Publ. I.R.M.A. Strasbourg, 1988, 361/S–19
Actes 19e Séminaire Lotharingien de Combinatoire, p. 5–12

A REMARK ON THE REPRESENTATION OF THE FREE PARTIALLY COMMUTATIVE MONOID

BY

CHRISTIAN CHOFFRUT†

Summary We consider free partially commutative monoids i.e., free monoids where some pairs of letters are allowed to commute. We show that such a monoid can be faithfully represented by 2x2-matrices with integer entries iff it is the direct product of a free commutative monoid with a free product of free commutative monoids.

Résumé Nous considérons les monoides libres partiellement commutatifs, c'est-à-dire les monoides libres où certaines paires de lettres sont autorisées à commuter. Nous montrons qu'un tel monoide admet une représentation fidèle par des matrices de dimension 2 à entrées dans les entiers ssi il est le produit direct d'un monoide libre commutatif et d'un produit libre de monoides commutatifs libres.

1. Introduction

It is well known that each free monoid can be faithfully represented by 2x2-matrices with entries in the integers $\mathbb{N}$. This result, apart from its theoretical interest, has some important consequences. One of them concerns decidability results on $\mathbb{N}$-rational series (cf. e.g. [Ei], Thm 12.1). Another one deals with a conjecture of Ehrenfeucht stating that any system of equations in the free monoid is equivalent to a finite subsystem (cf. [AL]). A major step in the proof of this conjecture relies on the existence of a faithful matrix representation of all free monoids .

Our purpose here is to characterize the free partially commutative monoids (i.e. the free monoids where some pairs of letters are allowed to commute), that can be faithfully represented by 2x2-matrices with entries in the integers $\mathbb{N}$. Our main result is the following:

Theorem

A free monoid with partial commutations can be faithfully represented by 2x2-matrices with entries in $\mathbb{N}$ iff it is a direct product of a free commutative monoid with a free product of free commutative monoids.

† Univerité de Rouen, Faculté des Sciences, Laboratoire d'Informatique de Rouen, B.P. 118, Place Blondel, F-76134 Mont-Saint-Aignan Cedex, France.

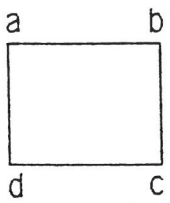
We now turn to a brief description of the various sections of our work. In Section 2 below we recall the basic definitions on free partially commutative monoids, the standard operations of direct and free products and the representations of free monoids that can be found in the literature. In section 3 some elementary results on commutativity in the monoid of 2x2-matrices with entries in the integers $\mathbb{N}$ are stated. As a consequence the "only if" part of the Theorem is established. Section 4 is devoted to the "if" part, i.e. essentially to finding a faithful representation of a free product of free commutative monoids by 2x2-matrices.

2. Preliminaries

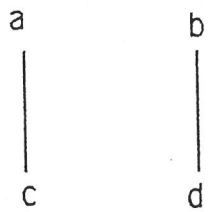
2.1 Free monoids _ Partial commutations

Given a finite nonempty alphabet A whose elements are letters, we denote by A^* the free monoid it generates.

Let $\theta \in A \times A$ be a fixed non reflexive symmetrical relation on A - a relation of partial commutations - and let $^-\theta$ be the relation consisting of all pairs of distinct elements in A not belonging to θ - the relation of conflicts -. We denote by $\sim_\theta$ or simply by $\sim$ when θ is understood, the congruence on A^* generated by the relators : $ab \sim ba$ for all $(a,b) \in \theta$. Then the quotient monoid $M(A,\theta) \approx A^*/_\sim$ is the free monoid generated by A with partial commutations θ or simply the free partially commutative monoid, in short f.p.c.m.(cf. [Fo] or [La]). The free monoid A^* and the free commutative monoid $A^\oplus$ are two extreme cases corresponding to θ and $^-\theta$ respectively being empty. A f.p.c.m. is entirely defined by the graph of its relation of commutations or equivalently by the graph of its relation of conflicts. For example if $A=\{a, b, c, d\}$ and if θ is the relation $ab \sim ba$, $bc \sim cb$, $cd \sim dc$, $da \sim ad$ then the graphs of θ and $^-\theta$ are as follows :



