RAIRO. INFORMATIQUE THÉORIQUE

JÜRGEN AVENHAUS
RONALD V. BOOK
CRAIG C. SQUIER

On expressing commutativity by finite Church-Rosser presentations : a note on commutative monoids

RAIRO. Informatique théorique, tome 18, nº 1 (1984), p. 47-52
<http://www.numdam.org/item?id=ITA_1984__18_1_47_0>

R.A.I.R.O. Informatique théorique/Theoretical Informatics
(vol. 18, n° 1, 1984, p. 47 à 52)

ON EXPRESSING COMMUTATIVITY BY FINITE CHURCH-ROSSER PRESENTATIONS: A NOTE ON COMMUTATIVE MONOIDS (*)

by Jürgen AVENHAUS [1], Ronald V. BOOK [2], and Craig C. SQUIER [2]

Communicated by J. E. PIN

Abstract. — *Let M be an infinite commutative monoid. Suppose that M has a Church-Rosser presentation. If M is cancellative or if the presentation is special, then M is either the free cyclic group or the free cyclic monoid.*

Résumé. — *Soit M un monoide commutatif infini. Supposons que M possède une présentation finie ayant la propriété de « Church-Rosser ». Si M est simplifiable ou si la présentation est spéciale, alors M est soit le groupe cyclique libre soit le monoide cyclique libre.*

INTRODUCTION

It is well known that it is undecidable whether the monoid presented by a Thue system is a group. However, if the Thue system is Church-Rosser and special, then this question is decidable. Cochet [3] has shown that if a group has a finite Church-Rosser special presentation, then the group is isomorphic with the free product of finitely may cyclic groups. Of course every countable monoid has a Church-Rosser presentation with infinitely many generators and infinitely many relators. It is challenging to ask which monoids admit a finite Church-Rosser presentation.

We regard a monoid as a quotient of a free monoid and ask for the possibility of expressing commutativity by the presentation. We prove that this is impossible in many cases. Let M be an infinite commutative monoid with a finite Church-Rosser presentation. If M is cancellative or the presentation is special, then M is either the free monoid on one generator or

(*) Received in October 1982, revised in April 1983.
This research was supported in part by the Fritz Thyssen Stiftung, West Germany, and by the National Science Foundation under Grants MCS80-11979 and MCS81-16327.
[1] Fachbereich Informatik, Universität Kaiserslautern, Postface 3049, 6750 Kaiserslautern, West Germany.
[2] Department of Mathematics, University of California, Santa Barbara, California 93106, U.S.A.

0399-0540/84/01 47 6/$ 2.60/

the free group on one generator. Thus, any commutative group with a finite Church-Rosser presentation is either finite or free cyclic.

SECTION 1

Thue systems

If Σ is a set of symbols (i. e., an alphabet), then Σ^* is the free monoid with identity 1 generated by Σ. If w is a string, then the length of w is denoted by $|w|$:

$$|1|=0, \qquad |a|=1 \quad \text{for } a\in\Sigma,$$

and:

$$|wa|=|w|+1 \quad \text{for } w\in\Sigma^*, \qquad a\in\Sigma.$$

A *Thue system* T on an alphabet Σ is a subset of $\Sigma^*\times\Sigma^*$; each pair in T is a *rule*. The *Thue congrence generated by* T is the reflexive transitive closure $\overset{*}{\leftrightarrow}$ of the relation $\leftrightarrow$ defined as follows: for any u, v such that $(u, v)\in T$ or $(v, u)\in T$ and any x, $y\in\Sigma^*$, $xuy\leftrightarrow xvy$. Two strings w, z are *congruent* (*mod* T) if $w\overset{*}{\leftrightarrow}z$ and the *congruence class* of z (*mod* T) is $[z]=\{w \mid w\overset{*}{\leftrightarrow}z\}$.

If T is a Thue system on alphabet Σ, then the congruence classes of T form a monoid M under the multiplication $[x]\circ[y]=[xy]$ and with identity [1]. This is the *monoid presented by* T.

