J. Symbolic Computation (1988) **6**, 99–104

The Word Problem for Free Partially Commutative Groups

C. WRATHALL

Department of Mathematics, University of California, Santa Barbara, CA 93106, U.S.A.

(*Received* 6 *February* 1987)

A linear-time algorithm is given for the word problem for free partially commutative groups. The correctness of the algorithm follows from the fact that certain Thue systems, presenting such groups, are preperfect.

1. Introduction

A finitely generated free partially commutative group can be specified by its finite set of generators Σ_0 along with a binary relation θ_0 on Σ_0 that contains the pairs of generators that commute. This corresponds to the presentation $\langle \Sigma_0; \{ab = ba : (a, b) \in \theta_0\}\rangle$. Such a group can be presented as a monoid by adding (in the usual way) formal inverses for the generators, and using the relations to express both the properties of the inverses and the partial commutativity. It is shown here that if partial commutativity is specified completely in the presentation, then the monoid presentation is preperfect as a Thue system. As a consequence, for a finitely presented free partially commutative group there is a linear-time algorithm to produce a 'projected' normal form of a given word, as a tuple of words over certain subsets of the original alphabet. From this projected normal form one can construct a shortest word equivalent to the given word; also, a pair of projected normal forms can be easily compared, to solve the word problem for the group in linear time. Using another notion of projection, Duboc (1986*b*, section 2.4) has described a different algorithm for the word problem, which can also be implemented in linear time.

On one hand, these results are an application of recent work on the algebraic properties of free partially commutative monoids (Cori & Perrin, 1985; Duboc, 1985, 1986), especially the device of translating between a free partially commutative monoid and a certain product of free monoids. On the other hand, they are a special case of questions about rewriting systems; Diekert (1987), for example, gives a quadratic-time algorithm for the word problem for certain systems of rewriting in partially commutative monoids.

2. Preliminary Definitions and Notation

For a set S, $\bar{S}$ denotes the complement of S (with respect to the appropriate universe) and $|S|$ denotes the cardinality of S.

For a finite set of letters (alphabet) A, A^* denotes the free monoid generated by A. The empty word, the identity element of the free monoid, is denoted by e. The length of word

This research was supported in part by the National Science Foundation under Grant No. CCR-8706976.

0747–7171/88/040099+06 $03.00/0

x, $|x|$, is the number of occurrences of symbols in x, with $|e| = 0$. For a word $x \in A^*$ and letter $a \in A$, $|x|_a$ denotes the number of occurrences of the letter a in x.

A Thue system T on an alphabet Σ is a set of pairs of words, $T \subseteq \Sigma^* \times \Sigma^*$. For u, $v \in \Sigma^*$, $u \longleftrightarrow v$ if there is some rule $(x, y) \in T$ such that, for some r and s, either $u = rxs$ and $v = rys$, or $u = rys$ and $v = rxs$. The congruence $\overset{*}{\longleftrightarrow}$ generated by T is the reflexive and transitive closure of $\longleftrightarrow$; the congruence class of $u \in \Sigma^*$ is $[u] = \{v : u \overset{*}{\longleftrightarrow} v\}$. The Thue system T is a presentation of the quotient monoid of Σ^* by $\overset{*}{\longleftrightarrow}$.

If $u \longleftrightarrow v$, then write $u \vdash\!\dashv v$ if $|u| = |v|$, $u \rightarrow v$ if $|u| > |v|$, and $u \vdash\!\rightarrow v$ if $|u| \geqslant |v|$. Let $\overset{*}{\vdash\!\dashv}$, $\overset{*}{\rightarrow}$ and $\overset{*}{\vdash\!\rightarrow}$ denote the reflexive transitive closures of $\vdash\!\dashv$, $\rightarrow$ and $\vdash\!\rightarrow$, respectively.

A Thue system is *preperfect* if whenever words u and v are congruent there is some word w such that $u \overset{*}{\vdash\!\rightarrow} w \overset{*}{\leftarrow\!\dashv} v$. An equivalent condition (Cochet & Nivat, 1971) is that if $u \overset{*}{\leftarrow\!\dashv} z \overset{*}{\vdash\!\rightarrow} v$ then, for some w, $u \overset{*}{\vdash\!\rightarrow} w \overset{*}{\leftarrow\!\dashv} v$. A Thue system is *almost-confluent* if u congruent to v implies that, for some x and y, $u \overset{*}{\rightarrow} x \overset{*}{\vdash\!\dashv} y \overset{*}{\leftarrow} v$. This is a stricter condition than preperfect, since all the reductions must be performed first, rather than being mixed with length-preserving rules. It is decidable whether a (finite) Thue system is almost-confluent (Nivat & Benois, 1971), but undecidable whether it is preperfect (Narendran & McNaughton, 1984).

