

J. L. LAMBERT

The local catenativity of DOL-sequences in free commutative monoids is decidable in the binary case

Informatique théorique et applications, tome 26, n° 5 (1992), p. 425-437

http://www.numdam.org/item?id=ITA_1992__26_5_425_0

© AFCET, 1992, tous droits réservés.

L'accès aux archives de la revue « Informatique théorique et applications » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

THE LOCAL CATENATIVITY OF DOL-SEQUENCES IN FREE COMMUTATIVE MONOIDS IS DECIDABLE IN THE BINARY CASE (*)

by J. L. LAMBERT ⁽¹⁾

Communicated by C. CHOFFRUT

Abstract. – Given a matrix $A \in \mathbb{Z}^{2 \times 2}$ and a vector $V_0 \in \mathbb{Z}^2$ we determine if there exists an integer m and m positive integers $a_{m-1} \dots a_0$ such that $A^m V_0 = \sum_{i=0}^{m-1} a_i A^i V_0$. When such an m exists, we compute the smallest one and m positive integers $a_{m-1} \dots a_0$ that satisfy the relation.

Keywords : DOL-Sequences; Commutative monoids.

Résumé. – Étant donné une matrice $A \in \mathbb{Z}^{2 \times 2}$ et un vecteur $V_0 \in \mathbb{Z}^2$ on détermine l'existence d'un entier m et de m autres entiers positifs $a_{m-1} \dots a_0$ tels que $A^m V_0 = \sum_{i=0}^{m-1} a_i A^i V_0$. Quand un tel m existe, on calcule le plus petit ainsi que les entiers $a_{m-1} \dots a_0$ qui satisfont la relation.

INTRODUCTION

The DOL sequences were introduced by Lindenmayer [3]. They are defined in a free monoid Σ^* (Σ being a finite alphabet) by a morphism $h: \Sigma^* \rightarrow \Sigma^*$ and an axiom $w \in \Sigma^*$; the DOL sequences is then the sequence $w, h(w), h^2(w), \dots, h^n(w), \dots$. Such a sequence in Σ^* is said locally catenative if there exists an integer m and some positive integers $i_0 \dots i_r$ smaller than m such that:

$$h^m(w) = h^{m-i_0}(w) \dots h^{m-i_r}(w)$$

(*) Received April 1991, revised October 1991.

A.M.S. 15A24, 15A36, 15A39, 20M14, 68Q45.

C.R. F.4.3.

This work was realised under the auspices of CNRS PRC Mathématiques et Informatique.

⁽¹⁾ Université de Paris-Nord, Centre Scientifique et Polytechnique, Département de Mathématiques et Informatique, Avenue Jean-Baptiste Clément, 93430 Villetaneuse, France.

C. Choffrut proved in [1] that when $\text{card}(\Sigma)=2$, then the local catenativity of DOL sequences is decidable since it is equivalent to $h^3(w) \in \{w, h(w), h^2(w)\}^*$. The problem of deciding if a given DOL sequence is catenative or not is still open.

In a free commutative monoid, the definition is easily extended. The morphism is given by a matrix $A \in \mathbb{N}^{n \times n}$ and the axiom is a vector $x \in \mathbb{N}^n$. The problem is then to determine if there exist an $m \in \mathbb{N}$ and m positive integers a_{m-1}, \dots, a_0 such that

$$A^m x = \sum_{i=0}^{m-1} a_i A^i x$$

The problem is then a decidability result concerning matrices with entries in \mathbb{N} ([4]).

In this article we will prove the decidability of this property when $n=2$ (the binary case). We will actually solve the more general problem:

Problem 1:

Instance: $V_0 \in \mathbb{Z}^2, A \in \mathbb{Z}^{2 \times 2}$

Question: Do there exist an integer $m \in \mathbb{N}$ and m positive integers a_{m-1}, \dots, a_0 such that

$$A^m V_0 = \sum_{i=0}^{m-1} a_i A^i V_0$$

We will prove that this problem is decidable and will compute the smallest m for which some integers a_{m-1}, \dots, a_0 satisfying the property exist.