If T is a Thue system, write $x\leftrightarrow y$ provided $x\leftrightarrow y$ and $|x|>|y|$, and write $\overset{*}{\rightarrow}$ for the reflexive transitive closure of the relation $\rightarrow$.

Without loss of generality, assume that for any Thue system T, $(u, v)\in T$ implies $|u|\geqq|v|$.

A Thue system T is *special* if $(u, v)\in T$ implies $|v|=0$.

A Thue system T is Church-Rosser if for all x, y, $x\overset{*}{\leftrightarrow}y$ implies that for some z, $x\overset{*}{\rightarrow}z$ and $y\overset{*}{\rightarrow}z$.

A string w is *irreducible* (mod T) if there is no z such that $w\rightarrow z$ in T.

It is useful to note that a Thue system is Church-Rosser if and only if each congruence class has a unique irreducible string [4, 6].

The definition of the Church-Rosser property by means of the reduction $\overset{*}{\rightarrow}$ which is defined in terms of length is a very strong restriction. However, the property provides a great deal of power in terms of deciding properties of the monoid so presented. For additional properties of such systems, *see* [2-4, 7].

SECTION 2

The result

In order to establish our results we study the structure of Thue systems that are Church-Rosser. The first two lemmas have elementary proofs that are left as exercices.

LEMMA 1: *Let T_1 be a Thue system on that alphabet Σ and let M be the monoid presented by T_1. Suppose that T_1 is Church-Rosser. Then there exists a Thue system T_2 on the alphabet Σ such that T_2 presents M, T_2 is Church-Rosser, and if $(u, v) \in T_2$, then $|u| > |v|$.*

LEMMA 2: *Let T_1 be a Thue system on the alphabet Σ and let M be the monoid presented by T_1. Suppose that T_1 is Church-Rosser. Then there exists a Thue system T_2 on an alphabet $\Delta \subseteq \Sigma$ such that:*

(i) *T_2 has no rules of the form $(a, 1)$ with $a \in \Delta$;*

(ii) *T_2 is Church-Rosser;*

(iii) *T_2 presents M.*

Henceforth we assume that T is a finite Thue system over the alphabet Σ, that T is Church-Rosser, that for every $a \in \Sigma$, $(a, 1) \notin T$, and that $(u, v) \in T$ implies $|u| > |v|$. Let M be the monoid presented by T.

LEMMA 3: *For any $a, b \in \Sigma$ with $a \neq b$, if $ab \overset{*}{\leftrightarrow} ba$, then either:*

(i) *there is an $i > 0$ such that $a^i b \overset{*}{\leftrightarrow} 1$;*

or:

(ii) *for some i, j with $0 \leqslant i < j$, $a^i b \overset{*}{\leftrightarrow} a^j b$.*

Proof: We claim that there is a sequence $c_1, c_2, \ldots \in \Sigma \cup \{1\}$ such that $a^i b \overset{*}{\leftrightarrow} c_i$ for every i. For $i = 1$, this follows from the fact that T is Church-Rosser and the hypothesis that $ab \overset{*}{\leftrightarrow} ba$. If $a^i b \overset{*}{\leftrightarrow} c_i$ for some i, then:

$$c_i a \overset{*}{\leftrightarrow} a^i ba \overset{*}{\leftrightarrow} a^i ab \overset{*}{\leftrightarrow} ac_i$$

so that T Church-Rosser implies that for some

$$c_{i+1} \in \Sigma \cup \{1\}, \quad c_i a \overset{*}{\rightarrow} c_{i+1} \qquad \text{and} \qquad ac_i \overset{*}{\rightarrow} c_{i+1}$$

so

$$a^{i+1} b \overset{*}{\rightarrow} ac_i \overset{*}{\rightarrow} c_{i+1}.$$

The alphabet Σ is finite so $\{c_i \mid i>0\} \subseteq \Sigma \cup \{1\}$ implies that either $c_i=1$ for some i so (i) holds, or there exist i and j with $0<i<j$ and $c_i=c_j$ so that (ii) holds. □