The commutation relation



The conflict relation

There are standard ways of defining new partial commutations from a given set of partial commutations. In particular the free product and the direct product of f.p.c.m.'s can be defined in terms of simple operations on the relations of commutations and of conflicts as follows:

Assume A and B are two disjoint alphabets with partial commutations θ and ϕ respectively. Then the free monoid generated by A U B with partial commutations $\theta \cup \phi$ is the free product of the two f.p.c.m.'s $M(A,\theta)$ and $M(B,\phi)$:

$$M(A \cup B, \theta \cup \phi) \approx M(A,\theta) * M(B,\phi).$$

Furthermore, the f.p.c.m. generated by A U B with the relation of conflicts $\bar{\theta} \cup \bar{\phi}$ is the direct product of the two f.p.c.m. $M(A,\theta)$ and $M(B,\phi)$. The example above is the direct product of two free monoids on two generators.

2.2. Representation of f.p.c.m. by matrices

It is well know that every free monoid can be faithfully represented by matrices with entries in $\mathbb{N}$. For example if A={x, y} then the two representations to be found in the literature are (cf. e.g., [Ei], Exercise 2.2. p. 106):

$$X = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad Y = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

and

$$X = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \qquad Y = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix}$$

The first two matrices generate a free monoid. Inded, to every row vector [a b] with $a > 0$ and $b > 0$, X assigns a row vector [c d] where $c < d$, while Y assigns a row vector [c d] where $c > d$. The last two matrices generate a free monoid for a different reason. Computing the matrix $Z_1 \ldots Z_n$ where $Z_i = X$ or Y for $i=1, \ldots, n$ one verifies easily that it is equal to:

$$\begin{bmatrix} 2^n & 0 \\ N & 1 \end{bmatrix}$$

where N is the integer whose binary expansion is $Z_1 \ldots Z_n$ when X is interpreted as 0 and Y as 1 (with possibly leading 0's).

We say that a f.p.c.m. $M(A,\theta)$ is 2-representable (or simply representable when no confusion may arise) if there exists an injective morphism of $M(A,\theta)$ into the multiplicative monoid $\mathbb{N}^{2x2}$. The purpose of this paper is to characterize the free partially commutative monoids which are representable.

3. Commuting matrices

This section states a few elementary results on commuting matrices which will be used in establishing a necessary condition for a f.p.c.m. to be 2-representable.

As usual we denote by I the identity matrix and the complex field by $\mathbb{C}$.

Lemma 3.1.

If X, Y are two matrices in $\mathbb{C}^{2x2}$ generating a free submonoid, then X and Y are invertible.

Proof.

Assume that X is singular. Then it satisfies its characteristic equation: $X(X - rI)=0$ where $r \in \mathbb{C}$. It follows: $X^2YX = r\,XYX = XY(rX) = XYX^2$ contradicting the fact that X and Y generate a free submonoid □

We now investigate under which conditions two matrices in $\mathbb{N}^{2x2}$ commute. This case is simpler than the general one where the matrices have an arbitrary dimension. The following result will be sufficient for our purpose.

Lemma 3.2.

Let X, Y be two matrices in $\mathbb{N}^{2x2}$.

i) If X has two distinct eigenvalues then Y commutes with X iff it is a polynomial in X: $Y = aI + bX$ where $a, b \in \mathbb{Q}$.

ii) If X has a characteristic root of multiplicity two then it is of the form:

(3.1.)
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where $a = d$ and $bc=0$. If say, $b \neq 0$ then X and Y commute iff Y is of the form:

(3.2.)
$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

If $b=c=0$ then every matrix Y commutes with X.