The following proposition gives a convenient sufficient condition for a system to be preperfect.

PROPOSITION. (*Narendran & McNaughton*, 1984, *theorem* 1.2). *Suppose a Thue system has the property that whenever* $x \leftarrow u \overset{*}{\vdash\!\dashv} v \rightarrow y$, *there is some* t *such that* $x \overset{*}{\vdash\!\rightarrow} t \overset{*}{\leftarrow\!\dashv} y$. *Then the Thue system is preperfect.*

3. Free Partially Commutative Groups

Suppose that Σ_0 is an alphabet and θ_0 is a partial commutativity relation on Σ_0: a binary relation that is symmetric and irreflexive. Let $\Sigma_1 = \{\bar{a} : a \in \Sigma_0\}$ be a set of formal inverses for the letters in Σ_0, and $\Sigma = \Sigma_0 \cup \Sigma_1$. For notational convenience, if d is $\bar{a} \in \Sigma_1$ then $\bar{d} = a$. Let $\theta \subseteq \Sigma \times \Sigma$ be the extension of θ_0 to Σ: $\theta = \{(a, b), (\bar{a}, b), (a, \bar{b}), (\bar{a}, \bar{b}) : (a, b) \in \theta_0\}$. The subject of the following development is the Thue system T_0 on Σ, where

$$T_0 = \{(a\bar{a}, e), (\bar{a}a, e) : a \in \Sigma_0\} \cup \{(cd, dc) : (c, d) \in \theta\}.$$

The Thue system T_0 presents the free partially commutative group $G(\theta_0)$, and, in a sense, it is the 'natural' presentation of $G(\theta_0)$ as a monoid.

If θ_0 is empty, then $G(\theta_0)$ is just the free group on the generators Σ_0, and if θ_0 contains every pair of distinct letters, then $G(\theta_0)$ is the free abelian group on Σ_0. Between these two extremes any choice of pairs of commuting letters in Σ_0 can be made, although (as a consequence of the first set of rules) the letters a and $\bar{a}$ will always commute. That relation is not included in the second set of rules, i.e. a letter and its inverse commute 'actually' but not 'formally'.

Some of the rules in the second set specifying T_0 are redundant, since, for example, if $(a, b) \in \theta_0$ then both (ab, ba) and $(a\bar{b}, \bar{b}a)$ are included. This redundancy is necessary if the presentation is to be preperfect: if $(ab, ba) \in T_0$, then $a\bar{b}$ is congruent to $\bar{b}a$ (via $a\bar{b} \leftarrow \bar{b}ba\bar{b} \vdash\!\dashv \bar{b}ab\bar{b} \rightarrow \bar{b}a$), so for $a\bar{b} \overset{*}{\vdash\!\rightarrow} w \overset{*}{\leftarrow\!\dashv} \bar{b}a$ to hold for some w, it must be the case that $a\bar{b} \overset{*}{\vdash\!\dashv} \bar{b}a$.

The Thue system T_0 is not almost-confluent (unless θ_0 is empty): if $(a, b) \in \theta_0$ (i.e. a and b are two positive letters that commute), then $ab\bar{a}$ is congruent to b, but no length-decreasing rule applies to $ab\bar{a}$ since b is neither a nor $\bar{a}$. Hence the relation $ab\bar{a} \xrightarrow{*} x \overset{*}{\vdash\!\dashv} y \xleftarrow{*} b$ does not hold for any x and y.

A very useful representation of free partially commutative monoids is as products of certain free monoids. The alphabets for the free monoids can be found by collecting together noncommuting letters, as follows.

Let $A_1, \ldots, A_p$ be a collection of subsets of Σ that cover Σ and have the following properties: for all $a, b \in \Sigma$

(i) for all i, $a \in A_i$ if $\bar{a} \in A_i$;
(ii) if $(a, b) \in \bar{\theta}$, then, for some j, A_j contains both a and b;
(iii) if, for some i, A_i contains both a and b, then $(a, b) \in \bar{\theta}$.

