INFORMATIQUE THÉORIQUE ET APPLICATIONS

T. HARJU
N. W. KEESMAAT
H. C. M. KLEIJN

The intersection problem for alphabetic vector monoids

Informatique théorique et applications, tome 28, nº 3-4 (1994), p. 295-301
<http://www.numdam.org/item?id=ITA_1994__28_3-4_295_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 28, n° 3-4, 1994, p. 295 à 301)

THE INTERSECTION PROBLEM FOR ALPHABETIC VECTOR MONOIDS

by T. HARJU (1), N. W. KEESMAAT (2) and H. C. M. KLEIJN (3)

Abstract. – *Let* Σ *and* Γ *be two vector alphabets consisting of alphabetic vectors* (a_1, a_2), *where* $a_1, a_2 \in A \cup \{\varepsilon\}$ *for an alphabet A. We show that it is decidable whether or not* $\Sigma^{\otimes} \cap \Gamma^{\otimes}$ *is the trivial submonoid of the direct product* $A^* \times A^*$ *for the generated submonoids* $\Sigma^{\otimes}$ *and* $\Gamma^{\otimes}$. *On the other hand we show that a simple version, obtained from letter-to-letter homomorphisms, of the modified Post Correspondence Problem is undecidable for alphabetic vectors.*

1. INTRODUCTION

Let A be a finite alphabet. Denote by A^* the free monoid generated by A, and let $A^* \times A^* = \{(u_1, u_2) | u_i \in A^*\}$ be the direct product of A^* with itself. Each element $u = (u_1, u_2)$ is called a *vector* over A^*. For a subset $\Sigma \subseteq A^* \times A^*$ we let $\Sigma^{\otimes}$ be the submonoid of $A^* \times A^*$ generated by Σ. The identity of $\Sigma^{\otimes}$ is $\epsilon = (\varepsilon, \varepsilon)$, where ε is the empty word of A^*.

Further, let Σ^* denote the free monoid generated by the vectors from Σ. In this case Σ is considered to be an alphabet and hence each element $u = (u_{11}, u_{12}) \dots (u_{k1}, u_{k2})$ of Σ^* is just a word of vectors.

We shall consider the *intersection problem* for the submonoids of $A^* \times A^*$, *i. e.*, whether or not $\Sigma^{\otimes} \cap \Gamma^{\otimes} = \{\epsilon\}$ for the submonoids $\Sigma^{\otimes}$ and $\Gamma^{\otimes}$ generated by the given subsets Σ and Γ of $A^* \times A^*$, respectively. The pair (Σ, Γ) is refered to as an *instance* of the intersection problem.

We observe that in general the intersection problem is undecidable, because for a pair of homomorphisms (α, β), $\alpha, \beta : B^* \to C^*$, we choose $A = B \cup C$

The authors are in debt to BRA Working Group 6317 ASMICS for its support.
(1) Dept. of Mathematics, University of Turku, SF-20500 Turku, Finland.
(2) PTT Research, P.O. Box 421, 2260 AK Leidschendam, The Netherlands.
(3) Dept. of Computer Science, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands.

and define the generator sets as follows: $\Sigma = \{(a, \alpha(a)) | a \in B\}$ and $\Gamma = \{(a, \beta(a)) | a \in B\}$. Clearly, now $\Sigma^{\otimes} \cap \Gamma^{\otimes} \neq \{\epsilon\}$ if and only if the instance (α, β) of Post Correspondence Problem (PCP) has a solution.

We shall now restrict the instantes (Σ, Γ) to cases, where the vectors are alphabetic. A vector $u = (u_1, u_2) \in A^* \times A^*$ is called *alphabetic*, if each of its components u_i is either a letter or the empty word $\varepsilon : u_i \in A \cup \{\varepsilon\}$. In particular, the identity $\epsilon = (\varepsilon, \varepsilon)$ of $A^* \times A^*$ is an alphabetic vector.

Let $\Delta(A)$ denote the set of all alphabetic vectors over A^*. Notice that here $\Delta(A)^{\otimes} = A^* \times A^*$, because the alphabetic vectors clearly generate $A^* \times A^*$. We say that $\Sigma^{\otimes}$ is an *alphabetic submonoid of* $A^* \times A^*$,if $\Sigma \subseteq \Delta(A)$.