Proof.

Assertion i) is well known and holds in the general case where the entries of

the two matrices are elements of the complex field (cf, e.g., [Ga], p. 206).
Now if X has an eigenvalue of multiplicity 2 then its characteristic polynomial is of the form: $P(t)= t^2 - (a+d)\, t + ad - cb$, with $(a-d)^2 + 4cb = 0$. This implies $a=d$ and $cb=0$. The completion of assertion ii) is then straightforward.

□

Proposition 3.3.

Let X, Y, Z be three matrices in $\mathbb{N}^{2x2}$ satisfying $XY = YX$, $XZ = ZX$ and $YZ \neq ZY$. Then $X = aI$ for some $a \in \mathbb{N}$.

Proof.

If X has two distinct eigenvalues then Y and Z are polynomials in X and therefore commute. Now if X is of the form (3.2.) with $b \neq 0$ then Y and Z are of the form (3.2.) and again Y and Z commute. This leaves the last case.

□

We may now state the main result of this section.

Proposition 3.4.

Let $M(A,\theta)$ be a representable f.p.c.m. Then A can be decomposed into B and C in such a way that:
1) the submonoid generated by B is a free commutative monoid
2) the submonoid generated by C is the free product of free commutative monoids
3) $M(A,\theta)$ is the direct product of the submonoids generated by B and C.

Proof

Let B be the subset of all elements of A commuting with every element in A. It suffices to verify that the submonoid generated by $C = A - B$ is a free product of free commutative monoids. Indeed, if this were not true then there would exist three letters x, y, z in C such that: $xy \sim yx$, $xz \sim zx$ and zy not $\sim yz$. By Lemma 3.3. this implies that the matrix associated with y commutes with all matrices, a contradiction. □

4. Free products of free commutative monoids

We shall exhibit a representation of the free product of an arbitrary number of free commutative monoids.

Proposition 4.1.

Every free product of free commutative monoids is representable.

Proof.

We first observe that two matrices:

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix}$$

commute iff $(a-1)\,d = (c-1)\,b$. Denote by $r = b/(a-1) = d/(c-1)$ the common value and assume it is an integer. Each matrix belonging to the submonoid generated by these two commuting matrices is of the form:

$$(4.1.) \qquad \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$$

with $r = y/(x-1)$ i.e. $y = rx - r$.

Consider a f.p.c.m. generated by the alphabet A that is the free product of the free commutative monoids generated by the subalphabets $A_1, A_2, \ldots A_n$ whose union is A. Set $m = \max(n, \max\{\mathrm{Card}(A_i) : i=1, \ldots n\})$ and denote by r_i the i-th prime integer. With every element of A associate an integer of the form:

$$(4.2.) \qquad k = r_1^{\varepsilon_1} r_2^{\varepsilon_2} \ldots r_m^{\varepsilon_m}$$

where $\varepsilon_i > 0$ for $i=1, \ldots, m$ in such a way that the vectors $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m)$ are linearly independent in $\mathbb{Q}$. A representation of the f.p.c.m. can be obtained by representing each letter a of A_i by a matrix of the form:

$$(4.3.) \qquad \begin{bmatrix} k & r_i k - r_i \\ 0 & 1 \end{bmatrix}$$

where r_i is the i-th prime integer and where k is the element associated with the letter a as in (4.2.). In particular the matrices associated with all letters of the subalphabet A_i generate a free commutative monoid as can be readily checked.