For example, the collection might consist of each four-element set $\{a, \bar{a}, b, \bar{b}\}$ for $(a, b) \in \bar{\theta}_0 (a \neq b$ in $\Sigma_0)$, together with the two-element sets $\{a, \bar{a}\}$ for those letters a that commute with all the other letters. Another choice, used by Duboc (1986, 1987), is to take the collection of 'maximal cliques' (i.e. maximally non-commuting sets of letters) of $\bar{\theta}_0$ and add the appropriate inverses to each one. If θ_0 is empty, then $p = 1$ and $A_1 = \Sigma$ will satisfy the conditions; if θ_0 contains all pairs of distinct letters then (essentially) the only collection that will serve is $\{\{a, \bar{a}\} : a \in \Sigma_0\}$.

For each i, let $\pi_i : \Sigma^* \to A_i^*$ be the projection of Σ onto A_i, that is, the homomorphism determined by defining $\pi_i(a) = a$ for $a \in A_i$ and $\pi_i(a) = e$ for $a \in \bar{A}_i$. Property (ii), above, ensures that, for any string x and letter a, if $a \in A_i$ implies $\pi_i(x) = e$, then all the letters in x commute with a.

Let $\Pi : \Sigma^* \to A_1^* \times \ldots \times A_p^*$ be the function defined by $\Pi(w) = [\pi_1(w), \ldots, \pi_p(w)]$. The set $A_1^* \times \ldots \times A_p^*$ forms a monoid under componentwise concatenation, and Π is a monoid homomorphism. Since the length-preserving rules of T_0 express a partial commutativity relation on Σ, we have the following correspondence between the quotient of Σ^* by $\overset{*}{\vdash\!\dashv}$ and $A_1^* \times \ldots \times A_p^*$.

LEMMA 1. *(Cori & Perrin, 1985; Duboc, 1986a). For all $u, v \in \Sigma^*$, $u \overset{*}{\vdash\!\dashv} v$ if and only if $\Pi(u) = \Pi(v)$.*

Free reduction in the group corresponds to the following reduction relation on $A_1^* \times \ldots \times A_p^*$. The correspondence is given in lemma 2, which also shows that the reduction on $A_1^* \times \ldots \times A_p^*$ has a local confluence property, when restricted to the range of Π.

DEFINITION. For tuples $\mathbf{s}, \mathbf{t} \in A_1^* \times \ldots \times A_p^*$, $\mathbf{s}$ *reduces to* $\mathbf{t}$ (in one step), written $\mathbf{s} \to \mathbf{t}$, if, for some $a \in \Sigma$ and some $k \geq 0$, for each i,

(i) if $a \in \bar{A}_i$ then $t_i = s_i$; and
(ii) if $a \in A_i$ then $s_i = u_i a \bar{a} v_i$, $t_i = u_i v_i$ and $|u_i|_a = k$.

Let $\xrightarrow{*}$ denote the reflexive, transitive closure of this relation. Call $\mathbf{s}$ *irreducible* if there is no $\mathbf{t}$ such that $\mathbf{s} \to \mathbf{t}$.

In this definition, the restriction that the deleted pair occur 'in the same position' in each component is necessary for the desired correspondence; that is, performing free reduction in the components independently may lead to incorrect results. Consider, for example, $\Sigma_0 = \{a, b, c\}$ and $\theta_0 = \{(a, b), (b, a)\}$, with $A_1 = \{a, \bar{a}, c, \bar{c}\}$ and $A_2 = \{b, \bar{b}, c, \bar{c}\}$. The word $w = \bar{c}acb\bar{c}\bar{a}c\bar{b}$ is a shortest word in its congruence class, and, in particular, is not congruent to the empty word, but $\pi_1(w) = \bar{c}ac\bar{c}\bar{a}c \xrightarrow{*} e$ and $\pi_2(w) = \bar{c}cb\bar{c}c\bar{b} \xrightarrow{*} e$. (This example is due to K. Zeger.)

LEMMA 2.

(i) *For all* $u, v \in \Sigma^*$, *if* $u \to v$ *then* $\Pi(u) \to \Pi(v)$.