Let $h_A : \Delta(A)^* \to A^* \times A^*$ be the monoid homomorphism defined by $h_A(a_1, a_2) = (a_1, a_2)$ for all $(a_1, a_2) \in \Delta(A)$. We shall write $u \equiv v$ for the words $u, v \in \Delta(A)^*$, if they produce the same element of the direct product, *i. e.*, if $h_A(u) = h_A(v)$. Thus given two sets Σ and Γ of alphabetic vectors, the problem is to determine whether or not there exists a pair $(u, v) \in \Sigma^* \times \Gamma^*$ such that $u \equiv v$. Such a pair (u, v) will be referred to as a *solution* of the instance (Σ, Γ).

Alphabetic submonoids occur in, e. g., [1], [3], [4], (*see* also their references for related work) where concurrent systems with a vector synchronization mechanism are studied. Such a concurrent system consists of a fixed, say n, number of sequential processes together with a control on their mutual synchronization. We shall now discuss only the simplest of these cases, $n = 2$.

The behaviour of the i-th sequential process is given as a language L_i over some alphabet A of actions. The basic units of the synchronization are alphabetic vectors which express which actions can be performed simultaneously in the system. These *synchronization vectors* form a set Σ. If Σ^* is used as the synchronization mechanism, then the valid concurrent computations of the system are those combinations (w_1, w_2) of computations $w_i \in L_i$ which have a decomposition in Σ^*: there is a $v \in \Sigma^*$ such that $h_A(v) = (w_1, w_2)$. Or, to put it differently, the set of concurrent computations is $(L_1 \times L_2) \cap \Sigma^{\otimes}$. If another set Γ of synchronization vectors is used, the question arises whether or not the new and the old system have common computations: is $(L_1 \times L_2) \cap (\Sigma^{\otimes} \cap \Gamma^{\otimes})$ nontrivial? Again this question is undecidable by a reduction from PCP, even in the case that the sets L_i are regular languages. To see this, let (α, β) be a pair of homomorphisms $\alpha, \beta : B^* \to C^*$ with B and C disjoint. Let $A = B \cup C$, and set $L_1 = \{b\alpha(b) | b \in B\}^*$ and

$L_2 = \{b\beta(b) | b \in B\}^*$, $\Sigma = \{(b, b) | b \in B\} \cup \{(c, \varepsilon), (\varepsilon, c) | c \in C\}$, and $\Gamma = \{(c, c) | c \in C\} \cup \{(b, \varepsilon), (\varepsilon, b) | b \in B\}$. Clearly, the instance (α, β) of PCP has a solution if and only if $(L_1 \times L_2) \cap (\Sigma^{\otimes} \cap \Gamma^{\otimes}) \neq \{\varepsilon\}$.

In this reduction the languages L_1 and L_2 play a crucial role. If we assume that they both are A^*, then we are asking whether or not $\Sigma^{\otimes}$ and $\Gamma^{\otimes}$ have a non-trivial intersection. This is the question considered in this paper.

In Setion 2 we shall prove that the intersection problem is decidable for alphabetic submonoids: Given two alphabetic submonoids $\Sigma^{\otimes}$ and $\Gamma^{\otimes}$ of $A^* \times A^*$, the problem whether or not $\Sigma^{\otimes} \cap \Gamma^{\otimes} = \{\epsilon\}$ is decidable.

An easy consequence of this result is that PCP is decidable when restricted to instances (α, β), where α and β are weak codings, *i. e.*, $\alpha, \beta : X^* \to A^*$ are such that $\alpha(a), \beta(a) \in A \cup \{\varepsilon\}$ for all a in X.

In Section 3 we consider the following variant of PCP: let $\alpha, \beta : X^* \to \Delta(A)^*$ be two homomorphisms that are letter-to-letter, *i. e.*, for each letter $a \in X$, $\alpha(a)$ and $\beta(a)$ are alphabetic vectors. Let $x, y \in X$ be two distinguished *border letters*. In the *alphabetic bordered* PCP we ask whether or not there exists a word $w = xuy$ in X^* with $u \in (X \setminus \{x, y\})^*$ such that $\alpha(w) \equiv \beta(w)$. This problem is shown to be undecidable and thus contrasts with the result from Section 2.

