and the recursive path ordering from the right, are not compatible with $R_2(G)$.

We shall give a new proof of the termination of $R_2(G)$.

Proposition 4. *The rewriting system $R_2(G)$ is terminating.*

Proof. We shall define a new simple ordering which proves the termination of $R_2(G)$. A similar ordering was defined by U. Martin [15, Example 5]. We use the abbreviation MO for the Martin ordering. Let $>$ denote the usual ordering on $\mathbb{N}$ and let $>_{\mathrm{Lex-L}}$ denote the lexicographic ordering from the left on 7-tuples of nonnegative integers, induced by $>$. Denote

$$\#(ca, u) + \#(ba^{-1}, u) + \#(b^{-1}c, u) + \#(a^{-1}c^{-1}, u) + \#(ab^{-1}, u) + \#(c^{-1}b, u).$$

by $V(u)$. Define $u >_{\mathrm{MO}} v$ iff

$$(\#(a,u), \#(b,u), \#(c,u), \#(a^{-1},u), \#(b^{-1},u), \#(c^{-1},u), V(u)) >_{\mathrm{Lex-L}}$$
$$(\#(a,v), \#(b,v), \#(c,v), \#(a^{-1},v), \#(b^{-1},v), \#(c^{-1},v), V(v)).$$

It is easy to verify that $>_{\mathrm{MO}}$ is a reduction ordering which is compatible with $R_2(G)$. E.g., $a^{-1}a >_{\mathrm{MO}} 1$, since $(1,0,0,1,0,0,0) >_{\mathrm{Lex-L}} (0,0,0,0,0,0,0)$ and $cba >_{\mathrm{MO}} abc$, since $(1,1,1,0,0,0,1) >_{\mathrm{Lex-L}} (1,1,1,0,0,0,0)$. Hence, by Theorem B, $R_2(G)$ is terminating. Proposition 4 is proved.

References

[1] B. Benninghofen, S. Kemmerich and M. M. Richter, *Systems of Reductions*, Lecture Notes in Computer Science, Vol. **277**, Springer, Berlin, 1987.

[2] D. E. Cohen, String rewriting—a survey for group theorists, in *Geometric Group Theory, Vol. 1* (ed. G. A. Niblo and M. A. Roller) London Mathematical Society Lecture Note Series, **181**, Cambridge University Press, 1993, pp. 37–47.

[3] D. V. Dekov, Free products with amalgamation of monoids, *J. Pure Appl. Algebra*, to appear.

[4] N. Dershowitz, Orderings for term-rewriting systems, *Theoret. Comput. Sci.* **17** (1982), 279–301.

[5] N. Dershowitz, Rewriting methods for word problems, in *Words, Languages and Combinatorics* (ed. M. Ito) World Scientific, Singapore, 1992, pp. 104–118.

[6] M. Greendlinger, Dehn's algorithm for the word problem, *Comm. Pure Appl. Math.* **13** (1960), 67–83.

[7] S. M. Hermiller, *Rewriting Systems for Coxeter Groups*, Ph. D. Thesis, Cornell University, 1992.

[8] S. M. Hermiller, Rewriting systems for Coxeter groups, *J. Pure Appl. Algebra* **92** (1994), 137–148.

[9] J. M. Howie, *An Introduction to Semigroup Theory*, Academic Press, London, 1976.

[10] C. Kosniowski, *A First Course in Algebraic Topology*, Cambridge University Press, 1980.

[11] D. S. Lankford, *Some approaches to equality for computational logic: A survey and assessment*, Report ATP-36, Department of Mathematics and Computer Science, University of Texas at Austin, 1977.

[12] Ph. Le Chenadec, *Canonical Forms in Finitely Presented Algebras*, Pitman, London and Wiley, New York, 1986.

[13] Ph. Le Chenadec, A catalogue of complete group presentations, *J. Symbolic Comput.* **2** (1986), 363–381.

[14] M. H. A. Newman, On theories with a combinatorial definition of "equivalence" *Ann. of Math.* **43** (1942), 223–243.

[15] U. Martin, *On the diversity of orderings on strings*, Report CS 93/13, University of St. Andrews, Scotland, 1993.

[16] F. Otto, Finite complete rewriting systems for the Jantzen monoid and the Greendlinger group, *Theoret. Comput. Sci.* **32** (1984), 249–260.

[17] J. Pedersen and M. Yoder, Term rewriting for the conjugacy problem and the braid groups, *J. Symbolic Comput.* **18** (1994), 563–572.

Received: January 1997

Revised: May 1997