(ii) *For all* $u \in \Sigma^*$ *and* $\mathbf{x} \in A_1^* \times \ldots \times A_p^*$, *if* $\Pi(u) \to \mathbf{x}$ *then there are words* u' *and* v *such that* $u \overset{*}{\vdash\!\dashv} u' \to v$ *and* $\mathbf{x} = \Pi(v)$.

(iii) *For all* $\mathbf{r}, \mathbf{s} \in A_1^* \times \ldots \times A_p^*$ *and* $u \in \Sigma^*$, *if* $\mathbf{r} \leftarrow \Pi(u) \to \mathbf{s}$ *then either* $\mathbf{r} = \mathbf{s}$ *or, for some* $\mathbf{t}$, $\mathbf{r} \to \mathbf{t} \leftarrow \mathbf{s}$.

PROOF

(i) Suppose $u \to v$, so that $u = xa\bar{a}y$ for some $a \in \Sigma$, and $v = xy$. Let $k = |x|_a$. If $a \in \bar{A}_i$ then also $\bar{a} \in \bar{A}_i$, and so $\pi_i(u) = \pi_i(xy) = \pi_i(v)$. If $a \in A_i$ then $\pi_i(u) = \pi_i(x)a\bar{a}\pi_i(y)$, $\pi_i(v) = \pi_i(x)\pi_i(y)$ and $|\pi_i(x)|_a = |x|_a = k$. Hence $\Pi(u) \to \Pi(v)$.

(ii) Suppose $\Pi(u) \to \mathbf{x}$, so that, for some $a \in \Sigma$ and some k, if $a \in A_i$ then $\pi_i(u) = \alpha_i a\bar{a}\beta_i$, $x_i = \alpha_i\beta_i$ and $|\alpha_i|_a = k$; and $\pi_i(u) = x_i$ otherwise. Since the letter a belongs to at least one of the sets $A_1, \ldots, A_p$, we may assume it belongs to A_1. Since $\pi_1(u)$ thus has the form $\alpha_1 a\bar{a}\beta_1$, write $u = ras\bar{a}t$ where $\pi_1(r) = \alpha_1$, $\pi_1(s) = e$, $\pi_1(t) = \beta_1$, $|r|_a = k$. Note that, since $\pi_1(s) = e$, s has no occurrence of a or of $\bar{a}$.

This particular decomposition of u as $ras\bar{a}t$ displays the occurrences of a and $\bar{a}$ that were cancelled in the other components to produce $\mathbf{x}$. To see this, consider any other set A_i such that $a \in A_i$; we will see that $\alpha_i = \pi_i(r)$, $\beta_i = \pi_i(t)$ and $\pi_i(s) = e$. Since $u = ras\bar{a}t$ and $\pi_i(u) = \alpha_i a\bar{a}\beta_i$, $\pi_i(r)a\pi_i(s)\bar{a}\pi_i(t) = \alpha_i a\bar{a}\beta_i$ with $|\pi_i(r)|_a = |r|_a = k = |\alpha_i|_a$, so $\pi_i(r) = \alpha_i$ and $\pi_i(s)\bar{a}\pi_i(t) = \bar{a}\beta_i$. Since $|s|_{\bar{a}} = 0$, $\pi_i(s)$ cannot begin with $\bar{a}$, so $\pi_i(s) = e$ and $\pi_i(t) = \beta_i$.

Now let $u' = rsa\bar{a}t$ and $v = rst$. If $a \in \bar{A}_i$ then $\pi_i(v) = \pi_i(u) = x_i$, and if $a \in A_i$ then $x_i = \alpha_i\beta_i = \pi_i(r)\pi_i(t) = \pi_i(r)\pi_i(s)\pi_i(t) = \pi_i(v)$; hence $\mathbf{x} = \Pi(v)$. Also, since $\pi_i(s) = e$ whenever $a \in A_i$, all the letters in s commute with a, so $u = ras\bar{a}t \overset{*}{\vdash\!\dashv} rsa\bar{a}t = u' \to v$.

(iii) Suppose $\mathbf{s} \leftarrow \Pi(u) \to \mathbf{t}$ where a subword $a\bar{a}$ was deleted in passing from $\Pi(u)$ to $\mathbf{s}$, and a subword $b\bar{b}$, in passing from $\Pi(u)$ to $\mathbf{t}$. Let $u_i = \pi_i(u)$.