2. THE INTERSECTION PROBLEM IS DECIDABLE

In this section we prove

THEOREM 1: *Let A be a finite alphabet. Given two alphabetic submonoids $\Sigma^{\otimes}$ and $\Gamma^{\otimes}$ of $A^* \times A^*$, the problem whether or not $\Sigma^{\otimes} \cap \Gamma^{\otimes} = \{\epsilon\}$ is decidable.*

Let us fix two alphabetic submonoids $\Sigma^{\otimes}$ and $\Gamma^{\otimes}$ of $A^* \times A^*$. We shall show that $\Sigma^{\otimes} \cap \Gamma^{\otimes} \neq \{\epsilon\}$ if and only if there is a solution (u, v) for the instance (Σ, Γ) such that the length $|u|$ of u is at most the cardinality $|\Sigma|$ of Σ.

We can clearly assume that $(\varepsilon, \varepsilon) \notin \Sigma \cup \Gamma$, and further that $\Sigma \cap \Gamma = \emptyset$, for otherwise we can check trivially that $\Sigma^{\otimes} \cap \Gamma^{\otimes} \neq \{\epsilon\}$.

Suppose that $u \equiv v$ is a nontrivial solution for $u \in \Sigma^*$ and $v \in \Gamma^*$ with $u, v \neq \epsilon$. We let

$$u = (a_1, b_1)(a_2, b_2) \dots (a_k, b_k) \quad \text{and} \quad v = (c_1, d_1)(c_2, d_2) \dots (c_t, d_t)$$

for $(a_i, b_i) \in \Sigma$ and $(c_i, d_i) \in \Gamma$. Assume further that u is of minimal length, that is, the number $k \geq 1$ of components of u is as small as possible.

First of all we can restrict the components of u as follows:

(1) $a_1 \neq \varepsilon$. Indeed, if $a_1 = \varepsilon$, then $b_1 \neq \varepsilon$ and we can consider the generators $\Sigma^{-1} = \{(b, a) | (a, b) \in \Sigma\}$ and $\Gamma^{-1} = \{(b, a) | (a, b) \in \Gamma\}$ instead of Σ and Γ, respectively. Clearly, $\Sigma^{\otimes} \cap \Gamma^{\otimes} \neq \{\epsilon\}$ if and only if $(\Sigma^{-1})^{\otimes} \cap (\Gamma^{-1})^{\otimes} \neq \{\epsilon\}$.

(2) $b_1 = \varepsilon$. Indeed, if $b_1 \neq \varepsilon$, then the first decomposing vector $v_1 = (c_1, d_1)$ for v would have to be either (a_1, ε) or (ε, b_1), since $(a_1, b_1) \in \Sigma$ and $\Sigma \cap \Gamma = \varnothing$. In the former of these cases, we may exchange Σ and Γ, and in the latter case we interchange Σ to Γ^{-1} and Γ to Σ^{-1} in order for (1) and (2) to be satisfied.

Now, since

$$h_A(u) = (a_1 a_2 \ldots a_k, b_1 b_2 \ldots b_k) = (c_1 c_2 \ldots c_t, d_1 d_2 \ldots d_t) = h_A(v),$$

there are order preserving bijections $\alpha : \{i | a_i \neq \varepsilon\} \to \{i | c_i \neq \varepsilon\}$ and $\beta : \{i | d_i \neq \varepsilon\} \to \{i | b_i \neq \varepsilon\}$ such that $a_i = c_{\alpha(i)}$ and $d_i = b_{\beta(i)}$.

Consider the word

$$\begin{aligned} w = {} & (a_1, b_{\beta\alpha(1)}) (a_{\beta\alpha(1)}, b_{(\beta\alpha)^2(1)}) \\ & \ldots (a_{(\beta\alpha)^i(1)}, b_{(\beta\alpha)^{i+1}(1)}) \ldots (a_{(\beta\alpha)^{r-1}(1)}, b_{(\beta\alpha)^r(1)}) \end{aligned}$$

obtained from a_1 by repeating the functions α and β until either of them becomes undefined, *i. e.*, until

(*a*) $a_{(\beta\alpha)^r(1)} = \varepsilon$, or

(*b*) $d_{\alpha(\beta\alpha)^r(1)} = \varepsilon$.

Notice that since α and β are order preserving bijections and $(a_1, b_1) \neq (c_1, d_1)$, the exponent r is always well-defined in above.

A pictorial representation of forming this word in Case (*a*) is given in figure 1.

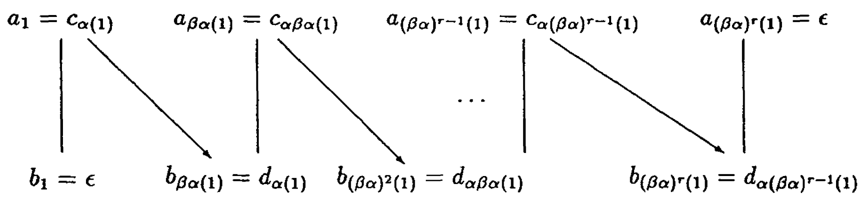

Figure 1.

