A normal-form theorem for monoids and groups with the single relation $xy \leftrightarrow yx$

Michael Batty
Amazing Media, Grey Steet, Newcastle, UK
Colm Ó Dúnlaing
Mathematics, Trinity College, Dublin 2, Ireland
Claas Röver[*]
Mathematics, National University of Ireland, Galway, Ireland

December 14, 2007

Abstract

The word problem for confluent Thue systems is linear-time and for almost confluent systems it is PSPACE-complete. Here we consider a single length-preserving rule, of the form $xy \leftrightarrow yx$, whose word problem could turn out to be tractable.

A search for normal forms leads to the conjecture that if $x^m y^n \leftrightarrow^* x^p y^q$ then $m = p$ and $n = q$.

We prove a stronger version of this: in a group G with the single relator $xyx^{-1}y^{-1}$, where x and y are positive words, if $x^m y^{-n} = 1$ in G then $m = n = 0$.

1 Introduction

It is known [2,1] that the word problem for confluent Thue systems is solvable in linear time, but for almost-confluent Thue systems (allowing length-preserving rules) it is PSPACE-complete. This paper considers Thue systems with a single (length-preserving) rule of the form $xy \leftrightarrow yx$. Our goal is to give efficient algorithms for such systems.

Such an algorithm should be based on some kind of normal form for strings which should be, say, of the form $x^m y^n$ for strings in $\{x, y\}^*$. This raises the question: is it possible to convert $x^m y^n$ to a different string $x^p y^q$ by exchanging adjacent occurrences of x and y? Of course, if the occurrences exchanged in a string in $\{x, y\}^*$ are only the obvious, 'aligned' ones, then such a conversion could not be made.

We prove the result for groups with a single relator $xyx^{-1}y^{-1}$, using the standard 'Freiheitsatz' method found in [3].

The final section considers a specimen word-problem in the group and the monoid where $x = a$ and $y = bab$.

[*]E-mail michaelbatty@minigalleryartists.co.uk, odunlain@maths.tcd.ie, claas.roever@nuigalway.ie.

2 Definitions, statement of theorem, and the case of a group

Fix an alphabet Σ, strings $x, y \in \Sigma^*$ with $xy \neq yx$, and the Thue system with the single rule $xy \leftrightarrow yx$.

We claim the following

(2.1) Theorem *If $x^m y^n \overset{*}{\leftrightarrow} x^p y^q$ then $m = p$ and $n = q$.*

More generally,

(2.2) Theorem *Let G be the group with presentation $\langle \Sigma \mid xy = yx \rangle$, where x and y are positive words. Then the subgroup $\langle x, y \rangle$ of G is free abelian of rank 2.*

(2.3) Lemma *If $xy \neq yx$ in the free monoid Σ^* (respectively, the free group $F(\Sigma)$), then x and y generate $\{x, y\}^*$ (respectively, $\langle x, y \rangle$) freely.*

Proof. The group result implies the monoid result. In order to prove the group case, assume that there exists a nontrivial relator in $\langle x, y \rangle$. This implies that $\langle x, y \rangle$ is trivial or free on one generator, so $xy = yx$ which contradicts our hypothesis. **Q.E.D.**

In the group case we consider single-relator groups of the form

$$\langle \Sigma \mid xyx^{-1}y^{-1} \rangle \tag{2.1}$$

where x and y are positive words.

The appropriate form for Theorem 2.2 is

(2.4) Theorem *In the group (2.1), if $m \neq 0$ or $n \neq 0$ then $x^m y^n \neq 1$ in G.*

Proof. An old result of Schützenberger [6] says that no non-trivial commutator is a proper power, which implies that G is torsion-free (see [3]). This deals with the case when either $n = 0$ or $m = 0$.

Now assume that $n \neq 0$ and $m \neq 0$ and that G is a counterexample with $R = xyx^{-1}y^{-1}$ of minimal length (w.r.t. Σ). Thus for some (non-zero) n and m we have $x^m = y^n$. Since x and y are non-commuting positive words, it is clear that R has length at least four and involves all the letters that occur in x or y. We use Magnus' standard method for one-relator groups (see [3]).

First assume that some letter, a say, occurs with exponent sum zero in x or y. Then, since every letter has exponent sum zero in $xyx^{-1}y^{-1}$, a has in fact exponent sum zero in both x and y. Let $\Sigma = \{a, b, c, \ldots\}$ and let H be the normal subgroup of G generated by $\Sigma \setminus \{a\}$. Then $x, y, R \in H$ and H has a presentation with generators

$$b_i = a^i b a^{-i}, c_i = a^i c a^{-i}, \ldots \qquad i \in \mathbb{Z}$$

and defining relators R_i, $i \in \mathbb{Z}$, where R_i is obtained by rewriting $a^i R a^{-i}$ in terms of these generators. This rewriting is done by replacing each occurrence of $b, c, \ldots$ in R, by $b_k, c_k, \ldots$ where k is the exponent sum of a in the prefix of R up to the letter to be replaced. For example, the word $ab^{-1}a^{-2}cab$ gets rewritten into $b_1^{-1}c_{-1}d_0$. It follows that, if Λ denotes the set of those generators that appear in R_0, then $\langle \Lambda \mid R_0 \rangle$ is a presentation for the subgroup, L say, of H generated by Λ (see II.5.2 in [5]). Since x and y are elements of L and $R_0 = \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1}$ where $\bar{x}$ and $\bar{y}$ denote the results of rewriting x (respectively, y), we see that L is also a counterexample. But, since a occurred in R, R_0 is shorter (w.r.t Λ) than R (w.r.t. $\{a, b, c, \ldots\}$). This contradicts our assumption that G was a 'minimal' counter example and hence finishes this case.