Case 1. First, suppose $(a, b) \in \theta$, so that, for each k, A_k contains at most one of a and b. From the definition of reduction, there are integers m and n such that, for all i, if $a \in A_i$ then $u_i = \alpha_i a\bar{a}\beta_i$, $r_i = \alpha_i\beta_i$ and $|\alpha_i|_a = m$; if $a \in \bar{A}_i$ then $r_i = u_i$; if $b \in A_i$ then $u_i = \gamma_i b\bar{b}\delta_i$, $s_i = \gamma_i\delta_i$ and $|\gamma_i|_b = n$; and if $b \in \bar{A}_i$ then $s_i = u_i$. Define a tuple $\mathbf{t}$ by taking $t_k = s_k$ if $b \in A_k$, $t_k = r_k$ if $a \in A_k$, and $t_k = u_k$ otherwise (in which case $t_k = r_k = s_k$). Then $\mathbf{r} \to \mathbf{t} \leftarrow \mathbf{s}$. The reduction of $\mathbf{r}$ to $\mathbf{t}$ is by deleting $b\bar{b}$ after the nth b: that is, if $b \in \bar{A}_k$ then $t_k = r_k$, and if $b \in A_k$ then $r_k = u_k$ and $t_k = s_k$, so $r_k = \gamma_k b\bar{b}\delta_k$, $t_k = \gamma_k\delta_k$, $|\gamma_k|_b = n$. Similarly, $\mathbf{s}$ reduces to $\mathbf{t}$ by deleting $a\bar{a}$ after the mth a.

Case 2. Now suppose $(a, b) \in \bar{\theta}$, so that one of sets, say A_1, contains a, $\bar{a}$, b and $\bar{b}$. As in the proof of part (ii), from $\Pi(u) \to \mathbf{r}$ it follows that $u = x_1az_1\bar{a}y_1$ with $\mathbf{r} = \Pi(x_1z_1y_1)$ and $\pi_i(z_1) = e$ whenever $a \in A_i$. Also, since $\Pi(u) \to \mathbf{s}$, $u = x_2bz_2\bar{b}y_2$, $\mathbf{s} = \Pi(x_2z_2y_2)$ and $\pi_i(z_2) = e$ whenever $b \in A_i$. Since a and b both belong to A_1, neither z_1 nor z_2 has any occurrence of a, $\bar{a}$, b or $\bar{b}$.

Consider the equation $u = x_1az_1\bar{a}y_1 = x_2bz_2\bar{b}y_2$, where we may assume that $|x_2| \geqslant |x_1|$. If $|x_2| = |x_1|$, then (since $\bar{a}$ does not occur in z_1 or z_2) $x_1 = x_2$, $z_1 = z_2$ and $y_1 = y_2$, so $\mathbf{r} = \mathbf{s}$. If $|x_2| > |x_1|$ then $|x_2| \geqslant |x_1az_1|$, since otherwise $\bar{b}$ would occur in z_1, so either (a) $|x_2| = |x_1 a z_1|$ or (b) $|x_2| > |x_1 a z_1|$. If (a) holds then $x_2 = x_1 a z_1$, $b = \bar{a}$ and $y_1 = z_2 \bar{b} y_2 = z_2 a y_2$, so $x_1 z_1 y_1 = x_1 z_1 z_2 a y_2 \overset{*}{\vdash\!\dashv} x_1 a z_1 z_2 y_2 = x_2 z_2 y_2$, and $\mathbf{r} = \mathbf{s}$. If (b) holds then $x_2 = x_1 a z_1 \bar{a} w$ for some w and $y_1 = w b z_2 \bar{b} y_2$. Let $v = x_1 z_1 w z_2 y_2$. Then $x_1 z_1 y_1 = x_1 z_1 w b z_2 \bar{b} y_2 \overset{*}{\vdash\!\dashv} x_1 z_1 w z_2 b \bar{b} y_2 \to v$ and $x_2 z_2 y_2 = x_1 a z_1 \bar{a} w z_2 y_2 \overset{*}{\vdash\!\dashv} x_1 z_1 a \bar{a} w z_2 y_2 \to v$, so $\mathbf{r} \to \Pi(v) \leftarrow \mathbf{s}$.

The two previous lemmas are the basis for the following proof that T_0 is preperfect.

THEOREM 1. *For a partial commutativity relation θ_0, the Thue system*

$$\{(a\bar{a}, e), (\bar{a}a, e) : a \in \Sigma_0\} \cup \{(cd, dc) : (c, d) \in \theta\}$$

on alphabet Σ is preperfect.