We shall verify that every matrix different from I belonging to the monoid generated by the matrices (4.3.) can be uniquely factorized as a product:

(4.4.) $$X_1X_2\ldots X_p$$

where for each $\ell = 1, \ldots, p$, X_ℓ is different from I and is a product of matrices representing elements of the same subalphabet A_i, while two consecutive factors X_ℓ and $X_{\ell+1}$ are products of matrices representing elements of two different subalphabets. Thus, X_ℓ is as follows:

(4.5.) $$X_\ell = \begin{bmatrix} k_\ell & r_{j_\ell} k_\ell & -r_{j_\ell} \\ & & \\ 0 & & 1 \end{bmatrix}$$

Identifying the matrix (4.1.) with the linear transformation of the projective line: $z \to x.z + y$, the linear transformation defined by the matrix (4.4.) assigns to z the value:

(4.6.) $$k_1k_2..k_p\, z + (-r_{\ell_1} + r_{\ell_1}k_1 - k_1r_{\ell_2}k_2 - k_1k_2r_{\ell_3} + \ldots + k_1k_2..k_{p-1}r_{\ell_p}k_p)$$

Assume that there exists a linear transformation of the form (4.4.) that has another factorization assigning to z the value:

(4.7.) $$t_1t_2\ldots t_q\, z + (-r_{g_1} + r_{g_1}t_1 - t_1r_{g_2}t_2 - t_1t_2r_{g_3} + \ldots + t_1t_2..t_{q-1}r_{g_q}t_q)$$

Furthermore assume that among all transformations with two factorizations, the coefficient of z is minimal. This implies:

(4.8.) $$k_1k_2..k_p = t_1t_2..t_q$$

and

(4.9.) $$-r_{\ell_1} + r_{\ell_1}k_1 - k_1r_{\ell_2}k_2 - k_1k_2r_{\ell_3} + \ldots + k_1k_2..k_{p-1}r_{\ell_p}k_p =$$
$$-r_{g_1} + r_{g_1}t_1 - t_1r_{g_2}t_2 - t_1t_2r_{g_3} + \ldots + t_1t_2..t_{q-1}r_{g_q}t_q$$

Because all k_ℓ's and t_ℓ's are divisible by all primes $r_1, r_2 \ldots r_m$, r_{ℓ_1} and r_{g_1} are equal. Assume k_1 and t_1 are different. By (4.2.) there exists a prime r_i, $i=1, \ldots, m$ and an integer $h>0$ such that k_1 say, is divisible by r_i^h by while t_1 is not. This proves that the first factor of the two decompositions (4.6.) and (4.7.) are equal, violating thus the minimality assumption on the coefficient of z. □

Finally we may state:

Theorem 4.2.

A free partially commutative monoid is representable by 2x2-matrices in $\mathbb{N}$ iff it is the direct product of a free commutative monoid with the free product of free commutative monoids.

Proof

The "only if" part was established in Proposition 3.4. It now suffices to prove that the direct product of a free commutative monoid generated by a alphabet A and of an arbitrary representable f.p.c.m. generated by an alphabet B disjoint from A is representable. This follows from the fact that we may assign to every letter in A a scalar matrix

$$\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$$

where the values of x are different primes that do not divide the determinants of the matrices representing the letters in B. □

5. References

[AL] Albert M. & Lawrence J., A proof of Ehrenfeucht's Conjecture, Theoretical Comput. Sci., 41, (1), 1985, pp. 121-123.

[Ch] Choffrut C., Free partially commutative monoids, Technical Report of the Laboratoire d'Informatique Théorique et de Programmation n°86.20, March 1986.

[Ei] Eilenberg S. , "Automata, Languages and Machines", Vol. A, Academic Press, 1974.

[Fo] Foata D., Etude de certains problèmes d'analyse combinatoire et du calcul des probabilités, Publ. Inst. Stat. Univ. Paris, 14, pp. 81-214

[Ga] Gantmacher F.R., "Matrizenrechnung", Teil I, VEB Deutscher Verlag der Wissenschaften, 1958.

[La] Lallement G., "Semigroups and combinatorial Applications", J. Wiley, New York, (1979).

[Ma] Magnus W., The use of 2 by 2 matrices in combinatorial group theory, Resultate der Mathematik, Vol. 4, (1981), pp. 171-192.