RAIRO
INFORMATIQUE THÉORIQUE

K. RUOHONEN

# A note on equal powers of word morphisms

*RAIRO – Informatique théorique*, tome 11, n° 3 (1977), p. 207-211.

<http://www.numdam.org/item?id=ITA_1977__11_3_207_0>

R.A.I.R.O. Informatique théorique/Theoretical Computer Science
(vol. 11, n° 3, 1977 p. 207 à 211).

# A NOTE ON EQUAL POWERS OF WORD MORPHISMS (*)

by K. RUOHONEN (1)

Communicated by J. Berstel

Abstract. — *It is shown to be decidable of any given two word endomorphisms with nonsingular Parikh matrices whether or not they have common positive composite powers.*

## INTRODUCTION

We report here some progress towards a positive solution of the following decidability problem. Is there an algorithm which, given any two endomorphisms $e_1$ and $e_2$ on a finitely generated free monoid (word monoid), decides whether or not $e_1^n = e_2^n$ for some $n > 0$ (here $e_i^n$ denotes the $n$-fold composition of $e_i$)? We show that such an algorithm exists if we restrict ourselves to endomorphisms with nonsingular Parikh matrices (these are special kind of monomorphisms, see Theorem 2.6 in Ruohonen [4]). Our main tools are certain combinatorial word mappings introduced in Ruohonen [4].

## NOTATION

The free monoid generated by a finite set (alphabet) $A$ is denoted by $A^*$. The length of a word $P \in A^*$ is denoted by $|P|$. By $[P]$ we denote the Parikh vector of $P \in A^*$ which we get by listing the numbers of occurrences of symbols of $A$ in $P$ in some preassigned order. The Parikh matrix of an endomorphism $e$ on $A^*$ is then $\sum_{a \in A} [a]^T [e(a)]$ where $T$ denotes transpose. The cardinality of $A$ is denoted by $\# A$.

## RESULTS

We begin with a theorem on equal powers of integer matrices.

THEOREM 1 : *It is decidable, given arbitrary two $n \times n$-matrices $M$ and $L$ with integer entries, whether or not there exists an $m > 0$ such that $M^m = L^m$.*

(*) Received September 1976, Revised Nov. 1976.
(1) Mathematics Department, University of Turku, Finland.

*Proof* : Let $M = (m_{ij})$ and $L = (l_{ij})$. If $M^m = L^m$ then also $M^{km} = L^{km}$ for all $k > 0$. Thus, if $M^m = L^m$ and $m > 0$ is the smallest number satisfying this relation, the sequences

$$(1) \qquad r_{ij}^{(t)} = [(m_{i1}, \ldots m_{in})M^t - (l_{i1}, \ldots, l_{in})L^t]e_j \quad (t \geqslant 0),$$

where $e_j$ is an $n$-column vector the only nonzero entry of which is the $j^{th}$ one which has the value 1, have infinitely many common zero terms with period $m$, the first such zero term being the $m^{th}$ one. Let $M \otimes L$ be the direct product of $M$ and $L$. Then, by the Cayley-Hamilton Theorem, each of the $n^2$ sequences in (1) is governed by the linear recurrence equation $q(E)r_{ij}^{(t)} = 0$ $(t \geqslant 0)$ where $q$ is the characteristic polynomial of $M \otimes L$ and $E$ is the operator (operating on number theoretic functions) given by $(Ef)(t) = f(t + 1)$.

Since, as is well known, every set of nonnegative integers which is closed under addition is a finite union of arithmetic progressions we have

$$\{ t \mid r_{ij}^{(t)} = 0 \} = \left( \bigcup_{v=1}^{u_{ij}} \{ gs + b_{ij}^{(v)} \mid s \geqslant 0 \} \right) \cup F_{ij}$$

for some $g \geqslant 1$, $u_{ij} \geqslant 1$, $b_{ij}^{(v)} \geqslant 0$ and some set $F_{ij}$. We may assume that $g$ and $F_{ij}$ are the smallest possible. Then (cf. the proof of Theorem 2 in Berstel & Mignotte [1])

$$b_{ij}^{(v)} \leqslant y + g - 1$$

where $y$ is the number of zero eigenvalues of $M \otimes L$. Furthermore (Proposition 1 in Berstel & Mignotte [1]) $g$ divides

$h$ = l.c.m. { degree (ε) | ε is a primitive root of unity expressible as a quotient of two eigenvalues of $M \otimes L$ }.