Now we treat the case when all letters that occur in R have non-zero exponent sum in x, and hence also in y. Observe that R involves at least two letters, a and b say. Let α and β be the exponent sum of a and b, respectively, in x. Let p and q be letters not in Σ and let $\hat{x}$, $\hat{y}$ and $\hat{R}$ denote the words obtained by replacing a by p^β and b by $qp^{-\alpha}$ in x, y and R, respectively. Now $\hat{x}$, $\hat{y}$ and $\hat{R}$ are all elements of a group generated by $\{p, q, c, d, \ldots\}$ and $\hat{R} = \hat{x}\hat{y}\hat{x}^{-1}\hat{y}^{-1}$. In fact, they are all elements of the normal closure of $\{q, c, d, \ldots\}$ in this group, as the exponent sum of p in $\hat{x}$ and $\hat{R}$, and hence in $\hat{y}$ is zero. Therefore, we can rewrite them in the generators $q_i = a^i q a^{-i}, c_i = a^i c a^{-i}, \ldots, i \in \mathbb{Z}$ of this normal subgroup, just as above. Since p occurred in $\hat{R}$, the result of rewriting $\hat{R}$, call it R', is shorter than R. It is clear that the subgroup K generated by those generators that appear in R' contains $\hat{x}$ and $\hat{y}$ and has a R' as its sole relator. Thus K is a counterexample with a shorter relator than G which is our final contradiction. **Q.E.D.**

3 Specimen algorithms

(3.1) Example: $x = a, y = bab$. If we first consider the group:

$$G = \langle a, b;\ abab = baba \rangle$$

$$\text{Let } c = ab$$

$$\langle a, c;\ c^2 = a^{-1}c^2a \rangle$$

$$\langle a, c; ac^2 = c^2a \rangle.$$

That is, the relator allows a to commute with c^2. Consequently a and a^{-1} both commute with c^2 and c^{-2}. We can apply these rules to push even powers of c as far to the left as possible, so every word z can be converted to the form $c^{2s}z_1$ where z_1 is a product of powers of a, only the first and last being possibly zero, alternating with $c^{\pm 1}$. This gives a normal form for z. Under the map $a \mapsto a, c \mapsto c$ we can map G to the group

$$G' = \langle a, c;\ c^2 = 1 \rangle \cong \mathbb{Z} * \mathbb{Z}_2$$

which sends z_1 to a word of identical appearance and sends c^{2s} to 1. If $z_1 \neq 1$ in G then its image is nontrivial in G', so z_1 must be unique for z. The map $a \mapsto a, c \mapsto 1$ sends $c^{2s}z_1$ and $c^{2s'}z_1$ to different elements of $\langle a \rangle \cong \mathbb{Z}$ if $s \neq s'$. In other words, we have a normal form for elements of G, and a polynomial-time solution to the word problem — for the group. (The textboox [4] contains several examples like this.)

The semigroup problem is harder. Starting with a string $z \in \{a, b\}^*$, we can, of course, introduce c into z to replace ab. To cut a long story short, we consider the following semi-Thue system over $\{a, b, c\}$:

$$ab \to c, ac^2 \to c^2a, bc^2 \to c^2b, bca \to c^2.$$

Two rules are length-reducing and the length-preserving rules move occurrences of c further to the left. If we apply leftmost reductions, the quantity

length of z + maximum distance of a redex from the right-hand end of z

is reduced in every step. Therefore the system is Noetherian; in fact, no string z can be reduced more than $2|z|$ times, and z can be reduced in linear time. Also it is Church-Rosser, since all critical pairs can be resolved:

$$\begin{aligned} abc^2 \to c^3, abc^2 \to ac^2b \to c^2ab \to c^3, \\ abca \to c^2a, abca \to ac^2 \to c^2a, \\ bcab \to c^2b, bcab \to bc^2 \to c^2b, \\ bcac^2 \to c^4, bcac^2 \to bc^3a \to c^2bca \to c^4. \end{aligned}$$

This is a Noetherian confluent semi-Thue system, and the word-problem is solvable in linear time.

4 References

1. Ronald V. Book and Friedrich Otto (1993). *String-rewriting systems.* Springer texts and monographs in Computer Science.

2. Ronald V. Book, Matthias Jantzen, Burkhard Monien, Colm Ó Dúnlaing, and Celia Wrathall (1981). On the complexity of word problems in certain Thue systems. Springer LNCS 118, 216–223.

3. Abraham Karrass, Wilhelm Magnus, and Donald Solitar (1960). Elements of finite order in groups with a single defining relation. *Communications in Pure and Applied Mathematics* **xiii**, 57–66.

4. Wilhelm Magnus, Abraham Karrass, and Donald Solitar (1966). *Combinatorial Group Theory*. Published in 1976 by Dover Press.

5. Roger Lyndon and Paul Schupp (1977). *Combinatorial Group Theory*. Springer.

6. M. P. Schützenberger (1959). Sur l'équation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre. *C. R. Acad. Sci. Paris* **248**, 2435–2436.