1. TURNING THE PROBLEM INTO A PROBLEM CONCERNING POLYNOMIALS

In this section, we will express our initial problem 1 into a more suitable form and study it in any dimension. It is first clear that we can rewrite and

generalize the problem under the following form:

Problem 2:

Instance: $V_0 \in \mathbb{Z}^n, A \in \mathbb{Z}^{n \times n}$

Question: Does there exist a polynomial $P \in \mathbb{Z}[X]$ of degree m such that $P = X^m - \sum_{i=0}^{m-1} a_i X^i$ where $a_i \in \mathbb{N}$ for $0 \leq i \leq m-1$ and $P(A) V_0 = 0$?

We just recall that for a polynomial $P(X) = \sum_{i=0}^m a_i X^i$ and a matrix $A, P(A)$ is the matrix given by:

$$P(A) = \sum_{i=0}^m a_i A^i$$

A polynomial P of degree m such that $a_m = 1$ is said **monic**. We will denote by $\mathbb{Z}_1[X]$ the set of monic polynomials with coefficients in \mathbb{Z} .

We prove here that the monic polynomials of $\mathbb{Z}[X]$ that satisfy $P(A) V_0 = 0$ are the multiples of a computable monic polynomial P_0 of degree at most n . This property is a consequence of the classical Gauss' lemma on integer polynomials and Hamilton-Cayley theorem ([2]).

LEMMA 1 (Gauss' Lemma): *Let P and Q be two polynomials in $\mathbb{Z}[X]$ and denote by $C(P)$ the GCD of the coefficients of P then*

$$C(P \cdot Q) = C(P) \cdot C(Q)$$

LEMMA 2 (Hamilton-Cayley Theorem): *Let $A \in \mathbb{Z}^{n \times n}$ and let $K_A(X)$ be the characteristic polynomial of A :*

$$K_A(X) = \text{Det}(A - XI)$$

then $K_A(A) = 0$.

We will use Gauss' lemma under the following more convenient form:

LEMMA 3: *Let $P \in \mathbb{Z}[X]$ a monic polynomial. Then if $P = Q \cdot R$ where Q and R are monic polynomials of $\mathbb{Q}[X]$ then $Q \in \mathbb{Z}[X]$ and $R \in \mathbb{Z}[X]$.*

Proof. – Let $Q' = \lambda Q$ and $R' = \mu R$ where λ and μ are the least positive integers such that Q' and R' have integer coefficients. Then since Q is monic, $C(Q')$ divides λ (λ is the highest degree coefficient of Q') and then $C(Q') = 1$

since λ is minimal. Similarly, $C(R')=1$. Now

$$C(\lambda\mu P)=\lambda\mu=C(Q')C(R')=1$$

Thus $\lambda=\mu=1$ and $Q=Q'$, $R=R'$. \square

We are in position to prove the first proposition:

PROPOSITION 1: Let $V_0 \in \mathbb{Z}^n$, $A \in \mathbb{Z}^{n \times n}$. Define the set

$$I = \{ P \in \mathbb{Z}_1[X] / P(A)V_0 = 0 \}$$

Then we can compute a monic polynomial of degree at most n : $P_0 \in \mathbb{Z}[X]$. Such that:

$$I = P_0 \cdot \mathbb{Z}_1[X]$$

Proof: — Let $I' = \{ P \in \mathbb{Q}[X] / P(A)V_0 = 0 \}$. Then I' is an ideal over $\mathbb{Q}[X]$ which is a principal ring then there exists a monic polynomial $P_0 \in \mathbb{Q}[X]$ such that $I' = P_0 \mathbb{Q}[X]$.

By lemma 2, the monic polynomial $(-1)^n K_A(X)$ is in I' thus

$$(-1)^n K_A(X) = P_0 Q$$

which implies by lemma 3 that $P_0 \in \mathbb{Z}_1[X]$. Since P_0 is a divisor of $K_A(X)$, it is clear its degree is at most n and that there exist only a finite set of values for P_0 which can easily be computed.