LEMMA 4: *Let M be cancellative. For any $a \in \Sigma$, if a^2 is reducible then a has finite order.*

Proof: If a^2 is reducible, then $a^2 \to 1$ or $a^2 \to b$ for some $b \in \Sigma$. If $a^2 \to 1$, then a has finite order. If $a^2 \to b$, then $b \neq a$ since M is cancellative and $a \neq 1$. Now $a^2 \to b$ implies $ab \overset{*}{\leftrightarrow} aa^2 \overset{*}{\leftrightarrow} ba$. By Lemma 3, either there is an i such that $a^{i+2} \overset{*}{\leftrightarrow} a^i b \overset{*}{\leftrightarrow} 1$ or for some

$$i,j \quad \text{with} \quad 0<i<j, \qquad a^i b \overset{*}{\leftrightarrow} a^i b. \text{ so } a^{j-i} \overset{*}{\leftrightarrow} 1$$

since M is cancellative. In either case, a has finite order. □

Now we have our result.

THEOREM: *Suppose that M is commutative and infinite. If M is cancellative or T is special, then M is either the free cyclic group or the free cyclic monoid.*

Proof: Since M is commutative and T is Church-Rosser, any irreducible word has the form a^i where $a \in \Sigma$ and $i \geqq 0$. If the cardinality of Σ is one, then M is the free cyclic monoid. Assume the cardinality of Σ is greater than one. We will show that Σ has exactly two elements. Since M is commutative and infinite, there is an element of Σ of infinite order, say a. Let b be any element in $\Sigma - \{a\}$.

Suppose that M is cancellative. We claim that $ab \to c$ with $c \in \Sigma$ is impossible. First note that $c \neq a$ and $c \neq b$ for otherwise $b \overset{*}{\leftrightarrow} 1$ or $a \overset{*}{\leftrightarrow} 1$ by cancellation, contradicting our assumptions on T. Now if:

$$ab \to c \qquad \text{and} \qquad ac \to d, \quad d \in \Sigma \cup \{1\},$$

then

$$ba \to c \qquad \text{and} \qquad ca \to d$$

since M is commutative. Thus:

$$c^2 \overset{*}{\leftrightarrow} abc \overset{*}{\leftrightarrow} bac \overset{*}{\leftrightarrow} bd \qquad \text{and so} \quad c^2$$

is reducible. By Lemma 4 this means c has finite order, say $c^k \overset{*}{\to} 1$. Since a has infinite order and M is cancellative, it is not the case that:

$$a^i c \overset{*}{\leftrightarrow} a^j c \qquad \text{with} \quad 0<i<j,$$

so by Lemma 3 there is an i such that $a^i c \overset{*}{\to} 1$. Thus:

$$a^{ki} \overset{*}{\leftrightarrow} a^{ki}c^k \overset{*}{\leftrightarrow} (a^i c)^k \overset{*}{\leftrightarrow} 1$$

contradicting the fact that a has infinite order. Hence, for all

$$b \in \Sigma - \{a\}, \quad ab \to 1 \qquad \text{and} \qquad ba \to 1.$$

This means that every element of Σ has infinite order since a has infinite order and if

$$b^j \overset{*}{\to} 1 \quad \text{for } b \in \Sigma \qquad \text{and} \qquad j > 0,$$

then

$$a^j \overset{*}{\leftrightarrow} a^j b^j \overset{*}{\leftrightarrow} (ab)^j \overset{*}{\leftrightarrow} 1,$$

since $ab \to 1 \in T$. Now

$$\Sigma = \{a, b\}, \qquad ab \to 1 \in T, \qquad ba \to 1 \in T,$$

and every element of Σ having infinite order implies M is the free cyclic group. If

$$c \in \Sigma - \{a, b\}, \quad \text{then } ac \overset{*}{\to} 1 \qquad \text{and} \qquad ab \overset{*}{\to} 1 \quad \text{so } b \overset{*}{\leftrightarrow} c$$

by cancellation; but $b \neq c$ so this is a contradiction of T being Church-Rosser.