We see that to check whether or not $M^m = L^m$ for some $m \geqslant 1$ it suffices to do this for $m = 1, \ldots, y + h$ whence the theorem follows. (A more explicit bound is given by e.g.

$$h \leqslant \exp(4(2n - y)\sqrt{10\log(2n - y)});$$

Corollary to Theorem 1 in Berstel & Mignotte [1].) □

REMARK 1 : In the sequel we use Theorem 1 only for nonsingular $M$ and $L$. In this case it suffices to check whether or not $M^m = L^m$ for some $1 \leqslant m \leqslant h$ as is seen.

LEMMA 1 : *Let* $\alpha_1, \ldots, \alpha_n$ *be real numbers and*

$$S = (\alpha_1 Z + \ldots + \alpha_n Z) \cap Q$$

*where* $Z$ *is the set of integers and* $Q$ *is the set of rationals. Then there exists a positive integer* $q$ *such that* $qx \in Z$ *for all* $x \in S$.

*Proof :* The set $S$ is a submodule of the finitely generated $Z$-module $\alpha_1 Z + \ldots + \alpha_n Z$. Thus $S$ is a finitely generated $Z$-module and the lemma follows when we take $q$ to be a common denominator of some numbers generating $S$. □

For our main result we recall some of our earlier results in Ruohonen [4]. Let $A$ be a finite alphabet. Then there is a sequence $\theta_i : A^* \to N^{p_i}$ $(i \geqslant 0)$ of mappings, where $p_i = \#A + \ldots + \#A^{i+1}$, such that $P = Q$ whenever $\theta_j(P) = \theta_j(Q)$ and $2j \geqslant |P|, |Q|$ (here $N$ denotes the set of nonnegative integers). Especially, $\theta_0$ is the Parikh mapping, i.e. $\theta_0(P) = [P]$. Moreover, for each endomorphism $e$ on $A^*$ there exists a sequence $(\Gamma_i)$ of integer matrices such that

(i) $\Gamma_i$ is of size $p_i \times p_i$;

(ii) $\theta_i(e(P)) = \theta_i(P)\Gamma_i$ for all $P \in A^*$;

(iii) $\Gamma_0$ equals the Parikh matrix of $e$;

(iv) $\Gamma_{i+1} = \left(\begin{array}{c|c} \Gamma_i & \overline{\Gamma}_{i+1} \\ \hline 0 & \Gamma_0^{(i+1)} \end{array}\right)$ where $\Gamma_0^{(i+1)}$ is the $(i+1)^{st}$ Kronecker power of $\Gamma_0$, $\overline{\Gamma}_{i+1}$ is an integer matrix and 0 is a zero matrix of appropriate size;

(v) for each $a \in A$, $\theta_i(e(a))$ appears as a (fixed) row in $\Gamma_i$.

By (v) $\Gamma_i$ completely determines $e$ for $2i \geqslant \max_{a \in A} \{ |e(a)| \}$. *By* (iii) and (iv) the eigenvalues of $\Gamma_i$ consist of all products of the form $\prod_{j=1}^{u} \gamma_j$ where $1 \leqslant u \leqslant i+1$ and $\gamma_j$ are eigenvalues of $\Gamma_0$. We will not give here the somewhat complicated definition of $\theta_i$ but refer instead to Ruohonen [4]. It should be stressed that $\theta_i$ as well as $\Gamma_i$ can be effectively obtained.

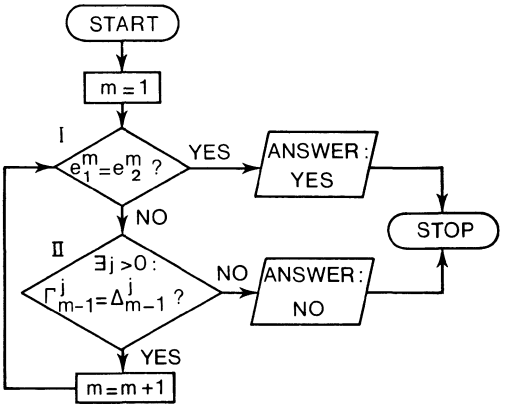
THEOREM 2 : *It is decidable, given arbitrary two endomorphisms $e_1$ and $e_2$ on $A^*$ with nonsingular Parikh matrices, whether or not there exists an $n > 0$ such that $e_1^n = e_2^n$.*