Now, by the definitions of the bijections α and β,

$$w = (c_{\alpha(1)}, d_{\alpha(1)})(c_{\alpha\beta\alpha(1)}, d_{\alpha\beta\alpha(1)}) \dots (c_{\alpha(\beta\alpha)^{r-1}(1)}, d_{\alpha(\beta\alpha)^{r-1}(1)}),$$

and hence $w \in \Gamma^*$.

We shall first consider Case (a). For this define

$$w_a = (a_1, \varepsilon)(a_{\beta\alpha(1)}, b_{\beta\alpha(1)}) \dots (a_{(\beta\alpha)^{r-1}(1)}, b_{(\beta\alpha)^{r-1}(1)}) \dots (\varepsilon, b_{(\beta\alpha)^r(1)}).$$

We have $w_a \in \Sigma^*$ and, moreover, $\omega_a \equiv w$. Thus in this case $h_A(w_a) \in \Sigma^\otimes \cap \Gamma^\otimes$ gives also a solution.

By the minimality assumption for u, it follows that $u = w_a$, and hence that $\alpha(i) = i$ and $\beta(i) = i + 1$, *i. e.*,

$$u = (a_1, \varepsilon)(a_2, b_2) \dots (a_{k-1}, b_{k-1})(\varepsilon, b_k),$$
$$v = (a_1, b_2)(a_2, b_3) \dots (a_{k-1}, b_k)$$

for nonempty letters $a_i, b_i \in A$.

Similarly, in Case (b) for the word

$$w_b = (a_1, \varepsilon)(a_{\beta\alpha(1)}, b_{\beta\alpha(1)}) \dots (a_{(\beta\alpha)^{r-1}(1)}, b_{(\beta\alpha)^{r-1}(1)})(a_{(\beta\alpha)^r(1)}, b_{(\beta\alpha)^r(1)}),$$

we have $h_A(w_b) \in \Sigma^\otimes \cap \Gamma^\otimes$. In this case, we obtain that

$$u = (a_1, \varepsilon)(a_2, b_2) \dots (a_{k-1}, b_{k-1})(a_k, b_k),$$
$$v = (a_1, b_2)(a_2, b_3) \dots (a_{k-1}, b_k)(a_k, \varepsilon)$$

for nonempty letters $a_i, b_i \in A$.

In both of these cases it is easy to see that if $u = w_1 \cdot (a_i, b_i) \cdot w_2 \cdot (a_j, b_j) \cdot w_3$, where $(a_i, b_i) = (a_j, b_j)$ for some indices i, j with $i < j$, then $w_1(a_i, b_i) w_3$ provides another solution. We deduce from this that a minimal solution u has length at most the cardinality of the alphabet Σ. This shows that it is decidable whether or not $\Sigma^\otimes \cap \Gamma^\otimes = \{\epsilon\}$, and hence Theorem 1 is proved.

3. UNDECIDABILITY OF ALPHABETIC BORDERED PCP

In the proof of the undecidability of the alphabetic bordered PCP we use the following modification of Post's Correspondence Problem.

Let $\alpha, \beta : X^* \to X^*$ be two nonerasing homomorphisms for an alphabet X, We shall say the pair (α, β) is a *bordered instance*, if there are two special letter $c, d \in X$ such that for $B = X \setminus \{c, d\}$,

$$\alpha(c),\ \beta(c) \in c \cdot B^* \quad \text{and} \quad \alpha(d),\ \beta(d) \in B^* \cdot d,$$
$$\alpha(a),\ \beta(a) \in B^* \quad (a \in B).$$

LEMMA: *It is undecidable whether or not there exists a word $w \in B^*$ such that $\alpha(cwd) = \beta(cwd)$ for a given bordered instance (α, β) of homomorphisms.*

The proof is standard, *see* [2] and omitted here.