Finally, Let $P \in I$, since $I \subset I'$:

$$P = P_0 Q$$

but since P is monic, $Q \in \mathbb{Z}_1[X]$ and $I = P_0 \mathbb{Z}_1[X]$. \square

With the help of proposition 1, one can see that problem 2 is decidable if the following one is:

Problem 3:

Instance: A polynomial $P_0 \in \mathbb{Z}[X]$ of degree at most n

Question: Does there exist a polynomial $Q \in \mathbb{Z}_1[X]$ such that

$$P_0 \cdot Q = X^m - \sum_{i=0}^{m-1} a_i X^i \quad \text{where } a_i \in \mathbb{N}$$

We now solve problem 3 in the case $n=2$.

2. SOLVING PROBLEM 3 FOR $n=2$, THE EASY CASES

Except in one case which is the most interesting one, problem 3 when $n=2$ is easy to solve. In this case the polynomial P_0 of proposition 3 has degree 1 or:

$$P_0(X) = X^2 - \text{Tr}(A)X + \text{Det}(A)$$

In this latter case the discussion will concern the signs of $\text{Tr}(A)$ and $\text{Det}(A)$. In the remainder of the paper a and b are positive integers.

1st case: P_0 has degree 1:

This means that V_0 is an eigenvalue of A .

If $P_0 = X - a$, let $Q = 1$ else if $P_0 = X + a$, then $Q = X - a$ works.

2nd case: $P_0 = X^2 - aX - b$:

$Q = 1$ is clearly suitable

3rd case: $P_0 = X^2 + aX + b, a \neq 0$:

Then for any large enough $\lambda \in \mathbb{N}$:

$$(X - \lambda)P_0 = X^3 + (a - \lambda)X^2 + (b - a\lambda)X - b\lambda$$

has the convenient form. Thus $Q = X - \lambda$ is suitable.

4th case: $P_0 = X^2 + aX - b, a \neq 0, b \neq 0$:

PROPOSITION 2: Let $P_0 = X^2 + aX - b$ where $(a, b) \in (\mathbb{N} - \{0\})^2$. Then there exists no polynomial $Q \in \mathbb{Z}_1[X]$ such that

$$P_0 \cdot Q = X^n - \sum_{i=0}^{m-1} \lambda_i X^i \quad \text{where } \lambda_i \in \mathbb{N}$$

Proof. - Let $Q = X^n + a_{n-1}X^{n-1} + \dots + a_0$. Then

$$\begin{aligned} P_0 \cdot Q &= (X^2 + aX - b)(X^n + a_{n-1}X^{n-1} + \dots + a_0) \\ &= X^{n+2} + (a + a_{n-1})X^{n+1} + (a_{n-2} + aa_{n-1} - b)X^n + \sum_{i=0}^{n-3} (a_i + aa_{i+1} - ba_{i+2})X^{i+2} \\ &\quad + (aa_0 - ba_1)X - ba_0 \end{aligned}$$

Now we want

$$\begin{aligned} -ba_0 &\leq 0 \\ aa_0 - ba_1 &\leq 0 \\ a_i + aa_{i+1} - ba_{i+2} &\leq 0 \quad \text{for } i=0, \dots, n-3 \end{aligned}$$

This implies directly that $a_0 \geq 0$ (since $b > 0$) and then $a_1 \geq 0$. By induction one has:

$$a_i \geq 0 \text{ and } a_{i+1} \geq 0 \Rightarrow a_{i+2} \geq 0$$

and thus $a_{n-1} \geq 0$ which gives $a + a_{n-1} \geq a > 0$. A contradiction. \square

We now deal with the interesting case $P_0 = X^2 - aX + b$.

3. PROBLEM 3: THE CASE $P_0 = X^2 - aX + b$, $b \neq 0$

3.1. The main result

PROPOSITION 3: *Let $P_0 = X^2 - aX + b$, $a \in \mathbb{N}$, $b \in \mathbb{N} - \{0\}$. Then there exists $Q \in \mathbb{Z}_1[X]$ such that*

$$P_0 \cdot Q = X^n - \sum_{i=0}^{n-1} \lambda_i X^i$$

with $\lambda_i \in \mathbb{N}$ iff P_0 has no root in \mathbb{R} .