Suppose that T is special. Then for every $b \in \Sigma$ with $b \neq a$, $ab \to 1 \in T$. Thus, as above, every element of Σ has infinite order, and if $\Sigma = \{a, b\}$, $b \neq a$, then M is the free cyclic group. If

$$c \in \Sigma - \{a, b\}, \quad \text{then } ab \overset{*}{\leftrightarrow} ba, \quad ac \overset{*}{\leftrightarrow} ca, \qquad \text{and} \qquad bc \overset{*}{\leftrightarrow} cb,$$

so T being Church-Rosser and special implies

$$\{(ab, 1), (ba, 1), (ac, 1), (ca, 1), (bc, 1), (cb, 1)\} \subseteq T.$$

Hence:

$$a \overset{*}{\leftrightarrow} abc \overset{*}{\leftrightarrow} c \quad \text{so } a \overset{*}{\leftrightarrow} c;$$

but $a \neq c$ so this is a contradiction of T being Church-Rosser. □

If the requirement that M be cancellative or T be special is omitted, then the result no longer holds. For example, let:

$$\Sigma = \{a, b\} \qquad \text{and} \qquad T = \{(ab, b), (ba, b), (bb, b)\};$$

the monoid M presented by T is commutative (since $ab \leftrightarrow b \leftrightarrow ba$) and infinite (since for all n, $[a^n] \neq [a^{n+1}]$) but not free (since for all n, $[a^n]\,[b] = [b]$).

SECTION 3

Remarks

As the referee has pointed out, in the literature on commutative monoid the monoid is often regarded as a quotient of a free commutative monoid [5, 8, 9]. In this case the commutativity must not be expressed by the presentation. Hence, our results do not hold in such a setting as seen by the following example. Let $M=(\Sigma, T)$ be the commutative monoid with:

$$\Sigma = \{ a, \bar{a}, b, \bar{b} \} \qquad \text{and} \qquad T = \{ (a\bar{a}, 1), (b\bar{b}, 1)) \}.$$

Then T is Church-Rosser and special but M is the free abelian group on two generators.

Even in this case there are commutative monoid with no finite Church-Rosser presentations, e. g., $M=(\{ a, b \}; a^2=b^2)$. Ballantyne and Lankford [1] use another notion of Church-Rosser presentation where reduction is not based on the length of strings and show that any commutative monoid with a finite presentation admits a finite presentation which is Church-Rosser in their sense. This gives a uniform method for solving the word problem in finitely presented commutative monoids.

REFERENCES

1. A. M. Ballantyne and D. S. Lankford, *New Decision Algorithms for Finitely Presented Commutative Semigroups*, Computation and Mathematics with Applications, Vol. 7, 1981, pp. 159-165.
2. R. Book, *Decidable Sentences of Church-Rosser Congruences*, Theoret. Comput. Sc., Vol. 24, 1983, pp. 301-312.
3. Y. Cochet, *Church-Rosser Congruences on Free Semigroups*, Colloquia Math. Soc. Janos Bolyai, Vol. 20, 1976, pp. 51-60.
4. Y. Cochet and M. Nivat, *Une generalisation des ensembles de Dyck*, Israel J. Math., Vol. 9, 1971, pp. 389-395.
5. S. Eilenberg and M. P. Schutzenberger, *Rational Sets in Commutative Monoids*, J. Algebra, Vol. 13, 1969, pp. 173-191.
6. G. Huet, *Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems*, J. Assoc. Comput. Mach., Vol. 27, 1980, pp. 797-821.
7. C. Ó'Dúnlaing, *Finite and Infinite Regular Thue Systems*, Ph. D. dissertation, University of California at Santa Barbara, 1981.
8. L. Redei, *The Theory of Finitely Generated Commutative Semigroups*, Pergamon Press, 1965.
9. J. Sakarovitch, *Sur les monoides commutatifs*, Seminaire d'Informatique Theorique, Institut de Programmation, n° 1, 1978, pp. 78-01.