We now prove

THEOREM 2: *The alphabetic bordered PCP is undecidable.*

Let then (α, β) be a bordered instance of homomorphisms as above. Set $X = \{a_1, a_2, \ldots, a_N\}$, where $a_1 = c$, $a_N = d$ and $B = \{a_2, \ldots, a_{N-1}\}$. Define

$$M = \max\{|\alpha(a_i)|,\ |\beta(a_i)| \quad |i = 1, 2, \ldots, N\},$$

and write $\alpha(a_i) = \alpha_{i1}\alpha_{i2}\ldots\alpha_{iM}$ and $\beta(a_j) = \beta_{j1}\beta_{j2}\ldots\beta_{jM}$, where α_{ij}, $\beta_{ij} \in X \cup \{\varepsilon\}$ and $\alpha_{11} = c = \beta_{11}$, $\alpha_{NM} = d = \beta_{NM}$. Clearly, we may assume that $M > 1$.

Further, let

$$D_1 = \{[i, j] \mid 1 \leqq i \leqq N,\ 1 \leqq j \leqq M\},$$
$$D_2 = \{[i, j],\ [i, 1, k] \mid 1 \leqq i,\ k \leqq N,\ 2 \leqq j \leqq M\}$$

be two new alphabets. Our basic alphabed for the components of the vectors will be $A = X \cup D_1$. Define two homomorphisms $\alpha_1, \beta_1 : D_2^* \to \Delta(A)^*$ as follows:

$$\alpha_1([1, 1, 1]) = (\alpha_{11}, \varepsilon),$$
$$\alpha_1([i, 1, k]) = (a_{i1}, [k, M]), \qquad (i \neq 1),$$
$$\alpha_1([i, j]) = (\alpha_{ij}, [i, j-1]), \qquad ((i, j) \neq (1, 1)),$$

and

$$\beta_1([i, 1, k]) = (\beta_{i1}, [i, 1]),$$
$$\beta_1([i, j]) = (\beta_{ij}, [i, j]), \quad ((i, j) \neq (N, M)),$$
$$\beta_1([N, M]) = (\beta_{NM}, \varepsilon).$$

Clearly, both of these homomorphisms map letters to alphabetic vectors, *i. e.*, they are letter-to-letter homomorphisms.

Consider the instance (α_1, β_1) with border letters [1, 1, 1] and [*N, M*], and define for each word $w = a_1 a_{i_1} \ldots a_{i_m} a_N \in cB^* d$, the word $\tau(w) = u_1 u_{i_1} \ldots u_{i_m} u_N$, where

$$u_1 = [1, 1, 1]\,[1, 2] \ldots [1, M], \qquad u_N = [N, 1, i_m]\,[N, 2] \ldots [N, M]$$
$$u_{ij} = [i_j, 1, i_{j-1}]\,[i_j, 2] \ldots [i_j, M].$$

We observe that

$$\alpha_1(u_1) \equiv (\alpha(a_1), [1, 1] \ldots [1, M-1]),$$
$$\beta_1(u_1) \equiv (\beta(a_1), [1, 1] \ldots [1, M]),$$
$$\alpha_1(u_{i_j}) \equiv (\alpha(a_{i_j}), [i_{j-1}, M]\,[i_j, 1] \ldots [i_j, M-1]),$$
$$\beta_1(u_{i_j}) \equiv (\beta(a_{i_j}), [i_j, 1]\,[i_j, 2] \ldots [i_j, M]),$$
$$\alpha_1(u_N) \equiv (\alpha(a_N), [i_m, M] \ldots [N, 1], [N, M-1]),$$
$$\beta_1(u_N) \equiv (\beta(a_N), [N, 1]\,[N, 2] \ldots [N, M-1]).$$

From these it is now straightforward to show that for all $u \in cB^* d$, $\alpha(u) = \beta(u)$ if and only if $\alpha_1(\tau(u)) \equiv \beta_1(\tau(u))$. Moreover, if v is a solution to the instance (α_1, β_1) of the alphabetic bordered PCP, then one can easily construct a word $u \in cB^* d$ such that $v = \tau(u)$. This proves Theorem 2.

REFERENCES

1. A. Arnold, Synchronized Behaviours of Processes and Rational relations, *Acta Informatica*, 1982, *17*, pp. 21-29.
2. J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages and Computation, Addison-Wesley*, Reading, Mass., 1979.
3. N. W. Keesmaat, H. C. M. Kleijn, The Effect of Vector Synchronization: Residue and Loss, *Lectures Notes in Comput. Sci.*, 1992, *609*, pp. 215-250.
4. N. W. Keesmaat, H. C. M. Kleijn and G. Rozenberg, Vector Controlled Concurrent Systems, Part I: Basic Classes, *Fundamenta Informaticae*, 1990, *13*, pp. 275-316.