Proof. – We first prove that the problem is equivalent to the existence of a non fully negative solution to a certain regular system of inequations. To check this existence, we use an easy criteria concerning the signs of the coefficients of a matrix. We compute that matrix and show that those coefficients are given by a linear recursion formula which the discussion is based on.

Let us look at a polynomial $Q = X^n + a_{n-1}X^{n-1} + \dots + a_0$ then

$$\begin{aligned} P_0 \cdot Q &= (X^2 - aX + b)(X^n + a_{n-1}X^{n-1} + \dots + a_0) \\ &= X^{n+2} + (a_{n-1} - a)X^{n+1} + (a_{n-2} - aa_{n-1} + b) + \sum_{i=0}^{n-3} (a_j - aa_{i+1} + ba_{i+2})X^{i+2} \\ &\quad + (ba_1 - aa_0)X + ba_0 \end{aligned}$$

We have to determine if there exists an integer n such that the system of inequation (I):

$$\begin{aligned}
 & ba_0 \leq 0 \\
 & -aa_0 + ba_1 \leq 0 \\
 & a_0 - aa_1 + ba_2 \leq 0 \\
 & \quad \ddots \\
 \text{(I)} \quad & a_i - aa_{i+1} + ba_{i+2} \leq 0 \\
 & \quad \ddots \\
 & a_{n-2} - aa_{n-1} + b \leq 0 \\
 & a_{n-1} - a \leq 0
 \end{aligned}$$

has a solution a_0, \dots, a_{n-1} in \mathbb{Z} .

We claim that this is equivalent to the existence of an integer n such that the system of equation (II):

$$\begin{aligned}
 & bx_0 \leq 0 \\
 & -ax_0 + bx_1 \leq 0 \\
 & x_0 - ax_1 + bx_2 \leq 0 \\
 & \quad \ddots \\
 \text{(II)} \quad & x_i - ax_{i+1} + bx_{i+2} \leq 0 \\
 & \quad \ddots \\
 & x_{n-2} - ax_{n-1} + bx_n \leq 0
 \end{aligned}$$

has a solution $(x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$ satisfying:

$$\exists i/x_i > 0.$$

First it is clear that if (a_0, \dots, a_{n-1}) is a solution of (I), then $x = (a_0, \dots, a_{n-1}, 1)$ is a solution of (II) with $x_n > 1$.

Conversely, let (x_0, \dots, x_n) be a solution of system (II) that satisfies $x_i > 0$. Since $bx_0 \leq 0$ and $b > 0$ one has $x_0 \leq 0$. Let x_{n_0} be the first x_i such that $x_{n_0} > 0$. By the previous remark, $n_0 > 0$.

Now we just have to check that $a_0 = x_0, \dots, a_{n_0-1} = x_{n_0-1}$ is a solution of system (I). The $n_0 - 1$ first inequations are satisfied and since

$$a_{n_0-2} - aa_{n_0-1} + b \leq x_{n_0-2} - ax_{n_0-1} + bx_{n_0} \leq 0$$

and

$$a_{n_0-1} - a \leq x_{n_0-1} \leq 0$$

all inequations of (I) are satisfied. This states the claim.

We will thus solve the latter problem. Let us define

$$A_n = \begin{pmatrix} b & & & & \\ -a & b & & & \\ 1-a & b & & & \\ & & \dots & & \\ & & & 1-a & b \end{pmatrix} \in \mathbb{Z}^{(n+1) \times (n+1)}$$

and for two vectors x, y in \mathbb{Z}^{n+1} :

$$x \leq y \Leftrightarrow \forall i, \quad 0 \leq i \leq n, \quad x_i \leq y_i$$

We have to determine if

$$\forall n \in \mathbb{N}, \quad \forall x \in \mathbb{Z}^{n+1}, \quad A_n x \leq 0 \Rightarrow x \leq 0$$