PROOF. From the proposition, it is sufficient to show that whenever $x \leftarrow u \overset{*}{\vdash\!\dashv} v \to y$, there is some z such that $x \overset{*}{\vdash\!\to} z \overset{*}{\leftarrow\!\dashv} y$. Suppose that $x \leftarrow u \overset{*}{\vdash\!\dashv} v \to y$. Then, from lemma 1 and lemma 2(i), $\Pi(u) \to \Pi(x)$ and $\Pi(u) = \Pi(v) \to \Pi(y)$, so, from lemma 2(iii), either $\Pi(x) = \Pi(y)$ or, for some $\mathbf{t}$, $\Pi(x) \to \mathbf{t} \leftarrow \Pi(y)$. In the first case, $x \overset{*}{\vdash\!\dashv} y$. In the second, since $\Pi(x) \to \mathbf{t}$, from lemma 2(ii), $\mathbf{t} = \Pi(z)$ for some z with $|z| = |x| - 2$ and $x \overset{*}{\vdash\!\to} z$, and $\mathbf{t} = \Pi(z')$ for some z' such that $y \overset{*}{\vdash\!\to} z'$. Since $\Pi(z) = \Pi(z')$, $z \overset{*}{\vdash\!\dashv} z'$, so $x \overset{*}{\vdash\!\to} z \overset{*}{\vdash\!\dashv} z' \overset{*}{\leftarrow\!\dashv} y$ and hence $x \overset{*}{\vdash\!\to} z \overset{*}{\leftarrow\!\dashv} y$.

Within the general framework of rewriting systems, the proof that the Thue system T_0 is preperfect can be viewed as follows. First, parts (i) and (ii) of lemma 2 (and induction on number of steps) show that $u \overset{*}{\vdash\!\to} v$ if and only if $\Pi(u) \overset{*}{\longrightarrow} \Pi(v)$; hence T_0 is preperfect exactly when the relation of reduction on tuples is confluent on $\Pi(\Sigma^*)$. Then, from parts (ii) and (iii), reduction on tuples is locally confluent on $\Pi(\Sigma^*)$, so, since that reduction relation is Noetherian, it is confluent on $\Pi(\Sigma^*)$.

The word problem for monoids presented by monadic Church–Rosser Thue systems can be solved in linear time (Book, 1982). Based on theorem 1, a 'synchronous' extension of that linear-time algorithm will serve for free partially commutative groups. A linear-time algorithm is also known for the word problem for almost-confluent Thue systems in which the length-preserving rules express (only) a partial commutativity relation (Book & Liu, 1987), but that algorithm cannot be applied directly here.

THEOREM 2. *For any finitely generated free partially commutative group $G(\theta_0)$, there is a linear-time algorithm to find a shortest word equivalent to a given word, and a linear-time algorithm for the word problem in the group.*

PROOF. Suppose $\theta_0 \subseteq \Sigma_0 \times \Sigma_0$ is a partial commutativity relation, and let T_0 be the Thue system $\{(a\bar{a}, e), (\bar{a}a, e) : a \in \Sigma_0\} \cup \{(cd, dc) : (c, d) \in \theta\}$ on alphabet Σ as constructed above. Let $A_1, \ldots, A_p$ be a collection of sets satisfying properties (i)–(iii). The construction, given a word w, of a shortest word in $[w]$ has two steps, reduction followed by reconstruction.

Consider first the following procedure, which uses p pushdown stores (initially empty):

Read an input symbol, say a. Is the symbol on top of the ith pushdown store $\bar{a}$ whenever a belongs to A_i? If so, erase all those symbols and go on to the next input. If not, write the symbol a onto the top of each store i for which $a \in A_i$ and go on.

This procedure clearly processes an input string w in $|w|$ steps, and produces some tuple $R(w) = (x_1, \ldots, x_p)$ of words on the pushdown stores (where the top of the store is at the right). A straightforward induction can be used to verify that $R(w)$ is irreducible and $\Pi(w) \xrightarrow{*} R(w)$.