*Proof :* Let $(\Gamma_i)$ and $(\Delta_i)$ be the matrix sequences corresponding to $e_1$ and $e_2$, respectively, as described above. For any quotient $\frac{\alpha}{\beta}$ where $\alpha$ and $\beta \neq 0$ are eigenvalues of $\Gamma_i \otimes \Delta_i$, the argument of $\frac{\alpha}{\beta}$ is a linear combination of arguments of eigenvalues of $\Gamma_0 \otimes \Delta_0$ with nonnegative integer coefficients. It follows from Lemma 1 that the nondecreasing sequence $(c_i)$ where $c_i$ is the l.c.m. of the degrees of primitive roots of unity expressible as quotients of eigenvalues of $\Gamma_i \otimes \Delta_i$ is bounded. Let $c = \max \{ c_0, c_1, \ldots \}$.

Assume that for each $i \geqslant 0$ there exists an $n_i > 0$ such that $\Gamma_i^{n_i} = \Delta_i^{n_i}$. By Remark 1 we may assume that the sequence $(n_i)$ is bounded, indeed we may assume that $n_i \leqslant c$ for $i \geqslant 0$. Let

$$2i \geqslant \max_{a \in A} \{ |e_1^c(a)|, |e_2^c(a)| \}.$$

Since $\Gamma_i^s = \Delta_i^s$ for some $s \leqslant c$ and $\Gamma_i^s$ and $\Delta_i^s$ completely determine $e_1^s$ and $e_2^s$ it must be the case that $e_1^s = e_2^s$. Thus there exist numbers $n_i > 0$ such that $\Gamma_i^{n_i} = \Delta_i^{n_i}$ if and only if there exists a number $s > 0$ such that $e_1^s = e_2^s$ (the reverse implication is of course trivial by (ii)). Our decision algorithm now works as shown in the following flow diagram.




The decision in I is trivial. The decision in II can be done by Theorem 1. □

In the above proof we do not need the effective calculability of the bound $c$, only its existence guaranteed by the ineffective Lemma 1. Using field theory we obtain further information (e.g. effective calculability) of such a bound. Indeed, let $K$ be the field which we get by adjoining the eigenvalues of $\Gamma_0 \otimes \Delta_0$ to $Q$. Then the degree $[K : Q]$ does not exceed $(2 \# A)!$. The eigenvalues of $\Gamma_i \otimes \Delta_i$ are in $K$ as well as their quotients. If $K$ contains a primitive root of unity of degree $r$, then $\varphi(r)$ divides $[K : Q]$ and thus $\varphi(r) \leqslant (2 \# A)!$ (here $\varphi$ is Euler's totient function). (See e.g. Borevich & Shafarevich [2].) Hence $c$ can be replaced by $d$ which is the largest number such that $\varphi(d) \leqslant (2 \# A)!$.

Such a number exists, we have e.g.

$$\varphi(n) > \frac{bn}{\log \log n} \quad (n > 3)$$

for some positive constant $b$ (see Theorem 6-26 in Le Veque [3]). However, these numbers are large and grow rapidly with respect to $\# A$, for instance, for $\# A = 2$ we have $d = 90$.

REMARK 2 : A generalization of our methods to prove the above kind of results for endomorphisms (or even monomorphisms) with singular Parikh matrices does not seem to be expectable. For instance, let the monomorphisms $e_1$ and $e_2$ on $\{ a, b \}^*$ be given by

$$e_1(a) = ab \quad , \quad e_1(b) = ba \quad , \quad e_2(a) = ba \quad , \quad e_2(b) = ab.$$

The common Parikh matrix of these monomorphisms is $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ the eigenvalues of which are 0 and 2. If our above results were to extend to this case then $e_1^n \neq e_2^n$ for $n > 0$ since $e_1 \neq e_2$ and the eigenvalues are nonnegative. However, $e_1^2 = e_2^2$.

*Acknowledgement :* I would like thank an anonymous referee for his comments which helped to simplify an earlier version of this note.

## REFERENCES

1. J. BERSTEL et M. MIGNOTTE, *Deux propriétés décidables des suites récurrentes linéaires*, Bulletin de la Société Mathématique de France, 104, 1976, 175-184.
2. Z. I. BOREVICH and I. R. SHAFAREVICH, *Number Theory*, Academic Press, New York & London, 1966.
3. W. J. LE VEQUE, *Topics in Number Theory I*, Addison-Wesley Publ. Co., Reading, Mass., 1956.
4. K. RUOHONEN, *Some combinatorial mappings of words.* Annales Academiae Scientiarum Fennicae, Series A.I., Mathematicae, Dissertationes, 9, 1976.