But this is clearly equivalent to

$$\forall n \in \mathbb{N}, A_n^{-1} \text{ is positive}$$

Now we easily compute that

$$A_n^{-1} = \begin{pmatrix} \frac{\alpha_0}{b} & & & & \\ \frac{\alpha_1}{b^2} & \frac{\alpha_0}{b} & & & \\ & & \dots & & \\ \frac{\alpha_n}{b^{n+1}} & \dots & \frac{\alpha_1}{b^2} & \frac{\alpha_0}{b} \end{pmatrix}$$

where $\alpha_0, \dots, \alpha_n$ is an integer sequence given by $\alpha_0 = 1, \alpha_1 = a$ and the recursion formula:

$$\alpha_n = a\alpha_{n-1} - b\alpha_{n-2}$$

The characteristic equation of the recursion is $P_0(X) = 0$.

We now have three cases.

1st case: P_0 has two distinct real roots. Let $\lambda_1 > \lambda_2 > 0$ be these roots. An elementary computation leads to the formula:

$$\alpha_n = \frac{(\lambda_1)^{n+1} - (\lambda_2)^{n+1}}{\sqrt{\Delta}} \quad (\Delta = a^2 - 4b)$$

and $\alpha_n > 0$ for every n , the problem has no solution.

2nd case: P_0 has an unique double root $\lambda = a/2$. The new formula is

$$\alpha_n = (n+1)(a/2)^n$$

then $\alpha_n > 0$ for every $n \in \mathbb{N}$, there is no solution either.

3rd case: P_0 has no root in \mathbb{R} then P_0 has two roots in \mathbb{C} : λ and $\bar{\lambda}$, we get the new formula:

$$\alpha_n = \frac{(\lambda)^{n+1} - (\bar{\lambda})^{n+1}}{i\sqrt{-\Delta}}$$

Let $\lambda = \rho e^{i\theta}$ then $\rho = \sqrt{b}$ and $\theta = \text{Arctan}(\sqrt{(4b/a^2) - 1})$ (if $a=0$ then $\theta = \pi/2$) and

$$\alpha_n = \frac{2\sqrt{b}^{n+1}}{\sqrt{-\Delta}} \sin(n+1)\theta$$

and $\alpha_n < 0$ as soon as $(n+1)\theta > \pi$ then for $n = [\pi/\text{Arctan}(\sqrt{(4b/a^2) - 1})]$ (where $[x]$ is the integer part of x) the problem has a solution of degree n . \square

3.2. Some examples

Let A be a 2×2 integer matrix such that $\text{Det}(A) > 0$ and $\text{Tr}(A) > 0$. When the matrix is positive, there is no solution since the characteristic equation has real roots. If we do not restrict the matrix A to be positive it is notable that even for matrices with coefficients of small size then the polynomial Q of proposition 3 can have a relatively high degree and surprisingly large size coefficients.

Before introducing some explicit examples, we note that it is easy to compute a polynomial Q satisfying the conclusion of proposition 3. Let X

and $a_{n-1} - a = -\alpha_{n-1} b - a$. Thus we get:

$$P_0 \cdot Q = X^{n+2} - (a + b\alpha_{n-1})X^{n+1} + (1 + \alpha_n)bX^n - b^{n+1}$$

Note that the computation of that polynomial is reduced to the computation of α_n and α_{n-1} by a simple linear recursion formula!

Now we can give some examples. We note that for matrices of the form:

$$A = \begin{pmatrix} a & -1 \\ 1 & a \end{pmatrix}$$

The characteristic polynomial is $X^2 - 2aX + a^2 + 1$ which discriminant is $\Delta = -4$. Thus the degree of the polynomial Q of lowest degree is:

$$n = \left\lceil \frac{\pi}{\text{Arctan}(\sqrt{1/a^2})} \right\rceil \geq [\pi a]$$