From $R(w)$ a word $r(w)$ can be constructed in linear time such that $\Pi(r(w)) = R(w)$. From lemma 2(ii), such a word exists; it can be printed from right to left by starting with $R(w)$ on the pushdown stores and successively (1) printing a letter $b \in \Sigma$ with the property that b is on the top (that is, right) of the ith pushdown store whenever $b \in A_i$, and (2) removing that occurrence of b from each such pushdown store, until all the pushdown stores are emptied. (If there is more than one candidate for the letter to be printed, any one can be chosen, or a fixed precedence used.) The justification for this process is that if $\Pi(u) = \mathbf{t}\Pi(b)$ then there is some v such that $\Pi(v) = \mathbf{t}$ and $u \overset{*}{\vdash\!\dashv} vb$.

From $\Pi(w) \xrightarrow{*} R(w)$ it follows that $w \overset{*}{\vdash\!\!\rightarrow} r(w)$. Moreover, $r(w)$ is a shortest word congruent to w: if v were a shorter word, then (since T_0 is preperfect) $v \overset{*}{\vdash\!\!\rightarrow} z \overset{*}{\leftarrow\!\!\dashv} r(w)$ for some z, so $\Pi(v) \xrightarrow{*} \Pi(z) \xleftarrow{*} \Pi(r(w)) = R(w)$. But $R(w)$ is irreducible, so $\Pi(v) \xrightarrow{*} \Pi(r(w))$ with $|v| < |r(w)|$, a contradiction.

To solve the word problem, reconstruction is not necessary: w_1 is congruent to w_2 if and only if $R(w_1) = R(w_2)$.

The arguments given here apply more generally. For example, it is not necessary that every symbol have an inverse, only that inverses be two-sided when they exist. Also, similar results can be developed for rewriting a free partially commutative monoid by a rule $w_0 \to e$ such that none of the letters in w_0 commute and w_0 has no overlap (i.e. there is no proper nonempty suffix of w_0 that is also a prefix of w_0). Such a system need not be almost-confluent.

The uniform word problem in this context is to test, given alphabet Σ_0, partial commutativity relation θ_0 and words x, y over $\Sigma_0 \cup \Sigma_1$, whether x is equivalent to y in $G(\theta_0)$. The algorithm of theorem 2 can be extended to this case, perhaps most easily by taking the collection $A_1, \ldots, A_p$ to be

$$\{\{a, \bar{a}, b, \bar{b}\} : (a, b) \in \bar{\theta}_0, a \neq b \text{ in } \Sigma_0\} \cup \{\{a, \bar{a}\} : a \in \Sigma_0, a \times (\Sigma_0 - \{a\}) \subseteq \theta_0\},$$

which avoids the problem of finding larger cliques in $\bar{\theta}_0$. The size of this collection is $(|\bar{\theta}_0| - |\Sigma_0|)/2$ plus the number of letters in Σ_0 that commute with all other letters, so that p is at most $|\Sigma_0|(|\Sigma_0| - 1)/2$. The total time required to form $R(x)$ and $R(y)$ and test if they are equal is at worst linear in the product $p \cdot |\Sigma_0| \cdot |xy|$, and so polynomial in the size of the input.

References

Book, R. (1982). Confluent and other types of Thue systems. *J. Assoc. Comp. Mach.* **29**, 171–182.

Book, R. & Liu, H.-N. (1987). Word problems and rewriting in a free partially commutative monoid. *Inf. Proc. Lett.* **26**, 29–32.

Cochet, Y., Nivat, M. (1971). Une généralisation des ensembles de Dyck. *Israel J. Math.* **9:3**, 389–395.

Cori, R., Perrin, D. (1985). Automates et commutations partielles. *RAIRO-Informat. Theor.* **19**, 21–32.

Diekert, V. (1987). On the Knuth-Bendix completion for concurrent processes. Automata, Languages, and Programming. *Springer Lec. Notes Comp. Sci.* **267**, 42–53.

Duboc, C. (1985). Some properties of commutation in free partially commutative monoids. *Inf. Proc. Lett.* **20**, 1–4.

Duboc, C. (1986*a*). On some equations in free partially commutative monoids. *Theor. Comp. Sci.* **46**, 159–174.

Duboc, C. (1986*b*). Commutations dans les monoides libres. Thesis. University of Rouen.

Narendran, P., McNaughton, R. (1984). The undecidability of the preperfectness of Thue systems. *Theor. Comp. Sci.* **31**, 165–174.

Nivat, M., Benois, M. (1971–72). Congruences parfaites et quasi-parfaites. Séminaire Dubreil, 25th année, 7–01–09.