For example, if $a = 1$, the degree of Q is 4 since:

$$\alpha_0 = 1, \alpha_1 = 2, \alpha_2 = 2, \alpha_3 = 0, \alpha_4 = -4$$

The polynomial $Q = X^4 - 8X^2 - 16X - 16$ and

$$(X^4 - 8X^2 - 16X - 16)(X^2 - 2X + 2) = X^6 - 2X^5 - 6X^4 - 32$$

The size of the polynomial grows rapidly with a . For $a = 3$ for example, the formula gives $n \geq 9$. In fact $n = 9$ is the lowest degree as one can see by computing the sequence:

$$\begin{aligned} \alpha_0 &= 1 \\ \alpha_1 &= 6 \\ \alpha_2 &= 26 \\ \alpha_3 &= 96 \\ \alpha_4 &= 316 \\ \alpha_5 &= 936 \\ \alpha_6 &= 2456 \\ \alpha_7 &= 5376 \\ \alpha_8 &= 7696 \\ \alpha_9 &= -7584 \end{aligned}$$

Q is then a polynomial of surprisingly large size while $P_0 = X^2 - 6X + 10$:

$$Q = X^9 - 76\,960 X^8 - 537\,600 X^7 - 2\,456\,000 X^6 - 9\,360\,000 X^5 - 31\,600\,000 X^4 \\ - 96\,000\,000 X^3 - 260\,000\,000 X^2 - 600\,000\,000 X - 1\,000\,000\,000$$

and we get by the proved formula:

$$(X^2 - 6X + 10) \cdot Q = X^{11} - 76\,966 X^{10} - 75\,830 X^9 - 10\,000\,000\,000$$

The size of the obtained polynomials is the most surprising fact. If $a = 5$ then the degree of the polynomial is at least 15 with very big coefficients, for the following polynomial

$$X^2 - 200X + 10\,001 \quad (a = 100)$$

We must search for a polynomial of degree at least 314!

4. CONCLUSIONS

We now easily express the results of section 3 in terms of problem 1.

THEOREM 1: *Problem 1 has a solution except if V_0 is not an eigenvector of A and*

i) $\text{Tr}(A) < 0$, $\text{Det}(A) > 0$

or

ii) $\text{Tr}(A) > 0$, $\text{Det}(A) > 0$ and A has eigenvalues in \mathbb{R} .

Moreover the smallest value m satisfying the property can be determined in each case. If V_0 is an eigenvector of A then it is 1 if the eigenvalue is positive, 2 otherwise. If V_0 is not an eigenvector then the results are summed up in the following tableau:

	$\text{Det}(A) > 0$	$\text{Det}(A) < 0$	$\text{Det}(A) = 0$
$\text{Tr}(A) > 0$	n or imp.	2	2
$\text{Tr}(A) < 0$	3	imp.	3
$\text{Tr}(A) = 0$	4	2	2

$$\text{where } n = \left\lceil \frac{\pi}{\text{Arctan}(\sqrt{(4 \det(A)/\text{Tr}(A)^2) - 1})} \right\rceil + 2$$

In the case where A and V_0 are positive, the result is greatly simplified:

THEOREM 2: *In a commutative free monoid, a Dol sequence given by a matrix A and an axiom V_0 is locally catenative iff V_0 is an eigenvector of A or $\text{Det}(A) \leq 0$. In both cases one has:*

$$A^2 V_0 \in \{ A V_0, V_0 \}^*$$

CONCLUSION

The technique involved to solve the problem in the binary case can be in part generalized to solve the other cases. But the analysis of the sequence α_n will not be possible in the same way (but perhaps the decidability will remain true) and principally the particularity of sign that permits to deduce from a suitable non monic polynomial another monic polynomial with the same quality will not remain valid. The generalization is then not so clear.

ACKNOWLEDGEMENTS

I thank the anonymous referees for their help in improving the presentation and C. Choffrut who made me know about this problem.

REFERENCES

- 1 C. CHOFFRUT, Iterated substitutions and locally catenative systems: a decidability result in the binary case, *private communication*.
- 2 S. LANG, Algebra, Addison Wesley 1965.
- 3 A. LINDENMAYER, G. ROZENBERG, Developmental systems with locally catenative formulas, *Acta Informatica*, 2, 1973, pp. 214-248.
- 4 WEBER, SEIDL, On finite generated monoids of matrices with entries in \mathbb{N} , *RAIRO, Inf. Theor. Appl.*, 25, 1991, pp. 19-38.